UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Frederico Schardong

Pioneering the Future of Electronic Identity: From Post-Quantum Cryptography to Fiduciary Principles

Florianópolis
2024

Frederico Schardong

Pioneering the Future of Electronic Identity: From Post-Quantum Cryptography to Fiduciary Principles

Tese submetida ao Programa de Pós-Graduação em Ciência da Computação para a obtenção do título de doutor em Ciência da Computação.
Orientador: Prof. Ricardo Custódio, Dr.

Florianópolis
2024

Ficha catalográfica gerada por meio de sistema automatizado gerenciado pela BU/UFSC.
Dados inseridos pelo próprio autor.

Schardong, Frederico
Pioneering the Future of Electronic Identity: From Post Quantum Cryptography to Fiduciary Principles / Frederico Schardong ; orientador, Ricardo Felipe Custódio, 2024.
188 p.

Tese (doutorado) - Universidade Federal de Santa Catarina, Centro Tecnológico, Programa de Pós-Graduação em Ciência da Computação, Florianópolis, 2024.

Inclui referências.

1. Ciência da Computação. 2. Identidade Digital. 3. Gestão de Identidade. 4. Criptografia Pós-Quântica. 5. Identidade Autossoberana. I. Custódio, Ricardo Felipe. II. Universidade Federal de Santa Catarina. Programa de Pós Graduação em Ciência da Computação. III. Título.

Frederico Schardong

Pioneering the Future of Electronic Identity:
From Post-Quantum Cryptography to Fiduciary Principles

O presente trabalho em nível de doutorado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Profa. Carla Merkle Westphall, Dra.
Universidade Federal de Santa Catarina

Prof. Arlindo Flávio da Conceição, Dr.
Universidade Federal de São Paulo

Prof. Marco Aurélio Amaral Henriques, Dr.
Universidade Estadual de Campinas

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de doutor em Ciência da Computação.

ICP-Edu
Documento assinado digitalmente
Marcio Bastos Castro
Data: 26/08/2024 18:47:15-0300
CPF: ***.707.720-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Márcio Bastos Castro, Dr
Coordenador do Programa

ICP-Edu
Documento assinado digitalmente
Ricardo Felipe Custodio
Data: 26/08/2024 17:24:19-0300
CPF: ***.981.609-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Ricardo Custódio, Dr.
Orientador

Florianópolis, 2024.

To all the giants on whose shoulders I stood, allowing me to see farther.

ACKNOWLEDGEMENTS

Agradeço, primeiramente, ao exímio professor Ricardo Custódio, que brilhantemente motivou-me a questionar. Seus ensinamentos e orientações me possibilitaram realizações que antes eram inimagináveis.

Agradeço também a minha noiva, Geovana Paixão Tegon, pelo companheirismo, paciência e compaixão durante os anos de doutoramento. Agradeço o apoio incondicional que sempre recebi dos meus pais, Valnir Schardong e Vera Schardong, que muito abdicaram para que seus filhos pudessem estudar. Agradeço aos meus irmãos, Gustavo Schardong e Marcelo Schardong, que sempre estiveram à disposição para me ajudar em tudo que precisei.

Também deixo meus agradecimentos aos outros docentes do Laboratório de Segurança em Computação, Professores Jean, Thaís e Martín. Todos me propiciaram importantes aprendizados e contribuições. Agradeço também os colegas discentes pelos importantes momentos de trocas. Menciono especialmente Alexandre, Lucas, Wellington, Thiago, Brendon, Fernanda, Arthur, Maurício, Eduardo, Victor, Augusto, Enzo, Matheus, João, e Gustavo. Também agradeço a Lucila e a Simone, por todo apoio e ensinamentos administrativos.

Agradeço aos meus amigos de infância que me acompanharam durante este longo processo. Menciono especialmente Matheus Fröhlich. Juntos percorremos o mestrado e doutorado, em áreas distintas, porém sempre compartilhando ideias e desafios.

Agradeço também a Rede Nacional de Ensino e Pesquisa (RNP), a Associação dos Registradores de Pessoas Naturais do Brasil (Arpen-Brasil), ao Operador Nacional do Registro Civil de Pessoas Naturais (ON-RCPN) e o Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC) de Moçambique.

Por fim, agradeço ao Instituto Federal do Rio Grande do Sul (IFRS) por permitir-me afastar das minhas atividades docentes e poder dedicar-me integralmente ao doutorado.

“I am putting myself to the fullest possible use, which is all I think that any conscious entity can ever hope to do” HAL 9000

RESUMO

Os sistemas de identidade digital são componentes essenciais da segurança, privacidade e funcionalidade das interações online. Como componentes fundamentais, o provedor de identidade e o provedor de serviço têm sido tradicionalmente separados, uma arquitetura aprimorada ainda mais por padrões como OAuth 2.0 e OpenID Connect. Esses protocolos são essenciais para simplificar a autenticação e autorização do usuário final em plataformas digitais. Ao mesmo tempo, o paradigma emergente de Identidade Autossoberana redefine a privacidade do usuário, capacitando os indivíduos com controle direto sobre suas identidades digitais, sem supervisão intermediária por provedores de identidade, evitando assim vigilância indevida e acesso a dados por parte de provedores de serviço. Esta tese de doutorado aborda desafios urgentes na gestão de identidade digital, enfatizando a necessidade urgente de criptografia pós-quântica para proteger os sistemas de autenticação contra a ameaça teórica da computação quântica. Através de modificações avançadas no OAuth 2.0 e OpenID Connect, particularmente em suas bases criptográficas — JSON Web Key e Transport Layer Security — este trabalho é pioneiro no desenvolvimento de soluções resistentes a computadores quânticos. Os protocolos seguros quânticos propostos são avaliados em um estudo de caso realista do mundo real para validar sua eficácia e praticidade. Além de fortalecer os padrões atuais, esta pesquisa avalia criticamente o campo relativamente nascente da Identidade Autossoberana. Uma revisão sistemática completa da literatura é conduzida, culminando em uma taxonomia nova e meticulosamente elaborada. Esta taxonomia categoriza os esforços acadêmicos e práticos existentes e identifica lacunas persistentes e direções de pesquisas futuras. Ao analisar rigorosamente temas emergentes e conclusões da literatura, esta tese fornece um roteiro para aprofundar a compreensão teórica e prática de Identidade Autossoberana. Explorando implementações práticas de Identidade Autossoberana, a tese também aborda os desafios inerentes à utilização da tecnologia de blockchain para gerenciamento de identidade. O foco é melhorar a eficiência e a precisão da busca de metadados armazenados em sistemas blockchain comumente empregados em soluções de Identidade Autossoberana. Um novo mecanismo de busca é proposto e validado empiricamente, demonstrando desempenho superior em relação aos métodos existentes para tarefas de processamento de linguagem natural, aumentando assim a viabilidade operacional do blockchain no suporte a consultas de identidade complexas. As contribuições teóricas desta tese são ainda aumentadas pela introdução do framework Role-Artifact-Function. Este modelo conceitual de camada dupla, composto por um meta-metamodelo e um metamodelo, fornece uma estrutura robusta para examinar e contrastar modelos de identidade digital. Através da aplicação detalhada, o framework Role-Artifact-Function ajuda a elucidar as estruturas ontológicas subjacentes a modelos de identidade, oferecendo uma ferramenta analítica abrangente que faz avançar o discurso sobre a identidade digital. Por último, a tese confronta os desafios centrados no usuário associados a Identidade Autossoberana, particularmente as complexidades relacionadas com as interações dos usuários e a gestão de credenciais criptográficas. Para resolver essas questões, é introduzido o modelo inovador de Identidade Fiduciária. Inspirado nos princípios jurídicos fiduciários, este modelo reduz a carga do utilizador, automatizando os processos de consentimento e delegando a tomada de decisões a entidades confiáveis, simplificando as interações e melhorando a experiência do utilizador nas transações de identidade digital.

Palavras-chave: Identidade Digital. Gestão de Identidade. Criptografia Pós-Quântica. Identidade Autossoberana. Identidade Fiduciária.

RESUMO ESTENDIDO

Introdução

A capacidade de provar que os indivíduos são quem dizem ser é essencial para as interações humanas na sociedade, seja no mundo físico ou online. A prova é normalmente apresentada como uma credencial que permite a identificação e autenticação de uma pessoa. Essa credencial, que consiste em uma coleção de atributos, é chamada de documento de identidade ou simplesmente identidade.

Grandes corporações como Google e Facebook emitem identidade eletrônica no mundo digital de hoje. Elas criaram essas identidades para facilitar a identificação do usuário, autenticação, autorização e fornecimento de atributos do usuário para seus serviços internos. Essas identidades se desenvolveram em uma ferramenta poderosa para identificar usuários que desejam acessar os serviços das empresas e de vários outros provedores de serviços. Como resultado, essas empresas atuam como provedores de identidade. Várias empresas terceirizaram o registro, a identificação e a autenticação do cliente para provedores de identidade.

Usar provedores de identidade tem muitos benefícios e desvantagens. O usuário se beneficia de ter uma única identidade para autenticar com vários provedor de serviços. Uma desvantagem pode ser que poucos provedores de identidade gerenciam dados para muitos usuários. Armazenar identidade eletrônicas de pessoas em alguns provedores de identidade tem sido uma fonte de discórdia, pois esses poucos silos de dados têm os dados de um grande número de pessoas. Esses enormes silos de dados se tornaram alvos atraentes para hackers porque contêm ativos de alto valor que podem ser mal utilizados ou até mesmo negociados com instituições que os usuários não autorizaram.

Embora a maioria dos usuários confie em provedores de identidade ingenuamente, muitos usuários e empresas ficam desconfortáveis com a exigência de usar e confiar nessas entidades. Identidade auto-soberana atraiu atenção neste contexto porque impede que provedores de identidade rastreiem as atividades de seus usuários. Ele também aumenta a privacidade das pessoas, permitindo que elas armazenem e gerenciem seus dados e especifiquem a granularidade das informações compartilhadas. No entanto, identidade auto-soberana distribui a tarefa de gerenciar dados pessoais do provedor de identidade para o usuário, o que é uma causa de frustração para usuários tecnologicamente não qualificados.

Motivação e Justificativa

Há muitos desafios na área de gestão de identidade. Notamos uma lacuna entre a literatura científica de gestão de identidade e a crescente preocupação com computadores quânticos criptograficamente relevantes, capazes de interromper dados em trânsito e em repouso. Notavelmente, os protocolos OAuth 2.0 e OpenID Connect, que são empregados diariamente por bilhões de pessoas por meio dos principais provedores de identidade, são vulneráveis a essa ameaça quântica, necessitando da transição para criptografia pós-quântica. Embora essa ameaça quântica também afete os protocolos e sistemas identidade auto-soberana, este manuscrito se concentra em explorar as implicações do criptografia pós-quântica para OAuth 2.0 e OpenID Connect e seus protocolos subjacentes.

Esta tese foi conduzida em um momento especial para a pesquisa da gestão de identidade porque as ideias que culminaram no identidade auto-soberana estavam ganhando força na indústria e na academia. Em relação a este último, observamos que os estudos secundários relatados na literatura são caracterizados pela falta de rigor metodológico, ou adaptados para soluções baseadas em blockchain — apesar da falsa alegação de que identidade auto-soberana depende

de blockchain. Essas razões motivaram o planejamento e a execução de uma revisão sistemática da literatura do identidade auto-soberana, que resultou na descoberta de desafios abertos neste domínio.
Talvez os desafios mais significativos identificados tenham sido aqueles relacionados à experiência ruim do usuário para o leigo, particularmente no que diz respeito ao gerenciamento de chaves criptográficas e credenciais, bem como à avaliação das solicitações de informações privadas do provedor de serviço. O gerenciamento de chaves criptográficas e carteiras digitais pode ser complexo para o usuário médio, potencialmente levando à perda de chaves, gerenciamento incorreto ou falta de compreensão. Além disso, compartilhar e verificar informações privadas de forma amigável ao usuário em vários serviços e plataformas digitais também é um desafio. Isso motiva a criação de um novo paradigma identidade eletrônica baseado em princípios fiduciários.

Objetivos
Dada a contextualização acima, agora estabelecemos os objetivos primários e secundários desta tese. Os dois objetivos primários são: (i) aprimoramento de sistemas de autenticação e autorização com criptografia pós-quântica; e (ii) introdução do modelo de identidade fiduciária. Os objetivos secundários desta tese são: (i) revisão sistemática, mapeamento e criação de uma taxonomia de identidade autossoberana; (ii) melhoria dos mecanismos de busca de metadados de blockchain para identidade autossoberana; e (iii) desenvolvimento e aplicação do framework Role-Artifact-Function.

Método de Pesquisa
Dada a natureza multifacetada desta tese, que contribui para diferentes aspectos da gestão de identidade, um método de pesquisa uniforme foi aplicável somente em algumas áreas. Três revisões sistemáticas da literatura foram conduzidas para garantir rigor e reprodutibilidade, cada uma aderindo à estrutura metodológica estabelecida por Kitchenham e Charters. Essas revisões apoiam a alegação de novidade para cada uma das contribuições feitas nesta tese. Primeiro, o Capítulo 3 detalha uma revisão sistemática da literatura sobre a adoção de algoritmos pós-quânticos dentro dos protocolos OAuth 2.0 e OpenID Connect. Em segundo lugar, o Capítulo 4 explora avanços conceituais e práticos em identidade auto-soberana, complementados por um estudo de mapeamento sistemático, conforme definido por Petersen, para mapear o relacionamento de pesquisadores e trabalhos. Este capítulo também emprega o método de Petersen para desenvolver uma taxonomia para classificar a literatura de identidade auto-soberana. A revisão sistemática da literatura final, apresentada no Capítulo 5, foca na identificação de soluções para buscar metadados de identidade eletrônica em blockchain.
Além de revisões sistemáticas, os Capítulos 3 e 5 abordam problemas concretos que exigem o desenvolvimento de artefatos computacionais para atingir seus objetivos. Esses artefatos foram empregados empiricamente em experimentos projetados para testar as hipóteses de pesquisa. Os softwares desenvolvido e as configurações experimentais são disponibilizados publicamente sob licenças de código aberto para garantir que outros possam replicar nossos resultados.

Resultados e Discussões
Os resultados da pesquisa confirmam a viabilidade das modificações propostas nos protocolos OAuth 2.0 e OIDC para torná-los resistentes a ataques quânticos. Os testes realizados demonstraram que os protocolos modificados mantêm a eficácia e a praticidade na autenticação e autorização de usuários em ambientes reais. A tese também propõem uma nova taxonomia de

SSI, que categoriza e organiza de forma abrangente os esforços acadêmicos e práticos existentes no campo, proporcionando uma visão clara das lacunas e oportunidades de pesquisa futuras.
No que diz respeito ao uso de blockchain para SSI, um novo mecanismo de busca de metadados proposto mostrou-se superior aos métodos atuais, oferecendo maior eficiência e precisão na execução de consultas complexas de identidade. Este avanço torna o uso de blockchain uma solução mais prática e funcional para o gerenciamento de identidades digitais em sistemas descentralizados.
Além desses avanços, a tese introduz o framework *Role-Artifact-Function* (RAF), um arcabouço conceitual composto por um meta-metamodelo e um metamodelo. O RAF é projetado para examinar e contrastar modelos de identidade digital, oferecendo uma estrutura robusta para elucidar as estruturas ontológicas subjacentes a esses modelos. Através de sua aplicação detalhada, o RAF facilita a compreensão dos relacionamentos entre os diferentes componentes dos modelos de identidade, destacando como os artefatos, funções e papéis interagem para formar sistemas de identidade digital coerentes e seguros. A aplicação do RAF também revelou perspectivas valiosas sobre as lacunas nas abordagens atuais e sugeriu melhorias para futuros desenvolvimentos no campo.
O modelo de Identidade Fiduciária, por sua vez, se apresenta como uma solução inovadora para os desafios relacionados à experiência do usuário em SSI. Inspirado nos princípios jurídicos fiduciários, o modelo propõe a delegação de decisões críticas para entidades de confiança, o que reduz a carga sobre o usuário e simplifica a gestão de credenciais e consentimentos. A tese discute as implicações desse modelo e sugere caminhos para sua implementação em larga escala.

Considerações Finais
Conclui-se que as contribuições teóricas e práticas desta pesquisa oferecem uma base sólida para futuras inovações no campo de IAM. A transição para a criptografia pós-quântica é não apenas necessária, mas urgente e factível, para garantir a continuidade da segurança em sistemas de identidade digital. O modelo de Identidade Fiduciária proposto apresenta um novo paradigma que pode transformar a experiência do usuário em sistemas de identidade digital, tornando-os mais acessíveis e menos complexos. Este trabalho abre caminho para novas pesquisas e desenvolvimentos na área, com o potencial de impactar significativamente a forma como a identidade digital é gerenciada em um mundo cada vez mais digital e ameaçado pela computação quântica.

Palavras-chave: Identidade Digital. Gestão de Identidade. Criptografia Pós-Quântica. Identidade Autossoberana. Identidade Fiduciária.

ABSTRACT

The security, privacy, and functionality of online interactions are integrally tied to Electronic IDentity (e-ID). As foundational components, Identity Provider (IdP) and Service Provider (SP) have traditionally been separated, an architecture further enhanced by standards such as Open Authorization 2.0 (OAuth 2.0) and OpenID Connect (OIDC). These protocols are critical in streamlining end-user authentication and authorization across digital platforms. Concurrently, the emergent Self-Sovereign Identity (SSI) paradigm redefines user privacy by empowering individuals with direct control over their e-IDs without intermediary oversight by IdPs, thereby preventing undue surveillance and data access by SPs. This thesis addresses pressing challenges in e-ID management, emphasizing the urgent need for Post-Quantum Cryptography (PQC) to safeguard authentication systems against the theoretical threat of quantum computing. Through advanced modifications to OAuth 2.0 and OIDC, particularly in their cryptographic foundations — JSON Web Key (JWK) and Transport Layer Security (TLS) — this work pioneers the development of quantum-resistant methodologies. The proposed quantum-safe protocols are evaluated in a comprehensive real-world OIDC case study to validate their effectiveness and practicality. In addition to fortifying current standards, this research critically assesses the relatively nascent field of SSI. A thorough systematic literature review is conducted, culminating in a novel, meticulously crafted taxonomy of SSI. This taxonomy categorizes existing scholarly and practical efforts and identifies persistent gaps and future research directions. By rigorously analyzing emergent themes and findings from the literature, this thesis provides a roadmap for deepening the theoretical and practical understanding of SSI frameworks. Exploring practical implementations of SSI, the thesis also tackles the inherent challenges of utilizing Distributed Ledger Technology (DLT) for identity management. The focus is improving the efficiency and accuracy of searching metadata stored on blockchain systems commonly employed in SSI solutions. A novel search mechanism is proposed and empirically validated, demonstrating superior performance over existing methods for natural language processing tasks, thereby enhancing the operational feasibility of blockchain in supporting complex identity queries. The theoretical contributions of this thesis are further augmented by the introduction of the *Role-Artifact-Function (RAF)* framework. This dual-layer conceptual model, consisting of a meta-metamodel and a metamodel, provides a robust structure for examining and contrasting e-ID models. Through detailed application, the RAF framework aids in elucidating the ontological structures underlying various identity models, offering a comprehensive analytical tool that advances the discourse on e-ID. Lastly, the thesis confronts the user-centric challenges associated with SSI, particularly the complexities related to user interactions and management of cryptographic credentials. To address these issues, the innovative Fiduciary Identity model is introduced. Inspired by fiduciary legal principles, this model reduces user burden by automating consent processes and delegating decision-making to trusted entities, simplifying interactions and enhancing user experience in e-ID transactions.

Keywords: Electronic Identity. Digital Identity. Identity Management. Post-Quantum Cryptography. Self-Sovereign Identity. Fiduciary Identity.

LIST OF FIGURES

LIST OF TABLES

LIST OF ALGORITHMS

LIST OF ACRONYMS

ABE	Attribute-Based Encryption
ACME	Automatic Certificate Management Environment
AES	Advanced Encryption Standard
AKE	Authenticated Key Exchange
Amazon EC2	Amazon Elastic Compute Cloud
API	Application Programming Interface
BLS	Boneh–Lynn–Shacham
BPMN	Business Process Model and Notation
CA	Certificate Authority
CAcc	Cryptographic Accumulator
CAFe	Comunidade Acadêmica Federada
CBOR	Concise Binary Object Representation
CCPA	California Consumer Privacy Act
CFG	Context-Free Grammar
CH	Chameleon Hashing
CLI	Command Line Interface
CMC	Certificate Management over CMS
CMP	Certificate Management Protocol
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
CPF	Cadastro de Pessoa Física
CPU	Central Processing Unit
CRL	Certificate Revocation List
CRQC	Cryptographically Relevant Quantum Computer
CSR	Certificate Signing Request
CSRF	Cross-Site Request Forgery
CSS	Cascading Style Sheets
CV	Curriculum Vitae
DHE	Diffie-Hellman Ephemeral
DID	Decentralized IDentifiers
DIDComm	Decentralized IDentifiers Communication
DIM	Digital Identity Model
DIoTComm	Decentralized IDentifiers-based Internet of Things Communication
DLP	Discrete Logarithm Problem
DLT	Distributed Ledger Technology
DNS	Domain Name System
e-ID	Electronic IDentity
EC	Exclusion Criteria
ECDHE	Elliptic-Curve Diffie-Hellman Ephemeral

ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
EDM	Electronic Document Management
eIDAS	electronic IDentification, Authentication and trust Services
FHE	Fully Homomorphic Encryption
FIDO2	Fast IDentity Online 2
FIM	Fiduciary Identity Model
FIMM	Fiduciary Identity Metamodel
FOL	First-Order Logic
GDPR	General Data Protection Regulation
GNS	GNU Name System
GPU	Graphics Processing Unit
HCI	Human-Computer Interaction
HR	Human Resources
HSM	Hardware Security Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IAM	Identity and Access Management
IANA	Internet Assigned Numbers Authority
IC	Inclusion Criterion
ICPEdu	Infraestutura de Chaves Públicas para Ensino e Pesquisa
IdP	Identity Provider
IdRC	Autenticação Eletrônica do Registro Civil
IFP	Integer Factorization Problem
ILP	Integer Linear Programming
INTIC	Instituto Nacional de Tecnologias de Informação e Comunicação
IoT	Internet of Things
IP	Internet Protocol
JS	JavaScript
JSON	JavaScript Object Notation
JWE	JSON Web Encryption
JWK	JSON Web Key
JWS	JSON Web Signature
JWT	JSON Web Token
KEX	Key Exchange
LoA	Level of Assurance
MFA	Multi-Factor Authentication
MPC	Multi-Party Computation
MS	Multi-Signature

NFC	Near-Field Communication
NIST	National Institute of Standards and Technology
NM	Norma Machine
NS	Name System
OAuth 2.0	Open Authorization 2.0
OCSP	Online Certificate Status Protocol
OffOIdPM	Offline Outsourced Identity Provider Model
OIDC	OpenID Connect
OIDC-D	OIDC Discovery
OIDC-DCR	OIDC Dynamic Client Registration
OnOIdPM	Online Outsourced Identity Provider Model
OpenCV	Open Source Computer Vision
OpenSSL	Open Secure Sockets Layer
OQS	Open-Quantum Safe
OTC	One-Time Certificate
OTP	One Time Password
PDF	Portable Document Format
Ph.D.	Doctor of Philosophy
PICOC	Population, Intervention, Comparison, Outcomes, and Context
PII	Personal Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PQ	Post-Quantum
PQ-JWTs	Post-Quantum JSON Web Tokens
PQ-KEX	Post-Quantum Key EXchange
PQ-OIDC	Post-Quantum OpenID Connect
PQ-TLS	Post-Quantum Transport Security Layer
PQC	Post-Quantum Cryptography
PRE	Proxy Re-Encryption
PSK	Pre-Shared-Key
RA	Registration Authority
RAF	Role-Artifact-Function
RNP	Rede Nacional de Ensino e Pesquisa
RP	Relying Party
RQs	Research Questions
RSA	Rivest-Shamir-Adleman
SAML	Security Assertion Markup Language
SCT	Signed Certificate Timestamp
SLR	Systematic Literature Review

SMS	Short Message Service
SP	Service Provider
SSI	Self-Sovereign Identity
SSS	Shamir's Secret Sharing
TCP	Transmission Control Protocol
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TOTP	Time-based One Time Password
TPL	Trust Policy Language
TSL	Trust Service List
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VC	Verifiable Credential
vCPU	virtual CPU
VP	Verifiable Presentation
W3C	World Wide Web Consortium
WebAuthN	Web Authentication
zk-SNARK	zero-knowledge Succinct Non-interactive ARguments of Knowledge
ZKP	Zero-Knowledge Proof

CONTENTS

1 INTRODUCTION

The ability to prove that individuals are who they claim to be is critical to human interactions in society, whether in the physical world or online. The proof is typically presented as a credential that enables the identification and authentication of a person. This credential, which consists of a collection of attributes, is referred to as an identity document or simply identity (1, 2).

Large corporations such as Google and Facebook issue Electronic IDentity (e-ID) in today's digital world. They created these identities to facilitate user identification, authentication, authorization, and provision of user attributes for their internal services. These identities have developed into a powerful tool for identifying users who wish to access the companies' services and those of various other Service Provider (SP)s. As a result, these businesses serve as Identity Provider (IdP)s. Numerous companies have outsourced customer registration, identification, and authentication to IdPs.

Using IdPs has many benefits and drawbacks. The user benefits from having a single identity to authenticate with multiple SPs. One disadvantage may be that few IdPs manage data for many users. Storing people's e-IDs in a few IdPs has been a source of contention since these few data silos have the data of a large number of people (3). These massive data silos have become attractive targets for hackers (4) because they contain high-value assets that can be misused (5) or even traded (6) with institutions that users have not authorized.

Although most users trust IdPs naively, many users and businesses are uneasy with the requirement to use and trust these entities. SSI (3) has garnered attention in this context because it prevents IdPs from tracking their users' activities. It also enhances people's privacy by enabling them to store and manage their data and specify the granularity of the shared information. Nonetheless, SSI distributes the task of managing personal data from the IdP to the user, which is a cause of frustration for technologically unskilled users.

In this thesis, we identify and address open challenges in many areas of e-ID. The following sections of this chapter are structured as follows. First, we lay down the motivation and justification of this thesis. Next, the objectives that guided our investigation are presented. Then, we describe the research methods employed. A discussion of the academic contributions of our work comes in sequence. Additionally, we present other contributions that extend beyond the academic realm. Finally, we conclude the chapter by presenting the structure of the manuscript.

1.1 MOTIVATION AND JUSTIFICATION

There are many challenges in the area of Identity and Access Management (IAM). We noted a gap between the IAM scientific literature and the growing concern of cryptographically relevant quantum computers capable of disrupting data both in transit and at rest. Notably, the Open Authorization 2.0 (OAuth 2.0) and OpenID Connect (OIDC) protocols, which are em-

ployed daily by billions through leading IdPs, are vulnerable to this quantum threat, necessitating to transition to Post-Quantum Cryptography (PQC). While this quantum threat also affects SSI protocols and systems, this manuscript focuses on exploring the implications of PQC for OAuth 2.0 and OIDC and their underlying protocols.

This thesis was conducted at a special time for IAM research because the ideas that culminated into SSI were getting traction in industry and academia. Regarding the latter, we observed that the secondary studies reported in the literature are either characterized by a lack of methodological rigor (7, 8, 9, 10, 11, 12, 13), or tailored to blockchain-based solutions (7, 14, 8, 9, 10, 11, 12, 13) — despite the false claim that SSI depends on blockchain (15, 16, 17, 18). Those reasons motivated the planning and execution of a Systematic Literature Review (SLR) of SSI, which resulted in the discovery of open challenges in this domain.

Perhaps the most significant challenges identified were those related to the poor user experience for the layman, particularly concerning the management of cryptographic keys and credentials, as well as the evaluation of SP's requests for private information. Managing cryptographic keys and digital wallets can be complex for the average user, potentially leading to key loss, mismanagement, or a lack of understanding. Additionally, sharing and verifying private information in a user-friendly manner across various digital services and platforms is also a challenge. These motivate the creation of a new e-ID paradigm based on fiduciary legal principles. A detailed account of how this thesis was conducted can be found in Appendix A.

1.2 OBJECTIVES

Given the above contextualization, we now lay down this thesis's primary and secondary objectives. The two primary objectives are:

- **Enhancement of Authentication and Authorization Systems with Post-Quantum Cryptography**: To develop and validate quantum-resistant methodologies within traditional e-ID architectures, specifically through modifications to OAuth 2.0 and OIDC;
- **Introduction of the Fiduciary Identity Model**: To define a new e-ID model that minimizes user burden in managing cryptographic credentials and enhances user experience by automating consent processes and delegating decision-making to trusted entities.

The secondary objectives of this thesis are:

- **Systematic Review, Map and create a Taxonomy of Self-Sovereign Identity**: To conduct a comprehensive systematic literature review, a systematic mapping and a systematic taxonomy to understand advances in conceptual and practical efforts in SSI, identifying gaps and setting directions for future research;
- **Improvement of Blockchain Metadata Search Mechanisms for Self-Sovereign Identity**: By proposing and testing a novel search mechanism for SSI metadata stored on

blockchain systems, this objective is to improve the efficiency and accuracy of such systems in supporting complex identity queries, which is crucial for the practical implementation of blockchain-based SSI solutions;

- **Development and Application of the Role-Artifact-Function Framework**: The Role-Artifact-Function (RAF) framework, consisting of a meta-metamodel and a metamodel, serves as an analytical tool for examining e-ID models. It aids in elucidating the ontological structures underlying various identity models, fostering a deeper theoretical and practical understanding of e-ID models.

1.3 RESEARCH METHOD

Given the multifaceted nature of this thesis, which contributes to different aspects of IAM, a uniform research method was only applicable across some areas. Three SLRs were conducted to ensure rigor and reproducibility, each adhering to the methodological framework established by Kitchenham and Charters (19). These SLRs support the claim of novelty for each of the contributions made in this thesis. First, Chapter 3 details a SLR on adopting post-quantum algorithms within OAuth 2.0 and OIDC protocols. Second, Chapter 4 explores conceptual and practical advancements in SSI, complemented by a systematic mapping study, as defined by Petersen (20), to map the relationship of researchers and works. This chapter also employs Petersen's method (20) to develop a taxonomy to classify the SSI literature. The final SLR, presented in Chapter 5, focuses on identifying solutions for matching e-ID metadata in blockchain.

In addition to SLRs, Chapters 3 and 5 tackle concrete problems that require the development of computational artifacts to achieve their objectives. These artifacts were empirically employed in experiments designed to test the research hypotheses. The developed software and experimental setups are made publicly available under open-source licenses to ensure others can replicate our results.

1.4 TEXT ORGANIZATION

The remainder of this thesis is organized as follows. Chapter 2 provides the essential background on IAM necessary to understand the subsequent discussions. The chapters that explore specific topics that necessitate more background knowledge integrate such details into the appropriate sections to improve coherence and clarity. Subsequently, Chapter 3 focuses on the first primary objective of this thesis, which is to enhance authentication and authorization systems using PQC. In Chapter 4, we tackle the first secondary objective, which is to conduct a systematic literature review and mapping of SSI, develop a taxonomy, and identify gaps and future research directions in this realm. Chapter 5 tackles the second secondary objective of this thesis of improving blockchain metadata search mechanisms, and Chapter 6 addresses the last

secondary objective by introducing the Role-Artifact-Function framework as a methodological tool to analyze e-ID models and clarify their underlying ontological structures. Next, Chapter 7 presents the Fiduciary Identity model, exploring how it automates consent processes and delegates decision-making to enhance user experience, thus addressing our last primary objective. The thesis concludes in Chapter 8, where we summarize the achievement of our objectives and their impact on e-ID management and discuss potential future research directions and unresolved issues.

2 IDENTITY AND ACCESS MANAGEMENT FUNDAMENTALS

This section provides the necessary background about IAM required for following this thesis. We begin with an introduction to identity documents, then discuss e-ID and its lifecycle to arrive at the IAM models.

2.1 IDENTITY DOCUMENTS

We can categorize identity documents into three distinct formats of representation. The traditional physical document is the first format. This format typically consists of a paper document or a plastic card on which the individual's identifying characteristics are printed by an issuer[1]. Paper and plastic cards are manufactured with care to avoid easy forgery. When people wish to prove their identity, they present a physical document. The Relying Party (RP)[2] performs the identification by reading the attributes. One of the most critical characteristics of this type of document is the photograph of the individual's face, which is used for authentication. This identification document is referred to as a face badge.

The digital identity document is the second format. It is the digitalized version of the physical document and is often used on mobile devices (21). Cryptographic techniques, such as digital signatures, are sometimes used to verify the integrity and authenticity of the data. Typically, the signature and identity attributes are encoded as a QR code so that the RP can verify the identity document's integrity and veracity offline.

The e-ID document is the third format. This is the identity that is used in the virtual world to authenticate users and enable them to consume electronic services on the web. Unlike a digital identity document, which is a visual representation, an electronic document is built from the ground up to be used electronically, removing the need for visual verification of its integrity. Multi-Factor Authentication (MFA) (22) and cryptographic techniques such as digital signatures and public-key cryptography (23) are used to carry out these processes, for instance, by combining a password known only to the identity holder with a key displayed in a time-based one-time password service (24, 25).

These three forms of identity must be impervious to forgery, fraud, and data leakage. As a result, the collection, storage, and processing of identity-related data must be handled with extreme caution, emphasizing appropriate data protection mechanisms. While each of the three types of identity listed above is vulnerable to fraud, the electronic version requires the most oversight. Numerous instances of fraud involving the misuse of e-IDs have been reported (5, 6).

While business cards and *curriculum vitae* are examples of self-issued identity documents, the vast majority of identities in use are issued by trusted third parties. For instance, national-level identification documents such as driver's licenses and passports are frequently issued by the government (26) or by private companies authorized to do so (27).

[1] We use the terms issuer and IdP interchangeably.
[2] We use the terms RP, SP and verifier interchangeably.

2.2 ELECTRONIC IDENTITY

Establishing trust in relationships between various entities requires identifying the communicating parts. In the physical world, proof of identity is accomplished through pre-agreed upon authentication factors or with the assistance of trusted third parties. Physical devices are frequently used as authentication factors. For instance, it is common for individuals to be identified visually through their identification documents, followed by a facial badge verification. Similarly, in the electronic world, communicating parties must have a certain Level of Assurance (LoA) regarding the other party's identity. This assurance is accomplished by using e-IDs on data communication networks such as the Internet.

As with physical identity, the e-ID is typically defined as a set of attributes that help describe or qualify an entity (1). Some authors limit this definition to a specific set of attributes in a given context (28, 29, 30). As a result, e-IDs are not simply digital representations of physical identities such as a passport or driver's license. They are created, used, and destroyed in accordance with the user's desires, frequently containing only the attributes necessary to accomplish the task at hand. For instance, a seller on eBay (31) may have an e-ID that conceals their name, age, and country of residence, as others are only concerned about whether or not this seller has a track record of successful transactions (32).

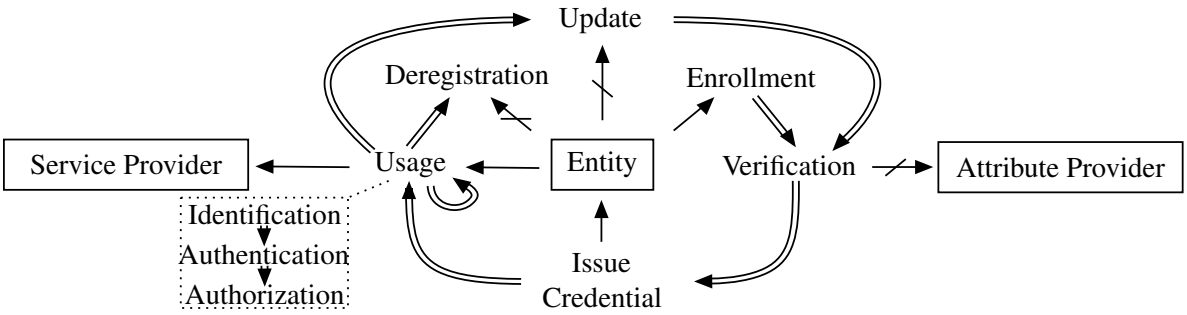
All identities, whether physical or electronic, are subject to ownership verification. That is, they require mechanisms for properly *identifying* and *authenticating* users (33). The identification process begins with the holder of an e-ID presenting a unique attribute in a given context, *i.e.*, an identifier that differentiates it from all other e-IDs in that context (34). The most common example is providing an email address when signing up for a subscription service. The subsequent stage is to authenticate the identified entity by verifying a security proof, which is traditionally accomplished via a secret password or digital signature, thereby ensuring that the holder of the identity is, in fact, its owner. In the subscription service example mentioned above, providing a code or clicking a link received via email proves that the email address belongs to the holder.

Identification and authentication are critical in our digital society because they enable citizens to access services electronically. As a result, the identification and authentication processes are carried out by specialized services trusted by the parties involved. These services are provided by systems that manage e-ID and are referred to as IAM systems.

2.3 ELECTRONIC IDENTITY LIFECYCLE

The e-ID lifecycle delineates the procedures and responsibilities of managing and utilizing e-ID. The e-ID lifecycle is illustrated in Figure 1 where rectangular boxes represent entities, double-shaft arrows represent process flow, single-shaft arrows represent entity-process associations, single-shaft arrows with crossings represent optional associations, and the dotted square represents e-ID usage inner processes.

Figure 1 – The e-ID lifecycle from the perspective of the IdP.



Source: The author.

Creating an e-ID is known as *enrollment*, which involves registering an entity with an IdP (*e.g.*, Meta, Google, or a government entity). Relevant attributes are collected and stored, and one or more are set as the e-ID's identifier. For example, in e-ID for humans, attributes like name, date of birth, and email may be collectively used as the identifier. Another attribute or set of attributes is used for authentication. The attributes used for authentication are kept secret.

The second step is the *verification* of the enrolled entity's provided attributes. The extent of verification depends on the IdP's policy. Verification may be required for all attributes, certain attributes, or none. Attributes like name and birthdate can be checked with government-issued credentials in the case of personal e-ID. In these circumstances, the government agency that provided the credential is the attribute provider. In contrast, authentication attributes are often continuously validated. For example, proof of ownership of the registered email address is verified each time it is used for password recovery.

The third step is to *issue a credential* that proves the existence of the identity relationship. This credential indicates that an entity has a digital representation in the IdP that issued the credential. One example of a credential is the x509 digital certificate (35). On the other hand, some IdPs do not issue digital certificates. Instead, they use the OAuth 2.0 (36) and OIDC identity (37) protocols to prove the identity's existence. A connection to the IdP is established each time users must prove their identity with an SP using these protocols. The most prominent IdPs on the web use these identity protocols instead of issuing digital certificates. We discuss them in detail in the following sections.

In the fourth stage of the lifecycle, the entity *uses* their e-ID to access services from the SP. This step includes *identifying* the entity through a unique set of attributes, *authenticating* their identity, and granting or revoking *authorization* to share attributes with the SP. Identification and authentication are essential, whereas authorization is often optional. Some SPs merely need to uniquely identify and authenticate their new and recurring users without needing any other attributes for their services.

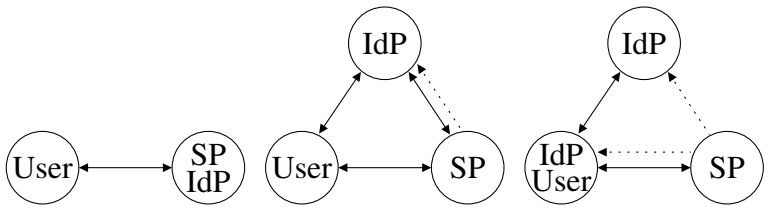
It is crucial to maintain accurate attribute values in the e-ID by consistently *updating* and *verifying* the attributes stored in the IdP. Finally, an e-ID may eventually reach the end of its lifecycle. It can occur because of causes like the controlling entity opting to destroy it or the IdP electing to remove it. *Deregistration* is the process of removing an e-ID.

It is important to emphasize that, irrespective of the technological framework employed for creating e-IDs, the IdP plays a crucial role in previously described functionalities. The following section will explore IAM models, elucidating facets of the foundational protocols facilitating the deployment of e-IDs.

2.4 THE EVOLUTION OF IAM MODELS

Different IAM models, also called e-ID models, can be categorized based on the responsibilities and interactions of the roles involved, namely user, IdP, and SP. Based on this classification approach, current e-ID systems can be categorized into three models, namely centralized (Figure 2a), outsourced IdP (Figure 2b), and SSI (Figure 2c). In these figures, circles represent entities, labels represent roles, solid lines represent interactions, and dashed lines represent trust. Next, we elaborate on these categories and highlight noteworthy protocols and standards for each model.

Figure 2 – IAM models.



(a) Centralized. (b) Outsourced IdP. (c) SSI.

Source: The author.

2.4.1 Centralized

In the early days of the Internet, SPs had no choice but to develop IdPs to authenticate consumers and offer customized products and services. Nevertheless, this resulted in the establishment of *centralized* authorities that served as both SPs and IdPs. Users frequently resorted to reusing weak passwords across multiple systems, resulting in many vulnerabilities and usability issues. Initiatives were initiated to inform users about the potential hazards associated with the reuse of simple passwords (38, 39).

In considering adopting the centralized model, it is pertinent to acknowledge the establishment of the server-client architecture as standardized in 1996 through the Hypertext Transfer Protocol (HTTP) version 1.0. This initial version featured a rudimentary method for client identification and authentication, reliant on a straightforward comparison of usernames and passwords lacking cryptographic safeguards. Subsequently, in 1997, Digest Access Authentication was introduced to enhance security. This method introduced a nonce-based challenge, requiring the client to hash its response using MD5 before transmitting it to the server (40).

Over time, this authentication mechanism underwent updates to accommodate internationalization concerns in 2015 (41) and incorporate support for newer hashing algorithms (42).

2.4.2 Outsourced Identity Provider

The next logical evolution was to replace the centralized authorities with third-party IAM solutions, *i.e.*, IdPs. With this new paradigm, users only need to be registered with a few IdPs to access the web's plethora of services. By contrast, SPs must be registered with the desired IdPs or IdP federations to work with the IdPs' identified and authenticated users. Through token exchange protocols such as Security Assertion Markup Language (SAML) (43), OAuth 2.0 (36), and OIDC (44), the interactions between the IdP, SP, and end user were standardized. Even though this identity model significantly simplified the management of multiple identifiers and passwords for users, it resulted in the creation of a few large silos of valuable private information. Let us briefly describe the OAuth 2.0 and OIDC protocols.

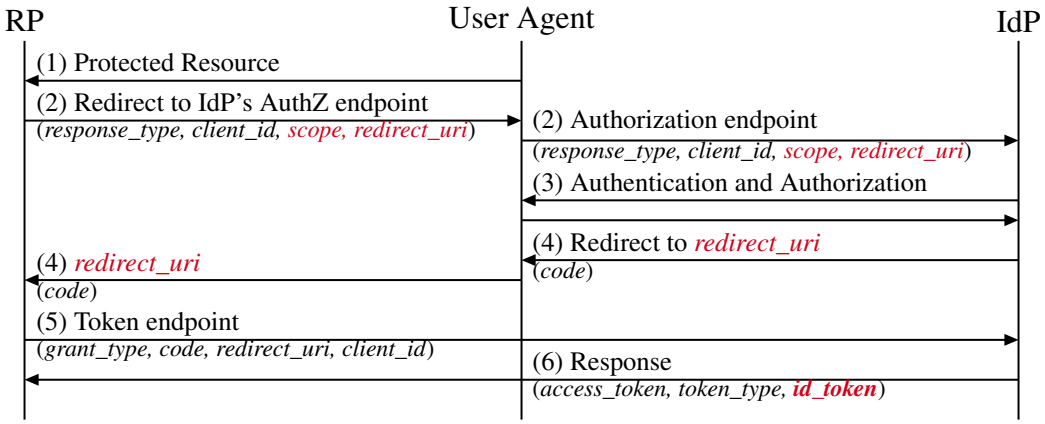
OAuth 2.0

The OAuth 2.0 protocol was introduced in 2012 to allow third-party applications to access data and perform actions on behalf of users (36). It is based on the distribution of tokens and establishes four roles: (i) the end-user is the *resource owner*; (ii) the *client* is the application that requests the resource owner's data; (iii) the *authorization server*, *i.e.*, the IdP, grants *access tokens* for a client to access the resource owner's data after authenticating the resource owner and obtaining their authorization; and (iv) the *resource server* hosts the protected resources and responds to requests.

The protocol provides three standardized flows for clients to obtain resource owner data, one of which is intended to facilitate the transition from basic and digest authentication schemes, as well as other schemes, to the two major flows. The *authorization code grant*, in which tokens are exchanged between the RP and the IdP over a secure back channel, and the *implicit grant*, in which all interactions occur through the user's browser, are the two flows in question. Effectively, only the *authorization code grant* should be used, as the *implicit grant* is known to have security flaws, such as the impossibility of detecting replay attacks (45). The *authorization code grant* is depicted in Figure 3, where dark-colored values indicate mandatory parameters, red-colored values are optional values made mandatory by OIDC, and bold red *id_token* is a new, mandatory OIDC value.

First, the user requests a protected resource from the RP via their user agent or attempts to access a restricted area. If no cookie or other storage mechanism is storing a session identifier proving that the resource owner has previously authenticated and authorized this client to access their data, the *authorization code grant* process begins. Users are frequently presented with one or more IdPs in which the RP is registered and asked to select one.

Figure 3 – OAuth 2.0's *authorization code grant* flow.



Source: The author.

Second, the RP directs the unknown user to the TLS-secured authorization endpoint of the selected IdP. The protocol does not specify how the RP finds the authorization endpoint. This usually occurs during the client registration process in the IdP, which is also out of scope. The user agent performs the redirect, which includes two mandatory parameters: `response_type`, which contains the value `token` indicating that this is the *authorization code grant* flow, and `client_id`, which contains the RP's identification. In OAuth 2.0, the `scope` and `redirect_uri` are optional parameters, whereas they are required in OIDC, as will be explained later. The `scope` parameter specifies which personal information the RP requests from the IdP or the permission to act on the user's behalf. The `redirect_uri` parameter specifies the RP-controlled Uniform Resource Locator (URL) to which the user agent will be redirected after authentication and authorization. These parameters are optional. If they are not specified, the values established during the client registration process are used.

Third, after receiving the request, the IdP authenticates the user and obtains their permission to access the requested resource. The protocol does not specify how users are authenticated or granted authorization. Similarly, available scopes are defined by the IdP and communicated to the RP either during the client registration process or via another mechanism. Authentication can be as simple as a username and password or as sophisticated and secure as MFA. This is not covered by OAuth 2.0.

Fourth, if the user is authenticated and grants authorization, the IdP issues a short-lived *authorization code*. The `code` parameter of the redirect response is used to send this to the RP via the user agent. If an error occurs, the IdP notifies the user and uses the `error` parameter instead of `code`.

Fifth, the client makes a TLS-secured token endpoint request. Four parameters are required: (i) `grant_type` is `authorization_code`; (ii) `code` is the authorization code from the previous step; (iii) `redirect_uri` is the same as in the second step or is omitted; and (iv) `client_id` is the same as in the second step if no client authentication is performed. It is important to note that in OAuth 2.0, web applications are considered *confidential clients* and

thus require some form of authentication to access the token endpoint. Although the protocol does not specify an authentication mechanism for clients, the OAuth 2.0 Security Best Current Practice (45), an RFC that addresses OAuth 2.0 security, recommends a challenge-response protocol specifically designed to authenticate clients (46).

In the sixth and final step, the IdP verifies that the `authorization_code` received was issued to the authenticated client and that the `redirect_uri` matches what was provided in the second step, if it was previously provided. An `access_token` is then issued along with a `token_type`, which instructs the RP on how to make requests to the user-authorized protected resources. In OIDC, an `id_token` is also issued. After receiving the `access_token`, the client can use it to request the protected resources from the resource server.

OpenID Connect

Even though OAuth 2.0 standardizes roles, flows, and messages, practitioners must still fill in numerous gaps. It does not, for example, address client registration, indicate the authentication factors used, or create a mechanism for clients to discover IdP endpoint Uniform Resource Identifier (URI) (47). OIDC was presented as a solution for these and other issues (37).

OIDC adds an identity layer to OAuth 2.0. This is accomplished in a non-destructive manner by leveraging OAuth 2.0 optional parameters and the requirement to ignore unrecognized request and response parameters to/from the token and authorization endpoints. The modifications to the OAuth 2.0 three-party handshake are depicted in red in Figure 3 and described below.

First, the `scope` parameter must contain the value `openid`. This is possible due to the fact that OAuth 2.0 permits multiple values separated by spaces for this parameter. OIDC defines four additional scopes that the RP can use to request user-related information: (i) `profile`, which requests the user's `name`, `nickname`, `picture`, `website`, `gender`, `birthdate`, and other personal data; (ii) `email` requests access to `email` address and `email_verified`, a boolean value indicating whether or not it has been verified; (iii) `phone` asks for `phone_number` and `phone_number_verified`; and (iv) `address`.

It is worth noting that in OIDC, user-related data is referred to as claims. A claim is a piece of information asserted about the user by the IdP or other attribute provider. The user claims requested by the client are accessed via the `userinfo_endpoint`, which receives a valid `access_token` and returns the claims this token is authorized to access.

Second, in OIDC, the `redirect_uri` parameter is required and must match the URI specified in the client registration. The *OIDC core* specification, like OAuth 2.0, assumes the RP is registered and knows the IdP's communication endpoints. These two challenges are addressed by two additional specifications: *OIDC Dynamic Client Registration (OIDC-DCR)* (48) and *OIDC Discovery (OIDC-D)* (49). These two specifications, along with the *OIDC core*, make up what is collectively referred to as the *OIDC dynamic*. In the OIDC-DCR

specification, a client sends one or more `redirect_uri` and other optional parameters and receives a `client_id` and optionally a `client_secret`. The OIDC-D protocol defines the URI `/.well-known/openid-configuration`, which clients use to discover the endpoints and algorithms supported by an IdP.

The final and most significant modification to the OAuth 2.0 three-party handshake occurs in the response of the token request: OIDC adds a required response argument named `id_token`. This token contains information regarding the user's authentication, including the token's issuer, the intended audience (one or more `client_id`), a unique identifier of the resource owner in the IdP, the date and time of the authentication, and the token's issued and expiration times. This token may also include optional information such as the *authentication context class*, which indicates the level of assurance of the authentication process (50), and an array of IdP-defined *authentication method reference*, such as password, Personal Identification Number (PIN), and facial recognition.

2.4.3 Self-Sovereign Identity

In the early days of the web, the conception of the client-server model shaped the idea that in the digital world, people are users of online systems rather than human beings, *i.e.*, entities that need identification, authentication, and authorization to access and perform tasks online (51). This digital model assumes administrative precedence because it was built on the foundation that servers (companies, online businesses) are more important than clients (individuals) and, therefore, dictate the rights of clients (52). This web fabric holds to this day and is exacerbated by the need for the creation of legislation, such as the European Union's General Data Protection Regulation (GDPR) (53) and the California Consumer Privacy Act (CCPA) (54), to specify the rights of individuals and their digital data in a society increasingly dependent on digital interactions.

The fundamental premise of SSI is that individuals have sovereignty over their digital selves and thus control over their data. This concept fundamentally distinguishes SSI from previous identity models, which viewed individuals as users. In this new model, sovereign individuals store and manage their data, thereby controlling with whom their private data are shared and to what extent.

Although philosophers such as John Locke and Stuart Mill have written about the sovereignty of individuals in past centuries (55, 56), Loffreto (57) established the first widely accepted (3, 58, 59, 60, 61) link between sovereignty and e-ID (57). Thereafter, the meaning of sovereign identity was debated (62, 63, 64, 65), and technology standards were proposed (66, 67). Significant momentum was obtained, especially in academia (13, 68), after Christopher Allen laid out what he proposed to be the ten principles of SSI (3), which are detailed next.

First, individuals must have an *existence* independent of their digital selves, *i.e.*, they cannot exist only virtually. A (self-sovereign) identity works by sharing the desired (digital) aspects of the individual. Second, people must *control* their identities by owning and managing

their attributes, which does not prohibit them from making *claims* about other people. Third, people must have *access* to their data and claims by storing them or being readily available if they are outsourced. Fourth, all systems must be *transparent*, and the underlying algorithms must be free and open-source, thus allowing detailed examination by anyone. Fifth, identities must *persist* forever, or as long as individuals wish. Sixth and seventh, identities and their claims must be *portable* across different systems and technologies, which requires *interoperability* between standards and implementations. Eighth and ninth, people need to *consent* to the use and sharing of their data, while data disclosure must be *minimized* to the absolute minimum. For instance, to find out if a person can buy an alcoholic beverage, it is unnecessary to share their date of birth. Tenth, at the end of the day, individuals' rights must be *protected*, which means that systems must be designed to avoid censorship and to protect individuals' rights, even at the expense of the system.

In SSI, any assertion about a subject is referred to as a *claim*. A *credential* is a collection of one or more assertions made about a subject by an entity. It could be, for example, a government-issued driver's license that contains a person's date of birth, name, and address. A *Verifiable Credential (VC)* is a credential that includes a revocation list or another method of revocation and contains cryptographic material that ensures the credential's integrity, as well as the issuer's identification and non-repudiation (66). Additionally, a tamper-resistant claim derived from a VC is referred to as a *verifiable claim* or *Verifiable Presentation (VP)*. Although we use these terms interchangeably throughout this chapter, we refer to tamper-proof claims and tamper-proof credentials.

In the same way that entities issue physical credentials to holders in the form of paper or plastic cards in the physical world, entities issue VCs to holders in SSI. However, unlike physical and digital identities, these electronic documents enable individuals to select which attributes (claims) to share, which is impossible with physical or digital credentials. They require the holder to present the identity document in its entirety, revealing all of its attributes.

Suppose that you are asked to prove that you have reached the age of majority. With a physical document, showing the paper or plastic card will reveal the birthdate and all other attributes to the RP. The same is true for digital identity documents, commonly implemented using X.509 attribute certificates (69). With traditional X.509 certificates, the whole certificate has to be shared with the RP to verify the document's integrity. However, in the context of SSI, you would construct a VP stating that: (i) a credential was issued to you by a trusted party; (ii) this credential has your birthdate in it; (iii) your birthdate was more than 18 years ago; and (iv) this credential has not been revoked by the government body. Hence, whoever receives this VP does not learn your name, birthdate, and any other information in the credential, only that you have reached the age of majority.

The recipient of a VP (*i.e.*, the RP) verifies the following: (i) who signed the credential that supports this VP; (ii) whether the VP is constructed correctly (*i.e.*, it contains the required information and is not corrupted or counterfeited); and (iii) whether the credential that supports this VP is valid (*i.e.*, whether the credential was revoked or not). It is important to note that

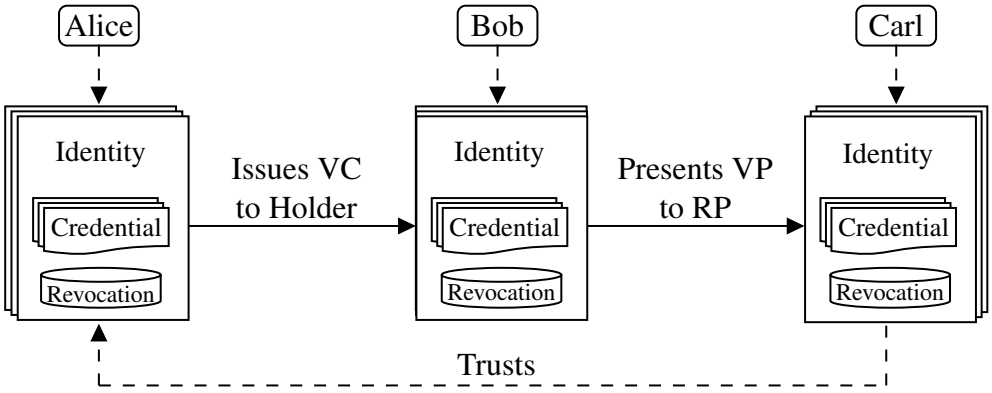
once the credential issuer has been verified in step (i), the RP can decide whether to trust the issuer. Moreover, step (iii) does not require the RP to inquire the IdP in any particular manner. Revocation registries are publicly available, and the verification is done anonymously (70, 71) without disclosing the credential's unique identifier.

While individuals in SSI have the autonomy to issue their own credentials, others are free to distrust them. For example, a bank is unlikely to accept the VP of a self-issued credential that contains a person's name and birthdate. This is true in both the real and virtual worlds. The diagram in Figure 2c depicts a high-level overview of SSI in which the user (*i.e.*, the holder) can interact with the SP using either self-issued or third-party-issued credentials. In either case, the SP is free to decide whether or not to trust the issuer.

Despite the SSI literature's use of the term VP, this concept predates SSI by many years. Prior to SSI, more than a decade of research had been conducted on how to share portions of a credential, as well as predicates over one or more attributes, without losing integrity and authenticity (72, 70). Zero-Knowledge Proof (ZKP) is the primary technique underlying VP (73, 74, 75). In short, a ZKP enables a prover to convince a verifier that she is aware of a value without disclosing the value (76). By combining ZKP and credentials, a credential holder can establish the validity and content of one or more credentials without disclosing the entire credential (74). The same is true for a VC's status. It is possible to demonstrate that a VC has not been revoked without disclosing the credential to the RP and without informing the issuer that a query for a specific credential was made (71).

In Figure 4, we illustrate the end-to-end process of issuing a VC and emitting a VP in a simplified three-actor model. In this example, three individuals own and control their e-IDs, each appropriate for a particular situation. Each e-ID is linked to a database of issued and received credentials and a revocation registry for expired or revoked credentials. One of Alice's e-IDs issues a credential to one of Bob's e-IDs, such as a declaration that he is a reputable seller of fine wines. Bob then creates and sends a VP to Carl, proving that he possesses a credential attesting to his good reputation. Carl trusts the issuer of the credential from which that VP was derived, Alice, an internationally renowned winemaker. Carl then begins negotiating with Bob. It should be noted that, in reality, the majority of people will not host revocation registries because they do not issue credentials, which is also the case for physical and digital identification documents. Moreover, it is common for SSI systems to store revocation records and VC metadata in blockchains due to its high availability (77).

Figure 4 – Actors, e-IDs, and interactions to issue a VC and present a VP.



Source: The author.

This simplified example demonstrates the trust mechanics of SSI. However, it lacks the depth and complexities of real-life scenarios. For instance, a user may create a VP using two credentials, one deemed trustworthy while the other not. Deriving trust in non-trivial scenarios is one of the open challenges in SSI.

3 POST-QUANTUM AUTHENTICATION AND AUTHORIZATION

3.1 INTRODUCTION

The OAuth 2.0 protocol introduced standard flows for a client (such as a web application or mobile app) to interact with an IdP and obtain *authorization* to share e-ID attributes or perform actions on behalf of the user (36). However, due to its emphasis on authorization rather than authentication, crucial aspects of e-ID were omitted. For example, there is no regulated method for requesting common e-ID attributes such as name and email address, nor for requesting two-factor authentication. The OIDC protocol was developed to address these issues (37). It is an extension of OAuth 2.0 that introduces uniformity for common attributes (*e.g.*, name, email, address, phone number, etc.) and permits SPs to request IdPs to enforce multi-factor authentication, among other features. OAuth 2.0 and OIDC are the current *de facto* standards for working with e-IDs. They are utilized daily by billions of users via industry-leading IdPs like Google and Facebook (now Meta).

However, these users are susceptible to quantum attackers disclosing their private information or impersonating them. Although there is no known quantum computer with sufficient processing power to break the cryptographic protocols underlying OAuth 2.0 and OIDC, intercepted communications can be stored for when such devices become available. Specifically, a *record-now-decrypt-later* attack could be used to retrieve access tokens from the past, enabling impersonation in the future. Consequently, these protocols (and their implementations) must be updated immediately to counteract this threat.

Quantum threats target applications and network protocols reliant on classical cryptography. By classical cryptography, we mean public-key schemes based on the Integer Factorization Problem (IFP), the Discrete Logarithm Problem (DLP), and the Elliptic Curve Discrete Logarithm Problem (ECDLP). Several network protocols, including JSON Web Token (JWT) and TLS, employ these schemes, which are vulnerable to Shor's algorithm (78). Under Grover's algorithm (79), symmetric-key schemes such as Advanced Encryption Standard (AES) are also threatened by quantum computing. If their security settings can be increased, they won't need to be replaced once their security is cut in half. Maintaining the initial guarantees only requires doubling the security parameters.

In this context, classical public-key schemes will likely be replaced in the future by PQC or quantum-safe cryptography (80). PQC algorithms are based on a variety of mathematical problems believed to be intractable by both non-quantum and quantum adversaries. The alternative PQC solutions are based on lattice-based cryptography, multivariate cryptography, code-based cryptography, hash-based cryptography, or isogeny-based cryptography. In this context, a global-scale transition to PQC is expected in the coming years, with systems, protocols, and applications in general beginning to use new cryptographic schemes. We anticipate that the same transition will occur for OAuth 2.0 and OIDC. One challenging part of this transition to PQC is the increased size, which can impose delays in the protocol. Besides, they can incur in

other performance drawbacks (*e.g.*, increased computational time).

In this chapter, we analyze the essential components of OAuth 2.0 and OIDC, suggesting and empirically evaluating modifications to protect them from quantum attackers. In conclusion, our contributions are as follows:

- We conduct a rigorous and reproducible SLR to determine the current state of post-quantum OIDC and OAuth 2.0;
- We propose improvements to OAuth 2.0 and OIDC, as well as their underlying protocols TLS and JWT, to make them quantum-safe;
- We provide a post-quantum implementation of OIDC, built with the integration of PQC algorithms in JWT and also TLS, as well increasing parameters in symmetric primitives; and
- We conduct a series of reproducible experiments using a realistic scenario and multiple configurations to evaluate the performance of our proposal.

The rest of this chapter is structured as follows. Section 3.2 provides a contextualization about the security considerations of OAuth 2.0 and OIDC, and also discusses TLS, and PQC. The rigorous SLR conducted to discover and evaluate existing approaches is then presented in Section 3.3. Section 3.4 proposes changes to these protocols to make them more resistant to quantum attackers, and Section 3.5 introduces our evaluation strategy and the results obtained. Section 3.6 concludes this chapter with closing remarks. This chapter has been previously published as a full conference paper (81):

Schardong, F., Giron, A. A., Müller, F. L., & Custódio, R. (2022, November). **Post-Quantum Electronic Identity: Adapting OpenID Connect and OAuth 2.0 to the Post-Quantum Era**. In International Conference on Cryptology and Network Security (pp. 371-390). Cham: Springer International Publishing. DOI: https://doi.org/10.1007/978-3-031-20974-1_20

3.2 CONTEXTUALIZATION

OAuth 2.0 and OIDC Security Considerations

Known threats to OAuth 2.0 and OIDC include resource owner password guessing, token fabrication, Cross-Site Request Forgery (CSRF), eavesdropping access tokens, and client impersonation of resource owner (82). Let us roughly divide the attack surfaces into two categories: communication and stationary. To mitigate communication-related threats, both OAuth 2.0 and OIDC require the use of TLS (83) to authenticate RP and IdP and to ensure the integrity and confidentiality of exchanged messages (36, 37). Regarding stationary data protection, however, the original OAuth 2.0 specification does not specify how tokens (`refresh_token` and

`access_token`) should be constructed; it only states that other parties should be unable to generate, modify, or guess them (36). The OIDC protocol, on the other hand, requires the use of JWT (84) to implement the `id_token` (37).

The JWT is a JavaScript Object Notation (JSON)-based data structure consisting of a header, content, and signature. The header describes the cryptographic operations performed on the content: none, encryption, signature, or both. The JWT-based `id_token` must be signed. The IdP makes the public keys for signature verification available in a publicly accessible endpoint called `jwks_uri`, the value of which can be found using OIDC-D (49). This URI returns a *JSON Web Key (JWK)* (85), a JSON structure containing the public key, key id, and other key-related data. It is worth noting that there is an OAuth 2.0 equivalent to the OIDC-D specification, namely the *OAuth 2.0 Authorization Server Metadata* (86), as well as a specification that standardizes the use of JWT for OAuth 2.0, namely the *JWT Profile for OAuth 2.0 Access Tokens* (87).

Transport Layer Security 1.3

To exchange protocol messages, OIDC and OAuth 2.0 require a secure and authenticated communication channel. Both standards require the use of TLS for communication security. The TLS protocol (version 1.3) is defined on RFC 8446 (83) and is often used in this scenario. TLS consists of three components: a Handshake protocol, where an Authenticated Key Exchange (AKE) takes place; a Record protocol specifies symmetric encryption for the communication; and an Alert Protocol, which specifies error messages and conditions.

An AKE is performed in every TLS 1.3 full handshake. The parties exchange a shared secret that is further derived into a set of traffic keys, later used in the Record Protocol for encrypting application data. During the handshake, the TLS server authenticates itself to the TLS client. A x509 digital certificate is often used, but authentication with Pre-Shared-Key (PSK) is also supported. The server can, optionally, request client authentication. We describe the handshake in three steps:

1. The client send the first handshake message: `ClientHello`, among with optional extensions. Normally it sends a random nonce, protocol versions, list of supported ciphersuites, among other information. For forward secrecy, a `keyshare` is sent composed by the Elliptic-Curve Diffie-Hellman Ephemeral (ECDHE) public part. Although optional, at least a keyshare or a Pre-shared-Key message must be sent.

2. The server replies with negotiated parameters, such as the selected ciphersuite, and additional (optional) messages. A certificate and certificate verify message is often present part of TLS server authentication. The first is the digital certificate and the second is a signature for key confirmation. An alternative is the server authentication through the PSK, *e.g.* in a resumption session, where the certificate is not sent by the server. The authentication ends with the `finished` message, where a HMAC is computed from the transcript

of the handshake context. At this point, the server can send encrypted application data to the client.

3. Upon reception, the client can complete the `ECDHE` Key Exchange (KEX) and derive symmetric keys for the communication. The handshake is completed with the client's `finished` message.

After the authentication and exchange of symmetric keys, the parties then communicate application data using encrypted records. The ciphersuite in use is the one agreed during the handshake; if they do not agree on a ciphersuite they abort the communication (specified in the Alert Protocol). Examples of ciphersuites specified by the Internet Assigned Numbers Authority (IANA) include (88): `TLS_AES_128_GCM _SHA256`, `TLS_CHACHA20_POLY1305_SHA256`, among others.

The TLS Alert Protocol defines error situations and actions that TLS peers have to take. There are two types of alerts: closure or error. Closure alerts are important to avoid the "truncation attack" (89), and they occur voluntarily, whereas an error alert causes both parties to immediately close the connection. All alert messages are encrypted as specified by the current connection state.

Post-Quantum Cryptography

At the time of writing, algorithms part of PQC (also called Quantum-Safe cryptography) are under scrutiny by the cryptographic community. Designed to be resistant to a Cryptographically Relevant Quantum Computer (CRQC), PQC algorithms can execute in classical computers to protect data against both classical and quantum attackers. The protection is based on mathematical assumptions with no (known) quantum or classical solution.

National Institute of Standards and Technology (NIST) is conducting a notable PQC standardization process (80), and several international agencies have declared that they will follow the NIST PQC process (90). The proposals are for KEX and digital signatures. Currently at Round 4, NIST selected CRYSTALS-Kyber for KEX, and Dilithium, denoted as the primary choice, Falcon, and SPHINCS+ for digital signatures. Even though some PQC algorithms belong to the same group (or type), their public keys and output sizes are different. This information is presented in Table 2. The sizes are given in bytes, and correspond to NIST security levels 1 through 5. Level 5 increases both security and the size of public keys and outputs.

The differences between the algorithms compose some of the important factors to consider when deploying PQC in network protocols. For instance, Sikeridis et al. (91) showed that the increased size of PQC can slowdown network performance due to Transmission Control Protocol (TCP) congestion control mechanisms. In addition to sizes, computational cost is also an important factor, but it can vary significantly on different hardware and specific implementations.

Table 2 – PQC algorithms sizes in bytes (NIST's Process Round 4 finalists).

Type	Based on	Algorithm	Public Key Size	Output Size
KEX	*Lattice*	Kyber	800 to 1568	768 to 1568
Signature	*Lattice*	Dilithium	1312 to 2592	2420 to 4595
		Falcon	897 to 1793	690 to 1330
	Hash	SPHINCS+	32 to 64	7856 to 49856

Source: The author.

One of the weaknesses of TLS 1.3 is that it does not prevent from quantum attacks. To address this issue, researchers start to develop and test quantum-safe algorithms integrated in the protocol's handshake. One notorious initiative is the Open-Quantum Safe (OQS) project, which provides PQC libraries and integrates it in a variety of network protocol implementations, such Open Secure Sockets Layer (OpenSSL) (92). Using those libraries, literature shows different TLS benchmarks comparing post-quantum and classical implementations (93, 91). In summary, lattice-based algorithms are generally fast but with an increase in terms of size of cryptographic objects (*e.g.*, public keys). Additionally, there are disruptive proposals, which changes the TLS handshake aiming for a better performance. One example is KEMTLS (94) and KEMTLS-PDK (95), which replaces signature schemes used in TLS handshakes by post-quantum KEMs. Still, PQC adoption in TLS remains challenging in practice, since revocation data in TLS, PKI migration issues and other situations are not yet fully explored by the literature.

3.3 SYSTEMATIC LITERATURE REVIEW

We perform a SLR to determine the current state of Post-Quantum designs for OIDC and OAuth 2.0.

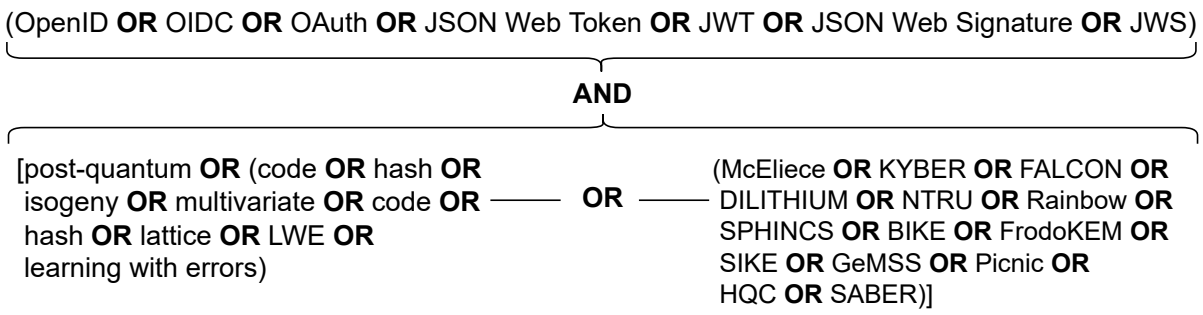
Method

The review protocol consists of five steps (19): (i) research questions definition; (ii) search strategy for primary studies; (iii) definition of inclusion criteria; (iv) classification of the papers; and (v) data extraction.

The first step is to establish the scope, which we do by developing two research questions. We want to understand "*How and which PQC algorithms were used to secure OIDC and OAuth 2.0?*" and "*What is the impact of replacing quantum-vulnerable cryptographic primitives with PQC alternatives?*" Our search strategy is based on these research questions and consists of using related PQC terms defined in a search string. The search string is used to query primary study sources (*e.g.*, SpringerLink). We constructed the string in accordance with the Population, Intervention, Comparison, Outcomes, and Context (PICOC) guideline (96), where the *population* consists of OIDC, OAuth 2.0, and JWT; PQC is the *intervention* tech-

nique; and the underlying mathematical assumptions and names of PQC algorithms were used for *comparison*. It is worth noting that when we ran the search string, we discovered that the terms referring to the PICOC *outcomes* and *context* significantly reduced the number of papers returned by the search libraries. As a result, we simplified the search string in order to increase the number of papers. Figure 5 depicts the final search string.

Figure 5 – Search string.



Source: The author.

Typically, a systematic study identifies selection criteria for relevant papers, *i.e.*, papers that provide (partial or complete) answers to the research questions. In Table 3, we define one Inclusion Criterion (IC) and two Exclusion Criteria (EC). In summary, ECs exclude papers that are not primary computer science studies, and if the paper satisfies IC-1, it will be included in our results set.

Table 3 – Inclusion and exclusion criteria.

Inclusion Criteria	
IC-1	The paper investigates or proposes post-quantum OAuth 2.0 or OIDC.
Exclusion Criterion	
EC-1	The search result is a book of proceedings.
EC-2	The research work is not in the area of computer science.

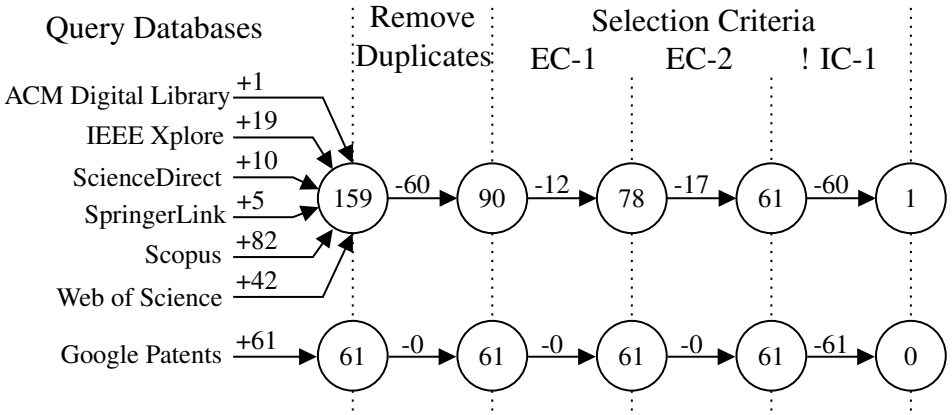
Source: The author.

Execution

Figure 6 depicts the search execution method. We queried databases for primary studies and patents on May 4, 2022. Each action outlined eliminates unrelated search results. After applying IC-1, the final set of related works consists of a single primary study. This finding suggests that little research has been conducted on this subject to date.

Our systematic search revealed a single relevant work. Alkhulaifi and El-Alfy (97) assessed the performance of two lattice-based signature algorithms for JWT authentication. They compared two PQC algorithms (Dilithium and qTesla) to Rivest-Shamir-Adleman (RSA)

Figure 6 – The steps of our SLR.



Source: The author.

in their study. They selected the NIST PQC process (Round 2) implementations using security levels one and three. The JWT body in their implementation is composed of random data. They demonstrated that Dilithium achieves superior performance when deployed in an HTTP client-server implementation, both in terms of requests per second and average response time. The comparison focuses solely on signatures, so the transfer of public keys does not factor into the evaluation. In addition, their research only considered local evaluations, *i.e.*, client and server running on the same machine, thereby excluding network conditions from the analysis.

After conducting a SLR, we identified open challenges. First, there are no practical OIDC or OAuth 2.0 post-quantum evaluations. A practical evaluation would include network conditions imposed by geographically distant servers and the connections required to complete authentication and authorization processes following these protocols. This void is the primary focus of our efforts. Secondly, the only post-quantum JWT evaluation does not take elliptic-curve signatures into account, resulting in superior performance and smaller sizes compared to RSA (97). It is crucial to include elliptic curves in the analysis, particularly when comparing to PQC sizes.

3.4 POST-QUANTUM OAUTH 2.0 AND OPENID CONNECT

OAuth 2.0 and OIDC are application-level protocols that delegate the majority of the security heavy-lifting to TLS and JWT. Aside from mandating the use of these protocols as building blocks and providing implementation guidance to prevent security flaws, few security requirements remain undefined.

OAuth 2.0 includes numerous security considerations for protocol-level messages and parameters. The only other security requirement besides the use of TLS is that the probability of an attacker guessing a token must be less than or equal to 2^{-128} and ideally 2^{-160} (36). In other words, servers must issue tokens randomly (one token must be independent from others). Consequently, given that: (i) access tokens can have a long lifetime; and (ii) a malicious agent

can perform a *record-now-decrypt-later-attack* with a quantum computer using Grover's algorithm (79); the probability of guessing a token must be reduced to less than 2^{-256} and preferably less than 2^{-320} to account for quantum attackers.

Transporting tokens via OAuth 2.0 and OIDC requires the use of the TLS protocol. At the time of writing, the most recent version of TLS is 1.3, which is also vulnerable to quantum attacks. In the context of TLS, there are three major concerns about quantum attackers. First, the minimum block size for symmetric encryption in AES is 128 bits, which is vulnerable to Grover's algorithm and must be increased to 256 bits in order to maintain the same level of security. Second, TLS authenticates the server and, if mutual authentication is enabled, the client using x509 digital certificates. Since the authenticity of digital certificates is dependent on digital signatures and Shor's algorithm (78) poses a threat to IFP, DLP, and ECDLP-based signature algorithms such as RSA and Elliptic Curve Digital Signature Algorithm (ECDSA), quantum-safe signature schemes must be utilized instead. Third, TLS employs KEX mechanisms such as Diffie-Hellman Ephemeral (DHE) and ECDHE to derive symmetric keys and for Forward Secrecy. However, these mechanisms are vulnerable to Shor's algorithm and must therefore be replaced with quantum-safe alternatives.

Quantum attackers also pose a threat to the JWT family of specifications. The JSON Web Encryption (JWE) (98) and JSON Web Signature (JWS) (99) standards describe, respectively, how to encrypt and sign JWTs. Although token encryption is not required by OAuth 2.0 or OIDC, 256-bit AES must be used to achieve 128-bit security against quantum attackers if it is used. JWE implementations must support both 128-bit and 256-bit AES block sizes (100), in general, not a significant issue. Additionally, the same flaws that affect x509 signatures also affect JWT signatures. Consequently, Post-Quantum (PQ) signature algorithms are required.

To successfully communicate, both IdP and RP must support PQ signature algorithms in their TLS and JWT implementations. Unlike TLS, where the handshake is terminated if client and server support different signature algorithms, in OIDC the "signing party MUST select a signature algorithm based on the algorithms supported by the recipient" (37). Thus, we propose replacing "MUST" with "MAY" to allow the signing party to refrain from signing a JWT with an insecure signature algorithm if the recipient does not support PQ signature.

Finally, it is critical to consider the implications of increasing symmetric encryption block and key sizes, as well as replacing KEX and signature algorithms with quantum-resistant alternatives. At the time of writing, the NIST standardization process was not completed. Nonetheless, the finalists' KEX and signature algorithms have larger key and signature sizes than elliptic curve solutions. As a result, identity architects and implementers must be aware of the additional requirements for storing and transporting Post-Quantum JSON Web Tokens (PQ-JWTs) in Post-Quantum Transport Security Layer (PQ-TLS). To that end, we empirically evaluate the NIST's final signature algorithms in a real-world OAuth 2.0 and OIDC implementation with PQ-TLS, as described below.

3.5 EMPIRICAL EVALUATION

Case Study

Although the three-party authorization handshake is emphasized in scientific and non-scientific literature, it represents only a portion of the interactions that occur when a real RP consumes user data from an IdP. Figure 7 depicts the entirety of our scenario, which includes the following interactions.

The first set of interactions is identified by the dotted rectangle with a capital letter A in the upper-right corner. As stated previously, an RP must first determine the URLs of an OIDC provider's endpoints. The OIDC-D (49) specification defines `/.well-known/openid-configuration` for this specific purpose. In response to an HTTP `GET` request to this resource, the IdP returns a JSON containing its endpoints. Figure 7 depicts the endpoints returned by the IdP that are subsequently utilized. The RP then accesses the `jwks_uri` returned in the previous step to obtain the public keys used to sign the tokens.

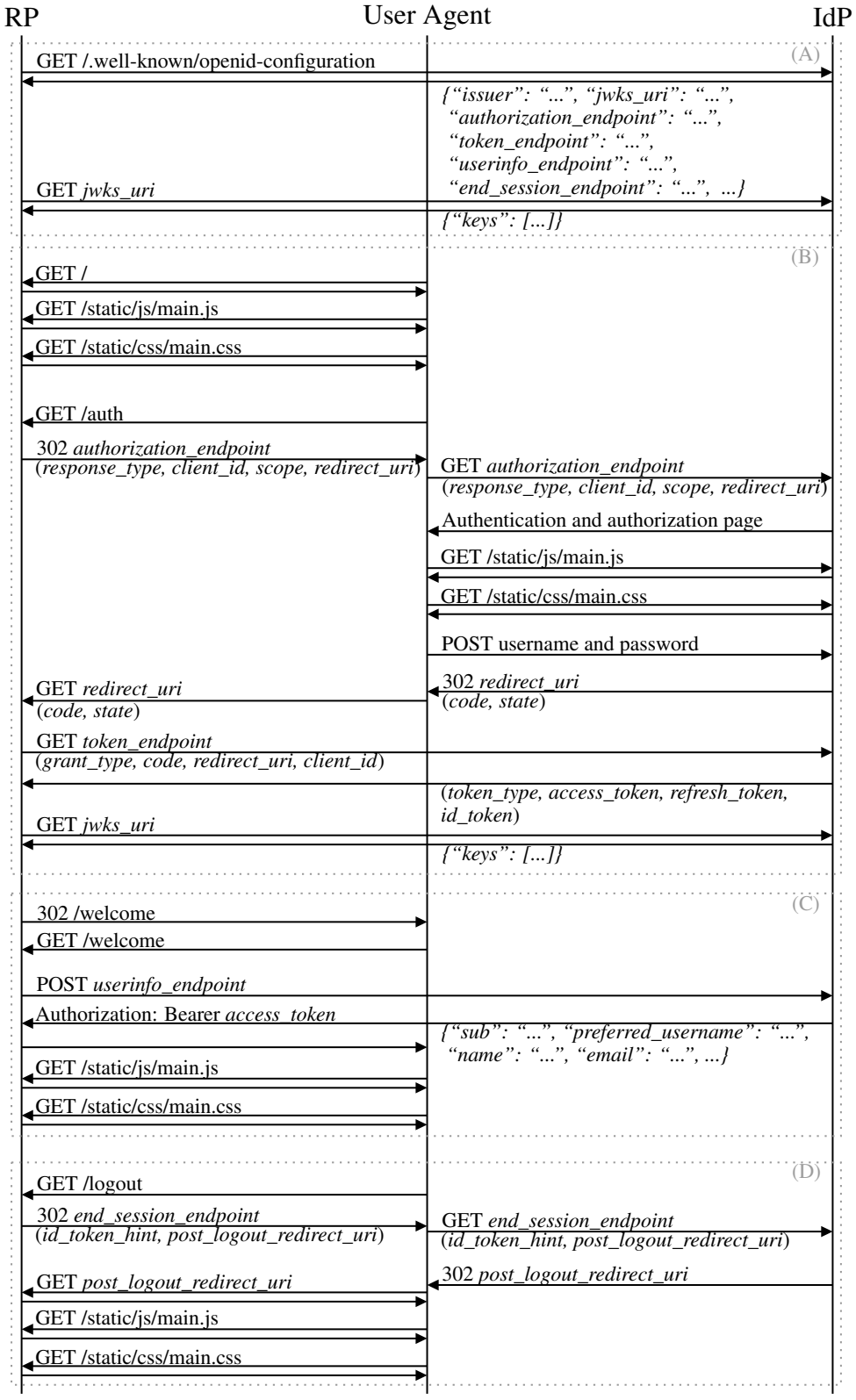
The second set of interactions, referred to as B, begins with the user accessing the RP's main page, which uses Cascading Style Sheets (CSS) and JavaScript (JS) resources. We combined all JS and CSS into a single file. The user then accesses a protected page, which requires identification and authentication of the end user as well as authorization for the RP to access their personal information. This initiates the three-party authorization handshake, which redirects the user to the IdP authentication and authorization page, which includes its own CSS and JS resources. The user then enters their username and password for authentication and, on the same page, checks the box to authorize the sharing of their nickname, full name, and e-mail.

The back-channel portion of the handshake begins after submitting the correct information and being redirected to the RP. Three tokens are created in our scenario: the OAuth 2.0 `access_token` and `refresh_token`, as well as the OIDC `id_token`. They are all JWT-based and signed with the same private key. It is worth noting that the RP then makes a second request to the `jwks_uri`. This occurs because the IdP may have rotated the keys used to sign the tokens, necessitating the acquisition of a new copy of the public key currently in use.

Following the authentication and authorization message exchange, the third set of requests and responses begins by redirecting the user to a welcoming page. The user agent requests the `welcome` page, causing the RP to contact the IdP and request the previously authorized user data. The RP incorporates the previously issued `access_token` into the request, which is validated by the IdP, resulting in the retrieval of the requested data. The RP assembles the welcoming page using this data and returns it to the user, including CSS and JS files.

The final group of interactions pertains to the user's logout. Beginning with the user requesting logout from the RP, the user agent is redirected to the `end_session_endpoint`URI of the IdP, which contains the `id_token`, and the `post_logout_redirect_uri` of the RP. This is theURI of the RP to which the user will be redirected after terminating her session on the IdP.

Figure 7 – The realistic evaluation scenario.



Source: The author.

There are twenty two GET and POST requests in our real-world scenario. It is build on top of OAuth 2.0 (36), JWT Profile for OAuth 2.0 Access Tokens (87), OIDC core (37), discovery (49), RP-Initiated Logout (101) and the JWT family (99, 98, 85, 100, 84).

Prototype Implementation

We implemented the evaluation scenario in Python 3 using `pyoidc`[1], an OpenID Foundation-certified OIDC Core, OIDC-D, and OIDC-DCR implementation. JWTs are assembled, encrypted, and signed using `pyjwkest`[2]. In order to have a functional Post-Quantum OpenID Connect (PQ-OIDC) implementation, the NIST's fourt round finalist signature algorithms were added. We used the Python 3 binding of OQS to access the C implementation of these algorithms (92). The OQS project also provides a modified `libssl` containing the Post-Quantum Key EXchange (PQ-KEX) and PQ singing algorithms, which our Python implementation employs for PQ-TLS. Our implementation and empirical evaluation are embedded within Docker containers, making it simple to reproduce our experiments. The source code for our implementation and experiments is open-source and publicly available[3].

Experiment Plan

The experiment entails evaluating the size of messages exchanged and the elapsed time for pre-quantum and post-quantum KEX and signature algorithms in the previously described evaluation scenario on servers with increasing geographical distance. Let us concentrate on the impact of size on PQ algorithms. Except for cryptographic objects, the content of messages exchanged in our scenario remains constant, allowing us to create an estimate of the impact of cryptographic objects in pre-quantum and post-quantum OIDC. The overall cost $OIDC^{size}$, in bytes, can be defined as shown in Equation 3.1.

$$\begin{aligned} OIDC^{size} =& N_{TLS} * (TLS^{size}_{KEX} + TLS^{size}_{Auth}) + \\ & N_{JWT} * JWT^{size}_{Sig} + \\ & N_{JWK} * JWK^{size}_{PK} \end{aligned} \tag{3.1}$$

Where N_{TLS} is the number of TLS Handshakes; TLS^{size}_{KEX} refers to the size of the TLS `ClientHello` and `ServerHello` messages; TLS^{size}_{Auth} corresponds to the size of TLS authentication considering handshake signature and certificates; N_{JWT} is the number of JWTs exchanged and JWT^{size}_{Sig} is the size of the signature present in each JWT; N_{JWK} is the number of public keys stored in JWKs exchanged in the scenario, and JWK^{size}_{PK} the size of those keys.

It is important to note that for TLS authentication, we incorporate the CA intermediate and root certificates. Also, to better reflect real-world settings, the server certificate incorporates

[1] https://github.com/OpenIDC/pyoidc
[2] https://github.com/IdentityPython/pyjwkest
[3] https://github.com/fredericoschardong/post-quantum-oidc-oauth2

Signed Certificate Timestamp (SCT)s, a standard for publicly reporting TLS server certificates as they are issued or observed for the sake of auditing CAs' activity (102). In addition, due to TLS connection resumption across peers, not all TLS handshakes in the real world have identical sizes. To simulate the worst-case scenario, however, we perform a new TLS handshake for each of the $N_{TLS} = 22$ connections. Consequently, this model provides an upper bound for the expected cost (in terms of size) for OIDC scenarios. Furthermore, N_{JWK} is 2 as there are two calls for the `jwks_uri`, and N_{JWT} is 8: the IdP issues one `access_token`, one `refresh_token`, and one `id_token` that are sent to the RP; the RP then sends the `access_token` to consume the `userinfo_endpoint`; and the request to `/logout` and the following redirect results in the exchange of the `id_token` four times.

Table 4 shows configurations used in each experiment, as well as the expected costs, in bytes. The first two rows show the experiments where classical cryptography is in use, while the following rows compose the post-quantum evaluations. We estimate the costs of the cryptographic objects present in each TLS handshake (second and fourth columns), as well as the JWT and JWK (fifth and sixth columns), which include a digital signature and the public key. Unlike the TLS handshake, which occurs for all twenty-two requests in our scenario, the JWT and JWK parts are present in some messages, as described above.

Table 4 – Algorithm configurations with expected costs in terms of size in bytes.

TLS_{KEX}	TLS_{KEX}^{size}	TLS_{Auth} JWT_{Sign}	TLS_{Auth}^{size}	JWT_{Sig}^{size}	JWK_{PK}^{size}	$OIDC^{size}$
ECDHE	626	ECDSA	1563	64	64	48798
		RSA 2048	3309	256	256	89130
Kyber512	1976	Dilithium 2	19419	2420	1312	492674
		Dilithium 3	26576	3293	1952	658392
		Dilithium 5	36309	4595	2592	884214
		Falcon-512	7541	690	897	216688
		Falcon-1024	13919	1330	1793	363916
		SPHINCS+128	103553	17088	32	2458406
		SPHINCS+192	215166	35664	48	5062532
		SPHINCS+256	316869	49856	64	2458406

Source: The author.

We selected ECDHE and Kyber512 for the pre-quantum and post-quantum TLS KEX, respectively. ECDHE p256 is standardized and Kyber is the finalist of the NIST Round 4 standardization process. As we can see in Table 4, TLS authentication have a significant impact, and so we compared two commonly-used classical algorithms (ECDSA p256 and RSA 2048) against three post-quantum (Falcon, SPHINCS+, and Dilithium), the latter are going to be standardized by NIST. For simplicity, the same algorithm is used for TLS authentication and JWT Signature. The overall cost is increased in the post-quantum scenarios. Regarding SPHINCS+, we selected SHAKE256 as hash function, due to the overall performance without considering

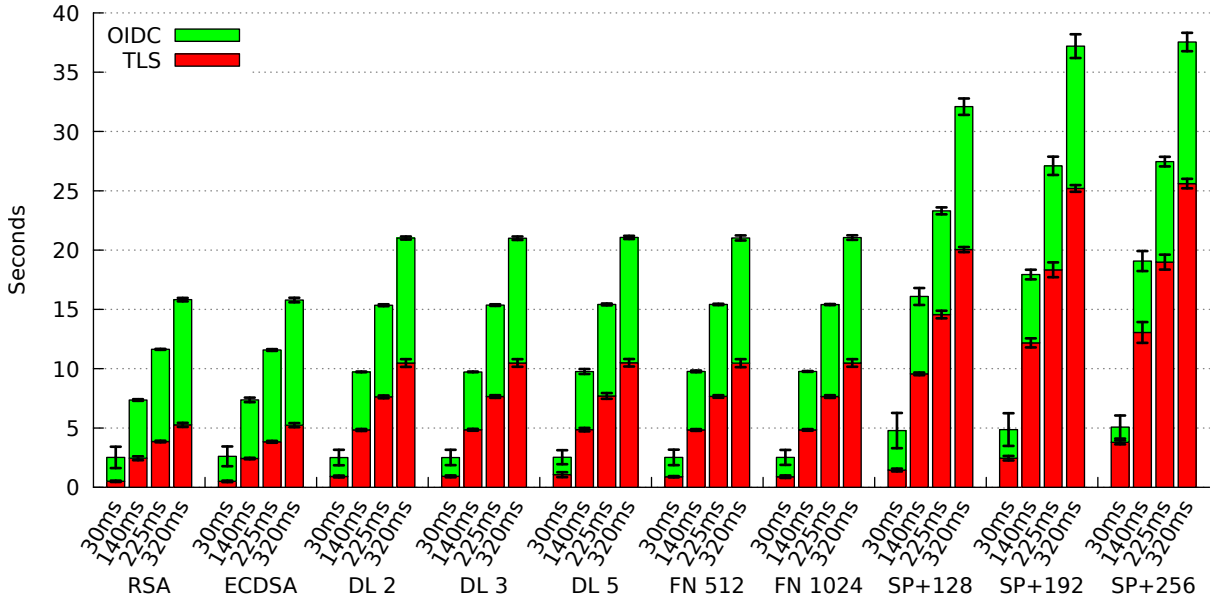
hardware optimizations; and with `fast-simple` parameter set, also focusing on performance (please refer to (103) for additional information).

Experimental Results

We ran the realistic scenario a thousand times for each algorithm configuration described in Table 4 on Amazon Elastic Compute Cloud (Amazon EC2) t2.micro instances with 1 virtual CPU (vCPU) and 1 GB of RAM in five distinct locations and collected data. We begin by outlining the timings for each algorithm option. Figure 8 depicts the results of all scenarios examined, highlighting the timings of TLS handshakes in relation to the entire OIDC time. When network latencies increase between scenarios, we can see distinct behavior. Post-quantum algorithms benefit from low latencies, achieving similar (or even greater) performance than classical algorithms. When considerable latencies are present (140ms, 225ms, and 320ms scenarios), RSA and ECDSA perform better. It is worth noting that the increasing latencies were only applicable to the communication between the simulated end-user and the SP and IdP servers. The service and identity providers were always placed on the same remote datacenter, having negligible latency between them.

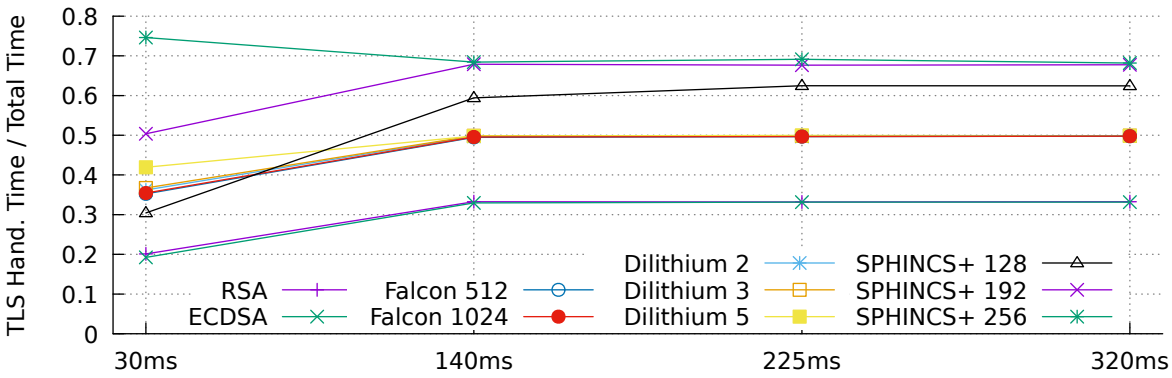
The increased size of PQC algorithms has a severe impact on network performance, frequently requiring additional round trips to convey data, particularly at the TCP level due to congestion management techniques. When post-quantum methods are tested at the same latency, the total duration varies little between Dilithium and Falcon, but significantly with SPHINCS+. We can also see that TLS costs account for a large portion of total time, particularly in PQC configurations.

Figure 8 – Average OIDC and TLS timings for various latency settings.



Source: The author.

Figure 9 – The ratio between TLS handshake and overall OIDC time.



Source: The author.

Figure 9 depicts a new perspective on TLS costs. It displays the average TLS handshake time in relation to the average total time, allowing us to compare the PQC and conventional algorithms. The ratio for Falcon and Dilithium is approximately 50% on the 140ms, 225ms and 320ms scenarios. This finding implies that enhancing TLS handshake may result in improved OIDC overall performance.

Finally, Table 5 compares the costs in terms of bytes of the 22 TLS handshakes (KEX and Authentication) to the application payloads (including Hypertext Markup Language (HTML), CSS, and JS content, as well as JWT and JWK sizes). It is evident that the larger application sizes (about 1 MB) contribute to obfuscating the distinctions between PQC instances (with different parameter sets). On the other hand, when these costs are compared to the traditional techniques, the slowdowns are considerably more visible, as seen in Figure 8. This is an interesting finding: despite increasing security parameters, the cost did not rise considerably enough to cause performance issues (from 1 to 5). However, our SPHINCS+ instances excessively increased the sizes, which explains the longer timings (Figure 8). This suggests that SPHINCS+ should not be the first option for all TLS components (*e.g.*, Online Certificate Status Protocol (OCSP) (104) Stappling, SCT Logs) or TLS-dependent protocols (*e.g.* OAuth 2.0, OIDC) due to the signature size.

3.6 CONCLUSION

Experimenting with PQC in protocols such as OIDC demonstrates the costs and consequences of its adoption. In this chapter, we assess a Quantum-safe implementation of OIDC with realistic scenarios, including the use of PQC signatures in JWT and post-quantum TLS as the underlying security protocol.

In our study of a realistic scenario, we demonstrated that the quantity and complexity of requests to use OIDC exceeds the three-party handshake established in OAuth 2.0. Nonetheless, we successfully incorporated PQC into the proposed OIDC study case, and the experiments demonstrated that the network has a considerable impact on performance. Our PQC implemen-

Table 5 – TLS cost versus OIDC cost, measured in bytes.

Algorithm	TLS Hand.	OIDC	Ratio
ECDHE/ECDSA	48158	1017405	0.0473
ECDHE/RSA2048	86570	1019903	0.0848
Kyber512/Dilithium2	470690	1043463	0.4510
Kyber512/Dilithium3	628144	1056528	0.5945
Kyber512/Dilithium5	842270	1072090	0.7856
Kyber512/Falcon512	209374	1025579	0.2041
Kyber512/Falcon1024	349690	1034530	0.3380
Kyber512/SPHINCS+128	2321638	1857118	1.2501
Kyber512/SPHINCS+192	4777124	2182244	2.1891
Kyber512/SPHINCS+256	7014590	2314753	3.0304

Source: The author.

tation in lower latencies has demonstrated competitive performance against RSA and ECDSA. Consequently, our empirical evaluation has demonstrated that PQC algorithms do not decrease OIDC performance in such scenarios. However, when latency increases, we discovered substantial performance issues, primarily owing to the increased size of PQC objects exchanged between the parties involved. Surprisingly, we found no significant variations in performance between PQC algorithms of varying security levels when comparing conventional to PQC methods.

We discovered that the TLS cost in OIDC constitutes a considerable portion of the costs, both in terms of time and size, particularly when network latencies are greater. Since we simulated actual setups (*e.g.*, SCTs and OCSP Stappling in certificates), we conclude that our findings provide an upper bound on TLS costs when evaluating it as a drop-in replacement for PQC in OIDC.

The scope of this work allows for several other areas of research to be pursued in the future. For example, we examine a PQC-only deployment, but another option may be hybrid PQC, which employs both PQC and classical algorithms. Using hybrids in OIDC would necessitate their deployment in TLS and JWT, the latter of which will almost certainly encounter compatibility challenges due to its list of authorized methods. Furthermore, certain techniques, such as KEMTLS (94), try to reduce the TLS costs of PQC. If TLS costs are reduced, performance benefits in PQ-OIDC can be expected.

4 SYSTEMATIC LITERATURE REVIEW OF SSI

4.1 INTRODUCTION

Despite the fact that SSI provides sovereignty over the digital presence, it introduces new challenges that must be overcome before widespread adoption can occur. The difficulties are conceptual and pragmatic in nature. The primary conceptual problems are defining SSI and defining what constitutes a self-sovereign system. The pragmatic challenges include, but are not limited to, how to coexist with and migrate existing IdPs' identities to the new model, how to trust data from other self-sovereign identities, and how to assist users, also known as identity holders, with managing, backing up, and recovering private data.

The advantages of this new identity paradigm over traditional models have attracted researchers' and professionals' attention in recent years, resulting in an increasing number of publications on the subject. Some initiatives aim to review and condense the body of knowledge thus far. However, current reviews do not address all facets of SSI. For instance, they omit publications that contribute to the conceptual debate over the meaning of the term "self-sovereign identity" and efforts that present novel problems and solutions in specific areas of SSI. Existing reviews are primarily concerned with applications and research papers that propose SSI systems such as Sovrin (105) and uPort (106).

In this chapter we conduct a comprehensive systematic review and mapping of the scientific and non-scientific literature that contribute to the debate over what SSI is, as well as works that address practical issues related to SSI. We searched for, selected, and reviewed publications in a systematic manner, which was guided by four research questions. Due to the systematic nature of our work, it may be reproduced and updated in the future to reflect new activity. The results include: (i) a taxonomy that enables hierarchical classification of the SSI literature; (ii) an in-depth and systematic analysis of the surveyed materials using our novel taxonomy; and (iii) analyses and maps of publication frequency, venues, co-references, and co-authorships, which provide a global view of the state of the art of SSI literature to the reader. Finally, open issues and recommendations for researchers and practitioners working with SSI are discussed.

In summary, we make the following three main research contributions to the field.

- Our survey examines both *conceptual* and *practical* advances in SSI, highlighting philosophical contributions to the definition of SSI, novel problems and proposed solutions, and promising directions for *future research*. The manuscript conducts an analysis of the body of knowledge established by over 80 research papers, scientific reports, patents, technological standards, and theses.

- Through a proposed *taxonomy*, we provide the reader with a comprehensive and organized understanding of the SSI literature. Additionally, the manuscript presents and discusses *maps* of authors' relationships, publication venues, and the shift in the focus of

research in the area over time. To our knowledge, this is the first survey of SSI to include a *systematic literature review*, a *systematic mapping*, and a *taxonomy*, all of which are based on *rigorous* criteria and *reproducible methodology*.

- Unlike previous surveys (14, 107, 108, 109, 7, 8, 9, 10, 11, 12, 13, 110), we examine *conceptual* discussions of SSI and include publications that are not *blockchain-based*.

The remainder of this chapter is structured in the following manner. Section 4.2 outlines the existing secondary studies that review the SSI literature and their shortcomings. Section 4.3 defines the method used in this study and how it was carried out. Section 4.4 presents the reader with the proposed taxonomy. In Section 4.5, we describe the practical research surveyed. Section 4.6 identifies and discusses mathematical and cryptographic tools used in applied research. In Section 4.7, we detail philosophical discussions regarding understanding what SSI is, and in Section 4.8, we present the results of our mapping. Finally, in Section 4.9, we discuss the open challenges and shortcomings, and in Section 4.10, we make final remarks. This chapter has been previously published as a full journal paper (77):

Schardong, F., & Custódio, R. (2022). **Self-sovereign identity: A systematic review, mapping and taxonomy.** Sensors, 22(15), 5641. DOI: https://doi.org/10.3390/s22155641

4.2 RELATED WORK

Blockchain technology pioneered the concept of Distributed Ledger Technology (DLT), in which peer consensus defines the immutable ledger's state rather than a central entity asserting authoritarian control (111). These concepts facilitate the implementation of SSI by providing a trusted online repository for electronic identities, credentials, and revocation registries (7). While blockchain technology can help the development of SSI solutions, it is not required (15, 16, 17, 18). Despite this, the majority of existing reviews claim that SSI cannot be implemented without blockchain (7, 14, 8, 9, 10, 11, 12, 13). In terms of research method, one of the existing surveys conducted a systematic mapping of the literature (107), two devised taxonomies (108, 110), one carried a meta-synthesis (109), and seven did not detail any method for selecting and analyzing primary sources (7, 8, 9, 10, 11, 12, 13). Next, we present existing secondary research in SSI.

Kuperberg (7) conducted a survey in which forty-three blockchain-based SSI market offerings were evaluated against seventy-five criteria, including compliance with applicable legislation, market availability, and cost. He stipulated that no reviewed application meets all criteria, and no SSI solution possesses the following characteristics: (i) the maturity of traditional IAM offerings; (ii) a production-level integration standard (such as OAuth 2.0 (36) or SAML (43)); and (iii) OS-level integration.

Although Liu et al. (14) presented their search string, they do not provide any information about their review method. Thirty-six research efforts and patents introducing SSI applications are reviewed in total. They examined these works from the standpoints of authentication,

privacy, and trust. They argued that despite blockchain-related innovations, there are still issues and implications remaining, namely: (i) users may lose their blockchain-based identities (wallets) and need to (ii) change their identities, which is trivial in traditional IAM but might be challenging in DLT; and (iii) the cost of integrating existing systems into the new paradigm.

Zhu and Badr (8) conducted a review of works that use DLT to implement SSI in the context of Internet of Things (IoT) devices. They expanded on the focus of Liu et al. (14) on authentication, privacy, and trust, adding a fourth dimension: performance. They alleged that the trustless environments in which IoT devices operate necessitate SSI solutions. Nonetheless, blockchain technology should be thoroughly investigated, as storing and maintaining public blockchains in IoT devices is prohibitively resource-intensive. As a result, forming small groups of private blockchains may be an option. According to the literature, one possible solution is for IoT devices to inherit the peer-to-peer trust established between their owner entities (humans, businesses, and governments) (112).

Despite the comparison of the underlying infrastructure of blockchain-based SSI offerings, three surveys that do not specify a search method produced similar results (9, 10, 11). They all mentioned the blockchain framework that the surveyed papers use, as well as the type of blockchain network (private, permissioned, permissionless, or other). Lim et al. (9) conducted a review of 15 for-profit and non-profit company-developed, government-related, and open-source applications, concluding that SSI is the optimal solution for user-centric, secure, and cost-effective IAM. Kaneriya and Patel (10) conducted a review of six SSI systems, identifying future enhancements that each system, according to the authors, should prioritize. Finally, Gilani et al. (11) reviewed eight SSI offerings, noting which support selective disclosure of personal information, how cryptographic keys are managed, and blockchain-specific details such as whether credentials are stored on or off the ledger, as well as the use of smart contracts. Smart contracts is a software that executes automatically and transparently on the ledger, allowing anyone to verify them (113).

The authors of (12) described ten SSI systems that utilize blockchain technology but did not specify how they were chosen. They did, however, conduct an analysis of these works in terms of their adherence to the SSI's ten principles, detailing which principle each reviewed paper satisfies.

In contrast to previous surveys, Mühle et al. (13) examined what they refer to as the "four basic components of SSI": identification; authentication; verifiable claims; and attribute storage. They discussed how various research studies and market offerings attempt to address each of the four components.

Čučko et al. (107) presented a systematic map of decentralized identity. They mapped one hundred and twenty papers in total, but only eighty were determined to be SSI-related. While they established a category for conceptual contributions, it was filled up with surveys and research articles highlighting SSI's challenges and opportunities. Alternatively, we consider conceptual contributions that refute or include new philosophical perspectives on what SSI is. Their map encompasses information technology fields and the various domains to which SSI is

applied, whereas our maps depict author–publication relationships.

Taxonomies for SSI are introduced by both (108, 110). The former proposes a four-tiered taxonomy encompassing registration, authentication, data management, and verifiable claims. They were used to categorize twenty-one blockchain-based solutions. The latter's taxonomy includes the facets member, interaction, ambition, and technology stack, which are used to classify one hundred and forty-seven results from a gray literature review of the SSI ecosystem culled from DuckDuckGo, Github, Reddit, and ArXiv. Both taxonomies fall short of incorporating philosophical debates about the meaning of SSI.

Finally, the authors of (109) created a meta-synthesis of SSI based on blockchain technology. Meta-synthesis is a qualitative method for aggregating knowledge derived from quantitative, qualitative, empirical, conceptual, and review studies (114). They evaluated sixty-nine works from an enterprise adoption perspective, summarizing the state of the art's technological and business challenges.

Secondary research has already revealed an increasing number of studies in this field. However, a rigorous systematic review of SSI studies is lacking. Earlier studies have examined both the practical and technical aspects of SSI systems. However, they do not evaluate conceptual debates about SSI or works that present and attempt to resolve particular pragmatic issues. On the other hand, we are interested in discovering and examining research materials that extend or refute Allen's ten principles of self-sovereign identity (3) or present and resolve practical problems in the SSI ecosystem. Table 6 summarizes the major differences between previous surveys and ours.

Table 6 – Comparison with other secondary studies in the literature.

	Systematic Review	**Systematic Mapping**	**Taxonomy**	**Include Patents**	**Other than Blockchain**	**Conceptual or Pragmatic**	**Covered Works**
Liu et al. (14)	**Yes** [1]	No	No	**Yes**	No	Pragmatic	50
Čučko et al. (107)	No	**Yes**	No	No	**Yes**	Pragmatic	80
Ghaffari et al. (108)	No	No	**Yes**	No	No	Pragmatic	21
Mulaji and Roodt (109)	No	No	No	**Yes**	No	Pragmatic	69
Kuperberg (7)	No	No	No	No	No	Pragmatic	43
Zhu and Badr (8)	No	No	No	No	No	Pragmatic	15
Lim et al. (9)	No	No	No	No	No	Pragmatic	15
Kaneriya and Patel (10)	No	No	No	No	No	Pragmatic	6
Gilani et al. (11)	No	No	No	No	No	Pragmatic	8
Dib and Toumi (12)	No	No	No	No	No	Pragmatic	10
Mühle et al. (13)	No	No	No	No	No	Pragmatic	9
Schmidt et al. (110)	No	**Yes**	**Yes**	No	No	Pragmatic	147
This work	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Both**	**82**

Source: The author.

4.3 METHOD

Secondary studies are necessary to keep track of advancements and developments as primary research efforts on a given topic evolve. Two types of secondary studies have gained

popularity in recent years in computer science (96): systematic mapping (20) and systematic literature review (19). Despite the fact that both are systematic and thus employ rigorous methods for identifying and interpreting relevant research, the former is intended to provide a broad overview and identify research trends, whereas the latter is intended to aggregate evidence in order to summarize and answer more specific Research Questions (RQs). In this study, we conducted a systematic review of the literature and a systematic mapping.

4.3.1 Planning

We followed Petersen *et al.*'s method (96), which provides detailed guidelines based on a systematic review of mapping studies. These guidelines require the following: (i) the definition of objectives and RQs; (ii) a strategy for identifying relevant studies; (iii) objective inclusion and exclusion criteria to ensure that only relevant material is reviewed; (iv) an extraction process for objectively obtaining evidence from papers relevant to the RQs; (v) a classification method; and (vi) a discussion of potential threats to the study's validity. Our research protocol, which is detailed in the following sections, complies with the aforementioned stipulations.

Research Questions

The objective of this systematic study is fourfold: (i) to examine practical challenges associated with SSI and potential solutions; (ii) to investigate mathematical formalism and cryptographic tools (primitives) used to solve these problems; (iii) to investigate conceptual advancements made to the informal definition of SSI (3); and (iv) to map SSI publications and authors. These goals result in the following RQs:

- RQ-1: What practical problems have been introduced and solved?
- RQ-2: What properties, formal definitions, and cryptographic tools have been used?
- RQ-3: What conceptual ideas have been introduced or refuted?
- RQ-4: When, where, and by whom were SSI studies published?

Search Strategy

Our investigation began by specifying a search string that was pertinent to the RQs previously mentioned. Rather than creating a potentially restrictive search query with PICOC (19) or another method of query framing, we searched for "self-sovereign identity" and variants in the title, author keywords, and abstract. Our search string is broad by design in order to encompass as many relevant articles, patents, and research materials as possible. Additionally, we placed no restrictions on the publication year, page count, conference, or journal. The following is the entirety of our query string.

self-sovereign identity **OR** self sovereign identity **OR** self-sovereignty **OR** self sovereignty

Study Selection

Our study selection process is divided into three stages. The first phase eliminates duplicate results and articles that have been republished in extended formats. Mendeley (115) was used to evaluate the results and eliminate duplicates. After a preliminary screening of the search results, it was determined that several papers do not belong in the field of computer science or are not relevant to our review. We then narrowed our search by developing two inclusion criteria and one exclusion criterion. These criteria are detailed in Table 7. In short, the exclusion criterion eliminates research that is not computer science-related, whereas the inclusion criterion prioritizes papers that contribute to SSI in response to our RQs. Articles had to meet at least one inclusion criteria.

Table 7 – Inclusion and exclusion criteria.

Inclusion Criteria	
IC-1	The paper includes a novel conceptual contribution to SSI.
IC-2	The research work makes practical progress towards SSI.
Exclusion Criterion	
EC-1	The research work is not in the area of computer science.

Source: The author.

We are not reviewing and mapping standalone SSI solutions, despite the fact that they may incorporate practical progress (such as Sovrin (105) and uPort (106)). Multiple surveys have been conducted on these works (9, 7, 14, 8). As a result, when it comes to practical progress, we prioritize works that raise specific pragmatic concerns about any aspect of the SSI ecosystem and propose solutions. Consider, for example, a piece that discusses the difficulty of recovering SSI keys that have been lost and offers a new solution to the problem. This work would comply with IC-2. Assume, however, that a research paper is published describing an implementation of SSI for IoT. While this work may make a significant contribution to the IoT literature, it does not satisfy IC-2 if it does not present a problem concerning SSI in general and a solution to that problem.

EC-1 is applied to the title, author keywords, and abstract in the second stage of our study selection process, effectively eliminating articles that are not related to computer science. The third phase involves obtaining and reading the remaining studies in their entirety, ensuring that they comply with IC-1, IC-2, or both. Then, articles that violate IC-1 or IC-2 are removed as well.

Data Extraction

To extract data from primary studies, we adapted Petersen's template (96). It is composed of three components: (i) a data item; (ii) a description; and (iii) the RQs to which the data item corresponds, as illustrated in Table 8. Except for the Study ID, which was generated manually, the *General* items were obtained from articles or their online metadata. Following the reading of a pilot set of articles, two *Conceptual* and two *Practical* data items were created to gather evidence and address the RQs.

Table 8 – Data extraction form.

Data Item	**Description**	**RQ**
General		
Study ID	Unique integer identifier per article	
Article Title	Name of the article	
Year	Year of publication	RQ-4
Article Authors	Name of the authors	RQ-4
Venue	Publication venue	RQ-4
Conceptual		
Add Concept	What concept/idea is introduced	RQ-3
Refute Concept	What concept/idea is refuted	RQ-3
Formalism		
Formal Model	How is SSI formally specified	RQ-2
Practical		
Novel Problem	What practical problem is presented	RQ-1
Proposed Solution	How is the practical problem solved	RQ-1

Source: Adapted from (96).

Taxonomy

To develop a taxonomy to categorize SSI research, we used the three-step keywording method (20): (i) the researcher reads the abstracts (and, if the abstract is of low quality, the introduction and conclusion as well), extracting keywords and concepts that indicate the article's contribution and the context of the research; (ii) the set of keywords is combined to create a high-level understanding of the research contribution; and (iii) the final set of keywords is clustered to create categories. The last step is the result of the process of making, updating, and merging categories, as well as classifying articles into the new categories that were made.

4.3.2 Execution

Search Execution

On February 15, 2022, this search string was entered into the ACM Digital Library (116), IEEE Xplore (117), ScienceDirect (118), and Springer Link (119) databases, which host popular computer science conferences and journals. To supplement our database search, we performed additional searches on Scopus Preview (120), Web of Science (121), and Google Scholar (122). Additionally, we queried Google Patents (123) on the same day and applied the search string to the title and abstract of patents, yielding seventeen results. Table 9 displays the number of search results returned by the queries.

Table 9 – Number of studies.

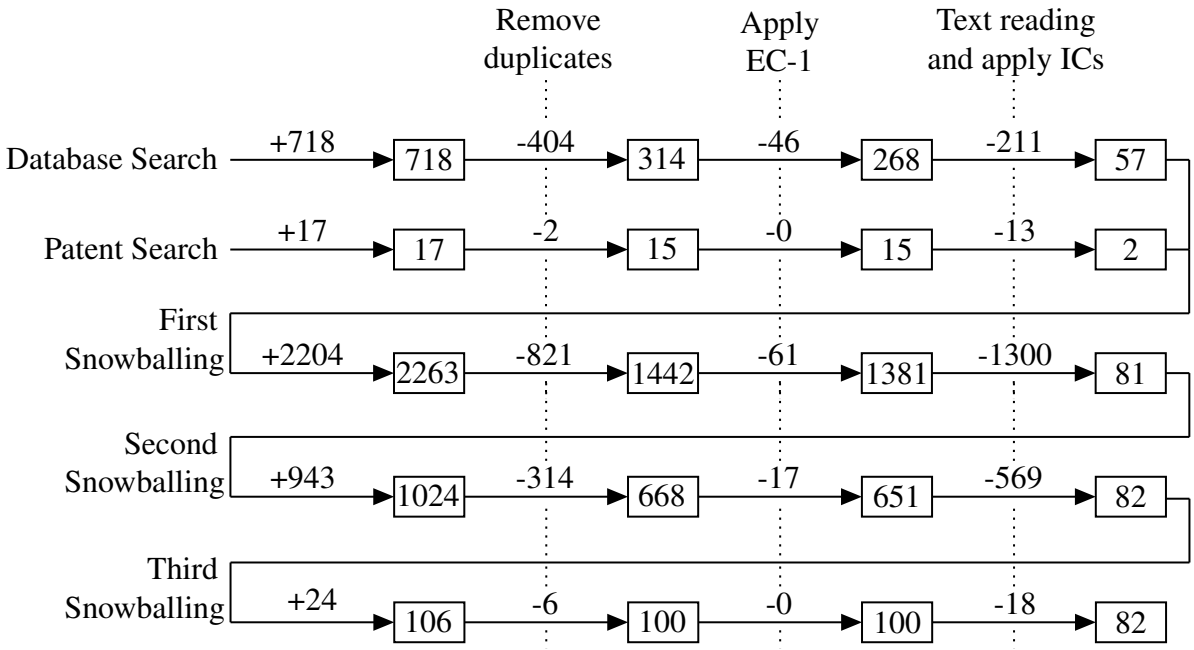
Tool	**Total**
ACM Digital Library	16
IEEE Xplore Digital Library	99
ScienceDirect	17
Springer Link	40
Scopus	235
Web of Science	131
Google Scholar	180
Database Search	**718**
Google Patents	17
Patent Search	**17**

Source: The author.

Study Selection and Data Extraction

Our three-phase study selection process was executed five times, as presented in Figure 10. We applied the first execution to the outputs of the database search and the second to the patent search results. The combined output was a set of fifty-nine works which formed the input set for both forward and backward snowballing (124). In short, backward snowballing consists of reviewing all references in a document, while forward snowballing finds other works that reference it. The snowballing was repeated until no new work was found that satisfied our selection process, which required three runs. The remaining eighty-two works constitute our result set. We should point out that two researchers independently assessed each paper at every stage of the selection process, and a conflict resolution meeting was organized. We point the interested reader elsewhere (125) for the complete list of papers, our evaluation regarding their inclusion or exclusion for all five runs of the study selection process, and the data extracted with our data collection form.

Figure 10 – Number of articles in each stage of our study selection.



Source: The author.

4.4 TAXONOMY

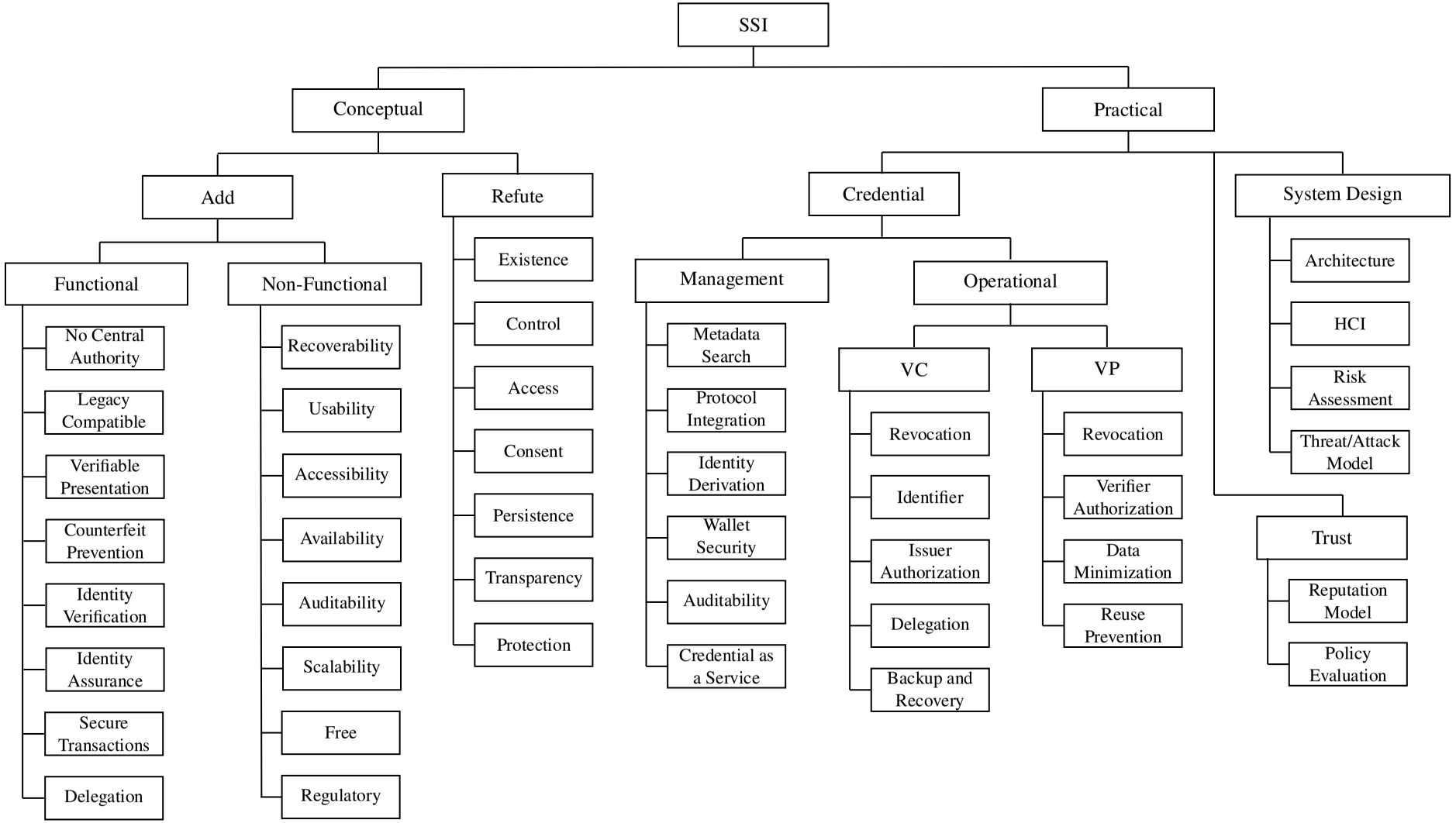
We used the keywording method (20) to identify distinguishing characteristics of the reviewed work. These characteristics were combined into a proposed taxonomy with two facets: *conceptual* and *practical*, as illustrated in Figure 11. These two facets are further subdivided into additional facets, forming a tree-like hierarchy. Concepts, sometimes referred to as terms, are the leaves of this hierarchical tree.

The *conceptual* facet categorizes the research efforts that, during our data extraction process, filled in the data items *Add Concept* or *Refute Concept* and thus help answer RQ-2. The new concepts are divided into two facets: *functional*, which refers to the well-defined functionalities of SSI systems; and *non-functional*, which refers to more generic behaviors.

The *practical* facet is used to classify publications that make pragmatic contributions, *i.e.*, those that contribute to the data items *Novel Problem* and *Proposed Solutions*, and thus related to RQ-1. It is divided into three facets that are used to analyze work that presents challenges and proposes solutions in the following areas: (i) *management* and *operational* aspects of *credentials*; (ii) *system design*; and (iii) *trust*.

The number of existing concepts under the facets of our proposed taxonomy, *i.e.*, the leaves, is likely to grow in the future. New research, for example, may introduce new pragmatic challenges. Future work can build on our proposed taxonomy and include new initiatives. We present and discuss the state-of-the-art of SSI in the following sections through the lens of the proposed taxonomy. We discuss them and the works in terms of their most defining facet, namely the objective or problem they are attempting to solve because the majority of surveyed works are classified under multiple facets due to exhibiting a variety of characteristics.

Figure 11 – Taxonomy of SSI.



Source: The author.

4.5 RQ-1: WHAT PRACTICAL PROBLEMS HAVE BEEN INTRODUCED AND SOLVED?

Our taxonomy enabled us to classify surveyed materials and generate visualizations to help answer our research questions. The data items in our data extraction form pertaining to our first research question are organized in Table 10 according to the facets and terms of our taxonomy under the *practical* facet, which were fulfilled by sixty-nine of the eighty-two reviewed materials.

4.5.1 Management

The *management* facet encompasses five characteristics that deal with the governance of credentials and claims presentation in SSI: (i) *metadata search*; (ii) *protocol integration*; (iii) *identity derivation*; (iv) *wallet security*; and (v) *credential as a service*. These concepts and the works that explore them are presented next.

Metadata Search

The authors of (126) introduced the problem of *metadata search* in blockchain-based SSI systems. Due to the unstructured nature in which data is stored in blockchain, it becomes a challenge to look for credential metadata stored on the ledger. The authors argued that creating new types of credentials comes at a monetary cost in Sovrin, and thus it is worth reusing existing credential metadata. Hence, effectively tackling the challenge of finding metadata in blockchain-based SSI results in reducing monetary cost for issuers. To attack this problem, the authors of (126) used Apache Solr (127) to build a search application that allows users to find credential metadata stored in Hyperledger Indy (128), which is the open-source SSI platform that powers Sovrin (105).

Similarly, in (129) the problem of searching metadata is also explored. The authors employed a natural language processing technique (130) and pre-trained word vectors (131) to enable users to query the Sovrin network's credential metadata using natural language. The reported results outperform (126) for queries with synonyms rather than exact terms.

Protocol Integration

Another area of study in SSI is *protocol integration* with production-level protocols such as SAML (43), OAuth 2.0 (36) and OIDC (37). Failure to successfully address this challenge may jeopardize the adoption of SSI, as billions of users have electronic identities in IdPs that can only communicate using the aforementioned protocols. This challenge was presented as the driving problem in eight research papers (132, 133, 134, 135, 136, 137, 138) and was also mentioned in three other works (139, 140, 141). Three articles aim to integrate SSI with

OIDC (132, 134, 136), two works focus on OAuth 2.0 (133, 137), one on SAML (137), and one paper on these three protocols (138).

Table 10 – Publications that introduced and solved novel problems in the SSI ecosystem.

	Credential															System Design				Trust	
	Management						Operational														
							VC					VP									
Works	Metadata Search	Protocol Integration	Identity Derivation	Wallet Security	Auditability	Credential as a Service	Revocation	Decentralized Identifiers	Issuer Authorization	Delegation	Backup and Recovery	Revocation	Verifier Authorization	Data Minimization	Reuse Prevention	SSI Design/Architecture	HCI	Risk Assessment	Threat/Attack Model	Reputation Model	Trust Policy Evaluation
(126, 129)	✓																				
(142)													✓						✓		
(75, 143)															✓						
(144, 145)			✓																		
(146)			✓																✓		
(147)			✓				✓							✓					✓		
(132, 138, 136)		✓	✓																		✓
(134)		✓	✓																		
(137, 135)		✓																			
(140)		✓																		✓	
(133)		✓																	✓		
(139, 141)		✓										✓							✓		
(148)		✓							✓										✓		
(149)									✓										✓		✓
(150)									✓												
(151)					✓							✓		✓		✓				✓	
(152)							✓					✓							✓		
(66)							✓							✓		✓					
(153)							✓							✓							
(154, 155)							✓												✓		
(73, 74, 156, 157)														✓					✓		
(158)						✓															
(159, 160)						✓													✓		
(161, 162, 163)																				✓	
(164)																			✓	✓	
(165, 166, 167)																✓					
(168)				✓																	
(169)				✓						✓						✓					
(170)										✓											
(171)					✓																
(172)					✓						✓							✓	✓		
(173, 174)											✓										
(18)										✓	✓										
(175)											✓								✓		
(176)											✓						✓				
(177, 178, 179, 180)																	✓				
(181)																	✓				✓
(182, 183, 184)																					✓
(67, 185, 186, 187, 188)								✓													
(189)								✓											✓		
(190)								✓										✓			
(191)																		✓			

Source: The author.

Using the OIDC protocol, (132) constructs a gateway between two SSI solutions (uPort (106) and Jolocom (192)) and web applications. Users can compose their identities by selecting claims, which are verified by the gateway and then transferred to the destination application for authentication via the OIDC protocol. Similarly, (134) implements an OIDC gateway between Hyperledger Indy (128) and other applications, from which users of any instance of Hyperledger Indy (such as Sovrin (105)) can benefit. In contrast to (132) a wallet application is designed to store credentials on the user's smartphone. Claims, which the user must present, are used to implement application-level authorization. (136) authenticates the issuer and holder and transfers VCs using OIDC. These VCs include an advanced or qualified signature or seal, which confirms the natural or legal person's identity. A bridge ensures that DID methods and signatures are interoperable among issuers, holders, and verifiers.

Hong *et al.* (133) used OAuth 2.0 for authorization, making it easier to integrate their solution with existing web services. In contrast to (132, 134) authentication in (133) uses a custom mechanism rather than OIDC. Lagutin *et al.* (137) were concerned about the burden of issuing and verifying VPs in resource-constrained devices such as IoT sensors and actuators. A bridge protocol is proposed in which a server receives and processes VPs before distributing modified OAuth 2.0 access tokens to authorized entities. These tokens are given to resource-limited devices, which authorize access to the resource or service.

The authors of (135) proposed an integration with SAML, which allows SSI-based identities to authenticate with SPs via SAML. Gruner *et al.* (138) presented a more comprehensive architecture that enables users to integrate various SSI offerings with SAML, OIDC, and OAuth 2.0. Additionally, they accomplished *identity derivation*, which is described below, as well as the evaluation of trust models used to accept or deny interactions.

Identity Derivation

Allowing users of SSI solutions to access web applications via the OIDC protocol resulted in the implementation of *identity derivation* mechanisms, that is, methods for deriving SSI identities from non-SSI identities. This is the primary goal of (147, 146), but it was also accomplished in (144, 145).

The authors of (147) proposed an electronic identity derivation protocol in which user attributes from various IdPs are collected and transformed into VCs. The transformed VCs can be presented using VPs. Differently, (146) employs x509 digital certificates (193) with high LoA to generate VCs with high LoA. Digital certificates achieve high LoA through a rigorous enrollment process in which the certificate subject must present government-issued documents in person. Both a digital wallet running on a device with a secure enclave and a Fast IDentity Online 2 (FIDO2) compatible token (194) equipped with a biometric fingerprint reader generate a key pair after authenticating the owner of an x509 certificate. The VC includes the two public keys. When this VC is used to generate VPs, the private keys of both the digital wallet and the FIDO2 token are accessed. Because the latter requires biometric authentication to perform

operations on the private key, the VC holder must be its owner.

Biometric data can be used to make SSI identities, so Bathen *et al.* (144) explored the possibility of replay attacks when an attacker has access to biometric templates. They contended that user-managed cancelable biometrics is the solution to this problem. A person's self-image, *i.e.*, a selfie, is passed through one-way functions to mask the original data, and the resulting data is then stored on a blockchain and managed as a credential. Mishra *et al.* (145) claimed that the underlying techniques used in (144), namely bloom filters (195), are vulnerable to invertibility and linkability attacks (196). To address these issues, their proposal uses Open Source Computer Vision (OpenCV) (197) to extract feature vectors from selfies, which are then subjected to a one-way transformation (198). Both methods generate revocable biometric credentials suitable for two-factor authentication.

Wallet Security

One patent (168) is concerned with *wallet security*. Its authors proposed a hardware-based wallet that stores cryptographic keys and credentials. It can connect to mobile devices when necessary and disconnect when not.

Auditability

When compared to other identity models, SSI provides more privacy. Nonetheless, some use cases necessitate the *auditability* of credentials or presentations. Lemieux *et al.* (171) claim there are use cases that require the collection of evidence that a VC was issued and sent to its holder, or that a VP was performed in order to comply with legal, audit, and accountability standards. They proposed using Shamir's Secret Sharing (SSS) (199) to generate a group key capable of encoding and decoding Personal Identifiable Information (PII), such as VCs or VPs, and storing it in a proof registry, *i.e.*, a persistent storage for auditing. This group includes the issuer, the trusted audit service, and the holder. The group key can be generated by two of the three members.

Credential as a Service

Three papers discuss the drawbacks of local credential storage and issuance (159, 158, 160). We classify them as credential as a service because their solutions involve outsourcing the storage or processing of credentials.

Samir *et al.* (159) affirmed that storing VCs in a single location is a potential point of failure in SSI implementations because wallets can be lost. Furthermore, they noted that digital wallets confined to a single mobile device might not remain online at all times. To address these concerns, an anonymous multi-party computation solution based on smart contracts and SSS is proposed. It uses SSS to divide a VC into multiple shares, which are then stored on

online platforms. Then, smart contracts use multi-party computation to process requests to the VC shares.

In the same way, in (158), holders do not keep their credentials. Credentials are instead stored on a storage service and protected by a two-party protocol. Furthermore, holders do not have direct access to their data. Instead, the VC holder has control over an agent that runs on the storage service and contacts the user to request permission to share information. Users never receive their credentials in this manner, and thus do not have to worry about storing them securely. Because the credentials are encrypted using a two-party encryption protocol, the storage service cannot misuse them.

The authors of (160) postulated that having the infrastructure to issue credentials is a barrier to SSI adoption. As a result, they proposed using a cloud-based Trusted Execution Environment (TEE) (200) to issue and distribute VCs to holders.

4.5.2 Operational

The *operational* facet is divided into two facets: *VC* and *VP*. They are a collection of concepts related to the functional aspects of VCs and VPs.

4.5.2.1 Verifiable Credentials

Revocation

Credential *revocation* and status verification are long-standing problems in IAM research. The OCSP of traditional PKI, for example, allows users to query the status of a certificate. However, the query sends the serial number to the CA, revealing to the CA where the certificates it issued are being used and thus infringing on user privacy. The revocation verification of VCs in a privacy-preserving manner is an active area of research in SSI. Seven works present new approaches to addressing this challenge (147, 152, 66, 153, 154, 155).

The VCs standard from the World Wide Web Consortium (W3C) defines the metastructure and lifecycle of VCs and VPs (66). Both VCs and VPs must have the following: (i) metadata describing the data; (ii) the data; and (iii) cryptographic proof of integrity and authenticity. Aside from the roles of issuer, holder, and verifier, a fourth role is the verifiable data registry, which incorporates credential metadata, revocation registries, issuer public keys, and other information. When a model instantiates this metamodel, it must specify the syntax, cryptographic algorithms, and proof format that will be used to construct VCs and VPs. For example, in Hyperledger Indy (128), a VC's metadata is stored in a DLT, whereas the data and proof are stored in a JSON file.

In (152), an approach is detailed in which social media platforms such as Facebook and LinkedIn are used to request, generate, and revoke credentials, as well as present and revoke

presented claims. Predicates over credential attributes, on the other hand, are not supported; only attribute disclosure is.

The authors of (154) designed a VC that can be issued and revoked by two parties. They argued that this is useful in the financial context. A financial company issues credit scores as VCs together with clients, but these can only be revoked by the financial company with the credit bureau's permission. Their VC includes two digital signatures, one for each entity. A protocol for revocation and status verification using ZKP is proposed.

Chotkan and Pouwelse (155) created a mechanism for propagating revocation information using a gossip-based algorithm. Users save the revocation information of their trusted authorities and broadcast it to random peers at predetermined intervals. As a result, issuers are not required to remain online in order to provide revocation data, nor are clients required to contact them in order to obtain such data. The authors provided a threat model as well as a thorough examination of various efficiency metrics.

Abraham *et al.* (153) also addressed the issue of offline credential status verification. Their approach is to implement the verifiable data registry as a blockchain, which generates attestation of the validity of requested certificates with a timestamp. When there is no connectivity to the revocation registry, this attestation is presented, and the relying party determines whether it is recent enough to be accepted.

Decentralized Identifiers

On the internet, entities are identified in a variety of ways. Identification occurs at all levels, from the application to the network. Identifiers are typically issued or controlled by a regulatory agency and assigned to users and machines. Internet Protocol (IP) addresses, for example, are managed by IANA (201), while e-mail providers manage e-mail addresses. A research trend in SSI is to create and improve *decentralized identifiers* from the machine to the human level. Four research articles (187, 189, 190, 188), two protocols (185, 186), and one W3C standard (67) have been written in response to various challenges associated with *decentralized identifiers*.

The Decentralized IDentifiers (DID) standard defines a metamodel to create identifiers that are issued and controlled by their owners (67). A DID method is an instance of this metamodel, which sets specific details such as the underlying encryption algorithms and the mechanism by which the method's identifiers are guaranteed to be unique. Each DID is a three-part URI separated by a colon: (i) the `did` scheme identifier; (ii) the DID method identifier; and (iii) the DID method-specific identifier. For instance, `did:key:z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH` is a valid DID identifier that uses the DID method `key` (202). In this method, the first character of the method-specific identifier is always `z`, and the following three characters represent the public-key algorithm used. In this case, the characters `6Mk` indicate that `Ed25519` (203) was used, and the subsequent characters are the multibase (204) encoded public-key. Other DID methods rely on

blockchain and other technologies to preserve the user-generated DID and its associated DID document, a JSON-based document with communication endpoints and cryptographic keys to ensure that the holder of a DID is its owner.

Although W3C's DID standard (67) provides a foundation for self-sovereign identifiers and the authentication of their owners, it does not define how two (or more) DIDs can interact. The authors of (185) proposed Decentralized IDentifiers Communication (DIDComm), a two-party protocol for establishing a secure communication channel between the holders of two DIDs. It allows messages to be sent via traditional protocols such as HTTP, BlueTooth, Near-Field Communication (NFC), and out-of-band channels such as QRcode and e-mail (205). Nonetheless, entities must first exchange DIDs before they can communicate. This is the driving problem of the DID Exchange protocol, which allows DID documents to be exchanged online or offline (186).

According to the authors of (188), transporting DID documents, which contain identifiers, keys, and communication endpoints, adds a significant overhead to IoT devices. They addressed this issue through three innovations: (i) a new DID method called `DID:SW` that has a smaller footprint than others; (ii) the use of Concise Binary Object Representation (CBOR) (206) to encode DID Documents; and (iii) an extension of DIDComm (185) to Decentralized IDentifiers-based Internet of Things Communication (DIoTComm), which reduces communication parameters and is based on CBOR. The DIoTComm protocol has a five-fold lower overhead than DIDComm.

According to Kim *et al.* (190), endpoint URLs in DID documents have an anonymity issue. They claimed that URLs could expose personal information such as country of origin and other affiliations. They proposed two countermeasures: (i) removing URLs and replacing them with other forms of communication; and (ii) using gateway URLs that only redirect authorized entities to the correct address.

From another angle, Smith (187) focused on self-certifying identifiers as a means of establishing trust. In this work, user-generated identifiers are coupled to public-key cryptography and explicitly disclose the hash of their next public key in their transactions. This proactive key rotation results in an auditable chain of digital identifier key transfers. To store the history of digital identifiers, a DLT is presented as a root-of-trust.

The key rotation challenge was also addressed in (189) using Lamport's one-way hash chain (207). This technique explores the pre-image resistance of cryptographic hash functions by constructing a chain of hash operations on a secret seed and revealing hash values in reverse order. Public-key cryptography is added to this scheme so that only the DID creator, *i.e.*, the person who knows the secret seed, can rotate to the next key pair (189).

Issuer Authorization

Three works present concepts for implementing *issuer authorization* (148, 149, 150), which entails issuers creating hierarchies akin to those found in traditional PKI.

Schanzenbach's Doctor of Philosophy (Ph.D.) thesis (148) describes a structure based on name systems (such as the Domain Name System (DNS) (208) and the GNU Name System (GNS) (209)) that enables an issuer to delegate authorization to other issuers to issue credentials with specific attributes. Additionally, these secondary issuers have the ability to delegate authorization to other issues, and so on.

With the same objective in mind, but a different approach, the authors of (149) formalized a model that utilizes the RSA cryptographic accumulator (71) to enable authorized issuers to issue credentials without disclosing their identity. The authors argued that this addresses a gap in the Hyperledger Indy framework (128), in which an issuer A cannot prevent another issuer B from issuing credentials in the same format as A.

According to the authors of (150), VCs issued in SSI today are assumed to be from trusted issuers, such as government agencies. Their work proposes an issuer authorization scheme based on policies, in which an issuer is only authorized to issue VCs if its policy allows it to. The root of authority serves as the policy authority, defining policies for issuers.

Delegation

Three research papers propose methods for achieving credential *delegation*. It refers to an individual's or group's ability to delegate some of their identity data to another individual or group of individuals. Two of them (18, 169) are discussed later in this chapter, as *delegation* is not their primary goal.

Lim *et al.* (170) proposed a system for VC delegation that requires the VC subject to confirm or deny the delegatee's use of the VC. A VP constructed by delegatees is limited in their method, as they only have the VC in an encrypted format. As a result, any VP presented by a delegatee induces communication with the VC subject in order to obtain authorization and incorporate the VP with required data.

Backup and Recovery

Another trend of research in SSI is the *backup and recovery* of keys and certificates. Empowering users with the ability to control their credentials currently comes with many burdens that were previously the tasks of IdPs. At this point, the *backup and recovery* of identity-associated materials are significant burdens. Proposing backup and recovery mechanisms to keys and credentials are the main objective of six research papers (173, 174, 18, 172, 175, 176).

Soltani *et al.* (173) used a decentralized protocol to handle key recovery. They created a wallet application in which users define their trusted peers and the recoverable keys. In a protocol based on SSS (199), key pieces are distributed to trusted users and can be recovered by the owner if a minimum number of parts can be retrieved from peers.

The authors of (176) presented a trade-off between security (storing an encrypted form of the private key in lower security environments) and usability (recovering the original private

key without the need for long passwords or Hardware Security Module (HSM)s). The private key is divided using SSS (199) to achieve this trade-off. The user must correctly answer a minimum number of previously registered questions, with each response constituting a component of SSS. To improve security, the minimum number of correct answers might be increased.

The authors of (174) also address the issue of identity recovery. Its authors suggested that a suitable solution would be to use another device in the identity owner's possession as a storage provider. To improve usability, it has been recommended that protocols could be developed and integrated with routers, resulting in a seamless user experience.

In (18), a self-signed root certificate acts as a CA that creates short-lived certificates for the users. The authors concluded that because certificates are rotated on a predetermined schedule, the key recovery issue is resolved as long as the CA's private key remain intact.

A private data backup system with two additional roles is proposed in (172): trusted audit service and trusted individuals. The trusted audit service receive portions of the keys. In contrast, the trusted individuals must physically meet to receive encrypted shares of the private data to store on short-range connectivity devices (such as infrared or near-field communication). Following the loss of personal data, trusted peers meet and confirm the affected user's newly generated electronic identity to the trusted audit service, which provide the user with the key necessary to decrypt the private data gathered from trusted peers.

From a different perspective, (175) uses Proxy Re-Encryption (PRE) (210). This technique allows data encrypted with a person's key to be decrypted using someone else's key without revealing anyone's data or key to the proxy. Trusted individuals execute a group key agreement, and then the derived group key is sent to the proxy that contains the encrypted user data. The user's private data can be retrieved from the proxy if the group recreates its key and uses it to authenticate with the proxy, which then uses the PRE scheme to have the user's private data accessible to the group.

4.5.2.2 Verifiable Presentation

Revocation

A challenging topic in SSI research is the *revocation* of VPs. Four research endeavors aspire to solve it (151, 152, 141, 139), one of which was presented above (152).

Concerned about the portability and interoperability of VPs, the authors of (151) introduced a metamodel for specifying VPs in blockchains. The VP metadata consists of the following elements: name, timestamp, expiration time, proof format, and proof link. The VP lifecycle is structured in a blockchain format with two types of blocks: one for adding a signature to a VP and one for revoking a signature. If all of the signatures endorsing a VP are revoked, the VP is deemed revoked as well.

The authors of (141), on the other hand, used chameleon hashing (211) to implement VP revocation. This one-way function family employs a trapdoor, so that without it, they behave

similarly to traditional one-way functions. If one has access to the trapdoor, such as via a key, one can easily find collisions for a given input. This special feature was used in (212, 213) to implement a rewriteable blockchain, that is, a blockchain whose history can be manipulated via the chameleon hash trapdoor. Based on these efforts, the authors of (141) designed their blockchain to allow users to revoke access to VPs anchored in the ledger via a trapdoor.

Lastly, in (139), it is argued that VPs cannot be revoked because they are likely to have been persisted locally by the RPs. The proposed solution to this problem is to grant access to up-to-date information via version control and encryption. Keys are distributed to authorized RPs.

Verifier Authorization

Verifier authorization is a relatively new topic. The idea is to give issuers some control over the credentials they issue by establishing rules that verifiers must follow in order to access holders' VPs. This appears to conflict with the philosophical basis of SSI, which specifies that issuers should not dictate what holders of VCs may or may not do.

The authors of (142) used Ciphertext-Policy Attribute-Based Encryption (CP-ABE) (214) to allow issuers to create a policy imposing minimum requirements on verifiers requesting VPs from holders. The decryption key in CP-ABE is derived from the attributes of the deciphering entity. A doctor, for example, who receives patient data must have a doctor registration VC and be specialized in a particular field.

Data Minimization

Perhaps the most valuable feature of SSI for individuals is its emphasis on *data minimization*. Three types of techniques are described in the literature: (i) selective disclosure (147, 153, 156), which enables the creation of VPs containing only some of the attributes of a VC rather than all of them; (ii) predicates, *i.e.*, boolean assertions over data (157); and (iii) arbitrary statements over attributes (73, 74, 75).

Abraham *et al.* (147) built a ZKP proof system using Water's signature (215) and Boneh–Lynn–Shacham (BLS) signature (216) that enables selective disclosure of certificate attributes. The same technique is employed in (153). Similarly, (156) uses zero-knowledge Succinct Non-interactive ARguments of Knowledge (zk-SNARK) (217) to create a VP format where holders can prove possession of a specific attribute and reveal its value.

In (157), ZKP allows the creation of a VP to mathematically prove that a VC was created by an issuer who is a member of a group of authorized issuers without revealing any unique identifier, such as the issuer's public key. Finally, the authors of (73), (74) and (75) enable credential holders to explore the full expressive power of zk-SNARK, *i.e.*, to produce proofs in any language in `NP`.

Reuse Prevention

Nothing stops the RP from copying what it learns from the user after receiving a VP. *Preventing the reuse* of acquired knowledge is one of the most challenging aspects of SSI. The creators of (143) attempt to solve this challenge. They proposed an architecture that allows holders to charge RPs to access their attributes while preventing reuse. Instead of selective disclosure or proofs over private data, Fully Homomorphic Encryption (FHE) (218) is used. FHE is a method for processing encrypted data and producing valid results without decryption. Their proposal uses FHE to process user data in a secure third-party environment that both the user and the RP trust. According to the authors, this technique prevents private information from being leaked. Although it is unlikely that FHE will reveal user attributes, information about the computation over private data can be revealed.

4.5.3 System Design

The facet *system design* encompasses four concepts related to the conceptualization of SSI: *design/architecture*, *Human-Computer Interaction (HCI)*, *risk assessment* and *security model*.

SSI Design/Architecture

Five articles discuss various aspects of what we refer to as *SSI Design* or *SSI Architecture* (66, 151, 169, 165, 166, 167). Rather than addressing specific issues or proposing SSI systems, these publications explore and analyze the planning, design, and construction of SSI systems. Previously, the W3C's VC metamodel (66) and Stokkink *et al.*'s (151) VP metamodel were examined. This section discusses the remaining three research papers in this category.

In (169), design patterns are presented to assist in the development of new SSI applications on the blockchain. The lifecycles of key management, identity management, and credential management are discussed. Then, twelve patterns are proposed within these three groups, following Martin *et al.*'s (219) format, which includes a pattern name, summary, context of use, problem statement, discussion, solution, and its consequences.

On the other hand, the authors of (166) asserted that identity management systems could be reduced to two mappings: (i) digital identifier and its owner, and (ii) digital identifier and its credentials. Furthermore, for both mappings, the following operations are required: create, read, update, delete, and verify. The system's chosen trust model determines the manner in which they are built. If the goal is SSI, all of them should be completed independently of any authority.

Barclay and colleagues (165) demonstrated a modeling technique that enables non-technical stakeholders to specify and comprehend SSI entities and their relationships. They used iStar 2.0 (220), an actor-based modeling language that enables the representation of actors

and the interdependence of their goals. In an SSI system, the actors are the users who issue credentials and present claims.

Finally, Ferdous *et al.* (167) created a detailed mathematical model of SSI. This formalization includes a feature that is unique in the SSI literature reviewed: user de-registration.

Human-Computer Interactions

There are five research materials (179, 180, 177, 181, 176) and one patent (178) that look into usability and human perception issues in SSI systems. Section 4.5.2.1 already introduced the work of Sign *et al.* (176). They are grouped under the *HCI* concept of our taxonomy.

Toth *et al.* (179) claimed that biometrics and other forms of two-factor authentication only marginally improved identity security. They then introduced a software agent to manage user data. It helps users decide which credentials to use and which private information to reveal, improving security through improved human-computer interactions.

With a different emphasis, the authors of (178) submitted a patent for an authentication method based on a users' interactions with their personal device. To determine if the person holding the device is the owner, the device monitors application usage patterns, browser history, location history, and other measurements.

Pertaining HCI and trust, (181) suggest that deciding whether or not to trust an identity and its claims is a major risk for an algorithm to decide on its own. The authors put forward a proposal in which the user must actively decide whether electronic identities can be trusted. The user is empowered to make that decision by viewing a graph of the proponent's previous interactions with other electronic identities, which is generated from the history stored in a DLT.

The authors of (177) presented an extensive study of SSI usability and discovered that current SSI systems interactions necessitate extensive prior knowledge and participant responsibility. The authors investigated the SSI interface layer using the human data interaction theory (221), which says that humans interact with data rather than computers. To increase the likelihood of adoption, the conclusion emphasizes the need for standardization and design thinking of interfaces and interactions.

Shanmugarasa *et al.* (180) addressed the issue of users managing VPs. Non-technically competent users, for instance, may agree to submit more information than the RPs actually needs. The proposed solution to this problem is a privacy preference recommendation system that employs machine learning algorithms and pre-trained models based on survey data on privacy preferences. This system assists the user by suggesting on which attributes can be shared.

Risk Assessment and Threat/Attack Model

In relation to the design of SSI, two concepts related to computer security were observed in the reviewed literature, namely *risk assessment* and *threat/attack model*. The latter

entails two activities: (i) identifying and analyzing potential threats; and (ii) comprehending how an attacker can exploit them. These two tasks are part of the risk assessment, which also includes calculating the potential loss if a vulnerability is exploited. Eighteen works described in the other sections incorporated one or both of these activities to improve their schemes. While three articles discussed risk assessment, only one makes a novel contribution by tying risk assessment and SSI together (191).

Naik *et al.* (191) developed a tree-based risk analysis method for SSI. The attack tree approach represents the attack goal as the root of a tree, and the methods and actions to achieve the goal as the leaves (222). In this work, important assets in an SSI system are identified first. Then, the attack tree is used to generate input for their risk analysis, which concludes with appropriate mitigations for the identified risks.

4.5.4 Trust

The final practical facet of our taxonomy is *trust*. Entities in any IAM model must decide whether they trust other entities and, as a result, the data they generate. Since the inception of SSI, a strong emphasis has been placed on the use of VCs in order for RPs to be certain about the origin of the credentials (66).

SSI promotes the decentralization of identity management. Furthermore, the majority of SSI offerings endorse the deconstruction of centralized sources of trust (*e.g.* IANA (201) and Certification Authority Browser Forum (223)). Most SSI platforms allow anyone to issue VCs in anyone's name. As a result, *reputation models* that allow RPs to quantitatively assess whether a VP (and thus a VC) is trustworthy or not have been an active topic of study. Another topic of interest is the development of *trust policy evaluation* techniques for evaluating policy-based reputation models.

Reputation Model

Six research articles present or discuss *reputation models* for SSI (164, 161, 162, 163, 140, 151). Section 4.5.2.2 introduced one of them. The rest are described below.

Gruner *et al.* (164) used graph theory to model trust in blockchain-based SSI systems. The originator of VPs is endorsed in a blockchain by system participants in their proposal. This enables the creation of an endorsement graph. They proposed an algorithm that navigates the graph and calculates a trust factor for the system's participants. This trust factor can be used to determine whether a participant can be trusted or if they are a malicious user.

Bhattacharya *et al.* (162) expanded on (164) by including time as a variable in their reputation model. They hypothesized that, in the context of Sovrin, the initial reputation of issuers could be influenced by Sovrin's onboarding process, which could be biased or falsified.

The authors of (161), on the other hand, developed a probabilistic model of trust. They applied probability theory to determine whether claims about the same information from

different issuers could be combined to generate trust about it.

Zhong *et al.* (140) raised the problem of current SSI offerings' lack of interoperability and how this restricts the evaluation of VC credibility. Their solution to this problem employs cross-chain smart contracts to compute a credibility score based on the boolean evaluation (either support or refuse) of all verifiers who verify the VC, taking into account each verifier's credibility.

Finally, Abramson *et al.* (163) described the different user roles and transaction types stored in the Hyperledger Indy blockchain, including the steps a verifier can take to gain confidence when receiving a presentation. For example, they argued that if multiple entities issue credentials of a given format (credential schema), this provides more assurance than a schema that is only endorsed by a single issuer.

Trust Policy Evaluation

The *trust policy evaluation* is covered in eight papers (132, 138, 136, 149, 181). Three of them (132, 138, 136), which were previously introduced, are concerned with *protocol integration* and *identity derivation*. One aims for *issuer authorization* (149), while the other for *HCI* (181). The following are the three papers that attempt to address this problem (182, 183, 184).

The authors of (183) proposed that entities define trust policies through lists of authorities they trust. These trusted entities, in turn, also publish which entities they recognize as trustworthy. For instance, one could trust a bank federation that periodically reports which banks it recognizes as credible. Thus, when receiving the VP of a person stating that she has an account on an unrecognized bank, a query to the bank federation's list of trusted banks is enough to decide if the VP can be trusted or not.

Inoue *et al.* (182) considered the task of updating an individual's information across multiple issuers and RPs, each with its own trust policy. This challenge was modeled as an Integer Linear Programming (ILP) problem, with trust policies defined as credibility requirements for incoming update requests. Updating a person's information in an issuer or RP increases its credibility. The ILP is then transformed into a graph problem, and an approximate solution is found using a heuristic based on Dijkstra's algorithm. This article is the only one in the survey that provides a formal description of the problem.

The Trust Policy Language (TPL) (224), a declarative language for specifying trust rules without concern for low-level details, was adapted to work in SSI in (184). The TPL has been enhanced with SSI-related concepts such as DID and VC, allowing the specification of rules to validate VPs.

4.6 RQ-2: WHAT PROPERTIES, FORMAL DEFINITIONS AND CRYPTOGRAPHIC TOOLS HAVE BEEN USED?

The first two years of examined papers were mostly focused on conceptual contributions to SSI. From 2018 forward, the works evaluated began to provide mathematical models to help represent concepts. There are twenty-seven articles in total that include some type of formalism. Table 11 shows these articles and the building blocks they utilized. We divide formal definitions into two categories: cryptographic tools and non-cryptographic tools. Cryptographic tools are well-known, low-level cryptographic algorithms that are employed in computer systems to develop secure protocols and systems (225, 226).

Table 11 – Publications that introduce mathematical formalism to SSI.

Concept	Works	Formalism	Non-Crypto. Tools				Cryptographic Tools								
			ILP	Graph	NS	Prob.	MPC	SSS	PRE	CH	ABE	ZKP	CAcc	MS	FHE
Identity Derivation	(146)	✓											✓		
Credential as a Service	(159)	✓					✓	✓							
Revocation	(139)	✓			✓						✓				
	(141)	✓								✓					
	(154)	✓										✓			
	(152, 155)	✓													
	(153)	✓										✓		✓	
Decentralized Identifiers	(187)	✓													
Issuer Authorization	(149)	✓										✓	✓		
	(148)	✓			✓						✓				
Backup and Recovery	(172)	✓				✓									
	(173, 176)	✓						✓							
	(175)	✓							✓						
Verifier Authorization	(142)	✓									✓				
Data Minimization	(74, 75, 156, 73)	✓										✓			
	(147)	✓										✓		✓	
Reuse Prevention	(143)	✓													✓
SSI Design/Architecture	(167)	✓													
Reputation Model	(161)	✓				✓									
	(164, 162)	✓		✓											
Trust Policy Evaluation	(182)	✓	✓	✓											

Source: The author.

Inoue et al. (182) modeled trust policy evaluation using *ILP*, which is an optimization formulation in which all variables are integers and the objective function is linear (227). It may be used with other formulations, such as *graph* theory to map graph-related problems such as the shortest path between two nodes. In addition to (182), two other papers used graph models to create reputation models (164, 162).

Two works led by Martin Schanzenbach (139, 148) used *Name System (NS)* (e.g. DNS (208), and GNS (209)) as blocks for attacking revocation and issuer authorization challenges. These systems are coupled with *Attribute-Based Encryption (ABE)*, which allows the

user to selectively give and revoke access to some of their attributes. Another work that models a solution based on ABE is (142).

Last in the non-cryptographyc tools category is *probability theory*. Both Gruner et al. (161) and Jakubeit et al. (172) base their contributions on this branch of mathematics.

We mapped nine cryptographic techniques formally defined in the examined literature. Most of the practical research we surveyed discussed how cryptographic primitives such as public-key cryptography and hash functions are used. Nevertheless, we only included those that did so with more than simple textual explanations in this study.

Multi-Party Computation (MPC) is formally described and used in (159). This field of research investigates methods for parties to compute a function together over their inputs without revealing them to the other parties (228). In (159), MPC was used in conjunction with *SSS* (199). This technique was used in two other articles to achieve the backup and recovery of credentials (173, 176). The SSS algorithm breaks a secret into shares. The original secret is recalculated using a predetermined number of shares, generally fewer than the total number of shares.

Another technique that was precisely described in the SSI literature was *PRE* (210). This technique allows data encrypted with a person's key to be decrypted using someone else's key without revealing anyone's data or key to the proxy. It was used by Kim et al. (175) to recover private data.

The authors of (141) implemented VP revocation with *Chameleon Hashing (CH)*. This family of one-way functions employs a trapdoor to find collisions for a given input (211).

User privacy is the utmost goal of SSI, and the most popular technique used to increase privacy is to use *ZKP* to convince the RP of statements regarding the user's private information. Five articles that mainly propose data minimization techniques formally defined their approaches (74, 75, 156, 73, 147), four of which use zk-SNARK to achieve ZKP (156, 73, 74, 75) and the other (147) uses *Multi-Signature (MS)*, which is also employed in (153). MS allows a set of participants to sign a document or message.

Two papers formally describe and use *Cryptographic Accumulator (CAcc)* as part of their solutions (146, 149). CAcc is a data structure that enables the accumulation of a large set of values into one short accumulator. One of the characteristics of CAcc is that set membership can be verified in constant time. The authors of (146) use it as part of the process of creating SSI identities from traditional PKI-based identities and (149) to achieve issuer authorization.

Lastly, FHE (218) is used to prevent the reuse of presented information in (143). FHE allows encrypted data to be processed without decryption.

4.7 RQ-3: WHAT CONCEPTUAL IDEAS HAVE BEEN INTRODUCED OR REFUTED?

Christopher Allen (3) stated that there is currently no agreement on a definition of SSI and then presented ten guiding principles as a starting point. Our third research question is answered by an examination of the literature's debates on the SSI definition, which is now

presented to the reader.

We found seventeen works that contribute to Allen's discussion regarding the meaning of SSI by using our review process. Table 12 summarizes these studies in accordance with our taxonomy, which has the facets *add* and *refute* under *conceptual*. Furthermore, the facet *add* is subdivided into *functional* and *non-functional*.

Table 12 – Publications that add or refute philosophical views of SSI.

	Add																Refute						
	Functional								Non-Functional														
Works	No Central Authority	Legacy Compatible	VP	Counterfeit Prevention	Identity Verification	Identity Assurance	Secure transactions	Delegation	Recoverability	Usability	Accessibility	Availability	Auditability	Scalability	Free	Regulatory	Existence	Control	Access	Consent	Persistence	Transparency	Protection
(151, 13, 229)			✓																				
(68)				✓	✓	✓	✓			✓							✓					✓	✓
(155)			✓													✓							
(167)												✓											
(230)	✓	✓	✓						✓					✓	✓								
(231)			✓				✓		✓		✓	✓		✓	✓								
(232)															✓		✓						
(233)			✓						✓							✓							
(234)	✓																						
(235)	✓									✓				✓									
(236)	✓								✓	✓													
(237)										✓													
(238)	✓	✓				✓	✓		✓	✓	✓												
(239)	✓		✓				✓	✓		✓	✓												
(240)													✓				✓	✓	✓	✓	✓		

Source: The author.

4.7.1 Add

Functional

No central authority means that no single organization should be in charge of or own an SSI solution (230, 234, 235, 236, 238, 239). The articles that define this property, as well as the articles that say that SSI should be *free* (230, 232, 231), make good arguments at first glance. However, upon closer examination, these characteristics may discourage businesses from investing in SSI. They would have to seek alternative sources of income and share control over their products. To some extent, this is what Evernym (241), a for-profit company, did when it split off Sovrin, a non-profit foundation that is supported by other organizations (242). Sovrin, on the other hand, is not free. While end users can join the network, receive VCs, and issue VPs for free, companies or other entities that enroll their end users must pay fees to (243):

(i) join the network; (ii) register a credential format, i.e., a credential schema; (iii) begin issuing credentials using a registered schema; (iv) register a revocation registry; and (v) revoke VCs.

According to two studies, SSI systems must be *compatible with legacy* identity management systems and protocols (230, 238). According to the reviewed literature, this is a highly researched subject. The applied research focuses on two aspects of legacy compatibility: (i) protocol integration with prior standards such as SAML, OAuth 2.0, and OIDC; and (ii) identity derivation in order to migrate identities from identity providers that adopt the aforementioned protocols to SSI systems.

According to (151, 13, 229, 230, 231, 233, 155, 239), the concept of *VP* is an integral part of SSI such that, without it, we cannot achieve SSI.

Toth and Anderson-Priddy (68) defined four additional *functional* properties of SSI, two of which have not been accounted for by others: (i) *counterfeit prevention*, which involves the impossibility of producing fake identities from others; and (ii) *identity verification*, which requires interacting parties to be assured of the authenticity of the identity owner. According to the property *identity assurance*, which has been proposed elsewhere (238), entities that rely on (self-sovereign) identities should be able to see proof that the entities with whom they interact are who they claim to be. The fourth additional property proposed by (68) and others (231, 238, 239) is the impossibility of tampering with communications between identity owners, *i.e. secure transactions*.

Delegation is the final *functional* characteristic of SSI proposed in the literature (239). It is the capacity of identity owners to delegate some of their identity data to other individuals or groups of individuals of their choosing. This is a developing field of study (18, 169, 170).

Non-Functional

According to the authors of (230, 231, 233, 236, 238), a critical component of SSI is ensuring that people's data are *recoverable* in the event of loss of personal device. This theoretical proposition is also an active area of applied research, as evidenced by six recent articles (172, 173, 174, 18, 175, 176).

Six studies assert that *usability* is critical in SSI (236, 68, 235, 237, 238, 239). These works affirm that: (i) interfaces and experience must be optimized (238, 239); (ii) users' needs and expectations must be met and consistent across all platforms and services (235); (iii) users should not require prior knowledge of blockchain technology (236); as well as (iv) other underlying technologies such as cryptographic operations, biometrics, databases, and protocols (68). One way to accomplish these goals is to mimic physical identities and the interactions we have with them, thereby exposing the user to familiar workflows (68). Ultimately, if the user does not comprehend what is occurring and is unable to reason about it, the user is not sovereign (237).

Accessibility is a concept related to usability but has a more specific focus. According to three research papers in the reviewed literature, identity-related solutions should be accessible to as many people as possible (231, 239, 238).

Two authors claim that identities should always be *available* (231, 167). The challenge of having highly available identity-related information in SSI is being addressed on multiple fronts. For example, (155) and (153) propose ensuring the availability of issuers' revocation registries in a decentralized and offline fashion.

In terms of *auditability*, Schutte (240) argued that auditing requires not only access to the details, but also the ability to read and understand them.

Another significant factor to consider is the *scalability* of SSI systems (231, 230, 235). While practical research observes and considers this aspect (129, 138, 148), it is not the norm in the surveyed literature.

Finally, there is a subset of articles arguing for the importance of *regulatory* compliance in the SSI ecosystem (233, 155), such as the GDPR (53) and CCPA (54). Chotkan *et al.* (155) argued for the importance of verification and legislation compliance, despite the fact that the latter may weaken the strength of other SSI principles (such as privacy). The author of (234) did not say that GDPR compliance was necessary, but they discussed about how SSI systems can use verifiable claims to meet the following articles of the GDPR: (i) consent; (ii) pseudonymization; (iii) the right to be forgotten; (iv) records of processing activities; (v) data portability; and (vi) data protection by design and by default.

4.7.2 Refute

There are three works (240, 68, 232) that add new properties to SSI while also refuting some of Allen's concepts (3). They all refute the *existence* principle, which states that individuals cannot exist entirely in digital form, and that (self-sovereign) identities expose some aspects of the user. Toth and Anderson-Priddy (68) have also argued against *transparency* and *protection*, suggesting that more debate is needed on these topics. Similarly, the authors of (232) argued that previous discussions (234, 244) about identity had failed to address the issue of *existence*.

Unlike the previous two studies, Schutte (240) examined Allen's principles through a more philosophical and less technical lens. He contended that an individual, or "self" is not an indivisible entity, but rather the result of constant interactions between various agents, both internal and external. He then criticized the principles of *existence*, *control*, *access*, and *consent*, claiming that an individual's identity is a "heuristic that simplifies information processing and decision making" (240), which is imprecise by nature and thus cannot fully anchor identity processes. Finally, he argued that claims are critical and can be viewed as signals broadcast by some actors and perceived by others, who must decide how to prioritize and interpret them.

4.8 RQ-4: WHEN, WHERE, AND BY WHOM WERE SSI STUDIES PUBLISHED?

To address RQ-4, we aggregate the *General* data items gathered via our data extraction form. The following section discusses the findings.

Frequency of Publication

In terms of publication frequency, Table 13 summarizes publications by year. Although it is a brief overview, it demonstrates the growing academic interest in SSI. Using Venn diagrams to represent the facets of our taxonomy, we can discern finer details regarding publication frequency. Figure 12 depicts the number of publications classified in this manner.

In response to Allen's introduction of the ten principles in 2016 (3), two publications were released in the same year (230, 240). Works published in 2016 and 2017 are mostly conceptual writings that expand on Allen's discussion, proposing new principles/requirements (230, 240, 234, 236, 233, 229) for SSI as well as refuting some (240). Since 2016, researchers have been conducting continuous conceptual research, indicating that the meaning of SSI is still being debated. Beginning in 2018, articles started to significantly introduce new pragmatic problems and solutions to the SSI ecosystem as well as mathematical formalisms. Nonetheless, mathematical formalization and a formal description of cryptographic tools in applied research, which help SSI grow into a well-defined field of study, account for less than or equal to half of all applied research published each year.

Table 13 – Publications per year.

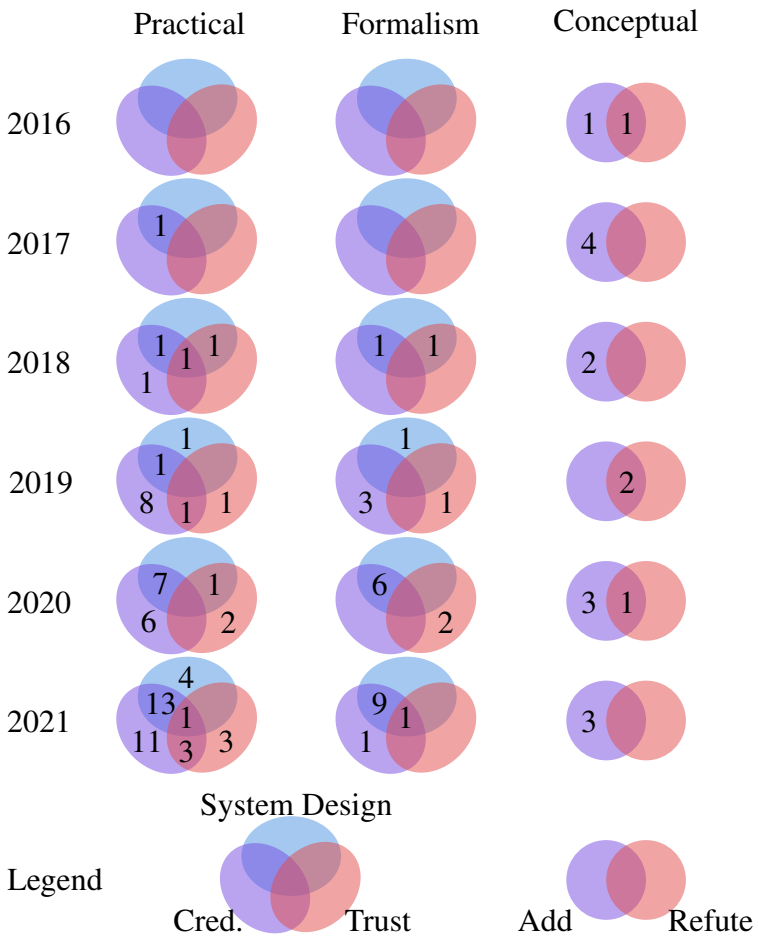
Year	Total	Studies
2016	2	(230, 240)
2017	5	(234, 236, 233, 66, 229)
2018	5	(164, 151, 18, 13, 139)
2019	14	(132, 161, 144, 167, 68, 173, 126, 232, 74, 75, 67, 187, 186, 137)
2020	19	(172, 235, 147, 169, 141, 133, 237, 165, 181, 231, 182, 166, 134, 179, 162, 153, 148, 185, 156)
2021	37	(129, 183, 176, 170, 177, 149, 180, 178, 168, 152, 163, 175, 158, 171, 159, 138, 73, 143, 145, 146, 136, 135, 160, 191, 154, 188, 150, 142, 155, 174, 238, 189, 157, 140, 239, 184, 190)

Source: The author.

Publishing Venues

In terms of publication venues, forty-two papers were held in congresses, symposia, or forums, as shown in Table 14 under the category conference. Forty-two conference papers and six master's theses demonstrate that SSI is gaining traction as a research subject. However, it is still in its infancy, with just one Ph.D. thesis and fifteen journal articles.

Figure 12 – The number of publications in each facet of our taxonomy over time.



Source: The author.

Table 14 – Types of publishing venues over the years.

Venue Type	Total	2016	2017	2018	2019	2020	2021
Blog Post	1	(240)					
Website	2		(229)				(239)
Report	1		(234)				
Standard	4		(66)		(67, 186)	(185)	
Web Archive	7				(74, 75, 187)	(165)	(238, 188, 73)
Conference	42	(230)		(164, 151, 18, 139)	(132, 161, 144, 173, 126, 137)	(172, 235, 147, 181, 175, 231, 166, 134, 179, 162, 153, 182)	(183, 176, 184, 170, 190, 149, 180, 158, 171, 160, 135, 191, 129, 136, 146, 150, 140, 145, 157)
Journal	15			(13)	(167, 68)	(169, 141, 133, 156)	(177, 152, 163, 159, 138, 154, 143, 189)
Patent	2						(168, 178)
Bachelor Thesis	1						(174)
Master Thesis	6		(236, 233)		(232)	(237)	(142, 155)
Ph.D.Thesis	1					(148)	

Source: The author.

The authors choose a wide variety of conferences, symposia, and forums in which to publish their works. Even though forty-two papers have been published in this sort of venue, only seven conferences have received more than one publication, as shown in Table 15. The IEEE colloquia, which received nineteen papers spread across fourteen different conferences, are the most popular choice. As illustrated in Table 16, the same trend holds true for essays published in scientific journals. Seven of the fifteen studies were published in journals published by the IEEE.

Authors

We gathered the authors' names using our data extraction form. This allowed us to construct a co-authorship network graph (245), which is a weighted undirected graph in which vertices represent authors and edges represent works shared between them. Figure 13 depicts our co-authorship network graph where vertices represent authors and edges their co-authorship of one or more works with edge weights displayed in different line diameters for ease of reading. The diameter of the vertices changes as well, representing the number of publications each author has. The vast majority of the edges in this network graph are thin, indicating that most authors only have one publication. Additionally, this disconnected graph shows that authors have mostly worked alone or in small groups.

The authors with the most publications in this survey are Andreas Grüner, Alexander Mühle, and Christoph Meinel. They have co-authored three research papers (132, 161, 138) and two more with Tatiana Gayvoronskaya (164, 13). As a result, the vertices and edges representing these three authors and their publications have the most weight in this graph (i.e., the thickest vertices and edges).

Andreas Abraham is the only author who has written four articles. Abraham's publications include a technical report (234), a research paper with Felix Hörandner, Olamide Omolola, and Sebastian Ramacher (147), a second paper with Felix Hörandner, Christof Rabensteiner, and Stefan More (153), and a third paper with the last two authors (146).

After introducing Andreas Abraham, who is a co-author of four publications, we now introduce the researchers who are co-authors of three: Stefan More, Martin Schanzenbach, and Hye-Young Paik. Apart from the two publications with Andreas Abraham, Stefan More also co-authored a research paper with Lukas Alber, Sebastian Mödersheim, and Anders Schlichtkrull (184). Schanzenbach's publications include his doctoral dissertation (148) and two articles co-written with Julian Schütte, one co-written with Georg Bramm (139), and one co-written with Thomas Kilian and Christian Banse (75). Hye-Young Paik and Liming Zhu co-authored an article with Yue Liu, Qinghua Lu, Xiwei Xu, and Shiping Chen (169), and Paik published another article with Yashothara Shanmugarasa and Salil S. Kanhere (180). Paik also shares a third article with Rahma Mukta, Qinghua Lu, and Salil S. Kanhere (150).

We present in Figure 14 the co-reference network of the surveyed literature. The vertices in this directed graph represent publications. The edges represent references between

Table 15 – Conferences, symposia and forums with multiple publications.

Venue Name	Total	Studies
Conference on Blockchain Research & Applications for Innovative Networks and Services	2	(166, 134)
Open Identity Summit	2	(183, 184)
International Conference on Information Networking	2	(170, 190)
IEEE Symposium Series on Computational Intelligence	2	(161, 191)
IEEE International Congress on Cybermatics	2	(164, 151)
IEEE International Conference on Blockchain and Cryptocurrency	2	(149, 158)
IEEE International Conference on Trust, Security and Privacy in Computing and Communications	2	(139, 153)
IEEE International Conference on Internet of Things: Systems, Management and Security	1	(126)
IEEE International Conference on Mobile Cloud Computing, Services, and Engineering	1	(231)
IEEE International Conference on Cloud Engineering	1	(160)
IEEE International Symposium on Network Computing and Applications	1	(132)
IEEE International Symposium on Dependable, Autonomic and Secure Computing	1	(173)
IEEE International Conference on Pervasive Computing and Communications Workshops	1	(180)
IEEE Annual Computers, Software, and Applications Conference	1	(171)
IEEE Conference on Computer Vision and Pattern Recognition Workshops	1	(144)
IEEE International Performance, Computing, and Communications Conference	1	(140)
IEEE International Conference on Systems, Man, and Cybernetics	1	(145)
IEEE Symposium on Computers and Communications	1	(135)
IFIP International Conference on Information Security Theory and Practice	1	(172)
IFIP International Summer School on Privacy and Identity Management	1	(235)
IFIP International Conference on New Technologies, Mobility and Security	1	(176)
ACM Celebration of Women in Computing	1	(150)
International Conference on Information and Communications Security	1	(147)
International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing	1	(175)
International Conference on Security and Cryptography	1	(146)
International Teletraffic Congress	1	(182)
International Symposium on Networks, Computers and Communications	1	(162)
International Conference on Business Process Management Workshops	1	(129)
International Conference on Cryptology and Network Security	1	(157)
Symposium on Cryptography and Information Security	1	(181)
Annual Privacy Forum	1	(179)
Annual Conference of the South African Institute of Computer Scientists and Information Technologists	1	(18)
Rebooting the Web-of-Trust	1	(230)
Gesellschaft fur Informatik (GI)	1	(136)
Workshop on Decentralized IoT Systems and Security	1	(137)

Source: The author.

articles, with the destination of an edge indicating that the source of the edge references this work. The number of received citations determines the diameter of the vertices, and the color of the vertices is determined by the year of publication.

This graph shows the significance of W3C standards DID (67) and VC (66) for SSI. They are the two most referenced works in this map, with twenty-nine and twenty-one refer-

Table 16 – Studies published in journals.

Journal Name	Total	Studies
Frontiers in Blockchain	2	(177, 163)
IEEE Access	2	(167, 138)
IEEE Internet of Things Journal	2	(159, 189)
IEEE Software	1	(169)
IEEE Security and Privacy	1	(68)
IEEE Transactions on Vehicular Technology	1	(141)
IEEE Transactions on Computational Social Systems	1	(152)
Elsevier Computer Science Review	1	(13)
Elsevier Computers & Security	1	(156)
MDPI Electronics	1	(133)
IEICE Transactions on Information and Systems	1	(154)
Ledger	1	(143)

Source: The author.

ences, respectively. The first survey of SSI (13), published in 2018, ranks third in terms of citations, with seventeen. It is followed by the fourth most cited article, a comprehensive mathematical formulation of SSI from 2019 (167).

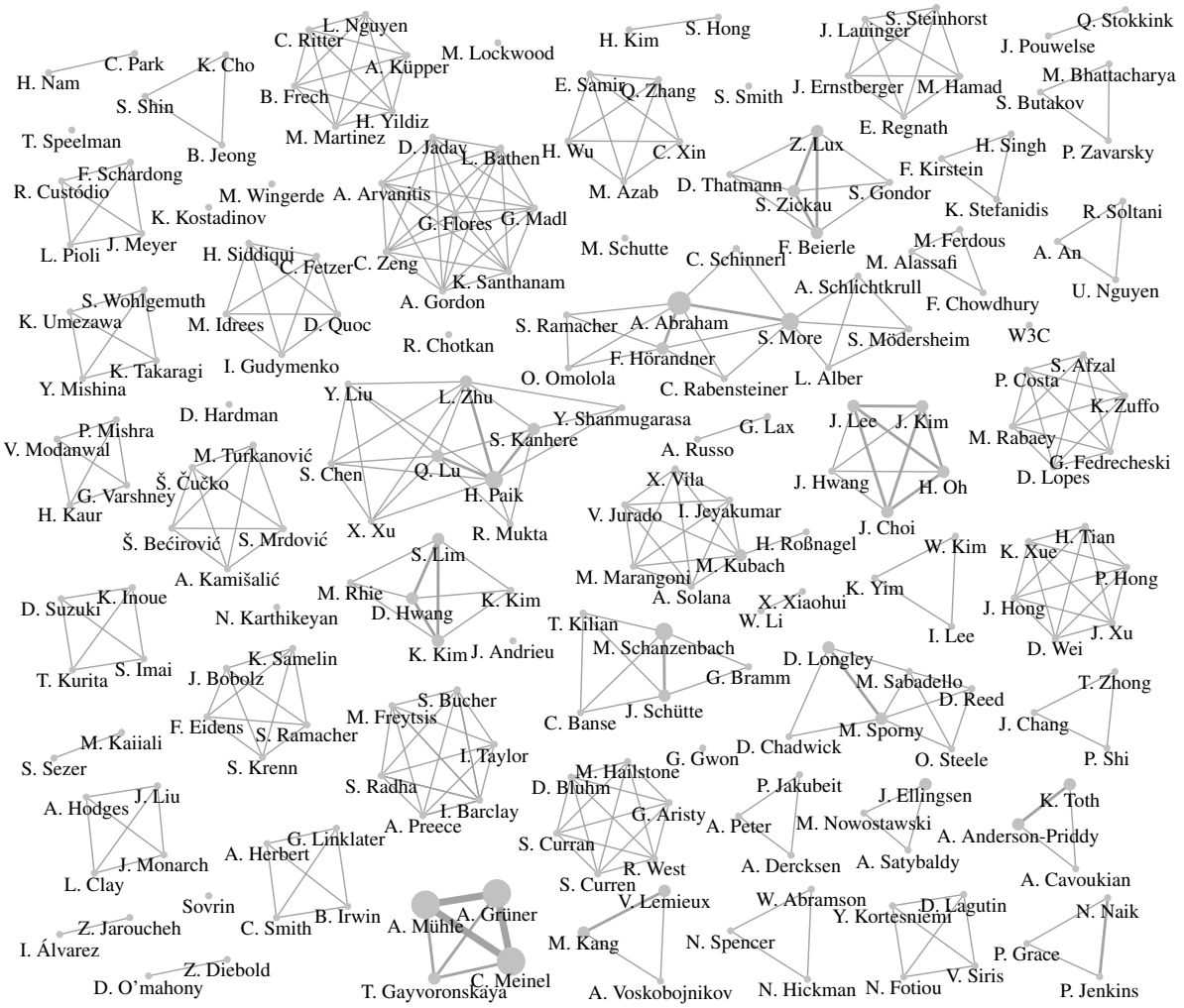
In terms of cross-references, forty-seven works are not cited in any of the surveyed publications. Thirty-five of these unreferenced works are from 2021, nine are from 2020, two are from 2019, and one is from 2018. Similarly, twenty-seven publications do not contain any references to mapped work. Eight of these are from 2021, three are from 2020, six are from 2019, three are from 2018, five are from 2017, and two are from 2016. The scope of our survey is one of the reasons for publications that do not include references to other mapped works. We excluded SSI platforms such as Sovrin, Uport, and Jolocom, which are mentioned in many of these essays.

4.9 OPEN CHALLENGES

The surveyed materials detail developments in the field of SSI. New publications will advance the conceptual debate about what it means for an identity to be self-sovereign while also introducing new and unexpected challenges to the SSI ecosystem. We identify future research challenges based on the evidence gathered to address our research questions. They are discussed in detail below along with recommendations.

A definition of SSI that researchers and practitioners accept. We have gathered evidence (see Section 4.7) that the majority of articles on SSI fundamentals agree with Allen's principles (3), while also adding new ones. Promoting a thorough review and discussion is critical in order to develop a new set of rules for defining SSI. Furthermore, mathematical formalization can be used to define precise boundaries. Having an exact definition of SSI will benefit future efforts and, ultimately, users who will be able to transition between SSI systems

Figure 13 – Co-authorship network graph.



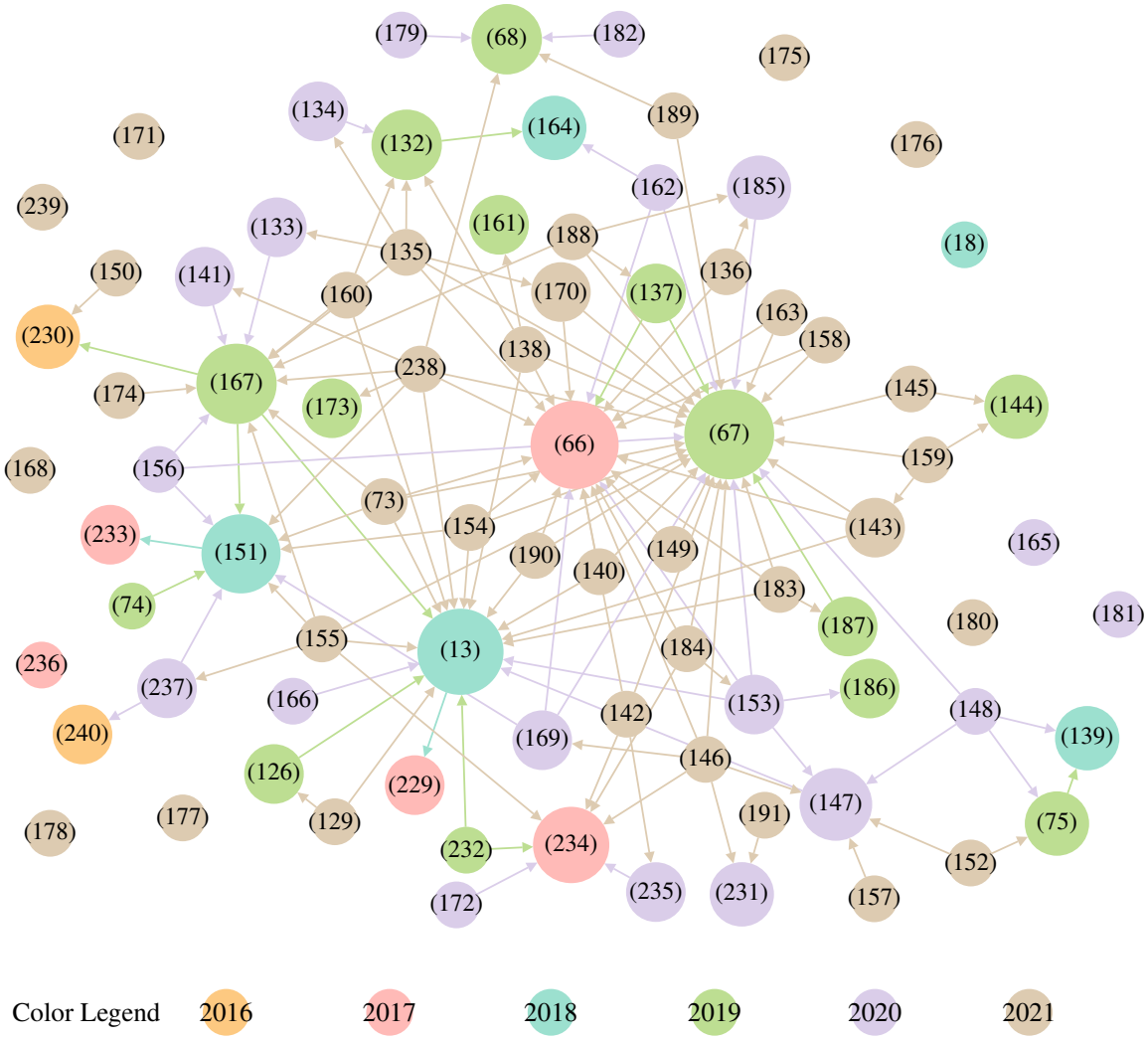
Source: The author.

with the confidence that they share the same fundamentals.

Fundamental research. The majority of materials surveyed that include a mathematical model do so by designing it to their particular context. Only one of the articles reviewed provides a comprehensive mathematical formulation of SSI (167), but it does not address the SSI's inherent decentralized trust properties. Another article (169) discusses realistic considerations and provides design patterns for numerous facets of SSI, including trust. These publications serve as a valuable starting point. However, additional basic research is necessary to foster discussion about how to jointly represent identities, credentials, claims, and trust, which is critical for future pragmatic research. By addressing RQ-2 and RQ-3 (see Sections 4.6 and 4.7), we established a foundation for future fundamental research.

Special case attribute sharing. Revised publications allow VPs to: (i) selectively disclose attributes (147, 153, 156); (ii) create boolean predicates about attributes (157); and (iii) produce general expressions over attributes (73, 74, 75). Nonetheless, these methods are unsuitable when sharing characteristics that will likely stay unchanged for several years: for instance, the shipping address associated with an online purchase. As a result, additional research on VP

Figure 14 – Co-reference network.



Source: The author.

is required to ensure that a diverse range of use cases is covered.

Sound trust models. Trust plays an essential role in SSI and will be of paramount importance for the adoption of SSI solutions. Without comprehensive testing, trust models will become attractive targets for hackers. This open challenge is exacerbated by the current standardization effort (246), which specifies a Boolean trust model in which a verifier either trusts or distrusts the issuer. This model does not cover the fuzzy scenarios of the real world. For example, an entity may present multiple claims about the same attribute where some issuers are trusted and others are not. Can this claim be trusted? Quantifiable trust/reputation models are needed, but only five of the surveyed articles address this issue (164, 161, 162, 140, 163). Trust models require strong security, so formal verification techniques must be employed (247).

Blockchainless SSI. On blockchain-based SSI systems, dependence in centralizing authorities has been reduced but not eliminated entirely; instead, it has been replaced by a decentralized entity in which the user must place their trust in order to embrace SSI. To participate in an SSI ecosystem, the user should not be required to rely on a blockchain. However, most

works operate under the erroneous assumption that blockchain is a needed component of SSI. To be self-sovereign, the user should not have to trust anyone, not even a blockchain.

To facilitate the migration from other paradigms. In federated and user-centric models, the IdP bears the administrative burden. Users need only to be concerned with their passwords. With SSI, users are also overburdened with management tasks such as backing up their keys, identities, and credentials as well as creating and presenting claims. We mapped publications that propose techniques for deriving (self-sovereign) identities from federated and user-centric identities (147, 146, 144) as well as those that discuss backup and recovery (173, 174, 18, 172, 175, 176). As a result, academia is gaining momentum on this migration issue.

Usability. Humans will interact with SSI systems. It is critical to research interfaces and how people engage with them as well as how users interact with one another. Meaningful interaction must occur between users and applications and, more importantly, between individuals in an SSI ecosystem. Otherwise, users are unlikely to leave the comfort of their current federated/user-centric identities. A common trend in usability research in SSI is to mimic physical wallets (179, 237), thus presenting the user with everyday interactions. Innovative solutions are necessary and can be decisive for the widespread adoption and success of SSI.

4.10 CONCLUSION

SSI is a new and promising identity management paradigm that increases people's agency in the digital world. It is gaining popularity among academics and industry. We filled in the gaps left by existing surveys, which lack methodological rigor and present biased results in favor of blockchain, thus missing the bigger picture.

In this chapter, we systematically surveyed both peer-reviewed and non-peer-reviewed literature that: (i) expanded the conceptual discussion on what SSI is; (ii) used mathematical formulation to precisely define one or more SSI-related problems and what cryptographic and non-cryptographic tools were used to solve them; and (iii) introduced novel pragmatical problem related to the SSI ecosystem and present a solution to it. After keywording the selected materials, a novel taxonomy of SSI was proposed.

To answer our four research questions, we conducted four separate investigations on the surveyed literature. The results were reported in accordance with the proposed taxonomy and summarized in tables. Maps and tables were also created to categorize the current state-of-the-art research in SSI. These resources, when combined, enable the reader to comprehend each contribution individually while also providing a broad understanding of the current state and maturity of research in SSI. The reported results of our systematic method serve as a foundation for researchers and entrepreneurs who wish to conceptually expand SSI or develop new SSI-related systems. Finally, we discussed unresolved issues and provided recommendations for future research.

In this thesis, we address some of the identified challenges. In Chapter 6 we tackle the challenge of *Fundamental research*, while in Chapter 7 we focus on the challenge of *Usability*.

5 MATCHING METADATA ON BLOCKCHAIN FOR SSI

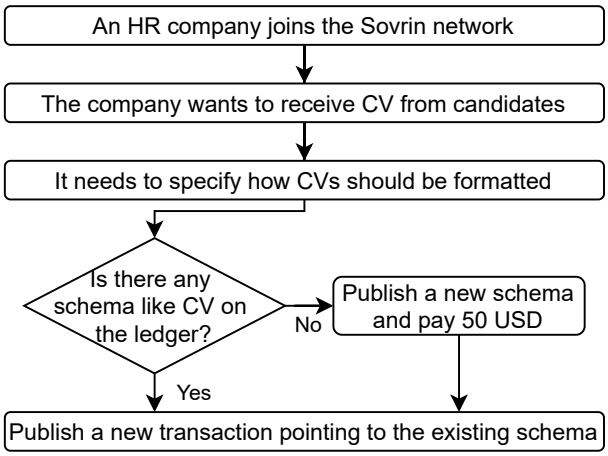
5.1 INTRODUCTION

Most SSI systems are implemented using DLT (*i.e.* blockchains) because of their immutability and fault tolerance (7, 13). As data stored in a blockchain cannot be changed, credentials or other critical information are usually not saved on-chain. What goes on the ledger are revocation registries (or pointers to the registries), end-points for communication, and schemas describing what information each type of credential has (105).

The objective of this chapter is to study the problem of matching metadata on blockchain-based SSI systems. Generally, a blockchain stores transactions describing new users joining the network, metadata[1] describing how users should organize their data to be exchanged with others, among other operations.

As a study case, we adopt Sovrin (105), one of the first SSI offerings made available to the general public and perhaps the most studied (7, 13, 9). However, for the use of Sovrin, there are some challenges. The main one is related to the monetary cost. It happens that most transactions are free, but some have a monetary cost to be handled. Registering a new block describing a new schema is currently the most expensive, costing 50 USD (243). Therefore, reusing existing schemas reduces the capital expenditure of users. Figure 15 presents the sequence of actions in a toy example where a Human Resources (HR) company joins the ledger and publicizes that it wants to receive Curriculum Vitae (CV) in a specific format. Due to the blockchain's structure, where one block is placed after another, searching if similar metadata was published in the ledger is not a trivial task. One would have to go through all the blocks and inspect their contents. Manually matching schemas is not only time-consuming but also error-prone.

Figure 15 – Action flowchart of a toy example in Sovrin.



Source: The author.

[1] The terms metadata and schemas are used interchangeably in this chapter.

Our contribution in this chapter is two-fold: (i) systematically review the blockchain-based SSI scientific literature to identify and investigate which research materials have been published that present any proposal, technique, or tool for retrieving metadata from blockchain-based identity solutions; and (ii) based on the analysis of these existing proposals, we introduced a novel tool to perform metadata matching on Sovrin that outperforms existing solutions by finding semantic similarities between user queries and schemas on the blockchain. Additionally, it can be easily expanded to other blockchain-based SSI systems. The rest of this chapter is organized as follows. In Section 5.2 we detail the SLR, while in Section 5.3 we describe our proposed solution, and Section 5.4 presents some experiments carried out with our proposal showing that it outperforms current solutions. Finally, in Section 5.5 our final observations are made. This chapter has been previously published as a workshop paper (129):

Schardong, F., Custódio, R., Pioli, L., & Meyer, J. (2021). **Matching Metadata on Blockchain for Self-Sovereign Identity**. In Business Process Management Workshops. BPM 2021. Lecture Notes in Business Information Processing, vol 436. (pp. 421-433). Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-94343-1_32

5.2 SYSTEMATIC LITERATURE REVIEW

The main idea of secondary studies is to follow a systematic method to gather evidence and answer specific research questions (19). In this chapter, we conduct a SLR to discover the state of the art regarding searching schemas on blockchain-based SSI.

Research Method

The review protocol we followed has five steps (19): (i) research questions definition; (ii) search strategy for primary studies; (iii) definition of inclusion criteria; (iv) classification of the papers; and (v) data extraction.

To accomplish the first step, we follow the suggestion of Petticrew and Roberts (248) and adopt the PICOC guideline to construct the research question. *Population* refers to a set of elements that we are investigating, blockchain. *Intervention* refers to the element that addresses the study, schema matching. *Comparison* seeks to compare the intervention with some element, which is not used in this study. *Outcome* describes the obtained results, including a practice point of view of them. Our study uses the terms technique, technology, strategy, method, approach, and solution. Finally, *context* is the context in which the comparison takes place, self-sovereign identity. As a consequence of the PICOC guideline, we define the research question guiding this SLR as follows.

Which techniques and technologies were used to search or match schema in blockchain-based self-sovereign identity solutions?

Next, our search strategy consists of using the terms defined in the PICOC guideline in addition to synonyms to create the search string. It is important to note that when running the search string, we noticed that the terms referring to the *outcomes* reduced considerably the number of papers returned by the search libraries. Therefore, we omitted the *outcome* terms to increase the number of papers. The final search string is presented below.

(blockchain **OR** ledger)
AND
(ontology **OR** retrieve **OR** matching **OR** similarity **OR** crosswalk **OR** mapping)
AND
(self-sovereign **OR** self-sovereignty **OR** self sovereign **OR** self-sovereignty **OR** decentralized identity **OR** decentralised identity **OR** distributed identity)

The third step is to define a set of inclusion criteria. These criteria aim to select research studies that fit the research question. In this SLR, we defined three inclusion criteria: (i) IC-1: articles written in English; (ii) IC-2: articles that necessarily have a title and abstract; and (iii) IC-3: articles that propose a technique to search or match schemas in blockchain-based identity management solutions. Papers should meet all IC to be selected for data extraction.

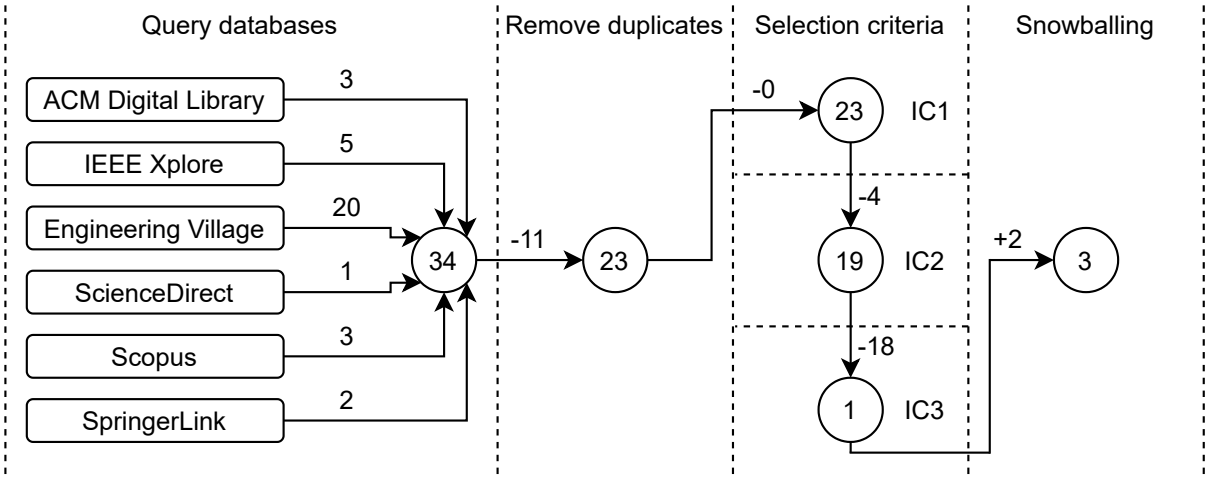
The fourth step, namely the classification of papers, was not performed as any article that meets all IC has equal value in this SLR. Lastly, the data extraction step consisted of reading the selected papers and identifying: (i) what algorithm/technique/technology was used to carry out the schema matching; and (ii) if the proposed solution is an algorithm, tool, framework, or other.

Execution

We conducted our search string on ACM Digital Library, Engineering Village, IEEE Xplore, ScienceDirect, Scopus, and SpringerLink on March 28, 2021, and retrieved a total of 34 primary studies. All the libraries were configured to execute the search string considering only the metadata fields (*i.e.* title, keywords, and abstract). However, in the ACM library, we had to run the search string only on the abstract field, and in Science Direct, we searched on the entire paper. In the second stage, we identified and removed 11 duplicated articles. Next, our IC were applied. As a result, IC-1 removed no paper, IC-2 removed four books of proceedings. Finally, we read all the 19 papers' metadata (*i.e.* keyword, title, and abstract) and applied IC-3, which discarded 18 articles.

The remaining paper was read and analysed (249). Then, to increase the scope of our SLR, a snowballing process was carried. We reviewed its references (backward snowballing) and other articles that cited it (forward snowballing) to identify other potential primary studies. Fifty-five references were reviewed in the backward and forward snowballing. Two new works (250, 251) were included in our set of final results. Figure 16 depicts the execution of our SLR protocol.

Figure 16 – Number of articles in each stage of the execution of our protocol.



Source: The author.

Report

With regards to the research question driving this SLR, our findings are summarized in Table 17. It lists the tools systematically discovered and what technologies were used to search for information in the blockchain. Furthermore, we included our tool in the last row for comparison and detailed it in the next section. Next, we report the three tools found in this SLR.

Table 17 – Comparison of the works found in our SLR and this work.

Work	Technique	Proposal	Search Technology
(249)	Full-text Search	Tool	Apache Solr
(251)	Full-text Search	Tool	Elasticsearch
(250)	Basic Search (249)	Tool	Apache Solr
This work	Semantic Search	Tool	spaCy

Source: The author.

The authors of (249) proposed a tool to perform a full-text search on Hyperledger Indy, which is the blockchain technology underlying Sovrin. This tool performs schema matching based on textual input. It stores a local copy of the ledger on a database and integrates it with Apache Solr[2] to do the matching.

Next, the authors of (251) proposed a tool, named Indyscan, that stores the transactions on a local database and uses Elasticsearch[3] to search for information on the Sovrin ledger based on user-inputted search terms. According to (249), Indyscan uses MongoDB for storing the blockchain's transactions. Moreover, an HTTP Application Programming Interface (API) wrapper was developed to display the ledger transactions as HTML pages and allow users to execute the searches.

[2] https://solr.apache.org/
[3] https://www.elastic.co/

Finally, the last work found in our SLR (250) also implemented an HTTP API to display and search for transactions on the Sovrin ledger. According to (249), this application performs a "basic search". For instance, when searching for a transaction with a person's name, which is the case of the first transaction of the ledger, any changed letter failed to find it. This tool also uses Apache Solr to perform the searches, and the transactions are stored in a PostgreSQL database.

5.3 SEMANTIC-BASED SCHEMA MATCHING

In this section, we describe our proposed solution to the problem of matching schemas in blockchain-based SSI. We use as a study case the Sovrin ledger, which is the first publicly available SSI system (252, 105). The Sovrin ledger is a public-permissioned blockchain where only registered members can write to it, *i.e.*, create e-IDs, and declare credential formats, but anyone can download and read them (252).

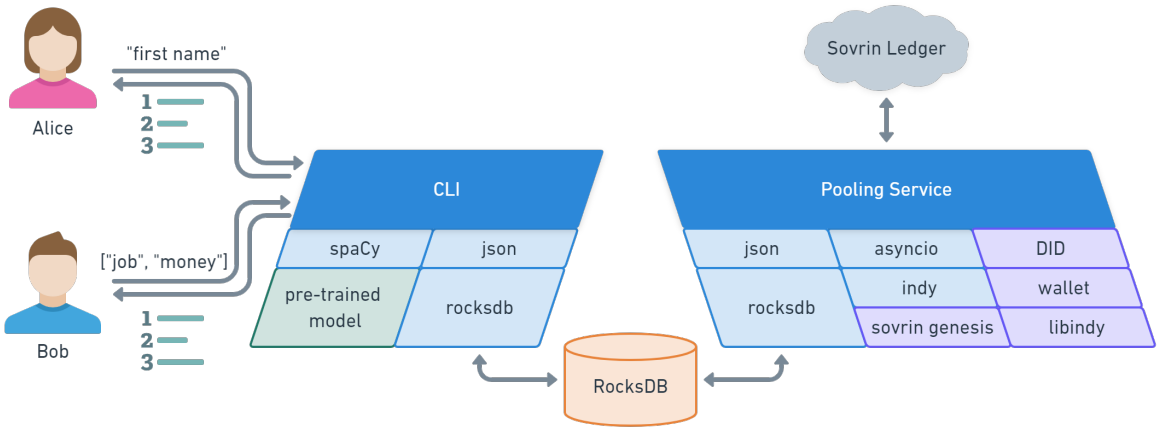
Following the design principles introduced by the authors of (249), which pointed out that sending requests to an online ledger for every system query could impact the performance of the system, we maintain a local copy of the ledger to perform schema matching. As of April of 2021, there are almost 60 thousand transactions registered in the Sovrin ledger. However, only 149 of these are transactions that register new schemas. Therefore, our prototype's persistent storage has less than 100 kilobytes, as only transactions registering schema are persisted. To ensure that the local storage is up-to-date, a pooling service was created and is executed at a constant interval.

Our approach to attack the schema matching problem consists of using a natural language processing tool named spaCy (130). Through the usage of pre-trained word-vectors (131), semantic similarities between user-inputted terms and existing schemas in the blockchain can be calculated. For instance, a pre-trained word-vector of the English language is likely to find a high similarity between the terms *surname* and *last name*. This sort of matching enables our solution to find similar schemas with high accuracy. We used spaCy because it outperforms other offerings (253) and has detailed documentation and active development (130).

Figure 17 shows an overview of our solution. Users can query existing schemas by inputting either natural language queries or presenting schemas formatted in JSON, as represented in Figure 17 by the queries of Alice and Bob to the Command Line Interface (CLI). Both the pooling service and CLI are built using Python 3, where blue parallelograms represent the modules embedded into Docker containers. On the CLI, a green parallelogram shows the pre-trained model of the English language made available by spaCy. The purple parallelograms of the pooling service (DID, wallet, etc.) represent Sovrin-related components. The transactions are stored in an instance of RocksDB, a persistent key-value store optimized for low latency queries (254). Our implementation is open-source and publicly available[4].

[4] https://github.com/fredericoschardong/sovrin-schema-matching/

Figure 17 – An overview of the proposed solution.



Source: The author.

For every query made to the CLI, the three most similar schemas are returned by default along with their score of similarity (calculated by spaCy) and transaction number as referenced in the Sovrin ledger. Two examples are provided: (i) the output of the query "money" is shown in Table 18; and (ii) the results for the JSON-formatted query `["student", "university", "degree"]` is shown in Table 19. These two concrete examples help illustrate the usefulness of semantic search. On the results of the former query, the term `money` is only present in the first result, which is the only schema in the ledger at this point to have this term. Nonetheless, the other two schemas have related terms such as `loan amount`, `interest rate`, `credit score`, `total deposits`, and others. Regarding the results of the latter query, the first and second schemas have the same score as they are composed of the same terms but arranged in a different order. None of the returned schemas have the terms `student` or `university`, but all of them have `degree` and other fields related to education such as `institution` and `GPA`.

Table 18 – Results for the query `"money"`.

Score	Trans. #	Schema Values
0.595	59556	State, Listing Agent, Lot Number, Buyer First Name, Contract Signed Date, Purchase Price, Postal code, Buyer Last Name, Subidivision, City, Street Address, Buyer Agent, Estimated Completion date, Model Name, Earnest Money
0.590	59555	Application Status, Loan Number, Loan Amount, Date of Approval, First Name, Subdivision, Lot Number, Last Name, Earliest Closing Date, Loan Term in Months, APR, Interest Rate, Lender Name
0.569	59551	Credit Score, Account Type, Institution Name, DOB, Total Deposits, SWIFT BIC, IBAN, Last Name, First Name, Statement Period, Average Montly Balance Last 12 months, Total Withrawwals, Account Number

Source: The author.

Table 19 – Results for the query `["student","university","degree"]`.

Score	Trans. #	Schema Values
0.660	54788	`degree, last_name, axuall_proof_id, institution, status, year, first_name`
0.660	54802	`first_name, institution, axuall_proof_id, last_name, degree, year, status`
0.620	33627	`DEMO-GPA, DEMO-Major, DEMO-Degree, DEMO-College Name, DEMO-Student Name`

Source: The author.

5.4 EMPIRICAL EVALUATION

In this section, we describe the method developed to conduct experiments and compare our tool with the solutions found on the SLR, then report the results of its execution and conduct a performance analysis.

Experiment Plan

We have defined three schema matching queries to evaluate our proposed solution and how it compares to the tools in the literature. For each query, a set of correct schemas, *i.e.* schemas that the evaluated technique should return, were manually selected by the fourth author and revised by the first author.

The first query is "address", and the 32 schemas that contain the terms `address`, `country`, `state`, `street`, `zip`, or `city` were manually selected. Next, the second query is "first name". The correct results are the 67 schemas that include `first name`, `given name`, `member name`, `full name`, or `student name`. The reasoning behind these two queries is to evaluate how our solution compares to the existing literature with regard to straightforward queries that might not gain significant advantage using a semantically aware search algorithm. On the other hand, our third query is "company job", and aims to evaluate the gains of performing semantic-aware searches. Correct results included the 23 schemas with any of those two terms or `organization`, `employer`, `department`, `role`, `contract`, or `payment`. All manually selected schemas were not chosen a priori, but rather during the selection of correct schemas on May 16, 2021.

To measure and compare the performance of our tool with the related work regarding those three queries, we have used the f-score, which is the harmonic mean of precision and recall. A confusion matrix for each query and tool was created to calculate those measurements, where the gold standard is the correct schema matching following our manual selection. Regarding our tool, only the results with a score greater than 0.6 were considered schema predictions.

Experimental Evaluation

The experimental evaluation happened on May 16, 2021, when the Sovrin ledger had 149 schemas. We ran the three queries on (251) and (250) through their publicly accessible websites and in our tool. It was not possible to empirically evaluate the work of Lux *et al.* (249) as their solution is not publicly available.

Having the correct and incorrect classification of each tool, we have used `sklearn`'s `classification_report`[5] to assemble the confusion matrices, which are omitted for brevity, and to calculate the f-score. The measurements are made for the two prediction classes: correct and incorrect prediction of schemas, respectively abbreviated to `True` and `False`. Table 20 presents the f-score for each class and their average, along with the support, which is the absolute value of schemas in the `True` and `False` classes.

Table 20 – Correct and incorrect schemas and the f-score of predictions.

Query	Technique	Support		f-score		
		True	False	True	False	Avg.
"address"	(249)	36	112	-	-	-
	(250)			0.65	0.92	0.79
	(251)			0.46	0.90	0.68
	This work			0.29	0.84	0.56
"first name"	(249)	67	81	-	-	-
	(250)			0.66	0.83	0.74
	(251)			0.48	0.78	0.63
	This work			0.76	0.84	0.80
"company job"	(249)	23	125	-	-	-
	(250)			0.00	0.92	0.46
	(251)			0.00	0.92	0.46
	This work			0.55	0.94	0.74

Source: The author.

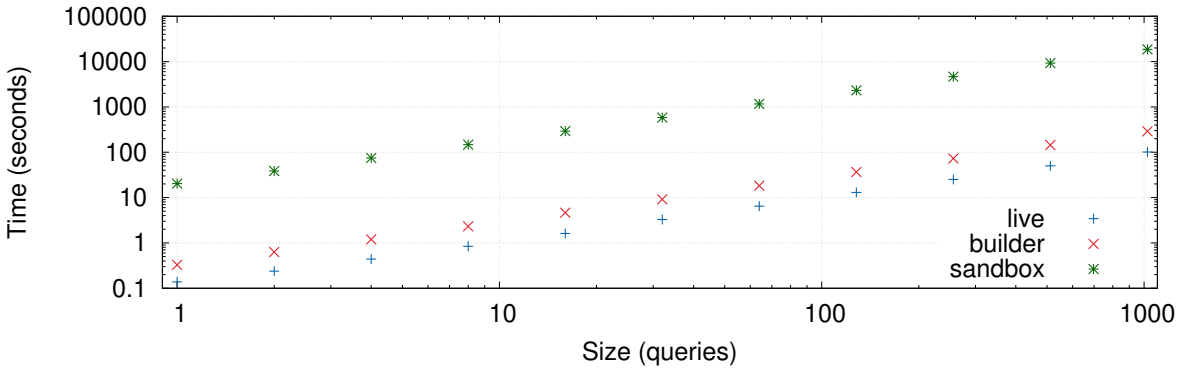
The existing tools produced better results (*i.e.* higher f-score) for the single-word query "address". Our solution returned few and incorrect predictions, which resulted in a low f-score of 0.29 for the `True` class. However, with regard to the query "first name", in which many of the correct schemas do not have the terms `first` and `name`, our tool had a precision of 0.88 and recall of 0.67, thus resulting in an f-score of 0.76 for the `True` class, surpassing the other offerings. Moreover, the advantage of our solution is evidenced in the last query, "company job", in which the other solutions were unable to predict a single schema correctly. That happened because no schema has the two terms `company` and `job`.

[5] https://scikit-learn.org/stable/modules/generated/sklearn.metrics.classification_report.html

Performance

In addition to the production-ready ledger called *live*, which currently has 149 schemas, Sovrin also offers two ledgers for development, *builder* and *sandbox*, which currently have, respectively, 875 and 34543 schemas. We evaluated the performance of our solution on the three ledgers running different amounts of queries and measuring how long they took on commodity hardware. Figure 18 shows how long, on average, each test took. In total, 11 tests composed of $[2^0, 2^1, 2^2, ..., 2^{10}]$ unique two-term queries were performed for each ledger. Although the running time of our tool has scaled linearly with the number of schemas on a ledger, it executed 10 queries per second on *live* and 4 on *builder* but took 20 seconds to run one query on *sandbox*. Therefore, we conclude that it has adequate performance for the short and middle-term future. Many improvements can be made, for instance, to use multi-threading on a Central Processing Unit (CPU) level or to use a Graphics Processing Unit (GPU).

Figure 18 – The performance of our semantically-aware schema matching tool.



Source: The author.

5.5 CONCLUSION

In this chapter, we investigated the problem of searching metadata in blockchain-based SSI. A SLR was conducted to identify the research materials that have been published considering this issue. Moreover, we proposed a novel tool to find similar schemas in this context. As a study case, our tool performs searches on the Sovrin (105) ledger, a publicly available blockchain-based SSI system. Nonetheless, it can be easily expanded to other SSI systems. We have conducted three experiments to measure and compare the proposed solution with the works found in the literature and a performance analysis regarding its scalability.

The experimental results show that it outperforms the existing works in scenarios where the query approaches natural language, which benefits non-specialists, thus popularizing SSI. Both the research method adopted in our SLR and experiments can be reused in future studies. In this sense, we intend to continue this research and: (i) experiment with a more extensive set of queries; (ii) evaluate how different pre-trained word-vectors impact the result; and (iii) add pre-trained word vectors of different languages to capture schemas in other languages.

6 THE ROLE-ARTIFACT-FUNCTION FRAMEWORK

6.1 INTRODUCTION

One of the open challenges identified in the SLR of SSI was the lack of fundamental research about SSI, see Section 4.9. More broadly than SSI itself, existing models lack formal descriptions on a shared ground, which would facilitate their comparison and evaluation. The increasing development of SSI has introduced new challenges and complexities to the field of IAM (3, 7), making formal matters more urgent (77). Formal studies can provide a common language and framework for evaluating e-ID models, allowing for more effective communication between researchers, practitioners, and policymakers. Additionally, such studies can help identify the strengths and weaknesses of different models, leading to the development of more robust and effective IAM solutions.

The IAM literature has often conceptualized e-ID models using a bottom-up approach, starting from real-world instances, such as the protocols and concrete implementations (77). In contrast, this chapter adopts a town-down approach to describe and comprehend e-ID models. We introduce the RAF framework, which comprises a meta-metamodel and a metamodel. The latter is instantiated to describe three IAM models: (i) offline outsourced IdP; (ii) online outsourced IdP; and (iii) SSI. While this work does not cover the instantiation of these models to concrete e-ID systems or protocols, we offer high-level protocols that illustrate the foundational concepts of real-world protocols and applications implementing these models.

In Section 6.2, we present the RAF framework. In Section 6.3, we describe existing models instantiating RAF, creating a shared ground to discuss them in Section 6.4. We explore related work in Section 6.5 and conclude in Section 6.6. This chapter has been accepted for publication as a full conference paper:

Schardong, F., & Custódio, R. (2024). **The Role-Artifact-Function Framework for Understanding Digital Identity Models**. Accepted for publication on the 43rd International Conference on Conceptual Modeling.

6.2 ROLE-ARTIFACT-FUNCTION FRAMEWORK

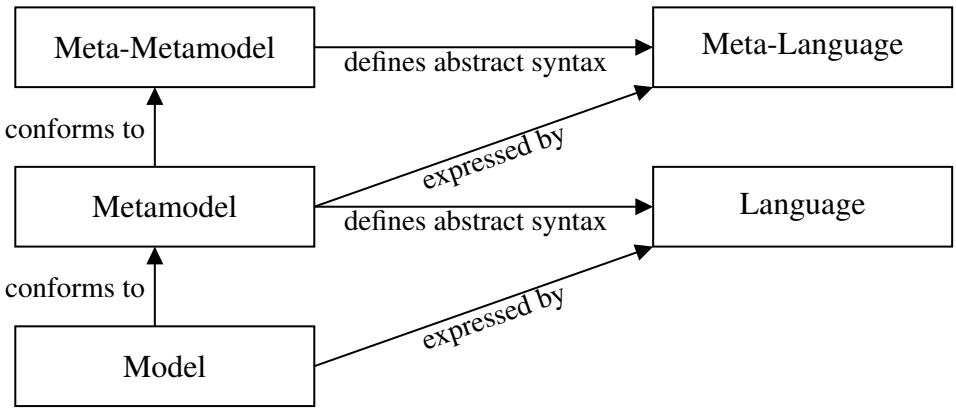
The IAM literature has often conceptualized e-ID models using a bottom-up approach, starting from real-world instances, such as the protocols discussed in Chapter 2. In contrast, the RAF framework adopts a top-down approach to describe and understand e-ID models. The reasoning behind the adoption of a top-down method is the following:

- Enables the creation of a structured and systematic conceptualization of complex systems by starting with a theoretical foundation to have clear definition and articulation of concepts;

- Promotes consistency and coherence across different levels of the model by ensuring that every element of the metamodel is directly traceable to the highest-level principles and constructions. Traceability is essential for model fidelity across contexts and scenarios;
- Allows to maintain a holistic view of the e-ID landscape, instead of being constrained by the specifics or limitations of existing protocols and models, as might occur in a bottom-up approach;
- By starting from a theoretical framework and working down to specific instances, the top-down approach allows for the predictive modeling of future developments in e-ID systems;
- Possesses a normative aspect, proposing how e-ID systems should be structured and managed rather than merely describing how they currently exist.

We adopt a three-level modelling strategy as illustrated in Figure 19 (255). In the first part of this section, the RAF meta-metamodel establishes a high-level abstract syntax, or a meta-language. In the second part, we introduce the RAF metamodel, an instance of the RAF meta-metamodel. Finally, in Section 6.3, we instantiate the RAF metamodel into the existing and so far loosely described e-ID models.

Figure 19 – Model hierarchy.



Source: Inspired by (255).

6.2.1 RAF Meta-Metamodel

The RAF meta-metamodel is grounded in set theory and is defined as follows.

Definition 6.2.1. The *RAF meta-metamodel* is a triple $(\mathbb{R}, \mathbb{A}, \mathbb{F})$, where:

- $\mathbb{R}$ is the set of *roles* played in the e-ID model.
- $\mathbb{A}$ is the set of *computational artifacts* employed by the roles.

- $\mathbb{F}$ is the set of *functions* in the metamodel with domain and co-domain in $\mathbb{R} \cup \mathbb{A}$, and subscript symbols represent the role executing said function.

The *roles* are abstract entities with distinctive computational artifacts and functions that the real-world actors in an IAM system can play. For instance, in SSI, the end-user acts as an IdP and user. The *computational artifacts* represent algorithms, data structures, and other IAM-related artifacts. The *functions* are operations executed by roles. To instantiate this meta-metamodel into a metamodel, we need to provide instances for the sets $\mathbb{R}, \mathbb{A}, \mathbb{F}$ as described next.

6.2.2 RAF Metamodel

Definition 6.2.2. The *RAF metamodel* is defined as an instance of the RAF meta-metamodel $(\mathbb{R}, \mathbb{A}, \mathbb{F})$, where:

- $\mathbb{R}$=$\{s,\ i,\ v\}$ represents the roles within the model.
- $\mathbb{A}$=$\{\mathcal{C},\ \mathcal{R},\ \mathcal{M},\ \mathcal{P},\ \mathcal{L}\}$ denotes the computational artifacts.
- $\mathbb{F}$=$\{issue_i,\ revoke_i,\ status_{s,v},\ trust_v,\ authn_s,\ authz_s,\ request_v,\ present_s,\ verify_v\}$ encompasses the set of functions.

Having established the RAF metamodel, we now detail each component.

Roles ($\mathbb{R}$):

- s: subject, *i.e.*, the user, with a set of attributes $s_A \subset A$ (*e.g.*, age and name) where A is the set of all possible attributes[1].
- i: issuer, *i.e.*, the IdP.
- v: verifier, *i.e.*, the SP.

Computational Artifacts ($\mathbb{A}$):

- $\mathcal{C}$: set of credentials, and each credential $c \in \mathcal{C}$ asserts a set of attributes $c_A \subset s_A$ about subject s[2]. Each attribute $a \in c_A$ has an associated value, denoted by c_a.
- $\mathcal{R}$: set of revocation registries, where each registry $r_c \in \mathcal{R}$ associated with a credential c is associated with a boolean value indicating whether the credential c is valid.
- $\mathcal{M}$: general-purpose machine, *i.e.*, a Turing machine.

[1] We delegate the specifics, such as the value of attributes or how they change over time, to the instances of the metamodel.

[2] The expiration of credentials based on time is excluded for simplicity of abstraction.

- $\mathcal{P}$: program for a general-purpose machine $\mathcal{M}$, *i.e.*, a tape with instructions for the Turing machine.

- $\mathcal{L}$: language for statements, *e.g.*, predicate or first-order logic, where $\mathcal{L}(c \cdot r_c)$ is a statement about a credential c and a revocation registry r_c in $\mathcal{L}$.

Functions ($\mathbb{F}$):

- $issue_i : \{s\} \times \wp(s_A) \nrightarrow \mathcal{C} \times \mathcal{R}$ — issuing a credential by issuer i takes the subject s into consideration, a subset of their attributes $s_{A'} \subset s_A$, and generates a credential $c \in \mathcal{C}$ with attributes $c_A = s_{A'}$ and a revocation record $r \in \mathcal{R}$.

- $revoke_i : \mathcal{C} \times \mathcal{R} \nrightarrow \mathcal{R}$ — given a credential $c \in \mathcal{C}$ and its associated revocation record $r \in \mathcal{R}$, this function updates the record to indicate that c is revoked, producing a new revocation record $r' \in \mathcal{R}$.

- $status_{s,v} : \mathcal{R} \to \{\texttt{true}, \texttt{false}\}$ — determines the revocation status of a credential c. If the revocation record r_c in the set $\mathcal{R}$ indicates that c is revoked, it returns `true`; otherwise, it returns `false`.

- $trust_v : \{i\} \to \{\texttt{true}, \texttt{false}\}$ — the trust function of verifier v returns a boolean indicating whether it trusts issuer i.

- $request_v : \wp(\mathcal{L}(\mathcal{C} \cup \mathcal{R})) \nrightarrow \{s, i\}$ — verifier v can request to subject s or issuer i to provide a program $\mathcal{P}$ that satisfies the set of statements in the language $\mathcal{L}(\mathcal{C} \cup \mathcal{R})$.

- $present_{s,i} : \wp(\mathcal{C}) \times \wp(\mathcal{R}) \times \wp(\mathcal{L}(\mathcal{C} \cup \mathcal{R})) \nrightarrow \{\mathcal{P}\}$ — presenting function takes sets of credentials, revocation registries, and statements as input and produces a program $\mathcal{P}$. The execution of $\mathcal{P}$ in $\mathcal{M}$ is designed to confirm the veracity of the provided statements without compromising the privacy of the associated credentials. Specifically, it ensures that no additional information about the credentials is disclosed.

- $authn_s : \{\mathcal{P}\} \to \{\texttt{true}, \texttt{false}\}$ — the authentication function of the subject s takes a program $\mathcal{P}$ as input and returns a boolean value indicating whether the subject is the owner of the credentials expressed in $\mathcal{P}$.

- $authz_s : \{\mathcal{P}\} \times \{v\} \to \{\texttt{true}, \texttt{false}\}$ — subject s authorization decision function receives a program $\mathcal{P}$ and a verifier v and returns `true` if program $\mathcal{P}$ can be shared with verifier v or `false` otherwise.

- $verify_v : \wp(\mathcal{L}(\mathcal{C} \cup \mathcal{R})) \times \{\mathcal{P}\} \to \{\texttt{true}, \texttt{false}\}$ — verification function returns `true` if the execution of program $\mathcal{P}$ in $\mathcal{M}$ satisfies the set of statements in language $\mathcal{L}$ about credentials and revocation records and `false` otherwise.

As we conclude our exploration of the RAF metamodel, we focus on its practical applications in the next section. We apply the RAF metamodel to two pivotal identity models: outsourced IdP and SSI. This shift is a move from understanding the foundational elements of the RAF framework to seeing it in action, highlighting how it can be used to break down and analyze specific identity management approaches. By examining different e-ID models through the RAF lens, we aim to showcase the framework's utility in describing the nuances that transverse identity systems and, in Section 6.4 arrive at conclusion regarding these models.

6.3 THE ART OF FORMALITY: IDENTITY MODELS THROUGH RAF

In this section, we instantiate the RAF metamodel into the outsourced IdP and SSI models. This process involves defining concrete instances of the abstract components of the RAF metamodel. For the sake of simplicity, we instantiate the most abstract and general elements of the metamodel, *i.e.*, we provide an instance of the language $\mathcal{L}$ and the function $present_s$ for each model. We then demonstrate that these instances meet the functional requirements defined for each e-ID model. While this chapter does not cover the instantiation of these models to concrete e-ID systems or protocols, we offer high-level protocols that illustrate the foundational concepts of real-world protocols and applications implementing these models.

Firstly, we decompose the outsourced IdP model into two: offline and online. The former pertains to outsourced IdP interactions in which the IdP plays no active role in transmitting personal information when the end-user utilizes their credentials, which improves privacy. In contrast, the latter involves the IdP actively engaging in this process, reducing the end-user's privacy but easing the burden of storing and managing their credentials.

6.3.1 Offline Outsourced IdP Model

This section delineates the Offline Outsourced Identity Provider Model (OffOIdPM), a paradigm that allows the credential presentation to occur asynchronously. The model revolves around issuing a credential and a corresponding revocation record to the subject by the IdP, facilitating a verification process that does not necessitate continuous online access to the IdP. It has been a cornerstone of the Internet through the x509 digital certificate (35) and its family of protocols (256, 257, 193, 104, 258, 259), which are detailed later in this section. Definitions 6.3.1 and 6.3.2 lay the foundation for this model, which is further explored through Lemmas 6.3.3, 6.3.5, Corollary 6.3.4, and Theorem 6.3.6.

Definition 6.3.1. In the OffOIdPM, the issuer i issues a credential c and a revocation record r_c to the subject s through executing the $issue_i$ function.

Definition 6.3.2. In the OffOIdPM, subject s shares statements about themselves in language $\mathcal{L}(\mathcal{C} \cup \mathcal{R})$ with verifier v without the involvement of issuer i.

Having defined the OffOIdPM, let us instantiate the RAF metamodel to describe it.

Lemma 6.3.3 ($\mathcal{L}^{\alpha}$ as an instance of $\mathcal{L}$)**.** *In the OffOIdPM, the set of statements regarding credentials and their revocation status can be represented by the language $\mathcal{L}^{\alpha}$, which is a particular instantiation of the RAF metamodel's abstract language $\mathcal{L}$.*

Proof of Lemma 6.3.3. Proof by construction. The language $\mathcal{L}^{\alpha}$ is a regular language over the alphabet $\Sigma = \{c, r_c\}$, and can be formally defined by the regular expression $\mathcal{L}^{\alpha} = (cr_c)^*$. This formulation establishes $\mathcal{L}^{\alpha}$ as a specific instance of the abstract language $\mathcal{L}$, directly applicable to modeling offline credential verification processes. □

Corollary 6.3.4. *The regular language $\mathcal{L}^{\alpha}$ encompasses the empty string $\{\varepsilon\}$ and any sequence of credential c and its revocation record r_c. This regularity confirms that $\mathcal{L}^{\alpha}$ aligns with the formal requirements of $\mathcal{L}$, demonstrating its suitability for modeling credential and revocation record handling in the specified model.*

Lemma 6.3.5 ($present_s^{\alpha}$ as an instance of $present_s$)**.** *In the OffOIdPM, the function that produces programs $\mathcal{P}^{\alpha}$ to prove statements in $\mathcal{L}^{\alpha}$ is $present_s^{\alpha}$, which is a particular instantiation of RAF metamodel's abstract function $present_s$.*

Proof of Lemma 6.3.5. Proof by construction. The function $present_s^{\alpha}$ first ensures by a matching operation that the inputted credentials and revocation records are those referenced by the inputted statement in language $\mathcal{L}^{\alpha}$. Since the statements in language $\mathcal{L}^{\alpha}$ are plain sequences of credentials and revocation records, the program $\mathcal{P}^{\alpha}$ is a sequence of instructions to output the inputted statements.

□

Theorem 6.3.6. *The instantiation of the RAF metamodel's $issue_i$ function following Definition 6.3.1 is trivial and is thus omitted for brevity. However, language $\mathcal{L}^{\alpha}$ and function $present_s^{\alpha}$ are explicitly defined to align with the requirements specified in Definition 6.3.2. Together, these elements provide a complete description of the OffOIdPM.*

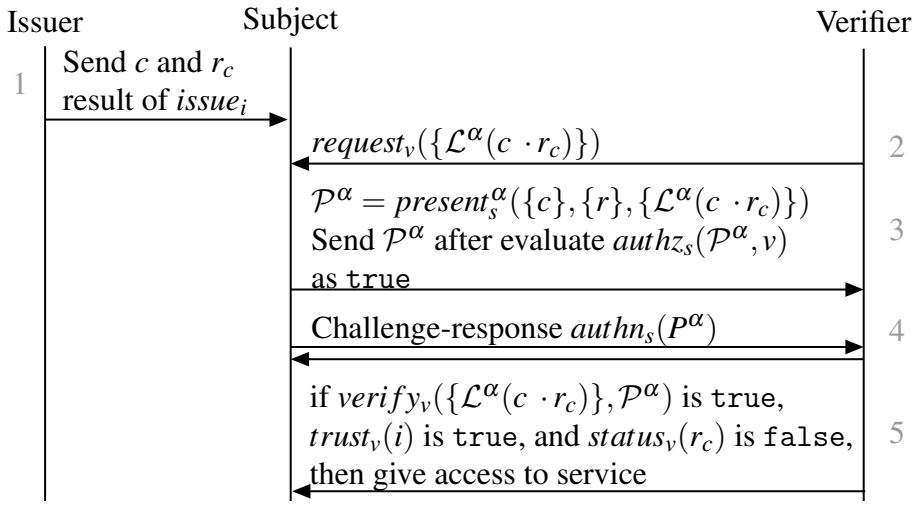
Proof. We prove Theorem 6.3.6 by construction using language $\mathcal{L}^{\alpha}$ and function $present_s^{\alpha}$. We present a high-level protocol that instantiates the OffOIdPM and describes the flow of information respecting Definitions 6.3.1 and 6.3.2. For simplicity, we refrain from instantiating the other functions of the RAF metamodel as their implementation is straightforward. The protocol is depicted in Figure 20 and proceeds as follows:

1. The issuer i generates a credential c and its revocation record r_c through the $issue_i$ function, dispatching both to the subject s.
2. The verifier v requests the credential c and its revocation record r_c from the subject s utilizing the $request_v$ function, specifying the desired language representation $\mathcal{L}^{\alpha}(c \cdot r_c)$.
3. Upon request, the subject s constructs program $\mathcal{P}^{\alpha}$ through the $present_s^{\alpha}$ function, embedding c and r_c within $\mathcal{L}^{\alpha}$ to fulfill the verifier's request, and transmits $\mathcal{P}^{\alpha}$ after evaluating $authz_s(P^{\alpha}, v)$ as `true`.

4. Authentication of ownership over program $\mathcal{P}^{\alpha}$ is achieved by s through the $authn_s$ function, establishing credibility in the presented credentials.

5. The verifier v grants access if it validates the received program $\mathcal{P}^{\alpha}$ against the requested information, the issuer's trustworthiness, and the credential's validity based on the revocation record, completing the verification process.

Figure 20 – An instance of the OffOIdPM high-level protocol.



Source: The author.

This high-level protocol exemplifies how the RAF metamodel's roles, computational artifacts, and functions can be instantiated to implement the OffOIdPM under Definitions 6.3.1 and 6.3.2.

□

Our OffOIdPM model's description and the high-level protocol closely resemble the x509 certificate system and their related protocols (35). For example, issuing x509 certificates, especially within national PKI systems (256), involves rigorous verification steps to confirm the accuracy of subject attributes, akin to our $issue_i$ function. Similarly, the Automatic Certificate Management Environment (ACME) protocol allows internet servers to secure x509 certificates for domain names (257), another practical application of the $issue_i$ function. For revocation, the CRL (193) serves as an example of revocation records R, with the OCSP (104) acting as an instance of the $status_v$ function. In our description, we emphasize offline verification, similar to how CRL might accompany a certificate without needing issuer contact due to both being digitally signed. Authentication is facilitated through the Certificate Management Protocol (CMP), a challenge-response system verifying private key ownership (258). Finally, the Certificate Management over CMS (CMC) protocol illustrates the $revoke_i$ function, showing how certificates are efficiently revoked (259).

The proposed high-level protocol and the digital certificate examples encounter two main problems: privacy and usability. Privacy is compromised because subjects cannot choose

which credential attributes to share. Usability must improve since individuals must always have their credentials for verification. The privacy concern can be addressed with cryptographic schemes that enable selective attribute disclosure (260), which we present in Section 6.3.2. However, the usability issue is fundamental to the model and necessitates changing how information flows, which we explore in Section 6.3.3.

6.3.2 Self-Sovereign Identity

The SSI model is portrayed in the literature as a revolutionary identity model that gives individuals control over their credentials, including who can access them and how they are used (77, 3, 66). However, it is simply a specialization of the OffOIdPM model, as seen below.

Definition 6.3.7. In the SSI model, issuer i issues a credential c and a revocation record r_c to subject s by executing the $issue_i$ function.

Definition 6.3.8. In the SSI model, subject s shares statements about themselves in language $\mathcal{L}(\mathcal{C} \cup \mathcal{R})$ with verifier v without the involvement of issuer i.

Definition 6.3.9. In the SSI model, the language $\mathcal{L}(\mathcal{C} \cup \mathcal{R})$ must allow to: (i) express the disclosure of any subset of attributes of a credential c; and (ii) express properties and relations of any subset of attributes of a credential c.

Note that Definitions 6.3.7 and 6.3.8 are copies of Definitions 6.3.1 and 6.3.2 from OffOIdPM framed for SSI. Thus, SSI is an extension of OffOIdPM that includes an extra bound, namely Definition 6.3.9. We formally describe SSI instantiating the RAF metamodel as follows.

Lemma 6.3.10 ($\mathcal{L}^{\beta}$ as an instance of $\mathcal{L}$)**.** *In the SSI model, the set of statements regarding credentials and their revocation status can be represented by the language $\mathcal{L}^{\beta}$, which is a particular instantiation of the RAF metamodel's abstract language $\mathcal{L}$.*

Proof of Lemma 6.3.10. Proof by construction. The language $\mathcal{L}^{\beta}$ can be created using the First-Order Logic (FOL) constructs to encapsulate SSI's entities, relationships, and processes. The syntax and semantic integration of RAF with FOL forms language $\mathcal{L}^{\beta}$ as follows:

- Variables: Let RAF roles and computational artifacts denote the variables of $\mathcal{L}^{\beta}$.
- Predicates: Let RAF functions be incorporated as FOL predicates by aggregating the inputs and outputs of RAF functions as parameters of the FOL predicates. Non exhaustive list of examples:
  - $issue_i(s, s_A, c, r_c)$: reflects the RAF function $issue_i$, where issuer i issues credential c with attributes s_A and revocation record r_c to subject s. This predicate represents the action of credential issuance.

  - $trust_v(i, \texttt{true})$: reflects the RAF function $trust_v$ indicating that verifier v trusts issuer i.

  Moreover, auxiliary predicates to access and manipulate properties of RAF roles and computation artifacts are defined as follows:

  - $has(a,b)$: indicates if entity a posses, or contains entity b.
  - $comp(op,a,b)$: indicates if the boolean operator op (*e.g.*, $<$, $\geq$, $=$, $\neq$, $\Leftrightarrow$, etc.) between the operands a and b is `true`.

- Functions: No function is required besides standard FOL logical connectives and quantifiers.

□

Corollary 6.3.11 (Direct mapping of $\mathcal{L}^{\beta}$ to RAF.)**.** *By directly mapping RAF functions into FOL predicates, this construction ensures that the language $\mathcal{L}^{\beta}$ accurately reflects the operational semantics of the RAF framework. This direct mapping affirms the language's completeness in representing SSI dynamics.*

Language $\mathcal{L}^{\beta}$ enables the creation of comprehensive statements tailored for the SSI model, in alignment with Definition 6.3.9. To illustrate the capability of $\mathcal{L}^{\beta}$ in formulating such statements, we present two examples:

- A valid credential c which includes an *age* attribute and ensures that the value of this attribute exceeds 18.

$$\mathcal{L}^{\beta}(\exists c\ \exists r_c\ ((status_s(r_c) \Leftrightarrow \texttt{false}) \wedge has(c, age) \wedge comp(>, c_{age}, 18)) \tag{6.1}$$

- A valid credential c from issuer i (*e.g.*, a government body) with a *name* attribute whose value matches that of another credential c''s *name* attribute. Additionally, this second credential c' must be valid and possess a *category* attribute valued at *premium* and should be issued by issuer i' (*e.g.*, a ticket seller for a football game):

$$\begin{aligned}&\mathcal{L}^{\beta}(\exists c\ \exists s_A\ \exists c'\ \exists s'_A\ (issue_i(s, c, s_A, r_c)\\ &\wedge issue_{i'}(s, c', s'_A, r_{c'}) \wedge (status_s(r_c) \Leftrightarrow status_s(r_{c'}) \Leftrightarrow \texttt{false})\\ &\wedge has(c, name) \wedge has(c', name) \wedge has(c', category)\\ &\wedge comp(\Leftrightarrow, c_{name}, c'_{name})\\ &\wedge comp(\Leftrightarrow, c'_{category}, premium)))\end{aligned} \tag{6.2}$$

Lemma 6.3.12 ($present_s^{\beta}$ as an instance of $present_s$)**.** *In the SSI model, the function that produces programs $\mathcal{P}^{\beta}$ that proves statements in $\mathcal{L}^{\beta}$ without revealing additional information is $present_s^{\beta}$, which is a particular instantiation of the RAF metamodel's abstract function $present_s$.*

Proof of Lemma 6.3.12. Proof by construction. The construction of $present_s^\beta$ is demonstrated through the pseudo-algorithm presented in Algorithm 1. To fulfill Definition 6.3.9, we adopt ZKP and use a widely recognized notation (73, 74, 75), symbolized by $\Sigma = (Gen, Prove, Verify)$. Within this scheme, *Gen* generates common parameters, *Prove* for creating a cryptographic proof, and $Verify$ for validating said proof.

Algorithm 1: $present_s^\beta$

Input: Set of credentials $C \subset \mathcal{C}$, set of revocation records $R \subset \mathcal{R}$, query Q in language $\mathcal{L}^\beta$
Output: Program $\mathcal{P}^\beta$

Initialize $\mathcal{P}^\beta$ as an empty list.
Initialize CR'_s as an empty set.
Derive a set of conditions D from Q.
Create tuples linking each credential to its revocation record $CR_s = \{(c_1, r_{c1}), (c_2, r_{c2}), ..., (c_n, r_{cn})\}$ from C and R.
foreach *$d \in D$ related to attribute a, its value c_v or r_c* **do**
    Add all tuples (c, r_c) to CR'_s in which any attribute $a \in c_A$ its value c_v or revocation record r_c is relevant to d.
end
foreach $(c', r_{c'}) \in CR'_s$ **do**
    Establish common parameters $p \leftarrow Gen()$.
    foreach *d requiring verification of a, c'_v or $r_{c'}$* **do**
        Extract witness w showing a, c'_v or $r_{c'}$ satisfies d.
        Create ZKP: $\pi \leftarrow Prove(p, \{a, c'_v, r_{c'}\}, w)$ without revealing w.
        Append $Verify(p, \pi)$ to $\mathcal{P}^\beta$.
    end
end
Combine all verification elements in $\mathcal{P}^\beta$ ensuring $\mathcal{P}^\beta$ ends with an evaluation that returns `true` if and only if all $Verify$ operations are successful, otherwise `false`.
return $\mathcal{P}^\beta$

□

Theorem 6.3.13. *The instantiation of the RAF metamodel's $issue_i$ function following Definition 6.3.7 is trivial and is thus omitted for brevity. However, language $\mathcal{L}^\beta$ and function $present_s^\beta$ are explicitly defined to align with the requirements specified in Definitions 6.3.8 and 6.3.9. Together, these elements provide a complete description of the SSI model.*

Proof. Proof by construction. Let $\mathcal{L}^\beta$, $present_s^\beta$ and $\mathcal{P}^\beta$ be employed in a protocol that describes the flow of information respecting Definitions 6.3.7, 6.3.8 and 6.3.9. We borrow the protocol from the Proof of Theorem 6.3.6, replacing $\mathcal{L}^\alpha$ by $\mathcal{L}^\beta$, function $present_s^\alpha$ for $present_s^\beta$, and program $\mathcal{P}^\alpha$ by $\mathcal{P}^\beta$. Moreover, the statement $\mathcal{L}^\alpha(c \cdot r_c)$ of steps two, three, and five are replaced by the FOL statement presented in Equation 6.1.

□

The SSI model preserves the user's privacy by allowing them to disclose only the necessary information. In this high-level protocol, the subject selects an attribute of one of their credentials to present to the verifier. The verifier does not receive the credentials or revocation registries directly. Instead, the subject constructs a program $\mathcal{P}^{\beta}$ using the selected credential and revocation registry and sends it to the verifier. The verifier trusts the program $\mathcal{P}^{\beta}$ because it is convinced of its truthfulness after executing it to verify the presented statements. The program $\mathcal{P}^{\beta}$ employs ZKP, a technique heavily used in the SSI literature (77).

The OffOIdPM requires users to disclose their credentials to the verifier, who may disseminate this information to other entities. On the other hand, the SSI model exhibits greater flexibility as it empowers users to generate statements regarding their credentials, enabling them to exert more precise control over disseminating their attributes on the Internet.

6.3.3 Online Outsourced IdP Model

Lastly, we diverge from the asynchronicity of OffOIdPM and SSI. This section delineates the Online Outsourced Identity Provider Model (OnOIdPM), which brings usability gains to the detriment of privacy towards the IdP. This model is today's *de facto* standard way of operating over e-ID on the web through the OAuth 2.0 and OIDC protocols. Let us formally define the OnOIdPM as follows:

Definition 6.3.14. In the OnOIdPM, the issuer i issues a credential c and a revocation record r_c and either stores them or sends them to the verifier v.

Definition 6.3.15. In the OnOIdPM, the verifier v inquires the issuer i with statements about a credential c and its revocation record r_c.

The Definitions 6.3.14 and 6.3.15 describe the OnOIdPM, which behaves very distinctively from OffOIdPM and SSI. From the beginning, it is evident that the user is not bothered by the need to store and manage credentials. Let us formally describe it, instantiating the RAF metamodel as follows.

Lemma 6.3.16 ($\mathcal{L}^{\gamma}$ as an Instance of $\mathcal{L}$)**.** *In the OnOIdPM, the set of statements regarding credentials and their revocation status can be represented by the language $\mathcal{L}^{\gamma}$, which is a particular instantiation of the RAF metamodel's abstract language $\mathcal{L}$.*

Proof of Lemma 6.3.16. Proof by construction. The language $\mathcal{L}^{\gamma}$ can be created using a Context-Free Grammar (CFG), which allows for queries regarding attributes in a credential. Let us define the CFG as $\mathcal{L}^{\gamma} = (V, \Sigma, O, S)$, where V is a set of variables (non-terminal symbols), Σ is a set of terminal symbols, O is a set of production rules, S is the start symbol.

Variables (V):

- Q - A query.

- L - A list of attributes to return the value.
- B - An attribute.

  Terminal Symbols (Σ):

- $age, name, \ldots$ - Attributes in A.
- s - The subject s.
- of - Indicates the subject from which to obtain the credential with the attributes.

  Start Symbol:

- $S = Q$ - The start symbol is the query.

  Production Rules (O):

1. $Q \rightarrow L\ of\ s$
2. $L \rightarrow B \mid B\ L$
3. $B \rightarrow age \mid name \mid \ldots$

□

Corollary 6.3.17. *The language $\mathcal{L}^{\gamma}$ facilitates querying one or more attributes from a credential. For example, the query "age name of s" is accepted by $\mathcal{L}^{\gamma}$, indicating it conforms to the grammar's rules for valid queries.*

Lemma 6.3.18 ($present_i^{\gamma}$ as an instance of $present_i$)**.** *In the OnOIdPM, the function that produces programs $\mathcal{P}^{\gamma}$ that proves statements in $\mathcal{L}^{\gamma}$ without revealing additional information is $present_i^{\gamma}$, which is a particular instantiation of the RAF metamodel's abstract function $present_i$.*

Proof of Lemma 6.3.18. The concrete function $present_i^{\gamma}$ has three steps. First, the query, *i.e.*, the statements in language $\mathcal{L}^{\gamma}$, are decomposed into a list of attributes and their credential using the CFG described in Proof 6.3.3. Second, for each existing attribute a in a queried credential c, an instruction is added to program $\mathcal{P}^{\gamma}$. This instruction outputs a and its value, namely c_a. Third, an instruction to output the revocation status of c, namely r_c, is added. □

Theorem 6.3.19. *The instantiation of the RAF metamodel's $issue_i$ function following Definition 6.3.14 is trivial and is thus omitted for brevity. However, language $\mathcal{L}^{\gamma}$ and function $present_i^{\gamma}$ are explicitly defined to align with the requirements specified in Definition 6.3.15. Together, these elements provide a complete description of the OnOIdPM.*

Proof. We prove Theorem 6.3.19 by construction using language $\mathcal{L}^{\gamma}$ and function $present_i^{\gamma}$. We present a protocol that describes the flow of information respecting Definitions 6.3.14 and 6.3.15. The protocol is depicted in Figure 21 and operates as follows:

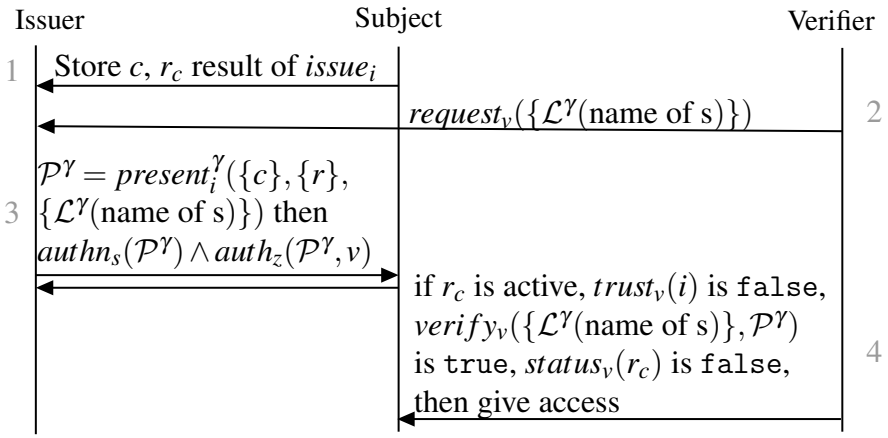
1. Subject s requests a credential from issuer i, which creates a credential c with attributes *age* and *name* and the revocation record r_c, using function $issue_i$ and stores them.

2. Verifier v requests to issuer i for the attribute *name* of subject s using $request_v(\mathcal{L}^{\gamma}(\texttt{name of s}))$.

3. Issuer i uses $present_i^{\gamma}(\{c\},\{r_c\},\{\mathcal{L}^{\gamma}(\texttt{name of s})\})$ to obtain program $\mathcal{P}^{\gamma}$, then asks subject s to prove they are s referenced in $\mathcal{P}^{\gamma}$ through $authn_s(P^{\gamma})$ followed by obtaining authorization to share program $\mathcal{P}^{\gamma}$ with v using the function $authz_s(P^{\gamma},v)$.

4. Issuer i shares the program $\mathcal{P}^{\gamma}$ with verifier v, which grants access to subject s if $\mathcal{P}^{\gamma}$ satisfies the requested statements, and if they trust the issuer, and if the credential is not revoked.

Figure 21 – An instance of the OnOIdPM high-level protocol.



Source: The author.

□

The protocol describes a different information flow than the SSI model. The subject s does not have to store its credentials as the issuer i does that and shares programs with verifier v. This protocol is similar to OAuth 2.0 (36) in three ways. Firstly, the responsibility of implementing an authentication mechanism is delegated to the implementer. Secondly, it requires an expression of intention from the user for the issuer to share their data with the verifier, *i.e.*, the $authz_s$ function. Lastly, the program $\mathcal{P}^{\gamma}$ represents an `access token` containing the authorized user attributes intended for sharing with the verifier.

6.4 DISCUSSION

The literature abstracts real-world applications that use e-ID in e-ID models. However, a thorough analysis demands more than abstracting roles and information flow. The RAF framework facilitates a deeper understanding, more effectively distinguishing between identity

models. This section will explore insights derived from the instantiation of identity models using the RAF metamodel.

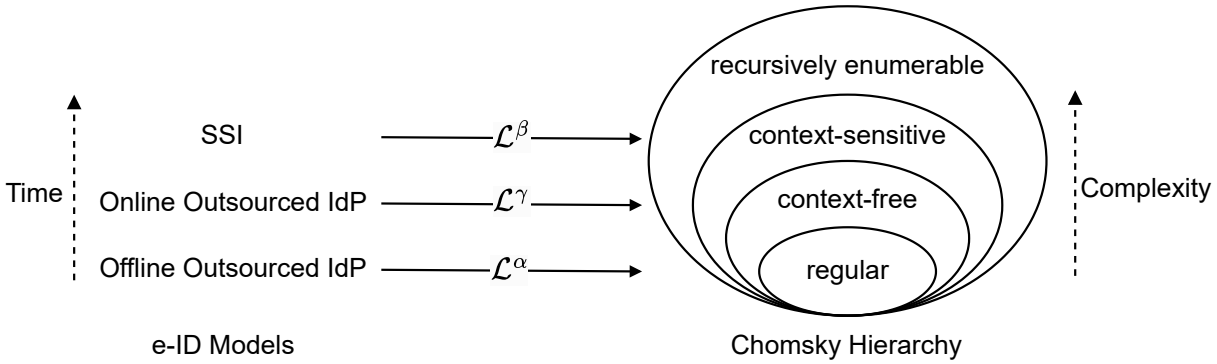
The OffOIdPM and SSI have a lot in common.

The literature points to SSI as a strong driver of innovation in the IAM field (13). Indeed, significant innovation is happening in ZKP and privacy-preserving protocols (77). Nevertheless, the Proof of Theorem 6.3.13 shows that SSI is, from a conceptual point of view, the result of the inclusion of privacy-preserving techniques to express statements about attributes, credentials, and revocation records to the OffOIdPM. This questions the need to abandon three decades of technological advances made in the x509 family of protocols and the myriad of applications that support them in favor of a new stack of technologies. Instead, integrating ZKP and similar modern technologies into existing x509 frameworks might offer users privacy benefits without discarding the existing infrastructure.

Chronological development and linguistic complexity of e-ID models

It is worth noting that the chronology of the creation and popularization of e-ID models aligns with Chomsky's hierarchy (261), depicted in Figure 22. Although we presented the models in the order of OffOIdPM, SSI, and OnOIdPM, their chronological development occurred as follows: first OffOIdPM, then OnOIdPM, and finally SSI. By analyzing the languages associated with these models in their chronological order and classifying them according to Chomsky's hierarchy, we find that the languages $\mathcal{L}^{\alpha}$, $\mathcal{L}^{\gamma}$, $\mathcal{L}^{\beta}$ correspond to Type-3, Type-2, and Type-1 grammars, respectively. The adoption and widespread use of one model over another may be influenced by the increased expressiveness of the languages associated with each model, in addition to the improvements in privacy and usability.

Figure 22 – e-ID models and Chomsky's hierarchy.



Source: The author.

A look into the future.

The chronological development of e-ID models highlights the early establishment of OnOIdPM over SSI (see Chapter 2), which was distinguished by its usability improvement for the end-user. Despite SSI's later introduction, which conceptually echoed OffOIdPM's approach, there are research and market opportunities to leverage OnOIdPM's inherent usability advantages and tackle its privacy disadvantages. To this end, privacy-preserving techniques are being integrated into OnOIdPM's protocols, exemplified by OpenID for Verifiable Presentations, aiming to meld OAuth 2.0 and OIDC with ZKP to reconcile the privacy divide between SSI and OnOIdPM (262).

6.5 RELATED WORK

There have been previous attempts to provide a meta-discussion on e-ID. The "The Laws of Identity" by Kim Cameron (244), for instance, attempts to develop an understanding of identity systems for the Internet. The author draws seven statements, named laws of identity, that they argue should guide the construction of e-ID systems. They range from user consent and minimal disclosure to the pluralism of technologies and consistent user experience. This work offers general guidelines instead of mathematically describing meta-identity with entities and their relationships as this chapter does. This is also the case for the seminal work of SSI, *i.e.* the "The Path to Self-Sovereign Identity" by Christopher Allen (3). Instead of detailing rules of a metamodel for identity or the SSI model itself, ten general directives for SSI are given. We have presented them in Chapter 2.

On the other hand, some related works formally describe identity models. In (34), an abstract identity model named the Digital Identity Model (DIM) is introduced. It defines domains of organizations, users, and their attributes, and a mapping between users, attributes, domains, and their values. In other words, users' attribute value depends on the domain. Other functions are also defined: *e.g.* *ident*, which returns the identifier for a given domain; *checkCredC*, which checks if an identifier and a credential with values match in a context. These are combined to describe existing identity models (34, 167) and protocols (263). In contrast to utilizing general functions as foundational elements that define identity models, *i.e.*, a bottom-up approach, our research presents a metamodel that is instantiated into a model, *i.e.*, a top-down approach. Through this process, entities, computation artifacts, and relationships are established, providing greater versatility and enabling the description of new models with novel relationships, a capability that DIM lacks.

6.6 CONCLUSION

Engaging in meta-discussions about scientific subjects is an essential endeavor that facilitates a deeper understanding of the objectives and methods employed within a particular

field of study. These attempts facilitate additional innovation by utilizing shared notation and establishing mutual knowledge about the various components and their interconnections.

This chapter introduced the RAF meta-metamodel and metamodel as a framework for examining identity and access management dynamics. It was used to formally describe three e-ID models. The utilization of the RAF metamodel facilitated the comparison between the models, effectively highlighting their shared and distinctive characteristics. We hope future IAM-related works employ our suggested notation to articulate their novel contributions.

7 FIDUCIARY IDENTITY

7.1 INTRODUCTION

While SSI promises to enhance user control and privacy, it also introduces challenges in terms of user experience (77). Managing cryptographic keys and digital wallets are inherent activities to SSI that can be challenging for the end user. If not carried out correctly, these activities might lead to credential mismanagement, which leads to the unwanted exposure of private data. Also, requesting and sharing private information in a user-friendly and standardized fashion across various digital services and platforms is challenging. Efforts to simplify the user experience of SSI are ongoing, but these usability limitations must be addressed to ensure its success in practical applications.

Figure 23 shows a typical interaction between the subject and the SP[1] using the Business Process Model and Notation (BPMN). This diagram shows a subject requesting access to a service. It triggers the SP to reply with the required statements, *i.e.*, statements about the attributes in credentials, such as being over a certain age. Here lies a cumbersome and error-prone usability matter of SSI: the user is presented with said required statements by their digital wallet, marked in red in the diagram. The user may lack the mental capacity to comprehend the request, be fatigued or stressed, or have encountered numerous permission prompts, leading to a tendency to accept any request. Drawing a parallel, consider browsing the modern web, where most websites seek user permission to store cookies and approve privacy policies.

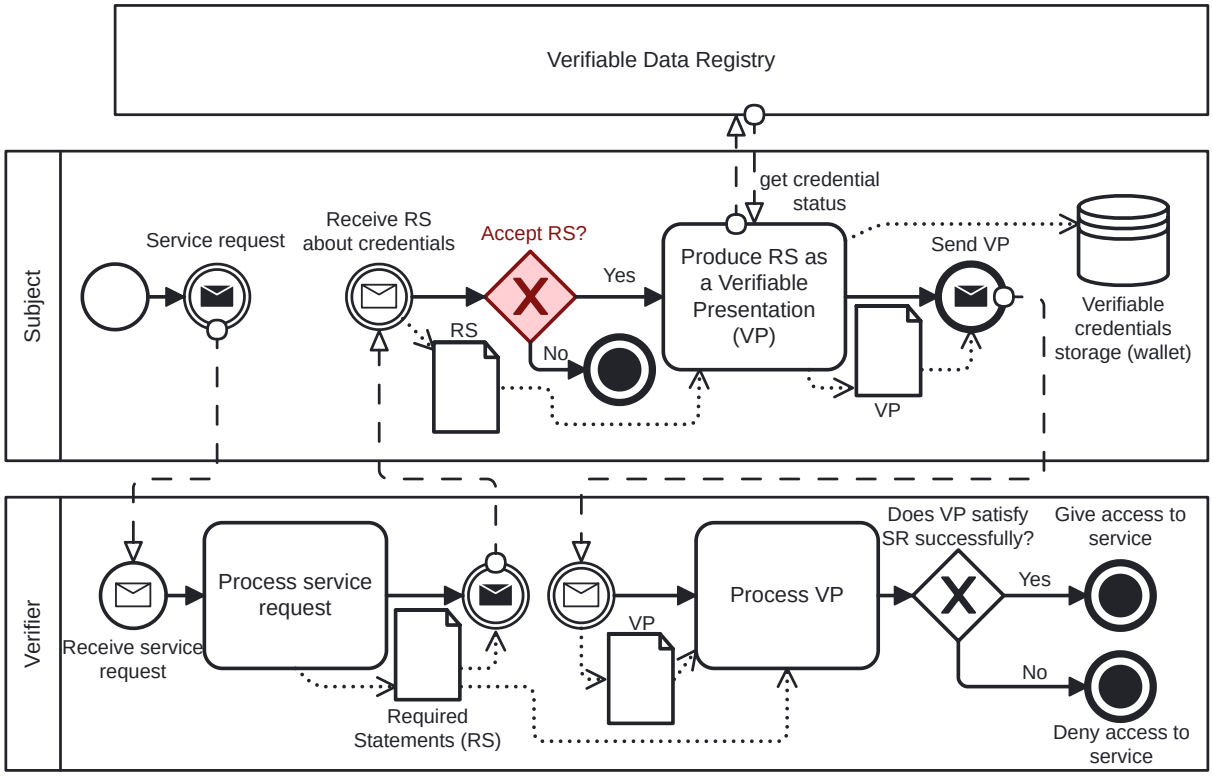
In this chapter, we propose the *Fiduciary Identity*, a new e-ID model that emphasizes user freedom through the fiduciary relationship between the beneficiary, *i.e.*, the user, and the fiduciary, *i.e.*, who manages and worries with day-to-day matters related to user identity. This particular kind of relationship implies that the fiduciary puts the beneficiary's interests over its own, not seeking advantages or misusing the data in any shape or form. This relationship is governed by explicit and implicit consent given or revoked by the user to the fiduciary at any time. The ultimate goal is to free the user from cumbersome, repetitive, and often intrusive interactions with SPs by offloading these interactions to one or more trusted representatives.

Chapter Organization. We introduce a computational model in Section 7.2 to describe the Fiduciary Identity formally. We then thoroughly discuss, formalize, and compare the Fiduciary Identity in Section 7.3. Finally, Section 7.5 concludes the chapter. This chapter has been previously published as a full conference paper (264):

Schardong, F., & Custódio, R. (2024). **From Self-Sovereign Identity to Fiduciary Identity: A Journey Towards Greater User Privacy and Usability**. In Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing (pp. 687-694). DOI: https://doi.org/10.1145/3605098.3636061.

[1] We use the terms subject and user, SP and verifier, and IdP and issuer interchangeably.

Figure 23 – A typical interaction between subject and SP in SSI using BPMN.



Source: The author.

7.2 COMPUTATIONAL MODEL

In the Chapter 2, we have laid the groundwork for various e-ID models. In this section, we delve into a general-purpose computational model, which will serve as the foundation for formally describing the Fiduciary Identity.

The Norma Machine (NM) (265) is similar to the Von Neumann architecture employed in contemporary computers and is equivalent to a Turing Machine (266). A distinguishing feature of the NM is its unlimited number of registers. Registers are memory locations that can store natural numbers of arbitrary sizes and can be accessed and modified at any point. The concept of a program is rigorously defined within the NM framework; it comprises a set of instructions that carry out operations on registers[2]. Programs consist of four fundamental instructions: increment, decrement, conditional jump, and stop.

Definition 7.2.1. Norma Machine is as tuple $NM = (R, Q)$.

Where R is the infinite set of indexed registers r_k, where $k \in [0, \infty]$, with each register capable of storing natural numbers ($\forall k \in [0, \infty], r_k \in \mathbb{N}$). Q comprises the set of operations performed on the registers. There are five operations: (i) e represents the initialization operation, where $e_k(w)$ stores the value w in register r_k, with all other registers set to zero; (ii) s is

[2] A clear differentiation exists between an operation and an instruction. Specifically, every non-empty instruction encompasses an operation, and this operation, in turn, represents the procedure carried out on one or more registers.

the retrieval operation, where s_k retrieves the value stored in register r_k; (iii) z denotes the test operation, with z_k returning `true` if $r_k = 0$ and `false` otherwise; (iv) *ad* signifies the increment operation, as ad_k adds one to register r_k and updates it with the result; and (v) *sub* is the decrement operation, reducing the value in r_k by one and storing the result in the same register. If r_k is at zero, it remains at zero.

With these operations, the *NM* can execute both arithmetic and logical operations on the registers, allowing for the implementation of general-purpose algorithms. The notation e_k, s_k, z_k, ad_k, and sub_k indicate that the respective operation is applied to register r_k.

Definition 7.2.2. A program for the *NM* is represented as a tuple $P = (x, y, I, C, i_0)$.

Here, r_x is the register where the input is stored, and r_y is the register for the output. I is the set of indexes for the program's instructions, while C is the instruction set of the program P. Finally, i_0 is the program's initial instruction index, with $i_0 \in I$. It is worth noting that the instruction pointed to by the address of the initial instruction i_0 must contain the operation e.

The instruction set C are tuples with three elements: $c = (i_\triangledown, o, i_\triangleright) \in C$. The first element of the tuple, $i_\triangledown \in I$, represents the index of the current statement c. The second element, $o \in Q$, specifies the operation to be executed by the instruction c. The third element, $i_\triangleright \in I$, is the index of the statement immediately following c. If $i_\triangleright = \varepsilon$, it indicates a stop instruction.

Let *mem* be defined as the set of pairs that represent all indexed registers r_k and their respective values, denoted by v_k, where k is the register index:

$$mem = \{(r_0, v_0), (r_1, v_1), ...\} \tag{7.1}$$

Definition 7.2.3. The *NM* execution history is a set of pairs $H = \{(c_0, mem_0), (c_1, mem_1), ..., (c_{n-1}, mem_{n-1})\}$

Each pair (c_j, mem_j) consists of the next instruction to be executed, c_j, and the state of the registers at that moment, denoted as mem_j. The index 0 to $n-1$ indicates the states of the program from its inception to its conclusion.

Each valid instruction c_j of the program P in the execution history H evolves the state of the machine from (c_j, mem_j) to (c_{j+1}, mem_{j+1}):

$$(c_0, mem_0) \vdash_{NM} (c_1, mem_1) ... \vdash_{NM} (c_{n-1}, mem_{n-1}) \tag{7.2}$$

The program accepts input w only if there exists a computation of the form:

$$((i_0, e_x(w), i_\triangleright), mem_0) \vdash^n_{NM} ((i_\triangledown, s_y, \varepsilon), mem_{n-1}) \tag{7.3}$$

To enhance convenience, we have compiled a table (Table 21) that includes mathematical symbols associated with the NM computational model, as referenced in the subsequent sections.

Table 21 – Notation table for the computational model.

Symbol	Definition
$NM = (R, Q)$	Norma Machine
$P = (x, y, I, C, i_0)$	Program executable in an NM
H	Execution history of a program P in an NM

Source: The author.

7.3 FIDUCIARY IDENTITY

Both the centralized, outsourced IdP and SSI models have drawbacks concerning user autonomy in managing their data, user-friendliness, or both. The *Fiduciary Identity* model is a novel e-ID approach that seeks to tackle these limitations by relieving users from burdensome and repetitive interactions with SPs. It is based on the fiduciary relationship, where the subject establishes consent rules that the fiduciary uses to reason and act on behalf of the subject.

This section is structured as follows. We initiate by introducing the concept of the fiduciary relationship to the reader. Next, we introduce and motivate the Fiduciary Identity. Subsequently, we delve into the core concepts of the Fiduciary Identity through a formal description aided by the computational model discussed earlier. Following this, we present a high-level protocol outlining the information flow within this model. An introductory discussion of security aspects is given, and finally, we engage in a comprehensive discussion that includes comparisons with existing models.

7.3.1 Foreword about the Fiduciary Relationship

Fiduciary relationships are rooted in trust and responsibility, playing a critical role in our lives. Consider, for instance, the doctor-patient relationship or the attorney-client dynamic, in which professionals are ethically and legally obligated to act in the best interests of their clients. These are instances of fiduciary relationships commonly bounded by law.

While a universally accepted definition of the fiduciary relationship remains unresolved (267), Rotman (268) contends that its inherent flexibility contributes to this lack of consensus. Nonetheless, there are identifiable characteristics of fiduciary relationships as described in common law (269).

In the fiduciary relationship, one party assumes a position of authority and responsibility over another, necessitating utmost care, loyalty, and transparency. In broad terms, a fiduciary is an individual who bears distinct responsibilities of loyalty and reliability towards another individual. The fiduciary must exercise caution and prioritize the other party's best interests, which may be referred to as the principal, beneficiary, or client. The beneficiary places their trust or confidence in the fiduciary, and it is the fiduciary's responsibility to refrain from breaching that trust or confidence (269).

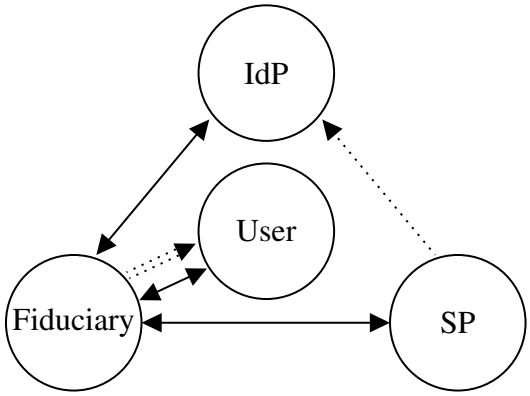
Another aspect of the fiduciary relationship is the consequence that may arise when one entity places its trust and confidence in another and, as a result, gains power and superiority over the other (270). The beneficiary's susceptibility to the fiduciary's abuse of power is a worrisome trait that legal foundations can mitigate.

7.3.2 The Fiduciary Identity Model

In (269), it was suggested that SPs should be considered information fiduciaries. This idea was picked up in (267) and re-framed for the narrow use case of health data SPs. We argue for a different approach. Instead of imposing a fiduciary relationship between end-users and SPs, our thesis argues for creating a fiduciary entity independent of IdPs or SPs. It aims to represent users and put their interests first in the digital world. To be more pragmatic, the fiduciary must manage, make decisions, and take action about the digital selves of whom it represents. It is worth noting that trust, transparency, and consent are, on their own, inadequate means to protect against privacy harms (267). The fiduciary relationship yields stronger bonds and is the ideal choice for the relationship between the end user and whoever represents them.

We introduce the *Fiduciary Identity*, a new e-ID model. It builds upon established concepts from existing identity models (13, 66, 77) to create a more comprehensive, inclusive, and robust e-ID. An architectural overview of the Fiduciary Identity Model (FIM) is shown in Figure 24, where solid lines represent interactions, dashed lines mean trust, and double dashed lines show the fiduciary relationship. The fiduciary represents the user, and thus interacts with the IdP and SP on the user behalf. These interactions are guided by implicit and explicit consent expressed as rules, policies, or guidelines for the fiduciary to reason when representing the user.

Figure 24 – Architectural overview of the FIM.



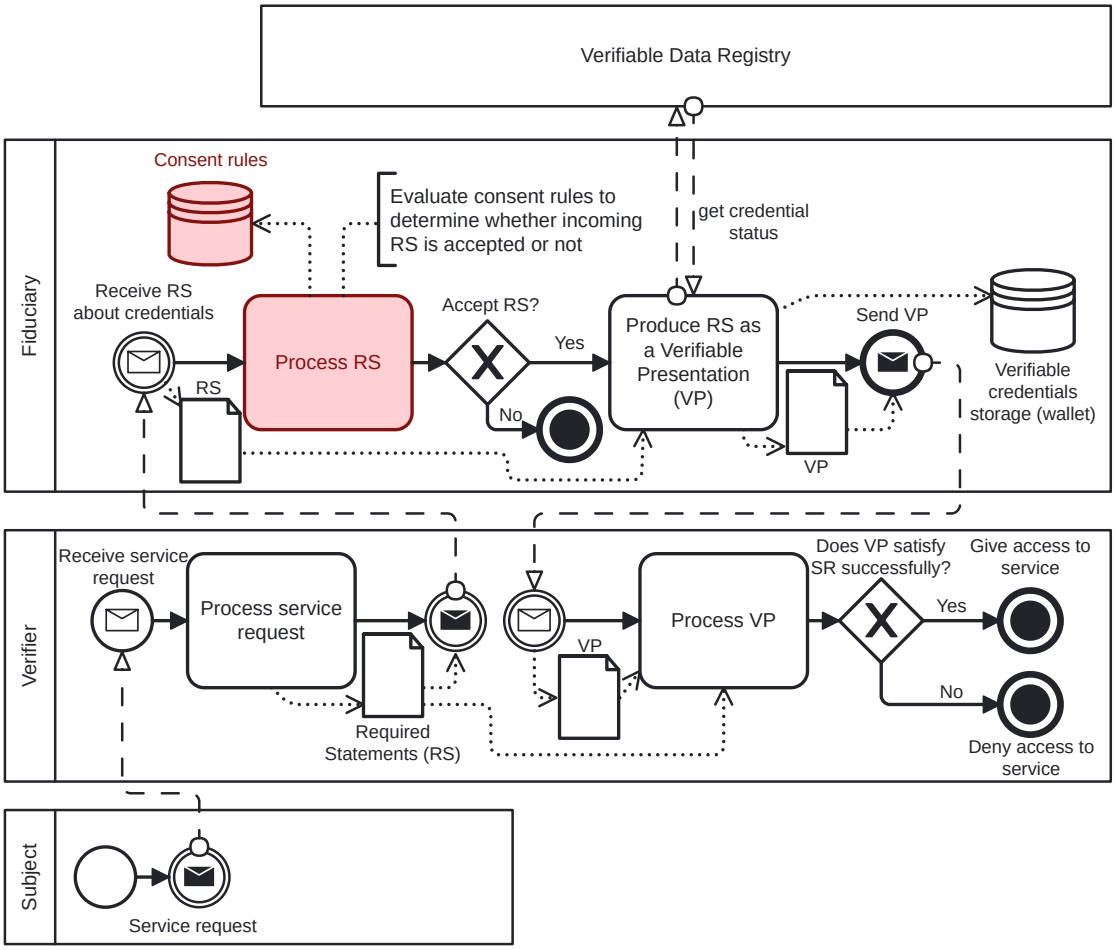
Source: The author.

In the outsourced IdP model, user consent is often implicit or assumed, such as when a user provides personal information to a company in exchange for access to a service. While the SSI model offers several advantages over earlier identity models, it still faces challenges and limitations. Users must actively consent to share their information with verifiers. This presents a challenge because users may need help understanding the full implications of their consent and

are prone to abusive verifiers that might require excessive information. In the FIM the subject must express their consent through rules, policies, or guidelines for the fiduciary to consider when representing the subject. In this model, the fiduciary and the verifier have their own computing devices, which can be used independently or in conjunction to execute algorithms that utilize the subject's data. This model allows the fiduciary to negotiate with verifiers where programs are executed. For example, a fiduciary may not trust a verifier to receive the subject's birthdate but may agree to run the verifier's algorithm on the fiduciary's computing device to ensure the verifier cannot access their birthdate.

Let us show how a vanilla service request interaction, *i.e.* the SP requires private information from the subject to allow access to the requested service, requires less effort from the user in the FIM than previous models. To do that, we step up the example given in Figure 23 to the FIM, shown in Figure 25. Note that all the subject has to do is make the service request. The previously cumbersome and tiring experience of interacting with the verifier is now performed by the user's fiduciary, marked in red, which reasons upon previously expressed consent rules. This example provides an overview of the possibilities. Naturally, the fiduciary might bother the user to request permission if the previously given consent rules ask for such behavior.

Figure 25 – Proposed interaction between subject, fiduciary, and SP.



Source: The author.

7.3.3 Formal Description

To articulate the FIM, we employ the RAF framework. First, we must extend the RAF metamodel to introduce new components. We name it the Fiduciary Identity Metamodel (FIMM), and it is defined as follows.

Definition 7.3.1. The FIMM is defined as an extension of the RAF metamodel as follows:

- $\mathbb{R}$=$\{s,\ i,\ v,\ f\}$ represents the roles.
- $\mathbb{A}$=$\{\mathcal{C},\ \mathcal{R},\ \mathcal{P},\ \mathcal{L},\ \mathcal{M}_f,\ \mathcal{M}_v,\ \mathcal{X},\ \mathcal{E}\}$ denotes the computational artifacts.
- $\mathbb{F}$=$\{issue_i, revoke_i, status_f, trust_v, request_v, present_f, authz_f, exec_{v,f}, verify_v, fiduciary_f, announce_s, express_s, audit_s\}$ encompasses the set of functions.

A detailed description of the new elements follows.

Roles ($\mathbb{R}$):

- $s,\ i,\ v$: as per the standard RAF metamodel, see Definion 6.2.2.
- f: the fiduciary associated with the subject s.

Computational Artifacts ($\mathbb{A}$):

- $\mathcal{C},\ \mathcal{R},\ \mathcal{P}$: following standard RAF metamodel, see Definion 6.2.2.
- $\mathcal{L}$: language for statements about credentials and revocation records following Definion 6.2.2, and also for statements about executions $\mathcal{X}$, represented by $\mathcal{L}(\mathcal{X})$.
- $\mathcal{M}_f,\ \mathcal{M}_v$: the general-purpose machine, *i.e.*, a Turing machine, for the fiduciary and verifier, respectively.
- $\mathcal{X}$: set of executions, each execution $x \in \mathcal{X}$ is a triple $(\mathcal{L}(\mathcal{C} \cup \mathcal{R}),\ \mathcal{P},\ \mathcal{M}')$, representing running a program $\mathcal{P}$ about statemets in language $\mathcal{L}(\mathcal{C} \cup \mathcal{R})$ in a set of general-purpose machines, *i.e.*, $\mathcal{M}' \in \wp(\mathcal{M}_f, \mathcal{M}_v) \setminus \{\emptyset\}$.
- $\mathcal{E}$: set of evidence where each evidence $e \in \mathcal{E}$ shows that running program $\mathcal{P}$ on $\mathcal{M}'$ proves statements in $\mathcal{L}(\mathcal{C} \cup \mathcal{R})$ successfully.

Functions ($\mathbb{F}$):

- $issue_i,\ revoke_i,\ trust_v$: following Definion 6.2.2;
- $status_f : \mathcal{R} \to \{\texttt{true}, \texttt{false}\}$ — following $status_{s,v}$ of Definion 6.2.2, except it is executed by fiduciary f.

- $request_v : \mathcal{X} \nrightarrow \{f\}$ — verifier v can request to fiduciary f an execution $x \in \mathcal{X}$, which has: (i) statements in the language $\mathcal{L}(C \cup R)$; (ii) $\emptyset$ as P, because P will be created by fiduciary f; and (ii) a unit set of $\mathcal{M}$s where program P will run.

- $present_f : \wp(\mathcal{C}) \times \wp(\mathcal{R}) \times \wp(\mathcal{L}(\mathcal{C} \cup \mathcal{R})) \nrightarrow \{\mathcal{P}\}$ — following $present_{s,i}$ of Definion 6.2.2, except it is executed by fiduciary f.

- $authz_f : \mathcal{X} \times \wp(\mathcal{L}(\mathcal{X})) \rightarrow \{\texttt{true}, \texttt{false}\}$ — fiduciary f's authorization decision function to authorize or reject the execution $x \in \mathcal{X}$, *i.e.,* running a program $\mathcal{P}$ in a set of $\mathcal{M}$, also receives a set of consent statements about x in the form $\mathcal{L}(\mathcal{X})$, and returns `true` if execution x may be carried out or `false` otherwise.

- $exec_{v,f} : \mathcal{X} \rightarrow \mathcal{E}$ — running an execution $x \in \mathcal{X}$, *i.e.,* running a program $\mathcal{P}$ in a set of $\mathcal{M}$, results in producing an evidence $e \in \mathcal{E}$.

- $verify_v : \mathcal{E} \rightarrow \{\texttt{true}, \texttt{false}\}$ — verification function takes as input the evidence $e \in \mathcal{E}$. It returns `true` if the execution $x \in \mathcal{X}$ holds, *i.e.*, the statements in $\mathcal{L}(\mathcal{C} \cup \mathcal{R})$ are provided in program $\mathcal{P}$, or `false` otherwise.

- $fiduciary_f : \{s\} \rightarrow \{\texttt{true}, \texttt{false}\}$ — fiduciary function takes as input a subject s and returns whether fiduciary f has a fiduciary relationship with subject s or not.

- $announce_s : \{f\} \rightarrow \{i, v\}$ — subject s announces their fiduciary f to issuer i or verifier v.

- $express_s : \wp(\mathcal{L}(\mathcal{X})) \nrightarrow \{f\}$ — subject s express function receives sets of statements about execution x in language $\wp(\mathcal{L}(\mathcal{X}))$ describing the subject's consent about the usage of their data in different contexts to fiduciary f.

- $audit_s : \wp(\mathcal{L}) \times \{f\} \nrightarrow \mathcal{X} \times \mathcal{E}$ — audit function of subject s receives statements $\wp(\mathcal{L})$ and a fiduciary f, returning any execution in $\mathcal{X}$ and its respective evidence in $\mathcal{E}$.

The FIMM introduces new components to the RAF metamodel to allow for the expressiveness of this proposal. One of the objectives is to enable subject s to express consent rules to their fiduciary f. For instance, subject s needs to be able to describe that certain programs running over some of their personal data can only be executed on the fiduciary's computing environment. This is not possible with the standard RAF metamodel. Therefore, the extensions enable the creation of e-ID models with broader expressiveness. Let us now define the requirements for the FIM using the terminology defined by the FIMM.

Definition 7.3.2. In FIM, issuer i issues a credential c and a revocation record r_c about a subject s through executing the $issue_i$ function and send to the subject's fiduciary f.

Definition 7.3.3. In FIM, fiduciary f shares statements about subject s in language $\mathcal{L}(\mathcal{C} \cup \mathcal{R})$ with verifier v without the involvement of issuer i.

Definition 7.3.4. In FIM, language $\mathcal{L}(\mathcal{C} \cup \mathcal{R})$ must allow to: (i) express the disclosure of any subset of attributes of a credential c; and (ii) express properties and relations of any subset of attributes of a credential c.

Definition 7.3.5. In FIM, verifier v inquires the fiduciary f through $request_v$ using language $\mathcal{L}(\mathcal{X})$ with statements about credentials, revocation records, and the computational environment $\mathcal{M}$ to be used to run program $\mathcal{P}$.

Definition 7.3.6. In FIM, subject s must be able to appoint and retract a fiduciary f to technically and legally represent them in all interactions with issuer i and verifier v. The fiduciary f, in turn, either accepts or denies such responsibilities, represented by the $fiduciary_f$ function.

Definition 7.3.7. In FIM, subject s must be able to set and revoke consent rules to fiduciary f using function $express_s$ and language $\mathcal{L}(\mathcal{X})$ to describe the situations that the creation of program $\mathcal{P}$ to satisfy statements requested by verifier v are allowed.

Definition 7.3.8. In FIM, both fiduciary f and verifier v hold their own computing environment, respectively $\mathcal{M}_f$ and $\mathcal{M}_v$, and both can execute programs $\mathcal{P}$.

Definition 7.3.9. In FIM, the fiduciary f must store executions $\mathcal{X}$ and evidences $\mathcal{E}$, providing them to their subject s upon request through function $audit_s$.

It is worth noting that Definitions 7.3.2, 7.3.3, and 7.3.4 are copies of SSI's Definitions 6.3.7, 6.3.8, and 6.3.9 reframed for FIM. Simiarly, Definition 7.3.5 is a copy of OnOIdPM's Definition 6.3.15 also reframed for FIM. The combination of definitions from both models aims to bring the privacy gains of SSI with the usability of OnOIdPM. In addition, Definition 7.3.6 introduces the fiduciary relationship to the model, and Definition 7.3.7 sets the stage for the consent rules that subject s specifies to fiduciary f. Then, Definition 7.3.8 adds the novelty of allowing the execution of program $\mathcal{P}$ on the fiduciary's computing device. In earlier models, the execution of algorithms over user private information has always happened in the verifier's computing device, see definition of $\mathcal{M}$ in Definition 6.2.2. Lastly, Definition 7.3.9 adds the requirement for the auditability of fiduciary f.

Let us describe FIM as an instance of the FIMM by providing concrete instances of the metamodel's abstract structures. We focus on explaining how the abstract concepts of the FIMM are concretely applied in the FIM, particularly highlighting the more complex and non-obvious aspects essential for understanding its practical application. We formally describe FIM instantiating the FIMM as follows.

Lemma 7.3.10 (NM_v and NM_f as instances of $\mathcal{M}_v$ and $\mathcal{M}_f$)**.** *In FIM, the fiduciary f owns and controls a general-purpose NM, named NM_f, and the verifier v owns and controls a general-purpose NM, named NM_v. The NM is a general-purpose computing machine equivalent to $\mathcal{M}$.*

Proof of Lemma 7.3.10. The general-purpose *NM*, according to Definition 7.2.1, is equivalent to a turin-machine $\mathcal{M}$ as proved in (266). □

Corollary 7.3.11. *Considering that NM is equivalent to $\mathcal{M}$, then it follows naturaly that the program P for an NM, as stated in Definition 7.2.2, is equivalent to the abstract tape with instructions $\mathcal{P}$.*

Corollary 7.3.12. *Considering that according to Collorary 7.3.11, a program P for an NM is equivalent to the abstract tape with instructions $\mathcal{P}$, and considering that according to Definition 7.2.3, the execution history of a program P in an NM is H, then H is an instance of the metamodel's abstract evidence of set $\mathcal{E}$.*

Lemma 7.3.13 (Language $\mathcal{L}^{\delta}$ is an instance of $\mathcal{L}(\mathcal{X})$)**.** *In FIM, the set of statements regarding executions $\mathcal{X}$ are transmitted by subject s to fiduciary f using the function $express_s$. The concrete language $\mathcal{L}^{\delta}$ is an instance of the abstract language $\mathcal{L}(\mathcal{X})$ that encompass credentials, their revocation records, and the NM in which the program P is allowed to be executed.*

Proof of Lemma 7.3.13. Proof by construction. Consider the language $\mathcal{L}^{\beta}$, which is designed to articulate statements about credentials and their revocation records and is built using FOL, see Lemma 6.3.10. Let us define language $\mathcal{L}^{\delta}$ as a variant of $\mathcal{L}^{\beta}$ that additionally incorporates roles, computational artifacts, and functions from the FIMM. The augmented FOL-based language is obtainable following the steps in Proof 6.3.2. □

Corollary 7.3.14. *Language $\mathcal{L}^{\beta}$ is designed for SSI and has enough expressiveness about credentials and revocation records to be used in FIM by the fiduciary f to create program P.*

Corollary 7.3.15. *In SSI, function $present_s^{\beta}$ transforms statements in language $\mathcal{L}^{\beta}$ into program $\mathcal{P}^{\beta}$, see Lemma 6.3.12. In FIM, fiduciary f uses $present_f^{\beta}$, their copy of function $present_s^{\beta}$ that transforms the instructions of program $\mathcal{P}^{\beta}$ into instructions of program P.*

Theorem 7.3.16. *The constructions below form a comprehensive description of FIM:*

1. *The functions $issue_i$ and $fiduciary_f$, as defined in Definitions 7.3.2 and 7.3.6 respectively, are trivially instantiated and omitted for brevity due to their straightforward derivations from the definitions.*

2. *Language $\mathcal{L}^{\beta}$ and function $present_f^{\beta}$, referenced in Corollaries 7.3.14 and 7.3.15, fulfill the criteria of Definitions 7.3.3 and 7.3.4.*

3. *Language $\mathcal{L}^{\delta}$, detailed in Lemma 7.3.13, meets the standards set forth in Definitions 7.3.5 and 7.3.7.*

4. *Computing environments NM_v and NM_f, as discussed in Lemma 7.3.10, comply with Definition 7.3.8.*

5. *The execution history H of a program P within an NM, as outlined in Corollary 7.3.12, satisfies Definition 7.3.9.*

These elements, when combined, form a cohesive and comprehensive representation of the necessary components and interactions defined in the FIMM.

Proof. Proof by construction. We introduce two high-level protocols to demonstrate typical interactions within the FIM, emphasizing secure and private identity information handling. These protocols illustrate how the model manages credential requests and verification processes, ensuring adherence to user-defined consent policies.

Protocol 1: Credential Request and Management

1. *Credential Request Initiation*:
   Subject s initiates a credential request to issuer i, signaling their fiduciary f using $announce_s$ to manage subsequent operations.

2. *Credential Issuance*:
   Upon meeting the requirements, issuer i generates the credential c and a matching revocation record r_c using $issue_i$.

3. *Credential Transfer*:
   Issuer i transmits the credential c and revocation record r_c to the subject's fiduciary f, who securely stores them.

4. *Consent Policy Granting*:
   Subject s assigns, via $express_s$, a set of consent policies in language $\mathcal{L}^{\delta}$. These policies dictate the conditions under which fiduciary f can use $present_f$ to create programs P for execution x.

Protocol 2: Private Attribute Sharing for Service Access

1. *Service Access Request*:
   Subject s seeks a service from verifier v, informing via $announce_s$ that fiduciary f will handle further interactions.

2. *Verifier's Execution Proposal*:
   Verifier v proposes an execution x to fiduciary f using $request_v$, detailing credential requirements in execution x and actions to be executed on their NM_v.

3. *Fiduciary's Authorization Check*:
   Fiduciary f evaluates the proposed execution x against consent policies in $\mathcal{L}^{\delta}$ using $authz_f$ and denies it as unauthorized, notifying verifier v.

4. *Revised Execution Submission*:
   Verifier v submits a revised x', specifying the same statements to be executed on the fiduciary's device NM_f.

5. *Fiduciary's Execution Approval*:
   Fiduciary f reassesses x' and, finding it compliant with $\mathcal{L}^{\delta}$, grants authorization.

6. *Credential Preparation*:
   Fiduciary f selects relevant credential c and its revocation registry r_c.

7. *Statement Generation*:
   Fiduciary f extracts the set of statements L in language $\mathcal{L}^{\beta}$ about credential c and its status r_c.

8. *Program Creation*:
   By using $present_f(\{c\},\{r_c\},L)$, fiduciary f builds program P with necessary credential assertions and revocation status.

9. *Execution and Evidence Generation*:
   Fiduciary f updates x' with P, executing it on NM_f to produce execution history H. The latter is sanitized, producing evidence H' sent to verifier v.

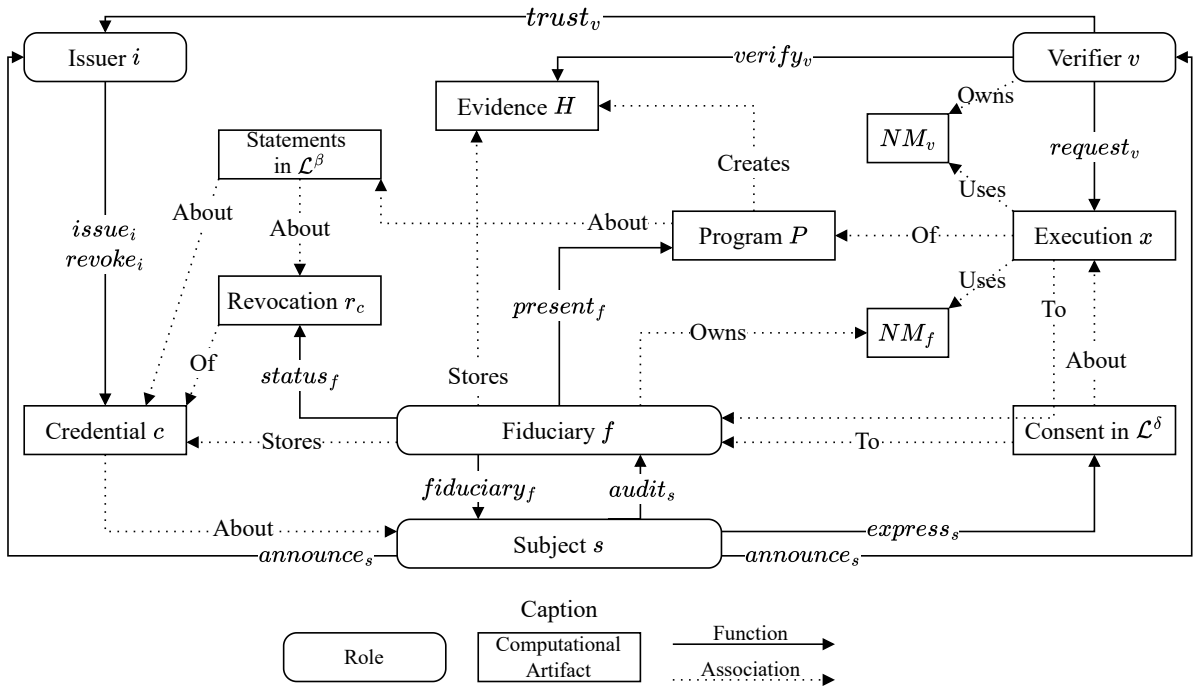
10. *Verifier's Verification*:
    Verifier v receives H', conducting a verification with $verify_v(H')$.

11. *Service or Data Access Decision*:
    If $verify_v(H')$ returns `true`, then verifier v accepts the result of execution of x' and grants access to the requested service or data. If it fails, verifier v denies access.

These protocols showcase the FIM's use of consent policies $\mathcal{L}^{\delta}$ in decision-making, ensuring that fiduciary actions align with user consent. Executing programs within the fiduciary's trusted environment NM_f heightens the security and privacy of the process. □

Figure 26 depicts the proposed FIM, featuring a visually intuitive representation that includes all previously established components and the addition of dashed directional arrows to convey nuanced associations embedded into the model's definitions. The rounded rectangles symbolize roles, the square-cornered rectangles represent computational artifacts, and the continuous directional arrows depict established functions. Notably, the dashed directional arrows introduce a layer of semantic richness by conveying supporting associations embedded into the model's definitions. Each dashed arrow serves as a visual cue, providing insights into relationships such as ownership ("owns"), relevance ("about"), composition ("of"), connection ("to"), storage ("stores"), and functionality ("uses").

Figure 26 – A depiction of FIM.



Source: The author.

7.4 ANALYSIS OF THE FIDUCIARY IDENTITY MODEL

7.4.1 Security Considerations

Like any other e-ID model, the FIM needs careful consideration of security aspects. This model relies on the fiduciary to represent individuals, which places significant responsibility on the fiduciary to protect user information from data breaches or unauthorized access. The reliance on the fiduciary introduces potential vulnerabilities regarding data in transit and at rest. Regarding the former, secure transportation protocols such as TLS can help overcome insecure channels and, with mutual authentication, ensure that the involved parties are who they say they are. Regarding the latter, using secure enclaves in the fiduciary and verifier computing environment can help minimize risks. Secure key management and encryption practices are essential to prevent identity theft and fraud, as malicious actors may attempt to compromise the fiduciary relationship between the subject and the fiduciary.

The communication between the fiduciary and verifier can lean on existing protocols and standards that currently place the user at the negotiation table with the verifier. As the formal description specifies, significant care needs to be placed on collecting and holding onto evidence related to the input and output of processes over user data. Currently, this is not encompassed by existing e-ID protocols to the author's knowledge. Therefore, adopting existing protocols to the FIM requires evolving existing protocols and standards, which naturally yields the necessity of analyzing the security of these protocols.

Specific security measures, including the definition of attack surfaces and threat models, can vary depending on how the FIM is instantiated. Different applications and implementations may face unique security challenges and adversaries. Therefore, any protocols or systems implementing this model must conduct a context-specific analysis of potential security threats and vulnerabilities. This process should include a detailed attack surface assessment, identifying potential weak points where malicious actors might exploit the system.

7.4.2 Comparison of e-ID models

Table 22 presents a comparison of the e-ID models. One of the most striking features of this table is the user autonomy level. The outsourced IdP model gives users more autonomy than the centralized model, as the latter has no user autonomy by design. The SSI and FIM place greater control in the hands of the end-user. In SSI, the subject is responsible for managing IdP-generated data. Differently, in DIM, the end-user has arguably the most autonomy because they are not required to manage anything. The end-user is free to live their life because the fiduciary is responsible for managing and sharing their private data.

Table 22 – Comparison between the main characteristics of the e-ID models.

IAM Model	User Autonomy Level	Driving Relationship	Usability Cognitive Load	Private Data Manager	Consent Management	Compute Site
Centralized	no	dependence	medium	SP	none	SP
Outsourced IdP	low	trust	low	IdP	on demand	SP
SSI	medium	trust	high	subject	on demand	SP
Fiduciary Identity	high	fiduciary	low	fiduciary	a priori; on demand; or a posteriori	SP; fiduciary; or both

Source: The author.

Another important feature to discuss is the usability cognitive load, which we classified according to the three-level scale (low, medium, and high) used in (271). Only the fiduciary and the outsourced IdP models have a low cognitive load, as the management of user information is made by someone else. Although it is common in the implementations of the outsourced IdP model to ask the user to accept or deny sharing their data with SPs on the first access, this is not mandatory on most protocols (37). In the fiduciary model, authorization decisions are made by the fiduciary following the subject's consent rules.

The private data manager column indicates who manages an individual's private data in each model. In the FIM, the fiduciary manages private data. This distinct characteristic sets it apart from other models. The variety in these approaches to data management showcases how different models handle user privacy and data protection, aligning with their overarching principles and trust relationships.

Finally, let us discuss consent management. While in the centralized model, there is no kind of consent, as the IdP and SP are a single entity, in the outsourced IdP and SSI models,

consent is only requested from the end-user once requests from the SP arrive. In other words, consent management happens on demand. In FIM, we bring consent to an architectural level, elevating consent's importance from a protocol implementation detail to a mandatory characteristic of the e-ID model. Our take on consent allows the end-user to provide consent rules, policies, or instructions to their fiduciary a priori to any interaction with SPs, as exemplified earlier in this chapter. Some fiduciary implementations might opt to, by default, inquire the user for any incoming request whose decision-making is not solvable by the user-provided consent rules. On the other hand, the fiduciary could decide independently, based on previous similar requests or some other metric. The subject could review those decisions later and state that the fiduciary's decision was wrong and that they do not consent to what was shared. Naturally, the information shared cannot be taken back. Nonetheless, if a dispute occurs, the fiduciary could be held accountable.

7.4.3 Limitations

Although the proposed mathematical formalization provides a fundamental building block for describing interactions in the FIM, more is needed to express concrete interactions among the subject, fiduciary, issuer, and verifier. Practitioners must fill in many implementation elements because we are proposing a model and not a specific instance. For example, the FIM does not provide details about how entities transfer information, *e.g.*, how subjects communicate consent or perform audits on fiduciaries. Protocols must be created to specify those and other interactions. Another complicated subject for experimentalists is expressing consent policies to a fiduciary. This is not simple, as it requires defining expressive semantics that enable the fiduciary to reason about unforeseen requests from verifiers.

We claim that FIM improves upon the privacy gains of SSI and the usability gains of OnOIdPM. However, the consequence of leaving implementation out of the scope of this thesis is that we do not present a concrete implementation of FIM to verify those claims empirically. The high-level protocols that exemplify interaction in FIM are thought exercises that require ground validation, followed by security and usability analysis, which are out of the scope of this thesis.

7.4.4 Discussion

It is worth pointing out that some authors in the SSI literature split the user role into subject and holder. Where the former has the same meaning as in FIM. However, the latter is different. Take the W3C's VC[3] definition for holder: "A role an entity might perform by possessing one or more verifiable credentials and generating verifiable presentations from them. A holder is often, but not always, a subject of the verifiable credentials they are holding. Holders store their credentials in credential repositories. Example holders include students, employees,

[3] One of the most influential works in the SSI literature as discovered in Chapter 4.

and customers" (66). This definition is much looser in terms of representativeness and responsibility. As the name suggests, the holder is a mere possessor of the credential. This relationship is often understood as the holder as a custodian of the subject, although the definition does not entail such understanding.

Concerning practical matters, the holder is often realized as a digital wallet. The digital wallet is a digitalization of the physical wallet with extra features. In the digitalized wallet, one adds, removes, and uses credentials. The usage involves the end-user choosing specific attributes from their credentials to share with a verifier to access a service. Alternatively, the end-user may accept a request to present attributes or demonstrate certain conditions or predicates related to these attributes that the verifier has pre-prepared with all the necessary details. Once digital wallets decide about verifiers' requests for sharing the subject's attributes automatically, they shall be considered fiduciaries and held accountable for misconduct or breaches. This responsibility implies they must mandatorily store evidence and take consent rules, thus approaching the fiduciary according to FIM's specification.

Nevertheless, the FIM is broader in scope than just automating decisions by a digital wallet. There are other structural changes to the digital wallet to achieve a comprehensive implementation of FIM. The most significant change is to allow the verifier's algorithm to be transferred and executed on the fiduciary's computing environment. This is an open challenge because most verifiers would not accept having their confidential algorithm elsewhere but in their possession. Furthermore, the FIMM is even broader in scope, permitting for an interpretation of FIM — or some new e-ID model — in which the computing environment of both fiduciary and verifier are used cooperatively to run some computation over the subject's information.

It is worth noting that Hardjono and Pentland (272) proposed sharing the verifier algorithm with a data cooperative in which the data cooperative inspects and decides whether it is safe to execute such algorithm over their associated member's data. However, the industry will likely reject the condition of algorithm disclosure for inspection by some third party. More research is needed to incorporate cryptographic techniques to enable algorithms to be executed on the fiduciary's device while offering guarantees to verifiers that their algorithms cannot be reverse-engineered by the fiduciary.

Our utmost objective with FIM is to let people live their lives without worrying about carrying computing devices to access services. People do not want to have e-ID but to use personalized services. The e-ID, and IAM as a whole, is a means to an end that the fiduciary identity could help achieve.

7.5 CONCLUSION

This Chapter introduced the FIM as a promising innovation, offering potential advantages in terms of usability for the end-user. Through the fiduciary relationship, this model significantly reduces the cognitive load on users, simplifying the e-ID experience. Unlike other

models where users must grapple with complex identity management tasks, the FIM entrusts these responsibilities to a fiduciary, streamlining user interactions. This reduction in cognitive load enhances user convenience. By relieving individuals from the intricacies of identity management, the FIM paves the way for a more user-friendly and accessible e-ID landscape.

Open challenges include creating or adapting existing protocols for the new model. In addition, there are challenges in ensuring scalability, analyzing security implications, and ensuring adaptation to global regulatory and cultural landscapes for any implementation of FIM. Future research should delve into these aspects, exploring the practicality of implementation across various regions.

8 FINAL REMARKS

Many systems rely on IAM to identify customers and provide personalized services. Due to the complexities of IAM, the IdP was segregated as a third-party entity responsible for dealing with those complexities. The industry's standard way of using the services of the outsourced IdP is through protocols such as OAuth 2.0 and OIDC, which improves user privacy towards SPs but jeopardize user privacy concerning IdPs. To this extent, the SSI model was conceived, which solved the privacy matter but introduced other challenges.

In this thesis, we attacked multiple challenges within IAM. First, we addressed the pressing concern of ensuring that leading protocols OAuth 2.0 and OIDC are immune to cryptographically relevant quantum computers by switching cryptographic primitives from classic to PQC. This was performed on both TLS and application level, ensuring that the entire stack of protocols that deal with cryptographic primitives is secured against the quantum threat. Concerning SSI, we tackled the problem of performing semantic searches on blockchain-based implementations. In addition, we conducted a rigorous SLR to identify existing literature dealing with conceptual and practical matters. This SLR allowed us to create a taxonomy to categorize and help understand the works in this area. Moreover, we identified open challenges. Some of which we attacked in this thesis. The first was the lack of basic studies trying to understand the properties and qualities of SSI in a formal notation, especially in a notation that enabled the comparison with other e-ID models. To address this challenge, we introduced the RAF framework composed of a meta-metamodel and a metamodel. Another problem identified on the SLR was the usability issue with delegating the management of credentials to end-users. To attack this problem, we introduced the fiduciary identity, formally described as FIM.

The detailed contributions of this thesis are presented in their respective chapters, along with recommendations for future research that may interest both researchers and practitioners. Additionally, this doctoral study's academic and non-academic achievements are outlined in Section 8.1 and Section 8.2, respectively.

In summary, this thesis advances IAM research by enhancing e-ID protocols with PQC, developing new approaches to SSI, introducing the RAF framework to comprehend e-ID models nuances, and tackling issues with the introduction of the fiduciary identity. While further work is needed to refine these innovations, our contributions are steps toward a more secure and inclusive future.

8.1 ACADEMIC CONTRIBUTIONS

This section details the academic contributions achieved during the Ph.D. program. The Chapters 3, 4, 5, 6, and 7 present novel contributions to the state-of-the-art of e-ID and have been published as full papers in peer-reviewed scientific workshops, conferences, or journals. The specific venue is presented on each chapters' introduction.

Beyond the scope of this thesis, there was active involvement in additional scholarly

activities during the doctoral studies. One such endeavor, not detailed within this manuscript, involved co-advising a master's student on the electronic authentication of health professionals during the COVID-19 pandemic. This collaboration led to a published paper on a risk analysis of touch-based authentication factors, exploring touchless alternatives and assurance-level recommendations (273).

Furthermore, the participation in research aimed at improving the security and usability of digital signatures using IdPs to authenticate users resulted in the filing of a patent (274), which is introduced in the next section. Other outcomes of the academic efforts include the publication of two extended abstracts; one describes the implementation of the patented technology by a non-profit company in Brazil (275), and the other details the architecture of a governmental IdP which was conducted on a role of leadership to help design and coordinate the team responsible for implementing it (276). These projects are described further in the subsequent section.

Below is a list of articles published in the course of this Ph.D., including collaborations and following a most-recent-first order:

- Schardong, F., & Custódio, R. (2024). **The Role-Artifact-Function Framework for Understanding Digital Identity Models**. Accepted for publication on the 43rd International Conference on Conceptual Modeling.

- Schardong, F., & Custódio, R. (2024). **From Self-Sovereign Identity to Fiduciary Identity: A Journey Towards Greater User Privacy and Usability**. In Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing (pp. 687-694). Springer, Cham. DOI: 10.1145/3605098.3636061.
  Referenced as (264) in this manuscript.

- Giron, A. A., Schardong, F., Perin, L. P., Custódio, R., Valle, V., & Mateu, V. (2024). **Automated Issuance of Post-Quantum Certificates: A New Challenge**. In International Conference on Applied Cryptography and Network Security (pp. 3-23). Springer, Cham. DOI: 10.1007/978-3-031-54773-7_1.
  Referenced as (277) in this manuscript.

- Schardong, F., Giron, A. A., Müller, F. L., & Custódio, R. (2022). **Post-Quantum Electronic Identity: Adapting OIDC and OAuth 2.0 to the Post-Quantum Era**. In 21st International Conference on Cryptology and Network Security. CANS 2022. Lecture Notes in Computer Science, vol 13641. Springer, Cham. DOI: 10.1007/978-3-031-20974-1_20.
  Referenced as (81) in this manuscript.

- Giron, A. A., Schardong, F., & Custódio, R. (2022). **TLS 1.3 Handshake Analyzer**. In Extended Proceedings of XXII Brazilian Symposium on Information and Computational Systems Security (pp. 63-70). SBC. DOI: 10.5753/sbseg_estendido.2022.226725.
  Referenced as (278) in this manuscript.

- Schardong, F., & Custódio, R. (2022). **Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy**. Sensors, 22(15), 5641. DOI: 10.3390/s22155641.
  Referenced as (77) in this manuscript.

- Vale, C. A., Schardong, F., Barros, M., & Custódio, R. (2022). **Touchless Authentication for Health Professionals: Analyzing the Risks and Proposing Alternatives to Dirty Interfaces**. In 2022 IEEE 35th International Symposium on Computer-Based Medical Systems (CBMS) (pp. 459-464). IEEE. DOI: 10.1109/CBMS55023.2022.00088.
  Referenced as (273) in this manuscript.

- Schardong, F., Custódio, R., Pioli, L., & Meyer, J. (2021). **Matching Metadata on Blockchain for Self-Sovereign Identity**. In Business Process Management Workshops. BPM 2021. Lecture Notes in Business Information Processing, vol 436. (pp. 421-433). Springer, Cham. DOI: 10.1007/978-3-030-94343-1_32.
  Referenced as (129) in this manuscript.

List of extended abstracts published in the course of this Ph.D.:

- Silva, B. V. R., Schardong, F., Junior, L. C. V., & Custódio, R. F. (2023). **Identificação Eletrônica do Registro Civil do Brasil**. In Extended Proceedings of XXIII Brazilian Symposium on Information and Computational Systems Security (pp. 89-92). SBC. DOI: 10.5753/sbseg_estendido.2023.235911.
  Referenced as (276) in this manuscript.

- Perottoni, E. D., Costa, B. P., Müller, F. L., dos Santos Camargo, V., Schardong, F., Silvano, W., ... & Rieckmann, N. (2023). **Menos Certificação Digital e Mais Identidade Eletrônica: ICPEdu e CAFe em um Assinador Digital Inclusivo**. In Extended Proceedings of XXIII Brazilian Symposium on Information and Computational Systems Security (pp. 93-96). SBC. DOI: 10.5753/sbseg_estendido.2023.235947.
  Referenced as (275) in this manuscript.

List of patents filed in the course of this Ph.D.:

- Schardong, F., Athayde, L. M., & Custódio, R. (2022). **Processos de verificação e assinatura digital de documentos eletrônicos baseado em identidade eletrônica, certificado digital de uso único e blockchain**. BR102022012874. Filed on June 28th, 2022. https://patents.google.com/patent/BR102022012874/en.
  Referenced as (274) in this manuscript.

8.2 OTHER CONTRIBUTIONS

During the Ph.D. program, the author participated in multiple endeavors related to the development and offering of e-ID and services. Below is a brief overview of these activities and their societal contributions.

The Brazilian government has implemented a national e-ID system, the gov-br identity (279). This e-ID allows citizens to access various federal, state, and municipal governmental services. It integrates databases from the transit and electoral authorities, which enroll citizens in their physical offices and authenticate them based on physical documents derived from birth certificates. In Brazil, all governmental identity documents, physical and virtual, trace back to the birth certificate issued by the Civil Registry Office for Natural Persons, a decentralized entity within the judiciary branch.

We proposed and conducted the development of an e-ID by the Civil Registry Office for Natural Persons in Brazil, a unique endeavor that aims to establish a national-level e-ID issued and maintained by the same entity responsible for issuing birth certificates. This approach offers distinct advantages, including reduced surveillance by the executive branch due to the judiciary's independence and the consolidation of biometric and biographical information, thereby minimizing data fragmentation across governmental and non-governmental entities. The e-IDs of this IdP are issued concurrently with a birth certificate and becomes fully controlled by the individual upon reaching the age of majority, following an online procedure, or visiting any registrar's office for biometric data collection. Both public and private SPs can utilize this identity through OIDC and OAuth 2.0. The architecture, features, and technologies of this e-ID system are detailed in Appendix B.

Furthermore, a patent filed during the Ph.D. program introduces a novel digital signature approach (274). Traditionally, to perform a digital signature, one must use an x509 digital certificate and its private key. These are issued by a Certificate Authority (CA) after having the user authenticated by a Registration Authority (RA). The basic concept behind the filed patent is to have the RA incorporate e-ID protocols such as OAuth 2.0 and OIDC to act as an online IdP to authenticate users and provide their attributes to CAs on the fly. This approach significantly differs from the traditional approach, in which the user is authenticated only once, and their attributes are provided to the CA only once. By having an IdP always providing the most up-to-date value of identifying characteristics of the user to the CA, the dynamics of digital certification can be drastically changed to improve security and reduce the cumbersome interactions usually associated with digital signature, *e.g.*, using smartcards to make digital signatures.

Another cornerstone of the patent is to have the CA issue a new digital certificate for each digital signature produced by the user. Each new certificate is embedded with the cryptographic hash of the signed document. A key innovation of the patent is the shift from reusing digital certificates between multiple signatures to issuing a One-Time Certificate (OTC) for each digital signature. The OTC incorporates the cryptographic hash of the signed document and al-

lows for the secure disposal of the private key after the realization of the signature. Because users do not have to interact with cryptographic material nor digital certificates, this apporach enhances the accessibility of Public Key Infrastructure (PKI) (280).

The Rede Nacional de Ensino e Pesquisa (RNP) is implementing this novel digital signature approach. RNP is a non-profit entity that played a crucial role in introducing and expanding the Internet in Brazil. RNP is also advancing a SAML-based federation of IdPs across Brazil's universities and research institutions, connecting over one million users and facilitating seamless access to inter-institutional services. The ongoing collaboration with RNP to deploy this patented technology is detailed in Appendix C.

Lastly, during the doctorate program, the author of this thesis was responsible for collaborating with Mozambique's information technology regulatory agency, Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC), to develop traditional and OTC-based PKI. The latter encompasses the creation of a federated e-ID infrastructure that integrates IdPs from various entities, enabling citizens, even those with basic feature phones (281), to digitally sign documents and access electronic governmental services[1].

8.3 AWARDS

The Kim Cameron prize was established by the OpenID Foundation to promote the participation of young individuals who possess a keen interest in topics aligned with the mission of the OpenID Foundation. This mission involves the development of identity standards that prioritize security, interoperability, and privacy preservation. The author of this thesis was among the four recipients of the inaugural Kim Cameron award in 2022[2].

The Vittorio Bertocci Award was created by the Digital Identity Advancement Foundation and aims to respect Vittorio Bertocci's legacy by motivating and helping the upcoming generation of identity experts. Among the three awardees of the first prize in 2024 was the author of this thesis[3].

[1] https://web.archive.org/web/20240602011602/https://assinadoravancado.gov.mz/

[2] https://web.archive.org/web/20231210201407/https://www.openid.net/2022-openid-foundation-kim-cameron-award-recipients-announced/

[3] https://web.archive.org/web/20240821003415/https://digitalidadvancement.org/news/celebrating-excellence-meet-the-first-vittorio-bertocci-award-winners/

BIBLIOGRAPHY

1 ISO Central Secretary. **IT Security and Privacy - A framework for identity management - Part 1: Terminology and concepts**. Geneva, CH, 2019. v. 2019. Available at https://www.iso.org/standard/77582.html, accessed on 13 February 2022.

2 BERTINO, E.; TAKAHASHI, K. **Identity management: Concepts, technologies, and systems**. London, United Kingdom: Artech House, 2010. ISBN 978-1-60807-039-8.

3 ALLEN, C. **The path to self-sovereign identity**. 2016. Available at http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html, accessed on 13 February 2022.

4 HACKETT, R. **LinkedIn Lost 167 Million Account Credentials in Data Breach**. [S.l.]: Fortune, 2016. Available at https://fortune.com/2016/05/18/linkedin-data-breach-email-password/, accessed on 13 February 2022.

5 ISAAK, J.; HANNA, M. J. User data privacy: Facebook, cambridge analytica, and privacy protection. **Computer**, IEEE, v. 51, n. 8, p. 56–59, 2018. https://dx.doi.org/10.1109/MC.2018.3191268.

6 MELENDEZ, S.; PASTERNACK, A. **Here are the data brokers quietly buying and selling your personal information**. 2019. Available at https://www.fastcompany.com/90310803, accessed on 13 February 2022.

7 KUPERBERG, M. Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective. **IEEE Transactions on Engineering Management**, Institute of Electrical and Electronics Engineers Inc., v. 67, n. 4, p. 1–20, 2019. https://dx.doi.org/10.1109/TEM.2019.2926471.

8 ZHU, X.; BADR, Y. Identity management systems for the internet of things: A survey towards blockchain solutions. **Sensors**, Multidisciplinary Digital Publishing Institute, v. 18, n. 12, p. 4215, 2018. https://dx.doi.org/10.3390/s18124215.

9 LIM, S. Y.; FOTSING, P. T.; ALMASRI, A.; MUSA, O.; KIAH, M. L. M.; ANG, T. F.; ISMAIL, R. Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey. **International Journal on Advanced Science, Engineering and Information Technology**, Insight Society, v. 8, n. 4-2, p. 1735–1745, 2018. https://dx.doi.org/10.18517/ijaseit.8.4-2.6838.

10 KANERIYA, J.; PATEL, H. A comparative survey on blockchain based self sovereign identity system. In: IEEE. **2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)**. Coimbatore, India: IEEE, 2020. p. 1150–1155. https://dx.doi.org/10.1109/ICISS49785.2020.9315899.

11 GILANI, K.; BERTIN, E.; HATIN, J.; CRESPI, N. A survey on blockchain-based identity management and decentralized privacy for personal data. In: IEEE. **2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)**. Paris, France: IEEE, 2020. p. 97–101. https://dx.doi.org/10.1109/BRAINS49436.2020.9223312.

12 DIB, O.; TOUMI, K. Decentralized identity systems: Architecture, challenges, solutions and future directions. **Annals of Emerging Technologies in Computing (AETiC), Print ISSN**, v. 4, n. 5, p. 2516–0281, 2020. https://dx.doi.org/10.33166/AETiC.2020.05.002.

13 MÜHLE, A.; GRÜNER, A.; GAYVORONSKAYA, T.; MEINEL, C. A survey on essential components of a self-sovereign identity. **Computer Science Review**, Elsevier, v. 30, p. 80–86, 11 2018. https://dx.doi.org/10.1016/j.cosrev.2018.10.002.

14 LIU, Y.; HE, D.; OBAIDAT, M. S.; KUMAR, N.; KHAN, M. K.; Raymond Choo, K.-K. K. Blockchain-based identity management systems: A review. **Journal of Network and Computer Applications**, Academic Press, v. 166, p. 102731, 9 2020. https://dx.doi.org/10.1016/j.jnca.2020.102731.

15 ALBOAIE, S.; COSOVAN, D. Private Data System Enabling Self-Sovereign Storage Managed by Executable Choreographies. In: **Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)**. Neuchâtel, Switzerland: Springer Verlag, 2017. v. 10320 LNCS, p. 83–98. https://dx.doi.org/10.1007/978-3-319-59665-5_6.

16 ALPÁR, G.; BROEK, F. van den; HAMPIHOLI, B.; JACOBS, B.; LUEKS, W.; RINGERS, S. Irma: practical, decentralized and privacy-friendly identity management using smartphones. In: **10th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2017)**. Minneapolis, USA: HotPETs, 2017. p. 1–2. Available at https://www.petsymposium.org/2017/papers/hotpets/irma-hotpets.pdf, accessed on 13 February 2022.

17 BOKKEM, D. van; HAGEMAN, R.; KONING, G.; NGUYEN, L.; ZARIN, N. Self-sovereign identity solutions: The necessity of blockchain technology. **CoRR**, abs/1904.12816, p. 1–8, 2019. https://dx.doi.org/10.48550/arXiv.1904.12816.

18 LINKLATER, G.; HERBERT, A.; SMITH, C.; IRWIN, B.; HERBERT, A.; IRWIN, B. Toward distributed key management for offline authentication. In: **Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists on - SAICSIT '18**. New York, NY, USA: Association for Computing Machinery, 2018. (SAICSIT '18), p. 10–19. ISBN 9781450366472. https://dx.doi.org/10.1145/3278681.3278683.

19 KEELE, S. et al. **Guidelines for performing systematic literature reviews in software engineering**. [S.l.], 2007. Available at: https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf, accessed on 28 June 2024.

20 PETERSEN, K.; FELDT, R.; MUJTABA, S.; MATTSSON, M. Systematic Mapping Studies in Software Engineering. In: **12th International Conference on Evaluation and Assessment in Software Engineering, EASE 2008**. Bari, Italy: ACM, 2008. p. 1–10. https://dx.doi.org/10.14236/ewic/ease2008.8.

21 ID123 Inc. **ID123**. 2021. Available at https://www.id123.io/, accessed on 13 February 2022.

22 OMETOV, A.; BEZZATEEV, S.; MäKITALO, N.; ANDREEV, S.; MIKKONEN, T.; KOUCHERYAVY, Y. Multi-factor authentication: A survey. **Cryptography**, v. 2, n. 1, p. 31, 2018. ISSN 2410-387X. https://dx.doi.org/10.3390/cryptography2010001.

23 STALLINGS, W. **Cryptography and Network Security: Principles and Practice**. 6th. ed. USA: Prentice Hall Press, 2013. ISBN 0133354695.

24 VIEW, M.; RYDELL, J.; PEI, M.; MACHANI, S. **TOTP: Time-Based One-Time Password Algorithm**. [S.l.]: RFC Editor, 2011. (Request for Comments, 6238). https://dx.doi.org/10.17487/RFC6238.

25 ERDEM, E.; SANDIKKAYA, M. T. Otpaas—one time password as a service. **IEEE Transactions on Information Forensics and Security**, IEEE, v. 14, n. 3, p. 743–756, 2018. https://dx.doi.org/10.1109/TIFS.2018.2866025.

26 BANK, W. **ID4D Practitioner's Guide**. [S.l.]: World Bank Washington, DC, 2019. Available at http://documents.worldbank.org/curated/en/248371559325561562/ID4D-Practitioner-s-Guide, accessed on 13 February 2022.

27 SERVICE, U. government digital. **Introducing GOV.UK Verify**. [S.l.]: Government of the United Kingdom, 2014. Available at https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify, accessed on 13 February 2022.

28 MIYATA, T.; KOGA, Y.; MADSEN, P.; ADACHI, S.-I.; TSUCHIYA, Y.; SAKAMOTO, Y.; TAKAHASHI, K. A survey on identity management protocols and standards. **IEICE TRANSACTIONS on Information and Systems**, v. 89, n. 1, p. 112–123, 2006. https://dx.doi.org/10.1093/ietisy/e89-d.1.112.

29 MALIKI, T. E.; SEIGNEUR, J.-M. A survey of user-centric identity management technologies. In: IEEE. **The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)**. Valencia, Spain: IEEE Computer Society, 2007. p. 12–17. https://dx.doi.org/10.1109/SECUREWARE.2007.4385303.

30 FERDOUS, M. et al. **User-controlled Identity Management Systems using mobile devices**. Tese (Doutorado) — University of Glasgow, 2015. Available at http://theses.gla.ac.uk/6621/, accessed on 13 February 2022.

31 INC. eBay. **eBay**. 1995. Available at https://www.ebay.com/, accessed on 13 February 2022.

32 RESNICK, P.; ZECKHAUSER, R.; SWANSON, J.; LOCKWOOD, K. The value of reputation on ebay: A controlled experiment. **Experimental economics**, Springer, v. 9, n. 2, p. 79–101, 2006. https://dx.doi.org/10.1007/s10683-006-4309-2.

33 KIENNERT, C.; BOUZEFRANE, S.; THONIEL, P. 3 - authentication systems. In: LAURENT, M.; BOUZEFRANE, S. (Ed.). **Digital Identity Management**. Amsterdam, The Netherlands: Elsevier, 2015. p. 95–135. ISBN 978-1-78548-004-1. https://dx.doi.org/10.1016/B978-1-78548-004-1.50003-1.

34 FERDOUS, M. S.; NORMAN, G.; POET, R. Mathematical modelling of identity, identity management and other related topics. In: **Proceedings of the 7th International Conference on Security of Information and Networks**. New York, NY, USA: Association for Computing Machinery, 2014. (SIN '14), p. 9–16. ISBN 9781450330336. https://dx.doi.org/10.1145/2659651.2659729.

35 ITU-T. **Recommendation X.509**. 2000. Available at https://www.itu.int/rec/T-REC-X.509-201910-I/en, accessed on 04 June 2023.

36 HARDT, D. **The OAuth 2.0 Authorization Framework**. [S.l.]: RFC Editor, 2012. (Request for Comments, 6749). https://dx.doi.org/10.17487/RFC6749.

37 SAKIMURA, N.; BRADLEY, J.; JONES, M.; MEDEIROS, B. D.; MORTIMORE, C. **Openid Connect Core 1.0**. [S.l.], 2014. Available at https://openid.net/specs/openid-connect-core-1_0.html, accessed on 13 February 2022.

38 TALIB, S.; CLARKE, N. L.; FURNELL, S. M. An analysis of information security awareness within home and work environments. In: IEEE. **2010 International Conference on Availability, Reliability and Security**. Krakow, Poland: IEEE, 2010. p. 196–203. https://dx.doi.org/10.1109/ARES.2010.27.

39 SCARFONE, K.; SOUPPAYA, M. **Guide to Enterprise Password Management**. [S.l.], 2009. Available at https://csrc.nist.gov/publications/detail/sp/800-118/archive/2009-04-21, accessed on 13 February 2022.

40 HALLAM-BAKER, P.; FRANKS, P. J.; STEWART, L. C.; SINK, E. W.; HOSTETLER, J. L.; LEACH, P. J.; LUOTONEN, A. **An Extension to HTTP : Digest Access Authentication**. [S.l.]: RFC Editor, 1997. (Request for Comments, 2069). https://dx.doi.org/10.17487/RFC2069.

41 RESCHKE, J. **The 'Basic' HTTP Authentication Scheme**. [S.l.]: RFC Editor, 2015. (Request for Comments, 7617). https://dx.doi.org/10.17487/RFC7617.

42 SHEKH-YUSEF, R.; AHRENS, D.; BREMER, S. **HTTP Digest Access Authentication**. [S.l.]: RFC Editor, 2015. (Request for Comments, 7616). https://dx.doi.org/10.17487/RFC7616.

43 HUGHES, J.; MALER, E. **Security Assertion Markup Language (SAML) V2.0 Technical Overview**. [S.l.], 2005. Available at https://www.oasis-open.org/committees/download.php/14361/sstc-saml-tech-overview-2.0-draft-08.pdf, accessed on 13 February 2022.

44 RECORDON, D.; REED, D. Openid 2.0: a platform for user-centric identity management. In: **Proceedings of the second ACM workshop on Digital identity management**. Alexandria, USA: ACM, 2006. p. 11–16. https://dx.doi.org/10.1145/1179529.1179532.

45 LODDERSTEDT, T.; BRADLEY, J.; LABUNETS, A.; FETT, D. **OAuth 2.0 Security Best Current Practice**. [S.l.], 2022. Available at https://datatracker.ietf.org/doc/html/draft-ietf-oauth-security-topics, accessed on 28 June 2024.

46 SAKIMURA, N.; BRADLEY, J.; AGARWAL, N. **Proof Key for Code Exchange by OAuth Public Clients**. [S.l.]: RFC Editor, 2015. (Request for Comments, 7636). https://dx.doi.org/10.17487/RFC7636.

47 BERNERS-LEE, T.; FIELDING, R. T.; MASINTER, L. M. **Uniform Resource Identifier (URI): Generic Syntax**. [S.l.]: RFC Editor, 2005. (Request for Comments, 3986). https://dx.doi.org/10.17487/RFC3986.

48 SAKIMURA, N.; BRADLEY, J.; JONES, M. Openid connect dynamic client registration. **The OpenID Foundation**, p. S3, 2014. Available at: https://openid.net/specs/openid-connect-registration-1_0.html, accessed on 28 June 2024.

49 SAKIMURA, N.; BRADLEY, J.; JONES, M.; JAY, E. Openid connect discovery. **The OpenID Foundation**, p. S3, 2014. Available at: https://openid.net/specs/openid-connect-discovery-1_0.html, accessed on 28 June 2024.

50 JOHANSSON, L. **An IANA Registry for Level of Assurance (LoA) Profiles**. [S.l.]: RFC Editor, 2012. (Request for Comments, 6711). https://dx.doi.org/10.17487/RFC6711.

51 SEARLS, D. **The Identity Problem**. 2012. Available at https://blogs.harvard.edu/vrm/2012/11/08/the-identity-problem/, accessed on 13 February 2022.

52 LOFFRETO, D. **Administrative Precedence**. 2013. Available at https://www.moxytongue.com/2013/01/administrative-precedence.html, accessed on 13 February 2022.

53 European Parliament, Council of the European Union. **Regulation (EU) 2016/679**. 2016. Available at http://data.europa.eu/eli/reg/2016/679/oj, accessed on 13 February 2022.

54 CHAU, E. P.; HERTZBERG, R. **California Consumer Privacy Act of 2018**. 2018. Available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375, accessed on 13 February 2022.

55 MILL, J. S. **On liberty**. London, England: John W. Parker and Son, West Strand, 1859. Available at https://socialsciences.mcmaster.ca/econ/ugcm/3ll3/mill/liberty.pdf, accessed on 28 June 2024.

56 UZGALIS, W. John Locke. In: ZALTA, E. N. (Ed.). **The Stanford Encyclopedia of Philosophy**. Spring 2020. Stanford, USA: Metaphysics Research Lab, Stanford University, 2020. Available at https://plato.stanford.edu/archives/spr2020/entries/locke/.

57 LOFFRETO, D. **What is "Sovereign Source Authority"?** 2012. Available at https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html, accessed on 13 February 2022.

58 SEARLS, D. **Some Perspective on Self-Sovereign Identity**. 2018. Available at https://www.kuppingercole.com/blog/guest/some-perspective-on-self-sovereign-identity, accessed on 13 February 2022.

59 YOUNG, K.; INFOMINER. The origins of the ssi community. In: **Self-Sovereign Identity: Decentralized digital identity and verifiable credentials**. Shelter Island, ÙSA: Manning, 2021. v. 1, p. 310–321. ISBN 9781617296598. Available at https://livebook.manning.com/book/self-sovereign-identity/chapter-16/, accessed on 13 February 2022.

60 VESCENT, H.; YOUNG, K.; DUFFY, H.; SABADELLO, M.; ZAGIDULIN, D.; CABALLERO, J. **A Comprehensive Guide to Self Sovereign Identity**. [S.l.]: The Purple Tornado, California, 2019.

61 YOUNG, K. **The Domains of Identity: A Framework for Understanding Identity Systems in Contemporary Society**. [S.l.]: Anthem Press, 2020. ISBN 9781785274916.

62 SEARLS, D. **Leveraging Whitman**. 2013. Available at http://blogs.harvard.edu/vrm/2013/08/21/leveraging-whitman/, accessed on 13 February 2022.

63 SEARLS, D. **IIW Challenge #1: Sovereign Identity in the Great Silo Forest**. 2013. Available at http://blogs.harvard.edu/doc/2013/10/14/iiw-challenge-1-sovereign-identity-in-the-great-silo-forest/, accessed on 13 February 2022.

64 SEARLS, D. **Personal = Sovereign**. 2014. Available at http://blogs.harvard.edu/vrm/2014/02/06/personal-sovereign/, accessed on 13 February 2022.

65 LOFFRETO, D. **Recalibrating Sovereignty**. 2013. Available at https://www.moxytongue.com/2013/04/recalibrating-sovereignty.html, accessed on 13 February 2022.

66 SPORNY, M.; LONGLEY, D.; CHADWICK, D. **Verifiable Credentials Data Model 1.0**. 2017. Available at https://www.w3.org/TR/vc-data-model/, accessed on 13 February 2022.

67 REED, D.; SPORNY, M.; LONGLEY, D.; CHRISTOPHER, A.; GRANT, R.; SABADELLO, M. **Decentralized Identifiers (DIDs)**. 2019. Available at https://www.w3.org/TR/did-core/, accessed on 13 February 2022.

68 TOTH, K. C.; ANDERSON-PRIDDY, A. Self-Sovereign Digital Identity: A Paradigm Shift for Identity. **IEEE Security and Privacy**, IEEE, v. 17, n. 3, p. 17–27, 5 2019. https://dx.doi.org/10.1109/MSEC.2018.2888782.

69 TURNER, S.; FARRELL, S.; HOUSLEY, R. **An Internet Attribute Certificate Profile for Authorization**. [S.l.]: RFC Editor, 2010. (Request for Comments, 5755). https://dx.doi.org/10.17487/RFC5755.

70 CAMENISCH, J.; LYSYANSKAYA, A. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: PFITZMANN, B. (Ed.). **Advances in Cryptology — EUROCRYPT 2001**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001. p. 93–118. ISBN 978-3-540-44987-4. https://dx.doi.org/10.1007/3-540-44987-6_7.

71 CAMENISCH, J.; LYSYANSKAYA, A. Dynamic accumulators and application to efficient revocation of anonymous credentials. In: YUNG, M. (Ed.). **Advances in Cryptology — CRYPTO 2002**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002. p. 61–76. ISBN 978-3-540-45708-4. https://dx.doi.org/10.1007/3-540-45708-9_5.

72 CHAUM, D. Security without identification: Transaction systems to make big brother obsolete. **Commun. ACM**, Association for Computing Machinery, New York, NY, USA, v. 28, n. 10, p. 1030–1044, 10 1985. ISSN 0001-0782. https://dx.doi.org/10.1145/4372.4373.

73 LEE, J.; CHOI, J.; OH, H.; KIM, J. Privacy-preserving identity management system. **Cryptology ePrint Archive 2021/1459**, 2021. Available at https://eprint.iacr.org/2021/1459.pdf, accessed on 13 March 2022.

74 LEE, J.; HWANG, J.; CHOI, J.; OH, H.; KIM, J. SIMS: Self-Sovereign Identity Management System with Preserving Privacy in Blockchain. **IACR Cryptology ePrint Archive**, v. 1, n. 2019/1241, p. 1–13, 2019. Available at https://eprint.iacr.org/2019/1241.pdf, accessed on 13 February 2022.

75 SCHANZENBACH., M.; KILIAN., T.; SCHüTTE., J.; BANSE., C. Zklaims: Privacy-preserving attribute-based credentials using non-interactive zero-knowledge techniques. In:

INSTICC. **Proceedings of the 16th International Joint Conference on e-Business and Telecommunications - SECRYPT,**. Prague, Czech Republic: SciTePress, 2019. p. 325–332. ISBN 978-989-758-378-0. ISSN 2184-2825. https://dx.doi.org/10.5220/0007772903250332.

76 SCHNORR, C. P. Efficient identification and signatures for smart cards. In: BRASSARD, G. (Ed.). **Advances in Cryptology — CRYPTO' 89 Proceedings**. New York, NY: Springer New York, 1990. p. 239–252. ISBN 978-0-387-34805-6. https://dx.doi.org/10.1007/0-387-34805-0_22.

77 SCHARDONG, F.; CUSTÓDIO, R. Self-sovereign identity: A systematic review, mapping and taxonomy. **Sensors**, MDPI, v. 22, n. 15, p. 5641, 2022. https://dx.doi.org/10.3390/s22155641.

78 SHOR, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In: IEEE. **Proceedings 35th annual symposium on foundations of computer science**. Santa Fe, NM, USA: IEEE, 1994. p. 124–134. https://dx.doi.org/10.1109/SFCS.1994.365700.

79 GROVER, L. K. A fast quantum mechanical algorithm for database search. In: **Proceedings of the 28th ACM symposium on theory of computing**. [S.l.: s.n.], 1996. p. 212–219. https://dx.doi.org/10.1145/237814.237866.

80 NIST. **Post-quantum cryptography**. 2016. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography, accessed on 28 June 2024.

81 SCHARDONG, F.; GIRON, A.; MüLLER, F.; CUSTÓDIO, R. Post-quantum electronic identity: Adapting openid connect and oauth 2.0 to the post-quantum era. In: SPRINGER. **International Conference on Cryptology and Network Security**. [S.l.], 2022. p. 371–390. https://dx.doi.org/10.1007/978-3-031-20974-1_20.

82 LODDERSTEDT, T.; MCGLOIN, M.; HUNT, P. **OAuth 2.0 Threat Model and Security Considerations**. [S.l.]: RFC Editor, 2013. (Request for Comments, 6819). https://dx.doi.org/10.17487/RFC6819.

83 RESCORLA, E. **The Transport Layer Security (TLS) Protocol Version 1.3**. [S.l.]: RFC Editor, 2018. (Request for Comments, 8446). https://dx.doi.org/10.17487/RFC8446.

84 JONES, M.; BRADLEY, J.; SAKIMURA, N. **JSON Web Token (JWT)**. [S.l.]: RFC Editor, 2015. (Request for Comments, 7519). https://dx.doi.org/10.17487/RFC7519.

85 JONES, M. **JSON Web Key (JWK)**. [S.l.]: RFC Editor, 2015. (Request for Comments, 7517). https://dx.doi.org/10.17487/RFC7517.

86 JONES, M.; SAKIMURA, N.; BRADLEY, J. **OAuth 2.0 Authorization Server Metadata**. [S.l.]: RFC Editor, 2018. (Request for Comments, 8414). https://dx.doi.org/10.17487/RFC8414.

87 BERTOCCI, V. **JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens**. [S.l.]: RFC Editor, 2021. (Request for Comments, 9068). https://dx.doi.org/10.17487/RFC9068.

88 (IANA), I. A. N. A. **Transport Layer Security (TLS) Parameters**. 2022. https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml, accessed on 28 June 2024.

89 BERBECARU, D.; LIOY, A. On the robustness of applications based on the ssl and tls security protocols. In: SPRINGER. **European Public key infrastructure workshop**. [S.l.], 2007. p. 248–264. https://dx.doi.org/10.1007/978-3-540-73408-6_18.

90 HOWE, J.; PREST, T.; APON, D. **SoK: How (not) to Design and Implement Post-Quantum Cryptography**. 2021. Available at https://ia.cr/2021/462, accessed on 28 June 2024.

91 SIKERIDIS, D.; KAMPANAKIS, P.; DEVETSIKIOTIS, M. Assessing the overhead of post-quantum cryptography in tls 1.3 and ssh. In: **Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies**. New York, NY, USA: Association for Computing Machinery, 2020. p. 149–156. https://dx.doi.org/10.1145/3386367.3431305.

92 STEBILA, D.; MOSCA, M. Post-quantum key exchange for the internet and the open quantum safe project. In: SPRINGER. **International Conference on Selected Areas in Cryptography**. [S.l.], 2016. p. 14–37. https://dx.doi.org/10.1007/978-3-319-69453-5_2.

93 PAQUIN, C.; STEBILA, D.; TAMVADA, G. Benchmarking post-quantum cryptography in tls. In: DING, J.; TILLICH, J.-P. (Ed.). **Post-Quantum Cryptography**. Cham: Springer International Publishing, 2020. p. 72–91. ISBN 978-3-030-44223-1. https://dx.doi.org/10.1007/978-3-030-44223-1_5.

94 SCHWABE, P.; STEBILA, D.; WIGGERS, T. Post-quantum tls without handshake signatures. In: **Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security**. New York, NY, USA: Association for Computing Machinery, 2020. p. 1461–1480. ISBN 9781450370899. https://dx.doi.org/10.1145/3372297.3423350.

95 SCHWABE, P.; STEBILA, D.; WIGGERS, T. More efficient post-quantum kemtls with pre-distributed public keys. In: BERTINO, E.; SHULMAN, H.; WAIDNER, M. (Ed.). **Computer Security – ESORICS 2021**. [S.l.]: Springer International Publishing, 2021. p. 3–22. ISBN 978-3-030-88418-5. https://dx.doi.org/10.1007/978-3-030-88418-5_1.

96 PETERSEN, K.; VAKKALANKA, S.; KUZNIARZ, L. Guidelines for conducting systematic mapping studies in software engineering: An update. **Information and Software Technology**, Elsevier, v. 64, p. 1–18, 8 2015. https://dx.doi.org/10.1016/j.infsof.2015.03.007.

97 ALKHULAIFI, A.; EL-ALFY, E.-S. M. Exploring lattice-based post-quantum signature for jwt authentication: Review and case study. In: **2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)**. [S.l.: s.n.], 2020. p. 1–5. https://dx.doi.org/10.1109/VTC2020-Spring48590.2020.9129505.

98 JONES, M.; HILDEBRAND, J. **JSON Web Encryption (JWE)**. [S.l.]: RFC Editor, 2015. (Request for Comments, 7516). https://dx.doi.org/10.17487/RFC7516.

99 JONES, M.; BRADLEY, J.; SAKIMURA, N. **JSON Web Signature (JWS)**. [S.l.]: RFC Editor, 2015. (Request for Comments, 7515). https://dx.doi.org/10.17487/RFC7515.

100 JONES, M. **JSON Web Algorithms (JWA)**. [S.l.]: RFC Editor, 2015. (Request for Comments, 7518). https://dx.doi.org/10.17487/RFC7518.

101 JONES, M.; MEDEIROS, B. D.; AGARWAL, N.; SAKIMURA, N.; BRADLEY, J. Openid connect rp-initiated logout 1.0. **The OpenID Foundation**, p. S3, 2022. Available at https://openid.net/specs/openid-connect-rpinitiated-1_0.html, accessed on 28 June 2024.

102 LAURIE, B.; LANGLEY, A.; KASPER, E.; MESSERI, E.; STRADLING, R. **Certificate Transparency Version 2.0**. [S.l.]: RFC Editor, 2021. (Request for Comments, 9162). https://dx.doi.org/10.17487/RFC9162.

103 BERNSTEIN, D. J.; DOBRAUNIG, C.; EICHLSEDER, M.; FLUHRER, S.; GAZDAG, S.-L.; HÜLSING, A.; KAMPANAKIS, P.; KÖLBL, S.; LANGE, T.; LAURIDSEN, M. M. et al. Sphincs+ submission to the nist post-quantum project. **Submission to NIST**, 2021. Available at http://sphincs.org/data/sphincs+-r3.1-specification.pdf, accessed on 28 June 2024.

104 SANTESSON, S.; MYERS, M.; ANKNEY, R.; MALPANI, A.; GALPERIN, S.; ADAMS, D. C. **X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP**. [S.l.]: RFC Editor, 2013. (Request for Comments, 6960). https://dx.doi.org/10.17487/RFC6960.

105 The Sovrin Foundation. **Sovrin**. 2016. Available at https://sovrin.org/, accessed on 13 February 2022.

106 uPort. **uPort**. 2020. Available at https://www.uport.me/, accessed on 13 February 2022.

107 ČUČKO, Š.; TURKANOVIĆ, M. Decentralized and self-sovereign identity: Systematic mapping study. **IEEE Access**, IEEE, v. 9, p. 139009–139027, 2021. https://dx.doi.org/10.1109/ACCESS.2021.3117588.

108 GHAFFARI, F.; GILANI, K.; BERTIN, E.; CRESPI, N. Identity and access management using distributed ledger technology: A survey. **International Journal of Network Management**, Wiley Online Library, p. e2180, 2021. https://dx.doi.org/10.1002/nem.2180.

109 MULAJI, S. S.; ROODT, S. S. The practicality of adopting blockchain-based distributed identity management in organisations: A meta-synthesis. **Security and Communication Networks**, Hindawi, v. 2021, 2021. https://dx.doi.org/10.1155/2021/9910078.

110 SCHMIDT, K.; MÜHLE, A.; GRÜNER, A.; MEINEL, C. Clear the fog: Towards a taxonomy of self-sovereign identity ecosystem members. In: IEEE. **2021 18th International Conference on Privacy, Security and Trust (PST)**. [S.l.], 2021. p. 1–7. https://dx.doi.org/10.1109/PST52912.2021.9647797.

111 SWAN, M. **Blockchain: Blueprint for a new economy**. Sebastopol, USA: "O'Reilly Media, Inc.", 2015. ISBN 978-1491920497.

112 ZHU, X.; BADR, Y. Fog computing security architecture for the internet of things using blockchain-based social networks. In: IEEE. **2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)**. Halifax, NS, Canada: IEEE, 2018. p. 1361–1366. https://dx.doi.org/10.1109/Cybermatics_2018.2018.00234.

113 ZHENG, Z.; XIE, S.; DAI, H.-N.; CHEN, W.; CHEN, X.; WENG, J.; IMRAN, M. An overview on smart contracts: Challenges, advances and platforms. **Future Generation Computer Systems**, Elsevier, v. 105, p. 475–491, 2020. ISSN 0167-739X. https://dx.doi.org/10.1016/j.future.2019.12.019.

114 FINFGELD-CONNETT, D. **A guide to qualitative meta-synthesis**. [S.l.]: Routledge New York, NY, USA:, 2018. ISBN 978-0815380627.

115 Elsevier. **Mendeley**. 2008. Available at https://www.mendeley.com/, accessed on 13 February 2022.

116 Association for Computing Machinery. **ACM Digital Library**. 2010. Available at https://dl.acm.org, accessed on 13 February 2022.

117 Institute of Electrical and Electronics Engineers. **IEEE Xplore**. 2000. Available at https://ieeexplore.ieee.org/, accessed on 13 February 2022.

118 Elsevier. **ScienceDirect**. 1997. Available at https://www.sciencedirect.com/, accessed on 13 February 2022.

119 Springer Nature. **Springer Link**. 2012. Available at https://link.springer.com/, accessed on 13 February 2022.

120 Elsevier. **Scopus Preview**. 2010. Available at https://www.scopus.com/, accessed on 13 February 2022.

121 Clarivate Analytics. **Web of Science**. 2006. Available at https://www.webofknowledge.com/, accessed on 13 February 2022.

122 Google. **Google Scholar**. 2004. Available at https://scholar.google.com/, accessed on 13 February 2022.

123 GOOGLE. **Google Patents**. 2006. Available at https://patents.google.com/, accessed on 13 February 2022.

124 WOHLIN, C. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: **Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering - EASE '14**. London, England: ACM Press, 2014. p. 1–10. https://dx.doi.org/10.1145/2601248.2601268.

125 SCHARDONG, F.; CUSTóDIO, R. **Study Selection Process, Spreadsheet**. 2021. Available at https://docs.google.com/spreadsheets/d/1FzUJRqe3WUhtsNYV6PyMZO8F14iQO-DXnBHR9xUsaiw, accessed on 23 April 2022.

126 LUX, Z. A.; BEIERLE, F.; ZICKAU, S.; GONDOR, S. Full-text Search for Verifiable Credential Metadata on Distributed Ledgers. In: **2019 6th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2019**. Granada, Spain: IEEE, 2019. p. 519–528. https://dx.doi.org/10.1109/IOTSMS48152.2019.8939249.

127 Apache Software Foundation. **Apache Solr**. 2010. Available at https://lucene.apache.org/solr/, accessed on 13 February 2022.

128 Hyperledger. **Hyperledger Indy**. 2020. Available at https://www.hyperledger.org/use/hyperledger-indy, accessed on 13 February 2022.

129 SCHARDONG, F.; CUSTÓDIO, R.; PIOLI, L.; MEYER, J. Matching metadata on blockchain for self-sovereign identity. In: SPRINGER. **International Conference on Business Process Management**. [S.l.], 2021. p. 421–433. https://dx.doi.org/10.1007/978-3-030-94343-1_32.

130 HONNIBAL, M.; MONTANI, I.; LANDEGHEM, S. V.; BOYD, A. **spaCy: Industrial-strength Natural Language Processing in Python**. [S.l.]: Zenodo, 2020. https://dx.doi.org/10.5281/zenodo.1212303.

131 MIKOLOV, T.; CHEN, K.; CORRADO, G.; DEAN, J. Efficient estimation of word representations in vector space. 2013. https://dx.doi.org/10.48550/arXiv.1301.3781.

132 GRÜNER, A.; MÜHLE, A.; MEINEL, C. An Integration Architecture to Enable Service Providers for Self-sovereign Identity. In: **2019 IEEE 18th International Symposium on Network Computing and Applications, NCA 2019**. Cambridge, USA: IEEE, 2019. p. 261–265. https://dx.doi.org/10.1109/NCA.2019.8935015.

133 HONG, S.; KIM, H. Vaultpoint: A blockchain-based ssi model that complies with oauth 2.0. **Electronics**, v. 9, n. 8, p. 1–20, 2020. ISSN 2079-9292. https://dx.doi.org/10.3390/electronics9081231.

134 Lux, Z. A.; Thatmann, D.; Zickau, S.; Beierle, F. Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials. In: **2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)**. Paris, France: IEEE, 2020. p. 71–78. https://dx.doi.org/10.1109/BRAINS49436.2020.9223292.

135 YILDIZ, H.; RITTER, C.; NGUYEN, L. T.; FRECH, B.; MARTINEZ, M. M.; KÜPPER, A. Connecting self-sovereign identity with federated and user-centric identities via saml integration. In: IEEE. **2021 IEEE Symposium on Computers and Communications (ISCC)**. [S.l.], 2021. p. 1–7. https://dx.doi.org/10.1109/ISCC53001.2021.9631453.

136 JURADO, V. M.; VILA, X.; KUBACH, M.; JEYAKUMAR, I. H. J.; SOLANA, A.; MARANGONI, M. Applying assurance levels when issuing and verifying credentials using trust frameworks. **Open Identity Summit 2021**, Gesellschaft für Informatik eV, 2021. Available at https://dl.gi.de/bitstreams/1db4a146-6d41-41c6-aba9-14a444bcdfef/download, accessed on 28 June 2024.

137 LAGUTIN, D.; KORTESNIEMI, Y.; FOTIOU, N.; SIRIS, V. A. Enabling decentralised identifiers and verifiable credentials for constrained iot devices using oauth-based delegation. In: **Proceedings of the Workshop on Decentralized IoT Systems and Security (DISS 2019), in Conjunction with the NDSS Symposium, San Diego, CA, USA**. [S.l.: s.n.], 2019. v. 24. https://dx.doi.org/10.14722/diss.2019.23005.

138 GRÜNER, A.; MÜHLE, A.; MEINEL, C. Atib: Design and evaluation of an architecture for brokered self-sovereign identity integration and trust-enhancing attribute aggregation for service provider. **IEEE Access**, IEEE, v. 9, p. 138553–138570, 2021. https://dx.doi.org/10.1109/ACCESS.2021.3116095.

139 SCHANZENBACH, M.; BRAMM, G.; SCHÜTTE, J. reclaimID: Secure, Self-Sovereign Identities Using Name Systems and Attribute-Based Encryption. In: **2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)**. New York, USA: IEEE, 2018. p. 946–957. https://dx.doi.org/10.1109/TrustCom/BigDataSE.2018.00134.

140 ZHONG, T.; SHI, P.; CHANG, J. Jointcloud cross-chain verification model of decentralized identifiers. In: IEEE. **2021 IEEE International Performance, Computing, and Communications Conference (IPCCC)**. [S.l.], 2021. p. 1–8. https://dx.doi.org/10.1109/IPCCC51483.2021.9679363.

141 XU, J.; XUE, K.; TIAN, H.; HONG, J.; WEI, D. S.; HONG, P. An Identity Management and Authentication Scheme Based on Redactable Blockchain for Mobile Networks. **IEEE Transactions on Vehicular Technology**, Institute of Electrical and Electronics Engineers Inc., v. 69, n. 6, p. 6688–6698, 6 2020. https://dx.doi.org/10.1109/TVT.2020.2986041.

142 KARTHIKEYAN, N. A. **Cryptographic Implementation of Issuer Policy for Self Sovereign Identity Systems**. Dissertação (Mestrado) — University of Twente, 2021. Available at http://essay.utwente.nl/88746/, accessed on 11 March 2022.

143 KANG, M.; LEMIEUX, V. A decentralized identity-based blockchain solution for privacy-preserving licensing of individual-controlled data to prevent unauthorized secondary data usage. **Ledger**, v. 6, 2021. https://dx.doi.org/10.5195/ledger.2021.239.

144 BATHEN, L.; FLORES, G. H.; MADL, G.; JADAV, D.; ARVANITIS, A.; SANTHANAM, K.; ZENG, C.; GORDON, A. SelfIs: Self-sovereign biometric IDs. In: **IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)**. Long Beach, USA: IEEE Computer Society, 2019. p. 2847–2856. https://dx.doi.org/10.1109/CVPRW.2019.00344.

145 MISHRA, P.; MODANWAL, V.; KAUR, H.; VARSHNEY, G. Pseudo-biometric identity framework: Achieving self-sovereignity for biometrics on blockchain. In: IEEE. **2021 IEEE International Conference on Systems, Man, and Cybernetics (SMC)**. [S.l.], 2021. p. 945–951. https://dx.doi.org/10.1109/SMC52423.2021.9659136.

146 ABRAHAM, A.; SCHINNERL, C.; MORE, S. Ssi strong authentication using a mobile-phone based identity wallet reaching a high level of assurance. In: **Proceedings of the 18th International Conference on Security and Cryptography - SECRYPT**. [S.l.: s.n.], 2021. https://dx.doi.org/10.5220/0010542801370148.

147 ABRAHAM, A.; HÖRANDNER, F.; OMOLOLA, O.; RAMACHER, S. Privacy-Preserving eID Derivation for Self-Sovereign Identity Systems. In: **Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)**. Copenhagen, Denmark: Springer International Publishing, 2020. v. 11999 LNCS, p. 307–323. ISBN 978-3-030-41579-2. https://dx.doi.org/10.1007/978-3-030-41579-2_18.

148 SCHANZENBACH, M. **Towards Self-sovereign, decentralized personal data sharing and identity management.** Tese (Doutorado) — Technical University of Munich, Germany, 2020. Available at https://mediatum.ub.tum.de/1545514, accessed on 13 February 2022.

149 LAUINGER, J.; ERNSTBERGER, J.; REGNATH, E.; HAMAD, M.; STEINHORST, S. A-poa: Anonymous proof of authorization for decentralized identity management. In: IEEE. **2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)**. Sydney, Australia: IEEE, 2021. p. 1–9. https://dx.doi.org/10.1109/ICBC51069.2021.9461082.

150 MUKTA, R.; PAIK, H.-y.; LU, Q.; KANHERE, S. S. Credential-based trust management in self sovereign identity. **womENcourage**, ACM, 2021. Available at https://womencourage.acm.org/2021/wp-content/uploads/2021/07/87_extendedabstract.pdf, accessed on 19 April 2022.

151 STOKKINK, Q.; POUWELSE, J. Deployment of a Blockchain-Based Self-Sovereign Identity. In: **2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and**

Social Computing (CPSCom) and IEEE Smart Data (SmartData). Halifax, NS, Canada: IEEE, 2018. p. 1336–1342. https://dx.doi.org/10.1109/Cybermatics_2018.2018.00230.

152 LAX, G.; RUSSO, A. A lightweight scheme exploiting social networks for data minimization according to the gdpr. **IEEE Transactions on Computational Social Systems**, IEEE, v. 8, n. 2, p. 388–397, 2021. https://dx.doi.org/10.1109/TCSS.2020.3049009.

153 ABRAHAM, A.; MORE, S.; RABENSTEINER, C.; HÖRANDNER, F. Revocable and offline-verifiable self-sovereign identities. In: IEEE. **2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)**. Guangzhou, China: IEEE Computer Society, 2020. p. 1020–1027. https://dx.doi.org/10.1109/TrustCom50675.2020.00136.

154 CHO, K. W.; JEONG, B.-G.; SHIN, S. U. Verifiable credential proof generation and verification model for decentralized ssi-based credit scoring data. **IEICE Transactions on Information and Systems**, The Institute of Electronics, Information and Communication Engineers, v. 104, n. 11, p. 1857–1868, 2021. https://dx.doi.org/10.1587/transinf.2021NGP0006.

155 CHOTKAN, R. **Industry-Grade Self-Sovereign Identity: On the Realisation of a Fully Distributed Self-Sovereign Identity Architecture**. Dissertação (Mestrado) — Delft University of Technology, 2021. Available at http://resolver.tudelft.nl/uuid:32711378-2f6f-452e-b65c-1866c471e934, accessed on 12 March 2022.

156 YANG, X.; LI, W. A zero-knowledge-proof-based digital identity management scheme in blockchain. **Computers & Security**, Elsevier, v. 99, p. 102050, 2020. https://dx.doi.org/10.1016/j.cose.2020.102050.

157 BOBOLZ, J.; EIDENS, F.; KRENN, S.; RAMACHER, S.; SAMELIN, K. Issuer-hiding attribute-based credentials. In: SPRINGER. **International Conference on Cryptology and Network Security**. [S.l.], 2021. p. 158–178. https://dx.doi.org/10.1007/978-3-030-92548-2_9.

158 JAROUCHEH, Z.; ÁLVAREZ, I. A. Secretation: Toward a decentralised identity and verifiable credentials based scalable and decentralised secret management solution. In: IEEE. **2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)**. Sydney, Australia: IEEE, 2021. p. 1–9. https://dx.doi.org/10.1109/ICBC51069.2021.9461144.

159 SAMIR, E.; WU, H.; AZAB, M.; XIN, C. S.; ZHANG, Q. Dt-ssim: A decentralized trustworthy self-sovereign identity management framework. **IEEE Internet of Things Journal**, IEEE, 2021. https://dx.doi.org/10.1109/JIOT.2021.3112537.

160 SIDDIQUI, H.; IDREES, M.; GUDYMENKO, I.; FETZER, C. et al. Credentials as a service providing self sovereign identity as a cloud service using trusted execution environments. In: IEEE. **2021 IEEE International Conference on Cloud Engineering (IC2E)**. [S.l.], 2021. p. 210–216. https://dx.doi.org/10.1109/IC2E52221.2021.00036.

161 GRUNER, A.; MUHLE, A.; MEINEL, C. Using Probabilistic Attribute Aggregation for Increasing Trust in Attribute Assurance. In: **2019 IEEE Symposium Series on Computational Intelligence (SSCI)**. Xiamen, China: IEEE, 2019. p. 633–640. https://dx.doi.org/10.1109/SSCI44817.2019.9003094.

162 BHATTACHARYA, M. P.; ZAVARSKY, P.; BUTAKOV, S. Enhancing the security and privacy of self-sovereign identities on hyperledger indy blockchain.

In: IEEE. **2020 International Symposium on Networks, Computers and Communications (ISNCC)**. Montreal, Canada: IEEE Computer Society, 2020. p. 1–7. https://dx.doi.org/10.1109/ISNCC49221.2020.9297357.

163 ABRAMSON, W.; HICKMAN, N.; SPENCER, N. Evaluating trust assurance in indy-based identity networks using public ledger data. **Frontiers in Blockchain**, v. 4, p. 18, 2021. ISSN 2624-7852. https://dx.doi.org/10.3389/fbloc.2021.622090.

164 GRÜNER, A.; MÜHLE, A.; GAYVORONSKAYA, T.; MEINEL, C. A Quantifiable Trust Model for Blockchain-Based Identity Management. In: **2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)**. Halifax, NS, Canada: IEEE, 2018. p. 1475–1482. https://dx.doi.org/10.1109/Cybermatics_2018.2018.00250.

165 Barclay, I.; Freytsis, M.; Bucher, S.; Radha, S.; Preece, A.; Taylor, I. Towards a modelling framework for self-sovereign identity systems. p. 1–5, 9 2020. https://dx.doi.org/10.48550/arXiv.2009.04327.

166 LIU, J.; HODGES, A.; CLAY, L.; MONARCH, J. An analysis of digital identity management systems - a two-mapping view. In: **2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS)**. Paris, France: IEEE, 2020. p. 92–96. https://dx.doi.org/10.1109/BRAINS49436.2020.9223281.

167 FERDOUS, M. S.; CHOWDHURY, F.; ALASSAFI, M. O. In Search of Self-Sovereign Identity Leveraging Blockchain Technology. **IEEE Access**, IEEE, v. 7, p. 103059–103079, 2019. https://dx.doi.org/10.1109/ACCESS.2019.2931173.

168 GWON, O. G. patenteu, **Content wallet device and self-sovereign identity and copyright authentication system using same**. 2021. Available at https://patents.google.com/patent/WO2021125586A1/en, accessed on 13 February 2022.

169 LIU, Y.; LU, Q.; PAIK, H.-Y.; XU, X.; CHEN, S.; ZHU, L. Design pattern as a service for blockchain-based self-sovereign identity. **IEEE Software**, IEEE, v. 37, n. 5, p. 30–36, 9 2020. https://dx.doi.org/10.1109/MS.2020.2992783.

170 LIM, S.; RHIE, M.-H.; HWANG, D.; KIM, K.-H. A subject-centric credential management method based on the verifiable credentials. In: IEEE. **2021 International Conference on Information Networking (ICOIN)**. Bangkok, Thailand: IEEE, 2021. p. 508–510. https://dx.doi.org/10.1109/ICOIN50884.2021.9333857.

171 LEMIEUX, V.; VOSKOBOJNIKOV, A.; KANG, M. Addressing audit and accountability issues in self-sovereign identity blockchain systems using archival science principles. In: IEEE. **2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)**. [S.l.], 2021. p. 1210–1216. https://dx.doi.org/10.1109/COMPSAC51774.2021.00167.

172 JAKUBEIT, P.; DERCKSEN, A.; PETER, A. Ssi-aware: Self-sovereign identity authenticated backup with auditing by remote entities. In: LAURENT, M.; GIANNETSOS, T. (Ed.). **Information Security Theory and Practice**. Cham: Springer International Publishing, 2020. p. 202–219. ISBN 978-3-030-41702-4. https://dx.doi.org/10.1007/978-3-030-41702-4_13.

173 SOLTANI, R.; NGUYEN, U. T.; AN, A. Practical Key Recovery Model for Self-Sovereign Identity Based Digital Wallets. In: **Proceedings - IEEE 17th International Conference on Dependable, Autonomic and Secure Computing, IEEE 17th International Conference on Pervasive Intelligence and Computing, IEEE 5th International Conference on Cloud and Big Data Computing, 4th Cyber Scienc**. Fukuoka, Japan: IEEE, 2019. p. 320–325. https://dx.doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00066.

174 KOSTADINOV, K.; VOS, M. de; POUWELSE, J. **Towards Data Resilience for Fully Distributed Self-Sovereign Identity Managers**. Dissertação (Bachelor's Thesis) — Delft University of Technology, 2021. Available at http://resolver.tudelft.nl/uuid:3ce2e3b3-8fd6-4831-a3ed-5f4dac492f7e, accessed on 12 March 2022.

175 KIM, W.-B.; LEE, I.-Y.; YIM, K.-B. Group delegated id-based proxy re-encryption for phr. In: BAROLLI, L.; PONISZEWSKA-MARANDA, A.; PARK, H. (Ed.). **Innovative Mobile and Internet Services in Ubiquitous Computing**. Cham: Springer International Publishing, 2021. p. 447–456. ISBN 978-3-030-50399-4. https://dx.doi.org/10.1007/978-3-030-50399-4_43.

176 SINGH, H. P.; STEFANIDIS, K.; KIRSTEIN, F. A private key recovery scheme using partial knowledge. In: IEEE. **2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)**. Paris, France: IEEE, 2021. p. 1–5. https://dx.doi.org/10.1109/NTMS49979.2021.9432642.

177 LOCKWOOD, M. An accessible interface layer for self-sovereign identity. **Frontiers in Blockchain**, Frontiers, v. 3, p. 63, 2021. https://dx.doi.org/10.3389/fbloc.2020.609101.

178 MUSTAFA, K.; SAKIR, S. patenteu, **Computer-implemented transaction system and method**. 2021. Available at https://patents.google.com/patent/WO2021064182A1/en.

179 TOTH, K. C.; CAVOUKIAN, A.; ANDERSON-PRIDDY, A. Privacy by design identity architecture using agents and digital identities. In: SPRINGER. **Annual Privacy Forum**. Lisbon, Portugal: Springer, 2020. p. 73–94. https://dx.doi.org/10.1007/978-3-030-55196-4_5.

180 SHANMUGARASA, Y.; PAIK, H.-Y.; KANHERE, S. S.; ZHU, L. Towards automated data sharing in personal data stores. In: IEEE. **2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)**. Pisa, Italy: IEEE, 2021. p. 328–331. https://dx.doi.org/10.1109/PerComWorkshops51409.2021.9431001.

181 WOHLGEMUTH, S.; UMEZAWA, K.; MISHINA, Y.; TAKARAGI, K. A Secure Decision-Support Scheme for Self-Sovereign Identity Management. In: **Symposium on Cryptography and Information Security (SCIS)**. Kochi, Japan: IEICE, 2020. p. 1–8. Available at https://www.researchgate.net/publication/338710779_A_Secure_Decision-Support_Scheme_for_Self-Sovereign_Identity_Management, accessed on 28 June 2024.

182 INOUE, K.; SUZUKI, D.; KURITA, T.; IMAI, S. Cooperative task scheduling for personal identity verification in networked systems. In: IEEE. **2020 32nd International Teletraffic Congress (ITC 32)**. Osaka, Japan: IEEE, 2020. p. 97–105. https://dx.doi.org/10.1109/ITC3249928.2020.00020.

183 KUBACH, M.; ROßNAGEL, H. A lightweight trust management infrastructure for self-sovereign identity. In: ROßNAGEL, H.; SCHUNCK, C. H.; MöDERSHEIM, S. (Ed.). **Open Identity Summit 2021**. Lyngby, Denmark: Gesellschaft für Informatik e.V., 2021. p.

155–166. Available at https://dl.gi.de/handle/20.500.12116/36489, accessed on 13 February 2022.

184 ALBER, L.; MORE, S.; MöDERSHEIM, S.; SCHLICHTKRULL, A. Adapting the tpl trust policy language for a self-sovereign identity world. In: ROßNAGEL, H.; SCHUNCK, C. H.; MöDERSHEIM, S. (Ed.). **Open Identity Summit 2021**. Lyngby, Denmark: Gesellschaft für Informatik e.V., 2021. p. 107–118. Available at https://dl.gi.de/handle/20.500.12116/36506, accessed on 13 February 2022.

185 HARDMAN, D. **DIDComm Messaging**. 2020. Available at https://identity.foundation/didcomm-messaging/spec/, accessed on 12 March 2022.

186 WEST, R.; BLUHM, D.; HAILSTONE, M.; CURRAN, S.; CURREN, S.; ARISTY, G. **Aries RFC 0023: DID Exchange Protocol 1.0**. [S.l.], 2019. Available at https://github.com/hyperledger/aries-rfcs/blob/master/features/0023-did-exchange/README.md, accessed on 13 February 2022.

187 SMITH, S. M. Key event receipt infrastructure (KERI). **CoRR**, abs/1907.02143, p. 140, 2019. https://dx.doi.org/10.48550/arXiv.1907.02143.

188 FEDRECHESKI, G.; COSTA, L. C.; AFZAL, S.; RABAEY, J. M.; LOPES, R. D.; ZUFFO, M. K. A low-overhead approach for self-sovereign identity in iot. 2021. https://dx.doi.org/10.48550/arXiv.2107.10232.

189 PARK, C.-S.; NAM, H.-M. A new approach to constructing decentralized identifier for secure and flexible key rotation. **IEEE Internet of Things Journal**, IEEE, 2021. https://dx.doi.org/10.1109/JIOT.2021.3121722.

190 KIM, K.-H.; LIM, S.; HWANG, D.-Y.; KIM, K.-H. Analysis on the privacy of did service properties in the did document. In: IEEE. **2021 International Conference on Information Networking (ICOIN)**. Bangkok, Thailand: IEEE, 2021. p. 745–748. https://dx.doi.org/10.1109/ICOIN50884.2021.9333997.

191 NAIK, N.; GRACE, P.; JENKINS, P. An attack tree based risk analysis method for investigating attacks and facilitating their mitigations in self-sovereign identity. In: IEEE. **2021 IEEE Symposium Series on Computational Intelligence (SSCI)**. [S.l.], 2021. p. 1–8. https://dx.doi.org/10.1109/SSCI50451.2021.9659929.

192 FEI, C.; LOHKAMP, J.; RUSU, E.; SZAWAN, K.; WAGNER, K.; WITTENBERG, N. **Self-Sovereign and Decentralised Identity By Design**. [S.l.], 2018. Available at https://github.com/jolocom/jolocom-lib/wiki/Jolocom-Whitepaper, accessed on 13 February 2022.

193 BOEYEN, S.; SANTESSON, S.; POLK, T.; HOUSLEY, R.; FARRELL, S.; COOPER, D. **Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**. [S.l.]: RFC Editor, 2008. (Request for Comments, 5280). https://dx.doi.org/10.17487/RFC5280.

194 ALLIANCE, F. **Client to authenticator protocol (ctap)**. [S.l.], 2019. Available at https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-client-to-authenticator-protocol-v2.0-id-20180227.html/, accessed on 22 March 2022.

195 PATEL, V. M.; RATHA, N. K.; CHELLAPPA, R. Cancelable biometrics: A review. **IEEE Signal Processing Magazine**, IEEE, v. 32, n. 5, p. 54–65, 2015. https://dx.doi.org/10.1109/MSP.2015.2434151.

196 HERMANS, J.; MENNINK, B.; PEETERS, R. When a bloom filter is a doom filter: security assessment of a novel iris biometric template protection system. In: IEEE. **2014 international conference of the biometrics special interest group (BIOSIG)**. [S.l.], 2014. p. 1–6.

197 BRADSKI, G.; KAEHLER, A. **Learning OpenCV: Computer vision with the OpenCV library**. [S.l.]: " O'Reilly Media, Inc.", 2008.

198 KAUR, H.; KHANNA, P. Random distance method for generating unimodal and multimodal cancelable biometric features. **IEEE Transactions on Information Forensics and Security**, IEEE, v. 14, n. 3, p. 709–719, 2018. https://dx.doi.org/10.1109/TIFS.2018.2855669.

199 SHAMIR, A. How to share a secret. **Communications of the ACM**, ACm New York, NY, USA, v. 22, n. 11, p. 612–613, 1979. https://dx.doi.org/10.1145/359168.359176.

200 SABT, M.; ACHEMLAL, M.; BOUABDALLAH, A. Trusted execution environment: what it is, and what it is not. In: IEEE. **2015 IEEE Trustcom/BigDataSE/ISPA**. [S.l.], 2015. v. 1, p. 57–64. https://dx.doi.org/10.1109/Trustcom.2015.357.

201 U.S. Federal Government. **Internet Assigned Numbers Authority (IANA)**. 1998. Available at https://www.iana.org/, accessed on 11 April 2022.

202 SPORNY, M.; ZAGIDULIN, D.; LONGLEY, D. **The did:key Method**. 2019. Available at https://w3c-ccg.github.io/did-method-key/, accessed on 13 February 2022.

203 JOSEFSSON, S.; LIUSVAARA, I. **Edwards-Curve Digital Signature Algorithm (EdDSA)**. [S.l.]: RFC Editor, 2017. (Request for Comments, 8032). https://dx.doi.org/10.17487/RFC8032.

204 BENET, J.; SPORNY, M. Internet-Draft, **The Multibase Data Format**. [S.l.]: Internet Engineering Task Force, 2021. Available at https://datatracker.ietf.org/doc/html/draft-multiformats-multibase-03, accessed on 28 June 2024.

205 WEST, R.; BLUHM, D.; HAILSTONE, M.; CURRAN, S.; CURREN, S.; ARISTY, G. **Aries RFC 0434: Out-of-Band Protocol 1.1**. 2019. Available at https://github.com/hyperledger/aries-rfcs/blob/main/features/0434-outofband/README.md, accessed on 13 February 2022.

206 BORMANN, C.; HOFFMAN, P. E. **Concise Binary Object Representation (CBOR)**. [S.l.]: RFC Editor, 2013. (Request for Comments, 7049). https://dx.doi.org/10.17487/RFC7049.

207 LAMPORT, L. Password authentication with insecure communication. **Communications of the ACM**, ACM New York, NY, USA, v. 24, n. 11, p. 770–772, 1981. https://dx.doi.org/10.1145/358790.358797.

208 MOCKAPETRIS, P. **Domain names: Concepts and facilities**. [S.l.]: RFC Editor, 1983. (Request for Comments, 882). https://dx.doi.org/10.17487/RFC0882.

209 WACHS, M.; SCHANZENBACH, M.; GROTHOFF, C. On the feasibility of a censorship resistant decentralized name system. In: SPRINGER. **International Symposium on Foundations and Practice of Security**. La Rochelle, France: Springer, 2013. p. 19–30. https://dx.doi.org/10.1007/978-3-319-05302-8_2.

210 BLAZE, M.; BLEUMER, G.; STRAUSS, M. Divertible protocols and atomic proxy cryptography. In: SPRINGER. **International Conference on the Theory and Applications of Cryptographic Techniques**. Espoo, Finland: Springer, 1998. p. 127–144. https://dx.doi.org/10.1007/BFb0054122.

211 KRAWCZYK, H.; RABIN, T. **Chameleon Hashing and Signatures**. 1998. Available at https://ia.cr/1998/010, accessed on 13 February 2022.

212 ATENIESE, G.; MAGRI, B.; VENTURI, D.; ANDRADE, E. Redactable blockchain - or - rewriting history in bitcoin and friends. In: IEEE. **2017 IEEE European Symposium on Security and Privacy (EuroS&P)**. Paris, France: IEEE Computer Society, 2017. p. 111–126. https://dx.doi.org/10.1109/EuroSP.2017.37.

213 DERLER, D.; SAMELIN, K.; SLAMANIG, D.; STRIECKS, C. **Fine-Grained and Controlled Rewriting in Blockchains: Chameleon-Hashing Gone Attribute-Based**. 2019. Available at https://eprint.iacr.org/2019/406, accessed on 13 February 2022.

214 BETHENCOURT, J.; SAHAI, A.; WATERS, B. Ciphertext-policy attribute-based encryption. In: IEEE. **2007 IEEE symposium on security and privacy (SP'07)**. [S.l.], 2007. p. 321–334. https://dx.doi.org/10.1109/SP.2007.11.

215 WATERS, B. Efficient identity-based encryption without random oracles. In: SPRINGER. **Annual International Conference on the Theory and Applications of Cryptographic Techniques**. Aarhus, Denmark: Springer, 2005. p. 114–127. https://dx.doi.org/10.1007/11426639_7.

216 BONEH, D.; LYNN, B.; SHACHAM, H. Short signatures from the weil pairing. In: SPRINGER. **International conference on the theory and application of cryptology and information security**. Gold Coast, Australia: Springer, 2001. p. 514–532. https://dx.doi.org/10.1007/3-540-45682-1_30.

217 BITANSKY, N.; CANETTI, R.; CHIESA, A.; TROMER, E. From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. In: **Proceedings of the 3rd Innovations in Theoretical Computer Science Conference**. New York, USA: Association for Computing Machinery, 2012. p. 326–349. https://dx.doi.org/10.1145/2090236.2090263.

218 GENTRY, C. Fully homomorphic encryption using ideal lattices. In: **Proceedings of the forty-first annual ACM symposium on Theory of computing**. [S.l.: s.n.], 2009. p. 169–178. https://dx.doi.org/10.1145/1536414.1536440.

219 MARTIN, R. C.; RIEHLE, D.; BUSCHMANN, F. **Pattern languages of program design 3**. Boston, USA: Addison-Wesley Longman Publishing Co., Inc., 1997. 529-574 p.

220 DALPIAZ, F.; FRANCH, X.; HORKOFF, J. istar 2.0 language guide. p. 1–15, 2016. https://dx.doi.org/10.48550/arXiv.1605.07767.

221 MORTIER, R.; HADDADI, H.; HENDERSON, T.; MCAULEY, D.; CROWCROFT, J. Human-data interaction: The human face of the data-driven society. 2015. https://dx.doi.org/10.48550/arXiv.1412.6159.

222 SCHNEIER, B. Attack trees. **Dr. Dobb's journal**, v. 24, n. 12, p. 21–29, 1999. Available at https://tnlandforms.us/cs594-cns96/attacktrees.pdf, accessed on 28 June 2024.

223 CA/Browser Forum. **Certification Authority Browser Forum**. 2005. Available at https://cabforum.org/, accessed on 11 April 2022.

224 MÖDERSHEIM, S.; SCHLICHTKRULL, A.; WAGNER, G.; MORE, S.; ALBER, L. Tpl: A trust policy language. In: MENG, W.; COFTA, P.; JENSEN, C. D.; GRANDISON, T. (Ed.). **Trust Management XIII**. Cham: Springer International Publishing, 2019. p. 209–223. ISBN 978-3-030-33716-2. https://dx.doi.org/10.1007/978-3-030-33716-2_16.

225 MENEZES, A. J.; OORSCHOT, P. C. V.; VANSTONE, S. A. **Handbook of applied cryptography**. [S.l.]: CRC press, 2018.

226 BARKER, E. et al. Guideline for using cryptographic standards in the federal government: Cryptographic mechanisms. **NIST special publication**, p. 800–175B, 2016. https://dx.doi.org/10.6028/NIST.SP.800-175Br1.

227 SCHRIJVER, A. **Theory of linear and integer programming**. [S.l.]: John Wiley & Sons, 1998.

228 GOLDREICH, O. Secure multi-party computation. **Manuscript. Preliminary version**, Citeseer, v. 78, p. 110, 1998.

229 W3C Technology and society domain. **Verifiable Claims Working Group Frequently Asked Questions**. 2017. Available at https://w3c.github.io/webpayments-ig/VCTF/charter/faq.html#self-sovereign, accessed on 25 September 2022.

230 ANDRIEU, J. A Technology-Free Definition of Self-Sovereign Identity. In: **Rebooting the Web of Trust III**. San Francisco, USA: Web of Trust, 2016. p. 2–5. Available at https://github.com/WebOfTrustInfo/rwot3-sf/blob/master/topics-and-advance-readings/a-technology-free-definition-of-self-sovereign-identity.pdf, accessed on 13 February 2022.

231 NAIK, N.; JENKINS, P. Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology. In: **2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)**. Oxford, United Kingdom: IEEE, 2020. p. 90–95. https://dx.doi.org/10.1109/MobileCloud48802.2020.00021.

232 ELLINGSEN, J. **Self-Sovereign Identity Systems Opportunities and challenges**. Dissertação (Mestrado) — Norwegian University of Science and Technology, 2019. Available at https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2617756, accessed on 13 February 2022.

233 Van Wingerde, M. **Blockchain-enabled Self-sovereign Identity**. Dissertação (Mestrado) — Tilburg University, 2017. https://dx.doi.org/10.13140/RG.2.2.17693.82406.

234 ABRAHAM, A. **Self-sovereign identity: Whitepaper about the Concept of Self-Sovereign Identity including its Potential**. [S.l.], 2017. Available at https://technology.a-sit.at/en/whitepaper-self-sovereign-identity/, accessed on 13 February 2022.

235 SATYBALDY, A.; NOWOSTAWSKI, M.; ELLINGSEN, J. Self-sovereign identity systems. In: **Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers**. Cham: Springer International Publishing, 2020. p. 447–461. ISBN 978-3-030-42504-3. https://dx.doi.org/10.1007/978-3-030-42504-3_28.

236 DIEBOLD, Z.; O'MAHONY, D. **Self-Sovereign Identity using Smart Contracts on the Ethereum Blockchain**. Dissertação (Mestrado) — University of Dublin, 2017. Available at https://www.scss.tcd.ie/publications/theses/diss/2017/TCD-SCSS-DISSERTATION-2017-016.pdf, accessed on 13 February 2022.

237 SPEELMAN, T. **Self-Sovereign Identity: Proving Power over Legal Entities**. Dissertação (Mestrado) — Delft University of Technology, 2020. Available at https://repository.tudelft.nl/islandora/object/uuid:aab1f3ff-da54-47f7-8998-847cb78322c8, accessed on 13 February 2022.

238 ČUČKO, Š.; BEĆIROVIĆ, Š.; KAMIŠALIĆ, A.; MRDOVIĆ, S.; TURKANOVIĆ, M. Towards the classification of self-sovereign identity properties. 2021. https://dx.doi.org/10.48550/arXiv.2112.04155.

239 SOVRIN. **The Principles of SSI**. 2021. Available at https://sovrin.org/principles-of-ssi/, accessed on 12 March 2022.

240 SCHUTTE, M. **Schutte's Critique of the Self-Sovereign Identity Principles**. 2016. Available at http://matthewschutte.com/2016/10/25/schuttes-critique-of-the-self-sovereign-identity-principles/, accessed on 13 February 2022.

241 Evernym. **Evernym**. 2013. Available at https://www.evernym.com/, accessed on 13 February 2022.

242 TOBIN, A.; REED, D. **The Inevitable Rise of Self-Sovereign Identity**. [S.l.], 2016. Available at https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf, accessed on 13 February 2022.

243 The Sovrin Foundation. **Write To The Sovrin Public Ledger**. 2016. Available at https://sovrin.org/issue-credentials/, accessed on 13 February 2022.

244 CAMERON, K. **The Laws of Identity**. [S.l.], 2005. Available at https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf, accessed on 13 February 2022.

245 SAVIĆ, M.; IVANOVIĆ, M.; JAIN, L. C. Co-authorship networks: An introduction. In: **Complex Networks in Software, Knowledge, and Social Systems**. Cham: Springer International Publishing, 2019. p. 179–192. ISBN 978-3-319-91196-0. https://dx.doi.org/10.1007/978-3-319-91196-0_5.

246 SPORNY, M.; LONGLEY, D.; CHADWICK, D. **Verifiable Credentials Data Model 1.0 - Trust Model**. 2019. Available at https://www.w3.org/TR/vc-data-model/#trust-model, accessed on 13 February 2022.

247 MEIER, S.; SCHMIDT, B.; CREMERS, C.; BASIN, D. The tamarin prover for the symbolic analysis of security protocols. In: SPRINGER. **International Conference on**

Computer Aided Verification. Saint Petersburg, Russia: Springer, 2013. p. 696–701. https://dx.doi.org/10.1007/978-3-642-39799-8_48.

248 PETTICREW, M.; ROBERTS, H. **Systematic reviews in the social sciences: A practical guide**. [S.l.]: John Wiley & Sons, 2008.

249 LUX, Z. A.; BEIERLE, F.; ZICKAU, S.; GÖNDÖR, S. Full-text search for verifiable credential metadata on distributed ledgers. In: IEEE. **2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)**. [S.l.], 2019. p. 519–528. https://dx.doi.org/10.1109/IOTSMS48152.2019.8939249.

250 WHITEHEAD, A. **Sovrin Main Net**. 2019. Available at: https://rocksdb.org/, accessed on 21 March 2021.

251 STAš, P. **Hyperledger Indy Transaction Explorer**. 2019. Available at: https://indyscan.io/, accessed on 24 June 2024.

252 TOBIN, A. **WriteSovrin: What goes on the ledger?** 2018. Available at: https://sovrin.org/wp-content/uploads/2017/04/What-Goes-On-The-Ledger.pdf, accessed on 24 June 2024.

253 OMRAN, F. N. A. A.; TREUDE, C. Choosing an nlp library for analyzing software documentation: a systematic literature review and a series of experiments. In: IEEE. **2017 IEEE/ACM 14th International Conference on Mining Software Repositories (MSR)**. [S.l.], 2017. p. 187–197. https://dx.doi.org/10.1109/MSR.2017.42.

254 Facebook Database Engineering Team. **RocksDB**. 2013. Available at: https://rocksdb.org/, accessed on 24 June 2024.

255 KERN, H. **Model interoperability between meta-modeling environments by using M3-level-based bridges**. Tese (Doutorado) — Universität Leipzig, 2016.

256 ADAMS, C.; LLOYD, S. **Understanding public-key infrastructure: concepts, standards, and deployment considerations**. [S.l.]: Sams Publishing, 1999.

257 BARNES, R.; HOFFMAN-ANDREWS, J.; MCCARNEY, D.; KASTEN, J. **Automatic Certificate Management Environment (ACME)**. [S.l.]: RFC Editor, 2019. (Request for Comments, 8555). https://dx.doi.org/10.17487/RFC8555.

258 KAUSE, T.; PEYLO, M. **Internet X.509 Public Key Infrastructure – HTTP Transfer for the Certificate Management Protocol (CMP)**. [S.l.]: RFC Editor, 2012. (Request for Comments, 6712). https://dx.doi.org/10.17487/RFC6712.

259 MYERS, M.; SCHAAD, J. **Certificate Management over CMS (CMC)**. [S.l.]: RFC Editor, 2008. (Request for Comments, 5272). https://dx.doi.org/10.17487/RFC5272.

260 POLK, T.; LEE, J.; PARK, S.; PARK, J.; LEE, H.; LEE, H. **Internet X.509 Public Key Infrastructure Subject Identification Method (SIM)**. [S.l.]: RFC Editor, 2006. (Request for Comments, 4683). https://dx.doi.org/10.17487/RFC4683.

261 SIPSER, M. **Introduction to the Theory of Computation**. 3. ed. [S.l.]: Cengage Learning, 2013.

262 TERBU, O.; LODDERSTEDT, T.; YASUDA, K.; LOOKER, T. **OpenID for Verifiable Presentations - draft 20**. 2024. Available at https://openid.net/specs/openid-4-verifiable-presentations-1_0.html, accessed on 12 March 2024.

263 FERDOUS, M. S.; POET, R. Formalising identity management protocols. In: IEEE. **2016 14th Annual Conference on Privacy, Security and Trust (PST)**. [S.l.], 2016. p. 137–146. https://dx.doi.org/10.1109/PST.2016.7906948.

264 SCHARDONG, F.; CUSTÓDIO, R. From self-sovereign identity to fiduciary identity: A journey towards greater user privacy and usability. In: ACM. **Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing**. [S.l.], 2024. p. 687–694. https://dx.doi.org/10.1145/3605098.3636061.

265 SHEPHERDSON, J. C.; STURGIS, H. E. Computability of recursive functions. **J. ACM**, Association for Computing Machinery, New York, NY, USA, v. 10, n. 2, p. 217–255, abr. 1963. ISSN 0004-5411. https://dx.doi.org/10.1145/321160.321170.

266 ÁLVES, D. P. **Equivalência de Máquinas Universais: Demonstração, Análise e Simulação**. 2007. Available at https://web.archive.org/web/20220414134543/http://debora.wait4.org/tc.pdf, accessed on 07/23/2023.

267 ARORA, C. Digital health fiduciaries: protecting user privacy when sharing health data. **Ethics and Information Technology**, Springer, v. 21, n. 3, p. 181–196, 2019. https://dx.doi.org/10.1007/s10676-019-09499-x.

268 ROTMAN, L. I. Fiduciary law's holy grail: Reconciling theory and practice in fiduciary jurisprudence. **Boston University Law Review**, v. 91, p. 921, 2011. Available at https://www.bu.edu/law/journals-archive/bulr/documents/rotman.pdf, accessed on 26 June 2024.

269 BALKIN, J. M. Information fiduciaries and the first amendment. **U.C. Davis Law Review**, v. 49, p. 1183, 2015. https://dx.doi.org/20.500.13051/4692.

270 DEMOTT, D. A. Beyond metaphor: An analysis of fiduciary obligation. **Duke Law Journal**, p. 879, 1988. Available at https://scholarship.law.duke.edu/faculty_scholarship/332, accessed on 26 June 2024.

271 KHAWAJA, M. A.; CHEN, F.; MARCUS, N. Measuring cognitive load using linguistic features: implications for usability evaluation and adaptive interaction design. **International Journal of Human-Computer Interaction**, Taylor & Francis, v. 30, n. 5, p. 343–368, 2014. https://dx.doi.org/10.1080/10447318.2013.860579.

272 HARDJONO, T.; PENTLAND, A. Data cooperatives: Towards a foundation for decentralized personal data management. 2019. https://dx.doi.org/10.48550/arXiv.1905.08819.

273 VALE, C. A.; SCHARDONG, F.; BARROS, M.; CUSTÓDIO, R. Touchless authentication for health professionals: Analyzing the risks and proposing alternatives to dirty interfaces. In: IEEE. **2022 IEEE 35th International Symposium on Computer-Based Medical Systems (CBMS)**. [S.l.], 2022. p. 459–464. https://dx.doi.org/10.1109/CBMS55023.2022.00088.

274 MAYR, L.; SCHARDONG, F.; CUSTÓDIO, R. **Processos de verificação e assinatura digital de documentos eletrônicos baseado em identidade**

eletrônica, certificado digital de uso único e blockchain. 2022. Available at https://patents.google.com/patent/BR102022012874/en, accessed on 28 June 2024.

275 PEROTTONI, E. D.; COSTA, B. P.; MÜLLER, F. L.; CAMARGO, V. dos S.; SCHARDONG, F.; SILVANO, W.; MAYR, L.; CUSTÓDIO, R. F.; ROCHA, L.; LYRA, C. et al. Menos certificação digital e mais identidade eletrônica: Icpedu e cafe em um assinador digital inclusivo. In: SBC. **Extended Proceedings of XXIII Brazilian Symposium on Information and Computational Systems Security**. [S.l.], 2023. p. 93–96. https://dx.doi.org/10.5753/sbseg_estendido.2023.235947.

276 SILVA, B. V. R.; SCHARDONG, F.; JUNIOR, L. C. V.; CUSTÓDIO, R. F. Identificaçao eletrônica do registro civil do brasil. In: SBC. **Extended Proceedings of XXIII Brazilian Symposium on Information and Computational Systems Security**. [S.l.], 2023. p. 89–92. https://dx.doi.org/10.5753/sbseg_estendido.2023.235911.

277 GIRON, A. A.; SCHARDONG, F.; PERIN, L. P.; CUSTÓDIO, R.; VALLE, V.; MATEU, V. Automated issuance of post-quantum certificates: A new challenge. In: SPRINGER. **International Conference on Applied Cryptography and Network Security**. [S.l.], 2024. p. 3–23. https://dx.doi.org/10.1007/978-3-031-54773-7_1.

278 GIRON, A. A.; SCHARDONG, F.; CUSTÓDIO, R. TLS 1.3 Handshake Analyzer. In: SBC. **Extended Proceedings of XXII Brazilian Symposium on Information and Computational Systems Security**. [S.l.], 2022. p. 63–70. https://dx.doi.org/10.5753/sbseg_estendido.2022.226725.

279 OLIVEIRA, A. D. A.; ELER, M. M. Accessibility in electronic government: a study on the implementation of web standads in sites gov.br. In: **Proceedings of the annual conference on Brazilian Symposium on Information Systems: Information Systems: A Computer Socio-Technical Perspective-Volume 1**. [S.l.: s.n.], 2015. p. 691–698. https://dl.acm.org/doi/abs/10.5555/2814058.2814166.

280 MAYR, L.; SCHARDONG, F.; CUSTÓDIO, R. Simplifying electronic document digital signatures. 2022. https://dx.doi.org/10.48550/arXiv.2208.03951.

281 JAMES, J. The smart feature phone revolution in developing countries: Bringing the internet to the bottom of the pyramid. **The Information Society**, Taylor & Francis, v. 36, n. 4, p. 226–235, 2020. https://dx.doi.org/10.1080/01972243.2020.1761497.

282 Council of European Union. **Regulation No 910/2014 of the European Parliament**. 2014.

283 GRASSI, P.; GARCIA, M.; FENTON, J. **Digital Identity Guidelines**. Gaithersburg, MD, 2017. https://dx.doi.org/10.6028/NIST.SP.800-63-3.

284 Brasil. Lei nº 6.015, de 31 de dezembro de 1973. **Diário Oficial**, Brasília, DF, 1973. Available at https://www.planalto.gov.br/ccivil_03/leis/l6015compilada.htm, accessed on 23 July 2023.

285 Keycloak. **Open source identity and access management**. 2013. Available at https://www.keycloak.org/, accessed on 26 June 2024.

286 HODGES, J.; JONES, J.; JONES, M. B.; KUMAR, A.; LUNDBERG, E. Web authentication: An api for accessing public key credentials level 2. **World Wide Web**

Consortium, 2021. Available at https://www.w3.org/TR/webauthn-2/, accessed on 26 June 2024.

287 MGISP. **Conta gov.br**. 2021. Available at https://www.gov.br/governodigital/pt-br/conta-gov-br. accessed on 24 July 2023.

288 LODDERSTEDT, T.; FETT, D.; HAINE, M.; PULIDO, A.; LEHMANN, K.; KOIWAI, K. **OpenID Connect for Identity Assurance 1.0**. [S.l.]: OpenID, 2022. Available at https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html/, accessed on 26 June 2024.

289 SAKIMURA, N.; BRADLEY, J.; JAY, E. **Financial-grade API Security Profile 1.0**. [S.l.]: OpenID, 2021. Available at https://openid.net/specs/openid-financial-api-part-1-1_0.html/, accessed on 26 June 2024.

290 THöNES, J. Microservices. **IEEE Software**, v. 32, n. 1, p. 116–116, 2015. https://dx.doi.org/10.1109/MS.2015.11.

291 DOCUMENT management — Portable document format — Part 2: PDF 2.0. [S.l.], 2020. Available at: https://www.iso.org/standard/75839.html, accessed on 24 June 2024.

APPENDIX A – RESEARCH JOURNEY

My doctoral research journey began with a series of thought-provoking discussions with Professor Ricardo, who, drawing from his extensive experience in e-ID, highlighted several critical gaps and limitations in the existing literature. His observations resonated with me, particularly as I navigated the early stages of the Ph.D. program, attended courses, and engaged with the academic community. Initially, my approach to the literature was unstructured. I oscillated between highly technical papers and more conceptual works, attempting to grasp the vast landscape of identity, not just in the electronic realm but as a broader philosophical and sociological concept.

The initial phase of broad exploration was not just a necessary step but a crucial one. It allowed me to gain diverse perspectives on identity, which later proved instrumental when I began to delve deeper into specific areas. This phase laid the foundation for my more focused work, taking me through various disciplines, from computer science to philosophy, and enabling me to see identity from multiple angles. This multidisciplinary approach, while challenging, provided a rich foundation that would later inform the more focused phases of my work.

After this period of extensive exploration, I began to concentrate on the SSI concept. This complex and time-consuming process spanned several months, if not over a year. My goal was to strip away the jargon and the often exaggerated claims surrounding SSI to understand it for what it truly is. This deep dive into SSI involved a systematic literature review, which was not limited to specific problems but aimed to understand the state of the art in SSI comprehensively. Through this process, I identified several issues that were surprisingly underexplored in the literature. One such issue was the search for metadata in blockchains, which struck me as a glaring gap that had yet to be adequately addressed. This realization led me to pursue this topic in parallel with my systematic review, driven by the desire to contribute novel insights to the field and produce tangible results, such as publications, to maintain progress in my doctoral journey.

Simultaneously, I engaged with my research group, where discussions on PQC were becoming increasingly prevalent. Many of my peers were working on PQC in much greater depth than I was then. These discussions, alongside guidance from my advisor, sparked the idea of merging the two seemingly disparate fields of PQC and e-ID management. This interdisciplinary approach led to exploring how to adapt OIDC and OAuth 2.0 protocols to be post-quantum resistant by modifying their cryptographic primitives. This work was conducted concurrently with the systematic literature review and the blockchain metadata search project, resulting in three significant publications. These efforts were not just academic exercises; they also had practical implications, as evidenced by our successful patent application and the subsequent implementation of this patented technology in collaboration with various institutions, including the civil registry of natural persons of Brazil, RNP, and the government of Mozambique.

During this period, I devoted a significant portion of my time — up to 90% — to these

projects, which, while immensely rewarding in terms of practical experience, led to a temporary shift away from the core focus of my thesis. Managing these projects, which involved coordinating with teams across different countries and working remotely, greatly enhanced my skills in project management, particularly in decentralized environments. However, as the qualification exam of my Ph.D. approached, I realized the need to refocus on my primary research contributions. This realization was a turning point, prompting me to re-engage with the literature and critically assess the shortcomings of SSI as identified in my systematic review.

During this reflective period, the concept of fiduciary identity began to take shape. Through extensive discussions with my advisor and other experts in the field, the idea of a fiduciary identity model emerged as a solution to some of the fundamental issues with SSI, particularly concerning user consent and the cumbersome nature of navigating the digital identity landscape. The fiduciary identity model I proposed during my qualification exam was designed to address these challenges by providing a more user-centric approach to identity management.

Following my qualification exam, which marked a significant milestone in my Ph.D. journey, I spent the next year and a half refining this concept and further developing the theoretical framework that would support it. This period of focused research led to the creation of the RAF framework, a theoretical model for describing e-ID systems. My earlier work during my master's degree on meta-models and formal descriptions influenced the RAF framework. I saw a clear gap in the identity management literature for such formalized descriptions, and my background in multi-agent systems, a much more formal area, gave me the tools to address this need.

As I moved closer to the final stages of my Ph.D., it became apparent that there was a disconnect between the RAF framework and the fiduciary identity model. In the two months leading up to the submission of my thesis, I dedicated my efforts to aligning these two components, ensuring that the fiduciary identity model was fully integrated within the RAF framework. This alignment was crucial for achieving coherence in the thesis, particularly given the potential for disjointedness between the chapters. While I acknowledge that some discontinuities may still exist, I made every effort to ensure that the theoretical framework and the fiduciary identity model were cohesively presented, providing a unified narrative underpinning this doctoral research's contributions.

APPENDIX B – ELECTRONIC AUTHENTICATION OF THE CIVIL REGISTRY OF BRAZIL

B.1 INTRODUCTION

The importance of e-ID is emerging in society, given the increasing digitalization of human interactions. Tasks and services that until then were carried out exclusively in the physical world are gradually transported to the virtual realm. In this sense, it is possible to observe a global technological movement towards the digitization and standardization of e-IDs, in order to formalize the digital recognition of citizens in a legal context (282, 283).

One of the biggest challenges in this scenario concerns the way to collect, ensure and verify the authenticity of user information, so that the veracity of their data can be accurately asserted. It is possible, for example, to request a person's physical documentation to prove their identity, in a similar way to the authentication process carried out in the real world. But, although this solution alleviates the problems mentioned, it still does not solve them. Physical documents can be fraudulent, need to be registered manually and may not reflect the most up-to-date data.

Thus, the search for an e-ID that reflects and aggregates the public records of Brazilian citizens in an integral way resulted in the creation of the Autenticação Eletrônica do Registro Civil (IdRC)[1]: an e-ID that is connected to the nation's primary database of natural persons. The data is verified, secured and constantly updated (according to Art. 106 and 107 of Law No. 6,015 (284)) by a government entity, without the need for administration by the identity owner.

The IdRC uses the OAuth 2.0 (36) and OIDC (37) protocols, the *de facto* standards used worldwide to implement e-ID (81). The system was implemented through the free and open source platform *Keycloak* (285), considering the wide adoption of this solution in the global market.

In this appendix, IdRC's architectural and technical choices will be described and supported, clarifying its characteristics and functioning, as well as future steps. The remainder of this appendix is organized as follows. Section B.2 presents the supported authentication factors. Section B.3 presents the system's LoA and the identity lifecycle. Section B.4 explains how integration with SPs are performed. Finally, Section B.5 concludes by pointing out future work. This appendix has been previously published as an extended abstract (276):

Silva, B. V. R., Schardong, F., Junior, L. C. V., & Custódio, R. F. (2023). **Identificação Eletrônica do Registro Civil do Brasil**. In Extended Proceedings of XXIII Brazilian Symposium on Information and Computational Systems Security (pp. 89-92). SBC. DOI: https://doi.org/10.5753/sbseg_estendido.2023.235911

[1] https://idrc.registrocivil.org.br/

B.2 AUTHENTICATION FACTORS

Authentication factors can be described as methods or techniques used to ensure that the user is who they say they are, that is, to ensure that the user is the owner of the e-ID they are trying to use. Typically three categories of authentication factors are described in the literature (283): (i) something you know (knowledge); (ii) something you own (possession); and (iii) something you are (intrinsic).

The IdRC currently has five authentication factors distributed across the three categories mentioned above. Knowledge: (i) password; and (ii) questionnaire on intergenerational biographical information. Possession: (iii) Time-based One Time Password (TOTP) sent by *e-mail* or Short Message Service (SMS), as well as presented in applications (*e.g.*, Google Authenticator and FreeOTP); and (iv) Web Authentication (WebAuthN) (286). Finally, the intrinsic factor is (v) facial biometrics, consults multiple government sources to assess the veracity of the information collected. These authentication factors make up, together with other parameters, the LoA of IdRC.

B.3 LEVEL OF ASSURANCE AND LIFE CICLE

The LoA of an e-ID is a concept that reflects the accuracy that the bearer of an identity is who the information contained in it describes (283). It is important to note that the biographical attributes of an IdRC are independent of LoA, as they are defined by each citizen's primary data. Based on international LoA models, such as those established by the US government (NIST-SP 800-63-3) (283) and by the European Union (electronic IDentification, Authentication and trust Services (eIDAS)) (282), and national use cases, such as the Gov.br (287) identity system, the IdRC proposes a three-level LoA: low, substantial and high. The low LoA implies low certainty that the IdRC holder is in fact its owner (this is the standard level of e-ID). The substantial LoA carries greater reliability. For an e-ID to have this level, authentication using facial biometrics or a qualified digital certificate must have been used at least once in the last 12 months. Finally, the high LoA means that the citizen appeared in person at a civil registry office of natural persons, to carry out facial biometric collection and define authentication factors. This LoA provides the system with the highest degree of certainty that the holder of the IdRC is who the data describes. We show in Table 23 the LoA of the aforementioned usecases, along with IdRC.

The IdRC lifecycle begins at a person's birth. Birth registration in a civil registry office for natural persons implies the creation of an IdRC for the newborn. All Brazilians born before the implementation of IdRC already had their identities created in the system. In other words, a citizen's first access to their IdRC, which is only permitted for users over the age of sixteen, consists of obtaining possession of their e-ID. This process can take place on the premises of a civil registration service for natural persons, which implies a high LoA of identity, or *online* by the user, which limits LoA to substantial.

Table 23 – The LoA of eIDAS, NIST, gov.br and IdRC.

eIDAS	**Low**	**Substantial**	**High**
	Identity self-declared	Remote or in-person proof of identity	In-person (or supervised remote) identity proofing and biometric data collection
NIST SP 800-63-3	**LOA 1**	**LOA 2**	**LOA 3**
	Self-declared attributes	Remote or in-person proof of identity	In-person proof of identity, with document checking.
Gov.br	**Bronze**	**Silver**	**Gold**
	Self-registration, with data checking in government databases	Data validation via authentication with an accredited bank or facial recognition	Validation of data with qualified certificate or facial recognition
IdRC	**Low**	**Substantial**	**High**
	Self-registration, with data checking in Civil Registry databases	Presentation of qualified certificate, online biometric validation or video conference.	In-person validation at the civil registry with document verification, with biometrics collection and definition of in-person access credentials

Source: The author.

The first access online begins with the individual entering their Cadastro de Pessoa Física (CPF) followed by the resolution of a challenge to ensure that a human being is using the system. The user is then subjected to facial biometrics capture, which requires that the process is being carried out on a device with a camera and that minimum image quality and ambient lighting requirements are met. If the biometrics are successfully captured and validated in all available government biometric databases in which the citizen is registered, the IdRC will have its LoA raised to substantial and the user will be able to proceed to register the authentication factors. In cases where capture fails, the user can continue the process by submitting an official document with photo. As a last resort, if any errors occur during submission, an intergenerational questionnaire will be conducted. If the document capture or questionnaire is completed successfully, the LoA will be set to low and the individual will proceed to register authentication factors. This registration begins with defining a password. No password policy is enforced. The user is then allowed to: (i) register a phone number to send One Time Password (OTP) credentials; (ii) register email address for also sending OTP credentials; (iii) scan QR code for offline TOTP; and (iv) register one or more devices for WebAuthN (286).

During the lifecycle of an IdRC's e-ID, it is possible for its LoA to be raised or lowered. The change of LoA of an e-ID from low to substantial is associated with the use of facial biometrics or qualified certificate. This elevation can happen automatically if a SP requests an e-ID authenticated with two factors and the user chooses facial biometrics or qualified certificate. These options are always presented together with the authentication factors that the user registered on the first access or *a posteriori*. The other form of elevation happens when a SP requires e-IDs with LoA of at least substantial, and the e-ID of the user performing the authentication is low. In this case, only the two factors associated with the increase in LoA from low to substantial will be presented and the user must necessarily complete the authentication process

with one of the two. The increase from substantial to high only occurs through attendance in person at a civil registration office of natural persons, with the presentation of documents and collection of biometrics.

A user may, on the other hand, have the LoA of their e-ID downgraded from high to substantial if they go more than one year without using facial biometrics. Similarly, the user may be downgraded from substantial to low if more than one year passes without using an authentication factor associated with the substantial level. Another important aspect is that in the event of death, which is detected through integration with the Brazilian Civil Registry database, access to the e-ID is automatically revoked and access tokens granted to SPs are invalidated.

When the e-ID owner is unable to use their password to access the IdRC, it is possible to resort to password recovery. This process allows low and substantial category users to reset their access credentials, using other registered authentication factors. In the case of identities with high LoA or that do not have other authentication methods available, it is necessary to attend a civil registry office for natural persons to carry out this process.

B.4 INTEGRATION WITH SERVICE PROVIDERS

The IdRC allows applications to connect to the system with the purpose of identifying, authenticating and obtaining user attributes. The integration between IdRC and SPs, *i.e.*, clients, takes place via the OIDC (37) and OAuth 2.0 (36) protocols. Clients connected to the IdRC are added to the system by an administrator and receive a unique identification *string* and an access *token*. Applications can request the IdRC to identify and authenticate a user, specifying the minimum LoA. It is also possible for the client to specify which second authentication factor should be used. Finally, user attributes, such as date, city and state of birth, name, telephone number, e-mail, affiliation (information on parents and grandparents) and gender can be requested. The user then authorizes or disallows their sharing.

B.5 CONCLUSION

The IdRC is a robust identity and attribute provider, as it is linked directly to the Brazilian citizen's primary data source. The assurance that user death implies the impossibility of using their respective IdRC's e-ID brings significant gains to SPs, that do not need to worry with such matter. Furthermore, by requiring face-to-face validation to obtain a high LoA, the IdRC provides a higher LoA than other IdPs, without imposing an excessive burden on the user, as all municipalities in Brasil have a civil registration service for natural persons.

As future work, new protocols are expected to be implemented, such as *OpenID Connect for Identity Assurance* (288) and *Financial-grade API Security Profile* (289). We are also studying the possibility of issuing verifiable credentials to users who wish to remain in the SSI paradigm (77).

APPENDIX C – LESS DIGITAL CERTIFICATION AND MORE ELECTRONIC IDENTITY

C.1 INTRODUCTION

Electronic identity is essential for creating secure systems. One effective approach is to establish federations of IdPs, which enhances interoperability and provides users with access to a wide range of services. The Comunidade Acadêmica Federada (CAFe), managed by Brazil's RNP since 2008, is an example of such an implementation. Currently, it connects over one million users across 380 IdPs from educational and research institutions in Brazil, facilitating access to numerous inter-institutional services.

Among the services CAFe offers is the issuance of digital certificates. These certificates, which are part of the Infraestutura de Chaves Públicas para Ensino e Pesquisa (ICPEdu), enable users to authenticate and digitally sign documents at no cost. However, only 4% of CAFe users utilize this service, despite an increasing need for digital signatures.

This appendix discusses a project that integrates CAFe, ICPEdu, and the OTC to develop a digital signer that requires no end-user interaction with the PKI, thus simplifying the signing process. The appendix is organized as follows: Section C.2 details the updated ICPEdu infrastructure for generating OTC. Section C.3 describes the architecture of the signer, the signing process, and relevant discussions. Lastly, Section C.4 concludes the appendix. This appendix has been previously published as an extended abstract (275):

Perottoni, E. D., Costa, B. P., Müller, F. L., dos Santos Camargo, V., Schardong, F., Silvano, W., ... & Rieckmann, N. (2023). **Menos Certificação Digital e Mais Identidade Eletrônica: ICPEdu e CAFe em um Assinador Digital Inclusivo**. In Extended Proceedings of XXIII Brazilian Symposium on Information and Computational Systems Security (pp. 93-96). SBC. DOI: https://doi.org/10.5753/sbseg_estendido.2023.235947

C.2 CHANGES TO ICPEDU

The PKI encompasses a range of operational and security policies, services, and interoperability protocols that facilitate the management of keys and certificates using public key cryptography. A traditional PKI is structured as a hierarchical network of CAs arranged in a tree format, with user certificates represented as leaves. A digital certificate, which is an electronic document, links a public key to a specific entity.

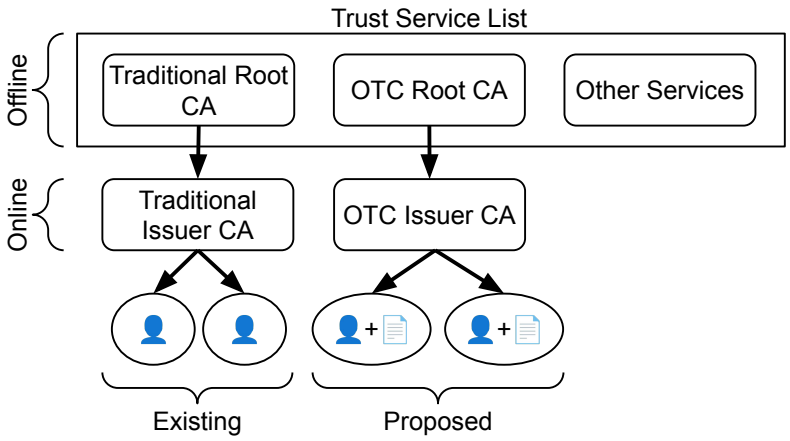
In the context of educational and research institutions affiliated with the CAFe network, ICPEdu issues digital certificates. However, managing these certificates poses significant challenges for users, including the responsibility of private key management, certificate installation, and ensuring secure system integration for digital signatures.

To address these challenges, a novel approach known as the OTC has been proposed. Each OTC is generated for a single digital signature, thereby eliminating risks associated with

private key exposure. The OTC directly incorporates the cryptographic hash of the document being signed, and its unique user attributes are verified through the IdP at the time of user authentication within the CAFe network. The key benefits of this approach include: (i) the OTC's validity is limited to the specific document it signs; (ii) user identification attributes are dynamically fetched from the IdP with each signature; and (iii) certificate revocation becomes unnecessary. Nonetheless, to maintain compatibility with existing systems, OTC CAs may still issue an empty Certificate Revocation List (CRL).

Furthermore, a new certification infrastructure has been developed featuring a Root CA and a CertAU issuing CA, both established with a 100-year validity period. An associated Trust Service List (TSL) has been created to manage the roots of trust for ICPEdu. This framework is depicted in Figure 27, showing the TSL along with the two root CAs and their corresponding certification trees.

Figure 27 – ICPEdu with TSL and two certification trees: traditional and OTC.



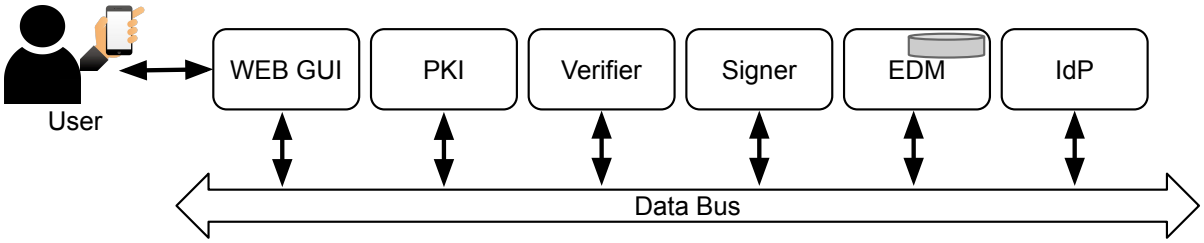
Source: Adapted from (275).

C.3 DIGITAL SIGNER

The Digital Signer is a project developed by the RNP that leverages the OTC tree from ICPEdu[1]. It is designed using a microservices architecture, meaning that each component of the application is developed as an independent service dedicated to a specific function. This design allows for each service to be developed, deployed, and scaled separately from others, enhancing the system's flexibility and modularity. This architecture choice aligns with modern software development practices that prioritize decentralized management of application components to facilitate easier updates and better scalability (290).

[1] Available at https://web.archive.org/web/20240628214754/https://cdd.icpedu.rnp.br/

Figure 28 – Digital signer architecture.

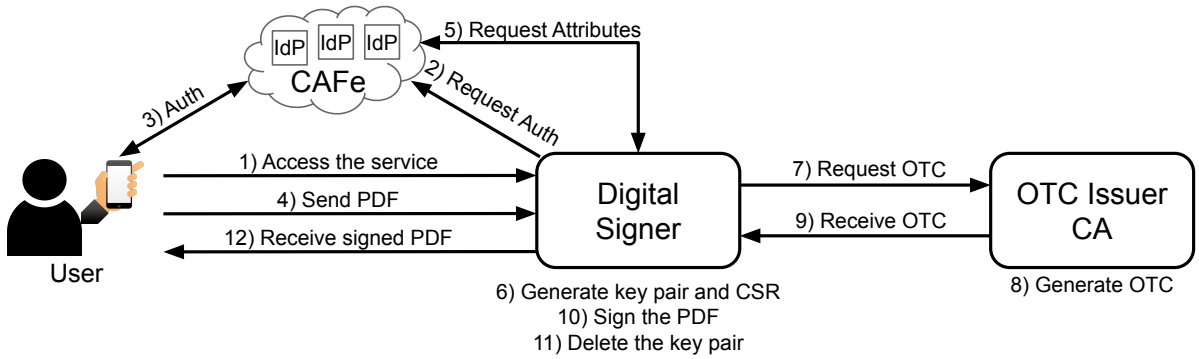


Source: Adapted from (275).

The Digital Signature system is comprised of the following services: (i) *web interface* serves as the user interface for accessing other services; (ii) *PKI* interacts with ICPEdu to issue OTCs; (iii) *verifier* is tasked with verifying the authenticity of signed documents; (iv) *signer* digitally signs Portable Document Format (PDF) documents following the ISO 32000-2 specification (291); (v) Electronic Document Management (EDM) stores signed documents and allows multiple users to sign the same document without needing to resend it; and (vi) IdP: This connects to CAFe to authenticate users and gather their attributes necessary for issuing OTC.

When an end user utilizes the digital signer through the web interface, they engage with the services outlined above. The flowchart depicted in Figure 29 demonstrates the interactions between the user, the digital signer, CAFe, and ICPEdu during the document signing process.

Figure 29 – Signature flowchart.



Source: Adapted from (275).

The document signing process using the digital signer involves the following steps: (i) the user accesses the digital signer via their browser; (ii) the signer requests authentication, redirecting the user to CAFe for this purpose; (iii) the user authenticates using MFA at one of the federation's IdPs; (iv) post-authentication, the user uploads the document they wish to sign; (v) without requiring further user intervention, the signer retrieves the user's attributes from the IdP; (vi) the signer then generates an asymmetric key pair and creates a Certificate Signing Request (CSR), which includes the hash of the uploaded document; (vii) this CSR is sent to the CA; (viii) the CA processes the CSR and issues the OTC; (ix) the OTC is sent back to the signer; (x) using the received certificate, the signer digitally signs the PDF according

to the ISO 32000-2 specification, incorporating the certificate into the PDF; (xi) after signing, the certificate and the generated key pair are deleted; and (xii) the signed document is returned to the user. This process ensures secure authentication and signing, with minimal user input required after the initial steps.

The OTC streamlines the PKI by eliminating the need to revoke OTCs and the need to apply timestamps to signed documents. This certificate is specifically generated for a single use—to sign the document that the user intends to sign. This simplifies the user experience significantly, as it removes the need for managing smartcards, cryptographic keys, cloud-based certificates, unlocking PINs, or other complexities associated with traditional digital certification methods. The user simply needs to authenticate via an IdP and interact with the signer to upload their document for signing and then download it once signed. These interactions are straightforward and do not require any specialized technical knowledge. Additionally, using IdPs instead of smartcards does not compromise the security level. While traditional PKI requires possession of a cryptographic token and its password, OTC requires MFA, maintaining robust security measures.

C.4 CONCLUSION

As of the latest data, ICPEdu has 42,000 valid certificates in use[2], even though there are approximately one million users across federated IdPs in CAFe. The RNP digital signature initiative aims to transform this scenario, enabling all CAFe users to utilize digital signatures. By integrating OTC with ICPEdu and the CAFe federation, the RNP digital signer simplifies the digital signing process for everyday users. It offers a user-friendly experience that does not require in-depth knowledge of digital certification or the management of cryptographic artifacts. Furthermore, it produces lifelong valid digital signatures using certificates that are valid for 100 years, thus ensuring long-term usability and security.

[2] https://web.archive.org/web/20230727134153/https://painel.icpedu.rnp.br/public/stats/certificate