

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO DE FLORIANÓPOLIS
CIÊNCIAS DA COMPUTAÇÃO

PEDRO HENRIQUE DE SENA TROMBINI TAGLIALENHA

VIABILIDADE DE IDENTIDADE AUTO-SOBERANA NO BRASIL: PROVA DE
CONCEITO COM CARTEIRA DIGITAL ACADÊMICA NA UFSC

Florianópolis
2026

PEDRO HENRIQUE DE SENA TROMBINI TAGLIALENHA

VIABILIDADE DE IDENTIDADE AUTO-SOBERANA NO BRASIL: PROVA DE
CONCEITO COM CARTEIRA DIGITAL ACADÊMICA NA UFSC

Trabalho apresentado como requisito para
obtenção do título de Bacharel em Ciências
da computação, no Centro Tecnológico de
Florianópolis, da Universidade Federal de
Santa Catarina.

Orientador(a): Doutor Lucas Machado da
Palma

Coorientador(a): Doutor Jean Everson
Martina

Florianópolis
2026

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

Taglialienha, Pedro Henrique de Sena Trombini
VIABILIDADE DE IDENTIDADE AUTO-SOBERANA NO BRASIL :
PROVA DE CONCEITO COM CARTEIRA DIGITAL ACADÊMICA NA UFSC /
Pedro Henrique de Sena Trombini Taglialienha ; orientador,
Lucas Machado da Palma, coorientador, Jean Everson
Martina, 2026.
149 p.

Trabalho de Conclusão de Curso (graduação) -
Universidade Federal de Santa Catarina, Centro Tecnológico,
Graduação em Ciências da Computação, Florianópolis, 2026.

Inclui referências.

1. Ciências da Computação. 2. Identidade
descentralizada. 3. Credencial verificável. 4. Privacidade
de dados. 5. Prova de conhecimento zero. I. Palma, Lucas
Machado da . II. Martina, Jean Everson. III. Universidade
Federal de Santa Catarina. Graduação em Ciências da
Computação. IV. Título.

PEDRO HENRIQUE DE SENA TROMBINI TAGLIALENHA

VIABILIDADE DE IDENTIDADE AUTO-SOBERANA NO BRASIL: PROVA DE
CONCEITO COM CARTEIRA DIGITAL ACADÊMICA NA UFSC

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do título de Bacharel em Ciências da computação, no Centro Tecnológico de Florianópolis, da Universidade Federal de Santa Catarina.

Florianópolis (SC), 03 de julho de 2026.

Banca Examinadora:

Doutor Lucas Machado da Palma
Orientador
UFSC

Doutor Jean Everson Martina
Coorientador
UFSC

Luis Felipe Fabiane
Membro(a)
UFSC

Lucas Silva da Costa
Membro(a)
UFSC

RESUMO

A transformação digital impulsionou a adoção de sistemas de identificação, gerando debates sobre privacidade e centralização de dados. Modelos de identidade baseados em credenciais verificáveis e provas de conhecimento zero surgem como alternativas para conceder ao indivíduo controle sobre seus atributos. Este trabalho investiga a viabilidade técnica da aplicação dessas tecnologias no contexto institucional brasileiro, caracterizado por infraestruturas centralizadas como a Infraestrutura de Chaves Públicas Brasileira e a plataforma gov.br. O estudo apoia-se em revisão bibliográfica, análise documental e no desenvolvimento de um protótipo de carteira digital acadêmica. O software móvel operou como um estudo preliminar focado no cenário universitário, implementando ciclos criptográficos de emissão, guarda e divulgação seletiva de informações em ambiente isolado. Os resultados da execução indicaram o funcionamento lógico dos protocolos de proteção de privacidade em dispositivos locais por meio de bibliotecas de código aberto. A avaliação dos cenários aponta para a formulação de um modelo de implementação híbrido, no qual a emissão de informações permanece sob a jurisdição do Estado para assegurar o lastro legal, enquanto a apresentação e o controle de divulgação ficam a cargo dos usuários. As limitações inerentes à operação isolada do aplicativo definem a necessidade de extrapolação dos algoritmos por meio de integrações com sistemas governamentais autênticos, etapa exigida para a avaliação concreta da viabilidade da tecnologia em escala nacional.

Palavra-chave: Privacidade de dados. Identidade descentralizada. Credencial verificável. Prova de conhecimento zero.

ABSTRACT

The digital transformation has driven the adoption of identification systems, sparking debates regarding privacy and data centralization. Identity models based on verifiable credentials and zero-knowledge proofs emerge as alternatives to grant individuals control over their attributes. This work investigates the technical feasibility of applying these technologies within the Brazilian institutional context, which is characterized by centralized infrastructures such as the Brazilian Public Key Infrastructure and the gov.br platform. The study relies on a literature review, documentary analysis, and the development of an academic digital wallet prototype. The mobile software acted as a preliminary study focused on the university scenario, implementing cryptographic cycles of issuance, custody, and selective disclosure of information in an isolated environment. Execution results indicated the logical functioning of privacy protection protocols on local devices through open-source libraries. The evaluation of scenarios points toward the formulation of a hybrid implementation model, where the issuance of information remains under State jurisdiction to ensure legal validity, while data presentation and disclosure control are managed by the users. The limitations inherent to the prototype's isolated operation define the need to extrapolate the algorithms through integrations with authentic governmental systems, a required step for a concrete assessment of the technology's viability on a national scale.

Keywords: Data privacy. Decentralized identity. Verifiable credential. Zero-knowledge proof.

LISTA DE FIGURAS

Figura 1 – Fluxograma geral das etapas de desenvolvimento da pesquisa. . . .	84
Figura 2 – Fluxo metodológico com iteração para seleção tecnológica.	85
Figura 3 – Mapeamento do triângulo de confiança SSI para os módulos concretos do protótipo.	91
Figura 4 – Arquitetura em camadas do protótipo de carteira digital acadêmica.	93
Figura 5 – Grafo de dependências do Composition Root (container.ts).	96
Figura 6 – Interfaces de serviço e implementações concretas seguindo o Princípio de Inversão de Dependência.	98
Figura 7 – Diagrama de classes dos modelos de dados com extensões sobre o W3C VC Data Model e DIF Presentation Exchange.	100
Figura 8 – Fluxo de emissão, apresentação e verificação de credenciais verificáveis.	103
Figura 9 – Comparação dos protocolos de emissão SD-JWT (construção direta) e AnonCreds (protocolo CL completo).	105
Figura 10 – Pipeline de verificação implementando o padrão Cadeia de Responsabilidade.	108
Figura 11 – Fluxos de verificação para os quatro cenários implementados no protótipo.	109
Figura 12 – Diagrama de classes do subsistema de Provas de Conhecimento Zero.	110
Figura 13 – Modelo hierárquico de cadeia de confiança PKI implementado no protótipo.	112
Figura 14 – Fronteiras de segurança e distribuição de material criptográfico entre camadas de armazenamento.	112
Figura 15 – Design System e componentes base do protótipo definidos no Figma.	115
Figura 16 – Exemplos do design inicial elaborado no Figma.	116
Figura 17 – Interfaces finais: geração de identidade, menu e emissão.	117
Figura 18 – Fluxo de apresentação e verificação no aplicativo móvel.	118
Figura 19 – Painel de Execução de Diagnósticos E2E com resultados temporais de execução.	118
Figura 20 – Fluxo de gerenciamento de dados: emissão, custódia, consentimento e validação.	122
Figura 21 – Painel de métricas de execução de testes de integração	123

LISTA DE TABELAS

Tabela 1 – Palavras-chave e sinônimos utilizados na busca.	33
Tabela 2 – Resultados do processo de busca e seleção de artigos.	34
Tabela 3 – Matriz Comparativa (Parte 1): Arquiteturas de Integração e Privacidade Avançada.	72
Tabela 4 – Matriz Comparativa (Parte 2): Casos de Uso Específicos, Segurança e Governança.	73
Tabela 5 – Tecnologias e padrões adotados pela especificação europeia. . . .	79
Tabela 6 – Síntese das tecnologias e bibliotecas selecionadas para o protótipo móvel	86
Tabela 7 – Hierarquia de diretórios do projeto e responsabilidades.	92
Tabela 8 – Hierarquia de injeção de dependências (Composition Root). . . .	94
Tabela 9 – Cenários de verificação implementados no protótipo.	109
Tabela 10 – Esquema de chaves de armazenamento cifrado.	113
Tabela 11 – Cobertura de testes automatizados por módulo.	120

LISTA DE ABREVIATURAS E SIGLAS

ABAC	<i>Attribute-Based Access Control</i> (Controle de Acesso Baseado em Atributos)
ARF	<i>Architecture and Reference Framework</i> (Arquitetura e Estrutura de Referência)
BLE	<i>Bluetooth Low Energy</i>
CA	<i>Certificate Authority</i> (Autoridade Certificadora)
CAB	<i>Conformity Assessment Body</i> (Organismo de Avaliação da Conformidade)
CBOR	<i>Concise Binary Object Representation</i>
CDT	Carteira Digital de Trânsito
CIA	Confidencialidade, Integridade e Disponibilidade
CIN	Carteira de Identidade Nacional
CPF	Cadastro de Pessoas Físicas
CRS	<i>Common Reference String</i>
DID	<i>Decentralized Identifier</i> (Identificador Descentralizado)
DLT	<i>Distributed Ledger Technology</i> (Tecnologia de Registro Distribuído)
DPKI	<i>Decentralized Public Key Infrastructure</i> (Infraestrutura de Chave Pública Descentralizada)
EAA	<i>Electronic Attestation of Attributes</i> (Atestado Eletrônico de Atributos)
EBSI	<i>European Blockchain Services Infrastructure</i>
ECC	<i>Elliptic Curve Cryptography</i> (Criptografia de Curvas Elípticas)
ECDSA	<i>Elliptic Curve Digital Signature Algorithm</i>
eIDAS	<i>Electronic Identification, Authentication and Trust Services</i>
EUDI Wallet	<i>European Union Digital Identity Wallet</i> (Carteira de Identidade Digital da União Europeia)
EUF-CMA	<i>Existentially Unforgeable under Chosen Message Attack</i>

HSM	<i>Hardware Security Module</i> (Módulo de Segurança de Hardware)
IAM	<i>Identity and Access Management</i> (Gestão de Identidade e Acesso)
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IdP	<i>Identity Provider</i> (Provedor de Identidade)
ITI	Instituto Nacional de Tecnologia da Informação
JSON-LD	<i>JavaScript Object Notation for Linked Data</i>
JWT	<i>JSON Web Token</i>
KYC	<i>Know Your Customer</i>
LGPD	Lei Geral de Proteção de Dados
mDoc	<i>Mobile Document</i> (ISO/IEC 18013-5)
MGI	Ministério da Gestão e da Inovação em Serviços Públicos
NFC	<i>Near Field Communication</i>
NIZK	<i>Non-Interactive Zero-Knowledge Proof</i> (Prova de Conhecimento Zero Não Interativa)
OIDC	<i>OpenID Connect</i>
OID4VCI	<i>OpenID for Verifiable Credential Issuance</i>
OID4VP	<i>OpenID for Verifiable Presentations</i>
PEX	<i>Presentation Exchange</i>
PID	<i>Person Identification Data</i> (Dados de Identificação Pessoal)
PKI	<i>Public Key Infrastructure</i> (Infraestrutura de Chaves Públicas)
PKCE	<i>Proof Key for Code Exchange</i>
R1CS	<i>Rank-1 Constraint System</i>
RSL	Revisão Sistemática da Literatura
SAML	<i>Security Assertion Markup Language</i>
SBT	<i>Soulbound Token</i>
SD-JWT	<i>Selective Disclosure for JSON Web Tokens</i>

SE	<i>Secure Element</i> (Elemento Seguro)
SERPRO	Serviço Federal de Processamento de Dados
SP	<i>Service Provider</i> (Provedor de Serviço)
SSI	<i>Self-Sovereign Identity</i> (Identidade Auto-Soberana)
TEE	<i>Trusted Execution Environment</i> (Ambiente de Execução Confiável)
TL	<i>Trusted List</i> (Lista de Confiança)
ToIP	<i>Trust Over IP</i>
VC	<i>Verifiable Credential</i> (Credencial Verificável)
VCDM	<i>Verifiable Credentials Data Model</i>
VDR	<i>Verifiable Data Registry</i> (Registro de Dados Verificável)
VP	<i>Verifiable Presentation</i> (Apresentação Verificável)
W3C	<i>World Wide Web Consortium</i>
WSCD	<i>Wallet Secure Cryptographic Device</i> (Dispositivo Criptográfico Seguro de Carteira)
ZKP	<i>Zero-Knowledge Proof</i> (Prova de Conhecimento Zero)
zk-SNARK	<i>Zero-Knowledge Succinct Non-Interactive Argument of Knowledge</i>
zk-STARK	<i>Zero-Knowledge Scalable Transparent Argument of Knowledge</i>

SUMÁRIO

1	INTRODUÇÃO	14
1.1	OBJETIVOS	16
1.1.1	Objetivo geral	17
1.1.2	Objetivos Específicos	17
2	FUNDAMENTAÇÃO TEÓRICA	18
2.1	IDENTIDADE DIGITAL	18
2.2	IDENTIDADE AUTO-SOBERANA (SSI)	20
2.3	FUNDAMENTOS CRIPTOGRÁFICOS	21
2.3.1	Infraestrutura de Chaves Públicas e Assinaturas Digitais	21
2.3.2	Prova de Conhecimento Zero	23
2.4	COMPONENTES E PADRÕES DA SSI	27
2.4.1	Identificadores Descentralizados (DIDs)	27
2.4.2	Credenciais Verificáveis	28
3	REVISÃO DA LITERATURA	32
3.1	METODOLOGIA	32
3.1.1	Estratégia de Busca	32
3.1.2	Crerios de Inclusão e Exclusão	33
3.1.3	Processo de Seleção	33
3.2	RESULTADOS DA PESQUISA	33
3.3	ANÁLISE DOS TRABALHOS SELECIONADOS	34
3.3.1	Integração com Sistemas Legados e Interoperabilidade Técnica	34
3.3.2	Governança, Confiança e Regulação (eIDAS 2.0)	41
3.3.3	Privacidade Avançada, Criptografia e Segurança	49
3.3.4	Casos de Uso Específicos: Educação e Cenários Offline	56
3.3.5	Estado da Arte: Barreiras, Adoção e Metodologias de Avaliação	61
3.4	SÍNTESE DOS RESULTADOS E RESPOSTAS ÀS QUESTÕES DE PESQUISA	69
4	ANÁLISE DE TECNOLOGIAS E IMPLEMENTAÇÕES DE REFERÊNCIA	74
4.1	ESPECIFICAÇÕES TÉCNICAS E PADRÕES DE INTEROPERABILIDADE GLOBAIS	74
4.1.1	Arquitetura de Segurança e Governança	74
4.1.2	Protocolos de Comunicação e Transporte de Dados	77
4.1.3	Formatos de Credenciais e Divulgação Seletiva	77
4.1.4	Interações de Proximidade e Operação Offline	78

4.2	ANÁLISE DE COMPATIBILIDADE E LIMITAÇÕES ARQUITETURAIS NACIONAIS	79
5	PROPOSTA E DEFINIÇÃO TECNOLÓGICA	83
5.1	METODOLOGIA DE SELEÇÃO E DESENVOLVIMENTO	83
5.2	SELEÇÃO DE TECNOLOGIAS E BIBLIOTECAS	83
5.3	DEFINIÇÃO DO PROTÓTIPO	86
5.3.1	Objetivo e Funcionalidades Centrais	86
5.3.2	Arquitetura de Provas de Conhecimento Zero	87
5.3.3	Cenários de Validação Requisitados	87
5.3.4	Hierarquia de Confiança Implementada	88
5.3.5	Limites Operacionais e Escopo do Protótipo	88
6	DESENVOLVIMENTO E ARQUITETURA DO PROTÓTIPO	90
6.1	ORGANIZAÇÃO DO PROJETO E HIERARQUIA DE MÓDULOS	90
6.2	PADRÕES DE PROJETO E COMPOSIÇÃO DE DEPENDÊNCIAS	94
6.3	MODELOS DE DADOS E TIPAGEM ESTÁTICA	99
6.3.1	Modelo de Dados do Estudante	101
6.3.2	Credenciais e Apresentações Verificáveis	101
6.3.3	Apresentação por Troca (Presentation Exchange)	101
6.3.4	Emissor Confiável (Trust Chain)	101
6.4	GERENCIAMENTO DE IDENTIDADE DESCENTRALIZADA (DIDS)	101
6.5	EMIÇÃO DE CREDENCIAIS	102
6.5.1	Formato SD-JWT	104
6.5.2	Formato AnonCreds	104
6.5.3	Validação e Análise de Credenciais	106
6.6	APRESENTAÇÃO SELETIVA E VERIFICAÇÃO DE CREDENCIAIS	106
6.6.1	Construção de Apresentações	106
6.6.2	Pipeline de Verificação	106
6.6.3	Catálogo de Cenários	109
6.7	PROVAS DE CONHECIMENTO ZERO (ZKP)	109
6.7.1	Circuito de Faixa Etária (age_range)	110
6.7.2	Circuito de Verificação de Status (status_check)	110
6.7.3	Circuito de Nullifier (nullifier)	111
6.7.4	Provisionamento de Chaves de Prova	111
6.8	CADEIA DE CONFIANÇA PKI HIERÁRQUICA	111
6.9	PERSISTÊNCIA E SEGURANÇA DE DADOS	112
6.9.1	Armazenamento Cifrado	113
6.9.2	Gerenciamento de Estado Reativo	114
6.9.3	Cofre Credo (Aries Askar)	114
6.10	SERVIÇO CRIPTOGRÁFICO	114

6.11	DESIGN DE INTERFACE E EXPERIÊNCIA DO USUÁRIO (UX) . . .	115
6.11.1	Telas Finais do Aplicativo	115
6.12	GARANTIA DE QUALIDADE: TESTES E ANÁLISE ESTÁTICA	119
6.12.1	Testes de Serviço	119
6.12.2	Testes Ponta-a-Ponta (E2E) com Jest	119
6.12.3	Análise Estática	119
6.13	TESTES DE TEMPO DE EXECUÇÃO (E2E NATIVOS)	119
6.13.1	Interface de Diagnósticos e Orquestração	120
6.13.2	Casos de Teste Avaliados	121
7	DISCUSSÃO E AVALIAÇÃO DE RESULTADOS	122
7.1	AVALIAÇÃO DO ATENDIMENTO AOS OBJETIVOS	122
7.2	ANÁLISE DOS TESTES DO PROTÓTIPO E DISCUSSÃO DO CE- NÁRIO UNIVERSITÁRIO	123
7.3	DESAFIOS DE INTEGRAÇÃO EM ENGENHARIA DE SOFTWARE .	125
7.4	IMPLICAÇÕES PARA PRIVACIDADE E EXPERIÊNCIA DE USUÁRIO	126
7.5	EXPANSÃO DE ARQUITETURA PARA CASOS DE USO GOVER- NAMENTAIS	127
7.6	A ARQUITETURA DE IDENTIDADE AUTO-SOBERANA FRENTE À INFRAESTRUTURA NACIONAL E PADRONIZAÇÃO INTERNACIO- NAL	128
7.7	LIMITAÇÕES DO ESTUDO	130
7.8	TRABALHOS FUTUROS	130
8	CONCLUSÃO	132
	REFERÊNCIAS	134
	 APÊNDICES	144
	APÊNDICE A – ARTIGO NO FORMATO DA SOCIEDADE BRASI- LEIRA DE COMPUTAÇÃO	145
	APÊNDICE B – REPOSITÓRIO DO PROJETO	161

1 INTRODUÇÃO

A transformação digital reconfigurou as interações sociais e econômicas, estabelecendo a identidade digital como um componente fundamental para a segurança e a confiança em serviços online. Modelos tradicionais de gerenciamento de identidade, frequentemente centralizados, apresentam desafios significativos relacionados à fragmentação de dados, soberania do usuário e privacidade (SOLTANI et al., 2021). Em resposta a essas limitações, emerge o paradigma da Identidade Auto-Soberana (SSI, do inglês Self-Sovereign Identity), um modelo descentralizado que confere aos indivíduos controle autônomo sobre seus próprios dados de identificação (PREUKSCHAT; REED, 2021; SCHARDONG; CUSTÓDIO, 2021). Este modelo propõe uma reestruturação fundamental na arquitetura de confiança da internet, afastando-se da dependência de provedores de identidade centralizados (MÜHLE et al., 2018; REECE; MITTAL, 2022).

A materialização do paradigma SSI é viabilizada por um ecossistema de tecnologias e padrões abertos. Nele, destacam-se as Credenciais Verificáveis (VCs, do inglês Verifiable Credentials), que funcionam como atestados digitais criptograficamente seguros sobre atributos de um indivíduo (SPORNY et al., 2025; Verifiable Credentials Working Group, 2025), e os Identificadores Descentralizados (DIDs, do inglês Decentralized Identifiers), que servem como âncoras de confiança globais e independentes de uma autoridade central (MAZZOCCA et al., 2025; BABEL et al., 2025). A segurança e a privacidade deste ecossistema são potencializadas por primitivas criptográficas, notadamente as Provas de Conhecimento Zero (ZKP, do inglês Zero-Knowledge Proofs) (GOLDWASSER et al., 1985). As ZKPs permitem que uma parte (o provador) convença outra (o verificador) da veracidade de uma asserção sem revelar qualquer informação além da própria validade da asserção, implementando o princípio da minimização de dados de forma robusta (European Telecommunications Standards Institute (ETSI), 2023; LAVIN et al., 2024; ZEIN; PINKWART, 2025).

No contexto global, diversos países exploram esses novos modelos, mas a União Europeia tem liderado a implementação prática e regulamentada desses conceitos por meio da revisão de seu regulamento para Identificação Eletrônica e Serviços de Confiança (eIDAS). A nova versão, conhecida como eIDAS 2.0, estabelece um quadro para uma identidade digital europeia por meio da Carteira de Identidade Digital da UE (EUDI Wallet) (Parlamento Europeu e Conselho da União Europeia, 2024; Trust Agency, 2024). A Arquitetura e Estrutura de Referência (ARF) da EUDI Wallet especifica uma solução de carteira interoperável que permite aos cidadãos armazenar e compartilhar VCs para acessar serviços públicos e privados em toda a União, aplicando os princípios de controle do usuário e divulgação seletiva de informações

(eIDAS Expert Group, 2023). Este modelo europeu constitui uma das iniciativas mais consolidadas em termos de regulação e padronização técnica de identidade digital descentralizada (GÓMEZ, 2025; SCHWALM et al., 2022).

Paralelamente, o Brasil demonstra um movimento robusto em direção à digitalização da identificação civil (NEVES; SILVA, 2023; SANTOS et al., 2023). Este esforço é fundamentado por um novo quadro legal, incluindo a Lei de Governo Digital (Lei n.º 14.129/2021) (Brasil, 2021b; NEVES; SILVA, 2023; SANTOS et al., 2023) e a instituição da Carteira de Identidade Nacional (CIN) (Lei n.º 14.534/2023 (Brasil, 2023; BIONI et al., 2022) e Decreto n.º 10.977/2022 (Brasil, 2022; BIONI et al., 2022; SANTOS et al., 2023)). A CIN adota o Cadastro de Pessoas Físicas (CPF) como número de registro geral, unificando a identificação em nível nacional (Brasil, 2023; BIONI et al., 2022). A plataforma `gov.br` consolida essa visão, fornecendo a Conta GOV.BR como meio de identificação digital (Ministério da Gestão e da Inovação em Serviços Públicos, 2024; LANZA et al., 2022; SPANÓ; SILVA, 2022; BIONI et al., 2022) e utilizando a plataforma de interoperabilidade Conecta GOV.BR para a troca de dados entre órgãos governamentais (NEVES; SILVA, 2023). Iniciativas como a Carteira Digital de Trânsito (CDT) já demonstram a ampla adoção de documentos digitais com validade legal (Governo do Brasil, 2024).

Contudo, a infraestrutura brasileira difere arquitetonicamente do modelo descentralizado europeu. O ecossistema nacional estrutura-se de forma predominantemente centralizada e federada, ancorado na plataforma `gov.br` e em uma Infraestrutura de Chaves Públicas (PKI) tradicional (ICP-Brasil), instituída pela Medida Provisória nº 2.200-2/2001 (Brasil, 2001). Diante deste cenário, emerge um problema de pesquisa: a ausência de implementações práticas que validem a viabilidade técnica das tecnologias de SSI, VCs e ZKPs no contexto regulatório e infraestrutural brasileiro, e que possam servir de referência para trabalhos futuros na área.

Este trabalho se justifica pela necessidade de produzir evidências técnicas sobre o funcionamento dessas tecnologias em um ambiente que reflita as características do ecossistema brasileiro (Brasil, 2023; BABEL et al., 2025). A literatura internacional, com destaque para o modelo europeu da EUDI Wallet (GÓMEZ, 2025), consolida padrões e arquiteturas de referência. No entanto, não foram identificados trabalhos que implementem e avaliem esses padrões em um protótipo funcional voltado ao contexto de instituições brasileiras. Uma prova de conceito nesse sentido contribui para documentar as barreiras técnicas, mapear as decisões de projeto e fornecer uma base concreta sobre a qual pesquisas futuras possam avançar em direção a soluções integradas com a infraestrutura nacional.

A revisão da literatura conduzida neste trabalho examina o estado da arte das carteiras de identidade digital e evidencia uma transição tecnológica de sistemas federados para arquiteturas descentralizadas centradas no usuário. A análise dos tra-

balhos correlatos revela a consolidação de padrões abertos da web, especificamente as especificações OpenID para Emissão e Apresentação de Credenciais Verificáveis, como mecanismos dominantes para a interoperabilidade em detrimento de soluções baseadas exclusivamente em registros distribuídos permissionados. O estudo crítico das referências identifica ainda uma tensão entre a eficiência de formatos de divulgação seletiva baseados em assinaturas tradicionais e a privacidade oferecida pelas Provas de Conhecimento Zero. Apesar da existência de propostas teóricas para a integração com sistemas legados por meio de agentes de tradução, constata-se a ausência de implementações práticas que validem o funcionamento dessas tecnologias em contextos institucionais de países com infraestruturas de chaves públicas centralizadas, como a ICP-Brasil. Esta lacuna fundamenta o desenvolvimento do protótipo apresentado nesta pesquisa, que visa demonstrar a viabilidade técnica de emitir, armazenar e verificar credenciais acadêmicas utilizando padrões abertos de SSI, e servir como referência para trabalhos futuros que busquem a integração com sistemas brasileiros.

A metodologia deste trabalho é baseada em uma Revisão Sistemática da Literatura (RSL), seguindo as diretrizes propostas por Kitchenham e Charters (KITCHENHAM; CHARTERS, 2007), combinada com uma análise documental e o desenvolvimento de um protótipo funcional. A primeira etapa consiste na RSL para consolidar o conhecimento sobre SSI, VCs, DIDs, ZKPs e a EUDI Wallet, utilizando fontes acadêmicas e documentação técnica de órgãos de padronização. A segunda etapa envolve uma análise documental da legislação (Brasil, 2023; Brasil, 2022), das especificações técnicas da ICP-Brasil (Brasil, 2001), da plataforma Gov.br (Ministério da Gestão e da Inovação em Serviços Públicos, 2024) e da Arquitetura de Referência da EUDI Wallet (eIDAS Expert Group, 2023), com o objetivo de identificar os padrões tecnológicos e as restrições do cenário brasileiro. A terceira etapa consiste no desenvolvimento e avaliação de um protótipo de carteira digital acadêmica, configurado como um estudo de caso no ambiente da UFSC, para validar a viabilidade técnica da emissão, armazenamento e verificação de credenciais verificáveis utilizando as tecnologias identificadas na revisão.

Este documento está organizado da seguinte forma: O Capítulo 2 apresenta a fundamentação teórica, detalhando os conceitos de Identidade Auto-Soberana, Credenciais Verificáveis, Identificadores Descentralizados, Provas de Conhecimento Zero e a infraestrutura de chaves públicas. O Capítulo 3 descreve a metodologia da Revisão Sistemática da Literatura e os resultados obtidos, analisando as arquiteturas e os modelos propostos na literatura. O Capítulo 4 detalha a análise das especificações técnicas europeias e o mapeamento das restrições da infraestrutura de confiança digital brasileira. O Capítulo 5 formaliza a proposta de pesquisa, detalhando o processo metodológico, a seleção da pilha tecnológica e a especificação dos requisitos para a

validação da prova de conceito no cenário da UFSC. O Capítulo 6 documenta o projeto arquitetural e a codificação técnica do protótipo desenvolvido. O Capítulo 7 promove o debate sobre os resultados, os desafios de engenharia de software e as implicações de adoção e privacidade na experiência de uso. Por fim, o Capítulo 8 apresenta a conclusão da pesquisa e as indicações para trabalhos futuros.

1.1 OBJETIVOS

Para abordar a problemática apresentada, propõem-se os seguintes objetivos.

1.1.1 Objetivo geral

Demonstrar a viabilidade técnica da aplicação de tecnologias de Identidade Auto-Soberana (SSI), Credenciais Verificáveis (VCs) e Provas de Conhecimento Zero (ZKPs) no contexto institucional brasileiro, por meio do desenvolvimento e avaliação de um protótipo de carteira digital acadêmica para a Universidade Federal de Santa Catarina (UFSC).

1.1.2 Objetivos Específicos

- Analisar os fundamentos teóricos da Identidade Auto-Soberana (SSI), Credenciais Verificáveis (VCs), Identificadores Descentralizados (DIDs) e Provas de Conhecimento Zero (ZKPs).
- Examinar a arquitetura, o modelo de governança e os padrões tecnológicos da EUDI Wallet, conforme especificado pelo regulamento eIDAS 2.0 e pela Arquitetura de Referência (ARF), como referência para o estado da arte.
- Caracterizar a infraestrutura de confiança digital brasileira, com foco na ICP-Brasil e na plataforma Gov.br, identificando as restrições e características que condicionam a adoção de tecnologias SSI.
- Desenvolver um protótipo funcional de carteira digital acadêmica que implemente o ciclo completo de emissão, armazenamento e verificação de credenciais verificáveis, incluindo divulgação seletiva e provas de conhecimento zero.
- Validar o protótipo por meio de cenários de uso representativos do ambiente universitário da UFSC, documentando as decisões de projeto, barreiras técnicas e lições aprendidas.
- Identificar as lacunas técnicas e regulatórias que devem ser abordadas por trabalhos futuros para viabilizar a integração dessas tecnologias com a infraestrutura de identidade digital brasileira.

2 FUNDAMENTAÇÃO TEÓRICA

Esta seção apresenta os conceitos teóricos que fundamentam a arquitetura e a operação de carteiras de identidade digital baseadas em Identidade Auto-Soberana. Inicialmente, aborda-se a transição dos modelos de identidade digital, contrastando os sistemas centralizados e federados com o paradigma emergente da SSI, o qual prioriza o controle do usuário e a minimização de dados. Para materializar este conceito, são examinados seus principais padrões tecnológicos: os DIDs, que estabelecem uma base para identificação persistente e verificável; as VCs, que funcionam como atestados digitais portáteis e à prova de violação; e as ZKPs, um protocolo criptográfico que permite a validação de informações sem a exposição dos dados subjacentes.

2.1 IDENTIDADE DIGITAL

A identidade digital é definida tecnicamente como um conjunto de reivindicações feitas por um sujeito digital sobre si mesmo ou sobre outros sujeitos em uma rede (CAMERON, 2005). A arquitetura original da Internet foi concebida sem uma camada nativa de identidade, uma lacuna projetual que resultou na proliferação de mecanismos isolados e proprietários para a autenticação de usuários (CAMERON, 2005). Essa ausência de um metassistema unificado forçou a criação de soluções de contorno para o estabelecimento de confiança, as quais historicamente fragmentaram a experiência do usuário e ampliaram os vetores de ataque para fraudes cibernéticas devido à falta de verificabilidade consistente da origem das credenciais (ALLEN, 2016).

O primeiro estágio na evolução da gestão de identidade é denominado modelo de Identidade Centralizada. Neste paradigma, a emissão, validação e custódia dos identificadores digitais são realizadas exclusivamente por autoridades administrativas hierárquicas, como Autoridades Certificadoras (CAs) ou diretórios corporativos (ALLEN, 2016). A identidade opera sob a propriedade da entidade emissora, não do usuário, o que confere à autoridade o poder unilateral de revogação e monitoramento do uso das credenciais. Embora eficaz em domínios de segurança fechados, a centralização gerou silos de dados intransponíveis, obrigando o usuário a gerenciar múltiplos fragmentos de identidade não interoperáveis (MÜHLE et al., 2018).

A fragmentação inerente ao modelo centralizado motivou o desenvolvimento da Identidade Federada, que visa permitir a portabilidade de credenciais entre diferentes domínios de confiança. Tecnologias como SAML (Security Assertion Markup Language) e OpenID Connect permitem que um Provedor de Identidade (IdP) afirme a autenticidade de um usuário para um Provedor de Serviço (SP) externo, eliminando

a necessidade de novos registros (National Institute of Standards and Technology, 2017). Apesar de reduzir a fadiga de senhas, as federações introduzem riscos de privacidade ao concentrar o tráfego de autenticação em poucos provedores intermediários, tecnicamente capazes de correlacionar as atividades do usuário em diversos serviços (ALLEN, 2016).

A resposta às limitações de privacidade da federação surgiu com o modelo de Identidade Centrada no Usuário (User-Centric Identity). Este modelo buscou tecnicamente devolver ao indivíduo o controle sobre a escolha de seus provedores e o consentimento na partilha de atributos, exemplificado pelo protocolo OpenID original (ALLEN, 2016). Entretanto, implementações práticas enfrentaram barreiras críticas de usabilidade e segurança; estudos demonstram que arquiteturas complexas de decisão de confiança sobrecarregam cognitivamente o usuário, tornando-o suscetível a ataques de phishing e incapaz de distinguir indicadores de segurança legítimos em interfaces web (DHAMIJA; DUSSEAU, 2008).

A evolução do modelo centrado no usuário foi prejudicada pela falta de incentivos econômicos para a adoção de padrões abertos por grandes provedores, resultando na consolidação de sistemas de "login social" proprietários. Embora esses sistemas ofereçam conveniência, eles não conferem soberania técnica ao usuário, pois a persistência da identidade depende da manutenção da conta em plataformas privadas que operam sob termos de serviço unilaterais (ALLEN, 2016). A dependência de identificadores omnidirecionais nestas plataformas facilita o rastreamento transversal (cross-site tracking), violando princípios de minimização de dados ao expor metadados de navegação (CAMERON, 2005).

Em contraposição aos modelos administrados por terceiros, a SSI propõe uma arquitetura onde a identidade digital possui existência independente e é controlada exclusivamente pelo titular, sem intermediários administrativos (PREUKSCHAT; REED, 2021). A SSI fundamenta-se na premissa de que a identidade deve ser inalienável e portátil, permitindo que atributos de reputação e identidade convirjam para se tornarem ativos transacionáveis em uma economia digital, de forma análoga ao numerário físico (BIRCH, 2014). A remoção da autoridade central exige que a confiança seja estabelecida algoritmicamente entre emissor, titular e verificador.

A viabilidade técnica da SSI depende da resolução do Triângulo de Zooko, que postulava a dificuldade de criar identificadores que fossem simultaneamente descentralizados, seguros e legíveis por humanos (MÜHLE et al., 2018). A aplicação de tecnologias de registro distribuído (blockchain) permitiu a superação deste trilema ao fornecer uma infraestrutura imutável para o registro de DIDs. DIDs são identificadores globalmente únicos, resolvidos criptograficamente através de documentos DDO (DID Documents) que contêm chaves públicas, eliminando a necessidade de um diretório central para a raiz de confiança (MÜHLE et al., 2018).

Este paradigma realinha a gestão de identidade com a minimização de dados através do uso de VCs e ZKPs. Diferentemente da validação federada que exige comunicação direta com o emissor ("phone home"), o modelo SSI permite que o titular apresente provas matemáticas de atributos (como maioria) diretamente ao verificador, preservando a privacidade da transação (MÜHLE et al., 2018). A ARF da EUDI Wallet incorpora esses conceitos para viabilizar a interoperabilidade transfronteiriça, integrando a segurança criptográfica da SSI com a validade jurídica de documentos oficiais.

2.2 IDENTIDADE AUTO-SOBERANA (SSI)

A SSI é um modelo de identidade digital centrado no usuário, no qual o indivíduo mantém e controla seus próprios dados (SCHARDONG; CUSTÓDIO, 2021). Diferentemente dos modelos tradicionais, onde provedores de identidade centralizados ou federados administram as informações, a SSI devolve o controle ao indivíduo, que pode gerenciar seus próprios identificadores digitais sem depender de uma autoridade central (REECE; MITTAL, 2022). Este paradigma propõe uma mudança fundamental na arquitetura de gerenciamento de identidade, que é inerentemente insegura nos sistemas padrão (REECE; MITTAL, 2022). A SSI visa estabelecer um ecossistema aberto para autenticação e troca de informações de identidade verificáveis por máquina, onde os usuários têm total controle sobre a divulgação de seus dados (BABEL et al., 2025).

A base conceitual da SSI foi articulada por meio de dez princípios que orientam o projeto de seus ecossistemas (MÜHLE et al., 2018). Estes princípios incluem a existência independente do usuário, o controle sobre suas identidades, o acesso aos seus próprios dados, a transparência dos sistemas, a persistência, a portabilidade, a interoperabilidade, o consentimento, a minimização da divulgação de dados e a proteção de seus direitos (SOLTANI et al., 2021). A arquitetura SSI é projetada para cumprir a tríade da segurança da informação: Confidencialidade, Integridade e Disponibilidade (CIA), priorizando a segurança da informação e o controle de acesso pelo usuário (REECE; MITTAL, 2022).

A arquitetura de um sistema SSI é fundamentada em um conjunto de componentes essenciais que operam de forma descentralizada (MÜHLE et al., 2018). A interação fundamental ocorre dentro de um "triângulo de confiança" que envolve três papéis principais: o Emissor (Issuer), o Portador (Holder) e o Verificador (Verifier) (BABEL et al., 2025). O Emissor é a entidade que cria e assina digitalmente as credenciais; o Portador é o indivíduo que armazena e gerencia suas credenciais; e o Verificador é a entidade que solicita a comprovação de uma credencial (REECE; MITTAL, 2022).

Para viabilizar este modelo, são utilizadas tecnologias-chave. Os DIDs funcionam como identificadores únicos e globais, controlados criptograficamente pelos usuários, que resolvem para um Documento DID contendo chaves públicas e metadados (REECE; MITTAL, 2022). As VCs são o formato para as declarações (claims) emitidas por um Emissor sobre um Portador. Elas são digitalmente assinadas, à prova de violação e verificáveis (SOLTANI et al., 2021). O Portador armazena e gerencia seus DIDs e VCs em uma carteira digital (digital wallet), que funciona como um agente de software para executar operações criptográficas e interagir com outras partes do ecossistema (SOLTANI et al., 2021; BABEL et al., 2025).

A carteira digital é o principal componente do lado do usuário na arquitetura SSI, responsável pelo armazenamento seguro de dados de identidade e chaves criptográficas (SOLTANI et al., 2021). Ela pode ser implementada como software (aplicativo móvel, navegador) ou hardware e é usada para executar operações como geração de chaves, criação e verificação de assinaturas digitais, e backup e recuperação de chaves (REECE; MITTAL, 2022; SOLTANI et al., 2021). No fluxo de interação SSI, um Portador utiliza sua carteira para apresentar uma Prova Verificável (Verifiable Presentation) a um Verificador. Essa prova é gerada a partir de uma ou mais Credenciais Verificáveis e permite a divulgação seletiva de informações, alinhando-se ao princípio de minimização de dados (BABEL et al., 2025).

A validação criptográfica é realizada através de um Registro de Dados Verificável (VDR), que funciona como uma fonte de verdade para os metadados públicos, como os DIDs e as chaves públicas dos emissores (REECE; MITTAL, 2022). Uma tecnologia frequentemente utilizada para implementar este registro é a tecnologia de registro distribuído (DLT), como a blockchain, que atua como substituta para a autoridade de registro em sistemas clássicos de gerenciamento de identidade (MÜHLE et al., 2018).

2.3 FUNDAMENTOS CRIPTOGRÁFICOS

2.3.1 Infraestrutura de Chaves Públicas e Assinaturas Digitais

A PKI tradicional é um sistema de componentes e procedimentos que permite a gestão e utilização da criptografia de chave pública (MENEZES et al., 1996). Seu objetivo é vincular chaves públicas a identidades de entidades, como pessoas ou organizações, por meio de um mecanismo de confiança. Um dos pilares deste modelo é a CA, uma entidade terceira confiável que emite e gerencia certificados digitais (COOPER et al., 2008). Um certificado, comumente seguindo o padrão X.509, é uma estrutura de dados assinada digitalmente que atesta que uma chave pública pertence a um determinado titular (*subject*), incluindo informações como o nome do titular, o período de validade do certificado e o nome da CA emissora (COOPER et al., 2008).

O modelo de confiança da PKI tradicional é inerentemente centralizado e hierárquico. A validade de um certificado é estabelecida pela verificação da assinatura digital da CA que o emitiu. Um verificador confia no certificado de um titular porque confia na CA, que por sua vez pode ser validada por uma CA raiz superior, formando uma cadeia de confiança (COOPER et al., 2008). No entanto, essa arquitetura introduz pontos centrais de falha e gargalos de confiança. O comprometimento de uma única Autoridade Certificadora, por exemplo, pode permitir a emissão de certificados fraudulentos para qualquer entidade, comprometendo a segurança de uma vasta porção do ecossistema digital. Esta dependência de intermediários centralizados para o registro e a validação de identificadores é uma das principais vulnerabilidades que os modelos descentralizados buscam solucionar (ALLEN et al., 2015).

A principal ferramenta operacional da PKI é a assinatura digital, um mecanismo matemático que provê os serviços de autenticidade, integridade de dados e não repúdio de origem a uma mensagem digital (MENEZES et al., 1996; National Institute of Standards and Technology, 2023). Formalmente, um esquema de assinatura digital é definido por um trio de algoritmos de tempo polinomial (Gen, Sign, Vrfy). O algoritmo de geração de chaves, Gen, produz um par de chaves, uma pública (pk) e uma privada (sk). O algoritmo de assinatura, Sign, recebe a chave privada e uma mensagem para produzir uma assinatura σ . O algoritmo de verificação, Vrfy, recebe a chave pública, a mensagem e a assinatura, e retorna uma decisão (válida ou inválida) (KATZ; LINDELL, 2007). A segurança de um esquema é formalizada pela noção de ser existencialmente inforjável sob um ataque de mensagem escolhida adaptativo (EUF-CMA), que garante que um adversário não consiga forjar uma assinatura para uma nova mensagem, mesmo que ele possa obter assinaturas para mensagens de sua escolha (KATZ; LINDELL, 2007).

A segurança dos esquemas de assinatura se ancora na intratabilidade computacional de certos problemas matemáticos. Por exemplo, a segurança do esquema RSA, um dos algoritmos especificados no Padrão de Assinatura Digital (DSS) do NIST, baseia-se na dificuldade de fatorar o produto de dois números primos grandes (National Institute of Standards and Technology, 2023). Para gerar um par de chaves, selecionam-se dois primos grandes, p e q , e calcula-se o módulo $n = pq$. Em seguida, escolhe-se um expoente público e e calcula-se um expoente privado d tal que $ed \equiv 1 \pmod{\phi(n)}$, onde $\phi(n)$ é a função totiente de Euler. A assinatura σ de uma mensagem m (tipicamente, do hash da mensagem, $H(m)$) é computada como $\sigma = (H(m))^d \pmod{n}$. A verificação consiste em confirmar se $\sigma^e \pmod{n} = H(m)$. A validade desta verificação é garantida pelo Teorema de Euler. Forjar uma assinatura sem a chave privada d é computacionalmente equivalente a resolver o problema RSA, que é considerado intratável (MENEZES et al., 1996; KATZ; LINDELL, 2007).

O arcabouço legal da União Europeia, por meio do regulamento eIDAS, es-

tabelece o valor jurídico das assinaturas eletrônicas, definindo diferentes níveis de garantia. Uma "assinatura eletrônica qualificada" é aquela que é criada por um dispositivo qualificado de criação de assinaturas eletrônicas e baseia-se em um certificado qualificado. Tal assinatura tem o efeito legal equivalente ao de uma assinatura manuscrita em toda a União Europeia, provendo um alicerce de confiança legal para transações digitais (The European Parliament and the Council of the European Union, 2014). Este reconhecimento legal é fundamental para a adoção de identidades digitais em casos de uso que exigem alta segurança e validade jurídica, como os previstos para a Carteira de Identidade Digital Europeia (EUDI Wallet).

Para superar as limitações da PKI centralizada, surge o conceito de Infraestrutura de Chaves Públicas Descentralizada (DPKI), que realinha a gestão de identificadores com os princípios da SSI (ALLEN et al., 2015). Na DPKI, a raiz de confiança não é uma CA, mas sim um registro de dados verificável e descentralizado (VDR), como uma blockchain. As entidades podem gerar seus próprios identificadores e pares de chaves criptográficas de forma autônoma e registrá-los nesse livro-razão público. Este modelo elimina a dependência de intermediários centrais, devolvendo ao usuário o controle sobre sua própria identidade e mitigando o risco de pontos únicos de falha (ALLEN et al., 2015; SOLTANI et al., 2021; VITALI, 2022). No ecossistema da EUDI Wallet, este paradigma se manifesta na forma como os emissores e verificadores (*Relying Parties*) se identificam e interagem, utilizando certificados específicos como os WRPACs, que podem ser ancorados em uma infraestrutura descentralizada para garantir a interoperabilidade e a soberania do usuário (ETSI, 2025).

2.3.2 Prova de Conhecimento Zero

As ZKPs são um conjunto de protocolos criptográficos que permitem que uma parte, o provador (Prover), convença outra parte, o verificador (Verifier), da validade de uma asserção sem revelar qualquer informação subjacente além da própria validade da asserção (GOLDWASSER et al., 1985). Essa propriedade de "conhecimento zero" é formalizada pela existência de um simulador de tempo polinomial que, sem acesso à informação secreta (a "testemunha"), consegue produzir uma transcrição da interação que é computacionalmente indistinguível de uma interação real. Esta capacidade é fundamental para sistemas de identidade digital, onde a verificação de atributos ou credenciais deve ocorrer com a mínima divulgação de dados possível (European Telecommunications Standards Institute (ETSI), 2023).

Formalmente, um sistema de prova deve satisfazer três propriedades. A primeira é a Completude (Completeness), que garante que, se a asserção for verdadeira, um provador honesto sempre convencerá um verificador honesto. A segunda é a Solidez (Soundness), que assegura que, se a asserção for falsa, um provador desonesto não conseguirá convencer um verificador honesto, exceto com uma probabilidade ne-

gligenciável (RASHME, 2024; GOLDRICH; OREN, 2002). A terceira, e mais distintiva, é a propriedade de Conhecimento-Zero (Zero-Knowledge), que estipula que o verificador não aprende nada além da veracidade da declaração. Isso é demonstrado pela capacidade de um simulador gerar uma transcrição de prova indistinguível de uma prova real, sem conhecer a informação secreta (GOLDWASSER et al., 1985).

É importante notar uma distinção técnica sutil na terminologia criptográfica. Um sistema de prova possui solidez incondicional (ou estatística), o que significa que nem mesmo um provador com poder computacional infinito pode enganar o verificador, exceto com uma probabilidade desprezível. Por outro lado, um argumento possui solidez computacional, garantindo que um provador desonesto com poder computacional limitado (polinomial no tempo) não consiga criar uma prova falsa (GOLDRICH et al., 2019). A maioria dos sistemas práticos e eficientes, como os zk-SNARKs, são tecnicamente "argumentos", pois sua segurança depende de premissas computacionais (como a dificuldade de certos problemas matemáticos). Esta distinção é a razão da letra 'A' no acrônimo SNARK (Argument of Knowledge).

As Provas de Conhecimento Zero são formalizadas no contexto de sistemas de prova interativos, que modelam a interação entre um provador (P) e um verificador (V), ambos representados como máquinas de Turing. V é limitado a tempo polinomial probabilístico (PPT), enquanto P, em teoria, pode ter poder computacional ilimitado. Para uma asserção x pertencente a uma linguagem L da classe NP (para a qual P possui uma testemunha w), o protocolo deve satisfazer três condições formais. Completude (Completeness) requer que a probabilidade de um provador honesto convencer um verificador honesto seja esmagadoramente alta: $\Pr[\langle P(w), V \rangle(x) \text{ aceita}] \geq 1 - \text{negl}(k)$, onde $\text{negl}(k)$ é uma função negligenciável no parâmetro de segurança k . Solidez (Soundness) requer que a probabilidade de qualquer provador desonesto P^* convencer um verificador honesto sobre uma asserção falsa seja negligenciável: $\Pr[\langle P^*, V \rangle(x) \text{ aceita}] \leq \text{negl}(k)$. A propriedade de Conhecimento-Zero (Zero-Knowledge) é a mais complexa: para qualquer Verificador de tempo polinomial V^* (potencialmente malicioso), deve existir um simulador de tempo polinomial S que, recebendo apenas a asserção pública x (sem acesso à testemunha w), é capaz de produzir uma transcrição da interação que seja computacionalmente indistinguível de uma transcrição real gerada pela interação entre o provador honesto $P(w)$ e V^* . É esta construção teórica do simulador que garante matematicamente que a "conversa" da prova não revela nenhuma informação além da veracidade da asserção inicial (GOLDWASSER et al., 1985; GOLDRICH; OREN, 2002).

Os protocolos ZKP podem ser classificados como interativos (IZK) ou não interativos (NIZK). Nos protocolos interativos, o provador e o verificador trocam uma série de mensagens. Embora robustos, essa necessidade de comunicação online constante os torna menos práticos para muitas aplicações em sistemas distribuídos, como

carteiras digitais (RASHME, 2024). As Provas de Conhecimento Zero Não Interativas (NIZKPs) são particularmente relevantes neste contexto, pois a prova pode ser gerada pelo provador e verificada posteriormente por qualquer pessoa, a qualquer momento, sem necessidade de interação online (WU; WANG, 2014).

A transição de um protocolo interativo para um não interativo é frequentemente realizada através da heurística de Fiat-Shamir. Este método transforma protocolos interativos do tipo "public-coin" (onde os desafios do verificador são moedas aleatórias públicas) em NIZKPs, substituindo os desafios aleatórios do verificador por saídas de uma função de hash criptográfica. A função de hash é aplicada à transcrição da prova até o momento do desafio, simulando um desafio imprevisível sem a necessidade de um verificador online (FIAT; SHAMIR, 1999; DIEYE et al., 2023). Outros sistemas NIZKP operam no modelo de "common reference string" (CRS), onde uma string pública, gerada de forma confiável, é utilizada tanto para a geração quanto para a verificação da prova (BLUM et al., 2019).

No contexto das carteiras digitais e credenciais verificáveis, a principal utilidade das provas de conhecimento zero reside na capacidade de implementar a divulgação seletiva (selective disclosure) e a prova de predicados sobre atributos. Conforme analisado pela ETSI, em vez de revelar um atributo completo (como a data de nascimento), um usuário pode gerar uma ZKP que atesta a veracidade de um predicado sobre esse atributo (por exemplo, idade ≥ 18), sem expor a informação original (European Telecommunications Standards Institute (ETSI), 2023). Adicionalmente, as ZKPs permitem a desvinculação (unlinkability), impedindo que diferentes serviços (verificadores) que recebem provas de um mesmo usuário consigam correlacionar suas interações e rastrear suas atividades, preservando assim a privacidade contextual.

Para que uma asserção computacional seja provada através de um sistema ZKP moderno, como zk-SNARKs ou zk-STARKs, ela deve primeiro ser convertida em uma representação matemática padronizada. Esse processo, conhecido como aritmética, transforma a lógica de uma computação em um circuito de "gates" aritméticos (adição e multiplicação) sobre um corpo finito. O resultado é um sistema de restrições, como o Rank-1 Constraint System (R1CS), que descreve as relações entre as entradas, saídas e variáveis intermediárias da computação. A testemunha (witness) é o conjunto de valores que satisfaz todas as restrições, e é o conhecimento dessa testemunha que o provador demonstra ter (LAVIN et al., 2024).

A "configuração confiável" (trusted setup), necessária para muitas construções de zk-SNARKs, é uma cerimônia criptográfica inicial na qual são gerados os parâmetros públicos (chaves de prova e verificação) para um circuito específico. Durante este processo, é criada uma informação secreta, frequentemente chamada de "lixo tóxico" (toxic waste). A segurança do sistema depende da destruição completa e segura deste "lixo tóxico". Se qualquer participante da cerimônia reter essa informação

secreta, ele terá a capacidade de gerar provas falsas, mas que seriam aceitas como válidas pelo sistema, comprometendo toda a sua integridade (BEN-SASSON et al., 2014). A "confiança", portanto, reside na crença de que os participantes da cerimônia agiram honestamente e descartaram essa informação.

Uma limitação significativa das primeiras construções de zk-SNARKs era a necessidade de um novo trusted setup para cada computação (ou "circuito") específico que se desejava provar. Para superar essa barreira, foram desenvolvidos sistemas mais recentes, como PLONK e Marlin, que utilizam uma configuração universal e atualizável (Universal and Updatable Setup), como sumarizado em (LAVIN et al., 2024). Nesses sistemas, uma única cerimônia de configuração gera parâmetros que podem ser reutilizados para provar a execução de qualquer programa até um determinado tamanho. Isso não apenas elimina a necessidade de repetir o custoso processo para cada novo caso de uso, mas a natureza "atualizável" também permite que novos participantes contribuam para a segurança da configuração sem precisar confiar nos participantes originais, mitigando parte dos riscos associados ao modelo de confiança.

A evolução teórica das ZKPs levou à distinção entre definições de segurança. O "auxiliary-input zero-knowledge" exige que o simulador funcione mesmo que o verificador possua informações auxiliares. Já o "blackbox-simulation zero-knowledge" é um modelo mais forte, onde o simulador trata o verificador como uma "caixa preta", podendo apenas fornecer entradas e observar saídas, mas sem acesso ao seu estado interno. Foi demonstrado que a simulação de caixa preta implica o modelo de entrada auxiliar, que por sua vez implica a definição original, tornando esses sistemas robustos para composição em protocolos criptográficos maiores (GOLDREICH; OREN, 2002).

A desvinculabilidade (unlinkability) entre diferentes apresentações de credenciais também é uma propriedade de privacidade vital, que as ZKPs ajudam a garantir. A "Relying Party unlinkability" impede que diferentes verificadores (partes confiadoras) correlacionem apresentações do mesmo usuário, enquanto a "Full unlinkability" estende essa proteção contra a colusão entre verificadores e os próprios emissores das credenciais. Esquemas ZKP, como os que utilizam credenciais anônimas, são projetados para alcançar esses níveis de privacidade (European Telecommunications Standards Institute (ETSI), 2023).

Os zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) são NIZKPs que se destacam por produzirem provas de tamanho extremamente pequeno (sucintas) e de verificação muito rápida, independentemente da complexidade da computação original. A maioria das construções de zk-SNARKs requer uma configuração confiável (trusted setup) para a geração de parâmetros públicos (o CRS), um processo que, se comprometido, pode permitir a falsificação de provas (RASHME, 2024; LAVIN et al., 2024).

Como alternativa, os zk-STARKs (Zero-Knowledge Scalable Transparent Argu-

ments of Knowledge) foram desenvolvidos para oferecer transparência, eliminando a necessidade de uma configuração confiável. Eles se baseiam em primitivas criptográficas mais simples, como funções de hash resistentes à colisão, e são considerados seguros contra ataques de computadores quânticos. Suas provas são maiores que as dos zk-SNARKs, mas os tempos de prova e verificação oferecem melhor escalabilidade para computações muito grandes (BEN-SASSON et al., 2018; RASHME, 2024).

Uma terceira família de protocolos ZKP são os Bulletproofs. Eles também não requerem uma configuração confiável e produzem provas de tamanho logarítmico em relação à complexidade do circuito. Embora a verificação de uma única prova seja mais lenta do que em um zk-SNARK, eles se destacam pela eficiência na verificação em lote de múltiplas provas, tornando-os adequados para certos casos de uso, como provas de intervalo (range proofs) em transações confidenciais (RASHME, 2024; SHEYBANI et al., 2025).

Dentro do domínio da SSI, as ZKPs são empregadas para permitir que os usuários gerenciem e apresentem suas credenciais verificáveis de forma descentralizada e com preservação da privacidade. Em uma carteira SSI, o usuário armazena credenciais emitidas por diversas entidades e utiliza ZKPs para gerar apresentações seletivas, provando apenas os fatos necessários para uma transação específica, sem depender de intermediários para a validação (AGARKAR et al., 2024; DIEYE et al., 2023).

Um exemplo clássico e fundamental de ZKP é o protocolo de Schnorr, que prova o conhecimento de um logaritmo discreto (provar o conhecimento de x em

$$y = g^x$$

). Sua versão não interativa, obtida pela heurística de Fiat-Shamir, é amplamente utilizada em assinaturas digitais e esquemas de autenticação. Em uma carteira digital, pode ser usado para que o usuário prove a posse da chave privada correspondente a um identificador público, sem revelar a chave em si (DIEYE et al., 2023).

Apesar do potencial, a adoção de ZKPs em carteiras digitais enfrenta desafios práticos. A geração da prova, especialmente para esquemas complexos como zk-STARKs, pode ser computacionalmente intensiva e consumir recursos significativos do dispositivo do usuário (e.g., bateria e processamento). Além disso, o tamanho da prova e dos dados auxiliares (como o CRS) pode impactar o armazenamento e a largura de banda necessários para a comunicação (RASHME, 2024; SHEYBANI et al., 2025). A integração de ZKPs com tecnologias de registro distribuído (DLTs), como blockchain, é uma estratégia para construir sistemas de identidade mais robustos, auditáveis e com privacidade, onde a DLT serve como uma camada de confiança para âncoras de identidade e status de revogação (AGARKAR et al., 2024).

2.4 COMPONENTES E PADRÕES DA SSI

2.4.1 Identificadores Descentralizados (DIDs)

Os DIDs são um tipo de identificador globalmente único que viabiliza a identidade digital verificável e descentralizada (SPORNY et al., 2023). Um DID pode se referir a qualquer sujeito, seja uma pessoa, organização ou objeto, e é projetado para ser desacoplado de registros centralizados, provedores de identidade e autoridades certificadoras (MAZZOCCA et al., 2025). O principal objetivo de um DID é permitir que a entidade controladora do identificador possa provar seu controle sobre ele sem necessitar de permissão de terceiros, constituindo um pilar fundamental para a SSI (SPORNY et al., 2023).

A estrutura sintática de um DID é definida pela especificação do W3C e consiste em três partes: o prefixo did, que identifica o esquema URI; o nome do método (method-name); e um identificador específico do método (method-specific-id) (SPORNY et al., 2023). O método DID é um componente crucial, pois especifica como um DID e seu respectivo Documento DID são criados, resolvidos, atualizados e desativados (operações CRUD) em um Registro de Dados Verificável (VDR) subjacente, como uma blockchain ou outra DLT (STEELE; PROROCK, 2022). A escolha do método determina características essenciais do DID, como seu nível de descentralização, segurança e privacidade (ANDRIEU et al., 2022).

Um DID é projetado para ser resolvido em um Documento DID, uma estrutura de dados, comumente em formato JSON, que contém as informações necessárias para interagir com o sujeito do DID (SPORNY et al., 2023). O Documento DID expressa material criptográfico, como chaves públicas, por meio da propriedade verificationMethod. Ele também pode conter services, que são endpoints de serviço utilizados para interações, como a troca de credenciais. A resolução de um DID é o processo de obter a versão mais recente e autoritativa de seu Documento DID associado a partir do VDR (MAZZOCCA et al., 2025).

A principal função dos DIDs no ecossistema de identidade digital é servir como âncoras de confiança para VCs. O DID do emissor, por exemplo, permite que um verificador localize a chave pública correspondente no Documento DID do emissor para validar a assinatura digital da credencial. Da mesma forma, o DID do sujeito da credencial (o portador) é incluído na VC para identificá-lo de forma única e inequívoca. Esta interdependência é a base operacional da DPKI introduzida anteriormente, permitindo que a confiança seja estabelecida diretamente entre as partes (MAZZOCCA et al., 2025).

No contexto da Carteira de Identidade Digital Europeia (EUDIW), a arquitetura proposta pelo regulamento eIDAS 2.0 adota os princípios da SSI, onde DIDs e VCs são tecnologias fundamentais. A arquitetura de referência da EUDIW prevê que cada

carteira seja associada a um DID, permitindo que os cidadãos europeus armazenem e apresentem suas credenciais (como a Identidade Pessoal ou a carteira de motorista móvel) de forma segura e com controle total sobre seus dados (MAZZOCCA et al., 2025). O uso de DIDs e VCs padronizados pelo W3C visa garantir a interoperabilidade, segurança e portabilidade da identidade digital em todo o bloco europeu (eIDAS Expert Group, 2023).

2.4.2 Credenciais Verificáveis

As VCs representam um formato padrão para a expressão de atestados (claims) digitais que são criptograficamente seguros, com respeito à privacidade e verificáveis por máquinas (Verifiable Credentials Working Group, 2025). Uma VC é definida como uma reivindicação digital à prova de adulteração sobre um determinado sujeito, que pode ser apresentada a outras partes (verificadores) sem a necessidade de envolver o emissor original da credencial (Verifiable Credentials Working Group, 2025). Este modelo foi proposto pelo W3C para facilitar a expressão e a verificação de credenciais de terceiros na Internet, como passaportes ou diplomas, de uma forma padronizada e interoperável (SPORNY et al., 2025).

As VCs funcionam, conceitualmente, como contêineres digitais. A prova criptográfica atua como um selo inviolável que garante a integridade do contêiner e a autenticidade de sua origem (o emissor), mas não valida a veracidade intrínseca de seu conteúdo. Essa separação é fundamental: a tecnologia provê a integridade da credencial, enquanto a decisão de confiar nos dados contidos nela permanece com o verificador, baseada em sua confiança no emissor (PREUKSCHAT; REED, 2021).

As VCs são um componente central no paradigma da SSI, um modelo que visa devolver aos indivíduos o controle sobre suas próprias identidades digitais (PREUKSCHAT; REED, 2021). Nesse contexto, as VCs funcionam como as manifestações digitais de atributos de identidade e qualificações. A arquitetura de uma solução baseada em SSI é composta por sete tecnologias-chave definidas pelo W3C, que incluem DIDs, Credenciais Verificáveis, DPKI, Blockchain, VDRs, Agentes e Carteiras Digitais (SCHARDONG; CUSTÓDIO, 2021).

A relação entre Emissor, Portador e Verificador é a base de todo o ecossistema de confiança da SSI. Diferentemente de modelos federados, onde a confiança é mediada por um provedor de identidade, o modelo de VCs permite que o Verificador confie diretamente no Emissor, com o Portador atuando como o canal de transmissão. Essa confiança é ancorada criptograficamente, de modo que o Verificador possa confirmar que a credencial foi de fato emitida pela entidade declarada e não foi alterada, estabelecendo um canal de confiança que independe da intermediação de terceiros no momento da verificação (PREUKSCHAT; REED, 2021).

O Modelo de Dados de Credenciais Verificáveis (VCDM) do W3C define a

estrutura fundamental de uma VC. Essa estrutura é composta por metadados da credencial, alegações sobre um ou mais sujeitos (encapsuladas no objeto `credentialSubject`) e uma ou mais provas criptográficas (SPORNY et al., 2025). A representação desses dados é tipicamente feita em formato JSON-LD, que permite a extensibilidade semântica através de contextos, garantindo que as alegações possam ser compreendidas de forma interoperável por diferentes sistemas (Verifiable Credentials Working Group, 2025). Esta estrutura assegura que a VC seja um contêiner de dados portátil e autocontido.

A segurança e a verificabilidade de uma VC são garantidas por uma prova criptográfica. O modelo do W3C especifica dois mecanismos principais para associar essa prova a uma credencial: provas encapsuladas (*enveloping proofs*) e provas incorporadas (*embedded proofs*) (Verifiable Credentials Working Group, 2025). As provas encapsuladas, como as baseadas em JSON Web Tokens (JWT), "envolvem" a credencial como uma carga útil assinada. Já as provas incorporadas, como as especificadas no padrão Data Integrity, são adicionadas como um objeto `proof` dentro da própria estrutura da credencial.

O objeto `proof` em uma prova incorporada contém metadados essenciais para a verificação criptográfica. Estes incluem o tipo da prova (`type`), a data de criação (`created`), o propósito da prova (`proofPurpose`), o valor da prova criptográfica (`proofValue`) e uma referência ao método de verificação (`verificationMethod`) (SPORNY et al., 2025). O `verificationMethod` geralmente aponta para a chave pública do emissor, que por sua vez é encontrada por meio da resolução do seu Identificador Descentralizado (DID), ligando a credencial a uma âncora de confiança descentralizada.

A utilização de um DID como `verificationMethod` permite que a chave pública do emissor seja descoberta em um registro de dados verificável, materializando a operação da DPKI. Nesse modelo, o emissor controla suas próprias chaves e pode rotacioná-las sem depender de uma CA centralizada, resolvendo um dos principais gargalos dos sistemas de PKI tradicionais (PREUKSCHAT; REED, 2021).

Para o compartilhamento de credenciais, o portador utiliza uma Apresentação Verificável (VP). Uma VP é uma estrutura de dados que encapsula uma ou mais VCs e é assinada pelo portador para ser enviada a um verificador. A VP permite ao portador agregar credenciais de diferentes emissores e provar seu controle sobre elas, ao mesmo tempo que possibilita a divulgação seletiva de informações (Verifiable Credentials Working Group, 2025). Assim, a VP serve como um envelope para a transmissão segura e contextualizada dos dados da credencial.

Um dos principais benefícios de privacidade das VCs é a capacidade de divulgação seletiva (*selective disclosure*), que permite ao portador revelar apenas um subconjunto das alegações contidas em uma credencial, sem invalidar a assinatura criptográfica do emissor. Formatos como o Selective Disclosure for JWTs (SD-JWT)

foram desenvolvidos para este fim. Neste mecanismo, algumas alegações são substituídas por seus hashes na credencial principal, e os valores originais são fornecidos separadamente ao verificador, que pode então reconstruir e verificar apenas as informações reveladas (FETT et al., 2024).

Apesar dos avanços, os mecanismos de assinatura padrão, como o ECDSA, apresentam limitações de privacidade. Como as assinaturas ECDSA são únicas e imutáveis, elas permitem que um verificador rastreie um portador simplesmente monitorando as assinaturas apresentadas (FLAMINI et al., 2024). Isso cria um vetor de correlação que compromete a privacidade do usuário. Tecnologias alternativas, como as assinaturas BBS+, foram propostas para mitigar esse problema, pois possuem a capacidade de "cegagem" (blinding), randomizando a assinatura a cada apresentação e impedindo a vinculação entre elas (LOOKER et al., 2026).

Para alcançar garantias de privacidade ainda mais fortes, as ZKPs podem ser integradas ao ecossistema de VCs. Um ZKP permite a um provador (o portador da credencial) convencer um verificador de que uma afirmação sobre sua credencial é verdadeira, sem revelar nenhuma informação além da validade da própria afirmação (GOLDWASSER et al., 1985). Por exemplo, um usuário pode provar que tem mais de 18 anos sem revelar sua data de nascimento, cumprindo o princípio da minimização de dados do GDPR de forma robusta (ZEIN; PINKWART, 2025).

A implementação de VCs baseadas em ZKPs de propósito geral, como zk-SNARKs, requer adaptações técnicas ao formato da credencial. Uma vez que as operações de verificação de assinatura e análise de dados devem ser expressas como circuitos aritméticos, analisar uma estrutura complexa como um JSON-LD dentro de um circuito é computacionalmente caro. Uma abordagem prática é introduzir uma nova alegação na VC, como uma raiz de uma Merkle tree (zk root), que agrega criptograficamente todas as outras alegações da credencial. O emissor então assina essa raiz. O portador, ao gerar a prova ZKP, pode reconstruir eficientemente essa raiz dentro do circuito a partir das alegações privadas, provando a posse e a integridade da credencial original de uma forma compatível com ZKP (BEN-SASSON et al., 2014).

A revogação de credenciais é outro desafio crítico. Modelos simples, como a verificação de um identificador da credencial em uma lista de revogação, podem criar problemas de privacidade, pois permitem que o emissor rastreie o uso da credencial. Para resolver isso, foram propostos mecanismos de revogação que preservam a privacidade e são à prova de adulteração. Uma abordagem combina o uso de acumuladores criptográficos com blockchain. O emissor publica o estado do acumulador (que representa o conjunto de credenciais não revogadas) na blockchain, e o portador pode gerar uma prova de não-inclusão em ZKP para demonstrar que sua credencial não está na lista de revogadas, sem revelar qual credencial possui (CAMENISCH; LYSYANSKAYA, 2002).

Em última análise, a combinação de VCs com DIDs, carteiras digitais e agentes de software materializa a promessa da SSI: devolver ao indivíduo a soberania sobre sua identidade digital. A capacidade de manter credenciais portáteis, apresentá-las de forma seletiva e contextual, e gerenciar a confiança em uma base peer-to-peer representa uma mudança de paradigma fundamental em relação aos modelos de identidade centralizados e federados que dominaram a era da Web 2.0 (PREUKSCHAT; REED, 2021).

3 REVISÃO DA LITERATURA

Este capítulo apresenta uma RSL sobre o estado da arte global em carteiras de identidade digital. O objetivo é consolidar o conhecimento existente sobre arquiteturas, tecnologias e modelos de governança propostos na literatura internacional. Os resultados desta revisão fornecem a base teórica e tecnológica para o desenvolvimento do protótipo de carteira digital acadêmica, além de permitir a identificação das lacunas que este trabalho busca abordar e das questões que permanecem em aberto para pesquisas futuras.

3.1 METODOLOGIA

A presente Revisão Sistemática da Literatura foi conduzida com base na metodologia proposta por Kitchenham (KITCHENHAM; CHARTERS, 2007). Para nortear a busca e a análise dos trabalhos, foram formuladas as seguintes perguntas de pesquisa (PQs):

- PQ1:** Quais são as principais propostas de arquitetura de carteiras de identidade digital na literatura?
- PQ2:** Quais são as principais tecnologias e padrões utilizados em implementações de carteiras de identidade digitais?
- PQ3:** Quais são os modelos de governança e regulamentação para carteiras digitais propostos na literatura?

As perguntas PQ1, PQ2 e PQ3 foram o foco principal desta revisão, visando estabelecer uma compreensão do panorama global. O processo de busca bibliográfica foi conduzido entre 18 de outubro e 20 de novembro, período no qual todas as consultas às bases de dados selecionadas foram executadas e documentadas. A query de busca foi a mesma entre todas as bases de dados.

3.1.1 Estratégia de Busca

A estratégia de busca foi definida a partir da decomposição das perguntas de pesquisa em conceitos principais e seus sinônimos em inglês. A Tabela 1 detalha os termos utilizados para a construção da string de busca.

A partir dos termos definidos, foi construída a seguinte query de busca, aplicada às bases de dados selecionadas:

```
("Digital Identity Wallet" OR "Identity Wallet" OR "EU Digital Wallet" OR "EUDI Wallet") AND ("Architecture" OR "Framework" OR "Model" OR "Standard" OR "Governance")
```

Tabela 1 – Palavras-chave e sinônimos utilizados na busca.

Tema	Palavras-Chave (Inglês)
<i>Carteira de Identidade Digital</i>	"Digital Identity Wallet", "Identity Wallet", "EU Digital Wallet", "EUDI Wallet"
<i>Arquitetura e Padrões</i>	"Architecture", "Framework", "Model", "Standard", "Interoperability"
<i>Governança e Regulação</i>	"Governance", "Regulation"

A busca foi realizada nas seguintes bases de dados acadêmicas: ACM Digital Library, IEEE Xplore, ScienceDirect, SpringerLink e Google Scholar.

3.1.2 Critérios de Inclusão e Exclusão

Foram aplicados os seguintes critérios de inclusão: (i) artigos publicados nos últimos cinco anos; (ii) trabalhos completos (full papers) de pesquisa; e (iii) disponibilidade em formato PDF; e (iv) trabalhos acessíveis gratuitamente por meio dos mecanismos institucionais usuais de pesquisa, incluindo acesso via redes privadas virtuais acadêmicas, autenticação federada (CAFe) ou plataformas disponibilizadas pela CAPES. Foram excluídos trabalhos que não se enquadravam como artigos de pesquisa, como resenhas de livros, editoriais e artigos curtos (short papers).

3.1.3 Processo de Seleção

O processo de seleção dos estudos foi realizado em quatro etapas sequenciais:

1. **Análise de Títulos:** Leitura dos títulos dos artigos para excluir aqueles claramente fora do escopo.
2. **Remoção de trabalhos duplicados:** São removidas cópias dos trabalhos que já foram encontrados em outra ferramenta de busca.
3. **Análise de Resumos:** Leitura dos resumos dos artigos restantes para avaliar a relevância em relação às perguntas de pesquisa.
4. **Leitura Completa:** Leitura integral dos artigos selecionados na etapa anterior para extração de dados e confirmação final de sua inclusão.

3.2 RESULTADOS DA PESQUISA

A aplicação da estratégia de busca nas bases de dados selecionadas resultou em um conjunto inicial de trabalhos, que foi subsequentemente refinado por meio do

processo de filtragem. A Tabela 2 sumariza os resultados quantitativos de cada etapa do processo.

Tabela 2 – Resultados do processo de busca e seleção de artigos.

Base de Dados	Resultados Iniciais	Filtro Título	Filtro Resumo	Final
ACM Digital Library	26	15	11	9
IEEE Xplore	13	11	9	9
ScienceDirect	38	14	8	8
SpringerLink	16	5	3	2
Research Gate	79	10	5	3
Google Scholar	59	13	10	9
Total	231	68	46	40

3.3 ANÁLISE DOS TRABALHOS SELECIONADOS

A partir do conjunto final de artigos selecionados, foi conduzida uma análise qualitativa para extrair as contribuições, tecnologias e lacunas relevantes para esta pesquisa. Para facilitar a compreensão e organizar as tendências encontradas, a análise foi estruturada em cinco eixos temáticos principais. O agrupamento visa consolidar o conhecimento sobre aspectos específicos das carteiras de identidade digital, desde a integração com sistemas existentes até os desafios de governança e segurança.

3.3.1 Integração com Sistemas Legados e Interoperabilidade Técnica

Esta seção agrupa os trabalhos que investigam os desafios e soluções para conectar a nova infraestrutura de identidade descentralizada com os sistemas de gestão de identidade e acesso (IAM) já existentes, bem como a interoperabilidade técnica entre diferentes domínios.

Integração SSI-OIDC via Ory Hydra

Hoops e Matthes (2024) propõem uma arquitetura de ponte SSI-para-OIDC projetada para abstrair a complexidade da autenticação descentralizada para serviços que operam sobre protocolos legados como OpenID Connect e OAuth 2.0. O sistema atua como um intermediário que se comporta como um Identity Provider (IdP) autoritativo para a aplicação cliente, enquanto executa os protocolos de verificação descentralizada com a carteira do usuário. A implementação técnica fundamenta-se no servidor OIDC open-source Ory Hydra, responsável por gerenciar o fluxo de código de autorização OAuth 2.0 com o serviço legado.

Para a interação com a carteira digital, o sistema emprega os protocolos OpenID for Verifiable Presentations (OID4VP) e Self-Issued OpenID Provider v2 (SIOPv2),

viabilizando fluxos cross-device onde a sessão é iniciada em um desktop e autenticada via leitura de QR Code em dispositivo móvel. Um componente crítico da arquitetura é o tradutor de políticas, que converte configurações de login locais, definidas em JSON, para o padrão DIF Presentation Exchange, instruindo a carteira sobre quais atributos apresentar. O processador de claims suporta credenciais no formato JSON-LD emitidas via métodos como did:web e realiza a verificação de revogação utilizando o esquema de bitstring StatusList2021. A validação experimental foi conduzida utilizando a Altme Wallet, confirmando a capacidade de mapear atributos verificados para tokens OIDC (id_token) padrão.

Apesar de viabilizar a integração sem refatoração dos sistemas legados, a arquitetura apresenta limitações arquiteturais relevantes. O modelo impõe um simple holder binding, o que impede o usuário de apresentar, em uma única transação, credenciais que tenham sido emitidas para DIDs distintos sob seu controle, restringindo a flexibilidade de composição de identidade. Além disso, ao centralizar a verificação no bridge, o sistema reintroduz um ponto único de confiança e falha; o serviço legado precisa confiar cegamente que a ponte validou a criptografia corretamente, perdendo a garantia matemática fim-a-fim (verificabilidade pelo Relying Party) que é nativa do modelo SSI.

Integração de Provedor SSI ao Keycloak

Castellano et al. (2024) desenvolvem e avaliam uma implementação prática de um provedor SSI integrado ao Keycloak, uma das soluções de Gestão de Identidade e Acesso mais utilizadas no meio acadêmico. A proposta visa habilitar o suporte ao ecossistema da Carteira de Identidade Digital Europeia sem exigir alterações nos Provedores de Serviço, que continuam operando via OIDC padrão. A arquitetura técnica é híbrida e composta por uma extensão nativa do Keycloak baseada na Service Provider Interface desenvolvida em Java e empacotada como arquivo .jar. Este componente opera em conjunto com uma aplicação auxiliar externa desenvolvida em Next.js. Esta aplicação web atua como a interface frontal do fluxo de verificação e gerencia a exibição do QR Code e a interação com a carteira, enquanto a extensão no Keycloak orquestra a sessão federada.

O fluxo de autenticação utiliza o protocolo OpenID for Verifiable Presentations. Nos experimentos realizados, o sistema foi validado utilizando a versão Android da implementação de referência da Carteira EUDI e credenciais no formato mDoc conforme a norma ISO/IEC 18013-5, especificamente o conjunto de dados de identificação pessoal PID. A infraestrutura foi implantada utilizando Docker e demonstrou a capacidade da versão 24.0.0 do Keycloak de mapear atributos verificados da carteira, como idade e nacionalidade, diretamente para tokens de acesso OIDC consumíveis por aplicações legadas.

Apesar de funcional, a abordagem apresenta limitações arquiteturais e de privacidade. A necessidade de um serviço Next.js separado para intermediar a apresentação adiciona complexidade de manutenção e latência ao fluxo de login, o que desvia da arquitetura monolítica padrão do Keycloak. De forma mais crítica, ao atuar como uma ponte, o Keycloak decifra e processa os dados pessoais do usuário antes do repasse à aplicação final. Isso implica a quebra da privacidade de ponta a ponta, pois o usuário precisa confiar que o servidor de gestão de identidade não armazenará registros dos atributos apresentados. Tal característica difere de modelos onde a verificação criptográfica ocorre diretamente no dispositivo do cliente na borda da rede ou na aplicação final.

Agentes de Tradução para Controle de Acesso Baseado em Atributos (ABAC)

Kudra et al. (2025) sistematizam a experiência de doze projetos-piloto de identidade digital na Europa e propõem um roteiro para a adoção de carteiras digitais em ambientes corporativos. O foco técnico do trabalho reside na reestruturação dos sistemas de Gestão de Identidade e Acesso Organizacional para suportar o Controle de Acesso Baseado em Atributos, ou ABAC. Essa mudança permite que permissões sejam concedidas dinamicamente com base em atestados verificáveis apresentados pela carteira do usuário, como diplomas ou licenças profissionais, em substituição ao modelo estático de Controle de Acesso Baseado em Papéis.

Para viabilizar a interoperabilidade com infraestruturas legadas que não suportam nativamente a verificação de credenciais, os autores introduzem o conceito arquitetural de Agentes de Tradução. Esses componentes de middleware atuam como intermediários que solicitam e validam as apresentações criptográficas da carteira e subsequentemente convertem os dados verificados para formatos de token tradicionais, como SAML ou asserções OIDC, consumíveis pelas aplicações internas. O estudo de caso também destaca barreiras críticas de hardware e aponta que a falta de padronização no acesso ao chip NFC e ao Elemento Seguro dos smartphones impediu a implementação de casos de uso offline em dispositivos pessoais heterogêneos e forçou o uso de hardware corporativo específico em projetos de controle de acesso físico.

Apesar de oferecer um guia estratégico valioso baseado em falhas e sucessos reais, o trabalho possui limitações para fins de engenharia de software. A proposta dos Agentes de Tradução é apresentada como um conceito funcional e carece de especificações técnicas detalhadas ou implementações de referência de código aberto. O artigo não aborda como esses agentes devem gerenciar o mapeamento de confiança entre emissores externos e políticas internas de segurança, nem define os protocolos exatos para a comunicação segura entre o agente e o sistema legado, o que deixa a operacionalização técnica dessa ponte como uma lacuna de implementação.

Descentralização da Infraestrutura Crítica do X-Road

Bakhtina et al. (2023) desenvolvem uma prova de conceito para descentralizar a infraestrutura de chave pública do sistema X-Road, a camada de troca de dados que serve como espinha dorsal dos serviços digitais na Estônia e em outros países. O objetivo central é substituir a dependência de Autoridades de Certificação centralizadas e certificados X.509 por uma arquitetura baseada em Identidade Auto-Soberana. A implementação técnica integra os componentes legados do X-Road, desenvolvidos em Java com Spring Boot, ao ecossistema Hyperledger. O framework Aries Cloud Agent Python, conhecido como ACA-Py, é utilizado como o agente de identidade responsável pelo gerenciamento de chaves e carteiras em cada nó da rede.

A solução adota o método DID `did:sov` sobre uma rede Hyperledger Indy para o registro imutável de identificadores e esquemas de credenciais. Para a emissão e verificação, o estudo emprega o formato AnonCreds, que habilita nativamente o uso de Provas de Conhecimento Zero e registros de revogação distribuídos baseados em acumuladores criptográficos. A comunicação segura entre os Servidores de Segurança das organizações é estabelecida através do protocolo DIDComm, o que substitui a autenticação mútua TLS tradicional e elimina a necessidade de validação via protocolo OCSP. O sistema demonstra funcionalmente como o processo de integração de novos membros pode ser automatizado através da verificação de credenciais de adesão assinadas digitalmente, sem intervenção manual de um operador central.

Apesar de demonstrar a viabilidade técnica de migrar uma infraestrutura nacional crítica para DPKI, a solução apresenta um forte acoplamento com o ecossistema Hyperledger Indy e o formato AnonCreds. Essa característica cria uma barreira de interoperabilidade com os padrões emergentes na Europa sob o eIDAS 2.0, que convergem para arquiteturas baseadas em OpenID4VP e ISO/IEC 18013-5. Outra limitação crítica é a complexidade operacional introduzida, pois exige que cada organização participante, independentemente de seu porte técnico, mantenha e opere sua própria instância do agente ACA-Py com alta disponibilidade. Além disso, o protocolo de não-repúdio implementado sobre DIDComm é uma solução customizada pelos autores e carece de padronização formal, o que dificulta a auditoria de segurança externa e a adoção em larga escala.

Sistemas de Interoperabilidade para Serviços Transfronteiriços Móveis

O trabalho de Corici et al. (2022) apresenta a arquitetura de referência do projeto mGov4EU, que visa integrar o regulamento Single Digital Gateway e o ecossistema eIDAS para habilitar serviços públicos móveis transfronteiriços. O desafio técnico central abordado é a incompatibilidade entre a infraestrutura de identidade europeia existente, baseada predominantemente no protocolo SAML2 e projetada para

navegadores desktop, e os requisitos modernos de aplicações móveis que demandam protocolos mais leves como OpenID Connect. Para solucionar essa dicotomia, os autores propõem uma arquitetura modular baseada no modelo C4, introduzindo camadas de software intermediárias denominadas Sistemas de Interoperabilidade.

No componente de troca de dados governamentais, a solução utiliza o perfil de mensagem AS4 do framework eDelivery para o transporte seguro e agnóstico de carga útil entre os nós nacionais. Para a descoberta dinâmica de provedores de dados, é empregado o Service Metadata Protocol. Uma inovação significativa do trabalho é a aplicação do padrão User Managed Access 2.0, uma extensão do framework de autorização OAuth 2.0. Esse mecanismo permite que o gerenciamento de consentimento para o acesso a evidências (como diplomas ou registros de residência) seja dissociado da transação de acesso em si, permitindo que o cidadão gerencie políticas de acesso de forma assíncrona e centralizada antes que o token de acesso seja emitido para a carteira digital ou para terceiros.

Apesar de fornecer um caminho viável para a migração de serviços legados, a arquitetura proposta introduz uma complexidade operacional considerável devido à dependência de múltiplos intermediários de tradução de protocolo. O Sistema de Interoperabilidade eID atua efetivamente como um proxy reverso que encapsula a complexidade do SAML2 e expõe interfaces OpenID Connect para o dispositivo móvel. Essa abordagem centralizada de adaptação contrasta com modelos de identidade auto-soberana mais puros, onde a interoperabilidade é resolvida no nível da credencial e não no transporte. Além disso, o trabalho identifica mas não soluciona tecnicamente o problema da correspondência de identidade ou Identity Matching, onde a variação de atributos identificadores entre diferentes Estados-Membros impede a vinculação automática de registros sem intervenção manual ou heurísticas falíveis.

Convergência de Carteiras Web3 para Identidade Off-Chain

Kersic et al. (2023) propõem uma arquitetura de convergência entre carteiras de ativos digitais baseadas em blockchain, denominadas on-chain, e carteiras de identidade auto-soberana, denominadas off-chain. A implementação de referência estende a popular carteira Web3 MetaMask através do recurso MetaMask Snaps, que permite a execução de código JavaScript em um ambiente isolado dentro da extensão do navegador. Para as funcionalidades de identidade descentralizada, o protótipo integra o framework Veramo, o que habilita a gestão de Identificadores Descentralizados e a verificação de Credenciais Verificáveis sem a necessidade de instalar um aplicativo dedicado adicional.

A solução técnica adota o método DID did:pkh para vincular a identidade off-chain ao endereço público da rede Ethereum e garante a consistência entre os identificadores. A assinatura de credenciais e apresentações utiliza o padrão EIP-712 para

assegurar a legibilidade dos dados estruturados assinados pelo usuário. A validação do sistema foi realizada através de um caso de uso de votação em Organizações Autônomas Descentralizadas na plataforma Snapshot, na qual o direito de voto foi condicionado à apresentação de uma credencial acadêmica armazenada localmente e verificada via IPFS, em substituição ao modelo puramente plutocrático baseado na posse de tokens.

Apesar de reduzir a fricção de usabilidade, a abordagem apresenta riscos de segurança significativos ao unificar a gestão de chaves. O comprometimento da chave privada mestra da carteira MetaMask resulta na perda simultânea de ativos financeiros e da identidade digital do usuário e cria um ponto único de falha crítico. Além disso, a dependência estrita da infraestrutura de plugins da MetaMask gera um acoplamento com um fornecedor específico, o que contradiz os princípios de neutralidade tecnológica da identidade auto-soberana. Por fim, o uso de padrões centrados no ecossistema Ethereum diverge das especificações baseadas em ISO/IEC 18013-5 e OpenID4VP que norteiam a Carteira de Identidade Digital Europeia, o que limita a interoperabilidade da solução com serviços públicos governamentais.

Preservação de Privacidade em Federação de Identidade

Bumiller et al. (2025) conduzem um mapeamento sistemático da literatura e uma revisão sistemática sobre a Federação de Identidade com Preservação de Privacidade, analisando a evolução das técnicas de mitigação de rastreamento em sistemas federados ao longo da última década. O estudo categoriza as abordagens técnicas para garantir requisitos como não-vinculabilidade e desvinculabilidade em dois grupos principais: técnicas criptográficas avançadas, como Provas de Conhecimento Zero e Computação Multipartidária Segura, e métodos de gestão de acesso baseados em atributos. A análise dos padrões de referência revela uma predominância do protocolo OpenID Connect, utilizado em 48% das propostas analisadas, seguido pelo SAML com 26%, enquanto os modelos de Credenciais Verificáveis do W3C aparecem em apenas 4% dos trabalhos, o que indica uma lacuna na adoção de padrões de identidade auto-soberana em pesquisas de federação.

Os autores identificam que a maioria das propostas acadêmicas falha em alinhar-se com infraestruturas produtivas. Estatisticamente, 75% das soluções de privacidade analisadas são desenvolvidas do zero, sem estender padrões existentes, o que inviabiliza sua integração em ecossistemas reais. Além disso, o estudo aponta uma negligência sistemática quanto à usabilidade, com 70% dos artigos ignorando o impacto das técnicas de privacidade no comportamento do usuário final. Para o contexto deste trabalho, a revisão serve como um alerta contra o desenvolvimento de protocolos proprietários e reforça a necessidade de utilizar extensões padronizadas, como OpenID for Verifiable Presentations, para garantir que a introdução de creden-

ciais verificáveis na infraestrutura universitária não resulte em uma solução isolada e inutilizável.

Discussão e Relevância para o Trabalho

A literatura sobre a integração de identidade descentralizada com sistemas legados converge para uma estratégia arquitetural predominante: o uso de componentes intermediários, ou middlewares, que atuam como pontes de tradução de protocolos. Hoops e Matthes (2024) e Castellano et al. (2024) demonstram a viabilidade prática dessa abordagem ao estenderem provedores OIDC consolidados, respectivamente Ory Hydra e Keycloak, para aceitarem Credenciais Verificáveis. Contudo, a análise crítica dessas implementações revela uma falha de privacidade inerente ao modelo de ponte. Ao terminar a conexão criptográfica no servidor intermediário e não na aplicação final, ambos os sistemas decifram os dados do usuário dentro do perímetro da infraestrutura de TI, o que reintroduz a necessidade de confiança em uma autoridade central e viola o princípio de verificação ponta a ponta da identidade auto-soberana.

Sob uma perspectiva de gestão organizacional, Kudra et al. (2025) formalizam a necessidade desses intermediários através do conceito de Agentes de Tradução, essenciais para migrar sistemas de controle de acesso baseados em papéis para modelos baseados em atributos sem refatoração massiva. Entretanto, a ausência de especificações técnicas abertas para esses agentes nos estudos de caso apresentados constitui uma lacuna que permanece em aberto. O protótipo desenvolvido neste trabalho não implementa essa camada de integração, mas documenta as interfaces e os pontos de extensão necessários para que trabalhos futuros abordem a integração com os sistemas de gestão acadêmica existentes.

No âmbito das infraestruturas de alta complexidade, Bakhtina et al. (2023) e Corici et al. (2022) oferecem modelos para ambientes governamentais e transfronteiriços. Embora Bakhtina et al. (2023) provem que é possível descentralizar sistemas críticos como o X-Road usando Hyperledger Indy, a complexidade operacional de manter agentes ACA-Py em cada nó da rede mostra-se proibitiva para instituições com recursos limitados. Por outro lado, a arquitetura proposta por Corici et al. (2022) depende excessivamente de proxies para habilitar o suporte móvel em infraestruturas legadas como a rede eIDAS, sugerindo que uma abordagem mais leve e direta, focada na borda, pode ser mais eficiente para o contexto de um campus universitário.

A convergência entre carteiras de criptoativos e identidade, explorada por Kersic et al. (2023), apresenta um caminho para reduzir a fricção de usabilidade através da extensão de carteiras Web3 populares como a MetaMask. Todavia, os riscos de segurança identificados, notadamente o comprometimento simultâneo de ativos financeiros e identidade em caso de vazamento de chaves, sugerem que o protótipo da

UFSC deve priorizar carteiras de identidade dedicadas ou arquiteturas que isolem as chaves de assinatura das chaves de gestão de ativos.

Finalmente, a revisão sistemática de Bumiller et al. (2025) serve como um alerta metodológico para o desenvolvimento do protótipo. A constatação de que 75% das soluções de privacidade na literatura são desenvolvidas sem aderência a padrões, e que 70% ignoram a usabilidade, orienta este trabalho a adotar especificações abertas e a considerar o impacto da latência das provas criptográficas na experiência do usuário. O estado da arte indica que a construção de implementações práticas que utilizem padrões consolidados e documentem as barreiras técnicas encontradas constitui uma contribuição para o avanço da área, particularmente em contextos institucionais que ainda não dispõem de implementações de referência.

3.3.2 Governança, Confiança e Regulação (eIDAS 2.0)

Esta seção agrupa os trabalhos que discutem os aspectos jurídicos, os modelos de confiança, os processos de certificação e o papel do Estado e das regulações (especificamente o eIDAS 2.0) na estruturação de ecossistemas de identidade digital.

Credenciamento Automatizado de Provedores de Serviço na Carteira

More et al. (2024) propõem uma arquitetura de confiança para ecossistemas de identidade digital focada na regulação técnica dos Verificadores ou Provedores de Serviço. O trabalho parte da premissa de que o consentimento do usuário é insuficiente para garantir a privacidade, pois os titulares carecem de conhecimento jurídico para avaliar a necessidade e a legalidade das solicitações de dados feitas por serviços online. Para solucionar esse problema de assimetria de informação, os autores introduzem um sistema de Credenciamento de Provedores de Serviço, no qual uma Autoridade de Credenciamento emite certificados digitais X.509 que contêm restrições de acesso legíveis por máquina. Essas restrições definem explicitamente quais credenciais, atributos ou predicados um serviço específico está autorizado a solicitar com base na sua função e conformidade regulatória.

A inovação central da proposta reside na delegação da verificação de conformidade para o software da carteira digital, que atua como um ponto de aplicação de políticas automatizado. Antes de apresentar qualquer solicitação de consentimento ao usuário, a carteira valida criptograficamente o certificado do Provedor de Serviço e confronta a solicitação de dados atual com as restrições embutidas no certificado. Se o serviço solicitar mais dados do que o permitido pelo seu nível de credenciamento, a carteira bloqueia a transação automaticamente. O modelo suporta granularidade fina, permitindo restringir o acesso apenas a provas de conhecimento zero em vez de atributos brutos, o que força tecnicamente a adesão ao princípio de minimização de dados da GDPR e do eIDAS 2.0.

Para mitigar os riscos de centralização e abuso de poder pela Autoridade de Credenciamento, a arquitetura incorpora um mecanismo de transparência baseado em registros públicos auditáveis, similar ao Certificate Transparency da Web PKI. As decisões de credenciamento são registradas em estruturas de dados imutáveis baseadas em Árvores de Merkle. Durante o protocolo de apresentação, a carteira exige que o Provedor de Serviço forneça uma Prova de Inclusão, como um Signed Certificate Timestamp, garantindo que o certificado utilizado é público e auditável por entidades de fiscalização. Isso cria um modelo de segurança reativo onde comportamentos maliciosos da autoridade ou do serviço podem ser detectados e auditados por terceiros.

Apesar de oferecer um modelo robusto para a governança de confiança, o trabalho permanece em um nível conceitual e arquitetural, sem apresentar uma implementação de referência de código aberto ou avaliações de desempenho. Não são abordados os impactos na latência da transação causados pela verificação adicional de provas de inclusão em dispositivos móveis com conectividade instável. Além disso, a proposta assume a existência de uma infraestrutura de Autoridades de Credenciamento funcional e confiável, o que pode representar um desafio de governança significativo para a adoção em ecossistemas menores ou privados, como o de uma universidade, onde a segregação de funções entre o emissor de credenciais e o acreditador de serviços pode não ser clara.

Orquestração Governamental e Infraestrutura Pública Digital

Degen e Teubner (2024) investigam o papel dos governos na orquestração de ecossistemas de identidade digital, utilizando o contexto da consulta nacional alemã sobre a implementação do eIDAS 2.0. O estudo preenche uma lacuna na literatura ao analisar como o Estado pode atuar não apenas como regulador, mas como um orquestrador ativo que equilibra a criação de valor público e privado. A pesquisa identifica tensões críticas na governança desses ecossistemas, como o controle versus abertura e a padronização versus diferenciação. A partir da análise de 80 documentos de posicionamento e entrevistas com especialistas, os autores propõem uma tipologia para os modelos de fornecimento de carteiras de identidade: a "Carteira de Infraestrutura de ID Governamental" e a "Federação de Carteiras de ID de Confiança".

O modelo de "Carteira de Infraestrutura" descreve um cenário onde o governo (ou um ator comunitário) fornece uma infraestrutura central, como um SDK ou uma carteira básica, que serve de fundação para o ecossistema. Neste modelo, o foco é a segurança, a proteção de dados e a garantia de uma base sólida para casos de uso regulados. Já o modelo de "Federação de Carteiras" promove um ambiente competitivo onde múltiplos provedores (públicos e privados) oferecem carteiras interoperáveis sob guardrails regulatórios comuns. Este segundo modelo favorece a inovação e a variedade de mercado, mas exige um esforço maior de certificação e monitoramento

por parte do Estado para garantir a confiança.

Um ponto crucial levantado pelo trabalho é a ameaça das "guerras de carteiras" (*wallet wars*). Os autores argumentam que, sem uma intervenção governamental estratégica e a provisão de uma infraestrutura pública digital (DPI) robusta, as grandes empresas de tecnologia (Big Techs), que controlam os sistemas operacionais móveis, estão posicionadas para dominar o mercado de identidade digital através do envelopamento de plataformas. Isso resultaria em uma infraestrutura de identidade privatizada de fato, comprometendo a soberania digital. O estudo conclui que o governo deve definir claramente os limites econômicos e as responsabilidades, criando incentivos (como a obrigatoriedade de aceitação por grandes plataformas) para atrair emissores e garantir a sustentabilidade do ecossistema.

Desafios de Certificação e Ameaças de IA no eIDAS 2.0

Loutocký et al. (2025) analisam os desafios jurídicos e técnicos da certificação das Carteiras de Identidade Digital da UE, argumentando que a harmonização dos processos de avaliação de conformidade é o pilar fundamental para a confiança no ecossistema eIDAS 2.0. O estudo examina o impacto dos cinco Atos de Execução (Implementing Acts) adotados até o final de 2024, que definem as funcionalidades, protocolos e regras de certificação das carteiras. Os autores alertam que a dependência de esquemas nacionais de certificação, permitida transitoriamente enquanto um esquema europeu unificado sob o Cybersecurity Act (CSA) não é estabelecido pela ENISA, cria um risco sistêmico de fragmentação. Diferentes Estados-Membros podem aplicar níveis de rigor distintos, levando a um cenário de "forum shopping" onde fornecedores buscam certificadores mais lenientes, comprometendo a segurança global da rede.

O trabalho aborda também a dualidade da Inteligência Artificial na verificação de identidade. Por um lado, a IA é essencial para detectar fraudes complexas e automatizar processos de Know Your Customer (KYC). Por outro, o avanço da IA generativa e dos deepfakes introduz novos vetores de ataque capazes de burlar verificações biométricas tradicionais. O artigo defende que os esquemas de certificação devem evoluir para incluir testes de robustez específicos contra ataques assistidos por IA e definir claramente a alocação de responsabilidade civil (liability) entre provedores de carteira, organismos de certificação e autoridades supervisoras em caso de incidentes de segurança transfronteiriços.

Apesar de oferecer uma análise regulatória abrangente, o trabalho permanece no nível da política legislativa e não propõe mecanismos técnicos para a automação da certificação ou para a auditoria contínua das carteiras. A sugestão de "harmonização" depende de processos burocráticos lentos que podem não acompanhar a velocidade de evolução das ameaças cibernéticas baseadas em IA. Para o contexto

de um protótipo acadêmico, a principal lição é a necessidade de desenhar a arquitetura de segurança de forma modular, permitindo a atualização ágil dos algoritmos de verificação biométrica e criptográfica sem depender de ciclos longos de recertificação monolítica.

Mapeamento entre eIDAS 2.0 e o Modelo Trust Over IP

Lepore et al. (2024) realizam um mapeamento estrutural entre o regulamento eIDAS 2.0 e o modelo de referência Trust Over IP (ToIP), utilizando grafos de conhecimento para alinhar as entidades regulatórias com camadas técnicas de interoperabilidade. O estudo posiciona a infraestrutura EBSI (European Blockchain Services Infrastructure) e as listas de confiança baseadas em PKI na Camada 1 do modelo, destinada ao suporte à confiança pública. Para a Camada 2, focada na comunicação segura entre agentes, os autores identificam o protocolo OpenID SIOPv2 como o padrão para autenticação peer-to-peer remota, operando em conjunto com a norma ISO/IEC 18013-5 para interações de proximidade via NFC ou Bluetooth. A troca de dados na Camada 3 é mapeada para os protocolos OpenID for Verifiable Credential Issuance (OID4VCI) e OpenID for Verifiable Presentations (OID4VP), suportando formatos de credenciais como SD-JWT e JSON-LD.

A análise comparativa revela uma divergência arquitetural significativa entre os modelos. O estudo aponta que o ecossistema eIDAS atual não suporta nativamente Identificadores Descentralizados (DIDs) na camada de utilidade pública, dependendo, em vez disso, de registros de confiança autoritativos geridos pelos Estados-Membros. Essa característica limita a capacidade do eIDAS de compor itens em uma pilha técnica vertical puramente descentralizada conforme preconizado pelo ToIP. Além disso, o trabalho limita-se a um exercício teórico de alinhamento de ontologias e revisão documental, não fornecendo componentes de software ou gateways práticos que automatizem a tradução técnica entre os ecossistemas, o que deixa a implementação da interoperabilidade real como um desafio de engenharia aberto para os desenvolvedores de carteiras.

Regulação de Provas de Conhecimento Zero: Software vs. Serviço

Ramos Fernández (2024) investigam a lacuna regulatória referente à implementação de Provas de Conhecimento Zero (ZKP) no contexto do eIDAS 2.0, contrastando dois regimes legais para sua adoção: como um "Serviço de Confiança"(SaaS) ou como um "Produto de Software"(SaaS). O autor utiliza o projeto europeu ARIES como estudo de caso para o modelo de serviço, onde um intermediário centralizado gera as provas em nome do usuário. Embora esse modelo facilite a atribuição de responsabilidade civil (liability) sob os artigos atuais do eIDAS, ele é criticado por exigir

que o usuário revele seus dados brutos ao provedor do serviço, violando o princípio de privacidade por design e reintroduzindo pontos de centralização de dados.

Como alternativa técnica superior, o estudo aponta o ecossistema Hyperledger Indy como referência para o modelo de "Produto de Software", onde a geração da prova criptográfica ocorre localmente no dispositivo do usuário (edge), sem interação com terceiros. Para que essas provas geradas localmente tenham validade jurídica equivalente aos documentos originais, o autor propõe um regime de certificação rigoroso para o software da carteira, fundamentado em normas como ISO/IEC 15408 (Common Criteria) e ISO/IEC 25000 (SQuaRE), sob o guarda-chuva do Cybersecurity Act da UE. A tese central é que a tecnologia de ZKP deve ser regulada através do controle de qualidade do código (homologação prévia do software), garantindo que a prova matemática gerada pelo smartphone seja legalmente irrefutável por Verificadores.

Apesar de oferecer uma solução jurídica elegante para o dilema da privacidade, o trabalho baseia-se na premissa de que a certificação de software é suficiente para garantir a segurança operacional. Do ponto de vista de engenharia, essa visão subestima os desafios de manter a integridade do ambiente de execução em dispositivos móveis não gerenciados (BYOD), onde malwares podem comprometer a geração da prova mesmo em softwares certificados. Além disso, o artigo não aborda o custo computacional da geração local de ZKPs em hardware de entrada, o que pode criar uma barreira de exclusão digital não resolvida apenas por mandatos legais.

Modelo Conceitual para Validação de Reivindicações e Políticas

Abe et al. (2025) propõem um modelo conceitual para suprir a lacuna semântica existente nos padrões atuais de assinatura digital, distinguindo formalmente os processos de verificação e validação. Os autores argumentam que especificações como o Modelo de Dados de Credenciais Verificáveis do W3C limitam-se à verificação, ou seja, à confirmação matemática da integridade dos dados e da autenticidade da fonte criptográfica. No entanto, esses padrões não cobrem a validação, definida no estudo como a confirmação de que a reivindicação satisfaz os critérios de negócio e a intenção específica do verificador em um determinado contexto. Para operacionalizar essa distinção, o trabalho introduz o conceito de Política de Validação, um conjunto de regras definido pelo verificador que estipula quais evidências são aceitáveis para considerar uma afirmação verdadeira.

A arquitetura proposta formaliza o modelo Requerente-Certificador-Validador para cenários onde o verificador final não possui competência ou acesso para auditar a evidência bruta. Nesse esquema, uma entidade intermediária denominada Certificador realiza a validação primária da reivindicação e emite um certificado assinado que atesta esse fato. O verificador final, ao confiar na política de certificação dessa

entidade, aceita o certificado como prova derivada. O estudo aplica esse modelo analiticamente a casos de uso como controle de acesso a registros médicos e prova de proveniência de dados, utilizando a infraestrutura de chave pública X.509 e registros de transação em blockchain como mecanismos de ancoragem de confiança.

Apesar de fornecer uma ontologia necessária para sistemas de identidade, a proposta permanece em um nível alto de abstração e carece de uma implementação de referência. O trabalho não define uma linguagem padronizada ou um formato legível por máquina para expressar as Políticas de Validação ou Políticas de Certificação, o que dificulta a automação do processo de decisão em carteiras digitais e agentes verificadores. Para o desenvolvimento de um protótipo prático, essa ausência exige que o arquiteto do sistema defina formatos proprietários ou adapte padrões de políticas existentes, como ODRL ou Rego, para preencher a lacuna de execução deixada pelo modelo conceitual.

Infraestrutura TRAIN e Descoberta de Confiança via DNSSEC

Jeyakumar e Kubach (2025) propõem a infraestrutura TRAIN como um modelo de implementação para gerenciar a confiança em ecossistemas de identidade descentralizada de forma interoperável. O trabalho aborda a fragmentação dos domínios de confiança atuais, como EBSI e Gaia-X, que operam em silos tecnológicos. A solução arquitetural utiliza o Sistema de Nomes de Domínio, especificamente com as extensões de segurança DNSSEC, como uma raiz de confiança global para ancorar e descobrir listas de emissores autorizados. Diferente de abordagens baseadas exclusivamente em blockchain, o modelo permite a descoberta de estruturas de confiança através de consultas DNS padronizadas, reduzindo a barreira de entrada para a verificação.

A inovação técnica central reside em um modelo unificado de assinatura e verificação onde a localização da Lista de Confiança (seja em um servidor web tradicional ou IPFS) é envelopada dentro de uma Credencial Verificável conforme o modelo de dados do W3C. Isso permite que a lista de confiança seja assinada e validada utilizando Identificadores Descentralizados, abstraindo o método de armazenamento subjacente. A implementação de referência, validada no contexto do ecossistema de dados Gaia-X, compõe-se de módulos como o Trust Framework Manager para a gestão do ciclo de vida das listas e o TRAIN Trust Validator para a resolução automática de credenciais. O sistema adota o padrão ETSI TS 119 612 para a estruturação das listas de confiança, garantindo compatibilidade com regulamentações europeias existentes.

Apesar de oferecer uma solução pragmática para a escalabilidade da confiança, a arquitetura apresenta limitações quanto à descentralização. A dependência da hierarquia do DNS implica que a raiz de confiança final permanece sob governança centralizada (ICANN), o que pode ser um ponto de conflito para casos de uso que exi-

gem soberania total contra censura. Além disso, o trabalho descreve o TRAIN como uma arquitetura de referência em processo de padronização, não como um padrão consolidado, e a análise de segurança fornecida é de alto nível, carecendo de uma avaliação formal de vetores de ataque específicos contra a infraestrutura de gerenciamento de zonas DNS proposta.

Tendências Tecnológicas em Esquemas de Identidade eIDAS

Sharif et al. (2022) conduzem uma análise sistemática da evolução tecnológica dos esquemas de identidade eletrônica na Europa, mapeando a transição dos paradigmas legados do eIDAS 1.0 para a arquitetura proposta do eIDAS 2.0. O estudo examina 24 esquemas notificados por 18 Estados-Membros, identificando uma predominância histórica do protocolo SAML 2.0, utilizado em 62% das soluções, o que reflete a herança de infraestruturas web-based de desktop. No entanto, a pesquisa detecta uma tendência clara de migração para OpenID Connect (OIDC) em esquemas mais recentes ou modernizados (como o SPID italiano, que adota o perfil OIDC iGov), impulsionada pela necessidade de suporte nativo a aplicativos móveis.

A análise de segurança revela uma adoção crescente de mecanismos de prova de posse criptográfica. Para níveis de garantia "Alto", 72% dos esquemas dependem de hardware dedicado, como Smart Cards ou Security Tokens compatíveis com FIDO, enquanto soluções móveis modernas frequentemente utilizam o armazenamento seguro do dispositivo (Keystore/Secure Element) protegido por biometria. O estudo também destaca a implementação massiva da extensão PKCE (Proof Key for Code Exchange) em fluxos OIDC (76% dos casos) para mitigar ataques de interceptação de código em dispositivos móveis.

Apesar dos avanços, o trabalho aponta lacunas críticas na implementação de privacidade e usabilidade. A maioria dos esquemas analisados (94%) já adota identificadores pairwise para evitar o rastreamento cruzado entre serviços, mas funcionalidades avançadas de minimização de dados, como a divulgação seletiva, ainda estão ausentes na camada de protocolo dos sistemas atuais. Além disso, a "neutralidade tecnológica" do regulamento original resultou em uma fragmentação significativa de padrões de autenticação, criando um passivo de interoperabilidade que a nova EUDI Wallet precisará gerenciar, especialmente ao tentar integrar ecossistemas nacionais que ainda operam exclusivamente com cartões inteligentes físicos e protocolos XML legados.

Discussão e Relevância para o Trabalho

A literatura sobre governança em ecossistemas de identidade descentralizada aponta para uma tensão entre a rigidez das estruturas hierárquicas governamentais e a flexibilidade exigida pela arquitetura da Web3. Lepore et al. (2024) e Jeyakumar

e Kubach (2025) abordam o problema da descoberta de confiança (Trust Discovery) por ângulos complementares. Enquanto Lepore et al. (2024) demonstram, através do mapeamento com o modelo Trust Over IP, que o regulamento eIDAS 2.0 impõe uma estrutura baseada em listas de confiança estáticas e PKI, limitando o uso nativo de DIDs, Jeyakumar e Kubach (2025) oferecem uma solução pragmática com o modelo TRAIN. Ao utilizar a infraestrutura global do DNS e as extensões de segurança DNSSEC como âncora de confiança, o modelo TRAIN permite que uma universidade publique seus metadados de emissor em seu próprio domínio institucional, garantindo interoperabilidade sem a complexidade de governança de redes blockchain permissi-onadas ou a burocracia de listas de confiança nacionais.

No âmbito da interação entre a carteira e o verificador, More et al. (2024) e Abe et al. (2025) estabelecem que a verificação criptográfica é insuficiente para garantir a segurança do ecossistema. More et al. (2024) argumentam que a carteira deve atuar como um Ponto de Aplicação de Políticas (Policy Enforcement Point), bloqueando tecnicamente solicitações de dados excessivas por parte de verificadores não credenciados. Essa visão é refinada conceitualmente por Abe et al. (2025), que distinguem a "verificação"(prova matemática) da "validação"(conformidade com regras de negócio). Para o protótipo deste trabalho, essa distinção implica que a arquitetura da carteira não deve apenas guardar chaves, mas também possuir um motor de regras capaz de interpretar certificados de credenciamento de serviços e políticas de validação antes de solicitar o consentimento do usuário.

A implementação de tecnologias de privacidade avançada, como Provas de Conhecimento Zero (ZKP), enfrenta desafios regulatórios significativos. Ramos Fernández (2024) defende que, para preservar a soberania do usuário, a geração de ZKPs deve ocorrer localmente no dispositivo (modelo de "Software como Produto"), e não delegada a servidores (modelo de "Serviço de Confiança"). Contudo, Loutocký et al. (2025) alertam que essa abordagem transfere a carga de segurança para o processo de certificação do software da carteira, que atualmente é fragmentado e lento. Isso sugere que o protótipo deve priorizar a execução local de provas criptográficas para alinhar-se aos princípios de privacidade, mas deve estar preparado para integrar-se a esquemas de certificação automatizada para garantir a confiança do verificador na integridade do ambiente de execução.

Por fim, a análise histórica de Sharif et al. (2022) fornece diretrizes práticas para a escolha de protocolos de transporte. A evidência de que a neutralidade tecnológica resultou em fragmentação no eIDAS 1.0, somada à tendência de convergência para o OpenID Connect em detrimento do SAML, orienta a decisão de projeto deste trabalho. Para garantir a viabilidade futura e a usabilidade em dispositivos móveis, o protótipo deve adotar estritamente o perfil OpenID for Verifiable Presentations (OID4VP) com extensões de segurança como PKCE, evitando protocolos legados que

não suportam nativamente os fluxos de carteira digital e divulgação seletiva.

3.3.3 Privacidade Avançada, Criptografia e Segurança

Esta seção aprofunda-se nos mecanismos técnicos fundamentais que garantem as propriedades de privacidade e segurança das carteiras digitais. Os trabalhos aqui reunidos discutem desde a escolha de primitivas criptográficas (Zero-Knowledge Proofs vs. Hashing) e a resistência pós-quântica, até a segurança de hardware e procedimentos de resposta a incidentes.

Divulgação Seletiva: SD-JWT vs. Assinaturas ZKP

Flamini et al. (2024) realizam uma análise comparativa técnica e experimental entre as duas principais famílias de mecanismos criptográficos que habilitam a divulgação seletiva em credenciais verificáveis: os baseados em compromissos ocultos (hiding commitments) e as assinaturas de divulgação seletiva (selective disclosure signatures). A pesquisa classifica o formato SD-JWT e o padrão ISO/IEC 18013-5 (mDoc) na primeira categoria, onde a privacidade é obtida através da não divulgação de salts criptográficos. Em contraste, a segunda categoria engloba esquemas de assinatura que suportam nativamente provas de conhecimento zero não interativas (NIZKPs), como Camenisch-Lysyanskaya (CL), BBS, BBS+ e Pointcheval-Sanders (PS).

Para a validação experimental, os autores desenvolveram implementações em Rust, normalizando o nível de segurança para 128 bits. Foram utilizadas as bibliotecas Hyperledger Ursa (para CL e PS) e Docknetwork (para BBS/BBS+), operando sobre a curva BLS12-381, enquanto os testes de resistência pós-quântica utilizaram a biblioteca Open Quantum Safe (algoritmos Dilithium, Falcon, SPHINCS+). As medições de desempenho foram conduzidas em processadores Raspberry Pi 3B+ e 4B para simular as restrições computacionais de dispositivos móveis (Holder), comparando o tempo de geração de provas e o tamanho dos artefatos gerados.

Os resultados revelaram trade-offs significativos. Os mecanismos baseados em commitments (SD-JWT) são computacionalmente eficientes e agnósticos quanto ao algoritmo de assinatura, facilitando a migração para criptografia pós-quântica. No entanto, falham em garantir a não-vinculabilidade entre múltiplas apresentações, pois os digests dos atributos permanecem estáticos. Por outro lado, as assinaturas BBS e PS permitem apresentações totalmente não vinculáveis e provas de predicados (como intervalos de idade) sem revelar dados, com o esquema BBS apresentando desempenho viável para uso móvel, ao contrário do CL. O estudo conclui apontando uma lacuna crítica no estado da arte: atualmente, não existem implementações maduras de assinaturas de divulgação seletiva que sejam simultaneamente eficientes e resistentes a computação quântica, forçando arquitetos de sistema a escolherem entre privacidade avançada (unlinkability) e segurança a longo prazo.

Avaliação de Privacidade e Risco de Vinculabilidade no eIDAS ARF

Álvarez et al. (2026) conduzem uma avaliação de privacidade da versão 2.4 da Arquitetura e Framework de Referência (ARF) da Carteira de Identidade Digital Europeia, utilizando a metodologia de modelagem de ameaças LINDDUN combinada com a taxonomia de danos de privacidade de Solove. O estudo formaliza a análise em três fluxos críticos de alto nível de garantia (LoA High): emissão de PID, apresentação remota e apresentação em proximidade (offline). A análise técnica abrange a pilha de protocolos mandatória, incluindo OpenID4VCI e OpenID4VP para transporte, e os formatos de dados SD-JWT e ISO/IEC 18013-5 (mDoc/mDL), identificando que as escolhas de design atuais introduzem vetores de vigilância inerentes, contradizendo os princípios de minimização de dados do GDPR.

Os autores demonstram tecnicamente que a implementação de divulgação seletiva via SD-JWT falha em garantir a não-vinculabilidade. Isso ocorre porque os salts criptográficos utilizados para ocultar atributos resultam em hashes imutáveis que persistem entre apresentações, permitindo que Relying Parties coludam para rastrear o usuário através de diferentes sessões. Similarmente, no fluxo de proximidade (mDoc), a persistência de chaves criptográficas no dispositivo seguro (WSCD) atua como um identificador único global. O estudo mapeia sete casos de ameaça, concluindo que a arquitetura atual expõe metadados de transação e identificadores de revogação que podem ser explorados para perfilamento de usuários, uma vez que a especificação técnica prioriza a interoperabilidade e a verificação de autenticidade em detrimento do anonimato de rede ou de aplicação.

A principal contribuição crítica do trabalho é a constatação de que a conformidade com o regulamento eIDAS 2.0 (que exige tecnologias de preservação de privacidade) é tecnicamente inviável se a implementação restringir-se estritamente aos formatos SD-JWT e mDoc definidos na ARF atual. O artigo aponta um gap significativo na ausência de suporte nativo para credenciais anônimas baseadas em Provas de Conhecimento Zero (como BBS+ ou Camenisch-Lysyanskaya) e na falta de estratégias de ofuscação de tráfego de rede, sugerindo que implementações acadêmicas e pilotos devem divergir da especificação oficial para alcançar propriedades reais de privacidade e resistência à correlação.

Extensão de Credenciais via Commit-and-Prove e PS-MS

García-Rodríguez et al. (2024) propõem uma extensão modular para sistemas de Credenciais Baseadas em Atributos com preservação de privacidade (p-ABC), focando na distribuição da emissão através de multi-assinaturas Pointcheval-Sanders (PS-MS). A arquitetura utiliza a técnica de commit-and-prove para acoplar funcionalidades avançadas ao protocolo de apresentação sem alterar a estrutura da assina-

tura original. As extensões implementadas incluem provas de intervalo baseadas em Bulletproofs, pseudônimos de escopo exclusivo criptograficamente desligáveis, mecanismos de inspeção auditável e um sistema de revogação baseado em listas de permissão (allow-lists) atualizadas pelo portador.

Para a validação, os autores desenvolveram uma biblioteca em Java (visando portabilidade) e um módulo de otimização em C, operando sobre a curva elíptica BLS12-461 para garantir um nível de segurança superior a 134 bits. A avaliação de desempenho, realizada em um dispositivo móvel de médio porte (POCO X3 NFC), demonstrou que a solução supera o sistema de referência Idemix (utilizado no ecossistema Hyperledger) em eficiência. O sistema permite a emissão distribuída onde a chave pública global é uma agregação das chaves de múltiplos emissores, eliminando a necessidade de uma autoridade central confiável para a geração de chaves.

Apesar dos avanços funcionais, a solução apresenta limitações de usabilidade em cenários reais. Os experimentos mostraram que a execução de provas de intervalo no dispositivo móvel pode levar entre 5,5 e 17 segundos dependendo da precisão (bits), o que é proibitivo para interações presenciais rápidas. Além disso, a escolha de Java para a implementação principal impõe overheads de desempenho em comparação com implementações modernas em Rust ou C++ nativo, comuns em carteiras digitais de alta performance. Por fim, o modelo de revogação exige que o usuário baixe e atualize credenciais de revogação periodicamente, o que pode introduzir atritos de sincronização em ambientes com conectividade intermitente.

Revogação com Preservação de Privacidade e Flexibilidade Temporal

Buccafurri e Licciardi (2025) abordam o problema da revogação de credenciais sem rastreamento, propondo um método que utiliza Anonymous Hierarchical Identity-Based Encryption (AHIBE) de maneira não convencional. A arquitetura constrói identidades efêmeras através da concatenação da identidade do portador com um carimbo de tempo ($H\|T$), permitindo a geração de chaves de decifração válidas apenas para janelas temporais específicas. O sistema opera através da publicação, pelo emissor, de uma tabela de revogação criptografada e uma tabela de verificação (check table) baseada em Message Authentication Codes (MACs) e sementes de geradores de números pseudoaleatórios (PRNGs).

A principal inovação técnica é a "flexibilidade temporal": o portador fornece ao verificador uma chave privada derivada correspondente apenas ao período autorizado (passado ou presente), impedindo que o verificador monitore o status da credencial perpetuamente. O processo de verificação ocorre localmente: o verificador baixa as tabelas públicas e tenta decifrar a entrada correspondente usando a chave efêmera e o valor do PRNG fornecidos pelo portador; o sucesso na decifragem indica que a credencial foi revogada. Isso elimina a necessidade de consultar o emissor em tempo

real (proteção contra phone-home) e garante a resistência à censura, pois a ausência de publicação de tabelas seria detectável.

Contudo, a proposta apresenta limitações de escalabilidade no lado do verificador. O modelo exige que o verificador faça o download de segmentos das tabelas de revogação e verificação para realizar a checagem, resultando em um consumo de largura de banda significativamente maior do que em protocolos leves como OCSP ou listas de bits. Além disso, o trabalho permanece em estágio de proposta teórica ("work-in-progress"), sem uma implementação de referência que valide o custo computacional das primitivas AHIBE em dispositivos móveis ou uma análise formal de segurança completa, representando uma lacuna para a adoção imediata em ecossistemas de produção como a EUDI Wallet.

Carteira Desktop Segura via Virtualization-Based Security (VBS)

Xie et al. (2025) propõem o SecuVault, uma arquitetura de carteira digital projetada especificamente para o ecossistema Windows, visando mitigar a ausência de ambientes de execução confiáveis (TEEs) padronizados em desktops, em contraste com os Secure Enclaves móveis. A solução utiliza a tecnologia de Virtualization-Based Security (VBS) para isolar o código crítico da carteira em um nível de confiança virtual elevado (VTL1), protegendo-o contra malwares que operam no nível do kernel do sistema operacional (VTL0). O controle de acesso é reforçado pela integração com o Trusted Platform Module (TPM) para a proteção de chaves e com o Windows Hello para autenticação biométrica do usuário.

Para garantir a privacidade na apresentação de credenciais, o SecuVault implementa um esquema de assinaturas Pointcheval-Sanders (PS), que permite a divulgação seletiva de atributos e a não-vinculabilidade (unlinkability) através de provas de conhecimento zero. O ciclo de vida da credencial, incluindo a emissão cega (blind issuance) e a verificação, é executado inteiramente dentro do enclave VBS. A avaliação de desempenho indica que, embora as operações de curva elíptica sejam eficientes, o cálculo de pareamentos bilineares necessários para a verificação da assinatura PS introduz uma latência de aproximadamente 0,2 segundos, o que é aceitável para uso desktop, mas impõe um custo computacional não desprezível.

Apesar de inovar na segurança para desktops, a arquitetura apresenta limitações críticas de interoperabilidade. A dependência estrita de tecnologias proprietárias da Microsoft (VBS, Windows Hello) cria um vendor lock-in que dificulta a portabilidade da carteira para outros sistemas operacionais, contrariando o princípio de independência de plataforma da EUDI Wallet. Além disso, o trabalho não aborda como a carteira interagiria com a infraestrutura de confiança europeia (como a validação de listas de confiança ou a comunicação com RPs remotos via OpenID4VP), focando exclusivamente na segurança local do dispositivo.

Distribuição de Ambientes de Execução Confiáveis (MultiTEE)

Ott et al. (2024) propõem o MultiTEE, uma arquitetura que estende o isolamento de hardware (TEE) para um cluster distribuído de dispositivos heterogêneos, visando suportar o caso de uso da EUDI Wallet em ecossistemas de múltiplos dispositivos (como smartphone emparelhado a um smartwatch). A implementação de referência utiliza hardware ARM TrustZone (processadores Cortex-A e Cortex-M) rodando os sistemas operacionais seguros OP-TEE e Trusted Firmware-M, respectivamente. Para garantir a segurança da comunicação entre os TEEs sem o overhead do TLS, os autores implementaram o Noise Protocol Framework (padrão de handshake "XX"), desenvolvido em Rust para mitigar vulnerabilidades de memória comuns em implementações C/C++. A integridade dos dispositivos no cluster é verificada através de atestação remota híbrida, utilizando TPM baseado em firmware para dispositivos potentes e DICE (Device Identifier Composition Engine) para dispositivos com recursos restritos.

A solução estende a GlobalPlatform Internal Core API para permitir que Aplicações Confiáveis (TAs) invoquem comandos em TAs remotas de forma transparente, abstraindo a complexidade da rede. A avaliação de desempenho demonstra que a solução é viável mesmo em microcontroladores com apenas 1MB de Flash (ocupando cerca de 20

Contudo, a arquitetura impõe desafios de latência e interoperabilidade. Os experimentos indicam que operações complexas, como a verificação de credenciais envolvendo pareamentos bilineares em dispositivos Cortex-M, geram latências perceptíveis (aprox. 3 segundos para emissão completa), o que pode impactar a experiência do usuário em fluxos de autenticação rápida. Além disso, a dependência estrita da arquitetura ARM TrustZone e das APIs da GlobalPlatform limita a aplicabilidade do MultiTEE em ambientes mistos que incluam outras tecnologias de enclave (como Intel SGX ou RISC-V Keystone), criando barreiras para uma adoção universal no mercado de eletrônicos de consumo fragmentado.

Ameaça Pós-Quântica e a Transição da Carteira Europeia

Comandè e Varilek (2024) analisam a implementação da EUDIW sob a perspectiva da ameaça da computação quântica, argumentando que a massiva escala de adoção prevista para a carteira (obrigatória para estados-membros e grandes plataformas) a torna o vetor ideal para liderar a migração da infraestrutura de chaves públicas da Europa. O estudo diagnostica que os atuais protótipos e pilotos da EUDIW, baseados em algoritmos clássicos como RSA e ECC, estão expostos ao risco de ataques "colher agora, descriptografar depois" (harvest now, decrypt later), onde tráfego criptografado hoje pode ser comprometido no futuro.

Para mitigar esse risco sistêmico, os autores defendem que a especificação técnica da carteira (ARF) deve incorporar imediatamente suporte para algoritmos de criptografia pós-quântica (PQC) selecionados pelo NIST, como CRYSTALS-Dilithium, Falcon e SPHINCS+. A estratégia proposta é a adoção de esquemas híbridos, combinando criptografia clássica e pós-quântica, para garantir segurança contra ataques quânticos sem sacrificar a confiança estabelecida nos algoritmos atuais. O trabalho revisa as estratégias nacionais de segurança cibernética de países como França (ANSSI), Alemanha (BSI) e Espanha (CCN), que já recomendam essa abordagem de hibridização como passo intermediário antes de uma transição completa.

Embora o artigo forneça uma justificativa política e regulatória robusta para a agilidade criptográfica na EUDIW, ele carece de uma análise de viabilidade técnica. Não são abordados os desafios práticos de implementar algoritmos PQC em ambientes restritos de carteiras móveis, como o aumento significativo no tamanho das chaves e assinaturas (que impacta a transmissão via QR Code ou NFC) e o custo computacional elevado para verificação em hardware seguro (SE/TEE) existente, que muitas vezes possui aceleradores apenas para ECC/RSA. A proposta permanece, portanto, no nível de diretriz estratégica, sem validar se a "arca" da EUDIW consegue tecnicamente suportar a carga da criptografia pós-quântica com a tecnologia de hardware atual.

Processos de Resposta a Incidentes de Segurança em SSI

Ziegler et al. (2025) abordam a lacuna crítica de procedimentos operacionais de segurança em ecossistemas de Identidade Auto-Soberana (SSI), propondo fluxos de Resposta a Incidentes de Segurança (SIR) adaptados para arquiteturas descentralizadas. A pesquisa baseia-se em entrevistas com operadores de redes produtivas, como IDunion e TNO, e na análise de frameworks como o Sirtfi (utilizado na federação eduGAIN). O estudo distingue três domínios de resposta: o nível da rede (focado na integridade dos nós do ledger e consenso), o nível da entidade (emissores e verificadores) e o nível do portador (usuário final).

Do ponto de vista técnico, os autores modelam cenários de ataque específicos, incluindo o comprometimento de chaves de assinatura de emissores e vulnerabilidades em registros de confiança (citando o CVE-2022-31020 em redes baseadas em Hyperledger Indy). Para a coordenação de incidentes, propõe-se o uso do protocolo DIDComm para estabelecer canais de comunicação seguros e autenticados entre as equipes de resposta (IRTs) e os agentes afetados, superando a dependência de canais fora de banda inseguros (como e-mail). A proposta enfatiza que, em um modelo descentralizado, a mitigação de incidentes (como a rotação de chaves comprometidas ou a atualização de listas de revogação) deve ser executada localmente pelas entidades afetadas, com a coordenação global servindo apenas para disseminação de

inteligência de ameaças.

Apesar de estruturar o processo, o trabalho revela uma limitação significativa na maturidade das ferramentas atuais: as carteiras digitais disponíveis no mercado carecem de interfaces e protocolos padronizados para que usuários finais reportem incidentes (como roubo de dispositivo) ou recebam alertas de segurança de forma verificável. O processo proposto ainda depende pesadamente de intervenção manual e governança humana, não oferecendo automação técnica para a detecção ou contenção de incidentes em tempo real na camada do protocolo.

Discussão e Relevância para o Trabalho

A análise cruzada da literatura revela uma dicotomia fundamental entre a eficiência computacional e as garantias de privacidade. Flamini et al. (2024) e Álvarez et al. (2026) convergem ao demonstrar que a atual especificação técnica da EUDIW (baseada em SD-JWT e mDoc) prioriza a performance em detrimento da não-vinculabilidade (unlinkability). Enquanto Flamini et al. (2024) quantificam empiricamente a eficiência dos mecanismos baseados em hash, eles alertam que essa escolha arquitetural cria identificadores persistentes. Álvarez et al. (2026) aprofundam essa crítica, provando que tal persistência viola os princípios de minimização de dados do eIDAS 2.0, justificando a necessidade de explorar, neste trabalho, implementações acadêmicas baseadas em Zero-Knowledge Proofs (ZKPs) para garantir privacidade real.

No entanto, a adoção de primitivas avançadas impõe custos operacionais significativos. Embora García-Rodríguez et al. (2024) ofereçam uma implementação funcional de credenciais distribuídas com provas de intervalo e inspeção, os testes de desempenho em dispositivos móveis revelam latências na ordem de segundos, o que pode inviabilizar o uso em catracas ou filas universitárias. Similarmente, a proposta de revogação com flexibilidade temporal de Buccafurri e Licciardi (2025), apesar de resolver o problema do rastreamento pelo emissor (phone-home), transfere uma carga excessiva de largura de banda para o verificador. Essas evidências sugerem que o protótipo da UFSC deverá encontrar um meio-termo prático, talvez restringindo o uso de provas criptográficas pesadas a cenários de alta sensibilidade.

No âmbito da segurança de plataforma, Xie et al. (2025) e Ott et al. (2024) propõem arquiteturas robustas baseadas em isolamento de hardware (VBS e TrustZone, respectivamente). Contudo, a análise crítica desses trabalhos expõe um problema de interoperabilidade: a dependência estrita de recursos proprietários (como Windows Hello ou extensões específicas da GlobalPlatform) cria barreiras de entrada e vendor lock-in. Para um ambiente universitário heterogêneo, onde estudantes utilizam dispositivos de diversas gerações e fabricantes, o modelo de segurança deve priorizar soluções agnósticas ao hardware ou adotar padrões abertos de atestação remota que

não excluam dispositivos de baixo custo.

Por fim, a literatura aponta para uma imaturidade na preparação para ameaças futuras e na governança de crises. Comandè e Varilek (2024) diagnosticam a vulnerabilidade dos algoritmos atuais à computação quântica, mas falham em apresentar soluções de engenharia compatíveis com o hardware móvel atual. Paralelamente, Ziegler et al. (2025) evidenciam que, apesar da existência de frameworks teóricos de resposta a incidentes, as carteiras atuais carecem de interfaces para que o usuário participe ativamente da segurança (ex: reportar roubo de forma verificável). Essas lacunas orientam o desenvolvimento do protótipo deste trabalho, que busca demonstrar a viabilidade técnica da execução de ZKPs em dispositivos móveis e documentar os compromissos entre privacidade e desempenho observados em cenários acadêmicos simulados.

3.3.4 Casos de Uso Específicos: Educação e Cenários Offline

Esta seção explora a aplicação prática das tecnologias de identidade descentralizada em dois contextos críticos para o escopo deste trabalho: o ambiente de ensino superior, com seus requisitos de longevidade e reconhecimento transfronteiriço, e os cenários de operação offline, essenciais para a usabilidade diária em campi universitários.

Longevidade de Credenciais Verificáveis (Diplomas)

Bochnia e Anke (2024) investigam a gestão do ciclo de vida de credenciais de longa duração (LLVCs), como diplomas, cujo período de validade frequentemente supera o tempo de existência da entidade emissora ou a vida útil dos dispositivos de armazenamento. O estudo aponta que o modelo de confiança padrão da SSI torna-se frágil nesse contexto, pois a verificação técnica, dependente de chaves públicas e registros de revogação mantidos pelo emissor, falha caso a instituição original seja dissolvida, invalidando a credencial digital, embora o direito adquirido pelo titular permaneça juridicamente válido.

Sob uma perspectiva técnica, os autores avaliam estratégias para mitigar essa dependência, contrastando o uso de Registros Distribuídos (DLTs), como os pilotos da EBSI e a rede acadêmica Bloxberg, com modelos de governança baseados na transferência de autoridade para entidades custodiantes. A análise destaca a incompatibilidade entre mecanismos de device binding baseados em Hardware Security Modules (HSMs) e a longevidade necessária para diplomas, visto que o ciclo de substituição de smartphones (2 a 3 anos) exigiria reemissões constantes. Adicionalmente, é discutida a instabilidade dos padrões atuais, citando o risco de remoção do mecanismo refreshService no Modelo de Dados de Credenciais Verificáveis do W3C 2.0, o que

complicaria a atualização de provas criptográficas obsoletas sem interação direta com o emissor.

A proposta central envolve requisitos arquiteturais para permitir que entidades sucessoras, como arquivos públicos ou ministérios, assumam a gestão do ciclo de vida das credenciais (revogação e reemissão) após a extinção do emissor original. Contudo, o trabalho apresenta limitações por ser estritamente teórico e focado no arcabouço regulatório alemão, não oferecendo uma implementação de referência ou protótipo. O estudo não detalha os protocolos técnicos necessários para a transferência segura de material criptográfico e logs de auditoria entre emissores, deixando a operacionalização técnica da "sucessão de emissores" como uma lacuna em aberto.

Impacto do eIDAS 2.0 no Ensino Superior da Croácia

Milenković e Vojković (2025) analisam os impactos legislativos e técnicos da implementação do eIDAS 2.0 no sistema de ensino superior da Croácia, diagnosticando a obsolescência dos atuais mecanismos de autenticação baseados na infraestrutura nacional AAI@EduHr. O estudo aponta que o modelo vigente, dependente exclusivamente de credenciais de usuário e senha sem autenticação multifator, é vulnerável a ataques em terminais públicos (como keyloggers e shoulder surfing) e não atinge o Nível de Garantia exigido pelo novo regulamento europeu. Essa insegurança sistêmica resulta na manutenção de processos manuais redundantes, como a impressão e assinatura física de listas de notas ("prijavnice") por professores, devido à falta de confiança jurídica nos registros puramente digitais atuais.

Do ponto de vista da infraestrutura tecnológica, o trabalho mapeia a necessidade de integração entre os sistemas de gestão de identidade acadêmica (geridos pela CARNET) e o Sistema de Informação sobre Direitos dos Estudantes (ISSP, gerido pelo centro de computação universitário Srce). Os autores discutem a participação nos Pilotos de Larga Escala, especificamente o DC4EU (Digital Credentials for Europe), como referência para a padronização de eDiplomas e credenciais de segurança social. Além disso, a European Blockchain Services Infrastructure é analisada como uma possível camada técnica para descentralizar a verificação e mitigar riscos de ataques man-in-the-middle, garantindo a integridade das credenciais sem depender exclusivamente de fornecedores de sistemas operacionais móveis.

A proposta central defende o uso da EUDI Wallet para automatizar a verificação de atributos de alunos (para mobilidade Erasmus+) e também de vínculos empregatícios temporários de docentes, eliminando a burocracia de recondução de contratos. Entretanto, o artigo limita-se a uma análise de lacunas processual e regulatória, não apresentando uma arquitetura de software ou protótipo que demonstre como a ponte técnica entre os protocolos legados da federação eduGAIN e os novos padrões da carteira digital deve ser implementada na prática.

Gestão Acadêmica via Soulbound Tokens (M.U.St)

Polychronaki et al. (2025) apresentam a plataforma M.U.St, uma prova de conceito para a gestão de identidades e ativos acadêmicos que implementa o protocolo Proof of Identity Ownership (PoIO). A arquitetura técnica é construída sobre uma rede Ethereum privada, utilizando contratos inteligentes desenvolvidos em Solidity para a emissão de Soulbound Tokens (SBTs) e Identificadores Descentralizados (DIDs). Para a interface do usuário, foi desenvolvida uma aplicação móvel multiplataforma utilizando o framework Flutter, que interage com um oráculo (servidor web/email) para vincular a carteira digital às credenciais institucionais legadas. Um componente crítico da implementação é o uso de um banco de dados MongoDB hospedado privadamente, utilizado para armazenar as representações das Credenciais Verificáveis (como passes de biblioteca e restaurante) off-chain, permitindo a geração de QR Codes para verificação rápida.

A abordagem difere das arquiteturas puramente baseadas em VCs no dispositivo (edge) ao utilizar SBTs intransferíveis on-chain como a âncora principal da identidade e propriedade dos ativos acadêmicos. O sistema busca garantir a integridade e a perenidade dos registros através da imutabilidade da blockchain, propondo uma camada de interoperabilidade que teoricamente permitiria a comunicação com outras redes (como Solana) e o uso de Zero-Knowledge Proofs.

Contudo, a arquitetura proposta apresenta limitações críticas quanto à privacidade e à verdadeira descentralização. A dependência de um banco de dados MongoDB centralizado para armazenar as representações das credenciais contradiz os princípios de soberania do usuário, criando um ponto único de falha e um alvo para vazamento de dados (honeypot). Além disso, o uso de SBTs imutáveis para representar atributos de identidade, mesmo em uma rede privada, impõe desafios severos à conformidade com o "direito ao esquecimento" do GDPR (e LGPD), contrastando com a abordagem de minimização de dados e armazenamento local preconizada pela EUDI Wallet. O trabalho também não detalha mecanismos de revogação de SBTs em casos de erro administrativo sem comprometer a integridade histórica da ledger.

Mensageria P2P Descentralizada via DIDComm e Bluetooth

Enge et al. (2022b) exploram a comunicação descentralizada em cenários sem conectividade com a Internet (offline), propondo um framework arquitetural que desacopla a troca de mensagens da infraestrutura de rede tradicional. O objetivo é permitir a interação segura diretamente entre dispositivos (peer-to-peer) através da combinação do protocolo DIDComm com a tecnologia Bluetooth Low Energy (BLE). O trabalho define os requisitos funcionais para o estabelecimento de conexão e troca de mensagens, avaliando a viabilidade de bibliotecas SSI existentes para suportar essa

arquitetura em ambientes onde a conectividade é intermitente ou inexistente.

Do ponto de vista técnico, a solução utiliza o perfil GATT (Generic Attribute Profile) do BLE como camada de transporte para o envio de mensagens criptografadas no padrão DIDComm v2. Os autores realizaram uma avaliação comparativa de frameworks de desenvolvimento, incluindo Hyperledger Aries, SpruceID e Veramo, identificando este último como o mais compatível com a especificação DIDComm v2 na época. Para garantir a operação offline, o sistema adota o método DID did:peer, que permite a geração e resolução de Identificadores Descentralizados localmente entre os pares, eliminando a dependência de ledgers públicos ou resoluções DNS. A segurança é assegurada em duas camadas: emparelhamento ao nível de transporte (BLE Secure Connection) e criptografia autenticada ao nível da aplicação (ECDH-1PU).

Embora o estudo valide a viabilidade técnica de mensageria offline segura na plataforma Android, ele permanece em um nível de design arquitetural e prova de conceito, sem uma análise formal de segurança do protocolo proposto. Uma limitação crítica para a aplicabilidade no contexto da EUDI Wallet é a divergência tecnológica: enquanto o estudo foca em DIDComm sobre BLE, os padrões europeus consolidam-se em torno da norma ISO/IEC 18013-5 (camada de dispositivo) e OpenID4VP. Além disso, o uso exclusivo de did:peer impõe desafios para a verificação de credenciais em domínios cruzados, uma vez que não há uma âncora de confiança pública acessível para validar a integridade do emissor fora do contexto da conexão local.

Controle de Acesso Físico Offline com Padrões SSI

Enge et al. (2022a) desenvolvem e avaliam um sistema de controle de acesso físico utilizando identidade auto-soberana em cenários sem conectividade com a Internet. O trabalho foca na combinação do protocolo de mensagens DIDComm v2 com a tecnologia Bluetooth Low Energy (BLE) para permitir a troca segura e descentralizada de credenciais verificáveis entre dispositivos móveis em proximidade. A arquitetura proposta elimina a necessidade de servidores centrais de autenticação ou conexão constante com a nuvem, delegando a verificação das credenciais para os dispositivos na borda através do perfil GATT do Bluetooth.

A implementação da prova de conceito utilizou o framework React Native para a aplicação móvel, integrando o Veramo como agente SSI para gestão de chaves, identificadores (utilizando o método did:key) e credenciais no formato JSON-LD. Para a comunicação via Bluetooth, foi desenvolvida uma biblioteca nativa Android personalizada que abstrai a API BLE, permitindo o transporte de mensagens DIDComm criptografadas (Authcrypt) sobre o canal físico. O fluxo de conexão é iniciado por um convite fora de banda (OOB) via código QR, seguido pelo estabelecimento de um canal seguro e a execução do protocolo de Presentation Exchange para validação de

atributos de acesso baseados em papéis (RBAC).

Apesar de demonstrar a viabilidade funcional, a solução apresenta limitações práticas significativas para implantação em larga escala. O uso do método did:key restringe a capacidade de rotação de chaves e revogação complexa, visto que o identificador é estático, diferindo de métodos mais robustos como did:peer ou did:web. Além disso, a latência total observada nos experimentos (média superior a 4 segundos para o fluxo completo sem reuso de conexão) pode ser proibitiva para cenários de alto tráfego, como catracas universitárias. Por fim, a arquitetura diverge dos padrões de proximidade adotados pela EUDI Wallet (ISO/IEC 18013-5).

Discussão e Relevância para o Trabalho

A aplicação de identidade descentralizada na educação exige o equilíbrio entre perenidade jurídica, privacidade e viabilidade técnica. O trabalho de Bochnia e Anke (2024) é relevante para a arquitetura do protótipo ao demonstrar que a validade criptográfica de credenciais de longa duração (LLVCs), como diplomas, não deve depender da existência perpétua das chaves do emissor ou do dispositivo do usuário. A crítica levantada sobre a inadequação de mecanismos rígidos de device binding em hardware (HSMs) para documentos que duram décadas informa a necessidade de estratégias de recuperação e rotação de chaves, uma questão que trabalhos futuros deverão abordar.

No âmbito da integração com sistemas legados, (MILENKOVIĆ; VOJKOVIĆ, 2025) validam a necessidade de migração de modelos federados tradicionais (como a infraestrutura AAI@EduHr, análoga à CAFé no Brasil) para carteiras digitais compatíveis com o eIDAS 2.0. Contudo, a ausência de uma arquitetura de software concreta nesse estudo constitui uma lacuna que permanece em aberto. A definição de uma ponte técnica capaz de traduzir atributos de sistemas legados para Credenciais Verificáveis sem interromper processos administrativos existentes constitui uma direção para trabalhos futuros que pode se apoiar nas evidências produzidas pelo protótipo desenvolvido nesta pesquisa.

A análise de Polychronaki et al. (2025) oferece um contraexemplo arquitetural importante. Ao identificar que o uso de Soulbound Tokens (SBTs) e armazenamento centralizado (MongoDB) compromete a privacidade e o direito ao esquecimento (GDPR/LGPD), este trabalho reforça a decisão de projeto de adotar uma arquitetura focada na minimização de dados e no armazenamento local (edge), em detrimento de soluções baseadas em imutabilidade on-chain. Isso justifica a escolha técnica por VCs e DIDs que não expõem metadados de alunos em ledgers públicos.

Finalmente, a viabilidade de operações em ambientes desconectados, relevante para a resiliência de ambientes institucionais, é abordada por Enge et al. (2022b) e Enge et al. (2022a). Embora demonstrem que a comunicação via Bluetooth Low

Energy (BLE) utilizando DIDComm é funcional, os resultados experimentais apontam latências que podem ser proibitivas para controle de acesso em larga escala. Além disso, a divergência desses estudos em relação ao padrão ISO/IEC 18013-5, adotado pela EUDI Wallet para interações de proximidade, indica que implementações futuras devem avaliar a adequação de cada protocolo ao cenário de uso pretendido.

3.3.5 Estado da Arte: Barreiras, Adoção e Metodologias de Avaliação

Esta seção reúne revisões sistemáticas, taxonomias e estudos de adoção que situam o nível de maturidade da tecnologia de identidade descentralizada. Os trabalhos aqui apresentados identificam as barreiras sociotécnicas, propõem metodologias de avaliação padronizadas e discutem os fatores que impedem ou aceleram a difusão dessas soluções no mercado e no setor público.

Barreiras Sociotécnicas para o Lançamento de Carteiras

Lukkien et al. (2023) conduzem um estudo de caso exploratório focado no ecossistema de identidade digital dos Países Baixos para identificar as barreiras sócio-técnicas que impedem o lançamento efetivo de carteiras alinhadas à regulação europeia. Utilizando a literatura de inovação em serviços públicos como lente teórica, os autores validaram, através de workshops com especialistas do setor público e privado, que a principal barreira não é a disponibilidade de tecnologia criptográfica, mas a ausência de recursos de fronteira padronizados. Esses recursos, definidos como interfaces técnicas e administrativas que facilitam a colaboração, incluem especificações de dados semânticos compartilhados e APIs de referência que permitiriam a interoperabilidade real entre diferentes fornecedores de carteira e serviços governamentais.

A análise classifica os obstáculos em quatro categorias: organizacionais, de interação, contextuais e relacionadas às características da inovação. Uma barreira técnica significativa identificada é a dependência de hardware seguro nos dispositivos móveis dos usuários, uma vez que muitos aparelhos em circulação não atendem aos requisitos de segurança exigidos para o armazenamento de credenciais de alto nível de garantia. Além disso, o estudo aponta para um impasse de governança na camada de interação, onde a indefinição sobre quem deve financiar e manter a infraestrutura de confiança, se o Estado ou o mercado, cria incerteza jurídica e inibe investimentos privados na construção de casos de uso além da simples identificação.

Apesar de oferecer um mapeamento abrangente dos desafios de adoção, o trabalho apresenta limitações metodológicas por se basear exclusivamente em percepções qualitativas de atores de um único país, o que pode restringir a generalização dos resultados para contextos com diferentes níveis de maturidade digital. O estudo não avalia tecnicamente se a introdução de frameworks mais recentes, como a Arquitetura de Referência da EUDI Wallet, resolve as barreiras de padronização identifica-

das ou se introduz novas complexidades de implementação. Para o desenvolvimento de um protótipo acadêmico, a principal lição é a necessidade de definir claramente o escopo de suporte a dispositivos legados e de adotar padrões abertos para minimizar a dependência de componentes proprietários de hardware.

Framework de Avaliação Sistêmica para Ecossistemas SSI

Yao et al. (2024) propõem um framework sistemático para a avaliação de sistemas de Identidade Auto-Soberana baseados em blockchain, visando estabelecer uma linha de base para medir capacidade, compatibilidade e interoperabilidade. A metodologia decompõe o ecossistema SSI em três camadas funcionais, Livros-Razão Distribuídos (DLTs), Agentes e Carteiras, e define um conjunto de 45 casos de teste atômicos que cobrem o ciclo de vida completo da identidade, desde o registro de DIDs e esquemas de credenciais até a emissão e verificação de apresentações verificáveis. O estudo valida experimentalmente esse framework aplicando-o a uma ampla gama de implementações de código aberto e comerciais, incluindo nove redes blockchain, dezessete agentes e dez carteiras digitais.

Os resultados da avaliação revelam disparidades significativas na maturidade das soluções. No nível de infraestrutura, redes permissionadas projetadas especificamente para identidade, como Hyperledger Indy, demonstraram total conformidade com os fluxos de trabalho de SSI, enquanto blockchains de propósito geral, como Bitcoin, falharam em suportar nativamente operações essenciais de gerenciamento de DID. Na camada de agentes, o componente ACA-Py (Aries Cloud Agent Python) destacou-se pela alta interoperabilidade, validando a eficácia da arquitetura modular do projeto Hyperledger Aries. No entanto, metade das carteiras testadas falhou na geração ou recuperação de apresentações verificáveis, indicando uma fragilidade crítica na interface com o usuário final.

Apesar de fornecer uma ferramenta valiosa para benchmarking, o trabalho identifica uma limitação estrutural no ecossistema atual: a falta de APIs RESTful padronizadas para a interação entre componentes, o que obriga o uso de SDKs proprietários e dificulta a automação de testes em larga escala. Além disso, o framework proposto foca primordialmente na funcionalidade ("caminho feliz") e na interoperabilidade sintática, deixando de fora uma avaliação profunda da robustez de segurança e das garantias de privacidade, como a resistência a ataques de correlação ou a eficácia de provas de conhecimento zero, aspectos que exigiram frameworks de avaliação dedicados em pesquisas futuras.

Implementação de Recibos de Privacidade no eIDAS

Lindquist (2023) analisam a interseção entre as normas de privacidade (GDPR), os padrões de identidade digital (eIDAS/EUDI) e as tecnologias de registro distribu-

ído (DLT), identificando uma lacuna crítica na gestão do consentimento. O autor argumenta que, embora a regulação exija transparência, os protocolos atuais de carteira digital não oferecem um mecanismo padronizado para gerar "recibos de privacidade"(privacy receipts) — artefatos digitais que registram o que foi consentido pelo usuário, para quem e para qual finalidade. A proposta técnica fundamenta-se na adoção do padrão emergente ISO/IEC 27560 para estruturar esses recibos e no uso da ontologia W3C Data Privacy Vocabulary (DPV) para garantir a semântica interoperável das políticas de privacidade.

No contexto de arquiteturas descentralizadas, o estudo sugere que o hash criptográfico desses recibos de consentimento seja ancorado em ledgers distribuídos ou blockchains, conforme diretrizes da norma ISO/TR 23249. Isso cria uma trilha de auditoria imutável que permite ao usuário comprovar a violação de acordos de dados sem expor o conteúdo sensível do consentimento na cadeia pública. Essa abordagem visa automatizar a verificação de conformidade ("compliance by code") e mitigar a fadiga de consentimento do usuário através de agentes de software que negociam termos com base em preferências pré-configuradas.

Apesar de conceitualmente robusta, a proposta enfrenta desafios de maturidade, uma vez que se baseia em padrões ISO ainda em fase de rascunho ou aprovação recente. O trabalho não apresenta uma implementação de referência que demonstre como a geração e armazenamento desses recibos impactam a performance e a usabilidade das carteiras móveis, nem como a revogação de consentimento seria propagada eficazmente em sistemas DLT imutáveis. Para o protótipo acadêmico, a lição principal é a necessidade de incluir metadados de consentimento estruturados nas transações de apresentação, mesmo que uma implementação completa da norma ISO/IEC 27560 seja inviável no curto prazo.

Mudança de Paradigma: Autossociedade e Minimização de Dados

Babel et al. (2025) analisam a mudança de paradigma da gestão de identidade federada para a Identidade Auto-Soberana, estabelecendo as bases teóricas para ecossistemas baseados em carteiras digitais. O trabalho fundamenta a arquitetura em torno do triângulo de confiança composto por emissores, portadores e verificadores, contrastando sistemas baseados em silos de dados com ecossistemas abertos onde a confiança é ancorada em registros de dados verificáveis, frequentemente implementados via tecnologias de registro distribuído. O estudo sistematiza as propostas de valor econômico e operacional, destacando que a eficiência para o verificador provém da automação criptográfica da validação, enquanto o emissor se beneficia da redução de responsabilidade sobre a custódia de dados pessoais.

No âmbito da privacidade, os autores discutem como a tecnologia pode mitigar o paradoxo da privacidade, onde usuários desejam controle mas frequentemente

cedem dados por conveniência. A solução técnica apontada reside na implementação de divulgação seletiva e Provas de Conhecimento Zero, permitindo que a carteira digital prove predicados, como a maioria, sem revelar a data de nascimento ou criar identificadores correlacionáveis. O artigo também aborda a integração com o regulamento eIDAS 2.0, posicionando a carteira europeia como um catalisador para a adoção de padrões de identidade descentralizada em mercados eletrônicos business-to-business e business-to-consumer.

Apesar de apresentar um panorama robusto dos benefícios, o trabalho identifica uma lacuna crítica na literatura referente aos modelos de incentivo econômico. A análise aponta um desequilíbrio onde os custos de infraestrutura recaem sobre os emissores, enquanto os benefícios financeiros de eficiência são capturados majoritariamente pelos verificadores, o que cria uma barreira para a adoção voluntária por emissores do setor privado. Além disso, os autores ressaltam que a pesquisa atual foca excessivamente em aspectos técnicos de protocolos e criptografia, negligenciando os desafios organizacionais e os efeitos de rede necessários para que as carteiras digitais superem a fase de projetos-piloto e alcancem massa crítica de uso.

Levantamento Abrangente sobre DIDs e Credenciais Verificáveis

O trabalho de Mazzocca et al. (2025) fornece um levantamento atualizado sobre os blocos de construção fundamentais da identidade descentralizada: Identificadores Descentralizados e Credenciais Verificáveis. Diferentemente de revisões anteriores focadas apenas em SSI, este estudo expande o escopo para incluir a aplicação dessas tecnologias em domínios emergentes como IoT e computação de borda, além de analisar a conformidade com regulações recentes como o eIDAS 2.0. Os autores realizam uma análise comparativa das principais implementações e bibliotecas disponíveis (como Hyperledger Aries, Veramo e DIDKit), oferecendo um guia prático para desenvolvedores selecionarem as ferramentas mais adequadas para prototipagem, uma contribuição direta para a fase de implementação deste trabalho.

O estudo aprofunda-se nas ameaças de segurança específicas a estes padrões, como a correlação de DIDs e ataques de repetição em apresentações verificáveis, propondo estratégias de mitigação que incluem a rotação de chaves e o uso de provas de conhecimento zero para minimização de dados. Uma contribuição significativa é a discussão sobre a interoperabilidade entre diferentes métodos DID e formatos de credenciais (JSON-LD vs. JWT), destacando que a fragmentação técnica ainda é uma barreira considerável para a adoção global. O artigo também mapeia iniciativas governamentais globais, situando a EUDI Wallet como um dos projetos mais ambiciosos de aplicação prática desses padrões em larga escala.

Os autores também discutem o ecossistema de governança, enfatizando que a tecnologia por si só não resolve problemas de confiança. Eles argumentam que a

adoção de DIDs e VCs exige um alinhamento estreito com estruturas legais, como o GDPR na Europa, para garantir que a “autossociedade” não se torne um vetor para a perda de responsabilidade legal. A revisão aponta para a necessidade de pesquisas futuras em mecanismos de revogação eficientes e na usabilidade de carteiras digitais, temas que são centrais para a aceitação de um protótipo no ambiente universitário.

Maturidade e Taxonomia de Aplicações de Identidade Descentralizada

Schumm et al. (2025) realizam um levantamento abrangente sobre o estado da adoção de tecnologias de identidade no mundo real, estabelecendo uma distinção taxonômica crítica entre Identidade Descentralizada e Identidade Auto-Soberana. Segundo os autores, enquanto a primeira refere-se à descentralização da infraestrutura técnica (como o uso de blockchain), a segunda exige necessariamente a descentralização da governança, onde nenhuma entidade única possui controle sobre o sistema. O estudo analisa 20 plataformas e diversos projetos-piloto, incluindo iniciativas governamentais como o ZugID na Suíça e o Bhutan NDI, e comerciais como o Worldcoin, contrastando as promessas teóricas dos whitepapers com as funcionalidades efetivamente implementadas.

A análise técnica revela que a maioria das implementações atuais falha em entregar a soberania completa prometida pelo modelo SSI. Observa-se uma forte dependência de modelos de negócio do tipo Software-as-a-Service (SaaS) e de carteiras proprietárias fechadas, o que reintroduz pontos de controle centralizados e vendor lock-in, contradizendo o princípio de portabilidade. Além disso, o estudo identifica lacunas tecnológicas severas que impedem a adoção em massa, especificamente a ausência de mecanismos padronizados para recuperação de chaves criptográficas (além das frases mnemônicas básicas) e a falta de suporte robusto para a verificação de credenciais em cenários offline, uma funcionalidade crítica para documentos de identidade oficiais.

A contribuição crítica do trabalho reside na desmistificação do cenário de adoção. Os autores evidenciam que muitos projetos rotulados como SSI utilizam o termo apenas para fins de marketing, mantendo estruturas de governança centralizadas (como o uso de blockchains privadas permissionadas onde apenas uma organização valida transações). Para o desenvolvimento de um protótipo acadêmico, este estudo serve como um alerta para evitar a dependência de plataformas comerciais “caixa-preta” e reforça a necessidade de focar em componentes de código aberto que garantam a transparência e a interoperabilidade real, em vez de apenas a descentralização da infraestrutura de armazenamento.

Convergência de IA e Blockchain em Carteiras Digitais

Leka et al. (2025) exploram a convergência entre Inteligência Artificial (IA) e blockchain no contexto da identidade digital na Albânia, visando o alinhamento com os padrões da União Europeia. O estudo discute o uso de IA para aprimorar a verificação biométrica e a detecção de fraudes em carteiras digitais, enquanto a blockchain é posicionada como a infraestrutura para garantir a descentralização e a imutabilidade dos registros.

Revisão Sistemática de Processos eKYC via SSI e DIDs

Ahmed et al. (2025) conduzem uma revisão sistemática da literatura fundamentada no método PRISMA para investigar a convergência entre tecnologias de registro distribuído e processos de Conheça Seu Cliente Eletrônico. O estudo analisa 44 trabalhos selecionados para avaliar como a Identidade Auto-Soberana e os Identificadores Descentralizados transformam a verificação de identidade, substituindo a gestão documental manual por automação baseada em contratos inteligentes. A análise tecnológica revela uma predominância da plataforma Ethereum, presente em 33% das soluções, seguida pelos frameworks Hyperledger como Fabric e Indy com 18%, enquanto o armazenamento de documentos criptografados é frequentemente delegado a sistemas descentralizados como o IPFS para garantir a integridade dos dados fora da cadeia.

No âmbito da privacidade e minimização de dados, os autores categorizam as técnicas de divulgação seletiva em três abordagens principais: o uso de credenciais atômicas, assinaturas criptográficas avançadas como BBS+ e estruturas de dados baseadas em hash como Árvores de Merkle. O trabalho destaca a aplicação crescente de Provas de Conhecimento Zero, especificamente zk-SNARKs e Bulletproofs, para permitir a validação de atributos sem a revelação dos dados subjacentes. Essas tecnologias são posicionadas como essenciais para cumprir regulamentações de proteção de dados, permitindo que instituições financeiras e outros verificadores autenticuem clientes sem a necessidade de custódia de dados sensíveis desnecessários.

Apesar do potencial disruptivo, a revisão identifica lacunas críticas que impedem a adoção em larga escala. Os autores apontam a vulnerabilidade dos algoritmos criptográficos atuais, como ECDSA e RSA, a futuros ataques de computação quântica, enfatizando a necessidade urgente de pesquisa em criptografia pós-quântica para identidades digitais. Além disso, o estudo critica a falta de padronização nas APIs de integração entre blockchains e sistemas bancários legados, bem como a ausência de avaliações de desempenho rigorosas que meçam a latência e o custo computacional dessas soluções em cenários de alta demanda. A usabilidade permanece um desafio não resolvido, especialmente no que tange aos mecanismos de recuperação de

chaves privadas e à gestão segura de carteiras por usuários não técnicos.

Vaziry et al. (2025) propõem uma taxonomia abrangente para classificar sistemas de gestão de identidade baseados em tecnologias de registro distribuído, desenvolvida através de um processo iterativo de revisão de literatura e validação com especialistas. A estrutura taxonômica organiza-se em três grupos de dimensões principais: Âncora de Confiança, Identidade e Livro-Razão. Na dimensão de confiança, o estudo diferencia entre modelos de âncora única e múltipla, e analisa como a confiança é tecnicamente realizada (por exemplo, via contratos inteligentes ou estruturas de dados autenticadas). Na dimensão de identidade, a taxonomia dissectiona a governança (centralizada vs. consórcio), os tipos de identificadores (físicos vs. lógicos) e os mecanismos de prova de posse.

A aplicação prática da taxonomia é demonstrada através da classificação de arquiteturas distintas, como sistemas de identidade para IoT e federações SAML distribuídas. O estudo revela que muitas soluções descritas na literatura como "descentralizadas" mantêm, na prática, âncoras de confiança centralizadas ou governança fechada. A taxonomia permite identificar nuances técnicas críticas, como a distinção entre credenciais ancoradas diretamente on-chain (com riscos de privacidade e escalabilidade) e aquelas que utilizam o ledger apenas para a resolução de identificadores e chaves públicas (modelo DID/VC padrão).

Apesar de fornecer um vocabulário comum e rigoroso para o campo, o trabalho limita-se a uma ferramenta de classificação descritiva. A taxonomia não incorpora métricas de qualidade ou desempenho, impedindo a comparação direta da eficácia das diferentes arquiteturas classificadas. Além disso, a granularidade das dimensões propostas pode adicionar complexidade excessiva para a avaliação de protótipos em estágio inicial, exigindo um nível de detalhamento técnico que muitas vezes não está disponível em especificações de alto nível. Para este trabalho, a taxonomia serve como um checklist para garantir que a arquitetura do protótipo seja descrita de forma completa e precisa, cobrindo aspectos frequentemente negligenciados como a revogação e a recuperação de identidade.

Feng et al. (2025) apresentam uma revisão abrangente da evolução dos sistemas de gestão de identidade (IDMS), traçando uma linha histórica que vai desde as arquiteturas cliente-servidor centralizadas baseadas em LDAP dos anos 1990, passando pelos modelos federados consolidados com SAML e Liberty Alliance, até chegar aos paradigmas descentralizados baseados em blockchain. O estudo classifica as soluções contemporâneas em dois grandes grupos: sistemas de propósito geral e implementações de domínio específico (saúde, educação, IoT e energia). A análise técnica destaca que, enquanto o setor financeiro e de saúde priorizam a divulgação seletiva e a revogação eficiente para conformidade regulatória (eKYC, GDPR), as implementações em IoT focam na interoperabilidade leve e na gestão autônoma de

identidade de dispositivos.

A revisão aprofunda-se na análise de segurança, identificando cinco categorias críticas de ameaças para IDMSs baseados em blockchain: impersonificação, repúdio, violação de integridade, ataques de vinculação (linkability) e ameaças quânticas. Os autores constataam que apenas uma fração mínima (4%) dos 47 estudos analisados aborda a resistência pós-quântica, apontando uma vulnerabilidade sistêmica em arquiteturas que dependem exclusivamente de criptografia de curvas elípticas tradicionais. Além disso, o trabalho evidencia que a maioria das soluções acadêmicas implementa funcionalidades de forma isolada, focando ou em privacidade (ZKP) ou em interoperabilidade, falhando em oferecer arquiteturas unificadas que atendam simultaneamente a todos os requisitos essenciais de um ecossistema maduro.

A contribuição crítica do artigo reside na identificação de lacunas não apenas técnicas, mas também sócio-econômicas. Os autores argumentam que a pesquisa atual negligencia os custos de transição e os incentivos econômicos necessários para que instituições legadas adotem modelos descentralizados. Para o desenvolvimento de um protótipo universitário, a revisão sugere que a arquitetura deve ser projetada desde o início com agilidade criptográfica para suportar futuros algoritmos pós-quânticos e deve priorizar a integração com padrões abertos (como W3C DID e VC) para evitar a criação de novos silos de identidade, mesmo que descentralizados.

Comparação entre Sistemas Centralizados e Descentralizados

Li et al. (2024) apresentam uma comparação direta entre sistemas de identidade centralizados e descentralizados, focando nas diferenças de controle de dados, segurança e ponto único de falha.

Discussão e Relevância para o Trabalho

A consolidação do estado da arte revela que, embora a tecnologia de identidade descentralizada esteja teoricamente madura, sua adoção enfrenta barreiras sistêmicas. Lukkien et al. (2023) contribuem fundamentalmente ao identificar que a prontidão tecnológica (TRL) das soluções não é suficiente para o sucesso da implementação em larga escala. O estudo fornece um mapeamento dos requisitos não funcionais críticos, como a usabilidade e a clareza nos modelos de responsabilidade, que devem ser considerados arquiteturalmente desde o início do desenvolvimento de protótipos de carteiras digitais.

Corroborando a necessidade de rigor na implementação, Yao et al. (2024) formalizam um framework de testes que pode ser utilizado para validar protótipos de carteiras digitais. A metodologia oferece um roteiro para garantir que novas implementações não apenas funcionem isoladamente, mas sejam capazes de interagir correta-

mente dentro de um ecossistema heterogêneo, validando a conformidade técnica com os requisitos arquiteturais.

Na esfera da usabilidade e transparência, Lindquist (2023) destacam que, sem um formato comum para recibos de consentimento, os usuários perdem a capacidade de rastrear seus dados. O artigo sugere que a carteira deve implementar "rótulos de privacidade" padronizados e auditáveis, permitindo alertar o usuário sobre solicitações excessivas.

Analisando a proposta de valor macroscópica, Babel et al. (2025) servem como fundamentação teórica para justificar a adoção do modelo descentralizado em detrimento de sistemas de login federados proprietários. Complementarmente, Schumm et al. (2025) sugerem que, para o contexto universitário, o protótipo não deve focar apenas na criptografia, mas na experiência do usuário e na facilidade de recuperação de credenciais, apontando a complexidade de gestão de chaves como um entrave crítico.

Fornecendo uma visão abrangente dos blocos de construção, Mazzocca et al. (2025) categorizam os casos de uso e as lições aprendidas sobre a integração de sistemas legados, servindo como base para modelar a emissão de credenciais acadêmicas. Em paralelo, Ahmed et al. (2025) indicam que o processo de eKYC é análogo ao processo de matrícula, e que o uso de Provas de Conhecimento Zero é essencial para a privacidade na verificação de elegibilidade.

Em contextos de mercados emergentes e integração regional, Leka et al. (2025) ilustram os desafios de infraestrutura enfrentados por países fora do bloco europeu que buscam interoperabilidade com a EUDI Wallet.

Por fim, as taxonomias e revisões gerais fornecem a estrutura conceitual para situar o protótipo. Vaziry et al. (2025) oferecem uma taxonomia para classificar a solução desenvolvida em relação a outras arquiteturas de mercado; Feng et al. (2025) servem como referência para a evolução histórica dos sistemas de gestão de identidade; e Li et al. (2024) contribuem para a fundamentação teórica ao contrastar modelos centralizados e descentralizados de identidade digital.

3.4 SÍNTESE DOS RESULTADOS E RESPOSTAS ÀS QUESTÕES DE PESQUISA

Em resposta à primeira questão de pesquisa sobre as principais propostas de arquitetura, a revisão indica uma consolidação do modelo centrado na carteira digital, no qual o usuário atua como o ponto de integração e transporte de dados entre emissores e verificadores. A literatura aponta que a Arquitetura e Estrutura de Referência da Carteira de Identidade Digital da União Europeia se estabeleceu como o modelo dominante para implementações governamentais ao definir uma separação estrita entre a camada de emissão de confiança e a camada transacional. Diferentemente dos modelos federados tradicionais, nos quais o Provedor de Identidade intermedeia cada

acesso, as arquiteturas descentralizadas modernas movem a lógica de apresentação para a borda da rede, o que exige que a carteira digital possua capacidades de gerenciamento de chaves e armazenamento seguro local.

Ainda no contexto da primeira questão, observa-se uma tendência arquitetural para a resolução de problemas de legado por meio de componentes de mediação denominados Pontes ou Agentes de Tradução. Trabalhos analisados demonstram que a substituição completa da infraestrutura de Gestão de Identidade e Acesso existente é inviável no curto prazo. Consequentemente, as arquiteturas mais robustas propõem a inserção de softwares intermediários que traduzem protocolos de identidade auto-soberana para padrões federados consumíveis por aplicações institucionais. No entanto, essa abordagem arquitetural introduz um ponto de compromisso na privacidade, pois exige que o componente de ponte processe os dados descriptografados antes de repassá-los ao serviço final, o que viola parcialmente o princípio de verificação de ponta a ponta.

No que tange à segunda questão de pesquisa referente às principais tecnologias e padrões, os resultados apontam para a obsolescência gradual de soluções baseadas exclusivamente em registros distribuídos permissionados, como o Hyperledger Indy, em favor de padrões abertos da web. A família de protocolos OpenID para Emissão e Apresentação de Credenciais Verificáveis emerge como o padrão de fato para interações remotas devido à sua compatibilidade com a infraestrutura web existente e suporte a dispositivos móveis. Para cenários desconectados e de proximidade, a norma ISO/IEC 18013-5, conhecida tecnicamente como mDoc, é a tecnologia predominante e mandatória na especificação europeia para credenciais de alta segurança como a carteira de motorista móvel.

Complementando a segunda questão no âmbito das primitivas criptográficas de privacidade, identifica-se uma dicotomia entre eficiência e anonimato. Enquanto formatos baseados em assinaturas digitais tradicionais e hashing, como o SD-JWT, oferecem desempenho superior e facilidade de adoção, eles falham em garantir a não vinculabilidade matemática entre múltiplas apresentações. Em contrapartida, tecnologias de Prova de Conhecimento Zero oferecem garantias robustas de privacidade e minimização de dados, mas enfrentam barreiras de implementação em hardware móvel restrito e falta de padronização em bibliotecas de produção. A literatura sugere que a adoção dessas provas criptográficas deve ocorrer no modelo de Software como Produto, executado localmente no dispositivo do usuário, para evitar a dependência de serviços de confiança centralizados.

A análise referente à terceira questão sobre modelos de governança demonstra que a confiança em ecossistemas de larga escala não pode ser puramente algorítmica e depende de âncoras de confiança institucionalizadas. O regulamento eIDAS 2.0 estabelece um modelo hierárquico no qual Listas de Confiança publicadas pelos

Estados-Membros servem como a raiz da cadeia de verificação. Para escalar esse modelo em ambientes transfronteiriços e entre domínios, a literatura propõe o uso da infraestrutura global do Sistema de Nomes de Domínio e suas extensões de segurança DNSSEC como mecanismo de descoberta e publicação de chaves de emissores, o que permite que organizações gerenciem sua autoridade de forma soberana sob seus próprios domínios de internet.

Ainda sobre a terceira questão, a literatura enfatiza a necessidade de mecanismos descentralizados de aplicação de políticas. A governança não deve se limitar à emissão de credenciais, mas deve incluir o credenciamento de verificadores. Modelos propostos sugerem que a carteira digital deve assumir a função ativa de auditoria ao verificar certificados de credenciamento e restrições de acesso dos provedores de serviço antes de permitir a liberação de dados pelo usuário. Contudo, a ausência de esquemas de certificação harmonizados e automatizados para essas carteiras representa um risco de fragmentação regulatória, onde diferentes jurisdições podem impor requisitos de segurança conflitantes.

A análise crítica do estado da arte revela uma lacuna na literatura técnica, caracterizada pela escassez de trabalhos que implementem e avaliem as tecnologias de identidade descentralizada em contextos institucionais de países com infraestruturas de chaves públicas centralizadas. A maioria dos estudos concentra-se em cenários teóricos de Identidade Auto-Soberana baseada em blockchain ou em ecossistemas governamentais com regulamentação específica para esse modelo, como o europeu. Não foram identificados trabalhos que apresentem implementações práticas dessas tecnologias em ambientes acadêmicos brasileiros, documentando as decisões de projeto, as barreiras técnicas e os compromissos envolvidos.

Diante deste cenário, este trabalho propõe o desenvolvimento e a avaliação de um protótipo de carteira digital acadêmica que implementa o ciclo completo de emissão, armazenamento e verificação de credenciais verificáveis utilizando padrões abertos de SSI. O protótipo é configurado como um estudo de caso no ambiente da UFSC e utiliza os padrões e tecnologias identificados nesta revisão, incluindo formatos SD-JWT e AnonCreds, assinaturas Ed25519, Provas de Conhecimento Zero baseadas em circuitos Groth16 e divulgação seletiva de atributos. O objetivo é produzir evidências técnicas sobre a viabilidade dessas tecnologias no contexto brasileiro e fornecer uma base documentada sobre a qual trabalhos futuros possam avançar em direção à integração com a infraestrutura de identidade digital nacional.

Tabela 3 – Matriz Comparativa (Parte 1): Arquiteturas de Integração e Privacidade Avançada.

Referência	Ano	Foco Arquitetural	Tecnologias Chave	Privacidade	Lacuna / Crítica (Gap)
Hoops; Matthes	2024	Ponte SSI-OIDC (Gateway)	Ory Hydra, OIDC4VP	Verificação no intermediário	Ponto único de falha; Quebra criptografia fim-a-fim ao processar dados no servidor.
Castellano et al.	2024	Extensão de IAM (Keycloak)	Keycloak, Java, mDoc	Híbrida; depende do IAM	Complexidade de manutenção; Decifra dados do usuário antes da aplicação final.
Kudra et al.	2025	Carteiras Corporativas	Agentes de Tradução, NFC	Controle de Acesso (ABAC)	Falta padronização técnica; Dificuldade de integração com hardware heterogêneo.
Bakhtina et al.	2023	Descentralização de PKI	Hyperledger Indy, Aries	AnonCreds, ZKP nativo	Alta complexidade operacional; Acoplamento com Hyperledger (difícil portar p/ eIDAS).
Kersic et al.	2023	Convergência On/Off-chain	MetaMask, Ethereum	Assinaturas EIP-712	Fricção de usabilidade (carteiras cripto); Riscos de segurança em plugins.
Flamini et al.	2024	Primitivas Criptográficas	SD-JWT vs. BBS+	Selective Disclosure	Foco teórico; Mecanismos baseados em Hash (SD-JWT) falham na não-vinculabilidade.
Polychronaki et al.	2025	Credenciais Web3	Soulbound Tokens (SBTs)	Imutabilidade via Blockchain	Privacidade comprometida (metadados on-chain); Viola direito ao esquecimento (GDPR).
Bochnia; Anke	2024	Ciclo de vida de Diplomas	DIDs, Logs de Auditoria	Renovação de chaves	Dependência do emissor para verificação a longo prazo; Falta protótipo prático.
Corici et al.	2022	Interoperabilidade Móvel	Proxies, eDelivery AS4	Federated IDs	Dependência excessiva de proxies de tradução; Abordagem centralizada de adaptação.
More et al.	2024	Credenciamento de Verificadores	Certificados X.509, Policies	Privacy-by-Design	Modelo conceitual; Assume existência de Autoridade de Credenciamento funcional.
García-Rodríguez	2024	Emissão Distribuída	Commit-and-prove, Java	Multi-assinaturas (PS-MS)	Alta latência em dispositivos móveis (segundos); Overhead da implementação Java.

Fonte: Elaborado pelo autor (2026).

Tabela 4 – Matriz Comparativa (Parte 2): Casos de Uso Específicos, Segurança e Governança.

Referência	Ano	Foco Temático	Tecnologias Chave	Mecanismo de Segurança	Lacuna / Crítica (Gap)
Buccafurri et al.	2025	Revogação c/ Flexibilidade	AHIBE (Cripto baseada em ID)	Chaves efêmeras	Custo de banda excessivo para o verificador baixar tabelas; Sem teste mobile.
Xie et al.	2025	Carteira Desktop (Windows)	VBS (Virtualization Security)	Isolamento via TPM/VTL1	Dependência de plataforma (Windows); Vendor lock-in; Não aborda interação com RPs.
Ott et al.	2024	TEEs Distribuídos	TrustZone, Noise Protocol	Atestação Remota	Latência em operações complexas; Dependência de hardware específico (ARM).
Comandè; Varilek	2024	Ameaça Pós-Quântica	Algoritmos PQC (NIST)	Criptografia Híbrida	Análise regulatória sem validação de engenharia; Ignora impacto de performance mobile.
Ziegler et al.	2025	Resposta a Incidentes	DIDComm, SIR Framework	Coordenação descentralizada	Processo manual; Carteiras atuais não possuem interfaces de reporte de usuário.
Enge et al.	2022	Comunicação Offline	BLE (GATT), DIDComm	Criptografia autenticada	Alta latência; Divergência do padrão europeu (ISO 18013-5) para proximidade.
Milenković et al.	2025	Regulação Acadêmica	eIDAS 2.0, AAI@EduHr	Autenticação Multifator	Estudo de lacuna legal; Não apresenta arquitetura de software concreta.
Lukkien et al.	2023	Barreiras de Adoção	APIs de Fronteira	N/A (Estudo Qualitativo)	Foco em percepção e governança, sem contribuição técnica de implementação.
Yao et al.	2024	Framework de Avaliação	Blockchain, Agentes SSI	Testes de Compatibilidade	Foco funcional ("caminho feliz"); Falta avaliação robusta de segurança/privacidade.
Lindquist	2023	Recibos de Privacidade	ISO 27560, Hashes em DLT	Trilha de auditoria imutável	Baseado em rascunhos de normas; Sem implementação de referência.
Mazzocca et al.	2025	Survey de VCs e DIDs	Hyperledger, Veramo, DIDKit	Rotação de chaves	Aponta fragmentação técnica e falta de maturidade nas bibliotecas de desenvolvimento.

Fonte: Elaborado pelo autor (2026).

4 ANÁLISE DE TECNOLOGIAS E IMPLEMENTAÇÕES DE REFERÊNCIA

A presente seção detalha a análise de documentos técnicos normativos e repositórios de código aberto pertinentes aos ecossistemas de identidade descentralizada. O foco reside na transição dos modelos conceituais levantados na revisão da literatura para as especificações técnicas de mercado. O texto examina o documento europeu de arquitetura de referência e os protocolos de transporte associados, utilizados como referência para o estado da arte. A infraestrutura de chaves públicas brasileira é analisada em seguida para mapear as restrições e características do cenário nacional. O escopo inclui a avaliação de bibliotecas criptográficas focadas em divulgação seletiva e protocolos de comunicação para dispositivos móveis. Esta análise documental embasa as escolhas tecnológicas para o desenvolvimento do protótipo de carteira digital acadêmica e documenta as condições técnicas que trabalhos futuros deverão considerar ao buscar a integração com a infraestrutura brasileira.

4.1 ESPECIFICAÇÕES TÉCNICAS E PADRÕES DE INTEROPERABILIDADE GLOBAIS

Esta subseção detalha a transição dos modelos conceituais abstratos para especificações de implementação em nível de produção. A análise concentra-se na Arquitetura e Estrutura de Referência da Carteira de Identidade Digital da União Europeia e no texto legal do regulamento europeu de identidade digital (European Digital Identity, 2025; Parlamento Europeu e Conselho da União Europeia, 2024). O estudo técnico destes documentos fundamenta as regras de segurança e as escolhas tecnológicas do protótipo de software. A literatura acadêmica propôs historicamente ecossistemas de identidade baseados em infraestruturas puramente descentralizadas e sem permissão. Os documentos normativos europeus introduzem restrições arquiteturais fortemente centralizadas para garantir segurança jurídica e conformidade regulatória transversal.

4.1.1 Arquitetura de Segurança e Governança

A arquitetura europeia divide a carteira digital em componentes lógicos estritos. O aplicativo instalado no sistema operacional móvel atua apenas como uma interface de gerenciamento para o usuário. As operações criptográficas críticas ocorrem obrigatoriamente dentro de um Dispositivo Criptográfico Seguro de Carteira (European Digital Identity, 2025). A revisão da literatura frequentemente assumiu a execução de provas de conhecimento zero no processador principal do smartphone. O padrão europeu não adota esta prática baseada apenas em software para credenciais de alto

nível de garantia. A exigência de isolamento em hardware visa mitigar a extração de chaves privadas por códigos maliciosos atuantes no sistema operacional.

A vinculação de credenciais ao dispositivo físico constitui um mecanismo central na especificação oficial. O hardware criptográfico seguro gera um par de chaves assimétricas exclusivo para cada nova credencial solicitada. A chave privada permanece bloqueada de forma inalterável na fronteira de segurança do processador. O aplicativo móvel envia apenas a chave pública ao emissor durante a requisição de dados (European Digital Identity, 2025). O emissor assina a credencial atrelando a titularidade dos atributos a esta chave pública específica. O verificador exige uma prova criptográfica de posse desta chave privada durante qualquer processo de apresentação futura.

O estabelecimento de confiança técnica entre a carteira e os provedores de serviços requer novos artefatos digitais. A especificação técnica da Comissão Europeia introduz o Atestado de Unidade de Carteira e o Atestado de Instância de Carteira (European Digital Identity, 2025). Estes dois atestados são assinados digitalmente pelo provedor governamental ou comercial da solução de software. O Atestado de Unidade de Carteira comprova as certificações de segurança subjacentes do componente de hardware local do usuário. O emissor valida obrigatoriamente estes atestados antes de transferir informações pessoais para o dispositivo móvel. Trabalhos acadêmicos focados na soberania do usuário raramente anteciparam a necessidade de certificar a integridade do próprio ambiente de execução em tempo real.

O modelo de confiança da União Europeia diverge estruturalmente das propostas acadêmicas calcadas em registros distribuídos. A revisão sistemática da literatura identificou a dominância de identificadores descentralizados ancorados em redes blockchain. O regulamento europeu institui um modelo ancorado em Infraestrutura de Chaves Públicas tradicional (Parlamento Europeu e Conselho da União Europeia, 2024). A raiz de confiança do sistema depende integralmente de autoridades certificadoras estatais designadas. Estas autoridades emitem certificados do padrão de mercado X.509 para todos os emissores e verificadores do ecossistema. A confiança entre as partes é estabelecida pela verificação matemática da cadeia de assinaturas até alcançar a respectiva raiz estatal.

A distribuição das raízes de confiança ocorre exclusivamente através das Listas de Entidades Confiáveis (European Digital Identity, 2025). Cada governo europeu publica arquivos digitais contendo as chaves públicas exatas de emissores e de verificadores autorizados. O software da carteira executa o download periódico e armazena cópias destas listas em cache local. Este mecanismo substitui completamente a resolução dinâmica de metadados em redes públicas de validação de transações. A pesquisa bibliográfica apresentou modelos arquiteturais alternativos utilizando extensões de segurança do Sistema de Nomes de Domínio para esta finalidade de descoberta

(JEYAKUMAR; KUBACH, 2025). O modelo oficial rejeita a dependência de infraestruturas de rede genéricas em favor de registros governamentais altamente curados.

A interação da carteira com terceiros exige um processo de registro formal rigoroso das entidades solicitantes. O regulamento de identidade determina o credenciamento prévio de qualquer serviço interessado em consumir dados de cidadãos (Parlamento Europeu e Conselho da União Europeia, 2024). O serviço solicitante recebe um Certificado de Acesso de Parte Confiadora após a análise documental do Estado. Este certificado define de forma imutável o escopo exato de atributos permitidos para consumo por aquele serviço específico. A carteira digital lê este certificado e atua ativamente como um ponto de aplicação restrita de políticas de privacidade. O aplicativo bloqueia silenciosamente requisições de dados não listados no certificado governamental da entidade.

A exigência de certificados de acesso materializa alguns achados teóricos recentes da pesquisa acadêmica em privacidade. Estudos prévios propuseram a acreditação obrigatória de verificadores para mitigar a assimetria de informação contra usuários leigos (MORE et al., 2024). A especificação de referência europeia consolida esta proposta ao forçar o aplicativo a validar o escopo do certificado antes da interface gráfica solicitar o consentimento humano (European Digital Identity, 2025). O fluxo de apresentação sofre interrupção imediata caso a assinatura do verificador conste como inválida nas listas estatais. Este design técnico impede a viabilidade de ataques de pescaria cibernética e limita a coleta de informações excessivas por empresas.

O tratamento da revogação de credenciais expõe uma clara tensão entre garantias de anonimato e eficiência de rede. A literatura focada em privacidade defende o uso de acumuladores criptográficos e complexas provas de não inclusão. Estas primitivas matemáticas impedem o rastreamento do usuário pelo emissor durante rotinas de verificação de status online. O documento arquitetural adota formatos pragmáticos de listas de status baseadas em vetores de bits compactados (European Digital Identity, 2025). O verificador realiza o download periódico de um arquivo binário hospedado pelo emissor para checar um índice numérico correspondente à credencial. A abordagem oficial prioriza larguras de banda reduzidas em dispositivos móveis sobre o anonimato absoluto contra o emissor.

O ciclo de vida de segurança introduz o mecanismo de revogação em cascata para proteger o ecossistema. O provedor do aplicativo monitora continuamente os sinais de integridade reportados pelo sistema operacional do dispositivo hospedeiro. A detecção de permissões administrativas abusivas ou modificações de sistema acarreta a revogação imediata do Atestado de Unidade de Carteira (European Digital Identity, 2025). Os emissores verificam regularmente o status de validade destes atestados atrelados às credenciais emitidas. A invalidação criptográfica do dispositivo força a revogação paralela de todos os documentos governamentais nele armazena-

dos (Parlamento Europeu e Conselho da União Europeia, 2024). O controle final do cidadão sobre seus dados permanece subordinado à manutenção da integridade do hardware verificada pela autoridade central.

A documentação estipula a obrigatoriedade absoluta de autenticação local de duplo fator para o desbloqueio do material criptográfico (European Digital Identity, 2025). O acesso operacional às chaves privadas requer a verificação biométrica associada ao conhecimento de senhas acionadas diretamente no componente de hardware seguro. O uso de mecanismos padrão de autenticação do sistema operacional principal é classificado como insuficiente para a liberação de atributos de alta sensibilidade. Este controle rígido busca garantir a propriedade inalienável da identidade e fornecer proteção técnica contra tentativas de clonagem física do aparelho. Os trabalhos analisados na revisão referem-se a esta capacidade fundamental sob a terminologia de vinculação forte de titularidade.

4.1.2 Protocolos de Comunicação e Transporte de Dados

O intercâmbio de dados entre os componentes do ecossistema depende de protocolos padronizados de transporte. A especificação técnica adota o protocolo OpenID for Verifiable Credential Issuance para a emissão remota de credenciais. Este protocolo estende o framework de autorização OAuth 2.0. O emissor atua como um Servidor de Autorização e a carteira digital atua como o aplicativo cliente (OpenID Foundation Standards, 2024a). O fluxo tem início com uma Oferta de Credencial fornecida pelo emissor. A carteira obtém um token de acesso após a autenticação do usuário. A requisição final é enviada ao Endpoint de Credencial do emissor (OpenID Foundation Standards, 2024a). Esta requisição inclui obrigatoriamente uma Prova de Posse (Proof of Possession) do material criptográfico gerado pela carteira (OpenID Foundation Standards, 2024a). O emissor verifica esta prova e emite a credencial vinculada exclusivamente à chave pública apresentada.

A apresentação remota de credenciais utiliza o protocolo OpenID for Verifiable Presentations. Este padrão define o mecanismo pelo qual a parte confiadora solicita e recebe credenciais da carteira digital (OpenID Foundation Standards, 2024b). A transação inicia-se com um Pedido de Autorização enviado pelo verificador. Este pedido utiliza linguagens de definição de dados, como o Presentation Exchange, para especificar de forma granular quais credenciais e atributos exatos são exigidos para a transação (OpenID Foundation Standards, 2024b). A carteira processa o pedido e constrói uma Resposta de Autorização contendo a Apresentação Verificável correspondente (OpenID Foundation Standards, 2024b). O protocolo suporta fluxos de autenticação executados no mesmo dispositivo e fluxos cruzados entre dispositivos distintos, viabilizando a transferência segura sobre a camada de rede.

4.1.3 Formatos de Credenciais e Divulgação Seletiva

A implementação da divulgação seletiva exige formatos de dados que suportem a ocultação de atributos sem acarretar a quebra da integridade original. A especificação Selective Disclosure for JSON Web Tokens (SD-JWT) define um mecanismo de ofuscação baseado em funções de dispersão criptográfica (hash) (VUCINIC et al., 2024). O emissor gera um valor aleatório único, denominado salt, para cada atributo da credencial. O emissor calcula o hash de um vetor estruturado contendo o salt, o nome do atributo e o valor correspondente (VUCINIC et al., 2024). Estes hashes são inseridos no arranjo explícito `_sd` dentro do corpo do token (VUCINIC et al., 2024). O emissor aplica sua assinatura digital sobre este conjunto de hashes, mantendo os dados originais fora da carga útil assinada.

Durante o fluxo de apresentação, o titular da carteira gera um novo artefato digital contendo o token assinado e as divulgações em texto claro. A carteira seleciona os vetores originais referentes apenas aos atributos explicitamente autorizados para compartilhamento (VUCINIC et al., 2024). O verificador computa o hash de cada vetor recebido e compara o resultado matemático com a lista de hashes presente no token assinado pelo emissor (VUCINIC et al., 2024). O protocolo exige a inclusão de um Key Binding JWT gerado pela carteira para provar criptograficamente a posse da chave privada associada à credencial no momento exato da apresentação (VUCINIC et al., 2024).

O ecossistema global de identidade descentralizada suporta paralelamente o Modelo de Dados de Credenciais Verificáveis definido pelo World Wide Web Consortium (W3C). A estrutura normativa expressa a semântica da credencial através de grafos de dados, frequentemente serializados no formato JSON-LD para garantir interoperabilidade informacional entre domínios (SPORNY et al., 2025). A integridade e a origem da credencial são asseguradas por um objeto de prova (proof) anexado à estrutura (SPORNY et al., 2025).

A resolução das chaves criptográficas necessárias para a verificação do modelo do W3C ocorre nativamente por meio de DIDs (SPORNY et al., 2023). O identificador é resolvido em um Documento DID público que contém a propriedade `verificationMethod` (SPORNY et al., 2023). Esta propriedade lista de forma autoritativa as chaves públicas válidas para a verificação das assinaturas daquela entidade específica (SPORNY et al., 2023). Esta arquitetura elimina a dependência estrita de certificados X.509 centralizados em cenários de identidade auto-soberana pura.

4.1.4 Interações de Proximidade e Operação Offline

Os cenários de verificação presencial sem acesso à rede de internet demandam padrões específicos de comunicação. A norma técnica ISO/IEC 18013-5 define o

formato mDoc para operações de proximidade física (European Digital Identity, 2025). A serialização de atributos utiliza a linguagem Concise Binary Object Representation (CBOR). A estruturação binária reduz significativamente o tamanho da carga útil em relação aos formatos textuais padrão, adequando-se às limitações de banda inerentes aos canais de rádio locais.

A transmissão de dados ocorre através de protocolos de curto alcance. A especificação técnica prevê a utilização mandatória de Near Field Communication (NFC) e Bluetooth Low Energy (BLE) para a troca de mensagens (European Digital Identity, 2025). O fluxo de verificação da credencial realiza-se de forma direta entre o dispositivo móvel do usuário e o terminal de leitura do verificador. A eliminação da dependência de resolução em rede externa assegura a operação ininterrupta do controle de acesso em infraestruturas isoladas.

Tabela 5 – Tecnologias e padrões adotados pela especificação europeia.

Categoria técnica	Padrão ou especificação adotada
Formatos de credencial	ISO/IEC 18013-5 e SD-JWT VC
Protocolo de emissão remota	OpenID for Verifiable Credential Issuance
Protocolo de apresentação remota	OpenID for Verifiable Presentations
Infraestrutura de chaves e confiança	Certificados X.509 e infraestrutura de chaves públicas (PKI)
Provas de conhecimento zero	Funcionalidade planejada, sem protocolo criptográfico fixado
Serialização de dados de proximidade	Concise Binary Object Representation (CBOR)
Mecanismo de descoberta de confiança	Listas de entidades confiáveis em formato de marcação estruturada

4.2 ANÁLISE DE COMPATIBILIDADE E LIMITAÇÕES ARQUITETURAIS NACIONAIS

A presente subseção estabelece a análise comparativa entre a topologia da infraestrutura de identidade digital brasileira e a ARF da EUDI Wallet. O escopo restringe-se à identificação de divergências arquiteturais e criptográficas que impactam a adoção do modelo SSI no cenário nacional (iDAKTO, 2025).

O arcabouço de identificação civil brasileiro opera sob um modelo centralizado, adotando o CPF como identificador universal (Brasil, 2021a) e a CIN como documento primário de identificação (Governo Federal do Brasil, 2026a; Brasil, 2022). A âncora de confiança do sistema é estatal, estruturada hierarquicamente por meio da ICP-Brasil, cuja topologia centralizada diverge fundamentalmente do paradigma de

redes não permissionadas e da utilização de DIDs preconizada pelas implementações de SSL.

A infraestrutura criptográfica nacional apresenta capacidade de atualização algorítmica. O documento normativo DOC-ICP-01.01 (Instituto Nacional de Tecnologia da Informação, 2022) especifica o suporte da ICP-Brasil para a operação com Criptografia de Curvas Elípticas (ECC). Adicionalmente, o regulamento estabelece a prontidão técnica da infraestrutura para a transição e integração de algoritmos de criptografia pós-quântica, com suporte mapeado para os padrões ML-DSA e ML-KEM.

A primeira incompatibilidade arquitetural entre o modelo nacional e a ARF europeia reside nos requisitos de homologação de hardware seguro. A regulamentação da ICP-Brasil exige que a operação de chaves criptográficas primárias seja executada em Módulos de Segurança de Hardware (HSMs) que possuam certificação laboratorial de nível NSH-3, ou em dispositivos físicos dedicados, como smartcards e tokens criptográficos, para a emissão de certificados de usuários finais nos níveis A3 e A4 (Instituto Nacional de Tecnologia da Informação, 2021).

A arquitetura europeia estabelece um modelo distinto para a custódia de chaves, fundamentado no conceito de Dispositivo Criptográfico Seguro de Carteira (WSCD). Esta abordagem delega o armazenamento do material criptográfico e a execução de operações de assinatura ao Ambiente de Execução Confiável (TEE) ou ao Elemento Seguro embutidos nativamente nos processadores de dispositivos móveis comerciais (GlobalPlatform, 2025).

A divergência nas exigências de hardware produz impactos jurídicos diretos no contexto brasileiro. A ausência de atestados de homologação laboratorial emitidos pelo Instituto Nacional de Tecnologia da Informação (ITI) para os módulos de segurança nativos de smartphones comerciais impede, sob a ótica normativa, que provas criptográficas geradas nestes terminais possuam o mesmo status de presunção de validade jurídica incontestável atribuído aos certificados do tipo A3 (Instituto Nacional de Tecnologia da Informação, 2022; Instituto Nacional de Tecnologia da Informação, 2021).

Na camada de autenticação e comunicação em rede, o ecossistema brasileiro concentra o controle de acesso na plataforma gov.br. O sistema opera sob a arquitetura de um Provedor de Identidade Federado, implementando o perfil governamental de garantia iGovBR sobre as especificações do protocolo OpenID Connect (OpenID Foundation, 2026; Ministério da Gestão e da Inovação em Serviços Públicos, 2025; Governo Digital, 2026).

A implementação técnica do fluxo de autorização do provedor governamental estabelece restrições estritas na camada de aplicação cliente. A arquitetura proíbe a utilização de tecnologias de encapsulamento web em ambientes móveis, exigindo a execução do fluxo de autenticação por meio de navegadores nativos. O processo

de requisição de autorização impõe a adoção obrigatória da extensão Proof Key for Code Exchange operando em conjunto com o parâmetro de estado validado no cliente para mitigar vulnerabilidades de interceptação de código e falsificação de requisições (Ministério da Gestão e da Inovação em Serviços Públicos, 2025).

O fluxo de autorização inerente ao modelo federado impõe restrições à privacidade na camada de rede. A arquitetura exige o redirecionamento do tráfego de dados para os servidores do Ministério da Gestão e da Inovação em Serviços Públicos (MGI), concedendo ao operador governamental visibilidade sobre as transações de autenticação e impossibilitando a garantia de desvinculabilidade (unlinkability) estruturalmente exigida em ecossistemas de Identidade Auto-Soberana (Ministério da Gestão e da Inovação em Serviços Públicos, 2025).

A estrutura de controle de acesso no ecossistema nacional opera mediante uma segmentação baseada em níveis de garantia da identidade. A asseveração do nível de garantia Ouro exige a validação da biometria facial contra as bases de dados do Tribunal Superior Eleitoral e da Secretaria Nacional de Trânsito, ou a autenticação via certificado criptográfico emitido sob a cadeia da ICP-Brasil (Governo Federal do Brasil, 2026b; Certifica Certificado Digital, 2026; Sebrae, 2026).

A asseveração dos níveis de garantia reflete-se tecnicamente na estrutura do Token de Identidade emitido pelo provedor governamental. O vetor de Referência de Métodos de Autenticação mapeia os múltiplos fatores de segurança utilizados pelo titular da conta, discriminando o uso de senhas, segundos fatores baseados em tempo e certificados digitais em hardware ou em provedores de nuvem. O objeto de informações de confiabilidade encapsula os identificadores numéricos exatos dos selos de validação, delegando à aplicação cliente a capacidade de verificar programaticamente o cumprimento dos requisitos do nível Ouro por meio da identificação da base biométrica do Tribunal Superior Eleitoral, do registro da Carteira de Identidade Nacional ou do emprego de certificado digital (Ministério da Gestão e da Inovação em Serviços Públicos, 2025).

A execução de processos de verificação de identidade em cenários offline no contexto brasileiro fundamenta-se na tecnologia Vio. Este padrão consiste na geração de um Código QR Seguro, desenvolvido pelo Serviço Federal de Processamento de Dados (SERPRO), programado para encapsular dados biográficos e biométricos do titular em um código bidimensional estático assinado digitalmente pela entidade emissora (Serpro, 2026b; Serpro, 2026a).

A arquitetura criptográfica do padrão Vio apresenta limitações técnicas referentes à preservação da privacidade do usuário. A aplicação de uma assinatura digital monolítica ao pacote de dados estruturado exige a exposição integral de todos os campos contidos na credencial durante a decodificação pelo aplicativo verificador, o que inviabiliza a implementação de mecanismos de Divulgação Seletiva e impossibilita a

adoção de ZKPs (Apple, 2026).

O estabelecimento de interoperabilidade com padrões internacionais em interações de proximidade requer a adoção de protocolos como a norma ISO/IEC 18013-5, a qual especifica a utilização de interfaces de rádio frequência locais (NFC e BLE), associada à reestruturação do formato de dados para o padrão Selective Disclosure JWT (SD-JWT). Estas questões permanecem como desafios para implementações futuras.

Para o protótipo acadêmico desenvolvido neste trabalho, adota-se o método de resolução did:web instanciado nos subdomínios da instituição emissora como mecanismo de ancoragem de confiança. Em uma implementação com integração completa, a validade jurídica do Documento DID poderia ser assegurada mediante a proteção dos canais de comunicação por certificados SSL/TLS emitidos e validados pela cadeia criptográfica da ICP-Brasil.

A integração com a plataforma gov.br para o processo de onboarding de usuários constitui uma direção para trabalhos futuros. Em um cenário de produção, o nível de garantia Ouro da plataforma gov.br poderia ser utilizado para a asseveração da identidade do discente, acoplada ao consumo de dados biográficos através do barramento de interoperabilidade baseado em mTLS do programa Conecta GOV.BR (Universidade Federal de Uberlândia, 2024). O protótipo atual opera sem essa integração, simulando os dados do emissor localmente para demonstrar a viabilidade do ciclo completo de credenciais verificáveis.

De forma análoga, a apresentação de credenciais em cenários de produção no perímetro do campus requer a implementação do protocolo OpenID for Verifiable Presentations (OID4VP), permitindo que a carteira digital móvel execute divulgação seletiva sobre a credencial original e transmita apenas os atributos requeridos para cada transação de acesso. O protótipo implementa esta funcionalidade utilizando o padrão Presentation Exchange (PEX) em modo local.

5 PROPOSTA E DEFINIÇÃO TECNOLÓGICA

A partir das restrições e características da infraestrutura nacional identificadas na análise tecnológica, este trabalho propõe o desenvolvimento de um aplicativo móvel estruturado como uma prova de conceito e um produto mínimo viável. O sistema simula o ciclo completo de emissão, armazenamento criptográfico e verificação de uma carteira digital acadêmica baseada no modelo de Identidade Auto-Soberana, orientada ao contexto da Universidade Federal de Santa Catarina.

O protótipo opera de maneira isolada e não realiza integrações com sistemas institucionais reais da universidade ou com bases governamentais. O objetivo central da proposta consiste em comprovar a viabilidade técnica da aplicação de credenciais verificáveis e estabelecer um estudo inicial sobre as capacidades destas tecnologias no ambiente móvel. Os resultados obtidos visam fundamentar trabalhos futuros voltados para o desenvolvimento de carteiras digitais de uso geral dotadas de integrações sistêmicas em ambiente de produção.

5.1 METODOLOGIA DE SELEÇÃO E DESENVOLVIMENTO

O desenvolvimento deste protótipo adotou um roteiro estruturado para garantir a fundamentação técnica do código implementado. A Figura 1 apresenta o fluxograma geral executado ao longo da pesquisa. A análise documental das especificações da Carteira de Identidade Digital Europeia e do ecossistema brasileiro embasou a definição da arquitetura do aplicativo móvel.

A materialização da proposta técnica exigiu um processo de definição metodológico, ilustrado na Figura 2. A seleção de ferramentas para o desenvolvimento do protótipo móvel envolveu a avaliação técnica dos frameworks Flutter e React Native, estritamente baseada na disponibilidade de bibliotecas de SSI e implementações criptográficas para o ambiente móvel. O processo adotou um fluxo iterativo para priorizar o uso de bibliotecas de código aberto em todos os protocolos do sistema.

5.2 SELEÇÃO DE TECNOLOGIAS E BIBLIOTECAS

A definição da topologia, do esquema de dados e do caso de uso da universidade demanda a especificação preliminar da pilha tecnológica. As capacidades de integração sistêmica e as restrições arquiteturais do protótipo móvel são delimitadas pelas bibliotecas de software adotadas no código-fonte.

A escolha do React Native fundamenta-se na abrangência do ecossistema de dependências voltadas para Identidade Auto-Soberana e execução de algoritmos criptográficos. A arquitetura estruturada sobre a implementação de TurboModules e

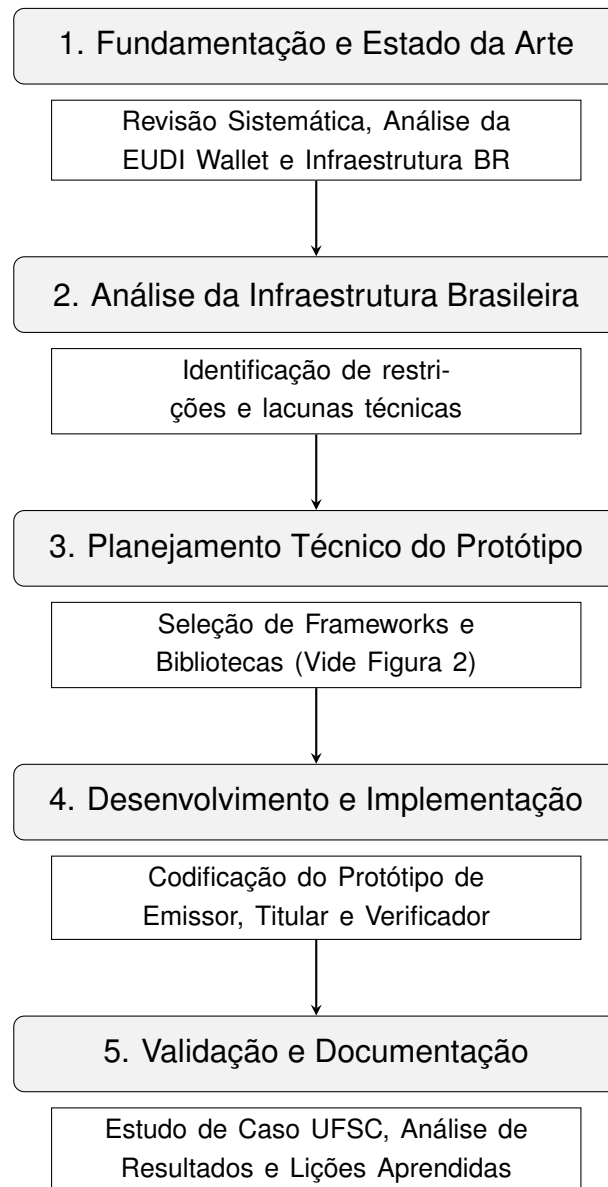


Figura 1 – Fluxograma geral das etapas de desenvolvimento da pesquisa.

da interface JavaScript viabiliza a execução de processos criptográficos intensos sem requerer o uso de código nativo direto (Meta Platforms, Inc., 2026).

O núcleo operacional da carteira digital provém da biblioteca de código aberto Credo-TS. Este módulo fornece as abstrações primárias do agente de identidade, instrumentando o ciclo de vida das credenciais verificáveis, as conexões de rede e o armazenamento protegido no dispositivo físico. A integração viabiliza a resolução de identificadores descentralizados baseados em domínio web (OpenWallet Foundation, 2026).

A implementação de provas de conhecimento zero no escopo móvel visa comprovar a utilidade dessas primitivas criptográficas em hardware com recursos limitados. O suporte à divulgação seletiva e à desvinculabilidade das transações origina-se da biblioteca AnonCreds implementada no React Native, englobando as assinaturas

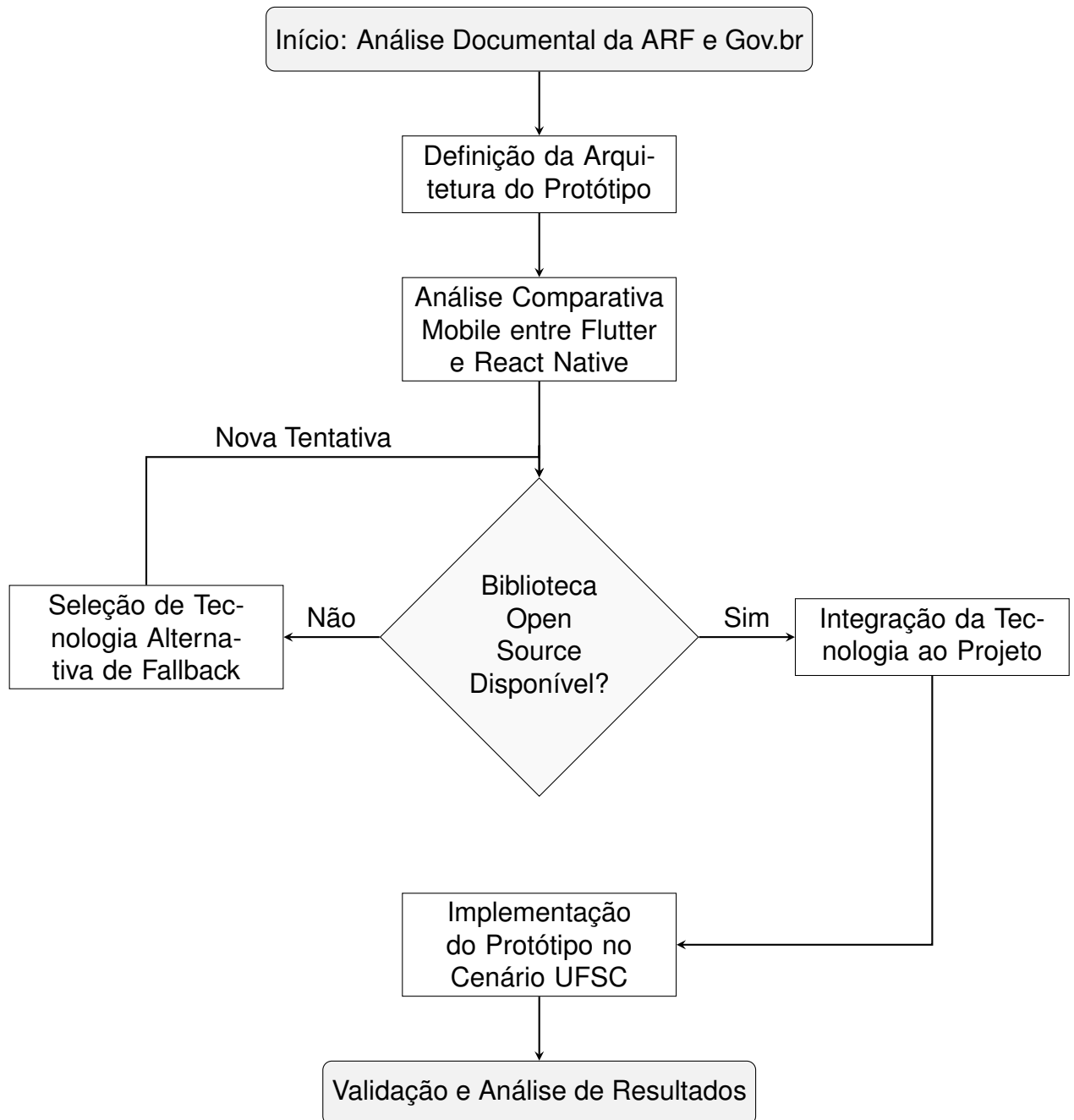


Figura 2 – Fluxo metodológico com iteração para seleção tecnológica.

exigidas pela especificação. A compilação de circuitos matemáticos de conhecimento zero e sua respectiva execução direta ocorrem através do pacote mopro, viabilizando a geração de provas matemáticas computacionais localmente no cliente (Hyperledger Foundation, 2026; Mopro, 2026).

O protótipo incorpora nativamente o formato de tokens web assinados por divulgação seletiva e a camada de requisições de Presentation Exchange. Este conjunto tecnológico estabelece interfaces explícitas para a separação de atributos por funções de dispersão criptográfica e para a formulação de respostas de apresentação padronizadas pelo consórcio responsável (European Commission, 2026). A Tabela 6

sintetiza as bibliotecas definidas pelo planejamento.

Tabela 6 – Síntese das tecnologias e bibliotecas selecionadas para o protótipo móvel

Componente Arquitetural	Tecnologia/Biblioteca	Justificativa Técnica
Framework de Desenvolvimento	React Native	Presença de bibliotecas SSI atualizadas e compilação híbrida com acesso as primitivas dos sistemas operacionais.
Agente de Identidade	@credo-ts/core	Orquestração de carteiras seguras e suporte nativo à geração de chaves privadas locais.
Privacidade e Assinaturas	@hyperledger/anoncreds-react-native	Implementação da especificação de conhecimento zero nativo para credenciais de escopo fechado.
Provas Matemáticas Complexas	mopro-react-native-package	Execução de circuitos Groth16 e algoritmos criptográficos avançados no cliente.
Formatos de Apresentação	eudi-wallet-kit-react-native	Adoção do modelo de ofuscação de atributos estruturados em tokens da web de divulgação seletiva.

5.3 DEFINIÇÃO DO PROTÓTIPO

A aplicação móvel resultante do planejamento, denominada Carteira Digital Acadêmica SSI, executa todo o fluxo de ciclo de vida atrelado a identidades auto-soberanas no contexto educacional. O sistema realiza as operações sem solicitar comunicação contínua com serviços de internet ou redes de registro distribuído de terceiros, encapsulando as entidades de emissor, titular e verificador no ambiente local.

5.3.1 Objetivo e Funcionalidades Centrais

A finalidade tecnológica do protótipo consiste em viabilizar a implementação de uma carteira estudantil capaz de preservar os limites de privacidade dos usuários a partir da divulgação seletiva de campos textuais. O sistema assegura o modelo de criptografia assimétrica na emissão, permite a comunicação local direta na verificação de autenticidade e utiliza provas de conhecimento zero em atributos onde revelar o conteúdo real não atende ao princípio da minimização de dados. A modelagem segue integralmente as determinações técnicas do World Wide Web Consortium e da Decentralized Identity Foundation.

Cinco funções organizam a arquitetura estrutural da aplicação desenvolvida:

1. **Geração de identidade digital:** Criação de perfis embasados em identificadores descentralizados com respectiva geração de chaves assímetrias Ed25519 armazenadas em cofre Aries Askar.
2. **Emissão de credenciais:** Simulação de uma central emissora de atestados acadêmicos englobando atributos de identificação primária, benefícios assistenciais booleanos e listas estáticas de permissão predial. O formato do objeto emitido pode adotar SD-JWT ou AnonCreds.
3. **Armazenamento cifrado:** Escrita de objetos assinados nos diretórios seguros das plataformas móveis nativas com uso de algoritmos AES-256 e aplicação de mecanismos anti-corrida concorrente.
4. **Apresentação com divulgação seletiva:** Leitura de pedidos originados por verificadores externos sob as normas de Presentation Exchange e consequente solicitação de aceite ao portador na interface gráfica.
5. **Verificação de credenciais:** Validação encadeada cobrindo assinatura, registro em hierarquia do emissor, correspondência estrutural da requisição, validade de provas e controle de uso único por indicadores fixos.

5.3.2 Arquitetura de Provas de Conhecimento Zero

A estrutura do protótipo engloba dois arranjos de ocultamento. O uso de assinaturas do tipo Camenisch-Lysyanskaya avalia os vínculos restritos da credencial. A execução via biblioteca mopro processa os arquivos lógicos em circuito Groth16. O circuito de função de faixa etária verifica matematicamente se o ano base do estudante excede a idade mínima para atividades reguladas. O circuito de equivalência executa correspondência com base na dispersão SHA-256 de um estado alfanumérico. O circuito bloqueador aplica a função determinística de Poseidon para entregar identificadores irreversíveis atrelados a cada sessão, evitando votos ou interações consecutivas sob o mesmo atestado de titularidade.

5.3.3 Cenários de Validação Requisitados

A delimitação do desenvolvimento da carteira fixou quatro casos de uso no perímetro educacional para a demonstração prática das tecnologias listadas:

1. **Restaurante Universitário:** Apresentação da situação estudantil e vínculo de subsídio alimentar perante as catracas eletrônicas empregando a separação de atributos de hash.
2. **Eleições Estudantis:** Liberação de urna para discentes mediante a prova de posse de credencial ativa contendo o identificador Poseidon anti-redundância.

3. **Verificação de Maioridade:** Comprovação inquestionável do limiar de idade necessário para acesso a eventos com classificação indicativa sem compartilhamento da data exata de nascimento.
4. **Acesso Físico:** Entrada em alas de centros tecnológicos dependendo da validação visual ou remota dos identificadores de local contidos nos vetores de dados autorizados da carteira digital.

5.3.4 Hierarquia de Confiança Implementada

O protótipo opera uma base algorítmica hierárquica baseada no formato das autoridades certificadoras brasileiras. O identificador eletrônico originado pelo reitor ou instância máxima atua com material auto-assinado. Os subcentros, as direções de campus e as secretarias mantêm pares de chaves validados pelo escalão superior na emissão do certificado. A verificação examina todos os nós registrados até localizar a chave raiz de confiança. A simulação da verificação cruzada comprova os modelos matemáticos teóricos da infraestrutura de chaves descentralizadas em topologias estritamente burocráticas.

5.3.5 Limites Operacionais e Escopo do Protótipo

Conforme introduzido, a natureza de prova de conceito da aplicação implica em simplificações em relação às imposições normativas de larga escala descritas na análise tecnológica. É fundamental enfatizar que o MVP não tem como objetivo o desenvolvimento de um aplicativo de carteira digital destinado ao uso geral. Ao invés disso, o sistema atua como um instrumento focado estritamente no estudo prático do ciclo de emissão e verificação de credenciais, servindo para testar e validar as tecnologias e bibliotecas de código aberto atualmente disponíveis para o ambiente móvel.

No que tange ao armazenamento criptografado, a custódia das chaves utiliza o enclave de segurança nativo do sistema operacional móvel (*Android Keystore*), uma vez que o acesso a hardwares seguros com certificação laboratorial rigorosa, como exigidos na infraestrutura europeia e brasileira, foge ao escopo restrito do desenvolvimento acadêmico.

Além da ausência de integrações institucionais com a ICP-Brasil ou com a plataforma gov.br para a asseveração do *onboarding* de usuários, o projeto adota um modelo em que o ciclo completo das credenciais, englobando os papéis lógicos de emissor, titular e verificador, é executado internamente dentro do próprio aplicativo. Esta decisão de design visa simplificar substancialmente a realização de testes e a demonstração do funcionamento ininterrupto do sistema. Como consequência dessa operação isolada, o uso de protocolos de transporte remoto (como OID4VCI e

OID4VP) sobre conexões de longa distância é dispensado, com a troca de atributos ocorrendo apenas através das interfaces locais.

As divergências documentadas entre o protótipo desenvolvido e os modelos de referência oficiais não inviabilizam a análise de viabilidade dos componentes criptográficos essenciais. Pelo contrário, tais limitações delimitam claramente o perímetro da pesquisa, estabelecendo um registro técnico que poderá orientar o planejamento e a adequação de futuros trabalhos que busquem a integração deste modelo ao ambiente de produção nacional.

6 DESENVOLVIMENTO E ARQUITETURA DO PROTÓTIPO

O presente capítulo documenta a estrutura técnica do protótipo de carteira digital acadêmica desenvolvido como instrumento de validação prática das especificações analisadas nos capítulos precedentes. A descrição abrange a organização modular do código-fonte, os padrões arquiteturais empregados, os modelos de dados, os mecanismos criptográficos implementados e as estratégias de garantia de qualidade adotadas. A Figura 3 apresenta o mapeamento do Triângulo de Confiança SSI para os módulos concretos implementados neste protótipo.

6.1 ORGANIZAÇÃO DO PROJETO E HIERARQUIA DE MÓDULOS

O protótipo foi desenvolvido como uma aplicação React Native gerenciada pelo framework Expo, utilizando TypeScript como linguagem principal. A Tabela 7 apresenta a hierarquia de diretórios de primeiro nível e a responsabilidade de cada módulo.

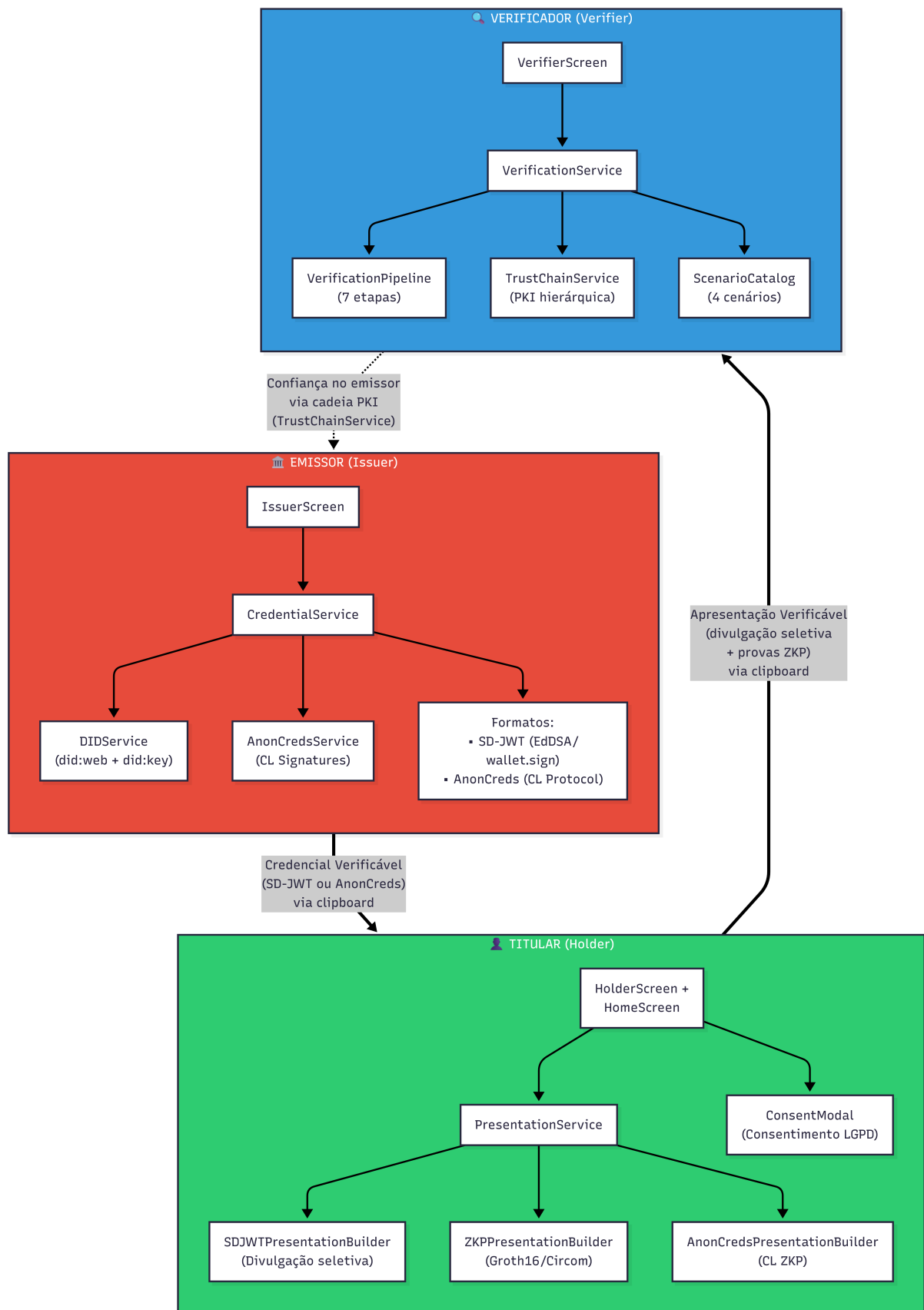


Figura 3 – Mapeamento do triângulo de confiança SSI para os módulos concretos do protótipo.

Tabela 7 – Hierarquia de diretórios do projeto e responsabilidades.

Diretório	Responsabilidade
src/App.tsx	Ponto de entrada da navegação (React Navigation). Contém as definições do <i>Stack Navigator</i> raiz e do <i>Bottom Tab Navigator</i> com as rotas para cada módulo funcional.
src/components/	Componentes visuais reutilizáveis: modais de consentimento, seletores de atributos, indicadores de cadeia de confiança, leitura de QR codes, entre outros (11 componentes).
src/screens/	Telas de apresentação: Emissor, Titular, Verificador, Home, Logs, Glossário, Diagnósticos e Inicialização (8 telas).
src/services/	Camada de lógica de negócios: 20 módulos de serviço organizados em subdiretórios para apresentações (presentations/), verificação (verification/) e testes de runtime (runtimeTests/).
src/stores/	Gerenciamento de estado reativo da interface utilizando a biblioteca Zustand.
src/types/	Definições de tipos TypeScript, interfaces de serviço e contratos de inversão de dependência (374 linhas).
src/utils/	Constantes compartilhadas, sistema de temas, utilitários de acessibilidade, rotas e mensagens de erro.
circuits/	Código-fonte dos circuitos Circom para provas de conhecimento zero: age_range, status_check and nullifier.
circuits/build/	Artefatos compilados dos circuitos: .r1cs, .sym, .vkey.json e o arquivo de cerimônia .ptau.
scripts/	Scripts de pós-instalação para correção de compatibilidade de compilação nativa (patch-hyperledger-cmake.js).
docs/	Documentação técnica auxiliar: arquitetura, decisões de projeto, guia de configuração ZKP e especificação de API.

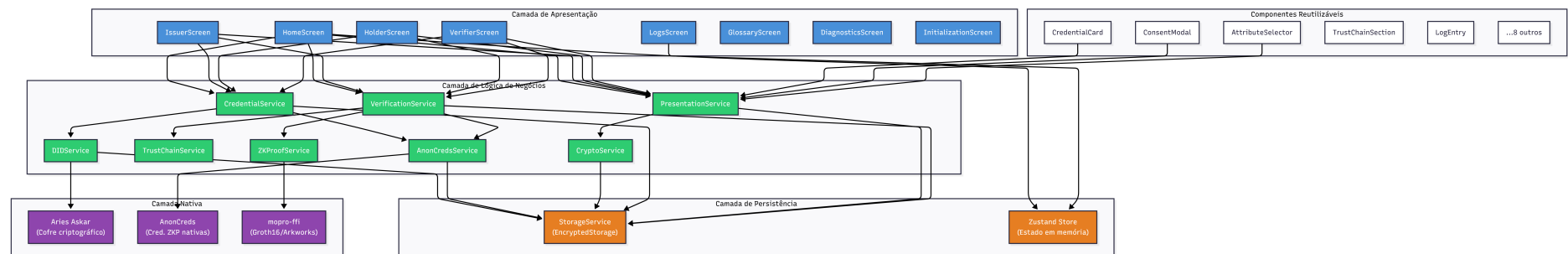


Figura 4 – Arquitetura em camadas do protótipo de carteira digital acadêmica.

A arquitetura em camadas do sistema, ilustrada na Figura 4, demonstra a separação do projeto. A camada de apresentação (`screens/` e `components/`) comunica-se exclusivamente com a camada de lógica de negócios (`services/`) por meio de interfaces tipadas. A camada de persistência (`StorageService`) encapsula o acesso ao armazenamento cifrado do dispositivo. A camada nativa é acessada indiretamente por meio de bindings React Native para as bibliotecas `aries-askar`, `anoncreds` and `mopro-ffi`.

6.2 PADRÕES DE PROJETO E COMPOSIÇÃO DE DEPENDÊNCIAS

A base de código estrutura-se sobre padrões de projeto consolidados para promover o desacoplamento e a testabilidade dos módulos. O sistema adota o padrão de Composição Raiz (*Composition Root*) para a instanciação e interligação de serviços. O módulo `container.ts` centraliza a criação de todas as instâncias por meio de injeção por construtor, organizadas em seis níveis hierárquicos de dependência. Cada serviço declara suas dependências como parâmetros do construtor tipados por interfaces abstratas, conforme o Princípio de Inversão de Dependência.

Adicionalmente, serviços complexos operam sob o padrão *Facade*, ocultando a complexidade de subsistemas internos. O `PresentationService` unifica a construção de apresentações delegando as operações específicas a construtores especializados em algoritmos estruturados. O `VerificationService` orquestra a validação por meio do padrão *Chain of Responsibility*, onde uma série de etapas independentes acumula resultados em um contexto assíncrono. O padrão *Strategy* é implementado na detecção de formatos de credenciais e na seleção de modos de transporte, permitindo a extensão do sistema sem alteração da lógica central.

A Tabela 8 apresenta os níveis de dependência e os respectivos serviços.

Tabela 8 – Hierarquia de injeção de dependências (Composition Root).

Nível	Serviços	Dependências
0	<code>LogService</code> , <code>StorageService</code>	Nenhuma (serviços folha)
1	<code>CryptoService</code> , <code>AgentService</code> , <code>ErrorHandler</code> , <code>TransportService</code>	Nível 0
2	<code>DIDService</code> , <code>AnonCredsService</code> , <code>ZKProofService</code> , <code>TrustChainService</code>	Níveis 0–1
3	<code>CredentialService</code>	Níveis 0–2
4	<code>PresentationService</code>	Níveis 0–2
5	<code>VerificationService</code>	Níveis 0–2

A Figura 5 apresenta visualmente o grafo de dependências detalhado na tabela anterior.

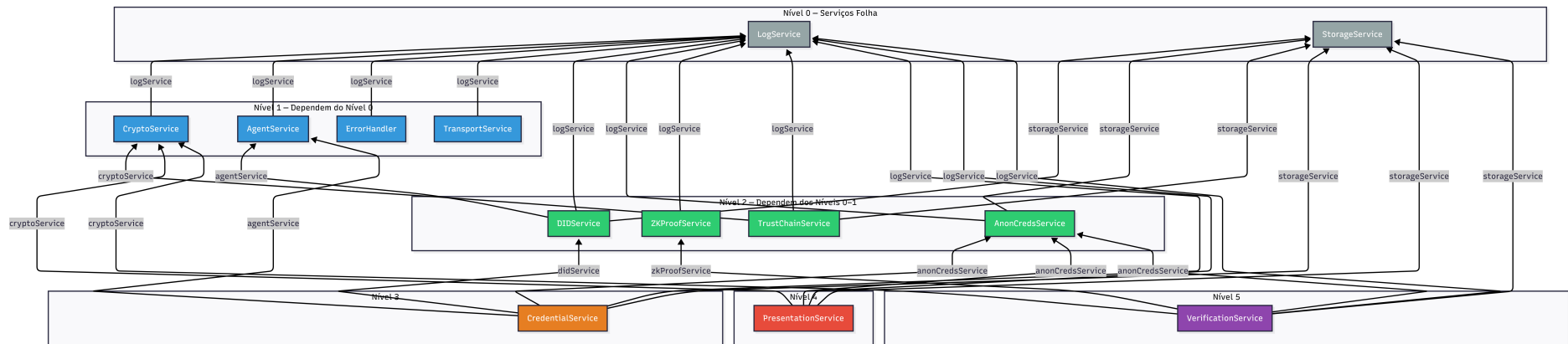


Figura 5 – Grafo de dependências do Composition Root (container.ts).

As interfaces abstratas que fundamentam a inversão de dependência estão definidas no módulo `types/index.ts`. O sistema define dez interfaces de serviço: `ICryptoService`, `IStorageService`, `ILogService`, `IAgentService`, `IDIDService`, `ICredentialSer`, `IAnonCredsService`, `IZKProofService`, `ITrustChainService` e `IVerificationService`. Esta arquitetura, conforme ilustrado no diagrama de classes da Figura 6, permite a substituição de qualquer implementação concreta por mocks nos testes automatizados sem alterar o código de produção.

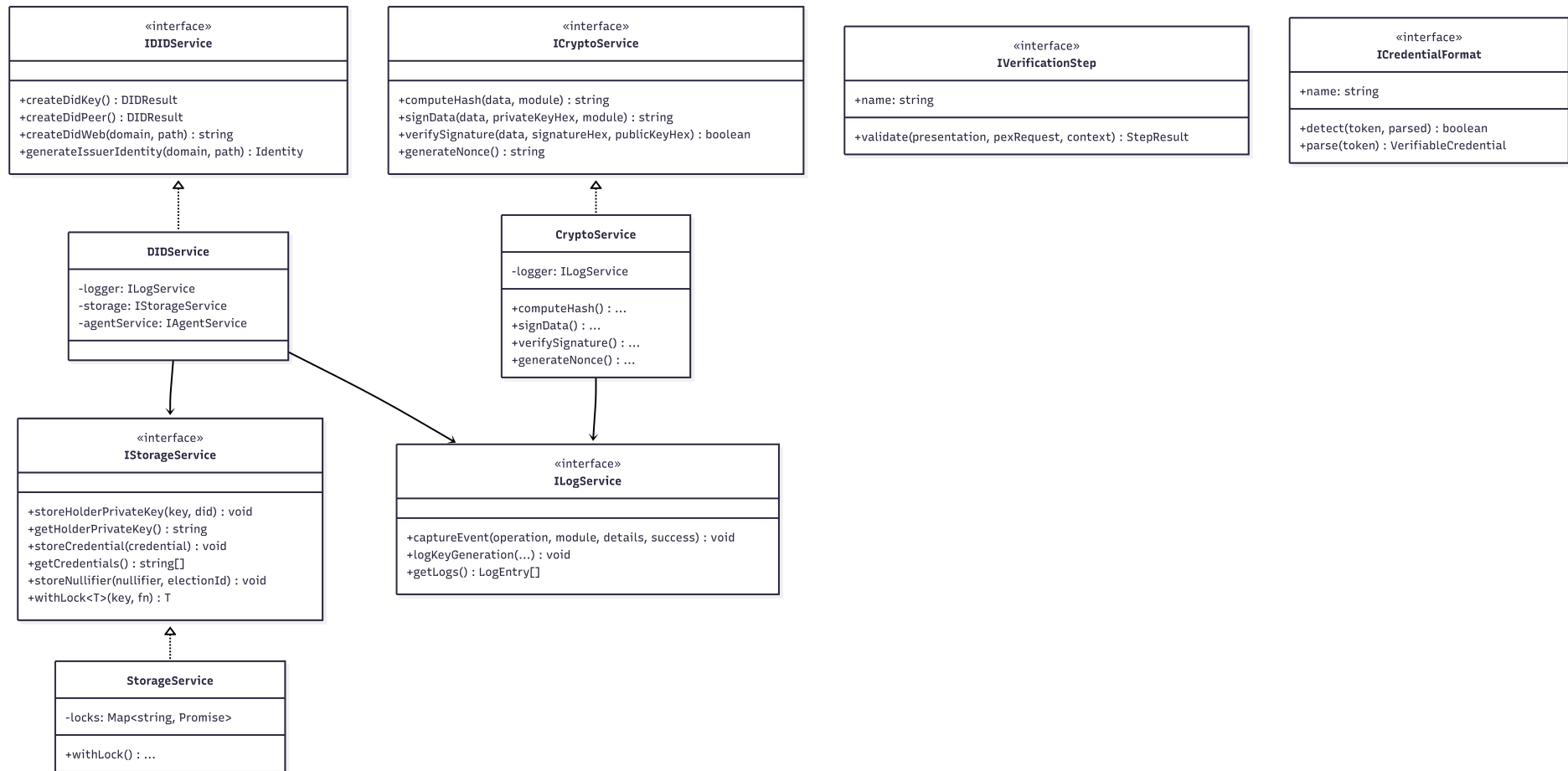


Figura 6 – Interfaces de serviço e implementações concretas seguindo o Princípio de Inversão de Dependência.

6.3 MODELOS DE DADOS E TIPAGEM ESTÁTICA

O sistema utiliza tipagem estática TypeScript para garantir a integridade dos modelos de dados em tempo de compilação. Os modelos centrais, cujas relações e extensões podem ser visualizadas no diagrama de classes da Figura 7, são derivados das especificações W3C Verifiable Credentials Data Model e DIF Presentation Exchange.

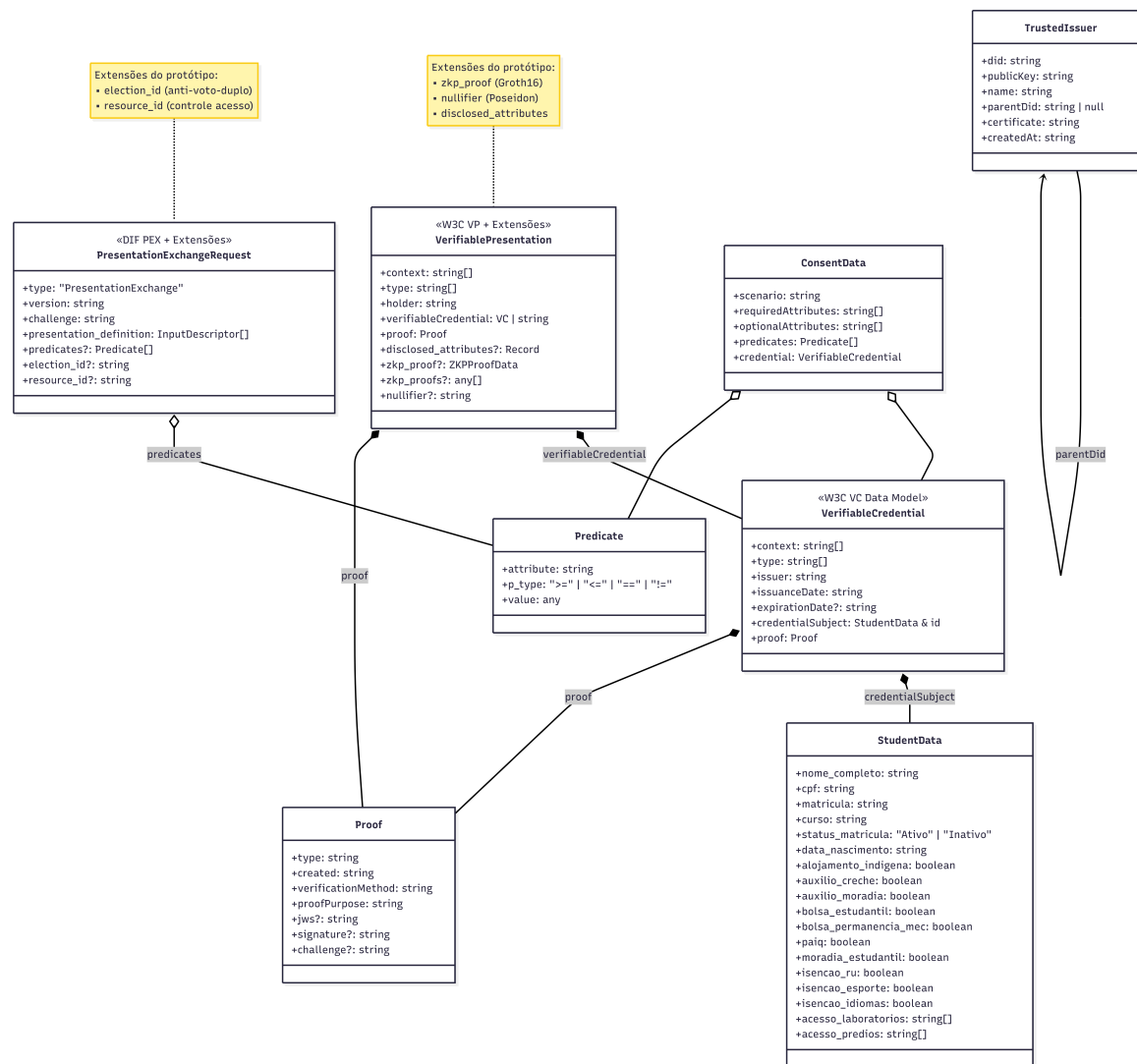


Figura 7 – Diagrama de classes dos modelos de dados com extensões sobre o W3C VC Data Model e DIF Presentation Exchange.

6.3.1 Modelo de Dados do Estudante

A interface `StudentData` define os atributos acadêmicos do titular da credencial, incluindo dados de identificação (nome, CPF, matrícula), vínculo acadêmico (curso, status de matrícula), data de nascimento e doze atributos booleanos e de lista que representam benefícios assistenciais e permissões de acesso físico. Os dez atributos booleanos incluem indicadores de alojamento (`alojamento_indigena`), bolsas (`bolsa_estudantil`, `bolsa_permanencia_mec`), auxílios (`auxilio_creche`, `auxilio_moradia`), moradia (`moradia_estudantil`), programas (`paig`) e isenções (`isencao_ru`, `isencao_esporte`, `isencao_idiomas`). Os dois campos de lista (`acesso_laboratorios`, `acesso_predios`) armazenam identificadores de recursos aos quais o estudante possui permissão de acesso.

6.3.2 Credenciais e Apresentações Verificáveis

A interface `VerifiableCredential` segue a estrutura W3C VC Data Model com os campos obrigatórios `@context`, `type`, `issuer`, `issuanceDate` e `credentialSubject`. O campo `proof` é tipado pela interface `Proof`, que suporta os tipos de assinatura `JsonWebSignature2020` (para SD-JWT) e `CLSignature2023` (para AnonCreds).

6.3.3 Apresentação por Troca (Presentation Exchange)

O tipo `PresentationExchangeRequest` implementa a especificação DIF Presentation Exchange com definição de apresentação, descritores de entrada, campos com filtros e restrições de divulgação. O sistema estende a especificação base com campos adicionais para cenários específicos: `election_id` para prevenção de voto duplicado e `resource_id` para controle de acesso a recursos físicos.

6.3.4 Emissor Confiável (Trust Chain)

A interface `TrustedIssuer` modela um emissor registrado na cadeia de confiança hierárquica, contendo o DID, a chave pública Ed25519, o nome legível, o DID do emissor pai (nulo para a raiz), o certificado digital (assinatura do payload canônico pelo pai) e a data de criação.

6.4 GERENCIAMENTO DE IDENTIDADE DESCENTRALIZADA (DIDS)

O serviço `DIDService` gerencia a criação e o armazenamento de identificadores descentralizados utilizando o agente Credo (`@credo-ts/core`) como infraestrutura de chaves. O sistema opera com três métodos DID complementares.

O método `did:key` é utilizado para operações criptográficas internas. A criação ocorre via a API `agent.dids.create()` do Credo, que gera um par de chaves

Ed25519 e deriva o DID a partir da chave pública conforme a especificação `did:key`. A chave privada permanece gerenciada internamente pelo cofre Aries Askar.

O método `did:peer` está disponível como alternativa para identificação *peerwise* do titular, sem necessidade de registro em ledger público.

O método `did:web` é construído localmente pelo sistema sem registrar em ledger, pois o Credo não possui registrador `did:web`. A construção segue a especificação W3C `did:web` com validação RFC 1123 do domínio. O protótipo utiliza o domínio `ufsc.br` com caminho `identidade-academica`, resultando no DID `did:web:ufsc.br:identidade-academica`.

A geração de identidade do emissor envolve a criação paralela de um `did:key` (para operações de assinatura no cofre Credo) e um `did:web` (como identificador público da instituição). Um par de chaves Ed25519 auxiliar é gerado fora do cofre Credo para operações de assinatura SD-JWT, utilizando a biblioteca `@noble/ed25519`. O mapeamento entre `did:web` e `did:key` de assinatura é persistido no armazenamento cifrado.

6.5 EMISSÃO DE CREDENCIAIS

A Figura 8 ilustra o fluxo completo de ponta a ponta, desde a emissão pelo emissor, passando pela apresentação pelo titular, até a verificação.

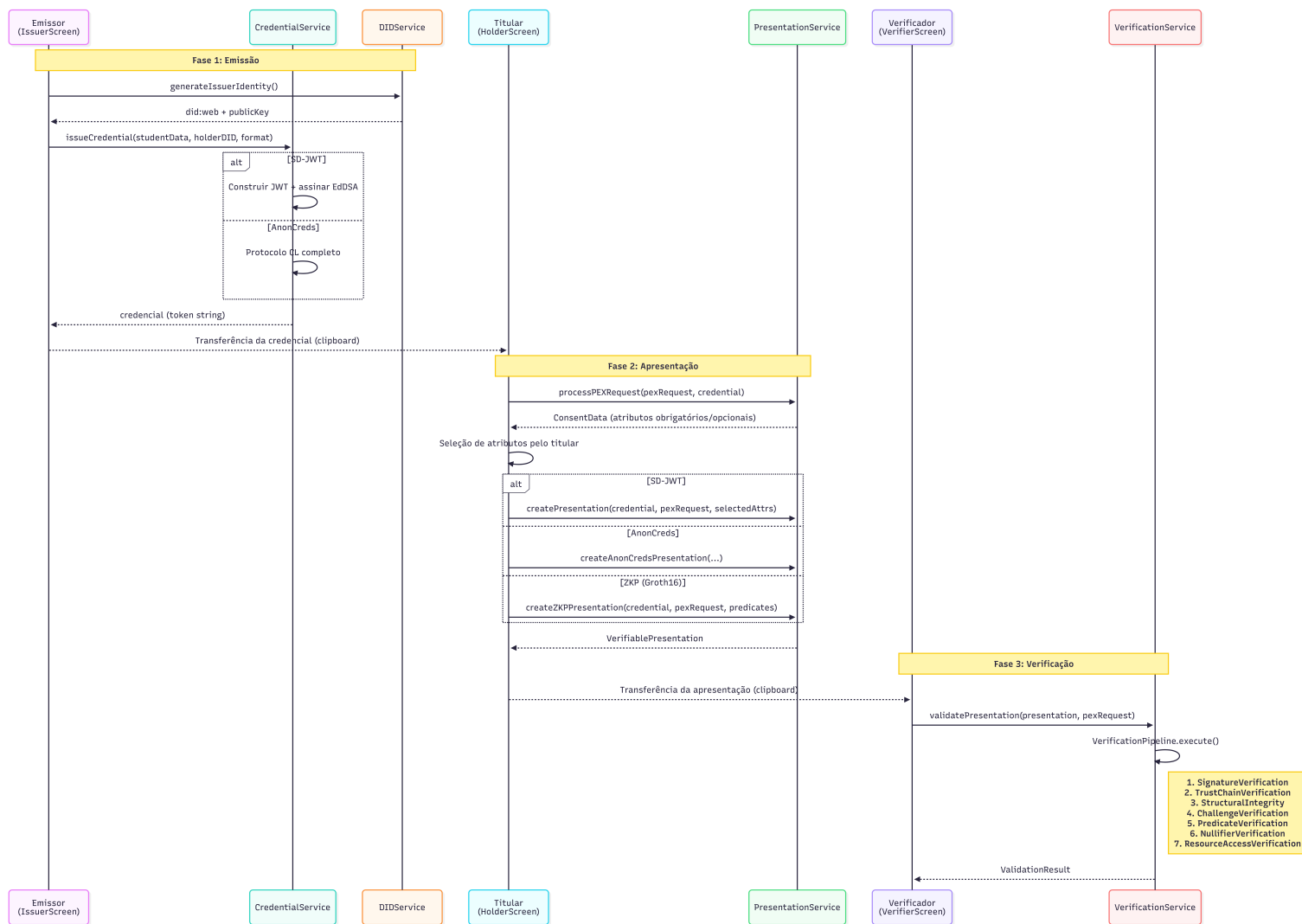


Figura 8 – Fluxo de emissão, apresentação e verificação de credenciais verificáveis.

O serviço `CredentialService` implementa a emissão de credenciais verificáveis em dois formatos distintos: SD-JWT e AnonCreds. O serviço adota o Princípio Aberto/Fechado (OCP) por meio de um registro de formatos extensível, onde novos formatos podem ser adicionados sem modificar a lógica de análise existente.

6.5.1 Formato SD-JWT

A emissão em formato SD-JWT constrói um token JWT com cabeçalho (`alg: EdDSA`, `typ: JWT`), payload contendo a credencial verificável completa, timestamps de emissão e expiração (validade padrão de um ano conforme a cadência acadêmica), e assinatura EdDSA. A assinatura é realizada pelo cofre Credo por meio da API `wallet.sign()`, que localiza a chave privada correspondente no Aries Askar a partir do objeto `Key` extraído do método de verificação. O resultado é codificado em `base64url` conforme RFC 4648 §5, implementado em JavaScript puro para compatibilidade com o motor Hermes.

6.5.2 Formato AnonCreds

A emissão em formato AnonCreds executa o protocolo completo de assinatura CL (*Camenisch-Lysyanskaya*): criação do esquema, definição da credencial, oferta, requisição e emissão. Os atributos da interface `StudentData` são convertidos para um mapa plano chave-valor exigido pelo protocolo AnonCreds, onde valores booleanos e arrays são serializados como strings.

Um desafio de integração inerente a este formato é o gerenciamento de memória. As estruturas de dados do protocolo AnonCreds operam na camada nativa (Rust) e interagem com o código React Native via ponte JSI, retornando alocações de memória que escapam do escopo do *Garbage Collector* do JavaScript. Para evitar vazamentos de memória (*memory leaks*), o serviço implementa a liberação manual de referências nativas (`handle.clear()`) em blocos `try/finally`.

Durante o protocolo, exige-se a geração do *Link Secret* localmente no cofre do titular. Esse artefato atua como um fator de ofuscamento aplicado à credencial recebida, garantindo criptograficamente que as futuras apresentações não possam ser vinculadas (*unlinkability*) nem mesmo pelo emissor original. Todos os artefatos estruturais (*schemas* e *credential definitions*) são armazenados localmente na base de dados cifrada, dispensando consultas a *ledgers* distribuídos.

A Figura 9 contrasta a complexidade protocolar da construção direta via SD-JWT com o protocolo CL completo utilizado no AnonCreds.

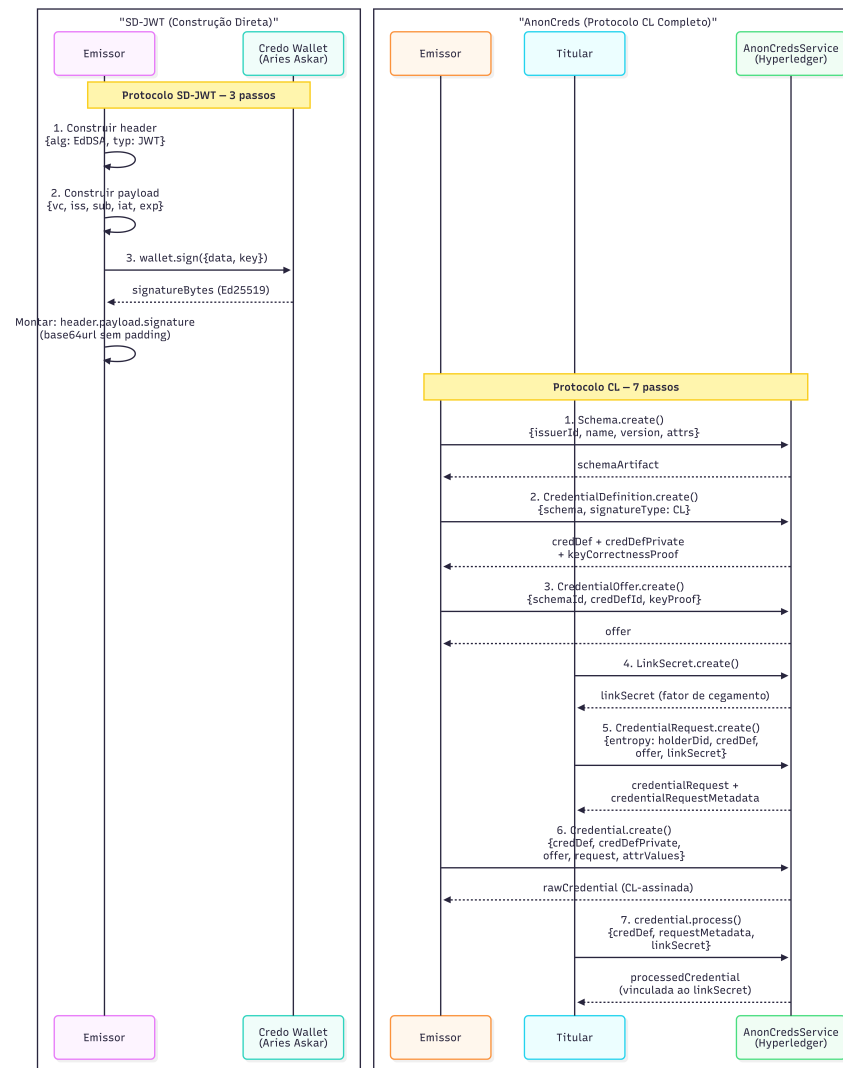


Figura 9 – Comparação dos protocolos de emissão SD-JWT (construção direta) e AnonCreds (protocolo CL completo).

6.5.3 Validação e Análise de Credenciais

O método `validateAndParseCredential` implementa detecção automática de formato por meio da iteração sobre o registro de formatos (primeiro match vence). A validação estrutural verifica a presença e tipagem de todos os campos obrigatórios da especificação W3C VC Data Model: `@context`, `type`, `issuer`, `issuanceDate`, `credentialSubject` e `proof`.

6.6 APRESENTAÇÃO SELETIVA E VERIFICAÇÃO DE CREDENCIAIS

A apresentação e verificação de credenciais são implementadas por dois serviços complementares: `PresentationService` (lado do titular) e `VerificationService` (lado do verificador), ambos compostos internamente por colaboradores de responsabilidade única.

6.6.1 Construção de Apresentações

O `PresentationService` atua como fachada compondo quatro colaboradores especializados:

- `PEXValidator`: valida e analisa requisições no formato DIF Presentation Exchange, extraindo atributos obrigatórios e opcionais para construir dados de consentimento do titular.
- `SDJWTPresentationBuilder`: constrói apresentações com divulgação seletiva baseada em SD-JWT, onde apenas os atributos selecionados pelo titular são incluídos na apresentação assinada.
- `AnonCredsPresentationBuilder`: constrói apresentações utilizando o protocolo AnonCreds com provas de conhecimento zero nativas para divulgação seletiva e provas de predicados.
- `ZKPPresentationBuilder`: constrói apresentações com provas Groth16 (Circom/mopro) para predicados complexos como verificação de faixa etária e status.

6.6.2 Pipeline de Verificação

O `VerificationService` implementa o padrão Cadeia de Responsabilidade (*Chain of Responsibility*) por meio da classe `VerificationPipeline`. Cada etapa de verificação é um objeto que implementa a interface `IVerificationStep`, com método `validate()` que recebe a apresentação, a requisição PEX e um contexto compartilhado. As etapas são executadas sequencialmente; falhas acumulam-se no contexto sem interromper o pipeline. O sistema registra sete etapas de verificação:

1. **SignatureVerification**: verifica a assinatura digital do emissor (Ed25519 para SD-JWT; CL-signature para AnonCreds).

2. **TrustChainVerification**: valida que o DID do emissor pertence à cadeia de confiança hierárquica registrada.
3. **StructuralIntegrity**: verifica a integridade estrutural da apresentação contra os descritores da requisição PEX.
4. **ChallengeVerification**: confirma que o challenge da apresentação corresponde ao challenge da requisição.
5. **PredicateVerification**: avalia os predicados declarados (comparações de igualdade, desigualdade, range).
6. **NullifierVerification**: detecta uso duplicado de credenciais em cenários eleitorais por meio de nullifiers determinísticos.
7. **ResourceAccessVerification**: verifica permissões de acesso a recursos físicos específicos.

A Figura 10 ilustra esse fluxo implementando o padrão Cadeia de Responsabilidade.

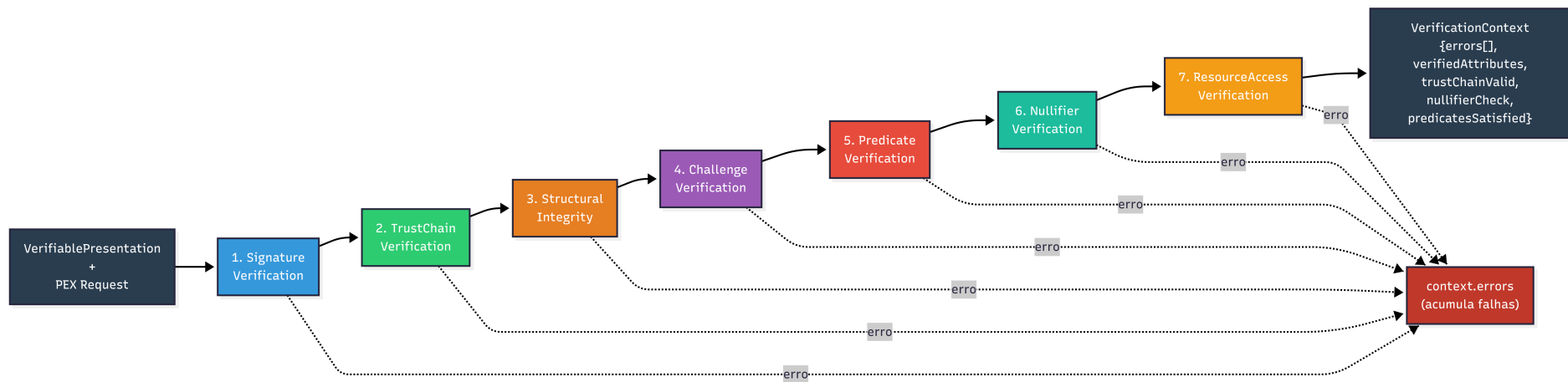


Figura 10 – Pipeline de verificação implementando o padrão Cadeia de Responsabilidade.

6.6.3 Catálogo de Cenários

O módulo `ScenarioCatalog` define quatro cenários de verificação pré-configurados que demonstram as capacidades do sistema:

Tabela 9 – Cenários de verificação implementados no protótipo.

ID	Tipo	Descrição
ru	Divulgação seletiva	Validação de vínculo e isenção tarifária no Restaurante Universitário, revelando apenas <code>status_matricula</code> e <code>isencao_ru</code> .
elections	ZKP de elegibilidade	Validação de elegibilidade eleitoral com prevenção de voto duplicado via nullifier determinístico (Poseidon hash).
age_verification	Range proof	Prova de maioridade civil ($\text{idade} \geq 18$) sem revelar a data de nascimento.
lab_access	Controle de acesso	Verificação de permissões de acesso a laboratórios e prédios específicos.

A Figura 11 apresenta de forma visual os fluxos de verificação e as tecnologias empregadas nos quatro cenários pré-configurados do protótipo.

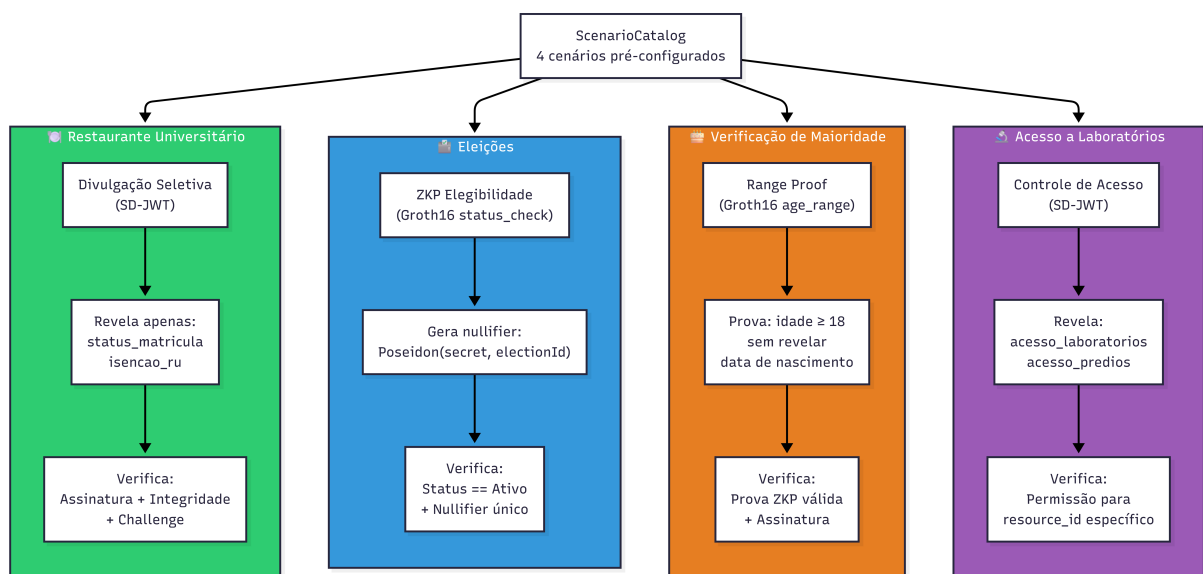


Figura 11 – Fluxos de verificação para os quatro cenários implementados no protótipo.

6.7 PROVAS DE CONHECIMENTO ZERO (ZKP)

O sistema implementa provas de conhecimento zero não interativas (NIZK) por meio de circuitos Circom compilados para o sistema de prova Groth16, executados

nativamente no dispositivo móvel pela biblioteca `mopro-ffi` com backend Arkworks. O serviço `ZKProofService`, cujas relações com os circuitos e a biblioteca nativa podem ser vistas no diagrama de classes da Figura 12, encapsula a geração e verificação de provas para três circuitos especializados.

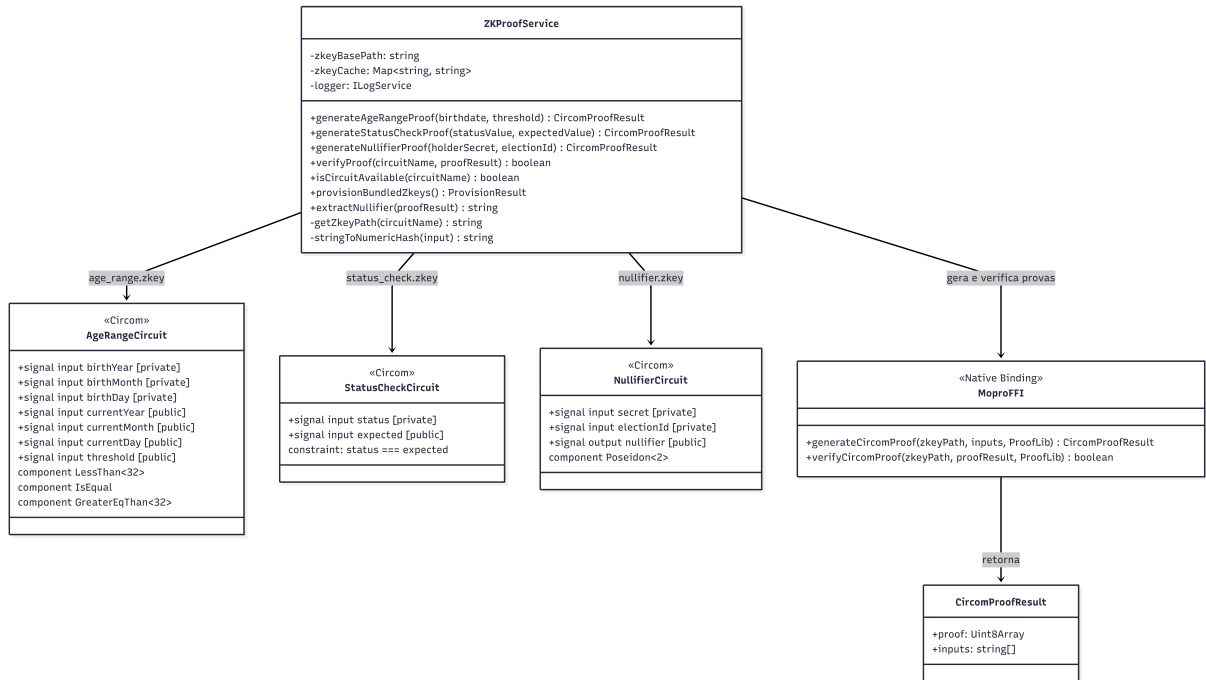


Figura 12 – Diagrama de classes do subsistema de Provas de Conhecimento Zero.

6.7.1 Circuito de Faixa Etária (`age_range`)

O circuito `age_range.circom` prova que a idade do titular é maior ou igual a um limiar sem revelar a data de nascimento. Os sinais privados são `birthYear`, `birthMonth` e `birthDay`; os sinais públicos são `currentYear`, `currentMonth`, `currentDay` e `threshold`. O circuito calcula a idade base ($\text{currentYear} - \text{birthYear}$), determina se o aniversário já ocorreu no ano corrente por meio de comparadores `LessThan(32)` e `IsEqual()` da biblioteca `circomlib`, e restringe que a idade efetiva seja $\geq \text{threshold}$ usando `GreaterEqThan(32)`. A prova é válida apenas se a restrição final `geq.out === 1` for satisfeita.

6.7.2 Circuito de Verificação de Status (`status_check`)

O circuito `status_check.circom` prova que o valor de um atributo de status é igual ao valor esperado sem revelar o valor real. Ambos os sinais são hashes numéricos SHA-256 truncados a 248 bits para compatibilidade com o campo escalar da curva BN254. A restrição do circuito é a igualdade direta: `status === expected`. A conversão de strings para representação numérica utiliza SHA-256 truncado a 31

bytes, evitando colisões triviais que eram possíveis com o hash DJBX33A de 32 bits anteriormente utilizado.

6.7.3 Circuito de Nullifier (`nullifier`)

O circuito `nullifier.circom` computa um identificador determinístico `nullifier = Poseidon(secret, electionId)` que permite detectar participação duplicada em votações sem vincular a identidade do votante. Os sinais `secret` e `electionId` são privados; o `nullifier` é a saída pública. O verificador armazena `nullifiers` já vistos e rejeita apresentações com `nullifiers` duplicados.

6.7.4 Provisionamento de Chaves de Prova

A execução nativa do provador Groth16 requer os binários da restrição de sistema (`.r1cs`) e da chave de prova gerada pela cerimônia de *trusted setup* (`.zkey`). O método `provisionBundledZkeys()` gerencia a extração destes arquivos pesados que são empacotados no binário da aplicação durante o processo de compilação (*build*).

No sistema Android, os artefatos residem isolados no diretório `assets/` do APK e são copiados via `RNFS.copyFileAssets()`. No iOS, o acesso ocorre no escopo do `MainBundlePath`. Em ambos os ecossistemas, o destino da cópia é o diretório de documentos acessível em modo usuário (`DocumentDirectoryPath/zkeys/`). A operação é executada de forma idempotente: a presença prévia dos arquivos interrompe o fluxo de extração, poupando recursos de processamento e entrada/saída (E/S) em inicializações subsequentes do aplicativo.

6.8 CADEIA DE CONFIANÇA PKI HIERÁRQUICA

O serviço `TrustChainService` implementa uma cadeia de confiança hierárquica inspirada no modelo de Infraestrutura de Chaves Públicas (PKI) da ICP-Brasil, utilizando criptografia Ed25519 da biblioteca `@noble/ed25519`. A cadeia, ilustrada na Figura 13, modela o cenário onde a universidade (raiz) delega autoridade de emissão a departamentos ou unidades administrativas.

A inicialização da raiz (`initializeRootIssuer`) gera um par de chaves Ed25519, constrói um certificado auto-assinado e persiste o emissor raiz no armazenamento. O registro de emissores filhos (`registerChildIssuer`) gera um novo par de chaves para o filho, constrói o payload canônico do certificado e o assina com a chave privada do pai.

A verificação da cadeia (`verifyTrustChain`) percorre recursivamente a hierarquia desde o emissor alvo até a raiz, verificando criptograficamente cada certificado contra a chave pública do emissor pai. O algoritmo inclui detecção de ciclos por meio

6.9.1 Armazenamento Cifrado

O serviço `StorageService` encapsula a biblioteca `react-native-encrypted-storage`, que utiliza o Android Keystore (Android) e o iOS Keychain (iOS) para cifrar dados em repouso com chaves gerenciadas pelo hardware seguro do dispositivo. O esquema de chaves de armazenamento utiliza prefixos para separar domínios de dados:

Tabela 10 – Esquema de chaves de armazenamento cifrado.

Prefixo	Chave	Conteúdo
holder_	private_key, public_key, did	Par de chaves Ed25519 e DID do titular
issuer_	private_key, public_key, did, signing_did	Chaves do emissor, DID público (did:web) e DID de assinatura (did:key)
—	holder_credentials	Array JSON de credenciais armazenadas
nullifiers_	{electionId}	Array JSON de nullifiers por eleição
—	trust_chain_issuers	Array JSON de emissores registrados na cadeia
—	credo_wallet_master_key	Chave mestra do cofre Aries Askar (32 bytes aleatórios, hex)

A arquitetura assíncrona do armazenamento de listas (como matrizes de `nullifiers` e coleções de credenciais do titular) introduz suscetibilidade a condições de corrida (*race conditions*) durante operações concorrentes de leitura-modificação-escrita. Para mitigar esse problema sem introduzir gargalos de *thread-blocking*, o `StorageService` implementa um sistema de semáforos (*mutex*) por meio da estrutura de dados `Map<string, Promise<void>`. O método de encapsulamento `withLock(key, fn)` enfileira as operações assíncronas específicas à mesma chave, forçando a execução sequencial por domínio sem impedir que operações de chaves independentes sejam processadas em paralelo.

6.9.2 Gerenciamento de Estado Reativo

O estado de interface é gerenciado pela store Zustand (`useAppStore`), que mantém em memória o DID do titular, o DID do emissor, o módulo de navegação ativo e o buffer de logs de auditoria (limitado a 1.000 entradas). Os dados na store Zustand não são cifrados e não persistem entre reinicializações do aplicativo, pois representam estado transiente da sessão.

6.9.3 Cofre Credo (Aries Askar)

O agente Credo mantém um cofre próprio baseado no Aries Askar com derivação de chave Argon2i-Mod. A chave mestra do cofre é gerada na primeira inicialização a partir de 32 bytes criptograficamente aleatórios (`@noble/ed25519 CSPRNG`) e armazenada no `EncryptedStorage` para reutilização em inicializações subsequentes. Um sentinela de versão (`credo_wallet_master_key_version`) é armazenado em paralelo para viabilizar futuras migrações de esquema de derivação.

6.10 SERVIÇO CRIPTOGRÁFICO

O `CryptoService` concentra as operações criptográficas fundamentais em JavaScript puro, projetado especificamente para o motor Hermes do React Native. As operações de hash empregam o SHA-256 da biblioteca `@noble/hashes`.

Um aspecto de integração arquitetural decorre da execução da biblioteca criptográfica `@noble/ed25519` sob o motor Hermes. Em ambientes web, esta biblioteca adota por padrão a rotina assíncrona `crypto.subtle.digest` para cálculo do SHA-512 subjacente ao protocolo EdDSA. Devido à inexistência da API *WebCrypto* no ambiente móvel do Hermes, a biblioteca falha silenciosamente. O protótipo resolve essa limitação técnica através de injeção de dependências estática no tempo de inicialização, sobrescrevendo a rotina `ed.hashes.sha512` para forçar a vinculação síncrona com o SHA-512 do pacote `@noble/hashes`. Essa estratégia possibilita operações Ed25519 em puro JavaScript, economizando os milissegundos de latência associados a invocações repetidas de módulos nativos.

Na geração de *nonces* (desafios criptográficos) que preservam a privacidade dos usuários nas apresentações AnonCreds, o sistema utiliza o *polyfill* `react-native-get-random-values`. Um vetor de bytes é alimentado a partir do Gerador de Números Pseudoaleatórios Criptograficamente Seguro (CSPRNG) oferecido pela interface nativa. Esta implementação afasta vulnerabilidades observadas em implementações primitivas (como o uso de `Date.now()`), evitando a probabilidade teórica de ataques de correlação temporal, nos quais um observador passivo poderia isolar e vincular apresentações.

6.11 DESIGN DE INTERFACE E EXPERIÊNCIA DO USUÁRIO (UX)

O desenvolvimento da interface gráfica e da experiência do usuário (UX) do aplicativo foi norteado pelos princípios do Design System do Governo Federal (gov.br). Para estabelecer a paleta de cores institucional, tipografia e os espaçamentos principais, realizou-se uma fase inicial de prototipação na ferramenta Figma (Figura 15).

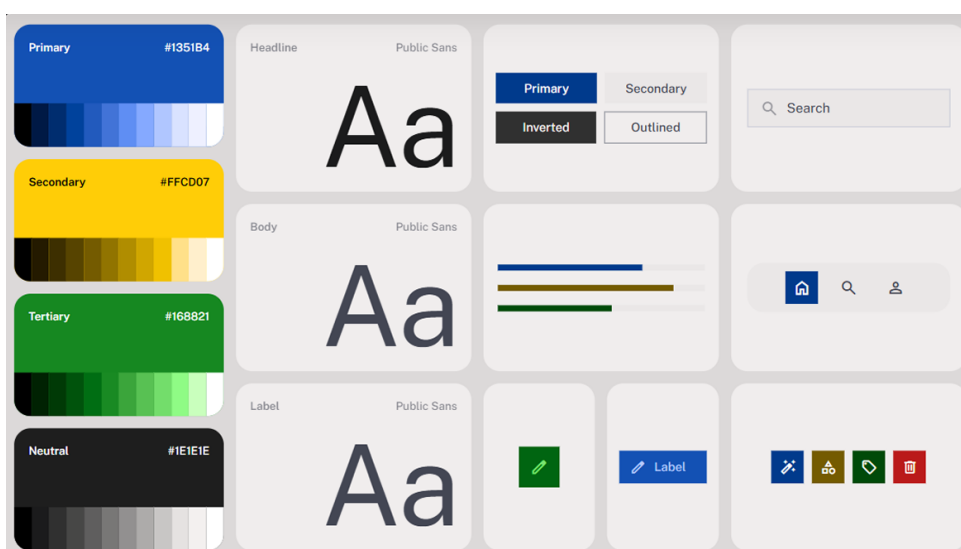


Figura 15 – Design System e componentes base do protótipo definidos no Figma.

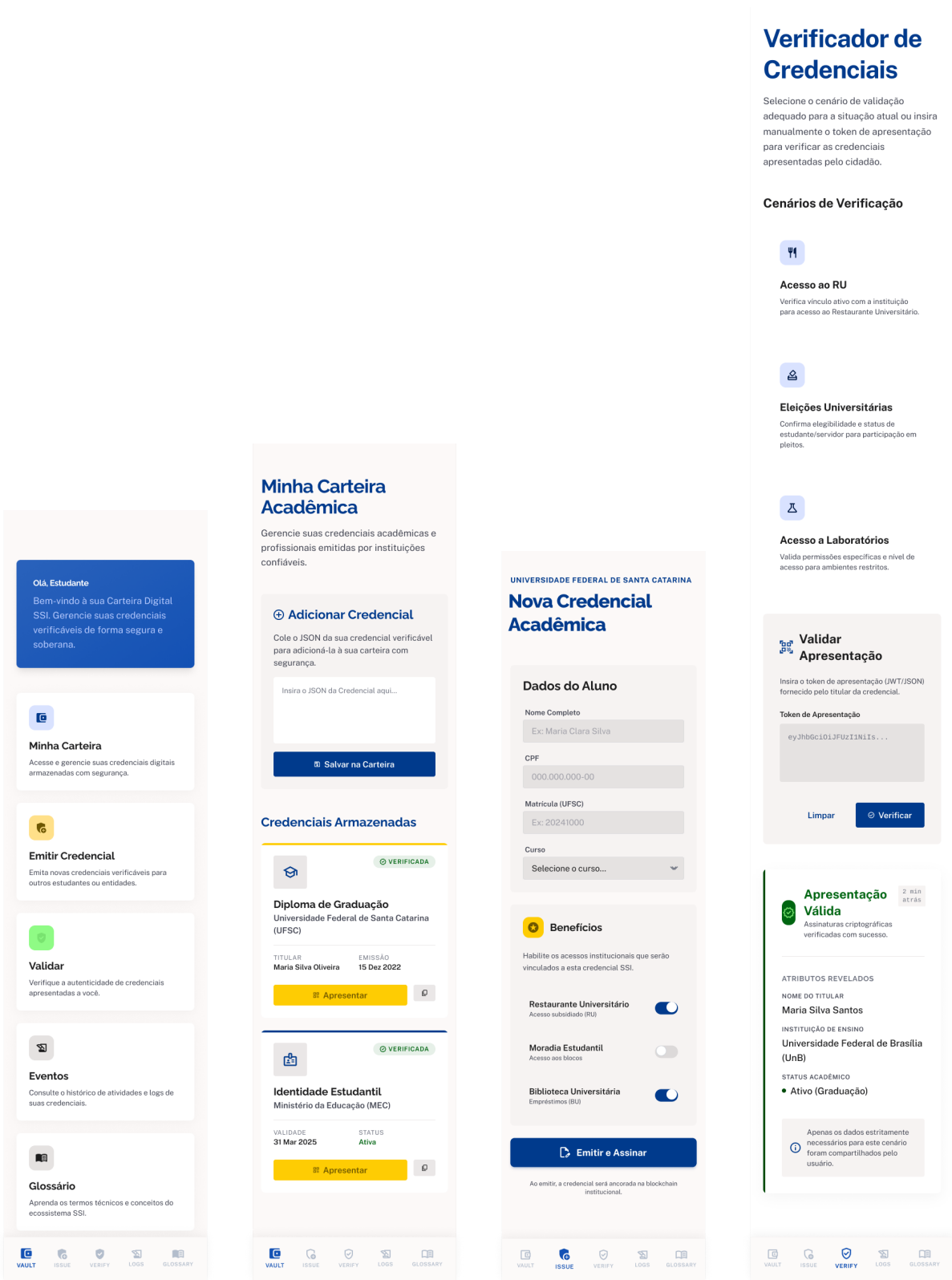
Essa etapa de design (Figura 16) demonstrou o esforço analítico para projetar uma experiência de usuário consistente antes da implementação em código. As telas planejadas incluíam o menu inicial, o cofre de credenciais, os formulários do emissor e os leitores do verificador.

Entretanto, conforme o aplicativo foi sendo desenvolvido e os testes em ambiente móvel (React Native) foram realizados, algumas telas e fluxos não seguiram estritamente o protótipo inicial. Modificações foram feitas para acomodar restrições técnicas do framework, criar novas funcionalidades e melhorar continuamente a usabilidade nos dispositivos móveis.

A navegação final do aplicativo utiliza a biblioteca React Navigation com uma estrutura de Stack (raiz) e Tabs (principal). O layout de abas define as rotas acessíveis e visíveis na barra de navegação inferior: Menu (*Home*), Titular (*Vault*), Emissor (*Issue*), Verificador (*Verify*), Logs e Glossário.

6.11.1 Telas Finais do Aplicativo

A interface final implementada consolida as adaptações realizadas durante o desenvolvimento. A Figura 17 ilustra a tela de inicialização (geração do DID nativo), o Menu principal e a interface de Emissão de Credenciais, demonstrando a aplicação do layout em um ambiente real.



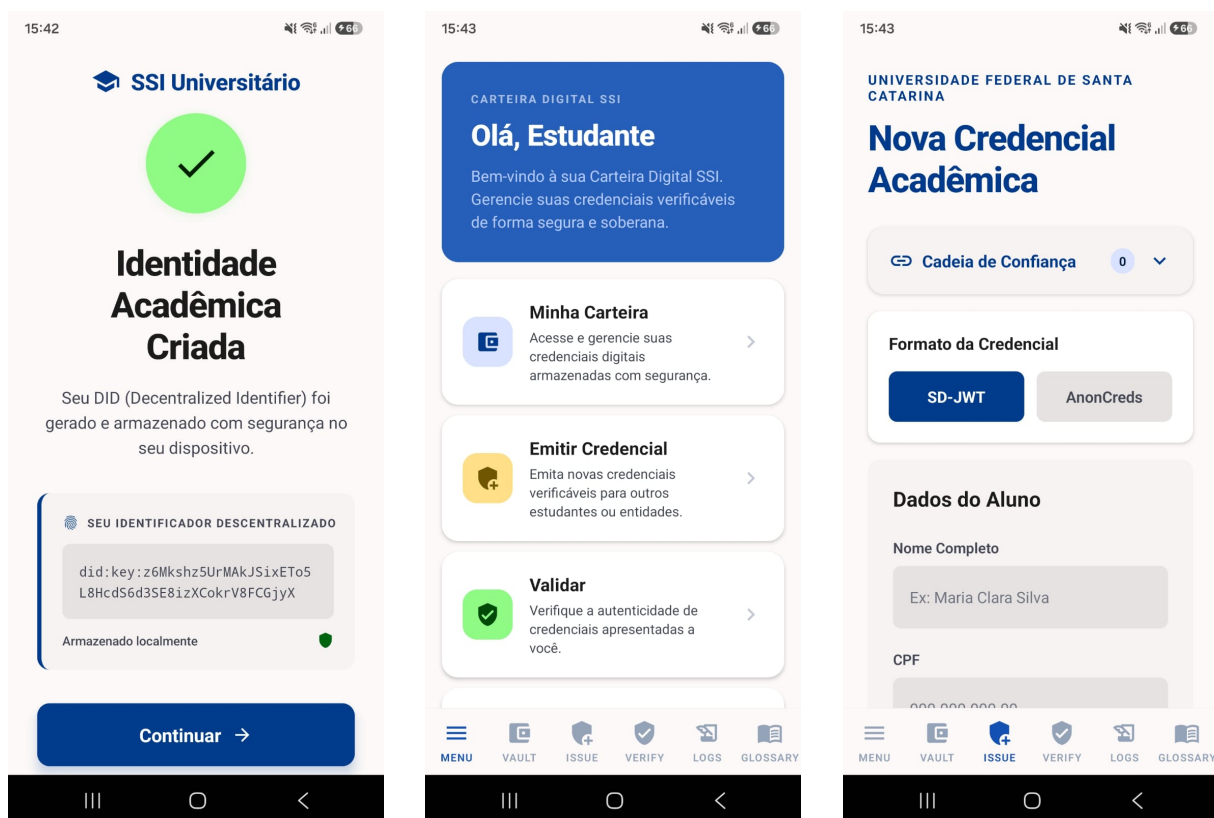
Tela Inicial

Cofre

Emissor

Verificador

Figura 16 – Exemplos do design inicial elaborado no Figma.



Criação de DID

Menu Principal

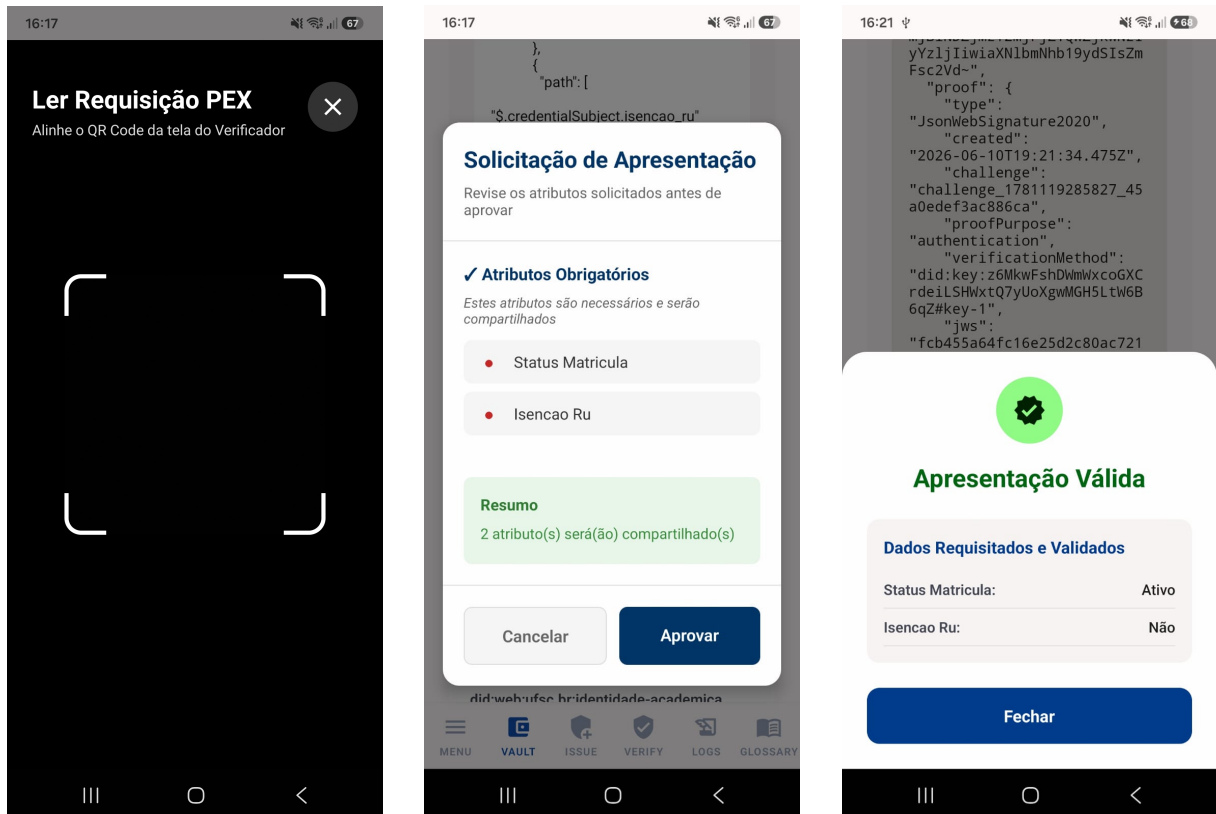
Formulário do Emissor

Figura 17 – Interfaces finais: geração de identidade, menu e emissão.

Para o fluxo central de verificação, a interface foi otimizada para garantir a clareza no compartilhamento de dados. A Figura 18 exhibe a sequência desde a leitura do código QR, passando pelo modal de consentimento do titular (em conformidade com a LGPD), até a visualização final do feedback de validação para o verificador.

Por fim, além das telas de negócio, a arquitetura final engloba módulos de monitoramento técnico (Figura 19). Estes componentes adotam tipografia monoespçada (*monospace*) para melhorar a legibilidade de métricas computacionais, endereços descentralizados e *logs*.

Os 11 componentes reutilizáveis que compõem este Design System interno incluem: `AttributeSelector` (seleção de atributos para divulgação seletiva), `ConsentModal` (consentimento explícito), `CredentialCard` (visualização principal de credencial), `Error Message` e `SuccessMessage` (alertas não-intrusivos), `LoadingIndicator` (bloqueio de estado de carregamento), `LogEntry` (entrada tipada de log), `ScannerModal` (captura de QR codes), `TransportModeSelector` (seleção de comunicação), `TrustChainSection` (cadeia hierárquica gráfica) e `ValidationResultModal` (feedback de validação final).



Leitura de QR Code

Consentimento (Titular)

Validação (Verificador)

Figura 18 – Fluxo de apresentação e verificação no aplicativo móvel.

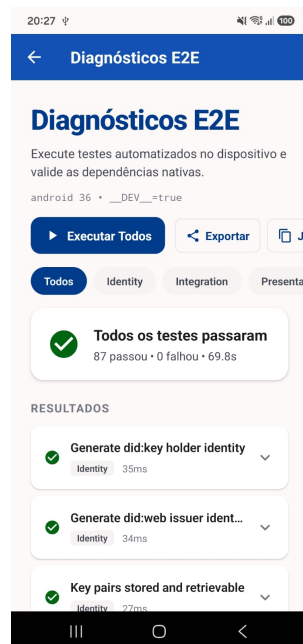


Figura 19 – Painel de Execução de Diagnósticos E2E com resultados temporais de execução.

6.12 GARANTIA DE QUALIDADE: TESTES E ANÁLISE ESTÁTICA

O projeto implementa uma estratégia de testes em múltiplas camadas, configurada com Jest (preset `jest-expo`) e um reporter customizado.

6.12.1 Testes de Serviço

O diretório `src/services/__tests__` contém 21 suítes de teste cobrindo todos os serviços do sistema. Os testes empregam três estratégias complementares:

- **Testes baseados em propriedades** (*property-based*): verificam invariantes do sistema sob entradas geradas aleatoriamente. Exemplos incluem `CredentialService.property.test.ts`, `DIDService.property.test.ts` e `Elections.property.test.ts`.
- **Testes de integração**: validam o fluxo completo entre múltiplos serviços. O `RangeProof.integration.test.ts` exercita a cadeia `ZKProofService` → `PresentationService` → `VerificationService`.
- **Testes de borda** (*edge cases*): validam o comportamento do sistema sob entradas limítrofes e condições de erro. O `Verification.edge.test.ts` testa cenários como apresentações malformadas e challenges expirados.

6.12.2 Testes Ponta-a-Ponta (E2E) com Jest

O diretório `src/__tests__` contém 8 suítes E2E que exercitam cenários completos do sistema: fluxo completo de emissão-apresentação-verificação, provas de faixa etária, divulgação seletiva no RU, eleições com nullifiers, acesso a laboratórios, cadeia de confiança, round-trip criptográfico e estado de navegação.

6.12.3 Análise Estática

A configuração do ESLint (`.eslintrc.js`) estende o preset `@react-native` com o parser TypeScript e inclui uma regra de segurança que proíbe o uso de `Math.random()` em código de produção via `no-restricted-syntax`, direcionando os desenvolvedores para alternativas criptograficamente seguras. O Prettier (`.prettierrc.js`) garante formatação consistente com aspas simples, vírgula final e parênteses de *arrow functions* omitidos quando possível.

A Tabela 11 resume a cobertura de testes por módulo de serviço.

6.13 TESTES DE TEMPO DE EXECUÇÃO (E2E NATIVOS)

As bibliotecas criptográficas utilizadas no aplicativo, como Aries Askar e mo-pro, possuem dependências nativas (C++ e Rust) acessadas via JSI (*JavaScript In-*

Tabela 11 – Cobertura de testes automatizados por módulo.

Módulo	Suítes	Tipos de Teste
CredentialService	2	Property-based, simplificado
CryptoService	2	Property-based, verificação de assinatura
DIDService	1	Property-based
PresentationService	4	Property-based, simplificado, PEX, ZKP
VerificationService	2	Property-based, edge cases
LogService	1	Property-based
StorageService	1	Unitário
TrustChainService	1	Integração
Range Proof	2	Property-based, integração
Elections	1	Property-based
Laboratory	1	Property-based
RU	1	Property-based
Design Patterns	1	Verificação de padrões OCP/DIP
ErrorHandler	1	Unitário

terface). Por esse motivo, a execução de testes falha em ambientes baseados em NodeJS (como o Jest), devido à ausência dos *bindings* nativos.

Para viabilizar a validação da integração do código nativo e coletar métricas de execução no dispositivo, o projeto implementa testes em tempo de execução (*Runtime Tests*). O conjunto de testes é composto por 16 suítes coordenadas pelo serviço orquestrador `RuntimeTestRunner`.

6.13.1 Interface de Diagnósticos e Orquestração

Os testes são gerenciados pelo componente `DiagnosticsScreen`, que implementa a interface de execução no aplicativo móvel. As funcionalidades disponíveis incluem:

- **Gestão de Execução:** Execução de categorias específicas de testes por meio de filtros ou validação de toda a suíte. O estado da execução é atualizado com indicadores de progresso e resultados por caso de teste.
- **Coleta de Métricas:** Cada suíte de testes mensura e consolida o tempo de duração das operações em milissegundos (`ms`). Essa captura é utilizada nas avaliações de desempenho discutidas em capítulos posteriores, mensurando o custo computacional das operações no hardware do dispositivo.
- **Telemetria e Depuração:** Em caso de falhas nas chamadas JSI, a interface captura a exceção da ponte nativa e exibe a *stack trace* para identificação de erros de integração com componentes nativos.
- **Exportação de Resultados:** Os resultados consolidados podem ser formatados em relatórios legíveis por máquina (*JSON*) ou para leitura humana (*Markdown*)

e exportados para análise externa.

6.13.2 Casos de Teste Avaliados

Os 16 arquivos de teste cobrem as operações do aplicativo nos seguintes eixos de integração:

1. **Identidade e Armazenamento:** Valida a geração de chaves públicas e privadas e sua persistência no cofre do dispositivo. Verifica a emissão e estruturação de DIDs nos formatos *did:key* e *did:web*.
2. **Fluxos SD-JWT e AnonCreds:** Executa o fluxo de ponta a ponta: emissão, armazenamento, criação de apresentações com divulgação seletiva e validação pelo verificador. Analisa a estruturação do *Disclosure Array* do SD-JWT em relação aos atributos consentidos.
3. **Circuitos de Eleição e Votação (ZKP):** Gera provas de conhecimento zero nativamente. Verifica a geração de *nullifiers* determinísticos que implementam a prevenção de voto duplicado e a característica de *unlinkability*.
4. **Provas de Intervalo (Range Proof):** Executa a verificação de predicados como maioria civil, assegurando que o atributo oculto (data de nascimento) não é retornado no *payload* da resposta.
5. **Cadeia de Confiança (PKI):** Realiza a verificação criptográfica da árvore de chaves (*Trust Anchors*) para esquemas de delegação hierárquica.
6. **Round-Trip Criptográfico:** Verifica as operações de serialização e desserialização de chaves e buffers na comunicação com o código nativo, assegurando a compatibilidade de conversões de tipo em *Base64/Hex* para operações no motor Hermes.
7. **Casos Institucionais:** Aplica os modelos Presentation Exchange aos cenários de Controle de Acesso e Divulgação Seletiva, verificando a seleção de credenciais baseada em predicados estritos definidos no formato DIF PEX.
8. **Tratamento de Exceções (Edge Cases):** Executa interações com manipulação intencional de dados em trânsito, submissão de apresentações com estrutura incorreta e uso de *challenges* expirados, com o objetivo de validar os mecanismos de tratamento de erro do aplicativo.

7 DISCUSSÃO E AVALIAÇÃO DE RESULTADOS

7.1 AVALIAÇÃO DO ATENDIMENTO AOS OBJETIVOS

A etapa de avaliação confirma o cumprimento do objetivo da pesquisa, uma vez que o trabalho resultou em um sistema capaz de operar os conceitos de Identidade Auto-Soberana. A implementação englobou rotinas de emissão, armazenamento e validação de Credenciais Verificáveis e provas ZKP. Os resultados demonstram ser viável executar essas arquiteturas criptográficas em um ambiente que simula uma instituição de ensino no Brasil.

O fluxo entre as interfaces de usuário ilustra de modo prático o ciclo de gerenciamento de dados, conforme consolidado na Figura 20. A primeira tela exibe a etapa de emissão, momento em que ocorre a assinatura das credenciais. Em seguida, o módulo de custódia salva essas informações de forma segura no dispositivo. Esse armazenamento prepara o sistema para o mecanismo de divulgação seletiva, que exige o consentimento explícito do usuário antes do envio de qualquer dado. O ciclo termina no módulo de análise de confiança, ilustrado pelo resultado da validação, que retrata a conclusão da verificação e do processamento das informações testadas.

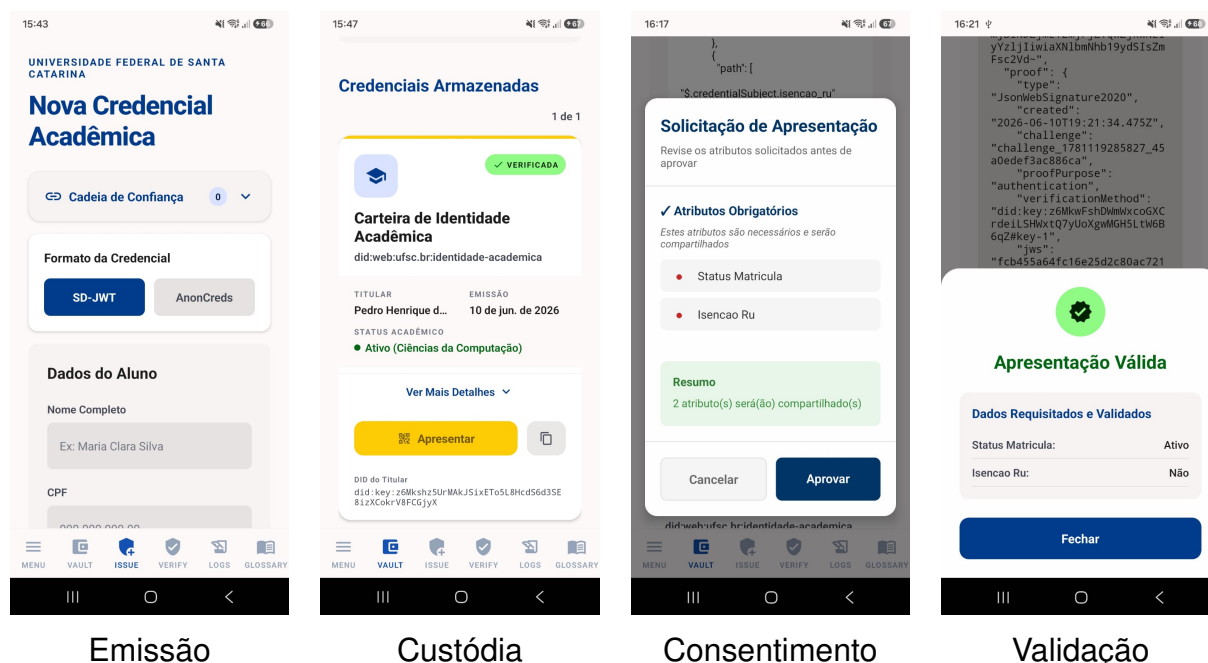


Figura 20 – Fluxo de gerenciamento de dados: emissão, custódia, consentimento e validação.

As regras de negócio projetadas para o cenário universitário funcionaram corretamente durante os testes de integração. A Figura 21 comprova esse funcionamento ao exibir o painel de métricas com a aprovação em todas as rotinas submetidas. O

processo de validação testou com sucesso a isenção no restaurante universitário, a prevenção de votos duplicados nas eleições, a verificação da faixa etária e o controle de acesso aos laboratórios.

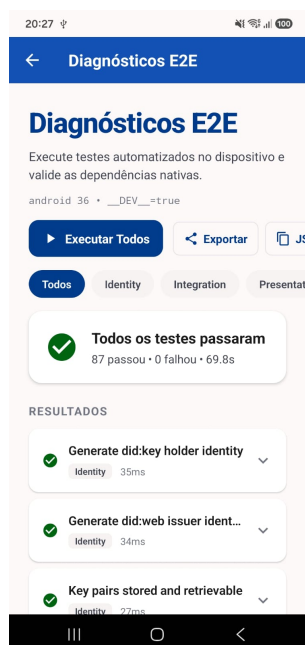


Figura 21 – Painel de métricas de execução de testes de integração

Esta pesquisa alinha a fundamentação teórica baseada na revisão de literatura sobre ferramentas de confiança digital com as barreiras arquiteturais mapeadas na legislação do Brasil e da Europa. A elaboração do código fonte traduziu essas normas em um artefato de demonstração de conceito. Como resultado, o levantamento das métricas de processamento fornece um referencial empírico para ajudar trabalhos futuros a identificar e solucionar desafios de integração.

7.2 ANÁLISE DOS TESTES DO PROTÓTIPO E DISCUSSÃO DO CENÁRIO UNIVERSITÁRIO

Ao avaliar a viabilidade com base nessas métricas, percebe-se que o tempo de execução dos algoritmos isoladamente não prejudica a fluidez do software. No entanto, o custo de tempo associado à interação do usuário na interface precisa ser somado à latência dos cálculos. No caso do acesso às catracas do restaurante universitário, as etapas necessárias geram lentidão no fluxo. Essas etapas incluem retirar o smartphone do bolso, desbloquear o dispositivo, abrir o aplicativo, escanear o QR Code e confirmar o consentimento na tela. Considerando que ambientes de alimentação nos campi recebem a passagem de milhares de estudantes em períodos de trinta a sessenta minutos, a autorização via aplicativo de smartphone se mostra inadequada para essa concentração populacional. Tecnologias consolidadas, como cartões RFID

ou leitura biométrica, continuam mais eficientes para garantir acesso rápido. É importante reconhecer que esse resultado representa uma tensão direta com o escopo definido na Seção 5.3.5: o cenário de Acesso Físico (item 4 da Seção 5.3.3), embora tenha sido implementado e testado com sucesso nos testes de integração, mostrou-se na avaliação o caso de uso menos adequado para SSI, uma vez que o anonimato não é uma propriedade desejável nesses contextos e a latência do fluxo é incompatível com o volume de passagens exigido. Esses resultados corroboram as limitações de alta latência identificadas em experimentos similares de controle de acesso físico com SSI (ENGE et al., 2022a).

Essa constatação reforça que adotar identidades descentralizadas apenas para controlar o acesso físico a laboratórios e demais ambientes do campus representaria uma solução tecnológica em busca de um problema. A garantia de anonimato nesses espaços não interessa aos alunos nem à administração, visto que impossibilitar a identificação dificultaria o rastreamento em casos de incidentes de segurança nas salas de aula. A infraestrutura de acesso das universidades já opera com sistemas de identificação funcionais. Portanto, os benefícios de minimização de dados não compensam a fricção gerada pela necessidade de instalação de aplicativos e pelo gerenciamento complexo de chaves de segurança imposto à comunidade acadêmica.

Por outro lado, processos como a comprovação de benefícios da assistência estudantil demonstram total aderência aos modelos de implementação de ZKP. A proteção da identidade durante avaliações socioeconômicas evita a exposição de dados sensíveis de grupos em condições de vulnerabilidade. A tecnologia oculta marcadores relacionados a cotas de ingresso e recebimento de auxílios, bloqueando a formação de perfis de dados por terceiros. Essa restrição, viabilizada pela divulgação seletiva via AnonCreds, reduziria consideravelmente os riscos de discriminação dentro da universidade, alinhando-se ao princípio de minimização de dados defendido por Babel et al. (2025).

De forma semelhante, a divulgação seletiva viabilizaria a realização segura de eleições para a reitoria pela internet, preservando os requisitos de integridade do processo democrático. A carteira digital combateria falhas comuns em sistemas de login tradicionais, nos quais o vazamento de senhas permite que uma pessoa vote no lugar de outra. Como a validação exige que o eleitor possua o smartphone cadastrado e realize o desbloqueio biométrico, a tecnologia dificultaria fraudes de substituição de identidade. Além disso, os circuitos ZK garantiriam o sigilo do voto e gerariam identificadores de sessão capazes de impedir o registro de votos duplicados.

A carteira digital também ganha forte justificativa de adoção na resolução de processos burocráticos focados na transferência de grandes blocos de dados, superando os casos de uso de controle físico. Rotinas administrativas complexas, incluindo inscrições em programas de intercâmbio ou o preenchimento de formulários de ma-

trícula, ganhariam extrema agilidade. O envio estruturado de informações por meio do aplicativo eliminaria a necessidade de digitação repetitiva de campos de texto em balcões de atendimento, assegurando precisão. A eliminação de erros humanos no fornecimento de dados incompletos constitui o principal atrativo para a administração acadêmica. Sob essa perspectiva, a tecnologia atuaria como um mecanismo de transmissão de Verifiable Credentials com autenticidade garantida na origem, viabilizando a gestão institucional sem a etapa lenta de conferência manual de documentos físicos.

7.3 DESAFIOS DE INTEGRAÇÃO EM ENGENHARIA DE SOFTWARE

A implementação das bibliotecas de criptografia descentralizada no ecossistema de dispositivos móveis apresentou obstáculos significativos de integração de sistemas. A execução de protocolos ZKP e a manipulação das Credenciais Verificáveis exigiu a construção de pontes de comunicação entre o código responsável por renderizar a interface e as linguagens de máquina nativas.

O gerenciamento de recursos computacionais foi particularmente crítico. Houve incompatibilidade entre a forma como o protocolo AnonCreds aloca estruturas na memória e o funcionamento do mecanismo automático de coleta de lixo do ambiente de interface. Essa divergência provocava retenção indevida de dados. O uso de ferramentas de auditoria revelou o vazamento de informações de sessões anteriores, exigindo o desenvolvimento de rotinas para liberar explicitamente os endereços de memória após as execuções criptográficas.

Integrar a geração de provas ZKP ao sistema operacional nativo exigiu reordenar o fluxo de compilação. A vinculação dos circuitos ZK (Groth16) aos módulos do aplicativo revelou problemas iniciais de compatibilidade de ferramentas. O primeiro obstáculo consistiu em alinhar os identificadores da ponte de comunicação nativa. O aplicativo de interface procurava uma biblioteca exportada com um nome específico, enquanto a ferramenta de compilação em baixo nível gerava o arquivo sob outro identificador. Essa diferença resultava em recusas de carregamento em tempo de execução. Para resolver o conflito, foi necessário modificar as regras de configuração do gerenciador de pacotes, alinhando as exportações geradas pela linguagem de máquina com as expectativas do ecossistema móvel.

A etapa de compilação também revelou problemas de comunicação entre os diretórios da máquina de desenvolvimento. A cadeia de montagem reportava a ausência de bibliotecas essenciais porque o motor de compilação criptográfico gerava seus arquivos em pastas separadas da árvore principal do projeto. A solução para essa barreira envolveu elaborar scripts automatizados responsáveis por copiar os arquivos binários gerados diretamente para os diretórios corretos, de acordo com a arquitetura dos processadores dos smartphones de destino.

Mesmo com os arquivos nos locais corretos, a inicialização no emulador registrou falhas ao carregar as ferramentas de criptografia. A biblioteca tentava importar caminhos absolutos atrelados aos diretórios do computador de desenvolvimento, inviabilizando a localização dos arquivos no smartphone. O ajuste estrutural demandou a substituição dos comandos de importação estática por marcadores dinâmicos, delegando a resolução das rotinas ao próprio sistema operacional do aparelho em tempo de execução.

A vinculação final ainda apontou um conflito de sintaxe na ferramenta de tradução matemática. O conversor removía caracteres como o traço inferior durante a geração das variáveis lógicas, quebrando as referências de conexão exigidas pelo aplicativo. Uma auditoria constatou a divergência nas chaves dos módulos gerados, exigindo a alteração manual dos nomes das funções exportadas nos arquivos de declaração para reestabelecer o funcionamento da ponte criptográfica.

Por fim, as restrições dos protocolos motivaram o uso de tecnologias híbridas. A primeira tentativa de validar limites de idade usando o protocolo AnonCreds demonstrou incompatibilidade técnica, pois o motor de provas dessa biblioteca exige números inteiros para criar provas de intervalo. A tentativa de converter as datas textuais para blocos inteiros quebrou a estrutura de dados e invalidou a segurança das provas ZKP. Diante dessa barreira, a verificação da idade foi delegada a circuitos ZK construídos de forma customizada via mopro, onde o envio dos dias como parâmetro supriu o requisito das políticas de acesso preservando a segurança do modelo de tipos.

7.4 IMPLICAÇÕES PARA PRIVACIDADE E EXPERIÊNCIA DE USUÁRIO

A Identidade Auto-Soberana impõe complexas barreiras de abstração cognitiva. Ao transferir a custódia das informações diretamente para o cidadão, o sistema requer telas capazes de traduzir a mecânica de compartilhamento de forma intuitiva. A interface precisa comunicar as distinções práticas entre o envio de um atributo em texto claro e o uso de uma prova ZKP, informando de modo claro os atestados de idade limite sem utilizar jargões criptográficos que possam causar confusão. Nesse sentido, Bumiller et al. (2025) alertam que 70% das soluções de privacidade na literatura ignoram o impacto das técnicas criptográficas na experiência do usuário final, uma fragilidade que o design de consentimento deste protótipo buscou mitigar.

A busca por um ponto de equilíbrio entre a transparência e a facilidade de uso motivou reestruturações nos módulos de consentimento do software. O desenvolvimento exigiu a separação visual das informações enviadas em formato aberto em contraste com os atestados fundamentados exclusivamente em provas ZKP. O projeto deve fornecer ferramentas claras para o acompanhamento dos dados expostos,

assegurando a premissa de consentimento informado característica da arquitetura de privacidade, ao mesmo tempo em que reduz a carga de leitura imposta em cada etapa.

Fica evidente que o aprofundamento da privacidade incorre na geração de atritos no fluxo operacional. A imposição de avisos de leitura e botões de permissão configura o custo inerente ao modelo das carteiras digitais. A viabilidade de adoção em instâncias de governo depende criticamente do desenvolvimento de metáforas visuais eficientes para abstrair a proteção de dados. Nesse cenário, o planejamento cuidadoso da experiência de usuário atua como pilar estrutural para garantir a aceitação de ferramentas com mecanismos restritivos de divulgação.

7.5 EXPANSÃO DE ARQUITETURA PARA CASOS DE USO GOVERNAMENTAIS

A expansão da arquitetura testada no ambiente acadêmico para o governo federal resolveria lacunas críticas de privacidade. Credenciais emitidas sob as chaves oficiais de estado disporiam de validade para aceitação unânime em setores públicos e privados. Sob a premissa da confiabilidade da fonte emissora, a adoção dessas tecnologias de preservação de dados viabilizaria o controle de usuários em plataformas online de maneira adequada, atendendo as exigências legais de verificação de faixa etária em plataformas digitais.

Atualmente, a verificação de idade para o acesso a determinados portais na internet tem sido repassada a corporações comerciais. Diante da ausência de um mecanismo estatal focado na emissão de atestados demográficos, as empresas impõem métodos de validação que comprometem a privacidade do cidadão. A exigência do envio de fotografias de documentos civis e capturas faciais resulta na construção de repositórios centralizados de dados sensíveis. Embora os vazamentos de dados representem uma ameaça considerável, o problema central reside na exploração comercial dessas informações pelas próprias empresas. Os dados coletados sob a justificativa de verificação etária frequentemente são reaproveitados para a criação de perfis comportamentais, direcionamento de publicidade hipersegmentada e até mesmo comercializados com terceiros sem o consentimento explícito do titular. Essa estrutura de monetização da identidade civil contrasta com o modelo proposto pelo eIDAS 2.0, que estabelece os Estados-membros como pilares emissores das credenciais de identidade, impedindo que verificadores solicitem mais dados do que o estritamente necessário (European Digital Identity, 2025).

O fornecimento estatal de uma carteira de identidade munida de SD-JWT e ZKP corrigiria essa defasagem estrutural. Os smartphones da população gerariam as provas ZKP de atestado de idade localmente, isentando as plataformas comerciais da coleta e custódia de dados de identificação cruzada. A combinação da divulgação seletiva com ZKP satisfaria os requisitos legais para impedir o acesso a serviços online restritos, removendo a necessidade de compartilhar documentos civis ou biometria em

texto aberto. Em conclusão, a integração das bases de governo a mecanismos de minimização forneceria o arranjo tecnológico necessário para compatibilizar a segurança de rede com o respeito à privacidade individual.

7.6 A ARQUITETURA DE IDENTIDADE AUTO-SOBERANA FRENTE À INFRAESTRUTURA NACIONAL E PADRONIZAÇÃO INTERNACIONAL

A validação do aplicativo extrapola o funcionamento dos algoritmos locais, demandando considerações sobre a expansão do modelo a âmbitos estatais. Embora a literatura de Identidade Auto-Soberana defenda a eliminação completa das autoridades de controle (BABEL et al., 2025), o cenário brasileiro atua amparado na solidez da infraestrutura de chaves públicas e do portal oficial do governo federal. Esses sistemas nacionais apresentam histórico consistente de funcionamento prático e abrangem grande parte da população. Descartar essa infraestrutura de identificação construída sobre segurança institucional confiável em favor de fundamentos puramente teóricos de descentralização resultaria no desperdício de investimentos acumulados por décadas.

Diante do contexto, apoiar as especificações globais de carteiras digitais sobre a estrutura já consolidada do Estado brasileiro reflete pragmatismo arquitetural. Combinar as emissões originadas do controle estatal com as técnicas de custódia e de apresentação descentralizada compõe um modelo de dados essencialmente híbrido. A adoção desse direcionamento implica renunciar ao requisito de descentralização completa das plataformas de governo em favor dos ganhos de escala proporcionados pela infraestrutura já existente. A manutenção das emissões sob tutela governamental preserva o lastro jurídico dos registros civis, fornece barreiras protetivas severas contra a falsidade ideológica e dispõe de meios efetivos para atuar na revogação de acessos ilícitos.

A continuidade da gerência institucional garante o lastro legal para arquivos de formato digital fundamentais, englobando registros civis e certidões acadêmicas. O uso das assinaturas digitais emitidas pelos órgãos de Estado viabiliza a rápida adoção da verificação em redes de bancos ou cartórios do setor privado, que baseiam os processos de auditoria exclusivamente nas raízes certificadoras governamentais. A tentativa de forçar a adoção paralela de redes de provedores descentralizados de identidade, desvinculados do controle federal, depararia com enormes rejeições em etapas de formalização de acordos comerciais.

Em contrapartida à dependência de emissão oficial, os mecanismos da carteira conferem ganhos decisivos no bloqueio ao rastreamento cotidiano. O modelo padrão de acesso federado impõe comunicações ativas com os portais governamentais para viabilizar login de identificação em sites particulares, alimentando servidores centrais com as métricas de tráfego populacional. A implementação da divulgação

seletiva via SD-JWT e ZKP transfere aos smartphones locais a responsabilidade da confirmação matemática. Essa lógica possibilita as validações sem qualquer tráfego externo simultâneo com o banco de dados oficial, impedindo o Estado de auditar os hábitos recorrentes e os serviços acessados pelo titular.

O balanço operacional evidencia que ceder a condição de anonimato ao emissor federal apresenta uma troca positiva frente à conquista de forte mitigação de exposição direcionada às empresas comerciais. O controle gerado pela gestão do próprio usuário sobre os atestados da carteira digital propicia níveis práticos de confidencialidade amplamente superiores às autenticações que dependem do redirecionamento de navegadores online. Esse modelo fragmentado de preservação da privacidade estabelece um compromisso viável entre os requisitos de controle administrativo e o direito do usuário à minimização de dados (Ramos Fernández, 2024).

A avaliação dos modelos de carteiras de identidade digital no cenário exterior reforça que a centralização da emissão configura um caminho de conformidade. O eIDAS 2.0 estipulou uma base na qual os Estados-membros se mantêm posicionados como pilares fornecedores do vínculo das chaves aos titulares civis (European Digital Identity, 2025). Esse distanciamento das pautas mais extremas do movimento de auto-soberania valida o direcionamento híbrido e deve atuar como referencial confiável aos projetos em elaboração em território brasileiro.

Nesse contexto, a relevância técnica da Identidade Auto-Soberana para a arquitetura do Brasil reside principalmente na adoção de um formato internacional unificado de representação de Verifiable Credentials. Documentos estruturados sob formatos baseados em especificações W3C e DIF permitem o desenvolvimento de softwares de verificação mantidos globalmente e de baixo custo. Os parâmetros padronizados minimizam a necessidade crônica de escrever diferentes códigos de integração para abranger cada emissão individual de governos regionais ou de certidões burocráticas específicas.

O alinhamento perante as normas consagradas amplia o uso prático da carteira digital para transações que extrapolem fronteiras nacionais, fator decisivo na elaboração dos laços econômicos com blocos e vizinhos geopolíticos. A compatibilidade das bibliotecas criptográficas com padrões como SD-JWT e OID4VP propicia o cenário para que a certificação de trânsito brasileira apresente funcionalidade no ecossistema viário das regiões fronteiriças internacionais em cenários sem exigência contínua de conexão ao banco de dados federal. A interoperabilidade criptográfica entre sistemas baseados em SD-JWT e OID4VP cria condições para que credenciais emitidas no Brasil sejam verificadas em contextos internacionais, favorecendo a mobilidade acadêmica e profissional.

Diante de todas essas análises, fica evidente a importância do Brasil adotar formatos de divulgação seletiva assentados nos sistemas operacionais da assinatura

nacional vigente. Essa combinação permite incorporar os avanços técnicos do ecossistema internacional às bases jurídicas das repartições públicas nacionais. A orientação europeia pauta uma via segura à mitigação dos impasses de aceitabilidade dos registros portáteis, estabelecendo um modelo de identidade digital que, ao mesmo tempo, respeita a soberania dos Estados e garante a privacidade dos cidadãos além das fronteiras nacionais.

7.7 LIMITAÇÕES DO ESTUDO

O planejamento e o desenvolvimento operaram restrições práticas no escopo da pesquisa de software, as quais limitam a aplicação universal e a transposição genérica das métricas obtidas. O esforço inicial na montagem do aplicativo concentrou atenções sobre o funcionamento no sistema operacional Android. A ausência de inspeções de fluxo nas plataformas baseadas em iOS impede que se promovam comparações eficientes a respeito dos atritos de vinculação do código e do gasto computacional do hardware entre marcas distintas de smartphones. Além disso, a validação orientou-se ao consumo exclusivo das estruturas de comunicação via requisições HTTP remotas, o que eliminou os ensaios da etapa de transação em proximidade baseada em NFC/BLE — item prioritário estipulado pelas especificações internacionais (ISO/IEC 18013-5) para momentos inóspitos à rede de telecomunicações convencional.

O fornecimento das credenciais dependeu integralmente de cenários contidos de simulação acadêmica, pois as arquiteturas atuaram desligadas das bases de dados reais das repartições de ensino da universidade e isentas do fluxo de autenticação governamental do portal gov.br. A ausência do vínculo limitou a análise de requisições de servidores, retendo as inferências de tempo às etapas criptográficas processadas sob a custódia das CPUs nos dispositivos locais, impedindo assim computar os atrasos estruturais provocados pelos percursos de transferência criptografada de pacotes nas infraestruturas brasileiras.

7.8 TRABALHOS FUTUROS

As restrições estipuladas apontam caminhos norteadores imediatos visando expandir a continuidade e maturação das tecnologias focadas nas identidades portáteis de código aberto. A inserção e teste aprofundado dos modelos voltados à conectividade direta por NFC/BLE entre smartphones representa um objetivo primário. Essa implementação proporciona um canal de transporte essencial para o controle de acesso local em ambientes sem conexão à internet. O acoplamento propicia que leitoras de controle de acesso físico reconheçam a DID do dispositivo do estudante

via protocolo de proximidade, alinhando o protótipo à funcionalidade requisitada pela norma ISO/IEC 18013-5.

A evolução do protótipo em direção a um sistema de produção demanda a integração com os sistemas de gestão acadêmica da universidade. A realização de testes com dados reais permitiria validar o comportamento do protótipo sob carga efetiva, verificando se os princípios de minimização de dados das Verifiable Credentials se mantêm em um ambiente institucional integrado.

Paralelamente, deve-se adotar o gerenciamento de chaves privadas nos enclaves de hardware seguros dos smartphones, como o Android Keystore e o Secure Element, elevando o nível de proteção contra ataques de extração de memória e acessos não autorizados ao repositório local. Além disso, os circuitos ZK empregados nas rotinas de prova exigem auditorias criptográficas independentes conduzidas por especialistas em segurança, fora do escopo do projeto originário. Somente essa certificação atestará a integridade técnica necessária para viabilizar o uso de ZKP e SD-JWT em atestados que envolvam dados pessoais sensíveis de cidadãos.

8 CONCLUSÃO

Este trabalho teve como objetivo investigar a viabilidade técnica da aplicação de tecnologias de identidade auto-soberana, Verifiable Credentials e provas ZKP no contexto institucional brasileiro. Para fundamentar a pesquisa, foi desenvolvido um protótipo de carteira digital orientado ao cenário operacional de uma instituição de ensino superior.

A revisão da literatura e a análise documental permitiram mapear as diferenças estruturais entre as propostas internacionais de identidade descentralizada, com destaque para a arquitetura europeia EUDI Wallet, e a infraestrutura brasileira, ancorada na cadeia de certificação ICP-Brasil e em plataformas centralizadas como o gov.br. O desenvolvimento do artefato de software funcionou como um estudo preliminar das capacidades de bibliotecas de código aberto em ambiente móvel para a execução dos ciclos de emissão, custódia e verificação de atributos, configurando um estágio anterior à construção de um produto mínimo viável de integração nacional.

Os ensaios de execução do sistema indicaram o funcionamento lógico das provas ZKP e dos protocolos de divulgação seletiva via SD-JWT nos cenários delineados. No entanto, o protótipo operou de forma isolada e sem comunicação com sistemas institucionais ou bases governamentais. A pesquisa não provou integralmente o funcionamento dos conceitos no cenário amplo do país. Os resultados demonstraram que é possível realizar o ciclo criptográfico em dispositivos locais usando ferramentas de acesso público, o que sugere a possibilidade de extrapolar os algoritmos para integrações reais. A validação concreta da viabilidade da tecnologia no Brasil dependeria da conexão do fluxo com serviços de dados autênticos e de testes em ambiente de produção.

A comparação de arquiteturas aponta para a consideração de um modelo de operação híbrido como alternativa de implementação. A concentração do processo de emissão nas autoridades de estado manteria o lastro jurídico dos registros. Em paralelo, a delegação da custódia e do controle de apresentação das Verifiable Credentials aos usuários introduziria métodos técnicos de limitação de rastreamento e divulgação seletiva minimizada, operando por meio de formatos padronizados como SD-JWT e OID4VP, sem substituir as entidades originais de registro.

As limitações metodológicas restringiram a abrangência das conclusões do estudo. O código executou rotinas exclusivamente no sistema operacional Android, operando sem os tempos de latência de tráfego de dados em redes de longa distância e sem protocolos de comunicação em proximidade por NFC/BLE. O desenvolvimento omitiu os testes de integração com esses canais de curta distância, limitando a avaliação dos cenários físicos de identificação.

A progressão da pesquisa na área demanda a formulação de sistemas conectados a interfaces dos provedores de identidade do estado, buscando a mensuração da escalabilidade em infraestruturas reais. Recomenda-se o estudo do intercâmbio de dados por NFC/BLE segundo a norma ISO/IEC 18013-5 e a investigação do armazenamento de chaves assimétricas em enclaves de hardware seguros dos smartphones. A condução de auditorias independentes dos circuitos ZK forma a base necessária para a evolução dos níveis de confiança nos protocolos de divulgação seletiva e ZKP.

REFERÊNCIAS

- ABE, R.; SUZUKI, S.; NAKAMURA, O. A conceptual model for claim validation based on cryptographically signed data. **IEEE Access**, v. 13, p. 2723–2735, 2025.
- AGARKAR, A. A. et al. Blockchain aware decentralized identity management and access control system. **Measurement: Sensors**, v. 31, p. 101032, 2024. ISSN 2665-9174. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2665917424000084>.
- AHMED, I. et al. A systematic review on blockchain-enabled ekyc: Leveraging ssi and did for secure and efficient identity verification. **IEEE Internet of Things Journal**, v. 12, n. 21, p. 44381–44401, 2025.
- ALLEN, C. **The Path to Self-Sovereign Identity**. 2016. <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>. Acessado em: 04/12/2025.
- ALLEN, C. et al. **Decentralized Public Key Infrastructure**. [S.l.], 2015.
- ANDRIEU, J.; HARDMAN, D.; GUY, A. **DID Method Rubric v1.0**. [S.l.], 2022. Disponível em: <https://www.w3.org/TR/did-rubric/>.
- Apple. **Vio: QR Seguro - App Store**. 2026. Acessado em: 21 mar. 2026. Disponível em: <https://apps.apple.com/cm/app/vio-qr-seguro/id1218953994>.
- BABEL, M. et al. Self-sovereign identity and digital wallets. **Electronic Markets**, Springer, Berlin, Heidelberg, v. 35, n. 1, 2025. ISSN 1422-8890. Disponível em: <https://hdl.handle.net/10419/323604>.
- BAKHTINA, M.; LEUNG, K. L.; MATULEVICIUS, R.; AWAD, A.; SVENDA, P. A decentralised public key infrastructure for x-road. *In: Proceedings of the 18th International Conference on Availability, Reliability and Security*. New York, NY, USA: Association for Computing Machinery, 2023. (ARES '23). ISBN 9798400707728. Disponível em: <https://doi.org/10.1145/3600160.3605092>.
- BEN-SASSON, E.; BENTOV, I.; HORESH, Y.; RIABZEV, M. Scalable, transparent, and post-quantum secure computational integrity. **IACR Cryptol. ePrint Arch.**, v. 2018, p. 46, 2018. Disponível em: <https://api.semanticscholar.org/CorpusID:44557939>.
- BEN-SASSON, E.; CHIESA, A.; TROMER, E.; VIRZA, M. Succinct non-interactive zero knowledge for a von neumann architecture. *In: Proceedings of the 23rd USENIX Conference on Security Symposium*. USA: USENIX Association, 2014. (SEC'14), p. 781–796. ISBN 9781931971157.
- BIONI, B.; GARROTE, M.; MEIRA, M.; PASCHOALINI, N. The digitization of the brazilian national identity system: A descriptive and qualitative analysis of its information architecture. **Data & Policy**, v. 4, p. e22, 2022.
- BIRCH, D. **Identity is the New Money**. [S.l.]: London Publishing Partnership, 2014. (Perspectives). ISBN 978-1-907994-12-8.

BLUM, M.; FELDMAN, P.; MICALI, S. Non-interactive zero-knowledge and its applications. *In*: _____. [S.l.: s.n.], 2019. ISBN 9781450372664.

BOCHNIA, R.; ANKE, J. Long-lived verifiable credentials: Ensuring durability beyond the issuer's lifetime. *In*: **Proceedings of the 19th International Conference on Availability, Reliability and Security**. New York, NY, USA: Association for Computing Machinery, 2024. (ARES '24). ISBN 9798400717185. Disponível em: <https://doi.org/10.1145/3664476.3669933>.

Brasil. **Medida Provisória nº 2.200-2, de 24 de agosto de 2001**. 2001. http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

Brasil. **Decreto nº 10.900, de 17 de dezembro de 2021**. 2021. Acessado em: 21 mar. 2026. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/2021/decreto-10900-17-dezembro-2021-792118-norma-pe.html>.

Brasil. **Lei nº 14.129, de 29 de março de 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública**. 2021. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14129.htm. Acesso em: 05 nov. 2025.

Brasil. **Decreto nº 10.977, de 23 de fevereiro de 2022. Regulamenta a Lei nº 7.116, de 29 de agosto de 1983, e a Lei nº 9.454, de 7 de abril de 1997, para estabelecer os procedimentos e os requisitos para a expedição da Carteira de Identidade Nacional**. 2022. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/D10977.htm. Acesso em: 05 nov. 2025.

Brasil. **Lei nº 14.534, de 11 de janeiro de 2023. Estabelece o Cadastro de Pessoa Física (CPF) como número único e suficiente para identificação do cidadão nos bancos de dados de serviços públicos**. 2023. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/L14534.htm. Acesso em: 05 nov. 2025.

BUCCAFURRI, F.; LICCIARDI, C. Towards privacy-preserving revocation of verifiable credentials with time-flexibility. *In*: **2025 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)**. [S.l.: s.n.], 2025. p. 516–521. ISSN 2768-0657.

BUMILLER, A.; KOZYRI, E.; DAGENBORG, H. Privacy preserving identity federation: A literature study. **ACM Comput. Surv.**, Association for Computing Machinery, New York, NY, USA, jul. 2025. ISSN 0360-0300. Just Accepted. Disponível em: <https://doi.org/10.1145/3745018>.

CAMENISCH, J.; LYSYANSKAYA, A. Dynamic accumulators and application to efficient revocation of anonymous credentials. *In*: **Advances in Cryptology — CRYPTO 2002**. [S.l.]: Springer Berlin Heidelberg, 2002. p. 61–76.

CAMERON, K. The laws of identity. **Microsoft Corporation**, May 2005. White Paper. Disponível em: <http://www.identityblog.com/stories/2004/12/09/thelaws.html>.

CASTELLANO, D.; PRISCO, R. D.; FARUOLO, P. Login system for openid connect with verifiable credentials. *In: 2024 22nd International Symposium on Network Computing and Applications (NCA)*. [S.l.: s.n.], 2024. p. 105–112. ISSN 2643-7929.

Certifica Certificado Digital. **Conta Gov.br Prata E Ouro: Guia Para Subir De Nível!** 2026. Acessado em: 21 mar. 2026. Disponível em: <https://certifica.com.br/blog/conta-govbr-prata-e-ouro/>.

COMANDÈ, G.; VARILEK, M. The many features which make the eIDAS 2 digital wallet either risky or the ideal vehicle for the transition to post-quantum encryption. **Computer Law & Security Review**, v. 54, p. 106022, 2024.

COOPER, D. et al. **Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**. [S.l.], 2008.

CORICI, A. A. et al. Enhancing european interoperability frameworks to leverage mobile cross-border services in europe. *In: Proceedings of the 23rd Annual International Conference on Digital Government Research*. New York, NY, USA: Association for Computing Machinery, 2022. (dg.o '22), p. 41–53. ISBN 9781450397490. Disponível em: <https://doi.org/10.1145/3543434.3543638>.

DEGEN, K.; TEUBNER, T. Wallet wars or digital public infrastructure? orchestrating a digital identity data ecosystem from a government perspective. **Electronic Markets**, 2024. Disponível em: <https://link.springer.com/article/10.1007/s12525-024-00731-1>.

DHAMIJA, R.; DUSSEAUT, L. The seven flaws of identity management: Usability and security challenges. *In: IEEE Security & Privacy*. [S.l.]: IEEE, 2008.

DIEYE, M. et al. A self-sovereign identity based on zero-knowledge proof and blockchain. **IEEE Access**, PP, p. 1–1, 01 2023.

eIDAS Expert Group. **Architecture and Reference Framework**. [S.l.], 2023. Documento de trabalho sobre a Carteira de Identidade Digital da UE.

ENGE, A.; SATYBALDY, A.; NOWOSTAWSKI, M. An offline mobile access control system based on self-sovereign identity standards. **Computer Networks**, v. 219, p. 109434, 2022.

HEIRETH ENGE, A.; SATYBALDY, A.; NOWOSTAWSKI, M. An architectural framework for enabling secure decentralized p2p messaging using didcomm and bluetooth low energy. *In: 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*. [S.l.: s.n.], 2022. p. 1579–1586. ISSN 0730-3157.

ETSI. **Electronic Signatures and Trust Infrastructures (ESI); Relying party attributes supporting EUDI Wallet user's authorization decisions**. [S.l.], 2025.

European Commission. **EUDI Wallet Kit React Native**. 2026. Acessado em: 21 mar. 2026. Disponível em: <https://github.com/openwallet-foundation-labs/eudi-wallet-kit-react-native>.

European Digital Identity. **Architecture and Reference Framework – EUDI Wallet**. 2025. Version 2.4.0, Accessed: November 2025. Disponível em: <https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/>.

European Telecommunications Standards Institute (ETSI). **Electronic Signatures and Infrastructures (ESI); Analysis of selective disclosure and zero-knowledge proofs applied to Electronic Attestation of Attributes**. [S.l.], 2023. Versão 1.1.1. Disponível em: https://www.etsi.org/deliver/etsi_tr/119400_119499/119476/01.01.01_60/tr_119476v010101p.pdf.

FENG, Z.; LI, Z.; CUI, H.; WHITTY, M. T. Identity management systems: A comprehensive review. **Information**, v. 16, p. 778, 2025. Disponível em: <https://doi.org/10.3390/info16090778>.

FETT, D.; CAMPBELL, B.; YASUDA, K. **Selective Disclosure for JWTs (SD-JWT)**. [S.l.], 2024. Disponível em: <https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/>.

FIAT, A.; SHAMIR, A. How to prove yourself: Practical solutions to identification and signature problems. *In*: . [S.l.: s.n.], 1999. v. 263. ISBN 978-3-540-18047-0.

FLAMINI, A. et al. On cryptographic mechanisms for the selective disclosure of verifiable credentials. **Journal of Information Security and Applications**, v. 83, p. 103789, 2024.

GARCÍA-RODRÍGUEZ, J.; KRENN, S.; Bernal Bernabe, J.; SKARMETA, A. Beyond selective disclosure: Extending distributed p-abc implementations by commit-and-prove techniques. **Computer Networks**, v. 248, p. 110498, 2024.

GlobalPlatform. **Securing the European Digital Identity Wallets**. [S.l.], 2025. Acessado em: 21 mar. 2026. Disponível em: <https://globalplatform.org/wp-content/uploads/2025/06/Securing-the-European-Digital-Identity-Wallets-Meeting-the-challenges-of-technology-sovereignty-and-certification.pdf>.

GOLDREICH, O.; MICALI, S.; WIGDERSON, A. Proofs that yield nothing but their validity and a methodology of cryptographic protocol design. *In*: _____. [S.l.: s.n.], 2019. ISBN 9781450372664.

GOLDREICH, O.; OREN, Y. Definitions and properties of zero-knowledge proof systems. **Journal of Cryptology**, v. 7, 06 2002.

GOLDWASSER, S.; MICALI, S.; RACKOFF, C. The knowledge complexity of interactive proof-systems. *In*: **Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing**. New York, NY, USA: Association for Computing Machinery, 1985. (STOC '85), p. 291–304. ISBN 0897911512. Disponível em: <https://doi.org/10.1145/22145.22178>.

GÓMEZ, S. **Trust Models for Digital Identity: State of play**. [S.l.], 2025.

Governo Digital. **Saiba mais sobre os níveis da conta gov.br**. 2026. Acessado em: 21 mar. 2026. Disponível em: <https://www.gov.br/governodigital/pt-br/identidade/conta-gov-br/niveis-da-conta-govbr>.

Governo do Brasil. **Obter Carteira Digital de Trânsito (CDT)**. 2024. <https://www.gov.br/pt-br/servicos/obter-carteira-digital-de-transito>. Acesso em: 05 nov. 2025.

Governo Federal do Brasil. **Carteira de Identidade Nacional CIN**. 2026. Acessado em: 21 mar. 2026. Disponível em: <https://www.gov.br/governodigital/pt-br/identidade/identificacao-do-cidadao-e-carteira-de-identidade-nacional/carteira-de-identidade-nacional-cin-1>.

Governo Federal do Brasil. **Obter Mais confiabilidade na Conta de Acesso**. 2026. Acessado em: 21 mar. 2026. Disponível em: <https://acesso.gov.br/faq/perguntasdafaq/obtermaisconfiabilidadenacontadeacesso.html>.

HOOPS, F.; MATTHES, F. A universal system for openid connect sign-ins with verifiable credentials and cross-device flow. *In: 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. [S.l.: s.n.], 2024. p. 296–298. ISSN 2832-8906.

Hyperledger Foundation. **Hyperledger AnonCreds React Native**. 2026. Acessado em: 21 mar. 2026. Disponível em: <https://github.com/anoncreds/anoncreds-wrapper-javascript/tree/main/packages/anoncreds-react-native>.

iDAKTO. **Profiles for Achieving Compliance and Interoperability in the EUDI Wallet Ecosystem**. 2025. Acessado em: 21 mar. 2026. Disponível em: <https://www.idakto.com/wp-content/uploads/2025/09/invited3.pdf>.

Instituto Nacional de Tecnologia da Informação. **DOC-ICP-10: Regulamento para Homologação de Sistemas e Equipamentos de Certificação Digital no Âmbito da ICP-Brasil**. [S.l.], 2021. Disponível em: <https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-10-versao-3-1-pdf>.

Instituto Nacional de Tecnologia da Informação. **Instrução Normativa ITI N° 22, de 23 de março de 2022. Aprova a versão revisada e consolidada do documento Padrões e Algoritmos (DOC-ICP-01.01)**. [S.l.], 2022. Acessado em: 21 mar. 2026. Disponível em: https://www.gov.br/iti/pt-br/assuntos/legislacao/documentos-principais/IN2022_22_DOCICP01.01_compilada.pdf.

JEYAKUMAR, I. H. J.; KUBACH, M. A trust implementation model for cross-domain decentralized identity ecosystems: architecture, use case, and implementation. **Procedia Computer Science**, v. 254, p. 10–19, 2025.

KATZ, J.; LINDELL, Y. **Introduction to Modern Cryptography**. [S.l.]: Chapman and Hall/CRC, 2007. ISBN 978-1584885511.

KERSIC, V.; VIDOVIC, U.; VRECKO, A.; DOMAJNKO, M.; TURKANOVIC, M. Orchestrating digital wallets for on- and off-chain decentralized identity management. **IEEE Access**, v. 11, p. 78135–78151, 2023. ISSN 2169-3536.

KITCHENHAM, B.; CHARTERS, S. Guidelines for performing systematic literature reviews in software engineering. v. 2, 01 2007.

KUDRA, A. et al. Digital identity wallets: A guide to the eu's new identity model. **Information Systems Journal**, p. n/a–n/a, 08 2025.

LANZA, B. B. B.; ÁVILA, T. J. T.; VALOTTO, D. An overview of rede.gov.br as a federative mechanism for digital government development in brazil. *In: Proceedings of the 23rd Annual International Conference on Digital Government Research*. New

York, NY, USA: Association for Computing Machinery, 2022. (dg.o '22), p. 380–390. ISBN 9781450397490. Disponível em: <https://doi.org/10.1145/3543434.3543655>.

LAVIN, R. et al. A survey on the applications of zero-knowledge proofs. **ArXiv**, abs/2408.00243, 2024. Disponível em: <https://api.semanticscholar.org/CorpusID:271600687>.

LEKA, B.; NIKOLLA, M.; KAMBO, A. The role of ai and blockchain in enhancing digital identity and digital wallets in albania. *In: .* [S.l.: s.n.], 2025.

LEPORE, C.; LABORDE, R.; EYNARD, J. Aligning eidas and trust over ip: A mapping approach. *In: **Proceedings of the 19th International Conference on Availability, Reliability and Security***. New York, NY, USA: Association for Computing Machinery, 2024. (ARES '24). ISBN 9798400717185. Disponível em: <https://doi.org/10.1145/3664476.3670919>.

LI, H.; JING, Y.; GUAN, Z. The review and comparison between centralized and decentralized digital identity systems. **Mobile Information Systems**, v. 2024, 2024. Disponível em: <https://doi.org/10.1155/2024/6651273>.

LINDQUIST, J. Introducing privacy receipts into dlt and eidas. **Journal of ICT Standardization**, v. 11, n. 2, p. 117–134, 2023. ISSN 2246-0853.

LOOKER, T.; KALOS, V.; WHITEHEAD, A.; LODDER, M. **The BBS Signature Scheme**. [S.l.], 2026. Disponível em: <https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/>.

LOUTOCKÝ, P.; STUPKA, V.; KASL, F. Certification of the eu digital identity wallets and its challenges in the era of ai. *In: **2025 MIPRO 48th ICT and Electronics Convention***. [S.l.: s.n.], 2025. p. 1636–1641. ISSN 1847-3938.

LUKKIEN, B.; BHAROSA, N.; DE REUVER, M. Barriers for developing and launching digital identity wallets. *In: **Proceedings of the 24th Annual International Conference on Digital Government Research***. New York, NY, USA: Association for Computing Machinery, 2023. (dg.o '23), p. 289–299. ISBN 9798400708374. Disponível em: <https://doi.org/10.1145/3598469.3598501>.

MAZZOCCA, C. et al. A survey on decentralized identifiers and verifiable credentials. **IEEE Communications Surveys & Tutorials**, p. 1–1, 2025.

MENEZES, A. J.; OORSCHOT, P. C. van; VANSTONE, S. A. **Handbook of Applied Cryptography**. [S.l.]: CRC Press, 1996. ISBN 0-8493-8523-7.

Meta Platforms, Inc. **React Native: The New Architecture**. 2026. Acessado em: 21 mar. 2026. Disponível em: <https://reactnative.dev/architecture/overview>.

MILENKOVIĆ, M.; VOJKOVIĆ, G. Implementation of regulation (eu) 2024/1183 in higher education in the republic of croatia. *In: **2025 MIPRO 48th ICT and Electronics Convention***. [S.l.: s.n.], 2025. p. 1642–1647. ISSN 1847-3938.

Ministério da Gestão e da Inovação em Serviços Públicos. **Conta gov br**. 2024. <https://www.gov.br/governodigital/pt-br/identidade/conta-gov-br>. Acesso em: 05 nov. 2025.

Ministério da Gestão e da Inovação em Serviços Públicos. **Passo-a-Passo para Integrar — Documentação Roteiro de Integração do Login Único**. [S.l.], 2025. Última atualização: 30/10/2025. Disponível em: <https://acesso.gov.br/roteiro-tecnico/iniciarintegracao.html>.

Mopro. **mopro-react-native-package: Client-side ZKP generation**. 2026. Acessado em: 21 mar. 2026. Disponível em: <https://github.com/zkmopro/mopro>.

MORE, S.; HEHER, J.; FASLLIJA, E.; MATHIE, M. Service provider accreditation: Enabling and enforcing privacy-by-design in credential-based authentication systems. *In: Proceedings of the 19th International Conference on Availability, Reliability and Security*. New York, NY, USA: Association for Computing Machinery, 2024. (ARES '24). ISBN 9798400717185. Disponível em: <https://doi.org/10.1145/3664476.3669934>.

MÜHLE, A.; GRÜNER, A.; GAYVORONSKAYA, T.; MEINEL, C. A survey on essential components of a self-sovereign identity. **Hasso Plattner Institute**, Potsdam, Germany, 2018.

National Institute of Standards and Technology. **Digital Identity Guidelines: Federation and Assertions**. Gaithersburg, MD, 2017.

National Institute of Standards and Technology. **Digital Signature Standard (DSS)**. [S.l.], 2023.

NEVES, F. R.; SILVA, P. B. d. From paper to digital: e-government's evolution and pitfalls in brazil. *In: _____. Recent Advances in Data and Algorithms for e-Government*. Cham: Springer International Publishing, 2023. p. 193–211. ISBN 978-3-031-22408-9. Disponível em: https://doi.org/10.1007/978-3-031-22408-9_9.

OpenID Foundation. **International Government Assurance Profile (iGov) for OpenID Connect 1.0 - draft 04**. [S.l.], 2026. Acessado em: 21 mar. 2026. Disponível em: https://openid.net/specs/openid-igov-openid-connect-1_0.html.

OpenID Foundation Standards. **OpenID for Verifiable Credential Issuance**. [S.l.], 2024. Version 1.0. Disponível em: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

OpenID Foundation Standards. **OpenID for Verifiable Presentations**. [S.l.], 2024. Version 1.0. Disponível em: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html.

OpenWallet Foundation. **Credo (formerly Aries Framework JavaScript)**. 2026. Acessado em: 21 mar. 2026. Disponível em: <https://github.com/openwallet-foundation/credo-ts>.

OTT, S. et al. Multitee: Distributing trusted execution environments. *In: Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*. New York, NY, USA: Association for Computing Machinery, 2024. (ASIA CCS '24), p. 1617–1629. ISBN 9798400704826. Disponível em: <https://doi.org/10.1145/3634737.3637675>.

Parlamento Europeu e Conselho da União Europeia. **Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho, de 11 de abril de 2024, que altera o Regulamento (UE) n.º 910/2014 no que diz respeito ao estabelecimento de um quadro para uma identidade digital europeia.** 2024.

POLYCHRONAKI, M.; CHRISTIDIS, I.; XEVGENIS, M. G.; KOGIAS, D. G.; LELIGOU, H. C. My university studies (m.u.st): An academic proof of concept for the web3.0. *In: Proceedings of the 28th Pan-Hellenic Conference on Progress in Computing and Informatics*. New York, NY, USA: Association for Computing Machinery, 2025. (PCI '24), p. 148–154. ISBN 9798400713170. Disponível em: <https://doi.org/10.1145/3716554.3716576>.

PREUKSCHAT, A.; REED, D. **Self-Sovereign Identity: Decentralized digital identity and verifiable credentials**. [S.l.]: Manning, 2021. ISBN 9781617296598.

Ramos Fernández, R. Evaluation of trust service and software product regimes for zero-knowledge proof development under eidas 2.0. **Computer Law & Security Review**, v. 53, p. 105968, 2024.

RASHME, T. Zero knowledge proof: An overview. **International Journal of Knowledge Based Computer Systems**, v. 12, p. 34–45, 07 2024.

REECE, M.; MITTAL, S. **Self-Sovereign Identity in a World of Authentication: Architecture and Domain Usecases**. 2022. Disponível em: <https://arxiv.org/abs/2209.11647>.

SANTOS, M.; FIGUEIREDO, R.; GOMES, M. Evolução das perspectivas sobre a digitalização do governo no brasil de 2000 a 2023. **REVES - Revista Relações Sociais**, v. 6, p. 17777, 12 2023.

SCHARDONG, F.; CUSTÓDIO, R. Self-sovereign identity: A systematic map and review. 08 2021.

SCHUMM, D.; MÜLLER, K. O. E.; STILLER, B. **Are We There Yet? A Study of Decentralized Identity Applications**. 2025. Disponível em: <https://arxiv.org/abs/2503.15964>.

SCHWALM, S.; ALBRECHT, D.; ALAMILLO, I. eidas 2.0: Challenges, perspectives and proposals to avoid contradictions between eidas 2.0 and ssi. *In: SCHWALM, S.; ALBRECHT, D.; ALAMILLO, I. (Ed.). Open Identity Summit 2022*. Bonn: Gesellschaft für Informatik, 2022. (Lecture Notes in Informatics (LNI)).

Sebrae. **Como aumentar o nível de acesso da conta GOV.BR?** 2026. Acessado em: 21 mar. 2026. Disponível em: <https://sebrae.com.br/sites/PortalSebrae/artigos/como-aumentar-o-nivel-de-acesso-da-conta-govbr>.

Serpro. **Gerar QR CODE VIO**. 2026. Acessado em: 21 mar. 2026. Disponível em: <https://loja.serpro.gov.br/gerar-qr-code-vio/product/viogeraqrqrcode>.

Serpro. **Vio**. 2026. Acessado em: 21 mar. 2026. Disponível em: <https://serpro.gov.br/en/our-services/vio>.

SHARIF, A. et al. The eIDAS regulation: A survey of technological trends for European electronic identity schemes. **Applied Sciences**, v. 12, n. 24, p. 12679, 2022. Disponível em: <https://doi.org/10.3390/app122412679>.

SHEYBANI, N.; AHMED, A.; KINSY, M. A.; KOUSHANFAR, F. Zero-knowledge proof frameworks: A systematic survey. **ArXiv**, abs/2502.07063, 2025. Disponível em: <https://api.semanticscholar.org/CorpusID:276258749>.

SOLTANI, R.; NGUYEN, U.; AN, A. A survey of self-sovereign identity ecosystem. 11 2021.

SPANÓ, E.; SILVA, V. Public service innovation in Brazil after COVID-19: digital platforms across the levels of public administration. **Revista Tecnologia e Sociedade**, v. 18, p. 324, 07 2022.

SPORNY, M. et al. **Verifiable Credentials Data Model v2.0**. [S.l.], 2025. Última versão consultada em 26 Nov 2025. Disponível em: <https://www.w3.org/TR/vc-data-model-2.0/>.

SPORNY, M. et al. **Decentralized Identifiers (DIDs) v1.1**. [S.l.], 2023. Consultado em Nov 2025. Disponível em: <https://www.w3.org/TR/did-1.1/>.

STEELE, O.; PROROCK, M. **DID Implementation Guide v1.0**. [S.l.], 2022. Disponível em: <https://w3c.github.io/did-imp-guide/>.

The European Parliament and the Council of the European Union. **Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC**. 2014. 73–114 p.

Trust Agency. **Unofficial Consolidated eIDAS 2 Text**. [S.l.], 2024. Documento não oficial consolidando o Regulamento (UE) N.º 910/2014 com o Regulamento (UE) 2024/1183.

Universidade Federal de Uberlândia. **Entenda o programa Conecta GOV.BR e os benefícios que a busca de informações governamentais pode trazer para os sistemas da UFU**. 2024. Acessado em: 21 mar. 2026. Disponível em: <https://comunica.ufu.br/comunicados/2024/09/entenda-o-programa-conecta-govbr-e-os-beneficios-que-busca-de-informacoes>.

VAZIRY, A.; GARZON, S. R.; HERBKE, P.; SEGAT, C.; KÜPPER, A. Sok: A taxonomy for distributed-ledger-based identity management. In: **2025 Crypto Valley Conference (CVC)**. [S.l.: s.n.], 2025. p. 56–80.

Verifiable Credentials Working Group. **Verifiable Credentials Overview**. [S.l.], 2025. Última versão consultada em 26 Nov 2025. Disponível em: <https://www.w3.org/TR/vc-overview/>.

VITALI, F. **SELF-SOVEREIGN IDENTITY: STUDY OF THE MODEL AND CENSUS OF INTERNATIONAL PROJECTS**. 2022. Dissertação (Mestrado) — Politecnico di Milano, 2022. Master of Science in Management Engineering.

VUCINIC, M.; SELANDER, G.; TOUTAIN, L. **CBOR Object Signing and Encryption (COSE): General Considerations and Selectors**. IETF, 2024. RFC 9901. Disponível em: <https://tools.ietf.org/html/rfc9901>.

WU, H.; WANG, F. A survey of noninteractive zero knowledge proof system and its applications. **TheScientificWorldJournal**, v. 2014, p. 560484, 05 2014.

XIE, C.; XIAO, R.; ZHANG, C.; WEI, L. Secuvault: A secure and private self-sovereign identity wallet for windows platform. *In: 2025 10th International Conference on Signal and Image Processing (ICSIP)*. [S.l.: s.n.], 2025. p. 448–452. ISSN 2642-6471.

YAO, W. et al. Establishing a baseline for evaluating blockchain-based self-sovereign identity systems: A systematic approach to assess capability, compatibility and interoperability. *In: Proceedings of the 2024 6th Blockchain and Internet of Things Conference*. New York, NY, USA: Association for Computing Machinery, 2024. (BIOTC '24), p. 108–119. ISBN 9798400717000. Disponível em: <https://doi.org/10.1145/3688225.3688239>.

ZEIN, D.; PINKWART, W. **Leveraging Zero-Knowledge Proofs for GDPR Compliance in Blockchain Projects**. [S.l.], 2025. Última versão consultada em 26 Nov 2025. Disponível em: <https://inatba.org/wp-content/uploads/2025/08/Leveraging-ZKP-for-GDPR-Compliance-in-Blockchain-Projects.pdf>.

ZIEGLER, L.; GRABATIN, M.; PÖHN, D.; HOMMEL, W. Designing a security incident response process for self-sovereign identities. **EURASIP Journal on Information Security**, 2025. Disponível em: <https://link.springer.com/article/10.1186/s13635-025-00195-6>.

ÁLVAREZ, I. A.; HÖLZMER, P.; SEDLMEIR, J. Privacy evaluation of the european digital identity wallet's architecture and reference framework. **Computers & Security**, v. 160, p. 104707, 2026.

Apêndices

**APÊNDICE A – ARTIGO NO FORMATO DA SOCIEDADE BRASILEIRA DE
COMPUTAÇÃO**

Identidade Auto-Soberana no Brasil: uma Análise da Convergência entre EUDI Wallet, gov.br e ICP-Brasil

Pedro Henrique de Sena Trombini Taglialenha¹
Jean Everson Martina¹, Lucas Machado da Palma¹

¹Departamento de Informática e Estatística – Universidade Federal de Santa Catarina (UFSC)
Florianópolis – SC – Brasil
phtaglialenha@gmail.com

Abstract. *Digital identity wallets promise to reduce data centralization while preserving institutional trust. This paper combines a systematic review of 40 studies with a comparative documentary analysis of the European Digital Identity Wallet, gov.br and ICP-Brasil. The literature indicates convergence toward wallet-centric architectures, OpenID protocols and selective disclosure, but also persistent challenges involving legacy integration, unlinkability, revocation, certification and usability. We argue that the Brazilian context favors a hybrid arrangement: the State and authorized institutions retain issuance and legal assurance, whereas citizens control credential custody and presentation. The analysis identifies convergence opportunities and a research agenda for interoperable, privacy-preserving digital identity in Brazil.*

Resumo. *Carteiras de identidade digital podem reduzir a centralização de dados sem eliminar a confiança institucional. Este artigo combina uma revisão da literatura de 40 estudos com uma análise documental comparativa da EUDI Wallet, do gov.br e da ICP-Brasil. A literatura converge para arquiteturas centradas na carteira, protocolos OpenID e divulgação seletiva, mas persistem desafios de integração legada, não vinculabilidade, revogação, certificação e usabilidade. Argumenta-se que o Brasil favorece um arranjo híbrido: Estado e instituições autorizadas preservam a emissão e o lastro jurídico, enquanto o cidadão controla a custódia e a apresentação das credenciais. A análise identifica oportunidades de convergência e uma agenda de pesquisa para identidade digital interoperável e orientada à privacidade.*

1. Introdução

A identidade digital tornou-se infraestrutura essencial para serviços públicos, relações de trabalho, finanças, saúde e educação. A expansão desses serviços, entretanto, ampliou a concentração de atributos pessoais em provedores de identidade e aplicações que intermedeiam repetidamente as transações. Em arquiteturas federadas, o provedor autentica o usuário e transmite declarações ao serviço; esse desenho simplifica a integração, mas permite que um intermediário observe acessos e favorece a replicação de dados por diferentes organizações. Revisões do ecossistema de Identidade Auto-Soberana (*Self-Sovereign Identity*, SSI) relacionam esse problema à dependência de autoridades centrais, à fragmentação de perfis e à perda de controle sobre a divulgação de atributos [Soltani et al. 2021, Schardong and Custódio 2021].

SSI desloca parte dessa mediação para uma carteira controlada pelo titular. Instituições continuam aptas a atestar fatos, mas o usuário recebe credenciais portáteis e decide quando apresentá-las. O modelo não implica, necessariamente, ausência de autoridades: sua contribuição prática pode estar na separação entre emissão, custódia e apresentação. Credenciais Verificáveis (VCs) padronizam declarações assinadas; Identificadores Descentralizados (DIDs) apoiam a resolução de chaves e serviços; mecanismos de divulgação seletiva permitem revelar somente os atributos necessários; e provas de conhecimento zero (ZKPs) permitem demonstrar propriedades sem expor seus valores subjacentes [Sporny et al. 2025, Sporny et al. 2023, Goldwasser et al. 1985].

A União Europeia converteu parte desses princípios em política pública por meio do Regulamento (UE) 2024/1183, conhecido como eIDAS 2.0, e da Arquitetura e Estrutura de Referência da Carteira Europeia de Identidade Digital (EUDI Wallet). O arranjo combina carteiras sob controle do usuário com listas de confiança, emissores qualificados, certificação e supervisão estatal [Parlamento Europeu e Conselho da União Europeia 2024, European Digital Identity 2025]. Trata-se, portanto, de uma arquitetura centrada na carteira, porém apoiada em governança institucional.

O Brasil parte de condições distintas. A Conta gov.br opera como provedor federado para serviços digitais; a ICP-Brasil estabelece uma cadeia hierárquica para assinaturas e certificados; e a Carteira de Identidade Nacional (CIN) unifica o CPF como identificador civil. Esses componentes alcançam escala e validade jurídica, mas não foram concebidos originalmente para apresentações portáteis com minimização de dados [Brasil 2001, Brasil 2023, Ministério da Gestão e da Inovação em Serviços Públicos 2024]. A questão relevante, assim, não é substituir toda a infraestrutura nacional por redes descentralizadas, mas compreender quais propriedades das carteiras podem ser incorporadas sem perder as garantias já existentes.

Este artigo investiga: *como credenciais portáteis, divulgação seletiva e apresentação controlada pelo titular podem convergir com o gov.br e a ICP-Brasil?* O objetivo é sintetizar arquiteturas, padrões e modelos de governança descritos na literatura, comparar os ecossistemas europeu e brasileiro e derivar diretrizes para um modelo híbrido. A contribuição é tripla: (i) síntese temática de 40 estudos sobre carteiras de identidade; (ii) matriz comparativa baseada em documentos técnicos, legais e normativos; e (iii) discussão dos compromissos necessários para adoção no Brasil.

2. Fundamentos e modelos de identidade digital

2.1. Do provedor federado à carteira

Em um sistema federado, um provedor de identidade autentica o usuário e emite uma asserção consumida por aplicações. O arranjo reduz o número de contas e centraliza políticas de garantia, mas o provedor participa de cada autenticação [Feng et al. 2025, Li et al. 2024]. Em uma arquitetura centrada na carteira, a interação é reorganizada em três papéis: o *emissor* atesta atributos; o *titular* recebe e guarda credenciais; e o *verificador* solicita e valida uma apresentação. Depois da emissão, uma apresentação pode ocorrer sem contato síncrono com o emissor, desde que o verificador disponha das chaves, dos metadados de confiança e de informação suficiente sobre o estado da credencial.

Essa mudança não elimina governança. O verificador precisa saber quais emissores são autorizados, quais esquemas são aceitos, como consultar revogação e quais políticas

limitam a coleta. O emissor, por sua vez, precisa vincular uma credencial ao titular correto e proteger suas chaves. A carteira deve proteger o material criptográfico, explicar solicitações e impedir liberação indevida. Por isso, estudos recentes descrevem carteiras digitais como sistemas sociotécnicos nos quais padrões criptográficos, regras institucionais e experiência do usuário são inseparáveis [Babel et al. 2025, Kudra et al. 2025].

2.2. Credenciais, identificadores e privacidade

O modelo de dados de VCs representa declarações de modo verificável e resistente a adulteração. Uma apresentação pode agrupar uma ou mais credenciais e incluir evidências de que quem apresenta está autorizado a usá-las [Sporny et al. 2025, Verifiable Credentials Working Group 2025]. DIDs fornecem identificadores resolvíveis em documentos que anunciam chaves, métodos de verificação e serviços, embora seu uso não obrigue blockchain e tampouco assegure, isoladamente, a legitimidade institucional de uma entidade [Sporny et al. 2023]. A confiança depende da combinação entre resolução técnica e regras externas que reconhecem o emissor.

Divulgação seletiva e ZKP respondem a necessidades distintas. Formatos baseados em ocultação e *hashes*, como SD-JWT, permitem revelar subconjuntos de atributos com custo compatível com tecnologias web [Fett et al. 2024]. Assinaturas com propriedades criptográficas avançadas e ZKPs podem demonstrar predicados e melhorar a não vinculabilidade entre apresentações, mas elevam complexidade, requisitos de certificação e custo computacional. A literatura recomenda avaliar essas técnicas pelo risco do caso de uso, e não tratar “mais criptografia” como objetivo autônomo [Flamini et al. 2024, European Telecommunications Standards Institute 2023, Ramos Fernández 2024].

Há, portanto, três modelos que não devem ser confundidos: identidade federada, na qual um provedor medeia o acesso; identidade centrada em carteira, na qual o titular transporta credenciais entre instituições; e descentralização completa, na qual se busca retirar também as âncoras institucionais [Li et al. 2024, Degen and Teubner 2024]. A EUDI Wallet aproxima-se do segundo modelo. Para o Brasil, essa distinção permite discutir autonomia de apresentação sem exigir abandono do Estado como fonte de registros civis.

3. Método de pesquisa

O estudo combina uma revisão estruturada da literatura e uma análise documental comparativa. A revisão foi organizada por perguntas, expressão de busca e etapas de triagem, mas não é classificada como sistemática, pois seu protocolo não reuniu todos os controles de qualidade e de reprodutibilidade exigidos para essa denominação. Três perguntas orientaram a leitura: **PQ1**: quais arquiteturas de carteiras de identidade digital são propostas? **PQ2**: quais tecnologias e padrões aparecem nas implementações? **PQ3**: quais modelos de governança e regulação são propostos?

A busca foi executada entre 18 de outubro e 20 de novembro de 2025 nas fontes ACM Digital Library, IEEE Xplore, ScienceDirect, SpringerLink e Google Scholar. A expressão comum foi:

```
("Digital Identity Wallet"OR "Identity Wallet"OR "EU
Digital Wallet"OR "EUDI Wallet") AND ("Architecture"OR
"Framework"OR "Model"OR "Standard"OR "Governance").
```

Foram incluídos artigos completos, disponíveis em PDF e publicados nos cinco anos anteriores à busca, com contribuição relacionada às perguntas. Resenhas, editoriais, trabalhos curtos e itens fora do tema foram excluídos. As duplicatas foram removidas antes da consolidação do conjunto inicial; apenas um ou dois registros se repetiam entre as fontes, e os 231 trabalhos reportados já correspondem ao conjunto deduplicado. A triagem posterior compreendeu leitura de título, resumo e texto integral. Como controle de qualidade, a leitura integral exigiu identificação de objetivo, proposta ou objeto analisado, evidência apresentada e limitações relevantes. A extração registrou arquitetura, padrões, mecanismo de confiança, propriedade de privacidade, forma de avaliação e lacuna.

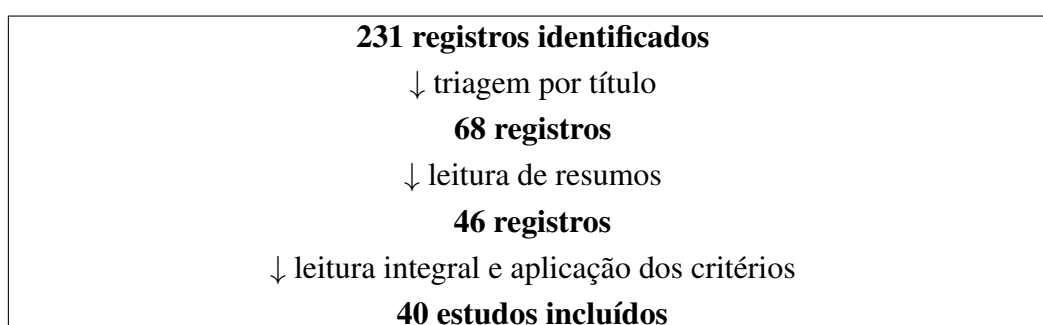


Figura 1. Fluxo consolidado de seleção dos estudos.

Os estudos foram inicialmente codificados em cinco eixos: integração legada; governança e regulação; privacidade e segurança; educação e operação offline; e adoção e avaliação. Para reduzir fragmentação, os resultados são apresentados em quatro grupos consolidados. A análise documental, conduzida separadamente, examinou legislação brasileira, especificações da ICP-Brasil e do gov.br, o regulamento eIDAS 2.0, a ARF da EUDI Wallet e padrões W3C, OpenID e ETSI. Os documentos foram comparados por cadeia de confiança, emissão, custódia, apresentação, operação offline, rastreabilidade, revogação, interoperabilidade e certificação.

4. Resultados da revisão da literatura

4.1. Arquiteturas e integração com sistemas legados (PQ1)

A resposta à PQ1 evidencia a consolidação da carteira como ponto de integração entre domínios. Em vez de um provedor transmitir atributos a cada acesso, o emissor entrega uma credencial e o titular a reapresenta conforme a necessidade. A arquitetura separa a camada de emissão confiável da camada transacional e reduz a visibilidade do emissor sobre os usos posteriores [Degen and Teubner 2024, Jeyakumar and Kubach 2025]. Essa propriedade, entretanto, depende de verificações locais ou distribuídas e de mecanismos de estado que não reintroduzam consultas identificáveis.

A substituição integral de sistemas de Gestão de Identidade e Acesso (IAM) não aparece como estratégia predominante. Os estudos propõem pontes SSI-OIDC, extensões de provedores existentes e agentes de tradução que convertem apresentações verificáveis em tokens ou atributos aceitos por aplicações legadas [Hoops and Matthes 2024, Corici et al. 2022]. A integração de credenciais com Keycloak, por exemplo, preserva interfaces OIDC consumidas pelas aplicações, enquanto adiciona uma etapa de verificação de carteira [Castellano et al. 2024]. O benefício é permitir migração incremental; o custo

é concentrar dados descriptografados e decisões de confiança no intermediário. Se a aplicação confia apenas no resultado da ponte, perde parte da verificabilidade fim a fim.

Outra linha substitui PKIs tradicionais por infraestruturas descentralizadas. A aplicação de DIDs e AnonCreds ao X-Road demonstra que credenciais podem automatizar a admissão de organizações e reduzir dependência de certificados X.509 [Bakhtina et al. 2023]. Contudo, o acoplamento a registros permissionados e agentes especializados transfere complexidade operacional a cada participante. Esse resultado reforça que descentralização da infraestrutura não é requisito para obter portabilidade e minimização: DIDs podem usar domínios web, e listas de confiança podem reconhecer emissores sem uma blockchain global.

Os estudos sobre adoção organizacional descrevem agentes de tradução como ponte entre credenciais externas e políticas internas baseadas em atributos [Kudra et al. 2025]. A lacuna recorrente é a falta de especificações abertas para mapear emissores, esquemas e níveis de garantia às regras locais. Para o Brasil, o problema é especialmente relevante porque serviços já integram o gov.br e cadeias ICP-Brasil. Uma arquitetura viável precisa conviver com esses contratos durante uma transição, mantendo auditável o ponto em que uma credencial portátil se converte em autorização.

4.2. Padrões e interoperabilidade (PQ2)

A resposta à PQ2 mostra deslocamento de soluções específicas de registros distribuídos para padrões abertos da web. OID4VCI organiza a emissão de credenciais e OID4VP organiza a solicitação e a apresentação remota [OpenID Foundation 2024a, OpenID Foundation 2024b]. Esses protocolos aproveitam conceitos conhecidos de OAuth e OpenID Connect, facilitando integração com aplicações móveis e serviços existentes. Para proximidade e cenários desconectados, a família mDoc, associada à ISO/IEC 18013-5, ocupa posição central na arquitetura europeia. A coexistência de fluxos remotos e de proximidade exige perfis interoperáveis, pois compatibilidade sintática não garante que carteiras e verificadores interpretem de modo idêntico políticas, formatos e estados.

O modelo de VC do W3C oferece vocabulário comum, mas admite diferentes formatos de prova e serialização. Essa flexibilidade favorece evolução, ao custo de perfis adicionais. DIDs também variam quanto a resolução, atualização e governança [Mazzocca et al. 2025]. A literatura, por isso, não sustenta a escolha de um único método DID universal. Métodos ancorados em domínios podem aproveitar governança e certificados web; registros distribuídos podem ser úteis quando não existe autoridade comum; identificadores pares podem reduzir correlação em relações bilaterais. A decisão deve considerar descoberta de emissores, portabilidade, privacidade e operação institucional.

A revogação permanece um ponto de tensão. Consultas online a cada apresentação fornecem estado recente, mas permitem ao emissor observar o uso. Listas agregadas e acumuladores reduzem essa correlação, porém demandam atualização, cache e tratamento de períodos offline [Sporny et al. 2025, European Telecommunications Standards Institute 2023]. O problema não é apenas criptográfico: regras precisam determinar validade, tolerância a desatualização e resposta a perda de dispositivo. Em credenciais de baixo risco, validade curta pode simplificar o ciclo; em documentos duradouros, preservação e renovação de chaves tornam-se centrais [Bochnia and Anke 2024].

4.3. Privacidade, segurança e usabilidade

Os estudos distinguem minimização de atributos de não vinculabilidade. SD-JWT permite ocultar campos e revelar apenas os necessários, mas apresentações repetidas podem conter elementos correlacionáveis. ZKPs e assinaturas que suportam provas derivadas oferecem garantias adicionais, sobretudo para predicados como “idade superior a um limite”, sem revelar data de nascimento. Em contrapartida, bibliotecas menos maduras, parâmetros criptográficos, auditoria e desempenho em dispositivos móveis limitam adoção. A comparação de mecanismos de divulgação seletiva confirma que nenhum formato domina todos os critérios [Flamini et al. 2024].

Segurança da carteira envolve proteção de chaves, vínculo ao dispositivo, recuperação e resistência a clonagem. Ambientes de execução confiável e elementos seguros elevam a proteção, mas não estão igualmente disponíveis em todos os aparelhos e podem depender de certificações específicas [European Digital Identity 2025, GlobalPlatform 2025]. Exigir hardware de alto nível para qualquer credencial ampliaria exclusão; aceitar somente armazenamento em software reduziria garantia em usos críticos. A literatura favorece níveis proporcionais ao risco e políticas que permitam mais de uma classe de dispositivo [Kudra et al. 2025].

Privacidade também depende do verificador. Consentimento não basta quando o usuário não consegue avaliar necessidade e finalidade de cada atributo. Propostas de credenciamento de provedores de serviço permitem à carteira verificar, antes da liberação, se o solicitante está autorizado a pedir determinada informação [More et al. 2024]. Esse mecanismo converte regras de proteção de dados em políticas executáveis, mas requer autoridades, certificados e vocabulários comuns. Sem governança do verificador, uma carteira pode oferecer controle formal enquanto normaliza solicitações excessivas.

Usabilidade aparece como fragilidade transversal. Pesquisa sobre federação com preservação de privacidade aponta desalinhamento entre propostas acadêmicas e padrões produtivos, além de atenção insuficiente à experiência do usuário [Bumiller et al. 2025]. Carteiras transferem decisões antes ocultas para telas de consentimento, recuperação e seleção de credenciais. Se o usuário não entende emissor, finalidade, atributos e consequência da recusa, a autonomia é nominal. A avaliação deve incluir compreensão, acessibilidade e recuperação, não apenas sucesso criptográfico.

4.4. Governança, adoção e resposta à PQ3

A PQ3 é respondida por uma conclusão consistente: ecossistemas de larga escala não dependem somente de prova matemática. É necessário reconhecer emissores, certificar componentes, credenciar verificadores, publicar políticas e resolver disputas. O eIDAS 2.0 organiza essa confiança por legislação, listas e supervisão dos Estados-membros. A carteira é controlada pelo usuário, mas a emissão de dados de identificação pessoal e atestados qualificados permanece vinculada a autoridades reconhecidas [Parlamento Europeu e Conselho da União Europeia 2024, Schwalm et al. 2022].

Modelos puramente baseados em blockchain não resolvem quem tem competência para afirmar nacionalidade, habilitação ou vínculo acadêmico. Um registro pode provar que uma chave publicou um dado, não que a entidade possuía autoridade jurídica. Em sentido inverso, governança excessivamente centralizada pode permitir rastreamento e criar pontos únicos de falha. A literatura converge para arranjos policêntricos: autoridades

estabelecem regras e âncoras; emissores operam em domínios próprios; carteiras aplicam políticas; verificadores validam localmente; e padrões comuns conectam as partes.

Tabela 1. Síntese temática dos resultados e implicações para o Brasil.

Categoria	Abordagens	Benefício e limitação dominante	Implicação nacional
Integração	Pontes le- OIDC, ex- tensões IAM, agen- tes ABAC	Adoção incremental; intermediário pode concentrar confiança e dados	Preservar contratos gov.br durante migração e tornar a tradução auditável
Padrões	VCs, DIDs, OID4VCI, OID4VP, mDoc	Portabilidade; diversidade de perfis e formatos	Adotar perfis internacionais ligados a emissores reconhecidos
Privacidade	SD-JWT, provas de- rivadas, ZKP	Minimização; compromisso entre eficiência e não vinculabilidade	Aplicar mecanismos proporcionais ao risco e evitar consulta identificável ao emissor
Estado e revoga- ção	Listas agregadas, acumuladores, validade curta	Menos correlação; atualização offline é difícil	Definir tolerância, cache e recuperação conforme a credencial
Governança	Listas de confiança, certificação e cre- denciamento	Escala institucional; risco de burocratização e fragmentação	Reutilizar âncoras ICP-Brasil e regular também verificadores
Usabilidade	Consentimento con- textual e recupera- ção	Autonomia; maior carga cognitiva	Avaliar compreensão, acessibilidade e inclusão digital

Em conjunto, as respostas mostram uma transição para carteiras portáteis e padrões web, sem evidência de que a governança estatal se torne dispensável. A lacuna mais relevante não é a ausência de primitivas criptográficas, mas a articulação entre elas, os sistemas legados, as regras de confiança e a experiência do cidadão.

5. Análise documental comparativa

5.1. EUDI Wallet e a institucionalização da carteira

O eIDAS 2.0 determina um quadro europeu de identidade digital no qual Estados-membros fornecem ao menos uma carteira ou reconhecem carteiras emitidas sob sua responsabilidade. A ARF traduz o regulamento em papéis, fluxos e requisitos. Dados de identificação pessoal e atestados de atributos são emitidos por fontes reconhecidas; a carteira guarda credenciais e prepara apresentações; partes confiantes validam assinaturas, estado e autoridade do emissor; organismos de avaliação e listas de confiança sustentam certificação e descoberta [Parlamento Europeu e Conselho da União Europeia 2024, European Digital Identity 2025, Sharif et al. 2022].

O desenho combina interoperabilidade transfronteiriça e controle do usuário. Protocolos OpenID atendem interações remotas, enquanto mecanismos de proximidade cobrem usos presenciais e offline [Enge et al. 2022]. Divulgação seletiva é requisito arquitetural, mas sua realização pode variar entre formatos. A carteira deve mostrar quem solicita dados e para qual finalidade, mantendo registros acessíveis ao titular. Ao mesmo tempo, componentes e dispositivos criptográficos ficam sujeitos a níveis de garantia e certificação

[Loutocký et al. 2025]. A soberania do usuário, portanto, opera dentro de uma moldura regulada.

Esse modelo evita dois extremos. O Estado não acompanha necessariamente cada apresentação, pois a validação pode ocorrer entre carteira e verificador. O usuário tampouco cria unilateralmente uma identidade civil: emissores autorizados mantêm o vínculo entre pessoa e atributo. A arquitetura também reconhece que verificadores representam risco, razão pela qual registro, autenticação e políticas de acesso integram a governança.

5.2. gov.br, ICP-Brasil, CIN e Vio

A ICP-Brasil, instituída pela Medida Provisória n.º 2.200-2/2001, organiza uma cadeia hierárquica de certificação cuja raiz é mantida pelo Estado [Brasil 2001]. Seu foco é garantir autenticidade, integridade e validade jurídica de documentos e assinaturas, com requisitos para algoritmos, autoridades e dispositivos [Instituto Nacional de Tecnologia da Informação 2022]. Essa infraestrutura oferece uma âncora nacional madura, mas seus certificados não equivalem automaticamente a credenciais portáteis com divulgação seletiva.

A Conta gov.br funciona como provedor de identidade para serviços integrados. O fluxo de autorização redireciona o usuário ao provedor, que autentica e devolve tokens segundo perfis de OpenID Connect. Níveis de conta expressam diferentes evidências de identidade, e a documentação de integração exige proteções como PKCE em clientes públicos [Ministério da Gestão e da Inovação em Serviços Públicos 2024, Ministério da Gestão e da Inovação em Serviços Públicos 2025, Governo Digital 2026, Governo Federal do Brasil 2026b]. O modelo simplifica acesso e centraliza garantia, mas o provedor participa das autenticações, diferentemente de uma apresentação verificável que pode ocorrer sem contato com o emissor.

A CIN estabelece o CPF como número único e suficiente para identificação em bases de serviços públicos, enquanto seu decreto regulamenta expedição e elementos do documento [Brasil 2023, Brasil 2022, Governo Federal do Brasil 2026a]. Essa unificação reduz inconsistências administrativas, mas o uso indiscriminado de um identificador estável pode facilitar correlação entre domínios. Uma carteira deveria permitir comprovar atributos sem transmitir o CPF quando ele não for necessário.

O Conecta GOV.BR viabiliza intercâmbio de dados entre órgãos, enquanto o Vio fornece código QR assinado para conferência de documentos [Universidade Federal de Uberlândia 2024, Serpro 2026b, Serpro 2026a]. Ambos podem participar de uma evolução, mas cumprem papéis diferentes de uma VC: interoperabilidade entre bases não concede custódia ao cidadão, e um pacote QR monolítico não oferece automaticamente divulgação seletiva. A convergência exige separar a fonte oficial do atributo, o formato portátil e a política de apresentação.

A comparação demonstra complementaridade. O Brasil já possui raízes de confiança, fontes de atributos e canais de integração; o que falta é uma camada padronizada de portabilidade e apresentação seletiva. A Europa oferece referência relevante para essa camada, mas seus mecanismos de certificação e divisão de competências não podem ser transplantados sem adaptação jurídica e institucional.

Tabela 2. Comparação entre o ecossistema EUDI e a infraestrutura brasileira.

Critério	EUDI Wallet	Brasil atual	Oportunidade de convergência
Raiz de confiança	Estados, listas e prestadores reconhecidos	ICP-Brasil e autoridades públicas	Publicar emissores de VCs vinculados às raízes nacionais
Emissão e validade	PID e atestados sob responsabilidade regulada	Registros oficiais, CIN e certificados	Transformar atributos oficiais em credenciais portáteis assinadas
Custódia	Carteira e dispositivo sob controle do titular	Conta e dados predominantemente em serviços	Permitir guarda local com níveis de proteção proporcionais
Apresentação	OID4VP, proximidade e divulgação seletiva	Redirecionamento gov.br ou QR/documento integral	Adotar apresentações verificáveis sem consulta síncrona ao emissor
Offline	Fluxos de proximidade e estado em cache	Vio e documentos assinados	Evoluir para formatos seletivos e regras explícitas de validade
Rastreabilidade	Separação entre emissão e uso reduz observação	Provedor pode participar de cada autenticação	Minimizar telemetria e desacoplar emissão de apresentação
Revogação	Mecanismos de estado e políticas comuns	Revogação de certificados e bases setoriais	Definir listas agregadas preservando privacidade
Certificação	Carteiras, componentes e prestadores avaliados	Regras ICP-Brasil focadas em certificados e equipamentos	Criar perfil nacional para carteira e hardware móvel
Interoperabilidade	Perfis europeus W3C, OpenID e ISO	OIDC governamental e integrações nacionais	Compatibilizar perfis sem abandonar contratos existentes

6. Discussão: diretrizes para um modelo híbrido brasileiro

6.1. Separar emissão institucional e apresentação pelo titular

O resultado central desta análise é que a adoção de propriedades de SSI no Brasil não requer eliminar o Estado da cadeia de confiança. Registros civis, habilitações, diplomas e licenças dependem de autoridades com competência legal. Estado e instituições autorizadas devem continuar responsáveis por verificar fatos, emitir credenciais e corrigir ou revogar registros. A mudança ocorre após a emissão: o cidadão recebe uma credencial interoperável, mantém sua custódia e prepara apresentações específicas para cada contexto.

Essa separação reduz a participação do emissor nas transações. Um serviço poderia validar uma prova de idade, vínculo ou habilitação com as chaves e políticas publicadas, sem redirecionar o cidadão ao provedor oficial em cada acesso. O emissor deixaria de observar diretamente a relação entre titular e verificador, salvo quando uma consulta de estado fosse indispensável. Para preservar essa propriedade, revogação deveria usar listas agregadas, validade limitada ou mecanismos que não revelem qual credencial está sendo apresentada.

ICP-Brasil pode atuar como âncora entre emissores e chaves de assinatura de VCs. Isso não significa reutilizar certificados existentes sem perfil ou atribuir presunção jurídica automática a todo formato. Seria necessário definir como uma autoridade certificadora, lista governamental ou domínio institucional publica os emissores autorizados, seus esquemas e níveis de garantia. A carteira e o verificador poderiam então construir a cadeia entre a credencial e uma raiz reconhecida.

O gov.br continuaria relevante no cadastramento e recuperação. Uma conta com garantia adequada pode apoiar a vinculação inicial do cidadão a uma carteira, enquanto o Conecta GOV.BR pode permitir que órgãos consultem fontes autênticas durante a emissão. Depois disso, a apresentação não precisaria repetir o fluxo federado. O resultado é complementar: federação para certas operações de alta confiança e credenciais portáteis para usos recorrentes e minimizados.

6.2. Divulgação proporcional e governança dos verificadores

Nem toda transação justifica ZKP. Para compartilhar um conjunto reduzido de atributos, SD-JWT ou mecanismo equivalente pode oferecer implantação simples e auditável. Quando a correlação entre apresentações ou a exposição do valor cria risco significativo, provas derivadas ou ZKPs tornam-se justificáveis. A política deve considerar sensibilidade, frequência, capacidade do dispositivo e maturidade da implementação. A regulamentação europeia reconhece que mecanismos avançados precisam de avaliação e integração ao regime de confiança [European Telecommunications Standards Institute 2023, Ramos Fernández 2024].

A minimização não pode depender exclusivamente da escolha do cidadão. Verificadores detêm poder econômico e podem condicionar serviços à coleta excessiva. Um modelo híbrido deve credenciar categorias de verificadores ou, no mínimo, publicar políticas assinadas que descrevam finalidade e atributos permitidos. Antes de apresentar dados, a carteira avaliaria identidade do solicitante, política e confiança. Esse desenho torna executáveis princípios de necessidade e finalidade, aproximando proteção jurídica de controles técnicos [More et al. 2024].

Agentes de tradução serão necessários durante a adoção. Eles podem receber uma apresentação, verificar sua cadeia e emitir um token interno compatível com aplicações existentes. Contudo, devem ser tratados como componentes de segurança: minimizar registros, preservar evidências verificáveis, separar clientes, limitar atributos e permitir auditoria. A tradução não deve converter a carteira em mero front-end para outro provedor central.

6.3. Compromissos e riscos

Soberania e governança estatal. Controle da apresentação não equivale a liberdade para autoemitir fatos oficiais. O modelo preserva autoridade na emissão, mas reduz controle transacional. Esse compromisso é coerente com a EUDI Wallet e mais compatível com a estrutura brasileira do que uma descentralização absoluta.

Privacidade, fraude e revogação. Quanto mais recente e individualizada a consulta de estado, maior a capacidade de bloquear fraude, mas também a possibilidade de rastreamento. Credenciais de riscos distintos devem adotar validade, atualização e prova de posse diferentes. Procedimentos de perda e recuperação precisam impedir que cópias antigas continuem utilizáveis sem transformar o emissor em observador permanente.

Interoperabilidade e certificação. Adoção de padrões internacionais reduz integrações particulares, mas perfis locais continuam necessários. O Brasil deve evitar extensões incompatíveis e participar dos processos de padronização. Ao mesmo tempo, requisitos ICP-Brasil para dispositivos não podem ser simplesmente aplicados a smartphones sem analisar ambientes seguros, atestação, cadeia de fornecimento e alternativas para cidadãos com aparelhos de menor capacidade.

Segurança e inclusão. Armazenar chaves em hardware seguro aumenta resistência a extração, porém exclui dispositivos sem suporte e dificulta portabilidade. Uma política em níveis pode permitir credenciais de baixo risco em software protegido e exigir hardware avaliado para operações críticas. Canais assistidos e credenciais alternativas são necessários para pessoas sem smartphone [Lukkien et al. 2023].

Offline e atualização. Apresentações offline aumentam disponibilidade e privaci-

dade, mas trabalham com informações de estado potencialmente desatualizadas. A política deve definir janela máxima, momento da última sincronização e comportamento diante de risco. Não existe solução única para uma carteira acadêmica, uma habilitação e uma credencial de acesso a instalação crítica [Enge et al. 2022, Bochnia and Anke 2024].

Consentimento e compreensão. Mais telas não significam mais autonomia. A carteira precisa apresentar solicitante, finalidade, atributos e alternativa de recusa em linguagem clara. Pedidos rotineiros devem ser compreensíveis sem habituar o usuário a aprovar automaticamente. Estudos de adoção devem medir compreensão e capacidade de recuperação, além de tempo de conclusão.

6.4. Requisitos derivados da análise

Os resultados permitem converter a discussão em requisitos verificáveis para uma futura política nacional, sem prescrever uma implementação específica. O primeiro é a *separação observável de papéis*: emissores não devem receber notificações individualizadas de cada apresentação, e verificadores não devem obter atributos fora da solicitação autorizada. Essa propriedade precisa ser demonstrável por análise de protocolo, registros de rede e auditoria de componentes intermediários. Quando uma consulta online for inevitável, ela deve revelar o mínimo necessário e, preferencialmente, operar sobre conjuntos ou estados agregados.

O segundo requisito é a *agilidade criptográfica e semântica*. Credenciais possuem vida útil superior à de bibliotecas e algoritmos. Perfis nacionais devem permitir evolução de formatos e conjuntos criptográficos sem invalidar documentos legítimos ou prender instituições a um fornecedor. A mesma cautela vale para esquemas: nomes, tipos e níveis de garantia precisam de versionamento, responsáveis e regras de compatibilidade. Um verificador não deve inferir que dois atributos com rótulos semelhantes possuem a mesma procedência ou significado.

O terceiro é a *confiança verificável e explicável*. A carteira deve construir uma cadeia entre a assinatura recebida e uma entidade reconhecida, e mostrar ao titular uma identificação compreensível do solicitante. O verificador, por sua vez, precisa justificar por que aceita determinado emissor e nível de garantia. Listas de confiança e certificados resolvem parte técnica, mas decisões de aceitação exigem políticas publicadas, tratamento de suspensão e canais de contestação.

O quarto requisito é a *continuidade inclusiva*. Perda, troca ou indisponibilidade do aparelho não pode produzir perda permanente de direitos. Recuperação deve equilibrar disponibilidade e resistência a tomada de conta, possivelmente combinando nova prova de identidade, revogação do dispositivo anterior e reemissão das credenciais. Respostas a comprometimento também precisam definir responsabilidades e procedimentos entre titular, carteira, emissor e verificador [Ziegler et al. 2025]. Serviços essenciais precisam manter canais alternativos para cidadãos sem carteira compatível. A solução só pode ser considerada soberana se o controle local não se converter em transferência integral do risco ao indivíduo.

Por fim, exige-se *interoperabilidade testada*, e não apenas declarada. Conformidade deve incluir testes entre carteiras, emissores e verificadores independentes, cobrindo emissão, apresentação, estado, erro, recuperação e proximidade. Perfis e conjuntos de teste públicos reduzem interpretações divergentes e permitem que órgãos adquiram componentes

substituíveis. Esses requisitos oferecem critérios concretos para avaliar pilotos e evitam que o debate se limite à oposição abstrata entre centralização e descentralização.

6.5. Agenda de pesquisa e de governança

A convergência depende de decisões ainda abertas. Primeiro, é necessário um perfil nacional de credenciais que delimite formatos, protocolos, esquemas, vínculo ao titular e mecanismos de estado. Segundo, deve-se definir como emissores e verificadores ingressam em listas de confiança e como políticas são auditadas. Terceiro, carteiras e componentes criptográficos móveis precisam de critérios de certificação proporcionais e compatíveis com a diversidade de hardware.

Também são necessárias avaliações empíricas que não se restrinjam ao desempenho criptográfico. Ensaios institucionais devem medir interoperabilidade entre fornecedores, compreensão, acessibilidade, recuperação, tratamento de incidentes e efeitos sobre coleta de dados. Por fim, o modelo deve ser submetido a análise jurídica sobre validade de apresentações derivadas, responsabilidades por falha e compatibilidade com regras de proteção de dados. A EUDI Wallet fornece um repertório, não uma especificação nacional pronta.

7. Limitações

A revisão está sujeita ao recorte de cinco anos, à disponibilidade em PDF, ao viés das fontes selecionadas e à realização da seleção por um único pesquisador. Embora perguntas, expressão de busca e etapas tenham estruturado o levantamento, não foram aplicados todos os procedimentos necessários a uma revisão sistemática, como avaliação independente e protocolo integralmente reproduzível. Os 40 estudos são heterogêneos quanto a método e maturidade, o que impede metanálise quantitativa. A análise documental compara objetivos e arquiteturas, mas não demonstra equivalência jurídica entre Brasil e União Europeia. Documentos técnicos evoluem rapidamente, e as conclusões devem ser reavaliadas conforme novos perfis e atos de implementação sejam publicados.

8. Conclusão

A literatura e os documentos analisados indicam que a contribuição mais promissora das carteiras de identidade para o Brasil é separar emissão institucional de apresentação controlada pelo titular. O país não precisa abandonar gov.br, ICP-Brasil, CIN ou suas fontes oficiais; pode utilizá-los para emitir e ancorar credenciais portáteis, enquanto padrões W3C, OpenID e mecanismos de divulgação seletiva reduzem exposição e consultas centrais durante o uso.

O modelo híbrido exige mais que escolher um formato: requer governança de emissores e verificadores, revogação com preservação de privacidade, certificação proporcional, integração legada auditável e experiência inclusiva. A EUDI Wallet oferece uma referência consistente para esses problemas, mas sua adaptação deve respeitar competências, garantias e desigualdades brasileiras. Pesquisas futuras devem validar o arranjo em ensaios interinstitucionais e avaliar simultaneamente interoperabilidade, segurança, privacidade, usabilidade e efeitos regulatórios.

Referências

- Babel, M., Willburger, L., Lautenschlager, J., Völter, F., Guggenberger, T., Körner, M.-F., Sedlmeir, J., Strüker, J., and Urbach, N. (2025). Self-sovereign identity and digital wallets. *Electronic Markets*, 35(1).
- Bakhtina, M., Leung, K. L., Matulevicius, R., Awad, A., and Svenda, P. (2023). A decentralised public key infrastructure for x-road. In *Proceedings of the 18th International Conference on Availability, Reliability and Security*.
- Bochnia, R. and Anke, J. (2024). Long-lived verifiable credentials: Ensuring durability beyond the issuer's lifetime. *Proceedings of the 19th International Conference on Availability, Reliability and Security*.
- Brasil (2001). Medida provisória n.º 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira.
- Brasil (2022). Decreto n.º 10.977, de 23 de fevereiro de 2022. Regulamenta a Carteira de Identidade Nacional.
- Brasil (2023). Lei n.º 14.534, de 11 de janeiro de 2023. Estabelece o CPF como número único e suficiente para identificação do cidadão.
- Bumiller, A., Kozyri, E., and Dagenborg, H. (2025). Privacy preserving identity federation: A literature study. *ACM Computing Surveys*.
- Castellano, D., De Prisco, R., and Faruolo, P. (2024). Login system for openid connect with verifiable credentials. In *2024 22nd International Symposium on Network Computing and Applications*, pages 105–112.
- Corici, A. A., Podgorelec, B., Zefferer, T., H"uhnlein, D., Cucurull, J., Graux, H., Dedovic, S., Romanov, B., Schmidt, C., and Krimmer, R. (2022). Enhancing european interoperability frameworks to leverage mobile cross-border services in europe. In *Proceedings of the 23rd Annual International Conference on Digital Government Research*, pages 41–53.
- Degen, K. and Teubner, T. (2024). Wallet wars or digital public infrastructure? orchestrating a digital identity data ecosystem from a government perspective. *Electronic Markets*.
- Enge, A., Satybaldy, A., and Nowostawski, M. (2022). An offline mobile access control system based on self-sovereign identity standards. *Computer Networks*, 219:109434.
- European Digital Identity (2025). Architecture and reference framework – eudi wallet. Technical report, European Commission. Version 2.4.0.
- European Telecommunications Standards Institute (2023). Analysis of selective disclosure and zero-knowledge proofs applied to electronic attestation of attributes. Technical Report ETSI TR 119 476 V1.1.1, ETSI.
- Feng, Z., Li, Z., Cui, H., and Whitty, M. T. (2025). Identity management systems: A comprehensive review. *Information*, 16:778.
- Fett, D., Campbell, B., and Yasuda, K. (2024). Selective disclosure for jwts (sd-jwt). Technical report, Internet Engineering Task Force.

- Flamini, A., Sciarretta, G., Scuro, M., Sharif, A., Tomasi, A., and Ranise, S. (2024). On cryptographic mechanisms for the selective disclosure of verifiable credentials. *Journal of Information Security and Applications*, 83:103789.
- GlobalPlatform (2025). Securing the european digital identity wallets. Technical report, GlobalPlatform.
- Goldwasser, S., Micali, S., and Rackoff, C. (1985). The knowledge complexity of interactive proof-systems. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, pages 291–304.
- Governo Digital (2026). Saiba mais sobre os níveis da conta gov.br.
- Governo Federal do Brasil (2026a). Carteira de identidade nacional – cin.
- Governo Federal do Brasil (2026b). Obter mais confiabilidade na conta de acesso.
- Hoops, F. and Matthes, F. (2024). A universal system for openid connect sign-ins with verifiable credentials and cross-device flow. In *2024 IEEE International Conference on Blockchain and Cryptocurrency*, pages 296–298.
- Instituto Nacional de Tecnologia da Informação (2022). Padrões e algoritmos criptográficos da icp-brasil (doc-icp-01.01). Technical report, ITI.
- Jeyakumar, I. H. J. and Kubach, M. (2025). A trust implementation model for cross-domain decentralized identity ecosystems: Architecture, use case, and implementation. *Procedia Computer Science*, 254:10–19.
- Kudra, A., Rieger, A., Sedlmeir, J., Roth, T., Fridgen, G., and Young, A. (2025). Digital identity wallets: A guide to the eu’s new identity model. *Information Systems Journal*.
- Li, H., Jing, Y., and Guan, Z. (2024). The review and comparison between centralized and decentralized digital identity systems. *Mobile Information Systems*, 2024.
- Loutocký, P., Stupka, V., and Kasl, F. (2025). Certification of the eu digital identity wallets and its challenges in the era of ai. In *2025 MIPRO 48th ICT and Electronics Convention*, pages 1636–1641.
- Lukkien, B., Bharosa, N., and De Reuver, M. (2023). Barriers for developing and launching digital identity wallets. In *Proceedings of the 24th Annual International Conference on Digital Government Research*, pages 289–299.
- Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., and Conti, M. (2025). A survey on decentralized identifiers and verifiable credentials. *IEEE Communications Surveys & Tutorials*.
- Ministério da Gestão e da Inovação em Serviços Públicos (2024). Conta gov.br.
- Ministério da Gestão e da Inovação em Serviços Públicos (2025). *Roteiro de Integração do Login Único*. Governo Federal do Brasil.
- More, S., Heher, J., Fasllija, E., and Mathie, M. (2024). Service provider accreditation: Enabling and enforcing privacy-by-design in credential-based authentication systems. In *Proceedings of the 19th International Conference on Availability, Reliability and Security*.
- OpenID Foundation (2024a). Openid for verifiable credential issuance. Technical report, OpenID Foundation.

- OpenID Foundation (2024b). Openid for verifiable presentations. Technical report, OpenID Foundation.
- Parlamento Europeu e Conselho da União Europeia (2024). Regulamento (ue) 2024/1183: Quadro para uma identidade digital europeia.
- Ramos Fernández, R. (2024). Evaluation of trust service and software product regimes for zero-knowledge proof development under eidas 2.0. *Computer Law & Security Review*, 53:105968.
- Schardong, F. and Custódio, R. (2021). Self-sovereign identity: A systematic map and review.
- Schwalm, S., Albrecht, D., and Alamillo, I. (2022). eidas 2.0: Challenges, perspectives and proposals to avoid contradictions between eidas 2.0 and ssi. In *Open Identity Summit 2022*. Gesellschaft für Informatik.
- Serpro (2026a). Gerar qr code vio.
- Serpro (2026b). Vio.
- Sharif, A., Ranzi, M., Carbone, R., Sciarretta, G., Marino, F. A., and Ranise, S. (2022). The eidas regulation: A survey of technological trends for european electronic identity schemes. *Applied Sciences*, 12(24):12679.
- Soltani, R., Nguyen, U., and An, A. (2021). A survey of self-sovereign identity ecosystem.
- Sporny, M., Longley, D., Chadwick, D., Herman, I., Cohen, G., Jones, M. B., and Thibodeau Jr., T. (2025). Verifiable credentials data model v2.0. W3c recommendation, World Wide Web Consortium.
- Sporny, M., Longley, D., Reed, D., Chadwick, D., Prorock, M., Jones, M., and Ribbens, Y. (2023). Decentralized identifiers (dids) v1.1. Technical report, World Wide Web Consortium.
- Universidade Federal de Uberlândia (2024). Entenda o programa conecta gov.br.
- Verifiable Credentials Working Group (2025). Verifiable credentials overview. Technical report, World Wide Web Consortium.
- Ziegler, L., Grabatin, M., Pöhn, D., and Hommel, W. (2025). Designing a security incident response process for self-sovereign identities. *EURASIP Journal on Information Security*.

APÊNDICE B – REPOSITÓRIO DO PROJETO

O código-fonte e os demais artefatos digitais produzidos durante o desenvolvimento deste trabalho estão disponíveis no repositório institucional de códigos da Universidade Federal de Santa Catarina:

<https://codigos.ufsc.br/pedro.taglialenha/tccpedrotaglialenha>