UNIVERSIDADE FEDERAL DE SANTA CATARINA

CENTRO DE CIÊNCIAS DA SAÚDE

PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA NA SAÚDE

Chiarelli Bezerra Albuquerque de Araújo Vale

Identidade Eletrônica e Autenticação de Médicos no Brasil

Florianópolis

2021

Chiarelli Bezerra Albuquerque de Araújo Vale

Identidade Eletrônica e Autenticação de Médicos no Brasil

Dissertação submetida ao Programa de Pós-Graduação em Informática na Saúde da Universidade Federal de Santa Catarina para a obtenção do título de mestre em Informática na Saúde.
Orientador: Prof. Ricardo Felipe Custódio, Dr.
Coorientador: Prof. Frederico Schardong, Me.

Florianópolis

2021

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Vale, Chiarelli Bezerra Albuquerque de Araújo
Identidade eletrônica e autenticação de médicos no Brasil / Chiarelli Bezerra Albuquerque de Araújo Vale ; orientador, Ricardo Felipe Custódio, coorientador, Frederico Schardong, 2021.
126 p.

Dissertação (mestrado profissional) - Universidade Federal de Santa Catarina, Centro de Ciências da Saúde, Programa de Pós-Graduação em Informática em Saúde, Florianópolis, 2021.

Inclui referências.

1. Informática em Saúde. 2. Identidade médica. 3. Autenticação em sistemas. 4. Nível de garantia. 5. Autenticação sem toque. I. Custódio, Ricardo Felipe. II. Schardong, Frederico. III. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Informática em Saúde. IV. Título.

Chiarelli Bezerra Albuquerque de Araújo Vale

Identidade Eletrônica e Autenticação de Médicos no Brasil

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

Prof. Lúcio José Botelho, Dr.
Departamento de Saúde Pública - UFSC

Prof. Martín Augusto Gagliotti Vigil, Dr.
Departamento de Computação - UFSC

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de mestre em Informática na Saúde.

Documento assinado digitalmente
Grace Teresinha Marcon Dal Sasso
Data: 05/11/2021 07:38:14-0300
CPF: 544.068.549-91
Verifique as assinaturas em https://v.ufsc.br

Coordenação do Programa de
Pós-Graduação

Documento assinado digitalmente
Ricardo Felipe Custodio
Data: 04/11/2021 10:27:25-0300
CPF: 485.981.609-97
Verifique as assinaturas em https://v.ufsc.br

Prof. Ricardo Felipe Custódio, Dr.
Orientador

Documento assinado digitalmente
Frederico Schardong
Data: 04/11/2021 11:57:25-0300
CPF: 004.893.690-14
Verifique as assinaturas em https://v.ufsc.br

Prof. Frederico Schardong, Me.
Coorientador

Florianópolis, 2021.

Este trabalho é dedicado aos meus filhos, Ayla e Dante,
e ao meu marido e eterno companheiro, Werley.

AGRADECIMENTOS

Agradeço a Deus por estar com saúde e me permitir a conclusão de mais uma etapa da minha vida.

Aos meus pais por me ensinarem a valorizar o conhecimento.

Ao meu marido, parceiro de 20 anos, por sempre me apoiar nas mais diversas empreitadas.

Agradeço especialmente aos meus filhos, Ayla e Dante, pelas inúmeras horas de ausência para dedicação ao mestrado, justamente em um momento tão especial da vida deles: a infância.

Aos meus colegas de trabalho e as minhas chefias que, sempre que possível, reduziram o meu volume de trabalho para que eu pudesse me dedicar a dissertação.

Aos professores do PPGINFOS pelo estímulo diário e pelo brilho nos olhos ao nos apresentar tantas mudanças espetaculares ocorrendo na área da saúde com a ajuda da informática.

Aos amigos que fiz durante o mestrado: Juliana e Luís Fabiano, espero que nossa amizade se aprofunde e permaneça!

Ao desenvolvedor do protótipo, Maurício, meu super obrigada!

Um agradecimento especial ao meu orientador, Dr Custódio, e ao meu co-orientador, Frederico, que sempre estiveram presentes e dispostos a me ensinar sobre esse novo mundo da tecnologia.

“Sou sempre eu mesma,
mas com certeza não serei a mesma para sempre.”
(LISPECTOR, ano desconhecido)

RESUMO

A identidade de um indivíduo pode ser conceituada como um conjunto de informações pessoais que caracterizam aquela pessoa e a individualiza perante a sociedade. Para o médico, muitas vezes basta um jaleco branco e um estetoscópio no pescoço para que essa identificação ocorra perante a sociedade. Mas este profissional também tem documentação própria para esta finalidade, embora ela quase nunca seja apresentada durante um atendimento médico. Em 2017, o Conselho Federal de Medicina (CFM) lançou a modalidade digital da identificação médica, o CRM Digital. Em seguida, foi lançado o E-CRM, versão para dispositivo móvel da Cédula de Identidade Médica, contendo as mesmas informações expressas no CRM Digital. Porém, até o momento, as identidades médicas eletrônicas não têm facilitado a autenticação nos diversos sistemas informatizados utilizados por esses profissionais. Mesmo com todo o avanço tecnológico, atualmente a autenticação e a autorização para o médico acessar os recursos essenciais no seu trabalho se dão de maneira burocrática e descentralizada. Em cada hospital, múltiplas senhas são necessárias para os vários sistemas. Assim, surge a pergunta desta pesquisa: **Como melhorar a autenticação e autorização do profissional médico nos diversos sistemas informatizados, incluindo a telemedicina, para que ocorra de forma mais segura, simples e célere?**. Uma identidade eletrônica eficiente é algo que você pode acessar facilmente em qualquer lugar, que é simples de usar e nacionalmente aceita, sendo confiável e econômica. Este trabalho apresenta uma proposta de identidade eletrônica eficiente e uma autenticação facilitada para o profissional da saúde. Para isso, a Gestão de Identidade e Acessos do médico foi centralizada em um único Provedor de Identidade (ligado ao CFM), capaz de fornecer credenciais e atributos médicos confiáveis a vários Provedores de Serviços. Em tempos de pandemia do COVID-19, apresentamos uma autenticação eletrônica sem toques em superfícies potencialmente contaminadas e com nível de garantia adequado à atividade. Para demonstrar a viabilidade da proposta, foi desenvolvido um protótipo com provedor de identidade único e autenticação eletrônica para o médico com as características mencionadas, onde o profissional pode perceber a segurança e a intuitividade do método proposto. Trabalhou-se para que, apenas ao se posicionar em frente ao computador, o médico tenha sua identidade reconhecida e sua autenticação validada com segurança naquele sistema de saúde informatizado, podendo cumprir o seu papel de cuidar da saúde dos pacientes sem entraves. Apresentamos também uma forma de prescrição médica eletrônica em nuvem computacional com assinatura qualificada sem qualquer burocracia.

Palavras-chave: Identidade médica eletrônica; autenticação; provedor de identidade; autenticação sem toque; nível de garantia.

ABSTRACT

The identity of an individual can be conceptualized as a set of personal information that characterizes that person and individualizes them in society. For the doctor, a white coat and a stethoscope around the neck are often enough for this identification to occur in society. But this professional also has its own documentation for this purpose, although it is almost never presented during a medical appointment. In 2017, the Federal Council of Medicine launched the digital modality of medical identification, the Digital CRM. Then, the E-CRM, mobile device version of the Medical Identity Card, was launched, containing the same information expressed in the Digital CRM. However, so far, electronic medical IDs has not facilitate authentication in the most diverse computer systems used by these professionals. Even with all the technological advances, currently the authorization and permission to doctor's access the essential resources in their jobs takes place in a bureaucratic and decentralized manner. In each hospital, multiple passwords are required for the various systems. Thus, the question of this research arises: **How to improve the authentication and authorization of the medical professional in the various computerized systems, including telemedicine, so that it occurs in a safer, simpler and faster way?**. An effective eID is something that you can easily access anywhere, that is simple to use, nationally accepted, reliable and cost-effective. This dissertation presents a proposal for an efficient electronic identity and an easy authentication for the health professional. For this, the physician's Identity and Access Management was centralized in a single Identity Provider (linked to CFM), capable of providing credentials and trusted medical attributes to multiple Service Providers. In times of the COVID-19 pandemic, we present electronic authentication without touches on potentially contaminated surfaces and with a level of assurance suitable for the activity. To demonstrate the feasibility of the proposal, a prototype was developed with a unique identity provider and electronic authentication for the physician with the aforementioned characteristics, where the professional can perceive the security and intuitiveness of the proposed method. Work was done so that, just by standing in front of the computer, the doctor has his identity recognized and his authentication securely validated in that computerized health system, being able to fulfill his role of taking care of the patients' health without obstacles. We also present a form of electronic medical prescription in a computer cloud with qualified signature without any bureaucracy.

Keywords: Medical electronic identity; authentication; identity provider; touchless authentication; level of assurance.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AAL	*Authenticator Assurance Level*
AC	*Attribute Certificate*
AC	Autoridades Certificadoras
Anvisa	Agência Nacional de Vigilância Sanitária
Art.	Artigo
C	*Information consumer*
CA	Certificado de Autoridade
CFF	Conselho Federal de Farmácia
CFM	Conselho Federal de Medicina
CIM	Cédula de Identidade Médica
CNH	Carteira Nacional de Habilitação
COVID-19	*Coronavirus Disease - 2019*
CPF	Cadastro de pessoa física
CREMESC	Conselho Regional de Medicina de Santa Catarina
CREMESP	Conselho Regional de Medicina de São Paulo
CRM	Conselho Regional de Medicina
CRM/SC	Conselho Regional de Medicina de Santa Catarina
DNA	*Deoxyribonucleic acid*
DNI	Documento Nacional de Identificação
DSRM	*Design Science Research Methodology*
DR.	Doutor
DRA.	Doutora
E-CRM	Cédula de Identidade Médica Eletrônica
eIDAS	*Electronic Identification, Authentication and Trust Services*

E-mail	*Eletronic mail*
EUA	Estados Unidos da América
GHz	GigaHertz
GIA	Gestão de Identidade e Acessos
GPS	Global Positioning System
HA	*Health Authority*
HCP	*HealthCare Professional*
IAM	*Identity and Access Management*
i.e.	Isto é
ITI	Instituto Nacional de Tecnologia e Informação
ICP-Brasil	Infraestrutura de Chaves Públicas - Brasil
ID	*Identity*
IdP	*Identity Provider*
IoT	*Internet of things*
LabSEC/UFSC	Laboratório de Segurança em Computação da Universidade Federal de Santa Catarina
LGPD	Lei Geral de Proteção de Dados Pessoais
ME	Ministério da Economia
MF	*Multifactor*
MFA	*Multifactor authentication*
MG	Minas Gerais
NDI	*National Identification Number*
NIST	*National Institute of Standards and Technology*
NRA	Notificação de Receita A
N/A	Não se aplica
n^o	Número

OAuth	*Open Authorization Protocol*
OTP	*One Time Password*
PDF	*Portable Document Format*
PEP	Prontuário Eletrônico do Paciente
PICO	*Population, Intervention, Comparison and Outcome*
PIN	*Personal Identification Number*
PKI	*Public Key Infrastructure*
PUK	*Personal Identification Number Unbloking Key*
QR Code	*Quick Response Code*
RFID	*Radio-Frequency Identification*
RG	Registro geral
RIC	Registro de Identidade Civil
RQE	Registro de Qualificação de Especialista
RSL	Revisão Sistemática da Literatura
RTS	Rede Temática da Saúde
SERPRO	Serviço Federal de Processamento de Dados
SF	*Single Factor*
SFA	*Single Factor Authentication*
SIAPE	Sistema Integrado de Administração de Recursos Humanos
SMS	*Short Message Service*
SP	*Service Provider*
SP	São Paulo
SSO	*Single Sign-On*
TMIS	*Telecare Medical Information System*
WBAN	*Wireless Body Area Network*
Wi-Fi	*Wireless Fidelity*

WOS	Web of Science
URI	*Uniform Resource Identifier*
2FA	*2-factor authentication*

SUMÁRIO

1 INTRODUÇÃO

A identidade de um indivíduo pode ser conceituada como sendo um conjunto de informações pessoais que caracterizam aquela pessoa e a individualiza perante a sociedade. Essas informações podem se constituir do nome da pessoa, altura, cor do cabelo, entre outros. Outros atributos também podem ser utilizados para caracterização da identidade de alguém, como, por exemplo, data/local de nascimento e nome dos pais (VERZELETTI *et al.*, 2014).

E por que precisamos nos identificar? Obrigatoriamente todo indivíduo deve possuir um ou mais documentos de identificação pessoal. No Brasil, o cidadão pode ter: carteira de identidade, carteira de motorista, carteira profissional, passaporte, entre outros. A Lei n^o 12.037 de 1 de Outubro de 2009 cita os documentos que podem ser utilizados como identificação civil (BRASIL, 2009).

Já a função subjacente de identificação ocorre desde que, socialmente, foram introduzidos papéis diferenciados, direitos, privilégios e recursos nas comunidades. Algumas dessas “habilidades únicas” vieram com a participação em uma categoria ou grupo, enquanto outras representaram características individuais. Às vezes, há um crachá de identificação, marca, vestimenta, objeto ou outra forma de distinguir visualmente o indivíduo com uma função específica; às vezes isso só pode ser conhecido por interação pessoal (VERZELETTI *et al.*, 2014).

Para o médico, frequentemente basta um jaleco branco e um estetoscópio no pescoço para que essa identificação ocorra perante a sociedade. Mas este profissional também tem documentação própria para essa finalidade, embora ela quase nunca seja apresentada durante um atendimento médico.

No dia-a-dia, inclusive para fins de fiscalização do exercício legal da Medicina, a Cédula de Identidade Médica (CIM) é o documento utilizado pelos profissionais.

Essa cédula de identidade foi construída conforme estabelece a Lei 6.206 de 1975 que deu valor ao documento de identidade às carteiras expedidas pelos órgãos fiscalizadores de exercício profissional no Brasil (BRASIL, 1975). Várias iniciativas foram tomadas pelo CFM para padronizar esse documento de identidade. A Resolução 1.983 de 2012 do CFM define o formato padronizado para esses documento de identidade (CFM, 2012).

Com isso, a cédula de identidade médica pode ser legalmente usada como prova de identidade em todo o país (CFM, 2010).

No mundo físico, a apresentação das cédulas de identidade (sejam elas profissionais ou não), de preferência com foto para conferência, é a forma mais tradicional de provar que *"você é você"*.

Desde que a internet passou a fazer parte rotineira do trabalho e da diversão das pessoas, o mundo digital e seus aspectos legais se fazem cada vez mais relevantes. Entre os diversos desafios para o funcionamento das sociedades digitais, um de grande importância é a necessidade de garantir, com adequado nível de confiança, que o indivíduo ou entidade que faz uso de um serviço virtual é, verdadeiramente quem diz ser. Para solucionar a questão da identidade no ambiente digital, diversos países têm adotado a estratégia de uma identificação eletrônica (ARAÚJO, 2020).

No Brasil, a conta gov.br é a proposta do Governo Federal para conduzir a identificação e autenticação do cidadão no mundo digital. É uma maneira segura de acesso digital do indivíduo aos serviços públicos digitais utilizando recursos tecnológicos atuais como smartphone, computador, laptop, tablet (GOV.BR, 2019).

A conta gov.br apresenta uma autenticação digital única do cidadão aos serviços públicos de acesso digital. Assim, com um único usuário e senha o indivíduo pode acessar todos os serviços públicos digitais que estejam disponíveis para a sua conta gov.br (GOV.BR, 2019).

Na área da saúde, a conta gov.br traz algumas funcionalidades voltadas para a utilização dos serviços de saúde. Porém a finalidade dessa plataforma pública não é a de contemplar serviços voltados para o exercício das atividades realizada por profissionais da saúde.

Muito embora a identidade eletrônica e a prestação de serviços médicos possam parecer desconectadas, a identidade eletrônica tem o potencial de mudar o atual cenário da assistência médica e a maneira como os dados de saúde são compartilhados (BOYSEN, 2019).

Com o avanço do mundo digital, até mesmo o exame físico que é parte essencial do ato médico, teve a possibilidade (embora não na sua totalidade) de ocorrer à distância, no ambiente virtual. Os sinais vitais captados por dispositivos vestíveis e a ausculta cardíaca através do estetoscópio digital são exemplos dessas tecnologias. A medicina caminha para mudanças muito significativas. Mas como saber se quem está do outro lado da tela é mesmo um médico?

O Conselho Federal de Medicina (CFM) lançou em 2017 a modalidade digital da identificação médica, o CRM Digital. Trata-se de um *smartcard* com sistema antifraude, possuindo um chip criptográfico para certificação digital (CFM, 2020b).

O CRM Digital possibilitou que o médico valide e libere documentos usando uma assinatura digital (certificada pela ICP-Brasil[1]) tendo o mesmo valor legal de um documento físico (DOCUSIGN, 2020).

O uso dos cartões inteligentes (*smartcards*) como documentos eletrônicos traz a necessidade de possuir uma leitora de cartões e a usabilidade deste modelo acaba sendo prejudicada.

Então, em seguida, foi lançado o E-CRM, versão para dispositivo móvel da Cédula de Identidade Médica (CIM) (CFM, 2019c). Essa versão, que contém as mesmas informações expressas no CRM Digital, necessita do uso de um aplicativo e possui componentes de segurança que protegem a identidade do médico (CFM, 2020a).

O referido aplicativo tem como uma de suas funções o gerenciamento da Carteira de Identidade Médica Digital (E-CRM), com a instalação e conferência de sua autenticidade por meio da leitura de um código de resposta rápida (QR Code[2]), além de possibilitar a emissão e o armazenamento de seu certificado digital ICP-Brasil e outras funcionalidades.

O CRM Digital e o E-CRM trouxeram novas funcionalidades para as cédulas de identidade médica e constituíram avanços consideráveis na identificação da profissão. Mas os avanços podem ser ainda mais significativos.

Com o surgimento das identidades eletrônicas, novas necessidades emergiram como, por exemplo, a de gerir essas identidades e os acessos que as mesmas podem permitir em tempo real.

A Gestão de identidade e Acessos (GIA), conhecida na língua inglesa como *IAM (Identity and Access Management)*, compreende um conjunto de processos com a finalidade de gerenciar todas as etapas dos acessos dos usuários dentro de uma organização (CABRAL; CAPRINO, 2015). Essas etapas compreendem, entre outras, a Autenticação e a Autorização, focos do nosso estudo.

A autenticação eletrônica é a identificação de usuários e legitimação de autoria por meios computacionais. Assegura que o usuário é quem afirma ser.

Já a autorização está relacionada com a concessão de permissões a uma determinada pessoa para acessar determinados recursos e dados (MELO, 2013).

Mesmo com todo o avanço tecnológico, atualmente a autenticação e a autorização para o médico acessar os recursos essenciais no seu trabalho acontecem

[1] Infraestrutura de Chaves Públicas - Brasil
[2] do Inglês *Quick Response (QR) Code*.

de maneira burocrática e descentralizada. Em cada hospital, múltiplas senhas são necessárias para os vários sistemas. Seja para acessar o prontuário do paciente, seja para ver os resultados dos exames realizados ali.

Durante a pandemia do COVID-19, com a necessidade crescente da demanda por atendimento de saúde ao mesmo tempo em que o distanciamento físico era e ainda é essencial, o CFM junto com o Instituto Nacional de Tecnologia da Informação (ITI) e o Conselho Federal de Farmácia (CFF) lançaram a plataforma "Prescrição Eletrônica" (CFM, 2020d).

O projeto passou a auxiliar o atendimento do doente e a interação remota entre médico, paciente e farmacêutico, trazendo a vantagem do paciente poder receber prescrições diretamente no celular, sem o trânsito de papéis (possíveis veiculadores de patógenos). A prescrição eletrônica pode ser conferida como documento válido diretamente no balcão da farmácia, via plataforma.

A plataforma conta com o direcionamento para um Validador de Documentos que valida prescrições médicas, relatórios, solicitações de exames e atestados em meio eletrônico quando em formato PDF. As verificações ocorrem quanto a autoria do documento, se assinada por um médico em exercício legal da profissão. Também checa se a dispensação do medicamento foi realizada por um farmacêutico (ITI, 2020).

A possibilidade de prescrição à distância foi um grande salto para a medicina, principalmente diante do avanço da telemedicina durante a pandemia.

Mesmo com o avanço, os passos para a finalização do atendimento médico e farmacêutico (assinatura digital e validação de documentos) também são bastante burocráticos, sendo um procedimento mais complexo do que esses profissionais estão habituados: de apenas carimbar e assinar usando uma caneta. Há como simplificar ainda mais esse processo digital com a tecnologia existente atualmente?

Assim, surge o nosso problema de pesquisa:

Como melhorar a autenticação e autorização do profissional médico nos diversos sistemas informatizados, incluindo a telemedicina, para que ocorra de forma mais segura, simples e célere?

Entendemos que uma identidade eletrônica eficiente é algo que você pode acessar facilmente em qualquer lugar, que é simples de usar e nacionalmente aceita, sendo confiável e econômica.

A proposta do nosso trabalho é que, aliada a uma identidade eletrônica efici-

ente, tenhamos uma autenticação digital facilitada para o médico, sem necessidade de possuir diversos usuários/logins, um para cada local de trabalho, e suas diversas senhas para os vários sistemas e acessos. Ele poderá usufruir de todos os serviços que lhe são permitidos, com uma única autenticação, de uma forma transparente, sem a necessidade de novamente passar todas as suas credenciais (CABRAL; CAPRINO, 2015).

Para que isso ocorra, a Gestão de Identidade e Acessos dos médicos deve ser do tipo centralizada onde há apenas um único Provedor de Identidade e vários Provedores de Serviços, os quais compartilham entre si as identidades dos usuários. É um modelo considerado mais simples do que o atual (tradicional) onde cada provedor de serviço é responsável pela identidade dos seus usuários (BATISTA NETO, 2014).

Trabalharemos com níveis de garantia dos métodos de autenticação propostos. Para reforçar a segurança deste procedimento, a autenticação em dois fatores (ou verificação em duas etapas) poderá ser utilizada. Autenticação em dois fatores ocorre quando, por exemplo, além de inserir a senha para acessar a conta, é preciso inserir uma nova informação para confirmar que é você, de fato, que está realizando a autenticação naquele sistema (como inserir um dado biométrico, por exemplo). Isso adiciona uma camada extra de segurança e garantia.

Os profissionais da saúde devem se concentrar apenas na parte técnica, na atividade profissional que já é complexa o suficiente. Não deve fazer parte da preocupação desses profissionais os melindres da tecnologia, usando a memória para gravar usuários e senhas. Trabalharemos para que, de forma intuitiva, o ato médico esteja validado e ele possa cumprir o seu papel de cuidar da saúde dos pacientes.

A proposta é que todo o processo ocorra em nuvem computacional e que a autenticação, autorização e a comunicação entre os provedores de identidade e de serviços sejam invisíveis para o médico. Em tempos de pandemia do COVID-19, também iremos considerar as possibilidades de uma autenticação sem toques em superfícies potencialmente contaminadas.

1.1 OBJETIVOS

Nas seções abaixo estão descritos o objetivo geral e os objetivos específicos.

1.1.1 Objetivo Geral

Propor um sistema de identidade eletrônica para profissionais de saúde no Brasil que facilite a autenticação e autorização com níveis de garantia em sistemas informáticos.

1.1.2 Objetivos Específicos

a) Estruturar os princípios necessários para identificação, autenticação e autorização do profissional de saúde;

b) Propor um provedor de identidade eletrônica para profissionais de saúde;

c) Fornecer uma identificação eletrônica para médicos, com identificadores, credenciais e atributos;

d) Propor formas de autenticação do médico nos sistemas sem o toque, evitando possíveis contaminações;

e) Propor autenticação digital com nível de garantia adequado para a situação;

f) Desenvolver um protótipo do sistema de autenticação e autorização eletrônicas para o médico com as características acima citadas.

1.2 JUSTIFICATIVA

A concepção da cédula de identidade médica em forma de *smartcard* (CRM digital) foi condizente com o nível tecnológico da época. Atualmente, o uso do CRM digital já é visto como obsoleto e com problemas de usabilidade. A necessidade do leitor de cartão e problemas de interoperabilidade são algumas das questões que levaram ao seu pouco uso.

O E-CRM traz a vantagem de não necessitar do cartão físico, mas ainda não trouxe maiores benefícios. O dispositivo eletrônico não traz facilitadores para a autenticação do médico nos diversos sistemas informatizados de uso diário, ainda sendo necessários múltiplas senhas para tal.

Também deve ser salientado que, os sistemas que contam com a segurança baseada apenas em senhas, independentemente de serem longas, alteradas várias vezes ou compostas de caracteres aleatórios, não são seguros o suficiente para quem lida com a saúde da população (BOYSEN, 2019). Ainda mais quando são múltiplas senhas para autenticação e autorização nos diversos sistemas usados pelos médicos.

Com os avanços da gestão de identidades no mundo, não há motivos para que o profissional da saúde não se beneficie com uma identidade eletrônica em nuvem. A ideia mostra-se promissora para atingir a praticidade e segurança ideais na autenticação e autorização que esses profissionais necessitam. Gerará confiança, redução de custos e usará menos dados. Trará informações de credenciais e atributos fiéis em tempo real, dificultando fraudes.

1.3 MOTIVAÇÃO

Durante o período de pandemia pelo COVID-19, o Governo Federal publicou a Medida Provisória n^o 983 em 16 de Junho de 2020 (BRASIL, 2020c) que posteriormente embasou a Lei n^o 14.063, de 23 de setembro de 2020 (BRASIL, 2020b). Nela, o Governo regulamenta as assinaturas eletrônicas em comunicações com entes públicos e em questões de saúde.

A referida legislação trouxe a classificação das assinaturas eletrônicas (simples [3], avançada [4] e qualificada [5]) e citou situações em que o tipo de assinatura pode ser revisto: os atos realizados durante o período da pandemia da COVID-19. Tal observação se deu com o objetivo explícito pelo dispositivo legal de minimizar contatos presenciais e também para a realização de atos que ficariam impossibilitados por outro modo (BRASIL, 2020b).

Esse objetivo de reduzir contato presencial impulsionou a telemedicina nos tempos atuais e necessita ser levado a sério para os procedimentos de saúde. O aprimoramento digital também deve ser pensado para ir além da assinatura eletrônica. Não temos no Brasil marco regulatório para autenticação, autorização e gestão de identidades e acessos.

Este estudo vem com o intuito de vislumbrar a autenticação e a autorização de acesso dos profissionais da saúde para um nível de mínimo ou nenhum contato físico em um provedor de identidade único para todos os sistemas informatizados.

Um ecossistema digital inicialmente pensado para as necessidades da saúde em tempos de pandemia se torna vital para o amadurecimento do acesso informatizado à saúde.

1.4 PRINCIPAIS CONTRIBUIÇÕES

Nosso trabalho trouxe propostas com contribuições significativas relacionadas a autenticação dos profissionais da saúde nos diversos sistemas informatizados. São elas:

- Fatores de autenticação considerando o nível de garantia adequado para as atividades ligadas a área da saúde;

[3] É aquela que permite identificar o seu signatário e que anexa ou associa dados do signatário em formato eletrônico.

[4] É aquela que utiliza certificados não emitidos pela ICP-Brasil. Está associada ao signatário de maneira unívoca, possui um grau mais elevado de segurança que a assinatura eletrônica simples.

[5] É considerada a modalidade mais segura. O assinante utiliza um certificado digital validado pela ICP-Brasil.

- Métodos de autenticação sem a necessidade do toque dos profissionais (livre de contaminação de pessoas e superfícies) para todos os níveis de garantia nas diversas circunstâncias de atendimento ao paciente;
- Proposta de um provedor único de identidade ligado ao conselho da categoria profissional, com identificadores, credenciais e atributos atualizados em tempo real para os provedores de serviço e;
- Desenvolvimento de um protótipo como prova de conceito da viabilidade das propostas acima citadas.

1.5 ESTRUTURA DA DISSERTAÇÃO

No Capítulo 2 temos o tipo de estudo proposto, os passos seguidos e todo o levantamento bibliográfico feito sobre autenticação dos profissionais da saúde em sistemas.

No Capítulo 3 apresentamos todo o referencial teórico sobre identidade eletrônica, autenticação, modelos de gestão de identidade e nível de garantia.

Já o Capítulo 4 tratou especificamente sobre a identidade eletrônica do médico, quais foram os avanços, qual o modelo usado atualmente, suas falhas e seus acertos.

A proposta trazida nesta dissertação encontra-se no Capítulo 5 onde apresentamos os facilitadores pensados para uma autenticação médica segura, simples e imediata.

Realizamos uma avaliação comparativa da nossa proposta com o modelo atual de identidade e autenticação médica em sistemas informatizados. Tal análise foi apresentada no Capítulo 6, juntamente com um protótipo desenvolvido como prova de conceito.

O Capítulo 7 trouxe uma reflexão sobre o desfecho e resultados obtidos, indicando possíveis trabalhos posteriores.

2 METODOLOGIA

2.1 INTRODUÇÃO

Para que uma pesquisa seja considerada relevante do ponto de vista social e acadêmico, ela deve ser passível de verificação e de reprodução, além de mostrar que foi produzida dentro dos preceitos metodológicos e éticos. Assim, o método de pesquisa adequado para aquele caso se torna necessário para o seu desenvolvimento e validação posterior (LACERDA *et al.*, 2013).

2.2 TIPO DE ESTUDO

Geralmente, as pesquisas dentro da área tecnológica são classificadas como pesquisas aplicadas e objetivam resolver problemas específicos de um determinado assunto. O foco dessa categoria é desenvolver um novo conhecimento tecnológico ou aprofundar um já existente, algumas vezes através da produção de um artefato. Um artefato pode ser algo material, mas também pode ser uma ideia, uma proposta ou um *framework* (FREITAS JUNIOR *et al.*, 2017).

Mesmo as produções tecnológicas ocorrendo em número elevado, grande parte dos estudos não trazem uma metodologia adequada para a necessidade específica daquele caso. Muitas vezes, os pesquisadores precisam adaptar outras metodologias usadas em áreas de conhecimento diversas (saúde, ciências humanas, sociologia). Porém, as pesquisas tecnológicas tem uma visão particular da resolução de problemas e as demais ciências não compartilham dessa natureza de conhecimento (FREITAS JUNIOR *et al.*, 2017).

Assim, o *Design Science Research Methodology (DSRM)* surgiu com princípios e fundamentos que suprem a pesquisa tecnológica, configurando como a metodologia adequada para o tipo de estudo (SIMON, 1969; SIMON, 1996).

A concepção da *DSRM* se deu a partir da necessidade de diferenciar os ambientes naturais dos artificiais. A ciência natural é tudo aquilo que explica o funcionamento dos fenômenos naturais e a conexão deles com o universo. Já a ciência artificial apresenta artefatos que solucionam problemas (SIMON, 1969; SIMON, 1996).

Design Science Research engloba todo o processo de projetar e desenvolver artefatos para resolver problemas, avaliar o protejo (ou o que já está em funcionamento), e apresentar os resultados da produção e avaliação (ÇAĞDAŞ; STUBKJÆR, 2011).

Os artefatos podem ser (MARCH; SMITH, 1995):

- Constructos: são os termos usados em determinada área de pesquisa que estão presentes e auxiliam na descrição das atividades.
- Modelos: conjunto de proposta que evidenciam as reações entre os diversos conceitos de um domínio.
- Métodos: É a descrição de cada passo para que se desenvolva a atividade.
- Instanciações: é a finalização com o artefato presente no ambiente para o qual foi desenvolvido, mostrando a concretização e a eficácia dos modelos e métodos.

A *DSRM* é desenvolvida em seis etapas, que são sugeridas na ordem especificada na Figura 1, mas que podem ser executadas de acordo com a necessidade de determinado projeto (PEFFERS *et al.*, 2007; FREITAS JUNIOR *et al.*, 2017):

Etapa 1 Identificação do problema e sua motivação: quando ocorre a definição específica do problema de pesquisa e a justificativa para aquela investigação. Deve-se empregar o conceito do problema na produção do artefato que pode solucionar o referido problema. Para que essa etapa aconteça, é necessário conhecer *"o estado da arte do problema"* e a importância da solução que se busca;

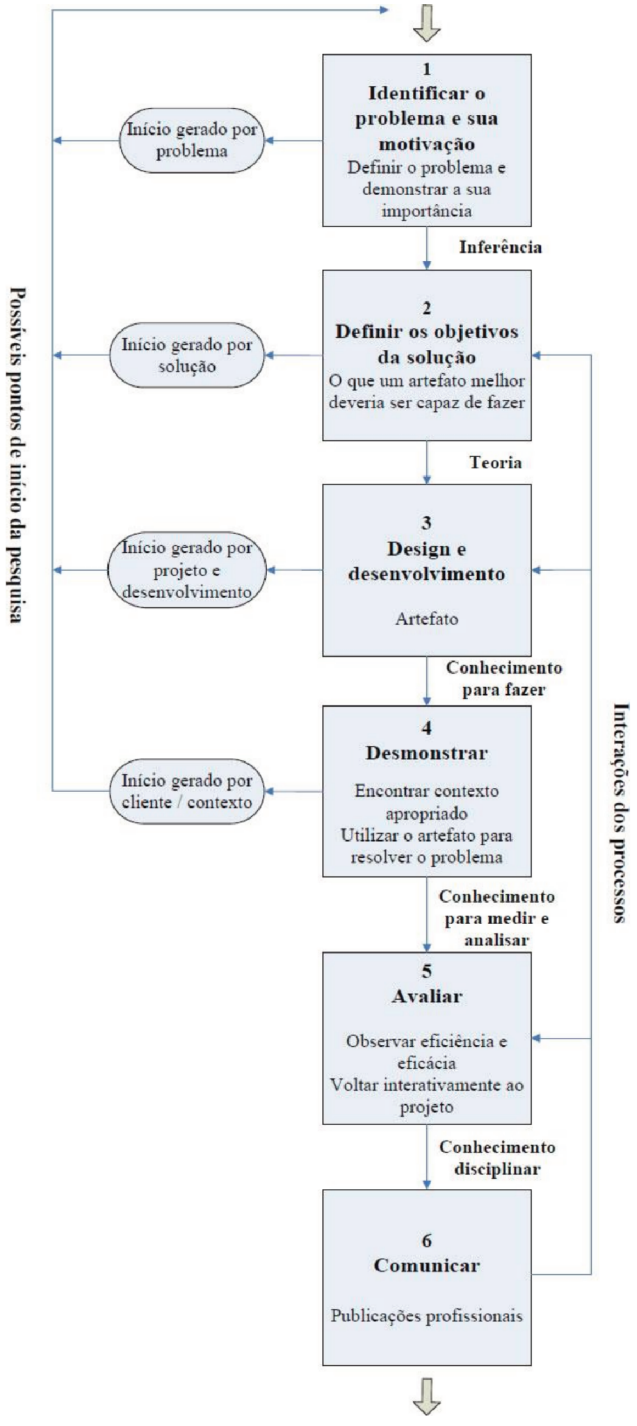
Etapa 2 Definição dos objetivos para a solução: ao conhecer o problema e entender o que é possível ser resolvido, defini-se os objetivos da solução a ser encontrada. Novamente é necessário conhecer o estado da arte do problema e as propostas que já foram apresentadas para solucioná-lo;

Etapa 3 Projetar e desenvolver: é a criação do artefato com a definição da sua função e a sua arquitetura. Em seguida, desenvolve-se o artefato em si. Para isso, deve-se conhecer a teoria que necessita ser executada para obter a resolução do problema;

Etapa 4 Demonstração: apresentação do uso do artefato para resolver o problema (no todo ou em partes). Pode ocorrer através de um estudo de caso, de um experimento ou simulação ou outra maneira apropriada. Deve-se saber como usar o artefato para solucionar o problema;

Etapa 5 Avaliação: deve-se observar se o artefato atende a resolução dos problemas, em que instâncias e em que intensidade. Os objetivos iniciais do projeto devem ser resgatados e comparados com os resultados encontrados com a aplicação do artefato. Para tal, pode ser necessário voltar as etapas 3 e 4 para que se aprimore o artefato;

Figura 1 – Etapas da *DSRM*.



Fonte: (JAPPUR *et al.*, 2014).

Etapa 6 Comunicação: etapa em que se divulga o problema, a importância de se encontrar uma solução e apresenta-se o artefato criado.

O desenvolvimento deste estudo procurou seguir as seis etapas acima descritas norteadas pela DSRM. Assim, temos:

Etapa 1 Buscou-se identificar as dificuldades sobre a maneira que se dá atualmente a identificação dos profissionais da saúde no Brasil e sua autenticação e autorização nos diversos sistemas informatizados utilizados na rotina de trabalho. Elencaram-se as consequências devido as falhas na gestão atual da identidade dos profissionais e da burocratização arcaica de autenticação e autorização nos sistemas: custos, dificuldades com senhas múltiplas para vários sistemas, repetição das credenciais, identidades falsas/falsos profissionais.

Adicionalmente, buscaram-se as soluções no mundo para problemas com a identificação, autenticação e autorização dos profissionais da saúde. Identificaram-se as necessidades geradas pela atual pandemia do COVID-19 no mundo relacionada ao acesso dos profissionais aos sistemas de saúde, a contaminação das digitais no processo de autenticação e a dificuldade/insegurança na produção de documentos para finalizar o ato médico à distância.

Etapa 2 O objetivo geral foi desenvolver um gerenciamento de identidade eletrônica para médicos no Brasil a fim de facilitar a autenticação e autorização nos sistemas informatizados. Além disso, os objetivos específicos foram: estruturar os princípios necessários para identificação, autenticação e autorização do profissional de saúde; propor formas de autenticação do médico nos sistemas sem o toque, evitando possíveis contaminações; propor um provedor de identidade eletrônica para profissionais da saúde; fornecer uma identificação médica eletrônica com identificadores, credenciais e atributos; e desenvolver um protótipo do sistema de autenticação e autorização eletrônicas para o médico com as características propostas.

Etapa 3 Elencou-se o conteúdo necessário para a criação de uma identidade médica eletrônica, analisaram-se os requisitos necessários, definiram-se aspectos da gestão da identidade e acessos, elaborou-se um *framework* de um ecossistema com apenas um provedor de identidade que atenda a vários provedores de serviços. Criação da arquitetura do protótipo e do protótipo em si. A funcionalidade de uma identidade médica eletrônica é de contato mínimo do profissional com as etapas informatizadas de autenticação e autorização, sendo intuitiva, que possa ser acessada de qualquer lugar por qualquer dispositivo com acesso à nuvem e de baixo custo.

Etapa 4 e 5 Com o protótipo pronto, foi demonstrado o seu uso através de uma simulação a fim de resolver os problemas descritos. Foi feita uma avaliação descritiva, comparando com o método de autenticação médica usado hoje em 2 cenários. Analisou-se se o artefato produzido atende à solução do problema, compararam-se os objetivos propostos para a solução com os resultados advindos da utilização dele.

Etapa 6 Pretende-se seguir com a divulgação do *framework* como fruto da produção tecnológica através de publicação em periódico acadêmico.

2.3 LEVANTAMENTO BIBLIOGRÁFICO

O estudo fez um levantamento do estado da arte dos métodos de autenticação eletrônica usados por profissionais da saúde em sistemas informatizados no mundo.

2.3.1 Revisão Sistemática da Literatura

Um das formas utilizadas para obter um entendimento abrangente sobre uma determinada área de pesquisa é a Revisão Sistemática da Literatura (RSL). Trata-se de um tipo de investigação focada em uma questão bem definida, que visa identificar, selecionar, avaliar e sintetizar as evidências relevantes disponíveis (GALVÃO; PEREIRA, 2014). As revisões sistemáticas mostram onde evidências específicas estão faltando ou são relatadas de forma insuficiente nos estudos existentes.

2.3.2 Questão de pesquisa

Para o encontro da questão principal da pesquisa, consideramos a estratégia de escolha de termos usando o acrônimo PICO [1] (população, intervenção, comparação/controle e resultado/desfecho) (PETTICREW; ROBERTS, 2008) a fim de detectar o máximo de trabalhos de interesse.

Assim, a população escolhida foi de profissionais da saúde, a intervenção foi a autenticação em sistemas, a comparação foi entre diferentes métodos de autenticação em sistemas, e desfecho foi de métodos que não exigissem toque em superfícies potencialmente contaminadas.

Portanto, o processo de revisão teve o intuito de buscar estudos que já tenham as respostas às questões da presente pesquisa:

Quais métodos de autenticação em sistemas foram usados/propostos para profissionais da saúde que não necessitavam de toque?

Porém ao testar *strings* de busca, notou-se que a combinação *((“Authentication") AND (“Health Professional” OR “Doctor”) AND ("System") AND ((“contactless” OR “without touch” OR “touchless”)* resultava em NENHUM estudo encontrado nas bases de dados selecionadas.

Então, para que o material de trabalho fosse amplo, deixamos o desfecho/resultado fora do *string* que será esclarecido a seguir.

[1] Do inglês: *Population, Intervention, Comparison and Outcome*

2.3.3 Método

As fontes de pesquisa utilizadas foram PubMed, Web of Science (WOS), IEEEXplore e Scopus, entre os meses de Outubro e Novembro de 2020. Não houve restrição relacionada a data da publicação dos materiais encontrados. O *string* de busca utilizado foi: *((“Authentication") AND (“Health Professional” OR “Doctor”) AND ("System"))*.

No total, 395 artigos foram encontrados com a busca predita, sendo 30 encontrados no IEEEXplore, 277 no Scopus, 22 no PubMed e 66 no Web of Science.

Como indica a Revisão Sistemática da Literatura, foi realizada a conferência dos documentos no que tange aos critérios de inclusão e exclusão.

Como **critérios de inclusão** foram considerados para o estudo: artigos originais; artigos disponíveis na íntegra; artigos no idioma inglês; artigos que abordam autenticação dos profissionais da saúde em sistemas informatizados.

Como **critérios de exclusão** foram desconsiderados: capítulos de livros, manuais ou cartilhas; artigos que não traziam o *Abstract* para análise preliminar; que estavam em idioma diverso da língua inglesa; que não puderam ser acessados na íntegra; que não descrevessem o método de autenticação do profissional de saúde proposto especificando a forma de interação humano-computador; e que não declarassem explicitamente no título ou resumo que versavam sobre autenticação dos profissionais da saúde em sistemas.

Dos artigos analisados na íntegra, muitos abordaram a autenticação com seu protocolo de segurança, com fórmulas computacionais, sem especificar quais fatores/métodos de autenticação foram usados. Por isso, um dos critérios de exclusão foi o de não descrever o método de autenticação do profissional de saúde proposto especificando a forma de interação humano-computador.

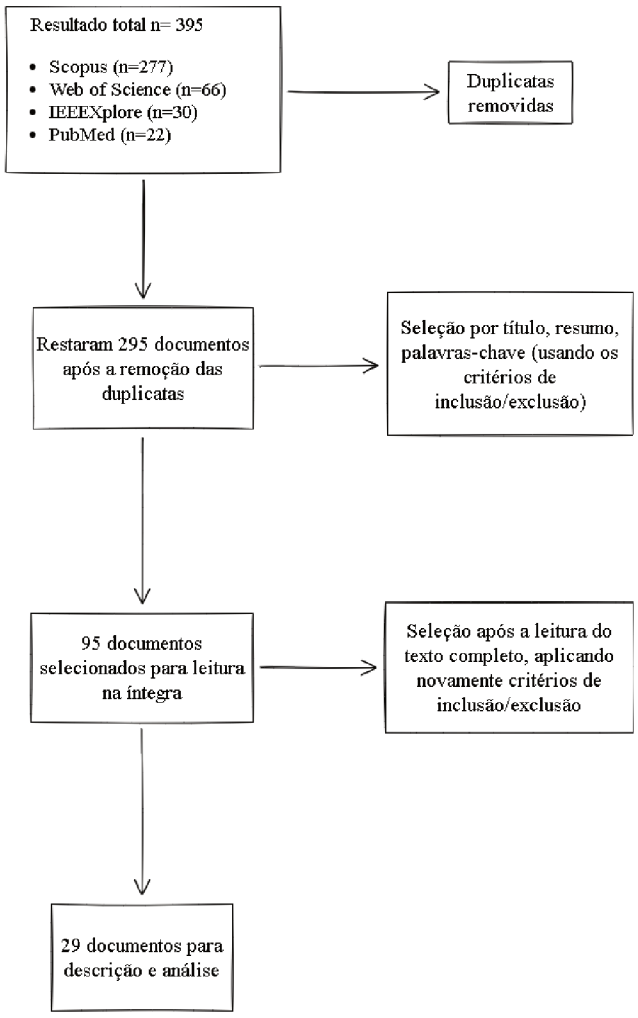
O processo de seleção foi conduzido pela autora desta dissertação, com o auxílio do seu orientador que avaliou os estudos selecionados por amostragem. A seleção seguiu os seguintes passos (Figura 2):

a) Pesquisa de strings: encontrados 395 artigos;

b) Remoção de duplicatas: restaram 297 artigos;

c) Seleção por título, resumo, palavras-chave (usando os critérios de inclusão/exclusão): 95 artigos selecionados para leitura na íntegra;

Figura 2 – Fluxograma da seleção utilizado na RSL.



Fonte: Própria autora.

d) Seleção após a leitura de texto completo dos 95 artigos, aplicando novamente critérios de inclusão/exclusão: 29 artigos para descrição e análise.

Após a seleção dos estudos por leitura do texto na íntegra, realizamos a extração e análise dos dados dos 29 artigos, segundo proposta de (KITCHENHAM, 2012). Não foi realizado a avaliação de qualidade dos artigos analisados porque, para tal, é necessário que haja um conhecimento aprofundado na área computacional, o que foge da formação desta mestranda.

2.3.4 Resultados

O objetivo dessa dissertação está em propor um método de autenticação fácil e seguro para profissionais da saúde. Assim, tentamos identificar no material selecionado quais métodos foram utilizados no processo de autenticação, quais recursos foram necessários e se necessitavam de toque para o processo de autenticação.

Um grande número de métodos pode ser usado para autenticar um usuário: senhas, técnicas biométricas, tokens ou cartões inteligentes, certificados digitais. Geralmente, os métodos de autenticação usados devem corresponder ao valor dos dados acessados. Também deve corresponder ao tipo e nível de acesso que o usuário está fornecendo. Além disso, é necessário um método de autenticação do usuário que imponha uma carga de trabalho adicional mínima ao usuário (AL-NAYADI; ABAWAJY, 2007).

Tentamos subdividir os métodos:

2.3.4.1 Login, senha e certificados digitais

O login do usuário e senha como método de autenticação dos profissionais da saúde foi o mais encontrado, abordando questões de segurança e de recuperação facilitada de senhas. Muitos estudos foram focados em como aumentar a segurança desse método de autenticação, trazendo senhas fortes com mudanças frequentes.

(LEE, Tian-Fu *et al.*, 2013) apresentam um protocolo de acordo de chave autenticada baseado em senha para o sistema de informação do prontuário eletrônico integrado do paciente. O protocolo proposto não requer o uso do servidor ou das chaves públicas dos usuários. Cada usuário se lembra da sua senha fraca compartilhada com um servidor confiável e, então, pode obter uma chave de sessão comum. Assim, todos os usuários podem se comunicar com segurança usando esta chave de sessão. Não há especificação sobre onde esta senha é inserida (Teclado? *Smartphone?*).

A telerradiologia pode ser usada com eficácia como uma solução para fornecer melhores cuidados de saúde a mais pacientes com menos especialistas. (BHARATH *et al.*, 2015) propõem um protótipo funcional de sistema de digitalização de ultrassom portátil integrado com conectividade sem fio, autenticação biométrica e sistema de posicionamento global (GPS). Escanearam um modelo de impressão digital de um usuário autorizado usando o scanner de impressão digital, recuperaram e armazenaram no servidor junto com uma identificação única. Assim, uma pessoa semiqualificada adquire as imagens de ultrassom de órgãos por meio de um dispositivo de ultrassom portátil e as transmite para o servidor centralizado. Os ultrassonografistas autorizados podem fazer login no servidor (digitando suas credenciais de ID e senha) e escrever o relatório de diagnóstico correspondente à imagem de ultrassom específica. O diagnóstico baseado na Web oferece flexibilidade para acessar o site por meio de um dispositivo conectado à Internet, inclusive por telefone móvel. A proposta é uma solução para a falta de ultrassonografistas, trazendo diagnósticos baseados na web, onde muitos médicos autorizados podem se cadastrar e fornecer seu serviço para pacientes remotos.

(KAMBOURAKIS *et al.*, 2005) publicaram um artigo ilustrando como a infraestrutura de chave pública (PKI [2]), certificados de atributo (ACs [3]) e protocolos habilitados para chave pública podem fornecer estrutura para apoiar eficazmente os serviços de autenticação, autorização e confidencialidade. O uso de dispositivos móveis permite ao usuário (profissional da saúde) autenticar-se por senha mesmo estando em um local diferente do paciente. Esse local pode ser as instalações do hospital ou um centro de tratamento / cuidado, um centro de instalações esportivas, uma ambulância, um centro de tratamento médico em uma ilha ou área urbana.

(AL-NAYADI; ABAWAJY, 2007), propuseram uma estrutura de autenticação baseada em certificados de identidade, atributo e consentimento que, juntos, identificam de maneira única o profissional da saúde, bem como as funções e acessos associados e as restrições impostas ao uso de dados de saúde. Essa arquitetura foi desenvolvida para autenticar os profissionais de e-saúde que acessam dados clínicos compartilhados entre um conjunto de instituições de saúde afiliadas com base em redes ponto a ponto. A identificação e a autenticação ocorre também usando seu ID e senha.

(SUDHA; GANESAN, 2013) proporcionaram ao usuário o acesso ao prontuário multimídia de qualquer lugar e a qualquer hora com segurança, incluindo autenticação e controle de acesso. Um celular habilitado para Wi-Fi é usado para receber ou transmitir os dados médicos protegidos, bem como a recuperação de imagens. Nome de usuário e senha individuais são fornecidos para o médico acessar o banco de dados usando o aplicativo móvel.

No trabalho de (LOUK *et al.*, 2014), a autenticação deve ser feita com o processo de login. Cada usuário se registra inicialmente ou é registrado por outra pessoa (hospital/ administração), usando uma senha atribuída ou autodeclarada. Em cada uso subsequente, o usuário deve saber e usar a senha declarada. Faz uso de certificados digitais emitidos e verificados por um Certificado de Autoridade (CA) como parte de uma infraestrutura de chave pública.

(POTDAR *et al.*, 2014), sugeriram o uso de um aplicativo em *smartphone* (ou outro dispositivo móvel) em sistema operacional Android, com autenticação do profissional da saúde necessitando apenas de login e senha. O aplicativo garante o atendimento rápido ao usuário por ser portátil, oferecendo o serviço em qualquer lugar, em qualquer tempo. Quando há necessidade de prescrição de medicação, o médico assina a receita usando seu certificado eletrônico e a prescrição é enviada para o *smartphone* do paciente. Quando o paciente vai à farmácia, o farmacêutico,

[2] *Public Key Infrastructure*
[3] *Attribute Certificate*

verificando a assinatura eletrônica, pode verificar a autenticidade da receita.

(SALEEM *et al.*, 2015), também apresentaram um sistema semelhante com funcionalidades *e-healthcare* em que os membros do sistema (incluindo os profissionais de saúde) se comunicam por meio de *smartphones*, realizando autenticação inteligente com base no gerenciamento de chaves distributivas aleatórias e distribuição de certificado eletrônico.

(AMIN *et al.*, 2015), propuseram uma arquitetura de sistema médico para TMIS[4] onde o paciente pode se comunicar com segurança com o médico. O esquema de autenticação de paciente usa cartão inteligente, e o médico, login e senha. O sistema usa carimbo de data e hora na fase de autenticação mútua.

Em Bangladesh, o governo fornece aos cidadãos um número de identificação única de 17 dígitos chamado de NDI . Com a autenticação do paciente utilizando o NDI (*National Identification Number*) por meio de um cartão inteligente, (ALAM; ALI, 2016) apresentaram o desenvolvimento e implantação de um sistema de gerenciamento de informações médicas. O sistema tem uma estrutura integrada para todos os serviços médicos e entidades (pacientes, médicos, enfermeiras, farmacêutico, organizações de saúde, laboratórios de patologia e farmácias) e garante a privacidade do paciente por acesso baseado em função. O paciente deve levar seu cartão inteligente para todo atendimento médico ou de saúde em geral para que haja o registro e consulta a dados necessários, inclusive prescrições. Já o médico e demais profissionais de saúde devem se autenticar no sistema com login e senha.

2.3.4.2 *Tokens*

Na Alemanha, (BLOBEL; PHAROW, 1999) apresentaram um projeto piloto regional na área de oncologia onde uma rede de saúde segura foi desenvolvida e implementada com um de *tokens*. Na Europa, e cada vez mais também em outras regiões do mundo, *tokens* de segurança como cartões inteligentes pessoais e/ou profissionais (cartões com chip com um controlador de criptografia) estavam sendo introduzidos. Eles mantém chaves privadas e fornecem serviços de segurança como autenticação, assinatura digital e criptografia.

Parte de um projeto do governo na República da Coréia para a separação do dispensário dos consultórios médicos, trouxe um sistema de comunicação de pedido de prescrição entre o hospital e a farmácia, com base na Internet, infraestrutura de chave pública, e cooperação paralela simultaneamente com cartões inteligentes de profissionais médicos e de pacientes em status sincronizado. (SONG *et al.*, 2002)

[4] Sistema de Informação Médica de Teleatendimento. Do inglês: *Telecare Medical Information System*

idealizaram um esquema de autenticação utilizando chaves públicas e privadas armazenadas no cartão inteligente do profissional médico no hospital (ou clínica) e na farmácia.

(ZÚQUETE *et al.*, 2008) descreveram uma arquitetura de autenticação forte para profissionais usando uma abordagem de dois fatores: posse de um *token* (*smartcard*) de segurança e conhecimento de um segredo. Cada profissional recebe um cartão inteligente para armazenar e usar suas credenciais pessoais para acessar o Portal RTS (Rede Temática da Saúde). RTS é uma uma plataforma regional para compartilhar dados clínicos entre um conjunto de instituições de saúde afiliadas. Os certificados são de curta duração e há acordos de certificação cruzada entre RTS e instituições de *e-health* para autenticação dos profissionais que acessam o RTS. Esses certificados carregam também a função do profissional em sua instituição de origem para autorização baseada em função.

(LEE, T.-F.; LIU, 2013) apresentaram um esquema de autenticação baseado em cartão inteligente para sistemas de telemedicina permitindo que pacientes, médicos, enfermeiras, profissionais de saúde e os sistemas de informações de saúde estabeleçam uma plataforma de comunicação segura por meio de redes públicas. Necessita que o usuário insira seu cartão inteligente em um leitor de cartão e também sua senha. Uma chave de sessão segura é negociada pelo servidor e pelos usuários para posterior comunicação segura de dados.

(AGHILI *et al.*, 2019) elaboraram um novo protocolo (denominado LACO) de autenticação e transferência de propriedade (titularidade do usuário / médico) para sistemas de e-saúde no contexto da *IoT* (*Internet of Things)*. O registro dos profissionais da saúde e a transferência de titularidade ocorre através do servidor médico. O uso dos cartões inteligentes (através da sua inserção nos terminais) operacionaliza o acesso aos dados armazenados, gerando um carimbo de data/hora em cada acesso.

(GARSON; ADAMS, 2008) sugerem uma autenticação de dois fatores para uma segurança aprimorada. Um fator escolhido foi o sistema de nome do usuário e senha sem restrições à senha. O segundo fator pode ser uma impressão digital biométrica ou etiqueta RFID. Os autores trabalharam com as falhas de usabilidade do fator de autenticação com tecnologia RFID (*Radio-Frequency Identification*), tentando contorná-las. A primeira questão de usabilidade é que, ao contrário do método de impressão digital, um médico pode esquecer seu cartão. Se eles pegarem emprestado o passe de outra pessoa ou conseguirem um temporário, isso não funcionará com o leitor, pois será uma senha diferente. Os autores trabalharam com a possibilidade de conseguir crachás temporários disponíveis para o dia que podem ser associados à sua conta. Outra maneira de contornar isso é usar um método de backup comum

para solicitar ao usuário uma série de perguntas pré-respondidas. Se o usuário responder corretamente e fornecer suas informações de login usuais junto com ele, então o usuário pode fazer login para o dia. Foi enfatizado que o rastreamento adequado desses eventos é importante para ser capaz de perceber e documentar comportamentos maliciosos. Assim, o leitor RFID oferece uma alternativa à autenticação médica conveniente. Os médicos carregam crachás de funcionários que podem ser equipados com um código de barras. Para assinar, um médico passa seu cartão ou, se for um leitor de proximidade, simplesmente tem seu crachá em algum lugar do seu corpo. Todos podem receber um crachá e sempre será aceito. No entanto, esta opção ainda está disponível se o médico desejar delegar suas tarefas a outro funcionário por um período de tempo.

2.3.4.3 Dispositivo móvel

(FOTOUHI *et al.*, 2020) propuseram um esquema leve de autenticação de dois fatores para redes corporais sem fio (*WBAN*) [5]. Para se comunicar com os sensores, cada médico ou enfermeiro, chamado de usuário, precisa de um dispositivo móvel e um par de ID e senha escolhidos arbitrariamente para se registrar em um sistema confiável chamado gateway. De acordo com o esquema de autenticação de dois fatores proposto, o usuário seleciona uma identidade e a senha correspondente como o primeiro fator e um dispositivo móvel para armazenar algumas informações sobre o registro como o segundo fator.

(KHATOON; UMADEVI, 2018) propuseram um aplicativo *e-health* que usa a autenticação Aadhaar para inscrever / conectar usuários. Os cartões de identificação Aadhaar[6] usados na Índia, contêm um código *QR* exclusivo impresso neles, contendo os dados do usuário. A autenticação é realizada via *SMS* de verificação única (OTP) [7] e não requer nenhum ID de usuário ou senha. Um usuário precisa apenas escanear o código *QR* presente no cartão Aadhaar, após o qual o aplicativo irá processar e extrair os dados do código *QR* escaneado e solicitar ao servidor central para enviar um *SMS OTP* para o número do celular vinculado o cartão Aadhaar digitalizado. Assim que o *SMS OTP* for recebido no telefone do usuário, o aplicativo iniciará automaticamente o processo de registro / login. Se o usuário for médico, no primeiro acesso, ele deve preencher no aplicativo um formulário referente à sua prática médica. Este formulário preenchido será enviado a um administrador que fará as verificações necessárias antes de aprovar o médico.

[5] *Wireless Body Area Network (WBAN)* é uma coleção de vários sensores médicos inteligentes dentro ou ao redor dos corpos dos pacientes, que são usados para monitoramento e suporte de saúde em tempo real.

[6] Número de identidade distinto de doze dígitos emitido em forma de cartão para todos os residentes da Índia com base em seus dados biométricos e demográficos

[7] Do inglês: *One Time Password*

2.3.4.4 Biometria

(SHIN *et al.*, 2008) propuseram um modelo que aplicou a tecnologia de reconhecimento de impressão digital ao sistema de informação médica, para garantir um sistema de prontuário eletrônico confiável. Aplicou-se o reconhecimento de impressão digital de médicos, enfermeiras e toda a equipe médica para fins de autenticação, juntamente com o ID e senha. O estudo fez um comparativo entre a comodidade e segurança das assinaturas eletrônicas e o uso da impressão digital, trazendo o método biométrico como mais adequado.

(CHEN *et al.*, 2012) propuseram um esquema de autenticação e autorização *online* para sistemas *e-health* baseado no uso de cartões eletrônicos de seguro saúde e impressão digital, tanto do paciente como do médico. Utilizou uma máquina de identificação de impressão digital à prova de violação para identificação no hospital ou clínica e um mecanismo de validação de carimbo de data / hora no esquema.

Para sua melhor acurácia, (AMIRTHALINGAM; THANGAVEL, 2019) mostraram a combinação do uso de assinatura *online* digitalizada e autenticação de impressão digital do profissional da saúde usando *deep learning*. Ampliando o espectro da impressão digital, o estudo de (RANA; KANG, 2019) citou a autenticação eletrônica usando polegar ou palma da mão.

(HAN *et al.*, 2006) apresentou uma arquitetura para autenticação e autorização dentro de um sistema de serviço de e-saúde. O mecanismo de autenticação de dois fatores foi integrado à arquitetura de autorização e autenticação do sistema de serviço de saúde eletrônica. No mecanismo de autenticação de dois fatores, cada função do sistema de serviço de *e-health* subjacente deve usar uma autenticação biométrica (*fingerprints*) junto com uma autenticação digital PIN. Se e somente se a autenticação de dois fatores for bem-sucedida, o mecanismo de política de autorização será ativado e o direito de autorização será concedido ao indivíduo subjacente.

(SAIF *et al.*, 2018) apresentou um *WBAN* seguro assistido por nuvem para aplicativo de saúde. Para autenticação do médico e do paciente, inicialmente a senha é usada e, em seguida, o biossinal é utilizado (impressão digital). As medidas de segurança adotadas neste trabalho, fazem com que seja difícil para um intruso interceptar qualquer nó regido pela autenticação dos biossinais dos pacientes e dos médicos.

Embora também exija o toque do profissional da saúde, um estudo de 2020 chamou a atenção. (FANG *et al.*, 2020) propuseram um esquema de autenticação de características fisiológicas e comportamentais através de gestos manuais, velocidade do toque e pressão. O mecanismo de autenticação solicita um gesto específico,

exigindo que o usuário feche quatro dedos e execute um determinado operação de deslizar na tela. Os fatores biométricos incluem a distância dos pontos de toque do dedo na tela, enquanto recursos comportamentais, como velocidade e pressão também contêm informações específicas do usuário.

A biometria da face, por exemplo, atende ao requisito de uma autenticação sem toque, sem contaminação de mãos. (GUILLÉN-GÁMEZ *et al.*, 2017) trouxeram a autenticação de médicos e pacientes usando a biometria da face em tempo real. A autenticação facial tem vantagens de ser um método melhor aceito pelos usuários e não requer equipamento especializado para a aquisição de dados. O estudo desenvolveu um novo banco de dados de fotos coletado para treinar o algoritmo de autenticação facial para variações de rotações, distâncias, expressões e acessórios. Considerou uso de óculos, chapéus e bonés, lenços. Além disso, a captura das imagens ocorreu com quatro tipos de expressões faciais. Além da expressão neutra, os participantes foram convidados a mostrar outros três tipos de expressões: (a) sorrindo, (b) gritando e (c) fechando os olhos e abrindo a boca. Consideraram que usuários amigáveis podem sorrir ao contatar serviços de saúde. O segundo tipo de expressão pode acontecer se o paciente estiver com muita dor. O último tipo de expressão foi realizada para considerar demandas emergenciais durante o noite, quando podem estar cansados e com sono.

Método mais caro, mas também mais preciso e sem toque, temos a biometria da íris que foi usada com sucesso como fator de autenticação para médicos e pacientes no estudo de (MAHTO; YADAV, 2020). Por causa das características distintivas da íris, a autenticação oferece um método altamente confiável de reconhecimento do usuário.

A biometria da voz foi usada no estudo de (KRAWCZYK; JAIN, Anil K, 2005) que analisou o desempenho de combinar o uso de assinatura *online* e biometria de voz a fim de executar autenticação de usuário.

Percebe-se que sistemas biométricos multimodais podem superar muitas das limitações de um sistema biométrico unimodal. (SATOH *et al.*, 2010) apresentou um sistema biométrico multimodal utilizando a biometria da face e a impressão digital.

2.3.5 Possíveis vieses de seleção

As revisões sistemáticas da literatura não estão isentas de vieses e, quando existem, podem comprometer a qualidade da evidência gerada. Eles podem ter sido gerados de várias formas ao longo do processo de localização e seleção dos estudos.

Tentamos identificar essas possibilidades a fim de analisar criticamente o processo de condução da revisão.

Inicialmente, desde a leitura do *Abstract* de cada estudo encontrado, pode ter ocorrido um viés de linguagem. A mestranda tem formação em medicina e alguns termos técnicos específicos da área da informática podem não ter sido compreendidos, comprometendo a seleção.

Alguns trabalhos podem ter abordado o assunto de interesse no seu texto na íntegra, mas foram excluídos por não trazerem referências no seu *Abstract*.

Outro viés que pode ter ocorrido em alguns casos, foi a inferência de como se dá a interação homem-máquina durante a autenticação do profissional nos sistemas. A descrição dos recursos usados não explicitava o passo-a-passo, mas possibilitava a dedução de como ocorria. Assim, os trabalhos não foram excluídos e compuseram a análise.

2.3.6 Lacunas de pesquisa

O foco da maioria dos trabalhos encontrados concentrou-se na segurança do método de autenticação proposto, não estando voltado para a especificidade do processo da autenticação dos profissionais da saúde.

O esquema de autenticação apresentado nos estudos abordou superficialmente a interação humano-máquina e apenas dois trabalhos apresentaram propostas de autenticação completamente sem toque: (GUILLÉN-GÁMEZ *et al.*, 2017) que trabalhou com a autenticação facial com suas variações; e (MAHTO; YADAV, 2020), apresentando um esquema de autenticação através da íris.

Não encontramos trabalhos com um olhar atual, voltados para a peculiaridade da autenticação em sistemas dos profissionais da saúde, apresentando métodos ideais para uma autenticação rápida e segura, sem contaminação das mãos nos diversos ambientes laborais.

O toque em superfícies potencialmente contaminadas não foi considerado como uma preocupação de higiene nos estudos encontrados. A pandemia do COVID-19 trouxe esse cuidado que deve permanecer, já que é uma preocupação permanente da categoria profissional. Essa lacuna procurou ser preenchida com a nossa proposta.

2.4 CONCLUSÃO

Sobre o tipo de estudo a ser realizado, o *DSRM* mostrou-se adequado para a pesquisa tecnológica. Assim, seguimos as 6 etapas preconizadas.

Sobre o levantamento bibliográfico, seguimos os passos da RSL. Nos estudos

encontrados inicialmente, o olhar foi voltado predominantemente para a autenticação dos pacientes nos diversos sistemas informatizados de saúde. Aplicando os critérios de inclusão e exclusão, dos 297 estudos encontrados com a *string* de busca, apenas 29 citavam com algum detalhe o processo de autenticação dos profissionais da saúde.

A Revisão Sistemática da Literatura mostrou uma grande lacuna no cuidado com a higiene do método de autenticação e de uma possível contaminação das superfícies e das digitais/mão do profissional da saúde.

3 GESTÃO DE IDENTIDADES

3.1 INTRODUÇÃO

Este capítulo traz todos os conceitos iniciais sobre identidade sustentável, ciclo de vida e gestão de identidades, autenticação e seus fatores, além do nível de garantia. São conceitos completamente novos para os profissionais da saúde, mas que refletirão nos próximos passos para a escolha de um modelo de autenticação ideal nos sistemas informatizados de saúde.

3.1.1 Gestão de Identidades

Ao longo da sua história, a sociedade desenvolveu sistemas para caracterizar os indivíduos para fins de estabelecer suas autorizações (por exemplo, carteira de motorista), suporte às necessidades de segurança (por exemplo, correspondência de impressão digital como um aspecto da investigação criminal), ou para agilizar a entrega de serviços ou direitos específicos (por exemplo, número da Seguridade Social). Na ausência de uma estrutura de Gestão de Identidade construída para um propósito, estas formas muitas vezes têm sido usados como “sistemas de identificação” de fato, com resultados desiguais.

Diariamente temos a necessidade de nos identificar em diversos domínios, sendo comum que um usuário tenha que criar e manter vários pares usuário-senha para executar tarefas corriqueiras. Essa necessidade rotineira de autenticação, além de ser um incômodo para o usuário, provoca um grande número de entraves aos prestadores de serviços, entre eles, o custo de manter e armazenar dados de diversos sistemas de autenticação. Um sistema de autenticação incômodo, repetitivo e pouco transparente forma uma barreira aos usuários do sistema, criando um difícil paradoxo, pois dada a importância vital da fase de autenticação, a mesma não pode ser ignorada (ANSELMO JUNIOR, 2011).

3.1.2 Conceitos iniciais

Os sistemas de gerenciamento de identidades estão relacionados com a criação, a administração e o emprego de:

Identificadores: Os identificadores são os dados usados para identificar uma pessoa. Por exemplo: nome completo, número CPF, e-mail, códigos da entidades de classe, número do telefone e página Web.

Credenciais: Dados provendo evidências das reivindicações sobre a identidade ou parte dela. Por exemplo: Login/senha, certificado digital, *tokens* e biometria.

Atributos: Dados que descrevem características da pessoa. Por exemplo: papel do profissional da saúde na organização, hospital ou clínica; privilégios e direitos; especialidade médica, entre outros.

Diante dos conceitos acima, o gerenciamento de identidades lida com as principais operações (BATISTA NETO, 2014):

Identificação: Através de um identificador, uma entidade fornece uma identidade ao sistema;

Autenticação: Através da verificação das credenciais, o sistema verifica se a identidade é legítima;

Autorização: O sistema concede privilégios a uma entidade, após a autenticação da sua identidade. Está relacionada com a concessão de permissões a uma determinada pessoa para acessar determinados recursos, controla quais dados o usuário pode acessar;

Auditoria: Tudo o que é realizado por uma entidade é registrado no sistema e serve de prova tanto para as partes envolvidas quanto para terceiros.

3.2 ID4D

Para auxiliar profissionais a projetar e implementar sistemas de identificação (ID) que sejam inclusivos e confiáveis, a Iniciativa de Identificação para o Desenvolvimento do Grupo Banco Mundial (ID4D) desenvolveu um guia . Usaram como base os dez Princípios de Identificação para o Desenvolvimento Sustentável, além de outros padrões internacionais e boas práticas (WORLD BANK, 2019a).

Os dez Princípios de Identificação para o Desenvolvimento Sustentável, são baseados em três pilares (WORLD BANK, 2019f):

1. Inclusão
   - Garanta o acesso universal aos indivíduos, livre de discriminação;
   - Remova as barreiras de acesso e uso.
2. Design

- Estabeleça uma identidade confiável - única, segura e precisa;
- Crie uma plataforma responsiva e interoperável;
- Use padrões abertos e evite o aprisionamento de fornecedores e tecnologias;
- Proteja a privacidade e a agência por meio do design do sistema;
- Plano de sustentabilidade financeira e operacional.

3. Governança

- Proteja dados pessoais, mantenha a segurança cibernética e proteja os direitos das pessoas por meio de uma estrutura legal e regulatória abrangente;
- Estabeleça mandatos institucionais claros e responsabilidade;
- Aplique estruturas legais e de confiança por meio de supervisão independente e julgamento de queixas.

Utilizamos os princípios acima citados como guia para a concepção de um *framework* para identidade eletrônica de médicos e demais profissionais de saúde.

3.3 MODELOS DE GESTÃO DE IDENTIDADE

O gerenciamento de identidades consiste em um conjunto de funções e habilidades, como administração, coleta, armazenamento e troca de informações, usadas para garantir a identidade de uma entidade e as informações contidas nessa identidade. Permite assim que relações entre entidades possam ocorrer de forma segura e que cada informação possa ser acessadas por quem realmente pode acessá-la, naquele momento, naquele sistema. Uma boa solução de gerenciamento de identidade deve ser capaz de elevar a produtividade, permitir maior eficiência na entrega dos serviços computacionais, diminuir custos e elevar a fidelidade dos utilizadores (ANSELMO JUNIOR, 2011).

São componentes do gerenciamento de identidades (BATISTA NETO, 2014; ANSELMO JUNIOR, 2011):

Identidade: Já definida anteriormente;

Usuário: Entidade que acessa algum serviço, fornecido pelo Provedor de Serviços;

Provedor de Serviços (SP, do inglês *Service Provider*, ou Provedor de Serviços): É uma aplicação web que possui o serviço ou informação que o usuário deseja obter acesso. O provedor de serviço delega o serviço de autenticação a uma

terceira parte, o provedor de identidade, que pode enviar ao SP informações sobre o usuário. Essa entidade dispõe recursos apenas a um usuário autorizado, isto é, aquele que teve sua identidade verificada quanto à autenticidade e que pode acessar o serviço;

Provedor de Identidade (IdP, do inglês *Identity Provider*): É responsável por emitir a identidade de um usuário, atestando-a perante os Provedores de Serviços;

Na prestação de serviços *online*, existem três principais modelos de gerenciamento de identidade, permitindo que os usuários sejam reconhecidos e autenticados por provedores de serviços (LAURENT; BOUZEFRANE, 2015):

Modelo de gerenciamento de identidade isolado ou tradicional: Cada provedor de serviço usa seu próprio domínio de identidade. Um usuário deve usar um identificador e uma credencial específica para cada domínio (LAURENT; BOUZEFRANE, 2015);

Modelo de identidade federada: Cada provedor de serviços usa seu próprio provedor de identidade, mas reconhece credenciais de outras prestadoras de serviço pertencentes à federação. O acesso a um provedor de serviços pode ser por meio de uma identidade fornecida por um provedor de identidade diferente do seu. O modelo de identidade federada está fundamentado sobre a distribuição da tarefa de autenticação dos usuários por múltiplos provedores de identidades, estando estes dispostos em diferentes domínios administrativos (ANSELMO JUNIOR, 2011);

Modelo de identidade centralizado: Este modelo permite centralizar tudo em um único provedor de identidade, onde todos os serviços o consultam para a realização da autenticação dos usuários. Não é necessário possuir diversas identidades como no modelo tradicional. Neste modelo é utilizado o conceito de autenticação única conhecido por *Single Sign-On (SSO)*, isto é, o usuário se autentica uma única vez obtendo credenciais para todos os Provedores de Serviços utilizados (MELO, 2013; BATISTA NETO, 2014).

Conectar pacientes, médicos e empresas farmacêuticas é complexo e caro. Ao longo do processo, é fundamental gerenciar o consentimento, a autenticidade dos documentos e das pessoas, garantir a privacidade e proteger o acesso aos dados de saúde do paciente (BOYSEN, 2019).

3.4 LPGD

Atualmente, os dados pessoais e profissionais dos trabalhadores da saúde estão presentes em todos os setores de Recursos Humanos dos hospitais, clínicas ou empresas onde cada um exerce sua profissão. Comumente, essa categoria profissional trabalha em mais de um local.

A Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), que entrou em vigor em agosto de 2021, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado (BRASIL, 2018).

Tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, e os dados tratados tanto nos meios físicos como nos digitais estão sujeitos à regulação (SOARES, R. R., 2020).

A LGPD disciplina sobre o tratamento dos referidos dados pessoais, abrangendo operações que deverão ser adequadas à legislação, como por exemplo: a coleta, a recepção, o compartilhamento, a classificação, o acesso, a reprodução, a utilização, a avaliação, o processamento, o armazenamento, a eliminação, entre outras operações (SOARES, R. R., 2020).

A referida lei traz o conceito de “dados sensíveis” vinculados a uma pessoa física sendo inclusive as **credenciais biométricas** classificadas assim. Os dados sensíveis necessitam de um tratamento diferenciado com relação a segurança do armazenamento e compartilhamento.

A necessidade para a adequação da LGPD no setor de Recursos Humanos precisa ser vista com atenção, pois atualmente é ali que a coleta e recepção de dados ocorre, sendo imperativo um tratamento de dados pessoais com máxima segurança (LBCA, 2021).

O dispositivo legal estabelece que falhas de segurança tem penalidades rígidas, podendo gerar multas pesadas. A adequação que as empresas e instituições de saúde precisam sofrer para garantir a segurança dos dados pessoais dos profissionais da saúde contratados pode ser aliviada com a existência de um provedor único de identidade para cada categoria profissional.

Nesse contexto, a proposta de um provedor de identidade único incentiva a minimização da disseminação de informações de identificação e credenciais, inclusive dos dados sensíveis.

O provedor de identidade deve cumprir suas respectivas políticas de retenção de registros de acordo com as leis, regulamentos e políticas aplicáveis. Ele deve conduzir um processo de gerenciamento de risco, incluindo avaliações de privacidade e riscos de segurança para determinar por quanto tempo os registros devem ser retidos e deverá informar ao usuário e aos provedores de serviço dessa política de retenção.

3.5 CICLO DE VIDA DA IDENTIDADE

O ciclo de vida da identidade não é um evento único. Em vez disso, é um processo que começa quando uma pessoa se registra pela primeira vez e sua identidade é criada; continua com a autenticação dessa identidade e atualizações de seus atributos e credenciais ao longo do tempo; e termina quando um registro de identidade é retirado ou invalidado (por exemplo, após a morte, pedido de remoção pelo indivíduo ou algum outro evento) (WORLD BANK, 2019c).

Discorreremos sobre o ciclo de vida da identidade do médico, sabendo que cada categoria de profissional da saúde possui um ciclo bem semelhante.

3.5.1 Cadastro

O início do ciclo de vida da identidade médica ocorre quando, ao concluir a graduação, o médico recém-formado busca o CRM do seu Estado para registrar-se. Sem o registro inicial, o médico não pode exercer a profissão. Nessa fase, o recém-formado apresenta seu diploma de conclusão do curso, além de todos os seus documentos pessoais (RG, CPF, título de eleitor, comprovante de residência). Também é nesse momento que os dados biométricos são colhidos: impressão digital dos 10 dedos das mãos e foto da face.

Apesar de haver registro e a coleta dos dados biométricos, essas digitais colhidas e o registro da face não são utilizados atualmente nem mesmo para a autenticação nos próprios serviços oferecidos pelo CFM/CRM nos seus respectivos sites.

A biometria do médico só é utilizada nos provedores de identidade próprios de cada ecossistema de saúde, não sendo provida pelo CRM onde foi cadastrado inicialmente.

3.5.2 Emissão

Após a verificação da autenticidade de toda a documentação apresentada, o CRM emite o registro, com um número único regional para cada médico. Há a entrega da famosa *"carteira verde"* onde serão anotados manualmente todas as atualizações de seus identificadores, atributos e credenciais ao longo do tempo (mudança de nome

após o casamento, registro da especialidade médica, suspensão do registro profissional em caso de punições, entre outros). Também há a entrega da carteira de identidade médica (CIM) onde constam dados pessoais e profissionais, foto e um chip para a inclusão futura de um certificado digital.

Para que uma identidade seja considerada digital, ela deve armazenar dados utilizáveis em um ambiente digital (por exemplo, serem legíveis por máquina e / ou utilizáveis na Internet). Tal como acontece com o registro, os tipos de credenciais emitidas, incluindo seu formato e recursos de segurança, têm implicações importantes para a robustez do sistema contra roubo de identidade e fraude, bem como acessibilidade. Além disso, o formato das credenciais, como cartões, é o principal fator para o custo dos sistemas de identificação (WORLD BANK, 2019c).

Percebe-se que a atual carteira médica tem um *"potencial"* de se tornar digital, assim que o certificado digital for incluído. Considerando o leitor de cartão necessário para a sua utilização, encontramos limitadores para este formato.

3.5.3 Autenticação

Depois que uma pessoa é registrada e credenciada, ela pode autenticar-se ou “provar” sua identidade quando necessário para acessar os benefícios e serviços associados. O processo de autenticação pode envolver um ou vários fatores - ou seja, credenciais de identidade e/ou atributos (WORLD BANK, 2019c).

O uso de vários fatores de autenticação aumenta o nível de garantia (ou seja, segurança ou confiabilidade) em uma transação (WORLD BANK, 2019c; SANTOS *et al.*, 2012; SANTOS, 2012).

Atualmente a CIM raramente é usada como forma de autenticação em sistemas informatizados já que depende da compra de um certificado digital e de um leitor de cartão.

No site do próprio CRM/SC, há a possibilidade de emissão de documentos médicos (prescrições, atestados, relatórios médicos) com a autenticação baseada em login (email do profissional) e senha, apenas. Isso traz uma fragilidade de segurança já que esses dados podem ser roubados ou informados conscientemente a terceiros para exercício ilegal da profissão.

3.5.4 Autorização

Depois que o indivíduo é autenticado, o provedor de serviços pode realizar um processo separado (mas às vezes automático) para determinar se essa pessoa

está autorizada a acessar diferentes serviços ou realizar algumas ações. A autorização pode ser baseada, por exemplo, em identificadores ou atributos fornecidos pelo provedor de identidade. Em um hospital, podemos ter a autorização de acesso a prescrição médica apenas para aqueles profissionais com número ativo de inscrição no CRM daquele Estado, impedindo, por exemplo, a prescrição feita por um médico cassado.

3.5.5 Gestão

Ao longo do ciclo de vida, os provedores de identidade gerenciam dados e credenciais de identidade por meio de um processo dinâmico. É importante ressaltar que isso inclui atualizar e reavaliar atributos e credenciais de identidade que mudam com o tempo - por exemplo, endereço, estado civil, especialidade médica, imagem facial, etc (WORLD BANK, 2019c).

A tecnologia e os protocolos usados ao longo do ciclo de vida - incluindo para registro, emissão de credenciais, autenticação e gerenciamento - são essenciais para garantir a inclusão e confiabilidade do sistema e sua capacidade de facilitar a autenticação para diferentes transações no *"nível de garantia"* apropriado (WORLD BANK, 2019c).

Atualmente, os profissionais da saúde tem o registro dinâmico das mudanças de atributos e credenciais ocorrendo nos conselhos de cada categoria profissional. Não há o mesmo dinamismo e atualização desses dados nos provedores de identidade descentralizados em cada instituição de saúde. Se o médico for cassado, o hospital provavelmente só terá conhecimento após receber a primeira denúncia. Isso nos faz pensar que, de forma ideal, o provedor de identidade deve estar ligado a cada conselho de categoria profissional.

3.6 CREDENCIAIS E AUTENTICAÇÃO

As credenciais e os mecanismos de autenticação adotados pelo sistema de identidade eletrônica ditam como o sistema será usado pelas pessoas em seu dia a dia. Como tal, eles são fundamentais para a experiência que os usuários finais e partes confiáveis (provedores de serviço) têm quando interagem com o sistema, o nível de garantia que ele fornece para transações e grande parte de sua funcionalidade e uso.

Além disso, os tipos de credenciais e mecanismos de autenticação adotados desempenham um grande papel na determinação do custo geral do sistema. Portanto, deve haver um esforço para fornecer credenciais e mecanismos de autenticação que possam fornecer um nível de garantia alto o suficiente, sendo ao mesmo tempo adequados ao contexto (WORLD BANK, 2019b).

Uma credencial é aquilo que uma pessoa apresenta - pessoalmente ou remotamente - para dizer *"este é quem eu sou"*. Os tipos de credenciais emitidas em um sistema de identificação variam em várias dimensões, incluindo se são ou não físicas (ou seja, devem ser carregadas fisicamente por uma pessoa para usá-las) e se são ou não digitais (ou seja, elas são legíveis por máquina e, portanto, podem ser usados em um ambiente digital) (WORLD BANK, 2019e).

3.7 AUTENTICAÇÃO

A autenticação da identidade digital do usuário é classificado nas três seguintes abordagens (CONTI *et al.*, 2017):

Algo que você sabe: Se o usuário conhece um pré-determinado segredo (geralmente representado por uma senha), então ele é a pessoa correta. Esta abordagem é chamada baseada em conhecimento, porque usa informações que só o usuário conhece;

Algo que se tem: Se um usuário possui um *token* (crachá magnético ou *smartcard*, por exemplo), então ele é a pessoa correta. Essa abordagem é chamada baseada em *tokens*, porque ela usa informações que o usuário possui;

Algo que se é: Nesta abordagem, o conceito é que o sistema compara as características biométricas do usuário com valores pré-cadastrados, conhecidos como *template*, permitindo apenas o acesso se a característica medida corresponde ao modelo armazenado no sistema.

Já com base no número de fatores aplicados no processo de autenticação, os esquemas de autenticação podem ser classificados como (OMETOV *et al.*, 2018):

Autenticação de fator único (SFA): a autenticação é realizada usando apenas um fator;

Autenticação de dois fatores (2FA): a autenticação é conduzida usando dois fatores diferentes. Por exemplo, usando biometria combinada com uma senha pode fornecer maior segurança para os esquemas de autenticação do que esquemas que apenas aplicam senhas;

Autenticação multifator (MFA): a autenticação é realizada com base em vários fatores diferentes.

Considerando as vulnerabilidades de cada método de autenticação , os esquemas de autenticação que utilizam menos fatores tornam-se mais vulneráveis a mais ataques à segurança. Por exemplo, quando um sistema de autenticação aplica cartão inteligente e senha, ele fica vulnerável aos ataques de adivinhação de senha, uma vez que o cartão inteligente é roubado ou perdido. Esse problema pode ser atenuado usando outro terceiro fator no esquema de autenticação. No entanto, a aplicação de mais fatores de autenticação torna o processo de autenticação mais complicado (MASDARI; AHMADZADEH, 2017).

3.7.1 Fatores de autenticação

A combinação de nome de usuário e senha é o mais popular método de autenticação em sistemas informatizados hospitalares. Existem muitas razões pelas quais este não é um método seguro. Os usuários escolherão senhas muito fáceis de lembrar que também são fáceis de quebrar. Quando são impostas restrições na escolha da senha para forçar os usuários a ter senhas mais fortes, eles fazem o que podem para tornar o login mais fácil, ou anotá-los, por exemplo. As senhas estão sujeitas a ataques de engenharia social que podem ser fáceis de manipular em um ambiente de emergência. Se uma pessoa mal-intencionada afirma que há uma emergência e pede a uma equipe a senha do membro, eles podem ser mais propensos a divulgarem (GARSON; ADAMS, 2008).

Identificamos através da RSL que, principalmente no início dos anos 2000, foi introduzido o uso dos *smartcards* na autenticação, tanto pelo paciente como pelo profissional da saúde, trazendo o dispositivo como inovação. As imperfeições desse método de autenticação mostram que essa alternativa ainda está longe do ideal. Um *smartcard* pode ser perdido, roubado, extraviado ou dado voluntariamente a um usuário não autorizado; e um segredo pode ser esquecido, adivinhado, e voluntariamente (ou não) ser divulgado a um usuário não autorizado.

Uma tecnologia que pode ser usada em um *token ou smartcard* é a identificação por Radiofrequência (RFID) que é uma tecnologia sem fio. Um sistema RFID típico inclui um leitor e uma série de etiquetas, que podem variar de etiquetas de alto custo e alimentadas por bateria com recursos de Wi-Fi a etiquetas de baixo custo que são bastante restritas em recursos e até mesmo sem alimentação interna. As etiquetas geralmente armazenam dados relacionadas ao titular e enviam essas informações para um leitor (SAFKHANI *et al.*, 2012).

Independente da tecnologia usada no *token*, esse método de autenticação torna-se pouco prático porque exige que o usuário carregue consigo *"algo"* contendo as informações necessárias para a autenticação. Com a abordagem por biometria, em

vez disso, o usuário não tem a necessidade de lembrar ou levar nada consigo: todas as informações necessárias para autenticação pertencem ao usuário.

Assim surgiram técnicas biométricas como uma ferramenta poderosa para autenticação de usuário para resolver estes problemas. Uma vez que é baseado no fisiológico e características comportamentais de um indivíduo, a biometria não sofre das mesmas desvantagens encontradas nos métodos de autenticação tradicionais (AWASTHI; SRIVASTAVA, 2013).

Credenciais biométricas são métodos automatizados de identificar uma pessoa ou verificar a identidade de alguém com base em uma característica fisiológica ou comportamental. Exemplos de características fisiológicas incluem imagens de mãos ou dedos, geometria do rosto, escaneamento da íris e retina, impressões digitais e voz. Características comportamentais são traços que são aprendidos ou adquiridos. Verificação de assinatura dinâmica e ritmo de pressionamento de teclas são exemplos de características comportamentais (CONTI *et al.*, 2017).

A biometria é proposta como um mecanismo de autenticação alternativo, pois a biometria é parte de nós e não pode ser compartilhada facilmente. Entre os parâmetros biométricos, chamamos a atenção para os que não necessitam de toque para sua efetivação, como o reconhecimento de face, por exemplo. É um identificador mais amigável que pode ser feito à distância, sem exigir contato físico, sem haver contaminação de mãos e superfícies.

Cada tecnologia tem vantagens e desvantagens, na verdade, não existe uma tecnologia correta para todos os fins. A seguir apresentaremos as características fisiológicas e comportamentais humanas mais usadas para implementar um sistema biométrico, baseado em (CONTI *et al.*, 2017):

Reconhecimento Facial ou Geometria da Face: Baseados na distância entre os atributos faciais (ou seja, a distância entre os olhos) e em sua forma (ou seja, a amplitude da boca). Esta tecnologia tem um bom impacto no usuário, pois é menos intrusivo e não é caro. Porém, a abordagem de reconhecimento de geometria facial é muito sensível as variações na iluminação, as diferentes posições da face e expressões. Os desempenhos diminuem quando a dimensão do banco de dados aumenta (os gêmeos dificilmente são distinguíveis) (CONTI *et al.*, 2017).

Reconhecimento de Impressão digital: As impressões digitais são únicas, não mudam com o tempo e são diferentes também em gêmeos idênticos. Tem alguns limites: a pele excessivamente úmida ou seca pode comprometer o desempenho dos sistemas, às vezes as impressões digitais não são utilizáveis devido a pre-

sença de lesões cortantes, cicatrizes ou uso de luvas, além de terem um impacto ruim no usuário, pela associação que se faz entre a figura do criminoso e as impressões digitais. Além disso, permite a contaminação das superfícies com o toque. Essa tecnologia é a mais comum, mesmo que não seja tão fácil de ser implementado devido aos custos computacionais e solicitações de recursos (CONTI *et al.*, 2017).

Geometria da mão: A forma e as dimensões da mão podem ser usadas como características biométricas. Os sistemas de reconhecimento de geometria da mão tem muitas vantagens em relação às impressões digitais: requer menos espaço para armazenar os modelos, todo o sistema é mais conveniente e tem pequena resistência psicológica de humanos. Mas também esta tecnologia tem alguns defeitos: os usuários não querem colocar a palma da mão onde muitos outros colocaram as suas, principalmente em tempos de pandemia. Os desempenhos dependem das condições de limpeza das mãos e a forma da mão não é invariante durante a vida. Finalmente, um problema real é a grande dimensão do sensor de mão, portanto, esta tecnologia não é apropriada para alguns aplicativos, como dispositivos portáteis (celulares, por exemplo) (CONTI *et al.*, 2017).

Escaneamento da íris: Depois do DNA, a íris é a característica biométrica mais discriminativa do corpo humano: também gêmeos idênticos têm íris diferentes. Esta tecnologia usa câmeras de vídeo para a digitalização e não é necessário contato entre o olho do sujeito e o *scanner* biométrico (CONTI *et al.*, 2017). A íris é menos suscetível a danos em relação a outras partes do corpo, o *template* pede apenas alguns *bytes* para armazenamento e o sistema funciona mesmo se a pessoa estiver usando óculos. No entanto, devido à íris ser bem pequena, há necessidade de uma câmera de alta resolução para ser capturada adequadamente. A câmera deve estar próxima para capturar a íris e todo esse processo é altamente sensível ao movimentos corporais (NANDAKUMAR; JAIN, Anil K., 2015). Esses sistemas podem falhar quando lentes de contato são usadas, ou ao piscar na hora de tirar o imagem. Além disso, existe uma série de doenças oculares que afetam a capacidade do sistema de reconhecimento da íris de capturar a imagem adequada do olho (DAUGMAN, 2005).

Escaneamento de retina: A conformação das vasos sanguíneos sob a superfície da retina do olho é única e, portanto, é uma característica utilizável para reconhecimento pessoal. A varredura da retina é realizada enviando um feixe de luz de baixa intensidade dentro do bulbo ocular e armazenando o padrão constituído pelo vasos oculares. O usuário deve estar perto do *scanner* e focar em um ponto específico com o próprio olho: este tipo de sistema é menos atraente. Além disso,

os sensores ainda são bastante caros e os vasos sanguíneos da retina tem distribuição que muda durante a vida;

Reconhecimento de voz: É a tecnologia menos precisa, mas é a preferida dos usuários e pode fornecer o acesso às informações por meio das linhas telefônicas. A voz para o reconhecimento pode ser dependente do texto ou independente do texto: no primeiro caso, o usuário diz uma frase predeterminada; no segundo caso (menos preciso), o usuário simplesmente diz algo. O problema desta tecnologia é que o usuário pode realizar uma grande variedade de inflexões de voz para variações de ambiente, por estresse ou por algum adoecimento. Além disso, os ruídos ambientais podem reduzir fortemente o desempenho. Os gêmeos e irmãos dificilmente são distinguíveis; também entre diferentes pessoas, as porcentagens de erro são altas (CONTI *et al.*, 2017).

A escolha da tecnologia biométrica geralmente é feita considerando o tipo de solução necessária, o ambiente onde o sistema biométrico será usado, o nível de aceitação do usuário final e o nível de segurança solicitado. Devido a pandemia do COVID-19, métodos de autenticação sem o toque são ideais para sistemas informatizados.

3.8 *OAUTH 2.0*

O *Open Authorization Protocol - OAuth* é um protocolo desenvolvido com o objetivo de solucionar os problemas relacionados com a gestão de identidades entre provedores de serviços (CONCEIÇÃO, 2014).

É um protocolo que recentemente se tornou um padrão aberto da indústria para fornecer delegação de acesso seguro e é usado por organizações da Internet como *Google, Twitter, Facebook*, etc. (KHATOON; UMADEVI, 2018).

OAuth 2.0 foi publicado em outubro de 2012 e não é compatível com o seu antecessor *OAuth 1.0*, que foi introduzido em 2007 (KHATOON; UMADEVI, 2018). Na última versão, 2.0, quatro papéis básicos são definidos e necessários para compreensão do fluxo de execução do protocolo, são eles (HARDT, 2012):

Proprietário do recurso É a entidade que tem o poder de conceder a permissão de acesso, aos seus recursos, às outras entidades;

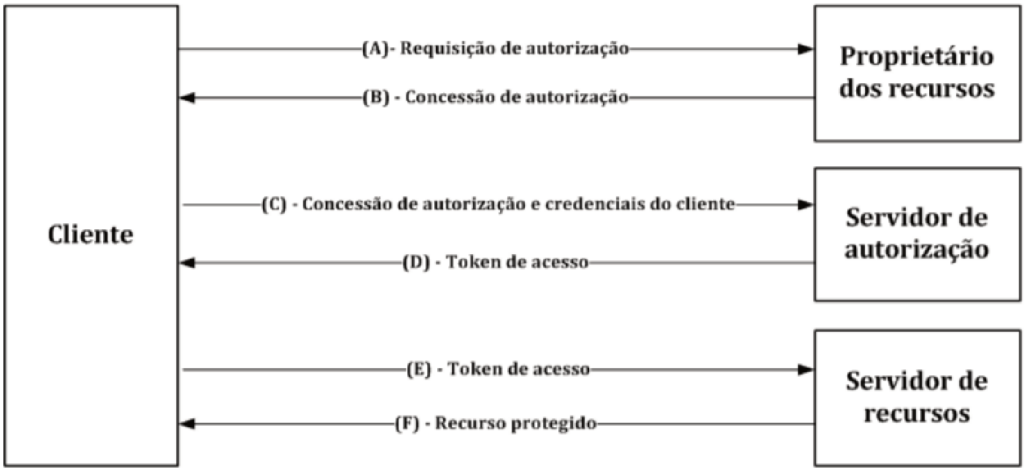
Servidor de recursos É o responsável por hospedar e responder às solicitações de acesso a recursos protegidos, usando *tokens* de acesso;

Cliente É uma aplicação, que realiza solicitações de acesso de recursos protegidos, ao servidor de recursos, em nome do proprietário, dono do recurso, após a obtenção de sua autorização;

Servidor de autorização É responsável por emitir *tokens* de acesso aos clientes, após autenticar e obter autorização do proprietário de recursos

Na maioria dos casos, o papel do servidor de autorização e o servidor de recursos podem ser representados por uma única entidade. A Figura 3 apresenta de forma abstrata o fluxo do protocolo *OAuth 2.0* e descreve a interação entre os quatro papéis (CONCEIÇÃO, 2014).

Figura 3 – Fluxo do protocolo *OAuth 2.0*.



Fonte: Adaptado de (HARDT, 2012).

As mensagens do fluxo de autenticação são as seguintes (CONCEIÇÃO, 2014):

(A) O cliente solicita a autorização do proprietário do recurso;

(B) O cliente recebe uma concessão de autorização, que representa a autorização fornecida pelo proprietário do recurso;

(C) O cliente solicita ao servidor de autorização um *token* de acesso que pode ser usado para acessar os recursos protegidos. Durante este processo, o cliente fornece suas credenciais e a concessão de autorização para autenticar-se com o servidor de autorização;

(D) O servidor de autorização confirma a validade das credenciais do cliente e da concessão de autorização. Se elas forem válidas, ele então fornece ao cliente um *token* de acesso;

(E) O cliente solicita os recursos protegidos, hospedados no servidor de recursos, apresentando o *token* de acesso;

(F) O proprietário do recurso verifica a validade do *token* de acesso e, se válido, ele atende ao pedido.

O *OAuth 2.0* permite que um cliente (médico) acesse os recursos dos usuários (pacientes) por um período limitado de tempo a partir de um servidor sem que o usuário precise compartilhar suas credenciais com o cliente. Em vez disso, o cliente usa um *token* de acesso como referência ao solicitar ao servidor o recurso de usuários (KHATOON; UMADEVI, 2018).

Os *tokens* de acesso têm uma vida útil muito curta e vêm com um carimbo de data e hora de expiração predefinido, geralmente uma hora a partir do momento da criação. Isso é feito para evitar ataques de repetição. É importante para vincular vários médicos, hospitais e departamentos de saúde e fornecem todos os recursos necessários sob um único teto (KHATOON; UMADEVI, 2018).

Em um país como a Índia, com mais de 1 bilhão de habitantes, muitos cidadãos não conseguiram obter acesso a várias instalações do governo por causa da verificação em papel. Mas isso mudou após a introdução do Aadhaar, que utiliza o *OAuth 2.0*, permitindo que agências e organizações autenticassem dados rapidamente, identificassem usuários e os integrassem instantaneamente em poucos minutos (KHATOON; UMADEVI, 2018).

Assim, tornou o mecanismo de inscrição/login fácil, onde os pacientes puderam se registrar sem esforço e começar a acessar as instalações do sistema sem ter que esperar por aprovações de terceiros. O processo de inscrição deve ser independente da verificação de documentos e papelada (KHATOON; UMADEVI, 2018).

Usamos esse recurso no nosso protótipo para a arquitetura do processo de autorização nos sistemas.

3.9 *OPENID CONNECT*

Já para o processo de autenticação no protótipo, utilizamos o *OpenID Connect*.

OpenID Connect 1.0 é uma camada de identidade simples no topo do protocolo *OAuth 2.0*. Ele permite que os clientes verifiquem a identidade do usuário final com base na autenticação realizada por um Servidor de Autorização, bem como permite obter informações básicas do perfil do usuário final de maneira interoperável (OIDF, 2020).

Estruturas de autenticação baseadas em criptografia de chave pública como *OpenID Connect* aumentam globalmente a segurança de toda a Internet, colocando a responsabilidade pela verificação da identidade do usuário nas mãos dos provedores de serviços mais especializados. Em comparação com seus predecessores, o *OpenID Connect* é muito mais fácil de implementar e integrar e pode esperar uma adoção muito mais ampla (OIDF, 2020).

O *OpenID Connect* permite que os desenvolvedores autentiquem seus usuários em sites e aplicativos sem ter que possuir e gerenciar arquivos de senha. Para o criador de aplicativos, ele fornece uma resposta segura e verificável para a pergunta: “Qual é a identidade da pessoa que usa atualmente o navegador ou aplicativo nativo que está conectado a mim?”. Ele permite que os desenvolvedores de aplicativos e sites autentiquem usuários sem assumir a responsabilidade de armazenar e gerenciar senhas diante de uma Internet que está repleta de pessoas tentando comprometer as contas de seus usuários para benefício próprio (OIDF, 2020).

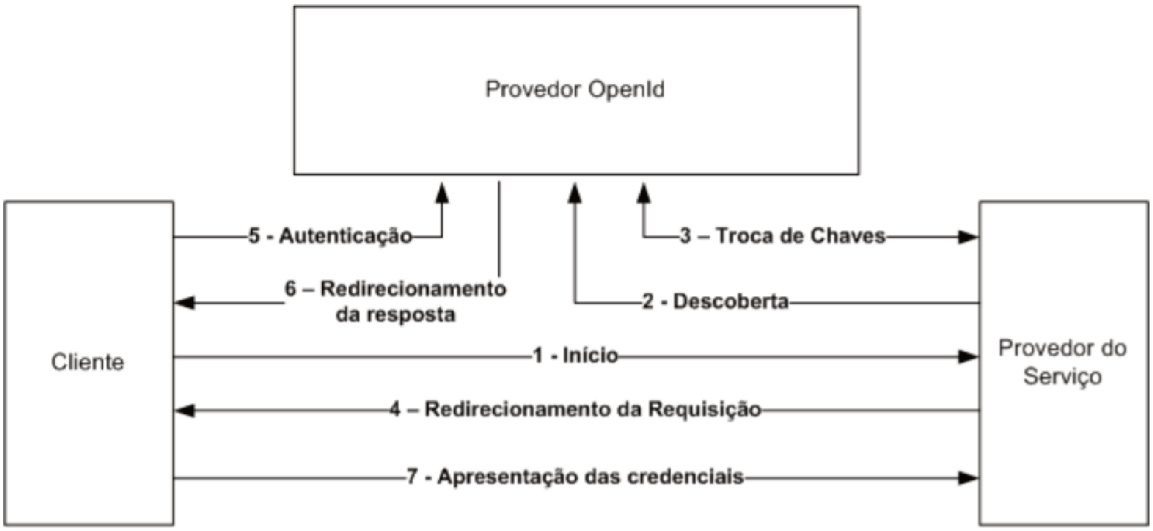
Novos métodos podem ser adotados por provedores de identidade *OpenID Connect* à medida que amadurecem para fornecer autenticação mais segura a eles. Por exemplo, a identificação de dois fatores já está em produção em alguns IdPs do OpenID Connect.

O *OpenID* é um protocolo *SSO (Single Sign-On)* que permite a autenticação em diversos websites através de um *Uniform Resource Identifier(URI)*. Ele foi desenvolvido em 2005 pela comunidade open source. Dentre as características inerentes a ele podem ser destacadas: a descentralização e a identidade única, compartilhada com consumidores diferentes. Ele é atraente por causa de sua simplicidade (CONCEIÇÃO, 2014).

Com apenas algumas interações, o cliente consegue solicitar e validar uma autenticação em um servidor OpenID e interagir com um serviço usando a alegação fundamentada (CONCEIÇÃO, 2014). O fluxo do protocolo *end-to-end* é apresentado na Figura 4:

Temos a seguinte descrição do fluxo (CONCEIÇÃO, 2014):

Figura 4 – Fluxo do protocolo *OpenID*.



Fonte: Adaptado de (HARDT, 2012).

1. Início, um cliente envia um identificador OpenID que alega possuir;
2. Descoberta, o Provedor do Serviço descobre o provedor OpenID correspondente ao identificador OpenID apresentado pelo cliente;
3. Troca de chaves, segredos são trocados entre o Provedor do Serviço e o Provedor OpenID;
4. O Provedor do Serviço redireciona o cliente para provedor de OpenID, para que ele possa se autenticar;
5. Autenticação, o cliente se autentica no provedor OpenID. A autenticação está fora do escopo OpenID;
6. O Provedor de OpenID redireciona novamente o Cliente para o Provedor do Serviço;
7. Apresentação das credenciais, finalmente, a carga OpenID contendo a declaração de identidade validada é enviada para o Provedor do Serviço (CONCEIÇÃO, 2014).

OpenID Connect pode ser usado livremente por qualquer pessoa. Os desenvolvedores do OpenID Connect não reivindicam nenhuma propriedade intelectual sobre ele.

3.10 IDENTIDADE ELETRÔNICA NO BRASIL

O advento da era digital viu um estrondoso crescimento da capacidade do cidadão em acessar informações e recursos globalmente através da internet.

À medida que a Internet se tornou o mecanismo preferido para muitos indivíduos receberem informações, se comunicarem e conduzirem negócios, as organizações oficiais responderam se interessando cada vez mais por essas possibilidades. Em nome da conveniência do cliente, elas começaram a projetar ferramentas e recursos acessíveis à rede de computadores para executar funções apenas uma vez alcançáveis por meio da interação pessoal com funcionários públicos em suas instituições. A proliferação desses serviços *online* explodiu e continua a explodir hoje.

Para uma adequada substituição da interação pessoal, o primeiro passo é a identificação dos envolvidos nos serviços. A identidade eletrônica tem dado passos largos para seu uso efetivo em todo o mundo.

No Brasil, já tivemos algumas experiências visando a constituição de um documento eletrônico nacional de identificação. O projeto RIC (Registro de Identidade Civil) tinha como objetivo garantir uma identificação civil nacional confiável contendo dados biométricos e biográficos, além de conter um certificado digital do titular do cartão RIC. Alguns poucos RICs foram emitidos para autoridades do alto escalão, mas o projeto não teve continuidade (ARAÚJO, 2020).

Uma segunda tentativa de possuir um instrumento digital de identificação nacional é o projeto DNI (Documento Nacional de Identificação). O projeto foi iniciado em 2018 e o conceito do DNI, diferentemente do RIC, é de ser um documento digital que centraliza vários outros documentos do cidadão (digitais ou físicos), a exemplo do seu CPF, título de eleitor e CNH. Em princípio o DNI é disponibilizado apenas como um aplicativo para dispositivos móveis e é fruto da interoperabilidade entre bases de dados do estado brasileiro (ARAÚJO, 2020).

Mas a novidade do Governo Federal é o gov.br: Fornece um nível de segurança compatível com o grau de exigência, natureza e criticidade dos dados e das informações pertinentes ao serviço público solicitado. O objetivo do governo federal é integrar todos serviços públicos digitais a conta gov.br. Foi criado pelo Ministério da Economia (ME), em parceria com o Serviço Federal de Processamento de Dados (Serpro) (GOV.BR, 2019).

O gov.br utiliza os mesmos recursos e protocolos (*OpenID Connect e OAuth 2.0*) de segurança de empresas renomadas, respaldados por uma especificação consolidada da indústria de software para identificação, autenticação e autorização de

usuários.

O *"potencial positivo"* de transações seguras e protegidas, sempre acessíveis a qualquer distância, começou a tomar substância. Ao fazer isso, a importância de estabelecer uma identidade para apoiar estas interações tornaram-se cada vez mais essencial. Neste ponto, a maneira casual de *"identificação"* empregada até o momento tornou-se insuficiente para estabelecer a relação de confiança necessária para essas transações.

O desafio é o de estruturar um sistema robusto, interoperável e com boa experiência de uso para a gestão de identidades, com um processo de emissão segura e viável. É preciso manter as diversas partes interessadas engajadas durante todo o processo e superar a resistência de atores que acabam por se beneficiar de um mecanismo de identificação frágil (ARAÚJO, 2020).

3.11 NÍVEL DE GARANTIA

Nível de garantia da identidade é a certeza com a qual se pode acreditar que uma solicitação de uma identidade específica durante a autenticação é realmente a “verdadeira” identidade do requerente (WORLD BANK, 2019d).

Os níveis de garantia dependem da força do processo de prova de identidade e dos tipos de credenciais e mecanismos de autenticação usados durante uma transação (WORLD BANK, 2019d).

Para prova de identidade, o nível de garantia depende do método de identificação (por exemplo, pessoalmente ou remoto), os atributos coletados e o grau de certeza com o qual esses atributos são verificados.

Para autenticação, o nível de garantia depende do tipo de credencial, do número de fatores de autenticação usados (ou seja, um contra vários) e da força criptográfica da transação. Nosso foco será o tipo de credencial e o número de fatores de autenticação.

Níveis mais altos de garantia reduzem o risco de uma identidade fraudulenta e aumentam a segurança das ações, porém também podem aumentar o custo e a inconveniência para os detentores de identidade e terceiros. Portanto, é essencial que sejam considerados as diversas exigências para as diferentes situações de uso com relação ao nível de garantia.

No Brasil o sistema gov.br trabalha com 3 níveis de garantia: ouro, prata e bronze. São chamados *"Selos de Confiabilidade"* e são usados para controle de

acesso a determinadas funcionalidade de serviços. Então, dependendo do usuário, do nível de autenticação requerido e do selo de confiabilidade que ele possui, poderá ter autorização para utilizar as suas credenciais no acesso a sistemas internos ou externos de atendimento ao cidadão (GOV.BR, 2021).

Em 2014, na União Européia, foi regulamentada a *eIDAS (Electronic Identification, Authentication and Trust Services)* com a finalidade de aumentar a confiança no sistema de negociações *online* entre os países pertencentes ao mercado único europeu. Com foco no desenvolvimento digital dos países, criou-se um *framework* de padronização da identificação e assinaturas eletrônicas. Inicialmente abrangeu apenas órgãos governamentais, mas rapidamente foi adotado pelo setor privado também para realização de transações entre países com identificação e autenticação seguras dos envolvidos (MENEZES, 2019). A classificação se dá em nível de garantia reduzido, substancial ou elevado, de acordo com o procedimento a ser realizado.

3.11.1 Riscos e Impactos

As avaliações de risco determinam até que ponto o risco deve ser reduzido pelos processos de prova de identidade, autenticação e federação. Essas avaliações levam a escolhas acertadas de tecnologias aplicáveis e estratégias de redução do risco, ao invés da aplicação de tecnologias aleatórias para este fim (GRASSI *et al.*, 2020b).

Para saber qual o nível adequado de garantia da autenticação do usuário, deve-se avaliar os riscos potenciais e identificar medidas para minimizar seu impacto. Erros de autenticação com consequências potencialmente piores requerem níveis mais altos de garantia. Porém, níveis de garantia muito acima do necessário podem gerar desconforto para o usuários e custos extras.

As categorias de dano e impacto potenciais que devem ser avaliados para orientar o nível de garantia exigido para a transação digital (no nosso caso, autenticação digital) incluem (GRASSI *et al.*, 2020b):

- Inconveniência, sofrimento ou danos à posição ou reputação;
- Perda financeira ou responsabilidade da agência;
- Danos aos programas da agência ou aos interesses públicos;
- Liberação não autorizada de informações confidenciais;
- Segurança pessoal;

- Violações civis ou criminais.

Os três valores de impacto potencial são: baixo impacto, impacto moderado e alto impacto. As definições de impactos potenciais dependerão do contexto e a natureza das pessoas ou entidades afetadas para decidir a importância relativa desses danos (GRASSI *et al.*, 2020b).

O Quadro 1 traz resumidamente o nível de garantia correspondente de acordo com o grau de impacto potencial máximo de cada categoria.

Quadro 1 – Impactos potenciais máximos para cada nível de garantia.

Categorias de impacto	**Nível 1**	**Nível 2**	**Nível 3**
Inconveniência, angústia ou danos à posição ou reputação	Baixo	Moderado	Alto
Perda financeira de responsabilidade da agência	Baixo	Moderado	Alto
Prejudicar programas de agências ou interesses públicos	N/A	Baixo/Moderado	Alto
Liberação não autorizada de informações confidenciais	N/A	Baixo/Moderado	Alto
Segurança Pessoal	N/A	Baixo	Moderado/Alto
Violações civis ou criminais	N/A	Baixo/Moderado	Alto

Fonte: (GRASSI *et al.*, 2020b).

3.11.2 Autenticadores para cada nível de garantia

O Quadro 2 traz resumidamente e de forma exemplificativa as características de cada método de autenticação para cada nível de garantia que consta no *guideline* de identidade digital elaborado pelo Banco Mundial.

As diretrizes do Instituto Nacional de Padrões e Tecnologia dos EUA (NIST) pormenorizaram as recomendações sobre os autenticadores possíveis e suas características de acordo com os níveis de garantia para prova de autenticação (*"nível de garantia do autenticador"* ou AAL).

É possível determinar alternativas para a orientação recomendada pelo NIST, para nível de garantia avaliado na autenticação digital, com base no seu propósito, tolerância ao risco, processos de negócios existentes, considerações especiais para determinadas populações, disponibilidade de dados que fornecem atenuações semelhantes às descritas, ou devido a outros recursos exclusivos do provedor de serviço (GRASSI *et al.*, 2020b).

Quadro 2 – Níveis de garantia de autenticação.

Níveis de garantia	Baixo (nível 1)	Substancial (nível 2)	Alto (nível 3)
Autenticação (AAL)	Pelo menos 1 fator de autenticação - algo que você tem, sabe ou é (por exemplo, senha ou PIN)	Pelo menos 2 fatores de autenticação (por exemplo, um token com uma senha ou PIN)	Pelo menos duas categorias diferentes de fatores de autenticação e proteção contra duplicação e adulteração por invasores com alto potencial de ataque (por exemplo, incorporar material de chave criptográfica em token de hardware resistente a adulteração + PIN, biometria com detecção de atividade + PIN / cartão inteligente)
Risco assumido pela parte confiável	mitigado	baixo	mínimo

Fonte: Adaptado de (WORLD BANK, 2019d)

3.11.3 AAL

O documento (WORLD BANK, 2019d) fornece recomendações sobre os tipos de processos de autenticação, incluindo opções de autenticadores, que podem ser usados em vários Níveis de Garantia de Autenticador (AALs).

Estes são os níveis de garantia do autenticador (GRASSI *et al.*, 2020a):

Nível 1 AAL1 fornece alguma garantia de que o reclamante controla um autenticador vinculado à conta do assinante. O AAL1 requer autenticação de fator único ou multifator, usando uma ampla variedade de tecnologias de autenticação disponíveis. A autenticação bem-sucedida exige que o reclamante prove a posse e controle do autenticador por meio de um protocolo de autenticação seguro;

Nível 2 AAL2 fornece alta confiança de que o reclamante controla um(s) autenticador(es) vinculados à conta do assinante. A prova de posse e controle de dois fatores de autenticação diferentes é necessária por meio de protocolo(s) de autenticação seguro(s). Técnicas criptográficas aprovadas são necessárias em AAL2 e superior;

Nível 3 AAL3 fornece uma confiança muito alta de que o reclamante controla o(s) autenticador(es) vinculados à conta do assinante. Para se autenticar no AAL3, os requerentes devem comprovar a posse e o controle de dois fatores de au-

tenticação distintos por meio de protocolo(s) de autenticação seguro(s). São necessárias técnicas criptográficas aprovadas.

3.11.3.1 AAL1

A autenticação AAL1 deve ocorrer pelo uso de qualquer um dos seguintes tipos de autenticador, que são definidos (GRASSI *et al.*, 2020a):

- Segredo memorizado;
- Segredo de pesquisa;
- Dispositivos fora de banda;
- Dispositivo de senha única de fator único (OTP);
- Dispositivo multifator OTP;
- Software criptográfico de fator único;
- Dispositivo criptográfico de fator único;
- Software de criptografia multifatorial;
- Dispositivo criptográfico multifator.

Na AAL1, a reautenticação do assinante deve ser repetida pelo menos uma vez a cada 30 dias durante uma sessão de uso prolongado, independentemente da atividade do usuário. A sessão deve ser encerrada (ou seja, desconectada) quando este limite de tempo for atingido (GRASSI *et al.*, 2020a).

3.11.3.2 AAL2

Em AAL2, a autenticação deve ocorrer pelo uso de um autenticador multifator ou uma combinação de dois autenticadores de fator único. Um autenticador multifator requer dois fatores para executar um único evento de autenticação, como um dispositivo criptograficamente seguro com um sensor biométrico integrado necessário para ativar o dispositivo.

Quando um autenticador multifator é usado, qualquer um dos seguintes pode ser usado (GRASSI *et al.*, 2020a):

- Dispositivo multifator OTP;

- Software de criptografia multifatorial;
- Dispositivo criptográfico multifator.

Quando uma combinação de dois autenticadores de fator único é usada, ela deve incluir um autenticador de segredo memorizado e um autenticador baseado em posse (ou seja, *"algo que você tem"*) da seguinte lista:

- Segredo de pesquisa;
- Dispositivo fora de banda;
- Dispositivo OTP de fator único;
- Software criptográfico de fator único;
- Dispositivo criptográfico de fator único.

Sobre a reautenticação periódica das sessões do assinante, em AAL2, a autenticação do assinante deve ser repetida pelo menos uma vez a cada 12 horas durante uma sessão de uso prolongado, independentemente da atividade do usuário. A reautenticação do assinante deve ser repetida após qualquer período de inatividade de 30 minutos ou mais. A sessão deve ser encerrada (ou seja, desconectada) quando um desses limites de tempo for atingido (GRASSI *et al.*, 2020a).

A reautenticação de uma sessão que ainda não atingiu seu limite de tempo pode exigir apenas um segredo memorizado ou uma biometria em conjunto com o segredo de sessão ainda válido. O verificador pode alertar o usuário para causar atividade antes do tempo limite de inatividade (GRASSI *et al.*, 2020a).

3.11.3.3 AAL3

A autenticação AAL3 deve ocorrer pelo uso de um de uma combinação de autenticadores. As combinações possíveis são (GRASSI *et al.*, 2020a):

- Dispositivo criptográfico multifator;
- Dispositivo criptográfico de fator único usado em conjunto com o segredo memorizado;
- Dispositivo multifator OTP (software ou hardware) usado em conjunto com um dispositivo criptográfico de fator único;

- Dispositivo multifator OTP (apenas hardware) usado em conjunto com um software criptográfico de fator único;
- Dispositivo OTP de fator único (apenas hardware) usado em conjunto com um Autenticador de software criptográfico multifator;
- Dispositivo OTP de fator único (somente hardware) usado em conjunto com um Autenticador de software criptográfico de fator único e um segredo memorizado.

Todos os processos de autenticação e reautenticação em AAL3 deverão demonstrar intenção de autenticação de pelo menos um autenticador (GRASSI *et al.*, 2020a).

Sobre a reautenticação periódica, em AAL3, a autenticação do assinante deve ser repetida pelo menos uma vez a cada 12 horas durante uma sessão de uso prolongado, independentemente da atividade do usuário. A reautenticação do assinante deve ser repetida após qualquer período de inatividade de 15 minutos ou mais. A reautenticação deve usar ambos os fatores de autenticação. A sessão deve ser encerrada (ou seja, desconectada) quando um desses limites de tempo for atingido. O verificador pode alertar o usuário para causar atividade antes do tempo limite de inatividade.

3.11.3.4 Resumo

O Quadro 3 resume os requisitos para cada um dos AALs citando os tipos de autenticadores permitidos, frequência da reautenticação e intenção de autenticação para cada nível de garantia:

3.11.4 Tipo de autenticador

De forma breve, esclarecemos cada tipo de autenticador recomendado pelas diretrizes do Instituto Nacional de Padrões e Tecnologia dos EUA (NIST) (GRASSI *et al.*, 2020a):

3.11.4.1 Segredos Memorizados

É um valor secreto (senha, por exemplo) que deve ser escolhido e memorizado pelo usuário. É algo que você sabe.

Quadro 3 – Resumo dos requisitos para cada um dos AALs: Tipos de autenticadores permitidos, frequência da reautenticação e intenção de autenticação para cada nível de garantia.

Requerimento	AAL1	AAL2	AAL3
Tipos de autenticador permitidos	Segredo memorizado; Segredo de pesquisa; Fora da banda; Disp. SF OTP; Disp. MF OTP; SF Crypto Software; SF Crypto Device; MF Crypto Software; Disp. de cripto. MF	Disp. MF OTP; MF Crypto Software; Disp. de cripto. MF; ou segredo memorizado e: - Pesquisar segredo - Fora de banda - Dispositivo SF OTP - Software de cript. SF - Dispositivo cript. SF	Disp. de cript. MF; Disp. de cript. SF e segredo memorizado; Disp. SF OTP e Disp. ou soft. MF Crypto; Disp. SF OTP e SF Crypto Software e segredo memorizado
Reautenticação	30 dias	12 horas ou 30 minutos de inatividade; pode usar um fator de autenticação	12 horas ou 15 minutos de inatividade; deve usar ambos os fatores de autenticação
Intenção de autenticação	Não requerido	Recomendado	Requerido

Fonte: Adaptado de (GRASSI *et al.*, 2020a).

3.11.4.2 Segredos de pesquisa

É um registro físico ou eletrônico que armazena um conjunto de segredos compartilhados entre o reclamante e o Provedor de Identidade/Credencial. Um segredo de pesquisa é algo que você possui .

3.11.4.3 Dispositivos fora de banda

Um autenticador fora de banda é um dispositivo físico endereçável exclusivamente e pode se comunicar com segurança com o verificador por meio de um canal de comunicação distinto, conhecido como canal secundário. É algo que você tem .

3.11.4.4 Dispositivo OTP de fator único

Inclui dispositivos de hardware e geradores OTP baseados em software instalados em dispositivos como telefones celulares. A OTP é exibida no dispositivo e inserida manualmente para transmissão ao verificador, comprovando a posse e o controle do dispositivo. Um dispositivo OTP de fator único é algo que você possui .

3.11.4.5 Dispositivos OTP Multifator

Um dispositivo OTP multifatorial gera OTPs para uso na autenticação após a ativação por meio de um fator de autenticação adicional. O dispositivo OTP multifatorial é algo que você possui e deve ser ativado por algo que você conhece ou algo que você é.

3.11.4.6 Software criptográfico de fator único

É uma chave criptográfica armazenada em disco ou alguma outra mídia *"soft"*. É algo que você possui.

3.11.4.7 Software de criptografia multifatorial

Já o multifatorial requer ativação por meio de um segundo fator de autenticação. A autenticação é realizada comprovando a posse e o controle da chave. É algo que você possui e deve ser ativado por algo que você conhece ou por algo que você é .

3.11.4.8 Dispositivos criptográficos de fator único

Um dispositivo criptográfico de fator único é um dispositivo de hardware que executa operações criptográficas usando chaves criptográficas protegidas e fornece a saída do autenticador por meio de conexão direta com o terminal do usuário. A autenticação é realizada comprovando a posse do dispositivo por meio do protocolo de autenticação. Um dispositivo criptográfico de fator único é algo que você possui .

3.11.4.9 Dispositivos criptográficos multifatoriais

Já os multifatoriais requerem ativação por meio de um segundo fator de autenticação. O dispositivo criptográfico multifatorial é algo que você possui e deve ser ativado por algo que você conhece ou algo que você é .

3.11.5 Requisitos Gerais do Autenticador Biométrico

O uso de biometria (algo que você é) na autenticação inclui a medição de características físicas (por exemplo, impressão digital, íris, características faciais) e características comportamentais (por exemplo, velocidade de digitação).

Existem críticas sobre o uso da biometria para autenticação. Essas críticas incluem (GRASSI *et al.*, 2020a):

- A comparação biométrica trata-se de uma probabilidade de acerto, enquanto os outros fatores de autenticação são exatos;
- As características biométricas não constituem segredos. Eles podem ser obtidos tirando uma foto de alguém com uma câmera de telefone (por exemplo, imagens faciais) com ou sem o seu conhecimento, levantados de objetos que alguém toque (por exemplo, impressões digitais latentes) ou capturados com imagens

de alta resolução (por exemplo, íris). Temos a detecção de vivacidade como um mitigador do risco de segurança.

Portanto, recomenda-se que a biometria deve ser usada apenas como parte da autenticação multifator como um autenticador físico (algo que você possui).

3.12 CONCLUSÃO

A identificação, a autenticação, a autorização e a auditoria fazem parte do gerenciamento das identidades eletrônicas e possibilitam tornar mais fáceis e seguras as diversas operações a distância.

O Brasil tem feito tentativas para uma identidade eletrônica eficiente e segura utilizando recursos reconhecidos mundialmente, mas os serviços acessados ainda são limitados.

O *OAuth 2.0* e o *OpenID Connect* foram usados pelo governo federal para a implementação da conta gov.br. São recursos eficientes e gratuitos para as etapas de autorização e autenticação das identidades eletrônicas e foram usados também no nosso projeto.

Trouxemos os conceitos gerais sobre gestão de identidade, seus diversos modelos e as etapas do ciclo de vida de identidade. Usamos a identidade médica para demonstração desse ciclo de vida e percebemos a inadequação de provedores de identidades descentralizados que não estão ligados a cada conselho de categoria profissional.

Os princípios de identificação para o desenvolvimento sustentável elaborado pelo grupo do Banco Mundial (ID4D) foram apresentados, juntamente com as várias classificações de autenticação em sistemas informatizados e os diversos fatores de autenticação. O conceito de nível de garantia mostrou-se importante com a avaliação para a definição do nível mais adequado para cada situação.

Chamaram atenção as ressalvas em considerar o fator de autenticação biométrico como seguro. Considerando a comodidade, o ambiente, o propósito e o tipo de solução necessária (autenticação sem toque), apresentaremos nos próximos capítulos alternativas seguras para a recomendação feita pelo *NIST* por haver considerações especiais na autenticação dos profissionais da saúde. Utilizaremos técnicas de minimização de riscos para conseguir o nível de garantia adequado para autenticação eletrônica em ambientes de cuidados com a saúde.

4 IDENTIDADE DOS PROFISSIONAIS DE SAÚDE

4.1 INTRODUÇÃO

Este capítulo apresenta revisão sobre os documentos de identidade, física e eletrônica, usados na área da saúde.

4.2 REGISTRO DO MÉDICO

Após a conclusão de um período mínimo de 6 anos de graduação em Medicina, o médico recém-formado com o diploma na mão, ainda não está apto para exercer a sua profissão. O Conselho Federal de Medicina (CFM), através do respectivo Conselho Regional de Medicina (CRM), é o órgão da categoria profissional onde é realizado o registro dos médicos habilitados em cada unidade da federação. É expressamente proibido, por lei, o exercício da medicina sem o devido registro nos órgãos de classe.

Para a concessão do primeiro registro, vasta documentação é exigida, entre elas o diploma original de conclusão da graduação em Medicina. A conferência da documentação leva cerca de 15 dias e, após não haver pendências, o número de inscrição para aquele Estado é liberado. O profissional recebe então uma cédula de identidade médica e está autorizado a exercer sua atividade laboral naquela unidade federativa [1].

Para iniciar o trabalho em uma instituição de saúde, seja quando presta um concurso público ou se candidata a uma vaga em hospital privado, ao assumir o cargo é necessário novamente a apresentação de toda a documentação original que comprove a titulação cabível a atividade (diploma, registro de especialista).

Qualquer organização hospitalar ou de assistência médica, pública ou privada, obrigatoriamente tem que funcionar com um diretor técnico, habilitado para o exercício da Medicina, sendo o principal responsável pelos atos médicos ali realizados (BRASIL, 1932). Segundo o CFM, é o diretor técnico o responsável por certificar-se se os médicos daquela unidade de saúde estão regularmente habilitados perante o Conselho de Medicina, bem como sua qualificação como especialista, exigindo a apresentação formal dos documentos. As cópias de toda essa documentação devem constar na pasta funcional do médico perante o setor responsável, aplicando-se essa mesma regra aos demais profissionais da área da saúde que atuem na instituição (CFM, 2016b).

Em termos práticos, o diretor técnico deve verificar a autenticidade dos di-

[1] Mais detalhes na Seção 3.5

plomas e se regularmente inscritos no CRM do Estado de atuação, além dos seus atributos. Dessa forma, coibirá o exercício ilegal da medicina por pessoas não graduadas ou que, graduadas no exterior, não tiveram seus diplomas revalidados ou que, tiveram seu registro profissional cassado por infração, ou ainda, que se apresentem como especialistas mas não tenham seu certificado registrado no CRM (CFM, 2016b).

Ao iniciar o trabalho, a identificação do médico e demais profissionais da saúde em hospitais públicos e privados não se dá rotineiramente através da apresentação da sua cédula de identidade profissional. É o crachá que na maioria das vezes faz esse papel. Tal instrumento, muitas vezes é útil para o registro da assiduidade do profissional, e também libera a entrada do mesmo na instituição onde há um controle deste acesso. Às vezes, esse controle é feito pelo reconhecimento da digital do profissional, tentando assim evitar que seja dependente de cartão que pode ser extraviado ou usado por terceiros.

Porém, uma parte dos médicos, odontólogos, nutricionistas, psicólogos e fisioterapeutas, por exemplo, atendem em consultório particular, desvinculado de qualquer clínica, sendo ele mesmo, o seu próprio responsável técnico. Nesses casos, habitualmente não há apresentação de documentação que comprove habilitação profissional e especialidade registrada nem mesmo para os pacientes. O profissional é o responsável pelo que divulga ser e inclusive pelas informações que constam nos seus documentos impressos (receituário médico, cartão de visita, entre outros impressos).

4.3 IDENTIFICAÇÃO DO MÉDICO

O Conselho Federal de Medicina (CFM) normatizou a identificação dos médicos através da Resolução 2.069/14 (CFM, 2014), alterada pela Resolução 2.119/15 (CFM, 2015).

Para que o paciente tenha o direito de saber quem irá atendê-lo e a formação desse profissional, o Conselho Federal de Medicina (CFM) padronizou a forma de identificação dos médicos nas unidades de assistência médica e de hospitalização no país. A resolução padroniza placas, impressos, vestimentas, crachás, carimbos e demais utensílios utilizados tanto nos serviços de saúde públicos quanto nos privados (CFM, 2015):

"*É dever do médico, quando em serviço em seus locais de trabalho, se identificar como MÉDICO, em tipo maiúsculo, quando detentor apenas da graduação e, quando especialista registrado no CRM, acrescer o nome de sua ESPECIALIDADE, também em tipo maiúsculo*", define a norma.

Sobre a propaganda do profissional e o que ele divulga ser, de acordo com o CFM, os anúncios médicos deverão conter, obrigatoriamente, os seguintes dados (CFM, 2011):

a) Nome do profissional;

b) Especialidade e/ou área de atuação, quando registrada no Conselho Regional de Medicina;

c) Número da inscrição no Conselho Regional de Medicina;

d) Número de registro de qualificação de especialista (RQE), se o for.

Para conferir se os dados divulgados pelos profissionais são reais, atuais e oficialmente reconhecidos, o CFM mantém um repositório, que pode ser livremente acessado a partir de um *site*, contendo o nome e o número de registro de todos os médicos habilitados no Brasil. Também contém o registro de especialista dos médicos que fizeram Residência Médica e/ou que possuem Título de Especialista em determinada área (obtido através de uma prova que valida profundo conhecimento naquela especialidade).

Nos últimos anos, com o recadastramento dos médicos em todo o país, o *site* do CFM também tem apresentado uma foto da maioria dos profissionais ativos, o que não tem se repetido no *site* de alguns conselhos regionais (a prática ainda não foi adotada pelo CREMESC, por exemplo).

4.4 PRESCRIÇÃO MÉDICA E O CARIMBO

São várias as situações na prática médica, quer para fins de diagnóstico, prognóstico, tratamento, comunicações e encaminhamentos, em que o profissional tem a necessidade de assinar documentos, conferindo-lhes legitimidade e validade (FONTASA-ROSA *et al.*, 2011).

O tratamento das doenças muitas vezes necessita da prescrição médica de fármacos e terapias coadjuvantes e isso é parte do ato médico. A prescrição médica constitui um documento médico que, para a maioria dos pacientes, é o resultado mais esperado da consulta médica. A aposição do carimbo com os dados do profissional, nestas situações, tem o objetivo de identificar o médico e validar o documento. A assinatura do médico nem sempre é legível e o documento impresso muitas vezes é institucional e não contém os dados de identificação do profissional.

Porém, culturalmente existe uma hipervalorização da aposição do carimbo em todos os documentos médicos, principalmente nas prescrições. Acredita-se que os documentos não são válidos quando não os possuem. Até mesmo o farmacêutico, profissional habilitado para a dispensação dos medicamentos, muitas vezes acredita não ser autêntico o documento quando não carimbado, mesmo quando apresenta a assinatura médica, o nome do profissional e o seu número do CRM do Estado atuante.

Ao reconhecer a suposta autenticidade que o carimbo médico confere aos documentos e prevendo atos ilícitos, o *"Manual de orientações básicas para prescrição médica"* traz a seguinte recomendação obre os cuidados com o carimbo:

> *O médico não deve deixar seu carimbo na instituição de saúde ou outro local, para evitar o desvio de sua finalidade ou facilitar validação indevida de atos profissionais não cometidos pelo mesmo* (CRM-PB, 2011, Pág. 45).

Sob o ponto de vista ético e legal, não existe obrigatoriedade da utilização do carimbo em documentos médicos no âmbito nacional. A exceção fica por conta da utilização do carimbo em situações específicas, como nos casos das Notificações de Receita de entorpecentes (carimbo padronizado no campo “Identificação do Emitente”), nas requisições de Notificação de Receita, e nos Termos de Responsabilidade para prescrição de Talidomida (FERREIRA, 2014; MS, 1998).

Na expressão da lei, para as denominadas receitas simples, personalizadas ou não, existe a obrigatoriedade da assinatura do profissional e identificação de seu número de inscrição no respectivo Conselho Profissional. O mesmo vale para outros documentos como declaração de óbito e atestado médico para afastamento laboral.

Deve ser lembrado que, para um fraudador, não há nada de complexo em confeccionar e imprimir receituários com todos os dados de um médico legalmente habilitado (dados facilmente encontrados no *site* do CFM) e mandar fabricar um carimbo com esses mesmos dados.

4.5 FORMULÁRIOS E SISTEMAS INFORMATIZADOS

Outra questão importante diz respeito ao que o profissional tem permissão para realizar em cada uma das instituição de saúde que trabalha e em que situação pode usar os impressos daquela entidade de saúde. Os formulários ainda em papel permitem que o médico, por exemplo, prescreva para um paciente particular em receituário de uma instituição pública. Isso inclusive constitui infração ética, segundo o Art. 82, Capítulo X, do Código de Ética Médica.

> *Art. 82. Usar formulários de instituições públicas para prescrever ou atestar fatos verificados na clínica privada* (CFM, 2009).

Quando o sistema de atendimento é informatizado, muitas vezes são necessárias múltiplas senhas para os vários sistemas (laboratório, prontuário eletrônico, exames de imagem). A senha realiza o papel de controle de acesso ao que pode ser visualizado e realizado pelo profissional, além de tentar promover a segurança na entrada dos sistemas. Com múltiplas senhas para acessar e realizar seu trabalho, resta ao médico a escolha de senhas de baixa qualidade para facilitar a memorização ou o registro escrito delas, que podem ser criminosamente utilizados por terceiros.

Também existem situações em que há um intercâmbio das senhas entre os colegas de profissão para o registro de atividades realizadas em equipe, situação que também deve gerar insegurança para todos os envolvidos.

4.6 INFRAÇÕES MÉDICAS

Quando o médico comete algum ato irregular no exercício da profissão, está sujeito às penalidades impostas pelo seu Conselho. Salienta-se que grande parte das penalidades tem sua investigação e punição em caráter sigiloso ou divulgada apenas em publicações específicas da categoria médica. Portanto, o público em geral conhece muito pouco quem são os médicos infratores.

As penas disciplinares aplicáveis pelos Conselhos Regionais estão descritas na lei 3.268/57, artigo 22, respeitando uma ordem de gradação. São elas: advertência confidencial em aviso reservado; censura confidencial em aviso reservado; censura pública em publicação oficial; suspensão do exercício profissional até 30 (trinta) dias; cassação do exercício profissional, *ad referendum* do Conselho Federal (CFM, 2016a, 2017, 2020e,f).

Apenas os médicos suspensos ou cassados (punição irreversível) têm a sua carteira profissional e cédula de identidade médica apreendida.

Mas a carteira profissional e a cédula de identidade médica não são habitualmente solicitadas durante o atendimento médico. Os profissionais cassados continuam a ter conhecimento na área e podem continuar atuando de forma irregular. Em setembro de 2019, a Polícia Militar prendeu um ex-médico, de 70 anos, que trabalhava com seu registro do CRM cassado e vendia atestados médicos em um consultório particular no centro de Belo Horizonte/MG. O ex-médico usava carimbos de outros profissionais em atividade médica regular (FONTES, 2019).

Para ter alguma segurança sobre a habilitação do médico que prestou o atendimento, o público pode consultar os *sites* dos conselhos de medicina para verificar se o registro no CRM do profissional está ativo e se a foto divulgada corresponde a fisionomia do médico consultado. O médico inativo pode ser um médico que solicitou transferência para atuação em outro Estado, que não exerça mais a medicina por escolha pessoal ou o médico cassado por infração gravíssima.

4.7 FALSO MÉDICO NOS DIAS ATUAIS

Também existem vários criminosos que exercem a medicina sem formação para tal. Em 2006, no *site* do CREMESP (Conselho Regional de Medicina de São Paulo), já encontramos relatos de sugestões para coibir a identificação dos falsos médicos. Naquele ano, um homem de 22 anos foi preso em flagrante atuando como médico ilegalmente. Ele se fez passar por médico em três clínicas da zona norte da Capital e em Guarulhos, usando números de CRM de médicos encontrados no site do próprio CREMESP. O homem falsificou, grosseiramente, o diploma universitário e a carteira de médico, e conseguiu atuar durante duas semanas (CREMESP, 2006).

Após o caso relatado e diversos outros semelhantes, o CREMESP propôs um novo modelo para carteira de médico (com tecnologia digital) e preparou o recadastramento dos profissionais em todo o Estado de São Paulo com o objetivo de evitar as falsificações de documentos. Também sugeriu a inclusão de fotos dos profissionais no Guia Médico do site do Conselho (CREMESP, 2006).

As sugestões foram acatadas pelo CFM, mas os casos de falsos médicos continuam acontecendo nos dias atuais, inclusive com criminosos atuando em instituições hospitalares.

Em 31/05/2020, um homem foi preso pela Polícia Federal acusado de se passar por médico e atender pacientes com COVID-19, no Hospital Municipal Irmã Dulce, localizado em Praia Grande/SP. Ele usava os documentos de um médico oftalmologista que atua na Colômbia (REDAÇÃO JORNAL DE BRASÍLIA, 2020).

Este caso surpreendeu pois o falso médico trabalhava no referido hospital há pelo menos um ano. A suspeita ocorreu quando as autoridades perceberam que sua identidade médica apresentava um homem branco, enquanto que o falsário era negro. A polícia constatou que o verdadeiro médico registrou boletim de ocorrência notificando o desaparecimento de seus documentos. Já a direção do hospital tentou se eximir da responsabilidade e alegou que o homem era funcionário de uma empresa médica que presta serviços ao hospital (REDAÇÃO JORNAL DE BRASÍLIA, 2020).

4.8 DOCUMENTOS FALSOS

Carteiras de identificação médica, receituários médicos, carimbos e diversos outros formulários e documentos de uso exclusivo do médico podem ser facilmente extraviados, produzindo vasta documentação falsa e até mesmo contratação de profissional não-habilitado como visto na seção anterior.

Porém, também existem os documentos médicos verdadeiros que foram adulterados posteriormente.

Embora não seja listado pelo Código de Ética do CFM, uma empresa ou um empregador também pode lidar com um atestado adulterado que, inicialmente, não era falso. Acontece quando o funcionário realmente passa por um atendimento médico e recebe um atestado condizente com sua situação, mas tenta tirar proveito rasurando e ampliando o período de afastamento. Outra situação possível é quando o trabalhador tenta usar um atestado de outro mês ou até outro ano para justificar uma ausência recente (BARROS, 2020).

Percebe-se então que o carimbo médico, a assinatura manual e o papel timbrado não garantem a integridade do conteúdo quando o texto é habilmente modificado.

4.9 TELEMEDICINA

Em tempos de pandemia, as consultas médicas presenciais passaram a ser dificultadas pela orientação de isolamento social. Principalmente durante o ano de 2020, apenas aqueles pacientes com sintomas emergenciais estavam enfrentando o risco de sair de casa para ir até uma instituição hospitalar ou clínica médica. A chance de encontrar, no caminho ou na entrada do consultório, com algum paciente apresentando sintomas respiratórios ainda é alta.

Assim, o Ministério da Saúde, após iniciada a pandemia pelo Coronavírus, tomou uma série de medidas emergenciais, visando a diminuição do deslocamento da população para unidades de saúde que são locais com alto risco de contágio. Através de dispositivos administrativos e legais, autorizou o uso da Telemedicina no Brasil, tanto na rede pública quanto privada, em caráter emergencial, contemplando inclusive a emissão de receitas e atestados médicos à distância (MS, 2020; BRASIL, 2020a).

A telemedicina é a prática médica à distância, a partir do uso da tecnologia da informação. É disciplinada pelo CFM (CFM, 2019b, 2002, 2019a), além de também já estar prevista no Código de Ética Médica a possibilidade de prescrição de tratamento ou outros procedimentos sem exame direto - ou seja, presencial - do médico com o paciente, em caso de urgência ou emergência.

A telemedicina tem avançado na sua regulamentação a passos largos. Com o avanço, os poucos profissionais da saúde que não usavam recursos de informática no exercício da sua profissão, depararam-se com a dependência do mundo digital. Foram cobrados inclusive pelos próprios pacientes que se interessaram por um atendimento à distância de forma imediata e na segurança do seu lar.

As principais vantagens da telemedicina são (GODINHO, 2021; LIMA E SILVA, 2020; EDITORIAL, 2020):

Acessibilidade: Consegue fornecer atendimento médico em áreas de difícil acesso e também aos pacientes que apresentam risco no deslocamento ou no contato com ambientes hospitalares;

Custos menores: Diminui a necessidade de uma grande infraestrutura para contar com os laudos, prescrições e prontuários médicos. Tudo está e pode ser consultado de forma *online* na rede a partir de uma solução na nuvem, sem a necessidade de fazer impressão e ter uma grande cadeia logística. Além disso, não é preciso manter um corpo clínico disponível em tempo integral para casos não emergenciais, e assim podem arcar com os custos conforme a demanda de pacientes e exames do dia;

Otimização do tempo e processos: Menos burocracia até no acesso de exames pelos profissionais. Não há a necessidade de deslocamento do paciente para as unidades de saúde para pegar laudos ou prescrições. Além disso, o próprio médico pode laudar à distância, agilizando a entrega dos exames com diagnósticos. Isso também diminui os erros de diagnósticos, já que os exames ficam disponíveis a mais de um médico para análise;

Maior segurança no armazenamento dos documentos: Reduzem os riscos de perda de papéis e prontuários físicos - e no acesso a eles.

Um ponto bem comentado sobre a prática de prescrições e atestados médicos é a fraude. Na telemedicina e com a assinatura digital é possível comprovar a identidade do médico prescritor no sistema e eliminar a necessidade de assinar à mão folhas e mais folhas de papel para que as suas orientações tenham a validade necessária (EDITORIAL, 2020).

Para assinar digitalmente uma receita de controle especial, o médico precisa contar com um certificado digital. O certificado digital equivale a uma carteira de identidade do mundo virtual, garantindo a identidade de um indivíduo ou instituição, sem necessidade de apresentação presencial (LIMA E SILVA, 2020). Porém, essa

identidade do prescritor não vem acompanhada de atributo como sua formação e especialidade.

Protegidos por criptografia e com prazo de validade pré-determinado, a certificação digital pode ser armazenada em um pendrive, smartcard, ou em uma nuvem (BRASIL, 2001).

No Brasil, o sistema de certificação digital foi adotado em 2001 com a instituição da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). A ICP-Brasil garante a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras (BRASIL, 2001).

Devido ao modelo adotado e aos custos relacionados, esta abordagem ainda não logrou êxito efetivo no processo de identificação virtual das pessoas físicas. Vejamos: em uma população de cerca de 210 milhões de pessoas físicas, somente cerca de 4 milhões têm certificado digital. Esses números demonstram a necessidade de que o Estado brasileiro busque uma alternativa para massificação das identidades eletrônicas (ARAÚJO, 2020).

A assinatura digital qualificada é gerada por meio de certificados e chaves emitidos pela ICP-Brasil. Para obtê-la é preciso escolher uma das Autoridades Certificadoras (AC) credenciadas à ICP-Brasil (como o Serviço Federal de Processamento de Dados - Serpro, a Caixa Econômica Federal ou a Receita Federal) que emitem o certificado digital. As ACs são entidades públicas ou privadas que estabelecem previamente a identidade do futuro portador do certificado digital por meio dos documentos necessários (através da Autoridade de Registro) e emitem o certificado (DOCUSIGN, 2020; ARAÚJO, 2020). É a Autoridade de Registro (AR) que promove a interface entre o usuário e uma AC. Ela é a responsável pela conferência de toda a documentação da identidade do usuário e é quem envia a requisição do certificado para a AC.

A Assinatura Digital, a Certificação Digital, o Prontuário Eletrônico do Paciente (PEP) e a adoção do CRM Digital figuram na lista das importantes inovações tecnológicas que surgiram para facilitar a rotina na área da saúde, reestruturando o trabalho médico (DOCUSIGN, 2020).

Quando a ICP-Brasil foi instituída, a Certificação Digital – com as prerrogativas de validade jurídica – abriu caminho para que diversos tipos de documentos fossem assinados em formato digital. Sistemas foram criados para coletar as assinaturas digitais e a todos se apresentou o desafio de validação semântica da assinatura digital. As aplicações tiveram que tratar informações (atributos) sobre os proprietários dos

certificados digitais por meio de integrações e/ou replicações de dados. O Certificado de Atributo Digital é uma tecnologia bastante estudada e documentada mundialmente, mas nunca foi usado num contexto tão grande como o criado pela ICP-Brasil (CERTFORUM, 2007).

Um Certificado de Atributo Digital é um documento eletrônico que apresenta qualidades associadas a uma pessoa (cargo, função, profissão) ou organização identificada por meio de um Certificado Digital (CERTFORUM, 2007).

Portanto, em uma prescrição médica, a assinatura eletrônica validada com um certificado digital pessoal apenas confirma que aquele que assinou é mesmo o *"João"*, mas não afirma que o João é médico. Apenas acrescentando um certificado de atributo para essa confirmação.

4.10 CRM DIGITAL

Esta foi a última ação do CFM para melhorar a confiabilidade e autenticidade dos documentos médicos: a normatização da Cédula de Identidade Médica (CIM) dos profissionais inscritos nos Conselhos Regionais de Medicina nas suas versões em cartão (CRM Digital) e para dispositivos móveis (E-CRM) (CFM, 2019c).

O CRM Digital é a versão tecnológica da identidade do médico. É confeccionada em cartão rígido e possui sistema antifraude, com chip criptográfico para certificação digital (CFM, 2020b).

A Figura 5 ilustra a Cédula de Identidade Médica.

Figura 5 – Cédula de Identidade Médica.

Fonte: (CFM, 2020b)

A certificação digital dificulta a falsificação já que a leitura de informações é feita por dispositivos eletrônicos de segurança, com a gravação de dados cadastrais de acordo com o padrão ICP-Brasil (CFM, 2020b).

O certificado digital pode ser utilizado tanto para uso profissional quanto para uso pessoal pelos médicos.

a) Uso profissional (CFM, 2020b).

   i) Aderir aos sistemas de Prontuário Eletrônico do Paciente (PEP), por meio de certificação digital;

   ii) Assinar documentos da rotina da prática médica;

   iii) Serviços do sistema do Conselho de Medicina no Portal Médico que serão disponibilizados. Para isso, é necessária a certificação digital.

b) Uso pessoal (CFM, 2020b).

   i) Enviar declarações de impostos pela internet;

   ii) Recuperar informações sobre histórico de declarações;

   iii) Assinar contratos digitais;

   iv) Consultar situação fiscal e cadastral na Receita Federal;

   v) Gerar procurações eletrônicas;

   vi) Acesso online a certidões e serviços da Receita Federal;

   vii) Transações bancárias e online.

Em termos legais, o CRM Digital já está amplamente instituído como documento oficial pelo Conselho Federal de Medicina (CFM) (CFM, 2012). Esse recurso possibilita que o médico valide e libere documentos por meio de uma assinatura digital, e com o mesmo valor legal de um documento em papel (DOCUSIGN, 2020).

O CRM Digital oferece uma série de benefícios, mas trata-se também de uma cartão físico com senhas/códigos. Portanto alguns pontos merecem atenção (CFM, 2020b):

a) A nova cédula de identidade médica não deve ser plastificada para não comprometer a imagem latente, um dos itens de segurança de suma importância do novo documento;

b) Nunca emprestar a cédula/certificado digital para terceiros (secretária/estagiário);

c) O CRM Digital tem validade jurídica, é pessoal e intransferível e deve ser usado somente pelo titular. Guardar o *PIN/PUK* [2] em local seguro para que não seja copiado ou usado por terceiros;

d) Ter atenção ao digitar o *PIN/PUK* para que não seja bloqueado. Caso isso ocorra, será necessário comprar um novo certificado digital;

e) Não emita um certificado digital fora da hierarquia da ICP-Brasil, pois não tem validade jurídica no Brasil.

Essa nova modalidade de documentos não exclui nem se sobrepõe aos documentos utilizados atualmente. São equivalentes e isonômicos. Isto é, o sistema de certificação eletrônica não introduz conceitos novos nas transações, apenas estabelece equivalência e isonomia legal entre os documentos produzidos e obtidos eletronicamente e os documentos firmados em papel, desde que certificados na ICP-Brasil (CFM, 2020b).

4.11 E-CRM

O Conselho Federal de Medicina (CFM) determinou que os Conselhos Regionais de Medicina adotarão progressivamente as novas Cédulas de Identidade Médica (CIM) nas versões física e digital (CFM, 2019c).

A CIM E-CRM, versão para dispositivo móvel, é fornecida exclusivamente pelo Conselho Federal de Medicina, mediante emissão da CIM CRM Digital, em cartão (CFM, 2019c).

Essa versão requer uso de um aplicativo[3], possui componentes de segurança que protegem a identidade do médico e tem as mesmas informações expressas no CRM Digital (CFM, 2020a).

O referido aplicativo tem como uma de suas funções o gerenciamento da Carteira de Identidade Médica Digital (E-CRM), com a instalação e conferência de sua autenticidade por meio da leitura de um código de resposta rápida (QR Code[4]), além de possibilitar a emissão e o armazenamento de seu certificado digital ICP-Brasil e outras funcionalidades.

[2] PIN – Personal Identification Number – senha utilizada para acessar o certificado digital armazenado no cartão ou *token* e PUK – Personal Identification Number Unbloking Key – senha usada para desbloqueio da senha PIN.

[3] aplicativo CREDENCIAL MÉDICA, disponível para dispositivos móveis Android ou IOS.

[4] do Inglês Quick Response (QR) Code.

A E-CRM é baseado no uso de certificado de atributo. A associação de um Certificado Digital (que estabelece a identidade do cidadão no mundo virtual) ao Atributo (que qualifica o cidadão identificado) abre a oportunidade de regular o uso das novas tecnologias na área médica para identificar os profissionais de forma segura e íntegra (CFM, 2019c).

Ele inclui dados biográficos (que registram informações históricas como nome, CRM, data de nascimento, filiação, entre outros) ou biométricos (que apresentam características físicas, tais como digitais, fotografias, íris, entre outros).

A ideia é que o E-CRM seja um instrumento importante para estabelecer um canal seguro para comutar informações entre meios humanos e tecnológicos. Pode permitir verificar e impedir que determinadas pessoas utilizem documentos falsos para personificar um médico já que por meio do aplicativo exclusivo do Conselho Federal de Medicina (CFM), a identidade do médico e seus atributos poderão ser autenticados eletronicamente (CFM, 2019c, 2020a).

4.12 DOCUMENTOS MÉDICOS EM MEIO ELETRÔNICO

Além das alterações na rotina médica, a Era Digital impacta visivelmente as relações que envolvem os processos administrativos e a interação entre hospitais, empresas parceiras e pacientes (DOCUSIGN, 2020).

Em meio as inovações tecnológicas alavancadas pela pandemia do COVID-19, o Conselho Federal de Medicina (CFM), o Instituto Nacional de Tecnologia da Informação (ITI) e o Conselho Federal de Farmácia (CFF) lançaram a plataforma “Prescrição Eletrônica” (CFM, 2020d).

O projeto auxilia a relação remota entre médico, paciente e farmacêutico, com a possibilidade do paciente receber prescrições diretamente no celular, sem uma via em papel, e ter o documento conferido, via plataforma, diretamente no balcão da farmácia (CFM, 2020d).

A plataforma conta também com o direcionamento para um Validador de Documentos (ITI, 2020) que valida prescrições médicas (formato PDF) quanto a sua autoria, se assinada por um médico habilitado e se dispensada por um farmacêutico. Permite, ainda, verificar a integridade do documento assinado com certificado digital ICP-Brasil.

A forma de funcionamento está representada na Figura 6 e é a seguinte (ITI, 2020):

a) O médico realiza o download dos modelos de receita, atestado ou relatório no site do CFM. Posteriormente realiza o preenchimento, assina digitalmente utilizando um certificado ICP Brasil por meio da ferramenta Adobe Acrobat e envia o arquivo assinado ao seu paciente.

b) O paciente envia o arquivo à parte interessada, que valida o documento por meio do validador de documentos.

c) Caso seja uma receita, o farmacêutico fará a dispensação desta receita, assinando-a digitalmente e registrando-a junto ao Registro de Dispensação.

Figura 6 – Validação da prescrição

Fonte: (CFM, 2020d).

Assim, a plataforma garante a segurança do sigilo profissional, pois os dados do paciente ficam resguardados. Nenhuma informação de conteúdo do documento validado é armazenada pela aplicação ou repassada a terceiros (ITI, 2020). Além disso, também há a defesa do ato médico, uma vez que a prescrição não pode ser feita por outros profissionais.

Para utilizar a ferramenta, o médico deve possuir uma assinatura eletrônica, já descrita anteriormente. De acordo com a Anvisa, a assinatura digital com certificados ICP-Brasil deve ser utilizada nas receitas de controle especial e nas prescrições de antimicrobianos.

As receitas de controle especial são aquelas utilizadas para medicamentos que contenham substâncias das listas C1 e C5 e dos adendos das listas A1, A2 e B1 da Portaria n^{o} 344 de 1998 da Secretaria de Vigilância em Saúde do Ministério da Saúde (MS, 1998).

A possibilidade de assinatura digital com certificação ICP-Brasil não se aplica a outros receituários eletrônicos de medicamentos controlados, como os talonários de Notificação de Receita A (NRA), Notificação de Receita Especial para Talidomida, Notificação de Receita B e B2 e Notificação de Receita Especial para Retinoides de uso sistêmico (CFM, 2020c).

Também é importante frisar que, posteriormente a criação da citada plataforma, os CRMs de cada Estado se mobilizaram para a criação de seu próprio espaço de prescrição médica. Atualmente, o site do CRM/SC já conta com o portal para confecção dos documentos médicos, inclusive para prescrição de medicação de controle especial. Nele, é possível realizar a prescrição de antimicrobianos, por exemplo, porém sem a exigência do certificado digital, usando apenas a assinatura simples, gerando um documento com *QR Code*. Percebe-se com isso que as tecnologias ainda estão sendo testadas no mundo da documentação médica digital, em seus diferentes níveis de segurança.

4.13 CONCLUSÃO

A forma de identificação do médico com o uso do jaleco branco e do estetoscópio no pescoço, aos poucos, está ficando para trás. Com a telemedicina no país, o contato através da tela trouxe dúvidas sobre quem de fato está se apresentando como médico.

A Identidade Médica evoluiu com a adoção do CRM Digital e do e-CRM. A versão atual traz a possibilidade do uso do certificado digital pessoal e do certificado de atributos. Mas mesmo na telemedicina, ela não é usada durante a consulta médica, nem na identificação do profissional, autenticação em sistemas ou prescrição médica.

Na prescrição eletrônica (usada não só na telemedicina) há diferentes formas de confecção dos documentos, principalmente das medicações de controle especial. A plataforma do CFM e dos CRMs mostram que a segurança das assinaturas (simples e qualificada) não é a mesma e o processo burocrático da validação do documento ainda pode evoluir.

5 IDENTIDADE ELETRÔNICA PARA PROFISSIONAIS DA SAÚDE

5.1 INTRODUÇÃO

O trabalho do profissional da saúde deve ter seu foco permanentemente nas questões técnicas sobre a manutenção ou reestabelecimento da saúde dos pacientes. Não deve haver espaço nessa rotina diária para a preocupação em como acessar e se autenticar nos sistemas informatizados necessários para a sua prática laboral ou qual tipo de assinatura usar na sua prescrição eletrônica.

Lembrar login e senhas, repetir credenciais a cada passo avançado e lidar com essa burocracia que tenta ser justificada pela segurança não devem fazer parte da rotina do médico. Em uma emergência hospitalar, por exemplo, o que importa é definir as condutas para manter a vida do paciente e não lembrar a senha para acesso ao sistema.

Porém, a identidade digital é algo complexo. Provar que alguém é quem ele diz ser - especialmente remotamente, por meio de um serviço digital - é repleto de oportunidades para um invasor se passar por alguém com sucesso (GRASSI *et al.*, 2020b).

5.2 MODELO PROPOSTO

Um provedor de identidades, como já definimos, é o responsável pela organização que gera e fornece uma identidade digital a um usuário. Esse usuário se autenticará a fim de obter acesso aos serviços fornecidos por um provedor de serviços.

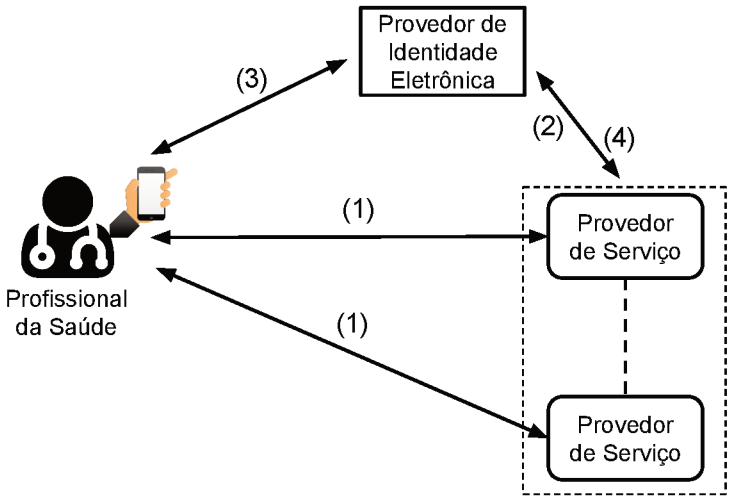
O Conselho Federal de Medicina (CFM) é o possuidor dos dados fiéis para uma identidade médica segura. Portanto, nossa proposta contempla um provedor de identidade ligado ao CFM. Todos os dados dos usuários (médicos) e a gestão do ciclo de vida da identidade passarão a ser administrados por um único provedor de identidade.

O modelo do provedor de identidade será de um provedor único, centralizado, permitindo uma autenticação única. Este provedor de identidade pode se conectar a vários outros provedores de serviço como mostra a Figura 7.

A Figura 7 ilustra como o profissional de saúde irá usar a sua identidade eletrônica para acessar os mais diversos serviços eletrônicos.

A proposta é uma identidade médica fornecendo identificadores, credenciais e atributos. A identidade médica eletrônica deve estar sempre disponível ao profissional,

Figura 7 – Provedor de Identidade Eletrônica.



Fonte: Própria autora.

deve ser de fácil acesso, segura e sem custo.

Propomos também mudar a forma de autenticação médica nos sistemas para um processo sem o toque de mãos/digitais, evitando assim a contaminação nas superfícies.

Propomos métodos de autenticação com níveis de garantia. A autenticação em dois fatores é uma alternativa para trazer segurança ao processo, tendo como credenciais possíveis um fator biométrico sem toque e a presença de um token, por exemplo.

Trabalhamos em um *framework* para que todo o processo ocorre em nuvem computacional e que a autenticação, autorização e a comunicação entre os provedores de identidade e de serviços sejam invisíveis para o médico.

Da mesma forma que deve ser simples para o profissional da saúde, deve ser simples para o paciente. Acreditamos que toda a documentação necessária para que o doente cuide da sua saúde deve estar disponível também na nuvem, de maneira personificada e sigilosa. Através de um *QR Code*, ele poderá apresentar a documentação médica para um farmacêutico, para o fisioterapeuta ou para qualquer outro profissional que ele necessitar, com segurança da autenticidade e integridade do documento. O paciente deve receber e ter disponível o documento médico (prescrição, laudo, solicitação de exames) na nuvem.

5.3 PRINCÍPIOS DA IDENTIFICAÇÃO

Seguindo os três pilares que norteiam os princípios de identificação para o desenvolvimento sustentável, segundo o ID4D (Seção 3.2), o *framework* proposto visa o seguimento de todos os pilares na concepção de uma identidade eletrônica. Vejamos:

No aspecto da **inclusão**, atualmente, o uso do certificado digital para a assinatura dos documentos médicos traz custo aos profissionais. Isso pode ser resolvido com a emissão de certificado digital sob demanda pelo próprio CFM, entidades responsáveis pela identidade médica eletrônica. A falta de habilidade com a tecnologia de alguns profissionais também é um fator dificultador para o modelo atual, que exige que o usuário manuseie certificados digitais e chaves privadas. Dessa forma, um sistema que emita certificados sob demanda para assinatura de documentos médicos naturalmente exige autenticação segura. Por fim, tal sistema traria um processo intuitivo e desburocratizado, aprimorando a experiência do usuário.

No pilar do **design**, teremos como garantir que os dados de identidade sejam precisos e atualizados já que o provedor de identidade será único e ligado diretamente ao Conselho Federal de Medicina (CFM) e seus respectivos representantes regionais. Trará mais segurança na identificação médica, garantindo também a singularidade dessa identidade.

A identificação eletrônica proposta passará a ser útil para os órgãos públicos e entidades do setor privado (provedores de serviços) para identificação e autenticação desses profissionais da saúde nos diversos sistemas informatizados. A interoperabilidade será alcançada com um único provedor de identidade se comunicando com os diversos provedores de serviço. Utilizando um padrão aberto, será possível trazer melhoria sempre que necessário, gerando também longevidade do método.

Em relação ao pilar da **governança**, sendo o CFM o responsável direto pelo provimento da identidade médica, todas as modificações e atualizações de atributos e credenciais serão facilitados, ocorrendo administrativamente, sem necessidade de envolvimento da justiça. Qualquer queixa do profissional deverá ser referenciada ao seu órgão de categoria profissional, o qual também rege eticamente a sua profissão. Como os dados da identidade com todas as suas credenciais e atributos são conhecidas, registradas e protegidas originalmente pelo CFM, o risco de vazamento de dados indesejados é bem menor do que hoje, onde cada instituição de saúde é responsável pela identificação e autenticação dos seus profissionais.

5.4 DIFERENCIAIS NO CICLO DE VIDA DA IDENTIDADE

Sobre o ciclo de vida da identidade apresentado na Seção 3.5, a nossa proposta apresenta as seguintes vantagens:

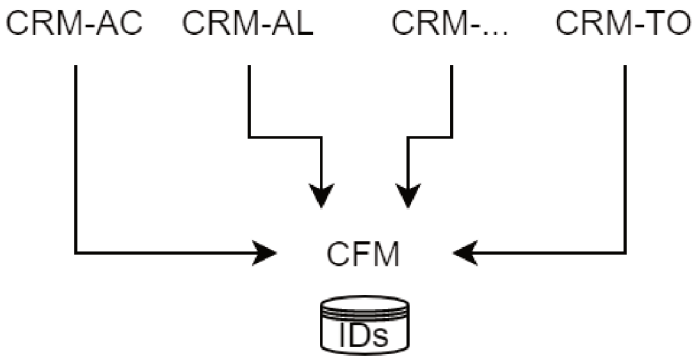
5.4.0.1 Cadastro

Todos as credenciais e atributos colhidos no cadastro inicial do médico poderão ser plenamente utilizadas para autenticação e autorização nos diversos sistemas informatizados, estando concentrados em um único provedor de identidade, facilitando a gestão desses dados e cuidados relacionados a LGPD.

Salientamos que um mesmo médico pode possuir vários cadastros com números de CRMs (identificadores) em vários Estados diferentes simultaneamente, mas a identidade do médico é única (ele é uma única pessoa). Esclarecemos que os Conselhos Regionais de Medicina de cada Estado são os responsáveis por realizar o cadastro/inscrição e, a partir daí, fornecer os dados atualizados e conferidos ao CFM. Na proposta deste trabalho, o provedor de identidade único está centralizado no CFM que é alimentado pelos diversos CRMs.

A Figura 8 ilustra a relação entre o CFM como provedor de identidade centralizado e os diversos CRMs fornecedores das inscrições regionais.

Figura 8 – Provedor de Identidade Eletrônica único, centralizado no CFM, sendo alimentado pelos diversos CRMs de cada Estado.



Fonte: Própria autora.

5.4.0.2 Emissão

Nada mais prático e seguro que a instituição central responsável pelo cadastro/registro inicial do médico (através das suas representantes regionais) seja o seu provedor de identidade. É o conselho da categorial profissional que controla, em tempo real (sem o *delay* da atualização de um certificado de atributo, por exemplo),

os novos registros médicos de especialidade e todas as *"interrupções de autorização"* para exercer a medicina devido a punições proferidas pelos conselhos por má prática profissional.

O *framework* apresentado nesta dissertação independe da emissão de cartão físico pois a identidade médica estará em nuvem, com toda a segurança necessária, sem custo e de fácil acesso. Ela será automaticamente atualizada com mudança de atributos e credenciais sempre que houver pois estará diretamente ligada ao órgão responsável por validar o exercício legal da profissão.

5.4.0.3 Autenticação

Nossa proposta traz a análise do nível de garantia adequado para o processo de autenticação para profissionais da saúde com o número necessário de fatores de autenticação e com as características ideais para atividades em ambientes de cuidado com a saúde.

5.4.0.4 Autorização

A autenticação bem-sucedida pode permitir que um médico prove sua identidade ao entrar no sistema informatizado de um hospital, por exemplo, mas a decisão de autorizá-lo a acessar, analisar e laudar as imagens radiológicas pode exigir por, parte da instituição, a verificação de informações adicionais (por exemplo, se o médico é especialista em radiologia). A autorização para acessar determinados serviços médicos traz segurança em uma unidade de saúde pois o gestor técnico daquela instituição pode selecionar quais profissionais tem acesso ou responsabilidade sobre qual serviço especializado dependendo da sua qualificação profissional (atributos).

A identidade eletrônica, tendo como provedor de identidade o próprio conselho da categoria de profissional da saúde, trará todos os atributos possíveis e necessários para o processo de autorização nos sistemas informatizados, seja baseado na *expertise* (experiência e formação) do profissional ou na posição funcional que ele ocupa na instituição, por exemplo. O provedor de serviço terá disponível um provedor de identidade único, acessível e seguro.

5.4.0.5 Gestão

Com o provedor de identidade centralizado e responsável por todo o ciclo de vida da identidade, o CFM/CRM pode atestar de forma dinâmica os vários atributos necessários para a prática médica, trazendo segurança para os diversos provedores de serviço.

5.5 AUTENTICAÇÃO E NÍVEL DE GARANTIA PARA PROFISSIONAIS DA SAÚDE

As diretrizes do Instituto Nacional de Padrões e Tecnologia dos EUA (NIST) trouxeram todo o embasamento teórico de uma autenticação com níveis de garantia, estabelecendo sugestões e obrigatoriedades de acordo com a necessidade de segurança da situação. Porém, os métodos de autenticação apresentados não são voltados para a necessidade específica dos profissionais da saúde: uma autenticação *"limpa"*, sem toque de superfícies.

5.5.1 Nível de garantia ideal

Tendo como referência a Subseção 3.11.1, para determinar qual o nível adequado de garantia da autenticação para profissionais da saúde e suas atividades relacionadas, realizamos a avaliação dos riscos e impactos potenciais.

Consideramos uma autenticação fraudulenta em ambiente médico-pericial com acesso a prontuário pericial e elaboração de laudos para licença e aposentadoria. Escolhemos uma área médica não-assistencial onde a repercussão para a saúde do paciente é menor em relação às áreas assistenciais:

- Inconveniência, sofrimento ou danos à posição ou reputação: **Moderado**: na pior das hipóteses, inconveniência séria de curto ou longo prazo, angústia ou dano à posição ou reputação de qualquer parte.
- Perda financeira ou responsabilidade da agência: **Moderado**: na pior das hipóteses, uma perda financeira séria para qualquer parte ou uma responsabilidade séria da instituição ou provedor de serviço.
- Danos aos programas da agência ou aos interesses públicos: **Moderado**: na pior das hipóteses, um efeito adverso sério nas operações ou ativos organizacionais, ou no interesse público.
- Liberação não autorizada de informações confidenciais: **Moderado**: na pior das hipóteses, a liberação de informações pessoais, confidenciais pessoais ou comercialmente confidenciais para partes não autorizadas, resultando em perda de confidencialidade com um impacto moderado.
- Segurança pessoal: **Baixo**: na pior das hipóteses, ferimentos leves que não requerem tratamento médico.
- Violações civis ou criminai: **Moderado**: na pior das hipóteses, um risco de violações civis ou criminais que podem estar sujeitas a esforços de fiscalização.

Na análise das categorias de impacto com o exemplo acima, chegamos ao Nível 2 de garantia como nível mínimo para profissionais da Perícia Médica, conforme Quadro 1. Ao transportar o exemplo para outras especialidades médicas e também para outras categorias de profissionais da saúde, devemos chegar a resultados semelhantes pois sempre haverá uma possibilidade de dano à segurança pessoal e prejuízo com a liberação não autorizada de informações confidenciais (mesmo que o prejuízo seja apenas ético-profissional) pois trata-se de ações ligadas à saúde.

A prescrição dietética feita por um nutricionista, a aplicação medicamentosa feita por um enfermeiro, o movimento inadequado feito por um fisioterapeuta, a verificação dos sinais vitais e orientações básicas feitas por um técnico de enfermagem: todo e qualquer ato de um profissional da saúde pode gerar dano ao paciente, em menor ou maior intensidade.

Assim, dependendo do sistema informatizado, do ambiente em que ele está inserido e, qual a categoria de profissional da saúde que essa autenticação irá atender, o dano e seu impacto pessoal e social mudará. No exemplo referido (perícia médica), o resultado final de uma falha de autenticação pode ser reparado ou revertido na maioria das categorias de impacto, através de uma solicitação de reconsideração ou recurso de um laudo emitido, ou até mesmo na instância de auditoria. O mesmo não ocorreria em ambiente médico-hospitalar em que uma autenticação fraudulenta poderia gerar um acesso a prescrição médica do paciente, com possível efeito imediato.

Atualmente, observa-se que na maioria das instituições públicas ou privadas no Brasil, o nível de garantia de autenticação usado por profissionais da saúde é o nível 1, de acordo com o Quadro 2 da Subseção 3.11.2. Após avaliação dos fatores de riscos e impactos que devemos considerar na escolha do nível de autenticação ideal, o nível 1 mostrou-se inadequado para as atividades ligadas a saúde.

Assim, para a área da saúde em que todos os profissionais trabalham com vidas humanas e a autenticação fraudulenta nos sistemas informatizados pode ocasionar de desconforto à morte dos pacientes, trabalharemos com o nível de garantia 2 como mínimo para estes profissionais.

Como a gama de atividades é imensa, passando por técnicos de enfermagem, nutricionistas, fisioterapeutas até médicos de uma Unidade de Terapia Intensiva, cada caso ou ambiente de trabalho deve ser analisado separadamente sobre o nível de garantia mínimo a seguir (AAL2 ou AAL3).

Um nível de garantia mais robusto também implica em um processo de autenticação mais complexo, mais caro e, por vezes, mais demorado. Além disso, quanto

maior o nível de garantia, maior a chance de exclusão, de uma autenticação sem sucesso do profissional correto. A depender da análise de cada situação, pode ser recomendado que se mantenha o nível de garantia mínimo (AAL2) e haja um incremento no processo de autorização para cada ambiente ou categoria profissional no acesso a determinado procedimento.

5.5.2 Fatores de autenticação ideais

Em relação aos fatores de autenticação, temos como requisito uma autenticação sem toque por profissionais da saúde, de forma rápida, segura e prática. Em busca de uma forma de autenticação ideal para esses profissionais e com um olhar voltado para a não-contaminação tanto do profissional da saúde como das superfícies em geral, temos como condição ideal a ausência de toque do requerente em qualquer superfície.

Salientamos que o cuidado para a não-contaminação de mãos e superfícies pode não ser necessário no uso da telemedicina, caso o profissional esteja no seu próprio domicílio. Porém, é recomendado que o nível de garantia da autenticação seja mantido, podendo usar a combinação de fatores diversos.

Entre os fatores de autenticação e credenciais sem toque, dentro das premissas *"o que você sabe"*, *"o que você tem"* e *"o que você é"*, temos limitações.

"O que você sabe" só pode ser transmitido sem toque através da voz, o que enfraquece a segurança do ato já que outros no mesmo ambiente passam a conhecer a informação. Por isso, sugerimos técnicas de anonimização desse fator de autenticação. A resposta ao segredo pode ser dada por numeração após a pergunta e suas opções serem lançadas na tela do computador. *"Em qual cidade você nasceu? 1.Florianópolis; 2.Porto Alegre; 3.Criciúma"*. Nesse exemplo, a resposta que outras pessoas podem ouvir seria um número. Poderia ser usado como segundo ou terceiro fator de autenticação, após a identificação ocorrida com o fator inicial.

"O que você tem" deve estar junto a você, sem precisar ser tocado para ser inserido em algum equipamento, aproximado a um *hardware* ou apresentado a um indivíduo. Temos como possibilidades o uso da tecnologia RFID e trouxemos como sugestão o uso do *bluetooth*.

A tecnologia RFID (do inglês *Radio-Frequency IDentification*) utiliza ondas eletromagnéticas (de rádio frequência) como meio para comunicar os dados de identificação de algum elemento (pessoa ou objeto). Esses dados de identificação e informações diversas ficam armazenados nas chamadas etiquetas RFID (PEDROSO *et al.*, 2009).

Como o RFID usa sinais de rádio, não há necessidade de grande aproximação entre a etiqueta (que pode estar em um crachá, em um colar, em uma pulseira ou fixado na própria roupa do profissional da saúde) e o leitor, eliminando a necessidade de toque. A etiqueta deve conter os dados pessoais necessários para a identificação do profissional.

Sobre o uso do *bluetooth*, é uma tecnologia de comunicação sem fio que permite a troca de dados e arquivos entre dispositivos de forma rápida e segura. O sistema utiliza uma frequência de rádio de onda curta (2.4 GHz) para criar uma comunicação entre aparelhos habilitados. Como seu alcance é curto, só permite a comunicação entre dispositivos próximos (CÂMARA, 2012). Nossa sugestão é que ele seja usado a partir de um *smartwatch*, transportando a informação de identificação até o computador onde ocorrerá a autenticação no sistema de saúde informatizado. Outros dispositivos que não necessitem de toque também podem ser utilizados.

"O que você é" traduz-se pela biometria, que só deve ser escolhida como credencial de autenticação para esta proposta se for livre de toque.

Em tempos de pandemia onde o uso da máscara facial ainda se faz obrigatória, é necessário que se apresente alternativas para a face como fator biométrico, embora ela seja mais amigável. O uso da face, retina, íris, da voz e de gestos manuais são apenas algumas alternativas que podem ser inseridas na nossa proposta.

Então, sugerimos como fatores de autenticação sem toque:

Nível 1 de garantia - Não recomendado RFID OU Biometria OU Bluetooth OU Segredo memorizado;

Nível 2 de garantia Biometria + RFID OU Biometria + Bluetooth OU RFID + Bluetooth OU Biometria + Segredo memorizado OU RFID + Segredo memorizado OU Bluetooth + Segredo memorizado;

Nível 3 de garantia 2 Biometrias + RFID OU 2 Biometrias + Bluetooth OU Biometria + Bluetooth + RFID OU 2 Biometrias + Segredo memorizado OU RFID + Bluetooth + Segredo memorizado OU Biometria + RFID + Segredo memorizado OU Biometria + Bluetooth + Segredo memorizado.

Atentamos que as credenciais baseadas no que você possui podem ser usadas como fatores de autenticação de forma *"acidental"* ou *"não intencional"*, apenas por estarem no mesmo ambiente próximo ao leitor ou *hardware* de destino. Portanto, para melhoria da segurança, as biometrias utilizadas devem, sempre que possível, che-

car a vivacidade e a intencionalidade tanto na autenticação como na reautenticação nos níveis 2 e 3 de garantia.

Na hipótese de que a credencial definida para a autenticação no sistema informatizado não esteja disponível, é essencial que seja garantida outra forma de autenticação segura como opção, mesmo que com toque. Por exemplo, no caso da presença de um curativo extenso em face ou deformidade por um estado pós-operatório.

Outros tipos de informações, como dados de localização, podem ser usados por um Provedor de Serviços para avaliar o risco em uma identidade reivindicada ser fraudulenta, mas não são considerados fatores de autenticação. Sugerimos que tais informações sejam orientativas e não limitantes na autenticação. Indicamos que o profissional da saúde seja alertado que foi realizada autenticação eletrônica com sucesso em máquinas fisicamente distantes no mesmo intervalo de tempo, por exemplo. Como muitas vezes trata-se de vidas sendo salvas em situações de emergência, a autenticação não pode ser uma barreira para tal.

5.5.3 Reautenticação

Trata-se da necessidade de que o sistema informatizado continue sendo operado pelo mesmo profissional que se autenticou inicialmente.

Como o trabalho em unidades de saúde mostra-se sempre dinâmico e com peculiaridades de vários profissionais transitando no mesmo ambiente (inclusive empregados de outras áreas como os responsáveis pela limpeza), além de turnos de trabalho onde os profissionais são trocados mas os pacientes e suas condutas terapêuticas seguem os mesmos, a necessidade de reautenticação frequente se faz necessária.

Descartamos completamente a orientação inicial trazida pelas diretrizes do Instituto Nacional de Padrões e Tecnologia dos EUA (NIST) que sugeriu períodos de 12 horas ou 15 minutos de inatividade para reautenticação no nível 3 de garantia e reautenticação a cada 30 dias no nível 1 de garantia, como mostra o Quadro 3.

Na nossa proposta, a escolha do período de tempo para reautenticação levou em consideração as escalas de trabalho dos profissionais da saúde, tanto em regime ambulatorial como em turnos de plantão, que são os dois mais frequentes. O tempo de inatividade considerou a duração média de um exame físico quando o profissional, por vezes, se afasta do computador/sistema informatizado. Entendemos que, caso a inatividade seja por afastamento do sistema por motivo diverso, há necessidade de reautenticação.

Assim, diversas situações na rotina de trabalho dos profissionais da saúde foram pensadas: consulta ambulatorial, evolução do paciente em internação hospitalar, atendimento em unidade de pronto-atendimento e telemedicina inclusive. Com essas particularidades, o intervalo para reautenticação foi de, no máximo, 12 horas em atividade e 15 minutos de inatividade no AAL1 (nível não recomendado).

No nível 2 de garantia (AAL2), o qual indicamos que seja utilizado como nível mínimo para todas os sistemas informatizados em saúde, sugerimos reautenticação a cada 6 horas de atividade (período máximo de trabalho contínuo indicado antes de um breve repouso do profissional, mesmo que em regime de plantão) e 15 minutos de inatividade (período estimado para um exame físico longe do *hardware* onde foi inicialmente autenticado). Todos os fatores da autenticação inicial devem ser usados na reautenticação.

Já no nível 3 de garantia, sugerimos a reautenticação a cada 4 horas em atividade ou a cada 5 minutos de inatividade. Salientamos que, nesse nível de garantia, todas as combinações, que necessariamente devem conter pelo menos 2 tipos diferentes de fatores de autenticação, tem a presença da biometria como um deles. Tal biometria deve ser acompanhada obrigatoriamente de sinais de vivacidade e de intencionalidade pela reautenticação. Ambos podem ser intuitivos e combinados, inclusive, no ato médico em curso. Pelo menos 2 fatores diferentes de autenticação devem estar presentes na reautenticação nesse nível de garantia.

Por exemplo, a biometria da face pode promover uma reautenticação facilitada na apresentação da vivacidade e da intencionalidade mantendo a prerrogativa de não haver toque. Perguntas como *"Deseja manter a autenticação neste sistema?"* tendo como possibilidade de resposta o movimento afirmativo com a cabeça, mostrando uma solução simples para uma reautenticação segura.

O Quadro 4 traz um resumo da nossa proposta para cada nível de garantia com exemplos de fatores de autenticação sem toque para profissionais da saúde, a frequência de reautenticação e o nível de risco correspondente.

Salientamos que a combinação do RFID + Bluetooth no nível 2 de garantia deve ser analisada de acordo com a necessidade do caso concreto, já que pecam em não haver possibilidade de prova de intencionalidade e vivacidade.

5.5.4 Protocolos Criptográficos

Segundo as diretrizes do Instituto Nacional de Padrões e Tecnologia dos EUA (NIST) sobre identidade digital e autenticação (GRASSI *et al.*, 2020a), a autenticação com nível de garantia 3 demonstra confiança de que o usuário tem controle dos seus

Quadro 4 – Exemplos de métodos de autenticação e níveis de garantia para profissionais da saúde.

Níveis de garantia	Baixo (nível 1)	Moderado (nível 2)	Alto (nível 3)
Fatores de autenticação sem toque	RFID ou Biometria ou Bluetooth ou Segredo Memorizado	Biometria + RFID Biometria + Bluetooth RFID + Bluetooth Biometria + Segredo Bluetooth + Segredo RFID + Segredo	2 biometrias + RFID 2 biometrias + Bluetooth Biometria + Bluetooth + RFID 2 biometrias + Segredo RFID + Bluetooth + Segredo Biometria + RFID + Segredo Biometria + Bluetooth + Segredo
Frequência de reautenticação	A cada 12 horas em atividade ou a cada 15 minutos em inatividade	A cada 6 horas em atividade ou a cada 15 minutos de inatividade	A cada 4 horas em atividade ou a cada 5 minutos em inatividade
Nível de risco assumido pela parte confiável	Mitigado **(Não recomendado)**	Baixo	Mínimo

Fonte: Própria autora

autenticadores. Ela deve ocorrer por meio de protocolos de autenticação seguros e a indicação é que sejam usadas técnicas criptográficas aprovadas. E a mesma exigência já ocorre no AAL2.

Nas sugestões que trouxemos de autenticação sem toque, o *bluetooth* entra como um protocolo de transporte e está previsto neste protocolo o uso da criptografia das informações/dados que são trafegados (PANSE; KAPOOR, 2012).

Já o RFID, que também é um protocolo de transporte, não traz por si só a criptografia vinculada ao dispositivo (SOARES, R. C., 2018), então indicamos que, ao escolher tal fator de autenticação para compor o método para AAL2 ou AAL3, deve ser incorporado um protocolo de segurança criptográfica a esse dispositivo.

Os demais fatores de autenticação também devem atender a esse requisito criptográfico.

5.6 ASSINATURA DE DOCUMENTOS MÉDICOS ELETRÔNICOS

Com o início da pandemia em março/2020, o site do CRM/SC (e demais conselhos regionais) passou a disponibilizar espaço para que o médico prescreva medicações, redija atestados de afastamento laboral, solicite exames e vários outros documentos importantes de forma digital, apenas utilizando login e senha. Os documentos gerados possuem *QR Code* e assinatura eletrônica simples que, nesse caso,

parte da autenticação no sistema com nível de garantia 1.

Já no site do CFM, o processo de confecção desses documentos segue um trâmite diferente, conforme exposto na Seção 4.12. O documento não é emitido na plataforma do conselho (o médico apenas realiza *download* do modelo do documento) e a assinatura digital indicada é a qualificada (usa o certificado digital validado pela ICP-Brasil), ou seja, tem garantia de autenticidade, integridade e validade jurídica.

Assim, as farmácias ficaram autorizadas a dispensar medicamentos de controle especial e antimicrobianos mediante receita de controle especial digital emitidas através das plataformas eletrônicas dos CRMs que contenham o *QR Code* para validação e assinatura eletrônica simples, e também as prescrições de controle especial que contenham somente a assinatura eletrônica digital qualificada com certificado ICP-Brasil.

Além de percebermos uma diferença no nível de segurança de cada assinatura (simples e qualificada) nos dois casos, o farmacêutico faz o registro da dispensação de forma eletrônica, mas precisa imprimir a prescrição para posterior conferência dos órgãos fiscalizadores. Então, o processo começa eletrônico e termina no papel.

Propomos que toda as prescrições eletrônicas (sejam receitas de medicações sem controle dos órgãos fiscalizadores ou as com controle especial) ocorram na plataformas dos conselhos profissionais. Sendo o CFM o provedor único de identidade, também é possível que ele emita certificados digitais ICP-Brasil pois pode se tornar uma Autoridade Certificadora, além de uma Autoridade de Registro. O processo de emissão de certificado digital para a assinatura digital dos documentos pode ocorrer de acordo com a demanda, ou seja, para cada novo documento médico eletrônico, um novo certificado digital gerando uma assinatura digital qualificada.

Dessa forma, um sistema ligado ao CFM que emita certificados sob demanda para assinatura de documentos médicos naturalmente exige autenticação com segurança e com atributos atualizados. O processo também ganha em praticidade: a única preocupação do médico é com a autenticação dele perante o provedor de serviço.

Assim, toda prescrição eletrônica teria uma assinatura digital qualificada, mas com o processo invisível para o médico (ou outro profissional da saúde). De forma intuitiva, sem custo, desburocratizado e segura, haverá aprimoramento da experiência do usuário. As prescrições médicas com assinatura qualificada ficariam disponíveis em nuvem para acesso de quem o paciente permitir.

A segurança e a melhoria da experiência se dará para todos os usuários. A proposta é que, a partir do momento em que a prescrição é apresentada na farmácia

e a medicação é dispensada e registrada pelo farmacêutico, a prescrição daquela medicação como "guia de compra"não ficará mais disponível na nuvem. Ela pode continuar existindo para ser consultada pelo paciente, pelo médico ou pelo próprio farmacêutico, mas ficará indisponível para venda ou modificações. Nesse momento, ficará disponível para acréscimo de informações e assinaturas apenas para os órgãos de vigilância sanitária/Anvisa (controle e conferência). Não há necessidade de imprimi-la nem validá-la porque todas as prescrições conterão os certificados digitais usados para as assinaturas (do médico, do farmacêutico, da Anvisa), conferindo integridade.

Assim, tendo uma prescrição emitida pelo próprio sistema do CFM e disponível como documento válido apenas na nuvem, o risco de ter esse documento adulterado é bastante reduzido pois o paciente não precisará descarregar e apresentar o documento ao farmacêutico.

Como não poderia ser diferente, todas as orientações de posologia, via de administração e qualquer outra orientação contida na prescrição médica é de livre acesso ao paciente, seja impressa ou na nuvem, e não deixará de existir após a dispensação das drogas.

5.7 RESULTADOS ESPERADOS

Nos dias atuais, a identificação e a autenticação dos profissionais da saúde continuam ocorrendo como há vários anos atrás. A forma como o profissional da saúde se veste e a posse de um crachá (que pode ser facilmente extraviado) é a maneira mais comum de identificá-lo. A apresentação da carteira profissional raramente ocorre. E a autenticação nos sistemas informatizados geralmente se dá através de login e senha, sem um nível de garantia adequado para aquela ação.

O provedor de identidade único e centralizado pelo Conselho Federal de Medicina traz segurança com a atualização em tempo real dos dados profissionais. Isso reduz o risco de uma autenticação de sucesso em um sistema informatizado de um médico recém cassado, por exemplo.

Centralizando as credenciais e todos os dados profissionais necessários para o exercício legal da profissão em um único provedor de identidade, a instituição de saúde e qualquer outro provedor de serviço se beneficia pela confiabilidade e também pela gestão desses dados (em tempos de LGPD).

Pretende-se com este estudo apresentar a possibilidade da identificação eletrônica e a autenticação dos profissionais da saúde para um nível de mínimo ou nenhum contato físico, e com o nível adequado de garantia para as atividades envolvendo

a saúde humana. Apesar da contaminação dos profissionais e superfícies com os mais diversos patógenos ser uma preocupação inerente ao trabalhador da saúde, a pandemia do COVID19 trouxe destaque e tentativa de adequação a todos os processos de trabalho.

Trouxemos uma simplificação da confecção e assinatura dos documentos médicos eletrônicos, principalmente voltada para a prescrição médica das medicações com controle especial. Adotando uma produção de certificado digital sob demanda pelo próprio CFM, para a assinatura eletrônica qualificada das prescrições, tornamos os documentos mais seguros e o processo mais simples. O médico se preocupará apenas em se autenticar no provedor de serviço e todo o processo de assinatura qualificada será invisível e intuitivo.

A perspectiva é que haja um incremento na experiência do usuário e que esse ganho seja reproduzido nas demais categorias de profissionais de saúde, tornando todo o ato (da prescrição ao controle da dispensação) completamente digital e seguro.

5.8 CONCLUSÃO

Apresentamos um *framework* com estrutura de design centrado no usuário/profissional da saúde. Propomos um sistema de identidade que permite a fácil adoção de várias tecnologias de credenciais, incluindo novas tecnologias que podem surgir no futuro . Por meio do uso de padrões abertos e práticas de aquisição que evitam o aprisionamento de tecnologias, os profissionais podem garantir que o sistema seja capaz de se adaptar e tirar proveito de novas soluções.

Trouxemos um modelo de autenticação em sistemas informatizados sem toque, ideal para profissionais da saúde, com nível de garantia adequado para as ações. O método é seguro, prático, rápido e sem custos. Deixa o médico livre para se preocupar apenas com a saúde dos pacientes. As novas tecnologias devem ser usadas para facilitar a rotina de trabalho e o acesso do profissional aos diversos sistemas informatizados, tornando o desconforto de memorizar login e senha, parte do passado.

Por fim, apresentamos uma maneira de tornar as prescrições eletrônicas mais seguras com o uso do certificado digital sob demanda, emitido pela plataforma do conselho da categoria profissional, gerando assinaturas eletrônicas qualificadas nos documentos médicos necessários. A experiência do usuário/médico será de desburocratização do processo, tendo ganhos em segurança.

6 AVALIAÇÃO

6.1 INTRODUÇÃO

Este capítulo traz uma avaliação descritiva, discutindo as principais contribuições deste trabalho. A Seção 6.2 avalia os resultados da proposta de um novo sistema de autenticação sem contato, com uma análise dos níveis de garantia necessários para a área da saúde. A Seção 6.3 analisa o provedor de identidades eletrônico proposto para profissionais de saúde. Como o provedor é da saúde, mostra-se que os atributos de autorização, podem ser facilmente controlados pelas entidades de classe. Na Seção 6.4 apresentamos as facilidades e a segurança na prescrição eletrônica de medicação com controle especial ao usar o modelo proposto em comparação ao modelo atual. Finalmente, a Seção 6.5 apresenta uma implementação prática, desenvolvida para mostrar experimentalmente, em dois cenários reais, a operação do provedor de identidade único com autenticação segura e sem toque.

6.2 AUTENTICAÇÃO DOS PROFISSIONAIS DA SAÚDE

6.2.1 Nível de garantia

Tomando como referência as diretrizes do Instituto Nacional de Padrões e Tecnologia dos EUA (NIST) para a autenticação digital, analisando riscos e categorias de impacto (expostas na Seção 5.5) classificamos o nível de garantia usado atualmente, tanto o método usado no próprio site do CRM/SC como na grande maioria dos sistemas informatizados de saúde, como nível 1. Segundo a avaliação do dano e impactos potenciais, temos o nível 2 como mínimo a ser utilizado pelos profissionais da saúde.

Trazendo uma autenticação fundamentada em um nível de garantia adequado para cada situação, uma possível falha ou fraude em uma autenticação do profissional da saúde previne os vários impactos negativos (vide Seção 3.11.1) que podem ser gerados, desde abertura de sigilo médico com acesso ao conteúdo do prontuário até riscos a integridade física do paciente. Dependendo do ambiente (hospitalar, ambulatorial, administrativo) e da função do profissional da saúde, os danos podem ser ainda mais significativos e irreversíveis. A atenção para uma autenticação com nível de garantia adequado é essencial no contexto de cuidados com a saúde.

Outro imenso ganho com a nossa proposta é a possibilidade de uma maior segurança para os atendimentos realizados através da Telemedicina. Atualmente, a anamnese (entrevista que o profissional da saúde realiza com o paciente) pode ser realizada por qualquer plataforma digital que garanta o sigilo e privacidade, mas nessa circunstância não há mecanismo seguro que prove para o paciente que a pessoa que

se apresenta como médico, por exemplo, é verdadeiramente quem diz ser.

Porém, ao final da consulta médica, as prescrições por meio eletrônico devem ser realizadas através do portal do CRM de cada Estado (ou do CFM). Para autenticação nesse portal, há necessidade de autenticação com *login* e senha apenas (nível 1 de garantia), sem nem mesmo a necessidade de certificação digital dos médicos para a maioria as prescrições (*sites* dos CRMs). O intuito foi de desburocratizar, mas acabou fragilizando bastante a segurança do ato.

Com a implementação de uma autenticação com nível de garantia 2 nas plataformas dos conselhos profissionais, a desburocratização pode permanecer e haverá um ganho considerável de segurança por parte do paciente de que os documentos (prescrições, atestados, solicitações de exames) foram confeccionados e assinados pelo profissional que se apresenta.

6.2.2 Autenticação sem toque

Além do nível de garantia da nossa proposta ser mais adequado para as ações dos profissionais de saúde, também temos a credencial sem toque trazendo uma preocupação com a não contaminação de superfícies e pessoas.

Sobre a autenticação dos profissionais da saúde nos diversos sistemas informatizados, não encontramos publicações na literatura que analisasse e propusesse uma autenticação *"limpa"*, preocupada com a não contaminação das pessoas e das superfícies.

O método tradicional de autenticação por login e senha continua sendo o mais utilizado, mesmo sendo pouco seguro e desconfortável para os profissionais, que necessitam contar com uma boa memória.

Apresentamos vários métodos de autenticação, para todos os níveis de garantia e para diversas situações, sem contaminação das mãos.

Com uma autenticação intuitiva, a resistência por parte do profissional para essa situação tende a desaparecer. Sem necessidade de armazenar na memória login e senha, bastando se posicionar em frente ao computador, a tecnologia passa a trabalhar a seu favor.

6.3 IDENTIDADE ELETRÔNICA PARA PROFISSIONAIS DE SAÚDE

Atualmente, a identificação, as credenciais e os atributos dos profissionais da saúde são solicitados por cada instituição de saúde separadamente na contratação

do profissional. A depender da *expertise* do setor de recursos humanos de cada local, pode haver inclusive a aceitação de dados falsos por documentos fraudulentos.

A proposta de um provedor de identidade único centralizado no próprio CFM traz mais segurança em tempo real para as informações profissionais, mitigando a atuação de falsos profissionais e reduzindo a reprodução de dados dos profissionais. O provedor de servidor terá um provedor de identidade confiável e atualizado.

A concentração das informações profissionais com credenciais e atributos em um único provedor de identidade que atende a vários provedores de serviços traz vantagens também para as empresas privadas e instituições públicas que agora necessitam de procedimentos especiais para atender a LGPD, ficando a cargo do CFM e CRM de cada Estado a maior parte desse cuidado.

O Quadro 5 apresenta de forma sintetizada as mudanças propostas:

Quadro 5 – Resumo das mudanças propostas para o provedor de identidade e métodos de autenticação dos profissionais da saúde.

Características	**Tradicional**	**Proposta**
Provedor de identidade	Descentralizado	Centralizado
Nível de garantia da autenticação	Nível 1	Nível 2 ou 3
Toque e possível contaminação na autenticação	Com toque	Sem toque

Fonte: Própria autora

6.4 ASSINATURA DE RECEITUÁRIO CONTROLADO

Contrastando com a Figura 6 na página 84 que representa o atual modelo de prescrição com assinatura qualificada (plataforma CFM), temos a Figura 9 que mostra o processo de prescrição eletrônica de controle especial com assinatura qualificada até a dispensação da medicação sem necessidade de validação.

Os conselhos de cada categoria profissional (tanto o CFM como o CFF), sendo provedores de identidade centralizados, podem emitir certificados digitais ICP-Brasil como Autoridades Certificadoras, que serão usados para assinaturas qualificadas (de acordo com a exigência da Anvisa para medicações de controle especial).

Não há necessidade de *smartcards* nem de prescrições impressas. Nossa proposta traz uma grande simplificação de todo o processo. As prescrições estariam disponíveis em nuvem computacional e o processo de emissão do certificado digital seria *online*, sob demanda, sem custo e invisível para os profissionais envolvidos.

Figura 9 – Passos para prescrição eletrônica e dispensação de medicação com controle especial no modelo proposto.

Fonte: Adaptado de (CFM, 2020d)

6.5 PROTÓTIPO

Um protótipo de identidade eletrônica centralizada para profissionais da saúde com suporte a autenticação sem toque foi implementando. O desenvolvimento técnico ocorreu no LabSEC/UFSC (Laboratório de Segurança em Computação da UFSC) pelo graduando Maurício Barros, seguindo os requisitos do projeto para esta dissertação.

Conforme descrito na seção 5.5.2, a autenticação de profissionais de saúde exige, no mínimo, o nível de garantia 2. Desta forma, nosso protótipo utiliza dois fatores de autenticação, biometria facial (*i.e.*, reconhecimento facial) do usuário e a presença de um dispositivo*bluetooth* do usuário.

O protótipo faz uso de um provedor de identidade chamado Keycloak (RED HAT, 2014), um sistema gratuito cujo código-fonte é aberto e desenvolvido pela RedHat há mais de 5 anos, com constantes atualizações de funcionalidades e segurança. Este provedor de identidade suporta, dentre outros, os protocolos OpenID Connect para realizar identificação e autenticação e OAuth 2.0 para autorização, vide seções 3.8 e 3.9.

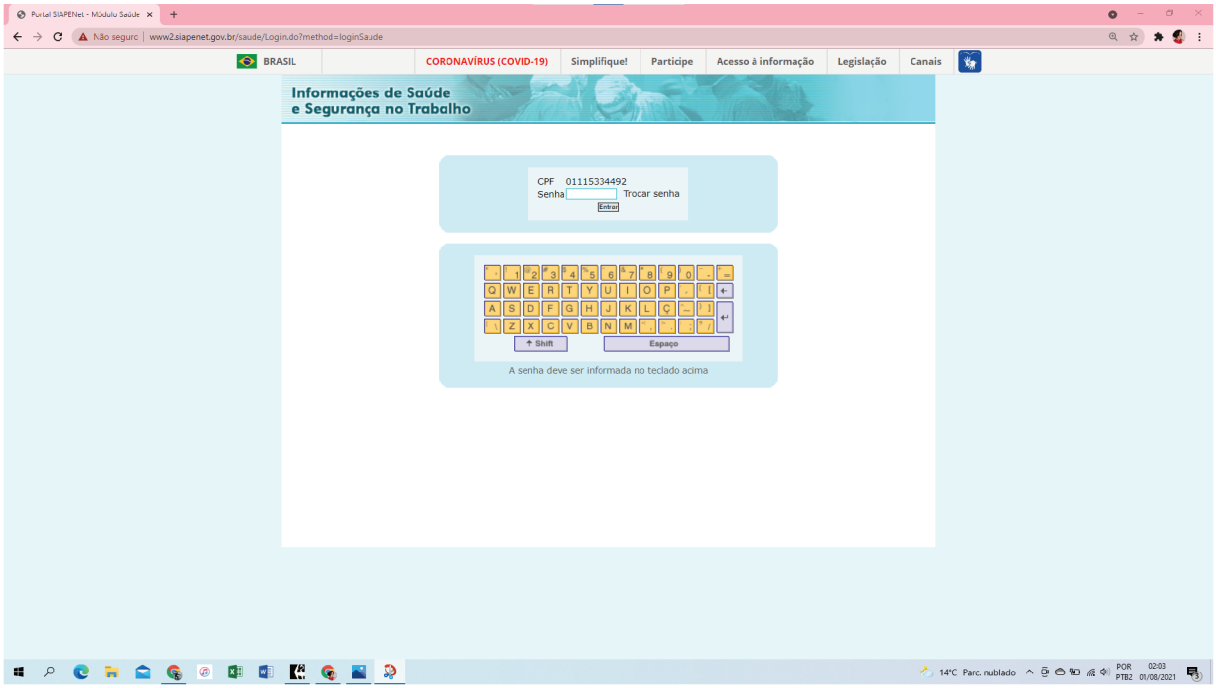
Em nossa instalação do Keycloak, que suporta a autenticação tanto por *login*

de usuário e senha, quanto a autenticação sem toque supracitada, os usuários são registrados no sistema por um administrador. Em um ambiente real de utilização deste protótipo, os próprios provedores de serviços que utilizam a autenticação do nosso provedor de identidade, podem cadastrar e descadastrar usuários. Isso aconteceria através de usuários com poderes administrativos, ou seja, mais elevados em relação aos profissionais da saúde que fazem uso operacional dos sistemas.

Considerando que o protótipo é uma prova de conceito, ou seja, nosso objetivo é demonstrar a viabilidade das propostas desta dissertação, apenas dois provedores de serviços foram desenvolvidos. Estes são réplicas de dois sistemas existentes, usados diariamente por profissionais da saúde, são eles: SIAPE Saúde (Portal Siapenet [1] [2]) e Espaço do Médico (site do CRM/SC [3]).

Atualmente, a autenticação no sistema SIAPE Saúde ocorre informando o CPF do profissional da saúde e senha em um teclado virtual, conforme ilustra a Figura 10.

Figura 10 – Identificação e autenticação no SIAPE Saúde com CPF e senha.



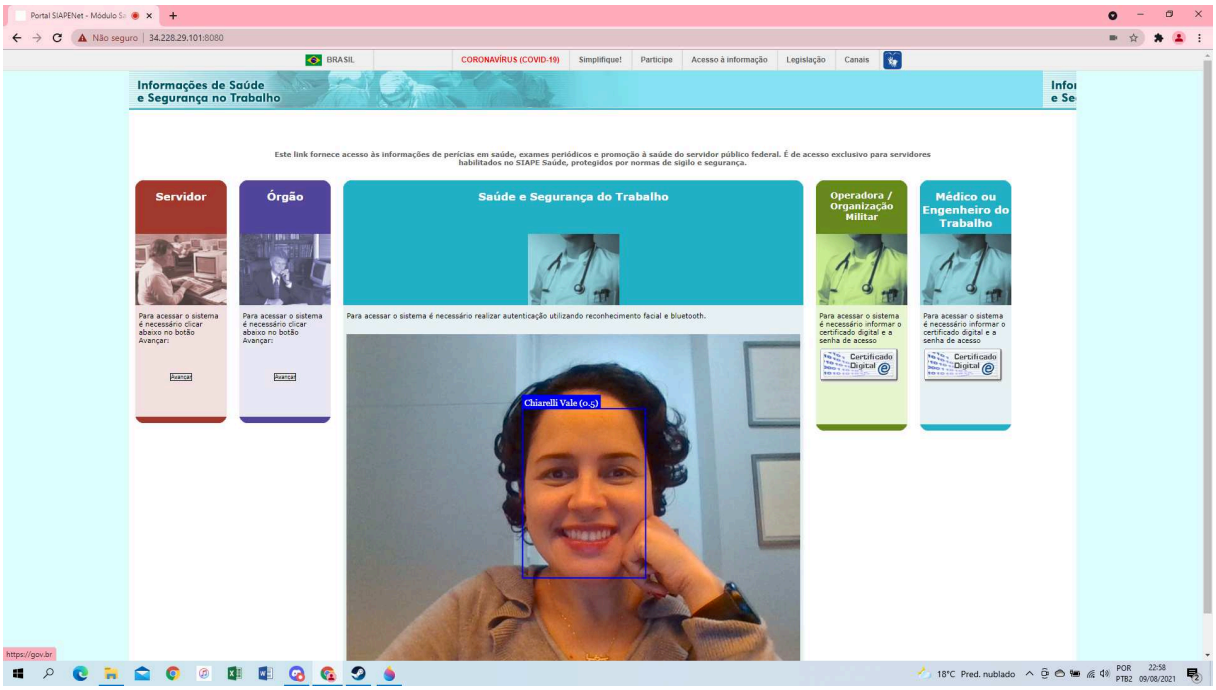
Fonte: Adaptado do Portal Siapenet

A Figura 11 mostra o mesmo sistema SIAPE Saúde adaptado para ser um

[1] Módulo Saúde: https://www2.siapenet.gov.br/saude/Login.do?method=login
[2] Autenticação da mestranda: https://www2.siapenet.gov.br/saude/Login.do?method=loginSaude
[3] Autenticação do médico: https://api.crmsc.org.br/crvirtual-pessoafisica-web/#/login

cliente do nosso provedor de identidade. É possível verificar que a identificação e autenticação em dois fatores inicia-se com o reconhecimento facial.

Figura 11 – Cliente SIAPE Saúde do provedor de identidade Keycloak. Identificação e parte da autenticação através de reconhecimento facial.



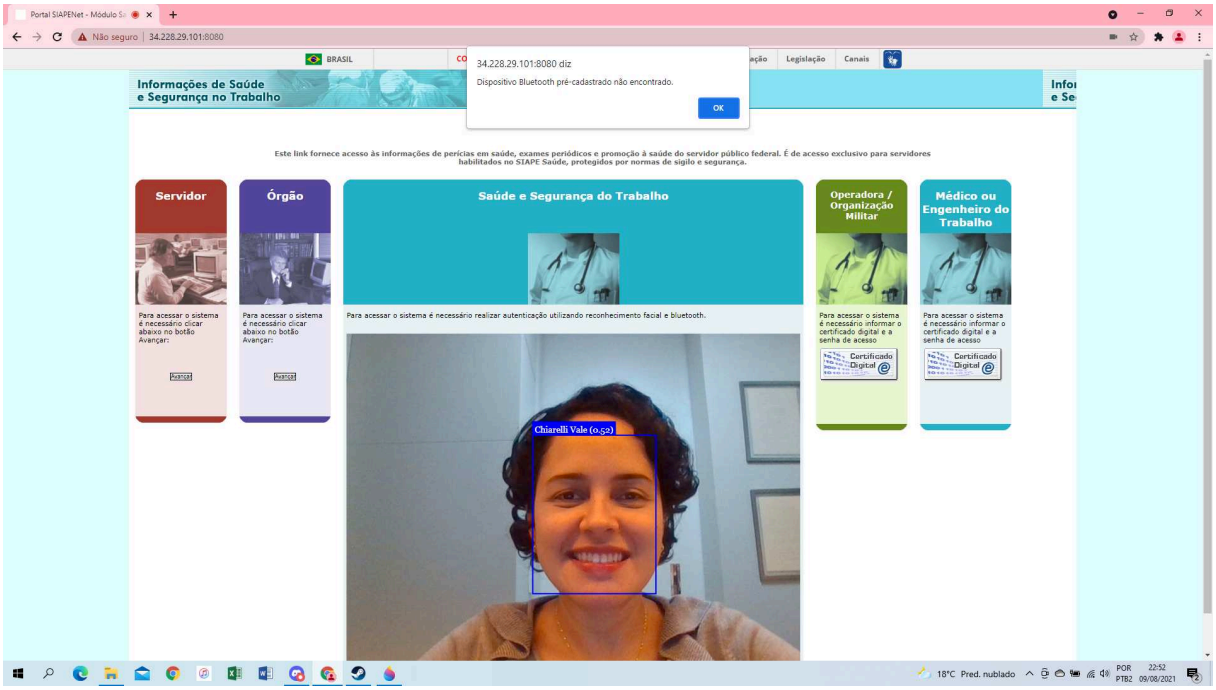
Fonte: Adaptado do Portal Siapenet

A Figura 12 demonstra um erro do segundo fator de autenticação, *i.e.*, a ausência do dispositivo *bluetooth* pré-cadastrado para o usuário em questão.

Por fim, a Figura 13 evidencia a autenticação em dois fatores com sucesso, o usuário é imediatamente redirecionado para a página que tem acesso dentro do sistema conforme suas credenciais.

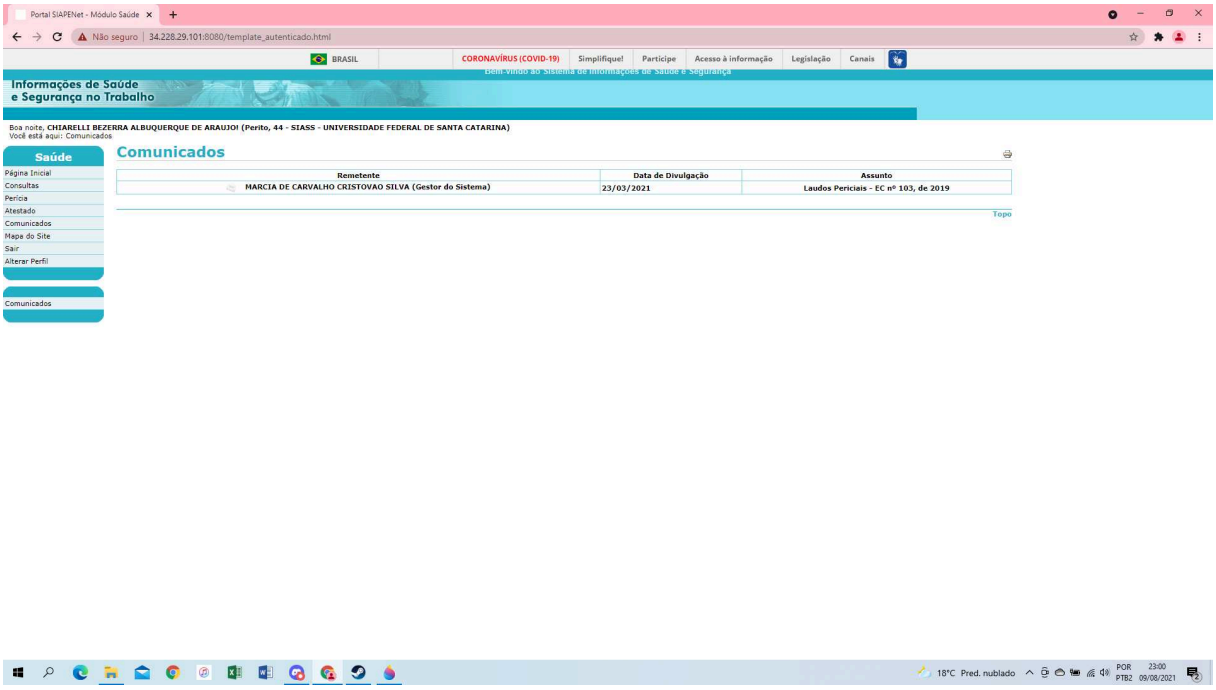
Com o uso frequente da telemedicina durante a pandemia do COVID19, o site do CRM/SC lançou um portal médico para elaboração de prescrições médicas eletrônicas, solicitação de exames, atestados médicos e formulários livres. Os documentos prontos podem ser enviados diretamente para o email do paciente já com a assinatura eletrônica simples. Para autenticação do profissional no *"Espaço do Médico"* e acesso a essas funcionalidades basta o email do usuário e senha (Figura 14).

Figura 12 – Erro no segundo fator de autenticação: ausência de dispositivo *bluetooth*.



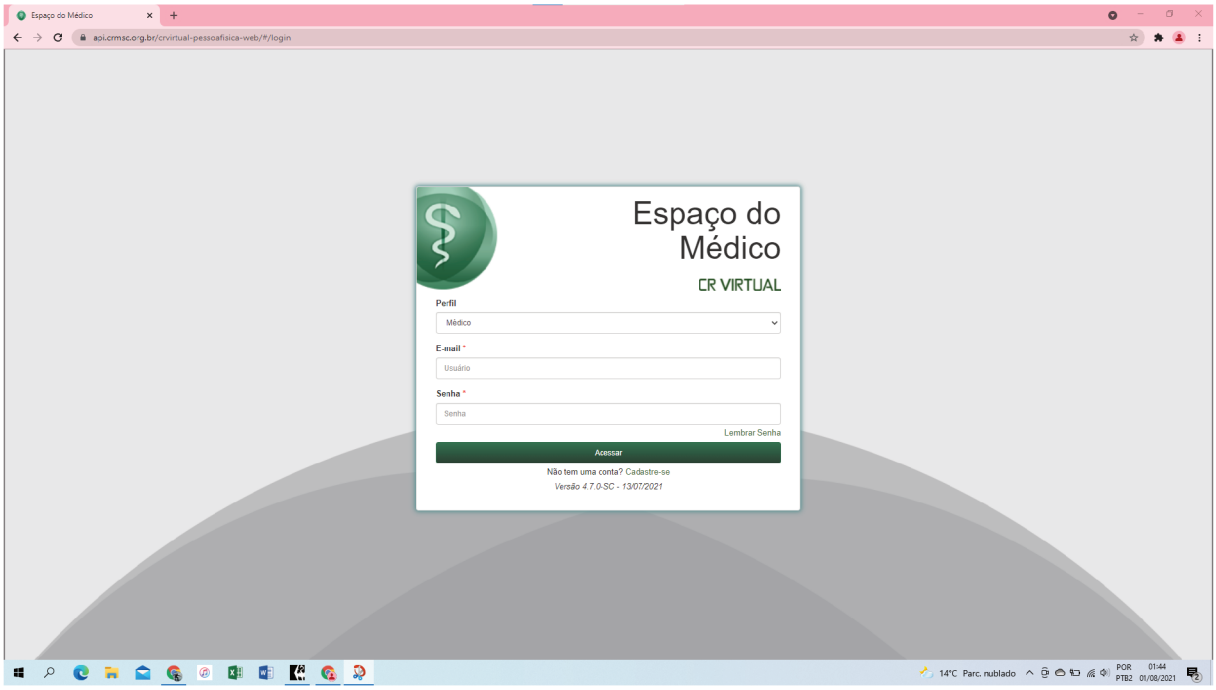
Fonte: Adaptado do Portal Siapenet

Figura 13 – Autenticação em dois fatores realizada com sucesso, usuário é redirecionado.



Fonte: Adaptado do Portal Siapenet

Figura 14 – Identificação e autenticação no "Espaço do Médico"do site do CRM/SC com email e senha.



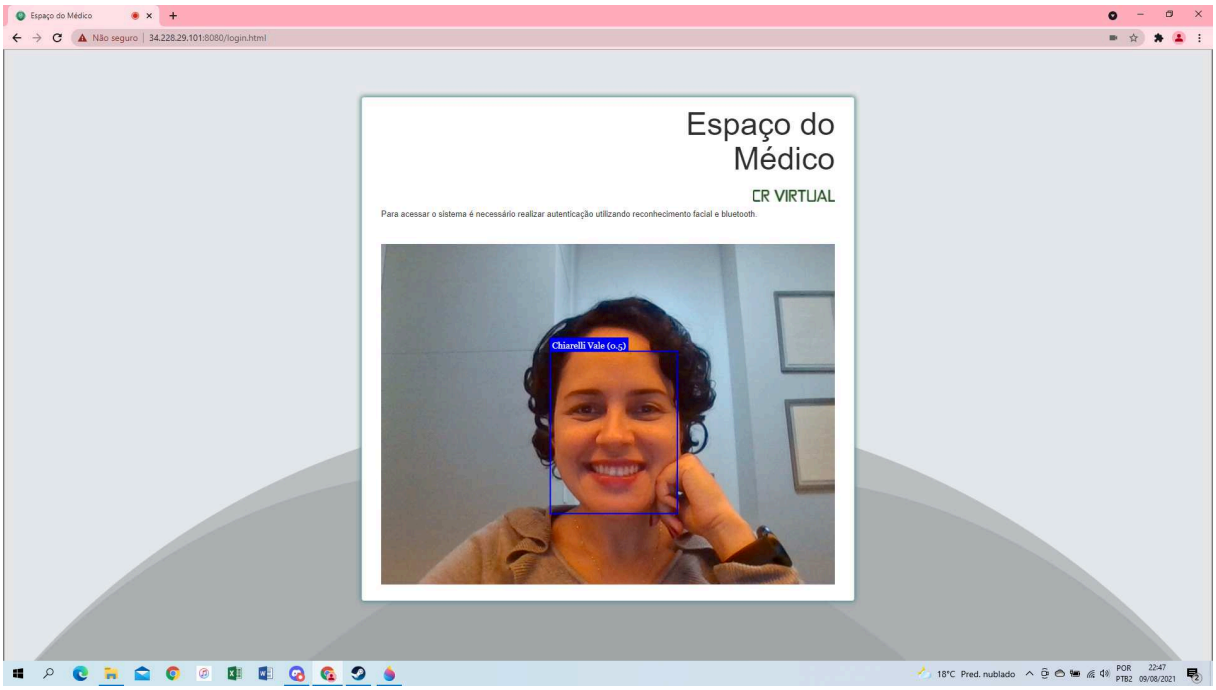
Fonte: Adaptado do site do CRM/SC

A Figura 14 apresenta o mesmo sistema do CRM/SC no *"Espaço do Médico"* com a adaptação do protótipo, seguindo a demonstração já realizada anteriormente:

- Figura 15: Reconhecimento facial como primeiro fator de autenticação;
- Figura 16: Erro com segundo fator de autenticação (*bluetooth*) não encontrado;
- Figura 17: Autenticação dos 2 fatores com sucesso, sendo direcionado para o acesso às funcionalidades.

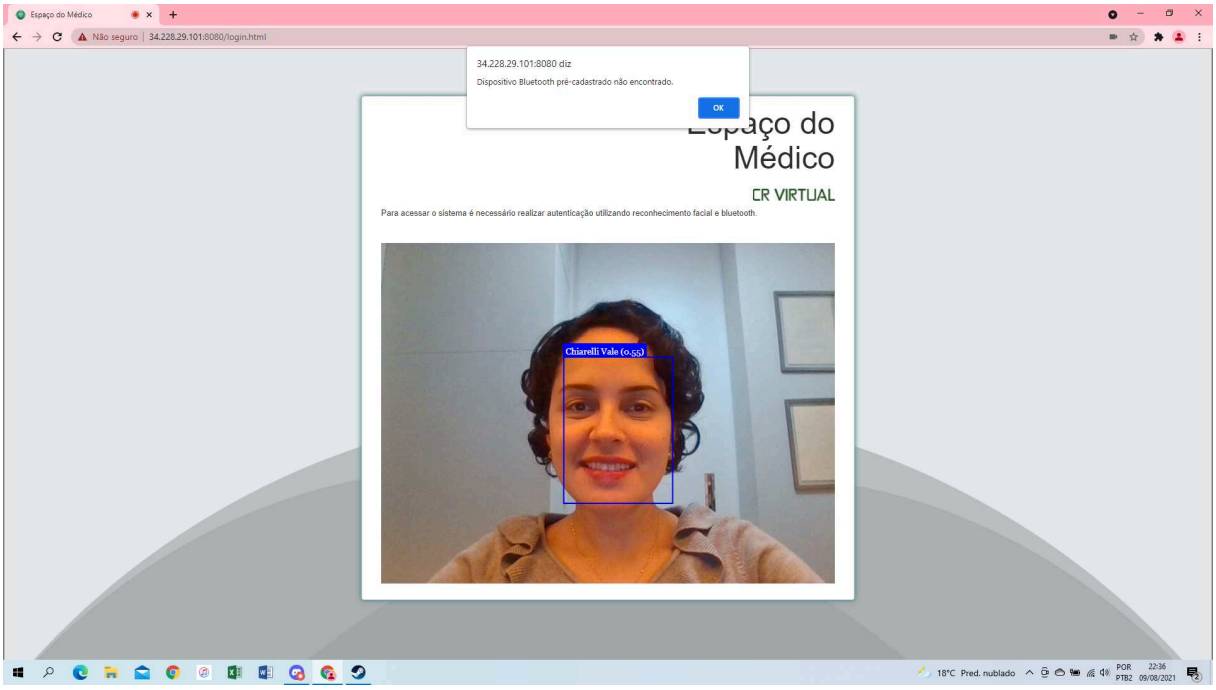
É importante ressaltar que a experiência do usuário com o sistema não é afetada pelo uso do provedor de identidade. Isso acontece pois os protocolos OpenID Connect e OAuth 2.0 são executados entre o provedor de serviço e o provedor de identidade sem a intervenção do usuário. O usuário é apenas apresentado com a interface para realizar a identificação e autenticação.

Figura 15 – Cliente CRM/SC do provedor de identidade keycloak. Identificação e parte da autenticação através de reconhecimento facial.



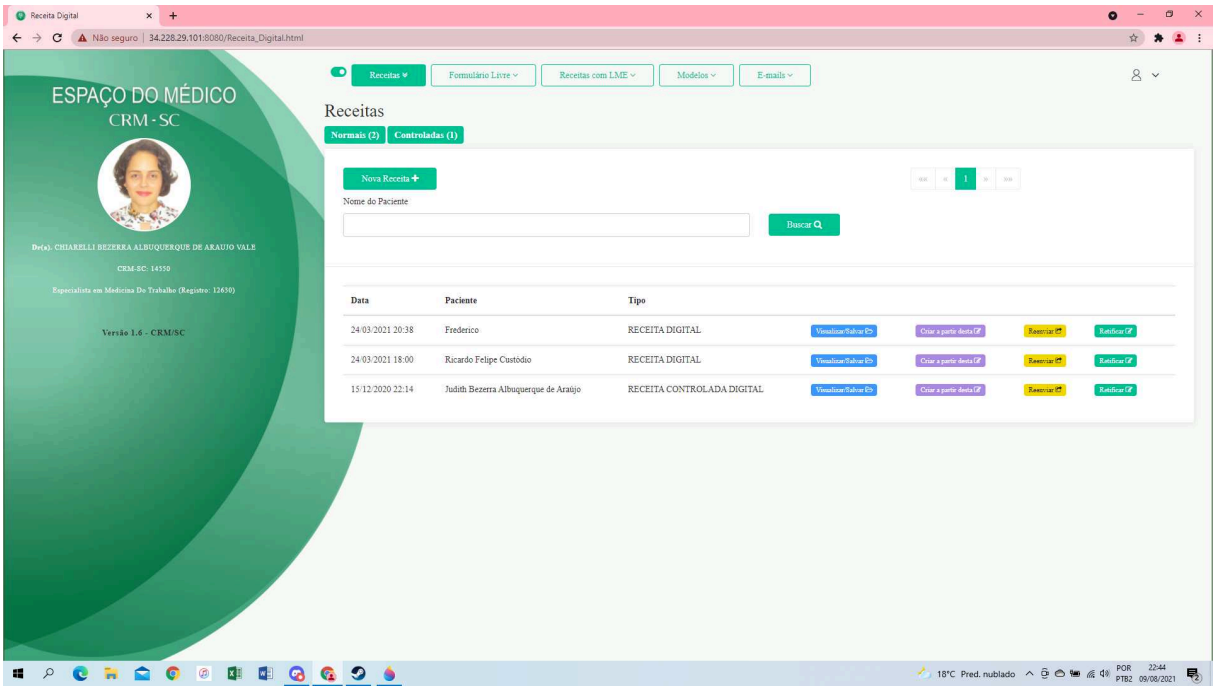
Fonte: Adaptado do site do CRM/SC

Figura 16 – Erro no segundo fator de autenticação: ausência de dispositivo *bluetooth*.



Fonte: Adaptado do site do CRM/SC

Figura 17 – Autenticação em dois fatores realizada com sucesso, usuário é redirecionado.



Fonte: Adaptado do site do CRM/SC

6.6 LIMITAÇÕES

Este capítulo discutiu as principais contribuições deste trabalho.

A proposição de um novo modelo de identidade para os profissionais de saúde, objeto deste trabalho, não vislumbra contemplar questões de ordem legal ou comportamental no âmbito da identificação, autenticação e autorização dos médicos nos variados sistemas informatizados.

Como limitação de uma abordagem digital para identidade e autenticação, temos a necessidade de conectividade com um provedor de identidade, o que pode não ser viável para profissionais da saúde que trabalham em localidades com internet ou cobertura móvel não confiável ou desigual, embora essas lacunas estejam diminuindo com o tempo.

Embora nossa proposta seja de uma identidade eletrônica com autenticação intuitiva, alguns profissionais ainda podem preferir credenciais físicas por considerarem o valor simbólico do documento, mesmo havendo restrição na autenticação em sistemas com a CIM atual.

Sobre a prescrição eletrônica dos medicamentos com controle especial, temos

como limitação para que o processo seja completamente digital, o fato de que todos os profissionais envolvidos necessitam ter os mesmos facilitadores aqui propostos.

6.7 CONCLUSÃO

Após uma breve comparação entre o modelo de autenticação atual dos profissionais da saúde nos diversos sistemas informatizados com a nossa proposta, percebe-se uma fragilidade de segurança com o modelo tradicional e certamente um ganho com os novos métodos apresentados que consideram a avaliação do nível de garantia adequado para a atividade ou ambiente de saúde.

No atual momento de pandemia pelo COVID-19, não existe método vigente descrito na literatura que tenha a preocupação de uma autenticação sem contaminação de pessoas e superfícies. Trouxemos modelos de autenticação sem toque com toda a segurança necessária para cada situação.

O provedor de identidade centralizado e ligado ao conselho de classe traz confiabilidade aos provedores de serviço nos identificadores, credenciais e atributos dos profissionais da saúde em tempo real, além de minimizar a disseminação dos dados pessoais e profissionais com melhor adequação a LGPD.

Com um provedor de identidade centralizado, o CFM tem um caminho traçado para credenciar-se como uma Autoridade Certificadora além de uma Autoridade de Registro, e tornar mais simples a emissão de certificados digitais sob demanda para assinaturas eletrônicas das prescrições medicamentosas. Isso gera um incremento em segurança, celeridade e desburocratização.

Por fim, apresentamos a viabilidade dos conceitos de provedor de identidade único e autenticação intuitiva, sem toque e com nível de garantia adequado com um protótipo que atendeu as principais características necessárias para essa autenticação.

7 CONSIDERAÇÕES FINAIS

A identidade médica apresentou um avanço com o surgimento da Carteira de Identidade Médica Eletrônica. Ela trouxe a possibilidade de assinatura digital para o médico através de um certificado digital. Porém, na rotina médica diária ela não passou a ser usada, nem para identificação médica nem para a autenticação digital nos diversos sistemas informatizados.

Estruturamos os princípios necessários para uma identidade médica, autenticação e autorização seguras e facilitadas, sem necessidade de *tokens/smartcards*. Seguimos os padrões internacionais de princípios de identificação para o desenvolvimento sustentável, com uma identidade médica eletrônica provida diretamente pelo Conselho Federal de Medicina.

A ligação direta com a CFM como provedor de identidade único e centralizado traz a segurança de atributos e credenciais confiáveis e atuais, podendo ser usadas na autenticação do profissional para diversos provedores de serviços. A entidade da categoria profissional tem a possibilidade de se tornar uma Autoridade de Registro e também Autoridade Certificadora, e assim, emitir certificados digitais que seriam usados para assinaturas qualificadas das prescrições médicas. Isso facilita todo o processo de emissão de documentos médicos eletrônicos, trazendo comodidade e segurança ao usuário.

Outro ponto que nossa proposta trouxe como avanço foi a atenção sobre o nível de garantia da autenticação necessária nos diversos sistemas informatizados para o ato médico. Na atualidade, o nível 1 de garantia é o mais utilizado (inclusive no site do CRM/SC). Após avaliarmos os risco e impactos de uma falha de autenticação, concluímos que o nível 2 é o nível mínimo necessário para autenticação em todas as atividades ligadas a saúde.

Na Revisão Sistemática da Literatura evidenciamos que a preocupação com a autenticação em sistemas informatizados está focada principalmente nos pacientes, sem nenhum método voltado para os profissionais da saúde com a necessidade específica dessa categoria de trabalhadores.

A pandemia do COVID19 trouxe um olhar em busca de processos "limpos", minimizando possíveis contaminações e transmissões de patógenos. É imperativo mostrar alternativas para uma autenticação sem contaminação de mãos e superfícies, com nível de garantia adequado, e que apresente praticidade e método ideal para cada contexto (hospitalar, ambulatorial, de emergência ou de atendimento à distância).

Nossa proposta traz alternativas para cada nível de segurança dentro de um contexto de saúde. A premissa de uma autenticação sem toque com provedor de identidade único foi apresentada e desenvolvemos um protótipo que mostrou a viabilidade da ideia.

O estudo foi focado principalmente no profissional médico, na concepção de um provedor de identidade e autenticação limpa em sistemas informatizados, mas pode e deve ser reproduzido para todos os profissionais da área da saúde com suas devidas particularidades.

7.1 TRABALHOS FUTUROS

Sugere-se que seja implantando no Brasil, um ou mais provedores de identidade para profissionais de saúde. Estes provedores deveriam ser administrados pelos Conselhos de Classe, responsáveis pelo registro de seus profissionais.

Mais estudos são necessários sobre identidade e autenticação eletrônica na área da saúde, considerando sempre o nível de garantia preconizado para cada ambiente e contexto de atendimento. O avanço e as melhorias só serão possíveis com a utilização e a experiência do usuário, vislumbrando um futuro em que o computador registre e valide o ato médico apenas *"vendo e ouvindo"* o que se passa durante o contato médico-paciente. O foco no usuário é primordial para que suas necessidades sejam percebidas e atendidas e que, com isso, ele possa se concentrar plenamente apenas na recuperação da saúde daqueles que o procuram.

Por fim, sugerimos uma atenção especial para o tema da prescrição eletrônica, com estudos que vislumbrem facilitadores para sua dinâmica digital. Trouxemos uma proposta e esperamos que as prescrições eletrônicas (e documentos eletrônicos de saúde em geral) sigam um caminho mais seguro, mas com desburocratização. Temos a perspectiva de que, em um futuro próximo, todas as prescrições e dispensações medicamentosas possam ser elaboradas eletronicamente, inclusive as de talonário especial, com total segurança e comodidade para os profissionais de saúde envolvidos.

REFERÊNCIAS

AGHILI, Seyed Farhad; MALA, Hamid; SHOJAFAR, Mohammad; PERIS-LOPEZ, Pedro. LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. **Future Generation Computer Systems**, Elsevier, Amsterdã, Holanda, v. 96, p. 410–424, 2019. ISSN 0167-739X. DOI: https://doi.org/10.1016/j.future.2019.02.020.

ALAM, Mohammad Tauhidul; ALI, Md Liakot. A Model of a Secured Smart e-Health System. *In*: INTERNATIONAL Conference on Industrial Engineering and Operations Management. Kuala Lumpur, Malaysia: IEOM Society, 2016. P. 2174–2181.

AMIN, Ruhul; ISLAM, Sk Hafizul; BISWAS, GP; KHAN, Muhammad Khurram; KUMAR, Neeraj. An efficient and practical smart card based anonymity preserving user authentication scheme for TMIS using elliptic curve cryptography. **Journal of medical systems**, Springer, v. 39, n. 11, p. 180, 2015. DOI: https://doi.org/10.1007/s10916-015-0351-y.

AMIRTHALINGAM, G; THANGAVEL, H. Multi-Biometric Authentication Using Deep Learning Classifier for Securing of Healthcare Data. **International Journal of Advanced Trends in Computer Science and Engineering**, v. 8, n. 4, p. 1340–1347, 2019.

ANSELMO JUNIOR, Ari Silveira. **Gerenciamento de identidades como um serviço para ambientes de computação em nuvem**. 2011. F. 84. Diss. (Mestrado) – Programa de Pós Graduação em Ciências da Computação (PPGCC) da Universidade Federal de Santa Catarina (UFSC). Disponível em: http://repositorio.ufsc.br/xmlui/handle/123456789/95004.

ARAÚJO, Ronald. Uma identidade eletrônica para uma sociedade digital. Acessado em 01/09/2020. Brasília, fev. 2020. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2020/identidade-eletronica-sociedade-digital.

AWASTHI, Amit K.; SRIVASTAVA, Keerti. A Biometric Authentication Scheme for Telecare Medicine Information Systems with Nonce. **J. Med. Syst.**, Plenum Press, USA, v. 37, n. 5, p. 1–4, out. 2013. ISSN 0148-5598. Disponível em: https://doi.org/10.1007/s10916-013-9964-1.

BARROS, Leonardo. **Atestado médico falso: como lidar com essa situação**. Minas Gerais: Tangerino, jan. 2020. Acessado em 27/07/2020. Disponível em: https://blog.tangerino.com.br/atestado-medico-falso-como-lidar-com-essa-situacao/.

BATISTA NETO, Luiz Aurélio. **Um mecanismo de integração de identidades federadas entre Shibboleth e SimpleSAMLphp para aplicações de nuvens**. 2014. F. 108. Diss. (Mestrado) – Programa de Pós-Graduação em Engenharia de Eletricidade da Universidade Federal do Maranhão (UFMA), São Luiz. Disponível em: https://tedebc.ufma.br/jspui/handle/tede/tede/1784.

BHARATH, R; CHANDRASHEKAR, Dusa; AKKALA, Vivek; KRISHNA, Divya; PONDURI, Harsha; RAJALAKSHMI, P; DESAI, Uday B. Portable ultrasound scanner for remote diagnosis. *In*: 2015 17th

International Conference on E-health Networking, Application Services (HealthCom). Boston, MA, USA: IEEE, 2015. P. 211–216. DOI: 10.1109/HealthCom.2015.7454500.

BLOBEL, Bernd; PHAROW, Peter. Secure Communications and Co-operations in Open Networks. **Technology**, v. 4, p. 7, 1999.

BOYSEN, Andre. The Need for a National Digital Identity Infrastructure. Centre for International Governance Innovation, Canada, p. 37–40, 2019. Acessado em 11/09/2020. Disponível em: https://www.cigionline.org/articles/need-national-digital-identity-infrastructure?utm_source=cigi_newsletter%5C&utm_medium=email%5C&utm_campaign=beware-fake-news.

BRASIL. **Decreto N^o 20.931, de 11 de Janeiro de 1932**: Regula e fiscaliza o exercício da medicina, da odontologia, da medicina veterinária e das profissões de farmacêutico, parteira e enfermeira, no Brasil, e estabelece penas. Rio de Janeiro: [*s.n.*], 1932. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1930-1949/D20931.htm.

BRASIL. **Lei N^o 12.037, de 1 de Outubro de 2009**: Dispõe sobre a identificação criminal do civilmente identificado, regulamentando o art. 5º, inciso LVIII, da Constituição Federal. Brasília, DF: Diário Oficial da União, 2009. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12037.htm.

BRASIL. **Lei N^o 13.709, de 14 de Agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: [*s.n.*], 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

BRASIL. **Lei N^o 13.989, de 15 de Abril de 2020**: Dispõe sobre o uso da telemedicina durante a crise causada pelo coronavírus (SARS-CoV-2). Brasília, DF: Diário Oficial da União, 2020a. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-13.989-de-15-de-abril-de-2020-252726328.

BRASIL. **Lei N^o 14.063, de 23 de Setembro de 2020**: Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos; e altera a Lei nº 9.096, de 19 de setembro de 1995, a Lei nº 5.991, de 17 de dezembro de 1973, e a Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Brasília, DF: Diário Oficial da União, 2020b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14063.htm.

BRASIL. **Lei N^o 6.206, de 7 de Maio de 1975**: Dá valor de documento de identidade às carteiras expedidas pelos órgãos fiscalizadores de exercício profissional e dá outras providências. Brasília, DF: Diário Oficial da União, 1975. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l6206.htm.

BRASIL. **Medida Provisória N^o 2.200-2, de 24 de Agosto de 2001**: Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação

em autarquia, e dá outras providências. Brasília, DF: [*s.n.*], 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm.

BRASIL. **Medida Provisória N^o 983, de 16 de Junho de 2020**: Dispõe sobre as assinaturas eletrônicas em comunicações com entes públicos e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos. Brasília, DF: [*s.n.*], 2020c. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Mpv/mpv983.htm.

CABRAL, Carlos; CAPRINO, Willian Okuhara. **Trilhas em Segurança da Informação: caminhos e ideias para a proteção de dados**. Rio de Janeiro: Brasport, 2015. P. 256. ISBN 9788574526867.

ÇAĞDAŞ, Volkan; STUBKJÆR, Erik. Design research for cadastral systems. **Computers, Environment and Urban Systems**, Elsevier, v. 35, n. 1, p. 77–87, 2011.

CÂMARA, Marlon. **Bluetooth: O que é e como funciona**. [*S.l.*]: Globo Comunicação e Participações S.A., jan. 2012. Acessado em 25/07/2021. Disponível em: https://www.techtudo.com.br/artigos/noticia/2012/01/bluetooth-o-que-e-e-como-funciona.html.

CERTFORUM. **Certificado de Atributo Digital na ICP-Brasil**. Brasília: Serasa e Microsoft, 2007. Acessado em 30/07/2021. Disponível em: http://www.certificadodigital.com.br/certforum2007/WhitePaperCertificadoAtributoDigital.pdf.

CFM. **Chegou o E-CRM**. Brasília: Conselho Federal de Medicina (CFM), ago. 2020a. Acessado em 10/08/2020. Disponível em: http://ecrm.cfm.org.br/.

CFM. **CRM Digital**. Brasília: Portal Médico 2010 do Conselho Federal de Medicina (CFM), jul. 2020b. Acessado em 17/07/2020. Disponível em: https://portal.cfm.org.br/crmdigital/crm-digital.html.

CFM. **Entra em funcionamento serviço que permite validar receitas médicas e atestados digitais**. Brasília: Conselho Federal de Medicina (CFM), abr. 2020c. Acessado em 27/07/2020. Disponível em: https://portal.cfm.org.br/index.php?option=com_content%5C&view=article%5C&id=28674:2020-04-23-13-38-34%5C&catid=3.

CFM. **Expedição de cédula de Identidade Médica e Carteira Profissional de Médico**. Brasília: Conselho Federal de Medicina (CFM), mai. 2010. Acessado em 27/07/2020. Disponível em: https://portal.cfm.org.br/index.php?option=com_content%5C&view=article%5C&id=84:expedicao-de-identidade-medica%5C&catid=31:requerimento.

CFM. **Prescrição Eletrônica**. Brasília: Conselho Federal de Medicina (CFM), 2020d. Acessado em 26/07/2020. Disponível em: https://prescricaoeletronica.cfm.org.br/.

CFM. **Resolução N^o 1.643, de 26 de Agosto de 2002**: Define e disciplina a prestação de serviços através da Telemedicina. Brasília, DF: Conselho Federal de Medicina (CFM), 2002. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1643.

CFM. **Resolução N^o 1.931, de 24 de Setembro de 2009**: Aprova o Código de Ética Médica. Brasília, DF: Conselho Federal de Medicina (CFM), 2009. Disponível em: http://portal.cfm.org.br/images/stories/biblioteca/codigo%5C%20de%5C%20etica%5C%20medica.pdf.

CFM. **Resolução N^o 1.974, de 14 de Julho de 2011**: Estabelece os critérios norteadores da propaganda em Medicina, conceituando os anúncios, a divulgação de assuntos médicos, o sensacionalismo, a autopromoção e as proibições referentes à matéria. Brasília, DF: Conselho Federal de Medicina (CFM), 2011. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2011/1974.

CFM. **Resolução N^o 1.983, de 22 de Março de 2012**: Normatiza o CRM Digital para vigorar como cédula de identidade dos médicos inscritos nos Conselhos Regionais de Medicina. Brasília, DF: Conselho Federal de Medicina (CFM), 2012. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2012/1983.

CFM. **Resolução N^o 2.069, de 29 de Abril de 2014**: Padroniza a identificação dos médicos (em placas, impressos, batas ou vestimentas e/ou crachás) nos estabelecimentos de assistência médica ou de hospitalização (serviços de saúde), públicos e privados, em todo o território nacional. Brasília, DF: Conselho Federal de Medicina (CFM), 2014. Disponível em: https://sistemas.cfm.org.br/normas/arquivos/resolucoes/BR/2014/2069_2014.pdf.

CFM. **Resolução N^o 2.119, de 20 de Agosto de 2015**: Altera o artigo 3^o da Resolução CFM n^o 2.069/14, que padroniza a identificação dos médicos (em placas, batas ou vestimentas e/ou crachás) nos estabelecimentos de assistência médica ou de hospitalização (serviços de saúde), públicos e privados, em todo o território nacional. Brasília, DF: Conselho Federal de Medicina (CFM), 2015. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2015/2119.

CFM. **Resolução N^o 2.145, de 27 de Outubro de 2016**: Aprova o Código de Processo Ético-Profissional (CPEP) no âmbito do Conselho Federal de Medicina (CFM) e Conselhos Regionais de Medicina (CRMs). Brasília, DF: Conselho Federal de Medicina (CFM), 2016a. Disponível em: https://sistemas.cfm.org.br/normas/arquivos/resolucoes/BR/2016/2145_2016.pdf.

CFM. **Resolução N^o 2.147, de 17 de Junho de 2016**: Estabelece normas sobre a responsabilidade, atribuições e direitos de diretores técnicos, diretores clínicos e chefias de serviço em ambientes médicos. Brasília, DF: Conselho Federal de Medicina (CFM), 2016b. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2016/2147.

CFM. **Resolução N^o 2.158, de 27 de Janeiro de 2017**: Altera o artigo 1^o da Resolução CFM n^o 2145/2016 - Código de Processo Ético-Profissional - CPEP, publicada no D.O.U. de 27 de outubro de 2016, Seção I, p. 329. Brasília, DF: Conselho Federal de Medicina (CFM), 2017. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2017/2158.

CFM. **Resolução N^o 2.227, de 6 de Fevereiro de 2019**: Define e disciplina a telemedicina como forma de prestação de serviços médicos mediados por tecnologias. Brasília, DF: Conselho Federal de Medicina (CFM), 2019a. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2018/2227.

CFM. **Resolução N^o 2.228, de 6 de Março de 2019**: Revoga a Resolução CFM n^o 2.227, publicada no D.O.U. de 6 de fevereiro de 2019, Seção I, p.58, a qual define e disciplina a telemedicina como forma de prestação de serviços médicos mediados por tecnologias, e restabelece expressamente a vigência da Resolução CFM n^o 1.643/2002, publicada no D.O.U. de 26 de agosto de 2002, Seção I, p.205. Brasília, DF: Conselho Federal de Medicina (CFM), 2019b. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2019/2228.

CFM. **Resolução N^o 2.233, de 21 de Agosto de 2019**: Normatiza a Cédula de Identidade Médica (CIM) dos profissionais inscritos nos Conselhos Regionais de Medicina, nas suas versões em cartão (CRM DIGITAL) e para dispositivos móveis (E-CRM), e dá outras providências. Brasília, DF: Conselho Federal de Medicina (CFM), 2019c. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2019/2233.

CFM. **Resolução N^o 2.275, de 9 de Abril de 2020**: Altera a Resolução CFM n^o 2145/2016, que aprovou o Código de Processo Ético-Profissional (CPEP) no âmbito do Conselho Federal de Medicina (CFM) e Conselhos Regionais de Medicina (CRMs) e altera a Resolução CFM n^o 2.234/2019, que dispõe sobre a tramitação eletrônica da sindicância, do processo ético-profissional, do procedimento administrativo para apuração de doença incapacitante do médico, do processo-consulta, da proposta de resolução e da proposta de recomendação no âmbito dos Conselhos Federal e Regionais de Medicina. Brasília, DF: Conselho Federal de Medicina (CFM), 2020e. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2020/2275.

CFM. **Resolução N^o 2.278, de 2 de Julho de 2020**: AAutoriza a realização por videoconferência de apreciação do relatório conclusivo da sindicância, julgamento de processo ético-profissional e outros processos administrativos, bem como dos atos de instrução e respectivos recursos. Altera a Resolução CFM n^o 2.145/2016 (CPEP), publicada no D.O.U. de 27 de outubro de 2016, Seção I, p.329, e a Resolução CFM n^o 2.234/2019 (PAe), publicada no D.O.U. de 11 de setembro de 2019, Seção I, p.223-4, no âmbito dos Conselhos Federal e Regionais de Medicina. Brasília, DF: Conselho Federal de Medicina (CFM), 2020f. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2020/2278.

CHEN, Chin-Ling; LU, Ming-Shaw; GUO, Zong-Min. A non-repudiated and traceable authorization system based on electronic health insurance cards. **Journal of medical systems**, Springer, v. 36, n. 4, p. 2359–2370, 2012.

CONCEIÇÃO, Rogério Alves da. **Um Protocolo de Autenticação e Autorização Seguro para Arquiteturas Orientadas a Serviços**. 2014. F. 92. Diss. (Mestrado) – Instituto de Ciências Exatas, Departamento de Ciência da Computação, Universidade de Brasília (UnB), Brasília.

CONTI, V; MILITELLO, C; VITABILE, S. Biometric authentication overview: a fingerprint recognition sensor description. **Int J Biosen Bioelectron**, v. 2, n. 1, p. 26–31, 2017. Disponível em: https://medcraveonline.com/IJBSBE/IJBSBE-02-00011.pdf.

CREMESP. **Cremesp adota medidas contra falsos médicos**. São Paulo: CREMESP, jul. 2006. Acessado em 21/07/2020. Disponível em: https://www.cremesp.org.br/?siteAcao=Jornal%5C&id=699.

CRM-PB. **Manual de orientações básicas para prescrição médica**. Brasília, 2011.

DAUGMAN, John. **Results from 200 billion iris cross-comparisons**. Cambridge, UK, 2005. P. 8. Disponível em: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-635.pdf.

DOCUSIGN. **CRM Digital: afinal, o que é esse documento e como os médicos usam?** São Paulo: DocuSign, 2020. Acessado em 26/07/2020. Disponível em: https://www.docusign.com.br/blog/crm-digital-afinal-o-que-e-esse-documento-e-como-os-medicos-usam.

EDITORIAL. **Telemedicina no Brasil: como e por que utilizar assinatura digital na saúde**. Valinhos, SP: Núcleo Contábil, 2020. Acessado em 11/01/2021. Disponível em: https://nucleocontabil.com.br/telemedicina-no-brasil-como-e-por-que-utilizar-assinatura-digital-na-saude/.

FANG, Liming; YIN, Changchun; ZHOU, Lu; LI, Yang; SU, Chunhua; XIA, Jinyue. A physiological and behavioral feature authentication scheme for medical cloud based on fuzzy-rough core vector machine. **Information Sciences**, Elsevier, v. 507, p. 143–160, 2020. ISSN 0020-0255. DOI: https://doi.org/10.1016/j.ins.2019.08.020.

FERREIRA, Pedro Eduardo Nader. **Parecer N^{o} 1, de 31 de Janeiro de 2014**: Autoprescrição de medicamentos e falta de carimbo na receita. Brasília, DF: CFM, 2014. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/pareceres/BR/2014/1.

FONTASA-ROSA, Júlio César; PAULA, Fernando Jorge de; MOTTA, Márcia Vieira da; MUÑOZ, Daniel Romero; SILVA, Moacyr da. Carimbo médico: uma necessidade legal ou uma imposição informal? **Revista da Associação Médica Brasileira**, Elsevier, v. 57, n. 1, p. 16–19, 2011. ISSN 0104-4230. DOI: https://doi.org/10.1590/S0104-42302011000100009.

FONTES, Letícia. **Suposto médico com CRM cassado é preso vendendo atestados em BH**. Belo Horizonte: O Tempo, set. 2019. Acessado em 31/07/2020. Disponível em: https://www.otempo.com.br/cidades/suposto-medico-com-crm-cassado-e-preso-vendendo-atestados-em-bh-1.2234672.

FOTOUHI, Mahdi; BAYAT, Majid; DAS, Ashok Kumar; FAR, Hossein Abdi Nasib; POURNAGHI, S. Morteza; DOOSTARI, M.A. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. **Computer Networks**, Elsevier, Amisterdan, v. 177, p. 107333, 2020. ISSN 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2020.107333. Disponível em: https://www.sciencedirect.com/science/article/pii/S1389128619316457.

FREITAS JUNIOR, Vanderlei; CECI, Flavio; WOSZEZENKI, Cristiane Raquel; GONÇALVES, Alexandre Leopoldo. Design Science Research Methodology Enquanto Estratégia Metodológica para a Pesquisa Tecnológica. **Revista Espacios**, Caracas, Venezuela, v. 38, n. 6, p. 25, 2017.

GALVÃO, Taís Freire; PEREIRA, Mauricio Gomes. Revisões sistemáticas da literatura: passos para sua elaboração. **Epidemiologia e Serviços de Saúde**, SciELO Public Health, v. 23, p. 183–184, mar. 2014. ISSN 1679-4974. Disponível em: http://scielo.iec.gov.br/scielo.php?script=sci_arttext&pid=S1679-49742014000100018&nrm=iso.

GARSON, Kathryn; ADAMS, Carlisle. Security and privacy system architecture for an e-hospital environment. *In*: PROCEEDINGS of the 7th symposium on Identity and trust on the Internet. Gaithersburg, Maryland, USA: Association for Computing Machinery, 2008. (IDtrust '08), p. 122–130. DOI: 10.1145/1373290.1373306. Disponível em: https://doi.org/10.1145/1373290.1373306.

GODINHO, Rafael. **Telemedicina no Brasil: como e por que utilizar assinatura digital na saúde**. [*S.l.*]: Bry Tecnologia, 2021. Acessado em 30/07/2021. Disponível em: https://www.bry.com.br/blog/telemedicina-no-brasil/.

GOV.BR. **O que é Selo de Confiabilidade (Ouro e Prata)? Como posso obter esses selos?** Brasília: Governo do Brasil, 2021. Acessado em 30/07/2021. Disponível em: https://www.gov.br/servidor/pt-br/acesso-a-informacao/faq/acesso-gov.br/5-o-que-e-selo-de-confiabilidade-ouro-e-prata-como-posso-obter-esses-selos.

GOV.BR. **Dúvidas Frequentes da Conta gov.br**. Brasília: Governo do Brasil, 2019. Acessado em 30/08/2020. Disponível em: http://faq-login-unico.servicos.gov.br/en/latest/index.html.

GRASSI, Paul A *et al.* **Digital identity guidelines: Authentication and lifecycle management**. Gaithersburg, MD, USA, 2020a. P. 79. NIST Special Publication 800-63B. DOI: 10.6028/NIST.SP.800-63b.

GRASSI, Paul A; GARCIA, Michael E; FENTON, James L. **Digital identity guidelines**. Gaithersburg, MD, USA, 2020b. P. 75. NIST Special Publication 800-63-3. DOI: https://doi.org/10.6028/NIST.SP.800-63-3.

GUILLÉN-GÁMEZ, Francisco D.; GARCÍA-MAGARIÑO, Iván; BRAVO-AGAPITO, Javier; LACUESTA, Raquel; LLORET, Jaime. A proposal to improve the authentication process in m-health environments. **IEEE Access**, v. 5, p. 22530–22544, 2017. DOI: 10.1109/ACCESS.2017.2752176.

HAN, Song; SKINNER, Geoff; POTDAR, Vidyasagar; CHANG, Elizabeth; WU, Chen. New framework for authentication and authorization for e-health service systems. *In*: IEEE. 2006 IEEE International Conference on Industrial Technology. [*S.l.*: *s.n.*], 2006. P. 2833–2838.

HARDT, Dick. **The OAuth 2.0 Authorization Framework**. [*S.l.*]: IETF, out. 2012. RFC 6749. (Request for Comments, 6749). DOI: 10.17487/RFC6749. Disponível em: https://rfc-editor.org/rfc/rfc6749.txt.

ITI. **Validador de Documentos Digitais**. Brasília: Instituto Nacional de Tecnologia da Informação (ITI), 2020. Acessado em 03/08/2020. Disponível em: https://assinaturadigital.iti.gov.br/.

JAPPUR, Rafael Feyh *et al.* Modelo conceitual para criação, aplicação e avaliação de jogos educativos digitais, 2014.

KAMBOURAKIS, G; MAGLOGIANNIS, I; ROUSKAS, A. PKI-based secure mobile access to electronic health services and data. **Technology and Health Care**, IOS Press, The Netherlands, v. 13, n. 6, p. 511–526, 2005. DOI: 10.3233/THC-2005-13606.

KHATOON, Abida; UMADEVI, V. Integrating OAuth and Aadhaar with e-Health care System. *In*: 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT). Bangalore, India: IEEE, 2018. P. 1681–1686. DOI: 10.1109/RTEICT42901.2018.9012487.

KITCHENHAM, Barbara A. Systematic Review in Software Engineering: Where We Are and Where We Should Be Going. *In*: PROCEEDINGS of the 2nd International Workshop on Evidential Assessment of Software Technologies. Lund, Sweden: Association for Computing Machinery, 2012. (EAST '12), p. 1–2. DOI: 10.1145/2372233.2372235.

KRAWCZYK, Stephen; JAIN, Anil K. Securing electronic medical records using biometric authentication. *In*: INTERNATIONAL Conference on Audio-and Video-Based Biometric Person Authentication. Berlin: Springer, 2005. P. 1110–1119. DOI: https://doi.org/10.1007/11527923_115.

LACERDA, Daniel Pacheco; DRESCH, Aline; PROENÇA, Adriano; ANTUNES JÚNIOR, José Antonio Valle. Design Science Research: método de pesquisa para a engenharia de produção. **Gestão & Produção**, Cubo, v. 20, n. 4, nov. 2013.

LAURENT, Maryline; BOUZEFRANE, Samia. **Digital identity management**. London, UK: Elsevier, 2015. P. 272.

LBCA. **LGPD no RH: O que o seu setor precisa para se adequar**. São Paulo: LGPD Brasil, jul. 2021. Acessado em 25/07/2021. Disponível em: https://www.lgpdbrasil.com.br/lgpd-no-rh-o-que-o-seu-setor-precisa-para-se-adequar/.

LEE, T.-F.; LIU, C.-M. A secure smart-card based authentication and key agreement scheme for telecare medicine information systems. **Journal of Medical Systems**, v. 37, n. 3, 2013. DOI: https://doi.org/10.1007/s10916-013-9933-8.

LEE, Tian-Fu; CHANG, I-Pin; WANG, Ching-Cheng. Simple group password-based authenticated key agreements for the integrated EPR information system. **Journal of medical systems**, Springer, v. 37, n. 9916, p. 1–6, 2013. DOI: https://doi.org/10.1007/s10916-012-9916-1.

LIMA E SILVA, Sérgio Roberto de. **Telemedicina no Brasil: como e por que utilizar assinatura digital na saúde**. Florianópolis: BRy, abr. 2020. Acessado em 26/07/2020. Disponível em: https://www.bry.com.br/blog/telemedicina-no-brasil/.

LOUK, Maya; LIM, Hyotaek; LEE, Hoon Jae. Security system for healthcare data in cloud computing. **International Journal of Security and Its Applications**, v. 8, n. 3, p. 241–248, 2014. Disponível em: https://www.earticle.net/Article/A230942.

MAHTO, Dindayal; YADAV, Dilip Kumar. Cloud-based Secure TeleMedicine Information System using Crypto-Biometric Techniques. **EAI Endorsed Trans. Pervasive Health Technol.**, v. 5, n. 20, e3, 2020. Disponível em: https://pdfs.semanticscholar.org/8083/d3ca537683dcbe9761dfadc9cc05a93138eb.pdf.

MARCH, Salvatore T; SMITH, Gerald F. Design and natural science research on information technology. **Decision support systems**, Elsevier, v. 15, n. 4, p. 251–266, 1995. ISSN 0167-9236. DOI: https://doi.org/10.1016/0167-9236(94)00041-2.

MASDARI, Mohammad; AHMADZADEH, Safiyyeh. A survey and taxonomy of the authentication schemes in Telecare Medicine Information Systems. **Journal of Network and Computer Applications**, Elsevier, v. 87, p. 1–19, 2017. ISSN 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2017.03.003.

MELO, Mauro José Araújo de. **Modelo de autenticação para sistemas de computação em nuvem**. 2013. F. 101. Diss. (Mestrado) – Programa de Pós-Graduação em Engenharia de Eletricidade da Universidade Federal do Maranhão (UFMA), São Luiz, MA. Disponível em: https://tedebc.ufma.br/jspui/handle/tede/tede/513.

MENEZES, Karina. **O que é a regulamentação eIDAS?** São Paulo: idwall, 2019. Acessado em 31/07/2021. Disponível em: https://blog.idwall.co/o-que-e-a-regulamentacao-eidas/.

MS. **Portaria N^o 344, de 12 de Maio de 1998**: Aprova o Regulamento Técnico sobre substâncias e medicamentos sujeitos a controle especial. Brasília, DF: Ministério da Saúde, 1998. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/svs/1998/prt0344_12_05_1998_rep.html.

MS. **Portaria N^o 467, de 20 de Março de 2020**: Dispõe, em caráter excepcional e temporário, sobre as ações de Telemedicina, com o objetivo de regulamentar e operacionalizar as medidas de enfrentamento da emergência de saúde pública de importância internacional previstas no art. 3^o da Lei nº 13.979, de 6 de fevereiro de 2020, decorrente da epidemia de COVID-19. Brasília, DF: Ministério da Saúde, 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/portaria/prt/portaria%5C%20n%5C%C2%5C%BA%5C%20467-20-ms.htm.

NANDAKUMAR, Karthik; JAIN, Anil K. Biometric Template Protection: Bridging the performance gap between theory and practice. **IEEE Signal Processing Magazine**, IEEE, New York City, v. 32, n. 5, p. 88–100, 2015. DOI: 10.1109/MSP.2015.2427849.

AL-NAYADI, Fahed; ABAWAJY, Jemal H. An Authentication Framework for e-Health Systems. *In*: 2007 IEEE International Symposium on Signal Processing and Information Technology. Giza, Egypt: IEEE, 2007. P. 616–620. DOI: 10.1109/ISSPIT.2007.4458207.

OIDF. **Welcome to OpenID Connect**. San Ramon, USA: OpenID Foundation (OIDF), 2020. Acessado em 10/08/2020. Disponível em: https://openid.net/connect/.

OMETOV, Aleksandr; BEZZATEEV, Sergey; MÄKITALO, Niko; ANDREEV, Sergey; MIKKONEN, Tommi; KOUCHERYAVY, Yevgeni. Multi-factor authentication: A survey. **Cryptography**, Multidisciplinary Digital Publishing Institute, v. 2, n. 1, p. 1, 2018.

PANSE, Trishna; KAPOOR, Vivek. A review on security mechanism of Bluetooth communication. **International Journal of Computer Science and Information Technologies**, Tech Science Publications, v. 3, n. 2, p. 3419–3422, 2012.

PEDROSO, Marcelo Caldeira; ZWICKER, Ronaldo; SOUZA, Cesar Alexandre de. Adoção de RFID no Brasil: um estudo exploratório. **RAM. Revista de Administração Mackenzie**, SciELO Brasil, v. 10, n. 1, p. 12–36, 2009. DOI: https://doi.org/10.1590/S1678-69712009000100002.

PEFFERS, Ken; TUUNANEN, Tuure; ROTHENBERGER, Marcus A; CHATTERJEE, Samir. A design science research methodology for information systems research. **Journal of management information systems**, Routledge, v. 24, n. 3, p. 45–77, 2007. DOI: 10.2753/MIS0742-1222240302.

PETTICREW, Mark; ROBERTS, Helen. **Systematic reviews in the social sciences: A practical guide**. Oxford, UK: Blackwell Publishing Professional, 2008. P. 336.

POTDAR, Mayur S.; MANEKAR, Amitkumar S.; KADU, Rajesh D. Android "Health-Dr."Application for Synchronous Information Sharing. *In*: 2014 Fourth International Conference on Communication Systems and Network Technologies. Bhopal, India: IEEE, 2014. P. 265–269. DOI: 10.1109/CSNT.2014.58.

RANA, S.; KANG, S.S. Implementation of biological key based security technique in wireless body area networks. **International Journal of Innovative Technology and Exploring Engineering**, v. 8, n. 8, p. 2156–2163, 2019. cited By 1. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85067896873%5C&partnerID=40%5C&md5=556a943ca9e40c032a126fdde2147d2a.

RED HAT. **Keycloak**. Raleigh, NC, USA: Red Hat, 2014. Acessado em 19/07/2021. Disponível em: https://www.keycloak.org/.

REDAÇÃO JORNAL DE BRASÍLIA. **Falso médico que atendia pacientes com Covid-19 é preso em Hospital**. Brasília: Jornal de Brasília, jun. 2020. Acessado em 27/07/2020. Disponível em: https://jornaldebrasilia.com.br/nahorah/falso-medico-que-atendia-pacientes-com-covid-19-e-preso-em-hospital/.

SAFKHANI, Masoumeh; BAGHERI, Nasour; NADERI, Majid. On the designing of a tamper resistant prescription RFID access control system. **Journal of medical systems**, Springer, v. 36, n. 6, p. 3995–4004, 2012. DOI: https://doi.org/10.1007/s10916-012-9872-9.

SAIF, Sohail; GUPTA, Rajni; BISWAS, Suparna. Implementation of Cloud-Assisted Secure Data Transmission in WBAN for Healthcare Monitoring. *In*: BHATTACHARYYA, Siddhartha; CHAKI, Nabendu;

KONAR, Debanjan; CHAKRABORTY, Udit Kr.; SINGH, Chingtham Tejbanta (Ed.). **Advanced Computational and Communication Paradigms**. Singapore: Springer Singapore, 2018. P. 665–674. DOI: https://doi.org/10.1007/978-981-10-8237-5_64.

SALEEM, Kashif; DERHAB, Abdelouahid; AL-MUHTADI, Jalal; SHAHZAD, Basit. Human-oriented design of secure Machine-to-Machine communication system for e-Healthcare society. **Computers in Human Behavior**, Elsevier, v. 51, p. 977–985, 2015.

SANTOS, Eduardo dos. **Formalização e verificação de um protocolo de autenticação multifator**. 2012. F. 161. Diss. (Mestrado) – Programa de Pós-Graduação em Ciência da Computação (UFSC), Florianópolis, SC. Disponível em: https://repositorio.ufsc.br/handle/123456789/100627.

SANTOS, Eduardo dos; MARTINA, Jean Everson; CUSTÓDIO, Ricardo. Towards a Formal Verification of a Multi-factor Authentication Protocol Using Automated Theorem Provers. *In*: 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. Liverpool, UK: IEEE, 2012. P. 84–91. DOI: 10.1109/TrustCom.2012.278.

SATOH, Hitoshi; NIKI, Noboru; EGUCHI, Kenji; OHMATSU, Hironobu; KANEKO, Masahiro; KAKINUMA, Ryutaro; MORIYAMA, Noriyuki. Computer-aided diagnosis workstation and teleradiology network system for chest diagnosis using the web medical image conference system with a new information security solution. *In*: LIU, Brent J.; BOONN, William W. (Ed.). **Medical Imaging 2010: Advanced PACS-based Imaging Informatics and Therapeutic Applications**. San Diego, California, United States: SPIE, 2010. International Society for Optics e Photonics, p. 290–301. Disponível em: https://doi.org/10.1117/12.843948.

SHIN, YongNyuo; LEE, YongJun; SHIN, Woochang; CHOI, Jinyoung. Designing Fingerprint-Recognition-Based Access Control for Electronic Medical Records Systems. *In*: 22ND International Conference on Advanced Information Networking and Applications and Workshops (AINAW). Gino-wan, Japan: IEEE, 2008. P. 106–110. DOI: 10.1109/WAINA.2008.289.

SIMON, Herbert Alexander. **The Sciences of the Artificial**. 3. ed. Cambridge, MA, USA: MIT Press, 1996. P. 241.

SIMON, Herbert Alexander. **The sciences of the artificial**. Cambridge, MA, USA: MIT Press, 1969.

SOARES, Rafael Ramos. **LEI GERAL DE PROTEÇÃO DE DADOS–LGPD: DIREITO À PRIVACIDADE NO MUNDO GLOBALIZADO**. Goiânia, GO, 2020. P. 31. TCC Direito. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1201.

SOARES, Rualyson Cavalcante. **Aspectos teóricos de segurança em RFID**. Rio Tinto, PB, 2018. Trabalho de Conclusão de Curso de Graduação. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/17163.

SONG, Won Jay; AHN, Byung Ha; KIM, Won Hee. Healthcare information systems using digital signature and synchronized smart cards via the Internet. *In*: PROCEEDINGS. International Conference

on Information Technology: Coding and Computing. Las Vegas, NV, USA: IEEE, 2002. P. 177–182. DOI: 10.1109/ITCC.2002.1000383.

SUDHA, G; GANESAN, R. Secure transmission medical data for pervasive healthcare system using android. *In*: 2013 International Conference on Communication and Signal Processing. Melmaruvathur, India: IEEE, 2013. P. 433–436. DOI: 10.1109/iccsp.2013.6577090.

VERZELETTI, Glaidson Menegazzo; WANGHAM, Michelle Silva; MELLO, Emerson Ribeiro de; TORRES, José Alberto Sousa. Um Estudo Comparativo de Estratégias Nacionais de Gestão de Identidades para Governo Eletrônico. *In*: IV Workshop de Gestao de Identidades (WGID), XIV Simpósio Brasileiro em Segurança da Informaçao e de Sistemas Computacionais (SBSeg). Belo Horizonte: SBC, 2014. P. 480–489.

WORLD BANK. **Practitioner's Guide: About this Guide**. Washington, DC, USA: World Bank, 2019a. Acessado em 14/04/2021. Disponível em: https://id4d.worldbank.org/guide/about-guide.

WORLD BANK. **Practitioner's Guide: Credentials & Authentication**. Washington, DC, USA: World Bank, 2019b. Acessado em 17/04/2021. Disponível em: https://id4d.worldbank.org/guide/credentials-authentication.

WORLD BANK. **Practitioner's Guide: Identity lifecycle**. Washington, DC, USA: World Bank, 2019c. Acessado em 16/04/2021. Disponível em: https://id4d.worldbank.org/guide/identity-lifecycle.

WORLD BANK. **Practitioner's Guide: Levels of assurance (LOAs)**. Washington, DC, USA: World Bank, 2019d. Acessado em 20/04/2021. Disponível em: https://id4d.worldbank.org/guide/levels-assurance-loas.

WORLD BANK. **Practitioner's Guide: Types of credentials and authenticators**. Washington, DC, USA: World Bank, 2019e. Acessado em 17/04/2021. Disponível em: https://id4d.worldbank.org/guide/types-credentials-and-authenticators.

WORLD BANK. **Principles on identification**. Washington, DC, USA: World Bank, 2019f. Acessado em 15/04/2021. Disponível em: https://id4d.worldbank.org/principles.

ZÚQUETE, André; GOMES, Helder; SILVA CUNHA, João Paulo da. Authentication of Professionals in the RTS E-Health System. *In*: INSTICC. FIRST International Conference on Health Informatics (HEALTHINF 2008). Funchal, Madeira, Portugal: SciTePress, 2008. P. 72–80. DOI: 10.5220/0001043200720080.