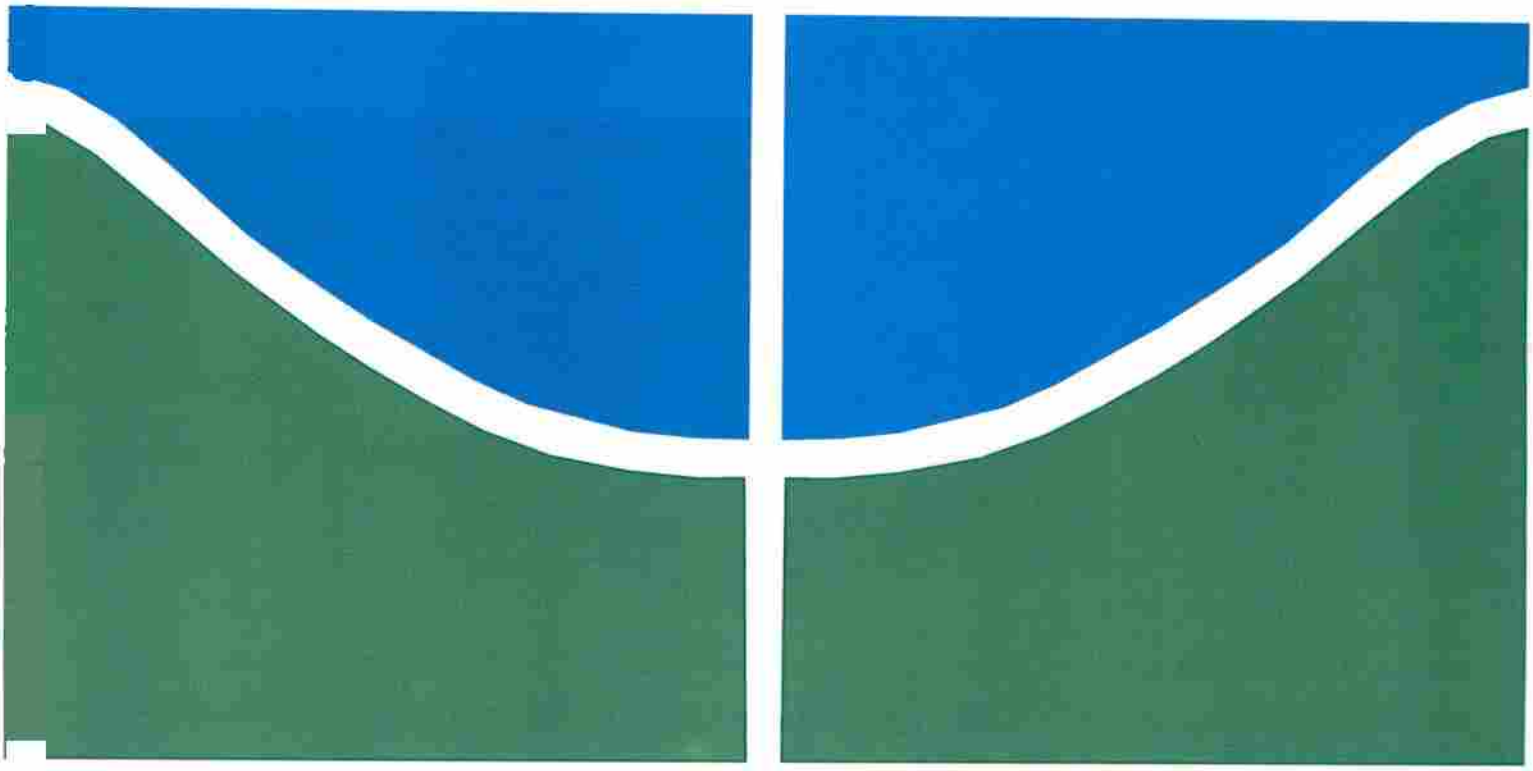

AUTENTICAÇÃO DIGITAL: CONFORMIDADE FIDO ALLIANCE

RAFAEL KASTEIN MORELLI

MONOGRAFIA DE ESPECIALIZAÇÃO EM GESTÃO DA SEGURANÇA DA INFORMAÇÃO

FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

AUTENTICAÇÃO DIGITAL: CONFORMIDADE FIDO ALLIANCE

RAFAEL KASTEIN MORELLI

ORIENTADOR: LAERTE PEOTTA DE MELO

MONOGRAFIA DE ESPECIALIZAÇÃO EM GESTÃO DA SEGURANÇA DA INFORMAÇÃO

PUBLICAÇÃO: UnBLabRedes.MFE.010/2017
BRASÍLIA, DF: AGOSTO/2017

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

AUTENTICAÇÃO DIGITAL: CONFORMIDADE FIDO ALLIANCE

RAFAEL KASTEIN MORELLI

TRABALHO DE CONCLUSÃO DE CURSO SUBMETIDO AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGOA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO TÍTULO DE ESPECIALISTA EM GESTÃO DA SEGURANÇA DA INFORMAÇÃO.

APROVADO POR:

_____

LAERTE PEOTTA DE MELO
DOUTOR, UNB/BB (ORIENTADOR)

_____

EDNA DIAS CANEDO
DOUTORA, UNB/FGA (EXAMINADOR INTERNO)

_____

ELIANE CARNEIRO SOARES
MESTRE, SEEDF (EXAMINADOR EXTERNO)

BRASÍLIA, DF, 15 DE AGOSTO DE 2017.

FICHA CATALOGRÁFICA

Morelli, Rafael Kastein.

Autenticação Digital: Conformidade FIDO Alliance [Distrito Federal], 2017.

63p., 210 x 297mm (ENE/FT/UnB, Especialização, Engenharia Elétrica, 2017).

Monografia – Universidade de Brasília, Faculdade de Tecnologia.

Departamento de Engenharia Elétrica.

1. Segurança da Informação
2. Identidade Digital
3. Autenticação Digital
4. Conformidade

I. ENE/FT/Unb

II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

Morelli, Rafael Kastein. (2017). Autenticação Digital: Conformidade FIDO Alliance. Monografia de Especialização, Publicação UnBLabRedes.MFE.010/2017, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 63p.

CESSÃO DE DIREITOS

AUTOR: Rafael Kastein Morelli

TITULO DA MONOGRAFIA: Autenticação Digital: Conformidade FIDO Alliance.

GRAU/ANO: Especialização/2017

Rafael Kastein Morelli
Rua das Pitangueiras, Lote 10, Apartamento 308
Águas Claras Sul
CEP: 71.938-540 – Brasília – DF
Tel. 55 – 61 – 993842260 / Email: kmorelli@gmail.com

AGRADECIMENTOS

Gostaria de agradecer primeiramente à minha família, pelo apoio e compreensão devido à distância por tanto tempo enquanto me dedicava a este trabalho.

Agradeço também à Adriana e ao Luciano da secretaria do LabRedes, por todo o suporte e por nos ter ajudado a concluir o trabalho.

E finalmente, porém não menos importante, ao Professor e orientador Laerte Peotta, por todo o apoio, paciência, e por ter acreditado neste trabalho.

Meus sinceros agradecimentos.

RESUMO

AUTENTICAÇÃO DIGITAL: CONFORMIDADE FIDO ALLIANCE

Autor: Rafael Kastein Morelli
Orientador: Professor Dr. Laerte Peotta de Melo
Especialização em Gestão da Segurança da Informação
Brasília, 15 de agosto de 2017

As senhas que os usuários costumam utilizar no dia a dia não são mais consideradas tão seguras. É necessário avaliar o risco do negócio ao expor serviços críticos com um nível de segurança tão fraco. O risco está em quanto uma aplicação confia que o usuário por trás da solicitação do serviço realmente é quem diz ser. Para isso, é necessário implementar mecanismos mais seguros que somente uma senha para aumentar esta confiança. O mundo está despertando para esta realidade, portanto é preciso oferecer alternativas robustas e confiáveis para cumprir as expectativas. A FIDO Alliance oferece tais mecanismos que podem aumentar a segurança na identificação e autenticação do usuário. A proposta da FIDO Alliance é padronizar a comunicação entre os autenticadores e a aplicação, facilitando a implementação de diversos mecanismos de autenticação e melhorando a experiência do usuário. Em paralelo ao surgimento destes mecanismos, também são publicados normativos e recomendações de segurança sobre como tais mecanismos devem se comportar. Antes que tais normativos se tornem mandatórios, é importante avaliar o quanto a FIDO Alliance está alinhada, de forma a atestar o seu valor como padronização de mecanismos de autenticação.

ABSTRACT

DIGITAL AUTHENTICATION: FIDO ALLIANCE COMPLIANCE

Author: Rafael Kastein Morelli
Supervisor: Professor Dr. Laerte Peotta de Melo
Especialização em Gestão da Segurança da Informação
Brasília, 15 August 2017

Passwords that users often use on a day-to-day basis are no longer considered as secure. It is necessary to evaluate the business risk by exposing critical services with such a poor security level. The risk lies in how much an application trusts that the user behind the service request really is who it claims to be. For this, it is necessary to implement more secure mechanisms than just a password to increase this trust. The world is awakening to this reality, so it is necessary to offer robust and reliable alternatives to meet expectations. The FIDO Alliance offers such mechanisms that can increase security in the identification and authentication of the user. The FIDO Alliance proposal is to standardize the communication between the authenticators and the application, facilitating the implementation of several authentication mechanisms and improving the user experience. In parallel to the emergence of these mechanisms, normative and security recommendations are also published on how such mechanisms should behave. Before such regulations become mandatory, it is important to assess how well the FIDO Alliance is aligned, in order to attest to its value as standardization of authentication mechanisms.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE ACRÔNIMOS

ECDSA	*Elliptic Curve Digital Signature Algorithm*
FIDO	*Fast IDentity Online*
FIPS	*Federal Information Processing Standard*
HMAC	*Hash-based Message Authentication Code*
HOTP	*HMAC-Based One Time Password*
MitM	*Man in the Middle*
NIST	*National Institute of Standards and Technology*
OTP	*One Time Password*
QRCode	*Quick Response Code*
RSA	*Rivest, Shamir, Adleman*
SHA	*Secure Hash Algorithm*
SM	*Security Measures*
TLS	*Transport Layer Security*
TOTP	*Time-Based One Time Password Algorithm*
UAF	*Universal Authentication Framework*
URL	*Uniform Resource Locator*
USB	*Universal Serial Bus*
U2F	*Universal 2nd Factor*

1. INTRODUÇÃO

Geralmente um provedor de serviço na internet, ao fornecer um determinado serviço a um usuário, necessita identifica-lo e armazenar algumas informações pessoais e de configurações personalizadas do serviço. Este cadastramento do usuário geralmente envolve a definição de um identificador e uma senha.

A senha é uma maneira tradicional e a mais utilizada para um usuário se autenticar na internet, também é a mais simples de ser implementada. No entanto, muitos usuários são descuidados e cometem diversas práticas inseguras em relação a guarda da senha.

Há usuários que acabam criando senhas que são facilmente dedutíveis, seja porque dão pouca importância, ou porque é simples de guardar. Se a senha é muito difícil de guardar, acabam anotando em algum lugar onde qualquer pessoa pode eventualmente ver. Os usuários também podem ser vítimas de diversos ataques, onde o fraudador acaba obtendo a senha. As formas de ataque são muitas, como engenharia social, onde o usuário é induzido a fornecer suas informações voluntariamente, páginas falsas, e instalação de programas maliciosos capazes de capturar a senha no computador.

A senha é uma credencial fraca e suscetível a diversos ataques. Confiar unicamente nela apresenta um risco de segurança que varia de acordo com o prejuízo decorrente do resultado do ataque, desde uma invasão a uma conta pessoal de correio eletrônico até a uma conta bancária.

No entanto, a senha não é a única forma de autenticação que existe, também nada impede que o usuário utilize mais de um método de uma só vez para provar a sua identidade.

Diversas tecnologias emergentes estão ao alcance dos usuários, pois estão presentes na maioria dos smartphones hoje em dia. É possível utilizar a câmera do seu dispositivo para reconhecimento facial ou ocular, o microfone para reconhecimento de voz, e em um conjunto pouco menor de dispositivos, estão presentes leitores de impressão digital.

1.1. MOTIVAÇÃO

A dispensa da senha como método padrão de autenticação está começando a ser considerada e amplamente discutida. O Reino Unido anunciou que irá dobrar o investimento em segurança cibernética, sendo que uma das iniciativas será reforçar a segurança no acesso a dados pessoais dos seus cidadãos. Isso implica em investir em tecnologias de autenticação mais confiáveis. Inclusive, a utilização de padrões definidos pela FIDO Alliance para criar métodos de autenticação sem utilização de senhas faz parte da iniciativa (BONDERUD, 2016).

A US Commission on Enhancing National Cybersecurity, um grupo de trabalho criado em 2016, emitiu um relatório com recomendações para aumentar a segurança cibernética em ambos os setores, público e privado. Uma das recomendações é justamente uma iniciativa público-privada para aumentar a segurança da autenticação de usuários, desencorajando a utilização de métodos baseados unicamente em senhas. O relatório menciona também sobre o desafio de implementar novas tecnologias de autenticação em larga escala devido à falta de padronização, propondo estudo e criação de protocolos abertos como os da FIDO Alliance (COMMISSION ON ENHANCING NATIONAL CYBERSECURITY, 2016).

A FIDO Alliance possui uma proposta de padronização de protocolos de autenticação utilizando múltiplos fatores, inclusive, métodos mais seguros que dispensam a utilização de senhas (FIDO ALLIANCE, 2017a). Tal padronização viabiliza a interoperabilidade entre diversos dispositivos seguros de autenticação de diversos fabricantes e tecnologias presentes nos dispositivos móveis.

Para o usuário, pode significar mais segurança combinada a usabilidade, pois permite utilizar um dispositivo seguro que seja mais adequado a seu dia-a-dia e personalidade. Em um contexto mais corporativo, permite que empresas tenham mais liberdade de decidir o uso de um mecanismo seguro que atenda a suas políticas internas de acesso e se alinhe a sua identidade e missão como empresa.

A tendência é que a senha como método de autenticação seja desencorajada ou não mais utilizada em grandes corporações, setor público, instituições financeiras e outros lugares que ofereçam serviços considerados críticos na internet, e a FIDO Alliance está no

meio desta revolução. Ao mesmo tempo, é preciso certificar que a FIDO Alliance de fato fornece a segurança exigida alinhado a normativos e recomendações que podem vir a ser exigência legal.

1.2. OBJETIVO

O objetivo deste trabalho é apresentar um estudo dos protocolos de autenticação desenvolvidos pela FIDO Alliance, analisando sob o aspecto da mitigação de riscos e ameaças em um processo de autenticação, baseado na série de publicações NIST 800-63 (GRASSI et al., 2017a).

1.3. METODOLOGIA

A metodologia utilizada envolve pesquisa bibliográfica para embasamento teórico sobre as principais tecnologias existentes, bem como levantamento das melhores práticas de segurança no escopo de autenticação de credenciais.

Em seguida, utilizando de todo o material estudado, identificar os requisitos de segurança que são exigidos por normativos e os requisitos que são de fato especificados pela FIDO Alliance, e avaliar o alinhamento destes requisitos com o que está normatizado.

1.4. ORGANIZAÇÃO DO TRABALHO

O capítulo 2 discorrerá sobre todo o embasamento teórico que sustenta o trabalho. O capítulo 3 irá detalhar toda a análise, bem como o seu resultado. O capítulo 4 irá concluir o trabalho, além de sinalizar expectativas de estudos futuros.

2. REVISÃO BIBLIOGRÁFICA

2.1. IDENTIDADE DIGITAL E AUTENTICAÇÃO DIGITAL

O usuário ao acessar um sistema deve ter em mãos um identificador e algo mais que possa utilizar para provar que possui realmente este identificador. Entre o ato de solicitar o acesso ao sistema e receber a confirmação, existe uma série de elementos que são validados e verificados para determinar se o usuário pode acessar ou não, e se acessar, até que ponto do sistema este usuário está autorizado. Para isso, são iniciados processos de identificação, autenticação e controle de acesso ou autorização.

2.1.1. Identidade digital

Identidade digital é a representação de um sujeito em uma transação digital. Uma identidade digital deve ser capaz de identificar unicamente um sujeito dentro do contexto de um serviço. A prova de identidade deve certificar que o sujeito é realmente quem ele diz ser, ou seja, deve provar a posse da identidade digital fornecida (GRASSI et al., 2017b).

2.1.2. Autenticação digital

Autenticação digital é o processo de verificação de um ou mais autenticadores que o sujeito utilizou para provar a posse de sua identidade digital (GRASSI et al., 2017c). Um autenticador é algo que está de posse do usuário que deve utilizar para provar a posse da identidade digital.

A prova se dá por meio da verificação das credenciais do usuário pelo sistema verificador. Uma credencial é o vínculo entre a identidade digital do usuário e seus autenticadores. As credenciais geralmente são objetos de dados, ou registros da tabela de credenciais e são mantidos pelo provedor de credenciais. O provedor de credenciais é uma entidade que realiza o gerenciamento das credenciais do usuário. O usuário deve registrar sua identidade digital e os autenticadores que serão utilizados e assim realizar o credenciamento neste provedor. O provedor então é capaz de autenticar o usuário utilizando as informações das credenciais.

Em serviços onde é previsto a visita constante do usuário, o resultado da autenticação pode ser empregado como mais um item em uma análise de risco de uma política de segurança, se assegurando, com um determinado grau de confiança, que o usuário que acessou ontem é o mesmo que está acessando hoje (GRASSI et al., 2017a).

Autenticação não deve ser confundido com autorização, pois autorização é o ato de conceder acesso a um recurso protegido, conforme determinado por um controle de acesso. As credenciais do usuário são confrontadas em uma lista provida pelo controle de acesso que irá determinar o nível de acesso que este usuário possui. Portanto, autenticação é o ato de confirmar que um usuário é realmente quem diz ser antes de concede-lo acesso ao recurso (WILLIAMSON et al., 2009).

Cada organização deve implementar um sistema de segurança de acordo com o valor da informação que deseja proteger. O acesso a informações críticas ou que agregam alto valor devem ser monitoradas por um controle de acesso mais restrito, e o mais importante, um mecanismo de autenticação que possa identificar um usuário inequivocamente. Quanto mais sofisticado for o mecanismo de autenticação, maior será o investimento para implementá-lo, portanto, é importante avaliar a razão entre o risco do comprometimento da informação e o esforço empreendido para protege-lo.

2.2. FATORES DE AUTENTICAÇÃO

Existem várias maneiras de um usuário se autenticar, ou seja, provar sua identidade. Um usuário pode ter tantos autenticadores quanto puder para isso. Um autenticador pode se manifestar na forma de um segredo ou algum objeto. Um autenticador difere do outro de acordo com o fator de autenticação implementado, e um autenticador pode ser considerado mais seguro que o outro, dependendo do fator de autenticação empregado e se houver mais de um fator empregado, inclusive.

Estes fatores de autenticação basicamente são classificados em três tipos: O que o usuário sabe, o que o usuário tem e o que o usuário é (GRASSI et al., 2017a).

2.2.1. O que o usuário sabe

Geralmente é uma espécie de segredo que o usuário deve memorizar e não compartilhar a mais ninguém. O autenticador mais conhecido nesta forma é a senha.

2.2.2. O que o usuário possui

Basicamente pode ser qualquer dispositivo físico que esteja de posse do usuário, de forma que tal dispositivo deve ser único, ou seja, não pode ser usado em dois lugares ao mesmo tempo (BURNETT, 2016). A autenticação utilizando este fator acontece quando o usuário manipula o dispositivo de forma a provar que está de posse dele naquele momento.

2.2.3. O que o usuário é

É a mensuração de uma característica física ou comportamental do usuário que normalmente nunca muda. Exemplos simples e bem comuns são as informações biométricas, como impressão digital, leitura da retina ou íris, mas há outras tecnologias emergentes como reconhecimento de voz, reconhecimento facial e frequência cardíaca. Outro exemplo são os padrões comportamentais do usuário, como padrão de digitação, movimentação do mouse, até mesmo a forma com que o usuário caminha, como velocidade e distância dos passos.

Os dispositivos móveis da atualidade geralmente vêm acompanhado de câmeras, leitores de impressão digital, acelerômetros e giroscópios, onde é possível capturar diversas características, a ponto de calcular um padrão das características físicas e comportamentais do usuário habitual daquele dispositivo.

Burnett (2006) observa que esta forma de validação não é exata, pois é baseado no julgamento do leitor biométrico e nos algoritmos utilizados para o reconhecimento, o que pode acarretar em falsos positivos ou falsos negativos. Além da falha no sistema, a característica de um usuário pode mudar drasticamente por conta de um acidente ou doença. O usuário pode ter cortado o dedo e comprometido a leitura de sua impressão digital, ou ter pego uma gripe e perder a voz ou mudar a entonação de tal forma a dificultar o reconhecimento por voz.

2.2.4. Autenticação multifator

Um autenticador não precisa estar limitado a implementar somente um dos fatores de autenticação. É possível combinar dois fatores diferentes ou até mesmo os três fatores juntos dentro de um autenticador, ou utilizar dois ou mais autenticadores em conjunto em uma autenticação. O resultado desta combinação produz métodos de autenticação mais seguros do que se fosse utilizado um único fator (WILLIAMSON et al., 2009).

Um exemplo problemático é a senha, que é um método tradicional e de fácil implementação. No entanto, pode ser considerada o autenticador mais fraco e vulnerável a diversos mecanismos simples de ataque. Apesar de suas vulnerabilidades, Burnett (2006) defende que a senha é um elemento essencial e que dificilmente será substituída. Os outros dois fatores de autenticação podem ser combinados com uma senha de forma bastante eficaz em um autenticador multifator.

A força de uma autenticação multifator está em combinar dois ou mais fatores de autenticação distintos. Então é válido combinar um dispositivo físico com uma senha, ou um dispositivo físico com biometria, mas não é considerado multifator o uso de duas senhas distintas ou dois dispositivos físicos diferentes, pois implementam o mesmo fator de autenticação. A segurança é aumentada no sentido de que o usuário deve provar a sua identidade digital apresentando dois fatores de tal forma que, caso um fator seja comprometido, o outro não seja exposto.

Por exemplo, um usuário possui um autenticador multifator na forma de um dispositivo físico, e para utilizá-lo, precisa digitar uma senha. Caso o usuário tenha perdido o dispositivo ou sido furtado, o atacante não conseguirá utiliza-lo, pois não conhece a senha. Também pode acontecer o contrário, o atacante descobriu a senha do usuário, mas não conseguirá acessar sem ter o dispositivo em mãos.

2.3. TIPOS DE AUTENTICADORES

Os autenticadores podem conter um dos fatores de autenticação ou uma combinação de dois ou três fatores de autenticação em um só dispositivo. Isso permite uma variedade de autenticadores diferentes, cada um com suas características próprias. No entanto, devido ao fator de autenticação implementado, o emprego de tecnologias de proteção de dados, algoritmos de criptografia e proteção de canais de comunicação, alguns autenticadores acabam sendo avaliados como sendo mais ou menos seguros.

A NIST classificou diversos tipos de autenticadores de acordo com o método e tecnologia empregados (GRASSI et al., 2017c). São listados autenticadores que utilizam um único fator e outros multifator:

2.3.1. Senha

A senha é um segredo que geralmente é escolhido e memorizado pelo próprio usuário. Senhas memorizadas devem ser complexas o suficiente para que um atacante em potencial seja incapaz de adivinhar.

2.3.2. Cartão de senhas

É uma espécie de tabela contendo senhas que são geralmente fornecidas pelo provedor de credenciais ao usuário. Pode ser no formato de uma cartela. Estes cartões geralmente possuem códigos em forma de linhas e colunas, onde o provedor de credenciais envia como desafio uma sequência de valores, e o usuário deve traduzir estes valores em uma sequência de códigos de acordo com a tabela, enviando esta sequência como resposta ao provedor de credenciais. O provedor de credenciais conhece o padrão das tabelas de cada usuário, sendo capaz de confrontar a resposta e verificar de fato que o usuário tem a posse do mesmo cartão.

2.3.3. Dispositivo Fora de Banda

É um dispositivo físico que deve ser unicamente endereçável e que se comunica com o verificador por um canal de comunicação secundário, ou seja, um canal que seja totalmente independente do canal de comunicação principal onde está ocorrendo a solicitação. Este dispositivo deve estar de posse e controle do usuário.

Existem três maneiras de uma autenticação fora de banda acontecer:

- O usuário envia um código que foi recebido no dispositivo via um canal secundário para o verificador, através do canal principal. Por exemplo, um usuário envia uma solicitação de login a uma página de internet, então recebe um código em seu dispositivo mobile e o digita no campo correspondente na página;
- O usuário envia um código que foi recebido via canal principal para o dispositivo, que se comunica com o verificador via um canal secundário. Por exemplo, o usuário recebe na página de login um código, e o transmite para o seu dispositivo, digitando este código ou o capturando via QRCode, por exemplo;

- O usuário recebe um código ou informações de confirmação tanto no canal principal quanto no secundário, compara os dois e então confirma através do canal secundário. Por exemplo, o usuário visualiza na página de login um código, e compara com o código que recebeu simultaneamente no dispositivo, mais algumas informações como local e hora do login, e então confirma no próprio dispositivo.

A autenticação fora de banda tem a característica de permitir iniciar o pedido de autenticação em um canal e finalizar em outro. A utilização de um código no momento da autenticação serve como um elo de ligação da operação entre o canal principal e o secundário naquele momento.

2.3.4. Dispositivo OTP

Pode ser um dispositivo físico ou um software que pode ser instalado em dispositivos mobile. O dispositivo OTP possui uma chave secreta que serve como semente para gerar códigos OTP. Este código é mostrado no visor do dispositivo e o usuário deve informa-lo manualmente no campo da página web, por exemplo. Ao informar o código, o usuário está provando que possui o dispositivo OTP ao verificador.

O verificador valida o código recebido pelo usuário realizando o mesmo procedimento de geração do OTP que o dispositivo, e assim comparar os dois valores. O algoritmo de geração do OTP deve ser aplicado de tal forma que o dispositivo e o verificador sejam capazes de gerar o mesmo valor independente um do outro. Este código deve ser computado de tal forma que seja único a cada requisição, ou pelo menos, que o código seja capaz de variar com o tempo, com a finalidade de evitar ataques de repetição.

Um dispositivo OTP é considerado "algo que o usuário tem", e pode ser de único fator ou multifator. O dispositivo de único fator não exige um segundo fator para ser ativado.

O Dispositivo OTP multifator exige um segundo fator para ativar a geração do código OTP, que deve ser obrigatoriamente "algo que o usuário sabe ", como uma senha, ou "algo que o usuário é", como alguma informação biométrica. O dispositivo OTP multifator não pode ser um software, deve ser obrigatoriamente um dispositivo físico.

2.3.5. Software criptográfico

O software criptográfico é basicamente o uso de uma chave criptográfica armazenada em disco, ou em uma mídia física similar. A forma como tal chave é aplicada pode variar de acordo com o algoritmo criptográfico empregado. É muito comum a utilização de algoritmos assimétricos, onde é gerado um par de chaves, sendo que a chave privada é a que deve estar de posse do usuário. A forma mais comum de utilização é por meio de uma infraestrutura de chaves públicas e certificados digitais.

O verificador deve gerar um desafio e enviar ao autenticador, este ao receber o desafio utiliza a chave criptográfica para assinar este desafio e devolve a assinatura digital ao verificador. O verificador também tem posse da chave criptográfica correspondente, ou no caso da utilização de um algoritmo assimétrico, tem posse da chave pública. O verificador é capaz de verificar que o usuário tem a posse do autenticador ao conferir a assinatura digital e validar a sua origem.

O software criptográfico é considerado como "algo que o usuário tem" e deve armazenar a chave privada da maneira mais segura disponível no disco, e seu acesso deve ser protegido contra acesso não autorizado, utilizando políticas de permissão de acesso para determinados módulos, restrições de acessos de determinados ambientes, etc.

2.3.6. Software criptográfico multifator

O software criptográfico multifator se assemelha ao software criptográfico anterior, ou seja, uma chave criptográfica considerada como "algo que o usuário tem". Porém esta chave tem o seu acesso e ativação protegidos por um segundo fator de autenticação, que deve ser "algo que o usuário sabe" ou "algo que o usuário é". O acesso à chave criptográfica é feito somente após a entrada e validação da senha ou biometria, e logo depois, a requisição é assinada com a respectiva chave.

2.3.7. Dispositivo criptográfico

Um dispositivo criptográfico é um hardware que possui dentro de si chaves simétricas ou assimétricas, e é capaz de, por conta própria, realizar operações criptográficas e transmitir como resultado uma assinatura digital ou um criptograma. A saída do dispositivo deve se comunicar fisicamente com o terminal, como por exemplo, uma porta USB.

O dispositivo não pode permitir que a chave encapsulada dentro de si seja exportada, e muito menos removida. A verificação do autenticador é idêntica ao do software criptográfico, com a diferença que o dispositivo recebe o desafio através de sua porta de comunicação e responde com dados de saída de acordo com o algoritmo e protocolo empregados. O verificador também conhece previamente a chave e o algoritmo, e é capaz de conferir a origem da assinatura e a posse do dispositivo pelo usuário.

2.3.8. Dispositivo criptográfico multifator

O dispositivo criptográfico multifator é um hardware que possui chaves criptográficas dentro de si, com a característica de que tais chaves são acessíveis somente após a validação de um segundo fator de autenticação, que deve ser "algo que o usuário sabe" ou "algo que o usuário é". O hardware também executa operações criptográficas por conta própria e possui uma porta para se comunicar diretamente com um terminal.

O hardware deste dispositivo deve ser "tamper-resistant", ou seja, deve possuir camadas de segurança de tal forma que seja inviolável contra tentativas de acesso às chaves criptográficas e outras informações. Além de ser inviolável, tais chaves somente podem ser acessíveis após a validação de uma senha ou biometria. A verificação do autenticador é semelhante à validação do dispositivo criptográfico de único fator.

2.4. PRINCIPAIS AMEAÇAS E CONTRAMEDIDAS

Um atacante nem sempre precisa quebrar a segurança de sistemas para obter acesso não autorizado. Dependendo do alvo, é mais fácil obter o controle do autenticador utilizado por um usuário e acessar o sistema legitimamente se passando por ele. Por conta disso, autenticadores também são alvo dos atacantes.

Os autenticadores estão expostos a diversas ameaças. Estas ameaças podem se originar de vulnerabilidades por conta da forma como o autenticador foi implementado, no entanto, também são comuns ameaças originadas do comportamento do usuário. Estas ameaças podem ser categorizadas de acordo com o fator de autenticação implementado (GRASSI et al., 2017c):

Algo que o usuário sabe pode ser exposto ao atacante. O atacante pode adivinhar a senha, ou se estiver muito próximo do usuário, pode observar a senha sendo digitada. O

usuário pode ser vítima de ataques de engenharia social, onde o atacante instiga o usuário a fornecer sua senha voluntariamente. O usuário pode instalar um software malicioso capaz de capturar a senha digitada. O atacante pode descobrir a senha ao realizar ataques offline sobre o segredo, utilizando um dicionário de senhas ou força bruta.

Algo que o usuário possui pode ser perdido, danificado, furtado ou clonado. Um software criptográfico pode ser copiado do computador do usuário quando o atacante obtém controle sobre o computador. Um dispositivo físico pode ser furtado, e caso este dispositivo não ofereça nenhuma proteção contra acesso e violação do hardware, pode ter seu material criptográfico extraído ou ser duplicado.

Algo que o usuário é pode ser replicado. Dependendo da informação biométrica, esta pode ser obtida e replicada. O exemplo clássico é um usuário ter a sua impressão digital capturada em um objeto qualquer e o atacante produzir um dedo artificial com a mesma informação.

No caso dos dispositivos fora de banda, o segredo trafegado em um dos canais pode ser interceptado. Por exemplo, o usuário recebe via SMS um código de liberação, e acaba repassando ao atacante por engenharia social.

2.4.1. Ameaças conhecidas

A NIST organizou as principais ameaças conhecidas sobre autenticadores descritas na Tabela 2.1:

Tabela 2.1 Principais ataques e ameaças sobre autenticação (GRASSI et al., 2017c)

Ataques e ameaças	Descrição	Exemplos
Roubo/Furto	O dispositivo físico é furtado pelo atacante	O dispositivo mobile do usuário é roubado
		O dispositivo OTP do usuário é roubado
Duplicação/Clonagem	O autenticador do usuário é copiado com ou sem o seu consentimento	A senha do usuário foi anotada pelo atacante
		A chave criptográfica que estava armazenada em um arquivo foi copiada

Eavesdropping	O atacante intercepta o segredo ou a resposta de um autenticador enquanto o usuário se autentica	A senha é capturada por meio de um keylogger
		O a senha em claro ou o hash da senha é interceptada na rede
		O segredo enviado por um dispositivo fora de banda via conexão sem fio é interceptado pelo atacante
Offline cracking	O atacante utiliza métodos analíticos ou criptoanalíticos para obter ou expor o segredo do autenticador	Um arquivo protegido obtido de um software é submetido a um ataque de dicionário para obter a senha e acessar o segredo.
Side channel attack	O autenticador é exposto por meio da análise de suas características físicas	Extração da chave criptográfica de um autenticador analisando o tempo de resposta após uma amostragem de várias tentativas
Phishing ou Pharming	O usuário passa o segredo do autenticador para o atacante se passando por um provedor autêntico	O usuário digita a sua senha em uma página falsa se passando pelo provedor
		O usuário responde a um e-mail cujo o remetente diz ser o banco, informando dados pessoais e a senha de sua conta
Engenharia Social	O atacante ganha a confiança do usuário, que acaba revelando o segredo do autenticador ou a resposta dele	O usuário informa sua senha para o atendente que o convence.
		O atacante convence o usuário a informar pelo telefone o OTP gerado pelo seu dispositivo
Online Guessing	O atacante se conecta com o provedor de credenciais e tenta acertar um resultado válido de um autenticador	O atacante utiliza uma lista de identidades digitais e realiza tentativas de acerto de senha com a intenção de descobrir algumas delas

		O atacante tenta acertar um OTP válido para o autenticador de um determinado usuário
Comprometimento do terminal	Códigos maliciosos instalados no computador do usuário podem fazer com que o atacante assuma o controle remotamente	Um autenticador conectado no terminal do usuário pode ser usado para autenticar o atacante remoto.
	Códigos maliciosos causam a autenticação em outro provedor que não o que o usuário escolheu	O autenticador é usado para autenticar o atacante em outro site ao invés do usuário
	Códigos maliciosos podem comprometer o autenticador do tipo software criptográfico	Programas instalados podem extrair e exportar as chaves criptográficas sem o conhecimento do usuário

2.4.2. Estratégias de mitigação

Apesar de as ameaças existirem, existem mecanismos e melhores práticas que podem fazer com que estas sejam suprimidas, dificultadas, ou no pior caso, sejam detectadas antes, durante ou prontamente após o ataque. A NIST destacou algumas técnicas e procedimentos que podem ser aplicados em várias situações (GRASSI et al., 2017c).

A utilização de múltiplos fatores, seja um dispositivo multifator ou a combinação de dois autenticadores, tornam o ataque mais complicado de ser realizado. O atacante terá que obter o dispositivo físico e a senha para desbloqueá-lo, muitas vezes o esforço empenhado para tal não compensa.

Mecanismos físicos de proteção podem ser utilizados para proteger as chaves contidas em um dispositivo criptográfico, como mecanismos "tamper resistant" e "tamper detection".

A obrigatoriedade de utilização de senhas mais compridas, como frases, números e outros elementos que dificilmente apareçam em dicionários, podem inviabilizar a utilização de mecanismos de quebra de senha.

A instalação de sistemas de segurança nos terminais e na rede podem prevenir um atacante de obter acesso ao sistema ou instalar softwares maliciosos para tal.

A utilização de autenticação fora de banda para verificar a posse de um dispositivo pelo usuário, como por exemplo, a prova da posse de um smartphone pelo usuário.

Treinamentos e programas de conscientização aos usuários que utilizam o sistema, de forma a diminuir as ameaças de origem humana, além de ensinar o usuário a reconhecer situações que podem ser possíveis ataques que comprometam o processo de autenticação.

Além destas recomendações, a NIST relacionou estratégias direcionadas para cada tipo de ameaça, conforme descrito na Tabela 2.2:

Tabela 2.2 Estratégias para as principais ameaças (GRASSI et al., 2017c)

Ataques e ameaças	Estratégia
Roubo/Furto	Utilizar autenticadores multifator que necessitam de senha ou biometria para serem ativados. Evitará o atacante de utiliza-lo facilmente.
Duplicação/Clonagem	Utilizar dispositivos que possuem proteção física contra extração da chave armazenada
Eavesdropping	Garantir a proteção do terminal contra a instalação de malwares que possam capturar a senha, como keyloggers
	Observar atentamente ao redor ao digitar uma senha ou o OTP, para garantir que outra pessoa não esteja observando a digitação
	Utilizar o autenticador somente em canais protegidos. Observar se no browser a imagem do cadeado aparece como fechada, indicando que aquela comunicação será criptografada.
	Utilizar protocolos que são resistentes a ataques de repetição, como HOTP e TOTP.
Offline cracking	Utilizar autenticadores cujo segredo possuem alta entropia, como senhas mais fortes
	Armazenar o hash da senha de forma salteada no provedor de credenciais
Side channel attack	Utilizar algoritmos capazes de manter constantemente uma medida de consumo de energia e de tempo de processamento, independentemente do valor da chave criptográfica

Phishing ou Pharming	Utilizar autenticadores que evitem que o atacante possa se passar pelo usuário facilmente, por exemplo, biometria
	O usuário deve estar atento a URLs desconhecidas
	Não clicar em links que chegam por e-mail
Engenharia Social	Não revelar a senha para nenhuma pessoa, não importa a situação
	Evitar utilizar autenticadores que necessite da validação por terceiros, como centrais de atendimento.
Online Guessing	Utilizar autenticadores que produzam respostas com alto nível de entropia
	Utilizar autenticadores que bloqueiam o acesso após determinada quantidade de tentativas
Comprometimento do terminal	Utilizar dispositivos que necessitem da interação física do usuário, como apertar um botão no dispositivo
	Prover uma maneira segura de mostrar a identidade do provedor
	Manter arquivos de chaves criptográficas em áreas de acesso restrito no sistema

2.5. NIST 800-63 – DIRETRIZES PARA IDENTIDADES DIGITAIS

É um documento de diretrizes publicado pela National Institute of Standards and Technology – NIST do Departamento de Comércio dos Estados Unidos da América. Estas diretrizes se destinam a prover requisitos técnicos para implementação dos sistemas remotos de identificação digital nos órgãos federais. Apesar disso, estas diretrizes possuem caráter normativo e informativo, que podem ser utilizados como referência para a discussão sobre análise de risco de um processo de identificação e autenticação digital (GRASSI et al., 2017c).

A publicação 800-63 atualmente está em sua quarta versão, a 800-63-3. Esta última versão trouxe mudanças significativas em relação a versão anterior:

- Passa a utilizar o termo identidade digital. Vem com a mudança do título, de Electronic Authentication Guideline (Diretriz de Autenticação Eletrônica) para Digital Identity Guidelines (Diretrizes de Identidade Digital);
- Grande parte do conteúdo fora revisado e atualizado, de forma a atender a um cenário mais atual. A divisão do documento em quatro seções, sendo que cada seção trata de um tema específico: modelo de identidade digital, cadastramento e validação de identidade, ciclo de vida da autenticação, e por último, federação de identidade digital. Este último tema é inédito nesta publicação e vem para normatizar os emergentes serviços de identidade digital de terceiros.

2.5.1. Autenticação e gerenciamento do ciclo de vida

A seção 800-63-3B da publicação trata especificamente sobre vários aspectos da autenticação. Descreve os autenticadores e os categoriza de acordo com o fator de autenticação utilizado e os requisitos de segurança. Também estabelece níveis de autenticação baseado no risco da utilização de determinado autenticador.

2.5.2. Requisitos gerais para autenticadores

Independentemente do autenticador utilizado, existem algumas recomendações e definições a respeito da segurança do dispositivo, onde se determina o quanto é confiável e resistente a alguns ataques ao processo de autenticação (GRASSI et al., 2017c).

2.5.2.1. Tentativas de acesso

Para que um autenticador seja resistente a ataques de adivinhação de um segredo ou ataques de força bruta sobre um dispositivo, deve ser implementado um controle de tentativas falhas. Algumas técnicas podem ser implementadas para tentar diminuir a diferença entre um usuário legítimo tentando se autenticar e um atacante tentando adivinhar o segredo.

Por exemplo, após uma certa quantidade de tentativas, solicitar que o usuário complete um desafio para provar que não é um script automatizado. Outro exemplo é fazer o usuário esperar um determinado tempo após uma tentativa falha, e aumentar este intervalo a cada tentativa sem sucesso, até atingir uma quantidade limite de tentativas.

2.5.2.2. Biometria

O uso da biometria como autenticador é "o que o usuário é", no entanto, alguns elementos devem ser considerados antes de utiliza-lo, assim, seu uso é limitado a alguns aspectos do processo de autenticação.

Enquanto os outros fatores são determinísticos, a validação de uma informação biométrica é considerada probabilística. Uma validação de biometria possui uma taxa de falsos positivos e taxa de falsos negativos, onde uma taxa alta não provê uma confiança adequada para a autenticação do usuário.

Informações biométricas não são secretas, uma vez que pode ser capturada do usuário, como por exemplo, fotos do rosto do usuário para enganar um autenticador de reconhecimento facial e a captura de impressões digitais deixadas em objetos. Uma solução para mitigar este ataque seria o sensor que captura o dado biométrico também detectar de alguma maneira se o usuário realmente está presente, como temperatura corporal, medição do pulso cardíaco, etc.

A biometria deve ser usada sempre em conjunto com outro fator de autenticação, algo que o usuário tem. A comunicação entre o sensor e o autenticador ou o provedor de autenticação deve ser protegido, de forma a não permitir que os dados do sensor sejam capturados.

Deve ser implementado um controle de quantidade de tentativas de validação da biometria também. Caso falhe, aumentar o intervalo de espera entre as tentativas, ou desabilitar o autenticador biométrico e oferecer outro autenticador no lugar, como uma senha ou outra informação biométrica cadastrada para o usuário.

A validação da biometria deve preferencialmente ser realizado localmente no dispositivo, ou seja, o próprio dispositivo armazena localmente a informação biométrica para a comparação e ativar uma chave criptográfica, como funciona geralmente os autenticadores multifator.

Também é possível realizar de forma centralizada, ou seja, a informação biométrica a ser comparada está armazenada em um servidor central. No entanto, devem ser tomados alguns cuidados, entre eles, limitar a uma quantidade certa de dispositivos identificados e

com a utilização de algoritmos criptográficos autorizados, controle do ciclo de vida da informação biométrica, e transmitir os dados somente em canais autenticados e protegidos.

2.5.2.3. Ataque de representação fraudulenta

Este ataque se refere ao atacante se passar por um provedor de acesso, onde o usuário acredita estar se autenticando em um provedor autêntico. Com isso, o atacante pode capturar a credencial do usuário e se passar por ele no provedor original. Este tipo de ataque se utiliza da técnica de MitM, sendo que um autenticador e um protocolo de comunicação que for resistente a este ataque deve ser resistente primeiramente ao MitM.

O protocolo TLS pode ser considerado resistente a este ataque, pois há uma autenticação anterior para estabelecer a comunicação entre o cliente e o servidor, e nesse caso a saída do autenticador pode utilizar desta comunicação.

Outra técnica efetiva é fazer com que o autenticador assine, junto com a sua saída, o endereço do provedor o qual o usuário está conectado. Isso impede que o autenticador consiga usar a saída do autenticador para se passar pelo usuário ao tentar se conectar em outro provedor.

2.5.2.4. Ataques de repetição

Um autenticador é considerado resistente ao ataque de repetição se conseguir produzir uma saída que não possa ser utilizada mais de uma vez em um determinado período de tempo. Com isso, mesmo que o atacante capture a saída do autenticador e a armazene para utilizar mais tarde, seria impossível, pois já teria se tornado inválida.

Para produzir esse resultado, o protocolo de autenticação deve utilizar de desafios, ou seja, valores aleatórios, contadores, ou uma informação difusa baseada no tempo, e o autenticador deva ser capaz de assinar este desafio. Assim, dado um determinado tempo ou a confirmação da autenticação, este desafio se torne inválido, tornando a assinatura gerada anteriormente igualmente inválida após o seu uso.

2.5.2.5. Intenção de autenticação

O objetivo da intenção de autenticação é fazer com que o usuário tome conhecimento do processo de autenticação em andamento, quando o seu dispositivo físico estiver

conectado no seu terminal. É comum, em sistemas comprometidos, em que o atacante acessa remotamente o terminal do usuário e realize uma autenticação sem o seu conhecimento.

Um autenticador multifator deve solicitar, sempre que ocorrer uma autenticação, que o usuário utilize um fator de autenticação, como uma senha ou biometria. No geral a maneira de estabelecer a intenção de autenticação é fazer com que o usuário interaja com o autenticador de alguma forma, como por exemplo, solicitar que o usuário pressione um botão ou qualquer outro comando solicitado pelo autenticador para prosseguir com a autenticação.

2.5.3. Nível de confiança da autenticação

Para que um usuário possa ser autenticado pelo provedor, é necessário que se garanta minimamente um nível de força da credencial, de forma que o processo de identificação e autenticação do usuário valide o usuário apropriadamente. Foram determinados três níveis de confiança da autenticação:

2.5.3.1. Nível de confiança 1

Este nível garante minimamente a validação de que o usuário de fato tem a posse do autenticador. Qualquer autenticador de um fator ou mais pode ser utilizado. É exigido a utilização de algoritmos criptográficos conhecidos tanto pelo autenticador quanto pelo canal de comunicação, que deve ser protegido contra-ataques MitM.

Autenticadores que se utilizem de software devem, se possível, verificar a integridade do ambiente ou sistema operacional onde está funcionando. Por exemplo, verificar a presença de malware instalado. Nesse caso, o autenticador deve se recusar a operar neste ambiente.

O provedor que realizará a validação do autenticador deve estar em conformidade com a FIPS-140 Nível 1 (NIST, 2001) pelo menos.

O autenticador deve ser revalidado a cada 30 dias, independente da atividade. Por exemplo, revalidação de sessão de usuário de longa duração.

Os autenticadores permitidos para este nível são:

- Senha
- Cartão de senhas

- Dispositivo Fora de Banda
- Dispositivo OTP
- Dispositivo OTP multifator
- Software criptográfico
- Software criptográfico multifator
- Dispositivo criptográfico
- Dispositivo criptográfico multifator

2.5.3.2. Nível de confiança 2

Este nível fornece uma confiança maior de que o usuário realmente possui os autenticadores registrados para tal. Para isso, é exigido o uso de um autenticador multifator ou mais de um autenticador que utilizem fatores distintos. É exigido a utilização de algoritmos criptográficos conhecidos tanto pelo autenticador quanto pelo canal de comunicação, que deve ser protegido contra-ataques MitM.

Autenticadores que se utilizem de software devem, se possível, verificar a integridade do ambiente ou sistema operacional onde está funcionando. Por exemplo, verificar a presença de malware instalado. Nesse caso, o autenticador deve se recusar a operar neste ambiente.

Pelo menos um dos autenticadores utilizados deve ser resistente a repetição, e um autenticador necessariamente deve demonstrar a intenção de autenticação.

O autenticador e o provedor que realizará a validação do autenticador devem estar em conformidade com a FIPS-140 Nível 1 (NIST, 2001) pelo menos.

O autenticador deve ser revalidado a cada 12 horas, independente da atividade. A reautenticação deve acontecer também após 30 minutos de inatividade do usuário na sessão, utilizando somente um fator de autenticação, se desejar.

Para este nível são permitidos autenticadores multifator:

- Dispositivo OTP multifator;
- Software criptográfico multifator;
- Dispositivo criptográfico multifator

Também são permitidos a combinação de dois autenticadores de um fator, sendo obrigatoriamente um autenticador do tipo senha ("o que o usuário sabe") com outro autenticador "que o usuário possui", como os listados a seguir:

- Cartela de senhas
- Autenticação fora de banda
- Dispositivo OTP de único fator
- Software criptográfico de único fator
- Dispositivo criptográfico de único fator

2.5.3.3. Nível de Confiança 3

Este nível fornece alta confiança de que o usuário realmente tem a posse do autenticador. Basicamente, este nível atesta a posse de uma chave criptográfica. Este nível difere do nível dois pela exigência exclusiva de um dispositivo criptográfico em hardware.

O canal de comunicação deverá ser protegido para garantir confidencialidade e ataques MitM. Todos os autenticadores devem ser resistentes a ataques de roubo de identidade e ataques de repetição. No processo de autenticação e reautenticação pelo menos um autenticador deve demonstrar intenção de autenticação.

Os autenticadores multifator utilizados neste nível devem possuir hardwares criptográficos em conformidade com a FIPS-140 nível 2 e com proteção física nível 3. Os autenticadores de um fator apenas utilizados neste nível devem estar em conformidade com a FIPS-140 nível 1 e com proteção física nível 3 (NIST, 2001).

O autenticador deve ser revalidado a cada 12 horas, independente da atividade. A reautenticação deve acontecer também após 15 minutos de inatividade do usuário na sessão, utilizando obrigatoriamente ambos os fatores de autenticação.

Os autenticadores permitidos são:

- Dispositivo criptográfico multifator;
- Dispositivo criptográfico com um fator em conjunto com uma senha

2.5.3.4. Resumo dos níveis de confiança

As informações de cada nível de confiança podem ser condensadas na Tabela 2.3 com a finalidade de facilitar visualmente a comparação entre eles:

Tabela 2.3 Resumo dos níveis de confiança da autenticação (GRASSI et al., 2017c)

Item	Nível 1	Nível 2	Nível 3
Fator de autenticação	Um fator	Multifator Dois autenticadores (o que o usuário sabe + o que o usuário tem)	Multifator (hardware) Dois autenticadores (dispositivo criptográfico + o que o usuário sabe)
FIPS-140	Nível 1 para o provedor	Nível 1 para o provedor e para o autenticador	Nível 1 para o provedor e para o dispositivo físico de um fator; Nível 2 para dispositivo físico multifator; Nível 3 para proteção física para todos os autenticadores
Resistencia a MitM	Obrigatório	Obrigatório	Obrigatório
Resistencia a ataque de roubo de identidade	Não obrigatório	Não obrigatório	Obrigatório
Resistência a ataques de repetição	Não obrigatório	Obrigatório	Obrigatório
Intenção de autenticação	Não obrigatório	Obrigatório	Obrigatório
Validação da integridade do sistema	Quando for possível	Quando for possível	Não se aplica
Reautenticação	A cada 30 dias	A cada 12 horas ou 30 minutos de inatividade (somente um fator)	A cada 12 horas ou 15 minutos de inatividade (ambos os fatores)

2.5.4. Ciclo de vida do autenticador

Durante o ciclo de vida de um autenticador, uma série de eventos podem afetar a sua utilização. Esses eventos podem ser o credenciamento, perda, roubo, danificação, duplicação não autorizada, expiração e revogação (GRASSI et al., 2017c).

2.5.4.1. Credenciamento

Durante o cadastramento de um usuário, um ou mais autenticadores devem ser vinculados ao identificador do usuário. O termo credenciamento se refere ao ato de se criar uma credencial, que é o vínculo do autenticador com o identificador do usuário. Este autenticador pode ser fornecido pelo provedor de credenciais ao usuário como parte do cadastramento, ou o usuário pode apresentar um autenticador próprio reconhecido pelo provedor e assim realizar a vinculação.

Os provedores de credenciais, quando possível, devem encorajar os usuários a vincular mais de um autenticador. O usuário pode ter múltiplos autenticadores de cada fator de autenticação, com exceção da senha. Para vincular um segundo autenticador, é necessário que o usuário se autentique utilizando um outro autenticador com o mesmo nível de confiança, ou maior. O provedor, se assim desejar, pode limitar a quantidade de autenticadores vinculados por usuário por questões de controle.

2.5.4.2. Perda, roubo, danificação e duplicação não autorizada

Estes eventos devem ser tratados todos de forma similar, pois deve-se assumir que houve comprometimento do segredo do autenticador. Uma exceção novamente se dá para a senha, quando for comprovado que o usuário simplesmente esqueceu, sem exposição do segredo.

O provedor deve fornecer ao usuário um canal para que este possa comunicar a perda ou roubo do seu autenticador. O usuário pode utilizar um autenticador secundário, ou até mesmo uma senha de segurança para estas situações. Outra alternativa é o provedor estabelecer uma comunicação segura com o usuário e realizar a prova da identificação do usuário, coletando dados como e-mail ou código postal do seu endereço.

O provedor pode manter este autenticador em um estado de suspensão, e se desejar, pode reverter a situação caso o usuário consiga provar a posse do autenticador.

2.5.4.3. Expiração

O provedor de credenciais pode fornecer autenticadores com data de expiração. Um exemplo é um autenticador que armazene um certificado digital, ou autenticadores que foram assinados por um certificado digital com data de expiração. Nessas situações, o uso do autenticador expirado deverá resultar em uma falha de autenticação pelo provedor pelo motivo de expiração.

2.5.4.4. Revogação

A revogação ocorre quando o autenticador é desvinculado do identificador do usuário. Essa desvinculação ocorre quando é verificado que o usuário não existe mais, como o falecimento ou a descoberta de que se tratava de uma fraude, quando for solicitado pelo próprio usuário, ou quando o provedor considerar que tal autenticador não cumpre mais os requisitos necessários.

2.6. FIDO ALLIANCE

O termo FIDO é um diminutivo de "Fast IDentity Online"; sua tradução seria identidade rápida online, o que se refere a sua filosofia de um usuário conseguir se credenciar facilmente a uma aplicação utilizando o seu autenticador.

A FIDO Alliance é uma organização fundada em 2012 por um grupo de fabricantes e empresas cujo objetivo era desenvolver e prover uma solução de autenticação digital que pudesse substituir as senhas por autenticadores mais seguros, mas sem se prender a padrões proprietários, ou seja, prover interoperabilidade entre os autenticadores de diversos fabricantes com os provedores de autenticação (FIDO ALLIANCE, 2017b).

A missão da FIDO Alliance é especificar padrões abertos de autenticação de forma escalável e que haja interoperabilidade, com foco em autenticadores seguros que dependam cada vez menos de senhas. Além de especificar os padrões, a FIDO Alliance também se responsabiliza em garantir e aplicar estes padrões no mundo todo (FIDO ALLIANCE, 2017a).

O resultado desta aliança resultou em dois protocolos: um para proteger e aumentar a segurança no uso de senhas como um segundo fator, e outro para substituir completamente a senha com outros fatores de autenticação.

2.6.1. Como funciona

Os protocolos de autenticação funcionam baseado na infraestrutura de chaves públicas, ou seja, é empregado o uso de chaves assimétricas para realizar a autenticação. Durante o credenciamento ou registro do usuário em uma aplicação web, o autenticador gera um par de chaves, onde a chave privada é mantida em segurança no autenticador e a chave pública é repassada para o provedor de autenticação. Durante o login, basta o usuário utilizar novamente o autenticador com a respectiva chave privada (FIDO ALLIANCE, 2017a).

2.6.2. Registro

Durante o registro ocorrem as seguintes etapas:

- A aplicação solicita ao usuário que apresente um autenticador reconhecido pela FIDO Alliance e que atenda às políticas de aceitação da aplicação;
- O usuário escolhe um dispositivo e o desbloqueia utilizando um fator de autenticação, como uma senha ou biometria, ou simplesmente pressionando um botão no dispositivo;
- O dispositivo então gera internamente um par de chaves criptográficas vinculadas unicamente ao usuário e à aplicação;
- A chave pública somente é passada para a aplicação, que a registra em nome do usuário. A chave privada, e qualquer informação sobre os métodos empregados pelo autenticador (biometria, senha) ficam somente no autenticador.

2.6.3. Autenticação

Após o registro do dispositivo em uma dada aplicação, o usuário poderá finalmente utiliza-lo para se identificar:

- A aplicação envia um desafio para o usuário, que deverá utilizar um dos dispositivos previamente registrados e que ainda atendam às políticas de aceitação;

- O usuário desbloqueia o seu dispositivo utilizando os mesmos métodos que utilizou durante o registro;
- O dispositivo utiliza os dados do usuário fornecidos pela aplicação para selecionar a chave privada correta para aquela aplicação, e assina o desafio enviado;
- O dispositivo envia como resposta o desafio assinado, e a aplicação utiliza a chave pública registrada ao usuário designado para validar a assinatura. Se a autenticação for bem-sucedida, o login é realizado.

2.6.4. Padronização

Uma das filosofias da FIDO Alliance é a padronização e interoperabilidade. Quando se decide utilizar outro fator de autenticação para substituir uma senha, o desenvolvedor precisa implementar protocolos e padrões proprietários de tal dispositivo para se comunicar com a sua aplicação, aumentando a complexidade e manutenção.

Para resolver este problema, a FIDO Alliance decidiu padronizar a camada do cliente e de comunicação.

Padronização do cliente: A FIDO Alliance padronizou a interface de comunicação do cliente com os autenticadores locais. Em resumo, os mais diversos métodos de autenticação, como reconhecimento de face, voz, impressão digital, etc. podem ser facilmente reconhecidos e conectados por meio de plugins instalados em navegadores de internet, ou aplicativos agentes instalados em um sistema operacional, graças a esta interface de comunicação padronizada.

Padronização do protocolo de criptografia: O protocolo de comunicação entre o cliente e a aplicação web também foi padronizada, de forma que o mesmo cliente possa se comunicar com outras aplicações e vice-versa. Além da interoperabilidade, o protocolo foi desenvolvido pensando nos requisitos de segurança, oferecendo autenticidade e confidencialidade ao canal de comunicação.

2.6.5. UAF - Universal Authentication Framework

O protocolo UAF permite que o usuário substitua a senha tradicional por autenticadores multifator. Graças a padronização do protocolo, o usuário poderá utilizar

qualquer dispositivo de qualquer fabricante, desde que este dispositivo seja homologado e certificado pela FIDO Alliance. Por outro lado, a aplicação web ou um provedor de serviço de autenticação deverá ser capaz de receber a requisição de qualquer um destes autenticadores, uma vez que o protocolo de comunicação também foi padronizado.

2.6.5.1. Visão geral da arquitetura

A Figura 2.1 resume a arquitetura desenhada para o funcionamento do protocolo:

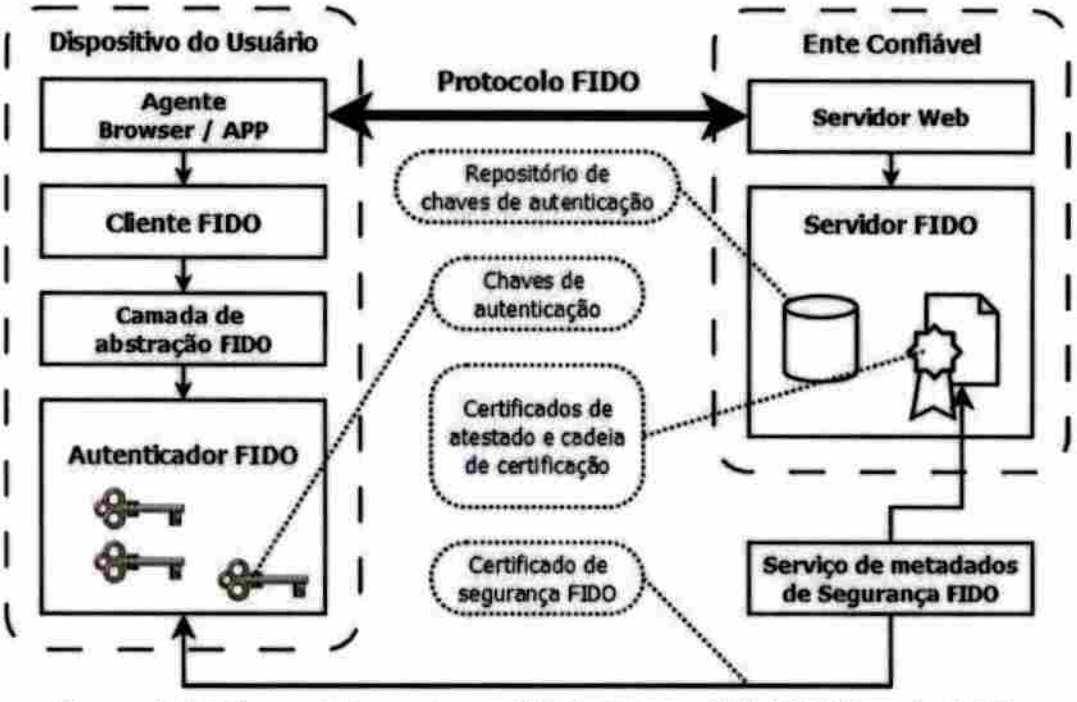

Figura 2.1 Visão geral da arquitetura FIDO Alliance (MACHANI et al., 2017)

Cliente FIDO UAF

O cliente UAF implementa a comunicação do lado do usuário. O cliente é capaz de se comunicar com o dispositivo local instalado no terminal ou dispositivo mobile do usuário através de uma interface de comunicação provida pela especificação do protocolo. O cliente também interage com o lado do servidor, o servidor UAF, na forma de um aplicativo instalado no dispositivo mobile ou um plugin instalado em um navegador. Resumindo, o cliente UAF é a ponte de ligação entre o autenticador e o servidor UAF que realizará a autenticação do dispositivo.

Servidor FIDO UAF

O servidor UAF é o componente do lado do provedor de autenticação. Ele é responsável por receber e tratar as requisições vindas do cliente UAF, realizar a conferência da solicitação do registro, confirmando de que se trata de um dispositivo realmente homologado pela FIDO Alliance. O servidor UAF também é responsável pela autenticação das mensagens vindas do cliente UAF, durante uma solicitação de login ou confirmação de transação, realizando a conferência através do dispositivo registrado para o usuário.

Camada de abstração FIDO UAF

Trata-se de uma interface entre o cliente e o autenticador que prove suporte às operações definidas pelo protocolo e facilitando o desenvolvimento entre os diversos fabricantes, abstraindo características da tecnologia do autenticador.

Autenticador FIDO UAF

O autenticador é o ente seguro responsável por prover e gerenciar as chaves criptográficas utilizadas na autenticação da mesma. O autenticador é conectado ou instalado internamente no dispositivo FIDO.

O autenticador é o que implementa o segundo fator de autenticação, como a biometria ou a senha, e é responsável por realizar localmente a autenticação deste fator. A confiança do servidor UAF na força do método de autenticação está na capacidade de o autenticador realizar esta validação e na segurança do processo.

Serviço de Metadados de Segurança FIDO

Durante o registro de um dispositivo FIDO, o servidor precisa se certificar de que se trata de um dispositivo genuinamente homologado. Por esse motivo, todo dispositivo homologado é assinado por um certificado digital da FIDO Alliance com a finalidade de atestar a sua autenticidade. O servidor UAF deve ser capaz de validar essa assinatura utilizando a chave pública deste certificado, que geralmente é distribuído pela FIDO por um canal em separado em um momento anterior.

2.6.5.2. Protocolos de comunicação

A troca de mensagens entre o cliente e o servidor acontece seguindo um protocolo especificado pela FIDO Alliance. Os protocolos são utilizados para os cenários descritos a seguir:

Registro

A aplicação web é capaz de identificar que um usuário está pretendendo registrar um autenticador. A Figura 2.2 ilustra o processo de registro:

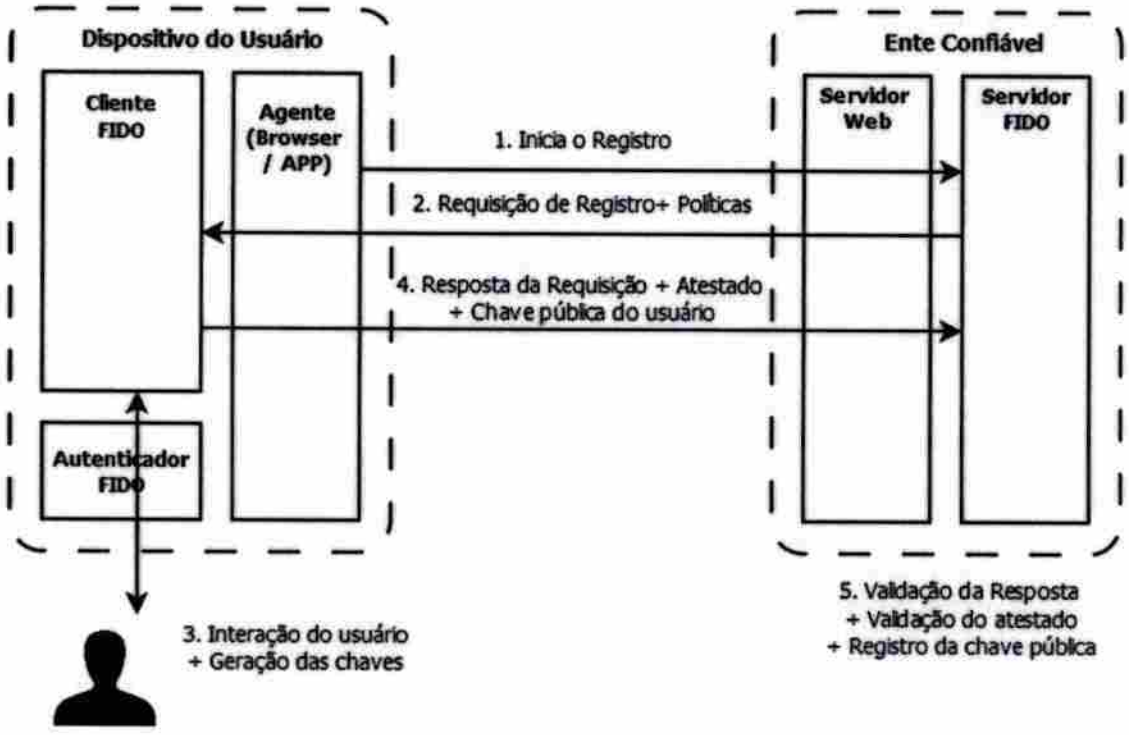

Figura 2.2 Processo de Registro do Autenticador (MACHANI et al., 2017)

1. O terminal do usuário envia o pedido de registro ao servidor;
2. O servidor FIDO entende que o usuário quer registrar o seu autenticador, então envia uma requisição de registro com um desafio;
3. O cliente UAF interage com o autenticador. O autenticador gera o par de chaves criptográficas especificamente para a aplicação que está requisitando, e interage com o usuário se necessário. O autenticador assina o desafio utilizando sua chave privada recém-criada;

4. O cliente UAF envia a resposta para o servidor UAF com a assinatura do desafio, a chave pública recém-criada e os dados da certificação de autenticidade do autenticador;
5. O servidor UAF valida a resposta com a chave pública que acabou de receber, valida a autenticidade do autenticador e registra a chave pública para o usuário.

Login e autenticação

Após o registro, a aplicação web poderá solicitar a autenticação do usuário sempre que achar necessário. O usuário deverá utilizar o mesmo autenticador que registrou. A Figura 2.3 ilustra o processo de autenticação:

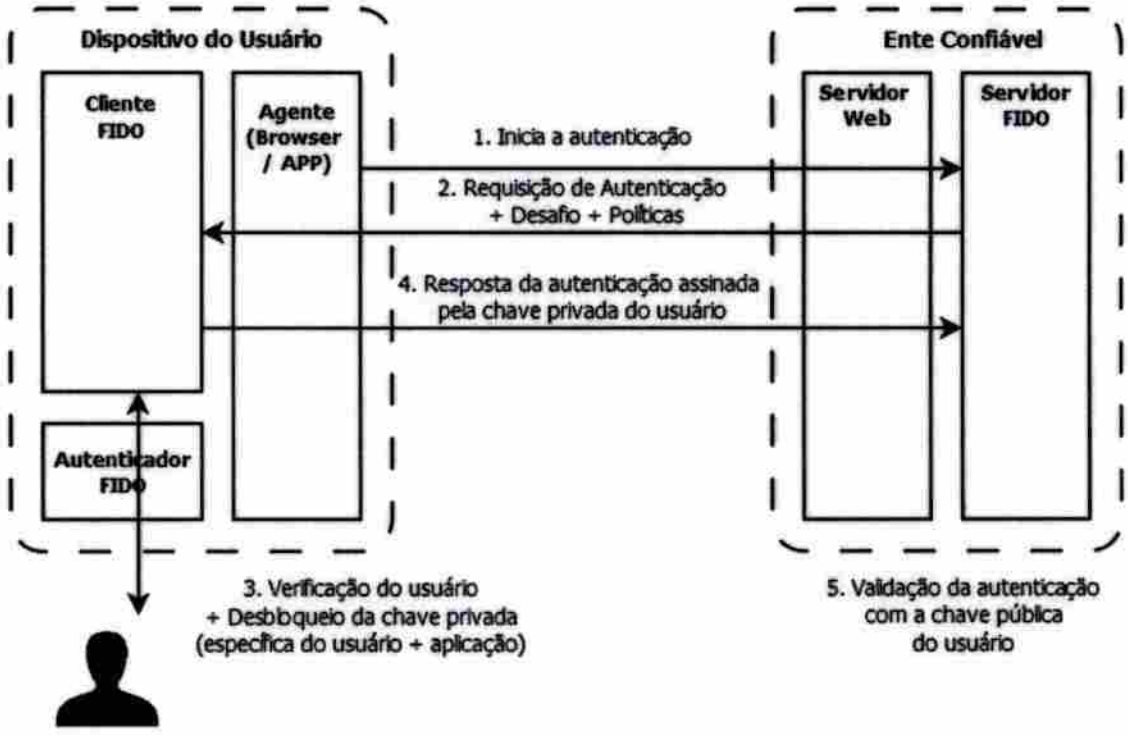

Figura 2.3 Processo de autenticação (MACHANI et al., 2017)

1. O terminal quer iniciar um processo de autenticação;
2. O servidor UAF envia uma requisição com um desafio junto com uma política de autenticação;
3. O cliente UAF acessa o autenticador. O autenticador identifica o usuário utilizando um dos fatores de autenticação, como biometria ou senha, e libera o uso da chave privada específica para aquele usuário e aplicação web. O autenticador assina a requisição e devolve para o cliente UAF;

4. O cliente UAF envia a resposta assinada pelo autenticador para o servidor UAF;
5. O servidor UAF valida a resposta assinada utilizando a chave pública registrada para o usuário.

Confirmação de transação

Uma variação do processo de autenticação envolvendo o protocolo UAF se aplica a confirmação de transações. Dependendo da criticidade da operação, faz-se necessário uma confirmação dos dados de entrada da operação, de forma a evitar adulteração durante a transação. Caso o dispositivo possua uma maneira de interagir com o usuário, este pode visualizar os dados da transação dentro do dispositivo, e ter a garantia que os dados assinados serão exatamente aqueles. A Figura 2.4 ilustra o processo de autenticação de uma transação:

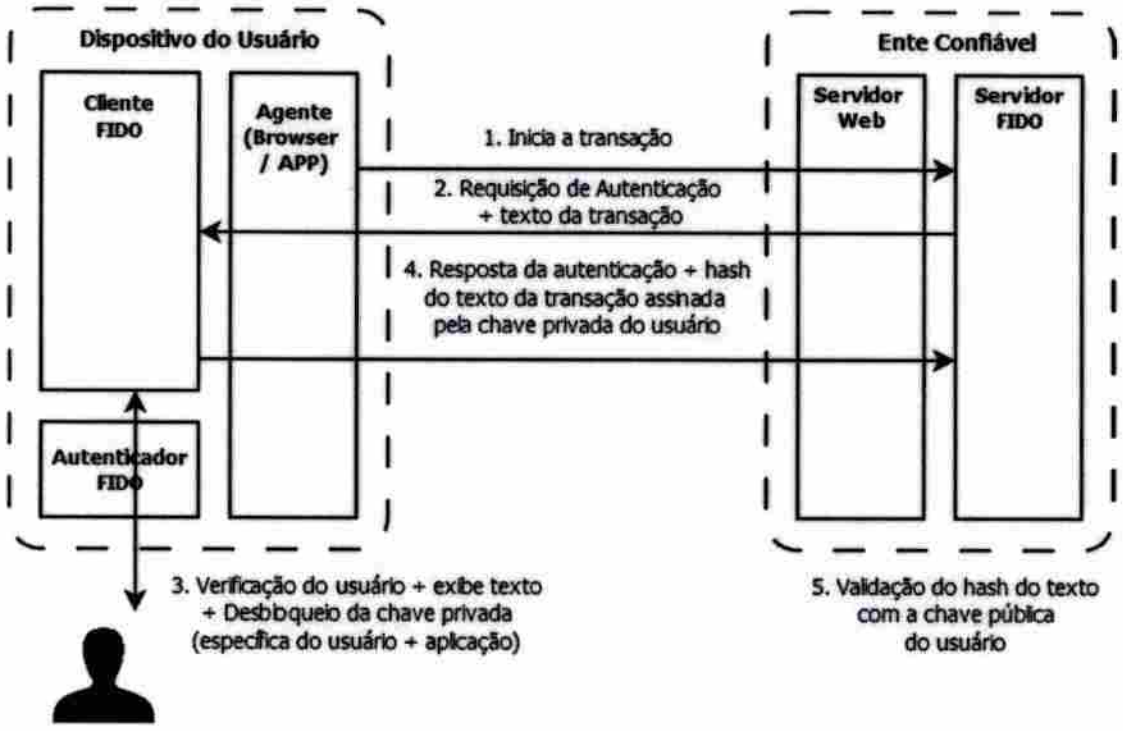

Figura 2.4 Processo de autenticação de uma transação (MACHANI et al., 2017)

1. O terminal do usuário inicia uma transação;
2. Supondo que a aplicação web necessite da confirmação dos dados, o servidor UAF envia uma requisição ao cliente, juntamente com os dados da transação;
3. O cliente UAF acessa o autenticador e envia os dados da transação; O usuário visualiza os dados e confirma com um fator de autenticação como a senha ou

biometria; O autenticador identifica o usuário, acessa a chave privada específica do usuário e da aplicação web e assina os dados da transação;

4. O cliente UAF envia a resposta, juntamente com a assinatura da transação;
5. O servidor UAF valida a assinatura da transação utilizando a chave pública registrada para o usuário. Se tudo correr bem, a transação pode ser liberada para ser executada.

Cancelamento do registro

Pode ocorrer a necessidade de o usuário remover o registro do seu dispositivo FIDO de uma aplicação. Nesse caso, o usuário solicita o cancelamento, e então o servidor UAF envia uma requisição de cancelamento para o cliente UAF. O cliente UAF então solicita ao autenticador que exclua a chave privada vinculado à aplicação web.

2.6.6. U2F – Universal 2nd Factor

O protocolo U2F permite aumentar o nível de confiança da autenticação em aplicações que utilizam senha, adicionando no login um dispositivo homologado pela FIDO Alliance como segundo fator de autenticação (FIDO ALLIANCE, 2017a). Isso significa que, ao contrário do UAF, o protocolo U2F não substitui completamente o uso da senha.

Os dispositivos U2F possuem somente sum fator de autenticação, ou seja, o usuário não precisa utilizar um segundo fator para acessar as chaves criptográficas. Esta característica se justifica pelo fato de o usuário já ter que inserir uma senha no sistema como o primeiro fator de autenticação. A exigência para estes dispositivos é que o usuário necessariamente precisa interagir, como pressionar um botão, para evitar o uso dele remotamente.

2.6.6.1. Arquitetura

A arquitetura desenhada para o uso do U2F é idêntica ao UAF, com algumas restrições de cenários de atuação. O foco do U2F é sobre os usuários que acessam aplicações web em um navegador e utilizam um dispositivo físico como segundo fator de autenticação. A especificação da camada do cliente U2F é focado em plugins para navegadores e interfaces de operações para implementação em páginas web (SRINIVAS et al., 2016).

2.6.6.2. Protocolos de comunicação

Os protocolos são usados somente em dois cenários. O registro e a autenticação acontecem semelhante ao UAF, com a diferença que é feito somente através de uma página web, e que o usuário precisa somente interagir com o dispositivo conectado, como pressionar um botão, por exemplo (SRINIVAS et al., 2016).

3. ANÁLISE E RESULTADOS

A metodologia empregada para a análise é basicamente bibliográfica. Foi estudado os requisitos normativos publicados no documento NIST 800-63-3B, e tais requisitos foram confrontados com as especificações publicadas em diversos documentos produzidos pela FIDO Alliance. A análise seguiu os seguintes passos:

- Identificação dos tipos de autenticador;
- Levantamento dos requisitos de segurança com ênfase nos autenticadores identificados;
- Combinação coluna a coluna das evidências do cumprimento ou não dos requisitos encontrados nas especificações da FIDO Alliance;
- Avaliação do nível de confiança que os autenticadores FIDO podem obter.

3.1. ANÁLISE DOS REQUISITOS

A análise segue com a avaliação e considerações dos principais tópicos que embasam os requisitos.

3.1.1. Identificação dos autenticadores

Dado a filosofia do FIDO Alliance, que é fornecer uma forma mais segura de um usuário se autenticar do que uma senha, significa que a intenção é fornecer autenticadores multifator ou um autenticador que suplemente o método atual do sistema, neste caso, a senha. Portanto, analisando as características dos autenticadores FIDO e confrontando com os tipos normatizado na NIST 800-63B:

Dispositivos UAF são dispositivos criptográficos multifator ou softwares criptográficos multifator, pois utilizam uma chave assimétrica para se autenticar com o servidor UAF e faz uso de um fator adicional.

Dispositivos U2F são dispositivos criptográficos ou softwares criptográficos de um fator, pois são utilizados como fator adicional para reforçar a autenticação com senha.

3.1.2. Atestado de segurança

O provedor deve receber informações certificadas de segurança do dispositivo no momento do seu registro. Para isso, a FIDO Alliance insere informações de segurança dentro do dispositivo e assina com o seu certificado.

A FIDO Alliance provê dois tipos de certificado: o de funcionalidade para os servidores e o de autenticador para os dispositivos autenticadores. O certificado de funcionalidade aplica uma espécie de teste de caixa preta para certificar que as funcionalidades estão de acordo com as especificações do protocolo. Assim, um servidor pode obter o selo de certificação da FIDO Alliance.

O autenticador, além de ter que passar pelos testes de funcionalidade, precisa obter o certificado de autenticador. Este certificado atesta o nível de segurança atestado pela FIDO Alliance. Atualmente, de acordo com a política de certificação (FIDO ALLIANCE, 2017c):

Certificação Nível 1: Certifica que o autenticador implementou os requisitos de segurança. Tais requisitos de segurança remete a implementação dos protocolos especificados e às camadas da arquitetura.

Certificação Nível 2: Certifica que o autenticador resistiu a diversos softwares de ataque testados em laboratório. Os autenticadores com este nível de certificação também estão em conformidade com um conjunto restrito de hardware e ambientes que utilizam para operar.

Há outros níveis de certificação ainda em fase de prospecção que irão garantir uma maior segurança e conformidade com outras especificações.

Como parte da certificação, a FIDO Alliance divulga as informações de todos os autenticadores certificados. Desta forma, os servidores FIDO se mantém atualizados sobre todos os autenticadores existentes, com informações diversas que ajudam as aplicações a tomar decisões sobre quais autenticadores permitirão utilizar ou não.

3.1.3. Algoritmos Criptográficos

Os algoritmos de assinatura utilizados são assimétricos, que são o ECDSA P-256 e o RSA 2048, que são algoritmos aprovados (BARKER, 2016). O tamanho das chaves também

segue o recomendado pela NIST 800-131A, com o mínimo de 112 bits de tamanho (BARKER; ROGINSKY, 2015). Os algoritmos de hash utilizados são o SHA-256 e SHA-512, aprovados em Barker (2016). O algoritmo utilizado para gerar valores aleatórios recomendado é o especificado em Barker e Kelsey (2015). Em resumo, as especificações da FIDO Alliance utilizam de algoritmos aprovados pela NIST.

A restrição do uso somente de algoritmos assimétricos desonera o provedor de implementar mecanismos de proteção para evitar o comprometimento da chave, pois se trata somente de uma chave considerada pública.

3.1.4. Proteção do canal de segurança

Como o NIST requisita em Grassi et al. (2017c), a especificação do FIDO Alliance requer a utilização o protocolo TLS versão 1.2 em suas comunicações. (BAGHDASARYAN et al., 2017). Ambas as especificações consideram a aplicação deste protocolo o suficiente para mitigar ataques de MitM.

3.1.5. Gerenciamento da chave criptográfica no dispositivo

Um usuário pode registrar o seu dispositivo FIDO em mais de uma aplicação web para se autenticar. Portanto, o dispositivo deve ser capaz de manter uma chave criptográfica para cada aplicação web distinta, e isso é feito utilizando o endereço da aplicação como parte do identificador, como https://fido.servidor.com/usu33323, por exemplo (SRINIVAS et al., 2016).

Essa estratégia permite a segregação das chaves por finalidade, e sem permitir que uma chave seja utilizada para uma aplicação a qual não pertence. O uso do endereço como identificador também oferece uma resistência a mais contra-ataques MitM, pois caso o endereço de origem seja diferente, a autenticação não será válida, pois o dispositivo não encontrará a chave ou gerará uma assinatura digital que não irá valer para a aplicação original.

3.1.6. Resistência a ataques de repetição

Além do uso do protocolo TLS, o ataque de replay é mitigado com o envio de um desafio, previsto nos protocolos de registro e de autenticação (SRINIVAS et al., 2016). O

provedor deve ser capaz de validar se este desafio foi gerado pelo próprio e se já não foi utilizado anteriormente ou fora da janela de tempo de validade.

3.1.7. Intenção de autenticação

Os requisitos de segurança do FIDO Alliance exigem que o autenticador implemente um mecanismo que exija a interação do usuário ao utilizar o autenticador, como um botão ou alguma característica biométrica que represente uma atitude explícita. O protocolo UAF define também uma operação de confirmação de transação, onde o usuário pode ser solicitado para confirmar uma operação.

3.1.8. Aderência a FIPS 140

A FIPS 140 (NIST, 2001) estabelece níveis de segurança para o uso de módulos criptográficos que operam com chaves criptográficas. No entanto, não foram encontradas evidências da exigência de um determinado nível de segurança nas políticas de certificação de autenticador da FIDO. Porém não pode ser descartado o fato de existirem fabricantes que certificam seus dispositivos com um determinado nível de segurança.

3.1.9. Biometria

Os requisitos no NIST são mais generalizados e determinam algumas metas de performance a ser cumprido (GRASSI et al., 2017c). Do lado da FIDO Alliance não foi encontrado nenhuma especificação de itens de segurança e performance.

3.2. EVIDÊNCIAS DOS REQUISITOS DE SEGURANÇA

As tabelas a seguir mostram todos os requisitos considerados para a análise, e as evidências encontradas nas especificações da FIDO Alliance. Os requisitos do autenticador e do provedor foram separados por protocolo. A Tabela 3.1 mostra as informações que devem conter ao atestar a certificação do autenticador; a Tabela 3.2 e a Tabela 3.3 listam as características e os requisitos para o autenticador U2F, respectivamente; a Tabela 3.4 e a Tabela 3.5 fazem o mesmo para os autenticadores UAF; e finalmente, a Tabela 3.6 e a Tabela 3.7 para os servidores FIDO:

Tabela 3.1 Atestado de informações de segurança do autenticador

NIST 800-63-3B	FIDO Alliance
Dados sobre a procedência do autenticador	Fornece dados da identificação do fabricante, versão do autenticador e descrição. Situação da certificação, como data de validade e situação da certificação
Características de segurança do autenticador	Fornece diversas informações de segurança, como protocolos criptográficos reconhecidos e forma de manuseio da chave criptográfica (LINDEMANN; KEMP, 2017a)
Modalidade do leitor biométrico	Informa o método de identificação do usuário (LINDEMANN; KEMP, 2017a)
Características de segurança e performance do leitor biométrico	Quando apropriado, fornece informações sobre taxa de falsos positivos, quantidade de tentativa até o bloqueio e tempo de espera para a próxima tentativa (LINDEMANN; KEMP, 2017a)
Deve ser assinado com um certificado digital	Metadados são inseridos no autenticador e assinados utilizando um certificado digital do nível de certificação apropriado (LINDEMANN, 2017a)

Tabela 3.2 Características do Autenticador U2F

NIST 800-63-3B	FIDO Alliance U2F 1.1
Dispositivo criptográfico ou software criptográfico de um fator	Dispositivo físico que complementa a autenticação com senha
Encapsula uma chave criptográfica única para o dispositivo, e tal chave não pode ser passível de extração. Esta chave pode ser tanto simétrica quanto assimétrica	Utiliza chave assimétrica especificado determinado pelo protocolo cujo par de chaves é gerado no dispositivo (SRINIVAS et al., 2016)
O autenticador assina o desafio que é recebido pela porta de comunicação a qual está conectado	O dispositivo realiza as operações e se comunica por meio de porta USB, NFC ou Bluetooth (SRINIVAS et al., 2016)

Tabela 3.3 Requisitos do Autenticador U2F

NIST 800-63-3B	FIDO Alliance U2F 1.1
Utilizar um algoritmo criptográfico aprovado	Utiliza ECDSA P-256 e SHA256 para assinatura digital (BALFANZ; EHRENSVARD; LANG, 2016)
O tamanho da chave deve ter o tamanho mínimo determinado	
A chave criptográfica deve ser armazenada em um repositório seguro de chaves disponível para a aplicação	Medida de segurança SM-1 (LINDEMANN, 2017c), a chave deve ser protegida contra mau uso
O acesso à chave deve ser limitado somente aos componentes do autenticador	Medida de segurança SM-13 (LINDEMANN, 2017c), deve haver um controle de acesso à chave
FIPS-140	Não especificado. Pode haver a certificação ou não, dependendo do fabricante
Resistencia a MitM	Utiliza o protocolo TLS e o gerenciamento da chave criptográfica é pelo endereço da aplicação legítima (SRINIVAS et al., 2016)
Resistência a ataques de repetição	É utilizado um valor aleatório e único para a requisição como desafio, gerado pelo servidor (SRINIVAS et al., 2016)
Intenção de autenticação	O dispositivo deve testar a presença do usuário com alguma forma de interação. (SRINIVAS et al., 2016)

Tabela 3.4 Características do Autenticador UAF

NIST 800-63-3B	FIDO Alliance UAF 1.1
Dispositivo criptográfico multifator	Dispositivo que utiliza senha ou biometria para identificar o usuário
Encapsula uma chave criptográfica única para o dispositivo, e tal chave não pode ser passível de extração. Esta chave pode ser tanto simétrica quanto assimétrica	O dispositivo cria chaves criptográficas para a autenticação durante o seu registro. (MACHANI et al., 2017). Geralmente são criadas um par de chaves assimétrica com

	o algoritmo ECDSA. (BAGHDASARYAN et al., 2017)
O uso da chave somente será possível após a verificação de um segundo fator, que deve ser uma senha ou biometria	Premissa de utilização de dispositivos de autenticação multifator (MACHANI et al., 2017)

Tabela 3.5 Requisitos do Autenticador UAF

NIST 800-63-3B	**FIDO Alliance UAF 1.1**
Utilizar um algoritmo criptográfico aprovado	Utiliza ECDSA P-256 e SHA256 para assinatura digital (LINDEMANN, 2017b)
O tamanho da chave deve ter o tamanho mínimo determinado	
Toda a autenticação que utilizar o autenticador deverá exigir a utilização do fator adicional	O autenticador sempre exigirá o segundo fator nas transações de autenticação e confirmação de transação (BAGHDASARYAN et al., 2017)
A impostação do fator adicional deverá ser feita diretamente no dispositivo ou por uma porta de comunicação via hardware, como USB, por exemplo	É encorajado o uso de sensores biométricos presentes nos dispositivos móveis do usuário. O usuário se autenticaria localmente no dispositivo (MACHANI et al., 2017)
Toda e qualquer informação que fora manipulada em memória, como a chave, senha ou dados de captura de biometria, devem ser sobrescritos imediatamente após ocorrida a autenticação	Não especificado
A chave criptográfica deve ser armazenada em um repositório seguro de chaves disponível para a aplicação	Medida de segurança SM-1 (LINDEMANN, 2017c), a chave deve ser protegida contra mau uso
O acesso à chave deve ser limitado somente aos componentes do autenticador	Medida de segurança SM-13 (LINDEMANN, 2017c), deve haver um controle de acesso à chave
FIPS-140	Recomenda a certificação FIPS-140 para facilitar na implementação do autenticador (LINDEMANN; KEMP, 2017a)
Senha como fator adicional	

A senha a ser utilizada como fator adicional deve ter um tamanho mínimo de seis dígitos	Não especificado
Quantidade de tentativas não maior que 100	Não especificado
Biometria como fator adicional	
Deve ser usado somente em conjunto com outro fator de autenticação em um dispositivo físico	Premissa de utilização de dispositivos de autenticação multifator (MACHANI et al., 2017)
A transmissão dos dados biométricos entre o dispositivo e o provedor deve ser feito por meio de um canal de comunicação protegido	Há uma especificação (BAK, 2017) que define estratégias para a comunicação segura entre o sensor e o componente do dispositivo
Deve operar com uma taxa de falso positivo de 1 em 1000, ou valor melhor (INTERNATIONAL STANDARD, 2017)	Não especificado
Implementação de técnicas de detecção de presença (INTERNATIONAL STANDARD, 2016)	Embora não estritamente exigido, recomenda a implementação de técnicas de detecção de presença (LINDEMANN; KEMP, 2017a)
Deve permitir até 5 tentativas consecutivas de erro na autenticação. Se houver alguma técnica de detecção de presença implementado, pode permitir até 10 tentativas	Não especificado
Após atingir a quantidade de tentativas, impor um intervalo de 30 segundos até a próxima tentativa, e aumentar o intervalo para cada nova tentativa	Não especificado
Desabilitar a autenticação biométrica e oferecer outro fator de autenticação no lugar, como um PIN de segurança ou uma senha	Não limita a implementação de somente um fator adicional exclusivo
Pode ser feita a verificação dos dados biométricos de forma centralizada ou local	Premissa de utilização de somente verificação local (MACHANI et al., 2017)

Tabela 3.6 Características do servidor FIDO

NIST 800-63-3B	FIDO Alliance UAF/U2F 1.1
Gera um desafio e envia para o autenticador	É utilizado um valor aleatório e único para a requisição como desafio (SRINIVAS et al., 2016)
Utiliza o protocolo específico do autenticador para validar a resposta baseada no desafio	O protocolo define o algoritmo assimétrico ECDSA P-256 e SHA256 para o hash (BALFANZ; EHRENSVARD; LANG, 2016)

Tabela 3.7 Requisitos do servidor FIDO

NIST 800-63-3B	FIDO Alliance UAF/U2F 1.1
A chave criptográfica que representa o autenticador deve ser protegida contra adulteração	Somente a chave pública gerada pelo autenticador é armazenada (SRINIVAS et al., 2016)
O desafio deve ter um tamanho mínimo de 64 bits e gerado de acordo com a NIST 800-90A (BARKER; KELSEY, 2015)	Exige entropia considerável e tamanho mínimo de 8 bytes (BALFANZ, 2016)
FIPS-140	Não especificado. Pode haver a certificação ou não, dependendo do sistema.
Resistencia a MitM	Utiliza TLS e a validação da assinatura da requisição é baseada na origem da solicitação. (SRINIVAS et al., 2016)
Resistência a ataques de repetição	É utilizado um valor aleatório e único para a requisição como desafio (SRINIVAS et al., 2016)

3.3. CONCLUSÃO DA ANÁLISE

Após analisado diversos itens de segurança nas especificações FIDO Alliance e os itens na publicação NIST 800-63-3B, observa-se que os autenticadores FIDO se alinham ao propósito de fornecerem métodos de autenticação mais seguros, no entanto, por pouco, não garante toda a segurança recomendada pela NIST. O motivo desta conclusão é resumido nas

Tabelas 3.8, 3.9, 3.10 e 3.11, onde mostra o que a especificação da FIDO Alliance garante e não garante o cumprimento dos requisitos dos níveis de confiança da autenticação:

Tabela 3.8 Cumprimento dos Requisitos Gerais

Requisitos Gerais	**Cumprimento**
Biometria	Não
Atestado de segurança	Sim
Comprometimento do servidor	Sim

Tabela 3.9 Cumprimento do Requisito de Nível de Confiança da Autenticação 1

Item	**Requisito Nível 1**	**Cumprimento**
Fator de autenticação	Um fator (mínimo)	Sim
FIPS-140	Nível 1 para o provedor	Sim
Resistencia a MitM	Obrigatório	Sim
Resistência a ataques de repetição	Não obrigatório	Sim
Intenção de autenticação	Não obrigatório	Sim

Tabela 3.10 Cumprimento do Requisito de Nível de Confiança da Autenticação 2

Item	**Requisito Nível 2**	**Cumprimento**
Fator de autenticação	Multifator, ou dois autenticadores (o que o usuário sabe + o que o usuário tem)	Sim
FIPS-140	Nível 1 para o provedor e para o autenticador	Não
Resistencia a MitM	Obrigatório	Sim
Resistência a ataques de repetição	Obrigatório	Sim
Intenção de autenticação	Obrigatório	Sim

Tabela 3.11 Cumprimento do Requisito de Nível de Confiança da Autenticação 3

Item	Requisito Nível 3	Cumprimento
Fator de autenticação	Multifator (hardware), ou dois autenticadores (dispositivo criptográfico + o que o usuário sabe)	Sim
FIPS-140	Nível 1 para o provedor e para o dispositivo físico de um fator Nível 2 para dispositivo físico multifator; Nível 3 para proteção física para todos os autenticadores	Não
Resistencia a MitM	Obrigatório	Sim
Resistência a ataques de repetição	Obrigatório	Sim
Intenção de autenticação	Obrigatório	Sim

Em geral, os autenticadores FIDO passam em todos os requisitos, menos na certificação FIPS-140, pois as especificações da FIDO Alliance não exigem. No entanto, é importante observar que embora não seja especificado, o nível de segurança 1 da FIPS-140 pode ser garantido nos servidores FIDO, e não há exigência nenhuma de segurança física neste nível de segurança para os autenticadores.

Outro requisito que não foi cumprido pelas especificações da FIDO Alliance é a segurança da biometria. A biometria é um ponto sensível do processo de autenticação, pois é o fator capaz de identificar o usuário. Diversos itens de configuração ficam em aberto, o que não dá a garantia de que estes estejam sendo cumpridos adequadamente.

Os autenticadores FIDO na situação atual conseguem garantir apenas o primeiro nível de confiança. O nível 1 da confiança de autenticação é o mais baixo e se equipara a utilização de um único fator de autenticação. Isso não é o suficiente para o FIDO Alliance,

cuja proposta é aumentar este nível de segurança. Os níveis de certificação determinados pela FIDO Alliance também não garantem o cumprimento de níveis mais altos de confiança.

Embora os requisitos de biometria e FIPS-140 não tenham sido suficientes para uma classificação de segurança mais elevada, não significa que os autenticadores FIDO estão condenados.

Tais requisitos possuíam itens de configuração ajustáveis cujos valores foram propostos pela NIST 800-63-3B, mas ficaram em aberto na especificação da FIDO para os fabricantes e desenvolvedores. Significa que um fabricante tem a escolha de cumprir estes requisitos por conta própria.

3.4. PROPOSTAS DE MELHORIA DO PROCESSO

O objetivo da FIDO Alliance é obter um alcance mundial e permitir que existam métodos de autenticação seguros e que se distinguem entre si de acordo com a sua configuração. Ficaria a cargo da aplicação que desejar utilizar o padrão FIDO criar uma política de segurança de quais autenticadores permitirá utilizar.

No entanto, uma empresa ou autarquia pode ser exigida a aderência à NIST 800-63. A primeira proposta para que a aderência à NIST 800-63-3B seja atingida é que tais empresas construam uma política de segurança que permita somente autenticadores FIDO com a configuração de biometria adequada e certificação FIPS-140 de acordo com o nível de confiança da autenticação que se deseja obter.

A segunda proposta seria que os fabricantes homologassem seus autenticadores de forma a aderir aos requisitos da NIST 800-63-3B, além de obter a certificação da FIDO Alliance. Assim os autenticadores já sairiam de fábrica com a informação de qual nível de confiança da autenticação são capazes de atingir.

Complementar à segunda proposta, a FIDO Alliance poderia ir além e criar níveis de certificação de acordo com o nível de confiança da autenticação:

Níveis de certificação FIDO Alliance 1, 2 e 3: conseguem garantir o primeiro nível de confiança da autenticação da NIST 800-63-3B. Qualquer modalidade de autenticador é permitido e não há maiores critérios de segurança física.

Nível de certificação FIDO 4: Exigir aos fabricantes que as especificações de segurança seguidas estejam aderentes ao NIST 800-63-3B com o nível de confiança de autenticação 2;

Nível de certificação FIDO 5: Exigir aos fabricantes que as especificações de segurança seguidas estejam aderentes ao NIST 800-63-3B com o nível de confiança de autenticação 3.

Com essa proposta, as aplicações que utilizarem um autenticador FIDO e necessitam estar aderentes ao NIST 800-63 não irão precisar se preocupar em manter políticas elaboradas. A própria FIDO Alliance seria encarregada de cuidar para que os autenticadores continuem aderentes às políticas, revogando sua certificação ou diminuindo o seu nível de segurança quando necessário.

4. CONCLUSÃO

A última publicação do NIST 800-63 conseguiu identificar os aspectos de segurança observados na atualidade e se mostrou uma importante fonte de informação a respeito da disciplina identidade digital. Entre vários assuntos, a autenticação, que foi o principal foco deste trabalho, oferece um modelo de autenticação muito completo e didático.

O estudo da publicação da NIST 800-63 expandiu a compreensão dos requisitos de segurança mais importantes, e aplica-lo ao estudo das especificações da FIDO Alliance permitiu avaliar de um modo mais crítico a proposta.

O conhecimento adquirido e a análise proposta e executada permitem concluir que a FIDO Alliance se preocupa em aplicar vários controles seguros ao processo de autenticação, e tem potencial de fornecer métodos ainda mais seguros. No entanto, precisa exigir mais a respeito dos requisitos de segurança física dos dispositivos, que são potenciais pontos fatalmente vulneráveis.

4.1. Trabalhos futuros

Tais normatizações e recomendações como a NIST 800-63 são escassas, por isso o trabalho teve como foco somente esta publicação. No Brasil principalmente, não existe nenhuma publicação com o mesmo nível de detalhe que normatize requisitos de segurança de identidade digital. Um documento que direcionasse entidades e autarquias com uma certa importância estratégica a implementar estes requisitos diminuiria bastante os riscos e incidentes de segurança no pais.

Sendo assim, uma proposta seria elaborar um documento de normatização da identidade digital no Brasil, tomando como base o que foi assimilado no estudo da NIST 800-63.

REFERÊNCIAS BIBLIOGRÁFICAS

BAGHDASARYAN, Davit et al. *FIDO UAF Protocol Specification*. [S.l.: s.n.], 2017. 43 p. Disponível em: <https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-uaf-protocol-v1.1-id-20170202.pdf>. Acesso em: 04 abr. 2017.

BAK, Naama. *FIDO UAF APDU*. [S.l.: s.n.], 2017. 10 p. Disponível em: <https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-uaf-apdu-v1.1-id-20170202.pdf>. Acesso em: 08 jul. 2017.

BALFANZ, Dirk. *FIDO U2F Implementation Considerations*. [S.l.: s.n.], 2016. 4 p. Disponível em: <https://fidoalliance.org/specs/fido-u2f-v1.1-id-20160915/fido-u2f-implementation-considerations-v1.1-id-20160915.pdf>. Acesso em: 06 jul. 2017.

BALFANZ, Dirk et al. *FIDO U2F JavaScript API*. 2016a. Disponível em: <https://fidoalliance.org/specs/fido-u2f-v1.1-id-20160915/fido-u2f-javascript-api-v1.1-id-20160915.html>. Acesso em: 04 abr. 2017.

BALFANZ, Dirk et al. *FIDO U2F Raw Message Formats*. 2016b. Disponível em: <https://fidoalliance.org/specs/fido-u2f-v1.1-id-20160915/fido-u2f-raw-message-formats-v1.1-id-20160915.html>. Acesso em: 04 abr. 2017.

BALFANZ, Dirk; EHRENSVARD, Jakob; LANG, Juan. *FIDO U2F Raw Message Formats*. [S.l.: s.n.], 2016. 9 p. Disponível em: <https://fidoalliance.org/specs/fido-u2f-v1.1-id-20160915/fido-u2f-raw-message-formats-v1.1-id-20160915.pdf>. Acesso em: 05 jul. 2017.

BARKER, Elaine. *NIST Special Publication 800 -57 Part 1 Revision 4: Recommendation for Key Management Part 1: General*. [S.l.: s.n.], 2016. 160 p. Disponível em: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf>. Acesso em: 08 jul. 2017.

BARKER, Elaine; KELSEY, John. *NIST Special Publication 800 -90A Revision 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. [S.l.: s.n.], 2015. 110 p. Disponível em: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf>. Acesso em: 07 jul. 2017.

BARKER, Elaine; ROGINSKY, Allen. *NIST Special Publication 800-131A Revision 1: Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*. [S.l.: s.n.], 2015. 29 p. Disponível em: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf>. Acesso em: 07 jul. 2017.

BONDERUD, Douglas. *Dogged Defense: UK Announces $2.3B Cybersecurity Investment for FIDO, Other IT Initiatives*. 2016. Disponível em: <https://securityintelligence.com/news/dogged-defense-uk-announces-2-3-cybersecurity-investment-for-fido-other-it-initiatives/>. Acesso em: 26 fev. 2017.

BURNETT, Mark; KLEIMAN, Dave. *Perfect Passwords: Selection, Protection, Authentication*. 2006. ed. Rockland, MA, USA: Syngress, 2006. 200 p.

COMMISSION ON ENHANCING NATIONAL CYBERSECURITY. *Report on Securing and Growing the Digital Economy.* 2016. Disponível em: <https://www.nist.gov/sites/default/files/documents/ 2016/12/02/cybersecurity-commission-report-final-post.pdf>. Acesso em: 26 fev. 2017.

FIDO ALLIANCE. *About the FIDO Alliance*. 2017a. Disponível em: <https://fidoalliance.org/about/ overview/>. Acesso em: 04 abr. 2017.

FIDO ALLIANCE. *History of FIDO Alliance*. 2017b. Disponível em: <https:// fidoalliance.org/about/history/>. Acesso em: 04 abr. 2017.

FIDO ALLIANCE. *FIDO Certification Program Policy: Authenticator Certification*. [S.l.: s.n.], 2017c. 63 p. Disponível em: <https://fidoalliance.org/wp-content/uploads/AuthenticatorCertificationProgramPolicy_20170420.pdf>. Acesso em: 04 jul. 2017.

GRASSI, Paul A. et al. *NIST Special Publication 800 -63-3: Digital Identity Guidelines*. [S.l.: s.n.], 2017a. 73 p. Disponível em: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>. Acesso em: 04 jul. 2017.

GRASSI, Paul A. et al. *NIST Special Publication 800 -63A: Digital Identity Guidelines - Enrollment and Identity Proofing*. [S.l.: s.n.], 2017b. 44 p. Disponível em: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf>. Acesso em: 04 jul. 2017.

GRASSI, Paul A. et al. *NIST Special Publication 800 -63B: Digital Identity Guidelines - Authentication and Lifecycle Management*. [S.l.: s.n.], 2017c. 78 p. Disponível em: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf>. Acesso em: 04 jul. 2017.

INTERNATIONAL STANDARD *ISO/IEC 2382-37: Information technology - Vocabulary - Part 37: Biometrics*. 2. ed. [S.l.: s.n.], 2017. 18 p.

INTERNATIONAL STANDARD *ISO/IEC 30107-1: Information technology - Biometric presentation attack detection - Part 1: Framework*. [S.l.: s.n.], 2016. 18 p.

LINDEMANN, Rolf. *FIDO Metadata Service*. [S.l.: s.n.], 2017a. 13 p. Disponível em: <https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-metadata-service-v1.1-id-20170202.pdf>. Acesso em: 08 jul. 2017.

LINDEMANN, Rolf. *FIDO Registry of Predefined Values*. [S.l.: s.n.], 2017b. 12 p. Disponível em: <https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-registry-v1.1-id-20170202.pdf>. Acesso em: 07 jul. 2017.

LINDEMANN, Rolf. *FIDO Security Reference*. [S.l.: s.n.], 2017c. 13 p. Disponível em: <https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-security-ref-v1.1-id-20170202.pdf>. Acesso em: 07 jul. 2017.

LINDEMANN, Rolf; KEMP, John. *FIDO UAF Authenticator Commands*. [S.l.: s.n.], 2017a. 31 p. Disponível em: <http:// https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-uaf-authnr-cmds-v1.1-id-20170202.pdf>. Acesso em: 08 jul. 2017.

LINDEMANN, Rolf; KEMP, John. *FIDO Metadata Statements*. [S.l.: s.n.], 2017b. 16 p. Disponível em: < https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-metadata-statement-v1.1-id-20170202.pdf>. Acesso em: 08 jul. 2017.

LUNDBLADE, Laurence; KARLSSON, Meagan. *FIDO Authenticator Allowed Restricted Operating Environments List*. [S.l.: s.n.], 2017. 4 p. Disponível em: <https://fidoalliance.org/specs/fido-security-requirements-v1.0-fd-20170524/fido-authenticator-allowed-restricted-operating-environments-list_20170524.pdf>. Acesso em: 06 jul. 2017.

MACHANI, Salah et al. *FIDO UAF Architectural Overview*. [S.l.: s.n.], 2017. 9 p. Disponível em: <https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-uaf-overview-v1.1-id-20170202.pdf>. Acesso em: 04 abr. 2017.

NIST. *Federal Information Processing Standards Publication 140-2: Security Requirements for Cryptographic Modules*. [S.l.: s.n.], 2001. 69 p. Disponível em: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>. Acesso em: 08 jul. 2017.

SRINIVAS, Sampath et al. *Universal 2nd Factor (U2F) Overview*. [S.l.: s.n.], 2016. 12 p. Disponível em: <https://fidoalliance.org/specs/fido-u2f-v1.1-id-20160915/fido-u2f-overview-v1.1-id-20160915.pdf>. Acesso em: 04 abr. 2017.

WILLIAMSON, Graham et al. *Identity Management: A Primer*. 2009. ed. Lewisville, TX, USA: MC Press, 2009. 220 p.