Transposição da Autenticação Federada para uma Solução de Controle de Acesso Físico no contexto da Internet das Coisas

Gabriela Cavalcante da Silva[1], Carlos Eduardo da Silva[1], Emerson Ribeiro de Mello[2], Michelle Silva Wangham[3], Samuel Bristot Loli[2]

[1]Instituto Metrópole Digital - Universidade Federal do Rio Grande do Norte (UFRN)

[2]Instituto Federal de Santa Catarina (IFSC)

[3]Universidade do Vale do Itajaí (UNIVALI)

gabicavalcantesilva@gmail.com, kaduardo@imd.ufrn.br,

mello@ifsc.edu.br, wangham@univali.br, samuel.loli@ifsc.edu.br

Abstract. *Internet of Things (IoT) has been applied to several application domains, including as mechanisms for physical access control. However, existing solutions do not take into account the transposition of federated authentication combined with unified physical and logical access. In this context, this paper describes a solution for physical access control systems based on the federated authentication SAML standard, the attribute-based access control model (ABAC), and the FIDO UAF standard to provide strong authentication.*

Resumo. *A Internet das coisas (Internet of Things - IoT) está sendo utilizada em diversos domínios de aplicação, incluindo sistemas de controle de acesso físico. Entretanto, as soluções existentes não consideram a transposição da autenticação federada combinada com o acesso físico e acesso lógico unificado. Neste contexto, este artigo descreve uma solução para sistemas de controle de acesso físico baseada no padrão SAML de autenticação federada, no modelo de controle de acesso baseado em atributos (ABAC) e no padrão FIDO UAF para prover autenticação forte.*

1. Introdução

Dentre as diversas soluções no contexto da Internet das Coisas, têm-se os sistemas de controle de acesso físico (do inglês *Physical Access Control Systems - PACS*). Neste contexto é possível identificar diversas soluções[1] que fazem uso de leitores de RFID, *Bluetooth* e leitores biométricos para controlar o acesso físico a ambientes. Entretanto, tais soluções não consideram o uso de protocolos seguros nos processos de autenticação e autorização, quando se baseiam no uso de identificadores de cartão RFID. Além disso, a gestão de identidade dos usuários destas soluções geralmente seguem ou um modelo tradicional (em silo) ou um modelo centralizado. Uma descrição detalhada sobre modelos de gestão de identidades encontra-se em [Wangham et al. 2010].

Até a data da escrita deste artigo, não foi identificado entre as soluções de mercado e as descritas na literatura, um PACS baseado no modelo de identidade federada, ou seja, que se beneficia da transposição da autenticação federada para solução de controle

[1]https://kintronics.com/solutions/ip-door-access-control

de acesso físico. A gestão de identidade federada torna possível ao domínio administrativo do PACS controlar o acesso físico de usuários externos ao domínio e viabiliza o compartilhamento de informações de identidade entre múltiplos domínios.

O objetivo deste trabalho é apresentar uma solução para sistemas de controle de acesso físico baseada no padrão SAML [Committee et al. 2012] de autenticação federada, no modelo de controle de acesso baseado em atributos (ABAC) [Hu et al. 2014] e no padrão FIDO UAF [Machani et al. 2014], que faz uso de criptografia de chave pública para oferecer uma experiência sem senha durante o processo de autenticação. A solução foi projetada para possuir baixo acoplamento com o provedor de identidade (*Identity Provider - IdP*) responsável pela autenticação de usuários, para ser flexível para usuários e para administradores das políticas de acesso do PACS.

Este artigo está organizado da seguinte forma. A Seção 2 apresenta um embasamento teórico sobre controle de acesso e soluções existentes que exploram IoT para controle de acesso. A solução proposta e o protótipo desenvolvido são apresentados na Seção 3. Na Seção 4, a implementação e os resultados do protótipo são analisados. Por fim, na Seção 6, são apresentadas as considerações finais e os trabalhos futuros.

2. Referencial teórico e trabalhos relacionados

O modelo de identidades federadas [Chadwick 2009] permite que um usuário empregue uma única credencial de acesso para pleitear acesso a qualquer provedor de serviço da federação. Nesse caso, cada provedor de serviço tem a liberdade de implementar uma política de controle de acesso própria e seus mecanismos deverão estar fundamentados sobre o consumo dos atributos dos usuários. Dessa forma, o modelo de controle de acesso baseado em atributos (*Attribute Based Access Control* – ABAC) [Hu et al. 2014] mostra-se como o mais adequado para tal cenário, pois as permissões são associadas a atributos e esses últimos são associados aos usuários. Assim, o acesso será concedido a um recurso caso o usuário requisitante tenha o atributo especificado na política.

A especificação FIDO UAF [Machani et al. 2014] permite a experiência sem senha, de forma que o usuário possa se autenticar localmente junto ao seu dispositivo. Isso pode ser feito, por exemplo, por meio de sensores biométricos (leitor de impressão digital, reconhecimento facial, etc) que o dispositivo possui ou com a senha usada para desbloquear o dispositivo. Por fim, o provedor de serviço confia na informação passada pelo dispositivo, indicando que o usuário foi autenticado corretamente. Têm-se aqui a transposição da autenticação local do usuário realizada no dispositivo para um serviço na *web*. Isso é possível devido à certificação de dispositivos, que é um serviço fornecido pela FIDO Alliance. Para um *hardware* ser certificado pela FIDO esse deverá respeitar alguns requisitos de projeto, como fazer uso de ambiente seguro de execução (*Trusted Execution Environment* – TEE) ou elemento seguro (*Secure Element* – SE) para armazenamento de material criptográfico.

Dentro do contexto de IoT para controle de acesso físico, a solução de [Fremantle et al. 2014] visa a autenticação e autorização do dispositivo através de uma extensão, desenvolvida pelos autores, do protocolo *Message Queue Telemetry Transport* (MQTT) [Banks and Gupta 2014], para controlar o acesso ao MQTT *broker*. A solução proposta faz uso do OAuth2.0 [Hardt 2012] como parte do fluxo do protocolo do MQTT, porém, por não fazer uso de um canal seguro para troca dessas credenciais, re-

quisito rígido do OAuth2.0, a solução está propensa a ataques de repetição e falsificação [Niruntasukrat et al. 2016].

Em [Liu et al. 2012], é proposto um esquema de autenticação baseado em duas autoridades confiáveis: o *Registration Authority* (RA), que possui o pré-registro de todos os dispositivos e funciona na arquitetura como um *gateway*, e a *Home Registration Authority* (HRA), que é um provedor de identidades OAuth. Para a política de controle de acesso foi adotado o modelo RBAC [Sandhu et al. 1996]. Porém, o trabalho não deixa claro como efetivamente o RBAC é usado. Por exemplo, não foi apresentado a forma como eles mapearam os papéis às operações. Além disso, adotar o RBAC para a solução limita o controle de acesso ser feito somente com base no papel do usuário, porém, para cenários IoT vários outros fatores, como a localização do usuário, o tempo de acesso, etc. também podem ser importantes no processo de concessão de acesso.

Em [Fremantle and Aziz 2018], é apresentado um modelo chamado *OAuthing*, que tem como objetivo prover autenticação de usuários e de dispositivos e a gerência de consentimento dos usuários no uso de dispositivos de IoT. Nesse modelo, o fabricante (organização que produz e comercializa o dispositivo) registra cada dispositivo em um único IdP de dispositivo (DIdP), gerando um identificador para este. Quando o dispositivo é adquirido, o usuário se autentica em seu IdP e autoriza o dispositivo a atuar em seu nome, junto do DIdP. O processo resulta em um token OAuth2 gerado pelo DIdP, que é armazenado no dispositivo e permite que este aja em nome do usuário. Embora a solução permita a delegação de privilégios entre usuários e dispositivos, esta não é aplicável em situações no qual o dispositivo não pertence a nenhum usuário, como um PACS.

Em [Domenech et al. 2016] foi proposta uma infraestrutura de autenticação e de autorização para Web das Coisas (AAI4WoT) baseada nos padrões SAML e XACML. A solução provê suporte a diferentes mecanismos de autenticação para dispositivos e usuários, além de permitir que provedores de serviço façam uso de diferentes modelos de controle de acesso. A infraestrutura proposta possibilita a transposição de autenticação federada para dispositivos na IoT (como os PACS), porém, os usuários podem somente se autenticar com certificados digitais ou nome de usuário e senha.

Considerando as soluções comerciais de PACS, como as da Intelbras S/A[2] ou as ASSA ABLOY Hospitality[3], constata-se o amplo uso de cartões RFID, senhas numéricas e impressão digital como credenciais de acesso. Cabe citar, que as soluções baseadas em cartões RFID ou que fazem uso do protocolo Wiegand[4] possuem vulnerabilidades conhecidas que comprometem a segurança da solução[5].

Uma tendência atual para o PACS é o uso do *smartphone* do usuário (*mobile key*) como credencial de acesso. Nestas soluções, notou-se que é feito uso do modelo de gestão de identidade em silo ou do modelo centralizado[6]. Ou seja, na busca realizada não foi encontrada nenhuma solução comercial que oferece a possibilidade de autenticação federada que atravesse diferentes domínios administrativos.

[2]http://www.intelbras.com.br/sites/default/files/tabela_comparativa_controle_de_acessos_intelbras_2018.pdf

[3]https://www.assaabloyhospitality.com/en/aah/com/products/electronic-locks/

[4]https://www.honeywellaccess.com/documents/Td2058.pdf

[5]https://www.bbc.com/news/technology-43896360

[6]https://www.getkisi.com/guides/internet-of-things-iot

3. Autenticação federada para solução de controle de acesso físico no contexto da Internet das Coisas

A solução proposta neste trabalho faz uso da especificação FIDO UAF para permitir que os usuários usem seus telefones móveis durante o processo de autenticação para acessar um ambiente físico. Ou seja, a autenticação do usuário é feita localmente em seu telefone móvel e essa informação é enviada a um provedor de identidade (IdP), por meio do protocolo FIDO UAF. O IdP emite uma asserção SAML que é então consumida pelo provedor de serviço para realização do controle de acesso físico.

3.1. Visão geral da solução

A solução desenvolvida é composta pelos seguintes componentes principais: (1) **aplicativo para telefone Android** – responsável pela autenticação do usuário através do protocolo FIDO e transposição do resultado dessa autenticação para o IdP do usuário, além da interação com o sistema de controle de acesso físico via NFC; (2) **controlador físico embarcado em uma Raspberry Pi** – que controla a interação com o telefone móvel do usuário através do leitor NFC e o mecanismo da porta (por exemplo, uma fechadura solenoide); (3) **controlador lógico também embarcado na Raspberry Pi** – que implementa a lógica de negócio do PACS e lida com questões relacionadas a autorização. (4) **módulo de autenticação no IdP Shibboleth** – estende o IdP Shibboleth[7] para que esse possa fazer uso do protocolo FIDO UAF para autenticar seus usuários. Na solução desenvolvida, esse módulo recebeu o nome de *Multi-Factor Provider* (**MFaP**), uma vez que o mesmo permite realizar a autenticação do usuário com mais de um fator de autenticação, apesar disso não ter sido explorado no presente trabalho.

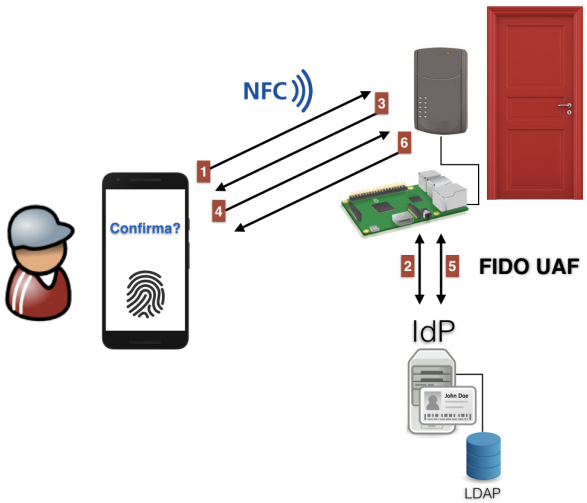

Figura 1. Componentes da solução e passos durante a autenticação de usuário

A Figura 1 ilustra os passos durante a autenticação de um usuário que está pleiteando o acesso a um ambiente físico qualquer. Previamente ao processo de autenticação, o usuário teve que registrar seu dispositivo móvel, usando o protocolo FIDO UAF, junto ao seu IdP. No passo 1, o usuário aproxima seu telefone do leitor NFC afixado junto à porta.

[7]Esta extensão está em conformidade com o padrão REFEDS MFA Profile que possibilita a definição de diferentes fluxos de autenticação em IdPs SAML.

O controlador físico identifica a aproximação, e então solicita um desafio FIDO ao IdP (que contém o MFaP), como mostra o passo 2, e o entrega ao telefone do usuário (passo 3). O usuário se autentica em seu telefone, fornecendo, por exemplo, sua impressão digital. O resultado desta autenticação é transmitida ao controlador físico (passo 4) que o envia ao IdP (passo 5) para que este verifique junto ao MFaP se a autenticação ocorreu com sucesso. Em caso afirmativo, o IdP emite uma asserção SAML, contendo o resultado da autenticação e um conjunto mínimo de atributos, e a encaminha para o telefone do usuário. Por fim, no passo 6, o controlador lógico envia o resultado da autenticação para o telefone e verifica suas políticas de controle de acesso para autorizar ou não o acesso do usuário. Em caso de acesso permitido, o controlador físico envia o comando para abrir a porta. Cabe citar que toda comunicação entre o telefone do usuário e o controlador embarcado é feita por meio do canal estabelecido via NFC. A comunicação entre a Raspberry Pi e o IdP/MFaP do usuário é feita por meio de uma conexão TCP/IP.

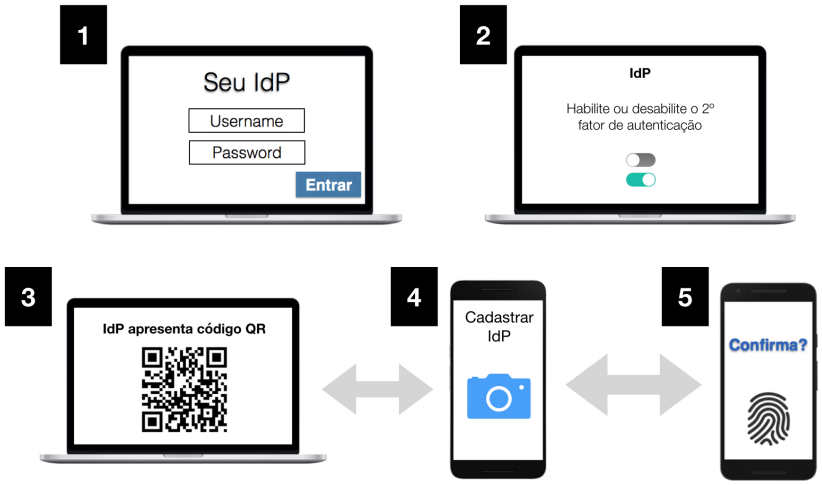

Figura 2. Habilitando FIDO UAF como único fator de autenticação.

Na Figura 2, é ilustrado o processo de registro do telefone do usuário. O usuário acessa a página *web* do MFaP e se autentica por meio de seu nome de usuário e senha que já possui cadastrado em seu IdP (passo 1). No passo 2, o usuário indica que quer registrar seu telefone e assim é apresentado um QRCode (passo 3) que o usuário deverá ler por meio do aplicativo instalado em seu telefone (passo 4) e se autenticar localmente junto ao seu dispositivo, por exemplo, fornecendo sua impressão digital (passo 5). Se a autenticação do usuário em seu dispositivo ocorreu com sucesso, então o aplicativo envia a resposta do desafio FIDO para o MFaP, que valida a resposta, armazena a chave pública enviada pelo aplicativo e envia para ele uma mensagem de sucesso.

3.2. Arquitetura

A Figura 3 ilustra a arquitetura da solução desenvolvida que possui os seguintes componentes: um *Controlador Físico*, atuando como um *gateway* para os dispositivos físicos (um leitor NFC e um mecanismo de trava de uma porta). Esse controlador físico por sua vez é conectado a um *Controlador Lógico*, que representa um componente de software capaz de armazenar e processar os dados produzidos pelas "coisas". Ambos os controladores físico e lógico são embarcados em uma Raspberry Pi.

No tocante a uma federação, o conjunto de dispositivos físicos, controladores físico e lógico constituem um provedor de serviço (*Service Provider* - SP). Desse modo, o *Controlador Lógico* é responsável por interagir com um provedor de identidades (*Identity Provider* - IdP) e com o *Servidor de Autorização*.

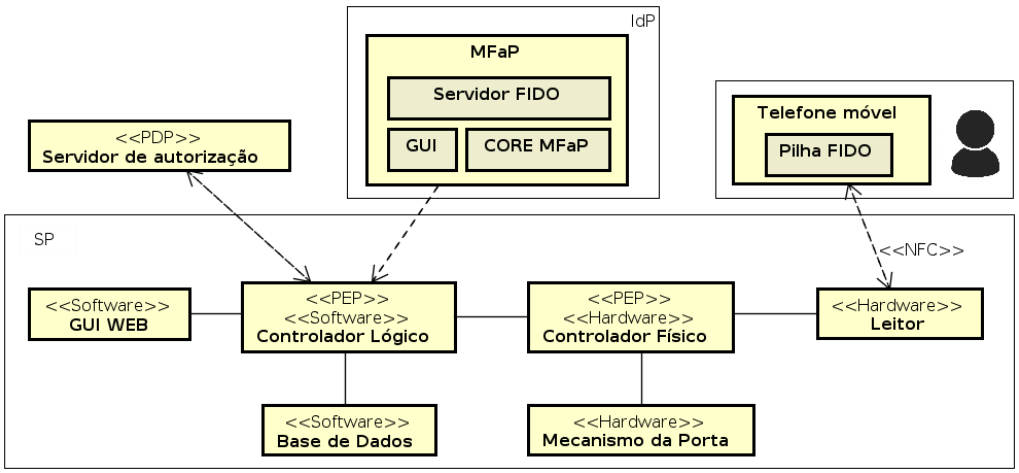

Figura 3. ***Diagrama de Componente do Protótipo IoT com AuthN/AuthZ em federação***

O IdP é o componente responsável pela autenticação do usuário e, acoplado a ele, está o *Multi-Factor Provider* (MFaP), para gerenciar a autenticação do usuário com FIDO UAF. O MFaP é responsável por implementar um Servidor FIDO que é acessado através de uma API REST. Adicionalmente, o MFaP também oferece um serviço de registro dos dispositivos móveis (módulo *CORE MFaP*) atuando como um SP dentro da federação que é acessado através de uma interface Web (módulo *GUI*).

O telefone móvel do usuário deve possuir suporte ao FIDO (representado pelo módulo *Pilha FIDO*) e contém um aplicativo desenvolvido neste trabalho. A *pilha FIDO* é um componente de software embarcado no telefone móvel durante seu processo de fabricação, isto é, de acordo com a especificação [Machani et al. 2014], todo dispositivo FIDO UAF deverá passar por um processo de certificação promovido pela *FIDO Alliance*. Para o desenvolvimento desse protótipo, como foi feito uso de telefone não certificado pela FIDO Alliance, optou-se por fazer uso do aplicativo *Dummy FIDO UAF Client* [De Mello 2017] que implementa o protocolo FIDO UAF.

O aplicativo Android permite ao usuário cadastrar o dispositivo como autenticador FIDO junto ao MFaP, além de atuar como cliente para a solução de controle de acesso físico, interagindo com o *Leitor* e permitindo ao usuário se autenticar através do FIDO. Deste modo, a solução faz uso do FIDO UAF [Machani et al. 2014] como único fator de autenticação, suportando a transposição de credenciais de uma federação para um ambiente de PACS baseado em IoT.

No que diz respeito ao controle de acesso, as políticas de autorização, assim como os mecanismos de suporte são responsabilidade do *Servidor de autorização*, que atua como um PDP (*Policy Decision Point*). O *Controlador Físico* e *Controlador Lógico* fazem o papel de PEP (*Policy Enforcement Point*), sendo responsáveis por executar as decisões do PDP.

4. Implementação e Resultados

A implementação do protótipo foi dividida em dois repositórios. O SP que roda embarcado no Raspberry Pi e controla os dispositivos IoT pode ser encontrada no repositório do GT-AMPTo[8]. A implementação do componente FIDO UAF do MFaP que é acoplado a um IdP SAML tem um repositório próprio[9]. Cada repositório contém suas respectivas documentações, incluindo informações e requisitos para instalação. Também foi disponibilizado um vídeo explicando as funcionalidades da ferramenta e como utilizá-la[10].

Para a atual demonstração, no protótipo disponibilizado nos repositórios, o IdP não emite a asserção SAML, no lugar disso, o identificador do usuário autenticado é utilizado como atributo para verificar as suas permissões nas políticas de acesso que foram implementadas através de uma ACL. Isso foi necessário devido a proteção de propriedade intelectual e, após a conclusão do registro do software realizado pelo grupo, o mesmo será completamente disponibilizado em seus respectivos repositórios.

Na solução implementada, utilizou-se um Raspberry Pi, um módulo Leitor RFID-RC522 e a trava magnética para porta como componentes de Hardware. A interface GUI provida pelo *Controlador Lógico* foi implementada usando *framework Flask*[11]. No *Controlador Lógico*, a comunicação NFC com o dispositivo móvel, a troca de mensagens com o IdP e o *PEP*, que intercepta a requisição e aplica o controle de acesso, foram implementados em *scripts python*.

5. Demonstração

Na demonstração planejada para o Salão de Ferramentas, vamos apresentar o cenário de controle de acesso físico e lógico integrado, com a tranca da porta e o leitor NFC. Necessitaremos de 1 ponto de rede e 3 tomadas de energia.

6. Conclusão

Este artigo apresentou uma solução para sistemas de controle de acesso físico (PACS) baseada no padrão SAML de autenticação federada, no modelo de controle de acesso baseado em atributos (ABAC) e no padrão FIDO UAF para prover autenticação forte. O protótipo implementado como prova de conceito comprovou a viabilidade e aplicabilidade da solução. Como trabalhos futuros, pretende-se implementar novos casos de uso, como um protótipo de registro de presença de alunos, e fazer uso de outras tecnologias como os *Bluetooth Proximity Beacons*, para geolocalização dentro de ambientes fechados [Gomez et al. 2012].

Agradecimentos

Este trabalho foi desenvolvido no contexto do Grupo de Trabalho Autenticação Multifator para Todos (GT-AMPTo)[12] financiado pela RNP.

[8]https://git.rnp.br/GT-AMPTo/IoT-Ampto
[9]https://git.rnp.br/GT-AMPTo/ampto-mfaprovider
[10]https://www.youtube.com/watch?v=kN10YRXkt9c
[11]http://flask.pocoo.org
[12]https://gtampto.sj.ifsc.edu.br

Referências

Banks, A. and Gupta, R. (2014). Mqtt version 3.1. 1. *OASIS standard*, 29.

Chadwick, D. W. (2009). Federated identity management. In *Foundations of Security Analysis and Design V*, pages 96–120.

Committee, O. S. S. T. et al. (2012). Security assertion markup language (saml) 2.0.

De Mello, E. R. (2017). A dummy fido uaf client suitable to conduct development tests on android smartphones that are not fido ready. https://doi.org/10.5281/zenodo.375567.

Domenech, M. C., Boukerche, A., and Wangham, M. S. (2016). An authentication and authorization infrastructure for the web of things. In *Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, Q2SWinet '16, pages 39–46, New York, NY, USA. ACM.

Fremantle, P. and Aziz, B. (2018). Cloud-based federated identity for the internet of things. *Annals of Telecommunications*, 73(7):415–427.

Fremantle, P., Aziz, B., Kopecký, J., and Scott, P. (2014). Federated identity and access management for the internet of things. In *Proceedings of the 2014 International Workshop on Secure Internet of Things*, SIOT '14, pages 10–17, Washington, DC, USA. IEEE Computer Society.

Gomez, C., Oller, J., and Paradells, J. (2012). Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors*, 12(9):11734–11753.

Hardt, D. (2012). The oauth 2.0 authorization framework. RFC 6749, RFC Editor. http://www.rfc-editor.org/rfc/rfc6749.txt.

Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., and Scarfone, K. (2014). SP 800-162. Guide to Attribute Based Access Control (ABAC) Definitions and Considerations. Technical report, National Institute of Standards and Technology, McLean and Clifton, VA, United States.

Liu, J., Xiao, Y., and Chen, C. L. P. (2012). Authentication and access control in the internet of things. In *ICDCS Workshops*, pages 588–592. IEEE Computer Society.

Machani, S., Philpott, R., Srinivas, S., Kemp, J., and Hodges, J. (2014). Fido uaf architectural overview. *FIDO Alliance, December*.

Niruntasukrat, A., Issariyapat, C., Pongpaibool, P., Meesublak, K., Aiumsupucgul, P., and Panya, A. (2016). Authorization mechanism for mqtt-based internet of things. In *ICC Workshops*, pages 290–295. IEEE.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., and Youman, C. E. (1996). Role-based access control models. *Computer*, 29(2):38–47.

Wangham, M. S., de Mello, E. R., da Silva Böger, D., Guerios, M., and da Silva Fraga, J. (2010). Gerenciamento de identidades federadas. In *Minicurso - SBSeg 2010 - Fortaleza - CE*, pages 1–52.