Proposta para Grupo de Trabalho

GT-CoFee: Um Esquema de Gestão de Identidade Federada para IoT

Serviços Avançados: Gestão de Identidade

Leonardo Barbosa e Oliveira

14 de março de 2017

1. Título

GT-CoFee: Gestão de Identidade Federada para Internet das Coisas

2. Coordenador

O coordenador proponente deste projeto é o Prof. **Leonardo B. Oliveira** Bolsista de Produtividade em Pesquisa do CNPq e professor do Programa de Pós-Graduação em Ciência da Computação da UFMG. Trabalhou com projetos na área de Segurança em parceria com a Microsoft Research, Intel Labs, Information Security Group de Royal Holloway e Palo Alto Research Center. Foi professor da Universidade Estadual de Campinas e publicou artigos em veículos de impacto como SenSys e IPSN. Seu trabalho científico foi agraciado com distinções de instituições como Intel, IEEE, Microsoft e SBC. Trabalhou na indústria coordenando projetos para agências governamentais e/ou grupos bancários na área de Segurança. É coordenador do Grupo de Pesquisa *Segurança Digital, Criptografia e Privacidade* do CNPq, foi coordenador geral do SBSeg'14 e coordenador do TPC do SBSeg'16. É membro do Comitê Consultivo da Comissão Especial de Segurança da Informação e Sistemas Computacionais (CESeg) da SBC e do Comitê de Gestão de Identidade da RNP.
Coordenou projetos do CNPq, FAPEMIG, Intel labs, LG Mobile Research e Microsoft Research. Seu h-index, número de trabalhos publicados, citações são aproximadamente: 20, 100, 2000, respectivamente. Seus interesses de pesquisa incluem Segurança Digital, Internet das Coisas e Computação Aplicada. http://lattes.cnpq.br/2522777418118689 **Contato**:

3. Programa de P&D

Serviços Avançados: Gestão de Identidade

4. Resumo

A gestão de identidade (IdM) em IoT é uma tarefa desafiadora. Com o crescimento dos serviços na Internet cresce também o risco de fraudes e, por sua vez, os desafios para garantir a autenticação, autorização e responsabilização. Tais desafios são potencializados quando a rede em questão é IoT. Aqui, até mecanismos como certificados digitais se mostram caros e, então, inadequados. Pior, os dispositivos, hoje, estão atrelados a usuários dos seus proprietários e não há IdM de dispositivos propriamente dita. Este trabalho objetiva, portanto, conceber um esquema de IdM para IoT. Mais precisamente, vislumbramos uma gestão federada dada a natureza móvel de dispositivos. Nosso trabalho, Coisas Federadas (CoFe), será complementar à Comunidade Acadêmica Federada (CAFe) para o uso em dispositivos IoT.

5. Abstract

Identity management (IdM) in IoT is a challenging task. With the growth of Internet services, the risk of fraud increases, as well as the challenges of ensuring authentication, authorization and accountability. Such challenges are enhanced when a network in question is IoT. Here, mechanisms such as digital certificates prove costly and therefore inadequate. Worse, devices today are tied to their owners users and there is no an IdM formed by devices themselves. This work aims, therefore, to conceive an IdM scheme for IoT. More precisely, we envisage federal management given the mobile nature of devices. Our work, Federated Things (CoFe), will complement the Federated Academic Community (CAFe) for use in IoT devices.

6. Parcerias

Para o desenvolvimento do projeto teremos o apoio da Universidade Estadual de Campinas (Unicamp), na pessoa do **Prof. Marco A. A. Henriques** do Depto. de Eng.

de**Coordenador Adjunto.** Computação da Fac. de Eng. Elétrica e de Computação, que atuará na condição de

Marco Aurélio possui graduação em Engenharia Elétrica pela Universidade Federal de Juiz de Fora (1986), mestrado em Engenharia Elétrica pela Universidade (Federal) de Chiba — Japão (1990) e doutorado em Computer Science, também pela Universidade (Federal) de Chiba - Japão (1993). Trabalhou como pesquisador e Professor Associado no Departamento de Engenharia da Informação da Universidade (Federal) de Shinshu — Nagano, Japão, de 1993 a 1996 e atualmente é Professor Associado da Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas (Unicamp). Além das atividades acadêmicas, exerceu também na Unicamp as funções de Coordenador do Curso de Graduação em Engenharia de Computação, de Superintendente do Centro de Computação (CCUEC) e de Coordenador Geral de Tecnologia de Informação e Comunicação (CTIC). Atualmente é o chefe do Departamento de Engenharia de Computação e Automação Industrial da FEEC/Unicamp, onde tem lecionado disciplinas, feito pesquisas e orientado trabalhos de iniciação científica, mestrado e doutorado nas áreas de Ciência e Engenharia da Computação, com ênfase em segurança da informação e processamento de alto desempenho. Participa do Projeto FORTE (Forense Tempestiva e Eficiente), financiado por 4 anos pela CAPES, junto com pesquisadores da Unicamp, UnB, UECe e Polícia Federal na busca de métodos mais eficazes para análise de grandes volumes de dados e mídias digitais capturados em investigações. Tem interesse em pesquisas nas áreas de criptografia e segurança aplicadas, gestão de identidades digitais e protocolos de suporte a criptomoedas. http://lattes.cnpq.br/8792400749259477 **Contato**:

7. Duração do projeto e marcos

Este projeto visa conceber, desenvolver e avaliar uma solução de gerenciamento de identidade federada adaptada para o contexto IoT. As atividades planejadas para este projeto estão resumidas na tabela 1 e detalhadas a seguir.

	Mês											
Marcos	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Revisão da literatura												
Especificação do Protocolo												
Desenvolvimento do Protótipo												

Avaliação do Protótipo												
Envio de Artigos e Disponibilização do Protótipo												

Tabela 1: Cronograma.

Revisão da literatura: examinaremos novamente a literatura e verificaremos se algo novo surgiu nos últimos meses. Vamos compilar todos os trabalhos relacionados em um relatório, destacando os aspectos-chave de cada um em uma tabela de comparação. **Produto**: compêndio dos principais artigos na área (RT1: Termo de Referência e Estado da Arte).

Especificação do Protocolo: vamos revisitar os vários tipos de criptossistemas para escolher aqueles que melhor se aplicam ao nosso contexto, ou seja, esquema de identidade federada mais leve. Vamos projetar um protocolo seguro, usando o estado-da-arte em primitivas criptográficas, para a comunicação de/para dispositivos (usuários), SPs e IdPs. **Produto** : um relatório técnico descrevendo os criptossistemas a serem combinados no CoFee (RT2: Proposta do Protótipo).

Desenvolvimento do Protótipo: vamos desenvolver um protótipo funcional do

CoFee. No qual iremos demonstrar a comunicação entre as entidades envolvidas no CoFee: device, SP e IdP, apresentando situações inerentes a um esquema de identidade federada, além da integração com a CAFe. **Produto** : um protótipo funcional do CoFee que pode ser implantado em dispositivos reais para demonstrar a solução (RA1 a RA4: Relatórios de acompanhamento trimestrais).

Avaliação: avaliaremos a nossa solução em termos de eficiência e segurança. Quanto à eficiência, vamos avaliar o uso de CPU, memória, armazenamento e a quantidade de tráfego de dados sobre o canal de comunicação. Avaliaremos o desempenho do CoFee nos principais tipos hardwares Android, PCs, bem como nós de IoT com recursos limitados. Quanto à segurança, vamos formalmente verificar a robustez do nosso protocolo usando uma ferramenta de verificação. **Produto** : um relatório que inclui os resultados da nossa avaliação com tabelas, diagramas e gráficos para as várias plataformas (RT3: Avaliação dos Resultados do Protótipo).

Disseminação do conhecimento: submeteremos nossos primeiros resultados a uma publicação nacional especializada e nossos resultados finais a uma publicação internacional especializada. Podemos também solicitar uma patente de nossa solução e outras inovações deste projeto. **Produto**: artigo enviado ao local de publicação nacional e internacional, bem como pedido de patente (observando item 12.1 do edital desta chamada).

8. Sumário executivo

8.1. Motivação

Dentre os serviços oferecidos pela Rede Nacional de Pesquisa (RNP) está a Comunidade Acadêmica Federada (CAFe). Trata-se de um serviço de gestão de identidade que reúne instituições de ensino e pesquisa brasileiras através da integração de suas bases de dados. A CAFe conta atualmente com cerca de 84 provedores de

identidade além de oferecer serviços como, Vídeo@RNP, PADBR entre outros[1]. A CAFe oferece provedores de identidade e serviços para usuários, não tendo suporte direto a dispositivos como os presentes na Internet das Coisas.

A Internet das Coisas (Internet of Things – IoT) é um tópico de pesquisa cada vez mais relevante (Atzori et al. 2010). Um exemplo de como tecnologias de IoT estão presentes na sociedade é a utilização de tecnologias vestíveis (*wearables*). São inúmeras as possibilidades de utilização da tecnologia que incluem, lentes de contato que exibem notificações de celulares, óculos que exibem trajetos de GPS, relógios que exibem notificações recebidas no *smartphone*, e muitas outras.

Soluções aplicadas a redes sensores e redes *wireless* com restrições de recursos não podem ser diretamente aplicadas ao contexto de IoT. Por exemplo, enquanto os nós em redes de sensores normalmente executam o mesmo aplicativo e são propriedade de uma única entidade, os nós IoT podem executar tarefas diferentes e pertencer a vários proprietários. Como resultado, é necessária a pesquisa de novos mecanismos adaptados exclusivamente a IoT.

Notoriamente, existe uma grande necessidade de um esquema de gestão de identidade adaptado à IoT. Os dispositivos IoT exigem uma forma de autenticação e autorização a outros dispositivos e servidores IoT. Devido a idiossincrasias dos elementos de IoT, no entanto, abordagens amplamente adotadas são inadequadas para este contexto. Veja, os esquemas tradicionais baseiam-se em PKI e incorrem em custos significativos de processamento, memória, armazenamento, comunicação e gerenciamento, acabando por ser inadequados para IoT (Stinson, 2002). Além disso, o modelo de mobilidade IoT requer um maior nível de interoperabilidade em vários domínios quando comparado com elementos computacionais convencionais.

Como solução para este problema, propomos desenvolver um esquema de IdM exclusivamente adaptado à IoT. Identidades Federadas para a Internet das Coisas, ou CoFee (**Co**isas **Fe** d **e** radas), visando substituir protocolos pesados e primitivas criptográficas assimétricas usadas em uma PKI convencional por outras mais leves e, como tal, bem adaptadas para IoT. Em particular, planejamos aplicar Certificados Implícitos (Brown et al., 2002) e HBSs (Lamport, 1979, Buchmann et al., 2009, Merkle, 1987) para criar um mecanismo de identidade federada leve para IoT.

8.2. Objetivos

Neste projeto, nosso objetivo é projetar, desenvolver e avaliar um protótipo de um sistema gestão de identidade federada complementar à CAFe adaptado
exclusivamente para IoT. Nossa solução deve ser, ao mesmo tempo, (i) segura; (Ii) exequível em dispositivos IoT com recursos limitados; (Iii) e suportar o modelo de alta mobilidade de IoT. CoFee, nossa solução, também deve atender aos requisitos de eficiência e restrições de recursos (computação, armazenamento, comunicação) de plataformas IoT populares.

[1] https://www.rnp.br/servicos/servicos-avancados/cafe

8.3. Metodologia

Apresentamos a seguir as tecnologias, métodos e abordagens que serão utilizadas para o desenvolvimento do trabalho.

Sistemas de Gestão de Identidade centralizam o controle de acesso aos recursos de um domínio (Hansen et al., 2008). As operações de autenticação, autorização, identificação e auditoria são administradas por um provedor de identidade (Identity Provider – IdP), responsável pela criação de uma relação de confiança entre usuários e serviços (Hansen et al., 2006).

Há situações, no entanto, em que um usuário ou dispositivo tem a necessidade de acessar recursos que não são provenientes de seu domínio. O processo de autenticação de um usuário que está fora de seu domínio de origem e precisa usar algum recurso em outro local pode acontecer de maneiras diferentes, como por exemplo, a recriação de credenciais no novo local. O problema com esta abordagem é a replicação dos bancos de dados e a necessidade de que o usuário memorize várias credenciais. O Gerenciamento de Identidade Federado aborda esse problema. Neste esquema, um dispositivo (D) tentando utilizar um serviço fornecido por um provedor de serviço (Service Provider – SP) fora do seu domínio, terá suas credenciais validadas pelo seu próprio IdP, tendo em vista uma relação de confiança entre o IdP e o SP. O processo de autenticação se dá através do uso e autenticação de uma identidade, uma vez que os SPs não retêm informações sobre D. Certificados, assinaturas e verificações são utilizados para garantir a identidade das entidades envolvidas.

Não temos problemas em utilizar criptossistemas em uma abordagem de gestão de identidades utilizando os recursos computacionais disponíveis nos computadores de hoje, que requerem uma utilização significativa de CPU, memória e disco. Problemas surgem ao tentarmos aplicar os mesmos mecanismos de criptografia a sistemas com recursos limitados, como os encontrados em IoT. Desenvolveremos o CoFee, uma solução para atender os requisitos de segurança, ao mesmo tempo em que mantém conformidade com as restrições de IoT. Nossa solução compreenderá os seguintes módulos.

Certificados Implícitos Qu-Vanstone: no esquema de certificados implícitos baseado em curvas elíptica de Qu-Vanstone (Brown et al., 2002), a chave pública de uma entidade é combinada com o certificado de forma a criar um elemento único, do qual a chave pública pode ser extraída sendo implicitamente verificada. Uma grande vantagem desse método reside no tamanho consideravelmente reduzido dos certificados implícitos, que os torna menores do que certificados tradicionais, o que torna o esquema muito interessante em cenários IoT.

Estudaremos a aplicabilidade de certificados implícitos para o gerenciamento de identidades federadas no CoFee, particularmente para conseguir uma autenticação mais eficiente em termos de recursos, reduzir os requisitos de armazenamento para certificados, além de economizar em largura de banda de rede e diminuir a latência no processo de autenticação. **Produto** : uma biblioteca de autenticação que usa certificados implícitos para dispositivos IoT (Android).

Hash Based Signatures: proposto por Merkle nos anos 70, os esquemas Hash-Based Signature (HBS) ganharam atenção na última década. Os HBSs usam apenas funções de hash criptográficas e, portanto, fornecem um *trade-off* entre eficiência e segurança a partir do qual a IoT pode se beneficiar (Rohde et al., 2008). Sua segurança depende da propriedade de resistência à colisão que a função hash escolhida oferece. Entre os esquemas HBS destacam-se, por exemplo, os esquemas de Lamport e Merkle (Lamport, 1979, Merkle, 1987). Vamos avaliar HBSs como uma forma de fornecer autenticação leve em nossa solução. **Produto**: Uma biblioteca de criptografia para assinaturas baseadas em hash em dispositivos IoT (Android).

Protocolo CoFee: Apresentaremos uma especificação formal do protocolo CoFee, cobrindo como dispositivos, SPs e IdPs trocam informações para permitir o gerenciamento seguro de identidades federadas. Nosso protocolo levará em conta as limitações dos dispositivos IoT. Apresentaremos uma solução que prioriza a redução da comunicação em dispositivos mais limitados em recursos e alimentados por baterias, com o objetivo de diminuir a largura de banda e o consumo de energia. A fim de verificar as garantias de segurança e de correção do protocolo, vamos usar ferramentas de verificação automática disponíveis na literatura, objetivando garantir a robustez do protocolo. **Produto**: Um relatório técnico com uma descrição formal do protocolo e sua verificação analítica.

Protótipo CoFee: implementaremos o protocolo CoFee para dispositivos IoT, utilizando as bibliotecas para certificados implícitos e assinaturas baseadas em hash. Implementaremos o protocolo CoFee em todas as entidades envolvidas no processo de autenticação: IdPs, SPs e dispositivos de usuários finais. Usaremos o protótipo para demonstrar situações inerentes a um esquema de gerenciamento de identidade federado para classes de dispositivos IoT. A figura 1 ilustra o funcionamento do protocolo e os dispositivos presentes no escopo do nosso protótipo. **Produto**: protótipo CoFee, abrangendo a implantação do SP, IdP e D.

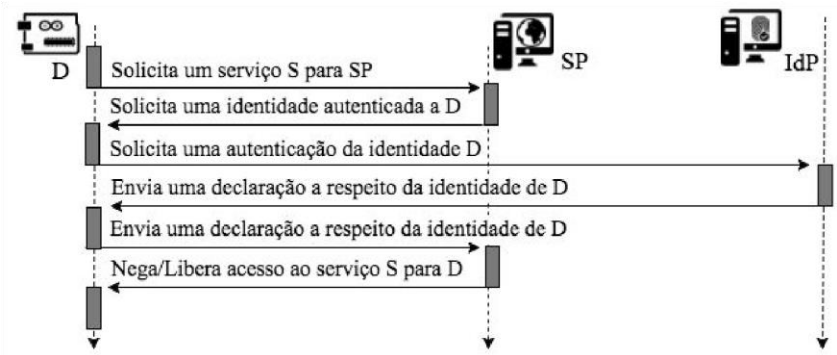

Figura 1: Etapas de comunicação e entidades na demonstração de protótipo.

8.3.1. Potencial de serviço para RNP

Uma das possíveis utilizações do protocolo CoFee é no controle de acesso a locais específicos dentro das universidades, assim como no provisionamento de recursos como alimentação em restaurantes universitários e livros em bibliotecas.

Um cenário de utilização do CoFee é apresentado na figura 2, onde temos 3 instituições, sendo que cada instituição possui seu próprio banco de dados, além também de praticar formas distintas de autenticação de seus alunos.

As instituições neste cenário representam IdPs, os SPs são representados por uma biblioteca, máquinas de vendas alocadas nas instituições e restaurantes universitários. Os alunos representam os utilizadores dos serviços ofertados.

Para que utilizem os recursos oferecidos pelos SPs os alunos devem se autenticar nos mesmos utilizando um dispositivo IoT, tendo em vista uma prévia aquisição de créditos. É interessante para as empresas de máquinas de vendas e do restaurante armazenar informações dos créditos referentes as credenciais dos utilizadores, prazos, hora de compras etc. Por outro lado, não é desejável nem seguro que as instituições forneçam outras informações senão as necessárias para que as empresas provedoras de serviço disponibilizam seus serviços.

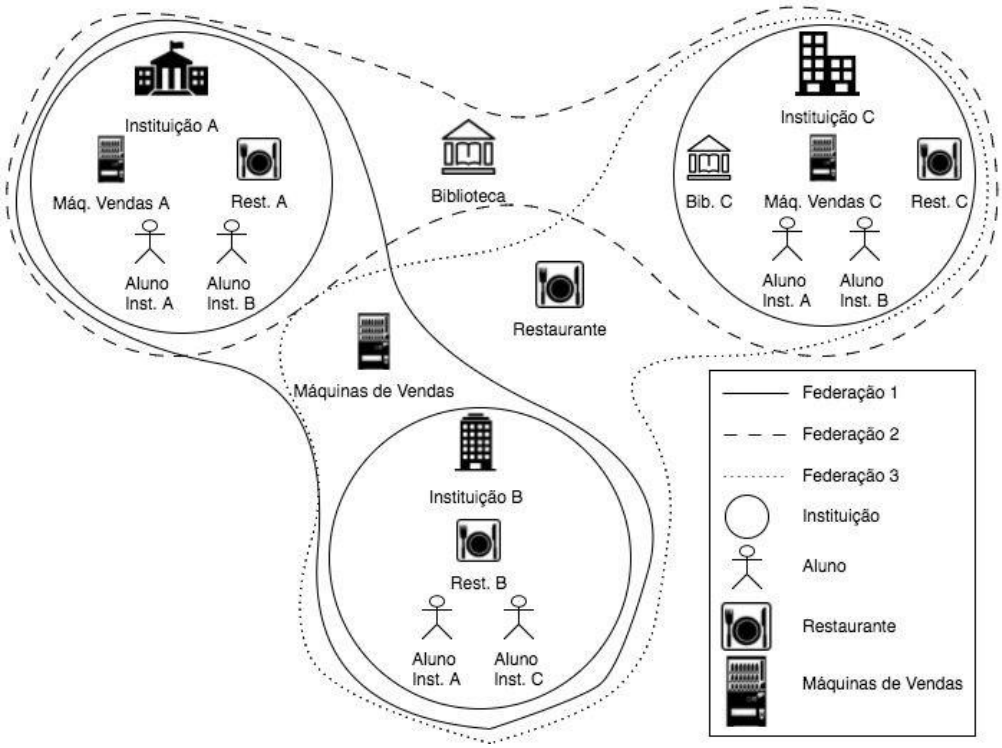

Figura 2: Cenário de utilização do CoFee

Na figura 2, temos uma linha contínua que indica que as instituições A e B pertencem a uma federação em conjunto com a empresa de máquinas de vendas. Alunos da instituição A podem adquirir produtos nas máquinas da instituição B e vice-versa, uma vez que a empresa de máquinas de vendas confia nas credenciais tanto da instituição A quanto nas da instituição B. A federação representada pela linha serrilhada indica que tanto alunos da instituição A quanto da instituição C podem utilizar os serviços da biblioteca. E por fim, a linha pontilhada indica que nesta federação os alunos das instituições B e C podem utilizar tanto as máquinas de vendas quanto os restaurantes umas das outras. Na figura 2 temos representados do lado externo dos círculos os serviços providos, e do lado interno temos uma instância daquele serviço provido.

A utilização de identidades federadas possibilita a autenticação de forma segura de credenciais não pertencentes à instituição, uma vez estando definida uma relação de confiança entre as partes envolvidas. O protocolo CoFee difere da CAFe devido a utilização de criptossistemas leves e adequados ao contexto de IoT, aplicados a dispositivos autômatos, que não requerem a interação de um usuário.

9. Recursos financeiros

9.1. Equipamentos e softwares

Para o desenvolvimento do protótipo, serão necessários um notebook e um dispositivo IoT por estagiário/assistente, que serão utilizados no desenvolvimento propriamente dito e na representação das entidades envolvidas no processo de comunicação do CoFee.

Descrição	**Quantidade**
Notebook 14" (Core i7 - 8GB - 500GB)	3
Dispositivo IoT Android	3

Coordenador geral: concepção da solução e coordenação das atividades desenvolvidas pelos demais membros da equipe.

Coordenador adjunto: concepção da solução e auxílio do coordenador geral das atividades desenvolvidas pelos demais membros da equipe.

Assistente 1: atuará desde a concepção e projeto da solução, bem como nas atividades para a implementação de criptossistemas. Realizará os testes e avaliações de protocolos criptográficos em diferentes plataformas / ambientes.

Estagiário #1: auxiliará o assistente 1 no desenvolvimento e testes das soluções propostas, e com a colaboração e supervisão dos outros participantes do projeto, realizará testes e avaliações.

Estagiário #2: atuará sob a supervisão do coordenador adjunto, colaborando no desenvolvimento e concepção das soluções propostas.

9.3. Viagens

Origem	**Destino**	**Membro**	**Data**
Campinas - SP	Belo Horizonte - MG	Estagiário #2	08/05/2017
Campinas - SP	Belo Horizonte - MG	Coord. adjunto	27/10/2017
Belo Horizonte	Campinas - SP	Coord. Geral	01/02/2018
Belo Horizonte	Campinas - SP	Assistente 1	01/02/2018

O objetivo das viagens é realizar alinhamentos do projeto com a Unicamp na qualidade de instituição parceira.

10. Ambiente para testes do protótipo

Será verificada a possibilidade de utilização do GIdLab da RNP, tendo em vista que algumas modificações deveriam ser aplicadas para a utilização deste ambiente. Outra opção que será levada em conta é a utilização dos recursos de IoT disponíveis no projeto GT-TeI[2] (Grupo de Trabalho - Testbed para Espaços Inteligentes) ambiente de experimentação físico (testbed) financiado pela RNP.

O ambiente de testes será composto por servidores existentes na UFMG para simular provedores de serviços e provedores de identidade, os dispositivos serão simulados utilizando os Dispositivos IoT solicitados nesta proposta.

11. Referências

[Atzori et al. 2010] Atzori, L., Iera, A., and Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15):2787–2805.

[Boneh and Franklin 2001] Boneh, D. and Franklin, M. (2001). Identity-based encryption from the weil pairing. In CRYPTO, pages 213–229. Springer.

[Buchmann et al. 2009] Buchmann, J., Dahmen, E., and Szydlo, M. (2009). Hash-based digital signature schemes. In Post-Quantum Cryptography, pages 35–93. Springer.

[Brown et al. 2002] Brown, D. R. L., Gallant, R. P., and Vanstone, S. A. (2002). Provably secure implicit certificate schemes. In: International Conference on Financial Cryptography. Springer Berlin Heidelberg, 2001. p. 156-165.

[Hansen et al. 2006] Hansen, M., Berlich, P., Camenisch, J., Clauß, S., Pfitzmann, A., and Waidner, M. (2006). Privacy-enhancing identity management. Information Security Technical Report, 11(3):119 – 128.

[Hansen et al. 2008] Hansen, M., Pfitzmann, A., and Steinbrecher, S. (2008). Identity manage- ment throughout one's whole life. Information Security Technical Report, 13(2):83 – 94.

[Horrow and Sardana 2012] Horrow, S.and Sardana, A.(2012). Identity management framework for cloud based internet of things. In SECURIT, pages 200–203.

[Karlof and Wagner. 2003] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1(2–3):293–315, 2003.

[Merkle. 1987] Merkle, Ralph C. A digital signature based on a conventional encryption function. Conference on the Theory and Application of Cryptographic Techniques. Springer Berlin Heidelberg, 1987.

[Lamport. 1979]. Lamport, leslie. Constructing digital signatures from a one-way function. Vol. 238. Palo Alto: Technical Report CSL-98, SRI International, 1979. [Stinson. 2002]. Stinson, Douglas. Cryptography: Theory and Practice. CRC/C&H,
2002.

[Torres et al. 2013] Torres, J., Nogueira, M., and Pujolle, G. (2013). A survey on identity management for the future network. *Communications Surveys Tutorials, IEEE*, 15(2):787–802.

[Wangham et al. 2010] Wangham, M. S., de Mello, E. R., da Silva Böger, D., Guerios, M., and da Silva Fraga, J. (2010). Gerenciamento de identidades federadas. *SBSeg*.

[2] https://ceunaterra.ufg.fibre.org.br/Site/sobre_projeto.html