UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Hendri Nogueira

APRIMORAMENTO DA PRIVACIDADE EM INFRAESTRUTURAS DE CHAVES PÚBLICAS CENTRADAS NO USUÁRIO E BASEADAS EM NOTÁRIOS

Florianópolis(SC)

2014

Hendri Nogueira

APRIMORAMENTO DA PRIVACIDADE EM INFRAESTRUTURAS DE CHAVES PÚBLICAS CENTRADAS NO USUÁRIO E BASEADAS EM NOTÁRIOS

Dissertação submetida ao Programa de Pós-Graduação em Ciência da Computação para a obtenção do Grau de Mestre em Ciência da Computação.
Orientador: Prof. Ricardo Felipe Custódio, Dr.
Universidade Federal de Santa Catarina

Florianópolis(SC)

2014

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

Nogueira, Hendri
Aprimoramento da Privacidade em Infraestruturas de Chaves Públicas Centradas no Usuário e Baseadas em Notários / Hendri Nogueira ; orientador, Ricardo Felipe Custódio - Florianópolis, SC, 2014.
115 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro Tecnológico. Programa de Pós-Graduação em Ciência da Computação.

Inclui referências

1. Ciência da Computação. 2. Infraestrutura de Chaves Públicas. 3. Infraestrutura de Autenticação e Autorização. 4. Gestão de Identidades. 5. Segurança da Informação. I. Custódio, Ricardo Felipe. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Computação. III. Título.

Hendri Nogueira

APRIMORAMENTO DA PRIVACIDADE EM INFRAESTRUTURAS DE CHAVES PÚBLICAS CENTRADAS NO USUÁRIO E BASEADAS EM NOTÁRIOS

Esta Dissertação foi julgada aprovada para a obtenção do Título de "Mestre em Ciência da Computação", e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Florianópolis(SC), 21 de fevereiro 2014.

Prof. Ronaldo dos Santos Mello, Dr.
Coordenador do Curso

Banca Examinadora:

Prof. Ricardo Felipe Custódio, Dr.
Universidade Federal de Santa Catarina
Orientador

Prof. Ricardo Alexandre Reinaldo de Moraes, Dr.
Universidade Federal de Santa Catarina
Presidente

Prof. Marco Aurélio Amaral Henriques, Dr.
Universidade Estadual de Campinas

Prof.ª Carla Merkle Westphall, Dr.ª
Universidade Federal de Santa Catarina

Prof.ª Michelle Silva Wangham, Dr.ª
Universidade do Vale do Itajaí

Dedico este trabalho aos meus pais pelo apoio para levantarmos nossos próprios voos, mas sempre por perto caso precisemos de um empurrãozinho. Aos meus irmãos, por serem meus irmãos, e à minha namorada, companheira de todos esses dias e compreendendo nas passagens dos desafios.

AGRADECIMENTOS

Agradeço ao Professor Ricardo Felipe Custódio, pelo suporte durante esses anos da realização deste trabalho. Agradeço também ao Professor Jean Everson Martina pelos diversos momentos de conversas, ideias e dicas nas melhorias das pesquisas e dos trabalhos realizados. Aos amigos e colegas do LabSEC pelo convívio do dia-a-dia, incentivando ou colaborando no aprendizado durante este período.

Agradeço à Rede Nacional de Ensino e Pesquisa (RNP) e ao Instituto de Tecnologia a Informação (ITI), pela oportunidade em participar de alguns projetos, aprendendo e discutindo sobre os assuntos correlatos durante a elaboração deste trabalho.

“A sabedoria consiste em compreender que o tempo dedicado ao trabalho nunca é perdido.”
(Ralph Emerson)

RESUMO

Este trabalho tem como objetivo propor novas alternativas de Infraestrutura de Chaves Públicas (ICP) para prover um melhor gerenciamento das identidades, dos atributos e da privacidade dos usuários finais no âmbito de uma Infraestrutura de Autenticação e Autorização (IAA). Neste trabalho são descritas três alternativas: ICP Baseada em Atributos, ICP Centrada no Usuário e ICP Centrada no Usuário com Autenticação Anônima. A partir de uma visão crítica apresentada ao modelo de uma ICP X.509 e também com o uso de certificados de atributos, foram levantadas as limitações de suas adoções e utilizações, bem como a falta de suporte e o fornecimento na privacidade do usuário. Baseadas em Autoridades Notariais para fornecer a confiabilidade dos dados, as propostas utilizam-se do paradigma centrado no usuário para prover um maior controle para o usuário gerenciar e apresentar seus atributos, facilitando nos procedimentos de emissão e verificação das credenciais. As principais diferenças entre as propostas estão no fornecimento de diferentes níveis de privacidade para o usuário final e por meio da utilização de diferentes mecanismos criptográficos, tais como a Criptografia Baseada em Identidades (CBI) e provas de autenticação *zero-knowledge*. As propostas são analisadas e comparadas entre si e entre cinco outros sistemas, protocolos ou tecnologias utilizadas em uma IAA: ICP X.509 com certificados de atributos, OpenID, *framework* Shibboleth, U-Prove e Idemix. As suas escolhas se dão pela ampla utilização ou pelos resultados de projetos e pesquisas no meio acadêmico e privado, destacando ou não na privacidade do usuário. Mostra-se que as alternativas de ICP permitem uma simplificação na emissão de credenciais com chaves criptográficas, na verificação destas credenciais, no suporte à diferentes níveis de privacidade para o usuário, com uma alternativa em definir um justo modelo de negócio e a possibilidade de utilização em procedimentos de assinatura de documentos eletrônicos.

Palavras-chave: Infraestrutura de Chaves Públicas, Autoridade Notarial, Centrado no Usuário, Gestão de Identidades, Atributos, Privacidade, Criptografia Baseada em Identidades

ABSTRACT

This work aims to propose new alternatives for Public Key Infrastructure (PKI) to improve the management of identities, attributes and privacy of end users within an Authentication and Authorization Infrastructure (AAI). In this work three alternatives are described: PKI Based on Attributes, User-Centric PKI and User-Centric PKI with Anonymous Authentication. From a critical view introduced to the X.509 PKI model and also with the use of attributes certificates, was raised the limitations of their adoption and uses, as well as the lack of the support and the supply of the user's privacy. Based on Notary Authorities to provide data reliability, the proposed alternatives use of user-centric paradigm to provide more control for the user to manage and to present their attributes, making it easier procedures for issuing and verificating credentials. The main differences between the proposals are in providing different levels of end-user's privacy and through the use of different cryptographic mechanisms, such as Identity-Based Cryptography (IBC) and zero-knowledge authentication proofs. The proposals are analyzed and compared with each other and with five other systems, protocols or technologies used in an IAA: X.509 PKI with attribute certificates, OpenID, Shibboleth framework, U-Prove and Idemix. The choices are given by the widespread use or the results from academic and private's research and projects, focusing or not on user's privacy. It is shown that the PKI's alternatives allow a simplification in the issuance of credentials with cryptographic keys, the verification of that credentials, in supporting different levels of user's privacy, an alternative to defining a fair business model and the possibility of using in procedures for signing electronic documents.

Keywords: Public Key Infrastructure, Notarial Authority, User-Centric, Identity Management, Attributes, Privacy, Identity-Based Cryptografy

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABC4Trust	*Attribute-based Credentials for Trust*
ABPKI	*Attribute Based Public Key Infrastructure*
AC	Autoridades Certificadoras
AN	Autoridade Notarial
AP-PZK	Atributos Públicos do Protocolo de *Zero-Knowledge*
APA	Autoridade Provedora de Atributo
APr-PZK	Atributos Privados do Protocolo de *Zero-Knowledge*
AR	Autoridade de Registro
CA	Certificado de Atributo
CBI	Criptografia Baseada em Identidade
CMP	Chave Mestra Pública
CMS	Chave Mestra Secreta
CP	Chave Pública
CPF	Cadastro de Pessoas Físicas
CPr	Chave Privada
CREA	Conselho Regional Engenharia Arquitetura e Agronomia
GCP	Gerador de Chaves Privadas
GId	Gestão de Identidades
IAA	Infraestrutura de Autenticação e Autorização
ICP	Infraestrutura de Chave Pública
ICSNC	*International Conference on Systems and Networks Communications*
Id	Identificador
IGP	Infraestrutura de Gerenciamento de Privilégios
IJCSIS	*International Journal of Computer Science and Information Security*
LCR	Lista de Certificados Revogados
OCSP	*On-line Certificate Status Protocol*
OECD	*Organisation for Economic Co-operation and Development*
OID	*Object Identifier*
OTP	*One Time Password*

PId Provedor de Identidades

PIS Programa de Integração Social

PKC *Public Key Certificate*

PKI *Public Key Infrastructure*

PMI *Privilege Management Infrastructure*

PRIME *Privacy and Identity Management for Europe*

PS Provedor de Serviços

SAML *Security Assertion Markup Language*

SBSeg Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais

SSO *Single Sign-On*

TLS *Transport Layer Security*

TSL *Trust-service Status List*

UCPKI-AA *User-Centric Public Key Infrastructure with Anonymous Authentication*

UCPKI *User-Centric Public Key Infrastructure*

URI *Uniform Resource Identifier*

VA Validação de Atributos

WGID Workshop de Gestão de Identidades

XML *Extensible Markup Language*

SUMÁRIO

1 INTRODUÇÃO

Os serviços eletrônicos providos por meio da Internet tem facilitado a vida de grande parte da população, e alguns se tornaram indispensáveis, tais como alguns dos serviços oferecidos pelo governo de um país. Tais serviços são cada vez mais elaborados e sofisticados. Muitos estão sendo providos a partir do conceito de nuvem computacional, o que tem facilitado tanto para o usuário final quanto para o desenvolvedor de aplicações. Uma das facilidades consiste na disponibilidade desses serviços a partir de qualquer equipamento conectado à Internet para o usuário final. Já para o desenvolvedor está na disponibilidade de ferramentas de desenvolvimento, componentes de software reutilizáveis, recursos de processamento e de memória abundantes e a redução dos custos. Indiferente por qual meio os serviços são viabilizados, por exemplo, serviços web (via utilização de navegadores) e não-web (via aplicativos *desktops* ou móveis), o gerenciamento dos usuários, dos dados e dos demais recursos ofertados são indispensáveis.

Tais serviços são disponibilizados e gerenciados pelos chamados Provedores de Serviços (PSs) e definem as políticas de utilização de seus serviços. Dentre os serviços ofertados, alguns podem requerer procedimentos de autenticação e autorização dos usuários. A autenticação do usuário perante um serviço tem como objetivo a identificação de quem está requisitando o acesso e a associação de suas ações. Os procedimentos de autorização determinam as permissões e as condições que um determinado serviço pode ser acessado. Normalmente, o responsável pelo serviço (administrador do sistema) é quem gerencia as permissões dos usuários. Entretanto, em larga escala, diante de muitos provedores de serviços, é indispensável a gestão cuidadosa e compartilhada dos dados de identificação e autorização. E para isso, é necessário criar uma infraestrutura adequada. Existem padrões, protocolos e sistemas para auxiliar na criação de uma Infraestrutura de Autenticação e Autorização (IAA) (WINDLEY, 2005; BERTINO et al., 2010).

Dentre os diversos métodos e tecnologias para realizar a autenticação de uma entidade, p. ex., *username* e senha, *token* (segredo compartilhado), certificação digital e biometria, cada um diferencia-se pelo fornecimento do nível de segurança para a IAA e para as entidades envolvidas. Consequentemente, existem diferenciações dos custos computacionais e econômicos envolvidos, na usabilidade e privacidade dos dados. Uma IAA também pode fornecer uma série de padrões de segurança, tais como procedimentos de auditoria das atividades do usuário (*logging*).

Um dos métodos mais utilizados para realizar a autenticação é por meio do registro de um identificador único (p. ex., *username*, e-mail) do

usuário e uma senha. O registro normalmente é realizado localmente no PS e algumas informações adicionais podem ser requeridas, como por exemplo, nome, sobrenome, data de nascimento, endereço de e-mail, entre outras. Este método se destaca pela simplicidade e o baixo custo exigido. Entretanto, o excesso de registros, de *usernames* e senhas, a autenticidade dos atributos informados pelos usuários e a necessidade do PS manter o gerenciamento com segurança destes dados são os principais pontos negativos.

A confiabilidade dos dados sobre o usuário e o método de autenticação utilizado são fatores importantes tanto para o PS quanto para o usuário. A obtenção dos dados, também conhecidos como atributos, deve garantir a sua veracidade para evitar alguns problemas de segurança. O PS deve, por exemplo, saber se a idade do usuário é autêntica para ceder ou negar um recurso com restrição à menores de idade. A autenticação do usuário deve ser segura o suficiente para que pessoas mal-intencionadas não roubem os dados de autenticação e não consigam se autenticar em nome da vítima. O acesso não autorizado ou o roubo dos dados afetam toda a infraestrutura e as entidades envolvidas.

Os sistemas que utilizam a criptografia assimétrica com o uso de certificados digitais, como os certificados de chave pública X.509 (COOPER et al., 2008), permitem a associação entre um par de chaves e um conjunto de atributos sobre o seu titular. As autenticidades dos dados contidos, do par de chaves, bem como o ciclo de vida dos certificados, são gerenciadas pelas Autoridades Certificadoras (ACs) pertencentes à um Infraestrutura de Chaves Públicas (ICP). O ponto de confiança das autoridades e da ICP é fornecida pela Autoridade Certificadora Raiz (AC-Raiz). Este tipo de certificado digital permite auxiliar e prover uma autenticação "forte" de seu titular e também procedimentos de assinatura digital (DIFFIE; HELLMAN, 1976). A Figura 1 ilustra o esquema da uma ICP e o certificado digital emitido para o usuário final.

A força provida na autenticação é determinada pelas premissas criptográficas que permitem provar matematicamente a posse da chave privada correspondente da chave pública apresentada. Por outro lado, estes certificados não são recomendados em conter dados para a realização de procedimentos de autorização, pois podem possuir um tempo de vida menor do que os de autenticação. Uma das consequências, caso a recomendação não seja aplicada, seria o excesso de revogação dos certificados e o aumento de custos para o usuário final. Para evitar tais revogações e dar mais dinamismo no uso da certificação digital, surgiu o Certificado de Atributo X.509 (CA) (FARRELL; HOUSLEY; TURNER, 2010).

O CA é um tipo especial de certificado digital e seu objetivo é ser aplicado em procedimentos de controle de acesso ou funções de delegações. Sua

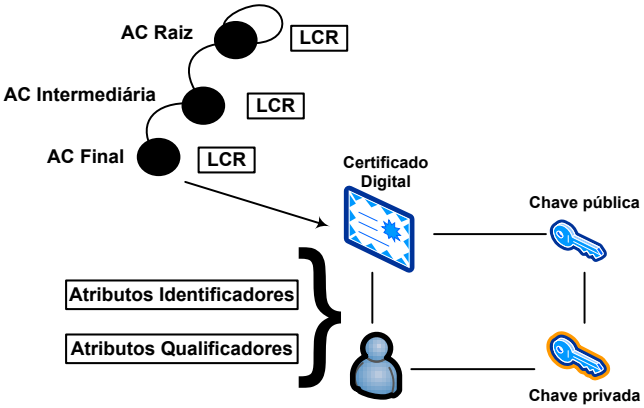


Figura 1 – Esquema de uma ICP X.509.

estrutura foi implementada para ser mais simples do que os certificados de chave pública e os CAs devem ser emitidos por autoridades específicas e responsáveis por gerenciar um determinado atributo, as Autoridades Provedoras de Atributos (APAs). O gerenciamento do ciclo de vida do CA é realizado por uma Infraestrutura de Gerenciamento de Privilégios (IGP) (ETSI, 2002; UNION, 2008). A Figura 2 demonstra o esquema de uma IGP baseada em certificado de atributos.

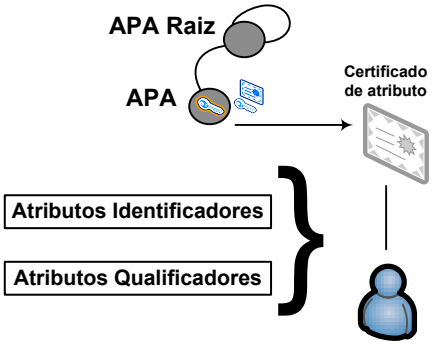


Figura 2 – Esquema de uma IGP baseada em CA.

Tanto uma ICP quanto uma IGP podem ser aplicadas separadamente uma da outra. Contudo, uma IGP pode ser implementada em conjunto com uma ICP para emitir certificados de atributos associados ao certificado de

chave pública do mesmo titular. A Figura 3 exemplifica um caso de uso onde o usuário possui um certificado digital emitido por uma ICP e diferentes certificados de atributos emitidos por diferentes entidades.

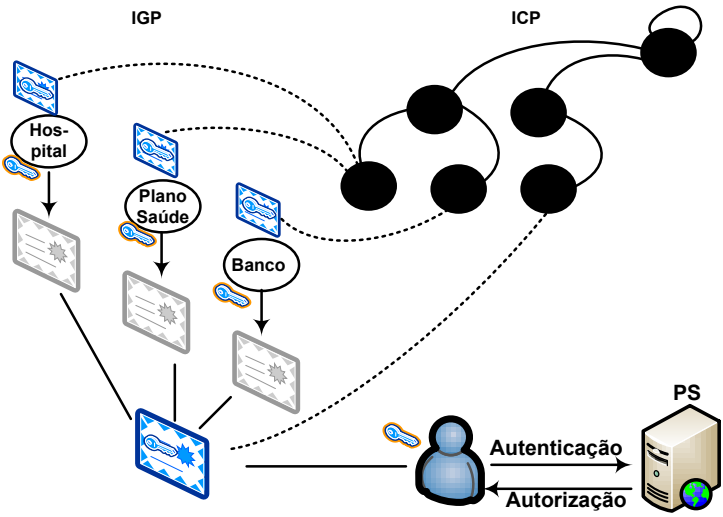


Figura 3 – Exemplo da arquitetura de uma ICP e IGP em conjunto.

Apesar de uma IAA baseada em certificação digital apresentar muitos benefícios, as ICPs são fortemente criticadas pela complexidade necessária para serem implementadas e gerenciadas (GUTMANN, 2002; LIOY et al., 2006; ADAMS; JUST, 2004; ELLISON; SCHNEIER, 2000). Adicionalmente a quantidade de procedimentos necessários para emitir, revogar, verificar e manter a segurança dos certificados deixam dúvidas quanto aos benefícios (p. ex., mão de obra qualificada e confiável, ambiente altamente seguro, necessidade de acesso à Internet). Apesar de uma IGP baseada em certificado de atributos ter sido especificada para ser mais simples do que uma ICP, a associação de uma CA com um certificado digital herda os mesmos desafios de complexidade exigida no uso de um certificado digital.

Outra desvantagem do certificado de chave pública é a impossibilidade de se alterar qualquer um dos seus atributos. Os atributos destes certificados são determinados e inclusos por uma autoridade certificadora final. Uma vez que o certificado é emitido, caso algum atributo tenha a necessidade de ser alterado, deve-se revogar o certificado e emitir um novo. Infelizmente, a revogação e a emissão de um novo certificado não é uma tarefa simples. Algumas autoridades certificadoras requerem a presença física do usuário para que um

novo certificado seja emitido. Além disso, o titular do certificado não tem qualquer controle sobre os seus atributos. Ele não pode, por exemplo, escolher quais atributos podem ser contidos no certificado. Como consequência, todos os atributos de um certificado serão públicos e visíveis.

A verificação de um certificado deve ser realizada com atenção e em alguns casos exige uma maior complexidade (BERBECARU; LIOY; MARIAN, 2001). A arquitetura e a implementação de uma ICP de forma hierárquica (amplamente utilizada), como no caso da ICP-Brasil (BRASIL, 2001), possui a consequência de alongar o procedimento da verificação de um certificado do usuário final. O caminho de certificação do certificado final, i.e., o conjunto de certificados das autoridades certificadoras que participaram para que o certificado final fosse emitido, deve ser determinado para verificar a autenticidade dos dados do certificado. Em outras palavras, a verificação de um certificado do usuário final necessita que os certificados das autoridades certificadoras participantes (autoridades certificadora raiz, intermediária e final) também sejam verificados. Estes procedimentos podem ter um elevado custo computacional, no canal de comunicação e nos recursos de armazenamento quando requisitado.

Dentro do processo de verificação de um certificado, deve-se analisar o seu estado de revogação, i.e., se foi revogado ou não. Dois dos métodos mais utilizados para gerenciar a revogação dos certificados emitidos são: Lista de Certificados Revogados (LCR) (COOPER et al., 2008) e *On-line Certificate Status Protocol* (OCSP) (MYERS et al., 1999). A obtenção do estado de revogação de um certificado é realizada online e sua atualização é definida de acordo com as políticas das autoridades certificadoras. Portanto, a verificação da validade de um certificado digital é realizada analisando todos os certificados digitais da cadeia de certificação, até um ponto de confiança de quem está verificando. Normalmente, o ponto de confiança é o certificado da autoridade certificadora raiz da cadeia de certificação. Em particular, cada certificado deve ser verificado quanto a sua integridade e autenticidade, além do respeito às políticas de certificação impostas pela ICP em questão.

A certificação digital pode ser tanto usada para autenticação quanto para assinatura digital. Uma assinatura digital necessita de um conjunto maior de artefatos digitais, como os carimbos do tempo (ou *timestamps*). A assinatura também deve ser mantida em longo prazo, o que implica na adição de novos carimbos do tempo de forma periódica. Assim, sua complexidade computacional, temporal e de armazenamento é diretamente proporcional com o prazo para manter a assinatura válida. Alguns trabalhos visam propor alternativas e soluções para melhorar a complexidade requerida para assinaturas de documentos (MOECKE et al., 2010; VIGIL, 2010; CUSTóDIO; VIGIL, 2012).

Acredita-se que grande parte da complexidade contida no uso da certificação digital possa ser eliminada se os atributos contidos forem melhor conduzidos por seus titulares e a arquitetura da ICP for simplificada com a eliminação da estrutura hierárquica. O controle dos atributos contidos nos certificados pelos próprios titulares também incrementaria a privacidade sobre seus dados (CLAYCOMB; SHIN; HARELAND, 2007; HANSEN; PFITZMANN; STEINBRECHER, 2008; AHN; KO; SHEHAB, 2009; BRAMHALL et al., 2007). A privacidade do usuário é um requisito não aprofundado em IAA baseado em certificação digital, pois os certificados não fornecem mecanismos para preservar a privacidade dos dados e a identificação do usuário.

Considerando a estrutura hierárquica de uma ICP, caso a mesma fosse modificada para determinar a responsabilidade da certificação dos dados dos usuários finais em apenas um tipo de autoridade, o caminho de certificação seria eliminado assim como a diminuição dos procedimentos de verificação do certificado (MOECKE, 2011; VIGIL et al., 2012).

O presente trabalho apresenta uma nova arquitetura de ICP que melhore o gerenciamento dos atributos dos usuários finais, suportando um dinamismo para a emissão dos certificados dos usuários, e permitindo que o usuário possua um maior controle sobre seus atributos a serem apresentados. Os certificados emitidos por esta nova ICP poderão ser utilizados para procedimentos de autenticação, autorização e também para assinaturas de documentos eletrônicos. Os certificados são auto-assinados pelos usuários e eles incluem os atributos que desejam ser apresentados. A validação dos dados dentro dos certificados é realizada pelas Autoridades Notariais (ANs) e não pelas autoridades certificadoras. Cada tipo de atributo nos certificados é gerenciado pela autoridade provedora de atributo e a AN se comunica com a respectiva APA para confirmar os valores dos atributos apresentados pelos usuários.

No decorrer de todo o trabalho, foram modelados e descritos três alternativas de infraestrutura de chaves públicas. A primeira é a base para as outras duas e é denominado de Infraestrutura de Chaves Públicas Baseada em Atributos, cuja sigla é ABPKI da tradução em inglês “Attribute-Based Public Key Infrastructure” (NOGUEIRA; MARTINA; CUSTóDIO, 2013). O esquema geral da comunicação envolvida na ABPKI pode ser visualizado pela Figura 4. A privacidade não é seu objetivo, entretanto é fornecida pelo aumento do controle de quais atributos o usuário deseja torná-los públicos. Não sendo o bastante, este trabalho aprimora a privacidade do usuário modelando outras duas arquiteturas de ICP, modificando principalmente a estrutura do certificado do usuário e os procedimentos exigidos para a validação e verificação do mesmo.

A segunda alternativa vem do modelo *User-Centric Public Key Infras-*

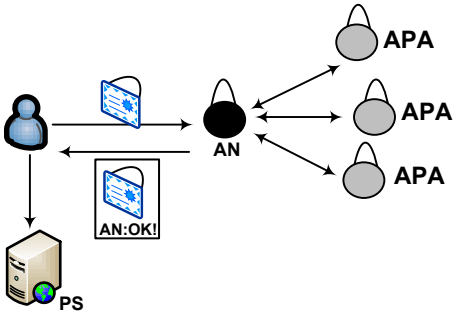


Figura 4 – Esquema de comunicação da arquitetura geral da ABPKI.

tructure based on notaries (UCPKI), cuja tradução é Infraestrutura de Chaves Públicas Centrada no Usuário e baseada em notários (NOGUEIRA; SOUZA; CUSTóDIO, 2013). Sua principal mudança ocorre para prover a privacidade na autenticação do usuário com o provedor de serviço que deseja acessar. Esta autenticação é realizada pelo uso de *nonces* e permite a não identificação do usuário pelo seu real nome ou sua chave pública. O modelo utiliza o conceito de Criptografia Baseada em Identidade (CBI) (SHAMIR, 1985) para suportar o uso de diferentes pares de chaves derivadas a partir de um par de chaves mestras. Este mecanismo e a adição do sigilo nos identificadores dificulta na associação de diferentes certificados para uma mesma chave pública.

Por fim, a terceira alternativa utiliza protocolos de provas *zero-knowledge* para prover uma autenticação anônima do usuário para substituir a utilização de *nonces*. Este modelo possui a base da UCPKI para aprimorar a privacidade fornecida para o usuário final. O modelo recebeu o nome de Infraestrutura de Chaves Públicas Centrada no Usuário com Autenticação Anônima ou do inglês *User-Centric Public Key Infrastructure with Anonimous Authentication* (UCPKI-AA). Além de poder utilizar o certificado com qualquer provedor de serviço e eliminar a possibilidade da AN reconhecer em qual PS o usuário irá acessar, a UCPKI-AA aplica a criptografia nos atributos dentro dos certificado para torná-los sigilosos. Deste modo, apenas as APAs responsáveis poderão visualizar os valores de seus respectivos atributos responsabilizados.

1.1 MOTIVAÇÃO

As abordagens apresentadas neste trabalho tem como motivação a busca de melhorias no gerenciamento de atributos dos usuários finais em in-

fraestrutura de chaves públicas e a utilização de mecanismos para aprimorar a privacidade dos dados nos certificados. Ao emitir e usar um certificado digital para procedimentos de autenticação, autorização e assinatura de documentos eletrônicos, o usuário deve possuir mais controle para decidir quais atributos serão apresentados em cada situação. Adicionalmente, a estrutura das novas ICPs e os procedimentos de revogação dos certificados não devem repetir os mesmos problemas apresentados em uma ICP X.509.

1.2 HIPÓTESES

O gerenciamento dos atributos pode ser melhorado se esta responsabilidade for apenas das autoridades responsáveis específicas. Estas autoridades são provedoras de atributos e mantém o armazenamento e o gerenciamento seguro dos atributos. Os valores dos atributos devem estar sempre atualizados e corretamente associados com os seus titulares. A eliminação do caminho de certificação existente em uma ICP X.509 diminui a complexidade na emissão e verificação de um certificado do usuário final. As autoridades certificadoras podem ser substituídas por autoridades notariais, diante do seu poder de notarização, em que valida a integridade e a autenticidade dos certificados auto-assinados dos usuários e os atributos contidos. A confiança das autoridades do domínio são definidas pelas Listas de Estados de Serviços Confiáveis (ETSI, 2009).

O aprimoramento da privacidade do usuário pode ser obtido nos dados contidos no certificado, no identificador (chave pública) e na autenticação com o provedor de serviço. O primeiro é realizado pela capacidade do usuário em escolher quais atributos ele inclui no certificado, na possibilidade dos atributos estarem sigilosos para serem visualizadas apenas pelas autoridades provedoras de atributos. O aumento da posse da quantidade de pares de chaves para o usuário emitir diferentes certificados associados a diferentes chaves públicas permite o uso variado de pseudônimos, aprimorando a privacidade na identificação. Já a autenticação do usuário com os provedores de serviços deve ser realizada de forma anônima para que o mesmo não seja identificado e associado (por terceiros) às suas ações realizadas.

1.3 OBJETIVOS

Propor, modelar e descrever alternativas de abordagens de Infraestrutura de Chaves Públicas para melhorar no gerenciamento dos atributos dos usuários finais e na privacidade. As arquiteturas de ICP devem fornecer di-

ferentes níveis de privacidade sobre o usuário final e os certificados devem conter apenas atributos escolhidos pelos seus titulares.

1.3.1 Objetivos Específicos

Os objetivos específicos deste trabalho são:

- Verificar se existem alternativas à ICP para o gerenciamento de atributos;
- Propor o uso de métodos e mecanismos para fornecer maior privacidade sobre os atributos, a identificação e a autenticação dos usuários por meio dos certificados apresentados para os provedores de serviços;
- Avaliar os modelos propostos quanto a confiabilidade dos dados providos e o aprimoramento da privacidade;
- Analisar e comparar as alternativas com os sistemas e esquemas já existentes na literatura.

1.4 METODOLOGIA

Para alcançar os objetivos deste trabalho, iniciou-se com o estudo de artigos, dissertações, normas e relatórios técnicos relacionados com: a) ICP e suas dificuldades; b) dificuldades na manutenção de documentos assinados; c) gerenciamento de atributos em ICP; d) certificados de atributos; e) gestão de identidades; f) infraestruturas de autenticação e autorização; g) privacidade e seus conceitos. Após observar as principais características de um sistema que compõe uma IAA, foram traçadas as limitações e dificuldades contidas em uma ICP X.509 e também com o uso de certificados de atributos.

A partir dos estudos, foi modelada a primeira abordagem de solução, o modelo Infraestrutura de Chaves Públicas Baseada em Atributos. Em seguida, e com foco no aprimoramento da privacidade do usuário, foram propostas mais duas alternativas proporcionando diferentes níveis de privacidade. Cada nova abordagem utiliza diferentes mecanismos e tecnologias para proporcionar o sigilo dos dados e para impor uma autenticação anônima do usuário.

Cada alternativa proposta foi modelada e descrita contendo cada estrutura de dados criada, cada comunicação e procedimentos envolvidos para a emissão do certificado, a validação perante uma AN e a sua utilização para

requisitar um recurso em um provedor de serviço. Por fim, as três abordagens de soluções foram comparadas e analisadas descritivamente entre si e perante o uso de certificados de uma ICP X.509 e certificados de atributos. As análises se baseiam nas características da complexidade computacional exigidas, na quantidade mínima de procedimentos criptográficos realizada, na complexidade de implementação quanto ao custos diretos (p. ex. pessoas, infraestrutura, ambiente) para a implementação da arquitetura e para o usuário final. Complementando as análises, os modelos foram comparados em relação ao nível de privacidade que cada um fornece para os usuários.

Uma segunda parte da análise foi realizada para comparar as características da privacidade fornecida. Esta etapa se baseou na proposta que forneceu o melhor nível de privacidade do usuário, em dois sistemas e esquemas amplamente utilizados em IAA (OpenID e Shibboleth) e dois sistemas projetados para prover melhorias de privacidade por meio de credenciais anônimas (U-Prove e Idemix).

1.5 LIMITAÇÕES DO TRABALHO

A complexidade computacional e a usabilidade para o usuário são os principais limitadores deste trabalho por estarem diretamente proporcional com o nível de privacidade fornecido pelos modelos. A quantidade de procedimentos criptográficos utilizados nos modelos UCPKI e UCPKI-AA tornam-os limitados em algumas situações, pois podem necessitar de uma maior quantidade de tempo para a validação do certificado. Adicionalmente, a utilização de um dispositivo de maior capacidade de memória e processamento para armazenar as chaves privadas e realização dos cálculos criptográficos pode ser necessário, pois um *smartcard* existente hoje no mercado é limitado para esta quantidade de complexidade exigida.

Algumas características dos sistemas computacionais presentes nas arquiteturas propostas limitam este trabalho e devem aplicar recursos externos para minimizar possíveis problemas, tais como a usabilidade da arquitetura para o usuário final, a alta disponibilidade das autoridades notariais para validação dos certificados e a segurança do serviço da AN contra ataques de negação do serviço.

1.6 ORGANIZAÇÃO DO TRABALHO

O Capítulo 2 apresenta uma revisão sobre os principais conceitos e paradigmas de gestão de identidades existentes na literatura para a compre-

ensão do trabalho. Em seguida, no Capítulo 3 são apresentados conceitos de privacidade e suas definições, além de alguns trabalhos existentes com este foco. No Capítulo 4, são levantadas as abordagens propostas por este trabalho. As comparações dos modelos propostos com outros modelos existentes está contido no Capítulo 5. Por fim, no Capítulo 6 estão as considerações finais e proposições de trabalhos futuros.

1.7 PUBLICAÇÕES

Parte dos resultados deste trabalho foram publicados em forma de artigo científico na 8ª Conferência Internacional em Sistemas e Comunicações de Rede, "The Eighth International Conference on Systems and Networks Communications" (ICSNC), com o título "A Privacy-Enhanced User-Centric Identity and Access Management Based on Notary" (NOGUEIRA; SOUZA; CUSTóDIO, 2013). Adicionalmente, foi publicado outro trabalho relacionado no "International Journal of Computer Science and Information Security" (IJCSIS) (NOGUEIRA; MARTINA; CUSTóDIO, 2013). Os estudos sobre a gestão de identidades e seus sistemas também resultaram em dois trabalhos prévios. Estes trabalhos foram apresentados em forma de artigo no Workshop de Gestão de Identidades (WGID), realizado em conjunto com o Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), em 2011 e 2012 (NOGUEIRA et al., 2011; NOGUEIRA; SANTOS; CUSTóDIO, 2012).

2 GESTÃO DE IDENTIDADES

2.1 INTRODUÇÃO

O conceito de identidade, de modo geral, é uma representação de uma entidade em um contexto particular (JØSANG; ZOMAI; SURIADI, 2007). A identidade consiste de identificadores, ou seja, caracteres próprios que sozinhos ou em conjunto sejam exclusivos para diferenciar entidades (p. ex., pessoas, organizações, sistemas, máquinas). No meio digital, a chamada "identidade digital" é a representação digital dos identificadores relacionados com a entidade e são acessíveis através de meios técnicos. Uma entidade pode conter diversas identidades digitais sendo representados por um conjunto de atributos.

Durante vários anos, a identidade digital era considerada uma equivalência da identidade na vida real, i.e., uma extensão da carteira de identidade ou passaporte, contendo quase os mesmos dados. Porém, na verdade, uma identidade digital consiste em atributos, peculiaridades e preferências da entidade. Estas particularidades permitem que os usuários recebam serviços personalizados. Dentro do conceito de atributos, estes são dados que caracterizam a entidade, identificando-a, classificando-a ou qualificando-a de forma única em um domínio.

Um atributo identificador é um conjunto de dados utilizados para identificar uma entidade dentro de um domínio e para realizar procedimentos de autenticação. Normalmente, o valor deste tipo de atributo não varia com o decorrer do tempo. Por exemplo, o nome de uma pessoa pode ser um atributo de identificação para um domínio representado por uma sala de aula. Dependendo do valor do primeiro nome da pessoa (p. ex., João), podem haver duas ou mais pessoas com este mesmo valor do atributo, necessitando utilizar um conjunto de atributos (p. ex., nome e sobrenome) para identificar unicamente a pessoa dentro de um domínio de maior abrangência (p. ex., instituição de ensino). Uma identificação pode ser *forte* ou *fraca* (BERTINO; PACI; SHANG, 2009). A identificação forte utiliza apenas um atributo e a identificação fraca necessita de um conjunto de atributos do indivíduo.

Os atributos classificadores são dados utilizados para classificar entidades em grupos, por exemplo, dados biológicos (p. ex., altura, peso, cor dos cabelos e da pele), o tipo de alguma doença, características culturais e genéticas. Estes tipos de atributos podem, em conjunto, ser utilizados para se comportar como atributos identificadores. Entretanto, estes possuem um alto grau de tolerância à modificações dos valores no decorrer do tempo, por

exemplo, a cor do cabelo de uma pessoa pode mudar no decorrer do tempo, seja por meio de fatores diretos ou indiretos.

Já os atributos qualificadores são dados atribuídos por outras entidades a fim de habilitar a entidade, como por exemplo, o número do CREA (Conselho Regional Engenharia Arquitetura e Agronomia), ou número do título de eleitor e o número do PIS (Programa de Integração Social). Todos estes atributos necessitam das autoridades confiáveis para associá-las às pessoas, habilitando-as de exercer atividades profissionais, eleitorais, e os ganhos dos benefícios governamentais respectivamente. Os atributos qualificadores são utilizados para procedimentos de controle de acesso, autorização, permissão e delegação. Em algumas situações, os atributos qualificadores podem identificar a entidade e possuir um tempo de vida longo ou curto.

Os atributos pessoais podem ser representados por identidades digitais e seus subconjuntos representam as chamadas identidades parciais (PFITZMANN; HANSEN, 2010; HANSEN; PFITZMANN; STEINBRECHER, 2008). Normalmente, uma pessoa se apresenta com diferentes identidades parciais para diferentes situações, seja no trabalho, atividades de lazer (p. ex., praticando algum esporte, com a família), ou lidando com serviços (p. ex., um banco, uma loja, um site). A Figura 5 mostra um exemplo de identidades parciais.

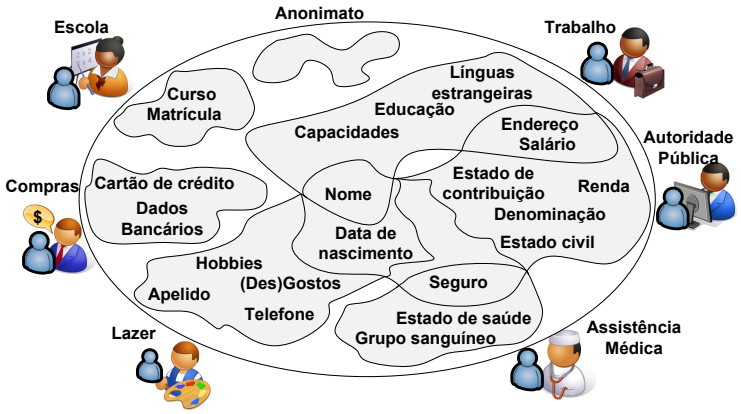


Figura 5 – Identidades parciais.

A Gestão de Identidades (GId) é um conjunto de ações e procedimentos para gerenciar um conjunto de atributos relacionados a uma entidade, compondo suas identidades parciais e utilizados para procedimentos de autenticação, autorização, controle de acesso, permissão, delegação, além de toda

a comunicação envolvida (BERTINO; TAKAHASHI, 2010). No meio digital, a gestão é realizada por meio de sistemas computacionais, *frameworks*, e infraestruturas para automatizar, controlar, gerenciar as identidades e efetuar a segurança da comunicação entre as partes envolvidas (DABROWSKI; PACYNA, 2008; WINDLEY, 2005; CAMP, 2004). A GId também envolve as relações de confiança sobre a identidade, a verificação da autenticidade, as políticas envolvidas em cada processo, os mecanismos e as regras de auditoria, a segurança dos dados, o gerenciamento do ciclo de vida das identidades, entre outros. Este conjunto de processos são realizados dentro do contexto de uma infraestrutura de autenticação e de autorização.

Existem diversos desafios no âmbito da gestão de identidades. O desafio de conciliar a simplicidade do sistema, os métodos de gerenciamento das identidades, a segurança, e a relação custo-benefício são os principais e os mais visados pela comunidade acadêmica científica e privada. Nos últimos anos, a privacidade dos usuários e seus dados começaram a ganhar atenção como um desafio necessário nos sistemas de gestão de identidades. Este capítulo descreve os principais conceitos e procedimentos envolvendo a gestão de identidades, modelos e paradigmas aplicados em um ambiente de infraestrutura de autenticação e autorização.

2.2 INFRAESTRUTURA DE AUTENTICAÇÃO E AUTORIZAÇÃO

O contexto de uma IAA é composto de três entidades principais: o Provedor de Serviços (PS), o usuário e o Provedor de Identidades (PId). O provedor de serviços é uma entidade que fornece um ou mais serviços e recursos (p. ex., sites web, *e-banking*, e-mail). O usuário (p. ex., uma pessoa, um sistema, um equipamento) é um cliente que utiliza e consome os recursos e serviços fornecidos pelo PS. O provedor de identidades é uma entidade que armazena e gerencia os atributos de seus usuários e fornece tecnologias e procedimentos de autenticação. Os PIds podem ser classificados de acordo com as suas funcionalidades (CAO; YANG, 2010). Um PId pode utilizar credenciais emitidas por outros PIds para realizar autenticação dos usuários, como por exemplo, um certificado digital X.509 emitido por uma autoridade certificadora.

Uma IAA deve fornecer procedimentos que envolvam desde a requisição de recursos pelo usuário até a liberação por parte do provedor de serviço. Estes procedimentos envolvem alguns conceitos importantes que estão descritos a seguir (CAMP, 2004):

Identificação O reconhecimento da associação de um identificador com o seu titular através da apresentação de seus atributos. Toda identifica-

ção requer um identificador, por exemplo, nome, endereço de e-mail, número do documento de identidade, numero do passaporte;

Autenticação A prova da posse de um atributo;

Autenticação da identidade Uma prova da associação entre uma entidade e um identificador. Por exemplo, a associação de uma pessoa com seu número de matrícula. A diferença entre identificação e autenticação da identidade pode ser exemplificado quando alguém diz que "Você é o João Silva" enquanto "Seus documentos ilustram que você é o João Silva". A segunda frase exemplifica uma autenticação da identidade;

Autenticação do atributo A prova da associação entre uma entidade e um atributo e este procedimento é realizado em duas etapas: autenticação da identidade seguida pela autenticação da associação do atributo e do identificador. Uma pessoa pode ser identificada pela carteira de habilitação de motorista e este documento também autentica o atributo sobre a permissão de dirigir;

Autorização Uma decisão para permitir uma ação em particular, baseada em identificadores ou atributos. Uma pessoa pode ter acesso a um ambiente restrito ou um grupo de pessoas com atributos semelhantes por exemplo;

Credencial Um conjunto de dados relativo a uma entidade, provendo evidências sobre a sua associação com uma identidade ou a posse dos dados (BERTINO; TAKAHASHI, 2010). As credenciais podem ser emitidas por autoridades (terceiras partes) confiáveis e devem possuir mecanismos de segurança para que a sua integridade, validade e autenticidade sejam verificadas. Alguns exemplos de credenciais são: documentos de papéis, cartões de plásticos, certificados digitais, logins e senhas, biometria.

Além da gestão dos dados do usuário, na IAA também são determinadas as políticas de controle de acesso. Uma IAA pode ser composta de diferentes mecanismos e tecnologias para ser amplamente utilizada, porém a sua integração não pode declinar competência da segurança de cada elemento. A gestão de identidades possui modelos ou arquiteturas de implementação que visam um melhor benefício de acordo com as necessidades requeridas. Uma IAA pode ser baseada em um ou mais modelos de gestão de identidades. Nas próximas seções são apresentadas três principais modelos, o Isolado, o Centralizado e o Federado. Adicionalmente, são descritos os principais paradigmas aplicados na gestão de identidades, tais como o centrado na rede, centrado no serviço ou centrado no usuário.

2.3 MODELOS DE GESTÃO DE IDENTIDADES

A classificação sobre os modelos de GId influenciam na composição dos serviços, os tipos de provedores de serviços, o gerenciamento dos atributos, o controle do usuário sobre a identidade e a proteção de privacidade. A seguir serão descritos os modelos isolado, centralizado e federado.

2.3.1 Modelo Isolado

O modelo de gerenciamento de identidades isolado é um dos mais utilizados. Caracteriza-se quando o provedor de serviços atua como provedor de identidades (CAO; YANG, 2010). Isto significa que todas as identidades e credenciais de seus usuários são armazenadas, emitidas e gerenciadas para serem utilizadas pelo próprio PS. Em cada PS, o usuário deve se registrar, apresentando todos os atributos necessários a fim de obter credenciais para realização de sua autenticação e autorização. A Figura 6 ilustra o modelo.

Este modelo, apesar da simplicidade no gerenciamento de identidades para os provedores de serviços, cria algumas dificuldades para o usuário e alguns problemas para os PSs. Isso ocorre cada vez que o número de diferentes PSs são utilizados por um mesmo usuário. A quantidade de registros realizados nos PSs faz com que os dados sejam replicados e difícil de mantê-los atualizados. Consequentemente, cresce o número de credenciais que o usuário necessita gerenciar. A dificuldade em memorizar todos os diferentes logins e senhas dos diferentes PSs faz com que os usuários constantemente requisitem uma nova senha para o PS, ou utilizem senhas mais fáceis de memorizar ou repetem a mesma senha em mais de um PS. Estas atitudes resultam na decadência da segurança do sistema, da privacidade do usuário, das credenciais e também dos próprios PSs.

2.3.2 Modelo Centralizado

O modelo de gestão de identidades centralizado caracteriza-se por ser implementado em um modelo cliente-servidor, na qual existe um único servidor (PId) responsável por registrar, gerenciar e autenticar os usuários de um mesmo domínio (uma organização por exemplo). Os inúmeros provedores de serviços que o domínio poderá oferecer são configurados para solicitar a autenticação do usuário por meio do provedor de identidades central. As funções do IdP e PS são bem definidas e distintas. Os PSs não armazenam os dados dos usuários localmente e podem realizar os procedimentos de autori-

Figura 6 – Modelo de GId isolado.

zação por meio de suas políticas de acesso e os atributos providos pelo PId. De acordo com Jøsang e Pope (JØSANG; POPE, 2005), o modelo centralizado pode ser implementado de diferentes formas, tais como o modelo com um identificador em comum, o modelo meta-identificador, e o modelo *Single Sign-On* (SSO). A Figura 7 ilustra o modelo centralizado.

O modelo com identificador em comum é quando uma autoridade separada e única atua exclusivamente como provedor de identidades e emissora de credenciais. Todos os PSs confiam neste PId para verificar as credenciais. Um exemplo deste tipo de modelo é a utilização de uma ICP para emitir certificados e serem utilizados em todos os PS. O modelo meta-identificador caracteriza-se pelo compartilhamento das identidades e credenciais dos usuários dos provedores de serviços de um domínio para serem associados a um único usuário. O provedor de meta-identidades gerencia esta associação e permite que o usuário utilize diferentes identidades e apenas uma única credencial no domínio. O modelo SSO permite que o usuário se autentique perante um PS apenas uma vez e, ao acessar outros PS do mesmo domínio, será automaticamente autenticado. A ocorrência do SSO é normalmente realizada por uma autoridade responsável por alocar os identificadores, emitir as credenciais e permitir a autenticação do usuário aos PSs.

Existem diversos sistemas de GId que implementam este modelo centralizado, do quais pode-se citar as ICPs, o Kerberos[1] e o CAS[2]. As vantagens deste modelo está na centralização da entidade (servidor) de gerenciamento dos atributos e autenticação do usuário e não necessitando obter registros dos usuários para cada serviço ofertado. Uma das desvantagens é a necessidade de todas as identidades do domínio estarem armazenadas e serem gerencia-

[1] http://web.mit.edu/kerberos/
[2] http://www.jasig.org/cas

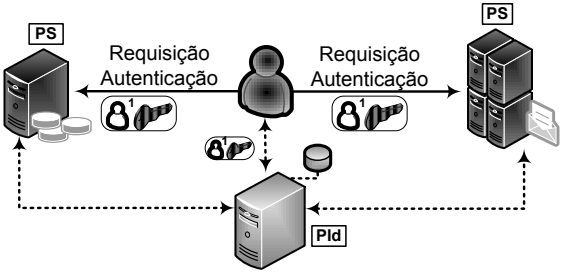


Figura 7 – Modelo de GId centralizado.

das por um único ponto de confiança. Como consequência, o PId deve manter níveis de segurança para que os dados dos usuários não sejam roubados ou modificados de forma não autorizada, além de manter a disponibilidade do serviço.

2.3.3 Modelo Federado

Com finalidade de integrar diferentes domínios e tornar um domínio virtual único, o modelo de GId federado caracteriza-se pelo conjunto de acordos, políticas, padrões e tecnologias que habilitam integrar provedores de serviços e identidades de diferentes domínios em um maior, o domínio federado. As políticas permitem que sejam estabelecidas comunicações confiáveis entre os PSs e os PIds, provendo o reconhecimento de diferentes PIds, a autenticidade dos dados dos usuários e o acesso de todos os serviços disponíveis na federação. O usuário deve estar vinculado a pelo menos um PId e este gerencia sua autenticação e seus atributos.

O modelo federado permite que o usuário se mantenha autenticado, ou "logado", para outros provedores de serviços da federação até que sua sessão se encerre (conceito de *single sign-on*). A re-autenticação só é necessária quando o tempo da sessão encerrar ou ocorrer a sua finalização por outros motivos. O SSO no modelo federado é diferente do modelo centralizado. Enquanto no modelo federado o SSO é inter-domínios, no modelo centralizado o SSO é intra-domínio (na maioria das vezes). Alguns protocolos, padrões e sistemas para o modelo federado são: OASIS *Security Assertion Markup Language* (SAML) (OASIS, 2005), *WS-Federation* (OASIS, 2009), e o framework *Liberty Alliance* (CANTOR et al., 2005). O Shibboleth (CARMODY et al., 2005) é um projeto de código aberto para este modelo que segue o padrão SAML.

A autenticação do usuário para os diversos PSs da federação ocorre, normalmente, pelo compartilhamento de asserções de atributos. A asserção identifica o usuário para o outro PS e também apresenta um conjunto de atributos para a realização da autorização. Caso o PS necessitar de alguma outra informação do usuário ainda não conhecida, então o PS pode requisitar os atributos adicionais necessários para o PId responsável pela autenticação e identificação do usuário. De posse dos atributos, o PS irá ceder ou não o acesso aos recursos (de acordo com as suas políticas de acesso). A Figura 8 ilustra o acesso do usuário pelo modelo federado.

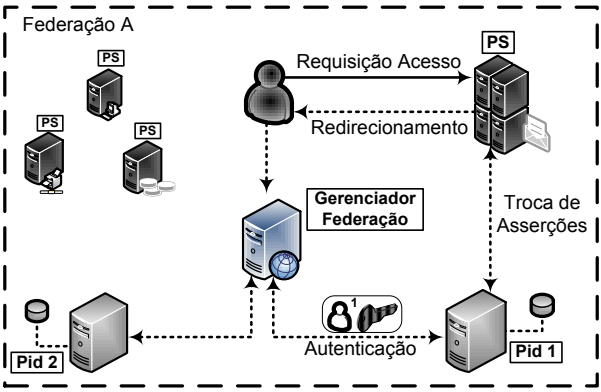


Figura 8 – Modelo de GId federado.

Um dos problemas que pode ocorrer neste tipo de modelo é quando o usuário possui mais de uma identidade e credenciais gerenciadas por mais de um provedor de identidades. Além do usuário ter que gerenciar mais de uma credencial, os valores de seus atributos podem estar em desconformidade entre os PIds, o que pode ocasionar um erro nos processos de autorização. Neste mesmo caso, há a dificuldade de se obter (ao mesmo tempo) diferentes atributos do usuário que são gerenciados por diferentes PIds. Desde modo, quando for acessar um PS, é complicado apresentar duas diferentes credencias em um sistema federado onde o protocolo aceita apenas a comunicação entre PS e um PId. Adicionalmente, o usuário teria que se autenticar duas vezes, uma para cada PID. O modelo federado também se limita para ser utilizado apenas em serviços web, não se preocupando em prover um controle sobre a liberação dos atributos do usuário e os requisitos sobre a sua privacidade.

2.4 PARADIGMAS DE GESTÃO DE IDENTIDADES

De acordo com Cao e Yang (CAO; YANG, 2010), três paradigmas de gestão de identidade podem ser definidos: centrado na rede, centrado no serviço e o centrado no usuário. Estes paradigmas não são isolados uns com os outros, mas possuem ligações próximas e alguns limites entre si.

2.4.1 Centrado na Rede

O paradigma centrado na rede ocorre nas fases iniciais de desenvolvimento de uma tecnologia de GId. Sua eficiência ocorre nas redes centrada nos serviços e aplicações. A gestão da identidade não está diretamente associada com o acesso ou com as políticas. O sistema de GId é criado e gerenciado por uma única entidade para um usuário fixo e um conjunto de recursos. Não é relacionado com serviços ou usuários. Um exemplo deste paradigma seria o domínio da Microsoft Windows, onde todas as contas dos usuários (p. ex., identificadores, credenciais, atributos), computadores, e outros dispositivos são registrados em um banco de dados central (um serviço de diretório) determinado por controladores do domínio. A autenticação ocorre nos controladores do domínio e cada pessoa do domínio recebe uma conta única que dá acesso aos recursos providos pelo domínio. Algumas limitações deste paradigma é a falta de suporte para extensões de atributos e federação.

2.4.2 Centrado no Serviço

O paradigma centrado no serviço é composto de provedores de serviços através de múltiplos domínios. Os serviços não estão necessariamente sob o controle de seus provedores. Este paradigma deve suportar a substituição dinâmica de serviços, ou seja, o usuário poderá usar o melhor serviço web de acordo com a sua preferência e a disponibilização na web. Considere um serviço web de agenda que um usuário acessa por possuir características de acordo com suas necessidades. Caso um novo serviço de agenda venha a estar disponível, o paradigma centrado no serviço irá adaptar (em tempo de execução) este novo serviço para ser utilizado pelo usuário. Além disso, todas as configurações personalizadas pelo usuário e contidas no serviço antigo devem ser transferidas para o novo serviço. Este paradigma é desafiador para ser implementado, pois é complicado alcançar a composição de serviços de diferentes PSs e domínios, além de cada entidade utilizar diferentes mecanismos de controle de acesso, de segurança e políticas.

2.4.3 Centrado no Usuário

No paradigma centrado no usuário, o usuário é o ponto central da arquitetura do sistema de gestão de identidades. O papel é transferido para o usuário obter mais controle das identidades digitais ao invés dos PSs. Em outras palavras, este paradigma coloca o usuário no meio das transações entre os provedores de identidade e terceiras partes. Obtendo mais controle sobre suas identidades, o usuário decide quais atributos podem ser compartilhadas e sob quais circunstâncias. Isso permite a satisfação de todas as necessidades dos usuários, implementando o gerenciamento do ciclo de vida de suas identidades, a proteção da privacidade e a divulgação. Alguns sistemas que são baseados no paradigma centrado no usuário são: OpenID (OPENID, 2007), Windows CardSpace (CHAPPELL, 2006), Higgins (FOUNDATION, 2012). Por outro lado, o usuário possui mais responsabilidades na comunicação com as entidades envolvidas no protocolo.

2.5 CONCLUSÃO

Neste capítulo, foi descrito os principais conceitos sobre gestão de identidades no meio digital. A gestão de identidades serve de suporte para a aplicação de uma infraestrutura de autenticação e autorização, na qual o usuário acessa um serviço fornecido pelo PS e o PId fica responsável por autenticá-lo e gerenciar seus atributos. Após a descrição dos conceitos, os tipos dos modelos dos sistemas foram descritos. O modelo isolado é bastante utilizado onde os provedores de serviços não necessitam de muitos investimentos e faz o papel de PId também. O modelo centralizado separa a responsabilidade do PS e do PId e um único PId fica responsável por atender os serviços providos. O modelo federado torna o modelo centralizado mais amplo, compartilhando recursos e políticas com outros domínios.

Os paradigmas de gestão de identidades se definem de acordo com os estágios de desenvolvimento de um sistema de GId e a transferência do núcleo principal da GId. Dentre as características foram descritos três paradigmas: centrado na rede, no serviço e no usuário. Sendo o paradigma centrado na rede o mais eficiente para as infraestruturas com uma rede de serviços e aplicações e que permite um melhor gerenciamento dos serviços acessados pelos usuários. O paradigma centrado no serviço visa tornar as configurações do usuário dinâmicas para serem aplicadas nos serviços que ele escolher utilizar. Já o paradigma centrado no usuário, permite colocá-lo no centro entre o provedor de identidade e os provedores de serviços, dando-lhe mais controle sobre a gestão dos seus atributos e a sua identificação.

3 PRIVACIDADE

3.1 INTRODUÇÃO

A gestão de identidades resulta na manipulação dos dados sobre os usuários para que possam ter condições de serem autenticados, identificados e autorizados perante os serviços requisitados (BERTINO; TAKAHASHI, 2010). Os sistemas de GId determinam diversos requisitos, tais como os considerados básicos (p. ex., políticas das entidades envolvidas, sobre armazenamento dos dados, formas de comunicação), os requisitos de segurança (p. ex., integridade , confidencialidade, disponibilidade, autenticidade, irretratabilidade), os requisitos de interação com o usuário, entre outros. Dentro dos requisitos de segurança estão aqueles que envolvem a privacidade do usuário. A privacidade (em muitos casos) não é levada em consideração nos projetos de desenvolvimento dos sistemas de gerenciamento de identidades, e sim como um recurso opcional do sistema (SHEEDY; KUMARAGURU, 2008).

A privacidade pode ser apreciada como "uma parte integral da humanidade" e "um direito humano fundamental" (SOLOVE, 2008). Entre as mais variadas definições de privacidade existentes, como por exemplo a proteção da personalidade e a intimidade (SOLOVE, 2008), a abordagem da privacidade no decorrer deste trabalho está relacionada com o gerenciamento de identidade e atributos dos usuário no meio digital. Neste trabalho, utiliza-se a definição de privacidade como o direito do usuário em controlar suas identidades e atributos nos procedimentos de autenticação e autorização e o nível de associabilidade entre os itens sobre a sua identidade requeridas pelos provedores de serviços (BERTINO; TAKAHASHI, 2010). Esta seção aborda os conceitos sobre privacidade, os problemas que a sua falta podem trazer para os sistemas de gerenciamento de identidades e os desafios existentes.

3.2 CONCEITOS

Dentre os conceitos que ajudam a determinar os diferentes níveis de privacidade existentes, segue abaixo os principais para a compreensão deste trabalho (PFITZMANN; HANSEN, 2010; SOLOVE, 2006):

Pseudônimo Utilizado como identificador ou para identificar a associação dos atributos de uma entidade (ou das atividades realizadas por ela), mas não retrata sua real identidade e nem tende a possuir uma longa duração;

Anonimato Uma condição para uma entidade não ser identificada dentro de um conjunto de entidades. A autenticação anônima de uma entidade não deve ser associada com nenhum atributo que possa identificar a entidade. Um identificador anônimo que é usado mais de uma vez se torna um pseudônimo;

Associabilidade A habilidade de associar dois ou mais itens de interesse (p. ex., sujeitos, mensagens, ações, atributos), permitindo que sejam detectadas as relações e as associações entre eles;

Dissociabilidade Negação de associabilidade, ou seja, qualidade de permitir a dissociação entre dois ou mais itens. Pode-se dizer que a dissociabilidade (ou a não-associação) garante que um usuário pode fazer múltiplos usos de uma mesma credencial para um mesmo serviço ou diferentes serviços. Neste caso, os PSs não devem ser capazes de saber que esta credencial pertence ao mesmo titular. O mesmo pode acontecer com o uso de múltiplas credenciais em que uma terceira parte pode não conseguir associá-las como sendo de um mesmo titular. Esta característica requer que as entidades sejam incapazes de determinar (por conta própria) quando um mesmo usuário realizou uma operação específica no sistema;

Indetectabilidade A habilidade de um item se tornar indetectável na percepção de uma terceira parte, i.e, a terceira parte não possui recursos suficientes para distinguir se o item existe ou não.

Os conceitos descritos acima possuem algumas relações entre si. Por exemplo, um usuário que deseja acessar de forma anônima um serviço web adulto, deve provar que a sua idade é maior que dezoito. Para realizar este procedimento de autorização sem que o requisitante seja identificado, o sistema de gestão de identidades deve habilitar a verificação do atributo "idade" sem associá-lo com um identificador. Apesar do anonimato trazer diversos benefícios aos usuários, este dificulta a realização dos procedimentos de prestação de contas (i.e., do termo em inglês *accountability*), procedimento de auditoria, e controles internos de segurança.

Um pseudônimo digital possui o poder de identificação maior do que o anonimato. Um atributo pseudônimo é como um identificador único e conveniente para autenticar o titular. Sua característica permite que o PS realize procedimentos de prestações de contas sobre o usuário. Se além da autenticação, o sujeito passar por um procedimento de autorização informando alguns de seus atributos para o PS, então os atributos serão associados a este pseudônimo. Caso um usuário venha a utilizar, em um mesmo PS, diferentes credenciais contendo diferentes atributos entre si e o mesmo pseudônimo, então

o PS será capaz de associar a igualdade de titularidade entre as credenciais. Adicionalmente, dentro desta associação, o PS poderá mapear todos aqueles atributos que foram apresentados pelas credenciais.

De acordo com Chaum (CHAUM, 1985), a preservação do anonimato ocorre quando se mantém o não-rastreamento dos pseudônimos envolvidos por meio da transferência de diferentes credenciais de um pseudônimo para outro sem provar a identidade do titular. A opção de manter o anonimato do usuário e a necessidade de poder autenticar o titular pelos provedores de serviços são um dos grandes desafios nos sistemas de GId.

O anonimato e os procedimentos de prestação de contas estão nas extremidades em relação a rastreabilidade dos usuários. O pseudo-anonimato é composto pelo conjunto destes extremos, ou seja, o pseudônimo abrange todos os níveis de associabilidade para um usuário. Este pode ser caracterizado em três tipos de vínculos: público, inicialmente não-público e inicialmente desvinculado. O pseudônimo público possui o vínculo com seu titular que pode ser conhecido publicamente desde o início, por exemplo, o telefone residencial de uma pessoa registrada em uma lista telefônica pública. O pseudônimo não-público inicialmente caracteriza-se pelo conhecimento da associação apenas por algumas entidades, mas não é público (pelo menos inicialmente). Um exemplo deste tipo seria uma conta bancária onde o banco pode verificar a associação entre a conta e o titular.

O terceiro tipo de associação do pseudônimo determina que a relação entre um pseudônimo não-associável e seu titular é, inicialmente, desconhecida para todos (com exceção do titular). Um exemplo deste tipo de pseudônimo é uma biometria associada com os dados sobre o DNA (a não ser que tenha sido armazenada em um banco de dados e associada ao titular). A força do anonimato diminui com o aumento do conhecimento da associação do pseudônimo. Um pseudônimo público não é transferível para outro titular e nunca poderá se tornar não-associável. Se um pseudônimo é transferido de titular de modo secreto, então este pseudônimo pode se tornar não-público novamente.

O anonimato é mais forte quando: menor for a quantidade de atributos associados com um pseudônimo; menor a frequência e o contexto da utilização dos pseudônimos; e a geração do pseudônimo é realizada de forma aleatória e independente. Um mecanismo bastante difundido que fornece um pseudônimo digital é a criptografia de chave pública, permitindo que o titular da chave pública consiga provar a sua titularidade e a pertinência da mesma através de funções criptográficas assimétricas envolvendo a chave privada correspondente.

3.3 A PRIVACIDADE NO CONTEXTO DE GID

As credenciais evoluíram para poder fornecer diferentes mecanismos de segurança. Brands (BRANDS, 2000) realizou diversos trabalhos para fornecer mais segurança na implementação de credenciais digitais em diversos dispositivos e a sua aplicação sobre os dados contidos nas credenciais. Alguns dos mecanismos de segurança nas credenciais são as possibilidades de seus titulares determinarem quando, como e em quais medidas os atributos contidos serão revelados para o verificador. Outros mecanismos também permitem incluir o controle sobre a privacidade, por exemplo, restrições da associação e do rastreamento dos dados.

A preocupação com a privacidade surgiu para que os usuários não sofram com o monitoramento de suas atividades pela rede e pelas organizações visitadas (CHAUM, 1985). A definição de privacidade em um certo contexto pode ser relativo para cada parte envolvida. Por exemplo, o fato de "coletar a menor quantidade de dados pessoais de um usuário" pode parecer como uma regra que ajudará na proteção da privacidade dos usuários em um sistema de GId. Embora esta abordagem seja atraente, na prática a relação entre o gerenciamento de identidades e a privacidade é sutil. O que poderia ser intuitivo, pode não ser aplicável.

É importante entender o contexto onde o sistema de gerenciamento de identidades será utilizado e as considerações para o montante de dados coletados. A ideia de "quanto menos dados coletados é equivalente a maior privacidade", pode falhar para explicar o tipo e a sensibilidade sobre a identidade envolvida. Um sistema que coleta e armazena a impressão digital de um usuário pode ser mais invasivo do que um sistema que armazena o histórico sobre o crédito de uma pessoa. Do mesmo modo, uma pequena quantidade de dados do usuário que é compartilhada com diversas entidades ou estiver em uma base de dados indevidamente protegida, pode colocar a privacidade do indivíduo em risco. Então, esta analogia pode ser mais prejudicial do que um ambiente onde uma grande quantidade de dados devidamente protegidos, nos quais são acessados somente por entidades autorizadas.

Devido a subjetividade do contexto em que a privacidade pode ser obtida ou fornecida, uma IAA deve definir bem seus objetivos e políticas para que esteja claro o nível de privacidade que a infraestrutura suporta. Na seção seguinte, são abordados alguns princípios relacionados com a privacidade.

3.3.1 Princípios sobre Privacidade

A privacidade nos sistemas de GId é determinada para um propósito específico, analisando os requerimentos necessários através de um sólido entendimento do ambiente em que o sistema opera e os riscos e benefícios em que deve balancear.

Existem diversas guias que foram escritas por entidades para fundamentar a privacidade e fornecer abordagens às práticas sobre o gerenciamento das informações. A *Organisation for Economic Co-operation and Development* (OECD, 2013) e a *European Union Data Protection Directive*[1] apresentam alguns princípios que abordam a coleção e o uso de dados pessoais (p. ex., nomes, endereços, identificadores emitidos pelo governo) para os sistemas de gerenciamento de identidades. Seguem abaixo as descrições de alguns deles.

Princípio da limitação da coleta dos dados A coleta de dados pessoais deve possuir um limite e deve ser obtidos por meios legais e justos e sempre que possível com consentimento do titular dos dados;

Princípio da qualidade dos dados O dado pessoal deve ser relevante para o propósito no qual está sendo usado, preciso, completo e atualizado (na medida do possível);

Princípio da especificação do propósito Os propósitos dos quais os dados pessoais são coletados devem ser especificados antes do momento da coleta e limitados ao uso que satisfaçam apenas aqueles propósitos;

Princípio da limitação do uso Os dados pessoais não devem ser divulgados, disponibilizados ou usados para outro propósito além do que foi especificado no acordo entre a entidade e o usuário. Pode haver uma exceção caso tenha consentimento do próprio titular dos dados ou intervenção de alguma autoridade da lei;

Princípio das medidas de segurança O dado pessoal deve estar protegido por uma medida de segurança sensata contra alguns riscos, tais como perda, acesso não-autorizado, destruição, uso, modificação ou divulgação;

Princípio da compreensão O sistema deve possuir uma política geral de compreensão sobre o desenvolvimento, as práticas e as políticas a respeito dos dados pessoais. Os recursos devem estar prontamente disponíveis para estabelecer a existência, a autenticidade dos dados pessoais,

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

e o principal propósito dos seus usos, assim como a identidade e o controlador usual dos dados no sistema;

Princípio da participação individual Um usuário deve ter o direito de obter a confirmação se o sistema possui dados sobre a sua pessoa ou não;

Princípio da responsabilidade O controlador dos dados deve ser responsável pelo cumprimento de medidas para tornar efetivo os princípios acima descritos.

3.3.2 Autenticação Privada

A autenticação de um usuário pode ser realizada por meio de diferentes mecanismos e tecnologias (SMITH, 2002). Os métodos de autenticação podem ser implementados para fornecer diferentes características, tais como usabilidade, segurança, custo, privacidade, entre outros (BRAZ; ROBERT, 2006). O fornecimento da privacidade para a realização da autenticação pode ser obtido por meio da utilização de protocolos de prova *zero-knowledge*, ou seja, protocolos de conhecimento zero. Estes tipos de protocolos permitem que um "provador" comprove a um terceiro (um "verificador") que uma determinada afirmação é verdadeira sem transmitir qualquer informação adicional além do fato de que a afirmação é realmente verdade (QUISQUATER et al., 1990). Muitos destes protocolos utilizam-se de diversas interações entre as entidades envolventes, protocolos criptográficos e funções matemáticas. Diversos protocolos de *zero-knowledge* foram estudados, especificados e implementados, por exemplo o de Feige-Fiat-Shamir (FEIGE; FIAT; SHAMIR, 1988), Guillou-Quisquarter(GQ) e Schnorr (BELLARE; PALACIO, 2002) e Blum-Feldman-Micali (BLUM; FELDMAN; MICALI, 1988).

Diferente dos métodos tradicionais de autenticação, em que o usuário necessita apresentar uma prova estática para o verificador, no protocolo *zero-knowledge* o usuário deve convencer o verificador de que ele possui a prova da autenticação interativamente. A autenticação *zero-knowledge* é realizada por meio de uma prova, trocada entre as partes interessadas, por meio de uma ou mais interações.

3.4 SISTEMAS COM APRIMORAMENTO DA PRIVACIDADE

Existem alguns modelos de sistemas que propõem mecanismos de usos de pseudônimos ou do anonimato para melhorar a privacidade dos usuários na interação com os provedores de serviços. Diante de diversos modelos

de sistemas com o foco no aprimoramento da privacidade, tal como o trabalho de Lysyanskaya et. al. (LYSYANSKAYA et al., 2000), esta seção apresenta dois sistemas baseados em credenciais anônimas: U-Prove e Idemix.

3.4.1 U-Prove

U-Prove é uma especificação criada por Brands (BRANDS, 2000) e atualmente está sob domínio da Microsoft (PAQUIN; ZAVERUCHA, 2013). Esta especificação é baseada em mecanismos criptográficos para permitir que os usuários divulguem, de forma seletiva e offline, seus atributos para os provedores de serviços. A tecnologia U-Prove permite que os usuários se autentiquem e apresentem seus atributos por meio de *tokens* U-Prove (denominação própria da especificação). Estes *tokens* são como credenciais contendo pseudônimos e um conjunto de atributos que podem ser selecionados para se tornarem visíveis para o provedor de serviços. A autenticidade de uma credencial e seus atributos é garantida por meio da assinatura das autoridades emissoras de credenciais U-Prove.

O sistema U-Prove permite que o usuário resguarde sua privacidade sobre os PSs que são visitados. Em outras palavras, as entidades emissoras das credenciais não conseguirão rastrear e associar as credenciais emitidas com os serviços que foram utilizados. Os atributos permitem que sejam inclusos em texto-claro ou de forma privada. Cada credencial é associada com uma chave pública para realização do protocolo. A chave privada correspondente é de conhecimento apenas do titular da credencial. A chave pública é inclusa na credencial, mas não fica visível para a entidade emissora, e sim, para o verificador. Este procedimento ocorre por meio de um protocolo de assinatura cega (CHAUM, 1983, 1984), da qual mantêm privado o conteúdo da mensagem para o signatário.

Além de um identificador único da credencial (a chave pública), dos atributos do titular e de outros dados para o protocolo U-Prove, a credencial também possui dois importantes campos: um definido pelo emissor para conter alguma informação sobre a credencial e um campo definido pelo titular para conter alguma informação que não seja visualizada pelo emissor e sim pelos verificadores. Existe também a possibilidade de envolver um dispositivo criptográfico (p. ex., *smartcard*) para estar associado à credencial e aumentar a segurança quanto aos procedimentos de emissão, utilização e revogação da credencial associada. Entretanto, este tipo de associação poderá elevar a complexidade dos protocolos envolvidos.

Após a obtenção da credencial, o titular pode utilizá-la e decidir por apresentar para o verificador qualquer atributo nele contido. Através de um

protocolo *zero-knowledge*, o usuário emite "provas de posse" para o verificador a fim de provar que sua credencial realmente contém os atributos que foram apresentados. Com este protocolo, os valores dos atributos que não foram apresentados se mantêm escondidos para o verificador.

A especificação U-Prove não entra em detalhes sobre como os procedimentos da comunicação entre o usuário e o emissor são realizados para a solicitação das credenciais, sobre a troca de mensagens, e como os requisitos de segurança são realizados. A solicitação do usuário por uma credencial pode necessitar de um procedimento prévio de autenticação para poder validar os atributos. Os mecanismos de revogação das credenciais não foram explicitamente especificados, mas algumas alternativas foram descritas. O uso do identificador único da credencial junto com uma lista de credenciais revogadas ou a revogação do dispositivo ao invés da credencial podem ser algumas das soluções. Outra solução é assumir que as credenciais possuem data de validade (e de curto período) e não necessitar de um mecanismo de revogação. Estes mecanismos de revogação não possuem propriedades para a preservação da privacidade. Dentre alguns dos recursos abordados, mas que não foram implementados até o momento pela especificação U-Prove (PAQUIN, 2013), está a função de apresentar a credencial através de protocolos *zero-knowledge*.

3.4.2 IDEMIX

Idemix (abreviação de *Identity Mixer*) é um sistema de credenciais anônimas baseado no esquema de Camenisch-Lysyanskaya (CAMENISCH; LYSYANSKAYA, 2001, 2003), que foi desenvolvido pela IBM. O protocolo Idemix teve origem a partir de dois projetos realizados anteriormente, o projeto PRIME[2] (*Privacy and Identity Management for Europe*) (ANDERSSON et al., 2005; LEENES; SCHALLABÖCK; HANSEN, 2008) e o projeto PrimeLife[3] (WÄSTLUND et al., 2011).

O protocolo Idemix permite a realização da autenticação anônima entre o usuário e o PS, com suporte à auditoria das transações (CAMENISCH; HERREWEGHEN, 2002). As credenciais Idemix são emitidas por uma autoridade confiável e atesta que os atributos do usuário são válidos utilizando o esquema de assinatura cega de Camenisch-Lysyanskaya. O usuário, por sua vez, atesta a posse e a validade das credenciais por meio da apresentação de provas *zero-knowledge*. Neste caso, o usuário não necessita revelar o conteúdo da mensagem ou a assinatura propriamente dita. Adicionalmente, o

[2] https://www.prime-project.eu/

[3] http://primelife.ercim.eu

titular pode utilizar a mesma credencial diversas vezes sem correr o risco de revelar a sua associação com a sua credencial e os dados contidos.

Cada usuário possui uma única chave mestra que é associada as suas credenciais Idemix. Desta chave mestra, deriva-se diferentes chaves para serem associadas a diferentes credenciais. A chave mestra permite provar que as credenciais de diferentes emissores estão relacionadas com o mesmo titular. Através das provas e o protocolo *zero-knowledge*, o usuário consegue provar que ele já possui as credenciais contendo os atributos associados com a chave mestra. O protocolo Idemix permite que o emissor valide as credenciais sem que os atributos e a chave mestra do usuário sejam revelados. Outro mecanismo para evitar que as credenciais sejam associadas uma das outras, é a habilidade de poder embaralhar as credenciais em cada apresentação dos atributos para o verificador. O esquema Idemix também permite que as credenciais não sejam rastreadas por seus emissores. A credencial é sempre emitida com um pseudônimo do usuário que é registrada (ou conhecida) pela entidade emissora.

A chave mestra do usuário permite derivar pseudônimos que podem ser utilizados para identificar a sessão, i.e., permite que a entidade com quem está se comunicando possa associar as ações do usuário. Todos os pseudônimos são não-associativos uns com os outros, a menos que o usuário prove que eles são gerados a partir de uma mesma chave mestra. A chave mestra também é codificada em todas as credenciais para prevenir que uma credencial seja compartilhada.

O usuário não apresenta a sua credencial para o provedor de serviços e sim, as provas de posse para comprovar a pertinência da credencial e dos valores dos atributos inclusos. As provas são emitidas através da posse de uma ou mais credenciais e é composta por uma prova de *zero-knowledge* e a chave mestra do usuário. Além de selecionar quais atributos podem se tornar visíveis para o verificador, o sistema Idemix permite que o usuário prove declarações a respeito do atributo, como por exemplo, provar que a data de nascimento contida na credencial informe que o titular possui mais de dezoito anos de idade. Esta prova pode não revelar a data de nascimento propriamente dita, tornando assim a apresentação parcial de um atributo. As provas de posse são verificáveis por meio da chave pública do emissor.

U-Prove e Idemix possuem objetivos semelhantes, mas cada um utiliza diferentes protocolos e fornecem opções diferenciadas um do outro (BICHSEL; CAMENISCH, 2010). No protocolo de emissão de credenciais do U-Prove, todos os atributos da credencial são conhecidos pelo emissor, enquanto o Idemix permite que o usuário escolha se deseja manter visível para qualquer um, visíveis por autorização ou sigilosos para todos. Como consequência, o protocolo U-Prove se limita em emitir várias credenciais para

um mesmo pseudônimo já que é necessário que todas as credenciais contenham a chave do usuário para comprovar da identidade do titular. O protocolo de apresentação da credencial U-Prove também possui algumas limitações. Algumas delas são: não suporta a prova de declaração sobre os atributos (p. ex., idade maior que dezoito anos), nem libera os atributos como comprometimentos ou criptograficamente verificáveis; utiliza várias credenciais ao mesmo tempo para comprovar diferentes atributos contidos em diferentes credenciais; necessidade de utilizar a credencial apenas uma vez para evitar a associabilidade entre os aqueles já utilizados.

O Idemix possui como desvantagem a performance computacional devido à complexidade computacional exigida pelas funções criptográficas. Outra característica que pode ser considerada como uma desvantagem seria a falta de um mecanismo de revogação das credenciais. As credenciais Idemix são emitidas com períodos de validades curtas.

Um dos grandes desafios para os sistemas de credenciais anônimas é a revogação. Uma vez que a credencial não possua um identificador visível e duradouro, existe a dificuldade de associá-la como sendo uma credencial revogada. Caso seja necessário um mecanismo de revogação, (p. ex., lista de credenciais revogados, lista negra), então será fundamental identificar a credencial. Neste caso, cria-se a possibilidade de que terceiras partes realizem algum tipo de rastreamento do uso destas credenciais. Algumas alternativas para revogar credenciais anônimas estão surgindo nos últimos anos e sendo aplicadas no sistema do Idemix (LAPON et al., 2011).

A complexidade dos sistemas U-Prove e Idemix são altas a fim de tornar um desafio a sua implementação utilizando *smartcards* (Idemix possui mais complexidade). Entretanto, existem alguns trabalhos nos quais implementam as duas especificações com diferentes propriedades criptográficas das originais, para torná-las mais leve e diminuir o tempo gasto para os procedimentos de criptografia (BICHSEL et al., 2009; MOSTOWSKI; VULLERS, 2012). As especificações dos dois sistemas não permitem concluir um possível valor necessário para o custo de suas implementações e para o usuário final. Adicionalmente, não há um requisito ou regra clara informando como é realizada a autenticação do usuário no momento da requisição de uma credencial. Infere-se que cada entidade emissora de credenciais gerencia uma base de dados com *logins* e senhas para poder autenticar seus usuários.

Atualmente, existe um projeto em desenvolvimento com o objetivo de desenvolver tecnologias que suportam credenciais baseadas em atributos de forma confiáveis e com preservação da privacidade a longo prazo. Este projeto é o ABC4Trust[4] (*Attribute-based Credentials for Trust*) e está sendo fundado pela União Europeia. A ideia do projeto é aproveitar o melhor dos

[4]https://abc4trust.eu/

sistemas U-Prove e Idemix e criar uma tecnologia mais aperfeiçoada para inibir os pontos negativos originados de cada um dos sistemas anteriores. Este projeto teve início em 2010 e possui a duração inicial de quatro anos. Já existem dois pilotos sendo executados, um na universidade de Patras na Grécia e outro em uma escola da Suécia.

3.5 CONCLUSÃO

Este capítulo apresentou os principais termos para compreender melhor a relação da privacidade em sistemas de gestão de identidades para seus usuários. Os termos descritos (pseudônimo, anonimato, associabilidade, dissociabilidade e indetectabilidade) possuem uma relação entre si, dos quais são necessários determinar as possibilidades das funções do sistema para que não impliquem em algum tipo de comprometimento da privacidade fornecida.

Em seguida, foram apresentados dois sistemas especificados que visam aplicar esquemas de preservação da privacidade do usuário em procedimentos de autenticação e autorização. Os sistemas U-Prove e Idemix objetivam a emissão e uso de credenciais anônimas para fornecer requisitos da privacidade aos usuários. Por meio de protocolos e mecanismos de criptografia, os esquemas implementados por cada um dos modelos, permitem a apresentação da autenticação das credenciais por meio de provas de posse das credenciais e dos atributos com a preservação do anonimato.

4 ICPS CENTRADAS NO USUÁRIO E BASEADAS EM NOTÁRIOS

4.1 INTRODUÇÃO

Este capítulo propõe novas modificações para o modelo tradicional de ICP. Essas modificações têm os seguintes requisitos gerais:

- Arquitetura voltada para o contexto de gerenciamento de identidades;
- Não perder a generalidade de uma ICP, quanto ao uso de chaves criptográficas assimétricas para procedimentos em IAA e validação para documentos eletrônicos;
- Melhorar na diminuição da complexidade dos procedimentos envolvendo a revogação do certificado e verificação de sua autenticidade;
- Promover um melhor gerenciamento dos atributos do usuário, ou seja, os atributos devem ser gerenciados apenas pelas autoridades responsáveis;
- Fornecer para o usuário-final um maior controle sobre seus atributos, podendo ele decidir quais atributos são apresentados para os provedores de serviços. Em outras palavras, deve ser possível para o usuário adicionar e remover seus atributos de acordo com as suas necessidades;
- Aplicar mecanismos para aprimorar a privacidade do usuário.

Neste capítulo, são descritas três alternativas de modelo de ICP que atendem os requisitos descritos acima. O primeiro modelo proposto é a ABPKI (*Attribute Based Public Key Infrastructure*), sigla do inglês para "Infraestrutura de Chaves Públicas Baseada em Atributos". A ABPKI permite que o usuário controle a apresentação de seus dados através das credenciais. O segundo modelo, é um aperfeiçoamento da ABPKI que, por meio da adição de novos recursos, aprimora o nível de privacidade do usuário. Este modelo denomina-se de UCPKI (*User-Centric Public Key Infrastructure*), traduzido para o português como "Infraestrutura de Chaves Públicas Centrada no Usuário". Por fim, o terceiro modelo tem como objetivo melhorar ainda mais o nível do fornecimento da privacidade em relação a UCPKI. A UCPKI-AA, sigla do inglês para "Infraestrutura de Chaves Públicas Centrada no Usuário com Autenticação Anônima" (*User-Centric Public Key Infrastructure with Anonymous Authentication*) é o nome deste terceiro modelo.

4.2 FUNDAMENTOS DAS PROPOSTAS

Nesta seção são apresentadas e justificadas as principais melhorias sobre as quais são fundamentadas as propostas.

4.2.1 Abordagem Centrada no Usuário

A emissão de certificados X.509 em um modelo tradicional de ICP ocorre pela apresentação obrigatória dos documentos necessários pelo titular para uma Autoridade de Registro (AR). A AR tem a responsabilidade de conferir a validade dos documentos, se eles foram emitidos por uma autoridade confiável, e garantir que o usuário tenha em posse a chave privada. As Autoridades Certificadoras (ACs) são responsáveis por delegar os poderes de verificação às ARs e determinar as políticas para a coleta das informações pessoais obrigatórias e opcionais a serem incluídas no certificado do usuário.

Assim como em diversos modelos de sistemas de autenticação e autorização, para que o usuário acesse um recurso, ele precisa apresentar seus dados para o provedor de serviços (ou provedor de identidades) a fim de realizar um cadastro e depois requisitar algum recurso. Estes cadastros são mantidos sob custódia destas entidades que, na maioria das vezes, não são responsáveis por gerenciar os dados e nem possuem requisitos necessários para mantê-los armazenados de forma segura. O gerenciamento dos atributos dos usuários (atualização, remoção, adição) fica comprometido por necessitar que os próprios usuários atualizem seus dados. Este pode ser um processo demorado ou até mesmo inviável. Em alguns casos, os PSs não fornecem a opção de remoção do cadastro do próprio usuário, ou dizem que o cadastro foi removido, mas, na verdade, seus dados continuam armazenados. Estes casos são exemplos da ausência do controle pelo usuário em relação aos seus próprios dados.

Considerando o fato de que sempre haverá uma autoridade responsável por gerenciar e informar pelo menos um atributo do usuário, não há a necessidade de que os PSs realizem cadastros de seus usuários para autenticá-los e autorizá-los. Como consequência, quanto menos atributos estiverem em mãos de outras entidades das quais não são as responsáveis, menos problemas de atualização, segurança e privacidade podem ocorrer.

As propostas descritas neste trabalho almejam que os atributos sejam apresentados pelo próprio titular em um certificado auto-assinado. Partindo do pressuposto que isso é uma característica dos modelos, ou seja, nas abordagens propostas sempre é preciso apresentar um certificado para requisitar um recurso ao PS e não há mais a necessidade do usuário apresentar docu-

mentos probatórios para que uma "autoridade certificadora" valide os dados. Os atributos informados pelo titular devem ser validados e confirmados pela própria autoridade que provê os determinados atributos.

4.2.2 Autoridades Notariais e Provedoras de Atributos

A auto-afirmação da posse dos atributos pelo usuário, na maioria das vezes, não é suficiente para que o PS confie no usuário e forneça os recursos requisitados. Os dados do usuário devem ser validados por uma autoridade confiável. Esta autoridade confiável é executada pela Autoridade Notarial (AN). Assim como no mundo real, a AN é responsável por certificar, registrar, comprovar, emitir provas, entre outras ações, perante seu poder notarial. Na arquitetura apresentada, a AN é responsável por certificar e validar as credenciais auto-assinadas pelo usuário. A validação de um certificado ocorre pela verificação de sua autenticidade e dos atributos inclusos. A AN não deve armazenar nenhum dado sobre o usuário e nem é responsável por gerenciar os atributos dos usuários. Então é necessário que a AN requisite a confirmação às autoridades responsáveis pelo registro e gerenciamento de tais atributos.

As autoridades responsáveis pelo gerenciamento dos atributos são as Autoridades Provedoras de Atributos (APAs). Assim como existem entidades governamentais responsáveis por registrar as pessoas para fornecer seus direitos como cidadãos, ou também para cobrar obrigações tributárias em diversos setores, estas entidades gerenciam os atributos que são considerados confiáveis para o uso em todo território nacional ou internacional. As entidades que emitem registros profissionais também devem ser confiáveis para certificar a permissão de uma determinada pessoa em exercer uma determinada profissão. Sendo assim, as APAs são entidades confiáveis que registram e gerenciam atributos das pessoas para diferentes finalidades. Por meio das chaves criptográficas assimétricas dos usuários para comprovar a autenticidade dos dados, a parte pública da chave deverá ser registrada nos bancos de dados de cada autoridade de atributos para conter a devida associação entre o titular da tal chave e os atributos.

Uma APA poderia certificar os atributos dos usuários diretamente ao invés da AN. Entretanto, por questões de segurança, privacidade e a descentralização providos pelos modelos, é necessário que a AN seja um ponto central de confiança da infraestrutura e de distribuição das funções para as diversas APAs existentes. Então, fica ao cargo das APAs apenas o gerenciamento dos atributos e informar se os atributos de um usuário realmente correspondem com os valores apresentados.

A verificação dos valores dos atributos ocorre apenas entre a AN e a

respectiva APA. Após a confirmação da veracidade dos atributos do usuário, a AN valida o certificado auto-assinado do usuário por meio de sua contra-assinatura. Sua assinatura significa que aquele certificado auto-assinado foi verificado e validado por uma autoridade notarial, tornando confiável para qualquer verificador até a expiração de sua data de validade. Esta função assemelha-se com a de uma autoridade certificadora, porém a contra-assinatura de um certificado resulta em uma credencial para ser utilizada para requisitar um recurso do PS e não há um caminho de certificação igual a uma ICP.

4.2.3 Confiança das Autoridades

Em uma ICP X.509, a confiança entre as autoridades certificadoras até o certificado do usuário final, é baseada no caminho de certificação até uma AC Raiz. A AC Raiz, por possuir um certificado auto-assinado, deve ter seu certificado incluso em uma lista de certificados confiáveis do sistema verificador. Caso esta autoridade deixe de ser confiável, seu certificado deve se removido desta lista. Normalmente, os sistemas já possuem uma lista padronizada de certificados confiáveis. Entretanto, este gerenciamento é realizado ou com a atualização do sistema ou de forma manual pelo utilizador do sistema o que torna um problema de gerenciamento e de atualização para garantir a confiabilidade desta lista.

Cada AN e APA possui seu par de chaves e um conjunto de informações a respeito. Para resolver o problema de gerenciamento das autoridades confiáveis, o excesso de procedimentos providos pelo caminho de certificação, e o tempo gasto para verificar a confiança da emissão do certificado do usuário final, o modelo proposto utiliza o padrão e a especificação de Listas de Estados dos Serviços Confiáveis, do inglês *Trust-service Status List* (TSL) (ETSI, 2009). Nestas listas, são informados os dados sobre as autoridades, tais como nome do serviço, endereço, URI e a chave pública correspondente. O administrador da lista deve indicar o estado atual em que o serviço se encontra. Os estados do serviço podem ser: aderente, expirado, suspenso, revogado ou não aderente.

Além dos estados atuais de cada serviço, a TSL suporta a manutenção do histórico dos estados ao longo do tempo para cada serviço. Os históricos dos estados devem ser registrados desde o momento em que o gerenciador da lista toma conhecimento da existência das autoridades. Uma TSL pode ser composta por uma lista de listas, i.e., uma TSL pode gerenciar uma lista de TSLs. Um exemplo de uma lista de listas seria na aplicação para gerenciar os serviços de um conjunto de federações acadêmicas, onde um país contém

várias federações internas, cada federação possui sua TSL e o país gerencia a TSL contendo as TSLs de cada federação nacional.

As abordagens apresentadas neste trabalho utilizam as TSLs para indicar a confiança das autoridades notariais e a confiança entre as ANs e as APAs. Toda AN é, em princípio, confiável. Entretanto, pode ser que a AN venha sofrer mudanças em suas políticas, ou em suas operações de forma que a AN perca a confiabilidade. Sendo assim, o estado indicado na TSL mostrará a situação de cada uma de acordo com as políticas do domínio gerenciador da TSL. As APAs podem ser confiáveis para algumas ANs, mas não para outras. Por exemplo, uma instituição de ensino contém atributos de alunos que indicam a sua formação. Devido à algumas políticas que não estão em conformidade com uma AN específica, esta AN pode não confiar na validade dos atributos acadêmicos dos alunos associados. Então esta APA, que informa atributos acadêmicos, não estará inclusa na TSL gerenciada por esta AN ou seu estado pode ser definido como suspenso ou revogado.

A TSL, possuindo as listas de autoridades notariais, é publicada online e atualizada sempre que alguma mudança ocorrer. As partes interessadas devem consultar a lista no momento da verificação.

4.2.4 Certificado Auto-Assinado

Um certificado auto-assinado é uma estrutura de dados, podendo ser implementado um XML ou ASN.1, no qual o usuário cria e assina utilizando sua chave privada. O certificado é utilizado para obter uma credencial. A chave pública correspondente deve ser inserida para que a assinatura possa ser verificada. A chave pública também serve como um identificador do titular e é responsável por indicar a associação com os atributos afirmados pelo titular. A associação entre o identificador (chave pública) e seus diversos atributos são gerenciadas pelas APAs.

O par de chaves do usuário pode ser obtido em uma agência física de uma APA ou o mesmo poderá criar em seu próprio dispositivo e depois provar a posse da chave privada para a APA. A chave privada deve ser armazenada em um dispositivo seguro (p. ex., *smartcard*) e a sua utilização deve ser protegida por uma senha ou PIN. Após a criação do par de chaves, o usuário deve registrar a chave pública em todas as APAs que gerenciam ao menos um atributo. No registro de cada APA, a chave pública funcionará como o identificador do usuário que será associado com os atributos que esta entidade gerencia.

O procedimento deste registro pode ser realizado pessoalmente (de preferência) ou através de um serviço web. Caso utilize-se de serviço web

para este cadastramento, a APA teria que possuir algum mecanismo de autenticação já em uso, em que o registro desta chave pública é realizado após a autenticação com este mecanismo próprio. Após o registro da chave, o mecanismo de autenticação poderá ser migrado para o uso de um protocolo de desafio-resposta com a chave pública registrada e a chave privada em posse do usuário.

A confiabilidade da chave é realizada através da associação com os atributos gerenciados pelas APAs. Se mantidas de forma segura, as chaves criptográficas podem possuir uma validade maior do que os certificados digitais, podendo igualar sua validade com a mesma validade associada com o algoritmo criptográfico utilizado. Quando o algoritmo utilizado deixar de ser considerado seguro, o mesmo deve ocorrer com a chave do usuário. Se algo ocorrer com a chave privada do usuário, a mesma deve ser trocada nas bases de todas as APAs. O procedimento da troca do registro da chave pública nas bases das APAs pode ser realizado de diferentes maneiras.

Uma alternativa proposta para o procedimento da troca da chave pelo usuário seria que no momento do primeiro registro da chave pública do usuário, o mesmo deve obter um código (uma sequência de caracteres) da APA. Este código é uma senha do padrão OTP (*One Time Password*)(HALLER et al., 1998) e utilizado apenas uma vez. A senha pode ser repassada para o usuário de diversas formas, por exemplo, via papel, e-mail, dispositivo específico. Através deste tipo de código, o usuário poderá acessar um serviço web para trocar a associação para uma nova chave pública. O procedimento pode requerer um mecanismo de desafio-resposta para confirmar a identidade do usuário, como a confirmação de um questionamento sobre os valores dos atributos armazenados na APA. Independente de qual mecanismo for utilizado, as APAs devem aplicar os mecanismos de segurança necessários para evitar que os serviços sofram ataques de negação do serviço e garantir que o usuário seja autenticado devidamente.

A auto-assinatura do certificado possui a finalidade de incluir as propriedades fornecidas pela assinatura digital, indicando que os dados apresentados estão íntegros, que são autênticos do ponto de vista do uso da chave assimétrica pelo usuário e o não-repúdio para auxiliar em um procedimento de auditoria quando necessário.

O certificado do usuário possui como uma estrutura base a chave pública do usuário, um conjunto de atributos com as referências das APAs responsáveis por gerenciar cada atributo, um período de validade e a assinatura do titular. O certificado deve ser validado por uma AN verificando a integridade, autenticidade e veracidade dos dados. A certificação dos valores dos atributos inclusos é realizada pela AN em comunicação com as APAs responsáveis. A segurança da comunicação para a verificação dos atributos dos

usuários registrados nas APAs é determinada pela restrição de que apenas as ANs confiáveis pela APA poderão realizar requisição em seus serviços.

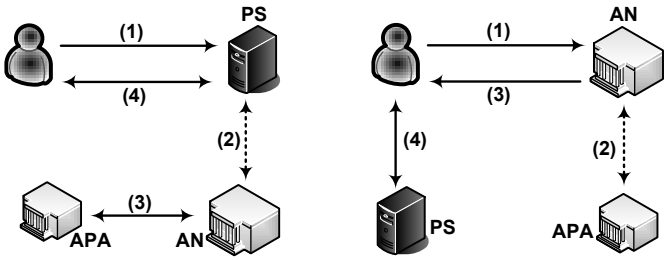
A utilização de um certificado auto-assinado pode ser realizada de duas formas pelo usuário: (1) apresentando-o para o PS e o mesmo ficando responsável por validá-lo junto à AN; ou (2) requisitando a validação diretamente para uma AN e depois apresentá-lo para o PS. O primeiro método denomina-se de método *pull*, enquanto o segundo é o método *push*.

4.2.4.1 Método Pull

O método para o uso do certificado no modo *pull* caracteriza-se quando ao mesmo tempo que o usuário está requisitando um recurso para o PS, o mesmo entrega seu certificado e o PS deve "puxar" a validação do certificado junto a uma autoridade notarial. Através deste método, o usuário pode criar o certificado apenas no momento em que for utilizá-lo. Caso o usuário apresente um certificado para um PS por meios físicos (no mundo real), o usuário não necessitará possuir acesso à Internet. Esta obrigatoriedade de haver uma conectividade com a Internet é transferida para o PS. Outra consequência do uso deste procedimento é que o PS poderá concluir que naquele exato momento os atributos do usuário são válidos.

4.2.4.2 Método Push

O método *push* corresponde quando o usuário obtém uma credencial (o certificado contra-assinado por uma AN) via requisição direta com uma AN, ou seja, não envolvendo o provedor de serviços. Neste método, o usuário requisita a validação previamente ao uso da credencial e requer que o mesmo tenha acesso à Internet. Entretanto, o provedor de serviços não necessita manter uma conexão com as ANs e a verificação da credencial do usuário poderá levar menos tempo do que através do método *pull*. O tempo de verificação pode ser menor pois o PS não necessitará requisitar para uma AN a validação do certificado do usuário. Além destas diferenças que podem facilitar o uso do certificado por parte do usuário, os dois métodos diferenciam-se principalmente no modelo de negócio a ser aplicado entre as ANs e os PSs (não abordado neste trabalho). A Figura 9 ilustra os dois métodos.



(a) Método *pull*. (b) Método *push*.

Figura 9 – Formas de utilização de um certificado auto-assinado.

4.3 INFRAESTRUTURA DE CHAVES PÚBLICAS BASEADA EM ATRIBUTOS

A fim de melhorar a gestão de atributos dos procedimentos de emissão dos certificados X.509, bem como diminuir a quantidade de procedimentos necessários para verificar a confiança de um certificado de chave pública e no gerenciamento dos procedimentos de revogação, o modelo apresentado nesta seção propõe uma nova alternativa do uso de chaves criptográficas assimétricas para sistemas de gestão de identidades, autenticação, autorização, e assinatura de documentos eletrônicos. A Infraestrutura de Chaves Públicas Baseada em Atributos (ABPKI) objetiva na realização das seguintes mudanças:

- Eliminar o caminho de certificação de um certificado de usuário-final. Com este elemento, o procedimento de verificação do certificado final adiciona custos (de tempo e financeiramente) e complexidade computacional. Em alguns ambientes, isto seria inviável. A verificação da revogação do certificado também pode ser afetada pela existência do caminho de certificação;

- Eliminar os procedimentos de revogação. A obtenção do conhecimento do estado de revogação de um certificado independente da técnica utilizada (p. ex., LCR, OCSP) nem sempre pode ser realizado de forma rápida, eficiente e mantida atualizada. O estado de revogação ainda prejudica para manter a confiabilidade em assinaturas de documentos eletrônicos a longo prazo;

- Permitir uma alternativa para diminuir nos custos para a obtenção de um certificado digital pelo usuário final e também na implementação

e manutenção exigida em uma ICP (p. ex., mão de obra, ambiente seguro);

- Melhorar a gestão dos atributos:
  - O procedimento para emitir certificado digital não garante que a autoridade certificadora é a mesma autoridade que gerencia os atributos incluídos no certificado. Adicionalmente, o usuário necessita apresentar uma série de documentos para comprovar alguns de seus atributos. Assim como na GId, as entidades responsáveis pelo gerenciamento e armazenamento dos atributos dos usuários devem ser únicas para cada tipo de atributo. A utilização dessas entidades para a validação dos atributos dos usuário aumentam a confiabilidade e evitam a reprodução de cópias destes dados;
- Permitir um maior controle do usuário sobre seus atributos:
  - O uso de um certificado digital obriga o titular a liberar todos os dados nele contidos, sendo que alguns deles não serão necessários para determinada situação. Os usuários devem possuir um maior controle quando apresentam seus atributos, informando apenas os que são necessários para cada situação.

4.3.1 Funcionamento da ABPKI

Esta seção descreve os principais pontos para o bom funcionamento do modelo ABPKI proposto. Nas próximas seções, são descritos os pré-requisitos necessários para que o usuário usufrua do modelo, a composição do certificado e a sua utilização para requisitar recursos de um provedor de serviços.

4.3.1.1 Pré-requisitos

O principal pré-requisito necessário para o funcionamento da ABPKI é a obtenção de um par de chaves pelo usuário, conforme descrito na Seção 4.2.4. Após a criação do par de chaves, o usuário deve registrar a chave pública em todas as APAs que gerenciam ao menos um atributo do usuário. Uma vez que a chave estiver corretamente registrada nas APAS, o usuário poderá criar e auto-assinar os certificados que serão utilizados com os provedores de serviços.

4.3.1.2 Composição do Certificado

O acesso a um recurso de um provedor de serviços é realizado através da análise de um certificado emitido pelo usuário. O certificado tem como principal característica a apresentação dos atributos e a auto-assinatura do usuário. Um certificado auto-assinado da ABPKI contém:

- Chave pública do usuário titular (cp_U);
- Um conjunto de tuplas de atributos. Cada tupla é composta pelo identificador do atributo, ou seja, um Identificador do Objeto (*Object Identifier*) – OID), o valor do atributo, e uma referência da APA responsável pelo seu gerenciamento (URI_{APA});
- Uma validade para o certificado. Apesar da validade ser determinada pelo próprio usuário, o mesmo deve seguir uma política da AN ou APA e esta validade não poderá ser maior do que o menor período de validade do atributo contido no conjunto incluso;
- A assinatura do usuário com a chave privada correspondente à chave pública inclusa.

Sabendo que a chave pública do usuário é o identificador associativo com os atributos dentro das bases das APAs, caso o usuário opte por utilizar diferentes chaves para diferentes APAs, o mesmo deve gerenciar essas diferentes chaves e mapear quais delas estão associadas com as determinadas APAs. Além disso, neste caso, cada certificado irá conter apenas os atributos referentes à APA em questão. A estrutura do certificado é ilustrada pela Figura 10.

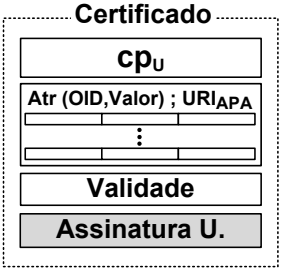


Figura 10 – Estrutura de um certificado na ABPKI.

Os provedores de serviços podem publicar suas políticas de acesso e informar quais atributos mínimos necessários para receber cada tipo de recurso. Esta política tem a intenção de facilitar na criação e apresentação dos certificados pelo usuário. O gerenciamento dos certificados emitidos pelos usuários pode ser realizado via software. O armazenamento dos certificados pode ser localmente ou na nuvem, mas independente do local, o usuário deve manter o controle da posse.

Nas próximas seções serão descritos os dois modos de utilização do certificado no modelo proposto: primeiro o usuário requisita a validação do certificado e depois o envia para o PS (método *push*), ou o usuário apresenta um certificado diretamente para o PS sem estar validado ainda por uma AN (método *pull*).

4.3.1.3 Acessando um Provedor de Serviço via Método Push

No método *push*, o usuário obtém a validação do certificado previamente da requisição de um recurso para um PS. Para obter a validação de um certificado, o usuário deve enviá-lo para uma AN, a qual realiza um protocolo de desafio-resposta para a autenticação do usuário e, caso autenticado, a AN verifica a assinatura do usuário inclusa no certificado. A validade também é verificada no caso do período não exceder o menor dos atributos dentro do conjunto. Caso a assinatura esteja de acordo, assim como a validade, então a AN prossegue para requisitar às APAs a verificação dos atributos do usuário.

A requisição realizada pela AN para cada APA referenciada nas tuplas, é realizada através de um envio de uma estrutura de dados denominada de Validação de Atributos (VA). Uma VA é estruturada contendo a chave pública do usuário e as tuplas de atributos. A VA é assinada pela AN e enviada para a APA correspondente. A Figura 11 mostra a estrutura de uma VA. Para diferentes APAs referenciadas no certificado, a AN deve criar e enviar diferentes VAs.

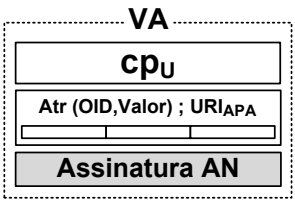


Figura 11 – Estrutura da VA para a validação dos atributos pela ABPKI.

As APAs que receberem uma VA devem verificar a assinatura realizada pela AN e a associação da chave do usuário com os atributos informados. Se todos os valores dos atributos estiverem corretos, a APA assina a VA e retorna a assinatura para a AN. Quando a AN receber a assinatura da APA, ela é verificada. Depois que receber e verificar todas as assinaturas de todas as APAs correspondentes, a AN assina o certificado do usuário. Esta contra-assinatura é retornada ao usuário e ele a anexa ao certificado. O certificado contra-assinado pela AN é denominado de credencial e determina que os atributos relacionados com aquela chave pública foram verificados e validados por uma AN. O usuário poderá utilizá-lo para processos de autenticação e autorização junto ao PS até que seu período de validade expire. O fluxo da obtenção de uma credencial se resume pela Figura 12.

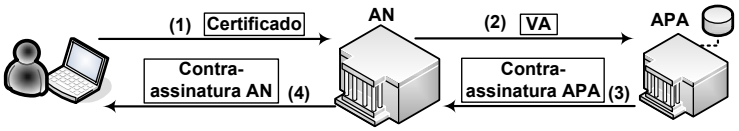


Figura 12 – Validando um certificado auto-assinado e seus atributos pela ABPKI.

No modelo ABPKI, a confiabilidade das ANs e das APAs são gerenciadas pela TSL. Então pode haver o caso de uma AN receber um certificado contendo a referência de uma APA que não está em sua lista de confiança, ou seja, uma APA que esta AN não confia. Como consequência, a AN não poderá validar este certificado do usuário. Uma alternativa para esta situação seria no redirecionamento da requisição de validação do usuário para uma outra AN que confie na determinada APA. Em outras palavras, quando uma AN receber um certificado do usuário e encontra uma APA pela qual não confia, ela pode enviar o certificado para outra AN que confia naquela APA e obter o certificado validada. Este procedimento é ilustrado pela Figura 13. Para prevenir que possíveis recursões venham a ocorrer no processo de verificação, a AN deve conferir a TSL do domínio e enviar o certificado do usuário diretamente para a AN que confia na APA em questão. Se não existir nenhuma AN que confie em uma determinada APA, então os atributos do usuário relativo àquela APA não poderão ser verificados.

4.3.1.4 Acessando um Provedor de Serviço via Método Pull

O método *pull* consiste em deixar a tarefa de validar o certificado do usuário por meio do PS que está sendo requisitado. O PS recebe o certifi-

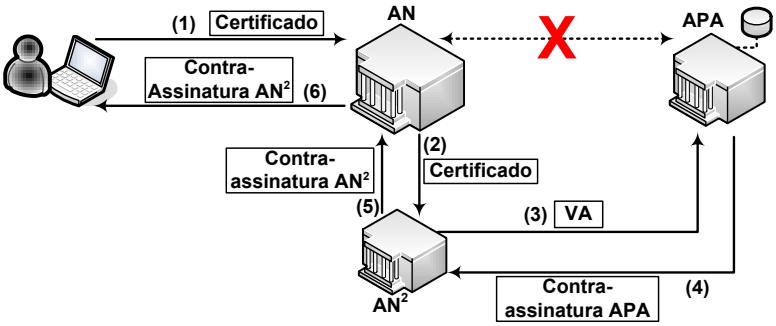


Figura 13 – Redirecionando o certificado do usuário para outra AN validar.

cado pelo usuário, realiza a autenticação do usuário por meio de sua chave pública, e caso autenticado, envia o certificado para uma AN validar. Junto com o certificado, o PS deve enviar também um termo (assinado digitalmente pelo usuário) permitindo que o PS realize esta verificação. A AN verifica a assinatura do termo e inicia a verificação dos dados contidos no certificado, assim como descrito no método *push*. Ao fim da verificação, o PS recebe a assinatura da AN e confirma a autorização do titular do usuário.

4.3.1.5 Verificando uma Credencial

A utilização da credencial (o certificado validado) se faz através do envio do certificado auto-assinado pelo seu titular e da assinatura da AN anexada para o PS. Quando o PS receber a credencial, é necessário que o usuário que está se comunicando seja autenticado. O procedimento de autenticação do usuário ocorre através do uso da chave pública contida na credencial e um protocolo de desafio-resposta. Se o usuário foi autenticado, então o PS verifica a validade da credencial. São verificados a assinatura da AN anexada e o campo "Validade". Caso ambas verificações estiverem corretas, então o PS analisa se os atributos alegados pelo usuário estão formatados de acordo com as políticas para liberar os recursos requisitados.

4.3.1.6 Assinando e Verificando Documentos

A ABPKI pode ser utilizada para validar e certificar assinaturas de documentos eletrônicos. Para validar uma assinatura de um documento, o usuá-

rio deve ter os pré-requisitos descritos na Seção 4.3.1.1. No procedimento da criação de um certificado, além dos atributos a serem incluídos, o usuário também pode incluir o resumo criptográfico do documento que se deseja validar e o algoritmo utilizado. A validação do certificado ocorre de maneira similar ao descrito na Seção 4.3.1.3. A AN aceita como verdade o valor do *hash* do documento incluso, pois a AN apenas está validando a associação do suposto *hash* com os valores dos atributos apresentados naquele exato momento. Após a validação, a credencial resulta na correta associação entre a chave pública, os valores dos atributos e o *hash* do documento. A credencial deve ser anexada ao documento que foi assinado.

A verificação da assinatura do documento pode ser realizada em diferentes etapas. Primeiro, a verificação matemática da assinatura do documento é realizada com o uso da chave pública inclusa no certificado, verificando a auto-assinatura do titular e a comparação do *hash* incluso no certificado e o *hash* calculado do documento. A correção semântica é garantida pela verificação da contra-assinatura do certificado pela AN, pois isto garante que a chave pública e os atributos são confiáveis no momento que a AN o contra-assina. Se o algoritmo criptográfico da assinatura ainda estiver válido, então os atributos do signatário, sua chave pública, e o *hash* do documento também estarão. Se todas as verificações matemáticas e semânticas estiverem corretas, o verificador pode inferir que o documento foi corretamente assinado por uma chave pública além dos atributos do signatário no momento em que o certificado foi validado pela AN.

4.3.2 Análises da ABPKI

Uma das principais vantagens da utilização dos certificados de atributos é prover um melhor gerenciamento dos atributos dos usuário em certificação digital e este também ser amplamente utilizado para procedimentos de autorização e controle de acesso. Portanto, a utilização em conjunto de certificados de chaves públicas e certificados de atributos permite uma melhor amplitude do uso da certificação digital e a diminuição da frequência de certificados revogados por causa da desatualização de algum atributo incluso no certificado de chave pública. Por outro lado, as IGPs baseadas em certificados de atributos X.509 herdam os mesmos problemas contidos em uma ICP X.509.

O gerenciamento dos atributos na ABPKI se difere de uma IGP e ICP X.509 pela eliminação de uma APA emitir certificados de atributos. Se uma APA não tiver mais a responsabilidade em emitir CAs, então toda a infraestrutura e procedimentos de segurança necessária para a emissão dos CAs são

eliminados. A ABPKI também permite que diferentes atributos de diferentes APAs possam estar em um mesmo certificado e a verificação de cada dado é realizada com suas respectivas autoridades. Ao invés do usuário gerenciar diferentes certificados de atributos, o mesmo pode gerenciar um único certificado.

O paradigma centrado no usuário permite que no modelo ABPKI os usuários emitam seus certificados contendo os atributos de suas escolhas de forma mais dinâmica. Uma vez validado os dados de um certificado pela AN (caracterizando-se uma credencial), o verificador (PS) realiza o procedimento de verificação por meio da contra-assinatura da credencial do usuário e a chave pública da AN contida na TSL do domínio. Cada credencial possui um período de validade o qual deve ser aprovado pela AN. Normalmente este período é curto o que possibilita o não uso de mecanismos de revogação.

O suporte da ABPKI em assinatura de documento permite que menos elementos sejam envolvidos, tais como os *timestamps* para validação a longo prazo, CRLs, certificados da cadeia certificadora. Caso seja aplicado em assinaturas a longo prazo, esta vantagem diminui na quantidade de procedimentos necessários para verificação e renovação da validação, podendo uma assinatura ser válida até o momento em que o algoritmo utilizado se torne inválido.

4.4 INFRAESTRUTURA DE CHAVES PÚBLICAS CENTRADA NO USUÁRIO

O modelo ABPKI, descrito na seção anterior, impõe um maior controle no gerenciamento e na apresentação dos atributos dos usuários para os procedimentos de autenticação e autorização do que em relação às ICPs e IGPs X.509. Contudo, ainda há algumas limitações relativas à privacidade do usuário das quais não foram consideradas. Algumas delas são:

- O fornecimento de melhores níveis na privacidade dos atributos dos usuários finais e de seus identificadores contidos nos certificados;
- Os atributos dos usuários são inclusos em texto-claro;
- O uso de uma única chave pública para emitir diferentes certificados. A ABPKI suporta o uso de diferentes chaves para diferentes APAs e consequentemente diferentes certificados, mas esta alternativa impõe uma grande complexidade no gerenciamento destas chaves para o usuário final;

- A possibilidade de mapear diferentes atributos em diferentes certificados de um mesmo usuário já apresentados.

O modelo descrito nesta seção recebeu o nome de "Infraestrutura de Chaves Públicas Centrada no Usuário" (UCPKI). UCPKI é baseada no modelo descrito anteriormente (ABPKI) com foco no aprimoramento da privacidade do usuário. As principais diferenças estão no modo como a geração e o gerenciamento das chaves ocorre e na aplicação de mecanismos para melhorar o suporte das questões relacionadas à privacidade do usuário. A privacidade fornecida pelo modelo UCPKI se concentra em tornar o uso de um identificador do usuário (a chave pública) um elemento mais dinâmico, permitindo que o usuário possa obter uma maior quantidade de identificadores a serem utilizados em diferentes credenciais. Adicionalmente, os identificadores devem ser confidenciais apenas para a autoridade responsável por validar o certificado (AN). O sigilo da chave tem o objetivo de dificultar, aqueles considerados mal intensionados, no mapeamento de diferentes certificados de um mesmo titular contendo diferentes atributos.

A melhoria da privacidade deste modelo ocorre com a adição na forma em que os identificadores são inseridos no certificado e na mudança dos mecanismos para criar o par de chaves do usuário. As chaves do usuário são criadas por meio do uso da Criptografia Baseada em Identidade (CBI). O conceito de CBI foi introduzido por Shamir (SHAMIR, 1985), com o intuito de reduzir a complexidade de sistemas criptográficos eliminando a necessidade de emissão e gerenciamento dos certificados dos usuários. Outra motivação era tornar mais fácil o uso das funções criptográficas para usuários finais, podendo uma mensagem ser cifrada para um outro usuário antes de terem uma interação com qualquer componente do sistema. Em outras palavras, a chave pública de um usuário é baseada em seu identificador (p. ex., nome, e-mail, telefone) e não há um certificado de chave pública para realizar funções criptográficas.

Apesar do trabalho do Shamir ter introduzido o conceito, ele apenas demonstrou o uso para as funções de assinatura baseada em identidade e deixando em aberto o problema de cifragem baseada em identidade. Em 2001, Boneh e Franklin (BONEH; FRANKLIN, 2001), assim como Cocks (COCKS, 2001), trouxeram soluções para o problema. A partir disso, diversas pesquisas e trabalhos relacionados surgiram com propostas de melhorias e algoritmos alternativos (BAEK et al., 2004; LI; KHAN, 2011).

A chave privada correspondente da chave pública (identificador) do usuário em um sistema de CBI é gerenciada e emitida por uma entidade confiável denominada de Gerador de Chaves Privadas (GCP). O usuário, titular do identificador, deve requerer a sua chave privada junto a um GCP. O GCP possui um par de chaves mestras sendo que a chave mestra pública (*cmp*) é

um parâmetro público e divulgado para ser utilizado junto com os identificadores (compondo a chave pública do usuário) para a realização das funções criptográficas. A chave mestra secreta (*cms*) é mantida em posse do GCP com todos os requisitos de segurança exigidos, como em uma ICP. A chave mestra secreta é utilizada para emitir chaves privadas correspondentes aos identificadores após a autenticação dos usuários.

4.4.1 Aprimoramento da Privacidade

A privacidade deve ser fornecida em qualquer sistema que envolve pessoas e o manuseio de seus dados, pessoais ou não. Uma das maneiras de aplicar um melhor nível de privacidade aos usuários de um sistema é o fornecimento de um maior controle sobre os seus dados. Neste caso, se o usuário possuir mais controle sobre o gerenciamento de seus dados e sobre a apresentação deles, ele poderá adicionar e remover seus atributos a qualquer momento e ainda escolher quais deles poderão ser visualizados por outras entidades.

A identificação de um usuário é primordial para os procedimentos de autenticação e autorização. Entretanto, podem haver situações em que o usuário não deseja que esta identificação seja revelada. A revelação da identificação, tanto de forma abrangente (além dos limites do domínio) quanto local (dentro do domínio) podem ter diferentes repercussões. Se uma identificação for reconhecida por qualquer um e em qualquer lugar, então as atividades e os dados referentes ao identificador poderão ser monitorados e rastreados. Caso a identificação realizada dentro de uma organização for reconhecida apenas dentro desta organização, então apenas pessoas autorizadas poderão monitorar o identificador e sob certas políticas. Por outro lado, se a infraestrutura desta organização não for bem estruturada, com requisitos de segurança necessários, então algum mal-intencionado poderá obter os dados referentes ao identificador, monitorar e rastrear as atividades do usuário.

4.4.2 Funcionamento da UCPKI

UCPKI permite, da mesma forma como o modelo ABPKI, que o usuário usufrua de certificados auto-assinados validados por uma autoridade notarial através de dois métodos, *pull* ou *push*. Nesta seção, serão descritos os dois métodos aplicados do modelo, listando as vantagens e desvantagens sobre cada um.

4.4.2.1 Pré-requisitos

Para o usuário adquirir uma credencial, primeiro ele deve ter criado sua chave mestra secreta (*cms*) e a chave mestra pública (*cmp*) correspondente. A *cms* deve ser protegida para o uso, da mesma maneira que uma chave privada do modelo ABPKI. Após a criação do par de chaves mestras, o usuário deve registrar sua chave mestra pública em cada APA na qual possui registro de pelo menos um atributo relativo a sua pessoa. O registro da chave segue a mesma descrição do modelo ABPKI (cf. Seção 4.3.1.1).

A validade do par de chaves mestras é igualmente associada com o algoritmo criptográfico utilizado. Caso algo aconteça com a *cms* do usuário durante seu período de validade, pode-se realizar o mesmo procedimento de troca das chaves descrita pelo modelo ABPKI.

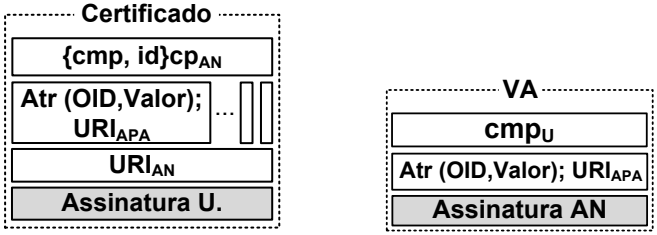
4.4.2.2 Composição do Certificado

O certificado deste modelo diferencia-se com a ABPKI pelo elemento da chave mestra pública e as consequências da sua forma. A estrutura do certificado é ilustrada pela figura 14(a) e possui os seguintes campos:

- A chave mestra pública do titular juntamente com um identificador (*id*) escolhido. Estes dois elementos correspondem com a chave pública do usuário relativo àquele identificador. Estes elementos são cifrados com a chave pública da AN ($\{cmp,id\}cp_{AN}$), pela qual deverá ser a única capaz de validar este certificado;
- Um conjunto de tuplas de atributos, contendo o identificador do atributo e o valor do atributo (*Atr (OID,Valor)*), e a referência da APA responsável por gerenciar o atributo (URI_{APA});
- A referência da AN (URI_{AN}) que será capaz em decifrar a chave mestra pública, o identificador do usuário e validar o certificado;
- Assinatura do usuário titular do certificado em questão.

4.4.2.3 Acessando um Provedor de Serviços via Método Pull

Para acessar e requisitar um recurso do provedor de serviços, o usuário necessita criar um certificado. No momento em que estiver criando o certificado, o usuário deve escolher um *id* para ser um identificador utilizado na



(a) Estrutura de um certificado da UCPKI.

(b) Estrutura de uma VA da UCPKI.

Figura 14 – Estruturas de dados utilizados no esquema UCPKI.

transação com o PS. Com este *id*, o usuário irá criar uma chave privada correspondente ao *id* que será utilizada para funções criptográficas relacionadas com este certificado em específico.

Os PSs possuem políticas indicando os termos do uso de seus recursos, e estas políticas deverão ser mostradas para informar aos usuários os principais atributos necessários. Cada tipo de permissão de acesso deve ser descrita as reais necessidades dos atributos exigidos. De acordo com a política do PS, o usuário irá decidir quais atributos ele incluirá no certificado. Além das tuplas de atributos, o certificado deve informar uma referência da AN que será requisitada a validação (este campo será explicado mais adiante). Por fim, o certificado deve ser assinado por seu titular, com o uso da chave privada referente ao *id* escolhido (cpr_{id}).

A utilização do certificado auto-assinado para requisitar um recurso do provedor de serviço por meio do método *pull* inicia-se pela criação e apresentação de um certificado auto-assinado para o PS. Como o certificado do usuário ainda não está validado, então o PS deve enviar para a AN referenciada no certificado. A AN, quando receber o certificado, deve decifrar o campo $\{cmp,id\}cp_{AN}$ com a sua chave privada para obter a chave mestra pública e o identificador do usuário. Utilizando a *cmp* e o *id* do usuário texto claro, a AN verifica a assinatura no certificado. Se a assinatura estiver correta, a AN se comunica com a APA correspondente aos atributos apresentados nas tuplas.

Um certificado pode conter diversas tuplas de atributos com atributos referentes a diferentes APAs em cada uma e cabe a AN se comunicar com cada uma delas para realizar a verificação de seus valores. Sendo assim, a AN realiza a verificação por meio da requisição da validação dos atributos (VA). A Figura 15 ilustra o fluxo da comunicação do modelo descrito até agora.

A estrutura de dados da VA contém a *cmp* do usuário e o subconjunto

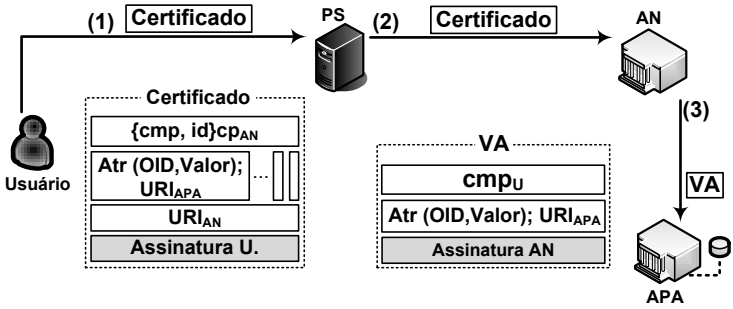


Figura 15 – Fluxo da apresentação e validação de um certificado pelo modelo UCPKI.

de tuplas associados com a mesma APA. Para cada APA, uma VA específica deve ser criada. As VAs são assinadas com a chave privada da AN. A APA quer receber uma VA, deve verificar a assinatura da AN e os dados do usuário. Se for confirmada a veracidade dos atributos, a APA contra-assina a VA e retorna a contra-assinatura para a AN. Depois de receber todas as assinaturas de confirmação de todas as APAs envolvidas, a AN cria e determina alguns elementos que irão ser anexados ao certificado do usuário e compor a sua credencial.

Um dos elementos é a validade para utilização dessa credencial. Esta validade deve respeitar as políticas das APAs e não deve ter um período maior do que o menor período de validade entre os atributos pertencentes ao conjunto de tuplas de atributos do certificado. Em seguida, a AN cria um *nonce* para auxiliar no mecanismo de desafio-resposta e a autenticação anônima do usuário para o PS. Para manter o sigilo do *nonce*, ele deve ser cifrado com a chave pública correspondente ao *id* do titular utilizado no certificado, ou seja, a *cmp* e o *id*. Desta forma, apenas este usuário poderá saber o valor do *nonce*.

O *nonce* também deve ser de conhecimento do PS que o usuário estiver acessando. Então a AN também deve cifrar o valor real do *nonce* com a chave pública do PS. Desta forma, apenas o titular desta credencial e o provedor de serviços que irá verificar esta credencial reconhecerão o verdadeiro valor deste *nonce*. Ambos os valores dos *nonces* cifrados são anexados ao certificado. E, para finalizar a criação dos elementos da credencial do usuário, a AN contra-assina toda a estrutura. A credencial do usuário é retornada para o PS que requisitou a verificação do certificado. O PS mantém uma cópia da credencial e a retorna para o titular. Estes procedimentos podem ser visualizados na Figura 16, onde os passos (4), (5) e (6) os representam.

Agora que o usuário já possui seus atributos validados e o provedor

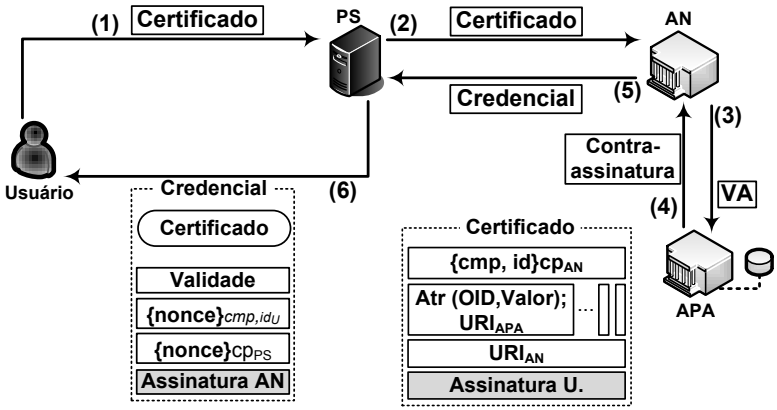


Figura 16 – Criação da credencial do usuário na UCPKI.

de serviços já sabe disso, o PS necessita saber se a pessoa quem criou o certificado é a mesma que está se comunicando. Esta autenticação ocorre de forma anônima, preservando a privacidade do usuário perante o PS. O procedimento é realizado pelo uso dos *nonces* criados pela AN e inserido na credencial. Sendo assim, o usuário decifra o *nonce* ($\{nonce\}cmp, id_U$) utilizando a chave privada relativa ao *id* utilizado no certificado. Com o *nonce* em texto claro, o usuário concatena com o valor da validade da credencial e cifra o resultado utilizando a chave pública do PS. Este resultado é enviado para o PS. O procedimento de concatenação serve apenas para prevenir que o mesmo conteúdo do *nonce* cifrado com a chave pública do PS na credencial seja utilizado indevidamente. O PS decifra este texto cifrado recebido e guarda o valor temporariamente. Em seguida, o PS decifra o *nonce* incluso na credencial do usuário.

Caso o valor do texto em claro recebido pelo PS for igual ao valor do *nonce* decifrado e concatenado com o valor do campo "Validade" da credencial, então deduz-se que: o usuário quem criou o certificado é o mesmo que possui a chave mestra secreta, i.e., o mesmo usuário que possui a capacidade de criar a chave privada para assinar o certificado com o *id* relacionado; os valores dos atributos foram validados pela AN e pelas APAs correspondentes; e o usuário está autorizado para ter acesso aos recursos de acordo com as políticas da AN. Assumimos que a *cms* do usuário e as derivações das chaves secretas para cada *id* (cms_{id}) são intransferíveis. O procedimento de autenticação do usuário por meio do *nonce* são representados pelas etapas (7) e (8) da Figura 17.

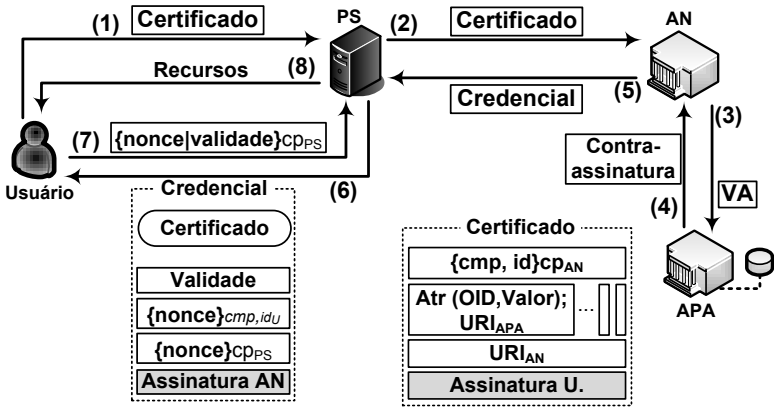


Figura 17 – Autenticação do usuário com o *nonce* de sua credencial.

A chave mestra pública e o identificador utilizados na UCPKI são cifrados com a chave pública da AN para inibir que as credenciais emitidas possam ser identificadas e mapeadas para um mesmo titular. Apesar do modelo não especificar diretamente a confidencialidade dos atributos nas credenciais, eles podem ser cifrados com a mesma chave privada correspondente ao *id* do usuário utilizados na emissão do certificado. Neste caso, para que os atributos sejam visualizados pelo PS, a AN decifraria os atributos no certificado e adicionaria os atributos cifrados com a chave pública do PS na credencial.

4.4.2.4 Acessando um Provedor de Serviços via Método Push

Com algumas similaridades com o método *pull*, o usuário deve ter em mãos seu par de chaves mestras e criar um certificado. A validação do certificado ocorre por uma requisição direta com a AN, onde o usuário deve apresentar seu certificado para a AN e também informar para qual PS o mesmo deverá ser utilizado ou repassar a chave pública do PS. Isso servirá para que a AN cifre o *nonce* com a chave pública do PS correspondente. A AN também poderá obter a chave pública do PS informado por meio de uma referência cedida pelo usuário.

Assim como no método *pull*, a AN decifra a *cmp* e o *id* do usuário, verifica a assinatura do certificado, cria as VAs necessárias e envia para as APAs correspondentes. Após as verificações e o recebimento das assinaturas das APAs, a AN cria um *nonce*, cifra com a *cpm* e o *id* do usuário e também

cifra o texto em claro do *nonce* com a chave pública do PS. A AN anexa os dois valores cifrados ao certificado e assina toda a estrutura, gerando assim a credencial. Depois de possuir sua credencial em mãos, o usuário poderá utilizá-la com o referente provedor de serviços.

4.4.3 Análises da UCPKI

Na UCPKI, a inclusão da chave mestra pública e o *id* do usuário cifrados pela chave pública da AN dentro do certificado necessita de um cuidado e um gerenciamento por parte do titular para reconhecer qual foi o *id* atribuído para aquele certificado. Como solução deste problema, o usuário deve gerenciar (em uma espécie de tabela) a indicação de qual *id* está associado ao certificado criado. Apesar do uso do procedimento de cifragem dos dados trazer sigilo para o usuário, quanto maior o número de processos de cifragem, maior será a complexidade computacional exigida, tanto para o usuário quanto para a AN.

A UCPKI e as funções criptográficas utilizadas podem exigir um poder de processamento maior do que um dispositivo de *smartcard* existente no mercado atual suporta. Além da geração das chaves, o dispositivo deve suportar o armazenamento de credenciais para facilitar o usuário. Caso isso não seja possível, uma alternativa de uso de dispositivo criptográfico seria um cartão do tipo *microsd* e utilizados em *smartphones*. Em conjunto, os dois dispositivos possuem um poder de processamento e armazenamento maior do que um *smartcard*.

O anonimato do usuário é alcançável se somente se o usuário não reutilizar um mesmo *id* e no conjunto de tuplas de atributos não tiver nenhum atributo identificador (p. ex., nome, e-mail). A autenticação anônima do usuário perante o PS realizada por meio dos *nonces*, permite auxiliar o titular da credencial a não revelar sua chave pública e o identificador utilizado. Por outro lado, a AN deverá ser informada de qual provedor de serviços o usuário utilizará a credencial. Outra consequência do uso dos *nonces* na UCPKI é que cada credencial irá funcionar apenas para um PS específico.

4.5 UCPKI COM AUTENTICAÇÃO ANÔNIMA

O modelo UCPKI descrito na seção anterior, utiliza-se de mecanismos para que a autenticação do usuário ocorra sem que ele revele a sua chave pública ou seu identificador para o PS. Apesar disso, a solução utilizada no modelo não é ótima, pois obriga o usuário a informar para a AN qual o pro-

vedor de serviços ele irá acessar, ou ao menos a chave pública do PS. Este conhecimento adquirido pela AN pode prejudicar a privacidade do usuário.

O modelo apresentado nesta seção tem como objetivo melhorar os pontos negativos do modelo UCPKI. O nível de privacidade deve ser melhorado por meio da apresentação dos atributos do usuário de forma cifrada e a utilização de outro mecanismo para prover a autenticação anônima do usuário com o provedor de serviço. Este mecanismo deve eliminar a necessidade da AN saber a respeito de qual PS o usuário irá acessar. O mecanismo aplicado no modelo ocorre por meio de provas de conhecimento zero (do inglês *zero-knowledge proofs*). Com a utilização destas provas, o provedor de serviços poderá autenticar o titular da credencial sem a necessidade de saber sua identificação. Por estes motivos, este novo modelo foi denominado de *User-Centric Public Key Infrastructure with Anonimous Authentication* (UCPKI-AA), ou "Infraestrutura de Chaves Públicas Centrada no Usuário com Autenticação Anônima".

4.5.1 Funcionamento da UCPKI-AA

A UCPKI-AA é semelhante ao UCPKI. As principais diferenças são a inclusão dos atributos cifrados no certificado e a realização da autenticação anônima *zero-knowledge*. Por causa destes novos elementos, o fluxo para a validação do certificado, emissão da credencial e a autenticação do usuário variam um pouco. Nesta seção, são descritos os procedimentos da emissão, validação e utilização do certificado auto-assinado no modelo UCPKI-AA.

4.5.1.1 Pré-requisitos

Assim como no modelo UCPKI, o usuário deve criar seu par de chaves mestras. Neste modelo, o usuário deve registrar tanto a sua *cmp* quanto um identificador (*id*) em cada APA em que possui registro de pelo menos um atributo. O usuário pode registrar diferentes *ids* para diferentes APAs. Os requisitos de segurança e armazenamento se mantêm os mesmos. A revogação da chave pode ser realizada da mesma forma da UCPKI. Caso a *cms* ainda esteja segura e válida, o usuário pode requisitar a troca do *id* registrado na APA. O procedimento desta troca poderá ser realizado através de um procedimento de desafio-resposta entre o usuário e a APA com o uso dos pares de chaves. Após a troca do *id* em uma determinada APA, todas as credenciais emitidas com referência a esta APA, se tornará incapaz de ser validada.

4.5.1.2 Composição do Certificado

Cada certificado deve conter a chave pública correspondente da assinatura, ou seja, a chave mestra pública e o identificador escolhido. A *cmp* e o *id* são, juntos, o identificador do usuário para aquele certificado específico. Por possuir características de identificação, esta informação deve ser protegida para que apenas a autoridade responsável possa visualizar seu verdadeiro valor. Logo, o conjunto *cmp,id* deve ser cifrado com a chave pública da AN ($\{cmp,id\}cp_{AN}$).

Assim como nos modelos anteriores, os atributos são apresentados em forma de tuplas. Entretanto, no modelo UCPKI-AA os valores dos atributos devem estar protegidos para que apenas a APA responsável consiga visualizá-los. Como solução, os atributos são cifrados com a chave privada do usuário correspondente a um identificador específico, que é obtida através do uso da chave mestra secreta (*cms*) e o *id* que foram registrados nas APAs. Caso diferentes identificadores sejam registrados para diferentes APAs, então o usuário deve gerenciar este mapeamento, lembrando qual identificador deve ser utilizado para cada APA.

Devido ao fato de que os valores dos atributos são cifrados e apenas a APA responsável é capaz de visualizá-los, é necessário apresentar ao PS uma prova indicando quais são os atributos dentro do certificado. Esta prova é determinada pelo valor do resumo criptográfico (*hash*) de cada atributo. No momento da criação do certificado, além dos atributos cifrados, o usuário também calcula e insere os resumos criptográficos dos valores dos atributos.

De acordo com as propriedades de um algoritmo que calcula o resumo criptográfico de uma mensagem, se a mensagem não sofrer nenhuma modificação e o cálculo for realizado com o mesmo algoritmo diversas vezes, o resultado vai ser sempre igual (HOUSLEY; POLK, 2001). Com base nessa premissa, um usuário poderá incluir seu nome como atributo em diferentes certificados e o valor dos resumos serão iguais em todos os certificados com este atributo incluso. Um mal-intencionado sabendo que o valor do *hash* se refere ao mesmo atributo do usuário, poderá rastrear todos os certificados emitidos pelo mesmo usuário. Para resolver este problema, no momento em que o usuário estiver emitindo e incluindo os atributos no certificado, o mesmo deve incluir um *timestamp* (carimbo do tempo) como sendo parte do atributo. O tempo é uma informação que sempre será diferente a cada momento e, consequentemente, o valor do *hash* do atributo junto com o *timestamp* será sempre diferente em cada certificado. O algoritmo do resumo criptográfico utilizado é o mesmo entre todas as entidades e definido na TSL.

O certificado do modelo UCPKI-AA é ilustrado pela figura 18. Os campos de um certificado podem ser resumidos da seguinte maneira:

- $\{cmp,id\}cp_{AN}$: chave mestra pública do usuário e um identificador utilizado para assinar o certificado;

- URI_{AN}: referência da AN que possui a chave privada correspondente para decifrar a *cmp* e o *id*;

- Atr$\{$(OID,Valor),*timestamp*$\}$*cms,id'*: um elemento da tupla de atributos, composto com um conjunto de atributos e cada atributo é representado pelo OID, valor, e *timestamp* do momento da criação do certificado. Os atributos com o *timestamp* são cifrados com a chave mestra secreta do usuário e o identificador (*id'*) que foi registrado na APA responsável;

- H(Atr(Valor),*timestamp*): resultado da função *Hash* do valor do atributo junto com o mesmo *timestamp* incluso no primeiro elemento da tupla [1];

- URI_{APA}: terceiro elemento da tupla e determina uma referência da APA responsável pelo gerenciamento dos atributos inseridos nesta mesma tupla;

- Assinatura Usuário: valor da assinatura realizada pelo usuário utilizando a chave privada originada pela chave mestra secreta correspondente à *cmp* e ao *id*, ambos incluídos no primeiro campo do certificado.

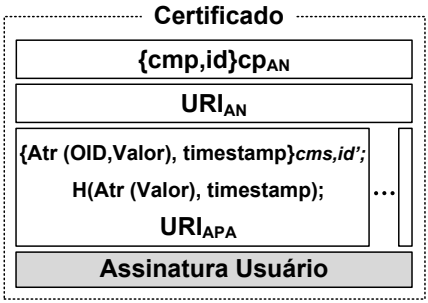


Figura 18 – Estrutura de um certificado na UCPKI-AA.

[1] É importante ressaltar que o *timestamp* pode ser baseado no relógio do dispositivo do usuário.

4.5.1.3 Acessando um Provedor de Serviços via Método Pull

Primeiro, o usuário deve emitir seu certificado auto-assinado. Ao emitir o certificado, o usuário deve escolher um *id* para criar uma chave privada correspondente. Esta chave privada relativa ao identificador (*cms,id*) é utilizada para assinar este certificado. A chave pública correspondente (*cmp,id*) deve ser inclusa de forma cifrada com a chave pública de uma AN. A escolha da AN dependerá das preferências do próprio usuário ou do modelo de negócio aplicado. Uma referência da AN escolhida também devem ser inclusa. O usuário inclui as tuplas de atributos e depois assina o certificado.

O usuário, com o seu certificado emitido, deve entregá-lo para o PS. Sabendo que o certificado ainda não foi validado, o PS o envia para a AN referenciada no certificado. A AN, ao receber o certificado do usuário, decifra o campo $\{cmp,id\}cp_{AN}$ com sua chave privada. Através da chave mestra pública e o *id* do usuário em texto-claro, a AN verifica a assinatura do certificado. Se a assinatura estiver correta, a AN se comunica com as APAs correspondentes aos atributos apresentados nas tuplas.

Podem haver diferentes tuplas com referências para APAs distintas e cabe a AN se comunicar com cada uma delas para realizar a verificação dos valores dos atributos. Sendo assim, a AN realiza a verificação por meio do envio da requisição de validação dos atributos (VA). A estrutura de dados da VA e o fluxo da comunicação entre o usuário, PS, AN e APA descritos até aqui podem ser visualizados na Figura 19. A estrutura de dados VA é semelhante ao modelo UCPKI, contendo a *cmp* do usuário e as tuplas de atributos correspondentes para uma APA.

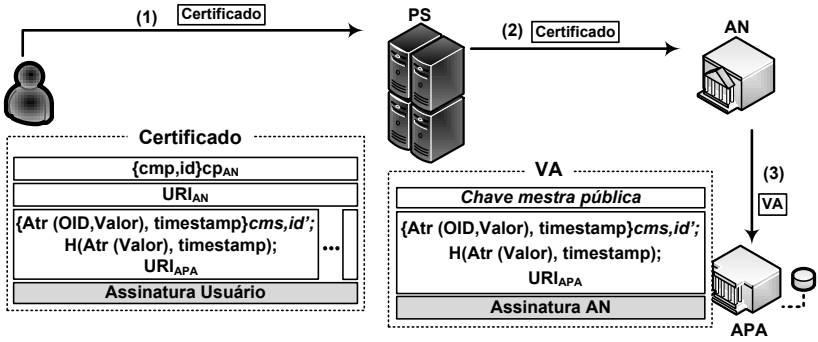


Figura 19 – Acessando um recurso do PS através do método *pull* da UCPKI-AA.

Quando a APA recebe uma VA, a sua assinatura é verificada. Utilizando a chave mestra pública do usuário, a APA realiza a busca dos dados do usuário nos registros e utiliza o identificador (*id'*) cadastrado para decifrar os valores dos atributos da VA. Com os atributos em texto claro, a APA pode verificar se os valores dos atributos estão corretos. Se a APA confirmar a veracidade dos atributos, então ela deverá verificar o valor do resumo criptográfico do atributo calculado pelo usuário. Esta verificação ocorre utilizando o valor do atributo em texto-claro e o *timestamp* inclusos na tupla. Depois que todos os valores forem verificados corretamente, então a APA deve contra-assinar a VA usando sua chave privada e enviá-la para a AN.

Depois de receber todas as assinaturas das APAs envolvidas, a AN deve criar e anexar os elementos para auxiliar na autenticação anônima do usuário com o PS. A AN gera os atributos públicos e privados do protocolo de autenticação *zero-knowledge*. Os atributos públicos do protocolo *zero-knowledge* (AP-PZK) são anexados em texto-claro no certificado. Já os atributos privados do protocolo *zero-knowledge* (APr-PZK) devem ser visíveis apenas pelo titular do certificado. Então, os atributos privados do protocolo devem ser cifrados utilizando a chave mestra pública e o *id* do usuário que foram utilizados no certificado e o resultado anexado ao certificado. Por fim, a AN anexa um *timestamp* e assina todos os elementos anexados (incluindo o certificado). O certificado validado e todos estes novos dados caracterizam-se como sendo uma credencial do usuário. A estrutura da credencial pode ser visualizada pela Figura 20.

A credencial do usuário é retornada para o provedor de serviços, sendo representada na Figura 20 (passo 5). O PS mantém uma cópia consigo e retorna a credencial para o usuário (passo 6). Agora que o usuário já possui seus

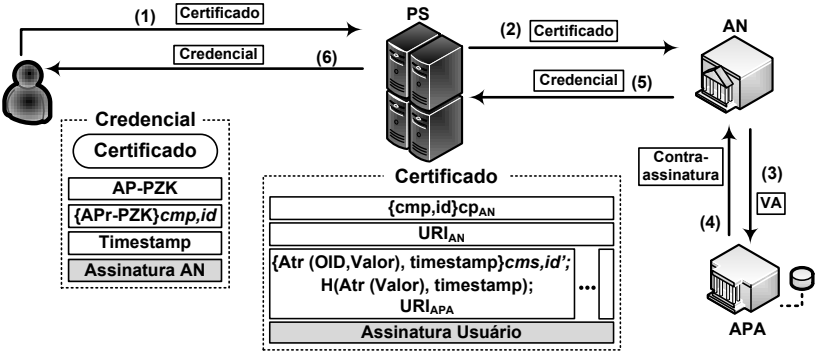


Figura 20 – Validação do certificado e emissão da credencial na UCPKI-AA.

atributos validados e o PS já sabe disso, o PS necessita saber se o usuário que criou o certificado é o mesmo com quem está se comunicando. O procedimento é realizado utilizando os atributos do protocolo *zero-knowledge* criado pela AN.

O protocolo *zero-knowledge* pode ser realizado com uma iteração com mais ou menos repetições, dependendo do protocolo utilizado. Para iniciar uma iteração, o usuário deve decifrar os atributos privados do protocolo (APr-PZK) inclusos na credencial e utilizar o texto em claro para provar sua autenticidade com o PS. O PS, no protocolo de autenticação anônima do usuário, utiliza-se dos atributos públicos do protocolo dentro da credencial do usuário. Se a verificação da prova for afirmativa, então o PS pode concluir que o usuário em questão está autenticado. A Figura 21 mostra esta etapa (passo 7).

Neste momento, o PS sabe que o usuário que está se comunicando é autêntico e que os atributos inclusos na credencial foram validados e pertencem a este usuário. Entretanto, o PS não sabe quais são os atributos de fato que foram validados. Então, o usuário deve informar para o PS os valores dos atributos que ele apresentou para a validação (passo 8). Adicionalmente, o usuário deve informar também os *timestamps* de cada conjunto de atributos. Com os valores dos atributos e os respectivos *timestamps*, o PS pode calcular os resumos criptográficos e compará-los com os valores dos resumos contidos na credencial. Se os valores coincidirem, então estes atributos são os mesmos que foram validados. Depois desta conclusão, o PS poderá liberar os recursos requeridos ao usuário, ilustrado pelo passo 9 da Figura 21.

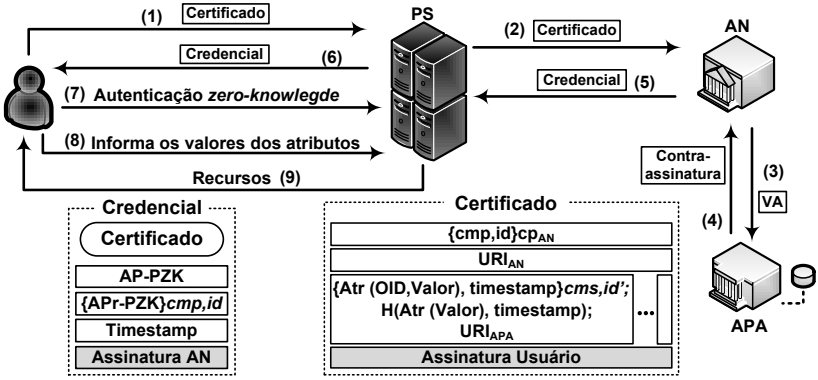


Figura 21 – Usuário acessando um recurso pela UCPKI-AA.

4.5.1.4 Acessando um Provedor de Serviços via Método Push

Com algumas similaridades com o método *pull*, ao invés de enviar o certificado para o PS, o usuário envia para a AN. A partir deste passo, os procedimentos são os mesmos até o momento em que a AN finaliza a emissão da credencial. Neste caso, por não envolver o PS, a AN retorna a credencial para o usuário.

Com a credencial em mãos, o usuário poderá utilizá-la a qualquer momento. Caso o PS possua em suas políticas alguma regra limitando um período de validade para a aceitação da credencial, o usuário deve tomar cuidado com esta restrição. Por exemplo, caso o usuário possua uma credencial que foi emitida há mais de seis meses e o PS aceitar apenas aquelas com um período máximo de 5 meses a partir da data de emissão (*timestamp* incluso pela AN), então esta credencial não será aceita pelo PS. Os procedimentos de apresentação da credencial para o PS até a liberação dos recursos são os mesmos apresentados no método *pull* (Seção 4.5.1.3). A Figura 22 ilustra um usuário acessando um recurso do PS através do método *push*.

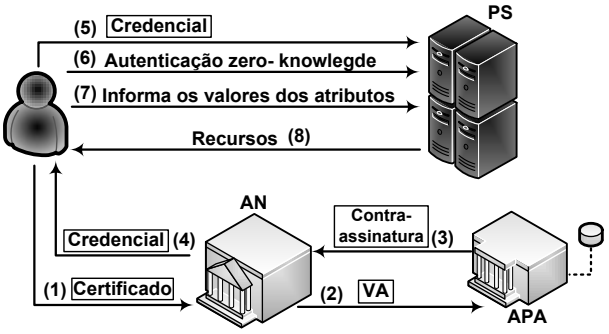


Figura 22 – Fluxo do método *push* do modelo UCPKI-AA.

4.5.2 Análises da UCPKI-AA

O modelo UCPKI-AA permite, por meio da utilização do protocolo de provas *zero-knowledge*, a autenticação do titular da credencial ocorre de forma anônima e mais simples do que na UCPKI. A eliminação da utilização dos *nonces* permite eliminar a obrigatoriedade do usuário em informar a chave pública do PS para a AN, deixando de saber em qual PS o usuário irá utilizar a credencial. A credencial criada na UCPKI-AA permite a sua

utilização por mais de um PS (caso o usuário queira).

A UCPKI-AA não determina qual o protocolo de provas *zero-knowledge* deve ser utilizado na autenticação. A escolha do protocolo é definida com base nas características de cada um, tal como a quantidade de interações mínimas necessárias para ser considerada verdadeira o conhecimento do segredo pelo usuário, a quantidade de recursos de memória e processamento necessários, tempo levado para autenticar o usuário, entre outros.

Uma desvantagem da UCPKI-AA em relação aos modelos anteriormente descritos, está na grande quantidade de procedimentos criptográficos utilizados para prover privacidade para os dados do usuário. Além de cifrar a chave mestra pública e o identificador utilizado no certificado, todos os atributos inseridos no certificado também devem passar por funções de cifragem e, consequentemente, funções de *hash*. No processo de validação dos dados do certificado, os dados precisam ser decifrados e os valores dos resumos criptográficos conferidos. Estes procedimentos requerem que o dispositivo utilizado possua um poder computacional e memória suficientes para que o tempo gasto não seja elevado.

4.6 MODELO DE NEGÓCIO

Diferentemente da ICP X.509, as três alternativas propostas neste trabalho permitem a aplicação de modelos de negócios mais flexíveis. Ao invés da aplicação de uma única tarifa para obtenção de um certificado a longo prazo (p. ex. 3 anos) e independente da frequência de seu uso, os preços pela validação dos certificados (pelas AN ou PS), através do método *pull* ou *push*, podem ser praticados de forma mais justa e proporcionais a quantidade de uso de cada serviço.

4.7 CONCLUSÃO

Neste capítulo, foram apresentados três propostas de modificações de ICPs com os objetivos de melhorar o gerenciamento dos atributos dos usuários e aprimorar a sua privacidade com a utilização do certificado. Os modelos ABPKI, UCPKI e UCPKI-AA apresentados possuem uma arquitetura em comum sem perder a generalidade de uma ICP. Na ABPKI, o usuário utiliza-se de chaves criptográficas assimétricas (como aquelas utilizadas em uma ICP X.509) para emitir certificados auto-assinados contendo os atributos de sua escolha. O certificado é utilizado para requerer recursos dos PSs. As chaves são criadas pelo próprio usuário e a parte pública é registrada nas autoridades

provedoras de atributos.

A UCPKI é baseada na ABPKI, mas diferenciando-se na utilização da criptografia baseada em identidades para prover um maior dinamismo no uso de diferentes pares de chaves. As chaves são derivadas a partir de um par de chaves mestras e diferentes identificadores. Neste modelo, a privacidade é melhorada permitindo que a autenticação do usuário com o provedor de serviço ocorra de forma anônima. O método de autenticação ocorre por meio do uso de *nonces*. Adicionalmente (como opção), o modelo permite que o usuário inclua nos certificado os atributos de forma cifrada, ou seja, dando sigilo para os atributos para que apenas o PS possa visualizá-los.

Diferentemente das outras propostas, a UCPKI-AA utiliza-se de protocolos de provas *zero-knowledge* para fornecer uma melhor autenticação anônima em relação à UCPKI. Além disso, seu protocolo obriga que os atributos sejam inclusos nos certificados de forma cifrada para serem visíveis apenas pelas APAs responsáveis e a utilização dos resumos criptográficos dos atributos para servirem como prova de validação para os provedores de serviços. Diante das características em comum e as peculiaridades entre si, o próximo capítulo irá descrever as análises entre os modelos propostos e alguns sistemas existentes.

5 ANÁLISES COMPARATIVAS

5.1 INTRODUÇÃO

Na seção anterior, foram apresentadas três alternativas de modificações para o modelo tradicional de ICP com foco em um sistema de gerenciamento de identidades em infraestrutura de autenticação e autorização. Com o uso de chaves criptográficas e provendo um paradigma centrado no usuário, as propostas fornecem um melhor controle para o usuário final tanto na emissão de certificados quanto na apresentação de seus atributos para os PSs.

As autoridades notariais e provedoras de atributos realizam a segurança na validação dos certificados e no gerenciamento dos atributos dos usuários, respectivamente. Todos os modelos apresentados possuem pontos positivos e negativos entre si. Além dos três modelos apresentados, esta seção realiza análises comparativas entre uma ICP X.509, uma infraestrutura de gerenciamento de privilégios baseada em certificado de atributos (IGP X.509) e alguns dos principais sistemas, protocolos e projetos existentes. Estes sistemas são: OpenID, Shibboleth, U-Prove e Idemix. O OpenID e o Shibboleth foram escolhidos por serem amplamente utilizados como sistema de autenticação e autorização e possuem limitações quanto aos recursos para aplicar privacidade para os usuários. Já o U-Prove e o Idemix foram projetados com o princípio de aprimorar a privacidade do usuário no âmbito da infraestrutura de autenticação e autorização.

5.2 COMPARAÇÃO COM AS ABORDAGENS EXISTENTES

5.2.1 ICP X.509 e IGP X.509

O Quadro 1 apresenta as principais vantagens e desvantagens do modelo de ICP X.509, ICP com a utilização de certificados de atributos e das propostas deste trabalho. As principais similaridades entre os modelos estão no uso de chaves criptográficas, suas funções providas (cifragem, decifragem e *hash*) e a assinatura digital para prover confidencialidade, integridade, autenticidade e não repúdio dos dados envolvidos. Entretanto, os modelos se diferem principalmente na composição das autoridades, no nível de privacidade fornecido para o usuário e na complexidade computacional exigida pelos procedimentos. Adicionalmente, há uma consequência na diferenciação da complexidade e dos custos de implantação e manutenção das infraestruturas.

Quadro 1 – Comparação entre os modelos: Aspectos Gerais.

Modelo	Vantagens	Desvantagens
ICP X.509	Padrão mais difundido, amplamente especificado e utilizado.	Instalação e manutenção complexa, excesso de recursos necessários (carimbos de tempo, consultas de revogação, etc.), emissão de certificados limitada às políticas das ACs, não oferece privacidade para o titular.
ICP e IGP X.509	Padrão difundido e amplamente especificado, melhor gerenciamento dos atributos (do que apenas em ICP).	Mesmos desafios de uma ICP, cada CA possui atributos de uma única APA, necessidade de cada APA gerenciar os CAs e não oferece requisitos sobre privacidade.
ABPKI	Simplificação para emissão do certificado, maior controle e gerenciamento dos atributos pelos usuários, menos procedimentos para verificação da confiabilidade do certificado.	Ainda há necessidade de definição e publicação de padrões, maior responsabilidade para o usuário, limitação no fornecimento da privacidade do dados.
UCPKI	Aprimora a privacidade da ABPKI pelo sigilo dos identificadores e nos atributos (opcional), uso dinâmico de diferentes pares de chaves (CBI), autenticação anônima do usuário com o PS (com *nonces*).	Complexidade computacional elevada (funções de cifragem e decifragem), a AN reconhece qual PS o usuário irá acessar, limite de uso de uma credencial por PS.
UCPKI-AA	Aprimora a privacidade da UCPKI, autenticação anônima com protocolo de *zero-knowledge*, a AN não reconhece qual PS acessado pelo usuário, sigilo dos atributos obrigatório, pode usar uma credencial em vários PSs.	Aumento da complexidade computacional exigida (fator tempo também pode ser aumentado), pode necessitar de várias interações para realizar a autenticação anônima.

5.2.1.1 Privacidade

As alternativas de ICP propostas se diferenciam principalmente pelo aprimoramento da privacidade fornecida para o usuário final em relação às ICPs e IGPs X.509. O Quadro 2 resume as características a respeito da privacidade do usuário, comparando se nos modelos existem ou não as características analisadas e se é possível ou não a ação de cada uma delas.

A primeira característica comparada é a possibilidade do usuário obter mais controle sobre seus atributos, ou seja, a capacidade do titular dos atributos decidir quais devem ser incluídos em um certificado ou apresentados para uma entidade. Todos as alternativas de ICP apresentadas possuem esta característica devido o uso do paradigma centrado no usuário. A UCPKI-AA ainda se diferencia das demais pela possibilidade do usuário restringir a vi-

Quadro 2 – Comparação da privacidade fornecida.

Características/Ações	Modelos			
	ICP+IGP	**ABPKI**	**UCPKI**	**UCPKI-AA**
Controle dos atributos pelos usuários	Não	Sim	Sim	Sim
Apresentar atributos parciais	Não	Sim	Sim	Sim
Tornar os atributos confidenciais	Não	Não	Possível	Sim
Usar diferentes chaves criptográficas	Não recomendável (custoso)	Não recomendável (complexo)	Sim (CBI)	Sim (CBI)
Tornar os identificadores confidenciais	Não	Não	Sim	Sim
Mapear os atributos das credenciais	Sim	Sim	Possível	Não
Rastrear o usuário	Sim	Sim	Possível	Não
Tipo de identificação do usuário com o PS	Identificável	Pseudônimo	Anônimo (*nonce*)	Anônimo (*zero-knowledge proof*)

sualização de um atributo para um PS, ou seja, não necessariamente todos de uma credencial serão visíveis para o PS. Isto permite que a mesma credencial possa ser utilizada mais de uma vez em diferentes PSs e ainda haver atributos inclusos na credencial e desconhecidos pela terceira parte.

Além de poder decidir quais atributos o usuário deseja incluir em seu certificado, o atributo pode ser apresentado parcialmente nas três alternativas de ICP propostas. Ao invés de informar a data de nascimento, o titular pode informar que possui idade maior que dezoito por exemplo. Outra característica que foi implantada, apenas na UCPKI (como opcional) e na UCPKI-AA (obrigatoriamente), é a confidencialidade dos atributos inclusos nos certificados. A confidencialidade (por meio das operações de cifragem) permite que, se alguém não autorizado obter o certificado ou a credencial do usuário, este não será capaz de ler os valores dos atributos.

A confidencialidade dos atributos nos certificados da UCPKI e da UCPKI-AA ainda se diferem em quem e como poderá acessar os valores dos atributos. Na UCPKI, é uma AN específica que poderá visualizar os atributos e, posteriormente, apenas um PS que a credencial será utilizada. Na UCPKI-AA, somente as APAs responsáveis pelo gerenciamento dos atributos inclusos no certificado poderão visualizar os atributos. Adicionalmente, na UCPKI-AA, o PS visualiza a prova de que o atributo informado pelo titular foi verificado pela AN. Esta prova é o resumo criptográfico do valor do atributo e um *timestamp* calculado pelo usuário e verificado pela APA.

Com este mesmo intuito de proteger o usuário e seus dados de terceiros não autorizados, a confidencialidade dos identificadores utilizados nos certificados também foi aplicada na UCPKI e UCPKI-AA. A identificação do usuário está diretamente associada no modo como o usuário é autenticado. Nos modelos ICP X.509 e ABPKI não há confidencialidade dos identificadores (chave pública) nos certificados. Embora a chave pública atue como um pseudônimo, nos certificados digitais X.509 existe a obrigatoriedade de identificar unicamente o titular pelo campo "Distinguished Name". Na ABPKI o usuário pode não querer incluir alguns atributos e caso não inclua algum que possa identificá-lo, então a chave pública funcionará como um pseudônimo.

Nos modelos UCPKI e UCPKI-AA, a confidencialidade dos identificadores existe em duas situações: com a AN e com o PS. A confidencialidade do identificador do usuário com a AN é realizada pela função de cifragem da chave pública a ser incluída no certificado por meio da chave pública da AN que irá validar o certificado. Esta confidencialidade permite que a associação entre os atributos inclusos no certificado e o identificador utilizado seja visualizada penas pela AN. Entretanto, caso a AN receba certificados contendo um mesmo identificador, alguém mal-intencionado poderá mapear este identificador com os atributos (diferentes ou iguais) contidos nos certificados recebidos.

A confidencialidade dos identificadores do usuário com o PS ocorre pelo uso de mecanismos providos pela AN e não pelo uso da chave pública do usuário. Na UCPKI um *nonce* é criado e utilizado na autenticação do titular da credencial e os atributos contidos. Esta autenticação é anônima pois identifica o usuário anonimamente e o *nonce* nunca é repetido. Na UCPKI-AA a autenticação ocorre por meio do protocolo de provas de *zero-knowledge*, um protocolo mais seguro para prover o anonimato do usuário.

Outro mecanismo para dificultar na tentativa do mapeamento dos atributos de um mesmo titular, o rastreamento das atividades do usuário e adicionalmente promover a autenticação anônima do usuário com a AN é a utilização de diferentes chaves em diferentes credenciais. Na ICP X.509, uma chave pública é associada a um certificado digital e caso um usuário queira obter outra chave, é necessário obter (comprar) outro certificado digital. A posse de diferentes chaves na ICP X.509 é cara para o usuário final, pois além de ter um custo elevado, não faz sentido ter diferentes chaves já que a intenção deste certificado é identificar e autenticar o titular.

No modelo ABPKI, não há cobrança pelo serviço de criação do par de chaves pelo usuário, mas ele é responsável por registrar e gerenciar as chaves públicas em cada APA. Na ABPKI não há preocupação com a privacidade nos dados e na identificação do titular do certificado, assim como não há necessidade de possuir diferentes chaves sendo que cada certificado

poderá associar apenas uma chave pública com os atributos inclusos. A apresentação de diferentes atributos para o PS, que são gerenciados por diferentes APAs, necessita da apresentação dos certificados emitidos por cada APA e, consequentemente, realizar a autenticação de cada um. Neste procedimento, a privacidade do usuário é sutilmente incrementada por lhe dar mais controle dos atributos, entretanto aumenta a responsabilidade e a complexidade dos procedimentos para o usuário.

Diferentemente da ABPKI, na UCPKI e UCPKI-AA o usuário pode derivar diferentes pares de chaves a partir de um par de chaves mestras e com a entrada de distintos identificadores na função (conceito de CBI). O uso de diferentes chaves para diferentes certificados dificulta a possibilidade da AN rastrear os certificados dos usuários. Enquanto na UCPKI o usuário utiliza o par de chaves derivado para assinar seu certificado e a AN verificá-lo, a UCPKI-AA permite utilizar um par de chaves para assinar o certificado e outro para cifrar os atributos. Assim, na UCPKI-AA, o usuário pode registrar diferentes derivações de chave pública em diferentes APAs. Neste caso, o usuário necessita gerenciar em quais APAs foram registradas as determinadas chaves.

5.2.1.2 Complexidade Computacional

A análise sobre a complexidade computacional exigida por cada modelo é centrada nas operações criptográficas realizadas sobre o certificado (ou credencial) e sobre os dados contidos. Estas operações são para assinar o certificado, verificar a assinatura, cifrar os atributos ou o identificador, decifrá-los e obter o resumo criptográfico dos atributos quando necessário. Os principais procedimentos ocorrem na emissão de um certificado, na sua validação (similar à emitir uma credencial pela AN), para a verificação da credencial ou na autenticação do usuário com o provedor de serviços.

Numa ICP X.509, quando a autoridade certificadora emite certificados para os usuários finais, além de conferir toda a documentação necessária apresentada, a operação realizada na emissão é basicamente a assinatura da AC no certificado digital do usuário. A mesma operação ocorre quando o usuário emite um certificado auto-assinado pela ABPKI. Por outro lado, na UCPKI e na UCPKI-AA, os identificadores devem ser cifrados assim como os atributos (opcionalmente na UCPKI). A quantidade de operações se eleva ainda mais na UCPKI-AA por causa das operações de *hash* dos atributos. Portanto, caso o sigilo dos atributos seja aplicado, a complexidade para tal é acrescida de acordo com a quantidade de atributos inclusos no certificado.

Assim como os atributos são cifrados pelo usuário no certificado, os

mesmos devem ser decifrados pela autoridade detentora da chave privada correspondente nos procedimentos de validação ou verificação do certificado. Adicionalmente, a UCPKI-AA utiliza-se de funções de *hash* sobre todos os atributos de um certificado e as APAs e os PSs também devem calcular o *hash* dos atributos para verificarem a veracidade. A quantidade de operações também é influenciada pelo método utilizado para o usuário se autenticar no provedor de serviços.

O uso de grandes quantidades de operações criptográficas faz com que o modelo UCPKI-AA exija uma complexidade computacional maior do que os outros. Como consequência, é necessário que o modelo utilize de componentes computacionais capazes de executar as operações em um tempo hábil para não tornar o protocolo inseguro ou inutilizável pelo usuário, pois teria que esperar muito tempo para obter os resultados esperados.

5.2.1.3 Implementação e Manutenção

Uma ICP X.509 que geralmente é implementada com uma arquitetura de autoridades certificadoras em nível hierárquico (formando uma arborescência de autoridades), possui a sua raiz como o ponto de confiança. Todas as autoridades devem manter níveis elevados de requisitos de segurança, com mão de obra especializada, ambiente e equipamentos adequados. Uma analogia com as alternativas propostas, onde todas possuem a mesma arquitetura, as autoridades notariais exercem as responsabilidade semelhantes com as autoridades certificadoras finais em ICP X.509.

As APAs mantêm as semelhanças tanto em IGP quanto nas propostas descritas neste trabalho. Sendo assim, em uma ICP e IGP X.509 a quantidade de autoridades (certificadoras e provedoras de atributos) será sempre maior do que em uma ABPKI, UCPKI ou UCPKI-AA quando as quantidades de ANs e APAs forem iguais as de ACs finais e APAs na ICP e IGP respectivamente. Isso ocorre devido a eliminação da estrutura acima destas autoridades e com a adição de uma TSL. A TSL possui a mesma responsabilidade do que uma autoridade certificadora raiz, sendo que a entidade responsável pelo gerenciamento da TSL deve mantê-la sempre disponível e atualizada. Portanto, a diminuição da quantidade de autoridades impactam na diminuição da complexidade de implementação, manutenção e custos nos modelos propostos.

5.2.2 OpenID

O protocolo OpenID é amplamente utilizado nos procedimentos de autenticação, autorização e utiliza-se do paradigma centrado no usuário. Entretanto, o OpenID possui algumas limitações no fornecimento da segurança da comunicação (DELFT; OOSTDIJK, 2010), na privacidade do usuário e na utilização de recursos externos para incrementar suas funcionalidades.

Fornecer privacidade no protocolo OpenID não é um objetivo da especificação, todavia alguns elementos podem ser aplicados nas implementações de recursos no Provedor OpenID (PO). O mecanismo para autenticação do usuário é especificado de forma generalizada, onde o PO escolhe aquele que mais lhe agrada. Um dos exemplos de mecanismo de autenticação é através do uso da certificação digital. Por outro lado, este mecanismo exigirá o gerenciamento das chaves utilizadas, ou pelo próprio PO ou por terceiros (uma ICP por exemplo). A privacidade dos atributos pode ser aplicável, mas sua implementação deve aplicar uma relação de confiança e responsabilidade conjunta entre o PO e o PS envolvido. Para prover algum controle da apresentação dos atributos dos usuário, o PO pode utilizar recursos para permitir que o usuário crie perfis com diferentes dados ou que ele possa selecionar quais atributos deseja liberar.

O URI utilizado no protocolo do OpenID informa em qual PO o usuário está vinculado e qual identificador está registrado. O problema deste URI é que ele é público e isto compromete na privacidade da identificação do usuário perante diversos PSs. Outra característica oriunda do uso do URI, é a possibilidade do provedor OpenID rastrear o usuário em todas as atividades realizadas com um URI específico.

O OpenID é um sistema online e suas credenciais são obtidas apenas de forma online e para aquela sessão específica. A revogação de uma credencial se faz pelo encerramento da sessão. Outra limitação do protocolo é a não especificação sobre a forma como os atributos do usuário são armazenados e apresentados, ou seja, fica ao cargo do PO definir estes requisitos. Os custos de implementação do sistema com este protocolo é baixo por ser considerado de fácil implementação, com pré-requisitos simples e o usuário não paga para utilizar este tipo de recurso.

5.2.3 Shibboleth

O uso do *framework* Shibboleth permite a implementação de uma IAA através do paradigma federado. Assim como no protocolo OpenID, o mecanismo utilizado para a autenticação é escolhido pela entidade que realiza este

procedimento, neste caso o PId. O fornecimento da privacidade do usuário no framework Shibboleth é limitado. O usuário não possui o controle sobre seus dados, onde o PS requisita para o PId o conjunto de atributos necessários para autorizá-lo. Foi implementado uma ferramenta para tentar amenizar esta situação. A aplicação web uApprove[1] permite que o usuário saiba quais dados o PS está requisitando para o seu PId. Entretanto, o uApprove não permite que o usuário bloqueie alguns dos atributos listados, e sim, apenas decidir liberar toda a lista de atributos ou não. Caso não aceite liberar, o usuário não irá obter o acesso aos recursos requisitados.

A arquitetura do Shibboleth faz com que o PS receba do PId o identificador do usuário autenticado. Este identificador é sempre igual no decorrer da vida do registro do usuário. Dessa maneira, os PSs possuem a identificação do usuário sempre que ele acessar seus serviços e os PIds poderão rastrear em quais PSs o usuário está requisitando um recurso. O *framework* funciona apenas para serviços web, e as credenciais emitidas pelo PIds possuem validade limitada ou até o encerramento da sessão do usuário.

5.2.4 U-Prove e Idemix

Os sistemas U-Prove e Idemix objetivam melhorar a privacidade do usuário nos procedimentos de autenticação e autorização. Eles protegem e dão mais sigilo à identificação dos usuários e na apresentação de seus atributos (cf. Seções 3.4.1 e 3.4.2 respectivamente). A análise comparativa desses dois sistemas se dará apenas junto à alternativa proposta de ICP que atribui melhores recursos para aprimorar a privacidade do usuário, ou seja, a UCPKI-AA. O Quadro 3 resume as características analisadas e comparadas entre o U-Prove, Idemix e a UCPKI-AA.

Tanto no U-Prove quanto no Idemix, o gerenciamento dos atributos do usuário é realizado pelas mesmas autoridades que emitem as credenciais. Nenhuma das especificações determinam que as autoridades são exclusivas para cada tipo de atributo e como as autoridades emissoras identificam e autenticam o usuário quando solicitada uma credencial. Nos três modelos analisados, o usuário possui o controle de determinar quais atributos ele deseja incluir na credencial e apresentar para o PS. Por outro lado, o U-Prove limita-se por não suportar que os atributos dos usuários sejam apresentados de forma parcial. Além desta característica semelhante, os três sistemas também permitem o uso de diferentes chaves criptográficas para cada credencial, essas chaves ou os identificadores são confidenciais para que apenas os PSs possam visualizá-los, o que não permite que os atributos sejam mapeados como sendo

[1] https://www.switch.ch/aai/support/tools/uApprove.html

Quadro 3 – Privacidade fornecida pelos sistemas de credenciais anônimas.

Características/Ações	**Modelos**		
	UCPKI-AA	**U-Prove**	**Idemix**
Autoridade Gerenciadora dos Atributos	Provedora de atributo	Emissora de credenciais	Emissora de credenciais
Controlar os atributos pelos usuários	Sim	Sim	Sim
Apresentar atributos parciais	Sim	Não	Sim
Tornar os atributos confidenciais	Sim	Sim	Sim
Usar diferentes chaves criptográficas	Sim	Sim	Sim
Tornar os identificadores confidenciais	Sim	Sim	Sim
Mapear os atributos das credenciais	Não	Não	Não
Rastrear o usuário	Não	Não	Não
Tipo de identificação do usuário com o PS	Anônimo	Pseudônimo ou Anônimo	Anônimo

de um mesmo titular. As entidades emissoras de credenciais ou provedoras de atributos, após a emissão das credenciais, não conseguem identificar onde o usuário utilizará a credencial, garantindo que o mesmo não seja rastreado nem por eles nem por terceiros.

Um dos grandes desafios para os sistemas de credenciais anônimas é a revogação. Uma vez que a credencial não possua um identificador visível e duradouro, existe a dificuldade de associar a credencial como um estado de revogação. Caso seja necessário um mecanismo de revogação, (p. ex., lista de credenciais revogadas, lista negra), é fundamental identificar a credencial. Neste caso, cria a possibilidade de que terceiras partes realizem algum tipo de rastreamento ou mapeamento do uso destas credenciais. Algumas alternativas para revogar credenciais anônimas estão surgindo nos últimos anos e sendo aplicadas no sistema do Idemix (LAPON et al., 2011). Os três sistemas permitem que este problema de revogação das credenciais seja eliminada através da determinação de uma validade para um curto período de tempo das credenciais.

A complexidade dos modelos UCPKI-AA, U-Prove e Idemix é alta a fim de tornar um desafio a sua implementação utilizando *smartcards*. Entretanto, existem alguns trabalhos nos quais implementam o protocolo do U-Prove e Idemix (com algumas modificações) para se tornarem mais leves e diminuir o tempo gasto para os procedimentos de criptografia (BICHSEL et al., 2009; MOSTOWSKI; VULLERS, 2012). Um diferencial da UCPKI-AA é a possibilidade da credencial ser utilizada para tornar válida uma assinatura de documento eletrônico, contendo os atributos escolhidos pelo signatário e

todos os dados validados pela autoridade notarial.

5.3 CONCLUSÃO

Este capítulo analisou comparativamente as três alternativas de ICP descritas neste trabalho (ABPKI, UCPKI, UCPKI-AA) com sistemas e modelos difundidamente utilizados na composição de uma infraestrutura de autenticação e autorização, ICP e IGP X.509, OpenID e Shibboleth. Adicionamente, foram comparados o modelo proposto que melhor aprimora a privacidade (UCPKI-AA) com dois sistemas de emissão de credenciais anônimas (U-Prove e Idemix).

Inicialmente, foi resumido as principais vantagens e desvantagens de uma ICP X.509, ICP com certificado de atributos X.509 e os modelos ABPKI, UCPKI e UCPKI-AA. A ABPKI possui o objetivo de remodelar uma ICP com um melhor gerenciamento dos atributos do usuário final em relação aos procedimentos utilizados por uma ICP e IGP X.509, dando um maior controle para o usuário sobre seus atributos e simplificando os procedimentos de verificação de uma credencial. O modelo UCPKI introduz melhorias para prover níveis de privacidade para o usuário, tais como o uso da criptografia baseada em identidades (permitindo a geração de pares de chaves de forma mais dinâmica) e o suporte da autenticação anônima (através do uso de *nonces* entre o usuário e o PS). Como consequências, modelo apresenta o aumento da complexidade computacional necessária em relação a proposta ABPKI. Outra desvantagem da UCPKI é a forma como a autenticação anônima é fornecida, onde a chave pública do PS deve ser repassada para a AN para cifrar o *nonce*, limitando o uso da credencial para este PS em questão e possibilitando o conhecimento de seu uso pela AN.

A comparação da UCPKI-AA permite visualizar o seu aprimoramento em relação a UCPKI, que evita o rastreamento do usuário através do uso de um protocolo de autenticação *zero-knowledge*. Além deste recurso, a UCPKI-AA aumenta o nível de privacidade dos atributos exigindo que eles sejam cifrados. A apresentação destes atributos também sofre mudança por meio do uso de seus resumos criptográficos. Como consequência das mudanças realizadas, sua complexidade computacional é caracterizada como sendo a maior entre os três.

Em seguida, foi mostrada a diferença entre dois sistemas diversificadamente utilizados para o gerenciamento de identidades e IAA. Estes sistemas (OpenID e Shibboleth) possuem como principais diferenças a falta de preocupação com a privacidade do usuário. Em contrapartida, os dois são sistemas online cuja complexidade exigida para a sua utilização é menor do que as

propostas deste trabalho e centrando mais na usabilidade do usuário final.

Por fim, foram comparadas e analisadas a UCPKI-AA com U-Prove e Idemix. A UCPKI-AA é aquela que melhor se compara com os sistemas U-Prove e Idemix. Os três sistemas possuem características semelhantes, mas os principais benefícios da UCPKI-AA em relação aos outros dois são no procedimento da emissão da credencial, que não precisa de uma infraestrutura de autenticação entre o usuário e a entidade emissora de credenciais (p. ex., banco de dados com registro de logins e senhas dos usuários) e na possibilidade de ser utilizada para validade de assinatura de documentos eletrônicos. Enquanto a UCPKI-AA ainda necessita ser implementada e testada, tanto o U-Prove quanto o Idemix possuem versões implementadas e aplicadas em alguns projetos pilotos. Isso permite que novas análises sejam feitas e algumas soluções para os problemas, como a revogação das credenciais, sejam testadas e aplicadas.

6 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Este trabalho teve como objetivo apresentar, modelar e descrever alternativas de Infraestruturas de Chaves Públicas X.509 a fim de aplicá-las como Infraestruturas de Autenticação e Autorização com melhorias no gerenciamento de identidades e atributos dos usuários. Por meio destes objetivos, as propostas também aplicam um aprimoramento da privacidade do usuário final e fornecendo um maior controle dos seus dados. Como resultado deste trabalho, três alternativas foram propostas: ABPKI, UCPKI e UCPKI-AA. Todas possuem a mesma arquitetura entre si, centradas no usuário e baseadas em notários para dar confiabilidade dos dados e na comunicação. Com maior controle para os usuários, são eles quem gerenciam suas chaves, emitem suas credenciais e apresentam seus atributos. Adicionalmente, para não perder a generalidade de uma ICP X.509, as três alternativas podem ser aplicadas para validar assinaturas de documentos eletrônicos. Cada uma das propostas provê diferentes níveis de privacidade por meio do uso de diferentes recursos.

A emissão dos certificados auto-assinados e a obtenção das credenciais permitem conter apenas os atributos escolhidos pelo titular, pois a arquitetura utiliza o paradigma centrado no usuário (presente em todas as propostas). A ABPKI fornece mais simplicidade do que em uma ICP X.509, melhorando o gerenciamento dos atributos ao invés do uso de certificados de atributos e utilizando menos processos externos para a verificação de um certificado (cadeia de certificação, estados de revogação, carimbos de tempo, etc.). A eliminação da cadeia de certificação deu origem à utilização de Listas de Estados dos Serviços Confiáveis, a fim de dar confiabilidade nas autoridades notariais e provedoras de atributos. As credenciais possuem validade curta, ou seja, não havendo a necessidade de utilizar mecanismos de revogação e a verificação dos estados de revogações.

A UCPKI e UCPKI-AA se baseiam na arquitetura da ABPKI e adicionam mecanismos para aprimorar a privacidade, tal como o uso da criptografia baseada em identidades e sigilo nos identificadores e nos atributos. O conceito de CBI permite derivar diferentes pares de chaves simplificando o gerenciamento. A principal diferença entre a UCPKI e a UCPKI-AA está no mecanismo utilizado para prover a autenticação anônima. A UCPKI utiliza-se de *nonces* enquanto a UCPKI-AA de protocolos de provas *zero-knowledge*. As diferenças entre a UCPKI e UCPKI-AA influenciam no aumento dos procedimentos para emissão da credencial. Outras características adicionadas na UCPKI-AA está na obrigatoriedade da confidencialidade dos atributos dentro das credenciais e o uso de resumos criptográficos dos atributos para tornar a apresentação seletiva com provas de que foram validados pelas autoridades

confiáveis. Estes mecanismos aumentam o nível de privacidade que o usuário obtém em relação ao uso da UCPKI. Por outro lado, a UCPKI-AA utiliza-se de grandes quantidades de procedimentos criptográficos, aumentando a complexidade computacional do modelo e limitando-se no uso de dispositivos com maior poder de processamento para não prejudicar na segurança e a sua adesão pelos usuários.

A validação dos certificados auto-assinados dos usuários é realizada pelas Autoridades Notariais. O gerenciamento dos atributos dos usuários e a validação daqueles apresentados nos certificados ficam sob a responsabilidade das Autoridades Provedoras de Atributos. O gerenciamento dos atributos centrado apenas nas APAs específicas, elimina a inconsistência dos atributos com cópias registradas em outras entidades e com valores desatualizados.

Nos sistemas analisados de gestão de identidades e na realização de procedimentos de autenticação e autorização, o OpenID e o Shibboleth, se limitam aos modelos propostos por serem sistemas exclusivamente onlines e não possuem princípios para prover a privacidade. Os sistemas que emitem credenciais anônimas, o U-Prove e o Idemix utilizam-se de esquemas criptográficos próprios para prover o anonimato dos usuários, mas não especificam a autenticação do usuário para a emissão das credenciais. A UCPKI-AA é a proposta que mais se assemelha com os sistemas U-Prove e o Idemix, e sua principal vantagem está na forma como o usuário controla a criação de suas chaves criptográficas e suas credenciais, além da possibilidade de utilizar as credenciais para validar assinaturas de documentos eletrônicos. Enquanto as alternativas propostas neste trabalho utilizam-se de chaves criptográficas assimétricas para prover as propriedades de autenticidade, confidencialidade, integridade e não-repúdio, os sistemas analisados necessitariam de um elemento externo caso queiram suportar as quatro propriedades.

Ainda existem aspectos a serem desenvolvidos em trabalhos futuros, como por exemplo, uma análise mais profunda da complexidade computacional exigida em cada modelo proposto, a implementação e aplicação em um projeto piloto, ou a aplicação de esquemas criptográficos mais leves. Os modelos de negócio que poderiam ser implantados na aplicação em larga escala, podem ser analisados de outras perspectivas, levando em conta os métodos utilizados para utilizar um certificado (*pull* ou *push*), os fatores econômicos e jurídicos por exemplo.

REFERÊNCIAS

ADAMS, C.; JUST, M. PKI: Ten Years Later. In: **In 3rd Annual PKI R&D Workshop**. [S.l.: s.n.], 2004. p. 69–84.

AHN, G.-J.; KO, M.; SHEHAB, M. Privacy-Enhanced User-Centric Identity Management. In: **Communications, 2009. ICC '09. IEEE International Conference on**. [S.l.: s.n.], 2009. p. 1 –5. ISSN 1938-1883.

ANDERSSON, C. et al. Trust in PRIME. In: **Signal Processing and Information Technology, 2005. Proceedings of the Fifth IEEE International Symposium on**. [S.l.: s.n.], 2005. p. 552–559.

BAEK, J. et al. A Survey of Identity-Based Cryptography. In: **Proc. of Australian Unix Users Group Annual Conference**. [S.l.: s.n.], 2004. p. 95–102.

BELLARE, M.; PALACIO, A. GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks. In: YUNG, M. (Ed.). **Advances in Cryptology – CRYPTO 2002**. Springer Berlin Heidelberg, 2002, (Lecture Notes in Computer Science, v. 2442). p. 162–177. ISBN 978-3-540-44050-5. Disponível em: <http://dx.doi.org/10.1007/3-540-45708-9_11>.

BERBECARU, D.; LIOY, A.; MARIAN, M. On the Complexity of Public-Key Certificate Validation. In: **Information Security**. Springer Berlin / Heidelberg, 2001, (Lecture Notes in Computer Science, v. 2200). p. 183–203. ISBN 978-3-540-42662-2. Disponível em: <http://dx.doi.org/10.1007/3-540-45439-X_13>.

BERTINO, E. et al. Digital Identity Management and Trust Negotiation. In: **Security for Web Services and Service-Oriented Architectures**. Springer Berlin Heidelberg, 2010. p. 79–114. ISBN 978-3-540-87741-7. Disponível em: <http://dx.doi.org/10.1007/978-3-540-87742-4_5>.

BERTINO, E.; PACI, F.; SHANG, N. Digital Identity Protection - Concepts and Issues. In: **Availability, Reliability and Security, 2009. ARES '09. International Conference on**. [S.l.: s.n.], 2009. p. 69 – 78, doi=10.1109/ARES.2009.176,.

BERTINO, E.; TAKAHASHI, K. **Identity Management: Concepts, Technologies, and Systems**. [S.l.]: Artech House, 2010.

BICHSEL, P.; CAMENISCH, J. Mixing Identities with Ease. In: LEEUW, E.; FISCHER-HüBNER, S.; FRITSCH, L. (Ed.). **Policies and Research in Identity Management**. Springer Berlin Heidelberg, 2010, (IFIP Advances in Information and Communication Technology, v. 343). p. 1–17. ISBN 978-3-642-17302-8. Disponível em: <http://dx.doi.org/10.1007/978-3-642-17303-5_1>.

BICHSEL, P. et al. Anonymous credentials on a standard java card. In: **Proceedings of the 16th ACM conference on Computer and communications security**. New York, NY, USA: ACM, 2009. (CCS '09), p. 600–610. ISBN 978-1-60558-894-0. Disponível em: <http://doi.acm.org/10.1145/1653662.1653734>.

BLUM, M.; FELDMAN, P.; MICALI, S. Non-interactive Zero-knowledge and Its Applications. In: **Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing**. New York, NY, USA: ACM, 1988. (STOC '88), p. 103–112. ISBN 0-89791-264-0. Disponível em: <http://doi.acm.org/10.1145/62212.62222>.

BONEH, D.; FRANKLIN, M. Identity-Based Encryption from the Weil Pairing. In: KILIAN, J. (Ed.). **Advances in Cryptology – CRYPTO 2001**. Springer Berlin Heidelberg, 2001, (Lecture Notes in Computer Science, v. 2139). p. 213–229. ISBN 978-3-540-42456-7. Disponível em: <http://dx.doi.org/10.1007/3-540-44647-8_13>.

BRAMHALL, P. et al. User-Centric Identity Management: New Trends in Standardization and Regulation. **Security Privacy, IEEE**, v. 5, n. 4, p. 84 – 87, 2007. ISSN 1540-7993.

BRANDS, S. A. **Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy**. Cambridge, MA, USA: MIT Press, 2000. ISBN 0262024918.

BRASIL. **Medida Provisória n° 2.200-2**. 2001.

BRAZ, C.; ROBERT, J.-M. Security and usability: The case of the user authentication methods. In: **Proceedings of the 18th International Conferenceof the Association Francophone D'Interaction Homme-Machine**. New York, NY, USA: ACM, 2006. (IHM '06), p. 199–203. ISBN 1-59593-350-6. Disponível em: <http://doi.acm.org/10.1145/1132736.1132768>.

CAMENISCH, J.; HERREWEGHEN, E. V. Design and implementation of the idemix anonymous credential system. In: **Proceedings of the 9th ACM**

conference on Computer and communications security. New York, NY, USA: ACM, 2002. (CCS '02), p. 21–30. ISBN 1-58113-612-9. Disponível em: <http://doi.acm.org/10.1145/586110.586114>.

CAMENISCH, J.; LYSYANSKAYA, A. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In: **Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology**. London, UK, UK: Springer-Verlag, 2001. (EUROCRYPT '01), p. 93–118. ISBN 3-540-42070-3. Disponível em: <http://dl.acm.org/citation.cfm?id=647086.715698>.

CAMENISCH, J.; LYSYANSKAYA, A. A Signature Scheme with Efficient Protocols. In: CIMATO, S.; PERSIANO, G.; GALDI, C. (Ed.). **Security in Communication Networks**. Springer Berlin Heidelberg, 2003, (Lecture Notes in Computer Science, v. 2576). p. 268–289. ISBN 978-3-540-00420-2. Disponível em: <http://dx.doi.org/10.1007/3-540-36413-7_20>.

CAMP, J. Digital identity. **Technology and Society Magazine, IEEE**, v. 23, n. 3, p. 34 – 41, 2004. ISSN 0278-0097.

CANTOR, S. et al. **Liberty ID-FF Architecture Overview Version: 1.2-errata-v1.0**. 2005. Liberty Alliance Project. Disponível em: <http://www.projectliberty.org/liberty/content/download/318/2366/file/draft-liberty-idff-arch-overview-1.2-errata-v1.0.pdf>.

CAO, Y.; YANG, L. A Survey of Identity Management Technology. In: **Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on**. [S.l.: s.n.], 2010. p. 287 – 293.

CARMODY, S. et al. **Shibboleth Architecture Protocols and Profiles**. 2005. Liberty Alliance Project. Disponível em: <https://wiki.shibboleth.net/confluence/download/attachments/2162702/internet2-mace-shibboleth-arch-protocols-200509.pdf>.

CHAPPELL, D. **Introducing Windows CardSpace**. abril 2006. Article. Disponível em: <http://msdn.microsoft.com/en-us/library/aa480189.aspx>.

CHAUM, D. Blind Signatures for Untraceable Payments. In: CHAUM, D.; RIVEST, R.; SHERMAN, A. (Ed.). **Advances in Cryptology**. Springer US, 1983. p. 199–203. ISBN 978-1-4757-0604-8. Disponível em: <http://dx.doi.org/10.1007/978-1-4757-0602-4_18>.

CHAUM, D. Blind Signature System. In: CHAUM, D. (Ed.). **Advances in Cryptology**. Springer US, 1984. p. 153–153. ISBN 978-1-4684-4732-3. Disponível em: <http://dx.doi.org/10.1007/978-1-4684-4730-9_14>.

CHAUM, D. Security without identification: transaction systems to make big brother obsolete. **Commun. ACM**, ACM, New York, NY, USA, v. 28, n. 10, p. 1030–1044, out. 1985. ISSN 0001-0782. Disponível em: <http://doi.acm.org/10.1145/4372.4373>.

CLAYCOMB, W.; SHIN, D.; HARELAND, D. Towards Privacy in Enterprise Directory Services: A User-Centric Approach to Attribute Management. In: **Security Technology, 2007 41st Annual IEEE International Carnahan Conference on**. [S.l.: s.n.], 2007. p. 212 –220.

COCKS, C. An Identity Based Encryption Scheme Based on Quadratic Residues. In: **Proceedings of the 8th IMA International Conference on Cryptography and Coding**. London, UK, UK: Springer-Verlag, 2001. p. 360–363. ISBN 3-540-43026-1. Disponível em: <http://dl.acm.org/citation.cfm?id=647995.742435>.

COOPER, D. et al. **Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**. IETF, maio 2008. RFC 5280 (Proposed Standard). (Request for Comments, 5280). Disponível em: <http://www.ietf.org/rfc/rfc5280.txt>.

CUSTóDIO, R. F.; VIGIL, M. A. G. Cleaning up the PKI for Long-term Signatures. In: **Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. Curitiba-PR, Brasil: SBSEG, 2012. p. 14.

DABROWSKI, M.; PACYNA, P. Generic and Complete Three-Level Identity Management Model. In: **Emerging Security Information, Systems and Technologies, 2008. SECURWARE '08. Second International Conference on**. [S.l.: s.n.], 2008. p. 232 –237.

DELFT, B.; OOSTDIJK, M. A security analysis of openid. In: LEEUW, E.; FISCHER-HüBNER, S.; FRITSCH, L. (Ed.). **Policies and Research in Identity Management**. Springer Berlin Heidelberg, 2010, (IFIP Advances in Information and Communication Technology, v. 343). p. 73–84. ISBN 978-3-642-17302-8. Disponível em: <http://dx.doi.org/10.1007/978-3-642-17303-5_6>.

DIFFIE, W.; HELLMAN, M. New directions in cryptography. **Information Theory, IEEE Transactions on**, v. 22, n. 6, p. 644–654, November 1976. ISSN 0018-9448.

ELLISON, C.; SCHNEIER, B. Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure. **Computer Security Journal**, v. 16, n. 1, p. 1–7, 2000. Disponível em: <http://www.schneier.com/paper-pki.pdf>.

ETSI. **Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates**. [S.l.], Dez 2002.

ETSI. **Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information**. [S.l.], 2009.

FARRELL, S.; HOUSLEY, R.; TURNER, S. **An Internet Attribute Certificate Profile for Authorization**. IETF, 2010. RFC 5755 (Proposed Standard). (Request for Comments, 5755). Disponível em: <http://www.ietf.org/rfc/rfc5755.txt>.

FEIGE, U.; FIAT, A.; SHAMIR, A. Zero-knowledge proofs of identity. **Journal of Cryptology**, Springer-Verlag, v. 1, n. 2, p. 77–94, 1988. ISSN 0933-2790. Disponível em: <http://dx.doi.org/10.1007/BF02351717>.

FOUNDATION, T. E. **Higgins - Personal Data Service**. 2012. Web site. Disponível em: <http://www.eclipse.org/higgins/>.

GUTMANN, P. PKI: It's Not Dead, Just Resting. **Computer**, v. 35, n. 8, p. 41–49, August 2002. ISSN 0018-9162.

HALLER, N. et al. **A One-Time Password System**. IETF, fev. 1998. RFC 2289 (Standard). (Request for Comments, 2289). Disponível em: <http://www.ietf.org/rfc/rfc2289.txt>.

HANSEN, M.; PFITZMANN, A.; STEINBRECHER, S. Identity management throughout one's whole life. **Information Security Technical Report**, v. 13, n. 2, p. 83 – 94, 2008. ISSN 1363-4127. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1363412708000198>.

HOUSLEY, R.; POLK, T. **Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure**. 1st. ed. New York, NY, USA: John Wiley & Sons, Inc., 2001. ISBN 0471397024.

JØSANG, A.; POPE, S. User centric identity management. In: **In Australian Computer Emergency Response Team Conference**. [S.l.: s.n.], 2005.

JØSANG, A.; ZOMAI, M. A.; SURIADI, S. Usability and privacy in identity management architectures. In: **Proceedings of the fifth**

Australasian symposium on ACSW frontiers - Volume 68. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2007. (ACSW '07), p. 143–152. ISBN 1-920-68285-X. Disponível em: <http://dl.acm.org/citation.cfm?id=1274531.1274548>.

LAPON, J. et al. Analysis of Revocation Strategies for Anonymous Idemix Credentials. In: DECKER, B. et al. (Ed.). **Communications and Multimedia Security**. Springer Berlin Heidelberg, 2011, (Lecture Notes in Computer Science, v. 7025). p. 3–17. ISBN 978-3-642-24711-8. Disponível em: <http://dx.doi.org/10.1007/978-3-642-24712-5_1>.

LEENES, R.; SCHALLABÖCK, J.; HANSEN, M. Prime white paper. **PRIME (Privacy and Identity Management for Europe), White Paper**, 2008.

LI, F.; KHAN, M. A Survey of Identity-based Signcryption. In: . [S.l.: s.n.], 2011. v. 28, n. 3, p. 265–272.

LIOY, A. et al. Pki past, present and future. **International Journal of Information Security**, Springer Berlin/Heidelberg, v. 5, p. 18–29, 2006. ISSN 1615-5262. Disponível em: <http://dx.doi.org/10.1007/s10207-005-0077-9>.

LYSYANSKAYA, A. et al. Pseudonym Systems. In: HEYS, H.; ADAMS, C. (Ed.). **Selected Areas in Cryptography**. Springer Berlin Heidelberg, 2000, (Lecture Notes in Computer Science, v. 1758). p. 184–199. ISBN 978-3-540-67185-5. Disponível em: <http://dx.doi.org/10.1007/3-540-46513-8_14>.

MOECKE, C. T. **NBPKI - Uma ICP Baseada em Autoridades Notariais**. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2011. Disponível em: <http://www.tede.ufsc.br/teses/PGCC0928-D.pdf>.

MOECKE, C. T. et al. Uma ICP baseada em certificados digitais autoassinados. In: **Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. Fortaleza-CE, Brazil: [s.n.], 2010. p. 91–104.

MOSTOWSKI, W.; VULLERS, P. Efficient U-Prove Implementation for Anonymous Credentials on Smart Cards. In: RAJARAJAN, M. et al. (Ed.). **Security and Privacy in Communication Networks**. Springer Berlin Heidelberg, 2012, (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, v. 96). p. 243–260. ISBN 978-3-642-31908-2. Disponível em: <http://dx.doi.org/10.1007/978-3-642-31909-9_14>.

MYERS, M. et al. **X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP**. IETF, 1999. RFC 2560 (Proposed Standard). (Request for Comments, 2560). Disponível em: <http://www.ietf.org/rfc/rfc2560.txt>.

NOGUEIRA, H. et al. Using Notary Based Public Key Infrastructure in Shibboleth Federation. In: **Workshop de Gestão de Identidades - WGID/SBSeg**. Brasília-DF, Brazil: WGID/SBSeg, 2011. p. 405–414.

NOGUEIRA, H.; MARTINA, J. E.; CUSTóDIO, R. F. An Attribute-Based Public Key Infrastructure. **International Journal of Computer Science and Information Security - IJCSIS**, v. 11, n. 11, p. 11–18, Nov. 2013. ISSN 1947-5500. Disponível em: <https://sites.google.com/site/ijcsis/vol-11-no-11-nov-2013>.

NOGUEIRA, H.; SANTOS, D. B.; CUSTóDIO, R. F. Um Survey sobre Ferramentas para Single Sign-On. In: **Workshop de Gestão de Identidades - WGID/SBSeg**. Brazil: [s.n.], 2012. p. 522–542.

NOGUEIRA, H.; SOUZA, R. L. de; CUSTóDIO, R. F. A Privacy-Enhanced User-Centric Identity and Access Management Based on Notary. In: **The Eighth International Conference on Systems and Networks Communications (ICSNC'13)**. IARIA XPS Press, 2013. ISBN 978-1-61208-305-6. Disponível em: <http://www.thinkmind.org/index.php?view=article&articleid=icsnc_2013_8_20_20125>.

OASIS. **Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0**. 2005. OASIS Standard. Disponível em: <httpd://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf>.

OASIS. **Web Services Federation Language (WS-Federation) Version 1.2**. 2009. OASIS Standard. Disponível em: <http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.pdf>.

OECD. **OECD Guidelines Governing the Protection of Privacy and Transborder Flows od Personal Data**. [S.l.], 2013. Disponível em: <www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>.

OPENID. **OpenID Authentication 2.0 - Final**. 2007. Disponível em: <http://openid.net/specs/openid-authentication-2_0.html>.

PAQUIN, C. **U-Prove Technology Overview V1.1**. [S.l.], Abril 2013. Revision 2. Disponível em: <http://research.microsoft.com/apps/pubs/default.aspx?id=166980>.

PAQUIN, C.; ZAVERUCHA, G. **U-Prove Cryptographic Specification V1.1**. [S.l.], Abril 2013. Disponível em: <http://research.microsoft.com/apps/pubs/default.aspx?id=166969>.

PFITZMANN, A.; HANSEN, M. **A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management**. ago. 2010. V0.34. Disponível em: <http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf>.

QUISQUATER, J.-J. et al. How to Explain Zero-Knowledge Protocols to Your Children. In: BRASSARD, G. (Ed.). **Advances in Cryptology – CRYPTO' 89 Proceedings**. Springer New York, 1990, (Lecture Notes in Computer Science, v. 435). p. 628–631. ISBN 978-0-387-97317-3. Disponível em: <http://dx.doi.org/10.1007/0-387-34805-0_60>.

SHAMIR, A. Identity-based cryptosystems and signature schemes. In: **Proceedings of CRYPTO 84 on Advances in cryptology**. New York, NY, USA: Springer-Verlag New York, Inc., 1985. p. 47–53. ISBN 0-387-15658-5. Disponível em: <http://dl.acm.org/citation.cfm?id=19478.19483>.

SHEEDY, C.; KUMARAGURU, P. A Contextual Method for Evaluating Privacy Preferences. In: LEEUW, E. et al. (Ed.). **Policies and Research in Identity Management**. Springer US, 2008, (The International Federation for Information Processing, v. 261). p. 139–146. ISBN 978-0-387-77995-9. Disponível em: <http://dx.doi.org/10.1007/978-0-387-77996-6_11>.

SMITH, R. E. **Authentication: From Passwords to Public Keys**. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2002. ISBN 0-201-61599-1.

SOLOVE, D. J. A taxonomy of privacy. **University of Pennsylvania Law Review**, JSTOR, p. 477–564, 2006.

SOLOVE, D. J. Understanding privacy. **GWU Legal Studies Research**, Harvard University Press, p. 24, 2008.

UNION, I. T. **ITU-T Recommendation X.509 | ISO/IEC 9594-8: Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certificate Frameworks**. [S.l.],

2008. 162+ p. (Tertiary ITU-T Recommendation X.509 | ISO/IEC 9594-8: Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certificate Frameworks).

VIGIL, M. A. G. **Infraestrutura de chaves públicas otimizadora**. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2010. Disponível em: <http://www.tede.ufsc.br/teses/PGCC0902-D.pdf>.

VIGIL, M. A. G. et al. The Notary Based PKI – A Lightweight PKI for Long-term Signatures on Documents. In: **EuroPKI**. [S.l.: s.n.], 2012.

WÄSTLUND, E. et al. Towards usable privacy enhancing technologies: Lessons learned from the primelife project. PrimeLife, 2011.

WINDLEY, P. **Digital Identity**. [S.l.]: O'Reilly Media, Inc., 2005. ISBN 0596008783.