UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Felipe Carlos Werlang

ASSINATURA DIGITAL COM RECONHECIMENTO DE FIRMA: UM MODELO DE ASSINATURA DIGITAL CENTRADO NO USUÁRIO

Florianópolis(SC)

2014

Felipe Carlos Werlang

ASSINATURA DIGITAL COM RECONHECIMENTO DE FIRMA: UM MODELO DE ASSINATURA DIGITAL CENTRADO NO USUÁRIO

Dissertação submetida ao Programa de Pós-Graduação em Ciência da Computação para a obtenção do Grau de Mestre em Ciência da Computação.

Prof. Ricardo Felipe Custódio, Dr.
Orientador

Florianópolis(SC)

2014

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

Werlang, Felipe Carlos
Assinatura digital com reconhecimento de firma : Um modelo de assinatura digital centrado no usuário / Felipe Carlos Werlang ; orientador, Ricardo Felipe Custódio - Florianópolis, SC, 2014.
76 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. Assinatura digital. 3. Documento eletrônico. 4. usabilidade. 5. modelo de confiança. I. Custódio, Ricardo Felipe. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Computação. III. Título.

Felipe Carlos Werlang

ASSINATURA DIGITAL COM RECONHECIMENTO DE FIRMA: UM MODELO DE ASSINATURA DIGITAL CENTRADO NO USUÁRIO

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), 28 de Fevereiro de 2014

Prof. Ronaldo dos Santos Mello, Dr.
Coordenador

Prof. Ricardo Felipe Custódio, Dr.
Orientador

Banca Examinadora:

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

Prof. Ricardo Pareira e Silva, Dr.
Universidade Federal de Santa Catarina

Prof. Antonio Marinho Pilla Barcellos, Dr.
Universidade Federal do Rio Grande do Sul

Prof. Mario Antônio Ribeiro Dantas, Dr.
Universidade Federal de Santa Catarina

Dedico este trabalho a meus pais que fizeram incontáveis sacrifícios para que eu tivesse a oportunidade de seguir o caminho de minha escolha e não ficasse à mercê das circunstâncias da vida.

AGRADECIMENTOS

Agradeço primeiramente ao meu orientador Prof. Dr. Ricardo Felipe Custódio pelo aprendizado e pelas oportunidades de crescimento profissional que me proporcionou ao longo de mais de 7 anos de trabalho conjunto, desde os primeiros anos da graduação.

Aos amigos e colegas do LabSEC, muitos dos quais eu considero verdadeiros irmãos. Alguns como irmãos mais velhos que me acolheram ainda um "garotinho inocente" e outros a quem eu "ajudei a criar" ao longo dos anos. Agradeço especialmente a Armindo, Lucas Martins, Lucas Ferraro, Rick, Hendri, Martín e Maurício pela ajuda, discussões, ideias e principalmente a motivação sem as quais eu não teria concluído este trabalho.

Agradeço ainda a *Moreiras* e *Paraíbas* que fizeram dos meus últimos anos na universidade uma coleção de histórias hilárias que vou levar pro resto da minha vida. Sua amizade foi indispensável para a minha sanidade.

Por fim, agradeço a toda a minha família e especialmente meus pais Wilson e Noeli e irmãos Everton e Mariane pelo apoio incondicional e as sinceras demonstrações de orgulho pelas minhas realizações. Sempre acreditaram em mim, as vezes mais do que eu mesmo.

“When we are no longer able to change a situation, we are challenged to change ourselves.”
{Viktor Frankl}

RESUMO

O crescimento do uso de documentos eletrônicos nas mais diversas atividades da sociedade vem atrelado à necessidade de garantias de autenticidade e integridade desses documentos, entre outras. Para esse fim, tem-se empregado normalmente assinaturas digitais em conjunto à Infraestruturas de Chaves Públicas (ICPs), principalmente do modelo X509. Contudo, observa-se que os modelos de assinatura digital proeminentes na atualidade são complexos e inconvenientes para os usuários finais. Neste trabalho são agrupados os principais problemas relacionados a esses modelos de assinatura e é proposta uma nova abordagem, centrada nas necessidades do usuário final. O foco está na melhoria de três aspectos: a) a complexidade do processo de assinatura sob a perspectiva do usuário final; b) o custo da manutenção da assinatura a longo prazo; c) o modelo de confiança exigido no processo de assinatura. O novo modelo proposto é uma revisão do modelo de assinatura como um todo, descartando certificados e a ICP X509 em favor de estruturas simples e relacionamentos de confiança naturais, modelados nas assinaturas manuscritas convencionais.

Palavras-chave: Assinatura digital, centrado no usuário, usabilidade, notário, notarização, manutenção a longo prazo, confiança

ABSTRACT

The growth in the use of electronic documents in various activities within society comes coupled with the necessity for, among others, authenticity and integrity guarantees upon these documents. Digital signatures in conjunction with Public Key Infrastructures (PKIs), mainly the X509 model, have commonly been employed to that end. However, we observe that current mainstream digital signature schemes are complex and inconvenient for end users. We group the main problems related to these schemes and propose a new approach, centered on the needs of the end user. Therefore, we focus on the improvement of three aspects: a) the complexity of the signature process from the end user perspective; b) the cost of long-term signature maintenance; c) the trust model required by the signature process. The new proposed scheme is a redesign of the overall signature process, discarding certificates and the X509 PKI in favor of simple structures and natural trust relationships modeled on conventional handwritten signatures.

Keywords: Digital signature, user-centric, usability, notary, notarization, long-term maintenance, trust

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

SUMÁRIO

1 INTRODUÇÃO

As duas últimas décadas têm marcado uma explosão no uso da Internet como um ambiente para negócios. A cada dia novos setores da economia aderem ao uso da rede em suas atividades. Ao mesmo tempo, o setor público corre para disponibilizar mais de seus serviços online afim de torná-los mais eficientes e prover conveniência. Como resultado, o fluxo de documentos associado a estas atividades começou a migrar para o meio eletrônico. Isso traz ganhos em velocidade, praticidade e redução de custos, além de diminuir o impacto do uso de papel no meio ambiente.

No entanto, a substituição de documentos em papel por documentos eletrônicos requer que estes ofereçam garantias equivalentes às de um documento em papel, i.e., *autenticidade* (a origem pode ser identificada), *integridade* (o conteúdo não sofreu alteração) e *evidência cronológica* (também conhecida como *prova de existência*, esta propriedade corresponde à data e hora em que um objeto existiu (ADAMS et al., 2001)). A tecnologia normalmente empregada para prover essas garantias é a assinatura digital.

Isso tem levado muitos países a criar leis e normas específicas para tratar da validade jurídica de assinaturas digitais e documentos eletrônicos. Exemplos incluem Estados Unidos da América, União Europeia e o Brasil. (United States, 2000a, 2000b), (European Parliament, Council, 2000), (Brasil, 2001). Essas normas têm favorecido processos de assinatura digital dependentes de Infraestruturas de Chaves Públicas (ICPs), com destaque ao modelo X509 (ITU-T, 2008).

Contudo, ICPs possuem deficiências bem conhecidas. Ellison e Schneier alertam em (ELLISON; SCHNEIER, 2000) sobre os principais riscos da ICP sob o ponto de vista da segurança. Lopez et al. descrevem em (LOPEZ; OPPLIGER; PERNUL, 2005) as principais razões técnicas, econômicas, legais e sociais que levaram a falhas no emprego da ICP em diferentes áreas. Aplicações e modelos de negócio do mundo real precisam ser adaptados e restringidos para funcionar dentro do modelo ICP (GUTMANN, 2002). Processos de assinatura digital não são exceção à essa regra.

Para poder realizar uma assinatura digital, uma pessoa precisa basicamente possuir um par de chaves criptográficas. No entanto, no modelo de ICP X509, para vincular sua identidade a essas chaves é necessário adicionalmente um certificado digital. Portanto, antes de poder assinar algo, a pessoa precisa ser credenciada em uma Autoridade de Registro (AR). Esta, por sua vez, solicita à uma Autoridade Certificadora (AC) que realize a emissão do certificado digital. Uma vez realizada a assinatura, alguém que deseje verificá-la precisa primeiro obter e validar os certificados e situação de re-

vogação dos certificados das ACs que compõe o caminho hierárquico da AC emissora até a AC Raiz (âncora de confiança comum). Se todos esses artefatos estiverem válidos é possível constatar se o certificado do signatário é válido e se não está revogado. A partir disso é possível verificar a assinatura. Se for necessário preservar a validade dessa assinatura por um período prolongado é preciso aplicar a ela sucessivos carimbos do tempo, emitidos por uma Autoridade de Carimbo do Tempo (ACT) (ADAMS et al., 2001).

No Brasil há duas ICPs hierárquicas de larga escala. Uma é a Infraestrutura de Chaves Públicas Educacional (ICPEdu) (Rede Nacional de Ensino e Pesquisa (RNP), 2013), mantida por universidades e instituições de pesquisa com o objetivo de servir como ambiente de teste para o desenvolvimento de novas tecnologias. A outra é a ICP Brasil (Instituto Nacional de Tecnologia da Informação (ITI), 2013), operada pelo governo. Ela foi criada como parte de um esforço para promover o uso de assinaturas digitais no país. Portanto, seu principal propósito tem sido fornecer os certificados digitais necessários para a assinatura de documentos eletrônicos e para garantir a autenticidade de transações eletrônicas diversas. Contudo, passada mais de uma década, e apesar de avanços expressivos, o uso de certificados digitais para a realização de assinaturas se dá principalmente no meio governamental e empresarial. A certificação digital ainda não é conhecida pela maioria dos cidadãos (Instituto Nacional de Tecnologia da Informação (ITI), 2011).

Um fator importante para a adoção limitada de assinaturas digitais é o custo de aquisição de certificados e dispositivos criptográficos. Comparada a documentos em papel com assinaturas manuscritas, a relação custo-benefício do uso de assinaturas digitais só se torna positiva em ambientes com um alto volume de assinaturas. Mas outros aspectos, como os desafios da preservação de assinaturas a longo prazo e a complexidade do processo de assinatura como um todo, tem uma influência ainda mais importante.

A análise desses fatores leva à conclusão de que, atualmente, o aparato necessário para a realização de uma assinatura digital é demasiadamente complexo e inconveniente para o usuário final. Além disso, o modelo em uso não reflete adequadamente as interações naturais e relações de confiança entre usuários e entre usuários e entidades.

Neste trabalho, é proposto um modelo de assinatura digital centrado nas necessidades do usuário final. A abordagem é inspirada no modelo de assinatura manuscrita praticado nos países que utilizam o sistema jurídico romano-germânico (MERRYMAN; PÉREZ-PERDOMO, 2007). Com isso, pretende-se aproximar a assinatura digital das práticas já culturalmente estabelecidas.

1.1 OBJETIVOS

Esta dissertação tem por objetivo propor um modelo de assinatura digital que seja centrado nas necessidades do usuário. Ele deve possibilitar ao usuário criar uma assinatura digital de forma rápida e fácil, sem a exigência de um processo de registro prévio. Adicionalmente, deve ser possível ao usuário certificar uma assinatura digital após sua criação, com a ajuda de uma terceira parte confiável de sua escolha.

1.1.1 Objetivos Específicos

- Prover mecanismos que facilitem a preservação a longo prazo da validade de assinaturas digitais;
- Possibilitar a transferência de confiança entre âncoras de confiança ao longo do tempo, de forma que as antigas possam ser descartadas;
- Reduzir a complexidade do processo de assinatura digital e da infraestrutura envolvida;
- Prover um modelo de confiança condizente com as relações naturais de confiança entre usuários e entidades.

1.2 MOTIVAÇÃO

O presente trabalho se insere na linha de pesquisa do Laboratório de Segurança da Computação (LabSEC) na área de segurança de documentos eletrônicos. Trabalhos que o precedem tratam dos requisitos de segurança necessários aos documentos eletrônicos para que estes substituam documentos em papel (DIAS, 2004), da datação de documentos por meio de carimbos do tempo (PASQUAL, 2001; DEMéTRIO, 2003; COSTA, 2003), de uma infraestrutura para o armazenamento e recuperação segura de documentos eletrônicos (NOTOYA, 2002), da preservação a longo prazo da validade de assinaturas digitais (VIGIL, 2010; SILVA, 2011) e da preservação a longo prazo aliada a um modelo de uso simplificado de assinaturas digitais (MOECKE, 2011).

Paralelamente a estes trabalhos de pesquisa, o LabSEC tem mantido parcerias com instituições governamentais e outras universidades para o desenvolvimento de normas e soluções de software e hardware para a ICPEdu e ICP Brasil, além da participação ativa no desenvolvimento do Padrão Bra-

sileiro de Assinatura Digial (PBAD) (Instituto Nacional de Tecnologia da Informação (ITI), 2010).

A proposta apresentada nesta dissertação é resultado da experiência obtida com este conjunto de trabalhos. Ela visa sanar alguns dos problemas remanescentes evidenciados pelos trabalhos anteriores e também se vale de muitas das soluções introduzidas por eles.

1.3 JUSTIFICATIVA

Documentos eletrônicos assinados digitalmente proveem uma série de vantagens e já são empregados com sucesso em diversos setores. No entanto, é de opinião do autor que o modelo de assinatura digital vigente, assim como as propostas alternativas presentes na literatura, ainda são demasiadamente complexos. Isto dificulta a sua difusão em meio às camadas periféricas da sociedade e usuários eventuais, que têm a simples expectativa de que a identidade do signatário de um documento possa ser confirmada por uma terceira parte confiável após a assinatura, em caso de necessidade.

A presente proposta aproxima o modelo de assinatura digital da assinatura manuscrita, historicamente consagrada, simplificando sua realização, sua validação e a preservação de sua validade.

1.4 METODOLOGIA

O trabalho inicia com a revisão de artigos, dissertações, normas e artigos técnicos na área de Assinaturas Digitais. Com base nisso, e guiado pelas experiências do autor em diversos projetos relacionados ao tema, são delimitados os principais problemas presentes no cenário atual da assinatura digital.

A partir daí, são revistas as abordagens existentes que tratam desses problemas, assim como suas limitações. Em seguida é proposto um processo de assinatura digital que aborda todos esses problemas.

Por fim, é avaliada a eficácia da proposta em relação aos problemas que ela se propõe a resolver e são feitas considerações relativas a custos de implementação e segurança.

1.5 PUBLICAÇÕES

Este trabalho foi pulicado na forma de artigo no 10° Workshop Europeu em Infraestruturas de Chaves Públicas, Serviços e Aplicações (EuroPKI),

realizado em Egham-Reino Unido, no dias 12 e 13 de setembro de 2013, com o título "A User-Centric Digital Signature Scheme"(WERLANG; VIGIL; CUSTóDIO, 2014).

1.6 ORGANIZAÇÃO DO TRABALHO

O Capítulo 2 apresenta uma revisão dos modelos de assinatura, manuscrita e digital, das estratégias de preservação de assinaturas digitais e dos problemas presentes no modelo vigente. Em seguida, são revisados outros trabalhos que buscam sanar as deficiências do modelo de assinatura digital vigente. No Capítulo 3 é apresentado o nova modelo proposto por este trabalho. Esse novo modelo é avaliado criticamente no Capítulo 4. Por fim, no Capítulo 5 são apresentadas as considerações finais e são propostos trabalhos futuros.

2 ASSINATURA

A assinatura é uma forma de identificar um indivíduo junto a um documento, ou registro, que expresse sua vontade ou que comunique algo. Contratos, testamentos, cartas e atestados são exemplos desses tipos de documento. Os meios nos quais esses documentos são concretizados e a forma como as assinaturas são realizadas, contudo, é algo que depende da tecnologia da época, e tem evoluído ao longo da história. Nos últimos séculos a ideia de documento e assinatura esteve associada ao papel e à assinatura manuscrita.

Com o advento da informatização nas décadas recentes vemos o surgimento dos documentos eletrônicos e consequentemente de inúmeras formas de assinatura eletrônica, das quais destaca-se a assinatura digital.

Nas seções a seguir será revisada a Assinatura Manuscrita (Seção 2.1) e serão descritos com mais detalhes os conceitos envolvidos na Assinatura Digital (Seção 2.2). Em seguida listamos os principais problemas presentes nas tecnologias de assinatura digital em uso atualmente (Seção 2.3). Por fim avaliamos trabalhos relacionados que tratam alguns dos problemas presentes nas assinaturas digitais atuais (Seção 2.4).

2.1 ASSINATURA MANUSCRITA

A assinatura manuscrita consiste na aplicação da marca gráfica do signatário em um documento de papel. Esta marca, normalmente o nome completo ou a rubrica do signatário, é criada com o auxílio de um instrumento de escrita, normalmente uma caneta. O ponto chave deste conceito está no fato de que a caligrafia de uma pessoa tende a apresentar características distintas da de outras pessoas. Dessa forma, se duas pessoas realizarem uma assinatura que contenha a mesma sequência de letras ou formas, a marca gerada ainda será distinta. Portanto, é a caligrafia única que identifica o signatário.

Contudo, é possível falsificar uma assinatura imitando a caligrafia do signatário. Essas falsificações podem ser identificadas por meio de técnicas como a grafoscopia, mas estas requerem treinamento e equipamentos especializados. Além disso, mesmo no caso de assinaturas autênticas, um indivíduo precisa conhecer de antemão a marca gráfica do outro para poder aferir sua identidade à partir da marca. Por esses motivos, normalmente recorre-se a uma terceira parte confiável para que essa ateste a autenticidade de uma assinatura. Dessa forma, é a terceira parte confiável que efetivamente garante o vínculo entre a assinatura e a identidade do signatário. Esse processo é chamado de notarização, mas também é conhecido popularmente como re-

conhecimento de firma, e o papel de terceira parte confiável geralmente é atribuído ao Notário.

Para poder efetuar um reconhecimento de firma, num primeiro momento, o Notário recolhe e guarda uma amostra da assinatura do indivíduo juntamente com cópias de documentos que comprovem sua identidade. A partir daí, para cada assinatura que este individuo realiza, o Notário faz uma comparação com a amostra guardada e então reconhece a firma por meio da aplicação de um celo ou carimbo acompanhado de sua própria assinatura. É importante notar que o reconhecimento de firma inclui ainda a data em que foi realizado, provendo a evidência cronológica necessária em muitos tipos de documentos.

2.2 ASSINATURA DIGITAL

Assinaturas digitais foram propostas inicialmente por Diffie e Hellman (DIFFIE; HELLMAN, 1976) ao introduzirem o conceito de criptografia assimétrica. Contudo a primeira implementação de um esquema de assinatura digital veio dois anos mais tarde, com o trabalho de Rivest, Shamir e Adleman (RIVEST; SHAMIR; ADLEMAN, 1978). Elas foram criadas com o objetivo de trazer para as transações eletrônicas as mesmas garantias oferecidas pelas assinaturas manuscritas junto a documentos em papel.

O desenvolvimento das assinaturas digitais contou também com a incorporação dos certificados digitais (KOHNFELDER, 1978). Eles atestam a ligação entre a identidade do signatário e sua chave pública, sendo portanto utilizados para fazer a distribuição confiável das chaves públicas dos signatários. Outra inovação importante foi a incorporação de funções de resumo criptográfico (DAMGARD, 1987) aos esquemas de assinatura. Isso trouxe garantias de integridade e melhorou o desempenho desses esquemas.

2.2.1 Processo de Assinatura Digital

Existem diferentes esquemas de assinatura digital, dentre os quais destacam-se as assinaturas RSA (RIVEST; SHAMIR; ADLEMAN, 1978) e Elliptic Curve Digital Signature Algorithm (ECDSA) (JOHNSON; MENEZES; VANSTONE, 2001). Todavia, independentemente do esquema em questão, o processo de assinatura digital envolve de forma básica as operações de geração de par de chaves, assinatura e validação de assinatura.

Geração de Par de Chaves: Na operação de geração de par de chaves o

signatário gera um par de chaves assimétricas onde a chave privada é mantida em sigilo e a chave pública é distribuída àqueles que desejam validar as assinaturas a serem produzidas.

Assinatura: A operação de assinatura é compreendida pelas seguintes etapas:

1. O Signatário gera um resumo criptográfico da mensagem a ser assinada;
2. O Signatário cifra a resumo com sua chave privada, o que constitui a assinatura;
3. O Signatário envia a mensagem e a assinatura (resumo criptográfico cifrado) ao destinatário (Verificador).

Validação de Assinatura: A validação de assinatura contempla as seguintes etapas:

1. O Verificador gera um novo resumo criptográfico da mensagem recebida do Signatário;
2. O Verificador decifra a assinatura (resumo criptográfico cifrado) recebida do Signatário. Para isso ele faz uso da chave pública do Signatário;
3. O Verificador compara os resumos criptográficos obtidos nos passos 1 e 2. Se os resumos forem idênticos a assinatura é considerada válida e de autoria inequívoca do Signatário em questão. Se não forem idênticos, significa que algum elemento foi modificado e portanto não se pode confirmar a autoria da assinatura.

O processo básico de assinatura acima descrito requer que o Verificador conheça de antemão a chave pública do Signatário, o que implica na necessidade de algum mecanismo de identificação e distribuição confiável de chaves públicas. Isso é feito geralmente por meio de uma Infraestrutura de Chaves Públicas (ICP), vista em mais detalhes na Seção 2.2.2

2.2.2 Infraestrutura de Chaves Públicas

Em 1978 Kohnfelder propôs os certificados digitais (KOHNFELDER, 1978) como uma forma de atestar a ligação entre uma chave e a identidade de seu titular. Um certificado digital contém: chave pública, informações de identificação do titular (nome, email, organização, etc.) e restrições referentes ao uso da chave privada (propósito, período de validade, etc.). Adicionalmente, o certificado contém uma assinatura que engloba todo o conteúdo

anterior. Essa assinatura é normalmente realizada por uma terceira parte, que dessa forma atesta a autenticidade das informações de identidade apresentadas pelo titular e estabelece um vínculo entre o titular e sua chave pública. É possível também criar um certificado autoassinado, i.e., assinado com a própria chave privada do titular.

O modelo de certificado mais difundido atualmente é o X509 (ITU-T, 2008). Nesse modelo os certificados de usuários finais são emitidos (assinados) por entidades denominadas Autoridades Certificadoras (ACs). A tarefa de reunir a documentação e demais dados necessários para a identificação inequívoca de um usuário pode caber à própria AC ou então ser delegada a uma Autoridade de Registro (AR).

ACs também possuem um par de chaves e um certificado. Este certificado pode ser autoassinado, constituindo uma AC Raiz, ou emitido por outra AC, formando assim uma cadeia de certificação. Quando o número de usuários finais é muito grande para ser atendido por uma única AC, normalmente cria-se uma estrutura hierárquica onde a AC Raiz emite certificados apenas para ACs subordinadas, delegando à elas o poder de emitir certificados para outras ACs ou usuários finais, dependendo da quantidade de níveis da estrutura. A essa estrutura dá-se o nome de Infraestrutura de Chaves Públicas (ICP) e sua AC Raiz é considerada a âncora de confiança da ICP, ou seja, seu certificado é aceito como confiável.

Ao se estabelecer que o certificado da AC Raiz é confiável, a partir dele é possível validar as assinaturas de todos os certificados que compõem o caminho de certificação da AC Raiz até o certificado do usuário final.

2.2.3 Validade de Assinaturas Digitais

Diferente de assinaturas manuscritas, que permanecem válidas indefinidamente, assinaturas digitais podem perder suas garantias técnicas de autenticidade devido à perda da segurança do esquema de assinatura utilizado ou devido à impossibilidade de validar o certificado do signatário.

Avanços nas técnicas de criptoanálise, aumento do poder computacional para ataques de força bruta e a descoberta de falhas em algoritmos são os principais fatores que podem levar um esquema de assinatura a ser considerado inseguro. A partir daí não é mais possível garantir a autenticidade de uma assinatura feita com esse esquema. Já a validade do certificado do signatário depende de fatores como data de expiração, revogação e a invalidação do certificado da AC Raiz ou de alguma AC que compõe a cadeia de certificação até o certificado do signatário. Além desses, é claro, se inclui também a segurança dos esquemas de assinatura usados na emissão dos certificados

da cadeia.

Ao emitir um certificado digital, uma AC define as datas de início e fim da validade do certificado, e consequentemente, da validade da chave privada correspondente. Isso significa que, passado esse período, não é mais possível garantir a autenticidade de uma assinatura realizada com àquela chave privada. Durante o período de validade do certificado, é possível ainda que o titular ou a AC solicite sua revogação, o que tem o mesmo efeito da expiração. Os mecanismos mais comuns para prover a situação de revogação de um certificado são a Lista de Certificados Revogados (LCR) (COOPER et al., 2008) e o Online Certificate Status Protocol (OCSP) (SANTESSON et al., 2013), ambos também objetos assinados. Esses fatores têm um grande impacto no processo de validação de assinatura. Na prática, o processo de validação descrito na Seção 2.2.1 tem de ser precedido pelos passos a seguir:

1. Obtenção dos certificados do caminho de certificação e respectivas situações de revogação;
2. Para cada certificado do caminho, iniciando pelo certificado da AC Raiz:
   (a) Verificar se certificado não está expirado;
   (b) Validar assinatura do certificado;
   (c) Validar assinatura da situação de revogação;
   (d) Verificar se o certificado está revogado.

Na tentativa de reduzir os riscos de invalidação de assinaturas provenientes dos fatores descritos acima, normas atuais (ETSI, 2013, 2010; Instituto Nacional de Tecnologia da Informação (ITI), 2010) recomendam o uso de Carimbos do Tempo em conjunto às assinaturas. Carimbos do Tempo são discutidos na seção seguinte.

2.2.4 Carimbos do Tempo

Um carimbo do tempo (ADAMS et al., 2001) é uma espécia de âncora temporal. Ao emitir um carimbo do tempo para uma determinada assinatura, a Autoridade de Carimbo do Tempo (ACT) atesta que aquela assinatura já existia previamente ao instante da emissão do carimbo. A partir daí, a assinatura, ou mais especificamente o certificado do signatário, passa a ser validada para a data e hora fornecidas pelo carimbo do tempo e não mais na data atual. Apenas a assinatura do carimbo é validada na data e hora atuais. Dessa forma,

se o certificado do signatário expirar ou for revogado após a aplicação do carimbo do tempo, a assinatura continua podendo ser validada. O carimbo também mitiga o problema da perda de segurança dos algoritmos utilizados na assinatura, desde que o carimbo tenha sido gerado com algoritmos diferentes que continuem seguros.

O uso de carimbos do tempo requer que a ACT seja considerada uma entidade confiável. O processo de validação de assinatura também precisa ser expandido. Agora ele é procedido pela validação do certificado da ACT e de sua situação de revogação e da validação do carimbo de tempo. Adicionalmente, por se tratar ele próprio de um objeto assinado, o carimbo do tempo eventualmente perde sua validade. Isso implica em um processo sem fim de acumulação de carimbos do tempo. Um novo carimbo do tempo precisa ser aplicado ao conjunto de assinatura e carimbos anteriores antes que o último carimbo aplicado se torne inválido.

2.3 PROBLEMAS

A extensão da autenticidade de assinaturas digitais além do período de validade de certificados e algoritmos criptográficos requer o uso de carimbos do tempo. Como carimbos do tempo são objetos assinados, sua autenticidade também fica incerta com o tempo. Adicionalmente, também é preciso confiar nas entidades que emitem os carimbos do tempo. Por fim, autenticidade duradoura depende de um uso interminável de carimbos do tempo, que leva a um número sempre crescente de autoridades confiáveis e um crescente acúmulo de *evidências criptográficas* (certificados, situações de revogação e carimbos do tempo).

Além disso, enquanto os pré-requisitos para uma assinatura convencional não excedem uma caneta comum e um pedaço de papel, uma assinatura digital requer a posse de um certificado digital. A obtenção de um certificado digital normalmente requer que o indivíduo passe por um processo de registro em uma AR, que então contata uma AC para emitir o certificado. Dependendo do provedor de serviços, esse processo pode levar dias. Em alguns aspectos, é possível até comparar o certificado digital a uma carteira de habilitação de condutores, já que nos dois casos há que se passar por um processo de obtenção e por renovações periódicas. Nesse caso, um habilita o portador a dirigir um automóvel e o outro a assinar documentos eletrônicos. Contudo, é de opinião do autor que não deveríamos precisar de uma "licença"para assinar algo, tampouco deveríamos precisar comprar uma nova depois de alguns anos.

Em seguida temos o problema do armazenamento das chaves. O certi-

ficado está ligado a uma chave privada específica que tem de ser armazenada em algum tipo de dispositivo criptográfico ou na forma de um arquivo cifrado. Dessa forma, se ela está dentro de um dispositivo, é necessário carregar esse dispositivo consigo todo o tempo, ou então prever quando será necessário assinar algo. Se estiver armazenada em um computador, só será possível gerar assinaturas a partir daquele computador. A necessidade de guardar essa chave faz com que o usuário vire uma espécie de refém de sua própria chave. Se em algum momento outra pessoa tiver acesso à chave, esta pessoa terá o poder de gerar assinaturas válidas se passando pelo dono real da chave.

Por último, há uma discrepância entre a noção de confiança do mundo real e aquela imposta pelos certificados digitais. Relacionamentos de confiança normais são bilaterais. Eles são estabelecidos lentamente, ao longo do tempo, e se baseiam em experiências. Todavia, um desses relacionamentos pode ser destruído rapidamente. Certificados, por outro lado, requerem confiança unilateral em uma terceira parte (i.e., a AC) e a confiança em um determinado certificado é imposta, sem a existência de experiências prévias (LOPEZ; OPPLIGER; PERNUL, 2005). Adicionalmente, o relacionamento de confiança com a terceira parte não pode ser encerrado.

Dado esse prospecto, enumeramos abaixo quatro problemas principais. Esses problemas são a origem dos objetivos específicos do presente trabalho.

Problema 1 (Custos de preservação) Quanto mais velha a assinatura do documento, maior o custo adicional de armazenamento e processamento. A razão para tal é: (i) o acúmulo de evidências criptográficas requer crescente espaço de armazenamento, e (ii) a validação da assinatura do documento requer, por sua vez, a validação da assinatura de cada evidência criptográfica acumulada. Isto é um problema especialmente para o uso da assinatura digital em dispositivos móveis com pouca capacidade de armazenamento e de processamento para realizar as verificação. Também causa impacto em instituições que trabalham com grandes volumes de assinaturas, como tribunais, empresas de grande porte, órgãos governamentais e outros.

Problema 2 (Confiança em entidades antigas) Confiar em partes confiáveis antigas é um problema. Uma parte em que se confiava no passado pode desaparecer sem deixar os dados necessários para que verificadores de assinatura futuros possam aferir a confiabilidade da parte. Também pode ser o caso de a parte não atender aos requisitos necessários no futuro (LEKKAS; GRITZALIS, 2004).

Problema 3 (Complexidade do processo de assinatura) A complexidade e características de projeto dos processos de assinatura digital atuais tornam a

geração de assinaturas inconveniente para os usuários finais. Além disso, tanto signatário quanto destinatário precisam estar cientes dos fatores que afetam a autenticidade de uma assinatura a longo prazo. A falta dessa consciência pode resultar em perdas para uma ou ambas as partes na ocorrência de uma invalidação da assinatura. Eles também precisam se preocupar com o armazenamento seguro de sua chave privada.

Problema 4 (Modelo de confiança) A noção de confiança aplicada a certificados digitais não é a mesma que a noção de confiança do mundo real, que é baseada em relacionamentos e experiências e consolidada ao longo do tempo (LOPEZ; OPPLIGER; PERNUL, 2005).

2.4 TRABALHOS RELACIONADOS À MELHORIA DA ASSINATURA DIGITAL

O aprimoramento das técnicas usadas na manutenção da autenticidade de assinaturas em documentos eletrônicos a longo prazo tem sido o foco de uma série de propostas encontradas na literatura. Muitas dessas dependem de uma terceira parte confiável para atestar aspectos específicos de uma assinatura, portanto vindo a ser caracterizadas como formas de notarização. A técnica de *Sobreposição de Carimbos do Tempo*, proposta em (HABER; STORNETTA, 1991) e (BAYER; HABER; STORNETTA, 1993), é o principal exemplo. Ela tem se tornado a técnica proeminente para estender a sobrevida de uma assinatura digital. Apesar de em última análise ser pouco prática, como visto no capítulo 2, ela é atualmente a estratégia recomendada em padrões de assinatura digital como CAdES (ETSI, 2013) e XAdES (ETSI, 2010).

Além do aspecto da sobrevida da assinatura digital, na seção anterior apresentamos outros problemas (Seção 2.3) que dificultam a adoção de assinaturas digitais por um público mais amplo. No restante desta seção revisamos trabalhos prévios que se propuseram a resolver um ou mais desses problemas. As propostas estudadas são, respectivamente, a Sobreposição de Notarizações (Seção 2.4.1), o Certificado Otimizado (Seção 2.4.2) e a NBPKI (Seção 2.4.3).

2.4.1 Sobreposição de Notarizações

A proposta da *Sobreposição de Notarizações* (LEKKAS; GRITZALIS, 2004) também se utiliza do conceito de notarização. Nela, a autenticidade de uma assinatura digital é mantida a longo prazo por meio de sucessivos

atestes realizados por notários. Seu principal objetivo é possibilitar que a verificação da assinatura seja feita com base apenas em relações de confiança, tecnologias e dados disponíveis no momento da verificação. O foco, portanto, é eliminar qualquer dependência para com relações de confiança, tecnologias e dados obsoletos que existiam no passado mas se tornaram inválidos. Isso é feito por meio de sucessivas transições de confiança para novas entidades, tecnologias e dados.

As entidades envolvidas no modelo são, respectivamente: o signatário, criador da assinatura digital inicial; a AC que provê o certificado digital do signatário; os notários que atestam as assinaturas; e o verificador que deposita confiança na AC e nos notários como provedores das informações corretas para verificar a assinatura.

Dada uma assinatura digital em um documento eletrônico, o processo de preservação dessa assinatura segundo o modelo de sobreposição de notarizações consiste basicamente das seguintes etapas:

1. O notário realiza a validação completa da assinatura, i.e., ele verifica se a assinatura está correta com base na chave pública do signatário, valida os certificados do signatário e das ACs que constituem o caminho de certificação e verifica se nenhum deles está revogado. Caso haja algum carimbo do tempo junto à assinatura, este também é devidamente validado;

2. O notário cria uma estrutura de dados contendo o documento assinado, metadados do documento, a assinatura inicial, metadados da assinatura e ateste do notário. O ateste do notário contém os detalhes relativos às verificações realizados pelo notário antes de assinar. Carimbos do tempo também são incluídos, se presentes;

3. O notário assina a estrutura de dados;

4. Na iminência da expiração do certificado do notário anterior ou do comprometimento de algum algoritmo criptográfico utilizado na notarização anterior, uma nova notarização é gerada. Para tanto, o novo notário também realiza os passos 2 e 3, mas agora aplicados à notarização anterior em vez da assinatura original. Com isso, a notarização anterior é encapsulada na estrutura de dados da nova notarização.

A validação de uma assinatura notarizada consiste apenas em realizar a validação da notarização mais recente. Uma vez que o notário é uma entidade considerada confiável neste modelo, seu ateste já indica a validade das notarizações encapsuladas, bem como da assinatura original. Com isso, o objetivo da proposta é alcançado pois existe uma transição de confiança da AC

para o notário e depois de um notário para o subsequente. Ao mesmo tempo os dados e tecnologias necessários para a verificação permanecem sempre atualizados.

A sobreposição de notarizações atende parcialmente ao Problema 1 (Custos de preservação). Apenas a notarização mais recente e suas evidências criptográficas precisam ser validadas, sem a necessidade de validar as notarizações e assinatura inicial encapsuladas. Isto simplifica bastante o processo de validação. Mas mesmo sendo opcional a inclusão de certificados do caminho de certificação e suas respectivas situações de revogação, a proposta ainda exige o acúmulo das notarizações. Isto, portanto, caracteriza um custo crescente no armazenamento, ainda que menor em relação ao processo de sobreposição de carimbos do tempo. O Problema 2 (Confiança em entidades antigas), por sua vez, é atendido adequadamente pois a confiança é transferida de um notário para o outro a cada nova notarização. Desse modo, entidades que eram confiáveis no passado deixam de ser relevantes.

2.4.2 Certificado Otimizado

Na proposta do *Certificado Otimizado* (CUSTÓDIO et al., 2008) apenas as evidências criptográficas são atestadas por uma terceira parte confiável. A ideia nesse caso é que as evidências criptográficas relacionadas à assinatura são enviadas para uma autoridade certificadora especial responsável por verificá-las. Esta então valida as evidências (certificado do signatário, certificados do caminho de certificação e situações de revogação) e emite um *certificado otimizado* que serve como um substituto do conjunto de evidências criptográficas originais.

O certificado otimizado é um certificado digital que mantém as informações relativas à identidade do signatário, mas sua validade é restrita ao momento de sua emissão, ou seja, os campos *notBefore* e *notAfter* contém o mesmo valor. Dessa forma, ele serve também como um carimbo do tempo. Além disso, essa característica faz com que não haja necessidade de um mecanismo de revogação para o certificado otimizado já que sua validade é restrita a um instante. Isso, por sua vez, simplifica o processo de validação da assinatura. A validação pode ser feita com base apenas nas informações contidas no certificado, sem a necessidade de uma conexão externa. A validação do certificado da AC emissora de certificados otimizados é feita por meio de uma prova de validade incluída em uma extensão do certificado otimizado. Esta prova é gerada pela própria AC Raiz sempre que um novo certificado otimizado é emitido.

Certificados otimizados podem ainda ser renovados quando for imi-

nente o comprometimento da segurança dos algoritmos criptográficos utilizados em sua emissão.

Com o certificado otimizado o Problema 1 (Custos de preservação) é completamente atendido pois não há acúmulo de evidências criptográficas. Apenas um certificado otimizado e o certificado da AC Raiz precisam ser armazenados e verificados. A proposta também atende ao Problema 2 (Confiança em entidades antigas), pois a confiança reside apenas na AC Raiz atual. Contudo, o modelo não é utilizável na prática pois requer a substituição do certificado do signatário pelo certificado otimizado dentro do contêiner de assinatura. Essa substituição não é permitida nos formatos de assinatura eletrônica avançada atuais.

2.4.3 NBPKI

Vigil et al. propuseram em (VIGIL et al., 2013) uma ICP para assinatura de documentos chamada *Notary Based PKI (NBPKI)*. Na NBPKI existem entidades confiáveis que atestam que o certificado do signatário de um documento é válido para verificar uma assinatura de documento em particular com uma data e hora específica. O objetivo da NBPKI é simplificar: (i) a manutenção das assinaturas de documentos, e (ii) as decisões de confiança que um verificador tem de tomar para verificar uma assinatura de documento.

As entidades confiáveis na NBPKI são as Autoridades Notariais (ANs). Signatários de documentos e ANs geram seus pares de chaves e geram seus próprios certificados X509, ou seja, os certificados são autoassinados. Signatários registram seus certificados nas Autoridades Registradoras (ARs). Um certificado registrado permanece válido até que o sujeito correspondente solicite a sua revogação ou o algoritmo criptográfico utilizado se torne inseguro. Dessa forma, o tempo de validade dos certificados das ANs e dos signatários é irrelevante. Uma AR provê a situação de validade de certificados de signatários para uma ou mais ANs.

Em contraste às ANs, o certificado do signatário de um documento só é confiável se tiver sido notarizado. Um verificador submete a assinatura do documento e o certificado do signatário para uma AN. A AN confere a situação de validade do certificado com uma ou mais ARs. Se o certificado se encontra válido, a AN retorna uma declaração assinada da validade do certificado e da existência da assinatura nesta data e hora. A AN requisitada contata outras ANs se ela não puder conferir a situação do certificado. Se uma AN contatada confirma a validade do certificado, a AN retorna a declaração. Com base apenas na declaração e no certificado do signatário, o verificador

consegue avaliar a existência e a autenticidade da assinatura do documento. O verificador precisa confiar apenas na chave pública da AN emissora.

A processo de manutenção de uma assinatura de documento é necessário para estender a autenticidade e a prova de existência além do tempo de vida dos algoritmos criptográficos utilizados. A manutenção consiste na substituição da declaração atual por uma nova declaração. O verificador submete a assinatura do documento, o certificado do signatário e a declaração atual para a AN. A AN retorna uma nova declaração se a declaração atual: (i) foi emitida por uma AN conhecida e (ii) seus algoritmos criptográficos ainda são seguros. A nova declaração é quase uma cópia do conteúdo da declaração atual. O verificador avalia a existência da assinatura e sua autenticidade como visto anteriormente. O verificador precisa confiar apenas na chave pública da AN emissora, não nas chaves públicas das ANs anteriores.

Na ICP X509 a manutenção também é necessária. Uma vez que o tempo de vida de certificados é mais curto que o dos algoritmos criptográficos, a manutenção em uma ICP X509 ocorre mais frequentemente do que na NBPKI. A manutenção na ICP X509 acumula certificados de âncoras de confiança (ACs Raízes), dados de revogação e carimbos do tempo. Na NBPKI os dados não são acumulados, e sim substituídos. Devido a isso, uma assinatura de documento na NBPKI tem uma sobrecarga de armazenamento e verificação menor. No modelo X509, deve-se confiar em todas as ACs Raízes acumuladas. Na NBPKY, apenas se confia na AN atual. Para um verificador, é mais fácil avaliar a confiabilidade de uma entidade confiável atual do que de entidades confiáveis antigas.

A NBPKI não acumula evidências criptográficas e a confiança é transferida para a AN vigente a cada substituição de notarização. Portanto, a proposta atende adequadamente os Problemas 1 (Custos de preservação) e 2 (Confiança em entidades antigas). Ela também adiciona flexibilidade e eficiência ao processo de assinatura, dessa forma atendendo parcialmente o Problema 3 (Complexidade do processo de assinatura). Todavia signatários continuam reféns de sua chave privada e verificadores ainda precisam se preocupar com a manutenção da validade da assinatura a longo prazo.

2.5 CONSIDERAÇÕES

Ao longo deste capítulo foram revisadas as características e tecnologias empregadas no modelo de assinatura digital vigente. Com base nisso foram delineados 4 problemas encontrados nesse modelo. São eles: 1) Custos de preservação; 2) Confiança em entidades antigas; 3) Complexidade do processo de assinatura e 4) Modelo de confiança. Em seguida foram avaliados

trabalhos existentes na literatura que propõe melhorias ao modelo de assinatura digital. A Tabela 1 faz uma comparação entre essas propostas. Apesar de todas as propostas tratarem os Problemas 1 e 2, o problema da complexidade (3) é tratado apenas parcialmente e somente pela NBPKI. Nenhuma das propostas trata do problema do modelo de confiança (4).

Proposta	**Problema 1**	**Problema 2**	**Problema 3**	**Problema 4**
Sobrep. de Notarizações	✓*	✓		
Certificado Otimizado	✓	✓		
NBPKI	✓	✓	✓*	

Tabela 1: Comparação de Propostas

Uma característica comum das propostas avaliadas é que todas tem seu foco principal em resolver, ou ao menos minimizar, o problema dos custos de preservação das assinaturas digitais a longo prazo. No entanto, ao mesmo tempo tentam manter interoperabilidade com padrões de assinatura existentes e ainda fazem uso de certificados e da ICP. Isso implica na impossibilidade de resolver os problemas 3 e 4, já que eles são intrínsecos à ICP.

O custo de preservação da assinatura é um elemento importante a ser considerado na adoção de um modelo de assinatura digital. Mas a complexidade do processo de assinatura e verificação e a as exigências de confiança são elementos igualmente essenciais. Levando em conta essa perspectiva, viu-se a necessidade de propor um novo modelo do zero, descartando certificados e a ICP, e tratando os 4 problemas levantados ao mesmo tempo. Esse modelo de assinatura é apresentado no próximo capítulo.

3 UM MODELO DE ASSINATURA DIGITAL COM RECONHECIMENTO DE FIRMA

Assinatura Digital com Reconhecimento de Firma é uma proposta para um modelo de assinatura centrado no usuário, ou seja, focado em melhor atender às necessidades do usuário. Com essa proposta espera-se prover um modelo de assinatura digital que facilite a adesão das massas ao uso de documentos eletrônicos assinados em seu dia a dia. O modelo é inspirado no modelo de assinatura manuscrita convencional praticado na maior parte da Europa e na América Latina, onde o sistema jurídico empregado é o romano-germânico (MERRYMAN; PÉREZ-PERDOMO, 2007). Outras culturas, contudo, possuem práticas de assinatura similares (LISE, 2011). Portanto, espera-se que as entidades envolvidas, assim como as interações entre elas, sejam familiares à maioria dos usuários.

A Figura 1 representa o modelo de assinatura, demonstrando as entidades envolvidas e quais interagem entre si.

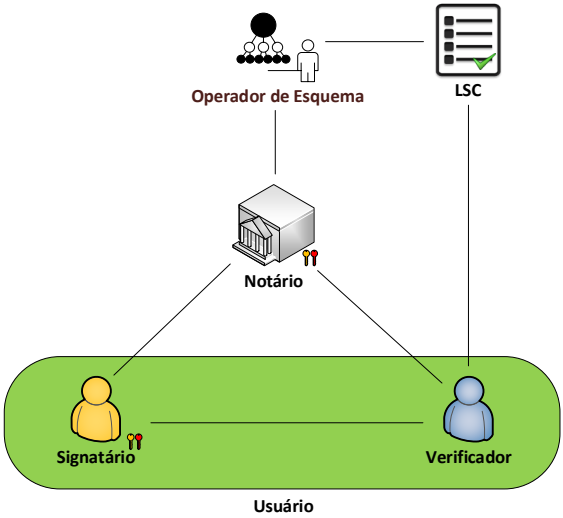

Figura 1: Modelo de assinatura

O foco da proposta é dar mais liberdade aos usuários finais, isto é, o Signatário e o Destinatário (doravante denominado Verificador) de um dado documento assinado. Isto significa que são os usuários que escolhem os requi-

sitos de uma determinada assinatura, com base na relevância do documento a ser assinado. Do mesmo modo, eles escolhem em quem confiar e para que fins.

De forma resumida, a assinatura segundo este modelo consiste no signatário assinando um documento com sua chave privada e repassando-o ao verificador. Caso não exista confiança entre as partes, ou no caso da necessidade de demonstrar a autenticidade da assinatura para outrem, o verificador pode recorrer a uma terceira parte (i.e., um Notário) de sua confiança para que este autentique a assinatura. Na prática, tanto signatário quanto verificador podem solicitar de um notário a autenticação da assinatura (doravante denominada reconhecimento de firma). Mas é direito do verificador definir o notário a ser utilizado. Nesse caso o signatário também tem que registrar seus atributos e sua chave pública no estabelecimento do notário se já não o tiver feito anteriormente.

O reconhecimento de firma consiste da assinatura do notário sobre a assinatura original e a data e hora correntes. No caso de *Reconhecimentos de Firma Completos* (cf. Definição 2), ele também engloba o documento assinado. Portanto, o reconhecimento de firma serve igualmente como uma afirmação de validade e uma evidência cronológica, i.e., um carimbo do tempo. Dessa forma, se comparado à ICP X509, um Notário engloba características de Autoridade Registradora, Certificadora e de Carimbo do Tempo (AR, AC e ACT respectivamente).

O restante deste capítulo é constituído inicialmente pela descrição das entidades envolvidas (Seção 3.1) e pelas suposições nas quais a proposta é baseada (Seção 3.2). Em seguida apresentamos nossas definições (Seção 3.3) e os procedimentos (Seção 3.4).

3.1 ENTIDADES

A proposta é composta por quatro entidades: usuários finais, isto é, o Signatário e o Verificador; o Notário e o Operador de Esquema.

O *Signatário* é um usuário que cria uma assinatura para um determinado documento. Ele é responsável por gerar seu próprio par de chaves e por registrar a chave pública em um estabelecimento notarial.

O *Notário* é uma parte confiável. Ele é responsável pelo cadastro de usuários, isto é, registrar os atributos e chave pública dos usuários e por realizar reconhecimentos de firma. Cada notário possui um escritório onde ocorre o cadastramento de usuários e um serviço autônomo de reconhecimento de firma online. Notários são listados como Provedores de Serviços Confiáveis (PSCs), do inglês *Trusted Service Providers (TSPs)*, na Lista de Situação de

Serviços Confiáveis (LSC), do inglês *Trusted-service Status List (TSL)* (ETSI, 2009).

O *Operador de Esquema* (Entidade *Scheme Operator* da especificação (ETSI, 2009)) é o organismo responsável pelo gerenciamento e publicação da LSC. Essa incumbência pode ficar a cargo de, por exemplo, uma agência governamental ou algum departamento específico dentro de uma organização. Para que possam ser listados na LSC, PSCs devem ser avaliados. Os critérios e métodos utilizados nessa avaliação podem variar com base na legislação e políticas organizacionais.

O *Verificador* é o usuário final interessado em aferir a autenticidade, integridade e a evidência cronológica de um determinado documento.

3.2 SUPOSIÇÕES

O modelo proposto está fundamentado nas seguintes suposições:

Suposição 1 O Notário é uma entidade confiável em meio ao sistema sócio-econômico, a nível nacional ou organizacional. Ele deve cumprir leis e regulamentações condizentes a um serviço notarial comum (LEKKAS; GRITZALIS, 2004).

Suposição 2 Estabelecimentos notariais são bem distribuídos geograficamente. Usuários Finais devem poder realizar procedimentos de cadastro ou substituição de par de chaves em sua própria cidade ou unidade organizacional.

Suposição 3 O estabelecimento notarial possui uma solução de *Armazenamento Seguro* para armazenar os dados dos Usuários Finais, documentos assinados e reconhecimentos de firma. Esta solução de armazenamento deve oferecer garantias de integridade, autenticidade e sigilo do conteúdo armazenado. Ela também deve estar equipada com contingências de backup adequadas. Adicionalmente, sua segurança deve ser independente da segurança do par de chaves do Notário.

3.3 DEFINIÇÕES

Definição 1 *Uma Assinatura é uma tupla* $S = (h, A, pk, \sigma)$*, onde* h *é o resumo criptográfico de um documento a ser assinado,* A *é um conjunto com os atributos do signatário onde* $A \neq \emptyset$*,* pk *é a chave pública do signatário,* σ *é a assinatura do signatário sobre a concatenação* $h||A||pk$*, usando sua chave privada* sk*.*

Definição 2 *Um Reconhecimento de Firma Completo é uma tupla* $RC = (id, v, y, f, t, nk, \delta)$*, onde id é um identificador único para RC,* $v > 0$ *é a versão atual do reconhecimento de firma, y é o resumo criptográfico da concatenação* $D||S$*, onde D é o documento assinado e S é a assinatura (cf. Definição 1), f é a data e hora do primeiro reconhecimento de firma, i.e.,* $v = 1$*, t é a data e hora da criação de* δ*, nk é um identificador único da chave pública do Notário,* δ *é a assinatura do Notário sobre a concatenação* $id||v||y||f||t||nk$*. Para* $v = 1$*,* $f = t$*.*

Definição 3 *Um Reconhecimento de Firma Parcial é uma tupla* $RP = (id, v, y, W, f, t, nk, \delta)$*, onde id é um identificador único para RP,* $v > 0$ *é a versão atual do reconhecimento de firma, y é o resumo criptográfico da concatenação* $h||S$*, onde h é o resumo criptográfico do documento assinado e S é a assinatura (cf. Definição 1), W é um conjunto de instâncias de h usando diferentes algoritmos de resumo criptográfico onde* $|W| = v$*, f é a data e hora do primeiro reconhecimento de firma, i.e.,* $v = 1$*, t é a data e hora da criação de* δ*, nk é um identificador único da chave pública do Notário,* δ *é a assinatura do Notário sobre a concatenação* $id||v||y||W||f||t||nk$*. Para* $v = 1$*,* $f = t$*.*

3.4 PROCEDIMENTOS

3.4.1 Gerenciamento de Notários

Gerenciamento de notários refere-se às tarefas realizadas pelo Operador de Esquema. Elas compreendem basicamente o registro de notários e alterações na situação de serviços confiáveis.

A Figura 2 demonstra o procedimento de registro de um notário. No passo (1), o notário fornece ao operador de esquema sua chave pública e sua documentação. No passo (2) o operador de esquema registra o notário na Lista de Situação de Serviços Confiáveis (LSC), incluindo para tanto sua chave pública, um conjunto de atributos extraídos da documentação e definindo a situação do serviço.

Um Notário é responsável pela geração de seu próprio par de chaves. No entanto, tamanhos de chave e os algoritmos empregados devem estar de acordo com as exigências do Operador de Esquema.

O Notário é listado como um Provedor de Serviços Confiáveis (PSC) na LSC. Sua chave pública serve como *identidade digital do serviço* (Campo *service digital identity* da especificação (ETSI, 2009)) e a situação do serviço é definida como “em conformidade” (Situação “in accordance” da especifica-

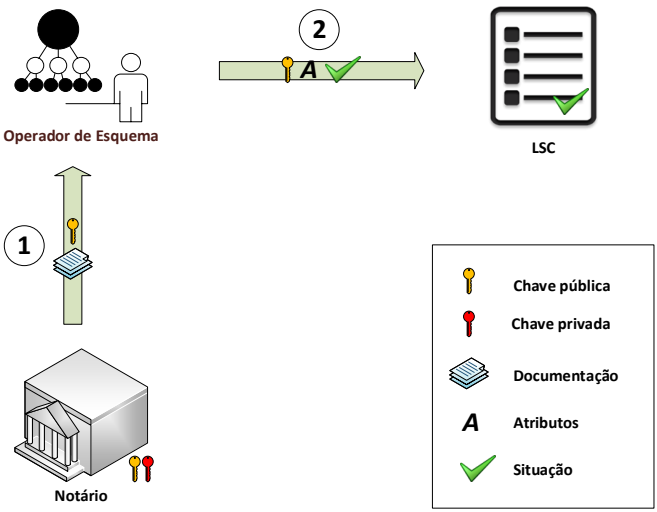

Figura 2: Registro de notário

ção (ETSI, 2009)). O Operador de Esquema pode mais tarde alterar a situação do serviço se necessário. Exemplos de tais situações incluem uma suspensão temporária ou a revogação do serviço. Neste último caso, o Notário precisa gerar um novo par de chaves e prover sua nova chave pública ao Operador de Esquema para que este a inclua na LSC e assim reabilite o serviço.

O par de chaves de um Notário não tem um período de validade fixo. Contudo, o Operador de Esquema pode revogar a situação de *conformidade* do Notário a qualquer momento. Isso geralmente ocorre se a chave privada do Notário é comprometida ou se os algoritmos criptográficos usados na geração de chaves estão próximos de se tornarem inseguros. Também existe a possibilidade de o Operador de Esquema aplicar uma politica de renovação periódica do par de chaves dos notários.

Se ocorrer de um Notário encerrar suas operações, a situação do serviço é alterado para “revogado” (Situação “revoked” da especificação (ETSI, 2009)) ou “não renovado” (Situação “not renewed” da especificação (ETSI, 2009)). Nesse caso, todos os dados armazenados relativos aos reconhecimentos de firma realizados por ele devem ser absorvidos por outro Notário. Informação relativas ao Notário receptor dos dados (identificador de chave, endereço, ...) devem ser incluídas por meio de uma extensão no campo de extensões de informação do serviço (Campo *service information extensions*

da especificação (ETSI, 2009)).

A avaliação dos notários, assim como o gerenciamento e implementação da LSC estão sujeitos à legislação local e/ou políticas organizacionais. Contudo, é recomendável que as normas existentes (ETSI, 2009) sejam respeitadas.

3.4.2 Gerenciamento de Usuários

O gerenciamento de usuários é realizado pelo Notário e compreende o registro de usuários e a atualização dos registros.

A Figura 3 demonstra o procedimento de registro de um usuário. Esse registro se dá em uma única interação, onde o usuário fornece ao notário sua chave pública e sua documentação.

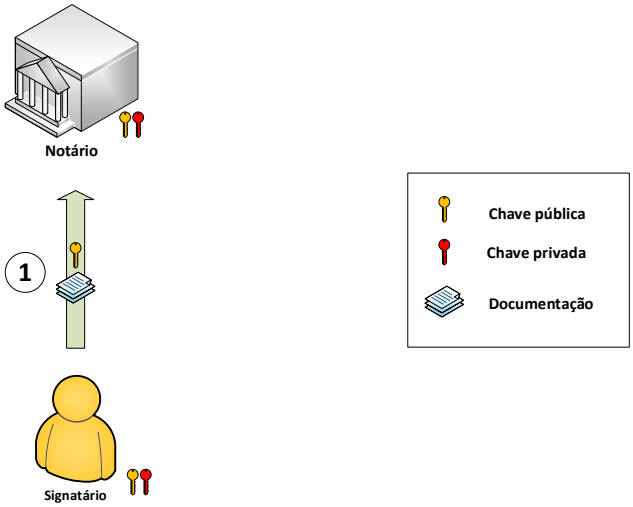

Figura 3: Registro de usuário

O Notário inicia o processo de registro verificando a documentação apresentada pelo usuário. Em seguida ele coleta os atributos e a chave pública do usuário. Atributos podem variar de informações pessoais como nome, data de nascimento e número da carteira de motorista até informações profissionais como o cargo dentro de uma organização e assim por diante. Eles podem ainda compreender quaisquer outras informações que o usuário julgar impor-

tantes, desde que a devida documentação comprovando sua veracidade seja apresentada. O Notário também exige do usuário uma prova de posse da chave privada por meio de um desafio resposta criptográfico ou outro mecanismo externo..

O registro de um usuário é atualizado quando há mudanças nos atributos ou se o par de chaves precisar ser substituído. Uma substituição de par de chaves ocorre quando a chave privada do usuário é comprometida ou quando os algoritmos utilizados em sua geração estão próximos de se tornarem inseguros. No caso de comprometimento de chave, o Notário suspende a emissão de novos reconhecimentos de firma para essa chave tão logo notificado pelo usuário. No caso de algoritmos em fim de vida, novos reconhecimentos de firma são suspensos para todas as chaves geradas com esses algoritmos. A emissão de reconhecimentos de firma é retomada com o registro de um par de chaves substituto. O Notário pode ainda exigir a substituição do par de chaves periodicamente ou baseado na quantia de vezes em que uma chave foi usada.

O usuário tem a possibilidade de manter múltiplas chaves registradas ao mesmo tempo. Adicionalmente, ele pode estipular restrições para a quantia de vezes que uma chave específica pode ser utilizada.

3.4.3 Assinatura

A Figura 4 demonstra em um único passo o procedimento de assinatura. Em suma, o signatário escolhe um documento a assinar e define quais de seu atributos pessoais são pertinentes a essa assinatura. Ele fornece ainda sua chave pública. A assinatura é então gerada com base na chave privada do signatário e um resumo criptográfico dos dados fornecidos.

Esse resumo criptográfico é calculado sobre a concatenação dos seguintes elementos: o resumo criptográfico do conteúdo, h, um conjunto contendo os atributos do signatário, A, e a chave pública do signatário, pk. A pode, opcionalmente, ser composto por apenas um subconjunto dos atributos do signatário levando em consideração a relevância dos mesmos para com o conteúdo sendo assinado. O valor da assinatura resultante, σ, em conjunto aos elementos assinados compõem o contêiner de assinatura S:

$$S = (h, A, pk, \sigma)$$

O signatário pode usar um par de chaves gerado previamente ou gerar um novo no momento da assinatura. Para que a assinatura possa ser reconhecida, a chave pública relacionada precisa primeiro ser registrada no estabelecimento notarial escolhido. Uma vez registrada, essa chave pode ser utilizada

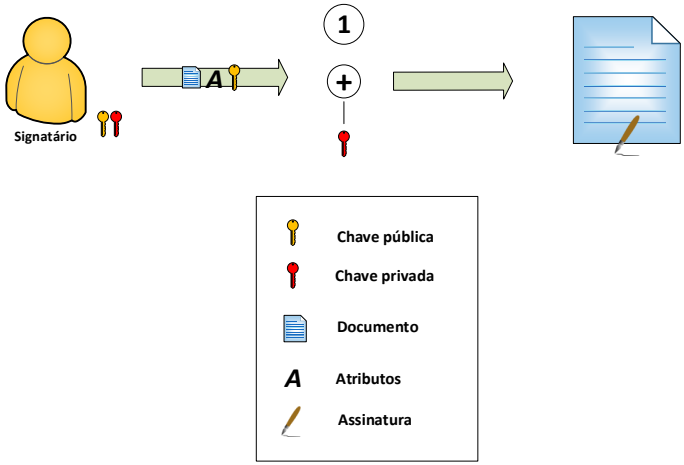

Figura 4: Assinatura

múltiplas vezes, i.e., reconhecimentos de firma futuros não requerem um novo registro de chave.

3.4.4 Reconhecimento de Firma

O reconhecimento de firma é basicamente a assinatura de uma terceira-parte que engloba o documento assinado, a assinatura e a data e hora atuais. Ele serve igualmente como uma afirmação de validade e um carimbo do tempo. Dessa forma, ele confirma a identidade e/ou os atributos declarados pelo signatário e atesta para a existência prévia da assinatura em relação a um determinado ponto no tempo.

A Figura 5 demonstra o procedimento de reconhecimento de firma em 3 passos: (1) A requisição de reconhecimento de firma, onde o usuário envia ao notário o documento com a assinatura; (2) A geração do reconhecimento de firma, onde o notário valida a assinatura, adiciona o tempo corrente e aposta sua própria assinatura; (3) O retorno do reconhecimento ao usuário que o requisitou.

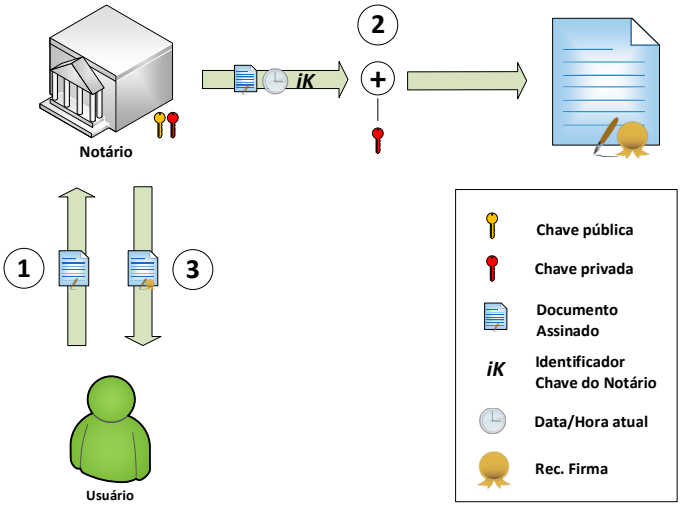

Figura 5: Reconhecimento de firma

Um Reconhecimento de Firma pode ser do tipo Completo ou Parcial. O reconhecimento de firma completo segue o protocolo abaixo:

$$\mathscr{U} \longrightarrow \mathscr{N} : (D, S)$$
$$\mathscr{N} \longrightarrow \mathscr{U} : \underbrace{(id, v, y, f, t, nk, \delta)}_{RC}$$

Um usuário solicita um reconhecimento de firma enviando ao Notário a assinatura, S, e o documento assinado, D. O Notário primeiramente identifica o signatário com base na chave pública presente na assinatura. Se a chave pertence a um usuário registrado, ele confere os atributos declarados pelo signatário e verifica a assinatura com a chave pública do usuário. Se a verificação for bem sucedida um reconhecimento de firma é gerado.

A primeira etapa para a geração do contêiner de reconhecimento de firma é o cálculo do resumo criptográfico do conteúdo, y, composto pelo documento assinado e pela assinatura. O próximo passo é a geração de um identificador único, id. Em seguida, o Notário adiciona a versão do reconhecimento de firma, v, que nesse momento deve ser 1, e a data e hora corrente, t. Como que se trata do primeiro reconhecimento de firma para a assinatura em questão, i.e., $v = 1$, f recebe o mesmo valor de t. Adicionalmente, o iden-

tificador da chave pública do Notário, *nk*, ié incluído no contêiner. Por fim, a assinatura englobando todos os elementos anteriores é gerada a partir da chave privada do Notário. O valor dessa assinatura, δ, também é incluído no contêiner de reconhecimento de firma. Antes de devolver o reconhecimento de firma ao usuário, o Notário o salva, juntamente com o documento assinado e a assinatura, em sua solução de armazenamento seguro.

Um Reconhecimento de Firma Parcial, por sua vez, é um reconhecimento de firma em que o Notário não tem acesso ao conteúdo do documento assinado. Ele segue o protocolo abaixo:

$$\begin{aligned} &\mathscr{U} \longrightarrow \mathscr{N} : (h, S) \\ &\mathscr{N} \longrightarrow \mathscr{U} : \underbrace{(id, v, y, W, f, t, nk, \delta)}_{RP} \end{aligned}$$

Ao solicitar um reconhecimento parcial, o usuário envia ao Notário o resumo criptográfico do documento, h, juntamente com a assinatura, S. O Notário procede basicamente da mesma forma que com um Reconhecimento de Firma Completo, a não ser pelas seguintes exceções:

- Ele não verifica a validade da assinatura com a chave pública do usuário. Para isto seria necessário estar em posse do documento assinado;
- Ele usa h em vez do documento assinado no cálculo do resumo criptográfico do conteúdo, y;
- Ele inclui o conjunto com os resumos criptográficos do documento assinado, W, no contêiner de reconhecimento de firma. Nesse momento, W é composto por um único elemento, h;
- Antes de devolver o reconhecimento de firma ao usuário, ele salva apenas a assinatura e o reconhecimento de firma em sua solução de armazenamento seguro.

Reconhecimentos de Firma Parciais são mais adequados para situações em que sigilo se faz necessário, ou para documentos com relevância temporária. Preservar a autenticidade de um reconhecimento de firma parcial a longo prazo requer que o usuário esteja constantemente ciente do nível de segurança dos algoritmos criptográficos envolvidos. Isso porque o usuário deve renovar o reconhecimento de firma antes que qualquer um dos algoritmos se torne inseguro.

É importante notar que qualquer um dos usuários, signatário ou verificador, podem solicitar um reconhecimento de firma para uma assinatura. O procedimento de renovação de Reconhecimento de Firma é descrito na Seção 3.4.6.

3.4.5 Validação de Assinatura

Para ser considerada confiável, uma assinatura precisa estar matematicamente e semanticamente correta. A assinatura é matematicamente correta se puder ser verificada com sucesso com a chave pública do signatário. Ela é semanticamente correta se o vínculo entre a chave pública do signatário e seus atributos era válido no momento da assinatura. Esse vínculo é atestado pelo reconhecimento de firma, o qual também precisa estar matematicamente e semanticamente correto. O reconhecimento de firma é matematicamente correto se puder ser verificado com sucesso com a chave pública do Notário. Ele é semanticamente correto se o serviço notarial estava "em conformidade" no momento do reconhecimento e continua nessa situação no momento da verificação da assinatura do usuário.

A Figura 6 demonstra as interações do procedimento de validação de assinatura. Passo (1): busca da situação e chave pública do notário com base em seu identificador de chave; passo (2): obtenção dos dados à partir da LSC.

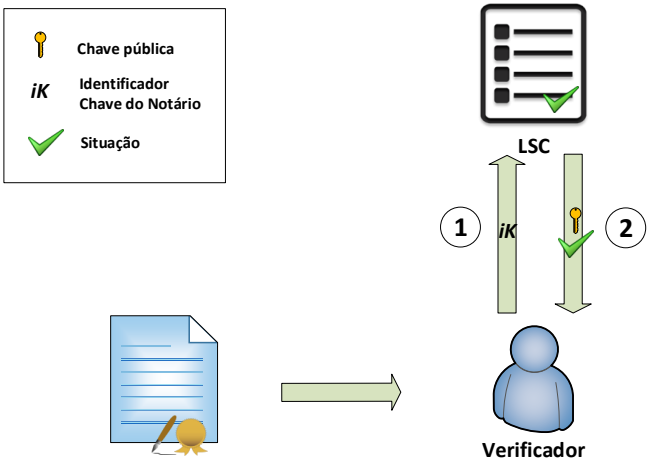

Figura 6: Validação de assinatura

De forma mais detalhada, dada uma assinatura *S* com um reconhecimento de firma completo *RC* (Definições 1, 2), o processo de validação de assinatura é composto das seguintes etapas:

1. *Validação de Notário*: O verificador usa o identificador da chave pública, *nk*, do reconhecimento de firma para checar se a chave correspondente identifica um Provedor de Serviços Confiável na LSC e se a situação atual do serviço é "em conformidade".

    1.1 *(OPCIONAL) Checagem de lista de confiança pessoal*: O verificador usa o identificador da chave pública, *nk*, para checar se o Notário está presente em sua lista pessoal de partes confiáveis.

2. *Validação de Reconhecimento de Firma:* O verificador verifica se o valor de assinatura, δ, está matematicamente correto. Ele usa como entrada desse processo o documento assinado, *D*, a assinatura, *S*, e os elementos assinados em *RC*, além da chave pública do Notário extraída da LSC.

Se as duas validações forem bem sucedidas, a assinatura é considerada confiável. Não há necessidade de verificar novamente se o valor de assinatura, σ, está matematicamente correto pois esta verificação já foi realizada pelo Notário durante o processo de reconhecimento de firma.

Na validação de uma assinatura *S* com um reconhecimento de firma parcial *RP* (Definições 1, 3), o processo de validação é composto pelas etapas 1 e 2 anteriores e pelas seguintes etapas adicionais:

3. *Detecção de colisão de resumo criptográfico:* O verificador calcula resumos criptográficos do documento assinado e os compara aos resumos presentes no campo *W*. Isto previne ataques de colisão de resumo.

4. *Validação da Assinatura do Usuário:* O verificador verifica se o valor de assinatura, σ, está matematicamente correto. Ele usa como entrada desse processo o documento assinado, *D*, e os elementos assinados em *S*, além da chave pública do signatário, *pk*.

Se todas as validações forem bem sucedidas, a assinatura é considerada confiável.

3.4.6 Renovação de Reconhecimento de Firma

Renovações de reconhecimentos de firma são necessárias quando: (i) a situação de conformidade do Notário é revogada ou (ii) os algoritmos criptográficos utilizados não são mais seguros ou estão próximos de se tornarem inseguros. Em outras palavras, não é mais possível aferir se o reconhecimento de firma é semanticamente correto.

A Figura 7 demonstra o procedimento de renovação do reconhecimento assinatura. Passo (1): busca do endereço eletrônico atualizado do serviço notarial com base em seu identificador de chave; passo (2): obtenção dos dados à partir da LSC; passo (3): requisição de renovação do reconhecimento de firma com base no identificador do reconhecimento antigo; passo (4): geração de novo reconhecimento de firma; passo (5): retorno do reconhecimento renovado ao usuário que o requisitou.

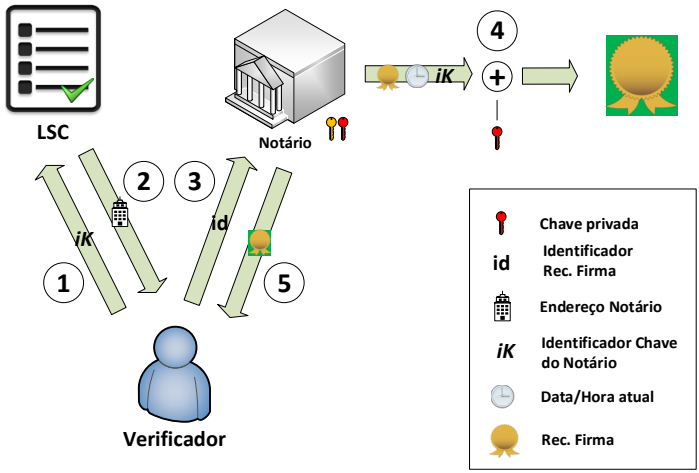

Figura 7: Renovação de reconhecimento de firma

Existem ligeiras diferenças entre o processo de renovação para Reconhecimentos de Firma Completos e Reconhecimentos de Firma Parciais. A renovação de um reconhecimento completo segue o protocolo abaixo:

$$\mathscr{U} \longrightarrow \mathscr{N} : id$$
$$\mathscr{N} \longrightarrow \mathscr{U} : \underbrace{(id, v, y, f, t, nk, \delta)}_{RC}$$

Um usuário solicita uma renovação de reconhecimento de firma enviando ao Notário o identificador do reconhecimento de firma, id. O Notário busca o respectivo reconhecimento de firma, juntamente com a assinatura e o documento assinado, em sua solução de armazenamento. Ele então calcula o resumo criptográfico do conteúdo, y, composto pelo documento assinado e

pela assinatura. Em seguida, ele gera um novo contêiner de reconhecimento de firma. Ele usa os mesmos valores da instância original para *id* e f. Adicionalmente, ele incrementa a versão do reconhecimento de firma, v, e inclui a data e hora correntes, t, e o identificador da chave pública atual do Notário, nk. Por final, o Notário assina todos os elementos anteriores com sua chave privada e inclui o valor de assinatura, δ, no contêiner de reconhecimento de firma. Antes de devolver o reconhecimento ao usuário, o Notário também substitui o reconhecimento de firma em sua solução de armazenamento pelo novo.

A renovação do reconhecimento de firma parcial segue o protocolo abaixo:

$$\begin{aligned} \mathscr{U} &\longrightarrow \mathscr{N} : (h_n, id) \\ \mathscr{N} &\longrightarrow \mathscr{U} : \underbrace{(id, v, y, W, f, t, nk, \delta)}_{RP} \end{aligned}$$

Ao solicitar a renovação de um reconhecimento de firma parcial, o usuário envia ao Notário um novo resumo criptográfico do documento, h_n, e o identificador do reconhecimento de firma, id. O Notário busca o respectivo reconhecimento de firma, juntamente com a assinatura, em sua solução de armazenamento. Ele então verifica se pelo menos um dos resumos criptográficos do documento contidos em W continua seguro, i.e., o algoritmo criptográfico utilizado continua seguro. Essa verificação previne colisões intencionais do documento assinado. Se a verificação for bem sucedida, o Notário renova o reconhecimento de firma. O restante do processo de renovação segue os mesmos passos da renovação do reconhecimento completo, com exceção de dois detalhes:

- Ele usa h_n em lugar do documento assinado no cálculo do resumo criptográfico do conteúdo, y;
- Ele inclui h_n no conjunto de resumos criptográficos do documento assinado, W;

É importante notar que um Reconhecimento de Firma Completo pode ser renovado em qualquer ponto no tempo, mesmo depois de os algoritmos criptográficos terem se tornado inseguros, pois o notário está em posse do documento assinado. O Reconhecimento de Firma Parcial, por outro lado, precisa ser renovado enquanto o algoritmo utilizado no cálculo de resumo criptográfico continua seguro. Caso contrário, o notário não tem mais como garantir que o novo resumo criptográfico enviado junto à requisição de renovação é mesmo do documento assinado originalmente. Portanto ele não

poderá efetuar a renovação. Adicionalmente, a responsabilidade de solicitar a renovação de reconhecimentos de firma é do verificador.

3.5 CONSIDERAÇÕES

Neste capítulo foi proposto um novo modelo de assinatura digital baseado em reconhecimentos de firma. Este modelo é inspirado nas assinaturas manuscritas convencionais, portanto delega a notários a responsabilidade de certificar, ou seja, prover garantias de autenticidade, integridade e evidência cronológica para uma assinatura digital.

Foram descritas as entidades envolvidas: o Signatário; o Verificador; o Notário e o Operador de Esquema. Também foram delineadas as suposições que dão base à proposta e definidas de forma conceitual as estruturas de um contêiner de assinatura e de reconhecimento de firma. Por fim foram detalhados os procedimentos envolvidos: Gerenciamento de Notários; Gerenciamento de Usuários; Assinatura; Reconhecimento de Firma; Validação de Assinatura e Renovação de Reconhecimento de firma.

Essa proposta buscou apresentar um modelo de assinatura digital que fosse fácil e conveniente para o usuário final, afim de possibilitar a adoção do documento eletrônico em conjunto à assinatura digital por uma parte mais significativa da população. Por esse motivo, ela foi projetada de forma a resolver quatro problemas chave existentes no modelo de assinatura digital convencional. No próximo capítulo é feita uma avaliação da proposta a fim de concluir se esses problemas são efetivamente resolvidos.

4 AVALIAÇÃO DO MODELO PROPOSTO

No Capítulo 2 foi estabelecido que os Problemas 1 (Custos de preservação) e 2 (Confiança em entidades antigas) já foram abordados nas propostas *Cumulative Notarization* (LEKKAS; GRITZALIS, 2004), *Optimized Certificate* (CUSTÓDIO et al., 2008) e *NBPKI* (VIGIL et al., 2013). Contudo, o Problema 3 (Complexidade do processo de assinatura) é apenas parcialmente abordado pela NBPKI e o Problema 4 (Modelo de confiança) permanece intocado. No restante deste capítulo, a nova proposta é avaliada em relação a todos os quatro problemas (Seções 4.1, 4.2, 4.3 e 4.4). São descritas também vantagens adicionais trazidas pelo modelo proposto (Seção 4.5). Por último, na Seção 4.6 são apresentadas as considerações.

4.1 PROBLEMA 1 (CUSTOS DE PRESERVAÇÃO)

Afim de comparar os custos de preservação a longo prazo de assinaturas digitais convencionais e de assinaturas com reconhecimento de firma foi realizado um ensaio com base em três cenários distintos:

(a) Uma ICP básica de um único nível. Essa ICP possui uma única AC emitindo certificados para os usuários e uma única ACT emitindo carimbos do tempo (Figura 8);

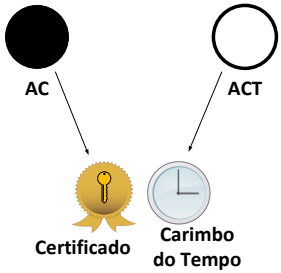

Figura 8: ICP nível único

(b) Uma ICP multinível composta de uma AC Raiz com uma AC e uma ACT abaixo, no segundo nível (Figura 9);

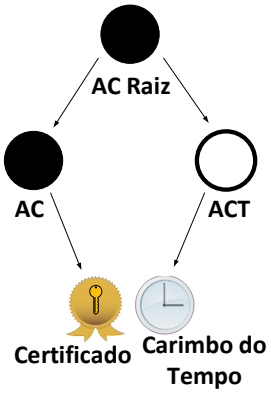

Figura 9: ICP multinível

(c) Um Notário emitindo reconhecimentos de firma parciais (c.f. Definição 3) para assinaturas (Figura 10).

Figura 10: Notário

Adicionalmente, consideremos que os carimbos do tempo em (a) e (b) tem validade de 5 anos e que, devido à obsolescência de algoritmos, os reconhecimentos de firma em (c) precisam ser renovados em média a cada 15 anos.

Em (a), o conjunto inicial de evidências criptográficas necessárias para preservar a validade da assinatura a longo prazo é composto de: carimbo do tempo, certificado do signatário, certificado da AC, certificado da ACT e si-

tuação de revogação do certificado do signatário. Adicionalmente, a cada 5 anos um novo carimbo do tempo e um certificado da ACT são adicionados ao pacote. Em (b) o conjunto inicial de evidências criptográficas é composto de: carimbo do tempo, certificado do signatário, certificado da ACT, certificado da AC Raiz e situações de revogação dos certificados do signatário e da AC. A cada 5 anos um novo carimbo do tempo e novo certificado da ACT são adicionados ao pacote, acompanhados ainda da situação de revogação do certificado da ACT anterior. Em (c) a única evidência criptográfica armazenada pelo usuário é um reconhecimento de firma. Ele é substituído, em média, a cada 15 anos.

A Figura 11 ilustra a tendência para a quantidade de evidências criptográficas acumuladas em cada cenário ao longo de um período de 40 anos. A figura mostra um crescimento linear na quantidade de evidências criptográficas armazenadas nos cenários (a) e (b), enquanto no cenário (c) apenas um reconhecimento de firma precisa ser contabilizado.

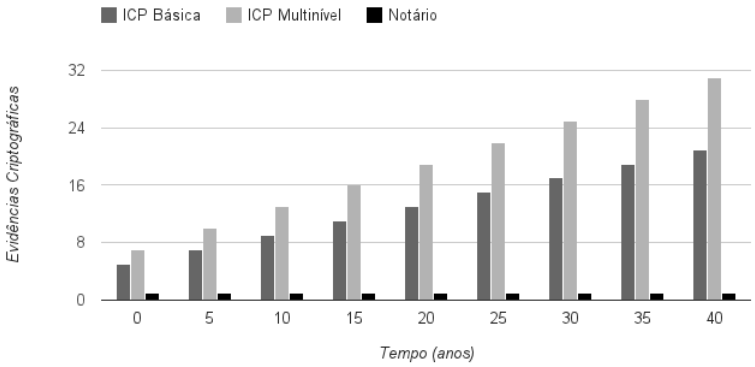

Figura 11: Evidências criptográficas por assinatura

O impacto real dessa diferença entre os cenários é evidenciado nas Tabelas 2, 3, e 4. Elas mostram uma estimativa do custo de armazenamento (em KB) de uma assinatura junto aos elementos necessários para preservá-la por um período de 40 anos nos cenários (a), (b) e (c).

Para esta estimativa foram levados em consideração os tamanhos médios de certificados e LCRs obtidos no repositório da ICP-Brasil (Ramo V2)[1]. Para assinaturas, carimbos do tempo e reconhecimentos de firma foi considerado o tamanho de uma assinatura no formato XAdES mínima, sem atributos,

[1] http://www.iti.gov.br/icp-brasil/certificados/

Elemento	Quantidade	Tamanho (KB)
Assinatura	1	2.4
Cert. Signatário	1	3
Cert. AC	1	2.3
LCR AC	1	483.9
Carimbo Tempo	8	19.2
Cert. ACT	8	18.4
Total	20	529.2

Tabela 2: Custo de armazenamento: Cenário (A)

Elemento	Quantidade	Tamanho (KB)
Assinatura	1	2.4
Cert. Signatário	1	3
Cert. AC Raiz	1	2.3
LCR AC Raiz	8	0.85
Carimbo Tempo	8	19.2
Cert. ACT	8	13.6
Cert. AC	1	1.7
LCR AC	1	483.9
Total	28	532.9

Tabela 3: Custo de armazenamento: Cenário (B)

utilizando o algoritmo de assinatura RSA com SHA1 e chave de 2048 bits.

Após 40 anos, é possível notar que a diferença no custo de armazenamento entre os cenários (a) e (b) é pequena, em torno de 0,7%, dado que o elemento de maior impacto é a LCR da AC que emite certificados para os usuários finais, que tem o mesmo tamanhos nos dois casos. No entanto a diferença relativa de custo entre os cenários (a) ou (b) e o cenário (c) é extremamente significativa, com uma redução em torno de 99% no cenário (c).

Há de se considerar, certamente, o impacto desse custo de armazenamento em termos práticos. Dada a capacidade de armazenamento de computadores, servidores e dispositivos móveis atuais, aliada ainda à rápida proliferação de serviços de armazenamento em nuvem, esse custo não é problemático para a maioria dos usuários. Ele é significativo apenas para usuários com um grande volume de assinaturas, como tribunais, empresas de grande porte e outros.

Elemento	Quantidade	Tamanho (KB)
Assinatura	1	2.4
Rec. Firma	1	2.4
Total	2	4.8

Tabela 4: Custo de armazenamento: Cenário (C)

Contudo, todos os tipos de usuários são beneficiados pelo ganho de eficiência no cenário (c), já que o número de operações criptográficas necessárias para realizar a validação das evidências criptográficas é reduzido.

4.2 PROBLEMA 2 (CONFIANÇA EM ENTIDADES ANTIGAS)

O comprometimento da chave privada do notário (que é indicado pela LSC), ou a obsolescência de algoritmos criptográficos, são razões que levam o verificador a renovar o reconhecimento de firma. De qualquer forma, durante o processo de validação de assinatura, ele só precisa confiar na chave do notário utilizada para assinar o reconhecimento de firma mais recente. As partes confiáveis anteriores não são mais necessárias no processo de validação.

4.3 PROBLEMA 3 (COMPLEXIDADE DO PROCESSO DE ASSINATURA)

O processo de assinatura proposto é projetado de forma que um uso simples ou ocasional seja fácil e exija pouco conhecimento por parte do usuário. Isso é ilustrado pelo exemplo abaixo.

Consideremos o exemplo de um pai e seu filho. O pai presenteia o filho com um automóvel, mas o mantêm registrado em seu próprio nome. Algum tempo depois, o filho se muda para outra cidade e leva o automóvel consigo. Certo dia, o filho recebe uma ótima oferta pelo automóvel, mas ela só é válida para aquele dia. Nessa situação, ele precisa de uma procuração assinada por seu pai para poder realizar a transferência do automóvel para o novo dono, mas, devido à restrição de tempo, enviar o documento por meio de uma correspondência não é uma opção viável.

Agora, assumindo que o pai não possui experiência prévia com assinaturas digitais, apliquemos uma implementação hipotética de nossa proposta: O pai vai a um computador e começa por baixar e abrir o software de assinatura (ou acessa uma versão do aplicativo na web). Ele então seleciona o

documento de procuração, preenche seu nome, seleciona o estabelecimento notarial mais próximo (ou aquele que ele costuma usar para autenticação de assinaturas manuscritas) na lista fornecida pelo software e clica em "assinar". O software então apresenta um código a ser anotado (ou impresso) e instruções para que o pai se dirija ao estabelecimento notarial para completar seu registro. Já no estabelecimento notarial, ele apresenta ao notário seus documentos pessoais e código recebido ao final da assinatura. De volta à sua casa, o pai acessa novamente o o software de assinatura, seleciona o documento assinado e clica em "reconhecer firma". Para completar, ele só precisa informar o endereço de email do filho e clicar em "enviar".

Nesse processo, várias coisas aconteceram sem o conhecimento do pai. Primeiro, o software baixou a versão mais recente da LSC. Em seguida, quando o pai clicou em "assinar", um par de chaves para uso único foi gerado, a assinatura foi criada, uma solicitação de registro contendo a chave pública foi enviada ao serviço online do notário e este, por sua vez, enviou de volta um desafio de prova de posse cifrado com essa chave pública. O software de assinatura, então, decifrou o desafio com a chave privada e apresentou o código resultante ao pai. Quando o pai clicou em "reconhecer firma", a assinatura foi enviada ao serviço do notário, que automaticamente a verificou, realizou o reconhecimento de firma e o enviou de volta. Por fim, a chave privada usada no processo foi destruída, eliminando assim qualquer necessidade posterior de gerenciamento ou revogação de chave.

Levando em consideração que o verificador nesse exemplo será o funcionário público responsável por inspecionar transferências de veículos, qualquer notário reconhecido pelo governo, i.e., presente na LSC, terá a confiança necessária.

O ponto chave demonstrado nesse exemplo é que agora o usuário está apto a assinar um documento de forma fácil, sem ter que aprender acerca de certificados, novas autoridades, ou mesmo que ele possui um par de chaves criptográficas. Em outras palavras, a complexidade é absorvida pelas aplicações. Além disso o usuário deixa de ser refém da chave privada, ou seja, não precisa se preocupar em guardar a chave de forma segura pois ela pode ser destruída imediatamente após a realização da assinatura.

No caso de usuários mais experientes, ou aqueles com uma demanda regular por assinaturas digitais, o modelo possibilita o uso da mesma chave múltiplas vezes. Possibilita também o registro de múltiplas chaves, cada uma para um propósito específico, e o estabelecimento de restrições para o número de utilizações permitido para uma determinada chave. Pequenas e médias empresas são exemplos desse tipo de usuário. Elas podem verificar quais são os notários em que cada um de seus principais clientes e fornecedores confia e então registrar chaves nesses estabelecimentos notariais. Em cidades

pequenas onde há apenas um notário o cenário é ainda mais simples. Outra aplicação possível é o registro de uma chave de backup de uso único para emergências. Por exemplo, um determinado usuário possui uma chave de "uso frequente" registrada e a chave privada correspondente armazenada no computador em sua casa. Então, durante uma viajem ao exterior, ele precisa assinar algo com urgência. Nesse caso ele pode usar sua chave de backup, previamente registrada, para a qual ele carrega a chave privada cifrada com uma senha em seu celular. Dessa forma, apenas um reconhecimento de firma será gerado e a chave privada pode ser destruída.

No que diz respeito à manutenção de assinaturas, o uso do Reconhecimento de Firma Completo (c.f. Definição 2) proporciona a manutenção mais fácil. Verificadores não precisam estar cientes da segurança dos algoritmos usados no processo de assinatura porque um reconhecimento de firma completo pode ser renovado em qualquer ponto no tempo. O software realizando uma validação de assinatura pode até solicitar uma renovação de reconhecimento de firma automaticamente, sem a interação do usuário. Reconhecimentos de Firma Parciais (c.f. Definição 3), em contrapartida, precisam ser renovados antes que os algoritmos criptográficos utilizados se tornem inseguros. Portanto, o usuário final precisa estar mais consciente da complexidade subjacente ao processo de assinatura do que com reconhecimentos de firma completos. O processo de renovação nesse caso até pode ser automaticamente gerido por um software de arquivamento especializado, contudo, este precisa ficar online todo o tempo para buscar informações atualizadas à respeito da segurança de algoritmos e para solicitar as renovações junto aos notários.

4.4 PROBLEMA 4 (MODELO DE CONFIANÇA)

Na ICP, a confiança tem uma característica booleana. Uma possibilidade é confiar na AC Raiz, e consequentemente em tudo que está baixo dela. Isso pode incluir centenas de autoridades certificadoras, autoridades de registro e autoridades de carimbo do tempo. Essas entidades podem ser controlados pelo governo, pela iniciativa privada ou uma mistura de ambos, com a influência de interesses políticos e comerciais, possivelmente conflitantes. A outra possibilidade é não confiar na AC Raiz, e por consequência não utilizar o aparato de assinatura digital.

Nossa proposta, por outro lado, possibilita diferentes níveis de confiança para diferentes entidades. Em primeiro lugar, o verificador tem a liberdade de escolher em quem depositar confiança para certificar a autenticidade de uma assinatura dentre a gama de notários existentes. Em segundo lugar, ele tem a possibilidade de estabelecer uma relação direta entre confiança e risco.

Em outras palavras, o verificador pode aceitar confiar em um determinado notário para certificar uma assinatura com base no risco de perdas pessoais agregadas ao documento assinado. Portanto documentos que envolvem baixo risco requerem pouca confiança enquanto documentos com maior risco agregado requerem maior confiança no notário responsável pela certificação da assinatura.

Uma construtora, por exemplo, pode estabelecer uma política interna em que as assinaturas em contratos envolvendo projetos pequenos podem ser autenticadas por qualquer notário listado na LSC. Mas para assinaturas em contratos com seus grandes fornecedores, a empresa aceita apenas reconhecimentos de firma emitidos por um notário específico com quem mantém um relacionamento comercial de longa data. Esse notário é especializado em reconhecimentos de firma de assinaturas digitais, empregando pessoal e tecnologias de segurança equivalentes ao que se emprega em uma Autoridade Certificadora de grande porte.

A proposta permite ainda que assinaturas nem passem pelo processo de reconhecimento de firma quando isto não for necessário. Isso se dá em casos onde existe um relacionamento de confiança entre signatário e verificador ou onde o documento em questão é de baixa relevância. Isso é análogo ao caso de muitos documentos em papel onde as firmas não precisam ser reconhecidas em cartório. A principal função desse tipo de assinaturas é garantir a integridade do documento e a chave privada é destruída logo em seguida à geração da assinatura.

4.5 VANTAGENS ADICIONAIS

Assinaturas digitais com reconhecimento de firma oferecem algumas vantagens adicionais se comparadas a assinaturas digitais tradicionais, dependentes de ICPs X509. Descrevemos essas vantagens a seguir:

4.5.1 Revogação de chave efetiva

A partir do momento que o usuário solicita ao notário a revogação de seu par de chaves, este interrompe imediatamente a emissão de reconhecimentos de firma para assinaturas feitas com aquele par de chaves. Em outras palavras, nenhuma nova assinatura autêntica pode ser gerada a partir desse momento. Em contrapartida, assinaturas dependentes de certificados ainda podem ser criadas mesmo depois de um certificado ser revogado. A efetividade da revogação, nesse caso, implica em todo mundo obter a versão atu-

alizada da situação de revogação do certificado e aplicá-la corretamente na validação de assinatura, o que é difícil de ser garantido.

4.5.2 Transferência do fardo do armazenamento de evidências

Uma característica importante da proposta é que o fardo do armazenamento das evidências criptográficas é transferido do usuário final para o notário. A fim de avaliar a viabilidade disso estimou-se o custo desse armazenamento com base na consulta do número médio de atos notarias praticados por um estabelecimento notarial por ano. Foram utilizados os dados da Escrivania de Paz do 4° Subdistrito de Florianópolis - SC, localizada próxima à Universidade Federal de Santa Catarina. A consulta foi realizada por meio do site do Conselho Nacional de Justiça[2].

Nesse estabelecimento, realizam-se em média 277618 atos notariais por ano. Considerando que para cado um desses atos fosse armazenada uma assinatura e um reconhecimento de firma, seguindo o custo estabelecido para tal na Seção 4.1, ao final de 40 anos o custo total de armazenamento seria de cerca de 50 GB. Em termos práticos esse é um custo muito pequeno, mesmo para a situação atual. Considerando a tendência de aumento da capacidade e redução do preço dos dispositivos de armazenamento observada ao longo das últimas décadas, esse custo se torna cada vez menos relevante.

Dessa forma, o usuário pode ficar livre da preocupação de guardar e gerenciar assinaturas e evidências criptográficas sem impor custos impeditivos ao notário que passa a realizar essa tarefa.

4.5.3 Atributos de signatário especificáveis dinamicamente

Os atributos do signatário, i.e., A (c.f., Definição 1), contidos em cada assinatura podem ser escolhidos especificamente por sua relevância ao conteúdo e/ou objetivo do documento assinado. Por exemplo, alguns tipos de documentos poderiam requirir apenas o nome do signatário, enquanto outros necessitam também números e endereços ou até informação de autorização como cargo organizacional e credenciais diversas.

[2] http://www.cnj.jus.br/corregedoria/justica_aberta/?

4.5.4 Evidências históricas

Ao armazenar todas as assinaturas e reconhecimentos de firma, e guardar alguns metadados adicionais, o Notário é capaz de prover informações úteis para casos de resolução de disputas. Considerando, por exemplo, um Notário que salva dados relativos ao endereço IP de origem e a data e hora em que um reconhecimento de firma foi solicitado. Se um usuário contestar uma de suas assinaturas, alegando que sua chave privada foi roubada, os dados armazenados pelo Notário, combinados a evidências externas, podem ajudar a confirmar se a alegação é verdadeira ou não.

4.5.5 Estruturas de dados coerentes

Normas modernas para assinaturas digitais, tais como CAdES (ETSI, 2013) e XAdES (ETSI, 2010) permitem que dezenas de elementos opcionais sejam incluídos no contêiner de assinatura. O problema disso é que muitos desses elementos são projetados para dar suporte às regras de negócio de alguns tipos específicos de aplicações. Em outras palavras, o contêiner de assinatura carrega informação que não é necessariamente essencial à assinatura em si. Isso torna os procedimentos de validação de assinatura desnecessariamente complexos.

Nós mantivemos nossos contêineres de assinatura tão simples quanto possível, carregando apenas dados que são relevantes para a própria assinatura.

4.6 CONSIDERAÇÕES

Neste capítulo foi realizada uma avaliação da proposta apresentada no Capítulo 3. Foi possível constatar que o modelo de Assinatura Digital com Reconhecimento de Firma atende aos quatro problemas levantados inicialmente e ainda traz algumas vantagens adicionais. A Tabela 5 faz uma nova comparação entre propostas, agora com a inclusão do modelo de assinatura apresentado neste trabalho junto às propostas anteriores da literatura revistas no Capítulo 2.

Adicionalmente, dadas as Suposições 2 e 3 em que a proposta está ancorada (estabelecimentos notariais bem distribuídos geograficamente e armazenamento seguro), cabem também algumas considerações relativas a custo e desafios de implementação.

Um estabelecimento notarial requer algum espaço de escritório, pes-

Proposta	Problema 1	Problema 2	Problema 3	Problema 4
Sobrep. de Notarizações	✓*	✓		
Certificado Otimizado	✓	✓		
NBPKI	✓	✓	✓*	
A.D com Rec. de Firma	✓	✓	✓	✓

Tabela 5: Comparação de Propostas

soal extra no caso de alta demanda e ainda equipamento especializado, incluindo servidores, dispositivos criptográficos, soluções de armazenamento e equipamentos de contingência. Em países que utilizam o sistema jurídico romano-germânico, esses estabelecimentos já estão instalados e supridos de pessoal. Nesse caso, apenas equipamento adicional e treinamento são requeridos. Em países onde não existe essa infraestrutura, ou no caso de a proposta ser aplicada dentro de um ambiente fechado, i.e., uma empresa privada, o impacto seria maior.

De qualquer forma, a implantação de uma ICP X509 também requer um investimento substancial. E uma Autoridade Registradora também precisa espalhar escritórios para atender ao público. Além disso, o nível das exigências de segurança de uma Autoridade Certificadora está relacionado a sua importância, i.e., a segurança em uma AC na base da hierarquia tende a ser mais branda se comparada a uma AC Raiz. O mesmo se aplica a estabelecimentos notariais. Quanto maior a abrangência e o número de clientes do estabelecimento, ou dependendo do tipo de negócio em que esses clientes operam, tanto maior a exigência de segurança.

Em relação à solução de armazenamento, a implementação de um armazenamento seguro é um desafio. Contudo, à medida que estabelecimentos notariais começarem a migrar para um ambiente sem papel, é natural supor que eles terão que adquirir tais capacidades de qualquer forma. Outros serviços realizados por notários também exigem que documentos sejam guardados por longos períodos e de forma segura. A mesma situação se aplica a tribunais, instituições governamentais e muitas empresas. Adicionalmente, o nível de segurança dos dados armazenados pode ser um diferencial no marketing do estabelecimento. Vigil et al. fazem em (VIGIL et al., 2012) uma avaliação das abordagens existentes para garantir autenticidade, integridade e evidência cronológica no arquivamento de dados a longo prazo. Abordagens para sigilo a longo prazo são descritas em (BRAUN et al., 2012).

5 CONSIDERAÇÕES FINAIS

Este trabalho teve início com o desafio de tornar o uso de documentos eletrônicos e assinaturas digitais mais acessível à usuários leigos e usuários eventuais. Ele também parte do pressuposto de que o modelo de assinatura digital deve se assemelhar mais ao modelo de assinatura manuscrita convencional, onde a autenticidade das assinaturas é garantida por meio de atos notariais.

Afim de delimitar o escopo do trabalho, no Capítulo 2, foram listados os principais problemas presentes no modelo de assinatura digital vigente que dificultam sua adoção por parte de usuários leigos e eventuais. São eles: 1) A manutenção de assinaturas a longo prazo é custosa, tanto em termos de armazenamento quanto em processamento; 2) É preciso confiar em âncoras de confiança antigas durante todo o tempo de vida de uma assinatura; 3) Processos de assinatura dependentes de ICPs X509 são complexos e inconvenientes para usuários finais; 4) O modelo de confiança exigido por esses processos não retrata a forma como relações de confiança normalmente são estabelecidas.

Averiguamos também que existem propostas na literatura que tratam de alguns desses problemas, mas nenhuma delas engloba todos os 4. Esse estudo evidenciou a necessidade da elaboração de uma nova proposta mais abrangente, que ao mesmo tempo pudesse fazer uso das soluções existentes e tratar dos problemas em aberto.

Tal proposta foi apresentada no Capítulo 3. Trata-se de um redesenho do modelo de assinatura digital como um todo. A proposta dá foco às necessidades do usuário final, deixando signatário e verificador livres para definir os requisitos de uma assinatura e para estabelecer suas próprias relações de confiança. São eles que escolhem o notário no qual vão depositar confiança. Isso vem em contraste aos processos de assinatura digital tradicionais com sua estrutura impositiva, tanto em relação ao tipo de atributos que as assinaturas devem conter quanto à âncora de confiança a ser utilizada. Desse modo, o modelo se aproxima das práticas de assinatura e modelos de confiança convencionais culturalmente estabelecidas em grande parte do mundo.

No Capítulo 4, por fim, fez-se uma avaliação da proposta em relação aos 4 problemas levantados. Com isso foi possível constatar que ela atende a todos os problemas, atingindo assim os objetivos específicos do trabalho que estão diretamente relacionados a esses problemas. Também é possível verificar que o modelo proposto permite que um usuário realize uma assinatura sem necessidade de registro prévio e a autentique posteriormente com um notário de sua escolha, atingindo em parte o objetivo geral.

Contudo, na etapa de avaliação foi encontrada a maior dificuldade, e por consequência, a maior limitação do trabalho. Constatou-se que, apesar de aparentemente ser o caso, não é possível afirmar de forma realista que o modelo proposto seja rápido e fácil para o usuário. Para isso seria necessário despender um grande esforço de implementação de sistemas e alocação de recursos para realizar uma avaliação de usabilidade com usuários reais. Isso foge do escopo do presento trabalho, mas é discutido em mais detalhes abaixo na Seção de trabalhos futuros.

A adoção dessa proposta requer a elaboração de um novo conjunto normativo, a implementação de novas soluções de software e a revisão dos aspectos legais de assinaturas digitais. Isso requer um grande esforço, mas a visão do autor é de que isto trará melhores resultados do que continuar tentando consertar e adaptar uma infraestrutura antiga, proposta para um propósito e uma realidade diferente da atual.

5.1 TRABALHOS FUTUROS

Os trabalhos futuros podem ser divididos em duas áreas, a técnica e a jurídica/normativa. Na parte técnica o primeiro passo é a implementação de protótipos de aplicações para um ambiente de testes. Isso inclui sistemas servidores de serviços para a Lista de Estado de Serviços Confiáveis (LSC) e para o estabelecimento notarial e aplicações clientes para a geração e verificação de assinaturas. Com isso é possível validar as estruturas de dados e protocolos propostos e fazer os ajustes necessários.

O segundo passo é a extensão dos protótipos para a implantação de um projeto piloto em estabelecimentos notarias reais, com usuários reais. Nessa etapa deve ser conduzida a avaliação de usabilidade do modelo de assinatura de forma a comprovar o mérito da proposta.

Paralelamente é preciso realizar um estudo para avaliar o impacto jurídico da proposta. Se ela se adéqua ou não ao atual arcabouço legal regendo assinaturas digitais, e quais as mudanças necessários. A partir dos resultados de uma prova de conceito com um amostra de usuários reais e o estudo jurídico é possível partir para a criação de um conjunto normativo e implementação em larga escala.

REFERÊNCIAS BIBLIOGRÁFICAS

ADAMS, C. et al. *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*. IETF, ago. 2001. RFC 3161 (Proposed Standard). (Request for Comments, 3161). Updated by RFC 5816. Disponível em: <http://www.ietf.org/rfc/rfc3161.txt>.

BAYER, D.; HABER, S.; STORNETTA, W. Improving the efficiency and reliability of digital time-stamping. *Sequences II: Methods in Communication, Security, and Computer Science*, Citeseer, p. 329–334, 1993.

Brasil. *Medida provisoria no 2.200-2, de 24 de agosto de 2001*. 2001.

BRAUN, J. et al. *Long Term Confidentiality: a Survey*. 2012. Cryptology ePrint Archive, Report 2012/449. `http://eprint.iacr.org/`.

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). Updated by RFC 6818. Disponível em: <http://www.ietf.org/rfc/rfc5280.txt>.

COSTA, V. *Análise da Confiança do Sistema de Protocolização Digital de Documentos Eletrônicos*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2003.

CUSTÓDIO, R. et al. Optimized certificates–a new proposal for efficient electronic document signature validation. In: *Public Key Infrastructure*: 5th European PKI Workshop: Theory and Practice, EuroPKI 2008 Trondheim, Norway, June 16-17, 2008 Proceedings. [S.l.]: Springer Berlin Heidelberg, 2008, (Lecture Notes in Computer Science). p. 49–59.

DAMGARD, I. Collision free hash functions and public key signature schemes. In: SPRINGER-VERLAG (Ed.). *Proceedings of the 6th annual international conference on Theory and application of cryptographic techniques*. [S.l.: s.n.], 1987. p. 203–216.

DEMéTRIO, D. B. *Infra-estrutura para Protocolização Digital de Documentos Eletrônicos*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2003.

DIAS, J. S. *Confiança no Documento Eletrônico*. Tese (Doutorado) — Universidade Federal de Santa Catarina, 2004.

DIFFIE, W.; HELLMAN, M. New directions in cryptography. *IEEE Transactions on information Theory*, v. 22, n. 6, p. 644–654, 1976.

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.

ETSI. *Provision of harmonized Trust-service status information*. 3.1.2. [S.l.], 2009.

ETSI. *XML Advanced Electronic Signatures (XAdES)*. 1.4.2. [S.l.], 2010.

ETSI. *CMS Advanced Electronic Signatures (CAdES)*. 2.1.1. [S.l.], 2013.

European Parliament, Council. *Directive 1999/93/ec of the european parliament and of the council of 13 december 1999 on a community framework for electronic signatures*. 2000. 12-20 p.

GUTMANN, P. Pki: it's not dead, just resting. *Computer*, IEEE, v. 35, n. 8, p. 41–49, 2002.

HABER, S.; STORNETTA, W. How to time-stamp a digital document. In: . [S.l.]: Springer Berlin Heidelberg, 1991, (Lecture Notes in Computer Science, v. 537). p. 437–455.

Instituto Nacional de Tecnologia da Informação (ITI). *Visão Geral Sobre Assinaturas Digitais na ICP-Brasil.* 2010. DOC-ICP-15.

Instituto Nacional de Tecnologia da Informação (ITI). *Revista Digital*. Setembro 2011. Disponível em: <http://www.iti.gov.br/images/publicacoes/revista-digital/revista_digital-2011-1.pdf>.

Instituto Nacional de Tecnologia da Informação (ITI). *Infraestrutura de Chaves Públicas Brasileira (ICP-Brazil)*. 2013. `http:/www.iti.gov.br/icp-brasil`.

ITU-T. *Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks*. 6th. ed. [S.l.], 2008.

JOHNSON, D.; MENEZES, A.; VANSTONE, S. The elliptic curve digital signature algorithm (ecdsa). *International Journal of Information Security*, Springer, v. 1, n. 1, p. 36–63, 2001.

KOHNFELDER, L. M. *Towards a practical public-key cryptosystem*. Tese (Doutorado) — Massachusetts Institute of Technology, 1978.

LEKKAS, D.; GRITZALIS, D. Cumulative notarization for long-term preservation of digital signatures. *Computers Security*, v. 23, n. 5, p. 413 – 424, 2004. ISSN 0167-4048. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0167404804001014>.

LISE, W. *The Practice of Using Seals in Japan*. dez. 2011. Disponível em: <http://www.lise.jp/seals.html>.

LOPEZ, J.; OPPLIGER, R.; PERNUL, G. Why have public key infrastructures failed so far? *Internet Research*, Emerald Group Publishing Limited, v. 15, n. 5, p. 544–556, 2005.

MERRYMAN, J.; PÉREZ-PERDOMO, R. *The civil law tradition: an introduction to the legal systems of Europe and Latin America*. [S.l.]: Stanford University Press, 2007.

MOECKE, C. T. *NBPKI: Uma ICP baseada em Autoridades Notariais*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2011.

NOTOYA, A. E. *IARSDE: Infra-estrutura de armazenamento e recuperação segura de documentos eletrônicos*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2002.

PASQUAL, E. S. *IDDE*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2001.

Rede Nacional de Ensino e Pesquisa (RNP). *Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEdu)*. 2013. `http://www.rnp.br/servicos/icpedu.html`.

RIVEST, R.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, ACM, v. 21, n. 2, p. 126, 1978.

SANTESSON, S. et al. *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*. IETF, jun. 2013. RFC 6960 (Proposed Standard). (Request for Comments, 6960). Disponível em: <http://www.ietf.org/rfc/rfc6960.txt>.

SILVA, N. da. *Preservação por Longo Prazo de Assinaturas Digitais*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2011.

United States. *Electronic Signature in Global and National Commerce Act ("E-Sign")*. 2000. Disponível em: <http://uscode.house.gov/download/pls/15C96.txt>.

United States. *Government Paperwork Elimination Act ("GPEA")*. 2000. Disponível em: <http://www.archives.gov/records-mgmt/policy/electronic-signature-technology.html>.

VIGIL, M. A. G. *Certificados Otimizados*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2010.

VIGIL, M. A. G. et al. *Authenticity, Integrity and Proof of Existence for Long-Term Archiving: a Survey*. 2012. Cryptology ePrint Archive, Report 2012/499. `http://eprint.iacr.org/`.

VIGIL, M. A. G. et al. The notary based pki – a lightweight pki for long-term signatures on documents. In: *Public Key Infrastructures, Services and Applications*: 9th European Workshop, EuroPKI 2012, Pisa, Italy, September 13-14, 2012, Revised Selected Papers. [S.l.]: Springer Berlin Heidelberg, 2013, (Lecture Notes in Computer Science). p. 85–97.

WERLANG, F. C.; VIGIL, M. A. G.; CUSTóDIO, R. F. A user-centric digital signature scheme. In: *Public Key Infrastructures, Services and Applications*: 10th European Workshop, EuroPKI 2013, Egham, UK, September 12-13, 2013, Revised Selected Papers. [S.l.]: Springer Berlin Heidelberg, 2014, (Lecture Notes in Computer Science). p. 152–169.