UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Cristian Thiago Moecke

NBPKI - UMA ICP BASEADA EM AUTORIDADES NOTARIAIS

Florianópolis
2011

Cristian Thiago Moecke

NBPKI - UMA ICP BASEADA EM AUTORIDADES NOTARIAIS

Dissertação submetida ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina para a obtenção do grau de mestre em Ciência da Computação.

Prof. Ricardo Felipe Custódio, Dr.
Orientador

Florianópolis
2011

Cristian Thiago Moecke

NBPKI - UMA ICP BASEADA EM AUTORIDADES NOTARIAIS

Esta dissertação foi julgada adequada para a obtenção do título de mestre em Ciência da Computação, área de concentração Sistemas de Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina.

Florianópolis, 14 de julho de 2011

Prof. Mário Antônio Ribeiro Dantas, Dr.
Coordenador do Curso

Banca Examinadora:

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

Prof. Ricardo Dahab, Dr.
Universidade Estadual de Campinas

Prof. Frank Augusto Siqueira, Dr.
Universidade Federal de Santa Catarina

Prof. João Bosco Mangueira Sobral, Dr.
Universidade Federal de Santa Catarina

Dedico este trabalho a Deus,
que me sustenta em todos momentos.
A minha Família, que me acompanhou
e apoiou até aqui.
E a minha noiva e futura esposa,
por todo amor, carinho, compreensão,
paciência e parceria.

AGRADECIMENTOS

Agradeço ao Professor Ricardo Felipe Custódio, por todo apoio e incentivo à realização deste trabalho, bem como pela oportunidade de integrar sua equipe no LabSEC.

Também à equipe do LabSEC por todo apoio e por tudo que aprendi com eles neste período. Em especial a Patrícia Dousseau, pela colaboração no desenvolvimento de um protótipo, objeto de Trabalho de Conclusão de Curso, que permitiu avaliar e definir os rumos da concepção deste trabalho. Ao Jonathan Kohler e Marcelo Carlomagno Carlos pelas colaborações, sugestões e opiniões na elaboração do trabalho.

Agradeço ainda a Rede Nacional de Ensino e Pesquisa (RNP), Câmara Brasileira de Comércio Eletrônico (Câmara-e.net), Instituto de Tecnologia da Informação (ITI) e Colégio Notarial do Brasil, Seção São Paulo (CNB-SP) pelo apoio aos projetos nos quais participei durante a elaboração deste trabalho.

"Sê humilde para evitar o orgulho, mas voa alto para alcançar a sabedoria.". Agostinho de Hipona

RESUMO

Infraestrutura de Chaves Públicas tem sido implementadas considerando o tradicional modelo de certificação digital baseado em serviços tais como autoridades de registro, autoridades de carimbo do tempo e autoridades certificadoras: um certificado digital certificando uma chave é somente emitido pela autoridade certificadora após a verificação pela autoridade de registro dos atributos da chave e de sua posse pelo titular. Nesse modelo, certificados podem ser revogados, o que implica, necessariamente, pela parte confiante, na verificação do seu status, antes que possa ser usado tanto para a verificação de um *token* de autenticação quanto para a verificação de uma assinatura digital. Esse modelo tem sido regulamentado e amplamente utilizado tanto por empresas e governos de todo o mundo quanto integrado em sistemas computacionais. Este trabalho apresenta uma visão crítica deste modelo, o que tem dificultado e encarecido sua adoção, bem como das alternativas existentes na literatura. Também apresenta-se uma nova alternativa ao modelo - denominada de Infraestrutura de Chaves Públicas baseadas em Autoridades Notariais - eliminando-se processos e serviços complementares que deixam de ser necessários. Mostra-se que o novo modelo é mais simples de ser implementado, mais fácil de se definir um justo modelo de negócio, além de simplificar o processo de verificação de assinatura.

Palavras-chave: Infraestrutura de Chaves Públicas, Autoridade Notarial, Caminho de Certificação, Assinatura Digital

ABSTRACT

Public Key Infrastructure has been implemented considering the traditional model based on digital certification services such as registration authorithies, time stamping, and certification authorities: a digital certificate certifying a key is only issued by the certification authority after verification by the registration authority of the key attributes and their possession by the holder. In this model, certificates can be revoked, which necessarily involves. for the confident part, verification of the certificate status before it can be used both for verifying an authentication token and to verify a digital signature. This model has been regulated and widely used by both businesses and governments around the world and integrated into computer systems. This work presents a critique of this model, which is more difficult and expensive for adoption, and also the existing alternatives available on the literature. It also presents a new alternative model - known as Notary Based Public Key Infrastructure (NBPKI) based on Notarial Authorities - eliminating redundant processes and services. It is shown that the new model is simpler to implement, easier to set a fair business model and streamline the process of signature verification.

Keywords: Public Key Infrastructures, Notary Authority, Certification Path, Signature

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ALGORITMOS

LISTA DE ABREVIATURAS E SIGLAS

AC	Autoridade Certificadora
ACT	Autoridade de Carimbo do Tempo
AN	Autoridade Notarial
ASN.1	*Abstract Notation One*
CAdES	*CMS Advanced Electronic Signatures*
CMS	*Cryptographic Message Syntax*
CRS	*Certificate Revocation Status*
DER	*Distinguished Encoding Rules*
ETSI	*European Telecommunications Standards Institute*
HTTP	*Hypertext Transfer Protocol*
ICP	Infraestrutura de Chaves Públicas
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
KGC	*Key Generating Center*
LabSEC	Laboratório de Segurança em Computação
LCR	Lista de Certificados Revogados
NA	*Notary Authorithy*
NBPKI	*Notary Based Public Key Infrastucture*
OCSP	*Online Certificate Status Protocol*
SCVP	*Simple Certificate Validation Protocol*
SPKI	*Simple Public Key Infrastructure*
XAdES	*XMLdSIG Advanced Digital Signatures*
XML	*Extensible Markup Language*
XMLdSig	*XML-Signature Syntax and Processing*

SUMÁRIO

1 INTRODUÇÃO

Infraestruturas de Chaves Públicas (ICPs, também amplamente conhecidas pelo termo inglês *PKI – Public Key Infrastuctures*) são uma alternativa já consolidada para fornecer a capacidade de estabelecimento de relações de confiança entre entidades envolvidas em uma transação em meio digital. Um dos usos mais comuns e difundidos das ICPs é o estabelecimento de confiança na navegação em sítios de internet (SSL/TLS) (DIERKS; RESCORLA, 2008; RESCORLA et al., 2010), que é uma aplicação de certificação digital utilizada frequentemente por usuários de internet, mesmo que estes muitas vezes nem ao menos entendem o que são ICPs. Existem muitas outras aplicações para ICPs, em grandes domínios, relações entre governos, empresas e pessoas ou como parte interna de sistemas computacionais.

Mais recentemente as ICPs tem ganho espaço também para a autenticação entre pessoas físicas e jurídicas. Processos que antes dependiam de documentos impressos em papel com assinaturas manuscritas estão sendo desmaterializados, ou seja, passados ao meio digital. A autenticidade e integridade nestes contextos é garantida por assinaturas digitais, que tem como base ICPs.

Uma ICP típica é formada de entidades que são detentoras de um par de chaves criptográficas assimétricas. A chave privada é mantida sob sigilo e controle exclusivo de cada entidade, e a chave pública é divulgada amplamente. As ICPs preocupam-se especialmente com a associação destas chaves públicas as respectivas identidades de cada entidade. Para atingir este objetivo existem diversos modelos de ICP, que serão expostos no decorrer deste trabalho. Destacam-se o X.509(COOPER et al., 2008), PGP(ZIMMERMANN, 1995), SPKI(ELLISON et al., 1999) e IBC(BOYEN; MARTIN, 2007). O mais proeminente desses modelos é o X.509 por ter sido ao longo do tempo adotado pelas empresas e governos para a emissão de certificados digitais para pessoas, instituições, sistemas e equipamentos. Ao leitor que não estiver familizarizado com estas e outras bases da criptografia assimétrica e certificação digital, recomenda-se a leitura do capítulo 2 que aborda os conhecimentos necessários para a compreensão deste trabalho.

No Brasil, destaca-se a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) (ITI, 2007) que provê presunção de veracidade jurídica a documentos assinados digitalmente com certificados digitais emitidos sob sua cadeia (BRASIL, 2001). Isso tem motivado o crescente uso da certificação digital, por exemplo, para assinatura digital de documentos eletrônicos. Diversos tribunais de Justiça do País já digitalizam seus processos através do uso de certificação digital para conferir autenticidade e integridade aos documentos envolvidos. Da mesma forma outros governos tem suas próprias iniciativas similares (STATE, 1999; STATES,

2000), além do uso de ICPs para desmaterialização de processos em empresas e outros domínios mais restritos.

Entretanto, o crescimento do uso das ICPs nestes novos contextos trouxe a tona uma série de limitações e dificuldades relacionadas à sua implantação e uso. Concebidas para serem flexíveis, as ICPs são difíceis de implementar, necessitam de demasiados recursos humanos e computacionais para mantê-las e muitas vezes mesmo na presença desses recursos não conseguem prover serviços confiáveis a longo prazo. Por isso, o mercado acaba muitas vezes preferindo adotar soluções alternativas mais eficientes, mesmo abrindo mão de importantes requisitos de segurança oferecidos pelas ICPs (GUTMANN, 2002). Discutiremos as limitações e problemas das ICPs atuais com mais detalhes no capítulo 3.

Linn (LINN, 2004) resumiu as razões que limitam o crescimento do uso das ICPs em três categorias:

- A pequena oferta de serviços que demandam os recursos oferecidos por ICPs;
- A forma que as ICPs atuais foram projetadas tornam-las difíceis de serem implementadas e dificultam a prestação de serviços pela ICP, tornando-as pouco atrativas diante de outras soluções alternativas existentes;
- A implantação de uma ICP implica em níveis de segurança muito mais elevados do que os que seriam apropriados ou com boa relação de custo/benefício em muitos contextos.

Os três pontos levantados tem um denominador comum: complexidade. A concepção demasiadamente generalista das ICPs, em especial a ICP x.509, fez com que esta se tornasse muito complexa, oferecendo serviços que a maioria dos cenários não necessita, tornando-as difíceis de implementar e com custo/benefício elevado, além de levarem complexidade desnecessária para os usuários finais. Uma Infraestrutura de Chaves Públicas deveria, tal qual outras infraestruturas com as quais diariamente lidamos (telecomunicações, etc.), ser totalmente transparente para o usuário final. Este está interessado em um serviço simples e fácil, sem necessitar tomar decisões complexas ou deparar-se constantemente com erros com os quais não pode lidar.

Um dos aspectos de maior complexidade em ICPs X.509 é a construção e validação de caminho de certificação. Para a validação de um certificado é necessária: a identificação de um caminho de certificados até uma âncora de confiança; a obtenção destes certificados; a validação das respectivas assinaturas digitais e verificação das informações de expiração e situação de revogação de cada certificado deste caminho. A complexidade é maior quanto maior for o tamanho da cadeia de certificação. São vários possíveis pontos de falha envolvidos, e em eventuais indisponibilidades ou erros o usuário da ICP tem de tomar decisões muitas vezes difíceis demais (STRAUB, 2006).

Ainda há mais pontos de complexidade envolvidos. Usualmente uma assinatura digital de um documento eletrônico contém carimbos do tempo para fornecer uma evidência temporal confiável de que a assinatura foi produzida quando o caminho de certificação era válido. Isso é fundamental para documentos eletrônicos cujas assinaturas devem ser verificáveis mesmo após a expiração ou revogação do certificado do signatário e até mesmo da sua cadeia de certificação. Entretanto o carimbo do tempo é, essencialmente, mais um documento assinado. E desta forma, tem os mesmos problemas e desafios da assinatura digital comum.

A Figura 1.1 representa as entidades e artefatos envolvidos na validação de um documento assinado digitalmente sob uma ICP tradicional com carimbo de tempo. Bolas representam entidades, e setas artefatos produzidos pelas entidades (por exemplo: certificados, LCRs, Carimbos de Tempo). Nota-se a grande quantidade de informações utilizadas para atestar a confiabilidade da assinatura digital aplicada no documento. Discutiremos de forma mais ampla os problemas relacionados à isso e as abordagens de solução existentes no decorrer deste trabalho.

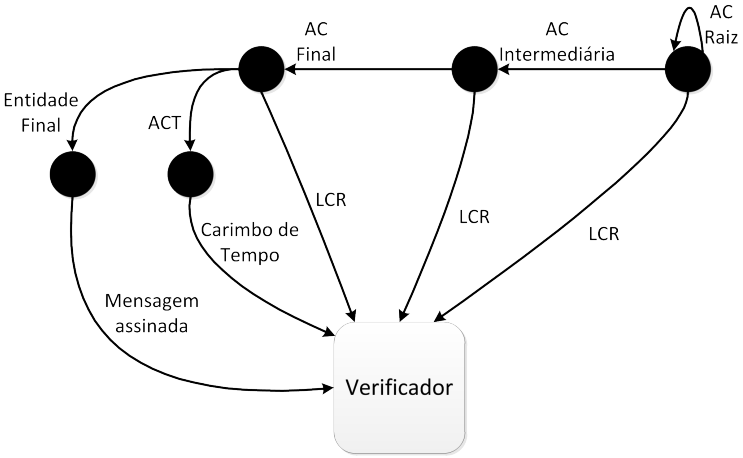

Figura 1.1: Um documento assinado em uma ICP tradicional

O que o presente trabalho propõe é um novo modelo de certificação digital, através do uso de certificados digitais autoassinados e a substituição das Autoridades Certificadoras (AC) finais por Autoridades Notariais (AN). Chamamos este modelo de NBPKI, sigla de *Notary Based Public Key Infrastructure*, tradução em inglês de "Infraestrutura de Chaves Públicas Baseada em Notários". Esta ICP faz uso de certificados autoassinados e também de provas de validade de curta duração obtidas online através das Autoridades Notariais. Apesar de já existirem outros modelos de certificação que utilizam certificados autoassinados (ZIMMERMANN, 1995) ou de curta duração (ELLISON et al., 1999) e ainda sistemas de validação online (FREEMAN et al., 2007), o que é proposto

neste trabalho é completamente diferente, conforme demonstraremos. A Figura 1.2 apresenta as entidades e artefatos por elas produzidos envolvidos na validação de um documento assinado sob essa nova abordagem de ICP.

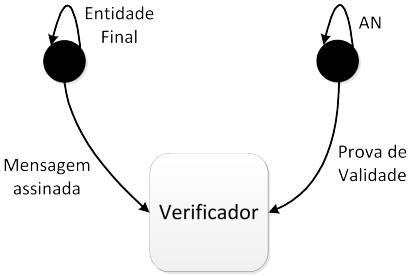

Figura 1.2: Um documento assinado no modelo proposto de ICP

Quando uma AC do modelo X.509 emite um certificado, pressupõe-se que ele seja válido por um determinado período do tempo determinado pela validade incluída pela AC nos dados do certificado. Entretanto, essa suposição não é correta uma vez que o certificado pode ser revogado a qualquer momento. Portanto, é necessária uma prova de que continua válido. Normalmente utilizam-se como prova listas de certificados revogados, uma lista publicada online e cuja localização *online* é indicada por uma URL também incluída no certificado. No caso de indisponibilidade desta lista ou de outra forma de verificar o estado de revogação de um certificado, não se pode afirmar que este certificado continua válido.

Considerando que é necessária a obtenção desta prova de validade, defendemos que o certificado não deve ser considerado válido quando emitido, mas sim somente na presença de uma prova. Assim, não há necessidade do certificado ser emitido por uma autoridade certificadora. Por razões práticas e de simplicidade, propomos que os certificados sejam emitidos por seus titulares, ou seja, autoassinados. Isso quer dizer que não haveria mais uma autoridade certificadora para a emissão dos certificados para o usuário final. Propomos ainda que as provas sejam de curta duração, e vinculadas às assinaturas digitais dos documentos eletrônicos, tornando desnecessário o uso de carimbos do tempo. Neste último caso a prova é válida para um determinado instante de tempo.

Isso muda completamente o modelo de certificação e, conforme será arguido neste trabalho, vários do problemas das ICPs tradicionais deixam de existir, além de tornar a ICP mais flexível e de menor custo de implantação. Tudo isso sem prejuízo dos serviços esperados de uma ICP.

1.1 OBJETIVOS

Propor uma nova abordagem de Infraestrutura de Chaves Públicas adequada para conservação em longo prazo de assinaturas digitais, sem

perder a generalidade esperada de uma ICP. Avaliar o modelo proposto quanto a sua eficiência e segurança e também compará-lo com outras abordagens existentes na literatura.

1.1.1 Objetivos Específicos

- Propor um modelo de Infraestrutura de Chaves Públicas;
- Avaliar a segurança e eficiência do modelo proposto;
- Comparar a abordagem com outros modelos já existentes na literatura;

1.2 MOTIVAÇÃO

A abordagem apresentada neste trabalho motiva-se na busca em se aproximar da expectativa comum de um usuário de infraestruturas de chaves públicas ao assinar documentos eletrônicos - ou seja: simplesmente a confirmação de uma terceira parte sobre a identidade do signatário. É opinião do autor que as abordagens existentes e em uso tornam a assinatura digital demasiadamente complexa, e a presente proposta permite simplificar muito a realização, validação e conservação de uma assinatura digital.

1.3 CONTRIBUIÇÕES

O presente trabalho apresenta uma nova abordagem em Infraestruturas de Chaves Públicas, inédita na literatura. Esta abordagem é definida e avaliada. O modelo é então comparado com outros modelos e soluções existentes na literatura, e seus benefícios e limitações são apresentados.

1.4 METODOLOGIA E ORGANIZAÇÃO DO TRABALHO

O trabalho inicia com a revisão de artigos, dissertações, normas e artigos técnicos relacionados à Infraestruturas de Chaves Públicas. Nestes, se buscará a visualização do cenário atual da certificação digital e suas principais limitações e dificuldades, muitas destas já observadas pelo autor na sua vivência com o tema.

Com base nisso, os principais problemas serão delimitados, bem como soluções atuais existentes e suas respectivas limitações.

Em seguida, será proposta uma nova abordagem de solução.

Por fim, será efetuado um comparativo e análise crítica dos resultados alcançados, com relação a outras abordagens existentes na literatura.

O capítulo 2 apresenta uma breve revisão sobre os principais conceitos de criptografia e infraestruturas de chaves públicas necessários para a compreensão do trabalho. Em seguida, no capítulo 3 são analisadas as

limitações e deficiências dos modelos de ICP utilizados atualmente. No capítulo 4 são visitados e revisados outros trabalhos, recentes e mais antigos, que buscam resolver problemas discutidos no capítulo anterior. No capítulo 5 apresenta-se a nova abordagem proposta por este trabalho, e esta é comparada com as abordagens existentes no capítulo 6. Os resultados obtidos são analisados no capítulo 7. Por fim, no capítulo 8 são apresentadas considerações finais e proposições de trabalhos futuros.

1.5 PUBLICAÇÕES

Parte dos resultados deste trabalho foram publicados em artigo no 10^o Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), realizado em Fortaleza-CE, nos dias 11 a 15 de outubro de 2010, com o título "Uma ICP baseada em certificados digitais autoassinados" (MOECKE et al., 2010).

2 CRIPTOGRAFIA E CERTIFICAÇÃO DIGITAL

Este capítulo apresenta uma revisão dos principais conceitos de criptografia e segurança da informação necessários para a compreensão do trabalho.

2.1 CRIPTOGRAFIA SIMÉTRICA

"Cripto" vem do grego "kryptos" e significa oculto, envolto, escondido. Também do grego, "graphos" significa escrever. Portanto *criptografia* pode ser entendido como *escrita oculta*, ou *ocultar o que foi escrito*. A *criptologia*, por sua vez, é o estudo da criptografia e suas aplicações.

Trata-se de uma técnica bastante antiga, que surgiu da necessidade de registrar e transmitir informações de maneira sigilosa. No princípio consistia no embaralhamento de letras, e mais tarde em operações matemáticas sobre números (por exemplo, informações binárias de um computador) que representam uma informação.

Uma aplicação da criptografia é a *cifragem*, que consiste no uso de criptografia para ocultar uma mensagem. O processo inverso, de recuperar uma mensagem a partir de um texto cifrado, é chamado de *decifragem*. Comumente a operação de cifragem faz uso de um parâmetro extra, além da própria mensagem, que é chamado de *chave*. Neste caso, a mensagem só pode ser decifrada com a posse da chave correta. Este tipo de operação, ilustrado pela Figura 2.1, recebe o nome de cifragem simétrica. Criptografia simétrica é o conjunto das técnicas de criptografia que fazem uso de uma única chave que é usada tanto na cifragem quanto na decifragem.

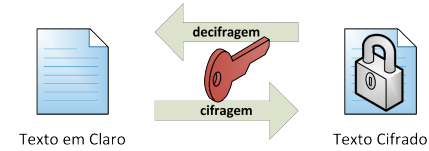

Figura 2.1: Operação de cifragem simétrica

2.2 CRIPTOGRAFIA ASSIMÉTRICA

A chave é um parâmetro importante dos algoritmos de cifragem, porém, a existência deste parâmetro leva ao problema da gestão e distribuição de chaves, que consiste no armazenamento e transmissão segura da chave com acesso apenas a quem é autorizado. Quando se deseja utilizar criptografia para cifrar uma comunicação entre duas entidades em

locais distantes, é necessário que a chave que cifrará esta comunicação seja previamente combinada, através de um canal seguro, entre as partes envolvidas.

Fruto do trabalho publicado por Diffie e Helmann em 1976 (DIFFIE; HELLMAN, 1976), a criptografia assimétrica permite a solução deste problema. Ao invés de uma chave compartilhada entre as partes envolvidas na comunicação, utilize-se um *par de chaves*: a chave pública (que, conforme o nome diz, não é secreta) e a chave privada (secreta, deve ser mantida em sigilo). Geradas adequadamente, o que é cifrado com o uso da chave pública somente pode ser decifrado com o uso da chave privada correspondente, e vice-versa. Um atacante, sem conhecimento da chave privada, não conseguirá decifrar mensagens interceptadas, conforme ilustrado na Figura 2.2.

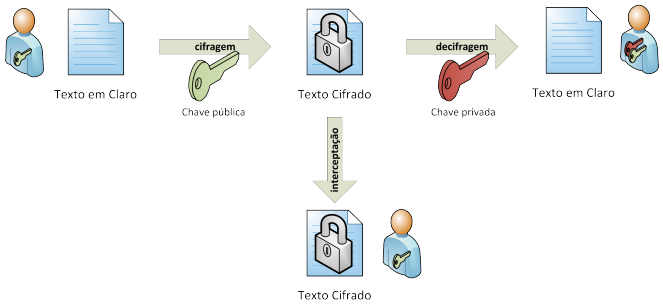

Figura 2.2: Operação de cifragem assimétrica

Vários algoritmos de criptografia assimétrica tem sido propostos, entretanto o mais utilizado atualmente ainda continua sendo o primeiro algoritmo proposto, denominado RSA. Além deste, começam a ganhar espaço os algoritmos baseados em Curvas Elípticas, como o ECDSA.

2.3 ASSINATURA DIGITAL

Uma aplicação importante da criptografia assimétrica é chamada de *assinatura digital*. Esta é baseada nas propriedades obtidas pelo uso invertido das chaves na operação de cifragem assimétrica, ou seja: a mensagem passa a ser cifrada com a chave privada. Deste modo, qualquer pessoa em posse da mensagem e da chave pública correspondente, poderá decifrar a mensagem. Logo, não há sigilo nesta operação uma vez que a chave para decifragem é pública, mas três outras propriedades importantes surgem:

Autenticidade O verificador, ao receber a mensagem cifrada, decifra-a com a chave pública do signatário, e obtém a mensagem em claro. Como apenas o signatário detém a chave privada que poderia ter

gerado aquele texto cifrado, o verificador pode afirmar que a mensagem realmente foi originada pelo signatário;

Não-repúdio De maneira análoga, o signatário não pode negar que foi ele quem gerou a mensagem cifrada, sendo ele o único a dispor da chave privada;

Integridade A mensagem estando cifrada com a chave privada, não pode ter sido adulterada por um terceiro, pois isso impediria a decifragem com a chave pública.

Desta forma alcançam-se as propriedades necessárias para a realização de uma assinatura em meio digital. Esta pode ser utilizada para comprovar a autoria de uma determinada mensagem ou conteúdo digital. Porém, sendo a operação de criptografia assimétrica computacionalmente cara, esta tornaria-se inviável para grandes quantidades de dados. Para resolver esta questão, faz-se uso das funções de resumo criptográfico, bastante conhecidas também pelo termo inglês: funções *hash*.

2.3.1 Resumo Criptográfico (*hash*)

Uma função de resumo criptográfico consiste em uma função H que, toda vez que aplicada a uma mesma mensagem m, gera um mesmo valor $H(m)$ de tamanho fixo. A função de resumo criptográfico deve ser irreversível, ou seja, não deve ser possível obter m a partir de $H(m)$ ou obter-se duas mensagens diferentes $m_1 \neq m_2$ que tenham o mesmo resumo criptográfico $H(m_1) = H(m_2)$.

Com estas propriedades, pode-se utilizar as funções de resumo criptográfico sobre a mensagem a ser assinada, de forma a reduzir a quantidade de dados a serem cifrados por criptografia assimétrica. O resultado de uma função de resumo criptográfico é uma representação inequívoca[1] da mensagem, e desta forma, ao assinar o resumo, pode-se concluir que as propriedades de autenticidade, não repúdio e integridade são mantidas.

As funções de resumo criptográfico mais utilizadas atualmente são o SHA-1 e os da família SHA-2 (SHA-224, SHA-384, SHA-256 e SHA-512).

2.3.2 O processo de Assinatura Digital

O esquema tradicional de assinatura digital, fazendo uso de criptografia assimétrica e funções de resumo criptográfico, é ilustrado na Figura 2.3 e consiste dos seguintes passos:

1. O Signatário gera um resumo criptográfico da sua mensagem;
2. O Signatário cifra este resumo com sua chave privada;

[1] A questão da colisão de resumos criptográficos é discutida na seção2.3.3

3. O Signatário envia para o Verificador a mensagem e o resumo criptográfico cifrado (assinatura);

4. O Verificador gera, de maneira independente, um novo resumo criptográfico da mensagem recebida do Signatário;

5. O Verificador decifra o resumo criptográfico (assinatura) recebido do Signatário;

6. O Verificador compara os resumos obtidos nos passos 4 e 5;

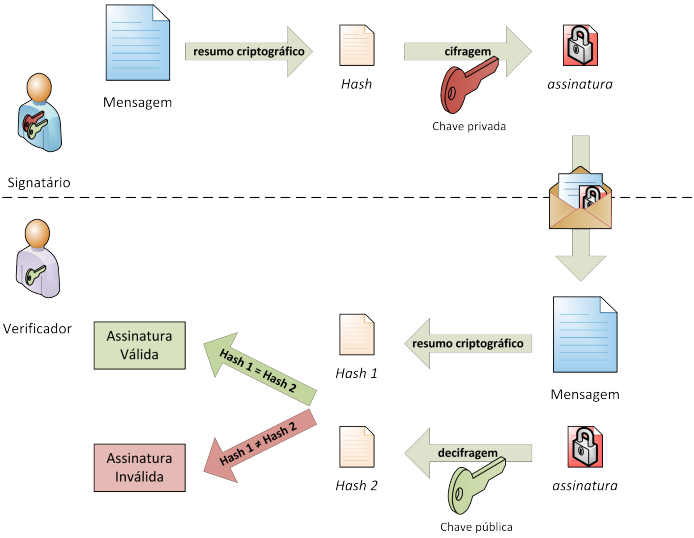

Figura 2.3: Assinatura Digital

Se os resumos criptográficos são idênticos, pode-se afirmar que foi o Signatário quem emitiu a mensagem e este não pode negar a autoria da mensagem. Caso contrário, a mensagem ou o resumo criptográfico foram modificados, não sendo possível, atribuir ao Signatário sua autoria.

2.3.3 Colisão de resumo criptográfico

Uma vez que uma função de resumo criptográfico relaciona qualquer mensagem um valor de tamanho fixo, como por exemplo 160 bits para o SHA-1, existe um número finito de resumos criptográficos que podem ser produzidos por uma determinada função de resumo criptográfico. E uma vez que são infinitas as mensagens possíveis mas finito o número de resumos possíveis, ocorrerá que mais de uma mensagem tem o mesmo resumo. Quando encontramos duas mensagens diferentes com o mesmo resumo criptográfico, dizemos que encontramos uma *colisão*.

A resistência a colisões da função de resumo criptográfico adotada é essencial para a segurança de uma assinatura digital. Se duas mensagens tem o mesmo resumo criptográfico, significa que a assinatura digital de ambas as mensagens será idêntica pois será realizada sobre o mesmo resumo criptográfico. Não será possível identificar qual é a mensagem que realmente foi assinada. A Figura 2.4 ilustra uma situação de ataque explorando uma colisão no algoritmo de resumo criptográfico utilizado na assinatura. Nessa figura, o Signatário assina uma mensagem, que o Interceptador substitui por uma mensagem forjada, que, neste exemplo, possui o mesmo resumo criptográfico da mensagem original. Assim, O Verificador não será capaz de perceber a substituição e portanto aceitará a mensagem como sendo assinada pelo Signatário.

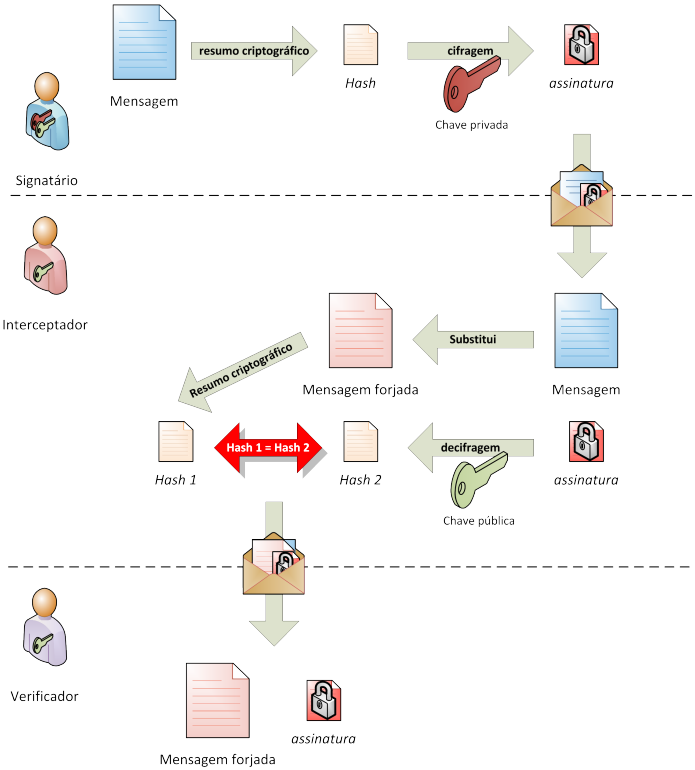

Figura 2.4: Colisão de resumo criptográfico em assinatura digital

Deve-se sempre utilizar algoritmos modernos para uma assinatura digital, para os quais não se conheça ou exista evidência de métodos para encontrar colisões. Por exemplo, até pouco tempo atrás a função de resumo criptográfico mais utilizada era o MD5, que produz resumos de 128 bits. Todavia, já existem ataques de colisão para este algoritmo: Mag-

nus Daum e Stefan Lucks produziram duas mensagens que apresentam o mesmo resumo MD5, sendo a primeira uma carta de recomendação, e a segunda uma carta de autorização de acesso a dados sigilosos (DAUM; LUCKS, 2005).

Uma vez que métodos para encontrar colisões simples sejam encontradas para uma determinada função de resumo criptográfico, é prudente iniciar o abandono desta função nos processos de assinatura digital, substituindo-a por algoritmos mais modernos. O algoritmo mais utilizado no momento é o SHA-1, que já começa a ter sua confiabilidade comprometida (WANG et al., 2005b; WANG et al., 2005a). Existe uma recomendação de que o SHA-1 seja abandonado a partir deste ano (2011) (BURR, 2006), e o substituto imediato são as funções da família SHA-2. Atualmente o NIST já busca uma nova função de resumo criptográfico que será chamado de SHA-3 (NIST, 2007).

É fundamental também que se exista uma preocupação na manutenção das assinaturas digitais já realizadas, para que as propriedades destas sejam mantidas mesmo após o comprometimento dos algoritmos utilizados, através da atualização dos algoritmos.

2.4 INFRAESTRUTURAS DE CHAVES PÚBLICAS

O uso de algoritmo criptográficos de chave pública não garantem por si só a autoria de uma mensagem, pois vinculam apenas a chave a uma mensagem. É necessário ainda associar a chave ao signatário de forma pública e verificável. Uma solução para isto é o uso de *Certificados Digitais*.

2.4.1 Certificado Digital

No mesmo ano que foi proposto o algoritmo RSA (1978), Kohnfelder (KOHNFELDER, 1978) propôs uma abordagem para ligar dados de uma chave a uma entidade, com isso introduzindo termos e conceitos até hoje utilizados, como *Certificado Digital* e *Lista de Certificados Revogados*.

O certificado digital é um conjunto de informações digitais que permitem associar com segurança uma identidade à uma chave. O certificado digital contém, além da chave pública, informações de identificação do titular da chave (como por exemplo, nome e email) e informações que definem os fins para os quais a chave pode ser utilizada (por exemplo: assinatura, cifragem, ou período no tempo em que a chave pode ser utilizada). Esse conjunto de informações é assinado digitalmente, para que exista a garantia de autenticidade e integridade. Esta assinatura pode ser feita pela própria chave, gerando um certificado digital autoassinado, ou por uma terceira parte que atestará a confiança no certificado, como no caso de Infraestruturas de Chaves Públicas (ICPs).

2.4.2 ICP

O certificado digital pode ser assinado por uma Autoridade Certificadora (AC). Em modelos como o x.509 (COOPER et al., 2008) as autoridades certificadoras são entidades, detentoras elas próprias de um par de chaves e um certificado digital, que tem a função de assinar certificados de outras entidades. Uma AC pode ter seu certificado assinado por uma outra AC, formando uma cadeia de certificação. Ou então ter o certificado autoassinado, constituíndo uma AC Raiz.

As ACs Raiz são as âncoras de confiança de uma ICP. Quando se estabelece confiança num certificado autoassinado de uma AC Raiz, é possível verificar os certificados de todas as cadeias de certificados abaixo desta raiz. Esta estrutura que envolve todas estas ACs recebe o nome de Infraestrutura de Chaves Públicas.

2.4.3 ICP-Brasil

A ICP-Brasil é uma Infraestrutura de Chaves Públicas Brasileira, instituída pelo governo, que dá presunção de veracidade jurídica aos documentos assinados digitalmente com certificados emitidos sob sua estrutura.

2.4.3.1 Legislação

A ICP-Brasil foi instituída pela Medida Provisória 2200, de 28 de Junho de 2001 - a última reedição, em vigor no presente momento é a MP 2200-2 de 24 de agosto de 2001 - com o objetivo de "garantir a autenticidade, a integridade, e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônica seguras" (BRASIL, 2001, Art. 1).

Além da medida provisória ainda existe uma série de decretos referentes à ICP-Brasil, bem como resoluções publicadas pelo ITI, que regulamentam o funcionamento de entidades credenciadas à ICP-Brasil.

2.5 CARIMBO DE TEMPO

A validade de uma assinatura digital pode ser limitada por diversos eventos relacionados ao ciclo de vida dos artefatos criptográficos envolvidos na sua realização. Destacam-se:

- Expiração ou revogação do certificado digital do signatário;
- Expiração ou revogação do certificado digital da(s) Autoridade(s) Certificadora(s);
- Comprometimento de algoritmos;

Para que uma assinatura não deixe de ser válida juntamente com os certificados digitais da cadeia de certificação acima dela, é necessário "ancorá-la" de maneira segura e inequivoca a um instante de tempo anterior ao comprometimento. Para isso, podem ser usados os Carimbos de Tempo (em inglês, *timestamps*) (ADAMS et al., 2001). A Figura 2.5 apresenta o processo de criação de um carimbo de tempo, que é bastante similar a uma assinatura digital comum. O carimbo de tempo, além de informações que permitam vinculá-lo inequivocamente a uma determinada informação (que pode ser, por exemplo, uma assinatura digital) acrescenta ainda uma data obtida de uma fonte de relógio confiável. A entidade responsável pela emissão de carimbos de tempo é chamada *Autoridade de Carimbo de Tempo* (ACT, ou TSA - *Time Stamping Authorithy*).

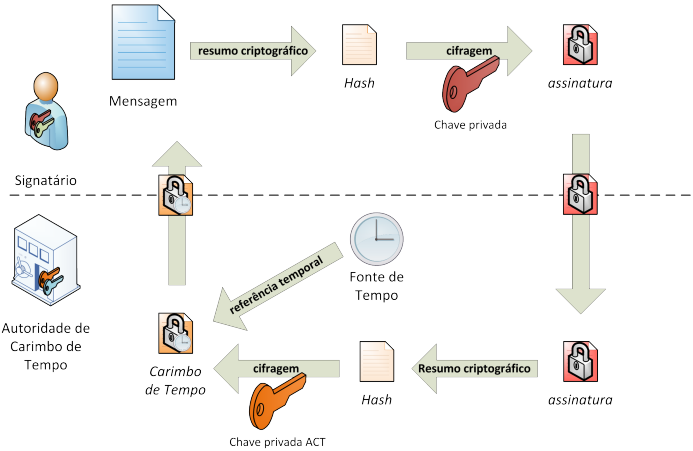

Figura 2.5: Carimbo de Tempo em uma Assinatura Digital

A data fornecida pela ACT é presumida confiável, e portanto a validação da assinatura pode ser realizada com base nesta data. Se os certificados foram revogados ou expiraram apenas após a data do carimbo de tempo, a assinatura ainda pode ser validada com segurança, pois há garantia de que ela existia antes da expiração ou revogação. O carimbo de tempo, entretanto, como qualquer assinatura também tem sua validade limitada e necessita de novos carimbos de tempo para manutenção da sua capacidade de prova.

3 LIMITAÇÕES DA ICP X.509

Neste capítulo serão discutidas as principais limitações e dificuldades enfrentadas na implantação e uso de uma ICP do padrão X.509. Esta visão crítica tem como objetivo fundamentar as tomadas de decisão para a elaboração de uma nova abordagem.

A literatura apresenta alguns trabalhos sobre os problemas e limitações de ICPs. Também existem trabalhos tentando resolver alguns destes problemas, muitas vezes para isso adicionando uma boa dose de complexidade (e redundância) ao processo de implantação e uso de certificação digital. No capítulo 4 analisaremos outros modelos de ICP, e porque estes não resolvem os problemas da ICP X.509. Também naquele capítulo analisaremos adições feitas ao X.509 ao longo do tempo que buscam resolver os problemas aqui apresentados, e quais são as limitações destas soluções.

O foco deste trabalho está principalmente na análise das limitações das ICPs na sua aplicação e uso para a realização de processos como assinaturas digitais. Estes são o produto de interesse de um usuário final em uma Infraestrutura de Chaves Públicas. Uma analogia pode ser feita com outras infraestruturas que usamos diariamente, como a de telefonia: Ao contratarmos um determinado provedor de uma infraestrutura de telefonia, pouco estamos interessados em como funciona a linha telefônica, como são realizadas as ligações, como o meu número está ligado ao meu aparelho de telefone. Usualmente estamos mais interessados em que o produto esperado (possibilidade de realizar ligações telefônicas) possa ser por nós utilizado com a devida qualidade, sem falhas, sem exigir procedimentos complexos e idealmente com o menor custo possível. A complexidade envolvida deve estar ao máximo delegada ao provedor do serviço, e escondida do nosso uso diário.

A mesmo princípio consideramos como direcionador para avaliar as Infraestruturas de Chaves Públicas. Como infraestruturas, estas devem ser transparentes tanto quanto possível para o usuário. Este não deve ser submetido a muitas decisões complexas e ter que processar muitas informações, cujo mal processamento ou avaliação possa levar a não prestação adequada do serviço. No caso de uma assinatura digital, por exemplo, a má prestação poderia ser eventos como uma assinatura válida não ser reconhecida como tal, ou uma assinatura inválida ser aceita como válida. Essa transparência e simplicidade não é alcançada pela ICP X.509, conforme argumentaremos neste capítulo.

Para tal, definiremos como uma ICP típica aquela que dispõe de uma “AC Raiz”, sob as quais estão ACs Intermediárias (também chamadas em alguns contextos como “ACs Normativas”), e por fim abaixo destas as “ACs Finais”. Estas últimas, emitem certificados tanto para Usuários Finais (que realizarão assinaturas digitais) e também para “Au-

toridades de Carimbo do Tempo" (que emitirão carimbos do tempo). A Figura 3.1 apresenta um exemplo desta ICP, onde entidades são representadas por uma bola e certificados por uma seta.

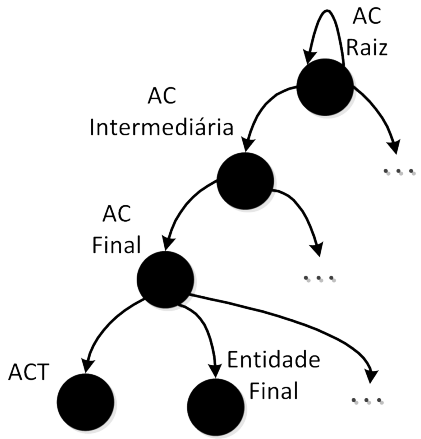

Figura 3.1: Cadeia de Certificação de uma ICP Típica

A verificação de uma assinatura digital gerada por um certificado sob uma ICP típica, que dispõe dos serviços de uma ou mais ACs e uma ou mais ACTs, dá-se conforme os seguintes procedimentos:

- Verificar a assinatura do carimbo do tempo;
- Verificar a validade do certificado da Autoridade de Carimbo do Tempo (ACT) e de sua cadeia de certificação, inclusive informações de revogação, com base no instante presente[1];
- Verificar a validade do certificado do signatário e de todos certificados de sua cadeia de certificação, inclusive informações de revogação, com base na data do carimbo do tempo;
- Verificar a assinatura do documento propriamente dita;

Cada um destes procedimentos tem uma série de desdobramentos e possíveis pontos de falha, que serão expostos e analisados nas seções seguintes, na ordem inversa da que são processadas durante a verificação.

[1] Usualmente a verificação é feita com base na data da verificação, a menos que exista evidência suficiente para considerar-se outra data, como por exemplo um outro carimbo do tempo sobre o carimbo do tempo anterior

3.1 VERIFICAÇÃO DA ASSINATURA DIGITAL

A assinatura digital propriamente dita envolve a operação assimétrica de assinatura digital, conforme visto no Capítulo 2. As propriedades de autenticidade e irretratabilidade estão vinculadas ao fato da chave do signatário ser gerada randômicamente sob condições adequadas, de forma que seja única e de exclusiva posse e controle do signatário. Estão vinculadas ainda a segurança dos algoritmos utilizados, que não podem permitir que uma assinatura seja forjada ou manipulada maliciosamente sem posse da chave privada do usuário.

A data que a assinatura foi realizada é informada pelo signatário. Os formatos de armazenamento e publicação de assinaturas digitais, como CMS (HOUSLEY, 2009), XMLdSIG (EASTLAKE et al., 2002), CAdES (PINKAS et al., 2008; ETSI, 2008) e XAdES (ETSI, 2006b) possuem campos onde esta informação pode ser armazenada. Esta data pode ser livremente escolhida pelo signatário, e a interpretação desta data deve ficar restrita como a data em que o signatário afirma ter efetuado a assinatura.

Um signatário mal intencionado pode gerar uma assinatura com data anterior a que de fato foi realizada, antes mesmo da existência do documento. Ou em caso de comprometimento de chave, o atacante pode gerar documentos com assinaturas cuja data remete a uma data anterior àquela que o comprometimento da chave foi detectado. Portanto, esta data não pode ser usada como referência para validação da assinatura, devendo a confiabilidade da chave ser atestada sempre para o momento da verificação quando não existir uma outra referencia de tempo mais confiável. A Figura 3.2 apresenta a validade de um documento digital assinado em uma ICP X.509.

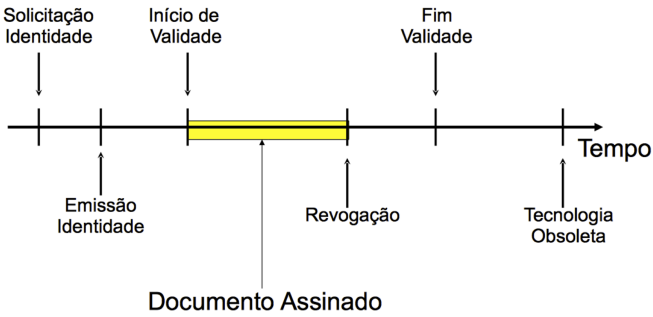

Figura 3.2: Validade de um documento assinado

3.2 VALIDAÇÃO DO CERTIFICADO DO SIGNATÁRIO

Em uma ICP tradicional, uma terceira parte confiável chamada Autoridade Certificadora (AC) emite um certificado digital usando sua chave

privada para assinar o certificado das entidades certificadas. Este certificado serve para vincular informações de identificação da entidade à sua chave pública e, indiretamente, à sua chave privada.

Em diversos ICPs, uma Autoridade Certificadora principal, chamada AC Raiz, delega a Autoridades Certificadoras Intermediárias (ACI), e essas por sua vez à Autoridades Certificadoras Finais (ACF), a função de emitir certificados para usuários finais. Isto é feito para que cada ramo criado por uma nova AC subordinada ou final possa ser dedicada a emitir certificados para um determinado grupo de entidades finais (seja por políticas de uso dos certificados, razões econômicas, distribuição de carga ou outras razões).

A cadeia de certificados formada do certificado da Entidade Final até a Autoridade Certificadora Raiz recebe o nome de cadeia de certificação. A Figura 3.3 representa uma cadeia de certificação com três autoridades certificadoras, onde bolas são entidades e setas certificados emitidos pelas entidades.

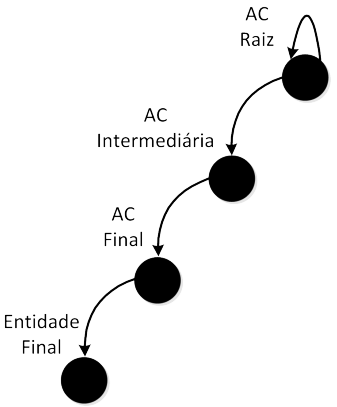

Figura 3.3: Cadeia de Certificação

O certificado será válido, e portanto estará confirmada a confiabilidade no vínculo entre a chave privada e a respectiva entidade, se todo o caminho de certificação acima dele estiver com os certificados dentro do seu período de validade, nenhum dos certificados estiver revogado e a AC Raiz for considerada confiável por parte do verificador. Para isto uma série de procedimentos devem ser realizados, e serão analisados com mais detalhes a seguir.

3.2.1 Âncoras de Confiança

Para verificar a validade do certificado do usuário final, é preciso verificar as assinaturas dos certificados da cadeia formada pelo certificado

alvo até a AC Raiz, isto é, até a âncora de confiança. Esta última tem um certificado autoassinado que precisa ser assumido como confiável pelo verificador. Usualmente os sistemas operacionais, navegadores de internet e outros softwares que fazem uso de ICPs trazem já pré-estabelecidas uma série de âncoras de confiança.

Em diferentes contextos distintas âncoras de confiança são consideradas válidas. Por exemplo, a AC Raiz ICP-Brasil não é aceita por outros países como válida. Para ser aceita, são necessários acordos internacionais, implementados tecnicamente por exemplo através de certificação cruzada entre ICPs, criando o que Gutmann (GUTMANN, 2002) chama de "spaghetti de dúvida", em alusão ao não determinismo da construção do caminho de certificação neste contexto.

Outro problema não adequadamente tratado é o de revogação destas âncoras de confiança. Não há LCR ou solução similar para consulta da situação de uma AC Raiz, por não existir uma entidade que a assine acima da AC Raiz. As Autoridades Certificadoras Raiz precisam ser assumidas como válidas ou inválidas. Caso uma AC Raiz seja comprometida, é necessário removê-la do repositório de âncoras de confiança do software utilizado. Sistemas Operacionais e outros sistemas obtém e atualizam estes repositórios automaticamente para seus usuários. Outras soluções possíveis são a publicação de Listas de Certificados Confiáveis, mas estas precisam ser assinadas também por uma outra entidade, cuja confiabilidade precisa ser assumida como verdadeira.

3.2.2 Obtenção dos Certificados

A determinação e a validação do caminho de confiança, também chamado caminho de certificação ou cadeia de certificação, é a fonte de muitos dos problemas das ICPs X.509. É necessário, antes de mais nada, obter os certificados da cadeia, que muitas vezes não estão publicados de forma padronizada. Uma solução comum, disponibilizada pelos formatos de armazenamento digital como CaDES e XaDES, é anexar os certificados junto à assinatura digital. Entretanto isso acarreta no aumento do tamanho do arquivo final de assinatura digital que nem sempre é aceitável.

Em outras situações, os certificados podem estar dentro de um repositório local de certificados. É preciso neste caso identificar quais pertencem ao caminho de certificação para que a verificação possa ser realizada, o que é uma operação também computacionalmente custosa.

O padrão X.509 prevê o uso da extensão *Authorithy Information Access* (AIA) (COOPER et al., 2008), um campo que pode ser adicionado à certificados e LCRs para indicar onde podem ser obtidos certificados e informações de revogação da cadeia de certificação de um determinado certificado.

3.2.3 Verificação da Expiração e Revogação de Certificados

Estando válidas as assinaturas do caminho de certificação, é preciso também considerar a validade e situação de revogação dos certificados digitais de toda a cadeia de certificação. A assinatura digital precisa ter sido realizada no período em que o certificado era válido e não revogado para que possa ser considerada confiável. Entretanto, na ausência de uma referência temporal segura (como um carimbo do tempo), somente pode-se verificar a assinatura com base na data da verificação, e não na data informada pelo signatário para a realização da assinatura, conforme já argumentado na Seção 3.2.

A Figura 3.4 apresenta a linha de tempo da validade de uma Assinatura Digital realizada sob a ICP típica. Os traços horizontais representam o período de validade no tempo dos certificados e demais artefatos envolvidos. A linha verde apresenta o período de tempo em que a assinatura pode ser verificada e constatada como válida por um verificador. Nota-se que este período vai desde a realização da assinatura até o momento da expiração do certificado do usuário. Um verificador interessado em verificar esta assinatura após este instante, não poderá mais concluir sobre a validade do certificado do signatário. O Certificado que realizava o vínculo entre chave e identidade não possui mais validade, e, mais importante, não existe mais qualquer informação sobre o estado de revogação que possa indicar o comprometimento daquele certificado, uma vez que certificados apenas são incluídos nas LCRs enquanto não-expirados (COOPER et al., 2008).

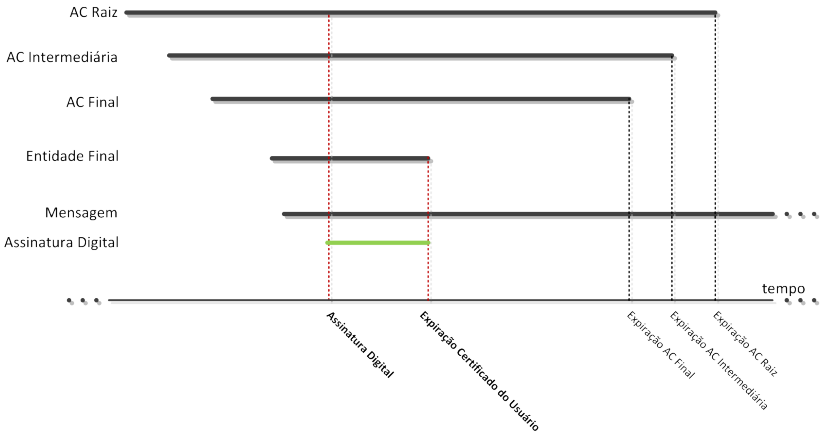

Figura 3.4: Validade de uma Assinatura Digital - Expiração do Certificado do Signatário

Poderia-se pensar, portanto, que uma assinatura digital tem uma data de validade pré-determinada equivalente a validade do certificado

do signatário. Entretanto, se o certificado for revogado antes da sua expiração, a situação é ainda mais problemática. Este é um evento que não tem tempo determinado para ocorrer. A Figura 3.5 ilustra esta situação. Se uma assinatura digital for verificada após a revogação do certificado, não será possível mais concluir sobre a validade da assinatura.

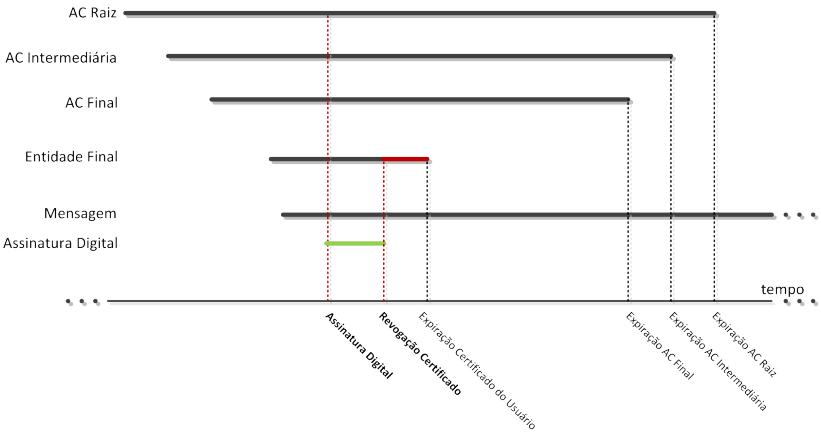

Figura 3.5: Validade de uma Assinatura Digital - Revogação do Certificado do Signatário

Nota-se aí que o certificado de uma ICP X.509, uma vez emitido, é presumido como válido por um determinado período de tempo arbitrado pela Autoridade Certificadora. Isso entretanto não é verdade, já que ele pode ter sido revogado a qualquer momento após a sua emissão. Para declará-lo válido, e consequentemente decidir sobre a validade da assinatura realizada com a chave a ele associada, a parte confiada precisa obter, além do certificado, evidência suficiente para descartar a possibilidade do certificado ter sido revogado. Por exemplo, através da obtenção e interpretação de uma Lista de Certificados Revogados (LCR) ou de uma resposta OCSP. Nenhum certificado ou assinatura pode ser considerada válida em uma ICP X.509 sem a presença e verificação tanto dos certificados da cadeia de certificação, como das informações de revogação de toda a cadeia. São portanto duas verificações paralelas da validade do mesmo certificado.

Nota-se que a LCR é emitida pela AC e pode ser usada para verificar a situação de todos os certificados não expirados emitidos pela mesma. Além disso, a LCR serve como prova de que o certificado permaneceu válido desde o momento que foi emitido até sua inclusão na lista. Essa informação, aparentemente importante, tem pouco efeito sobre a assinatura de documentos eletrônicos, uma vez que é preciso saber unicamente se o certificado era válido quando o documento foi assinado, e não por todo o período de tempo.

3.2.3.1 *Grace-time*

Há na LCR o chamado "*grace-time*". Como, para reduzir custos, uma LCR é emitida em intervalos de tempo relativamente grandes, existe uma janela de tempo em que um certificado comprometido continua válido. Por exemplo, se um titular de certificado solicita a revogação logo após a emissão de uma LCR, seu certificado continuará sendo válido até que a próxima LCR seja emitida. Isto é um problema especialmente em casos de revogação por comprometimento da chave privada. Assim, um verificador atencioso, consideraria somente válido o certificado após passado o período de "*grace-time*" do instante onde inicia a verificação, tendo a certeza de ter havido tempo hábil para que uma vez solicitada a revogação de um certificado, tenha sido publicada uma nova LCR onde constará este certificado.

Entretanto, este inteervalo de tempo não é aceitável para muitas aplicações, que precisam processar e validar o certificado de maneira imediata.

3.2.3.2 O problema da abordagem "lista negra"

Gutmann (GUTMANN, 2002) afirma que o problema fundamental da abordagem de LCRs e abordagens baseadas em LCR, é que ela responde a pergunta errada. Ao invés de responder a pergunta "Este certificado é válido?", abordagens baseadas em "listas negras" só podem responder a pergunta "Este certificado foi revogado?". Não é esta a pergunta que realmente interessa a um verificador de certificado, uma vez que o certificado não ter sido revogado não diz nada sobre ele ter sido sequer emitido, ou estar expirado, por exemplo.

Na verdade, existem duas "perguntas", opostas mas redundantes, que são realizadas no modelo X.509: primeiro se responde a pergunta "Esse certificado é válido?" e busca-se a resposta avaliando o certificado assinado pela AC. No entanto, a resposta que o certificado fornece é "Este certificado deveria ser válido, mas verifique uma LCR para confirmar" (caso esteja dentro do período de validade do certificado e a assinatura seja correta) ou "Este certificado não é válido" (caso a assinatura seja inválida ou o certificado já esteja expirado). Efetivamente o certificado sozinho apenas pode dar uma resposta negativa conclusiva, que é a resposta "Este certificado não é válido". Para obter uma resposta positiva conclusiva, é necessária a combinação da resposta da validação do certificado com a resposta da validação através da LCR.

3.3 VALIDAÇÃO COM CARIMBO DO TEMPO

O carimbo do tempo, conforme visto no Capítulo 2, é um artefato que tem como objetivo atestar, por parte de uma entidade confiável chamada Autoridade de carimbo do tempo, a existência de uma determinada

informação em uma determinada data. Pode-se portanto obter através dele uma referência temporal segura da existência de uma assinatura. Uma vez existindo esta referência segura de data, não é mais necessário avaliar a assinatura com base na data de verificação, e pode-se fazer esta avaliação com base na data do carimbo do tempo.

Isto traz uma série de vantagens. Seja considerando uma possível expiração ou revogação do certificado, desde que exista uma referencia temporal segura anterior, pode-se afirmar que a assinatura foi realizada enquanto o certificado do signatário ainda era válido, e portanto quando a chave privada estava sob seu exclusivo controle. Note-se que o carimbo do tempo não atesta a data em que a assinatura foi realizada, mas sim uma data em que a assinatura já existia. Estas podem ser similares, caso o carimbo do tempo seja obtido após a realização de assinatura, mas também podem estar muito distanciadas, por exemplo em um caso que o carimbo do tempo seja aposto apenas numa protocolação do documento. O verificador, entretanto, para efeito de verificação, deve confiar na data forneceida pela Autoridade de Carimbo do Tempo, e não na data informada pelo signatário. A Figura 3.6 apresenta o período em que uma assinatura pode ser validada quando é aplicada sobre esta assinatura um carimbo do tempo.

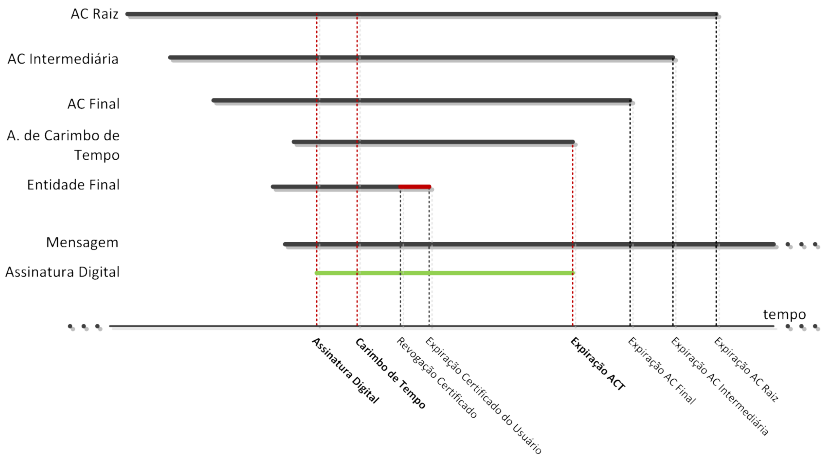

Figura 3.6: Validade de uma Assinatura Digital com carimbo do tempo - Revogação do Certificado do Signatário

Entretanto, deve-se notar que o carimbo do tempo é essencialmente uma assinatura da ACT sobre a assinatura digital realizada pela entidade final. E portanto, está sujeita a muitas das limitações da primeira assinatura, mas dessa vez associada a validade do certificado e cadeia de certificação da ACT. Na ausência de uma outra referência temporal confiável, o carimbo do tempo e a cadeia de certificação acima dele

precisam ser avaliados quanto a sua expiração e revogação com base no instante da verificação. Espera-se portanto que esta tenha um período de validade superior ao das entidades finais, e também que tenha uma possibilidade inferior, idealmente nula, de ser revogada ou ter sua chave comprometida.

Para extender a validade desta assinatura além do período de validade do certificado da ACT, é necessário aplicar novos carimbos do tempo sobre o carimbo do tempo anterior. Desta forma, o carimbo "mais externo" é avaliado na data da verificação, e os carimbos são sequencialmente validados com base na data atestada pelo anterior, até chegar-se a uma data onde pode ser validada a assinatura digital propriamente dita. Isto naturalmente implica em uma série de verificações de certificado e suas situações de revogação, e um aumento substancial no tamanho do arquivo de assinatura a medida que essas informações são anexadas.

3.3.1 Obtenção de Informações de Revogação do Passado

Um aspecto importante a ser considerado é que, como na presença de um carimbo do tempo a verificação da cadeia de certificação do signatário é realizada no passado, é fundamental que se tenha acesso as informações sobre situação de revogação daquela data, em especial quando a verificação é feita após a expiração do certificado. Este é um problema relevante a ser considerado, pois caso estas informações não estejam anexas ao documento, normalmente não há uma forma padronizada de consultar LCRs antigas. Como as informações sobre revogação do certificado serão removidas da LCR após sua expiração, as LCRs atuais publicadas nos repositórios não conterão nenhuma informação sobre se o certificado era ou não revogado antes de expirar.

3.3.2 Comprometimento de ACT

Para alguns autores, uma ACT pode ter seus carimbos do tempo aceitos como válidos mesmo após a expiração do certificado da ACT, desde que se possa afirmar no momento da verificação que a chave privada e os algoritmos envolvidos continuam seguros. Desta forma, é preciso assumir que a chave é considerada segura enquanto a ACT opera, e destruída de forma segura após esta operação, e não há possibilidade de comprometimento do certificado da ACT pois isso não seria algo detectável após a sua expiração (PINKAS et al., 2003). Atendidos estes requisitos, os carimbos do tempo podem ser avaliados como seguros mesmo após a expiração da ACT que os emitiu. A Figura 3.7 representa o período que uma assinatura poderia ser avaliada com segurança adotando esta interpretação.

Entretando normas internacionais, como por exemplo as Européias da ETSI (ESI, 2008a; ESI, 2008b), discordam desta interpretação e uso, exigindo a aplicação de novos carimbos do tempo antes da expiração ou

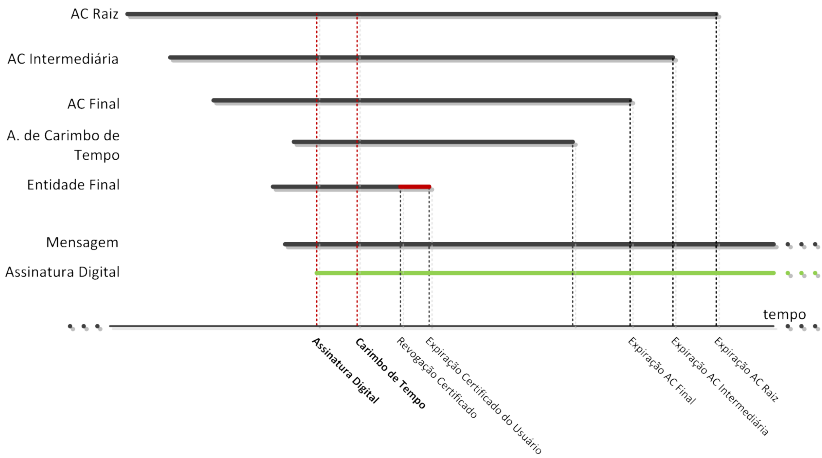

Figura 3.7: Validade de uma Assinatura Digital com carimbo do tempo não revogável - Revogação do Certificado do Signatário

revogação dos anteriores. A revogação em especial é uma situação problemática neste contexto. Assim como no caso da assinatura digital, é um evento imprevisível. Caso seja comprometida a Autoridade de Carimbo do Tempo, todos os carimbos por ela já emitidos tornam-se inválidos, caso não exista um segundo carimbo de outra ACT contraposto ao anterior. A Figura 3.8 apresenta o período em que uma assinatura pode ser validada quando é revogado o certificado da ACT geradora do carimbo do tempo.

Na ausência de evidência temporal que permita avaliar os carimbos do tempo emitidos antes de uma revogação, estes somente podem ser considerados válidos após a revogação da ACT se estiver registrado um motivo de revogação que não seja comprometimento das chaves na LCR mais atual. Caso o motivo de revogação seja *unspecified*, *affiliationChanged*, *superseded* ou *cessationOfOperation*, é possível considerar os certificados emitidos anteriormente à revogação como válidos, pois a chave não deve ser considerada como violada nesses casos. Caso o motivo de revogação seja *keyCompromise* ou não seja especificado, não se deve considerar os carimbos emitidos como válidos, sejam eles emitidos antes ou depois da revogação (ADAMS et al., 2001). Após a expiração, no entanto, não é mais possível verificar qual é a situação da chave privada da ACT, uma vez que o motivo de revogação não estará mais disponível na LCR.

Além de causar o crescimento contínuo do arquivo de assinatura, só faz sentido a aplicação de novos carimbos do tempo se o novo carimbo for de uma outra ACT, com maior prazo de validade. Para evitar o risco do comprometimento de uma ACT antes de uma recarimbagem, é recomendável que sejam apostos dois carimbos do tempo de ACTs dife-

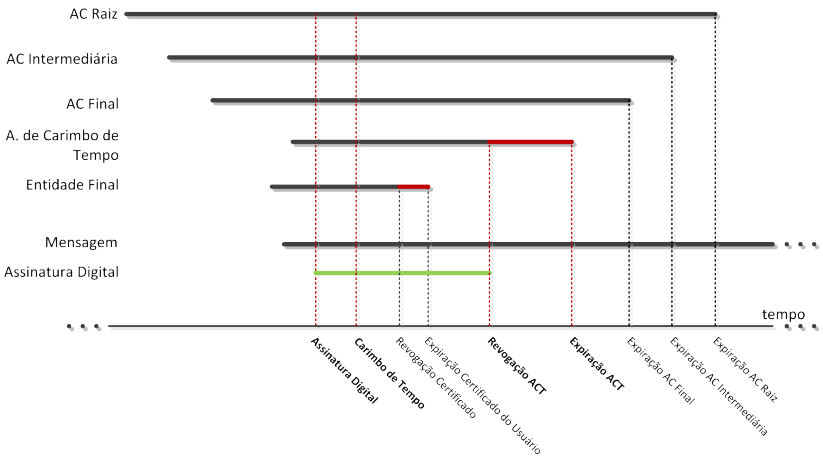

Figura 3.8: Validade de uma Assinatura Digital com carimbo do tempo - Revogação do Certificado da ACT

rentes em um documento (ADAMS et al., 2001). Isso reduz significativamente o risco, necessitando que duas ACTs tenham suas chaves violadas para que se perca a referência temporal segura sobre o documento. Naturalmente isso implica na necessidade de obtenção e armazenamento das informações sobre caminho de certificação e revogação de tantas ACTs quantos forem os carimbos do tempo apostos.

3.4 MODELO DE NEGÓCIO

O modelo de negócios das ICPs X.509 é voltado para entregar como produto um certificado digital, e não os serviços de certificação digital. O usuário solicita e paga por um certificado digital que tem uma determinada validade, e nesse preço (muitas vezes altíssimo) está embutido todo o alto custo de implantação de uma ICP, como ambientes seguros ("salas-cofre"), instalações de AR, equipes técnicas, equipamentos, entre outros. Não há diferenciação no preço de um certificado se ele será usado uma vez, ou a todo tempo. Se terá uma assinatura digital associada a ele ou milhões de assinaturas. Isso engessa o modelo de negócio aplicado pela AC para fornecer certificados com preços baseados apenas na sua valiade e tipo de uso.

O modelo de negócio também traz implicações para a operação das Autoridades Certificadoras, como argumenta Gutmann (GUTMANN, 2002): Estas não podem cobrar por operações custosas computacionalmente, como as consultas a LCRs. As LCRs são disponibilizadas gratuitamente e esta é a expectativa geral dos usuários de uma ICP. Mas mesmo que se desejasse cobrar, não há mecanismos adequados para fazer essa

cobrança. Não se sabe quantas vezes a LCR será consultada para validar um determinado certificado, nem quem executará essa consulta, se é o signatário ou o verificador. Mas ela precisa ser emitida sempre, e em intervalos de tempo relativamente curtos para mitigar problemas como o do *grace-time*. E o preço por essa operação, que exige uma série de operações criptográficas para geração das LCRs e também de banda e servidores para a publicação das mesmas, acaba tendo que ser adicionado de alguma forma ao custo do certificado digital, na ausência de outra forma de cobrar por isso. Isso serve de desincentivo para as Autoridades Certificadoras de prestar este serviço com a qualidade necessária.

De maneira geral, as ICPs X.509 não permitem o estabelecimento de um modelo de negócios justo, onde os serviços possam ser oferecidos a diversos tipos de consumidores conforme a necessidade de uso de cada um. Isso inibe a popularização do uso de ICPs X.509 em diversos contextos.

3.4.1 O papel da Autoridade de Registro

Como a operação de uma AC é altamente custosa, especialmente pela necessidade de garantir a segurança de todo o ciclo de vida de sua chave privada, utilizam-se as Autoridades de Registro (AR), que assumem a função de validação dos dados do titular do certificado digital. Um usuário que deseja obter seu certificado digital deve ir pessoalmente a uma instalação técnica da AR, onde uma pessoas chamada de Agente de Registro (AGR) confere os dados do titular e, principalmente, verifica a a posse da chave privada.

O peso da confiança sobre a identidade do detentor do certificado, portanto, recai sobre estas ARs. Entretanto na prática o que ocorre é que a AC é o foco da confiança das ICPs X.509 e que publica as relações entre entidades e suas chaves, enquanto a AR não recebe a devida atenção, sendo normalmente uma prestadora de serviços das ACs.

4 ANÁLISE CRÍTICA DE TRABALHOS RELACIONADOS

Entre as possíveis soluções que existem na literatura para os problemas citados no capítulo 3 estão novos modelos de ICP bem como adições ao modelo X.509. Os modelos de certificação mais conhecidos e usados são: PGP, SPKI/SDSI, IBC além do X.509. Alguns novos modelos tem sido propostos, como CLC (*Certificateless cryptography*) e CBC (*Certificate Based Cryptography*). Já entre as adições ao X.509, citamos CRT, NPKI, OC, SCVP, OCSP, entre outros.

Neste capítulo analisaremos estas abordagens, realizando uma análise crítica das suas vantagens e limitações.

4.1 MODELOS DE ICP

4.1.1 PGP

O PGP (ZIMMERMANN, 1995) apresenta uma arquitetura de ICP onde também são utilizados certificados digitais autoassinados, assim como a proposta defendida neste trabalho. A confiança nestes certificados é estabelecida através das "redes de confiança", ou seja, os usuários do PGP assinam os certificados em quem confiam, e publicam os certificados e estas assinaturas em repositórios públicos. Desta forma, consultando estes repositórios pode-se obter cadeias de confiança entre os certificados que o destinatário confia até o certificado do signatário, por exemplo. Ao optar por confiar em determinados certificados, passa-se a confiar nos certificados assinados por estes, e assim por diante.

Para determinados contextos a abordagem é útil, mas sua principal limitação é o fato de não ser escalável, pois torna-se muito fácil qualquer nodo mal intencionado da rede de confiança comprometer a confiabilidade da infraestrutura. Se um dos usuários de uma rede de confiança PGP for convencido a assinar um certificado forjado, toda a rede passa a estar comprometida, uma vez que este certificado poderá assinar quaisquer outros certfificados também forjados. Desta forma, o uso de PGP é mais comum dentro de pequenos grupos de interesse, que possam ter suas chaves verificadas de maneira mais eficiente e onde qualquer tentativa de engenharia social seja mais facilmente detectada.

Outro uso comum de chaves PGP é para assinatura de pacotes de distribuição de software, especialmente no contexto de software livre. Comumente a chave é publicada no site do desenvolvedor ou incluída em uma lista de chaves confiáveis do sistema operacional (abordagem utilizada em algumas distribuições Linux, por exemplo). O usuário normalmente não faz uso da cadeia de confiança para estabelecer confiança no certificado, antes estabelece confiança no próprio certificado autoassinado inserindo-o em uma lista de certificados confiáveis no seu sis-

tema. Nesta situação, a infraestrutura PGP e a rede de confiança não é de fato utilizada na verificação do certificado, apesar de ser possível a um verificador interessado buscar assinaturas da chave de assinatura de código que estejam relacionados, por exemplo, a chaves conhecidas dos desenvolvedores envolvidos no projeto, como forma de aumentar a sua confiança de que o software realmente foi publicado pelos seus desenvolvedores.

O uso seguro do PGP portanto depende muitas vezes de entender a implicação de que nodos não confiáveis podem causar na confiabilidade da rede de confiança, e tomar decisões baseadas neste entendimento. Essa é uma decisão complexa demais para um usuário comum e complexa de ser automatizada, o que limita muito a aplicação do PGP em diversos contextos.

4.1.2 SPKI/SDSI

O SPKI (ELLISON et al., 1999) propõe uma arquitetura simplificada de ICP, mais voltada a autorização do que a autenticação (ELLISON et al., 1999). Um certificado de SPKI (*Simple Public Key Infrastructure*) objetivam relacionar uma chave e que autorização essa chave tem dentro de um determinado sistema, do que no estabelecimento de uma relação entre uma chave e uma entidade (apesar de prover suporte a isso). Na mesma linha está o SDSI (*Simple Distributed Security Infrastructure*) (RIVEST; LAMPSON, 1996), outra abordagem simplificada de ICP onde o foco está na definição de grupos de acesso e emissão de certificados para estes grupos. Em ambas abordagens as entidades ou grupos tem determinadas autorizações, e estas autorizações podem ser delegadas através de uma cadeia de relacionamentos entre entidades ou grupos. No modelo SPKI os certificados não necessitam de revogação, pois são sempre de curto prazo.

Uma das críticas dos proponentes do SPKI/SDSI ao modelo X.509 está na questão de o modelo X.509 pressupõe a existência de identificadores únicos para distringuir as entidades da ICP, seja um nome ou número de identidade (ELLISON et al., 1999). Enquanto isso realmente não é verdade em um contexto global, devido a inexistência de identificadores únicos padronizados para distinguir entidades em todo o mundo, é sim aplicável em contextos de ICPs dentro de domínios restritos e até mesmo dentro de ICPs não tão restritas como as ICPs nacionais, onde cada entidade que poderá receber um certificado pode ser diferenciada por um identificador único, como por exemplo documentos nacionais de identidade como o CPF/CNPJ.

Uma vez que o foco em autorização não é o principal interesse em diversas ICPs, a limitação do modelo SPKI/SDSI está no próprio objetivo com que foi desenvolvido: embora mais simples para aplicações que envolvam autorização, é uma abordagem não tão adequada para uso em autenticação, e em especial para assinatura digital de documentos. O

foco desta abordagem não está em garantir uma identidade, mas sim uma autorização.

4.1.3 IBC

A IBC (*Identity Based Criptography*) (BOYEN; MARTIN, 2007) é uma abordagem proposta por Shamir em 1984 (SHAMIR, 1984), onde as chaves não são geradas randômicamente, mas sim calculadas. A chave pública é calculada a partir de uma identidade e a interação com um gerador de chaves (KGC - *Key Generating Center*), e a chave privada é gerada a partir da chave pública e a interação com este mesmo Gerador de Chaves. A chave pública, desta forma, não precisa ser randômica, mas sim é gerada com base uma identidade. Isso minimiza os problemas de distribuição das chaves, já que uma terceira parte interessada em enviar uma informação cifrada para um determinada entidade pode obter a chave pública diretamente com base na informação de identidade desta pessoa.

Nota-se que existe uma forte dependência de confiança com o Gerador de Chaves, que conhece a chave privada da entidade e pode assumir a identidade de qualquer entidade. É necessário também um modo autenticado e seguro de comunicação entre as entidades e o KGC para obtenção a chaves privadas, o que tem suas próprias implicações de segurança.

4.1.4 CLC

O conceito de CLC (*Certificateless Cryptography*) (AL-RIYAMI; PATERSON, 2003) busca um esquema de distribuição de chaves públicas sem o uso de certificados. Para isso cada entidade detem dois segredos: um valor secreto e uma chave privada parcial. O primeiro valor secreto é gerado pela própria entidade, e o segundo por uma terceira parte geradora de chaves (KGC) a partir da identidade da entidade solicitante. A chave privada da entidade é obtida por uma função cujos parâmetros são o valor secreto conhecido pela entidade e o valor obtido de KGC, desta forma eliminando o problema inerente do IBC de conhecimento da chave por parte do KGC.

A entidade pode então gerar uma chave pública a partir da chave privada, e não a partir da identidade (como no esquema IBC). Entretanto, o esquema não dá suporte a qualquer garantia de autenticidade da chave, sendo vulnerável a ataques de substituição de chave (WU et al., 2009). Desta forma, é adequado apenas para esquemas de cifragem e decifragem, e não para assinatura digital.

4.1.5 CBC

A CBC (*Certificate Based Cryptography*) foi proposta por Gentry (GENTRY, 2003), buscando integrar as vantagens de IBC com as vantagens do uso de Certificados Digitais. No CBC cada entidade gera sua própria chave privada e também solicita um certificado para uma

Autoridade Certificadora. Entretanto esse certificado não é apenas uma vinculação da chave com a identidade do usuário, mas também é utilizado como chave de decifragem de um esquema IBC ou CLC (ou seja, através da interação com o KGC). Para um esquema de cifragem e decifragem, a abordagem dispensa a distribuição de informações de revogação. Para cifrar, um remetente precisa apenas da chave pública do destinatário e os parâmetros da AC. Para decifrar, o destinatário precisa obter um certificado atualizado interagindo com a AC. Entretanto, assim como no IBC e CLC, não há uma garantia para o remetente de que ele está com a chave pública certa.

O CBC foi extendido para suportar assinaturas por Kang et. all. (KANG; PARK, 2004), levando para a assinatura digital a não necessidade de obtenção de informações de revogação, uma vez que é necessária uma interação válida com o KGC para gerar uma assinatura válida, e se a entidade estiver com seu certificado revogado não será possível gerar uma assinatura válida. Há, assim como nos esquemas IBC e CLC, uma forte dependência com o gerador de chaves, com o qual é necessário realizar uma transação segura para obter uma informação atualizada que é parte da chave a ser usada em decifragem ou assinatura.

4.2 ADIÇÕES AO X.509

O X.509 foi proposto como certificado digital em diretórios X.500. Esse modelo de certificação consiste em uma ou mais árvores de certificados, cada uma com sua raiz, e autoridades certificadoras finais que emitem certificados para os usuários.

A maior parte das dificuldades estão relacionadas a validação do certificado do usuário, tanto para determinação e validação do seu caminho de certificação quanto da gestão de revogação dos certificados. Os seguintes trabalhos e métodos permitem resolver partes destes problemas.

4.2.1 *Certificate Revocation Tree*

O maior problema quanto a revogação está na busca constante de LCRs atualizadas e o tamanho destas listas. Para contornar estes problemas, Kocher propôs a Árvore de Revogação de Certificados (*Certificate Revocation Tree – CRT*) (KOCHER, 1998), que provê respostas de tamanho levemente menor a consultas sobre revogação de certificados. O problema é minimizado, mas não eliminado.

Outra alternativa é a validação de Certificados em Árvore-Lista (*Tree-List Certificate Validation – TLCV*) (LIM et al., 2008) que usa uma estrutura do tipo árvore-lista para promover um ganho de performance sobre a proposta de Kocher.

A abordagem é uma maneira mais eficiente computacionalmente que as LCRs, mas mantém, de maneira geral, os demais problemas apontados no Capítulo 3 relacionados a LCRs.

4.2.2 Certificados Aninhados

Quanto a complexidade da construção da cadeia de certificação Levi propôs o uso de certificados aninhados (*Nested-certificate-based PKI – NPKI*) (LEVI et al., 2004). Tais certificados criam uma infraestrutura especial ligando o ponto de confiança ao certificado do usuário através de uma lista de hashes. A idéia é substituir operações criptográficas complexas de criptografia assimétrica por operações de resumo criptográfico, simplificando o processo de validação de uma cadeia de certificação.

Trata-se de uma adição bem vinda para a diminuição da complexidade computacional do processo especifico de construção de cadeia de certificação, mas não resolve os problemas relacionados a revogação de certificados da cadeia e da conservação a longo prazo de assinaturas digitais.

4.2.3 Certificados Otimizados

Uma outra proposta para resolver esta mesma questão é a apresentada por Custódio (CUSTóDIO et al., 2008), que propõe que o problema da validação de assinaturas digitais pode ser resolvido usando um tipo especial de certificado, chamado Certificado Otimizado (*Optimized Certificates – OC*). Esta proposta minimiza o número de operações aritméticas na validação de um certificado. Além disso outro problema, também tratado por Custódio, está na conservação a longo prazo de documentos eletrônicos, que consiste na emissão periódica de carimbo de tempo que leva ao aumento do tamanho do arquivo de assinatura digital.

A proposta no entanto busca manter a compatibilidade com as ICPs X.509, apenas adicionando este novo certificado para que em determinados domínios e contextos a validação seja simplificada. Não é uma mudança na estrutura de uma ICP como um todo.

4.2.4 Validação Online - SCVP e OCSP

Outra dificuldade desses modelos tradicionais de certificação é a necessidade de muitos recursos e poder de processamento para validação do caminho de certificação. Vários dispositivos atuais, tais como celulares e PDAs não dispõem de recursos e/ou informações suficientes para efetuar esta operação. Para contornar essa dificuldade são usados serviços especializados tal como o SCVP (FREEMAN et al., 2007).

O SCVP é uma serviço (terceira parte) que pode ser invocado para construção e/ou validação de cadeias de certificação em uma ICP usual. Contudo este esquema adiciona mais uma parte confiável no sistema, sujeito a alta demanda de carga, e não elimina os problemas existentes na ICP tradicional, pois apenas delega a outra entidade a resolução do desafio.

O OCSP igualmente é um serviço (terceira parte) que oferece respostas específicas do estado de um determinado certificado. O servi-

dor OCSP, para isso, consulta as LCRs fornecidas pela AC. Entre as limitações, destaca-se o fato de que, por basear suas respostas nas LCRs que apenas podem responder a pergunta sobre o estado de revogação de maneira negativa ("não é válido"), o servidor OCSP também apenas pode fornecer a informação de que "o certificado foi revogado" ou "não tem informações sobre o certificado ter sido revogado". Esta última resposta, no entanto, não serve de evidência de que o certificado sequer tenha sido emitido ou continue válido, apenas informa que ele não consta como revogado na LCR fornecida pela AC. Como interpretar esta informação varia entre os implementadores existentes (GUTMANN, 2002).

Gutmann (GUTMANN, 2002) compara as LCRs às "listas negras de cartão de crédito" dos anos 70. Ambas são soluções inerentemente *offline* para um mundo cada vez mais *online*. Nos anos 80 os fornecedores de cartão de crédito perceberam isso e passaram a fazer uso de solução de consulta de situação online, que retorna uma resposta booleana de "verdadeiro" ou "falso" para a validade de um cartão. Para certificados, estas respostas equivaleriam a "O certificado é válido agora" ou "O certificado não é válido agora", respostas que o OCSP e outras abordagens baseadas em LCRs não podem responder.

4.2.5 *Fast Digital Certificate Revocation*

A proposta de *Fast Digital Certificate Revocation* (GOYAL, 2004) propõe que certificados digitais X.509 possuam uma extensão não assinada onde é inserida uma informação, atualizável, sobre a situação de revogação do próprio certificado. O processo de obtenção dessa prova é chamado de "renovação de certificado".

Essa informação é assinada pela Autoridade Certificadora, e é formada essencialmente pelo serial do certificado e uma data confiável. Se o crtificado é válido, a prova conterá a data do pedido de verificação. Se o certificado estiver revogado, é utilizada uma data anterior a de criação do certificado, servindo como evidência de revogação. Desta forma, o verificador decide se a data em que existe a prova é suficientemente próxima a atual para seu modelo de negócio. Desta forma, elimina-se a necessidade de consultas à LCRs, mas torna-se necessário obter sempre renovações do certificado para o instante da verificação.

4.2.6 Método de Revogação de Novomodo

Uma vantagem do método de revogação por LCRs citada pela própria RFC5280 (COOPER et al., 2008) é o fato de que estas podem ser distribuídas da mesma forma que os certificados, ou seja, por métodos não confiáveis. A LCR, sendo assinada, pode ser replicada e disponibilizada em qualquer servidor, sem necessidade de confiar-se neste servidor.

Existe um outro método, que será usado neste trabalho, que também não depende de confiança no local onde está publicada a ori-

gem da informação. Trata-se do método de Novomodo, proposto por Micali (MICALI, 2002).

Neste método a AC, ao emitir um certificado, seleciona dois valores secretos e randômicos para o certificado, X_0 e Y_0. A AC ainda define um valor para o intervalo de tempo (i) entre as publicações de situação do certificado. Este valor é análogo ao período de tempo que seria definido entre publicações de uma LCR. A AC gera então n valores que serão publicados a cada intervalo de tempo caso o certificado continue válido, utilizando uma função de resumo criptográfico H sobre o valor de X_0. Desta forma, para cara intervalo de tempo i, será obtido um novo $X_i = H^i(X_0)$, conforme demonstra a Figura 4.1.

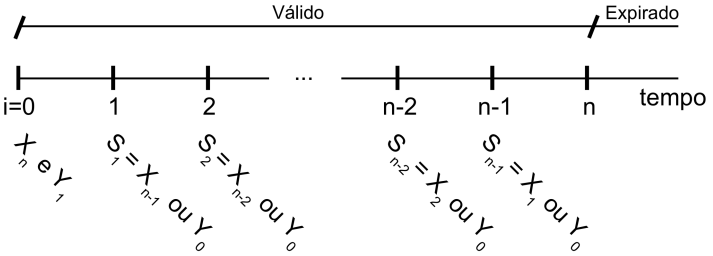

Figura 4.1: Provas de Validade de Novomodo

No certificado são incluídos os valores de $X_n = H^n(X_0)$ e de $Y_1 = H(Y_0)$. Durante o período de validade do certificado, a AC publica a cada intervalo de tempo i um valor de situação do certificado S_i, com valor X_i ou o valor Y_0. Se for publicado $S_i = X_i$, o verificador pode confirmar a validade do certificado fazendo i operações de resumo criptográfico sobre o valor X_i, e deverá chegar ao valor de X_n incluído no certificado. Caso tenha sido publicado $S_i = Y_0$, o verificador, com uma operação de resumo criptográfico sobre este valor chegará ao valor de revogação Y_1 publicado no certificado, confirmando que ele não é mais válido. A Figura 4.2 ilustra um certificado revogado no tempo r, e o Algoritmo 4.1 descreve o processo de verificação de um certificado através das informações publicadas por uma AC.

4.2.7 Outros trabalhos

Outras pesquisas tem proposto diferentes abordagens (LAIH; YEN, 1995; SATIZáBAL et al., 2007; RIVEST, 1998; COOPER, 1999; HUNTER, 2002). Todas tentam melhorar o tempo de resposta das consultas a informações de revogação, criar mecanismos mais eficientes de validação, ou até mesmo eliminar a necessidade de revogação de certificados. Entretanto nenhuma das propostas tenta mudar os fundamentos da validação de certificados. Este trabalho seguirá uma abordagem diferente,

Entrada: S_i, X_n, Y_1, H
Saída: Situação do Certificado

início
  se $H^i(S_i) = X_n$ **então**
    "O Certificado continua Válido"
  senão
    se $H(S_i) = Y_1$ **então**
      "O Certificado foi Revogado"
    senão
      "Não é possível concluir sobre Situação do Certificado"
    fim
  fim
fim

Algoritmo 4.1: Verificação da validade de certificado pelo método de Novomodo

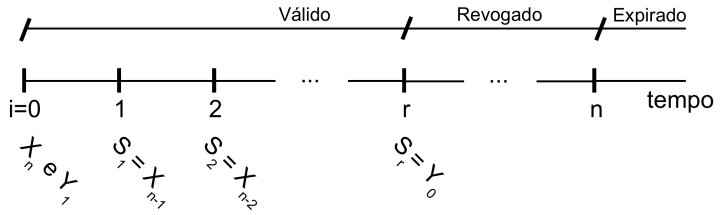

Figura 4.2: Revogação de um Certificado pelo método de Novomodo

propondo uma nova modelagem de ICP, adequada para assinatura digital de documentos, sem perder a aplicabilidade para autenticação e demais usos de uma ICP tradicional.

5 NBPKI - UMA ICP BASEADA EM AUTORIDADES NOTARIAIS

Diante das limitações da ICP usualmente utilizada (X.509) e das suas principais alternativas, e também da complexidade das soluções existentes para solução desses problemas, propõe-se neste capítulo uma nova abordagem de ICP, que através de sua simplicidade torne-se adequada em especial para o contexto de assinatura digital de documentos eletrônicos, mas sem perder a generalidade esperada de uma ICP.

De maneira geral, deseja-se que esta ICP:

- Tenha uma complexidade baixa de processamento exigido para validação de uma assinatura digital, em especial para o signatário e verificador;
- Exija uma quantidade mínima de informações para ser validada com segurança;
- Assinaturas digitais sejam de simples manutenção e conservação a longo prazo;
- Mantenha-se a generalidade de uso de uma ICP;
- Possua mecanismos de segurança adequados para a comprovação legal da autenticidade de assinaturas digitais;

A abordagem que será apresentada neste capítulo recebeu o nome NBPKI, sigla em inglês para "Infraestrutura de Chaves Públicas Baseada em Notários" (*Notary Based Public Key Infrastructure*), em referência ao papel que a Autoridade Notarial desempenha no modelo proposto.

Esta abordagem não propõe novos algoritmos criptográficos como as propostas de IBC, CLC e CBC. Também não propõe adições ao padrão X.509. Antes, propõe uma nova estrutura e organização de ICP, baseada nos mesmos algoritmos criptográficos já amplamente difundidos, testados e utilizados em ICPs X.509 e suas variantes.

5.1 FUNDAMENTOS DA ABORDAGEM

Nesta seção são apresentadas e justificadas as principais idéias sobre as quais é fundamentada a proposta da NBPKI, e porque estes fundamentos fazem com que a NBPKI não apresente os mesmos problemas das ICPs tradicionais, em especial as ICPs X.509.

5.1.1 Abordagem baseada em certificados autoassinados

No esquema tradicional de certificação digital, quando um certificado é emitido, ele é assumido como válido por um determinado tempo,

definido pela validade do certificado (campos *notAfter* e *notBefore*). Entretanto, como visto no Capítulo 3, certificados digitais podem ser revogados a qualquer momento. Portanto, efetivamente, o certificado não é válido até o momento que seja obtida uma prova fornecida por uma terceira parte confiável de que ele continua válido. Usualmente usam-se LCRs como esta prova, ou alternativas como a consulta online a um servidor OCSP. Nos Capítulos 3 e 4 foram expostos os problemas relacionados a estas abordagens e suas alternativas.

Considerando o fato de que é necessária uma prova de validade do certificado na data da verificação, não é necessário pressupor que o certificado seja válido quando emitido. O certificado pode ser emitido sem ser considerado válido e somente quando for necessário busca-se a prova que o torna válido.

Assim, propomos que o certificado do usuário só seja considerado válido quando houver uma prova de que ele é válido. Partindo do pressuposto que isso é uma característica do modelo, ou seja, na abordagem proposta sempre é preciso obter uma prova da validade do certificado para o instante onde se quer evidenciar sua validade, não há a necessidade de que o certificado seja emitido por uma Autoridade Certificadora. A prova de sua validade, obtida quando necessário, pode fornecer a evidência suficiente para a comprovação das informações do certificado.

Para isso, é possível fazer uso de um certificado autoassinado para vincular as informações da chave e da entidade detentora dessa chave. Desta forma, neste modelo não há caminho de certificação acima do certificado, e todos os problemas relacionados a isso são automaticamente eliminados.

O certificado nesta abordagem passa a ser apenas um documento com as informações declaradas pela entidade, e uma assinatura que tem o efeito de prova de posse da chave privada e integridade das informações declaradas. O formato deste certificado é similar a um certificado autoassinado proposto no modelo X.509, portanto o próprio padrão X.509 pode ser utilizado para a codificação do mesmo, por questão de simplicidade e pelo fato de já existir uma boa base de código para a implementação de sistemas baseados neste padrão. A Figura 5.1 demonstra a estrutura básica da infraestrutura proposta, onde a bola representa uma entidade, a linha contínua representa uma assinatura e a linha pontilhada uma referência.

5.1.2 Autoridades: Notarial e de Registro

É necessário que exista ao menos uma entidade responsável pela emissão das provas de validade do certificado autoassinado proposto, com papel de Autoridade análogo a Autoridade Certificadora (AC) do padrão X.509. Para a NBPKI, são propostas duas autoridades: A Autoridade de Registro (AR) e a Autoridade Notarial (AN).

A Autoridade de Registro tem um papel bastante semelhante àquele desempenhado por uma AR em uma infraestrutura X.509. Na nova

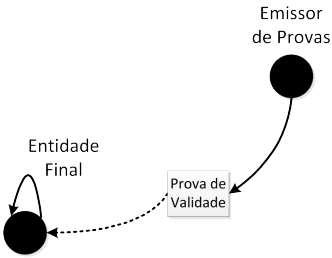

Figura 5.1: Certificado Autoassinado e Prova de Validade

abordagem proposta, o usuário gera seu próprio certificado autoassinado e realiza uma autenticação segura com uma Autoridade de Registro para provar sua identidade e posse da chave privada. A AR verifica os dados do certificado e a posse da chave, e os envia para a Autoridade Notarial, através de uma mensagem que informa a aprovação do certificado autoassinado do usuário. A Autoridade Notarial é a entidade responsável por emitir provas, quando solicitado, de que o certificado do usuário é válido num determinado instante de tempo.

Para uso em uma ICP onde documentos serão assinados digitalmente e a identidade do detentor da chave deve ser fortemente garantida, a autenticação segura deve ser feita de forma presencial, confirmando a posse da chave em hardware seguro e a identidade do signatário. Neste modo de autenticação, o usuário precisa ir a uma instalação técnica da AR para se apresentar, provar (através de documentos) que ele é quem alega ser e provar a posse da chave privada ou dizer-se responsável pela mesma. Esta abordagem é a que é praticada comumente em ICPs X.509, e é mantida na NBPKI. Após esta confirmação, o certificado autoassinado será enviado pela AR para uma ou mais Autoridades Notariais.

Como não existe uma AC para assinar o certificado do usuário, então este não precisa mais esperar por sua emissão. O certificado pode ser emitido a qualquer momento por conta própria, e o usuário apenas precisa ir até a AR quando desejar que seu certificado possa ser validado por terceiros. As assinaturas feitas pelo usuário a partir do momento que uma AN passa a responder por sua validação podem ser verificadas. A Figura 5.2 ilustra as possíveis mensagens envolvidas na emissão e validação de uma prova de validade.

No modelo tradicional de ICP, o usuário precisa aguardar até que a AC emita seu certificado. Em caso de ACs offline, a operação pode levar alguns dias. Em geral, uma AC offline acumula uma certa quantidade de certificados para emití-los em lote. No nosso modelo, após a AN receber da AR a mensagem com a aprovação do certificado, apenas é necessário um processo simples e automático de registro de dados em uma base segura e a AN já está pronta para responder consultas sobre a validade do certificado.

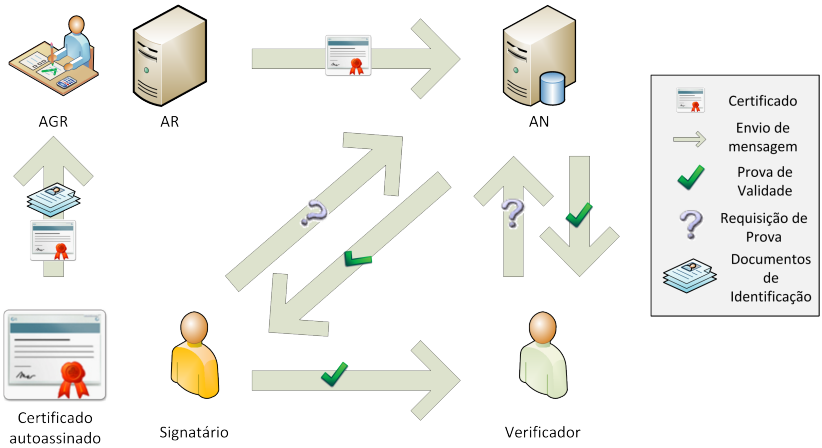

Figura 5.2: Mensagens envolvidas na validação de um certificado

5.1.3 A prova de validade (*token*)

Na NBPKI, o certificado autoassinado é usado apenas para distribuição da chave pública correta do usuário e para vincular a mesma ao seu detentor. Não há cadeia de certificação entre este e a âncora de confiança, já que isto não é necessário. A prova de validade evidenciará a validade do certificado. Com estas modificações, o verificador não precisa mais construir o caminho de certificação para verificar a integridade e posse do par de chaves do signatário.

Quando o verificador precisar validar a integridade de um certificado de usuário, este precisa obter uma prova de validade de uma Autoridade Notarial. Esta prova pode ser obtida pelo detentor do certificado e enviada ao verificador, ou solicitada pelo próprio verificador. Quando recebe uma requisição de verificação de validade, a AN verifica a situação do certificado em questão na sua base de dados e retorna uma prova, a qual também chamamos de *token*, e que contém a situação de revogação do certificado. Este *token* contém a prova de que o certificado é válido ou inválido em um determinado período de tempo. Propõe-se que o período de validade do *token* seja o mais curto possível, desta forma pode-se dispensar a utilização de um mecanismo de revogação para validar o *token*, conforme argumentam os trabalhos de Rivest e Elisson (RIVEST, 1998; ELLISON et al., 1999). De fato, é necessário que o *token* seja válido apenas por um instante de tempo t.

A data incluída no *token* é obtida da AN a partir de um relógio seguro, de maneira similar a o que ocorre em Autoridades de Carimbo de Tempo. Desta forma, a data pode ser considerada confiável, desde que a Autoridade Notarial que emitiu a prova também o seja.

5.2 MÚLTIPLAS AUTORIDADES NOTARIAIS

Assim como no modelo X.509, para dar escalabilidade ao modelo poderá ser necessário dispor de mais de uma Autoridade Notarial em um determinado domínio. Isso implica na necessidade de algumas adições ao modelo para que seja possível dispor de múltiplas ANs. Algumas diferentes abordagens foram consideradas, buscando-se minimizar a quantidade de informações necessárias para a validação de certificados e suas assinaturas digitais

5.2.1 ANs não violáveis

Assim como ACTs, as ANs são serviços que operam em ambientes altamente controlados. Desta forma, poderiam ser consideradas invioláveis, e portanto dispensariam a possibilidade de revogação, permitindo que as ANs tivessem simplesmente seus certificados assinados por uma AN Raiz, e não fossem revogadas. Entretanto essa possibilidade certamente encontraria resistência, da mesma forma que propostas similares referentes à ACTs.

5.2.2 A abordagem tradicional

A abordagem tradicional é a utilização de uma Autoridade Certificadora Raiz para a emissão de certificados para as Autoridades Notariais e Autoridades de Registro. A revogação dos certificados ocorre com o uso de LCRs. Entretanto, desta forma traria-se ao modelo os problemas já levantados no Capítulo 3, em especial aqueles relacionados aos carimbos de tempo. Estes problemas ocorreriam em escala menor do que na ICP X.509, uma vez que as LCRs apenas estariam sendo utilizadas para os níveis superiores da ICP, onde há menos atualizações de LCRs e menor probabilidade de revogação de certificados uma vez que todas entidades operam em ambientes fortemente controlados. Além disso, pelo fato de não serem usadas ACTs, documentos assinados sob uma NBPKI que usasse esta abordagem teriam apenas um ramo de cadeia de confiança a ser verificado, e não dois ou mais.

5.2.3 Cadeia de Autoridades Notariais

A substituição da AC Raiz por uma AN raiz também seria possível. Esta emitiria provas para a AN subordinada. Entretanto uma prova atualizada teria que ser obtida no momento da verificação, de forma similar e pelo mesmo motivo citado no caso anterior, gerando uma demanda muito grande para a AN Raiz que teria que responder ao menos uma requisição de prova para cada prova emitida pelas suas ANs subordinadas. Do ponto de vista de escalabilidade, facilmente esta situação se tornaria rapidamente problemática.

5.2.4 Novomodo

Outra possível abordagem é a baseada no método de Novomodo. Para isso, propõe-se que as ANs e ARs de uma ICP NBPKI tenham certificados digitais assinados por uma Autoridade Certificadora Raiz, similar a AC raiz de uma ICP X.509. Essa é a única hierarquia que existe no modelo, e permite que todas as ANs e ARs, bem como os usuários finais, reconheçam quais entidades fazem parte do domínio.

Como a AR só assina mensagens destinadas à ANs, não haveria maiores problemas em se manter o esquema de LCRs para verificar, por parte da AN, se um certificado de AR continua válido. Esta complexidade seria tratada apenas por entidades da infraestrutura, e o que se objetiva é limitar a complexidade para os usuários finais. Mas há ainda o certificado da AN, que precisa ser validado pelos usuários da NBPKI.

Para evitar o uso de LCRs como prova de que o certificado da AN é válido, propõe-se usar o as provas do Novomodo do protocolo de Micali (MICALI, 1995), de forma semelhante à descrita por Custódio (CUSTóDIO et al., 2008). Isso implica na inserção de uma prova de novomodo do certificado da AN dentro do *token* emitido. Tal prova, produto de uma lista de resumos criptográficos conforme descrito na seção 4.2.6, é produzido diretamente pela AC Raiz.

Para a validação também é necessário que uma prova recente seja utilizada. Caso a prova incluída no *token* não seja mais a prova atual no momento da verificação, será necessário que o verificador obtenha uma nova prova mais recente. Entretanto, diferente da abordagem por Listas de Certificados Confiáveis ou mesmo de encadeamento de Autoridades Notariais, esta é uma informação pequena, e pode ser verificada apenas com operações de resumo criptográfico, que são mais baratas computacionalmente.

A mesma técnica poderia ser usada para provar a validade dos certificados das ARs. Assim, eliminariamos a lista de certificados revogados de nosso modelo de certificação. E com isso, elimina-se a maior parte dos problemas que essas trazem para a ICP, com todas as informações necessárias para validação da prova dentro do *token*.

A prova de Novomodo é uma informação de pequeno tamanho e que dá uma resposta objetiva a situação presente de um certificado: "É válido agora" ou "Não é válido agora". É uma informação de pequeno porte, que pode ser inserida na própria prova publicada pela AN, em um campo não assinado (de forma que possa ser atualizável a qualquer momento).

5.2.5 Listas de Confiança

Em uma ICP X.509, as ACs emissoras dos certificados, bem como as ACTs emissoras dos carimbos de tempo, são confiadas com base na montagem de um caminho de certificação destas até uma AC Raiz. Já a

confiança nesta AC Raiz é estabelecida através da adição da mesma em uma lista de certificados confiáveis, usualmente gerenciada pelo sistema operacional. A revogação da confiança neste certificado ocorre através da remoção do certificado desta lista. Não há LCRs, mas a lista de certificados confiáveis deve ser mantida atualizada e existe o problema de como gerenciar esta atualização e garantir a segurança desta lista.

O gerenciamento destas listas tradicionalmente é feito de maneira não padronizada. Cada sistema lida com esta lista de um modo diferente. Entretanto, recentemente surgiu uma iniciativa para padronização destes procedimentos, publicada pela ESTI (ETSI, 2006a). Este padrão prevê a utilização da TSL (*Trust-service Status List*), uma lista que indica a situação de cada provedor de serviços de confiança em uma ICP, como ACs e ACTs.

Uma abordagem possível para o gerenciamento das ANs confiáveis foi a publicação online de uma Lista de Autoridades Notariais confiáveis. As ANs, desta forma, também poderiam ter certificados autoassinados. Esta lista, formada por resumos criptográficos das ANs, publicada online e assinada por uma Autoridade Certificadora Raiz, deve ser sempre atualizada, tendo para isso um determinado período de validade restrito, análogo ao das LCRs. As partes interessadas devem que consultar a lista no momento da verificação, para assegurar que a AN que emitiu a prova continua válida.

A abordagem tem vantagens diante da abordagem tradicional. Primeiro, a pergunta esperada é respondida: "Que ANs são confiáveis neste momento?". O verificador pode, com uma simples consulta, determinar se o certificado que ele dispõe é ou não fruto de uma AN confiável naquele momento. Cabe no entanto destacar que a verificação precisa necessariamente ser feita com base em uma lista válida para o instante onde é realizada a validação, uma vez que não se pode confiar na data informada por uma AN que se supõe ser violável, e portanto não se pode basear a verificação na lista de autoridades notariais confiáveis da data em que a prova de validade foi emitida.

O gerenciamento de atualização destas listas fica a cargo do sistema operacional. Simplifica-se de maneira significativa a questão da gestão de confiança nas ANs, que não possuem mais cadeias de certificação e todos os problemas relacionados.

5.3 IDENTIFICAÇÃO DAS AUTORIDADES

A abordagem, tal como proposta, permite a livre associação entre ARs e ANs. As ARs podem informar situação dos certificados para as ANs com as quais mantém acordo, e a qualquer momento cancelar acordos existentes (com o descredenciamento dos certificados na AN) ou criar novos acordos.

Entretanto, considerando que podem existir várias autoridades notariais dentro de uma mesma ICP NBPKI, é necessário que exista um

mecanismo para a identificação de qual é a Autoridade Notarial a ser consultada quando se deseja verificar a validade e uso de um determinado certificado. Mais especificamente, um endereço (exemplo: URI) precisa ser disponibilizado apontando para a localização da Autoridade Notarial na internet. Duas abordagens principais foram analisadas, mas em ambos os casos propõe-se que a Autoridade de Registro seja a responsável por indicar quais as Autoridades Notariais habilitadas a responder por um determinado certificado.

5.3.1 Valorização da Autoridade de Registro

No modelo usual de ICP, a Autoridade de Registro é quem de fato é responsável pela ligação efetiva entre uma entidade e sua chave. É esta autoridade que faz a verificação dos documentos pessoais da pessoa física e jurídica, verifica a posse da chave privada, em alguns casos verifica até mesmo que esta chave foi gerada e armazenada um dispositivo seguro, por exemplo em um *smartcard*. Entretanto, no modelo de negócios de uma ICP usual, a Autoridade de Registro tem um papel secundário na validação do certificado, participando apenas de uma etapa inicial de validação, e depois delegando a responsabilidade de provar a validade do certificado para uma Autoridade Certificadora (através da emissão de um certificado inicial e de provas de não-revogação - LCRs onde não constam este certificado).

No nosso modelo de ICPs, a Autoridade de Registro pode assumir um papel muito mais importante. O usuário, ao invés de ter seu certificado atrelado a uma única AC, passa a atrelar o seu certificado a uma AR, escolhida de acordo com seus interesses, oferta de Autoridades Notariais, qualidade de serviço, políticas, entre outros possíveis motivos. Esta AR poderá escolher livremente com quais Autoridades Notariais firmará parcerias, ou seja, para quais ANs informará o estado dos certificados digitais. A AR pode firmar parcerias novas a qualquer momento, adicionando, removendo ou trocando ANs dentre as suas relacionadas.

Para isso, é necessário que a Autoridade de Registro publique uma lista de ponteiros para Autoridades Notariais. Essa lista pode ser assinada, mas isso não é realmente necessário. Caso uma lista forjada, com Autoridades Notariais não habilitadas seja publicada, não há risco para o verificador, uma vez que as Autoridades Notariais para as quais a lista forjada apontaria ainda teriam que estar na lista de Autoridades Notariais confiáveis, e portanto, supõe-se que operam de forma confiável. E caso as ANs presentes na lista sejam confiáveis, mas não possuem acordo com a referida AR, a AN deverá responder que não conhece o certificado, forçando o verificador a consultar novamente outras ANs habilitadas até encontrar uma resposa positiva. Estas listas podem ser armazenadas localmente e atualizadas conforme o interesse do verificador, limitando a necessidade de acessos constantes ao endereço da AR.

Entretanto, ainda resta a questão de como ligar o certificado au-

toassinado a Autoridade de Registro correspondente, de forma que um verificador possa encontrar, através da lista publicada por esta AR, a AN onde pode validar seu certificado. A primeira proposta é incluir o ponteiro para a AR no certificado, e a segunda é incluir o ponteiro nas provas. Cada proposta possui as suas respectivas vantagens e desvantagens, analisadas a seguir.

5.3.2 Ponteiro no certificado

Um ponteiro no certificado para uma AR permitiria de forma simples que qualquer verificador ou servidor de autenticação encontrasse a Autoridade de Registro onde o certificado está cadastrado. Entretanto, é necessário que essa informação seja inserida no certificado antes do próprio credenciamento junto a AR (onde já se supõe a existencia do certificado autoassinado). O emissor do certificado deverá portanto emitir o seu certificado com seus dados pessoais e já tendo escolhido uma AR onde irá se credenciar, adicionar também as informações necessárias para acesso a lista de ANs publicada por essa AR. Apesar de um impecilho a proposta de que o certificado apenas seja credenciado quando for necessário, é possível implementar isso tecnicamente. A Figura 5.3 ilustra essa abordagem.

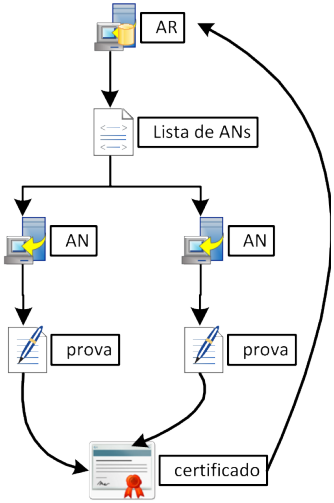

Figura 5.3: Ponteiro para AR no certificado

Outra desvantagem desta abordagem é que adiciona um impedimento a migração do certificado para uma nova AR, caso isso seja necessário, forçando a emissão de um novo certificado.

5.3.3 Ponteiro nas provas

Uma segunda abordagem é que o ponteiro para a AR seja adicionada à prova de validade propriamente dita. Uma grande vantagem imediata desta abordagem é que o verificador da prova sempre terá acesso à AR que era a aprovadora do certificado no momento que a prova foi emitida, mesmo que ocorra uma mudança deste certificado para uma nova AR no futuro. Outra característica importante desta modalidade é que ela adiciona uma grande flexibilidade a NBPKI, pois como o vínculo com a AR não é mais dado pelo certificado, e sim pela prova, um mesmo certificado pode ser validado por mais de uma AR ou até mesmo dentro de mais de uma ICP, em diferentes domínios. E o certificado pode de fato ser emitido de maneira completamente independente, sem interação ou vínculo com uma determinada Autoridade de Registro. A Figura 5.4 ilustra esta abordagem.

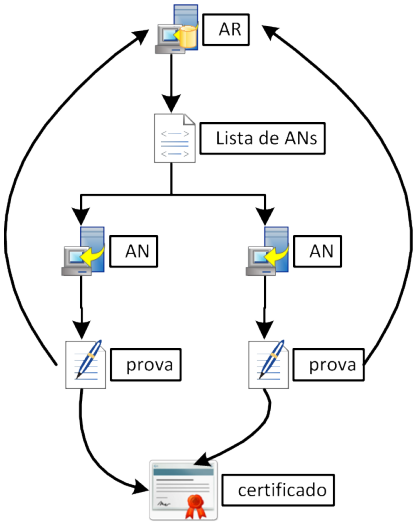

Figura 5.4: Ponteiro para AR na prova

A desvantagem principal do modelo é que ela força a existência da prova para permitir a um verificador obter informações sobre o estado do certificado, necessitando a primeira prova ser obtida pelo próprio detentor do certificado em consulta direta à uma das ANs da lista publicada pela AR onde este se credenciou. Uma abordagem facilitadora deste processo é a própria AR já solicitar e fornecer esta primeira prova no próprio processo de credenciamento.

Entretanto, esta abordagem inviabiliza esquemas de autenticação com prova obtida pelo servidor ou de validação de assinatura com prova obtida pelo verificador, como será proposto em 5.4. O verificador e o

servidor de autenticação, no entando, poderiam continuar obtendo reemissões de provas sem qualquer problema, pois aí já teriam acesso ao ponteiro para a AR correspondente.

Desta forma, a abordagem adotada neste trabalho é de adicionar os ponteiros para a AR no certificado.

5.4 APLICAÇÃO DO MODELO

Além da própria simplificação do processo de validação de certificados, propomos que a AN possa atuar também como uma fornecedora de prova de confiabilidade temporal para assinaturas digitais de longo prazo. Para melhor analisar a questão da aplicação deste modelo em cada situação, classificamos o uso dos certificados em dois tipos: autenticação e assinatura de documentos. A aplicação da proposta em ambos os casos é melhor detalhada nas próximas duas sessões.

5.4.1 Autenticação

Para processos de autenticação, o *token* emitido pela AN apenas prova que o certificado é válido para um instante de tempo. Esta opção pode ser útil para assinaturas de curto prazo e especialmente mecanismos de autenticação. Um único *token* pode ser utilizado inúmeras vezes para quantas autenticações forem necessárias, sem necessidade de obtenção de mais dados externos pelo verificador.

Para uma autenticação, a aplicação do usuário obtém o *token* de curta duração com a AN que detém prova que seu certificado é válido. Após isso, a aplicação do usuário envia o certificado e o *token* para o servidor de autenticação. O servidor pode então confirmar os dados do usuário no certificado, bem como a validade do mesmo através do *token*. A Figura 5.5 apresenta este processo.

Se a aplicação cliente não tem recursos suficientes para enviar o *token*, o servidor pode realizar o procedimento de obtenção do *token* por conta própria. A aplicação cliente apenas envia o certificado, e o servidor consulta uma Autoridade Notarial para confirmar a validade do mesmo. A Figura 5.6 apresenta este processo.

5.4.2 Assinaturas de Documentos

Quando um usuário assina um documento, a aplicação pode encaminhar à AN o certificado e o resumo criptográfico da assinatura. A AN verifica a validade do certificado, e retorna para a aplicação um *token*. Este *token* fornece uma prova de validade não apenas da certificado, mas também de que a assinatura existia naquele instante de tempo. A sessão 5.8.2 detalha a estrutura proposta para este *token*. O *token* pode ser usado para provar que determinada assinatura era válida para a data em que foi gerado. A Figura 5.7 apresenta as informações relacionadas a um docu-

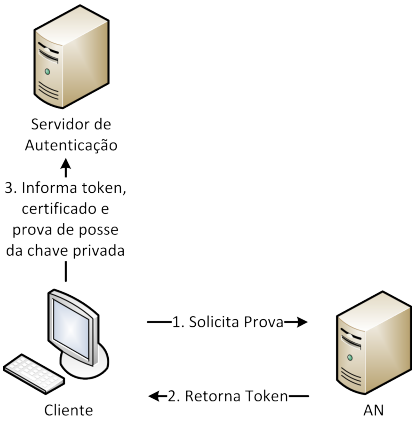

Figura 5.5: Auntenticação com *token* obtido pelo cliente

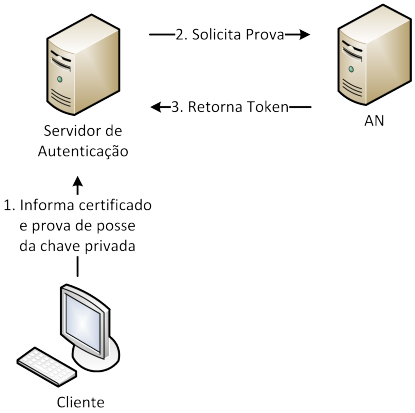

Figura 5.6: Autenticação com *token* obtido pelo servidor

mento assinado sob a NBPKI. A bola representa uma entidade, a linha contínua representa uma assinatura e a linha pontilhada uma referência.

O *token* deve ser anexado como um atributo não-assinado da assinatura digital e é apenas útil quando alguém quer validar a assinatura de um documento eletrônico. Note que se o signatário não anexar o *token* conforme demonstrado na Figura 5.8, o primeiro verificador interessado pode fazê-lo (Figura 5.9). Se o certificado for válido quando esta solicitação é feita, a AN envia o *token* ao verificador que pode anexa-lo à assinatura. Um próximo verificador ao receber o documento assinado poderá verificar a validade desta sem mais consultas à AN.

Na verificação de assinatura nos modelos tradicionais de

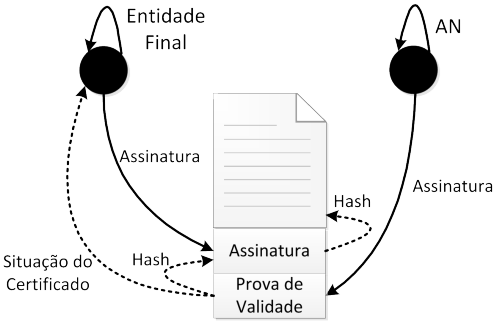

Figura 5.7: Um documento assinado sob a NBPKI

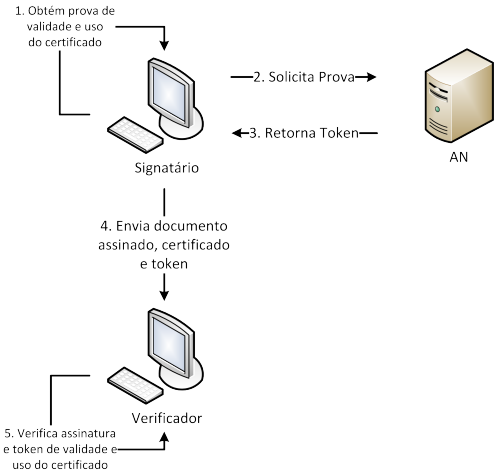

Figura 5.8: Assinatura com *token* obtido pelo signatário

certificação digital, o verificador precisa primeiro verificar a integridade do carimbo do tempo e depois a integridade e validade da assinatura digital. Para verificar a integridade do carimbo do tempo, o usuário precisa construir e validar o caminho de certificação entre o certificado da Autoridade de Carimbo do Tempo (ACT) emissora do carimbo do tempo e a âncora de confiança. E depois, construir e validar o caminho de certificação do certificado do signatário. Com o modelo de certificação que está sendo proposto é preciso somente verificar a validade do *token*. Se o *token* for válido, o verificador verifica a integridade da chave pública do signatário, mas sem precisar construir ou validar cadeias de certificação, uma vez que trata-se de um certificado autoassinado.

Se a assinatura do *token* é válida, então a assinatura era existente

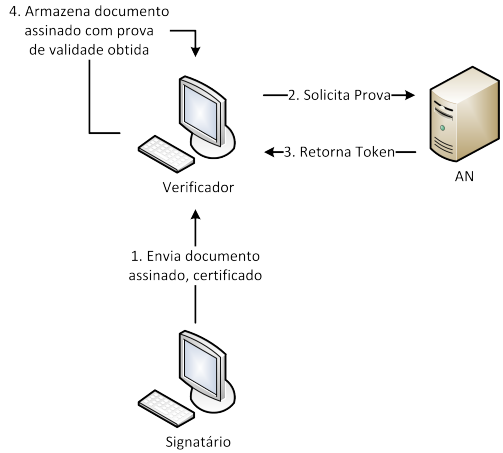

Figura 5.9: Assinatura com *token* obtido pelo verificador

na âncora de tempo especificada pelo *token*. E desta forma ela pode ser verificada com a chave pública do certificado autoassinado do signatário, com base na data de emissão do *token*, sem mais consultas externas.

A mesma assinatura digital pode ser validada por mais de uma AN. O verificador pode validar a situação do certificado em qualquer uma das ANs que receberam informações da AR.

5.4.3 Manutenção a longo prazo da assinatura

Para a conservação da validade de uma assinatura, é necessário obter provas atualizadas emitidas por novas ANs, antes que a prova anterior perca sua validade. Neste sentido, o comportamento da AN é bem parecido com o de uma ACT do modelo tradicional. Entretanto, é importante destacar que se propõe que não seja necessário adicionar um novo *token*, mas sim substituir o antigo. A AN, ao receber um *token* para ser revalidado, confirma as informações do *token* antigo e gera um novo *token*, com as mesmas informações do anterior, mas com sua assinatura.

Caso se necessite atualizar o algoritmo de resumo criptográfico utilizado para a identificação da assinatura (por exemplo, caso o algoritmo antigo esteja prestes a ser comprometido), é necessário adicionar um novo resumo criptográfico da assinatura, gerada com algoritmos mais modernos, na requisição de revalidação. A revalidação deve ocorrer antes da quebra do resumo criptográfico anteriormente adicionado.

Note-se que o *token* revalidado poderá ter dois ou mais resumos criptográficos apontando para a assinatura do documento, o original e os novos, entretanto não há nenhuma comprovação por parte da AN de que todos os resumos criptográficos incluídos referem-se à mesma assinatura

digital. O primeiro resumo é o da assinatura declarada como existente no momento da emissão da prova, e os demais são resumos adicionados por qualquer entidade interessada.

Um eventual atacante pode solicitar, sem qualquer problema, *tokens* com resumos criptográficos que não são se referem à mesma assinatura original. Mas não há qualquer violação de segurança nisso, uma vez que um verificador facilmente detectará ao verificar todos os resumos criptográficos que estes não se referem ao mesmo documento. Considerando-se que revalidações com adição de novos resumos somente são aceitos enquanto os algoritmos de ao menos um dos já existentes continuam seguros, é probabilisticamente impossível que um atacante tenha, antes da quebra dos algoritmos, forjado uma assinatura diferente da original que no futuro seja apontada por todos os resumos criptográficos.

No modelo tradicional de ICP, para a conservação de longo prazo de um documento eletrônico, é necessário sempre adicionar novos carimbos do tempo sobre os carimbos do tempo anteriores, antes que estes percam sua validade. Cabe destacar que se comprometida a Autoridade de Carimbo do Tempo, todos os carimbos por ela já emitidos tornam-se inválidos, caso não exista um segundo carimbo contraposto ao primeiro. Isto é um problema, pois não há como prever a violação de uma ACT. Essa abordagem leva ao crescimento contínuo do arquivo de assinatura.

No presente modelo a assinatura tem sempre praticamente o mesmo tamanho, sendo acrescido apenas de um novo valor de resumo criptográfico. E também possibilita a atualização de algoritmos de maneira extremamente simples. Os novos *tokens* podem fazer uso de algoritmos mais seguros e assim manter a confiabilidade da validação mesmo após a quebra dos algoritmos anteriormente usados.

5.5 FUNCIONAMENTO INTERNO DA AUTORIDADE NOTARIAL

5.5.1 Armazenamento de estados de certificados

Neste modelo, a Autoridade de Registro é a entidade responsável por definir os certificados que são ou não confiáveis. Ela armazena estes dados e repassa a Autoridade Notarial, mantendo esta informada sobre revogação e outros possíveis incidentes. É importante que tanto uma quanto a outra possuam um forte sistema de segurança interno para armazenar estes estados, com garantia de integridade.

A Autoridade de Registro comunica-se principalmente com a Autoridade Notarial. Com uma boa infraestrutura de controles de segurança na comunicação com os usuários (que se restringe a pedidos de aprovação ou revogação de certificados) pode-se obter um bom grau de segurança.

Já a Autoridade Notarial tende a ser o alvo principal de ataques, pois é a entidade que é constantemente consultada. Além dos sistemas de controle básicos esperados de qualquer sistema crítico online, é importante que medidas de contingência sejam tomadas. Caso uma Autoridade

Notarial tenha detectada uma invasão, ela deve ser marcada como revogada na Lista de Autoridades Notariais. Nesta situação, uma nova AN deverá assumir responsabilidade sobre os certificados (ou as demais ANs por ela credenciadas, caso sejam mais de uma), recebendo da Autoridade de Registro as informações sobre validade e revogação dos certificados. O tratamento das provas já emitidas, que precisarão neste contexto ser reemitidas, está descrito na seção 5.5.3.2.

5.5.2 Emissão de uma prova

O processo de emissão da prova segue o fluxo descrito pelo Algoritmo 5.1. Essencialmente, a AN realiza uma verificação na sua base de dados sobre a situação do certificado no instante da consulta, e caso tenham sido informados dados de uma assinatura digital, adiciona os mesmos na prova.

```
Entrada: "Identificador do Certificado",("Resumo criptográfico da
         assinatura")
Saída: "Prova de Validade"
início
    se "AN conhece o certificado" então
        se "Certificado consta como válido" então
            se "Prova contém dados de documento" então
                "Token: Certificado Válido e Dados informados"
            senão
                "Token: Certificado Válido"
            fim
        senão
            "Token: Status do certificado'
        fim
    senão
        "Token: Não conheço o certificado"
    fim
fim
```

Algoritmo 5.1: Emissão de Prova NBPKI

5.5.3 Reemissão de uma prova

Existem três contextos onde uma prova pode ter que ser re-emitida: caso deseje-se atualizar os algoritmos utilizados na prova, caso a autoridade notarial correspondente tenha chegado ao fim do seu tempo de operação (e portanto não existam mais informações sobre a continuidade da sua operação), e por último, caso a autoridade notarial tenha sido comprometida. Analisaremos cada caso de maneira separada.

5.5.3.1 Mudança de algoritmo

Caso deseje-se obter, por qualquer motivo, uma prova atualizada com uso de novos algoritmos, o processo de emissão da prova segue o fluxo descrito pelo Algoritmo 5.2.

```
Entrada: "Prova de Validade", "Novos Resumos Criptográficos"
Saída: "Prova de Validade"
início
    se "Prova é íntegra e emitida por AN válida, com algoritmos
    ainda seguros" então
        se "Requerente informou novos resumos criptográficos"
        então
            "Token: mesmos dados, com novos resumos
            criptográficos informados"
        senão
            "Token: mesmos dados"
        fim
    senão
        "Token original não confiável"
    fim
fim
```

Algoritmo 5.2: Reemissão de Prova NBPKI - Alteração de Algoritmos

Note-se que inclusive a data de emissão é mantida, bem como outras informações. A AN apenas atualiza os algoritmos, por confiar na AN que emitiu o *token* anterior.

5.5.3.2 AN revogada

Caso a AN tenha sido revogada (comprometida), não será possível reemitir provas de validade diretamente. É necessário que uma AN especialmente designada, que receba um histórico das provas de fato emitidas pela AN, reemita esta prova. Por esse motivo é fundamental que as Autoridades Notariais armazenem de modo seguro um histórico das provas que emitem. Existem diversas soluções adequadas para este armazenamento na literatura (SCHNEIER; KELSEY, 1999; MA, 2008; MA; TSUDIK, 2009), que não serão abordadas em detalhes trabalho.

As demais Autoridades Notariais credenciadas à AR assumem o papel de validar e confirmar os dados de certificados emitidos por ANs revogadas.

5.5.3.3 AN expirada

Se a AN não tiver sido revogada, pode-se considerar que a chave da AN foi destruída após sua expiração, e portanto não pode ter sido usada para simular novas provas. A prova pode ser assumida como válida neste contexto, evitando a necessidade de reemissão.

Outra abordagem possível é que, uma vez expirada a AN, seja dado tratamento similar a de uma AN revogada, ou seja, através da publicação de um histórico de provas emitidas para as ANs ainda em operação. Desta forma, mesmo após a expiração, as ANs podem verificar de maneira segura quais provas podem ser reemitidas.

5.6 INTEGRAÇÃO E FEDERAÇÕES NBPKI

A abordagem proposta abre espaço para uma nova abordagem de integração entre ICPs. Quando é solicitada a reemissão de uma prova de uma ICP diferente, a AN pode consultar as ANs desta outra ICP e, existindo um acordo de confiança entre estas ICPs e uma vez verificada a confiabilidade daquele certificado, emitir uma nova prova dentro da cadeia da sua própria ICP, sem necessidade de estabelecimento de um novo caminho de certificação.

Isso simplifica de maneira significativa as relações de confiança entre diferentes domínios, deixando para as entidades superiores da cadeia, e não para o usuário final, a complexidade do estabelecimento de confiança entre as ICPs.

5.7 MODELO DE NEGÓCIOS

Ao contrário da ICP X.509, a NBPKI é muito mais flexível no que diz respeito a modelos de negócio. O serviço de credenciamento de um certificado junto a AR não é mais o único serviço tarifável, mas também serviços como emissão e reemissão de provas. Preços diferenciados podem ser praticados, mais justos e proporcionais a quantidade de uso de cada serviço.

5.8 PROTOCOLO PROPOSTO

Apresentamos a seguir a estrutura básica para a proposta de um protocolo de requisição de provas de validade para uma AN.

5.8.1 Requisição de Prova de Validade

Quando uma entidade qualquer deseja solicitar uma prova de validade à Autoridade Notarial, esta tem duas opções básicas: solicitar uma prova de validade do certificado (que chamaremos de prova de

autenticação), ou uma prova de validade e uso do certificado (que chamaremos de prova de assinatura). No primeiro caso, a prova apenas confirma a existência e ligação do certificado com os dados nele contidos. No segundo caso, a prova também contém informações sobre os dados onde este certificado foi efetivamente utilizado para uma assinatura digital.

Para obter uma prova de validade do certificado P_V, o cliente envia à Autoridade Notarial a mensagem $R_V(Hid_C, H_C, Sid_R, S(R))$, onde:

Hid_C Identificador de algoritmo de resumo criptográfico utilizado;

$H(C)$ Resumo criptográfico do certificado;

Sid_R contém o identificador do algoritmo do resumo criptográfico e assinatura sobre os dados de requisição

$S(R)$ contém a assinatura sobre os dados da requisição

Para obter uma prova de validade e uso do certificado P_U, o cliente envia à Autoridade Notarial a mensagem acrescida dos parâmetros referentes ao documento assinado $R_U(Hid_C, H(C), Aid_D, S(D), Sid_R, S(R))$, onde:

Hid_S Identificador de algoritmo de resumo criptográfico utilizado;

$H(S)$ Resumo criptográfico da assinatura digital;

O código abaixo representa a estrutura ASN.1 proposta para estas requisições:

```
ValidityProofRequest ::= SEQUENCE {
    version            INTEGER { v1(1) },
    signerCertificateDigestAlgorithm
                       AlgorithmIdentifier
    signerCertificateDigest   OCTET STRING
    signature           SignatureInfo OPTIONAL }

SignatureInfo ::= SEQUENCE {
    digestAlgorithm   AlgorithmIdentifier,
    signatureHash     BIT STRING           }
```

O campo *version* identifica a versão da requisição. A versão atual é v1.

O campo *signerCertificateDigest* contém um identificador único do certificado do usuário, correspondente ao resumo criptográfico do certificado. O algoritmo utilizado é identificado em *signerCertificateDigestAlgorithm*.

O campo *signature* é composto por dois sub-campos: *signatureAlgoritm* e *documentSignature*. Estes dois campos são apenas utilizados quando é solicitado uma prova de validade de assinatura de documento. Quando uma prova de autenticação é solicitado estes campos não devem ser preenchidos.

O campo *digestAlgorithm* identifica o algoritmo utilizado para gerar o resumo criptográfico sobre a assinatura do documento. E o campo *signatureHash* contém o resumo criptográfico da assinatura digital sobre o documento.

5.8.2 Resposta de Validade

Em resposta a requisição, a Autoridade Notarial responde com uma prova de validade. Dependendo do tipo de solicitação, a prova será de validade do certificado P_V ou de uso P_U, sendo $P_V(T, Hid_C, H(C), St_C, Pl_C, C_{NA}, St_NA, Sid_P, S(P))$ e $P_U(T, Hid_C, H(C), St_C, Pl_C, \{Hid_S, H(S)\}, C_{NA}, Nv_NA, St_NA, Sid_P, S(P))$ onde:

T é a data de emissão da prova;

Hid_C é o identificador do algoritmo de resumo criptográfico utilizado pra identificar o certificado

$H(C)$ é o resumo criptográfico do certificado

St_C é a situação do certificado informado pela autoridade notarial

Pl_C é a lista de políticas sob as quais o certificado é válido

Hid_S para provas de uso do certificado, contém o identificador do algoritmo de resumo criptográfico utilizado sobre a assinatura digital realizada pelo usuário

$H(S)$ para provas de assinatura realizada pelo certificado, contém o resumo da assinatura digital realizada pelo usuário

C_{NA} contém o certificado da autoridade notarial (opcional)

St_NA contém o status da resposta

Sid_P contém o identificador do algoritmo do resumo criptográfico e assinatura sobre os dados de resposta

$S(P)$ contém a assinatura sobre os dados da resposta

O código abaixo representa em ASN.1 a prova de validade e uso do certificado. O campo *version* identifica a versão da requisição. A versão atual é v1.

```
ValidityProoftoken ::= SEQUENCE {
    version              INTEGER { v1(1) },
    tokenValidity        Time,
    signerCertificateDigestAlgorithm
                         AlgorithmIdentifier
    signerCertificateDigest
                         OCTET STRING
```

```
    signerCertificateStatus
                        SigCertStatus,
    validPolicies       ValidPolicies,
    signatureProof      SignatureProof OPTIONAL,
    extraSigProofs      SET { SignatureProof } OPTIONAL,
    naCertificate       Certificate    OPTIONAL,
    responseStatus      ResponseStatus,
    signatureAlgorithm  AlgorithmIdentifier,
    signatureValue      BIT STRING     }

SigCertStatus ::= ENUMERATED {
    valid               (0),
    revoked             (1),
    expired             (2),
    removed             (3),
    error               (4)     }

ResponseStatus ::= ENUMERATED {
    successful          (0),
    invalidRequest      (1),
    internalError       (2),
    tryLater            (3),
    unknownCertificate  (4),
    badDigestAlgorithm  (5),
    unsupportedVersion  (6) }

ValidPolicies ::= SEQUENCE {
    policyIdentifier    OBJECT IDENTIFIER }

SignatureProof ::= SEQUENCE {
    hashDate          Time,
    digestAlgorithm   AlgorithmIdentifier,
    signatureHash     BIT STRING   }

AlgorithmIdentifier  ::=  SEQUENCE  {
     algorithm        OBJECT IDENTIFIER,
     parameters       ANY DEFINED BY algorithm
                                 OPTIONAL  }
```

O campo *tokenValidity* indica o a data onde a AN emitiu a prova de validade do certificado descrito no campo *userCert* com a situação definida no campo *userCertStatus*. É deixado para o domínio da aplicação que usará o token definir qual a janela de tempo aceitável para considerar o certificado válido.

O campo *signerCertificateDigest* contém um identificador único do certificado do usuário, correspondente ao resumo criptográfico do certificado. O algoritmo utilizado é identificado em *signerCertificateDigestAlgorithm*. O campo *signerCertificateStatus* é um código numérico que informa a situação do certificado do usuário, e assinatura quando aplicável. Os possíveis estados são:

- valid (0) - O certificado é válido entre as datas especificadas em notBefore e notAfter, e a assinatura foi corretamente validada, se aplicável.
- revoked (1) - O certificado foi revogado.
- expired (2) - O certificado expirou.

- removed (3) - O certificado é conhecido mas foi descredenciado desta AN sem ter sido revogado, e a AN não dispõe mais de informações atualizadas sobre o mesmo.

- error (4) - Ocorreu um erro processando o estado do certificado. Mais informações sobre o erro são descritos no campo *responseStatus*

O campo *validPolicies* é uma sequência de OIDs que representam políticas sob as quais o certificado é válido. Se não existir uma política válida, o campo tem valor nulo.

O campo *signatureProof* é composto por uma sequencia de três campos: *hashDate*, *digestAlgorithm* e *signatureHash*. O primeiro registra a data que a prova de existência da assinatura foi adicionada ao *token*. Para uma primeira emissão, será igual a data de emissão do *token*, e para uma revalidação de token, caso sejam adicionados novos resumos criptográficos, será a data da revalidação. O segundo campo descreve o algoritmo utilizado para computar o resumo criptográfico da assinatura encaminhada na requisição. O segundo contém o valor do resumo criptográfico da assinatura enviada na requisição.

O campo *extraSigProofs* permite a adição de novos resumos criptográficos, na ocasião da renovação de um certificado onde deseja-se conservar a assinatura provendo resistência a quebra dos algoritmos usados no *token* anterior. Note-se que estes valores não são verificados pela AN. Podem apenas ser considerados caso o *token* tenha sido reemitido antes da quebra do algoritmo da prova original, informação a ser validada pelo uso da data informada no campo *hashDate*.

O campo *signatureProof* é preenchido se a requisição contém o campo *documentInfo*. Neste caso o servidor retorna uma prova que a assinatura era válida numa data específica. A assinatura do *token* prova que o certificado usado para assinar um arquivo específico era válida em uma data específica. Este *token* deve ser anexado a uma assinatura para simplificar o processo de verificação da validade da assinatura no futuro. Se o campo *documentInfo* não é preenchido na requisição, então o servidor retorna uma prova que o certificado é válido durante um determinado período. Este período é definido pelos campos *notBefore* e *notAfter*. Este *token* pode ser anexado a assinaturas para provar que um determinado certificado é válido e as assinaturas feitas por ele são válidas até que o *token* expire.

O campo *naCertificate* contém o certificado da AN codificado em DER.

O campo *responseStatus* fornece informação da situação sobre a resposta de requisição. Trata-se de um código numérico, com os seguintes significados:

- successful - A requisição foi corretamente processada

- invalidRequest - Requisição inválida

- internalError - O servidor apresentou problemas internos
- tryLater - O servidor estava ocupado demais para atender o pedido
- unknownCertificate - O certificado da requisição não é conhecido pela AN
- badDigestAlgorithm - O algoritmo usado para resumo criptográfico não é conhecido ou aceito pelo servidor
- unsupportedVersion - A versão de requisição não é suportada

O campo *signatureAlgorithm* representa o algoritmo de assinatura utilizado pela AN para assinar o *token*, codificado de acordo com as regras associadas com o valor do campo *signatureAlgorithm* de um certificado digital (COOPER et al., 2008). E o campo *signatureValue* contém a assinatura digital de todos os demais campos do ASN.1 codificado em DER.

5.8.3 Requisição de Reemissão de Prova de Validade

Quando uma entidade qualquer deseja solicitar uma reemissão de prova de validade à Autoridade Notarial, esta deve receber a prova antiga para que esta possa ser verificada.

Para obter uma reemissão de prova de validade do certificado P_V, o cliente envia à Autoridade Notarial a mensagem $R_V(P_V)$, onde:

P_V Prova de validade que deve ser revalidada;

O código abaixo representa a estrutura ASN.1 proposta para estas requisições:

```
ValidityProofRequest ::= SEQUENCE {
    version           INTEGER { v1(1) },
    oldProof          ValidityProoftoken,
    extraHashes       ExtraHashes OPTIONAL}

ExtraHashes ::= SEQUENCE {
    digestAlgorithm   AlgorithmIdentifier,
    signatureHash     BIT STRING   }
```

O campo *version* identifica a versão da requisição. A versão atual é v1.

O campo *oldProof* contém a prova anterior a ser revalidada, e o campo *extraHashes* permite informar a AN novos resumos criptográficos que devem ser adicionados à prova. Estes somente serão aceitos caso os resumos criptográficos anteriormente adicionados à prova continuem sendo considerados seguros pela AN.

6 COMPARAÇÃO COM ABORDAGENS EXISTENTES

Neste capítulo são comparados os principais modelos de ICP existentes com o modelo proposto neste trabalho.

6.1 GERAL

A Tabela 6.1 apresenta as principais vantagens e desvantagens dos modelos de ICP, no que diz respeito a seus aspectos gerais. Incluem-se aí custos de operação e manutenção, segurança, escalabilidade, entre outros aspectos.

Modelo	**Vantagens**	**Desvantagens**
PGP	Baixo custo	Pouco escalável, altamente vulnerável a ataques de engenharia social
SPKI	Foco em autorização	Não adequado para outros usos
IBC	Foco em identidade	Dependência do KGC
CLC	A chave privada contém parte secreta, obtida sem interação com KGC	Dependência do KGC
CBC	Une vantagens do certificado com IBC/CLC	Dependência do KGC
X.509	Padrão mais difundido. Flexível e abrangente	Instalação e manutenção complexa, excesso de recursos adicionais necessários (carimbos de tempo, consultas de revogação, etc.)
NBPKI	Simples e flexível	Ainda há necessidade de definição e publicação de padrões

Tabela 6.1: Comparação entre modelos: Aspectos Gerais

6.2 ASSINATURA DIGITAL

A Tabela 6.2 apresenta as principais vantagens e desvantagens dos modelos de ICP, no que diz respeito a aplicação destes para assinatura digital.

Modelo	Vantagens	Desvantagens
PGP	Simples	Fácil forjar uma identidade
IBC	Não há consulta a informação de revogação	Ausência de dados de autenticidade, Dependência do KGC para realização de assinatura
CLC	Não há consulta a informação de revogação	Ausência de dados de autenticidade, Dependência do KGC para realização de assinatura
CBC	Não há consulta a informação de revogação	Dependência do KGC para realização de assinatura
X.509	Uso difundido	Grande quantidade de operações e dados para validação
NBPKI	A prova tem efeito de carimbo de tempo	Exige obtenção de prova online

Tabela 6.2: Comparação entre modelos: Assinatura Digital

6.2.1 Tamanho do arquivo assinado

A Tabela 6.3 apresenta o acréscimo ao tamanho de uma assinatura digital nos respectivos modelos de ICP, sem considerar conservação a longo prazo (que é analisada na seção 6.3).

O tamanho dos documentos assinados, bem como das assinaturas digitais propriamente ditas, são identicos para ambos os casos. O tamanho de um arquivo com a assinatura digital, no entanto, deverá contemplar todos os dados necessários para a validação de um documento. Serão considerados na análise abaixo portanto apenas a quantidade de informações acrescentadas a um documento assinado para atestar sua validade, sem considerar a assinatura propriamente dita nem o documento.

Para a ICP X.509, consideram-se os seguintes dados:

- 1 carimbo de tempo
- n certificados de ACs acima do certificado do signatário (constante)
- m certificados de ACs acima do carimbo de tempo (constante)
- $n - 1$ LCRs pequenas + 1 LCR grande (é necessário diferenciar as LCRs de ACs, que costumam possuir apenas poucos certificados, das LCRs de ACs finais, que costumam acumular um grande volume de informações)

Para a NBPKI, consideram-se os seguintes dados:

- 1 token

- 1 certificado de AN

Seguem alguns valores de referência para o tamanho das informações contidas em uma assinatura digital. Os valores foram estimados através da obtenção de dados de certificados da ICP-Brasil. Destaca-se o tamanho de uma LCR de ac final, para as quais foram encontrados casos onde a mesma possuia tamanho na ordem de 100Kb ou superiores. Optou-se por considerar um valor moderado. Um *token* conforme a codificação proposta neste trabalho NBPKI também foi codificado em DER para obtenção de uma estimativa de tamanho.

- Certificado X.509: 1,1kB
- Carimbo de Tempo: 1kB
- LCR vazia: 0,5kb
- LCR AC Final: 50kb
- Token: 1kB

Portanto:

- X.509: $1 + 1,1(n + m) + 0,5(n - 1) + 50$
- NBPKI: $1 + 1, 1$

Desta forma, considerando-se $n = m = 3$, obtém-se os seguintes dados:

- X.509: $1 + 1, 1(6) + 1 + 50 = 58, 6$
- NBPKI: $2, 1$

Modelo	**Kb**
X.509	58,6
NBPKI	2,1

Tabela 6.3: Comparação entre modelos: Tamanho de arquivo assinado

6.2.2 Complexidade computacional para assinatura com carimbo de tempo

6.2.2.1 Para o signatário

A Tabela 6.4 analisa o número de operações necessárias para o signatário para a realização de uma assinatura digital em cada um dos

Modelo	Consultas Online	Assinaturas
X.509	2	1
NBPKI	1	1

Tabela 6.4: Comparação entre modelos: Complexidade computacional para asinatura

modelos de ICP, sem considerar conservação em longo prazo. Será considerado que o signatário obtém e envia junto com a assinatura todos dados relevantes que podem ser adicionados junto a assinatura no momento que a mesma é realizada, como LCRs, carimbos de tempo e provas.

Para a ICP X.509, consideram-se as seguintes operações:

- Assinatura: 1 assinatura
- Consulta a LCR atual: 1 consulta
- Carimbo de tempo: 1 consulta

Para a NBPKI, consideram-se as seguintes operações:

- Assinatura: 1 assinatura
- Obtenção de prova: 1 consulta

6.2.2.2 Para as autoridades envolvidas

A Tabela 6.5 analisa o número de operações necessárias nas autoridades envolvidas (Notarial, Carimbo de Tempo, Certificadora) para a realização de uma assinatura digital em cada um dos modelos de ICP, sem considerar conservação em longo prazo.

Modelo	Consultas Online	Assinaturas
X.509	0	1
NBPKI	0	1

Tabela 6.5: Comparação entre modelos: Complexidade computacional para asinatura - Autoridades

Para a ICP X.509, consideram-se as seguintes operações:

- Autoridade Certificadora: não participa
- Emissão de Carimbo de tempo: 1 assinatura

Para a NBPKI, consideram-se as seguintes operações:

- Emissão de Token: 1 assinatura

6.2.3 Complexidade computacional para verificação

A Tabela 6.6 analisa o número de operações necessárias para a verificação de uma assinatura digital em cada um dos modelos de ICP, sem considerar conservação em longo prazo, considerando que os dados de revogação foram já obtidos e anexados à assinatura pelo signatário quando isto é possível

Modelo	Consulta Online	Verificação de Assinatura
X.509	m	$2n + 2m + 2$
NBPKI	1	4

Tabela 6.6: Comparação entre modelos: Complexidade computacional para verificação

Para a ICP X.509, consideram-se as seguintes operações:

- Autoridade Certificadora: não participa
- Carimbo de tempo: 1 verificação
- Assinatura do Documento: 1 verificação
- Verificação de Cadeia de Certificação (n = quantidade de ACs acima do certificado do signatário): n verificações
- Verificação de LCRs: n verificações
- Verificação de Cadeia de Certificação do Carimbo de Tempo (m = quantidade de ACs acima do certificado da ACT): m verificações
- Verificação de LCRs da Cadeia de Certificação do Carimbo de Tempo (m = quantidade de ACs acima do certificado da ACT): m verificações, m consultas de LCRs atualizadas

Para a NBPKI, consideram-se as seguintes operações:

- Assinatura do Documento: 1 verificação
- Verificação de Token: 1 verificação
- Verificação de Certificado AN: 1 verificação
- Verificação de Lista de ANs válidas: 1 verificação

6.3 CUSTO DE MANUTENÇÃO DE ASSINATURA POR LONGO PRAZO

As próximas seções, alguns dados são reanalizados agora sob a perspectiva da necessidade de conservação em longo prazo dos documentos assinados. Em ICPs x.509, a grosso modo, isso implica na adiçã de novos carimbos de tempo sobre a assinatura. No caso da NBPKI, a reemissão de provas.

6.3.1 Complexidade computacional para adição de carimbo de tempo

6.3.1.1 Para o usuário

Modelo	Consultas Online	Assinaturas	Verificações de Assinatura
X.509	1	0	0
NBPKI	1	0	0

Tabela 6.7: Comparação entre modelos: Complexidade computacional para manutenção a longo prazo - Usuário

Para a ICP X.509, consideram-se as seguintes operações:

- Novo Carimbo de tempo - Usuário: 1 consulta

Para a NBPKI, consideram-se as seguintes operações:

- Reemissão de Token - Usuário: 1 consulta

6.3.1.2 Para as Autoridades Envolvidas

Modelo	Consultas Online	Assinaturas	Verificações de Assinatura
X.509	0	1	0
NBPKI	2	1	4

Tabela 6.8: Comparação entre modelos: Complexidade computacional para manutenção a longo prazo - Autoridades

Para a ICP X.509, consideram-se as seguintes operações:

- Novo Carimbo de tempo - ACT: 1 assinatura

Para a NBPKI, consideram-se as seguintes operações:

- Reemissão de Token - AN: 1 verificação de token (1 consulta, 3 verificações) e 1 emissão de token (1 consulta e 1 assinatura)

Nota-se um incremento substancial nas operações que precisam ser realizadas pela Autoridade Notarial, já que esta precisa validar o token antes de emitir um novo. Estão desconsiderados aqui os casos onde a AN foi comprometida e portanto a verificação deve seguir procedimento envolvendo consulta a uma AN que disponha das informações dos *tokens* emitidos.

6.3.1.3 Tamanho da assinatura

O tamanho dos documentos assinados, bem como das assinaturas digitais propriamente ditas, são identicos para ambos os casos. O tamanho de um arquivo com a assinatura digital, no entanto, deverá contemplar todos os dados necessários para a validação de um documento. Serão considerados na análise abaixo portanto apenas a quantidade de informações acrescentadas a um documento assinado para atestar sua validade, sem considerar a assinatura propriamente dita nem o documento.

Para a ICP X.509, consideram-se os seguintes dados:

- t carimbos de tempo (acrescentados antes da revogação dos anteriores)
- n certificados de ACs acima do certificado do signatário (constante)
- m certificados de ACs acima de cada carimbo de tempo (constante)
- $n - 1$ LCRs pequenas + 1 LCR grande (é necessário diferenciar as LCRs de ACs, que costumam possuir apenas poucos certificados, das LCRs de ACs finais, que costumam acumular um grande volume de informações)

Para a NBPKI, consideram-se os seguintes dados:

- 1 token
- 1 certificado de AN

Portanto, considerando os mesmos valores de referência da seção 6.2.1:

- X.509: $t + 1,1(n + t * m) + 0,5(n - 1) + 50$
- NBPKI: $1 + 1,1$

Desta forma, considerando-se $n = m = 3$, obtém-se os seguintes dados:

- X.509: $t + 1,1(3 + 3t) + 1 + 50 = 54,3 + 4,3t$

Modelo	Kb
X.509	54,3+ 4,3t
NBPKI	2,1

Tabela 6.9: Comparação entre modelos: Tamanho de arquivo assinado - Longo Prazo

- NBPKI: $2,1$

A assinatura digital comum, além de necessitar de mais informações a curto prazo, ainda apresenta crescimento significativo a longo prazo, com a adição de novos carimbos de tempo.

7 ANÁLISE DOS RESULTADOS

O modelo proposto apresenta aplicação em duas principais formas: autenticação e prova de uso para assinatura.

Com o *token* de autenticação, o usuário pode usar o mesmo *token* várias vezes para se autenticar em um sistema, e o servidor não precisa com isso obter novas informações de revogação com tanta frequência. O usuário é quem envia a prova de validade ao servidor, distribuíndo assim a carga de validação que estava exclusivamente sobre o servidor de autenticação entre os usuários interessados em autenticar-se.

Como o *token* de autenticação é pequeno, o servidor pode armazenar esses *tokens* (*cache*) durante o período que considerar relevante. Não é mais a Autoridade que define o tempo que é razoável para uma autenticação ser considerada válida, mas sim a aplicação na qual está sendo autenticado o usuário. Se desejado um, novo token pode ser solicitado a cada nova autenticação. A validação do token depente apenas da confiança na AN, e não em uma série de informações da cadeia de certificação e situação dos certificados a serem obtidas.

Com o *token* de prova de uso do certificado em uma assinatura, não é necessária a validação de um carimbo do tempo, e a avaliação do certificado do signatário é bastante simplificada. Em especial para a conservação a longo prazo, a proposta apresenta vantagens significativas na simplicidade da validação da assinatura e *token*, cuja confiabilidade depende apenas da verificação de novos resumos criptográficos.

A maior limitação da proposta é a mesma de uma Autoridade de Carimbo do Tempo (ADAMS et al., 2001), que é a de que se uma chave de ACT for comprometida, todos os carimbos do tempo deixam de ser válidos. De igual modo, se uma AN é comprometida, todos *tokens* por ela emitidos deixam de ser confiáveis. Por esta razão, é extremamente importante que as chaves privadas da AN sejam protegidas com segurança apropriada. No caso da violação da chave, a única forma de distinguir entre *tokens* válidos e inválidos seria com a auditoria da AN. Entretanto, cabe destacar que a manutenção dos *tokens*, através da substituição destes por novos emitidos por novas ANs, também é bastante simplificado, facilitando a manutenção da verificabilidade da assinatura digital.

Outra solução para minimizar esta limitação é acrescentar mais de um *token* a uma mesma assinatura. Caso uma AN seja comprometida, dificilmente a outra também terá sido, e a validação pode ser ainda realizada. Mais do que isso, o *token* ainda válido pode ser submetido à outra AN para obtenção de um novo *token* para substituir o comprometido.

O Capítulo 6 apresenta dados concretos do impacto de uso do novo modelo ao invés do X.509. Os dados permitem observar uma diminuição drástica na quantidade de dados que são acrescentados a uma assinatura digital. Isso se deve principalmente ao fato de as Listas de Certificados

Revogados apresentarem um tamanho elevado, as vezes até mesmo superando o tamanho do próprio documento assinado. Mas também devido à necessidade de incluir novos carimbos de tempo sobre os anteriores, o que faz com que a assinatura digital continue crescendo.

Do ponto de vista de complexidade, também nota-se uma relevante diminuição, em especial na validação de uma assinatura digital. Uma assinatura comum possui uma quantidade muito grande de dados a serem verificados, o que inclui grande quantidade de operações assimétricas e hashes. O método proposto diminui significativamente esta quantidade de operações.

8 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Este trabalho propôs um novo modelo de Infraestruturas de Chaves Públicas que possibilita reduzir a dificuldade de validação de uma assinatura digital. Neste novo modelo sugerimos que o certificado do usuário deve ser autoassinado, e a Autoridade Certificadora seja substituída por uma Autoridade Notarial. Esta última é responsável pela emissão de *tokens* que servem como prova de validade do certificado do usuário, e também do uso deste para assinaturas digitais. Com este *token* não é mais necessário montar e validar o caminho de certificação do usuário nem utilizar uma Autoridade de Carimbo do Tempo para produzir uma assinatura de longo prazo.

O novo modelo traz uma série de vantagens com relação aos modelos de certificação anteriores, ao eliminar a cadeia de certificação do usuário e assumir como parte do modelo a obtenção de provas de validade do certificado. Conforme proposto, o modelo também apresenta características importantes, como facilitar a conservação de longo prazo de documentos, inclusive no que diz respeito a atualização de algoritmos criptográficos. A abordagem definida no trabalho também reduz a quantidade de código a ser implementado em um verificador de assinaturas digitais, e pode acelerar o desenvolvimento de aplicações baseadas em ICP, em especial para dispositivos com recursos limitados como sensores e telefones móveis.

Ainda existem aspectos a serem desenvolvidos em trabalhos futuros, como por exemplo análise de outras perspectivas de modelo de negócio que poderiam ser implantadas quando da aplicação do modelo em larga escala. Uma série de fatores econômicos e jurídicos podem ser levados em consideração para isto.

Esse modelo proposto é aderente aos padrões e métodos dos modelos de negócio atuais, utilizando serviços online para validação e autenticação (FREEMAN et al., 2007; GUTMANN, 2002).

REFERÊNCIAS

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). Disponível em: <http://www.ietf.org-/rfc/rfc3161.txt>.

AL-RIYAMI, S.; PATERSON, K. Certificateless Public Key Cryptography. *Advances in Cryptology-ASIACRYPT 2003*, p. 1–40, 2003.

BOYEN, X.; MARTIN, L. *Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems*. IETF, dez. 2007. RFC 5091 (Informational). (Request for Comments, 5091). Disponível em: <http://www.ietf.org/rfc/rfc5091-.txt>.

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

BURR, W. E. *NIST COMMENTS ON CRYPTANALYTIC ATTACKS ON SHA-1*. 2006. Disponível em: <http://csrc.nist.gov/groups/ST/hash-/statement.html>.

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

COOPER, D. A. A Model of Certificate Revocation. In: *ACSAC '99: Proceedings of the 15th Annual Computer Security Applications Conference*. Washington, DC, USA: IEEE Computer Society, 1999. p. 256. ISBN 0-7695-0346-2.

CUSTóDIO, R. et al. *Optimized Certificates – A New Proposal for Efficient Electronic Document Signature Validation*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008. 49–59 p. (Lecture Notes in Computer Science, v. 5057). ISBN 978-3-540-69484-7.

DAUM, M.; LUCKS, S. *Hash Collisions - The Poisoned Message Attack*. 2005. Acesso em: Junho 2008. Disponível em: <http://th.informatik.uni-mannheim.de/People/lucks/HashCollisions/>.

DIERKS, T.; RESCORLA, E. *The Transport Layer Security (TLS) Protocol Version 1.2*. IETF, ago. 2008. RFC 5246 (Proposed Standard). (Request for Comments, 5246). Updated by RFC 5746. Disponível em: <http://www.ietf.org/rfc/rfc5246.txt>.

DIFFIE, W.; HELLMAN, M. E. New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT-22, p. 644–654, 1976.

EASTLAKE, D. E.; REAGLE, J. M.; SOLO, D. *XML-Signature Syntax and Processing*. 2002.

ELLISON, C. et al. *SPKI Certificate Theory*. IETF, set. 1999. RFC 2693 (Experimental). (Request for Comments, 2693). Disponível em: <http://www.ietf.org/rfc/rfc2693.txt>.

ESI. *Electronic Signatures and Infrastructures (ESI); CMS Advanced electronic Signatures (CAdES)*. [S.l.], oct 2008.

ESI. *Electronic Signatures and Infrastructures (ESI); Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES)*. [S.l.], nov 2008.

ETSI. *Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information*. [S.l.], 2006. v. 1, 1–87 p.

ETSI. *XML Advanced Electronic Signatures (XAdES)*. [S.l.: s.n.], 2006.

ETSI. *CMS Advanced Electronic Signatures (CAdES)*. [S.l.: s.n.], 2008.

FREEMAN, T. et al. *Server-Based Certificate Validation Protocol (SCVP)*. IETF, dez. 2007. RFC 5055 (Proposed Standard). (Request for Comments, 5055). Disponível em: <http://www.ietf.org/rfc/rfc5055-.txt>.

GENTRY, C. Certificate-based encryption and the certificate revocation problem. In: *22nd Annual International Conference on the Theory and Applications of Cryptographic Techniques*. [S.l.: s.n.], 2003.

GOYAL, V. Fast digital certificate revocation. In: *SEC*. [S.l.: s.n.], 2004. p. 489–500.

GUTMANN, P. PKI: It's Not Dead, Just Resting. *Computer*, IEEE Computer Society Press, Los Alamitos, CA, USA, v. 35, n. 8, p. 41–49, 2002. ISSN 0018-9162.

HOUSLEY, R. *Cryptographic Message Syntax (CMS)*. IETF, set. 2009. RFC 5652 (Draft Standard). (Request for Comments, 5652). Disponível em: <http://www.ietf.org/rfc/rfc5652.txt>.

HUNTER, B. Simplifying PKI usage through a client-server architecture and dynamic propagation of certificate paths and repository addresses. In: *Database and Expert Systems Applications, 2002. Proceedings. 13th International Workshop on*. [S.l.: s.n.], 2002. p. 505–510. ISSN 1529-4188.

ITI. *Glossário ICP-Brasil*. v.1.2. Brasília, Outubro 2007.

KANG, B.; PARK, J. A certificate-based signature scheme. In: *Topics in Cryptology–CT-RSA 2004*. [s.n.], 2004. p. 1–18. Disponível em: <http://www.springerlink.com/index/2l5fuh7hjce8mj80.pdf>.

KOCHER, P. C. On Certificate Revocation and Validation. In: *FC '98: Proceedings of the Second International Conference on Financial Cryptography*. London, UK: Springer-Verlag, 1998. p. 172–177. ISBN 3-540-64951-4.

KOHNFELDER, L. M. Towards a practical public-key cryptosystem. In: . [S.l.: s.n.], 1978.

LAIH, C.-S.; YEN, S.-M. Improved Digital Signature Suitable for Batch Verification. *IEEE Transactions on Computers*, IEEE Computer Society, Los Alamitos, CA, USA, v. 44, p. 957–959, 1995. ISSN 0018-9340.

LEVI, A.; CAGLAYAN, M. U.; KOC, C. K. Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure. *ACM Transactions on Information and System Security (TISSEC)*, v. 7, n. 1, p. 21, 2004. ISSN 1094-9224.

LIM, T.-L.; LAKSHMINARAYANAN, A.; SAKSEN, V. A practical and efficient tree-list structure for public-key certificate validation. In: *ACNS'08: Proceedings of the 6th international conference on Applied cryptography and network security*. Berlin, Heidelberg: Springer-Verlag, 2008. p. 392–410. ISBN 3-540-68913-3, 978-3-540-68913-3.

LINN, J. An Examination of Asserted PKI Issues and Proposed Alternatives. *Proceedings of the 3rd Annual PKI R&D Workshop*, Proceedings of the 3rd Annual PKI R&D Workshop, 2004.

MA, D. Practical forward secure sequential aggregate signatures. *ASIAN ACM Symposium on Information, Computer and Communications Security*, p. 11, 2008.

MA, D.; TSUDIK, G. A new approach to secure logging. *ACM Transactions on Storage (TOS)*, v. 5, n. 1, 2009. ISSN 1553-3077.

MICALI, S. Enhanced certificate revocation system. *Massachusetts Institute of Technology, Cambridge, MA*, Citeseer, p. 1–10, 1995.

MICALI, S. NOVOMODO: Scalable Certificate Validation and Simplified PKI Management. In: *Proceedings of the 1st Annual PKI Research Workshop*. NIST, Gaithersburg MD, USA: [s.n.], 2002.

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

NIST. *Federal Register Vol. 72*. [S.l.], 2007. v. 72, n. 212, 62212–62220 p.

PINKAS, D.; POPE, N.; ROSS, J. *Policy Requirements for Time-Stamping Authorities (TSAs)*. IETF, nov. 2003. RFC 3628 (Informational). (Request for Comments, 3628). Disponível em: <http://www.ietf.org/rfc/rfc3628.txt>.

PINKAS, D.; POPE, N.; ROSS, J. *RFC5126 - CMS Advanced Electronic Signatures (CAdES)*. 2008.

RESCORLA, E. et al. *Transport Layer Security (TLS) Renegotiation Indication Extension*. IETF, fev. 2010. RFC 5746 (Proposed Standard). (Request for Comments, 5746). Disponível em: <http://www.ietf.org-/rfc/rfc5746.txt>.

RIVEST, R. L. Can We Eliminate Certificate Revocations Lists? In: *FC '98: Proceedings of the Second International Conference on Financial Cryptography*. London, UK: Springer-Verlag, 1998. p. 178–183. ISBN 3-540-64951-4.

RIVEST, R. L.; LAMPSON, B. *SDSI - A Simple Distributed Security Infrastructure*. 1996.

SATIZáBAL, C. et al. Reducing the Computational Cost of Certification Path Validation in Mobile Payment. In: *EuroPKI '07: Proceedings of the 4th European PKI workshop: Theory and Practice on Public Key Infrastructure*. Berlin, Heidelberg: Springer-Verlag, 2007. p. 280–296. ISBN 978-3-540-73407-9.

SCHNEIER, B.; KELSEY, J. Secure audit logs to support computer forensics. *ACM Transactions on Information and System Security (TISSEC)*, v. 2, n. 2, 1999. ISSN 1094-9224.

SHAMIR, A. Identity-based Cryptosystems and Signature Schemes. In: *Advances in Cryptology-Crypto'84*. [S.l.: s.n.], 1984. p. 47–53.

STATE, N. C. O. C. O. U. *Uniform Electronic Transactions Act (UETA)*. 1999. Disponível em: <http://www.law.upenn.edu/bll/ulc/uecicta/uetast84.htm>.

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

STRAUB, T. *Usability Challenges of PKI*. Tese (Doutorado) — Technischen Universität Darmstadt, 2006.

WANG, X.; YIN, Y. L.; YU, H. Finding Collisions in the Full SHA-1. v. 3621, p. 17–??, 2005. ISSN 0302-9743.

WANG, X.; YU, H.; YIN, Y. L. Efficient Collision Search Attacks on SHA-0. *Lecture Notes on Computer Sciences*, v. 3621, p. 1–??, 2005. ISSN 0302-9743.

WU, W. et al. Certificate-based Signatures Revisited. *Journal of Universal Computer Science*, v. 15, n. 8, p. 1659–1684, 2009.

ZIMMERMANN, P. R. *The official PGP user's guide*. [S.l.: s.n.], 1995. 127 p.