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

Nelson da Silva

PRESERVAÇÃO POR LONGO PRAZO DE ASSINATURAS DIGITAIS

Florianópolis
2011

Nelson da Silva

PRESERVAÇÃO POR LONGO PRAZO DE ASSINATURAS DIGITAIS

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.

Ricardo Felipe Custódio, Dr.
Orientador

Florianópolis
2011

Catalogação na fonte pela Biblioteca Universitária
da
Universidade Federal de Santa Catarina

S586p Silva, Nelson da
Preservação por longo prazo de assinaturas digitais [dissertação] / Nelson da Silva ; orientador, Ricardo Felipe Custódio. - Florianópolis, SC, 2011.
99 p.: il., grafs., tabs.

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

Inclui referências

1. Ciência da computação. 2. Assinaturas digitais. 3. Infraestrutura de Chaves Públicas. 4. Documentos eletrônicos. 5. Sistemas de segurança. 6. Arquivos e arquivamento – (Documentos). I. Custodio, Ricardo Felipe. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Computação. III. Título.

CDU 681

Nelson da Silva

PRESERVAÇÃO POR LONGO PRAZO DE ASSINATURAS DIGITAIS

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, 1 de Março de 2011

Mário Antonio Ribeiro Dantas, Dr.
Coordenador do PPGCC

Banca Examinadora:

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

Lau Cheuk Lung, Dr.
Universidade Federal de Santa Catarina

Ricardo Pereira e Silva, Dr.
Universidade Federal de Santa Catarina

Luciano Paschoal Gaspary, Dr.
Universidade Federal do Rio Grande do Sul

Aos meus pais que nunca pouparam esforços para dar aos seus filhos condições melhores do que tiveram.

AGRADECIMENTOS

Meus sinceros agradecimentos a todos aqueles que, de alguma forma, colaboraram com este trabalho. Primeiramente, aos meus pais Nelson F. da Silva Filho e Tânia Regina da Silva a quem atribuo tudo aquilo que sou hoje. Esses nunca pouparam esforços para dar aos seus filhos condições melhores do que tiveram, tendo sempre a felicidade desses como prioridade.

À minha namorada Roberta, que esteve ao meu lado nos momentos bons e ruins, torcendo e me incentivando a seguir em frente. Agradeço, em especial, por seu carinho, compreensão e por tornar tão valorosos os raros momentos que tínhamos juntos. Sem sua companhia o mestrado perderia muito de seu significado.

Ao meu orientador Ricardo Felipe Custódio, a quem tenho grande respeito e admiração. Suas contribuições foram muito além daquelas que cabem a um orientador, sendo seus conselhos muitas vezes conselhos de um amigo. Agradeço por seus ensinamentos, confiança e pelas inúmeras oportunidades que me foram dadas.

Aos meus amigos Thiago Acordi Ramos e Fabiano Castro Pereira sem os quais teria sido inviável conciliar minhas atividades no mestrado, Laboratório de Segurança em Computação (LabSEC) e no Serviço Federal de Processamento de Dados (SERPRO). Ainda ao Thiago agradeço pela honra de termos compartilhado tantos desafios.

Aos outros membros do LabSEC com quem pude trabalhar e discutir ideias. Particularmente, aos doutores Ricardo Moraes, Ricardo Pereira e Silva e Roberto Samarone dos Santos Araújo, aos mestrandos Cristian Thiago Moecke, Jeandré Monteiro Sutil, Jonathan Gehard Kohler, Martin Augusto Gagliotti Vigil e Rogerio Bodemüller Junior, além dos alunos de graduação Deise Luise Wrasse, Lucas Ferraro, Lucas Silveira e Maurício Simões de Oliveira. Agradeço ainda à Lucila Alosilla pela atenção com que sempre me tratou.

Por fim, agradeço à Câmara Brasileira de Comércio Eletrônico (Camara-e.net) que há muito acompanha e patrocina atividades que culminaram neste trabalho. Agradeço, igualmente, aos parceiros do LabSEC com quem tive a oportunidade de trabalhar durante o mestrado, dentre eles o Instituto Nacional de Tecnologia da Informação (ITI), Colégio Notarial do Brasil (CNB), Rede Nacional de Ensino e Pesquisa (RNP), SERPRO, Softplan e BRy.

“Quer você pense que pode ou não fazer algo, você está certo”.
Henry Ford

RESUMO

Assim como ocorre com as assinaturas manuscritas, muitas assinaturas digitais precisam comprovar a autenticidade do documento assinado por anos, décadas ou mesmo por um período indefinido. Assinaturas digitais, contudo, acabam perdendo sua validade por fatores como o enfraquecimento de algoritmos criptográficos ou o comprometimento da chave privada do signatário. Assim, são necessárias estratégias que permitam preservar essas assinaturas por longo prazo. Este trabalho estuda a influência do tempo sobre as assinaturas digitais e propõe alternativas para minimizar alguns dos principais problemas hoje relacionados a essa preservação. Inicialmente, são apresentados os fatores que comprometem a validade das assinaturas com o tempo, seguido das principais estratégias até então propostas para sua preservação. A principal delas, baseada em carimbos do tempo, é então analisada, sendo propostos protocolos criptográficos para aumentar sua confiabilidade e reduzir os custos de preservação para o usuário final. Tais protocolos deram origem a duas novas implementações de carimbos, os Carimbos do Tempo Renováveis e Carimbos do Tempo Autenticados. Finalmente, foram realizadas análises teóricas dos benefícios e limitações trazidos por eles, sendo os resultados confirmados por meio de testes e simulações. Dentre os carimbos, os Carimbos do Tempo Autenticados são aqueles que oferecem uma maior redução de custos. Os de armazenamento, por exemplo, chegam a ser 99% menores, considerando a preservação de uma assinatura por cinquenta anos numa Infraestrutura de Chaves Públicas típica. Além disso, se destacam ao permitirem a validação *offline* das assinaturas preservadas. Carimbos do Tempo Renováveis, por outro lado, mantêm maior compatibilidade com a base instalada, sendo possível validar suas assinaturas da maneira convencional. Em contrapartida aos benefícios trazidos por esses protocolos, existem principalmente custos a serem absorvidos pelas Autoridades de Carimbo do Tempo e Autoridades Certificadoras Raiz.

Palavras-chave: assinatura digital, infraestrutura de chaves públicas, X.509, carimbo do tempo, arquivamento.

ABSTRACT

As with handwritten signatures, many digital signatures need to prove the authenticity of signed documents by years, decades or even for an indefinite period. Digital signatures, however, lose their validity by factors such as the weakening of cryptographic algorithms or the signer's private key compromising. Thus, strategies are needed to preserve these signatures for long term. This work studies the influence of time on digital signatures and propose alternatives to minimize some of the major problems currently related to this preservation. Initially, we present the factors that compromise the validity of signatures with time, followed by the main strategies proposed so far for its preservation. The main one, based on timestamps, is then analyzed and cryptographic protocols to increase its reliability and reduce preservation costs for the end user are proposed. Such protocols have resulted in two new implementations of stamps, Renewable Timestamps and Authenticated Timestamps. Finally, we carried out theoretical analysis of the benefits and limitations brought by them, with results confirmed by tests and simulations. Among the stamps, Authenticated Timestamps are those that offer greater cost savings. The storage ones, for example, are up to 99% lower, considering the preservation of a signature for fifty years in a typical Public Key Infrastructure. They also stand by enabling offline validation of preserved signatures. Renewable Timestamps, on the other hand, remain more compatible with the installed base, being able to validate their signatures in the conventional manner. In contrast to the benefits brought by these protocols, there are mainly costs to be absorbed by Time Stamping Authorities and Root Certification Authorities.

Keywords: digital signature, public key infrastructure, X.509, timestamp, archiving

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AC	Autoridade Certificadora
ACT	Autoridade de Carimbo do Tempo
ASN.1	*Abstract Syntax Notation One*
CAdES	*CMS Advanced Electronic Signatures*
CMS	*Cryptographic Message Syntax*
DER	*Distinguished Encoding Rules*
DN	*Distinguished Name*
ERS	*Evidence Record Syntax*
ETSI	*European Telecommunications Standards Institute*
ICP	Infraestrutura de Chaves Públicas
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IETF	*Internet Engineering Task Force*
LabSEC	Laboratório de Segurança em Computação
LCR	Lista de Certificados Revogados
NIST	*National Institute of Standards and Technology*
PAdES	*PDF Advanced Electronic Signatures*
PBAD	Padrão Brasileiro de Assinatura Digital
PDF	*Portable Document Format*
PKCS#7	*Public Key Cryptography Standards #7*
XAdES	*XML Advanced Digital Signatures*
XML	*Extensible Markup Language*
XMLDSig	*XML Digital Signature*

SUMÁRIO

1 INTRODUÇÃO

Recentemente vem sendo observado um uso cada vez maior pela sociedade dos meios eletrônicos para a realização de suas atividades diárias. Nesse cenário, o papel vem dando lugar a uma forma alternativa para o registro de informações, os documentos eletrônicos. Tais documentos acabam oferecendo uma série de vantagens e passaram a servir de base para muitas das relações entre os cidadãos, empresas e governos. Seu uso vem, particularmente, diminuindo custos e dando maior celeridade aos negócios e as instituições governamentais.

Assim como ocorre com o papel, em muitas dessa relações existe a necessidade de se comprovar a autenticidade do documento eletrônico, verificando sua origem e integridade. Tal propriedade é essencial, por exemplo, para a confiança nas transações eletrônicas, onde a comercialização de bens, produtos e serviços depende dessa segurança. Para o papel, são muitos os mecanismos até então desenvolvidos para permitir essa comprovação. Assinaturas, marcas d'agua e carimbos são exemplos desses mecanismos. No caso dos documentos eletrônicos, tal função é exercida, principalmente, pelas assinaturas digitais.

Frente a isso muitos países vêm promovendo o uso dessas assinaturas como forma de facilitar o emprego de documentos eletrônicos como meio de prova. Alguns desses, inclusive, já atribuem às assinaturas digitais o mesmo valor legal das assinaturas manuscritas. Na União Européia, por exemplo, tal assunto é tratado pela Diretiva Européia 1999/93/EC(PARLIAMENT; COUNCIL, 2000). No Brasil, pela Medida Provisória 2.200-2, de 24 de agosto de 2001(BRASIL, 2001).

Assim como ocorre com as assinaturas manuscritas, muitas assinaturas digitais precisam comprovar a autenticidade do documento assinado por anos, décadas ou mesmo por um período indefinido. Tal proteção é necessária, por exemplo, para suportar eventuais litígios que porventura venham a ocorrer(BLANCHETTE, 2004). Assinaturas digitais, contudo, acabam perdendo sua validade por fatores como o enfraquecimento de algoritmos criptográficos ou o comprometimento da chave privada do signatário. Problema esse que vem sendo evidenciado com a popularização dessas assinaturas.

Nesse sentido, a preservação de assinaturas digitais tem sido abordada em várias recomendações técnicas. Dentre as principais, estão as recomendações *CMS Advanced Electronic Signature* (CAdES)(ETSI, 2009a), *XML Advanced Electronic Signature* (XAdES)(ETSI, 2009a), *PDF Advanced Electronic Signature* (PAdES)(ETSI, 2009b) e *Evidence Record Syntax (ERS)*(GONDROM; BRANDNER; PORDESCH, 2007). No Brasil, tal problema vem sendo tratado, principalmente, por meio do Padrão Brasileiro de Assinatura Digital (PBAD)(ITI, 2010).

Todas essas recomendações, contudo, fazem uso de uma mesma es-

tratégia de preservação, a sobreposição de carimbos do tempo. Apesar de ser uma das mais estudadas na literatura, mesmo ela é incapaz de garantir que uma assinatura seja preservada pelo tempo necessário. São vários os fatores que podem levar o processo de preservação a falhar(ETSI, 2009a; ETSI, 2009c; ETSI, 2009b; GONDROM; BRANDNER; PORDESCH, 2007). Além disso, seus custos tendem a ser inadequados quando são consideradas plataformas com poucos recursos computacionais ou a preservação de grandes volumes de documentos assinados(BLAZIC; SETCCE, 2007; GONDROM; BRANDNER; PORDESCH, 2007; VIGIL et al., 2009).

Assim, apesar de a sociedade há muito lidar com a preservação de assinaturas manuscritas, o conhecimento em relação à preservação das assinaturas digitais é algo muito mais limitado. O presente trabalho estuda tal problema e propõe alternativas para minimizar alguns dos principais obstáculos hoje relacionados à preservação de assinaturas digitais.

1.1 OBJETIVOS

Esta dissertação de mestrado tem por objetivo estudar a influência do tempo sobre a validade das assinaturas digitais, bem como propor alternativas que permitam reduzir os riscos e custos hoje associados a sua preservação.

1.1.1 Objetivos Específicos

Tem-se como objetivos específicos:

- Apresentar os fatores que, com o tempo, comprometem a validade das assinaturas digitais;
- Apresentar as principais estratégias até então propostas para a preservação dessas assinaturas;
- Discutir, em maiores detalhes, os problemas relacionados à preservação de assinaturas por meio de carimbos do tempo;
- Propor protocolos criptográficos que permitam aumentar a confiabilidade e reduzir os custos associados à preservação de assinaturas por meio de carimbos do tempo;
- Discutir os benefícios e limitações trazidos pelos protocolos propostos, confirmando os resultados teóricos por meio de testes e simulações;
- Discutir o grau de compatibilidade desses protocolos com a base instalada.

1.2 TRABALHOS RELACIONADOS

A preservação de assinaturas digitais é um tema quase tão antigo quanto a própria criptografia assimétrica. Já no final da década de 70, Popek e Kline (1979) sugeriam que a validade de uma assinatura fosse preservada por meio de "carimbos do tempo", emitidos por terceiras partes confiáveis, onde constaria o momento em que a assinatura fora produzida. A ideia era que assinaturas autênticas seriam aquelas realizadas antes de se tornar viável a sua falsificação.

Outros trabalhos, contudo, propuseram a autenticação de outros fatos sobre uma assinatura, que não o momento em que fora criada, como forma de preservá-la. Massias e Quisquater (1997), por exemplo, sugeriram que tal fato compreendesse a sua própria validade. Desse modo, teria-se uma forma alternativa para se validar uma assinatura, quando essa já não fosse mais válida pelos meios convencionais.

Ambas as formas de notarização, como essas estratégias ficaram conhecidas por remeter aos atos praticados pelos notários no mundo real (JUST, 1998), têm sido tema de diversos outros trabalhos. Haber e Stornetta (1991), por exemplo, propuseram o encadeamento de carimbos do tempo, como forma de reduzir a confiança necessária nessas entidades responsáveis pela emissão de carimbos. Blibech e Gabillon (2006), por sua vez, reduziram os custos necessários à validação desses carimbos, redefinindo a forma como são encadeados.

Para a autenticação da validade de assinaturas, Ansper et al. (2001) sugeriram a agregação dessas assinaturas por meio de Árvores de Merkle(MERKLE, 1980), de modo a reduzir o esforço computacional necessário para o ateste. Por outro lado, Custodio et al. (2008), propuseram a associação do método de NOVOMODO (MICALI, 2002) a esses atestes, como forma de minimizar os recursos computacionais necessários à sua validação.

Paralelamente a essas propostas, uma outra abordagem vem sendo usada para a preservação de assinaturas, focada nas primitivas criptográficas envolvidas em sua geração e validação. São esquemas de assinatura com propriedades especiais, que as tornam menos vulneráveis ao efeito do tempo. Um exemplo desses esquemas são os esquemas de chave evolutiva onde assinaturas produzidas são protegidas de futuros comprometimentos da chave privada do signatário, pela evolução dessa chave (ANDERSON, 1997; BELLARE; MINER, 1999; DODIS et al., 2002; DODIS et al., 2003). A ideia dessas propostas é que se a chave comprometida não é mais a mesma que foi usada em alguma assinatura passada, então tal assinatura preserva sua validade.

Esquemas de assinaturas incondicionalmente seguras, por sua vez, tratam do problema relacionado ao enfraquecimento dos algoritmos criptográficos(CHAUM; ROIJAKKERS, 1991; HANAOKA, 2005). Diferentemente dos esquemas convencionais, tais esquemas não baseiam sua segurança em suposições quanto ao poder computacional do adversário. Po-

der esse que tende a aumentar com o tempo.

Nenhuma dessas propostas, contudo, é capaz de preservar uma assinatura por um período de tempo arbitrariamente grande. Carimbos do tempo, por exemplo, igualmente tornam-se falsificáveis, perdendo assim sua validade (HABER; STORNETTA, 1991; BAYER; HABER; STORNETTA, 1993). O mesmo ocorre com os atestes quanto à validade das assinaturas (LEKKAS; GRITZALIS, 2004; VIGIL et al., 2009). Esquemas especiais de assinatura, por sua vez, tendem a tratar apenas uma parte dos problemas e, dessa forma, tornam-se vulneráveis a todos os outros.

Um dos primeiros trabalhos a tratar da preservação por longo prazo de assinaturas digitais foi então o trabalho de Bayer, Haber e Stornetta (1993). Na proposta, parcialmente apresentada num trabalho anterior (HABER; STORNETTA, 1991), uma assinatura digital seria preservada pela sobreposição de carimbos do tempo. A idea era que novos carimbos seriam adicionados, na medida que os anteriores estivessem por perder sua validade. Cada um dos carimbos, então, demonstraria que o anterior fora produzido antes de tornar-se falsificável.

Desde sua proposta, a estratégia de sobreposição de carimbos do tempo vem sendo explorada por diversos trabalhos (BLAZIC; SETCCE, 2007; TRONCOSO; COCK; PRENEEL, 2008; ZIMMER; LANGKABEL; HENTRICH, 2008; HUHNLEIN et al., 2010), bem como em recomendações técnicas como as do ETSI (ETSI, 2009a; ETSI, 2009c; ETSI, 2009b) e da IETF (GONDROM; BRANDNER; PORDESCH, 2007; PINKAS; POPE; ROSS, 2008). Particularmente em (BLAZIC; SETCCE, 2007; GONDROM; BRANDNER; PORDESCH, 2007) foram apresentadas alternativas para reduzir os riscos e custos dessa estratégia.

Ideia semelhante à sobreposição de carimbos do tempo foi proposta para a autenticação da validade de assinaturas (LEKKAS; GRITZALIS, 2004). Nesse caso, novos atestes seriam realizados quando os anteriores estivessem por se tornar inválidos. Tal estratégia, por sua vez, tem sido explorada em trabalhos como o de VIGIL et al. (2009).

1.3 JUSTIFICATIVA

Graças aos benefícios trazidos pelos documentos eletrônicos, esses vêm substituindo o papel em muitas das relações entre os cidadãos, empresas e governos. Nesse contexto, as assinaturas digitais vêm desempenhando uma importante função por ser uma das principais formas de se comprovar a autenticidade desses documentos. Todavia, por perderem sua validade com o tempo, estratégias de preservação são necessárias para aquelas assinaturas que, como algumas assinaturas manuscritas, precisam se manter válidas por anos, décadas ou mesmo por um período indefinido.

A principal estratégia em uso, contudo, é incapaz de garantir a preservação das assinaturas digitais(ETSI, 2009a; ETSI, 2009c; ETSI, 2009b; GONDROM; BRANDNER; PORDESCH, 2007). Além disso, apresenta custos inapropriados para diversos contextos, particularmente

para plataformas com recursos computacionais escassos ou em cenários onde grandes volumes de documentos assinados precisam ser preservados(BLAZIC; SETCCE, 2007; GONDROM; BRANDNER; PORDESCH, 2007; VIGIL et al., 2009). Dessa forma, tais empecilhos acabam oferecendo um obstáculo para a adoção dos documentos eletrônicos.

Tais obstáculos podem, portanto, ser reduzidos através do aumento na confiabilidade e redução de custos propostos pelo presente trabalho. Por serem voltadas para a principal estratégia de preservação em uso, essas melhorias ainda podem ser implantadas com maior facilidade, pois aproveitam a infraestrutura já existente.

1.4 MOTIVAÇÃO

O presente trabalho se insere na linha de pesquisa do Laboratório de Segurança da Computação (LabSEC), referente à segurança de documentos eletrônicos. Este foi precedido por trabalhos como a tese de doutorado de Dias (2004) e as dissertações de mestrado de Pasqual (2001), Demétrio (2003), Costa (2003) e Notoya (2002).

No primeiro, foram analisados os requisitos de segurança necessários aos documentos eletrônicos para que esses pudessem substituir aqueles em papel. Nos trabalhos de Pasqual (2001), Demétrio (2003) e Costa (2003), por sua vez, foram tratadas questões relacionadas à datação desses documentos, por meio de carimbos do tempo. Finalmente, em (NOTOYA, 2002), foi proposta uma infraestrutura para o armazenamento e recuperação segura de documentos eletrônicos.

As atividades que culminaram no desenvolvimento desta dissertação foram patrocinadas pela Câmara Brasileira de Comércio Eletrônico (Camara-e.net) e tiveram início em 2006, com um Trabalho de Conclusão de Curso (TCC) onde foi desenvolvido um projeto para a modernização e integração dos cartórios do Brasil(SILVA; RAMOS, 2007). Nesse TCC, que posteriormente deu origem a um livro(SILVA et al., 2007), já eram tratadas questões relacionadas à preservação por longo prazo de documentos eletrônicos, incluindo a preservação de suas assinaturas digitais.

Seguindo esses trabalhos, vieram colaborações com o Instituto Nacional de Tecnologia da Informação (ITI), no desenvolvimento e implantação do Padrão Brasileiro de Assinatura Digital (PBAD)(ITI, 2010) e com o Arquivo Nacional na revisão do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ Brasil)(CONARQ, 2009). Particularmente no desenvolvimento do PBAD, foi possível a troca de experiências com diversas empresas, incluindo as multinacionais *Microsoft* e *Adobe*.

Tais atividades acabaram evidenciando diversos problemas relacionados à preservação de assinaturas digitais ainda não tratados de maneira satisfatória. Problemas esses que motivaram a publicação de dois artigos(VIGIL et al., 2009; RAMOS et al., 2010) e o desenvolvimento desta dissertação de mestrado. O primeiro desses artigos aborda a preser-

vação de assinaturas digitais por meio de autenticações de sua validade. O segundo trata da preservação da autenticidade e sigilo de documentos eletrônicos por longo prazo.

1.5 METODOLOGIA

Para se alcançar os objetivos desse trabalho, inicialmente foram estudadas diversas publicações, incluindo artigos, livros, normas e recomendações técnicas, sobre os problemas que limitam o tempo de vida das assinaturas digitais e as estratégias existentes para a preservação dessas assinaturas. Particularmente quanto ao estudo dessas estratégias, foram realizadas buscas exaustivas nas principais bases de dados relacionadas, incluindo *Web of Science*, *Google Scholar*, *ACM*, *IEEE*, *SpringerLinks*, *CiteSeer* e *Scirus*. Nessas buscas, os artigos relacionados às palavras-chave escolhidas eram sistematicamente filtrados, primeiramente através de seu título, seguido pelo resumo, e, finalmente, por seu conteúdo.

As estratégias de preservação existentes foram então analisadas quanto a sua efetividade na preservação de assinaturas digitais por longo prazo. Dentre elas, aquela baseada em carimbos do tempo mostrou-se como a principal estratégia até então proposta, sendo tema da maioria dos artigos e igualmente das recomendações técnicas que atualmente tratam do assunto. Tal estratégia foi então avaliada quanto a sua confiabilidade e custos computacionais. Juntamente, foram avaliadas abordagens até então propostas para tratar desses problemas.

Finalmente foram definidos protocolos criptográficos para aumentar a confiabilidade e reduzir os custos relacionados à preservação de assinaturas digitais por meio de carimbos do tempo. Tais protocolos deram origem a duas novas implementações de carimbos, os Carimbos do Tempo Renováveis e os Carimbos do Tempo Autenticados. Enquanto os primeiros buscam uma maior viabilidade prática, os últimos procuram oferecer uma redução mais acentuada nos custos de preservação.

A preservação por meio dos protocolos propostos foi então avaliada frente à preservação tradicional, incluindo as estratégias até então propostas para aumentar a confiabilidade e reduzir os custos dessa preservação. Para tanto, foram realizadas análises teóricas, cujos resultados foram então confirmados por meio de testes e simulações. Para tais experimentos foram desenvolvidos, além de protótipos, modelos matemáticos representando aspectos da preservação de assinaturas, tanto por meio dos carimbos do tempo tradicionais quanto através dos protocolos criptográficos propostos. Por fim, foram avaliadas a compatibilidade dos Carimbos do Tempo Renováveis e Carimbos do Tempo Autenticados com a base instalada, bem como as limitações trazidas por esses protocolos.

1.6 LIMITAÇÕES DO TRABALHO

O presente trabalho se atém ao estudo da implementação mais comum de assinaturas digitais, sendo aquela baseada em esquemas de assinatura convencionais como o RSA(RIVEST; SHAMIR; ADLEMAN, 1978), e certificados digitais X.509(COOPER et al., 2008). Outras implementações baseiam-se, por exemplo, em esquemas especiais de assinatura, tais como os de chave evolutiva(ANDERSON, 1997; BELLARE; MINER, 1999; DODIS et al., 2002; DODIS et al., 2003), ou outros modelos de Infraestruturas de Chaves Públicas (ICP)(CALLAS et al., 2007; ELLISON, 1999). Ainda quanto a essas assinaturas, são estudadas apenas os problemas que comprometem a sua validade com o tempo.

Dentre as estratégias de preservação de assinaturas até então propostas, este trabalho trata daquela baseada em carimbos do tempo assinados, tais como os carimbos do tempo X.509(ADAMS et al., 2001). Existem, todavia, outras estratégias, menos aceitas, capazes de preservar uma assinatura por longo prazo. Esse é o caso, por exemplo, daquelas baseadas na autenticação da validade das assinaturas(LEKKAS; GRITZALIS, 2004; VIGIL et al., 2009). Ainda quanto à preservação por meio de carimbos do tempo, foram estudados apenas os riscos e custos relacionados a ela.

Por fim, é interessante notar que a preservação por longo prazo de documentos eletrônicos vai além da preservação de suas assinaturas. Devem ser tratadas, igualmente, questões como a obsolescência dos formatos e das mídias de armazenamento desses documentos(LEE et al., 2002).

1.7 ORGANIZAÇÃO DO TRABALHO

O restante desta dissertação de mestrado é organizado em 5 capítulos, sendo eles:

Capítulo 2: revisa alguns conceitos básicos necessários ao entendimento deste trabalho. Particularmente, a forma como assinaturas digitais vêm sendo atualmente implementadas, e o tempo de vida dessas assinaturas;

Capítulo 3: apresenta as principais estratégias até então propostas para a preservação por longo prazo de assinaturas digitais, sendo elas, aquelas baseadas em carimbos do tempo e na autenticação da validade das assinaturas;

Capítulo 4: analisa a estratégia tradicional de preservação, baseada em carimbos do tempo, e propõe protocolos criptográficos para aumentar a confiabilidade e reduzir os custos dessa estratégia;

Capítulo 5: avalia a preservação de assinaturas por meio dos protocolos propostos, frente à preservação tradicional, apresentando, igual-

mente, as limitações trazidas por esses protocolos e sua compatibilidade com a base instalada;

Capítulo 6: conclui a dissertação, revendo os capítulos anteriores e principais resultados alcançados. Por fim, discute suas limitações e trabalhos futuros.

Este trabalho assume conhecimento intermediário por parte do leitor em Segurança da Informação, particularmente no que diz respeito a primitivas criptográficas e Infraestruturas de Chaves Públicas (ICP). Para a compreensão desses conceitos é sugerida a leitura de livros como o *Handbook of Applied Cryptography*(MENEZES; OORSCHOT; VANSTONE, 1997) e o *Planning for PKI*(HOUSLEY; POLK, 2001).

2 ASSINATURAS DIGITAIS

2.1 INTRODUÇÃO

Assinaturas digitais são primitivas criptográficas, propostas na década de 70 por Diffie e Hellman (1976), como alternativas digitais às assinaturas manuscritas. Na época, os autores acreditavam que a plena adoção dos meios eletrônicos para transações comerciais dependia de uma maior proteção contra disputas entre as partes envolvidas. Algo que poderia ser oferecido por assinaturas reproduzíveis apenas pelo legítimo signatário mas verificáveis como autênticas por qualquer um.

Desde então, diversas contribuições vêm sendo incorporadas a essas assinaturas. Dentre elas, o uso de funções de resumo criptográfico, como forma de aumentar a segurança e performance dos esquemas relacionados(DAMGÅRD, 1987), e certificados digitais para uma distribuição confiável das chaves públicas dos signatários(KOHNFELDER, 1978). Neste capítulo é apresentada a forma como tais assinaturas vêm sendo atualmente implementadas, bem como o tempo de vida dessas implementações. Tais conceitos são fundamentais para o entendimento do restante deste trabalho.

Assim, na Seção 2.2, são descritas as operações que definem uma assinatura digital. A Seção 2.3, por sua vez, apresenta a forma mais comum de certificados digitais, os certificados X.509. Na Seção 2.4 são apresentados os principais pacotes de assinatura em uso, fundamentais para o armazenamento e intercâmbio das assinaturas digitais e informações necessárias a sua validação. A Seção 2.5 apresenta o tempo de vida dessas assinaturas. Finalmente, a Seção 2.6 conclui o capítulo.

2.2 ESQUEMAS DE ASSINATURA

Esquemas de assinaturas definem a forma como assinaturas digitais devem ser produzidas e validadas. Em geral, tais esquemas compreendem três operações, sendo elas a de geração do par de chaves e de geração e validação de assinaturas.

Geração do par de chaves: gera o par de chaves assimétricas a partir de parâmetros com o tamanho das chaves geradas. Do par, a chave privada deve ser mantida em segredo pelo signatário, e a chave pública distribuída àqueles que precisem validar as assinaturas produzidas.

Geração da assinatura: produz uma assinatura com base na chave privada e no documento eletrônico a ser assinado. Basicamente, é calculado um resumo criptográfico do documento, sendo tal resumo posteriormente cifrado com a chave privada do signatário. O uso da

chave privada, em princípio conhecida apenas pelo signatário, identifica o autor da assinatura. O resumo, por sua vez, indica a qual documento a assinatura se refere.

Validação da assinatura: verifica se uma assinatura é válida para um determinado documento e chave pública. Em suma, decifra a assinatura com a chave pública e compara o resultado com o resumo criptográfico do documento. A assinatura é válida se ambos são iguais, confirmando tanto a sua autoria quanto a integridade do documento assinado.

Um esquema de assinatura é considerado seguro quando é computacionalmente inviável falsificá-la. Deve ser inviável, por exemplo, deduzir a chave privada do signatário a partir de sua chave pública, ou alterar o documento assinado de maneira imperceptível, através da quebra da função de resumo criptográfico usada.

São exemplos de esquemas de assinatura, as assinaturas RSA(RIVEST; SHAMIR; ADLEMAN, 1978) e *Elliptic Curve Digital Signature Algorithm* (ECDSA)(JOHNSON; MENEZES; VANSTONE, 2001). As assinaturas RSA foram propostas por Rivest, Shamir e Adleman, como uma das primeiras implementações práticas das ideias de Diffie e Hellman, e ainda hoje constituem a principal implementação de assinaturas digitais.

2.3 CERTIFICADOS DIGITAIS X.509

Certificados digitais, igualmente conhecidos por certificados de chaves públicas, permitem uma distribuição confiável das chaves públicas necessárias à validação de assinaturas. Atualmente, a forma mais comum desses certificados são os certificados X.509, cuja origem remonta aos serviços de diretórios X.500(CHADWICK, 1996) onde foram inicialmente usados em larga escala. Tais certificados já estão disponíveis em três versões (ITU-T, 1988; ITU-T, 1993; ITU-T, 2008).

2.3.1 Certificado

Certificados digitais X.509 são documentos eletrônicos emitidos por uma terceira parte confiável, denominada Autoridade Certificadora (AC), onde constam informações como a chave pública, dados de identificação de seu titular, o prazo de validade do certificado e a assinatura da AC. Em geral, tais certificados são emitidos mediante confirmação de algumas dessas informações pela AC. Seu formato é especificado em ASN.1, sendo os certificados codificados em DER. Na figura 2.1 é apresentada uma visão geral desses documentos.

Os campos da estrutura *Certificate* compreendem os campos *tbsCertificate*, *signatureAlgorithm* e *signature* que trazem, respectivamente,

```
Certificate  ::=  SEQUENCE  {
     tbsCertificate TBSCertificate,
     signatureAlgorithm AlgorithmIdentifier,
     signatureValue BIT STRING
}

TBSCertificate  ::=  SEQUENCE  {
     version [0] EXPLICIT Version DEFAULT v1,
     serialNumber CertificateSerialNumber,
     signature AlgorithmIdentifier,
     issuer Name,
     validity Validity,
     subject Name,
     subjectPublicKeyInfo SubjectPublicKeyInfo,
     issuerUniqueID [1] IMPLICIT UniqueIdentifier OPTIONAL,
     subjectUniqueID [2] IMPLICIT UniqueIdentifier OPTIONAL,
     extensions [3] EXPLICIT Extensions OPTIONAL
}
```

Figura 2.1: Estruturas ASN.1 *Certificate* e *TBSCertificate*.

as informações assinadas pela AC, o identificador do esquema de assinatura por ela usado e, finalmente, sua assinatura.

A estrutura *TBSCertificate*, por sua vez, traz como principais informações os campos:

version: identifica a versão do formato usado, podendo ser 1, 2 ou 3, dependendo dos campos presentes;

serialNumber: inteiro positivo que identifica unicamente um certificado dentre aqueles emitidos pela AC;

issuer: contêm os dados de identificação da AC. Tal identificação se dá através de *Distinguished Names* (DN), que são nomes hierárquicos compostos por pares de atributo e valor.

validity: define o prazo de validade do certificado, ou seja, o período pelo qual se assumem verdadeiras as informações ali contidas. Terminado o prazo, o certificado é considerado expirado.

subject: contêm o DN do titular do certificado;

subjectPublicKeyInfo: traz a chave pública do titular do certificado, bem como identificador do algoritmo de criptografia assimétrica relacionado;

extensions: quando presente, contêm extensões do certificado. Cada uma delas é marcada como crítica ou não crítica, sendo que sistemas incapazes de reconhecer e processar alguma extensão crítica deverão rejeitar o certificado.

2.3.2 Dados de Revogação

Um certificado X.509 é válido até expirar ou ser revogado. Tais revogações visam atender principalmente àqueles casos onde as informações contidas no certificado deixam de ser verdadeiras antes da sua expiração. Isso ocorre, por exemplo, por mudanças nos dados de identificação do titular ou quando a sua chave privada é comprometida. O mesmo se dá no término das operações da AC.

Existem algumas formas de revogação desses certificados(MYERS et al., 1999; COOPER et al., 2008), sendo a principal delas as Listas de Certificados Revogados (LCR). Tais listas são documentos eletrônicos publicados periodicamente pela AC onde constam os números seriais dos certificados revogados que ainda não expiraram. Seu formato é especificado em ASN.1, sendo as LCRs codificadas em DER. Na figura 2.2 é apresentada uma visão geral desses documentos.

```
CertificateList  ::=  SEQUENCE  {
     tbsCertList TBSCertList,
     signatureAlgorithm AlgorithmIdentifier,
     signatureValue BIT STRING
}

TBSCertList  ::=  SEQUENCE  {
     version Version OPTIONAL,
     signature AlgorithmIdentifier,
     issuer Name,
     thisUpdate Time,
     nextUpdate Time OPTIONAL,
     revokedCertificates SEQUENCE OF SEQUENCE  {
          userCertificate CertificateSerialNumber,
          revocationDate Time,
          crlEntryExtensions Extensions OPTIONAL
     }  OPTIONAL,
     crlExtensions [0] EXPLICIT Extensions OPTIONAL
}
```

Figura 2.2: Estruturas ASN.1 *CertificateList* e *TBSCertList*.

Os campos da estrutura *CertificateList* compreendem os campos *tbsCertList*, *signatureAlgorithm* e *signatureValue* que trazem, respectivamente, as informações assinadas pela AC, o identificador do esquema de assinatura por ela usado e, finalmente, sua assinatura.

A estrutura *TBSCertList*, por sua vez, traz como principais informações os campos:

issuer: contêm o DN da AC;

thisUpdate: traz a data em que a LCR foi emitida;

nextUpdate: informa a data em que a próxima LCR será emitida;

revokedCertificates: contêm os números seriais dos certificados revogados, e informações adicionais sobre a revogação;

Apesar de incomum, outras entidades podem emitir as LCRs, desde que previamente delegadas pela AC.

2.3.3 Caminho de Certificação

Um certificado digital X.509 é confiável se os serviços oferecidos pela AC que o emitiu igualmente o são. Assim, é primordial conhecer a origem do certificado do signatário, bem como dos dados de revogação relacionados. Para tanto, é necessário validar a assinatura desses documentos, o que implica em conhecer, dentre outras informações, a chave pública da AC, seus dados de identificação e prazo de validade. Nesse caso, pode ser necessário obter o próprio certificado da AC. Em geral, uma cadeia de certificados é necessária, partindo do certificado do signatário até uma AC previamente conhecida, chamada de âncora de confiança.

O algoritmo para validação dessa cadeia, conhecida por caminho de certificação, é definido na recomendação X.509(COOPER et al., 2008). Outros algoritmos, todavia, podem ser usados, desde que os mesmos critérios sejam atendidos. Basicamente, um caminho de certificação $\mathcal{C} = \{c_1, c_2, ..c_n\}$ é válido se:

- c_1 foi emitido por alguma âncora de confiança;
- para todo c_i em $\mathcal{C}$, com $1 \leq i \leq n-1$, c_i é o emissor de c_{i+1};
- para todo c_i em $\mathcal{C}$, c_i não expirou nem foi revogado.

Além dessas ainda existem outras restrições que devem ser obedecidas, como aquelas impostas por extensões críticas dos certificados. Um exemplo dessas extensões é a *id-ce-basicConstraints* que indica se o certificado pode ser usado pra assinar outros, e o número máximo de certificados entre esse e o do signatário. Além disso, um caminho de certificação é válido se os esquemas de assinatura usados pelas ACs forem seguros. Do contrário, a autenticidade dos certificados e dados de revogação fica comprometida.

Âncoras de confiança são geralmente distribuídas por meio de certificados digitais auto-assinados, cuja autenticidade deve ser verificada por outros meios. Em geral, ficam disponíveis aos sistemas que lidam com assinaturas digitais por meio de repositórios de âncoras de confiança, onde os usuários podem adicionar e remover suas âncoras. Por fim, como quaisquer outros certificados, esses podem ser revogados. Apesar das iniciativas nesse sentido(HOUSLEY; ASHMORE; WALLACE, 2010; REDDY; WALLACE, 2010), contudo, ainda não existe uma forma comum para essas revogações.

2.4 PACOTES DE ASSINATURA

Pacotes de assinatura procuram oferecer um meio comum para o intercâmbio e armazenamento das assinaturas digitais, incluindo as infor-

mações necessárias a sua validação. Seu objetivo é acomodar além da própria assinatura, informações como o documento eletrônico assinado, certificados do caminho de certificação e atributos relacionados. Atualmente, são três os principais formatos para pacotes de assinatura usados, o *Cryptographic Message Syntax* (CMS), o *XML Digital Signature* (XMLDSig), e o *Portable Document Format* (PDF).

2.4.1 *Cryptographic Message Syntax* (CMS)

O formato CMS(HOUSLEY, 2004), evolução do antigo PKCS#7(KALISKI, 1998), é especificado em ASN.1, sendo os pacotes codificados em DER. Por esse motivo, um dos principais benefícios desse formato é o tamanho reduzido dos pacotes gerados. Outra característica do CMS está em suportar múltiplas assinaturas. A figura 2.3, apresenta uma visão geral desses pacotes.

```
ContentInfo ::= SEQUENCE {
   contentType          ContentType,
   content              [0] EXPLICIT ANY DEFINED BY contentType
}

ContentType ::= OBJECT IDENTIFIER

id-signedData OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs7(7) 2 }

SignedData ::= SEQUENCE {
   version              CMSVersion,
   digestAlgorithms     DigestAlgorithmIdentifiers,
   encapContentInfo     EncapsulatedContentInfo,
   certificates         [0] IMPLICIT CertificateSet OPTIONAL,
   crls [1]             IMPLICIT RevocationInfoChoices OPTIONAL,
   signerInfos          SignerInfos
}

EncapsulatedContentInfo ::= SEQUENCE {
   eContentType         ContentType,
   eContent [0]         EXPLICIT OCTET STRING OPTIONAL
}

SignerInfos ::= SET OF SignerInfo
```

Figura 2.3: Estruturas ASN.1 *ContentInfo* e *SignedData*.

Pacotes de assinatura CMS são estruturas *ContentInfo* onde os campos *contentType* e *content* correspondem, respectivamente, ao OID 1.2.840.113549.1.7.2 e a estrutura *SignedData*. Essa flexibilidade dada por *ContentInfo* se justifica pelo fato desses pacotes poderem ser usados para outros propósitos além do empacotamento de assinaturas digitais, tais como o intercâmbio e armazenamento de documentos cifrados.

Os campos da estrutura *SignedData* compreendem:

version: identifica a versão do formato usado;

digestAlgorithms: contêm os identificadores das funções de resumo criptográfico usadas nas assinaturas;

encapContentInfo: identifica o conteúdo assinado, podendo trazer o próprio documento;

certificates: quando presente, contêm certificados necessários à validação das assinaturas, podendo incluir o caminho de certificação de cada signatário ou apenas parte desses;

crls: quando presente, traz dados de revogação necessários à validação dos certificados em *certificates*;

signerInfos: contêm as assinaturas digitais;

Cada uma das assinaturas, por sua vez, é acomodada numa estrutura *SignerInfo*, detalhada na figura 2.4.

```
SignerInfo ::= SEQUENCE {
   version              CMSVersion,
   sid                  SignerIdentifier,
   digestAlgorithm      DigestAlgorithmIdentifier,
   signedAttrs          [0] IMPLICIT SignedAttributes OPTIONAL,
   signatureAlgorithm   SignatureAlgorithmIdentifier,
   signature            SignatureValue,
   unsignedAttrs        [1] IMPLICIT UnsignedAttributes OPTIONAL
}

SignedAttributes ::= SET SIZE (1..MAX) OF Attribute

UnsignedAttributes ::= SET SIZE (1..MAX) OF Attribute

Attribute ::= SEQUENCE {
   attrType                OBJECT IDENTIFIER,
   attrValues              SET OF AttributeValue
}
```

Figura 2.4: Estruturas ASN.1 *SignerInfos* e *SignerInfo*.

Os campos dessa estrutura são:

version: identifica a versão do formato usado;

sid: identifica o certificado do signatário, por exemplo, através de seu número serial e do DN da AC que o emitiu;

digestAlgorithm: identifica a função de resumo criptográfico usada pelo signatário;

signedAttrs: quando presente, contêm atributos assinados juntamente com o documento. Esses atributos são informações adicionais, em geral sobre a assinatura, o documento assinado ou sobre o signatário;

signatureAlgorithm: identifia o esquema de assinatura usado;

signature: contêm a assinatura gerada;

unsignedAttrs: quando presente, contêm atributos não assinados;

2.4.2 *XML Digital Signature* (XMLDSig)

O formato XMLDSig(BARTEL et al., 2002) é especificado em XML *Schema* e *Document Type Definition* (DTD), sendo os pacotes codificados em XML. Apesar de não suportarem múltiplas assinaturas como o CMS, tal formato pode acomodar mais de um documento assinado. A figura 2.5 apresenta uma visão geral desses pacotes.

```
<Signature ID?>
   <SignedInfo>
      <CanonicalizationMethod/>
      <SignatureMethod/>
      (<Reference URI? >
         (<Transforms>)?
         <DigestMethod>
         <DigestValue>
      </Reference>)+
   </SignedInfo>
   <SignatureValue>
   (<KeyInfo>)?
   (<Object ID?>)*
</Signature>
```

Figura 2.5: Representação da estrutura XML *Signature*.

Os campos da estrutura *Signature* compreendem:

CanonicalizationMethod: especifica o algoritmo de canonização aplicado sobre a estrutura *SignedInfo* antes de ser assinada. Diferentemente do CMS, no XMLDSig existe uma indireção onde os documentos são assinados indiretamente pela assinatura da estrutura *SignedInfo*;

SignatureMethod: informa o esquema de assinatura usado;

Reference: identifica cada um dos documentos assinados. Cada documento é identificado pelo seu resumo criptográfico e, opcionalmente, por seu URI;

SignatureValue: contêm a assinatura gerada;

KeyInfo: quando presente, contêm informações para a validação da assinatura, tais como certificados digitais;

Object: quando presente, pode trazer informações arbitrárias. Em geral, tal campo é usado para acomodar o documento assinado assim

como atributos da assinatura, documento assinado ou do signatário. Atributos assinados são implementados através de referências a esses atributos em *Reference*.

2.4.3 *Portable Document Format* (PDF)

O formato PDF suporta assinaturas digitais desde 1999, com a publicação de sua versão 1.3(ADOBE, 2006). Sua principal diferença em relação aos formatos CMS e XMLDSig está em integrar o próprio formato do documento ao pacote de assinatura, o que permite, por exemplo, incluir representações gráficas das assinaturas digitais. Nesse formato, tanto a assinatura quanto algumas das informações necessárias a sua validação são acomodadas numa área do documento PDF. Apesar de existir flexibilidade quanto a estrutura dessa área, por padrão, trata-se de um pacote PKCS#7.

2.5 TEMPO DE VIDA

Como visto ao longo deste capítulo, para que uma assinatura digital seja válida, o esquema de assinatura usado deve ser seguro e o caminho de certificação relacionado ao signatário, válido. Com o tempo, contudo, tanto o esquema perde sua segurança quanto esse caminho perde sua validade(JUST, 1998). A segurança de um esquema de assinatura se perde, por exemplo, por avanços em criptoanálise, ou com o aumento do poder computacional disponível para ataques. Um caminho de certificação, por sua vez, perde sua validade com a expiração ou revogação dos certificados, incluindo aquele da âncora de confiança, assim como pela quebra dos esquemas de assinatura usados nos certificados e dados de revogação relacionados.

Assim, uma assinatura digital possui um tempo de vida limitado. Seu prazo de validade, ou seja, seu tempo de vida esperado, é geralmente limitado pela expiração do certificado do signatário. Mesmo antes disso, contudo, a assinatura pode perder sua validade por fatores como a revogação de algum certificado, ou a quebra inesperada de algum esquema de assinatura. A partir de então, a segurança oferecida pela assinatura acaba sendo comprometida.

Uma assinatura cujo certificado do signatário tenha sido revogado devido ao comprometimento de sua chave privada, por exemplo, não oferece um mesmo nível de segurança pois a autoria dessa assinatura acaba se tornando duvidosa. O mesmo ocorre quando o certificado revogado é o de alguma AC do caminho de certificação ou da âncora de confiança. De posse da chave privada da AC, um adversário seria capaz de forjar certificados do caminho de certificação e, em última instância, a assinatura.

Mesmo que o certificado do signatário ou de alguma das ACs tenha sido revogado por outro motivo, que não o comprometimento da chave privada, a assinatura poderia ter sido falsificada pois comprometimentos

ocorridos após essa revogação não seriam notados(COOPER et al., 2008). Isso ocorre pois não se espera que sejam publicadas novas informações sobre um certificado após esse ter sido revogado. O mesmo problema ocorre com certificados expirados.

A autoria da assinatura se torna igualmente duvidosa quando o esquema de assinatura usado pelo signatário deixa de ser seguro. Se, por exemplo, o algoritmo de criptografia assimétrica for inseguro a ponto de ser possível deduzir a chave privada do signatário a partir de sua chave pública, então o autor dessa assinatura poderia ser um adversário. O mesmo se dá quando a chave privada de alguma AC é que pode ser deduzida. Em assinaturas RSA, por exemplo, isso é possível a partir do momento em que seja viável derivar o Módulo RSA, presente na chave pública, em seus fatores primos, algo já realizado para Módulos de 718(KLEINJUNG et al., 2010) e 512 bits(CAVALLAR et al., 2000).

Da mesma forma, um adversário poderia ter gerado a assinatura se a função de resumo criptográfico usada na assinatura de algum dos certificados ou dados de revogação relacionados não for mais segura. Nesse caso, um adversário poderia ter substituído o corpo do certificado por outro, relacionado a um par de chaves por ele conhecido. A partir daí, poderia ter gerado certificados do caminho de certificação e, em última instância, a assinatura. Molnar et al. (2008), por exemplo, realizaram um ataque semelhante onde uma AC *VeriSign* foi levada a assinar um certificado de entidade final cujo corpo possuía o mesmo resumo criptográfico MD5 de outro certificado de AC produzido pelo grupo.

Por fim, se a função de resumo criptográfico usada pelo signatário não for mais segura, então é a integridade do documento assinado que se torna duvidosa. Caso essa função não seja mais resistente a colisão, o signatário pode ter sido levado a assinar um outro documento de mesmo resumo criptográfico, o qual foi posteriormente substituído. Um exemplo desse ataque foi demonstrado por Lucks e Daum (2005), onde dois documentos *PostScript* com conteúdos completamente distintos, porém de mesmo resumo criptográfico MD5, foram gerados. Caso a função de resumo critpográfico tenha perdido sua resistência a segunda inversão, mesmo documentos assinados sem a intervenção do adversário seriam falsificáveis.

2.6 CONCLUSÃO

Neste capítulo foram apresentados detalhes quanto a forma como assinaturas digitais vêm sendo implementadas assim como os fatores que limitam o tempo de vida dessas implementações. Como visto, essas assinaturas são produzidas e validadas de acordo com algum esquema de assinatura, sendo, em geral, resultado da cifragem do resumo criptográfico do documento eletrônico com a chave privada do signatário.

A chave pública do signatário, necessária para validação das assinaturas tende a ser distribuída por meio de certificados digitais X.509,

onde uma Autoridade Certificadora (AC) confirma a titularidade dessa chave pelo signatário. Para validá-los, é geralmente necessária uma cadeia de certificados, conhecida por caminho de certificação, que vai desde uma AC previamente conhecida, chamada de âncora de confiança, até o certificado em questão, incluindo esse último. Para acomodar tais informações, juntamente com a assinatura e documento assinados, ainda são usados os pacotes de assinaturas, sendo os principais, os pacotes CMS, XMLDSig e PDF.

Finalmente, assinaturas digitais possuem um tempo de vida limitado pois tanto o esquema de assinatura se enfraquece com o tempo, quanto o caminho de certificação do signatário perde sua validade, comprometendo a segurança oferecida pela assinatura. Em geral, essas duram até a expiração do certificado do signatário, podendo perder sua validade antes disso, pela revogação de certificados ou a quebra de esquemas de assinatura relacionados.

3 PRESERVAÇÃO DE ASSINATURAS DIGITAIS

3.1 INTRODUÇÃO

A preservação de assinaturas digitais tem sido um tema recorrente na literatura desde a década de 70. Como citado no Capítulo 1, muitas das estratégias propostas, contudo, apenas ofereciam uma sobrevida para essas assinaturas. Nesse sentido, o trabalho de Bayer, Haber e Stornetta (1993) foi um dos primeiros a propor uma estratégia para a preservação por longo prazo das assinaturas digitais.

Atualmente, são duas as principais estratégias capazes de preservar uma assinatura por longo prazo. Ambas, baseadas no conceito de notarização (JUST, 1998), onde uma terceira parte confiável é usada para autenticar fatos sobre a assinatura. Numa delas, o fato autenticado é o momento em que a assinatura foi produzida. Na outra, esse fato é a própria validade da assinatura.

Neste capítulo, são apresentadas cada uma dessas estratégias, bem como a forma como a preservação por longo prazo de assinaturas digitais vem sendo tratada nas principais recomendações técnicas sobre o tema. Assim, a Seção 3.2 descreve a preservação por meio de carimbos do tempo. A Seção 3.3, por sua vez, apresenta a segunda dessas estratégias, baseada em autenticações da assinatura. Na Seção 3.4 são vistas as principais recomendações técnicas sobre o assunto. Finalmente, a Seção 3.5 conclui o capítulo.

3.2 PRESERVAÇÃO POR CARIMBOS DO TEMPO

Na preservação por carimbos do tempo, uma assinatura é preservada por meio de evidências que demonstram o momento em que fora produzida. A ideia é que uma assinatura seria autêntica se produzida antes de se tornar viável falsificá-la. Por exemplo, antes de a chave privada do signatário ser comprometida ou seu esquema de assinatura se tornar inseguro. Tais evidências, por sua vez, são chamadas de carimbos do tempo.

Na principal implementação desses carimbos, esses são documentos eletrônicos assinados por uma terceira parte confiável, denonimada Autoridade de Carimbo do Tempo (ACT), onde constam tanto o resumo criptográfico da informação datada, quanto a data em que o carimbo foi emitido. São duas as operações relacionadas a esses carimbos, a sua solicitação e validação. A primeira segue o protocolo representado a seguir:

$$\begin{aligned} &\mathcal{U} \longrightarrow \mathcal{ACT} : \mathcal{H}(x) \\ &\mathcal{ACT} \longrightarrow \mathcal{U} : \underbrace{((\mathcal{H}(x), t), \mathcal{S}ign_{\mathcal{ACT}}((\mathcal{H}(x), t)))}_{ts} \end{aligned}$$

Um usuário solicita um carimbo do tempo para uma informação qualquer $x \in \{0,1\}^+$, enviando seu resumo criptográfico $\mathcal{H}(x)$ para a ACT. Ao receber o resumo, a ACT então anexa a data atual t, assina o conjunto e retorna o carimbo formado. A partir de então é possível comprovar que x existia em t. Para tanto, é necessário validar o carimbo.

Um carimbo do tempo é válido se:

- a assinatura da ACT for válida;
- o resumo criptográfico presente no carimbo for igual a $\mathcal{H}(x)$ e $\mathcal{H}$ for uma função de resumo criptográfico segura.

A primeira condição tem por objetivo comprovar a autenticidade do carimbo. Já a segunda, visa comprovar a integridade da informação datada. Nota-se que a função $\mathcal{H}$ deve ser segura pois, do contrário, torna-se duvidosa a integridade dessa informação. Em maiores detalhes, $\mathcal{H}$ poderá ser apenas resistente à segunda inversão, desde que em t tenha sido resistente, igualmente, à colisão.

O tempo de vida desses carimbos é limitado por aquele da assinatura da ACT e pela segurança da função de resumo criptográfica usada. Assim, seu prazo de validade termina com a expiração do certificado da ACT, podendo se tornar inválido antes disso por meio da revogação de algum certificado do caminho de certificação, quebra de algum esquema de assinatura ou da função de resumo criptográfico usada.

3.2.1 Carimbos do Tempo X.509

Atualmente, uma das principais recomendações técnicas a especificar carimbos do tempo como esses é a RFC 3161 (ADAMS et al., 2001). Nessa recomendação, carimbos do tempo são pacotes *Cryptographic Message Syntax* (CMS), cujo conteúdo assinado segue a estrutura ASN.1 apresentada na figura 3.1.

```
TSTInfo ::= SEQUENCE  {
   version                 INTEGER { v1(1) },
   policy                  TSAPolicyId,
   messageImprint          MessageImprint,
   serialNumber            INTEGER,
   genTime                 GeneralizedTime,
   accuracy                Accuracy OPTIONAL,
   ordering                BOOLEAN DEFAULT FALSE,
   nonce                   INTEGER OPTIONAL,
   tsa                     [0] GeneralName OPTIONAL,
   extensions              [1] IMPLICIT Extensions OPTIONAL
}
```

Figura 3.1: Estrutura ASN.1 *TSTInfo*.

Os principais campos dessa estrutura compreendem:

policy: identifica a política sob a qual o carimbo do tempo foi emitido. Tais políticas são definidas na recomendação técnica RFC 3628(PINKAS; POPE; ROSS, 2003);

messageImprint: traz o resumo criptográfico da informação datada;

genTime: informa o momento em que a informação existia;

extensions: quando presente, contêm extensões do carimbo do tempo.

A solicitação desses carimbos, por sua vez, envolve as mensagens detalhadas na figura 3.2.

```
TimeStampReq ::= SEQUENCE  {
   version              INTEGER  { v1(1) },
   messageImprint       MessageImprint,
   reqPolicy            TSAPolicyId OPTIONAL,
   nonce                INTEGER OPTIONAL,
   certReq              BOOLEAN DEFAULT FALSE,
   extensions           [0] IMPLICIT Extensions OPTIONAL
}

TimeStampResp ::= SEQUENCE  {
   status               PKIStatusInfo,
   timeStampToken       TimeStampToken OPTIONAL
}
```

Figura 3.2: Estruturas ASN.1 *TimeStampReq* e *TimeStampResp*.

Uma requisição *TimeStampReq* possui como principais campos:

messageImprint: traz o resumo criptográfico calculado pelo usuário;

reqPolicy: quando presente, identifica a política sob a qual o carimbo deve ser emitido;

certReq: informa se o carimbo do tempo retornado deverá carregar o certificado da ACT e, opcionalmente, outros certificados do caminho de certificação;

extensions: quando presente, contêm extensões da requisição.

Uma resposta *TimeStampResp*, por sua vez, indica o sucesso ou fracasso da operação, e, em caso de sucesso, traz o carimbo do tempo requisitado.

3.2.2 Preservação e Validação de Assinaturas

A preservação de assinaturas digitais por meio de carimbos do tempo como esses inicia pela adição de um carimbo sobre a assinatura de modo a demonstrar que ela foi produzida antes de se tornar viável falsificá-la. Como o próprio carimbo acaba se tornando falsificável com

o tempo, outro carimbo deverá demonstrar sua validade. Um processo de sobreposição de carimbos que perdura enquanto for necessário preservar a assinatura digital.

Em maiores detalhes, sendo s, d, $\mathcal{C}_s$ e $\mathcal{R}_s$, respectivamente, a assinatura, o documento assinado, os certificados do caminho de certificação do signatário e os dados de revogação relacionados, a preservação de s segue os seguintes passos:

1. adiciona-se um carimbo do tempo ts^1 sobre $(s, d, \mathcal{C}_s, \mathcal{R}_s)$, sendo $\mathcal{R}_s$ dados de revogação atuais. Como resultado, obtêm-se ((s, d, $\mathcal{C}_s$, $\mathcal{R}_s$), ts^1, $\mathcal{C}_{ts}^1$);

2. agenda-se a adição do próximo carimbo do tempo com base na data de expiração do certificado da ACT. Tal agendamento pode ser revisto ao longo do tempo, caso novas informações que afetem a validade do carimbo tornem-se disponíveis;

3. no momento agendado, valida-se ts^1 e, sendo válido, adiciona-se ts^2 sobre ((s, d, $\mathcal{C}_s$, $\mathcal{R}_s$), ts^1, $\mathcal{C}_{ts}^1$, $\mathcal{R}_{ts}^1$), onde $\mathcal{R}_{ts}^1$ são dados de revogação atuais. Como resultado, obtêm-se (((s, d, $\mathcal{C}_s$, $\mathcal{R}_s$), ts^1, $\mathcal{C}_{ts}^1$, $\mathcal{R}_{ts}^1$), ts^2, $\mathcal{C}_{ts}^2$). Caso ts^1 já tenha perdido sua validade, a preservação falha;

4. para os próximos carimbos, repete-se os passos 2 e 3 enquanto for necessário preservar a validade da assinatura. Dessa forma, na adição do n-ésimo carimbo, obtêm-se ((...((((s, d, $\mathcal{C}_s$, $\mathcal{R}_s$), ts^1, $\mathcal{C}_{ts}^1$, $\mathcal{R}_{ts}^1$), ts^2, $\mathcal{C}_{ts}^2$, $\mathcal{R}_{ts}^2$), ...), ts^n, $\mathcal{C}_{ts}^n$).

Assinaturas preservadas por carimbos do tempo, por sua vez, requerem uma validação diferenciada. Sendo ((...((((s, d, $\mathcal{C}_s$, $\mathcal{R}_s$), ts^1, $\mathcal{C}_{ts}^1$, $\mathcal{R}_{ts}^1$), ts^2, $\mathcal{C}_{ts}^2$, $\mathcal{R}_{ts}^2$), ...), ts^n, $\mathcal{C}_{ts}^n$) a assinatura preservada, ela é válida se:

1. o carimbo do tempo ts^n for atualmente válido.

2. para todo ts^i, com $1 \leq i \leq n-1$, ts^i era válido na data indicada por ts^{i+1};

3. a assinatura s era válida na data indicada por ts^1.

Tais condições visam comprovar que a assinatura e cada um dos carimbos do tempo adicionados durante a preservação foram produzidos antes de se tornar viável falsificá-los.

3.3 PRESERVAÇÃO POR AUTENTICAÇÕES DA ASSINATURA

Na preservação por autenticações da assinatura, uma assinatura é preservada por meio de atestes onde uma terceira parte confiável, denominada Notário Digital (ND), confirma que a assinatura já foi válida no

passado. Em linhas gerais, tal ateste é um documento eletrônico, onde constam tanto dados de identificação do signatário quanto o resumo criptográfico do documento eletrônico assinado. São três as operações relacionadas a esses atestes, a sua solicitação, validação e renovação. A primeira segue o protocolo representado a seguir:

$$\begin{aligned} &\mathcal{U} \longrightarrow \mathcal{ND} : (s, d, \mathcal{C}_s) \\ &\mathcal{ND} \longrightarrow \mathcal{U} : \underbrace{((id_{\mathcal{S}}, \mathcal{H}(d)), \mathcal{S}ign_{\mathcal{ND}}((id_{\mathcal{S}}, \mathcal{H}(d))))}_{at} \end{aligned}$$

Sendo s, d, $\mathcal{C}_s$, respectivamente, a assinatura, o documento assinado e os certificados do caminho de certificação do signatário, um usuário solicita seu ateste enviando tais informação para o Notário Digital. Ao recebê-las, tal entidade obtêm dados de revogação atuais sobre os certificados e então valida s. Sendo válida, retorna o ateste, onde confirma que o signatário $\mathcal{S}$ assinou d.

Por sua vez, um ateste é válido quando:

- a assinatura do Notário Digital for válida;
- o resumo criptográfico presente no ateste for igual a $\mathcal{H}(d)$ e $\mathcal{H}$ for uma função de resumo criptográfico segura.

A primeira condição tem por objetivo comprovar a autenticidade do ateste. Já a segunda, visa comprovar a integridade da informação assinada por $\mathcal{S}$. Nota-se que a função $\mathcal{H}$ deve ser segura pois, do contrário, torna-se duvidosa a integridade dessa informação.

O tempo de vida desses atestes é limitado por aquele da assinatura do Notário Digital e pela segurança da função de resumo criptográfico usada. Assim, seu prazo de validade termina na expiração do certificado do notário, podendo se tornar inválido antes disso por meio da revogação de algum certificado do caminho de certificação, quebra de algum esquema de assinatura ou da função de resumo criptográfico usada.

Para tornar possível a preservação por longo prazo de assinaturas, um segundo protocolo ainda é necessário, o de renovação do ateste:

$$\begin{aligned} &\mathcal{U} \longrightarrow \mathcal{ND} : (d, at, \mathcal{C}_{at}) \\ &\mathcal{ND} \longrightarrow \mathcal{U} : \underbrace{((id_{\mathcal{S}}, \mathcal{H}'(d)), \mathcal{S}ign'_{\mathcal{ND}}((id_{\mathcal{S}}, \mathcal{H}'(d))))}_{at'} \end{aligned}$$

Quando um ateste estiver próximo de perder sua validade, o usuário o envia, juntamente com o documento assinado, pra o Notário Digital. Ao recebê-los, tal entidade valida at, e então renova o ateste, possivelmente com uma nova função de resumo de resumo criptográfico, um novo esquema de assinatura ou uma nova chave privada.

3.3.1 Preservação e Validação de Assinaturas

A preservação de assinaturas digitais por meio de autenticações da assinatura inicia pela substituição dessa por um ateste, de modo a demonstrar que em algum momento passado tal assinatura foi válida. Como o próprio ateste acaba se tornando falsificável com o tempo, outro deverá ser usado para demonstrar sua validade. Um processo de renovação de atestes que perdura enquanto for necessário preservar a assinatura digital.

Em maiores detalhes, sendo s e d, respectivamente, a assinatura e o documento assinado, a preservação de s segue os seguintes passos:

1. substitui-se a assinatura s, por um ateste at^1, obtendo $(d, at^1, \mathcal{C}^1_{at})$, onde $\mathcal{C}^1_{at}$ é o caminho de certificação do Notário Digital;

2. agenda-se a renovação do ateste com base na data de expiração do certificado de ND. Tal agendamento pode ser revisto ao longo do tempo, caso novas informações que afetem a validade do ateste tornem-se disponíveis;

3. no momento agendado, valida-se at^1 e, sendo válido, substitui-se at^1 por sua versão renovada at^2, obtendo $(d, at^2, \mathcal{C}^2_{at})$. Caso at^1 já tenha perdido sua validade a preservação falha;

4. para os próximos atestes, repete-se os passos 2 e 3 enquanto for necessário preservar a validade da assinatura. Dessa forma, com a renovação do n-ésimo ateste, obtêm-se $(d, at^n, \mathcal{C}^n_{at})$.

Assinaturas preservadas por autenticações, por sua vez, requerem uma validação diferenciada. Sendo $(d, at^n, \mathcal{C}^n_{at})$ a assinatura preservada, ela é válida se at^n for válido. Tal condição visa confirmar que em algum momento passado um Notário Digital confirmou a validade da assinatura.

3.4 RECOMENDAÇÕES TÉCNICAS

Atualmente as principais recomendações técnicas sobre a preservação por longo prazo de assinaturas digitais são as recomendações CMS Advanced Electronic Signature (CAdES)(ETSI, 2009a), XML Advanced Electronic Signature (XAdES)(ETSI, 2009c), PDF Advanced Electronic Signature (PAdES)(ETSI, 2009b) e Evidence Record Syntax (ERS)(GONDROM; BRANDNER; PORDESCH, 2007). Todas elas empregam a estratégia de preservação baseada em carimbos do tempo descrita na Seção 3.2.

As recomendações CAdES, XAdES e PAdES são extensões dos pacotes de assinatura apresentados no Capítulo 3, propostas pelo ETSI como implementação das assinaturas digitais previstas na Diretiva Européia 1999/93/EC(PARLIAMENT; COUNCIL, 2000). A recomendação

CAdES estende os pacotes CMS. Nela, cada carimbo do tempo adicionado, assim como as informações necessárias a sua validação, como certificados e dados de revogação, é acomodado por meio de uma extensão não assinada, a *id-aa-ets-archiveTimestampV2*.

A recomendação XAdES, por sua vez, estende os pacotes XMLDSig. De maneira semelhante à recomendação CAdES, nela cada carimbo adicionado, juntamente com as informações necessárias a sua validação, é suportado por meio de uma extensão não assinada, a *ArchiveTimeStamp*.

No PAdES, que estende os pacotes PDF, a preservação por meio de carimbos do tempo envolve duas estruturas de dados, a *Document Timestamp* e a *Document Security Store* (DSS). Cada carimbo do tempo adicionado é então acomodado numa estrutura *Document Time-stamp*, sendo as informações necessárias a sua validação armazenadas num DSS.

Finalmente, a recomendação ERS suporta a preservação de assinaturas digitais de maneira independente do pacote de assinatura usado. Nela cada pacote pode ser tratado como uma sequência de *bytes*, datada por meio de carimbos do tempo. Tal recomendação permite ainda reduzir custos relacionados a preservação de grandes volumes de documentos assinados, de modo que cada carimbo do tempo possa datar mais de um deles. Para tanto, conjuntos de documentos assinados são agrupados por meio de Árvores de Merkle(MERKLE, 1979), sendo os carimbos adicionados sobre o seu nó raiz. Tais árvores são detalhadas no Capítulo 4, Seção 4.4.1.1.

3.5 CONCLUSÃO

Neste capítulo foram apresentadas as principais estratégias até então propostas para a preservação por longo prazo de assinaturas digitais, assim como as recomendações técnicas, de maior relevância, que atualmente abordam o assunto. Como visto, tais estratégias se baseiam no conceito de notarização onde uma terceira parte confiável é usada para autenticar fatos sobre a assinatura.

Na primeira dessas estratégias esse fato é o momento em que a assinatura foi produzida. Para tanto, são adicionados carimbos do tempo, onde o primeiro demonstra a validade da assinatura e os seguintes a validade dos carimbos anteriores. Algo necessário pois os próprios carimbos acabam se tornando inválidos com o tempo. Por outro lado, na segunda estratégia o fato autenticado é a própria validade da assinatura. Nesse caso o processo de preservação consiste na renovação desses atestes.

Finalmente, as principais recomendações técnicas sobre o assunto, são as recomendações CAdES, XAdES e PAdES. Tais recomendações estendem, respectivamente, os pacotes de assinatura CMS, XMLDSig e PDF, adicionando suporte à preservação por longo prazo das assinaturas. Em todas essas recomendações, a estratégia usada é aquela baseada em carimbos do tempo.

4 CARIMBOS DO TEMPO DE LONGO PRAZO

4.1 INTRODUÇÃO

Dentre as estratégias até então propostas para a preservação de assinaturas digitais, aquela baseada em carimbos do tempo, desenvolvida por Bayer, Haber e Stornetta (1993), é a que atualmente possui maior aceitação, sendo usada pelas principais recomendações técnicas sobre o assunto. Apesar de sua popularidade, todavia, tal estratégia é incapaz de garantir a preservação de assinaturas digitais, além de apresentar custos inadequados para certos contextos.

São vários os fatores que podem levar esse processo de preservação a falhar, tais como o comprometimento da chave privada de Autoridades Certificadoras (AC), das Autoridades de Carimbo do Tempo (ACT), ou o enfraquecimento repentino de algoritmos criptográficos. Seus custos, por outro lado, são problemáticos principalmente para plataformas com recursos computacionais escassos ou quando grandes volumes de documentos são considerados.

Neste capítulo são propostos protocolos criptográficos para aumentar a confiabilidade e reduzir os custos relacionados a essa estratégia. Por meio deles, duas novas implementações de carimbos são obtidas, os Carimbos do Tempo Renováveis e os Carimbos do Tempo Autenticados. Assim, na Seção 4.2 as origens dos riscos e custos geralmente associados à preservação por carimbos do tempo são analisadas. As Seções 4.3 e 4.4, por sua vez, apresentam os Carimbos do Tempo Renováveis e os Carimbos do Tempo Autenticados. Finalmente, a Seção 5.5 conclui o capítulo.

4.2 CARIMBOS DO TEMPO TRADICIONAIS

Como visto no Capítulo 3, Seção 3.2.2, a preservação de uma assinatura por meio de carimbos do tempo consiste essencialmente na sobreposição desses carimbos ao longo do tempo, conforme a validade desses esteja próximo de terminar. Em termos de recursos computacionais, tal abordagem acaba levando a custos crescentes na preservação e validação dessas assinaturas.

Na preservação, para cada carimbo do tempo adicionado, mais espaço de armazenamento é necessário para acomodar a ele e as informações necessárias a sua validação, tais como certificados e dados de revogação. Da mesma forma, na validação da assinatura preservada, cada carimbo a mais implica num aumento dos custos relacionados. A figura 4.1, por exemplo, apresenta uma simulação desses custos de armazenamento ao longo de 50 anos, considerando valores de uma Infraestrutura de Chaves Públicas (ICP) típica. Tal ICP é detalhada no Capítulo 5.

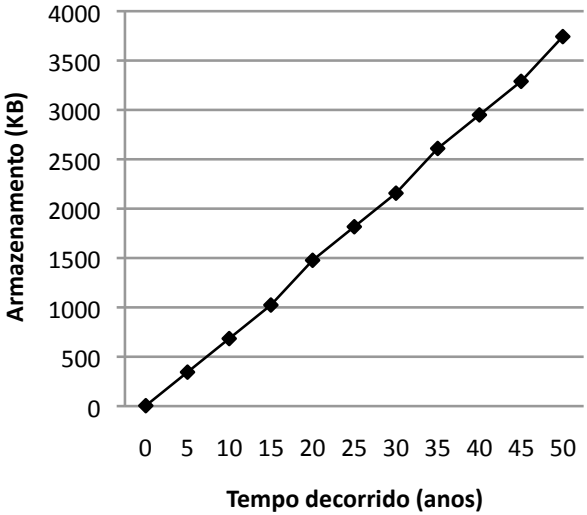

Figura 4.1: Simulação dos custos da preservação tradicional ao longo de 50 anos.

Como citado por Troncoso, Cock e Preneel (2008), tais custos acabam sendo razoáveis quando o aumento no processamento, banda, e capacidade de armazenamento disponíveis, decorrentes do avanço tecnológico, é considerado. Todavia, podem ser inadequados quando grandes volumes de documentos ou plataformas com recursos computacionais escassos são levados em consideração(BLAZIC; SETCCE, 2007; GONDROM; BRANDNER; PORDESCH, 2007; VIGIL et al., 2009).

A confiabilidade do processo de preservação, por sua vez, é limitada por diversos fatores. Dentre eles estão os problemas que podem impedir a sobreposição de um carimbo do tempo antes desse perder sua validade (ETSI, 2009a; ETSI, 2009c; ETSI, 2009b; GONDROM; BRANDNER; PORDESCH, 2007). Isso ocorre, por exemplo, quando um carimbo torna-se inválido antes do previsto ou quando sua sobreposição é impedida por problemas de disponibilidade da ACT. Além disso, mesmo que uma assinatura seja corretamente preservada, existe a possibilidade de futuramente se descobrir que alguma das ACTs usadas no processo não era honesta, ou que algum dos algoritmos criptográficos empregados eram, de fato, inseguros.

Tanto os custos quanto a confiabilidade desse processo tem sido tema de trabalhos. Em relação aos custos, em geral, é proposto o uso de Árvores de Merkle(MERKLE, 1980) para reduzir o número de carimbos do tempo necessários para preservar a assinatura de grandes volumes de documentos (BLAZIC; SETCCE, 2007; GONDROM; BRANDNER; PORDESCH, 2007; ZIMMER; LANGKABEL; HENTRICH, 2008).

Nessa abordagem, a cada sobreposição, ao invés de um carimbo por documento assinado, é obtido um carimbo por conjunto de documentos. Quanto à confiabilidade do processo, em geral, é sugerido o uso de carimbos do tempo redundantes para tolerar possíveis falhas durante a preservação. Tais carimbos acabam, contudo, multiplicando os custos do processo(BLAZIC; SETCCE, 2007; GONDROM; BRANDNER; PORDESCH, 2007).

Neste trabalho é proposta uma abordagem diferente para reduzir os custos e aumentar a confiabilidade da preservação de assinaturas por meio de carimbos do tempo. São definidos protocolos criptográficos que permitem tanto estender o tempo de vida de um carimbo quanto tornar esse tempo mais previsível. Assim, os custos são reduzidos devido a um número menor de carimbos necessários num mesmo período de preservação. Já a confiabilidade aumenta devido a um risco menor de algum carimbo do tempo perder sua validade antes do previsto. Por modificarem os carimbos, tais protocolos ainda podem ser usados como complemento às abordagens tradicionais.

4.3 CARIMBOS DO TEMPO RENOVÁVEIS

Carimbos do Tempo Renováveis são carimbos que suportam além das tradicionais operações de solicitação e validação, a operação de renovação. Por meio dessa operação, é possível restabelecer a validade da assinatura do carimbo, quando essa não for mais válida. Dessa forma, o tempo de vida do carimbo deixa de ser influenciado pelos fatores que levam tais assinaturas a perderem sua validade. Como resultado, esse tempo tende a ser maior e mais previsível. Sua emissão, por outro lado, depende de novos serviços a serem oferecidos pela Autoridade de Carimbo do Tempo (ACT).

4.3.1 Suporte pela ACT

Uma ACT que suporte a emissão de Carimbos do Tempo Renováveis deve oferecer os serviços de emissão e renovação de carimbos. Para suportá-los, ela ainda precisa manter uma estrutura de dados chamada Repositório de Carimbos do Tempo.

4.3.1.1 Repositório de Carimbos do Tempo

Um Repositório de Carimbos do Tempo suporta as seguintes operações:

$add(ts)$**:** registra um carimbo do tempo ts, armazenando o resumo criptográfico de suas informações, ou seja $\mathcal{H}((\mathcal{H}(x), t))$. A função $\mathcal{H}$ deve ser a mesma usada pelo carimbo sobre a informação datada;

$exists(ts) \longrightarrow \{1, 0\}$**:** verifica se um carimbo ts foi previamente registrado. Para tanto, busca $\mathcal{H}((\mathcal{H}(x), t))$ dentre os resumos armazenados. Se o carimbo foi registrado retorna 1, do contrário 0;

$remove(\mathcal{H})$**:** remove do repositório os resumos criptográficos relacionados a função $\mathcal{H}$.

4.3.1.2 Emissão de Carimbos

Um Carimbo do Tempo Renovável é emitido segundo uma versão estendida do protocolo tradicional, apresentado no Capítulo 3:

$$\begin{aligned} &\mathcal{U} \longrightarrow \mathcal{ACT} : \mathcal{H}(x) \\ &\mathcal{ACT} \longrightarrow \mathcal{U} : \underbrace{((\mathcal{H}(x), t), \mathcal{S}ign_{\mathcal{ACT}}((\mathcal{H}(x), t)))}_{ts} \end{aligned}$$

Como descrito no Capítulo 3, o usuário solicita um carimbo do tempo para uma informação qualquer $x \in \{0, 1\}^+$, enviando seu resumo criptográfico $\mathcal{H}(x)$ para a ACT. Ao receber o resumo, tal entidade anexa a data atual t, assina o conjunto e então retorna o carimbo do tempo formado. Diferentemente do tradicional, contudo, tal carimbo ainda deverá ser registrado pela ACT, por meio de $rep_{\mathcal{ACT}}.add(ts)$.

4.3.1.3 Renovação de Carimbos

A renovação de um carimbo, por sua vez, segue o seguinte protocolo:

$$\begin{aligned} &\mathcal{U} \longrightarrow \mathcal{ACT} : ts \\ &\mathcal{ACT} \longrightarrow \mathcal{U} : \underbrace{((\mathcal{H}(x), t), \mathcal{S}ign'_{\mathcal{ACT}}((\mathcal{H}(x), t)))}_{ts'} \end{aligned}$$

Quando o usuário não puder mais comprovar a autenticidade do carimbo, devido a perda da validade da assinatura, ele pode solicitar sua renovação enviando-o para a ACT. Uma vez recebido, tal entidade confirma a autoria do carimbo, consultado o Repositório de Carimbos do Tempo por meio de $rep_{\mathcal{ACT}}.exists(ts)$. Com a autoria confirmada, a ACT renova sua assinatura e então retorna o carimbo para o usuário.

Para poder renovar sua assinatura, contudo, é necessário que a ACT tenha contornado os fatores que levaram a anterior a perder sua validade. Por exemplo, se sua chave privada foi comprometida e, consequentemente, seu certificado foi revogado, um novo certificado para um novo par de chaves deverá ter sido obtido. Assim, cabe a ACT prezar pelas condições necessárias às renovações, obtendo novos certificados e atualizando seus esquemas de assinatura.

Renovações são negadas em duas situações principais. A primeira ocorre quando a função de resumo criptográfico usada no carimbo sobre a

informação datada não é mais resistente a segunda inversão. Com a perda dessa resistência o carimbo acaba perdendo sua serventia, uma vez que não é mais possível comprovar a integridade da informação datada. Além disso, o próprio registro no Repositório de Carimbos do Tempo perde sua utilidade. A segunda situação se dá quando a ACT perdeu sua capacidade de renovar o carimbo. Isso ocorre, geralmente, com o término prematuro das operações da ACT, ou quando o Repositório de Carimbos do Tempo é comprometido de maneira irreversível.

4.3.1.4 Otimização do Repositório de Carimbos do Tempo

Por fim, de modo a limitar os custos relacionados à renovação dos carimbos, ocorre periodicamente a otimização do Repositório de Carimbos do Tempo. Quando alguma função de resumo criptográfico perde sua resistência à segunda inversão, cabe à ACT remover os registros relacionados desse Repositório por meio de $rep_{\mathcal{ACT}}.remove(\mathcal{H})$.

4.3.2 Operações do Carimbo

As operações disponíveis ao usuário final são, portanto:

Solicitação: permite a obtenção do carimbo. Segue o protocolo descrito na Seção 4.3.1.2;

Renovação: possibilita a renovação do carimbo quando sua assinatura não for mais válida. Segue o protocolo apresentado na Seção 4.3.1.3;

Validação: permite a validação do carimbo. Segue os passos tradicionais descritos no Capítulo 3.

4.3.3 Preservação de Assinaturas

A preservação de uma assinatura por meio de Carimbos do Tempo Renováveis apresenta poucas diferenças em relação aquela com carimbos tradicionais. Basicamente, o agendamento da adição de um novo carimbo passa a ser orientado não mais pela expiração do certificado da ACT, mas pela segurança da função de resumo criptográfico usada pelo carimbo sobre a informação datada.

Em maiores detalhes, sendo s, d, $\mathcal{C}_s$ e $\mathcal{R}_s$, respectivamente, a assinatura, o documento assinado, os certificados do caminho de certificação do signatário e os dados de revogação relacionados, a preservação de s segue os seguintes passos:

1. adiciona-se um carimbo do tempo ts^1 sobre $(s, d, \mathcal{C}_s, \mathcal{R}_s)$, sendo $\mathcal{R}_s$ dados de revogação atuais. Como resultado, obtêm-se ((s, d, $\mathcal{C}_s$, $\mathcal{R}_s$), ts^1, $\mathcal{C}^1_{ts}$);

2. agenda-se a adição do próximo carimbo do tempo com base na segurança da função de resumo criptográfico usada por ts^1 sobre a informação datada. Tal agendamento pode ser revisto ao longo do tempo, conforme novas informações sobre essa função tornem-se disponíveis;

3. no momento agendado, valida-se ts^1. Se inválido, tal carimbo deverá ser substituído por sua versão renovada. Sendo ts^1 o carimbo do tempo em questão, possivelmente renovado, adiciona-se ts^2 sobre $((s, d, \mathcal{C}_s, \mathcal{R}_s), ts^1, \mathcal{C}^1_{ts}, \mathcal{R}^1_{ts})$, onde $\mathcal{R}^1_{ts}$ são dados de revogação atuais. Como resultado, obtêm-se $(((s, d, \mathcal{C}_s, \mathcal{R}_s), ts^1, \mathcal{C}^1_{ts}, \mathcal{R}^1_{ts}), ts^2, \mathcal{C}^2_{ts})$. Caso ts^1 já tenha perdido sua validade, e sua renovação não seja possível, a preservação falha;

4. para os próximos carimbos, repete-se os passos 2 e 3 enquanto for necessário preservar a validade da assinatura. Dessa forma, na adição do n-ésimo carimbo, obtêm-se $((...(((s, d, \mathcal{C}_s, \mathcal{R}_s), ts^1, \mathcal{C}^1_{ts}, \mathcal{R}^1_{ts}), ts^2, \mathcal{C}^2_{ts}, \mathcal{R}^2_{ts}), ...), ts^n, \mathcal{C}^n_{ts})$.

4.3.4 Validação de Assinaturas

Assinaturas preservadas por meio de Carimbos do Tempo Renováveis podem ser validadas seguindo os mesmos passos da validação tradicional, exceto quando a assinatura do último carimbo não é mais válida. Nesse caso, é necessário renová-lo. Sendo $((...(((s, d, \mathcal{C}_s, \mathcal{R}_s), ts^1, \mathcal{C}^1_{ts}, \mathcal{R}^1_{ts}), ts^2, \mathcal{C}^2_{ts}, \mathcal{R}^2_{ts}), ...), ts^n, \mathcal{C}^n_{ts})$ a assinatura preservada, ela é válida se:

1. o carimbo do tempo ts^n for atualmente válido. Para tanto pode ser preciso renová-lo;

2. para todo ts^i, com $1 \leq i \leq n-1$, ts^i era válido na data indicada por ts^{i+1};

3. a assinatura s era válida na data indicada por ts^1.

4.4 CARIMBOS DO TEMPO AUTENTICADOS

Carimbos do Tempo Autenticados são carimbos do tempo que suportam, além das tradicionais operações de solicitação e validação, as operações de autenticação e renovação. Por meio da operação de renovação é possível restabelecer a validade do carimbo, de maneira similar aquela dos Carimbos do Tempo Renováveis, prolongando, assim, o seu tempo de vida. A operação de autenticação, por outro lado, busca reduzir os custos relacionados à verificação da autenticidade do carimbo. Através dela é possível substituir o caminho de certificação do carimbo, assim como seus dados de revogação, por um Selo de Autenticidade, onde uma âncora de confiança confirma a validade da assinatura da Autoridade de Carimbo do Tempo (ACT).

4.4.1 Preliminares

A ideia por trás dos Carimbos do Tempo Autenticados é remover, da validação de um carimbo, a necessidade de validar o seu caminho de certificação. Isso porque tal caminho, juntamente com seus dados de revogação, tendem a ser os maiores responsáveis pelos custos de armazenamento e validação de carimbos do tempo(MARTINEZ-PELáEZ et al., 2008). Para tanto, a própria âncora de confiança passa a autenticar a origem dos carimbos emitidos por meio de um Selo de Autenticidade.

Nesse caso, contudo, é primordial que os usuários compartilhem a mesma âncora de confiança. Assim, Carimbos do Tempo Autenticados foram projetados para Infraestruturas de Chaves Públicas Hierárquicas, onde a Autoridade Certificadora Raiz (AC-Raiz) é geralmente a âncora escolhida. Para facilitar o entendimento da proposta, a seguir é apresentado um esquema simplificado para a autenticação de um carimbo do tempo:

$$\mathcal{ACT} \longrightarrow \mathcal{ACR}aiz : ts$$
$$\mathcal{ACR}aiz \longrightarrow \mathcal{RP} : \underbrace{((\mathcal{H}(ts), id_{\mathcal{ACT}}), \mathcal{S}ign_{\mathcal{ACR}aiz}((\mathcal{H}(ts), id_{\mathcal{ACT}})))}_{sl_{ts}}$$

Ao emitir cada carimbo do tempo ts a ACT solicita o Selo de Autenticidade correspondente enviando o carimbo para a AC-Raiz. A AC-Raiz, por sua vez, valida a assinatura do carimbo e, sendo válida, publica num repositório público o selo atestando essa validade. Por fim, o usuário autentica o carimbo do tempo substituindo as informações necessárias à verificação da sua autenticidade pelo selo. Assim, para validar o carimbo, basta validar o Selo de Autenticidade no lugar da assinatura da ACT.

Um Selo de Autenticidade, por sua vez, é válido se:

- a assinatura da AC-Raiz em sl_{ts} é válida;
- o resumo criptográfico de ts é igual aquele presente em sl_{ts}, sendo a função de resumo criptográfico segura.

Nesse caso, renovações do carimbo ocorreriam pela renovação de seu Selo de Autenticidade pela AC-Raiz, quando esse perdesse a validade. Apesar de funcional, na prática essa abordagem é inviável por dois motivos principais. O primeiro diz respeito à boa prática de manter a AC-Raiz *offline* buscando uma melhor proteção de sua chave-privada. O segundo motivo se refere aos custos elevados tanto para a ACT, quanto para a AC-Raiz, no envio e autenticação de cada um dos carimbos do tempo emitidos.

Por outro lado, se a chave privada da AC-Raiz fosse usada apenas em intervalos, como já ocorre na emissão de suas LCRs, e ao fim desses intervalos fosse enviado, apenas, uma pequena representação do conjunto de carimbos do tempo emitidos no período, seria alcançada uma implementação de maior viabilidade. É essa, então, a abordagem proposta. Para

a representação em questão, são usadas Árvores de Merkle(MERKLE, 1979). O emprego de outras implementações de Dicionários Autenticados(ANAGNOSTOPOULOS; GOODRICH; TAMASSIA, 2001), contudo, seria igualmente viável.

Por fim, deve-se notar que, por receber apenas uma representação do conjunto de carimbos do tempo emitidos, e não os próprios carimbos, a AC-Raiz é incapaz de validar a assinatura de cada um deles. A única assinatura validada é a da própria representação, pela qual a ACT declara ter emitido os carimbos do tempo ali representados. Nota-se, portanto, que nesse caso ocorre uma "autenticação às cegas", por parte da AC-Raiz. Assim, assume-se que a ACT seja honesta tanto na emissão de seus carimbos do tempo quanto no envio dessas representações.

4.4.1.1 Árvores de Merkle

Árvores de Merkle são construções criptográficas que permitem autenticar conjuntos de elementos, de forma que se possa comprovar, com custos mínimos, se um dado elemento foi autenticado. Tais estruturas são árvores binárias onde os nós folhas são os resumos criptográficos desses elementos e cada um dos outros nós é o resumo criptográfico de seus dois nós filhos. Um exemplo dessas árvores é apresentado na figura 4.2.

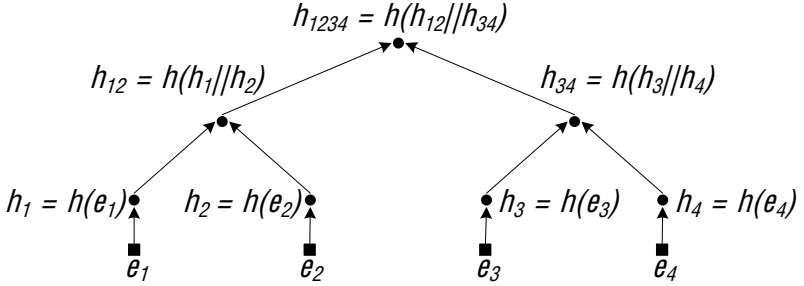

Figura 4.2: Exemplo de Árvore de Merkle.

Os nós h_1, h_2, h_3 e h_4 são, respectivamente, resumos criptográficos dos elementos e_1, e_2, e_3, e e_4, sendo tais elementos informações binárias quaisquer, cujo tamanho máximo é limitado pela função de resumo criptográfico escolhida. Aos pares, tais resumos criptográficos são concatenados, servindo de entrada para a geração dos nós do nível superior. O nó h_{12} é resultado de $h(h_1||h_2)$. Por sua vez, h_{34} é dado por $h(h_3||h_4)$. Finalmente, o nó raiz h_{1234} é o resultado de $h(h_{12}||h_{34})$.

Por meio de construções como essa, autenticar um conjunto de elementos se resume a autenticar o nó raiz da árvore de Merkle que os representa. Essa autenticação poderia ser dada, por exemplo, assinando digitalmente tal nó. Por outro lado, para se comprovar se um dado ele-

mento é um dos autenticados, é necessário obter e validar o caminho de autenticação relacionado.

Dado um elemento qualquer, seu caminho de autenticação é dado pelos nós irmãos do caminho entre o nó raiz e o elemento em questão. Tomando-se e_4, por exemplo, seu caminho de autenticação é formado por h_3 e h_{12}, conforme representado na figura 4.3.

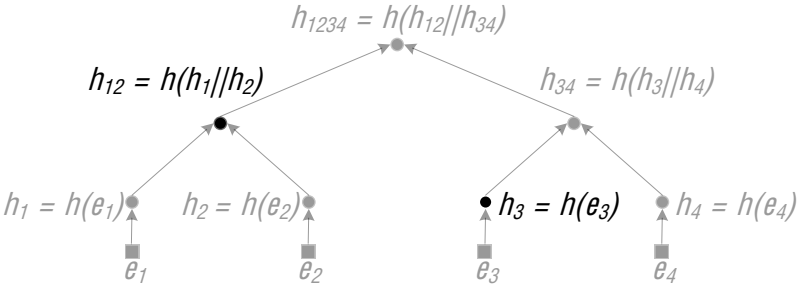

Figura 4.3: Caminho de autenticação de e_4.

Um caminho de autenticação é válido quando pode ser reconstruído. No caso do caminho de e_4, isso implica em:

- $h(e_4) = h_4$;
- $h(h_3||h_4) = h_{34}$;
- $h(h_{12}||h_{34}) = h_{1234}$.

Nota-se que, no exemplo dado, para um conjunto de 4 elementos, a validação de cada um deles requer caminhos de autenticação formados por 2 resumos criptográficos. De fato, para árvores de Merkle de n elementos, são obtidos caminhos de autenticação formados por, no máximo, $log_2(n)$ resumos.

Um problema fundamental, relacionado a tais árvores, é a definição de um algoritmo de travessia que permita construir o caminho de autenticação de cada um dos elementos de maneira eficiente. A solução trivial, onde são armazenados todos os nós da árvore em memória, requer espaço excessivo. Por outro lado, computar tais caminhos na medida em que são necessários pode implicar em custos altos para determinados elementos. Para tal questão, todavia, já existem diversos algoritmos(SZYDLO, 2004; BERMAN; KARPINSKI; NEKRICH, 2007; BUCHMANN; DAHMEN; SCHNEIDER, 2008). No de Szydlo (2004), por exemplo, a geração de cada caminho de autenticação requer o cálculo de no máximo $2log_2(n)$ resumos criptográficos, e o armazenamento de menos de $3log_2(n)$ resumos em memória.

4.4.1.2 Orquestração de Serviços

Carimbos do Tempo Autenticados são então implementados com a divisão das operações da ACT e AC-Raiz em intervalos de tempo, chamados Rodadas. Tais Rodadas devem ter a mesma duração, todavia, iniciando em momentos diferentes, como ilustrados na figura 4.4.

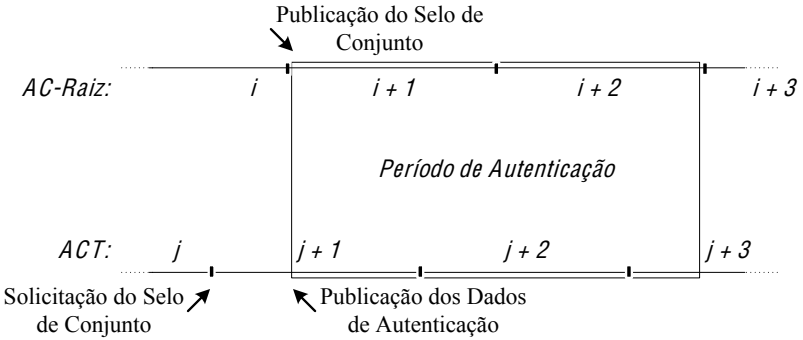

Figura 4.4: Orquestração dos serviços necessários à emissão de Carimbos do Tempo Autenticados.

Assim, ao invés de enviar cada carimbo para a AC-Raiz, a ACT aguarda o fim de sua Rodada para enviar uma pequena representação dos carimbos emitidos, o nó raiz da Árvore de Merkle formada a partir deles. A AC-Raiz, por outro lado, só autentica esses carimbos, no fim de sua Rodada, quando assina a representação recebida, dando origem a um Selo de Conjunto. Dessa forma, Selos de Autenticidade são formados por dois componentes, o Selo de Conjunto e os Dados de Autenticação, sendo esses últimos o caminho de autenticação do carimbo na Árvore de Merkle.

Esses Selos ficam disponíveis durante o Período de Autenticação do carimbo. Esse período inicia com a Rodada da AC-Raiz terminando com a remoção dos Dados de Autenticação relacionados pela ACT. Sua duração compreende uma ou mais Rodadas da AC-Raiz, ficando a critério da ACT. Renovações do carimbo, por sua vez, são implementadas pela renovação de seu Selo de Conjunto. Tais renovações são possíveis até que a AC-Raiz remova o Selo de Conjunto correspondente.

4.4.2 Suporte pela ACT e AC-Raiz

Em maiores detalhes, a emissão de Carimbos do Tempo Autenticados depende dos serviços de emissão, autenticação e renovação oferecidos pela ACT em conjunto com a AC-Raiz. Para suportá-los, tais entidades precisam manter duas estruturas de dados. A ACT mantêm seu Repositório de Dados de Autenticação, já a AC-Raiz, o Repositório de Selos de Conjunto.

4.4.2.1 Repositório de Dados de Autenticação

Um Repositório de Dados de Autenticação suporta as seguintes operações:

$add(tr, ts)$**:** registra um carimbo do tempo ts, emitido na Rodada tr da ACT, armazenando seu resumo criptográfico $\mathcal{H}(ts)$. A função $\mathcal{H}$ deve ser a mesma usada pelo carimbo sobre a informação datada;

$getSummary(tr) \longrightarrow \{\phi, 0\}$**:** retorna um resumo dos carimbos do tempo emitidos na Rodada tr da ACT, sendo ele o nó raiz ϕ da Árvore de Merkle formada a partir desses carimbos. Se um ou mais carimbos foram emitidos em tr, retorna ϕ, do contrário, 0;

$genAuthData(tr)$**:** gera os Dados de Autenticação da Rodada tr da ACT, formados pelos caminhos de autenticação $\mathcal{A}uth_{ts}$ de cada um dos carimbos emitidos na rodada;

$getAuthData(h) \longrightarrow \{\mathcal{A}uth_{ts}, 0\}$**:** retorna os Dados de Autenticação do carimbo de resumo criptográfico h, sendo tais dados o caminho de autenticação $\mathcal{A}uth_{ts}$ do carimbo. Se existir tal caminho, retorna $\mathcal{A}uth_{ts}$, do contrário, 0;

$remAuthData(tr)$**:** remove os Dados de Autenticação da rodada tr.

4.4.2.2 Repositórios de Selos de Conjunto

Um Repositório de Selos de Conjunto, por sua vez, suporta as operações a seguir:

$add(ar, id_{\mathcal{ACT}}, \phi)$**:** registra uma requisição de Selo de Conjunto recebida na Rodada ar da AC-Raiz;

$sign(ar, \xi, sk_{\mathcal{AC}raiz})$**:** gera os Selos de Conjunto para as requisições recebidas na Rodada ar da AC-Raiz, usando o esquema de assinatura ξ e a chave privada $sk_{\mathcal{AC}raiz}$;

$get(\phi) \longrightarrow \{sl_{\phi}, 0\}$**:** retorna o Selo de Conjunto dos carimbos representados por ϕ. Se existir, retorna sl_{ϕ}, do contrário, 0;

$renewAll(\xi, sk_{\mathcal{AC}raiz})$**:** renova todos os Selos de Conjunto inválidos por meio da renovação de suas assinaturas;

$remove(\mathcal{H})$**:** remove do repositório os registros relacionados a função de resumo criptográfico $\mathcal{H}$.

4.4.2.3 Emissão de Carimbos

Um Carimbo do Tempo Autenticado é emitido segundo uma versão estendida do protocolo tradicional, apresentado no Capítulo 3:

$$\mathcal{U} \longrightarrow \mathcal{ACT} : \mathcal{H}(x)$$
$$\mathcal{ACT} \longrightarrow \mathcal{U} : \underbrace{((\mathcal{H}(x), t), \mathcal{S}ign_{\mathcal{ACT}}((\mathcal{H}(x), t)))}_{ts}, p_a$$

O usuário solicita o carimbo do tempo para uma informação qualquer $x \in \{0,1\}^+$, enviando seu resumo criptográfico $\mathcal{H}(x)$ para a ACT. Ao receber o resumo, tal entidade anexa a data atual t, assina o conjunto e então retorna o carimbo do tempo formado. Diferentemente do tradicional, contudo, a ACT deverá retornar, além do carimbo, o seu Período de Autenticação p_a. Esse é indicado pela ACT por duas datas, uma de início e outra de fim, devendo a primeira coincidir com a de início da próxima Rodada da AC-Raiz quando o Selo de Conjunto correspondente estará disponível. Outra diferença em relação à emissão tradicional está no registro do carimbo emitido. Ao emitir o carimbo do tempo, cabe a ACT registrar seu resumo criptográfico no Repositório de Dados de Autenticação por meio de $rep_{\mathcal{ACT}}.add(tr, ts)$.

4.4.2.4 Autenticação

A autenticação de um carimbo ocorre com a obtenção dos Dados de Autenticação e do Selo de Conjunto correspondente pelo usuário. A geração desse selo, inicia com a solicitação da ACT, como representado a seguir:

$$\mathcal{ACT} \longrightarrow \mathcal{ACR}aiz : ((id_{\mathcal{ACT}}, \phi), \mathcal{S}ign_{\mathcal{ACT}}((id_{\mathcal{ACT}}, \phi)))$$
$$\mathcal{ACR}aiz \longrightarrow \mathcal{ACT} : ok$$

A ACT requisita o Selo de Conjunto enviando o nó Raiz da Árvore de Merkle formada a partir dos carimbos registrados na Rodada e calculado por meio de $rep_{\mathcal{ACT}}.getSummary(tr)$. Ao receber esse nó assinado, juntamente com os dados de identificação da ACT, a AC-Raiz verifica sua procedência e registra a requisição no Repositório de Selos de Conjunto através da operação $rep_{\mathcal{ACR}aiz}.add(ar, id_{\mathcal{ACT}}, \phi)$. Essa dará origem ao Selo de Conjunto correspondente apenas no fim da Rodada da AC-Raiz.

Chegado o momento, a AC-Raiz gera esse Selo por meio de $rep_{\mathcal{ACR}aiz}.sign(ar_i, \xi, sk_{\mathcal{AC}raiz})$. A ACT, por sua vez, gera os Dados de Autenticação do carimbo, usando $rep_{\mathcal{ACT}}.genAuthData(tr_j)$. Finalmente, com a publicação dessas informações, tem início o Período de Autenticação. Os Dados de Autenticação podem ser obtidos por meio do seguinte protocolo:

$$\mathcal{U} \longrightarrow \mathcal{ACT} : \mathcal{H}(ts)$$
$$\mathcal{ACT} \longrightarrow \mathcal{U} : \mathcal{A}uth_{ts}$$

O usuário solicita os Dados de Autenticação do carimbo enviando o seu resumo criptográfico $\mathcal{H}(ts)$ para a ACT, onde $\mathcal{H}$ deve ser a mesma função usada pelo carimbo sobre a informação datada. Ao receber o resumo, a ACT consulta seu Repositório de Dados de Autenticação por meio de $rep_{\mathcal{ACT}}.getAuthData(\mathcal{H}(ts))$ e, existindo tais Dados, retorna-os para o usuário.

O Selo de Conjunto, por sua vez, pode ser obtido através do protocolo abaixo:

$$\mathcal{U} \longrightarrow \mathcal{ACR}aiz : \phi$$
$$\mathcal{ACR}aiz \longrightarrow \mathcal{U} : \underbrace{((id_{\mathcal{ACT}}, \phi), \mathcal{S}ign_{\mathcal{ACR}aiz}((id_{\mathcal{ACT}}, \phi)))}_{sl_{\phi}}$$

O usuário solicita o Selo de Conjunto do carimbo, enviando o resumo criptográfico que representa os carimbos emitidos na mesma rodada da ACT. Tal resumo é calculado a partir dos Dados de Autenticação, sendo o nó raiz da Árvore de Merkle que contêm esses Dados. Uma vez recebido pela AC-Raiz, ela busca o Selo no Repositório de Selos de Conjunto através de $rep_{\mathcal{ACR}aiz}.get(\phi)$. Existindo o Selo requisitado, esse é retornado para o usuário.

Finalmente, com o término do Período de Autenticação, ocorre a destruição dos Dados de Autenticação pela ACT. Para tanto é usada a operação $rep_{\mathcal{ACT}}.remAuthData(tr_j)$.

4.4.2.5 Renovação

A renovação de um carimbo pode ser realizada por meio do seguinte protocolo:

$$\mathcal{U} \longrightarrow \mathcal{ACR}aiz : \phi$$
$$\mathcal{ACR}aiz \longrightarrow \mathcal{U} : sl'_{\phi}$$

Quando o usuário não puder mais comprovar a autenticidade do carimbo, devido a perda da validade do Selo de Conjunto, ele pode solicitar sua renovação enviando o resumo criptográfico que representa os carimbos emitidos na mesma rodada da ACT. Uma vez recebido pela AC-Raiz, ela consulta seu Repositório de Selos de Conjunto por meio de $rep_{\mathcal{ACR}aiz}.get(\phi)$ e, existindo um Selo válido, retorna-o para o usuário.

Tais Selos são reassinados, através da operação $rep_{\mathcal{ACR}aiz}.renewAll(\xi, sk_{\mathcal{AC}raiz})$, assim que a AC-Raiz se recupera dos problemas que levaram os anteriores a perderem sua validade. Por exemplo, se sua chave privada foi comprometida e, consequentemente, seu certificado foi revogado, um novo certificado para um novo par de chaves deverá ter sido criado. Assim, cabe a AC-Raiz manter seus

Selos de Conjunto válidos, reassinando-os por meio de novos certificados ou esquemas de assinatura.

De maneira semelhante aos Carimbos do Tempo Renováveis, renovações são negadas em duas situações principais. A primeira ocorre quando a função de resumo criptográfico usada no carimbo sobre a informação datada não é mais resistente à segunda inversão. Com a perda dessa resistência o carimbo acaba perdendo sua serventia, uma vez que não é mais possível comprovar a integridade da informação datada. Além disso, o próprio registro no Repositório de Selos de Conjunto perde sua utilidade. A segunda situação se dá quando a AC-Raiz perdeu sua capacidade de renovar o Selo de Conjunto. Isso ocorre, geralmente, com o término prematuro das operações da AC-Raiz, ou quando o Repositório de Selos de Conjunto é comprometido de maneira irreversível.

4.4.2.6 Otimização do Repositório de Selos de Conjunto

Por fim, de modo a limitar os custos relacionados à autenticação e renovação dos carimbos ocorre periodicamente a otimização do Repositório de Selos de Conjunto. Quando alguma função de resumo criptográfico perde sua resistência à segunda inversão, cabe a AC-Raiz remover os registros relacionados desse Repositório por meio de $rep_{\mathcal{AC}Raiz}.remove(\mathcal{H})$.

4.4.3 Operações do Carimbo

As operações disponíveis ao usuário final são, portanto:

Solicitação: permite a obtenção do carimbo. Segue o protocolo descrito na Seção 4.4.2.3;

Autenticação: possibilita a autenticação do carimbo, substituindo as informações necessárias à verificação de sua autenticidade, como certificados e dados de revogação, por um Selo de Autenticidade. Tal selo deve ser obtido, durante o Período de Autenticação do carimbo, por meio dos protocolos de solicitação do Selo de Conjunto e dos Dados de Autenticação, apresentados na Seção 4.4.2.4;

Validação: permite a validação do carimbo. Segue os passos tradicionais descritos no Capítulo 3, com exceção da verificação de sua autenticidade. Ao invés de validar a assinatura do carimbo, deve-se validar o seu Selo de Autenticidade;

Renovação: possibilita restabelecer a validade do Selo de Conjunto, presente no Selo de Autenticidade, quando esse não for mais válido. Segue o protocolo descrito na Seção 4.4.2.5.

Um Selo de Autenticidade, por sua vez, é válido quando:

- a assinatura da AC-Raiz, no Selo de Conjunto, for válida;
- o caminho de autenticação do carimbo, que forma seus Dados de Autenticação, for válido.

4.4.4 Preservação de Assinaturas

A preservação de uma assinatura, por meio de Carimbos do Tempo Autenticados, apresenta algumas diferenças em relação àquela com carimbos tradicionais. O agendamento da adição de um novo carimbo passa a ser orientado não mais pela expiração do certificado da ACT, mas pela segurança da função de resumo criptográfico usada pelo carimbo sobre a informação datada. Além disso, após a adição de um carimbo, ocorre a substituição das informações necessárias à validação de sua assinatura, pelo seu Selo de Autenticidade.

Em maiores detalhes, sendo s, d, $\mathcal{C}_s$ e $\mathcal{R}_s$, respectivamente, a assinatura, o documento assinado, os certificados do caminho de certificação do signatário e os dados de revogação relacionados, a preservação de s segue os seguintes passos:

1. adiciona-se um carimbo do tempo ts^1 sobre $(s, d, \mathcal{C}_s, \mathcal{R}_s)$, sendo $\mathcal{R}_s$ dados de revogação atuais. Como resultado, obtêm-se ((s, d, $\mathcal{C}_s$, $\mathcal{R}_s$), ts^1, $\mathcal{C}^1_{ts}$);

2. durante o Período de Autenticação, autentica-se o carimbo, obtendo ((s, d, $\mathcal{C}_s$, $\mathcal{R}_s$), ts^1, sl^1_{ts}) e então agenda-se a adição do próximo carimbo do tempo com base na segurança da função de resumo criptográfico usada por ts^1 sobre a informação datada. Tal agendamento pode ser revisto ao longo do tempo, conforme novas informações sobre essa função se tornem disponíveis;

3. no momento agendado, valida-se ts^1. Se inválido, tal carimbo deverá ser renovado. Sendo ts^1 o carimbo do tempo em questão, possivelmente renovado, adiciona-se ts^2 sobre ((s, d, $\mathcal{C}_s$, $\mathcal{R}_s$), ts^1, sl^1_{ts}) obtendo (((s, d, $\mathcal{C}_s$, $\mathcal{R}_s$), ts^1, sl^1_{ts}), ts^2, $\mathcal{C}^2_{ts}$). Caso ts^1 já tenha perdido sua validade, e sua renovação não seja possível, a preservação falha;

4. para os próximos carimbos, repete-se os passos 2 e 3 enquanto for necessário preservar a validade da assinatura. Dessa forma, na adição do n-ésimo carimbo, obtêm-se ((...((((s, d, $\mathcal{C}_s$, $\mathcal{R}_s$), ts^1, sl^1_{ts}), ts^2, sl^2_{ts}), ...), ts^n, $\mathcal{C}^n_{ts}$).

4.4.5 Validação de Assinaturas

Assinaturas preservadas por meio de Carimbos do Tempo Autenticados são validadas de maneira semelhante àquelas preservadas através de carimbos tradicionais. A diferença está, essencialmente, em comprovar a

autenticidade de cada carimbo por meio de seu Selo de Autenticidade ao invés da sua assinatura. Sendo ((...(((s, d, $\mathcal{C}_s$, $\mathcal{R}_s$), ts^1, sl^1_{ts}), ts^2, sl^2_{ts}), ...), ts^n, $\mathcal{C}^n_{ts}$) ou ((...(((s, d, $\mathcal{C}_s$, $\mathcal{R}_s$), ts^1, sl^1_{ts}), ts^2, sl^2_{ts}), ...), ts^n, sl^n_{ts}) a assinatura preservada, ela é válida se:

1. o carimbo do tempo ts^n for atualmente válido. Se ainda não autenticado, pode-se, primeiramente, autenticá-lo. Caso já tenha sido, pode ser preciso renovar o carimbo;

2. para todo ts_i, com $1 \leq i \leq n-1$, ts^i era válido na data indicada por ts_{i+1}. Na verificação da autenticidade dos carimbos seus Selos de Autenticidade devem ser validados;

3. a assinatura s era válida na data indicada por ts^1.

4.5 CONCLUSÃO

Neste capítulo foram analisados alguns dos problemas relacionados à preservação por carimbos do tempo e propostos protocolos criptográficos para reduzir os custos e aumentar a confiabilidade dessa preservação. Como visto, tais problemas estão relacionados a fatores como a frequência com que novos carimbos são adicionados e a perda inesperada da validade desses carimbos. Assim, os protocolos propostos buscaram tanto estender o tempo de vida dos carimbos como tornar esse tempo mais previsível.

Esses deram origem a duas novas implementações de carimbos do tempo, os Carimbos do Tempo Renováveis e os Carimbos do Tempo Autenticados. Carimbos do Tempo Renováveis são carimbos que suportam além das operações tradicionais, a operação de renovação. Por meio dela, é possível restabelecer a validade da assinatura do carimbo, quando essa não for mais válida, desvinculando sua validade da assinatura. A preservação por meio desses carimbos varia, portanto, no uso dessa operação.

Carimbos do Tempo Autenticados, por sua vez, suportam duas operações adicionais, a de renovação e de autenticação. A primeira, assim como a dos Carimbos do Tempo Renováveis, busca prolongar a validade do carimbo. A segunda, busca reduzir os custos relacionados à verificação de sua autenticidade. Para tanto, são substituídas informações como certificados e dados de revogação por um Selo de Autenticidade, formado pelo Selo de Conjunto publicado pela AC-Raiz, e os Dados de Autenticação publicados pela ACT. Da mesma forma, a preservação de assinaturas por meio desses carimbos varia no uso das operações de renovação e autenticação no decorrer do processo.

5 AVALIAÇÃO

5.1 INTRODUÇÃO

Os protocolos criptográficos propostos no Capítulo 4 deram origem a duas novas implementações de carimbos do tempo, os Carimbos do Tempo Renováveis e Carimbos do Tempo Autenticados. Tais protocolos têm por objetivo aumentar a confiabilidade do processo de preservação bem como reduzir os custos desse processo para o usuário final. Em contrapartida, o suporte a eles implica, principalmente, em custos adicionais para a Autoridade de Carimbo do Tempo (ACT) e Autoridade Certificadora Raiz (AC-Raiz).

Neste capítulo são avaliados os principais benefícios e limitações trazidos pelos Carimbos do Tempo Renováveis e Carimbos do Tempo Autenticados. Para tanto, foram realizadas análises teóricas, cujos resultados foram então confirmados por meio de testes e simulações. Para tais experimentos foram criados, além de protótipos, modelos matemáticos representando alguns dos principais aspectos relacionados. Os protótipos, por sua vez, implementam os módulos ASN.1, apresentados no Anexo A, que especificam os protocolos propostos. Outras especificações, contudo, são igualmente possíveis.

Assim, na Seção 5.2 são avaliados os benefícios trazidos pelos Carimbos do Tempo Renováveis e Carimbos do Tempo Autenticados. A Seção 5.3, por sua vez, apresenta os custos de operação desses protocolos, tanto para a ACT quanto para a AC-Raiz. Na Seção 5.4 é então avaliada a compatibilidade das assinaturas preservadas por meio desses carimbos com a base instalada. Finalmente a Seção 5.5 conclui o capítulo.

5.2 BENEFÍCIOS

Os principais benefícios trazidos pelos Carimbos do Tempo Renováveis e Carimbos do Tempo Autenticados são a redução nos custos de preservação para o usuário final, e o aumento na confiabilidade desse processo. Além desses ainda existem outros benefícios como a possibilidade de validação *off-line* das assinaturas preservadas.

5.2.1 Redução de Custos

A redução de custos oferecida pelos Carimbos do Tempo Renováveis e Carimbos do Tempo Autenticados tem sua origem na diferença entre os prazo de validade desses carimbos e dos tradicionais. Como visto no Capítulo 3, nos tradicionais esse prazo termina na expiração do certificado da ACT. Nos carimbos propostos, por outro lado, isso ocorre no

enfraquecimento da função de resumo criptográfico usada pelo carimbo. Particularmente, na perda de sua resistência à segunda inversão.

Esse prazo de validade diferenciado para os Carimbos do Tempo Renováveis e Carimbos do Tempo Autenticados decorre da possibilidade de renová-los com o tempo. Por meio dessas renovações, é possível recuperá-los de praticamente todos os fatores que tradicionalmente limitariam o seu prazo de validade. A única exceção está nessa perda da resistência à segunda inversão, quando não é mais possível identificar qual informação foi, de fato, datada.

Dessa forma, a redução de custos ocorre, pois o tempo até o enfraquecimento da função de resumo criptográfico é geralmente maior que aquele até a expiração do certificado da ACT. Enquanto tais funções costumam se manter seguras por mais de 10 anos(ETSI, 2007; BARKER; ROGINSKY, 2010; PRENEEL, 2010), instituições como o NIST(BARKER et al., 2007) e a IETF(PINKAS; POPE; ROSS, 2003) recomendam que tais certificados durem um tempo menor. O NIST, por exemplo, recomenda que tenham um prazo de validade de, no máximo, 3 anos, de modo a limitar problemas como aqueles causados por um eventual comprometimento da chave privada da ACT.

Por terem um tempo de vida maior, Carimbos do Tempo Renováveis e Carimbos do Tempo Autenticados precisam ser sobrepostos menos frequentemente, reduzindo o número de carimbos do tempo necessários num mesmo período de preservação. Com um número menor de carimbos, o espaço necessário para armazenar a assinatura preservada é reduzido, assim como o esforço computacional para a validação da assinatura.

Carimbos do Tempo Autenticados ainda são capazes de oferecer uma redução mais acentuada nos custos, pois além do prazo de validade maior, têm as informações necessárias a sua validação, como os certificados e dados de revogação, substituídas por Selos de Autenticidade. Tais selos, formados pelo Selo de Conjunto e os Dados de Autenticação relacionados, tendem a requerer tanto um espaço de armazenamento, quanto um tempo para sua validação, menores. Isso se deve, particularmente, a remoção das LCRs da validação de um carimbo, pois o armazenamento e obtenção dessas informações tendem a ser os maiores responsáveis por esses custos.

Selos de Autenticidade, contudo, podem extrapolar o tamanho das informações tradicionalmente necessárias à verificação da autenticidade de um carimbo. O tamanho desses selos é influenciado, particularmente, pelo número de carimbos do tempo emitidos na Rodada correspondente da ACT. Quanto maior, maior o caminho de autenticação que compõe os Dados de Autenticação do carimbo e, consequentemente, maior o Selo de Autenticidade. A dificuldade disso ocorrer está fundamentada, principalmente, no fato desses caminhos de autenticação crescerem logaritmicamente com o número de carimbos do tempo emitidos. Além disso, é possível regular esse número reduzindo a duração das rodadas.

$$\theta_{\mathcal{U}}(p_p) = \sum_{i=1}^{n_{p_p}} (\alpha(ts^i) + \alpha(\mathcal{C}_{ts}^i)) + \sum_{i=1}^{n_{p_p}-1} \alpha(\mathcal{R}_{ts}^i))$$

$$n_{p_p} = \left\lceil \frac{p_p}{0,5.\overline{p}_{\mathcal{ACT}}} \right\rceil$$

Variável	Descrição
$\theta_{\mathcal{U}}(p_p)$	custo de armazenamento ao fim de um período de tempo p_p
n_{p_p}	número de carimbos adicionados no período p_p
$\alpha(x)$	custo de armazenamento de x
ts^i	i-ésimo carimbo adicionado
$\mathcal{C}_{ts}^i$	caminho de certificação relacionado ao carimbo ts^i
$\mathcal{R}_{ts}^i$	dados de revogação relacionadas ao carimbo ts^i
$\overline{p}_{\mathcal{ACT}}$	prazo de validade médio de um certificado de ACT

Tabela 5.1: Função representando os custos de armazenamento para o usuário na preservação tradicional.

5.2.1.1 Simulações

De modo a confirmar alguns dos resultados da análise teórica foram realizadas simulações e testes com protótipos. Nesses experimentos foram considerados valores de uma Infraestrutura de Chaves Públicas (ICP) típica, bem como modelos matemáticos criados para representar os custos de armazenamento relacionados ao processo de preservação. O primeiro desses modelos é apresentado na tabela 5.1.

Tal função reflete as informações armazenadas durante o processo de preservação por carimbos tradicionais, descrito no Capítulo 3, Seção 3.2.2. Assim, o custo de armazenamento após um certo período de preservação é dado pelo espaço necessário para cada carimbo adicionado, bem como para as informações necessárias a sua validação. Para todos os carimbos, com exceção do último, são armazenados tanto o caminho de certificação quanto os dados de revogação necessários a validação desse caminho. Para o último carimbo não são armazenados os dados de revogação pois esses são obtidos durante a validação da assinatura preservada.

$$\theta_{\mathcal{U}}(p_p) = \sum_{i=1}^{n_{p_p}} (\alpha(ts^i) + \alpha(sl_{ts}^i))$$

$$n_{p_p} = \left\lceil \frac{p_p}{0,5.\overline{p}_{\mathcal{H}}} \right\rceil$$

$$\alpha(sl_{ts}^i) = \alpha(\mathcal{A}uth_{ts}^i) + \alpha(sl_{\phi}^i)$$

Variável	Descrição
sl_{ts}^i	selo de autenticidade relacionado ao carimbo ts^i
$\mathcal{A}uth_{ts}^i$	caminho de autenticação do i-ésimo carimbo
sl_{ϕ}^i	selo de conjunto do i-ésimo carimbo

Tabela 5.2: Função representando os custos de armazenamento para o usuário na preservação por Carimbos do Tempo Autenticados.

O número de carimbos do tempo adicionados no período, por sua vez, é dado pelo período de preservação divido pelo tempo de vida médio dos carimbos adicionados, considerado $0,5.\overline{p}_{\mathcal{ACT}}$. Nesse caso, assume-se que carimbos do tempo serão obtidos tanto próximo do início desse prazo de validade da ACT, quanto próximo do fim.

Os custos de preservação por meio de Carimbos do Tempo Renováveis, decorrentes do processo de preservação descrito no Capítulo 4, Seção 4.3.3, podem ser representados pela mesma função, exceto no que diz respeito ao cálculo do número de carimbos do tempo adicionados. Nesse caso, ao invés de se considerar o prazo de validade médio de um certificado de ACT, considera-se o tempo médio $\overline{p}_{\mathcal{H}}$ pelo qual funções de resumo criptográfico se mantêm seguras, particularmente, resistentes à segunda inversão. Assim, o tempo de vida médio de um Carimbo do Tempo Renovável é dado por $0,5.\overline{p}_{\mathcal{H}}$, igualmente, assumindo-se que carimbos do tempo serão obtidos tanto próximo do início desse período, quanto próximo do fim.

Por último, a função apresentada na tabela 5.2 reflete as informações armazenadas durante o processo de preservação por meio de Carimbos do Tempo Autenticados, descrito no Capítulo 4, Seção 4.4.4.

Nesse caso, o custo de armazenamento após um certo período de

Variável	Valor
$\alpha(ts^i)$	700 *bytes*
$\alpha(\mathcal{C}_{ts}^i)$	3700 *bytes*
$\alpha(\mathcal{R}_{ts}^i)$	111600 *bytes*
$\overline{p}_{\mathcal{ACT}}$	3 anos
$\overline{p}_{\mathcal{H}}$	10 anos
$\alpha(\mathcal{A}uth_{ts}^i)$	380 *bytes*
$\alpha(sl_{\phi}^i)$	700 *bytes*

Tabela 5.3: Valores para simulação dos custos de preservação durante 50 anos.

preservação é dado pelo espaço necessário para cada carimbo, bem como para seu Selo de Autenticidade. Cada Selo de Autenticidade compreende os Dados de Autenticação e o Selo de Conjunto relacionado ao carimbo. O tempo de vida médio de um carimbo, por sua vez, é calculado da mesma forma que nos Carimbos do Tempo Renováveis.

Finalmente, para as simulações foram usados os valores da tabela 5.3, relacionados a uma ICP típica. Como alguns desses valores crescem com o tempo, assume-se que sejam os valores médios encontrados durante o período de preservação, considerando que tenha começado no passado e que continue no futuro.

Tais valores refletem aqueles comumente encontrados, levando em consideração recomendações técnicas e medições realizadas com os protótipos implementados. O espaço de armazenamento necessário para os carimbos, caminhos de certificação e dados de revogação relacionados, por exemplo, considera valores médios segundo amostras da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e *VeriSign*. O prazo de validade dos certificados de ACT, por sua vez, é o tempo máximo citado por recomendações técnicas como a do NIST(BARKER et al., 2007), sendo, igualmente, aquele usado na ICP-Brasil.

O tempo pelo qual funções de resumo criptográfico se mantêm seguras considera o passado e futuro das principais funções de resumo criptográfico até então publicadas(ETSI, 2007; BARKER; ROGINSKY, 2010; PRENEEL, 2010). Acredita-se ainda que esse período seja conservador no caso dos protocolos criptográficos propostos, pois esses são vulneráveis apenas a quebra da resistência a segunda inversão, algo que tende a ocorrer certo tempo após as funções serem consideradas inseguras. Considerando ataques de força bruta, por exemplo, a quebra da resistência à colisão, que já tornaria a função insegura, requer o cálculo de $2^{n/2}$ resumos criptográficos, sendo n o número de *bits* do resumo. A quebra da resistência à segunda inversão, por outro lado, requer 2^n operações(MENEZES; OORSCHOT; VANSTONE, 1997).

Por fim, os valores relacionados aos Selos de Autenticidade foram obtidos de selos gerados por meio do protótipo para a emissão de Ca-

rimbos do Tempo Autenticados. Nesse caso, foi considerado o cenário de operação apresentado na Seção 5.3, onde uma Rodada da ACT dura 7 dias, sendo que, durante cada rodada, a ACT emite um carimbo do tempo por segundo, continuamente.

A figura 5.1 apresenta o resultado das simulações envolvendo a preservação de uma assinatura, ao longo de 50 anos, por meio de carimbos do tempo tradicionais, Carimbos do Tempo Renováveis e Carimbos do Tempo Autenticados.

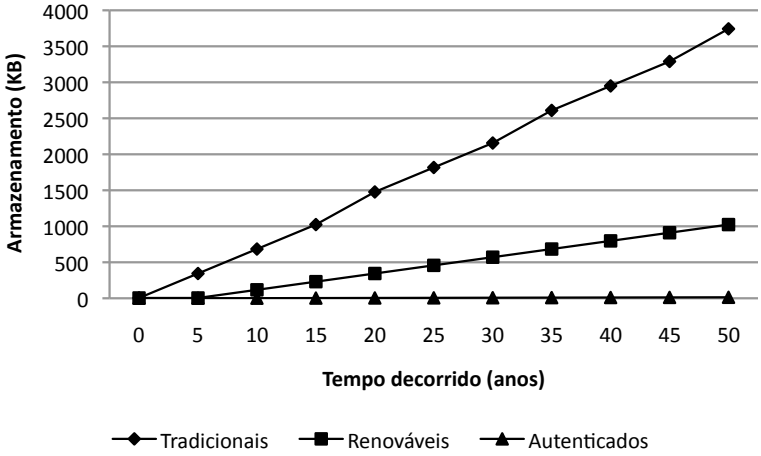

Figura 5.1: Simulação dos custos de preservação durante 50 anos.

Ao fim de 50 anos, o *overhead* relacionado à preservação da assinatura por meio de carimbos do tempo tradicionais atinge 3.742,57 KB. Na preservação por Carimbos do Tempo Renováveis, por sua vez, esses custos foram de 1023,82 KB, uma redução de 72,64%. Finalmente, por meio de Carimbos do Tempo Autenticados, esse *overhead* foi 99,58% menor, alcançando 15,42 KB. No caso dos Carimbos do Tempo Autenticados, a maior contribuição para essa redução diz respeito ao tamanho dos Selos de Autenticidade, quando comparados às informações tradicionalmente necessárias para verificar a autenticidade de um carimbo, aqueles são 99,23% menores.

Como a validação com Carimbos do Tempo Autenticados não requer a obtenção de dados de revogação, uma operação em geral custosa, foram ainda realizados testes envolvendo o tempo necessário para validá-los. Esse foi, em geral, mais de 50 vezes inferior ao tempo para validação de carimbos do tempo tradicionais, considerando uma ICP típica e conexão de 1 *Mbps*.

5.2.2 Aumento na Confiabilidade

O aumento na confiabilidade oferecido pelos Carimbos do Tempo Renováveis e Carimbos do Tempo Autenticados tem sua origem na diferença entre o conjunto de fatores que levam esses carimbos e os tradicionais a perderem sua validade antes do previsto. Como visto no Capítulo 3, nos tradicionais esse conjunto é formado pela revogação de algum certificado do caminho de certificação, dos dados da âncora de confiança, ou da quebra repentina de algum algoritmo criptográfico usado nos certificados, dados de revogação ou no carimbo. Nos carimbos propostos, por outro lado, apenas dois desses problemas podem levar tais carimbos a perderem sua validade de maneira imprevisível.

Isso se dá pois Carimbos do Tempo Renováveis e Carimbos do Tempo Autenticados são capazes de tolerar praticamente todos esses problemas. No caso dos Carimbos do Tempo Renováveis, quando ocorre a revogação de algum certificado do caminho de certificação, dos dados da âncora de confiança ou a quebra repentina de algum algoritmo criptográfico usado nos certificados, dados de revogação ou no carimbo, basta renovar o carimbo para sua validade ser restabelecida. Existem, contudo, duas exceções. A primeira ocorre quando o certificado revogado é o da ACT, e tal revogação foi motivada pelo comprometimento irreversível do Repositório de Carimbos do Tempo. A segunda exceção, por sua vez, ocorre quando o algoritmo criptográfico em questão é a função de resumo criptográfico usada no carimbo sobre a informação datada.

No caso dos Carimbos do Tempo Autenticados, a maioria desses problemas já é anulada na própria autenticação do carimbo. Das revogações fica restando apenas a revogação da AC-Raiz. Dos algoritmos criptográficos, sobram a quebra repentina dos algoritmos usados pela AC-Raiz e da função de resumo criptográfico usada no carimbo sobre a informação datada. Alguns desses problemas, todavia, são tolerados pela renovação do Selo de Conjunto, existindo, igualmente, duas exceções. A primeira ocorre quando o certificado da AC-Raiz é revogado devido ao comprometimento irreversível do Repositório de Selos de Conjunto. A segunda exceção, por sua vez, ocorre na quebra da função de resumo criptográfico usada no carimbo.

Por comprometimento irreversível desses Repositórios entende-se o comprometimento da sua integridade de um modo que não possa ser restaurada. Tal restauração é viabilizada, por exemplo, por meio de cópias *offline* desses repositórios, realizadas periodicamente. Mesmo seguindo esse procedimento, contudo, existiriam momentos onde a restauração de todos ou parte dos registros não seria possível. Esse é o caso, por exemplo, de registros recentes, ainda não protegidos, que seriam perdidos no comprometimento.

Dessa forma o aumento na confiabilidade ocorre pois o conjunto de fatores que podem levar os carimbos propostos a perderem sua validade antes do previsto é reduzido. Sendo menor, são maiores as chances de se prever corretamente o momento em que o carimbo do tempo deverá

ser sobreposto e, assim, conseguir realizar tal sobreposição antes de sua validade ser perdida. Como visto no Capítulo 3, quando há erro nessa previsão e um carimbo do tempo perde sua validade antes de ser sobreposto por outro, a preservação falha.

5.2.3 Outros

Além da redução de custos e do aumento na confiabilidade providos pelos protocolos criptográficos propostos, esses ainda oferecem outros benefícios. Carimbos do Tempo Autenticados, por exemplo, possibilitam a validação *offline* de assinaturas preservadas, possibilitando seu uso em dispositivos sem conexão de rede. Tradicionalmente, tal conexão é necessária para possibilitar a obtenção de dados de revogação. Nos Carimbos do Tempo Autenticados ela se torna dispensável pois a validação desses carimbos prescinde desses dados, envolvendo apenas a validação da assinatura da AC-Raiz e comparações entre resumos criptográficos.

Tanto os Carimbos do Tempo Autenticados quanto os Carimbos do Tempo Renováveis ainda permitem melhorias nos serviços oferecidos por instituições arquivísticas. Tais instituições, geralmente responsáveis por preservar documentos eletrônicos de outras entidades(BLAZIC; SETCCE, 2007; TRONCOSO; COCK; PRENEEL, 2008; ZIMMER; LANGKABEL; HENTRICH, 2008; HUHNLEIN et al., 2010), podem oferecer uma garantia maior quanto à preservação da autenticidade desses documentos, uma vez que ambos os carimbos tornam mais confiável o processo de preservação de assinaturas digitais.

Por fim, como os protocolos criptográficos propostos se concentram, particularmente, em novas implementações de carimbos do tempo, esses ainda podem beneficiar outras áreas, além da preservação por longo prazo de assinaturas, onde tais carimbos são necessários. São exemplos dessas áreas a proteção da propriedade intelectual, o comércio e votação eletrônicos.

5.3 CUSTOS DE OPERAÇÃO

Em contrapartida aos benefícios trazidos pelos Carimbos do Tempo Renováveis e Carimbos do Tempo Autenticados existem, particularmente, custos adicionais a serem absorvidos pela ACT e AC-Raiz. Uma ACT que suporte a emissão de Carimbos do Tempo Renováveis, por exemplo, terá custos adicionais relacionados, principalmente, à manutenção do Repositório de Carimbos do Tempo. Tais custos são representados pela função da tabela 5.4.

Tal função representa as informações armazenadas durante as operações da ACT, descritas no Capítulo 4, Seção 4.3.3, desconsiderando otimizações do Repositório de Carimbos do Tempo. Assim, após certo período de operação, esse custo é dado pelo espaço necessário para o armazenamento dos resumos criptográficos de todos os carimbos emiti-

$$\theta_{\mathcal{ACT}}(p_o) = \sum_{i=0}^{n_{ts}^{po}} \alpha(h_{ts}^i)$$

Variável	Descrição
$\theta_{\mathcal{ACT}}(p_o)$	custo de armazenamento ao final de um período de operação p_o
$n_{ts}^{p_p}$	número de carimbos do tempo emitidos
h_{ts}^i	resumo criptográfico do i-ésimo carimbo emitido
$\alpha(x)$	custo de armazenamento de x

Tabela 5.4: Função representando os custos de armazenamento para a ACT no suporte a Carimbos do Tempo Renováveis.

dos até então. O tamanho de cada registro, por sua vez, pode variar dependendo de quantas funções de resumo criptográfico sejam suportadas pela ACT. Quando a otimização do Repositório de Carimbos do Tempo é implementada, registros antigos dão lugar aos novos conforme novas funções de resumo criptográfico sejam adotadas e funções já inseguras, abandonadas.

Uma ACT que suporte a emissão de Carimbos do Tempo Autenticados, por sua vez, terá custos adicionais relacionados, principalmente, à publicação dos Dados de Autenticação de cada rodada da ACT. Nesse caso, merecem destaque tanto os custos de armazenamento desses dados quanto os custos de memória e processamento relacionados a sua geração. Os primeiros são representados na função da tabela 5.5

Tal função representa os custos de armazenamento durante as operações da ACT, descritas no Capítulo 4, Seção 4.4.4. Dessa forma, após certo período de operação, esse custo é dado pelo espaço necessário para os Dados de Autenticação de rodadas anteriores, em Período de Autenticação, somado aos custos de armazenamento dos resumos criptográficos de cada carimbo do tempo até então emitido na rodada atual.

Os custos de memória e processamento necessários a geração dos Dados de Autenticação, por sua vez, dependem principalmente do algoritmo usado para a travessia da Árvore de Merkle. Vários algoritmos já foram propostos para tal(SZYDLO, 2004; BERMAN; KARPINSKI; NEKRICH, 2007; BUCHMANN; DAHMEN; SCHNEIDER, 2008). No de Szydlo (2004), por exemplo, a geração de cada caminho de autenticação requer o cálculo de no máximo $2log_2(n)$ resumos criptográficos, e o armazenamento de menos de $3log_2(n)$ resumos em memória, onde n é o número de carimbos do tempo emitidos na rodada.

$$\theta_{\mathcal{ACT}}(p_o) = \sum_{i=tr-n_{otr}}^{tr-1} (\sum_{j=1}^{n_{ts}^i} \alpha(\mathcal{A}uth_{ts}^{i,j})) + \sum_{i=0}^{n_{ts}^{tr}} \alpha(h_{ts}^i)$$

$$tr = \left\lceil \frac{p_o}{p_{tr}} \right\rceil$$

$$n_{otr} = tr - \frac{tr - n_{tr}^{p_a} + |tr - n_{tr}^{p_a}|}{2}$$

Variável	Descrição
$\theta_{\mathcal{ACT}}(p_o)$	custo de armazenamento ao final de um período de operação p_o
tr	rodada atual da ACT
n_{otr}	número de rodadas em Período de Autenticação
n_{ts}^i	número de carimbos emitidos na i-ésima rodada
$\alpha(x)$	custo de armazenamento de x
$\mathcal{A}uth_{ts}^{i,j}$	Dados de Autenticação do j-ésimo carimbo emitido na i-ésima rodada
n_{ts}^{tr}	número de carimbos emitidos na rodada atual
h_{ts}^i	resumo criptográfico do i-ésimo carimbo emitido na rodada atual
p_{tr}	duração de uma rodada
$n_{tr}^{p_a}$	número de rodadas de um Período de Autenticação

Tabela 5.5: Função representando os custos de armazenamento para a ACT no suporte a Carimbos do Tempo Autenticados.

$$\theta_{\mathcal{ACR}aiz}(p_o) = \sum_{i=0}^{ar}(\sum_{j=1}^{n^i_{\mathcal{ACT}}} \alpha(sl^{i,j}_{\phi})) + \sum_{i=0}^{n^{ar}_{\phi}} \alpha(\phi^i)$$

$$ar = \left\lceil \frac{p_o}{p_{ar}} \right\rceil$$

Variável	Descrição
$\theta_{\mathcal{ACR}aiz}(p_o)$	custo de armazenamento ao final de um período de operação p_o
ar	rodada atual da AC-Raiz
$n^i_{\mathcal{ACT}}$	número de ACTs em operação na i-ésima rodada
$\alpha(x)$	custo de armazenamento de x
$sl^{i,j}_{\phi}$	Selo de Conjunto emitido para a j-ésima ACT requisitante na i-ésima rodada
n^{ar}_{ϕ}	número de requisições recebidas na rodada atual
ϕ^i	i-ésima requisição recebida na rodada atual

Tabela 5.6: Função representando os custos de armazenamento para a AC-Raiz no suporte a Carimbos do Tempo Autenticados.

Para a AC-Raiz os custos desse suporte a emissão de Carimbos do Tempo Autenticados estão relacionados principalmente a manutenção do Repositório de Selos de Conjunto. Tais custos são representados na função da tabela 5.6.

Essa função representa as informações armazenadas durante as operações da AC-Raiz, descritas no Capítulo 4, Seção 4.4.4, desconsiderando otimizações do Repositório de Selos de Conjunto. Assim, após certo período de operação, esse custo é dado pelo espaço necessário a cada um dos Selos de Conjunto emitidos somado ao custo de armazenamento das requisições até então recebidas na rodada atual. Os Selos de Conjunto emitidos a cada rodada, refletem o número de ACTs em operação, que requisitaram seus Selos. Quando a otimização do Repositório de Selos de Conjunto é implementada, registros antigos dão lugar aos novos conforme novas funções de resumo criptográfico sejam adotadas e funções já inseguras, abandonadas.

Variável	Valor
$n_{ts}^{p_o}$	315.360.000 carimbos
$\alpha(h_{ts}^{i})$	20 bytes
n_{ts}^{i}, n_{ts}^{tr}	604.800 carimbos
$\alpha(\mathcal{A}uth_{ts}^{i,j})$	380 bytes
p_{tr}	7 dias
$n_{tr}^{p_a}$	4 rodadas
$n_{\mathcal{ACT}}^{i}$	100 ACTs
$\alpha(sl_{\phi}^{i,j})$	500 bytes
n_{ϕ}^{ar}	0 requisições
$\alpha(\phi^{i})$	20 bytes

Tabela 5.7: Valores para simulação dos custos de operação durante 10 anos.

5.3.1 Simulações

De modo a clarificar alguns dos custos analisados foram simuladas as operações da ACT e AC-Raiz ao longo de 10 anos. Para tais simulações foram considerados valores de uma Infraestrutura de Chaves Públicas (ICP) típica, descrita na tabela 5.7. Tais valores refletem aqueles comumente encontrados, levando em consideração recomendações técnicas e medições realizadas com os protótipos implementados.

O número de carimbos do tempo emitidos ao longo desses 10 anos, no caso dos Carimbos do Tempo Renováveis, e em cada rodada, no caso dos Carimbos do Tempo Autenticados refletem um cenário em que a ACT emite um carimbo por segundo durante toda sua operação. O valores relacionados aos Selos de Autenticidade, por sua vez, foram obtidos de selos gerados por meio de um protótipo para a emissão de Carimbos do Tempo Autenticados.

A figura 5.2 apresenta o resultado das simulações. No caso do suporte a emissão de Carimbos do Tempo Autenticados são considerados tanto os custos de armazenamento para a ACT quanto para a AC-Raiz.

Ao fim de 10 anos os custos de armazenamento para uma ACT que suporte a emissão de Carimbos do Tempo Renováveis chega a 6.015 MB. No caso dos Carimbos do Tempo Autenticados esse custo é de 888 MB somados aos 24 MB necessários ao armazenamento dos Selos de Conjunto pela AC-Raiz. Nota-se que o suporte a Carimbos do Tempo Autenticados requer custos praticamente constantes para a ACT pois os registros de cada rodada são removidos ao final do Período de Autenticação relacionado.

Nessas simulações não foram consideradas otimizações dos Repositórios de Carimbos do Tempo nem de Selos de Conjunto. Por meio dessas otimizações, parte desses registros seriam removidos de tempos em tempos dando lugar aos novos.

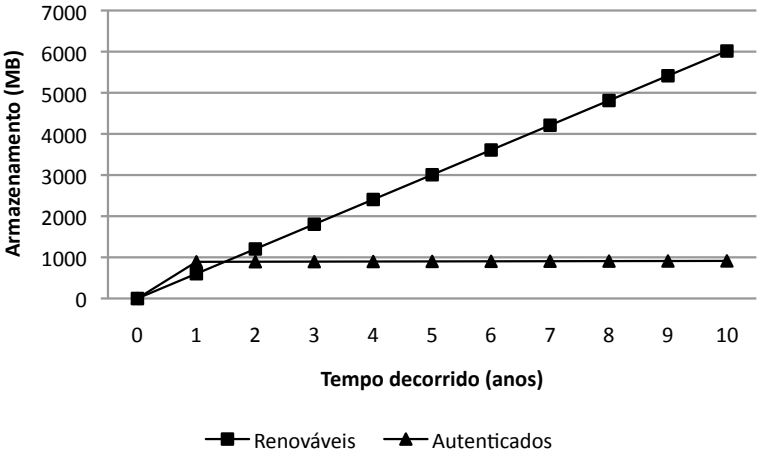

Figura 5.2: Simulação dos custos de operação durante 10 anos.

5.4 INTEROPERABILIDADE

Para verificar a interoperabilidade das assinaturas digitais preservadas por meio dos protocolos criptográficos propostos, foram confrontadas as especificações desses protocolos com as principais recomendações técnicas que atualmente abordam o problema da preservação por longo prazo de assinaturas digitais, sendo elas as recomendações CMS Advanced Electronic Signature (CAdES)(ETSI, 2009a), XML Advanced Electronic Signature (XAdES)(ETSI, 2009c), PDF Advanced Electronic Signature (PAdES)(ETSI, 2009b) e Evidence Record Syntax (ERS)(GONDROM; BRANDNER; PORDESCH, 2007). Foram analisados os processos de preservação, de validação e o formato das assinaturas preservadas.

A preservação por meio de Carimbos do Tempo Renováveis difere da tradicional no que diz respeito ao agendamento de cada sobreposição, bem como na renovação dos carimbos. Uma assinatura preservada, contudo, pode ser validada como de costume. A única exceção ocorre quando a assinatura do último carimbo já perdeu sua validade. Nesse caso, é necessário renovar esse carimbo antes da validação tradicional. No que diz respeito ao formato da assinatura, esse se mantêm inalterado. Isso ocorre porque o formato dos carimbos permanece sendo aquele recomendado pela RFC 3161(ADAMS et al., 2001), e as informações necessária à validação desses carimbos continuam sendo os certificados e dados de revogação tradicionais.

Há, todavia, uma particularidade na data informada por esses carimbos, essa pode não estar dentro do prazo de validade do certificado da ACT. Isso decorre do processo de renovação, onde o certificado da ACT pode ser substituído com o tempo, possivelmente por um certificado onde

o prazo de validade começa após a data indicada no carimbo. Apesar de a RFC 3161 não impor nenhuma restrição nesse sentido, foram realizados testes de compatibilidade com as bibliotecas OpenSSL 1.0 e BouncyCastle 1.45, assim como com o aplicativo Adobe Reader 9.3.

Foram escolhidas as bibliotecas OpenSSL e BouncyCastle pois essas estão entre as principais bibliotecas criptográficas usadas no desenvolvimento de aplicativos C/C++ e Java, respectivamente. O Adobe Reader, por sua vez, foi escolhido por ser um dos aplicativos mais populares na lida com documentos eletrônicos assinados. Para os testes foi desenvolvida uma ACT que permitisse a renovação de carimbos do tempo, de modo que os carimbos renovados tivessem a particularidade em questão.

No caso das bibliotecas, os testes compreenderam a validação de carimbos renovados. Com o Adobe Reader foi necessária a renovação de um carimbo do tempo presente num documento PDF assinado. Nos testes, tanto o OpenSSL quanto o Adobe Reader aceitaram como válidos carimbos do tempo com a data anterior aquela de início do prazo de validade do certificado da ACT. A biblioteca BouncyCastle, por outro lado, rejeitou tais carimbos lançando uma exceção Java.

A preservação por meio de Carimbos do Tempo Autenticados difere da tradicional quanto ao agendamento de cada sobreposição, e a necessidade de autenticação e renovação dos carimbos. A validação das assinaturas preservada, por sua vez, requer a validação de Selos de Autenticidade no lugar da validação das assinaturas de cada carimbo. Além disso, pode ser necessário renovar o último carimbo caso seu Selo de Conjunto já tenha perdido sua validade. No que diz respeito ao formato da assinatura, a diferença está na necessidade de acomodar Selos de Autenticidade ao invéz de certificados e dados de revogação relacionados a cada carimbo. No caso das recomendações técnicas CAdES, XAdES, PAdES e ERS, essa incompatibilidade pode ser resolvida por meio de uma extensão para carimbos do tempo que ofereça esse suporte. No Anexo A, uma possível extensão é apresentada.

5.5 CONCLUSÃO

Neste capítulo foram avaliados os benefícios e limitações trazidos pelos protocolos criptográficos propostos frente a preservação tradicional por carimbos do tempo. Para tanto, foram realizadas análises teóricas cujos resultados foram confirmados por meio de testes e simulações. Esses últimos, baseados em protótipos e modelos matemáticos criados para representar alguns dos principais aspectos relacionados.

A redução nos custos, esperada para esses protocolos, foi alcançada ao tornar o tempo de vida dos carimbos maior, reduzindo a quantidade de carimbos necessária durante o processo de preservação. O aumento na confiabilidade, por outro lado, foi conseguido ao tornar toleráveis a maioria dos fatores que originalmente levariam a preservação de uma assinatura a falhar. Dos carimbos, os Carimbos do Tempo Autenti-

cados foram aqueles que alcançaram uma redução de custos mais acentuada, alcançando 99% nas simulações realizadas. Carimbos do Tempo Renováveis, por sua vez, mantiveram maior compatibilidade com a base instalada, podendo ser validados da maneira convencional.

Em contrapartida aos benefícios alcançados foram observados, principalmente, custos adicionais a serem absorvidos pelas Autoridades de Carimbo do Tempo (ACT) e Autoridades Certificadoras Raiz (AC-Raiz). Ao simular as operações dessas entidades por 10 anos, por exemplo, foram necessários aproximadamente 6 GB de espaço para uma ACT que suportasse a emissão de Carimbos do Tempo Renováveis. No caso dos Carimbos do Tempo Autenticados, foram precisos em torno de 888 MB para a ACT e 24 MB para a AC-Raiz.

6 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo o estudo da influência do tempo sobre as assinaturas digitais, bem como a proposta de alternativas para minimizar alguns dos principais problemas hoje relacionados a sua preservação. Como visto, apesar de necessário em muitos casos, assinaturas digitais são incapazes de comprovar a autenticidade de documentos eletrônicos por longo prazo, pois perdem sua validade por fatores como o enfraquecimento de algoritmos criptográficos ou o comprometimento da chave privada do signatário. Mesmo a principal estratégia de preservação hoje em uso, sugerida pelas recomendações técnicas de maior relevância sobre o assunto, é incapaz de garantir a preservação dessas assinaturas, apresentando, igualmente, custos inapropriados para diversos cenários. Tais questões foram analisadas no decorrer da dissertação culminando com a proposta de protocolos criptográficos para amenizar alguns dos principais problemas encontrados.

Assim, no Capítulo 2, foram apresentados detalhes quanto a forma com que assinaturas digitais vêm sendo implementadas assim como os fatores que limitam o tempo de vida dessas implementações. Como visto, essas assinaturas são produzidas e validadas de acordo com algum esquema de assinatura, sendo a chave pública, necessária à validação, geralmente distribuída por meio de certificados digitais X.509. Assim, tais assinaturas costumam ser armazenadas e transferidas em conjunto com os certificados e outras informações necessárias a sua validação, sendo usados, para tanto, pacotes de assinatura, que permitem acomodar além dessas, atributos sobre a assinatura, signatário ou documento assinado. Em relação ao tempo de vida das assinaturas digitais, esse é limitado pois tanto o esquema de assinatura se enfraquece com o tempo, quanto o caminho de certificação do signatário perde sua validade, comprometendo a segurança oferecida pela assinatura.

O Capítulo 3, por sua vez, apresentou as principais estratégias até então propostas para a preservação por longo prazo de assinaturas digitais, assim como as recomendações técnicas, de maior relevância, que atualmente abordam o assunto. Como visto, tais estratégias se baseiam no conceito de notarização onde uma terceira parte confiável é usada para autenticar fatos sobre a assinatura. Na primeira dessas estratégias esse fato é o momento em que a assinatura foi produzida. Por outro lado, na segunda estratégia o fato autenticado é a própria validade da assinatura. Dentre elas, aquela sugerida pelas principais recomendações técnicas sobre a preservação por longo prazo de assinaturas digitais é a primeira, conhecida por sobreposição de carimbos do tempo. Tais recomendações em geral estendem os pacotes de assinatura permitindo que esses acomodem os carimbos do tempo adicionados durante o processo de preservação.

No Capítulo 4 foram então analisados alguns dos problemas re-

lacionados a preservação por carimbos do tempo e propostos protocolos criptográficos para reduzir os custos e aumentar a confiabilidade dessa preservação. Como visto, tais problemas estão relacionados a fatores como a frequência com que novos carimbos são adicionados e a perda inesperada da validade desses carimbos. Assim, os protocolos propostos buscaram tanto estender o tempo de vida dos carimbos como tornar esse tempo mais previsível. Esses deram origem a duas novas implementações de carimbos do tempo, os Carimbos do Tempo Renováveis e os Carimbos do Tempo Autenticados, sendo o processo de preservação de assinaturas modificado pelo uso das novas operações disponíveis para esses carimbos. Particularmente, tal processo passou a se orientar não mais pela expiração do certificado da Autoridade de Carimbo do Tempo, mas pelo enfraquecimento da função de resumo criptográfico usada.

Por fim, o Capítulo 5 avaliou os benefícios e limitações trazidos pelos protocolos criptográficos propostos frente à preservação tradicional por carimbos do tempo. Para tanto, foram realizadas análises teóricas cujos resultados foram confirmados por meio de testes e simulações. A redução nos custos, esperada para esses protocolos, foi alcançada ao tornar o tempo de vida dos carimbos maior, reduzindo a quantidade de carimbos necessária durante o processo de preservação. O aumento na confiabilidade, por outro lado, foi conseguido ao tornar toleráveis a maioria dos fatores que originalmente levariam a preservação de uma assinatura a falhar. Em contrapartida aos benefícios alcançados foram observados, principalmente, custos adicionais a serem absorvidos pelas Autoridades de Carimbo do Tempo (ACT) e Autoridades Certificadoras Raiz (AC-Raiz). Finalmente, foi avaliada a compatibilidade desses protocolos com o legado.

Como visto, dentre os carimbos, os Carimbos do Tempo Autenticados são aqueles que oferecem uma maior redução de custos. Os de armazenamento, por exemplo, chegam a ser 99% menores, considerando a preservação de uma assinatura por cinquenta anos numa Infraestrutura de Chaves Públicas típica. Além disso, se destacam ao permitirem a validação *offline* das assinaturas preservadas, o que acelera a validação e possibilita sua realização em dispositivos sem conexão de rede. Carimbos do Tempo Renováveis, por outro lado, oferecem uma redução menor, alcançando 72% nas simulações, mas mantêm maior compatibilidade com a base instalada, sendo possível validar suas assinaturas da maneira convencional.

Em termos de custos para a ACT e AC-Raiz, esses se mostraram aceitáveis. Uma ACT que suporte a emissão de Carimbos do Tempo Renováveis terá custos adicionais relacionados, principalmente, à manutenção do Repositório de Carimbos do Tempo. Nas simulações tais custos chegaram a 6 GB após 10 anos de operação. No caso de uma ACT que suporte a emissão de Carimbos do Tempo Autenticados, esses estão em sua maioria relacionados à publicação dos Dados de Autenticação. Nas mesmas simulações, o espaço necessário para o Repositório de Dados de

Autenticação chegou a 888 MB. Já o Repositório de Selos de Conjunto, mantido pela AC-Raiz, alcançou 24 MB. Vale salientar que, graças às operações de otimização desses Repositórios, tais custos não crescem indefinidamente. Por meio delas, registros antigos dão lugar aos novos conforme novas funções de resumo criptográfico sejam adotadas e funções já inseguras, abandonadas.

6.1 TRABALHOS FUTUROS

Neste trabalho foram abstraídas algumas questões que podem servir de ponto de partida para trabalhos futuros. Uma delas é a segurança dos Repositórios de Carimbos do Tempo, Dados de Autenticação e Selos de Conjunto. Deve ser particularmente inviável a um adversário importar registros para esses Repositórios, do contrário as operações de renovação dos carimbos e Selos de Conjunto, assim como as solicitações desses Selos pela ACT ficariam comprometidas.

Um dos maiores desafios a essa proteção está no tamanho desses Repositórios. Os carimbos do tempo, por exemplo, são emitidos com o auxílio de plataformas especializadas, conhecidas por Módulos de Segurança Criptográfica, que tendem a oferecer uma maior proteção mas apresentar poucos recursos computacionais(ROMANI, 2009). É de se esperar, portanto, que os Repositórios de Carimbos do Tempo e Dados de Autenticação sejam mantidos fora dessas plataformas, o que os torna mais vulneráveis à ataques. Vale salientar que mecanismos semelhantes já são esperados para Carimbadoras que emitam carimbos do tempo encadeadosPasqual (2001).

Outra questão se refere à localização dos serviços de renovação e autenticação de carimbos. Foi assumido que esses serviços seriam localizados por outros meios, assim como já ocorre com a própria solicitação de carimbos. Por exemplo, o usuário que contratasse os serviços seria informado sobre a forma de acessá-los. Todavia, seria interessante que esses fossem descobertos de maneira automatizada. Principalmente se forem implementados mecanismos de herança para as ACTs e AC-Raiz, onde essas entidades poderiam continuar os serviços das anteriores caso aquelas terminassem suas operações.

De modo que os protocolos criptográficos propostos ofereçam uma redução ainda mais acentuada nos custos e uma maior confiabilidade, seria possível que esses empregassem ao invés de uma, duas ou mais funções de resumo criptográfico(HERZBERG, 2005; FISCHLIN; LEHMANN, 2007). Assim o prazo de validade dos carimbos seria dado por aquela função que viesse a durar mais tempo. Além disso, seriam toleradas quebras inesperadas dessas funções, desde que pelo menos uma se mantivesse segura.

Por fim algumas questões mais gerais são igualmente interessantes, como a análise formal dos protocolos criptográficos propostos e a aplicação das ideias por trás desses protocolos na segunda estratégia de

notarização, vista no Capítulo 3. Essa estratégia apesar de menos aceita, apresenta alguns benefícios como a possibilidade de migração do formato do documento assinado(PIECHALSKI; SCHMIDT, 2006) e custos geralmente menores quando comparados aqueles da estratégia de preservação por carimbos do tempo(VIGIL et al., 2009). Por meio dessas ideias seria possível reduzir ainda mais esses custos bem como aumentar a confiabilidade do processo de preservação.

REFERÊNCIAS BIBLIOGRÁFICAS

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

ADOBE SYSTEMS INCORPORATED. *Digital Signatures in the PDF Language*. [S.l.], 2006.

ANAGNOSTOPOULOS, A.; GOODRICH, M.; TAMASSIA, R. Persistent authenticated dictionaries and their applications. *Information Security*, Springer, p. 379–393, 2001.

ANDERSON, R. Invited lecture. In: *Fourth Annual Conference on Computer and Communications Security, ACM*. [S.l.: s.n.], 1997.

ANSPER, A. et al. Efficient long-term validation of digital signatures. In: SPRINGER. *Public Key Cryptography*. [S.l.], 2001. p. 402–415.

BARKER, E. et al. *NIST SP800-57: Recommendation for key management–part 1: General (revised)*. [S.l.], 2007.

BARKER, E.; ROGINSKY, A. *DRAFT NIST SP800-131: Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes*. [S.l.], jan 2010.

BARTEL, M. et al. XML-signature syntax and processing. *W3C recommendation*, v. 12, p. 2002, 2002.

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

BELLARE, M.; MINER, S. A forward-secure digital signature scheme. In: SPRINGER. *Advances in Cryptology—CRYPTO'99*. [S.l.], 1999. p. 786–786.

BERMAN, P.; KARPINSKI, M.; NEKRICH, Y. Optimal trade-off for Merkle tree traversal. *Theoretical Computer Science*, Elsevier, v. 372, n. 1, p. 26–36, 2007. ISSN 0304-3975.

BLANCHETTE, J. The digital signature dilemma: To preserve or not to preserve. In: *Proceedings, IS&T's 2004 Archiving Conference*. [S.l.: s.n.], 2004. p. 221–226.

BLAZIC, A.; SETCCE, L. Long term trusted archive services. In: *Digital Society, 2007. ICDS'07. First International Conference on the*. [S.l.: s.n.], 2007. p. 29–29.

BLIBECH, K.; GABILLON, A. A new timestamping scheme based on skip lists. *Computational Science and Its Applications-ICCSA 2006*, Springer, p. 395–405, 2006.

BRASIL. *Medida provisória nº 2.200-2, de 24 de agosto de 2001*. Poder Executivo, Brasília, DF, 2001.

BUCHMANN, J.; DAHMEN, E.; SCHNEIDER, M. Merkle tree traversal revisited. *Post-Quantum Cryptography*, Springer, p. 63–78, 2008.

CALLAS, J. et al. *OpenPGP Message Format*. IETF, nov. 2007. RFC 4880 (Proposed Standard). (Request for Comments, 4880). Updated by RFC 5581. Disponível em: <http://www.ietf.org/rfc/rfc4880.txt>.

CAVALLAR, S. et al. Factorization of a 512-bit RSA modulus. In: SPRINGER. *Advances in Cryptology—EUROCRYPT 2000*. [S.l.], 2000. p. 1–18.

CHADWICK, D. W. *Understanding X.500 (The Directory)*. International Thompson Publishing, 1996. Disponível em: <http://www.cs.kent.ac-.uk/pubs/1996/2051>.

CHAUM, D.; ROIJAKKERS, S. Unconditionally-secure digital signatures. *Advances in Cryptology-CRYPT0'90*, Springer, p. 206–214, 1991.

CONARQ. *Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ Brasil)*. v.1.1. [S.l.], Dezembro 2009.

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>.

COSTA, V. *Análise da Confiança do Sistema de Protocolação Digital de Documentos Eletrônicos*. 165 f. Dissertação (Mestrado em Ciência da Computação) — Curso de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2003.

CUSTODIO, R. et al. Optimized Certificates–A New Proposal for Efficient Electronic Document Signature Validation. In: SPRINGER-VERLAG NEW YORK INC. *Public Key Infrastructure: 5th European PKI Workshop: Theory and Practice, EuroPKI 2008 Trondheim, Norway, June 16-17, 2008, Proceedings*. [S.l.], 2008. p. 49. ISBN 3540694846.

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

DEMéTRIO, D. B. *Infra-estrutura para Protocolização Digital de Documentos Eletrônicos*. 140 f. Dissertação (Mestrado em Ciência da Computação) — Curso de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2003.

DIAS, J. S. *Confiança no Documento Eletrônico*. 141 f. Tese (Doutorado em Engenharia de Produção) — Curso de Pós-Graduação em Engenharia de Produção, Universidade Federal de Santa Catarina, Florianópolis, 2004.

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

DODIS, Y. et al. Key-insulated public key cryptosystems. In: SPRINGER. *Advances in Cryptology—EUROCRYPT 2002*. [S.l.], 2002. p. 65–82.

DODIS, Y. et al. Strong key-insulated signature schemes. *Public Key Cryptography—PKC 2003*, Springer, p. 130–144, 2003.

ELLISON, C. *SPKI Requirements*. IETF, set. 1999. RFC 2692 (Experimental). (Request for Comments, 2692). Disponível em: <http://www.ietf.org/rfc/rfc2692.txt>.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. *Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms*. [S.l.], Nov 2007.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. *Electronic Signatures and Infrastructures (ESI); CMS Advanced electronic Signatures (CAdES)*. [S.l.], Nov 2009.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. *Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term – PAdES-LTV Profile*. [S.l.], Jul 2009.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. *Electronic Signatures and Infrastructures (ESI); XML Advanced electronic Signatures (XAdES)*. [S.l.], Jun 2009.

FISCHLIN, M.; LEHMANN, A. Security-amplifying combiners for collision-resistant hash functions. *Advances in Cryptology-CRYPTO 2007*, Springer, p. 224–243, 2007.

GONDROM, T.; BRANDNER, R.; PORDESCH, U. *Evidence Record Syntax (ERS)*. IETF, ago. 2007. RFC 4998 (Proposed Standard). (Request for Comments, 4998). Disponível em: <http://www.ietf.org/rfc/rfc4998-.txt>.

HABER, S.; STORNETTA, W. How to time-stamp a digital document. *Advances in Cryptology-CRYPT0'90*, Springer, p. 437–455, 1991.

HANAOKA, G. Unconditionally secure signatures and its related schemes. In: IEEE. *Theory and Practice in Information-Theoretic Security, 2005. IEEE Information Theory Workshop on*. [S.l.], 2005. p. 7–12. ISBN 0780394917.

HERZBERG, A. On tolerant cryptographic constructions. *Topics in Cryptology–CT-RSA 2005*, Springer, p. 172–190, 2005.

HOUSLEY, R. *Cryptographic Message Syntax (CMS)*. IETF, jul. 2004. RFC 3852 (Proposed Standard). (Request for Comments, 3852). Obsoleted by RFC 5652, updated by RFCs 4853, 5083. Disponível em: <http://www.ietf.org/rfc/rfc3852.txt>.

HOUSLEY, R.; ASHMORE, S.; WALLACE, C. *Trust Anchor Management Protocol (TAMP)*. IETF, ago. 2010. RFC 5934 (Proposed Standard). (Request for Comments, 5934). Disponível em: <http://www.ietf.org/rfc/rfc5934.txt>.

HOUSLEY, R.; POLK, T. *Planning for PKI: best practices guide for deploying public key infrastructure*. [S.l.]: John Wiley & Sons, Inc. New York, NY, USA, 2001. ISBN 0471397024.

HUHNLEIN, D. et al. A comprehensive reference architecture for trustworthy long-term archiving of sensitive data. In: IEEE. *New Technologies, Mobility and Security (NTMS), 2009 3rd International Conference on*. [S.l.], 2010. p. 1–5.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. *Visão Geral Sobre Assinaturas Digitais na ICP-Brasil*. v. 2.0. Brasília, Abril 2010. DOC-ICP-15.

ITU-T. *Recommendation X.509 (11/88) - Information Technology - Open Systems Interconnection - The Directory: Authentication Framework*. 1988.

ITU-T. *Recommendation X.509 (11/93) - Information Technology - Open Systems Interconnection - The Directory: Authentication Framework*. 1993.

ITU-T. *Recommendation X.509 (11/2008) - Information Technology - Open Systems Interconnection - The Directory: Authentication Framework*. 2008.

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

JUST, M. *On the temporal authentication of digital data*. Tese (Doutorado) — Carleton University, 1998.

KALISKI, B. *PKCS #7: Cryptographic Message Syntax Version 1.5*. IETF, mar. 1998. RFC 2315 (Informational). (Request for Comments, 2315). Disponível em: <http://www.ietf.org/rfc/rfc2315.txt>.

KLEINJUNG, T. et al. Factorization of a 768-bit RSA modulus. Cryptology ePrint Archive, Report 2010/006, 2010. http://eprint. iacr. org/2010/006. pdf, 2010.

KOHNFELDER, L. M. *Towards a practical public-key cryptosystem*. [S.l.], 1978.

LEE, K. et al. The state of the art and practice in digital preservation. *Journal of Research-National Institute of Standards and Technology*, Citeseer, v. 107, n. 1, p. 93–106, 2002. ISSN 1044-677X.

LEKKAS, D.; GRITZALIS, D. Cumulative notarization for long-term preservation of digital signatures. *Computers & Security*, Elsevier, v. 23, n. 5, p. 413–424, 2004.

LUCKS, S.; DAUM, M. The story of alice and her boss: Hash functions and the blind passenger attack. *Presentation at Rump Sessions of Eurocrypt 2005*, 2005.

MARTINEZ-PELáEZ, R. et al. Efficient certificate path validation and its application in mobile payment protocols. In: *ARES '08: Proceedings of the 2008 Third International Conference on Availability, Reliability and Security*. Washington, DC, USA: IEEE Computer Society, 2008. p. 701–708. ISBN 978-0-7695-3102-1.

MASSIAS, H.; QUISQUATER, J. Time and cryptography. *US-patent n*, Citeseer, v. 5, p. 12, 1997.

MENEZES, A.; OORSCHOT, P. V.; VANSTONE, S. *Handbook of applied cryptography*. [S.l.]: CRC, 1997.

MERKLE, R. Protocols for public key cryptosystems. Published by the IEEE Computer Society, 1980.

MERKLE, R. C. Secrecy, authentication, and public key systems. fev. 1979. ISSN 01681702. Disponível em: <http://portal.acm.org/citation-.cfm?id=909000>.

MICALI, S. NOVOMODO: Scalable certificate validation and simplified PKI management. In: *Proc. of 1st Annual PKI Research Workshop*. [S.l.: s.n.], 2002.

MOLNAR, D. et al. MD5 Considered Harmful Today. In: *25th Chaos Communication Congress*. [S.l.: s.n.], 2008.

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

NOTOYA, A. E. *IARSDE*: Infra-estrutura de armazenamento e recuperação segura de documentos eletrônicos. 110 f. Dissertação (Mestrado em Ciência da Computação) — Curso de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2002.

PARLIAMENT, E.; COUNCIL. Directive 1999/93/ec of the european parliament and of the council of 13 december 1999 on a community framework for electronic signatures. *OJEC L13*, p. 12–20, 2000.

PASQUAL, E. S. *IDDE*. 110 f. Dissertação (Mestrado em Ciência da Computação) — Curso de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2001.

PIECHALSKI, J.; SCHMIDT, A. Authorised translations of electronic documents. *Arxiv preprint cs/0606046*, 2006.

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. *CMS Advanced Electronic Signatures (CAdES)*. IETF, mar. 2008. RFC 5126 (Informational). (Request for Comments, 5126). Disponível em: <http://www.ietf.org/rfc/rfc5126-.txt>.

POPEK, G.; KLINE, C. Encryption and secure computer networks. *ACM Computing Surveys (CSUR)*, ACM, v. 11, n. 4, p. 331–356, 1979.

PRENEEL, B. The First 30 Years of Cryptographic Hash Functions and the NIST SHA-3 Competition. *Topics in Cryptology-CT-RSA 2010*, Springer, p. 1–14, 2010.

RAMOS, T. A. et al. An Infrastructure for Long-term Archiving of Authenticated and Sensitive Electronic Documents. In: *Public Key Infrastructure: 7th European PKI Workshop: Theory and Practice, EuroPKI 2010 Athens, Greece, September 23-24, 2010, Proceedings*. [S.l.: s.n.], 2010.

REDDY, R.; WALLACE, C. *Trust Anchor Management Requirements*. IETF, out. 2010. RFC 6024 (Informational). (Request for Comments, 6024). Disponível em: <http://www.ietf.org/rfc/rfc6024.txt>.

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

ROMANI, J. *Integração de Serviços de Relógio para Infra-estrutura de Chaves Públicas*. 118 f. Dissertação (Mestrado em Ciência da Computação) — Curso de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2009.

SILVA, N. da et al. *Central Notarial de Serviços Eletrônicos Compartilhados*. São Caetano do Sul, SP: Yendis Editora, 2007.

SILVA, N. da; RAMOS, T. A. *Preservação de Longo Prazo de Documentos Eletrônicos na CNSEC*. 130 f. Monografia (Bacharelado em Ciência da Computação) — Curso de Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2007.

SZYDLO, M. Merkle tree traversal in log space and time. In: *In Eurocrypt 2004, LNCS*. [S.l.]: Springer-Verlag, 2004. p. 541–554.

TRONCOSO, C.; COCK, D. D.; PRENEEL, B. Improving secure long-term archival of digitally signed documents. In: ACM. *Proceedings of the 4th ACM international workshop on Storage security and survivability*. [S.l.], 2008. p. 27–36.

VIGIL, M. A. G. et al. Infra-estrutura de chaves públicas otimizada: Uma icp de suporte a assinaturas eficientes para documentos eletrônicos. In: *Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. [S.l.]: Springer-Verlag, 2009. p. 129–142.

ZIMMER, W.; LANGKABEL, T.; HENTRICH, C. Archisafe: Legally compliant electronic storage. *IT Professional*, v. 10, n. 4, p. 26–33, 2008.

A ESPECIFICAÇÕES EM ASN.1

Algumas das análises realizadas no Capítulo 5 foram baseadas em implementações dos Carimbos do Tempo Renováveis e Carimbos do Tempo Autenticados. Para suportá-las foram criadas especificações em *Abstract Syntax Notation One* (ASN.1) dos protocolos criptográficos envolvidos. Apesar de outras especificações serem igualmente viáveis, essas já trazem informações suficientes para o correto funcionamento desses protocolos.

A.1 CARIMBOS DO TEMPO RENOVÁVEIS

A especificação em ASN.1 dos Carimbos do Tempo Renováveis compreende a especificação dos protocolos de solicitação e renovação dos carimbos. Esses foram apresentados, respectivamente, nas Seções 4.3.1.2 e 4.3.1.3 do Capítulo 4. De modo a aumentar a compatibilidade com a base instalada, o protocolo de solicitação permanece sendo aquele especificado na recomendação técnica RFC 3161(ADAMS et al., 2001).

O protocolo de renovação desses carimbos, por sua vez, é apresentado na figura A.1, onde *TimeStampRenewalReq* é a requisição enviada pelo usuário e *TimeStampRenewalResp* é a resposta da ACT.

```
TimeStampRenewalReq ::= SEQUENCE  {
  version               INTEGER  { v1(1) },
  timeStampToken        TimeStampToken, -- importado da RFC 3161
  certReq               BOOLEAN DEFAULT FALSE,
  extensions            [0] IMPLICIT Extensions OPTIONAL
  -- importado da RFC 5280
}

TimeStampRenewalResp ::= SEQUENCE  {
  status                Status,
  timeStampToken        TimeStampToken OPTIONAL -- importado da RFC 3161
}

Status ::= INTEGER {
  granted               (0),
  rejected              (1),
  badRequest            (2)
}
```

Figura A.1: Estruturas ASN.1 *TimeStampRenewalReq*, *TimeStampRenewalResp* e *Status*.

Os campos de uma solicitação *TimeStampRenewalReq* tem o seguinte significado:

version: identifica a versão da especificação usada. Neste trabalho é defi-

nida a primeira versão dessa especificação;

timeStampToken: contêm o carimbo do tempo a ser renovado;

certReq: indica se a ACT deve retornar, junto com o carimbo, novos certificados que porventura sejam necessários na validação do carimbo renovado;

extensions: quando presente, contêm extensões da solicitação.

Os campos de uma resposta *TimeStampRenewalResp*, por sua vez, são:

status: indica o sucesso ou fracasso da renovação.

timeStampToken: sendo a renovação bem sucedida, contêm o carimbo do tempo renovado;

Os possíveis valores de *status* significam:

granted: indica uma operação bem sucedida;

rejected: informa o fracasso da operação;

badRequest: sinaliza má formação na solicitação recebida.

A.2 CARIMBOS DO TEMPO AUTENTICADOS

A especificação ASN.1 dos Carimbos do Tempo Autenticados compreende a especificação dos protocolos de solicitação, autenticação e renovação de carimbos. Esses foram apresentados, respectivamente, nas Seções 4.4.2.3, 4.4.2.4 e 4.4.2.5 do Capítulo 4. De modo a aumentar a compatibilidade com o legado, o protocolo de solicitação permanece sendo aquele especificado na recomendação técnica RFC 3161(ADAMS et al., 2001). A única exceção está na extensão não assinada, apresentada na figura A.2, que deve estar presente no carimbo. Por meio dessa extensão a ACT informa o Período de Autenticação do carimbo emitido.

```
id-authPeriod OBJECT IDENTIFIER ::= { ... }

AuthPeriod ::= SEQUENCE {
  notBefore            Time,
  notAfter             Time
}
```

Figura A.2: Estruturas ASN.1 *id-authPeriod* e *AuthPeriod*.

O protocolo de autenticação de carimbos, por sua vez, é composto pelos protocolos de solicitação dos Dados de Autenticação e do Selo de

```
AuthDataReq ::= SEQUENCE {
  version              INTEGER  { v1(1) },
  timeStamp            MessageImprint  -- importado da RFC 5280
}

AuthDataResp ::= SEQUENCE {
  authStatus           Status,
  authData             AuthData
}
```

Figura A.3: Estruturas ASN.1 *AuthDataReq* e *AuthDataResp*.

Conjunto. Na figura A.3 é apresentado aquele para solicitação dos Dados de Autenticação, onde *AuthDataReq* é a requisição enviada pelo usuário e *AuthDataResp* é a resposta da ACT.

Os campos de uma requisição *AuthDataReq* têm o seguinte significado:

version: identifica a versão da especificação usada. Neste trabalho é definida a sua primeira versão;

timeStamp: contêm o resumo criptográfico do carimbo.

Os campos de uma resposta *AuthDataResp* são:

authStatus: informa o sucesso ou fracasso da operação;

authData: quando presente, contêm os Dados de Autenticação desejados.

O protocolo para solicitação do Selo de Conjunto, por sua vez, é apresentado na figura A.4, onde *SetSealReq* é a requisição enviada pelo usuário e *SetSealResp* é a resposta da AC-Raiz.

```
SetSealReq ::= SEQUENCE {
  version              INTEGER  { v1(1) },
  timeStamp            MessageImprint -- importado da RFC 3161
}

SetSealResp ::= SEQUENCE {
  authStatus           Status,
  setSeal              ContentInfo OPTIONAL -- importado da RFC 3852
}
```

Figura A.4: Estruturas ASN.1 *SetSealReq* e *SetSealResp*.

Os campos de uma requisição *SetSealReq* têm o seguinte significado:

version: identifica a versão da especificação usada. Neste trabalho é definida a sua primeira versão;

timeStamp: contêm o resumo criptográfico calculado a partir dos Dados de Autenticação.

Os campos de uma resposta *SetSealResp* são:

authStatus: informa o sucesso ou fracasso da operação;

setSeal: sendo a solicitação bem sucedida, contêm o Selo de Conjunto desejado.

Um Selo de Autenticidade, obtido por meio do protocolo de autenticação, é apresentado na figura A.5, onde *SetSeal* é o Selo de Conjunto e *AuthData* são os Dados de Autenticação. O primeiro é um pacote *Cryptographic Message Syntax* (CMS), *signedData*, onde o conteúdo assinado é identificado por *id-setSeal*. Os Dados de Autenticação, por sua vez, são inseridos no pacote através da extensão não assinada *id-authData*.

```
id-setSeal OBJECT IDENTIFIER ::= { ... }

SetSeal ::= SEQUENCE  {
  version              INTEGER  { v1(1) },
  tsa                  GeneralName,
  timeStamps           MessageImprint -- importado da RFC 3161
}

id-authData OBJECT IDENTIFIER ::= { ... }

AuthData ::= SEQUENCE {
  version              INTEGER  { v1(1) },
  digestAlgorithm      AlgorithmIdentifier, -- importado da RFC 5280
  authData             SEQUENCE OF OCTET STRING
}
```

Figura A.5: Estruturas ASN.1 *id-setSeal*, *SetSeal*, *id-authData*, e *AuthData*.

Os campos de um Selo de Conjunto *SetSeal* têm o seguinte significado:

version: identifica a versão da especificação usada. Neste trabalho é definida a sua primeira versão;

tsa: traz os dados de identificação da ACT que solicitou o Selo de Conjunto;

timeStamps: contêm o resumo criptográfico que representa todos os carimbos emitidos na rodada da ACT;

Dados de Autenticação *AuthData* são formados pelos seguintes campos:

version: identifica a versão da especificação usada. Neste trabalho é definida a sua primeira versão;

digestAlgorithm: informa a função de resumo criptográfico usada nos Dados de Autenticação;

authData: contêm os Dados de Autenticação.

Para a geração dos Selos de Autenticidade ainda é necessária a especificação do protocolo usado pela ACT para a solicitação de Selos de Conjunto. Esse é apresentado na figura A.6, onde *TimeStampsAuthReq* é a requisição enviada pela ACT e *TimeStampsAuthResp* é a resposta da AC-Raiz.

```
id-timeStampsAuthReq OBJECT IDENTIFIER ::= { ... }

TimeStampsAuthReq ::= SEQUENCE  {
  version              INTEGER  { v1(1) },
  tsa                  GeneralName, -- importado da RFC 5280
  timeStamps           MessageImprint -- importado da RFC 3161
}

TimeStampsAuthResp ::= SEQUENCE {
  authStatus           Status,
}
```

Figura A.6: Estruturas ASN.1 *id-timeStampsAuthReq*, *TimeStampsAuthReq* e *TimeStampsAuthResp*.

Requisições *TimeStampsAuthReq* são pacotes CMS, *signedData*, cujo conteúdo assinado é identificado por *id-timeStampsAuthReq*. Seus campos têm o seguinte significado:

version: identifica a versão da especificação usada. Neste trabalho é definida a sua primeira versão;

tsa: traz os dados de identificação da ACT;

timeStamps: contêm o resumo criptográfico que representa todos os carimbos emitidos na rodada da ACT.

Respostas *TimeStampsAuthResp*, por sua vez, indicam apenas o sucesso ou fracasso da operação.