Carimbos do Tempo Autenticados para a Preservação por Longo Prazo de Assinaturas Digitais

Nelson da Silva[1], **Thiago Acórdi Ramos**[1], **Ricardo Felipe Custódio**[1]

[1]Laboratório de Segurança em Computação (LabSEC)
Universidade Federal de Santa Catarina (UFSC)
Caixa Postal 476 – 88040-900 – Florianópolis – SC – Brasil
{nelson, thg, custodio}@inf.ufsc.br

Abstract. *Digital signatures are usually employed as the digital counterpart of handwritten signatures, allowing the authentication of electronic documents. These signatures, however, may quickly lose its validity, creating a preservation challenge for those documents that must be kept for a longer period of time. In this paper, we improve the efficiency and reliability of the usual approach for this problem, through a new time-stamp scheme. Such time-stamps carries a Certificate of Authenticity, with reduces its storage and validation costs, while protecting the signature even in the presence of an adversary able to compromise the Time Stamping Authority's private key or its signature scheme.*

Resumo. *Assinaturas digitais são comumente usadas como a contraparte digital das assinaturas manuscritas, possibilitando a autenticação de documentos eletrônicos. Tais assinaturas, contudo, podem rapidamente perder sua validade, criando um desafio para a preservação daqueles documentos que precisam ser guardados por um tempo maior. Neste trabalho, aumentamos a eficiência e confiabilidade da abordagem usual para o problema, através de um novo esquema de datação. Esses carimbos carregam um Certificado de Autenticidade, que reduz seus custos de armazenamento e validação, enquanto protege a assinatura mesmo na presença de um adversário capaz de comprometer a chave privada da Autoridade de Carimbo do Tempo ou seu esquema de assinatura.*

1. Introdução

Assinaturas digitais são comumente usadas como a contraparte digital das assinaturas manuscritas, possibilitando a autenticação de documentos eletrônicos. Diversos países vêm, inclusive, atribuindo a elas o mesmo valor legal das assinaturas manuscritas, como forma de facilitar o uso de documentos eletrônicos como meio de prova. Na União Européia, por exemplo, essa questão é abordada na Diretiva Européia 1999/93/EC. No Brasil, isso é assunto da Medida Provisória 2.200-2.

Apesar de amplamente usadas, as assinaturas digitais podem rapidamente perder sua validade, o que constitui um desafio para a preservação daqueles documentos eletrônicos que precisam ser guardados por um longo período de tempo. Na implementação usual dessas assinaturas, por exemplo, tal problema ocorre por diversos fatores, tais como o enfraquecimento do esquema de assinatura usado pelo signatário e a perda de validade de seu caminho de certificação X.509. Nesses casos, a segurança oferecida pela assinatura acaba sendo comprometida.

Tal problema torna necessária alguma forma de preservação que permita manter a validade dessas assinaturas pelo tempo que for necessário. Assim várias estratégias já foram propostas, sendo a sobreposição de carimbos do tempo, criada por Bayer, Haber e Stornetta [6], a principal delas. É essa a estratégia usada nas principais recomendações técnicas que atualmente abordam o problema [12, 13, 14], sendo igualmente uma das mais estudadas na literatura. Do mesmo modo, é essa a estratégia usada no Padrão Brasileiro de Assinatura Digital, publicado pelo Instituto Nacional de Tecnologia da Informação (ITI).

A preservação por carimbos do tempo, contudo, implica em custos cumulativos para o usuário, além de não garantir que a assinatura realmente mantenha sua validade pelo tempo necessário. Tais custos dificultam a preservação e validação dessas assinaturas em dispositivos com poucos recursos computacionais, bem como a preservação de grandes volumes de documentos [24]. A baixa confiabilidade dessa estratégia, por sua vez, acaba tornando necessárias medidas preventivas, como o uso de carimbos do tempo redundantes [14], que terminam por aumentar ainda mais os custos de preservação.

Neste trabalho aumentamos a eficiência e confiabilidade da preservação por carimbos do tempo através de um novo esquema de datação, os Carimbos do Tempo Autenticados. O uso desse esquema permite reduzir drasticamente os custos de armazenamento e validação das assinaturas preservadas, assim como ter maiores garantias quanto a preservação da assinatura pelo tempo que for necessário. Além disso, seu uso torna possível a validação *off-line* de assinaturas, uma vez que essas se tornam auto-contidas.

O restante deste trabalho é organizado da seguinte forma. A Seção 2 apresenta o estado da arte sobre a preservação de assinaturas digitais. A Seção 3 descreve o esquema de datação tradicional e revisa a preservação por carimbos do tempo. A Seção 4 apresenta o esquema de datação proposto, assim como as suas implicações sobre os procedimentos de preservação e validação de assinaturas. A Seção 5 avalia os benefícios e limitações da proposta. Finalmente, a Seção 6 apresenta as considerações finais.

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 [21] 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 sua falsificação se tornar viável.

Massias e Quisquater [18], por outro lado, propuseram a preservação de assinaturas digitais através da autenticação de outro fato, a sua própria validade. Esse ateste seria uma alternativa para a comprovação da validade da assinatura quando, através das verificações tradicionais, essa já fosse inválida.

Ambas as estratégias de notarização, como ficaram conhecidas por remeter aos atos praticados pelos notários no mundo real [16], foram tema de diversos trabalhos. Carimbos do tempo, por exemplo, foram aprimorados por Haber e Stornetta [15], que sugeriram seu encadeamento como forma de reduzir a confiança necessária nas entidades responsáveis por sua produção. Blibech e Gabillon [7], por sua vez, reduziram os custos decorrentes da validação desses carimbos, redefinindo a forma como são encadeados.

Atestes da validade de assinaturas, por outro lado, foram aprimoradas por Ansper et al. [3], que sugeriram a agregação das assinaturas em Árvores de Merkle [19], de modo a reduzir o esforço computacional necessário para a sua produção. Por outro lado, Custodio et al. [10], propuseram a associação do método de NOVOMODO a esses atestes, como forma de minimizar os recursos computacionais necessários à sua validação.

Além das estratégias de notarização, uma outra abordagem vem sendo usada na literatura para a preservação de assinaturas digitais, focada nas primitivas criptográficas envolvidas em sua geração e validação. São os esquemas especiais de assinatura, com propriedades que as tornam menos vulneráveis ao efeito do tempo. São exemplos desses esquemas o de chave evolutiva e as assinaturas incondicionalmente seguras.

Esquemas de chave evolutiva [2] são voltados à proteção das assinaturas produzidas contra o comprometimento da chave privada do signatário. Nesses esquemas a chave privada evolui de modo que o comprometimento da chave privada atual, não invalidaria assinaturas realizadas com as chaves anteriores.

Esquemas de assinaturas incondicionalmente seguras, por sua vez, tratam do problema relacionado ao enfraquecimento dos algoritmos criptográficos [8]. Diferentemente dos esquemas convencionais, tais esquemas não baseiam sua segurança em suposições quanto ao poder computacional do adversário. Poder esse que tende a aumentar com o tempo.

Nenhuma das estratégias citadas, contudo, é capaz de preservar assinaturas digitais por um prazo arbitrariamente grande. Carimbos do tempo e atestes, por exemplo, perdem com o tempo sua validade assim como as próprias assinaturas. Esquemas especiais de assinatura, por sua vez, tendem a tratar apenas uma parte dos problemas, sempre deixando as assinaturas vulneráveis a problemas remanescentes.

Um dos primeiros trabalhos a tratar da preservação por longo prazo de assinaturas digitais foi o trabalho de Bayer, Haber e Stornetta [6]. Na proposta, parcialmente apresentada num trabalho anterior [15], 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 demonstraria que o anterior fora produzido antes de se tornar falsificável. Ideia semelhante à sobreposição de carimbos do tempo foi posteriormente proposta para atestes da validade de assinaturas [17, 24].

3. Preservação por Carimbos do Tempo

Dentre as estratégias até então propostas para a preservação por longo prazo de assinaturas digitais, a preservação por carimbos do tempo é aquela adotada pelas principais recomendações técnicas sobre o tema [12, 13, 14], sendo, igualmente, uma das mais estudadas na literatura. Nessa estratégia, carimbos do tempo são usados para demonstrar a validade da assinatura e dos próprios carimbos usados no processo.

3.1. Carimbos do Tempo

Em sua forma mais comum, usada em recomendações técnicas como a RFC 3161 [1], carimbos do tempo 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:

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

Nele, um usuário solicita um carimbo do tempo para uma informação qualquer $x \in \{0,1\}^+$, enviando seu resumo criptográfico $\mathcal{H}(x)$. 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.

Tais condições visam comprovar, respectivamente, a autenticidade do carimbo e a integridade da informação datada. A função $\mathcal{H}$ deve ser segura pois, do contrário, essa integridade acaba se tornando duvidosa. Em maiores detalhes, $\mathcal{H}$ poderá ser apenas resistente à segunda inversão, desde que em t tenha sido resistente, igualmente, à colisão. Dessas condições é possível concluir o prazo de validade de um carimbo. Esse termina com a perda de validade da assinatura da ACT ou com o enfraquecimento de $\mathcal{H}$, o que ocorrer primeiro.

3.2. Preservação de Assinaturas

A preservação de uma assinatura digital por meio de carimbos do tempo segue os seguintes passos, onde s, d, $\mathcal{C}_s$ e $\mathcal{R}_s$, são, respectivamente, a assinatura, o documento assinado, os certificados do caminho de certificação do signatário e os dados de revogação atuais:

1. **inicialização:** adicionar um carimbo do tempo ts^1 sobre $\{s, d, \mathcal{C}_s, \mathcal{R}_s\}$, obtendo $\{\{s, d, \mathcal{C}_s, \mathcal{R}_s\}, ts^1, \mathcal{C}^1_{ts}\}$;
2. **agendamento:** agendar a sobreposição do carimbo. Essa sobreposição deve ocorrer antes de o carimbo perder sua validade, sendo, em geral, agendada para um momento próximo da expiração do certificado da ACT;
3. **sobreposição:** no momento agendado, validar ts^1. Sendo válido, adicionar ts^2 sobre $\{\{s, d, \mathcal{C}_s, \mathcal{R}_s\}, ts^1, \mathcal{C}^1_{ts}, \mathcal{R}^1_{ts}\}$, obtendo $\{\{\{s, d, \mathcal{C}_s, \mathcal{R}_s\}, ts^1, \mathcal{C}^1_{ts}, \mathcal{R}^1_{ts}\}, ts^2, \mathcal{C}^2_{ts}\}$. Caso ts^1 já tenha perdido sua validade, a preservação falha;
4. **repetição:** para os próximos carimbos, repetir os passos 2 e 3 enquanto for necessário preservar a validade da assinatura. Dessa forma, na adição do n-ésimo carimbo, obtêm-se $\{\{...\{\{\{s, d, \mathcal{C}_s, \mathcal{R}_s\}, ts^1, \mathcal{C}^1_{ts}, \mathcal{R}^1_{ts}\}, ts^2, \mathcal{C}^2_{ts}, \mathcal{R}^2_{ts}\}, ...\}, ts^n, \mathcal{C}^n_{ts}\}$.

3.3. Validação de Assinaturas

Uma assinatura preservada $\{\{...\{\{\{s, d, \mathcal{C}_s, \mathcal{R}_s\}, ts^1, \mathcal{C}^1_{ts}, \mathcal{R}^1_{ts}\}, ts^2, \mathcal{C}^2_{ts}, \mathcal{R}^2_{ts}\}, ...\}, ts^n, \mathcal{C}^n_{ts}\}$ é válida se:

- o carimbo do tempo ts^n for atualmente válido;
- para todo ts^i, com $1 \leq i \leq n-1$, ts^i era válido na data indicada por ts^{i+1};
- a assinatura s era válida na data indicada por ts^1.

4. Carimbos do Tempo Autenticados

Neste trabalho aumentamos a eficiência e confiabilidade da preservação baseada em carimbos do tempo por meio de um novo esquema de datação, chamado Carimbos do Tempo Autenticados. Esse esquema estende o convencional adicionando duas novas operações, as operações de autenticação e renovação de carimbos, viabilizadas pela cooperação entre a Autoridade de Carimbo do Tempo (ACT) e a Âncora de Confiança do usuário, comumente, a Autoridade Certificadora Raiz (AC-Raiz). Tal esquema tem como objetivo reduzir a velocidade com que crescem os custos relacionados às assinaturas preservadas assim como aumentar as chances de a assinatura permanecer válida pelo tempo necessário.

A operação de autenticação busca reduzir os custos por carimbo adicionado. Através dela é possível substituir as informações necessárias à verificação da autenticidade do carimbo, tais como seu caminho de certificação, por um Certificado de Autenticidade, onde a própria Âncora de Confiança confirma essa propriedade. A operação de renovação, por sua vez, busca reduzir o número de carimbos do tempo adicionados durante a preservação. Por meio dela é possível renovar o Certificado de Autenticidade do carimbo, prolongando sua validade, e assim postergando a adição de novos carimbos.

4.1. Certificados de Autenticidade

Certificados de Autenticidade são documentos eletrônicos, assinados pela Âncora de Confiança, onde ela reconhece a autenticidade dos carimbos do tempo emitidos pela ACT. Por meio desse certificado a Âncora de Confiança persiste a autenticidade do carimbo, tornando desnecessária a validação de sua assinatura bem como do caminho de certificação relacionado. Como resultado, é possível minimizar os custos de armazenamento e validação do carimbo, bem como tolerar a maioria dos fatores que tradicionalmente levariam a perda de sua validade.

De maneira simplificada, tal conceito poderia ser implementado através de um serviço *online*, oferecido pela Âncora de Confiança, onde ela publicaria um Certificado de Autenticidade para cada carimbo do tempo a ela apresentado. Nesse caso, cada carimbo emitido pela ACT, seria encaminhado a Âncora de Confiança, que então validaria sua assinatura e, sendo válida, publicaria um documento eletrônico assinado, onde reconheceria a autenticidade do carimbo.

Apesar de funcional, uma implementação como essa possui problemas de ordem prática que a tornam inviável. Um dos principais problemas está na necessidade de manter a Âncora de Confiança *online* de modo a atender às solicitações recebidas. Algo que contraria boas práticas de segurança caso, por exemplo, essa âncora seja uma AC-Raiz. Outro problema reside no volume de informações necessárias para a produção dos Certificados de Autenticidade. Ela requer o envio de cada um dos carimbos do tempo para a Âncora de Confiança.

Dessa forma, na abordagem adotada, a Âncora de Confiança publica um Certificado de Autenticidade para cada conjunto de carimbos emitido. Nesse caso, ao invés de receber cada um dos carimbos, ela recebe pequenas representações desses conjuntos, calculadas por meio de construções criptográficas como as Árvores de Merkle. O Certificado de Autenticidade de cada carimbo é então formado pelo certificado do conjunto ao qual

ele pertence, e por sua Prova de Associação, capaz de comprovar que o carimbo é um dos elementos desse conjunto.

Tal abordagem permite à Âncora de Confiança operar de maneira periódica, publicando Certificados de Autenticidade apenas ao fim desses períodos, de modo semelhante ao que já ocorre na publicação de Listas de Certificados Revogados (LCRs) [9]. Algo particularmente interessante caso, por exemplo, a Âncora de Confiança seja mantida *off-line* em uma Sala Cofre. Essa abordagem igualmente reduz o volume de informações necessárias para a produção desses certificados.

4.2. Serviços de Suporte

Nesse sentido, a produção de Carimbos do Tempo Autenticados depende de três serviços, o de emissão de carimbos do tempo e os de publicação e renovação de Certificados de Autenticidade. O fornecimento desses serviços ainda requer a manutenção de estruturas de dados pela ACT e pela Âncora de Confiança, respectivamente, o Repositório de Provas de Associação (RPA) e o Repositório de Certificados para Conjuntos (RCC).

A emissão desses carimbos ocorre mediante a solicitação do usuário, seguindo uma versão estendida do protocolo tradicional representada a seguir:

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

Nessa versão estendida, a ACT registra o resumo criptográfico $\mathcal{H}(ts)$ de cada carimbo do tempo emitido no RPA, e informa, por meio de uma extensão não assinada do carimbo, o período pelo qual o seu Certificado de Autenticidade ficará disponível, chamado de Período de Autenticação. Nesse registro, a função de resumo criptográfico usada deve ser segura e igual aquela usada no carimbo.

A publicação do Certificado de Autenticidade de cada carimbo emitido ocorre no início de seu Período de Autenticação e é precedida por uma fase de preparação, onde se dá a solicitação e posterior produção do certificado para o conjunto ao qual ele pertence. Tais Certificados para Conjuntos são solicitados periodicamente pela ACT.

Em cada solicitação a ACT calcula uma representação do conjunto de carimbos do tempo registrados durante o período no RPA, enviando para a Âncora de Confiança um documento eletrônico assinado contendo essa representação, e seus dados de identificação. Por meio de tal solicitação a ACT declara ter emitido os carimbos do tempo ali representados. A representação desses carimbos, por sua vez, é o nó raiz da Árvore de Merkle formada a partir deles e calculada por meio de algoritmos como o TREEHASH [23].

Por igualmente operar de maneira periódica, a Âncora de Confiança apenas valida e registra a solicitação no RCC, aguardando o fim do período para assinar o Certificado de Autenticidade do conjunto ali representado. É com a publicação desse certificado e da Prova de Associação correspondente, que termina a fase de preparação. Tais provas, por sua vez, são os caminhos de autenticação de cada carimbo na Árvore de Merkle, calculados pela ACT por meio de algoritmos de travessia como o de Szydlo [23].

Iniciado o Período de Autenticação, é possível obter o Certificado de Autenticidade do carimbo por meio dos protocolos de solicitação de Provas de Associação e de Certificados para Conjuntos. O primeiro é apresentado a seguir:

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

Nele, o usuário solicita a Prova de Associação de um carimbo, enviando o seu resumo criptográfico $\mathcal{H}(ts)$. Ao receber o resumo, a ACT obtêm a Prova de Associação correspondente no RPA e a retorna para o usuário. Certificados de Conjunto, por sua vez, são obtidos através do seguinte protocolo:

$$\mathcal{U} \longrightarrow \hat{A}ncora : \phi$$
$$\hat{A}ncora \longrightarrow \mathcal{U} : \underbrace{\{id_{\mathcal{ACT}}, \phi\}, \mathcal{S}ign_{\hat{A}ncora}(\{id_{\mathcal{ACT}}, \phi\})}_{sl_{\phi}}$$

Nesse protocolo, o usuário solicita o Certificado para Conjuntos de um carimbo, enviando a representação de seu conjunto. Ao receber a representação, a Âncora de Confiança obtêm o Certificado para Conjuntos correspondente no RCC e o retorna para o usuário. Tal representação pode ser calculada a partir da Prova de Associação do carimbo, empregando o algoritmo para validação de caminhos de autenticação em Árvores de Merkle [19].

Terminado o Período de Autenticação do carimbo, ocorre a destruição de sua Prova de Associação pela ACT. Tal destruição tem por objetivo limitar os custos de armazenamento relacionados a essas provas. Certificados para Conjuntos, por outro lado, permanecem no RCC de modo a suportar futuras renovações do Certificado de Autenticidade do carimbo.

A renovação de Certificados de Autenticidade ocorre mediante a solicitação do usuário, e segue o protocolo a seguir:

$$\mathcal{U} \longrightarrow \hat{A}ncora : \phi$$
$$\hat{A}ncora \longrightarrow \mathcal{U} : \underbrace{\{id_{\mathcal{ACT}}, \phi\}, \mathcal{S}ign'_{\hat{A}ncora}(\{id_{\mathcal{ACT}}, \phi\})}_{sl'_{\phi}}$$

Nele, o usuário solicita a renovação de seu Certificado de Autenticidade, enviando a representação presente no Certificado para Conjuntos. Ao receber tal representação, a Âncora de Confiança obtêm a nova versão do Certificado para Conjuntos no RCC e a retorna para o usuário. O Certificado de Autenticidade é renovado pela substituição do antigo Certificado para Conjuntos pelo novo.

Novas versões do Certificado para Conjuntos ficam disponíveis a medida que as anteriores perdem sua validade. Tal problema ocorre com a revogação ou expiração do certificado de chaves públicas da Âncora de Confiança, ou com o enfraquecimento do esquema de assinatura usado no Certificado para Conjuntos. Nesses casos, cabe a Âncora de Confiança contornar tais problemas e se preciso reassinar o certificado no RCC. Para tanto, pode ser necessário que ela primeiramente renove seu certificado de chaves públicas ou atualize seu esquema de assinatura.

Por fim, de modo a limitar os custos relacionados à renovação dos Certificados de Autenticidade, ocorre periodicamente a otimização do Repositório de Certificados para Conjuntos. Nessas otimizações são removidos do RCC todos os registros cuja função de resumo criptográfico usada não seja mais resistente à segunda inversão. Quando essa resistência é perdida, tanto o registro perde sua serventia, quanto o carimbo do tempo perde sua capacidade de comprovar a integridade da informação datada.

4.3. Preservação de Assinaturas

A preservação de uma assinatura digital por meio de Carimbos do Tempo Autenticados segue os seguintes passos, onde s, d, $\mathcal{C}_s$ e $\mathcal{R}_s$, são, respectivamente, a assinatura, o documento assinado, os certificados do caminho de certificação do signatário e os dados de revogação atuais:

1. **inicialização:** adicionar um carimbo do tempo ts^1 sobre $\{s, d, \mathcal{C}_s, \mathcal{R}_s\}$, obtendo $\{\{s, d, \mathcal{C}_s, \mathcal{R}_s\}, ts^1, \mathcal{C}_{ts}^1\}$;
2. **agendamento:** agendar a sobreposição do carimbo. Essa sobreposição deve ocorrer antes de o carimbo não poder mais ser renovado, sendo, em geral, agendada para um momento próximo ao enfraquecimento da função de resumo criptográfico usada;
3. **autenticação:** autenticar o carimbo durante o seu Período de Autenticação, obtendo $\{\{s, d, \mathcal{C}_s, \mathcal{R}_s\}, ts^1, sl_{ts}^1\}$;
4. **sobreposição:** no momento agendado, validar ts^1. Se inválido, renovar o carimbo. Sendo ts^1 o carimbo possivelmente renovado, adicionar ts^2 sobre $\{\{s, d, \mathcal{C}_s, \mathcal{R}_s\}, ts^1, sl_{ts}^1\}$ obtendo $\{\{\{s, d, \mathcal{C}_s, \mathcal{R}_s\}, ts^1, sl_{ts}^1\}, ts^2, \mathcal{C}_{ts}^2\}$. Caso ts^1 já tenha perdido sua validade, e sua renovação não seja possível, a preservação falha;
5. **repetição:** para os próximos carimbos, repetir os passos 2 e 3 enquanto for necessário preservar a validade da assinatura. Dessa forma, na adição do n-ésimo carimbo, obtêm-se $\{\{...\{\{\{s, d, \mathcal{C}_s, \mathcal{R}_s\}, ts^1, sl_{ts}^1\}, ts^2, sl_{ts}^2\}, ...\}, ts^n, \mathcal{C}_{ts}^n\}$.

4.4. Validação de Assinaturas

Uma assinatura preservada $\{\{...\{\{\{s, d, \mathcal{C}_s, \mathcal{R}_s\}, ts^1, sl_{ts}^1\}, ts^2, sl_{ts}^2\}, ...\}, ts^n, \mathcal{C}_{ts}^n\}$ ou $\{\{...\{\{\{s, d, \mathcal{C}_s, \mathcal{R}_s\}, ts^1, sl_{ts}^1\}, ts^2, sl_{ts}^2\}, ...\}, ts^n, sl_{ts}^n\}$ é válida se:

- o carimbo do tempo ts^n for atualmente válido. Caso já esteja inválido, pode ser preciso autenticar e/ou renovar o carimbo;
- para todo ts^i, com $1 \leq i \leq n-1$, ts^i era válido na data indicada por ts^{i+1}, sendo que a autenticidade de cada carimbo deve ser verificada através de seu Certificado de Autenticidade.
- a assinatura s era válida na data indicada por ts^1.

Um Certificado de Autenticidade $\{\mathcal{A}uth_{ts}, sl_{\phi}\}$, por sua vez, é válido se:

- seu caminho de autenticação, presente na Prova de Associação, for válido;
- a assinatura da Âncora de Confiança, presente no Certificado para Conjuntos, for válida.

5. Análise

Os principais benefícios trazidos pelo uso de Carimbos do Tempo Autenticados são o aumento na eficiência e confiabilidade na preservação das assinaturas digitais. Um outro benefício está na possibilidade de validação *off-line* dessas assinaturas, permitindo que essa ocorra em dispositivos sem conexão de rede. O suporte à emissão, autenticação e renovação desses carimbos, todavia, implica em custos adicionais para a Autoridade de Carimbo do Tempo (ACT) e Âncora de Confiança.

5.1. Custos na Preservação e Validação de Assinaturas

O esquema de datação proposto é capaz de reduzir os custos na preservação e validação de assinaturas digitais por diminuir tanto a quantidade de carimbos adicionados durante a preservação, quanto os custos por carimbo adicionado. Tais melhorais podem ser observadas considerando o modelo matemático apresentado abaixo.

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

$$n_{p_p} = \left\lceil \frac{p_p}{\overline{p}_{ts}} \right\rceil \tag{2}$$

A função 1 reflete as informações armazenadas durante a preservação por carimbos do tempo, onde o custo de armazenamento após um certo período de preservação p_p é dado pelo espaço necessário para cada carimbo adicionado $\alpha(ts^i)$, bem como para as informações necessárias a sua validação, representado por $\alpha(\mathcal{V}^i)$. O número de carimbos adicionados n_{p_p}, por sua vez, é dado pelo período de preservação divido pelo tempo médio pelos quais os carimbos permanecem válidos, até que a sua sobreposição seja necessária.

A quantidade de carimbos do tempo adicionados é reduzida graças as operações de autenticação e renovação que permitem postergar a sobreposição dos carimbos. Graças a elas, dentre todos os problemas que tradicionalmente demandariam essa sobreposição, fica restando apenas um, o enfraquecimento da função de resumo criptográfico usada, geralmente um dos últimos a ocorrer. Essa redução pode ser observada considerando a forma como o período entre as sobreposições passa a ser calculado.

Tradicionalmente, esse período pode ser aproximado pelo prazo de validade médio dos certificados da ACT, pois a sua expiração tende a ser o primeiro problema a demandar a sobreposição do carimbo. De maneira mais realista, é usual considerar a metade desse prazo, pois os carimbos tendem a ser obtidos tanto em seu início quanto no fim. Nos Carimbos do Tempo Autenticados, por outro lado, esse período é dado pela metade daquele pelo qual as funções de resumo criptográfico usadas geralmente permanecem seguras.

Assim, o número de carimbos adicionados diminui pois o período entre as sobreposições aumenta, uma vez que a segurança de funções de resumo criptográfico tende a durar mais que certificados. Algo que pode ser observado ao se considerar recomendações técnicas sobre o período de validade desses certificados [4, 20], bem como o histórico das principais funções de resumo criptográficas até então publicadas. Enquanto o NIST, por exemplo, recomenda prazos de até 3 anos, funções de resumo tendem a permanecer seguras por mais de 10 anos [11, 22].

Os custos por carimbo adicionado, por sua vez, são reduzidos graças a operação de autenticação que modifica a forma como a autenticidade desses carimbos deve ser verificada bem como as informações necessárias para essa verificação. O que tradicionalmente ocorreria pela validação da assinatura do carimbo e de seu caminho de certificação X.509, passa a ocorrer pela validação de seu Certificado de Autenticidade, que tende a requerer tanto um espaço de armazenamento, quanto um tempo para validação, menores.

Os custos de armazenamento por carimbo são reduzidos pois, enquanto os tradicionais requerem a guarda de cada certificado do caminho de certificação, bem como dos

Variável	Valor	Variável	Valor	Variável	Valor
$\alpha(ts)$	700 *bytes*	$\overline{p}_{\mathcal{H}}$	10 anos	n^i_{ts}, n^{tr}_{ts}	604.800 carimbos
$\alpha(\mathcal{C}_{ts})$	3700 *bytes*	$\alpha(\mathcal{A}uth_{ts})$	380 *bytes*	p_{tr}	7 dias
$\alpha(\mathcal{R}_{ts})$	111600 *bytes*	$\alpha(sl_{\phi})$	500 *bytes*	$n^{p_a}_{tr}$	4 períodos
$\overline{p}_{\mathcal{ACT}}$	3 anos	$\alpha(h_{ts})$	20 bytes	$n^i_{\mathcal{ACT}}$	100 ACTs

Tabela 1. Valores usados nas simulações.

dados de revogação relacionados, tais como Listas de Certificados Revogados (LCR) ou respostas OCSP, nos Carimbos do Tempo Autenticados é necessário apenas o armazenamento do Certificado de Autenticidade. Esse último formado por um Certificado para Conjuntos, e por uma cadeia de resumos criptográficos que cresce logaritmicamente em função do número de carimbos que o certificado autentica.

O tempo para validar o carimbo, por sua vez, é menor principalmente por tornar desnecessária a obtenção de informações complementares pela rede. Nos carimbos tradicionais isso é requerido para permitir a validação do caminho de certificação com dados de revogações atuais. Nos Carimbos do Tempo Autenticados isso não ocorre porque o Certificado de Autenticidade é auto-contido. Nesse caso, considerando a implementação tradicional, onde uma Âncora de Confiança é válida se estiver cadastrada no repositório de âncoras do usuário.

De modo a estimar os ganhos trazidos na prática por essa proposta, foram realizadas simulações da preservação de uma assinatura por 50 anos, empregando valores tipicamente encontrados em infraestruturas de chaves públicas (ICP) de grande porte. Dois desses valores requerem maiores considerações, sendo eles o prazo de validade dos certificados da ACT e o período de uso das funções de resumo criptográfico.

O prazo de validade desses certificados é o prazo máximo citado em recomendações técnicas como a do NIST [4], sendo, igualmente, aquele usado na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). O período de uso das funções de resumo criptográfico, por sua vez, considera o histórico das principais funções já publicadas, assim como previsões quanto a segurança das funções atualmente em uso [11, 5, 22].

Tal período pode ser considerado conservador, uma vez que no esquema proposto a resistência à segunda inversão é suficiente para a renovação dos carimbos, e essa tende a se perder certo tempo após tais 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.

Os valores relacionados ao esquema proposto, usados na simulação, por sua vez, foram obtidos a partir de uma implementação dos Carimbos do Tempo Autenticados, realizada sobre uma especificação ASN.1 dos protocolos. Esses valores, assim como aqueles usados na configuração desse esquema de datação, são apresentados na tabela 1. Como alguns deles 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.

Nas simulações, os custos de armazenamento com carimbos tradicionais chegaram a 3,65 MB. Na preservação com Carimbos do Tempo Autenticados, por outro lado, esse custo foi de apenas 15,42 KB, uma redução de 99,59%. Essa redução foi particularmente influenciada pelo espaço necessário para o armazenamento das informações de validação desses carimbos, esse foi 99,23% menor que o requerido pelos carimbos tradicionais.

5.2. Confiabilidade na Preservação de Assinaturas

O esquema de datação proposto é capaz de aumentar a confiabilidade do processo de preservação por carimbos do tempo por tornar toleráveis a maioria dos problemas que tradicionalmente levariam a preservação a falhar. Particularmente, aqueles problemas que impediriam futuras sobreposições do último carimbo até então adicionado, por torná-lo inválido antes do previsto no agendamento. Tradicionalmente tais problemas compreendem:

1. revogação do certificado da Âncora de Confiança;
2. quebra do esquema de assinatura usado pela Âncora;
3. revogação do certificado de alguma das ACs do caminho de certificação;
4. quebra de algum esquema de assinatura usado por essas ACs;
5. revogação do certificado da ACT;
6. quebra do esquema de assinatura usado pela ACT;
7. quebra da função de resumo criptográfico usada pela ACT.

No caso dos Carimbos do Tempo Autenticados, a maioria desses problemas (3, 4, 5 e 6) já é anulada na autenticação do carimbo. Os restantes são tolerados por meio da operação de renovação do carimbo que permite restabelecer a sua validade quando perdida. As únicas exceções são a revogação da Âncora de Confiança, devido a perda de integridade do Repositório de Certificados para Conjuntos (RCC), e a quebra da função de resumo criptográfico usada no carimbo pela ACT. Particularmente, a perda de sua resistência à segunda inversão. Nesses casos, mesmo a renovação do carimbo não é mais possível.

5.3. Serviços de Suporte

Apesar dos benefícios oferecidos por esse novo esquema de datação, seu suporte implica em custos adicionais para a ACT e Âncora de Confiança. No caso da ACT, tais custos estão particularmente relacionados à produção e armazenamento das Provas de Associação, no Repositório de Provas de Associação (RPA).

A produção dessas provas possui custos de memória e processamento que dependem principalmente do algoritmo adotado para a travessia da Árvore de Merkle. No de Szydlo [23], 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 no período. Os custos de armazenamento dessas provas, por sua vez, podem ser representados por meio do seguinte modelo:

$$\theta_{\mathcal{ACT}}(p_o) = \sum_{i=tr-n_{otr}}^{tr-1} (\sum_{j=1}^{n_{ts}^i} \alpha(\mathcal{A}uth_{ts}^{i,j})) + \sum_{i=1}^{n_{ts}^{tr}} \alpha(h_{ts}^i) \quad (3)$$

$$n_{otr} = tr - \frac{tr - n_{tr}^{p_a} + |tr - n_{tr}^{p_a}|}{2} \tag{4}$$

$$tr = \left\lceil \frac{p_o}{p_{tr}} \right\rceil \tag{5}$$

A função 3 reflete as informações armazenadas no RPA durante as operações da ACT. Nessa função, o custo de armazenamento após um período de operação p_o, é dado pelo caminho de autenticação de cada um dos n_{ts}^i carimbos emitidos, nos n_{otr} períodos anteriores que ainda estão em Período de Autenticação, somado ao espaço necessário para o resumo criptográfico h_{ts}^i de cada um dos n_{ts}^{tr} carimbos emitidos no período atual tr. Onde p_{tr} é a duração de um período e $n_{tr}^{p_a}$ é a duração do Período de Autenticação em número de períodos.

No caso da Âncora de Confiança, o suporte a esse esquema de datação traz custos relacionados, principalmente, à reassinatura dos Certificados para Conjuntos e armazenamento desses certificados no RCC. A reassinatura dos certificados possui custos relacionados principalmente ao esquema de assinatura usado e ao número de certificados emitidos e ainda suportados. Número esse que depende da quantidade de ACTs em operação, bem como da duração dos períodos da Âncora de Confiança. Os custos de armazenamento desses certificados, por sua vez, podem ser representados por meio do seguinte modelo:

$$\theta_{\hat{A}ncora}(p_o) = \sum_{i=0}^{ar-1} \left(\sum_{j=1}^{n_{\mathcal{ACT}}^i} \alpha(sl_\phi^{i,j}) \right) + \sum_{i=1}^{n_r^{ar}} \alpha(r^i) \tag{6}$$

$$ar = \left\lceil \frac{p_o}{p_{ar}} \right\rceil \tag{7}$$

A função 6 reflete as informações armazenadas no RCC durante as operações da Âncora de Confiança, desconsiderando as otimizações periódicas do RCC. Nessa função, o custo de armazenamento após um período de operação p_o é dado pelos Certificados para Conjuntos até então publicados para as $n_{\mathcal{ACT}}^i$ ACTs em operação, somado ao espaço necessário para cada uma das n_r^{ar} solicitações recebidas no período atual ar. Onde p_{ar} é a duração de um período de Âncora de Confiança.

De modo a estimar os custos trazidos na prática para a ACT e Âncora de Confiança, foram realizadas simulações das operações dessas entidades por 10 anos. Nessas simulações foram igualmente considerados os valores da tabela 1, sendo que o número de carimbos emitidos em cada período da ACT assume a taxa de um carimbo por segundo durante todo o período.

Nas simulações os custos de armazenamento para a ACT chegaram a 888 MB, se mantendo praticamente constantes devido a remoção das Provas de Associação ao fim do Período de Autenticação dos carimbos emitidos. No caso da Âncora de Confiança, foram necessários 24 MB para o armazenamento dos Certificados para Conjuntos emitidos ao longo desses 10 anos. Nesse caso, não foi considerada a operação de otimização do RCC, que removeria registros conforme a função de resumo criptográfico usada se tornasse insegura.

6. Conclusões

O uso de documentos eletrônicos vem crescendo em importância nas relações entre os cidadãos, empresas e governos, tornando a preservação de assinaturas digitais uma questão fundamental no caso daqueles documentos que precisam ser preservados por um longo período de tempo. Assim, várias estratégias já foram propostas, sendo a sobreposição de carimbos do tempo a principal delas.

Neste trabalho aumentamos a eficiência e confiabilidade dessa estratégia de preservação por meio de um novo esquema de datação, os Carimbos do Tempo Autenticados. Tal esquema reduz drasticamente os custos na preservação e validação de assinaturas digitais, além de oferecer maiores garantias quanto a preservação dessas assinaturas pelo tempo necessário.

Esses benefícios, além da possibilidade de validação *off-line* das assinaturas, tornam esse esquema de datação particularmente interessante para dispositivos com poucos recursos computacionais, ou na preservação de grandes volumes de documentos. Tal esquema pode ser usado não só na preservação de assinaturas digitais, mas igualmente em outras áreas onde carimbos do tempo são empregados. Exemplos dessas áreas incluem a proteção da propriedade intelectual, o comércio e votação eletrônicos.

Trabalhos futuros podem focar na análise formal dos protocolos criptográficos envolvidos nesse esquema de datação, bem como na implementação de mecanismos de herança que permitam migrar o conteúdo dos Repositórios de Certificados para Conjuntos para novas Âncoras de Confiança. Outros tópicos incluem o uso dos Certificados de Autenticidade para a otimização de assinaturas de curto prazo, bem como a integração das operações de autenticação e renovação em outras estratégias de notarização, aumentando sua eficiência e confiabilidade.

Referências

[1] C. Adams, P. Cain, D. Pinkas, and R. Zuccherato. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). RFC 3161 (Proposed Standard), August 2001. Updated by RFC 5816.

[2] R. Anderson. Invited lecture. In *Fourth Annual Conference on Computer and Communications Security, ACM*, 1997.

[3] A. Ansper, A. Buldas, M. Roos, and J. Willemson. Efficient long-term validation of digital signatures. In *Public Key Cryptography*, pages 402–415. Springer, 2001.

[4] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid. Nist sp800-57: Recommendation for key management–part 1: General (revised). Technical report, NIST, 2007.

[5] E. Barker and A. Roginsky. Draft nist sp800-131: Recommendation for the transitioning of cryptographic algorithms and key sizes. Technical report, NIST, jan 2010.

[6] D. Bayer, S. Haber, and W.S. Stornetta. Improving the efficiency and reliability of digital time-stamping. *Sequences II: Methods in Communication, Security, and Computer Science*, pages 329–334, 1993.

[7] K. Blibech and A. Gabillon. A new timestamping scheme based on skip lists. *Computational Science and Its Applications-ICCSA 2006*, pages 395–405, 2006.

[8] D. Chaum and S. Roijakkers. Unconditionally-secure digital signatures. *Advances in Cryptology-CRYPT0'90*, pages 206–214, 1991.

[9] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280 (Proposed Standard), May 2008.

[10] R.F. Custodio, M.A.G. Vigil, J. Romani, F.C. Pereira, and J. da Silva Fraga. Optimized Certificates–A New Proposal for Efficient Electronic Document Signature Validation. In *Public Key Infrastructure: 5th European PKI Workshop: Theory and Practice, EuroPKI 2008 Trondheim, Norway, June 16-17, 2008, Proceedings*, page 49. Springer-Verlag New York Inc, 2008.

[11] European Telecommunications Standards Institute. *Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms*, Nov 2007.

[12] European Telecommunications Standards Institute. *Electronic Signatures and Infrastructures (ESI); CMS Advanced electronic Signatures (CAdES)*, Nov 2009.

[13] European Telecommunications Standards Institute. *Electronic Signatures and Infrastructures (ESI); XML Advanced electronic Signatures (XAdES)*, Jun 2009.

[14] T. Gondrom, R. Brandner, and U. Pordesch. Evidence Record Syntax (ERS). RFC 4998 (Proposed Standard), August 2007.

[15] S. Haber and W. Stornetta. How to time-stamp a digital document. *Advances in Cryptology-CRYPT0'90*, pages 437–455, 1991.

[16] M.K. Just. *On the temporal authentication of digital data*. PhD thesis, Carleton University, 1998.

[17] D. Lekkas and D. Gritzalis. Cumulative notarization for long-term preservation of digital signatures. *Computers & Security*, 23(5):413–424, 2004.

[18] H. Massias and J.J. Quisquater. Time and cryptography. *US-patent n*, 5:12, 1997.

[19] R.C. Merkle. Protocols for public key cryptosystems. 1980.

[20] D. Pinkas, N. Pope, and J. Ross. Policy Requirements for Time-Stamping Authorities (TSAs). RFC 3628 (Informational), November 2003.

[21] G.J. Popek and C.S. Kline. Encryption and secure computer networks. *ACM Computing Surveys (CSUR)*, 11(4):331–356, 1979.

[22] B. Preneel. The First 30 Years of Cryptographic Hash Functions and the NIST SHA-3 Competition. *Topics in Cryptology-CT-RSA 2010*, pages 1–14, 2010.

[23] Michael Szydlo. Merkle tree traversal in log space and time. In *In Eurocrypt 2004, LNCS*, pages 541–554. Springer-Verlag, 2004.

[24] M. A. G. VIGIL, N. SILVA, R. MORAES, and R. F. CUSTODIO. 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*, pages 129–142, 2009.