UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Maurício Simões de Oliveira

ATUALIZAÇÃO DINÂMICA DE POLÍTICAS DE ASSINATURA DIGITAL

Florianópolis

2017

Maurício Simões de Oliveira

ATUALIZAÇÃO DINÂMICA DE POLÍTICAS DE ASSINATURA DIGITAL

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

Florianópolis

2017

Maurício Simões de Oliveira

ATUALIZAÇÃO DINÂMICA DE POLÍTICAS DE ASSINATURA DIGITAL

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

Florianópolis, 18 de janeiro 2017.

Profa. Dra. Carina Friedrich Dorneles
Universidade Federal de Santa Catarina
Coordenador do Curso

Banca Examinadora:

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

Profa. Tereza Cristina Melo de Brito Carvalho, Dra.
Escola Politécnica da Universidade de São Paulo

Prof. Marco Carvalho, Dr.
Florida Institute of Tecnology

Prof. Jean Everson Martina, Dr.
Universidade Federal de Santa Catarina

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

AGRADECIMENTOS

Agradeço primeiramente a minha família, principalmente meus pais Olivia e Pedro por sempre me apoiarem e me incentivarem mesmo nos momentos mais difíceis. São eles as pessoas que mais bem me conhecem e por causa deles consegui chegar onde cheguei.

Agradeço também ao meu orientador Prof. Ricardo Felipe Custódio que me apoiou e me direcionou na execução desse trabalho. Se não fosse pelo seu apoio esse trabalho não teria sido concluído.

Ao Martín Augusto Gagliotti Vigil e Marcelo Carlomagno também meus sinceros agradecimentos, pois sem os dois não teria sido possível alcançar a publicação desse trabalho em forma de artigo. O que foi parte fundamental para execução desse trabalho.

Agradeço também a todos os que participam do LabSEC, principalmente a equipe do projeto códigos de referência: Gabriel Garcia Becker, Douglas Simões Silva, Douglas Marcelino Beppler e Gustavo Zambonin, com quem eu sempre pude discutir as idéias e parar para conversar sobre qualquer assunto aleatório quando estava saturado das tarefas técnicas do dia a dia. Também não posso esquecer da Lucila Allocila, sem seu conhecimento do funcionamento interno da universidade a conclusão do meu mestrado teria demorado muito mais.

Também agradeço a CAPES pelo apoio financeiro fornecido para execução desse mestrado. Sem este apoio seria impossível dedicar tanto tempo à pesquisa e estudo.

Uma longa viagem começa com um único passo.

Lao-Tsé

RESUMO

Políticas de assinatura auxiliam os usuários nos processos de assinatura digital. Entretanto, políticas de assinatura digital não resolvem todos os problemas e acabam introduzindo alguns outros no processo de assinatura e sua manutenção. Este trabalho explica e demonstra como resolver o problema de mudança de política de assinatura. A mudança de política de assinatura é necessária quando os requisitos sobre uma assinatura digital mudam, por exemplo, será necessário um tempo de preservação de uma assinatura digital maior do que o esperado inicialmente. A prática de assinar documentos é bastante antiga, porém, a assinatura digital é bastante recente se comparada com a assinatura manuscrita. Assim como a assinatura de próprio punho, a assinatura digital precisa comunicar seu objetivo, isso é feito através de políticas de assinatura ou de alguma técnica equivalente na maior parte das vezes, o que acaba diferenciando assinaturas digitais de assinaturas manuscritas. Este trabalho trata de políticas de assinatura como foram propostas pelo ETSI. O método proposto para atualização da política indicada na assinatura é totalmente compatível com os padrões de assinatura digital avançada bem como com as especificações técnicas sobre políticas de assinatura dessa entidade. Esse método é composto de dois componentes principais. O primeiro uma extensão para políticas de assinatura que permitem indicar quais as transições previstas. O segundo um atributo com o propósito de ser incluído nas assinaturas digitais indicando se alguma transição ocorreu. Esse método foi testado e avaliado utilizando softwares produzidos para o PBAD. Embora o método seja suficiente para a maioria das transições de políticas que se pode prever, percebeu-se que este método ainda não é suficiente para o arquivamento das assinaturas feitas utilizando políticas de assinatura. Observou-se que o método proposto simplifica a participação dos assinantes no processo de assinatura e que através desse método é possível que uma entidade independente fique responsável pela manutenção das assinaturas digitais.

Palavras-chave: Assinatura Digital Avançada; Infraestrutura de Chaves Públicas; Política de Assinatura; XAdES; CAdES.

ABSTRACT

Signature policies help users in the digital signature process. However, signature policies do not solve all digital signature process problems and introduce some new ones. We explain and show how to solve the necessity to change the signature policy. The change of signature policy need to happen when the digital signature requirements change, for example, the verifier needs the signature to be valid for a greater period than initially thought. Sign is a old practice, but, digital signatures are relatively new to this practice if we are comparing with manuscript signatures. Digital signatures, as manuscript signatures, need to communicate their commitment, this most of time is done trough signature policies or some equivalent technology, this ends up differentiating digital signatures from its manuscript counterparts. The signature policies used in this work follow the proposes of ETSI. The method we propose for updating the signature policy complains with the formats of advanced electronic signature as with signature policies proposed by ETSI. We proposed a method that can be split in two main components. First component is an extension for signature policies that indicates what transitions are possible. Second component is an attribute compatible with CAdES and XAdES that indicates a change in the signature policy. Tests of the method were made using the reference code for Brazilian Digital Signature Standards(PBAD). The method can solve the majority of transitions in the signature policy of a digital signature, however, the transitions needed for archieving a signature cannot be solved by this method. We noted that the method proposed simplifies the iteration of signers in the process. We noted as well that an idependent entity can do the maintenance of the digital signature.

Keywords: Advanced Electronic Signatures. Public key infrastructure. XAdES. CAdES.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AC	Autoridade Certificadora
AD	Assinatura Digital
AIA	Authority Information Access
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation 1
BER	Regras de Codificação Básicas
BES	Assinatura Eletrônica Básica
CAdES	Assinatura Eletrônica Avançada em CMS
CMS	Sintaxe de Mensagem Criptográficas
DER	Regras de Codificação Distinta
EPES	Assinatura Eletrônica com Política Explícita
ETSI	European Telecommunications Standard Institute
ICP	Infraestrutura de Chaves Públicas
ISO	Organização Internacional para Padronização
ITI	Instituto Nacional de Tecnologia da Informação
LCR	Lista de Certificados Revogados
LPA	Lista de Políticas Aprovadas
ODF	Formato de Documento Aberto
OID	Object Identifier
OpenXML	Formato de Documento Aberto em XML
PA	Política de Assinatura
PAdES	Assinatura Digital Avançada em PDF
PBAD	Padrão Brasileiro de Assinatura Digital
PDF	Formato de Documento Portátil
RA	Referência de Arquivamento
RB	Referência Básica
RC	Referência Completa
RFC	Request for Comments
RT	Referência de Tempo
RV	Referências de Validação
XAdES	Assinatura Digital Avançada em XML
XML	Extensible Markup Language

XMLDSig	Assinatura Digital em XML
XSD	Linguagem de Definição de Esquema XML
URI	Identificador Universal de Recursos
URL	Localizador Universal de Recursos
URN	Nome Universal de Recursos

SUMÁRIO

1 INTRODUÇÃO

Documentos eletrônicos são muito utilizados em sistemas de informação e comunicação. Esses sistemas precisam manter o registro sobre a procedência e a integridade desses documentos e isso tem sido uma tarefa muito difícil. Muitas vezes esses documentos podem fazer parte de um acordo comercial ou ter algum outro valor jurídico. Provar a autenticidade e integridade desses documentos é, dessa forma, de suma importância. As assinaturas digitais são normalmente utilizadas como uma solução para isso. Elas proveem evidências sobre a autenticidade e integridade do documento eletrônico através de processos criptográficos.

Entretanto, o uso de assinaturas digitais no contexto de documentos eletrônicos não é uma tarefa simples. Assinaturas digitais necessitam de dados adicionais para que seja possível verificar as suas propriedades de segurança, tais como, a integridade e a autenticidade. Esses dados podem ser representados e obtidos de diversas formas. Os padrões e normas de assinatura digital de documentos eletrônicos propostos na literatura técnica e científica preveem procedimentos de como isso deve ser feito. Esses padrões estabelecem regras de como representar a informação de verificação das assinaturas e muitas vezes tratam a forma como essas informações podem ser obtidas.

Em geral, a padronização de formatos de assinatura digital é independente de algoritmos criptográficos ou outros serviços computacionais que possam vir a ser utilizadas. Entretanto, normalmente são estabelecidos quais algoritmos e serviços devem ser utilizados a fim de garantir que todos sejam capazes de verificar as assinaturas.

Um dos problemas desses padrões é que, normalmente, não capturam as regras de negócio em sua totalidade. Para que dois sistemas ou agentes diferentes possam trocar documentos eletrônicos assinados é necessário um conjunto de metadados estabelecendo quais informações são necessárias para possibilitar o reconhecimento desses documentos e de suas assinaturas. O principal interesse é do agente que receberá os documentos, pois ele precisa verificar a autenticidade e integridade desses documentos. O agente que produz os documentos também tem interesse de que os documentos assinados sejam aceitos como válidos pelo agente receptor.

Existem várias maneiras de se deliberar quais informações são necessárias para a validação de uma assinatura digital. Isso pode ser feito através de um acordo verbal entre o assinante e o destinatário do documento ou através da inclusão das regras de validação em arquivos próprios para esse fim.

Normalmente, os padrões de assinatura definem quais os dados podem ser incluídos nesses arquivos. Entretanto, muitas das informações a ser incluídas são situacionais e podem vir a ser críticas para que a validação da assinatura seja possível. Pode-se tomar, por exemplo, o padrão Assinatura Eletrônica Avançada em XML (XAdES) (1–3). É possível incluir no arquivo da assinatura vários dados, como certificados digitais utilizados para verificar a procedência da chave criptográfica utilizada para gerar a assinatura, carimbos do tempo para prover informação sobre quando a assinatura foi produzida ou até mesmo metadados sobre onde a assinatura foi gerada. Diante de todas essas possibilidades, é possível que o verificador e o assinante tenham problemas para entrar num acordo sobre quais dados devem ser incluídos. Para amenizar e simplificar essa negociação são utilizadas políticas de assinatura (4). Uma política de assinatura define formalmente quais os dados devem ser incluídos na assinatura pelo signatário e que deverão ser verificados pelo agente verificador.

Os usuários de assinatura digital podem ter dificuldades em identificar qual a política de assinatura deve ser adotada para uma determinada situação em particular, uma vez que a política definida pode não ter uma descrição clara o suficiente. Além disso, as políticas colocadas a disposição do assinante, podem ser muito parecidas, o que dificulta a escolha da mais adequada por parte do signatário do documento eletrônico. Pode-se ainda tecer algumas criticas à rigidez imposta pelas políticas de assinatura, dependendo da forma como estas são aplicadas à assinatura, por impedirem o verificador de modificar alguns dos requisitos da assinatura digital. Alterar os requisitos sobre a assinatura digital se justifica pois pode ser uma maneira de responder às mudanças no contexto em que a assinatura está incluída. Um exemplo bastante direto é a necessidade de provar a procedência do documento por um período maior do que o inicialmente previsto. Finalmente, ainda existem problemas quanto o arquivamento de assinaturas digitais. Pois como políticas de assinatura fazem parte do documento eletrônico, deve existir um procedimento para arquivar a política com o documento ele-

trônico de tal forma que a validação da assinatura seja possível mesmo na ausência, por exemplo, da estrutura fornecida pelos agentes envolvidos para uso das assinaturas digitais.

Tanto o documento eletrônico quanto a assinatura digital devem ser descritos de tal forma que se garanta interoperabilidade entre diferentes sistemas de informação. Os formatos mais utilizados para representação de documentos eletrônicos são: OpenXML (5); ODF (6) e o PDF (7). Todos esses formatos, de maneiras diferentes, permitem a representação de assinaturas digitais. Todavia esses padrões não são interoperáveis entre si. Para evitar atrelar a assinatura digital a um determinado formato de documento eletrônico, os padrões de assinatura digital normalmente consideram o documento como um conjunto de dados, independentes do documento eletrônico. Podemos citar como exemplos o XAdES (1–3), o CAdES (8–11) e o PAdES (12–17). Nesses padrões, produz-se uma assinatura que pode vir a conter um campo que embarca o documento eletrônico sendo assinado. Além do documento poder ser embarcado dentro da assinatura, é comum colocar a assinatura em arquivos separados ou incluí-la dentro do documento. Por exemplo, os formatos de representação de documentos eletrônicos PDF, ODF e OpenXML permitem que a assinatura seja embarcada dentro do documento.

Dado que é possível produzir uma assinatura digital de diversas maneiras, é interessante produzir meios e ferramentas que auxiliem os usuários na escolha da melhor forma de produzir suas assinaturas digitais. Orgãos reguladores podem fazer uso dessas ferramentas e melhorar a interoperabilidade das assinaturas. Políticas de assinatura são ferramentas bastante interessantes nesse contexto, pois elas possuem tanto uma parte textual, quanto uma parte processável por máquina. A parte textual ajuda o assinante a escolher a melhor política para um determinado contexto. A parte processável por máquina fornece as regras que serão utilizados tanto pela plataforma computacional de geração da assinatura quanto por aquela responsável por verifica-la. Assim, políticas de assinatura podem ser utilizadas pelos usuários na produção de assinaturas digitais que correspondem as expectativas dos envolvidos, mitigando possíveis confusões em acordos.

Políticas de assinatura tem sido muito utilizadas em processos de assinatura de documentos eletrônicos. Entretanto, os formatos, protocolos e soluções de políticas de assinatura, propostos na literatura,

ainda acarretam dificuldades para os usuários. Por exemplo, as políticas existentes na literatura não permitem que seja estendido o período de validade do documento eletrônico, uma vez que esse é definido quando o documento é assinado. Essa e outras deficiências das políticas acabam forçando os usuários a utilizar assinaturas digitais mais custosas de forma a previnir até mesmo os casos mais improváveis. Este trabalho é uma proposta de extensão para políticas de assinatura que visa resolver esse tipo de problema.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Propor um método que possibilite o controle das atualizações do nível do acordo para Políticas de Assinatura Digital de Documentos Eletrônicos.

1.1.2 Objetivos Específicos

Os objetivos específicos são os seguintes:

- Especificar uma estrutura de extensão para políticas de assinatura e adapta-lá aos padrões XAdES e CAdES;
- Verificar a funcionalidade das extensões propostas através de um protótipo;
- Manter a compatibilidade dessas extensões com os formatos já estabelecidos;
- Comparar o novo processo de assinatura com os processos de assinatura mais utilizados.

1.2 MÉTODO

O problema da rigidez no uso da políticas de assinatura nos padrões foi identificado através da experiência do autor desenvolvendo trabalhos relacionados com o tema e também a partir de relatos de especialistas no tema. Adicionalmente, a partir de experimentos realizados em implementações dos padrões CAdES e XAdES foi possível

vislumbrar uma solução para esse problema.

De posse da fundamentação teórica necessária foi formulada a proposta de solução. Esta então foi discutida e avaliada, através de protótipos e artefatos produzidos, a fim de demonstrar a viabilidade da solução do problema proposto e a sua utilidade para a comunidade. Durante a execução deste trabalho buscou-se utilizar apenas técnicas já bem estabelecidas, ou seja, não fugir ou contradizer os padrões mais utilizados: CAdES, XAdES e PAdES. Buscou-se nesse trabalho apenas estender os padrões, de forma que a adoção da proposta seja o mais factível possível.

1.3 JUSTIFICATIVA

É de interesse de todos que as assinaturas digitais se adequem o melhor possível às necessidades dos usuários, sendo essas necessidades tanto dos que regulam as regras quanto dos que necessitam de assinaturas digitais no seu negócio. Embora os padrões contemplem as soluções de interoperabilidade e questões de segurança, as propostas CAdES (8–11) e XAdES (1–3) e PAdES (12–17) ainda carecem da flexibilidade necessária para se adequarem totalmente aos negócios cotidianos das organizações, tornando por vezes a adoção de tais soluções demasiadamente custosas. Não é de conhecimento do autor a existência de um trabalho que trate deste problema.

A necessidade dessa flexibilidade também foi observada através do envolvimento do grupo de pesquisa na produção de ferramentas e em discussões com os gestores, reguladores e usuários dos padrões de assinatura digital no Brasil. Assim, entende-se como de interesse da comunidade a proposta de uma solução para o problema.

É possível observar, por exemplo, ao utilizar as políticas de assinatura (18) para o formato de assinatura CAdES (8, 10, 11), uma discrepância entre as expectativas do usuário quando a política de assinatura é referenciada de forma explícita ou de forma implicita. Com a validação de forma implícita, cabe a aplicação ou usuário do sistema decidir em qual contexto a assinatura digital se encontra e qual a política de assinatura deve ser usada.

Entretanto, quando a assinatura digital explicita a política de

assinatura referenciando o arquivo de política contendo a descrição das informações necessárias à validação assinatura, os requisitos de informações que devem ser incluídas na assinatura digital não podem ser mais alterados. Ardieta et. al. (19) afirmam que é importante definir a política de assinatura de forma explícita para evitar que a assinatura digital seja mal interpretada e possa ser utilizada de forma a obter vantagem sobre o assinante, assumindo, por exemplo, que o tipo de comprometimento que a assinatura representa seria diferente do primeiramente intencionado.

Além disso, em alguns cenários seria interessante ter a possibilidade de mudar os requisitos de informação a ser incluídos na assinatura digital. Por exemplo, se a assinatura digital for expirar antes que o processo em que ela está envolvida seja concluído, o verificador poderia incluir as informações de validação na assinatura para estender a sua validade.

O Brasil, assim como vários outros países, tem adotado padrões e políticas de assinatura. No Padrão Brasileiro de Assinatura Digital (PBAD)(20), por exemplo, podemos observar que a versão textual da política de assinatura permite a inclusão de diferentes atributos opcionais em distintas políticas de assinatura. Entretanto, nas versões codificadas para máquina não há qualquer referência aos atributos opcionais.

É de entendimento do autor que a adição de atributos opcionais na versão textual das políticas de assinatura no PBAD são uma consequência da limitação das políticas de assinatura como definidas em ASN.1 (21) e XML (4). O uso de alguns atributos opcionais pode fazer com que uma assinatura num determinado perfil fique idêntica a uma assinatura que utiliza outra política. Isso pode descaracterizar as políticas de assinatura uma vez que, se considerados os atributos opcionais, não há diferença entre utilizar uma ou outra política de assinatura.

1.4 MOTIVAÇÃO

Desde 2001 vêm-se desenvolvendo projetos de pesquisa científica e tecnológica relativos à assinatura digital e à certificação digital no Laboratório de Segurança em Computação (LabSEC). Dentre esses projetos, trabalhou-se no desenvolvimento de um padrão de assinatura digital para o Brasil e na implementação dos códigos de referência para

mesmo, incluindo um gerenciador de políticas de assinatura. De posse dos conhecimentos adquiridos na execução desses projetos e da experiência trocada com outros pesquisadores que vêm executando trabalhos relacionados às dificuldades encontradas na adoção de assinaturas digitais, percebeu-se que a assinatura digital ainda carece de praticidade e é uma área de grande interesse tanto no Brasil como no exterior.

Esse trabalho é fruto de um esforço de pesquisa desenvolvido durante vários anos no LabSEC, em que todos os trabalhos visam aproveitar melhor os serviços de uma infraestrutura de chaves públicas (ICP). Consideramos que grande parte dos problemas de adoção de assinaturas digitais advém de problemas ainda não explorados na literatura como o problema tratado nesse trabalho.

1.5 LIMITAÇÕES DO TRABALHO

Mesmo que a transição de políticas de assinatura por vezes se justifique pelo interesse em estender a validade de uma assinatura digital, esse trabalho não busca fornecer todo o conjunto de procedimentos para que isso possa ser feito. Não foi tratado também a forma como um emissor de políticas de assinatura pode identificar as relações de transição entre políticas de assinatura. Entende-se que esse procedimento de identificação das transições é de conhecimento tácito dos emissores, uma vez que são eles que estabelecem as diferentes políticas de assinatura. Esse trabalho concentra-se em possibilitar a transição e demonstrar os fatores envolvidos.

Esse trabalho apenas define as extensões para as políticas nos formatos ASN.1 e XML, associadas aos formatos de assinatura CAdES e XAdES respectivamente. O formato de assinatura PAdES, mesmo que suporte processos muito parecidos com os formatos anteriormente citados, não possui um formato de política de assinatura estabelecido associado a ele. Por essa razão, não foi considerado relevante a protosta desse método para algum formato de política de assinatura para PAdES.

1.6 CONTRIBUIÇÕES DESSE TRABALHO

Nesse trabalho foi esposto um método para possibilitar o processo de transição de política de assinatura. Esse processo advém dos requisitos de assinatura digital e da não compatibilidade da política de assinatura com esses processos na literatura sobre o assunto. O método proposto permite que emissores de políticas de assinatura caracterizem as transições de políticas possíveis. Foram definidos os atributos para que os usuários de assinatura digital pudessem usufruir da transição de políticas de assinatura de forma totalmente transparente.

Para proposta de tal método, foi feito todo um levantamento sobre os processos de assinatura digital. Esses processos envolvem vários conceitos que vão além das primitivas criptográficas. O levantamento feito mostra uma visão de mais alto nível sobre a assinatura digital, demonstrando o papel da mesma em processos de documentos eletrônicos.

Nesse trabalho são descritas as ferramentas "Gerenciador de Políticas de Assinatura" e "Códigos de Referência", do qual o autor desse trabalho participou ativamente. Essas ferramentas são amplamente utilizadas em processos dentro da infraestrutura do PBAD.

Experimentos com o método proposto foram feitos utilizando ferramentas desenvolvidas para o PBAD. Para tal foram implementadas as extensões de políticas de assinatura na ferramenta "Gerenciador de Políticas de Assinatura". Também foram implementados o suporte ao processamento dessas extensões e os atributos associados à essas extensões nos "Códigos de Referência do PBAD". Essas implementações demonstram a viabilidade da solução proposta tanto no PBAD como em outras soluções baseadas no CAdES e XAdES.

1.7 CONTEÚDO DO TRABALHO

No Capítulo 2 são explicados os conceitos de assinatura digital. Na Seção 2.9 desse capítulo, é discutido o padrão de assinatura digital adotado no Brasil que serviu como caso de estudo para este trabalho. No Capítulo 3, são discutidos os trabalhos sobre política de assinatura que estão relacionados com esse trabalho de alguma maneira, seja com definições ou com exemplos de uso. Na Seção 3.4 desse capítulo, é explicada a política de assinatura, explicitando as informações contidas

nela. No Capítulo 4, é apresentada a extensão de política proposta nesse trabalho. No Capítulo 5, é apresentado o protótipo desenvolvido para avaliação da proposta desse trabalho junto dos resultados obtidos. Finalmente, no Capítulo 6 são sumarizados os resultados obtidos com esse trabalho e discutidos os problemas ainda em aberto, bem como propostas para futuras soluções desses problemas.

2 ASSINATURA DIGITAL DE DOCUMENTOS ELETRÔNICOS

2.1 INTRODUÇÃO

Este capítulo contém o referencial teórico que serve de base para o entendimento assinaturas digitais e documentos eletrônicos. São apresentados os principais conceitos relativos ao tema. O material do qual esse capítulo trata advém de uma revisão da literatura técnica e científica, e também de normas e padrões internacionais.

A Seção 2.2 expõe um histórico da assinatura. É dado ênfase na assinatura digital, relatando os trabalhos científicos que serviram de base para confecção dos padrões relacionados ao uso de assinatura digital. Nesse histórico, observa-se que a necessidade de autenticar documentos é muito antiga. Entretanto, a autenticação de documentos eletrônicos é relativamente recente.

Na Seção 2.3, são explicados os conceitos fundamentais sobre uma Infraestrutura de Chaves Públicas (ICP). O entendimento de ICP é fundamental para a compreensão dos processos de assinatura digital de documentos eletrônicos. Uma ICP trata de emitir os certificados digitais das entidades envolvidas no processo de geração e verificação de assinaturas digitais. Ainda nessa seção, é explicado o processo de revogação de certificados, que permite um usuário da ICP comunicar os outros que por alguma razão perdeu o controle de sua chave.

Juntamente com os certificados digitais de chave pública são explicados também os certificados de atributo. Esses certificados são utilizados para representar atributos associados a alguma identidade. Atributos podem ser utilizados em assinaturas digitais para caracterizar tipos de comprometimento.

Ainda nessa seção são descritos os carimbos do tempo, que são artefatos providos dentro da ICP por carimbadoras. Esses artefatos tem por finalidade prover uma fonte confiável de tempo dentro de uma ICP. Carimbos do tempo são fundamentais para assinaturas eletrônicas avançadas.

A Seção 2.4 apresenta o padrão *Cryptographic Message Syntax*

(CMS), que é utilizado para descrever mensagens criptográficas, incluindo a de assinatura digital, de interesse para esse trabalho. Esse padrão é a base para especificação do *CMS Advanced Electronic Signature* (CAdES). Em seguida, é apresentado o formato *XML Digital Signature* (XMLDSig), na Seção 2.5. Esse formato é amplamente utilizado na web. Ele serve de base para o formato *XMLDSig Advanced Electronic Signature* (XAdES). A forma de se fazer assinaturas em documentos PDF é apresentada, na Seção 2.6. Documentos PDF são assinados utilizando assinaturas CMS. O padrão PDF especifica estruturas especiais para o uso de assinaturas digitais. Entretanto, como o padrão PDF embarca a assinatura CMS dentro de si, são especificadas particularidades no uso e processamento do CMS. Existe uma proposta para o formato *PDF Advanced Electronic Signature (PAdES)* também.

Assinaturas digitais avançadas são descritas na Seção 2.7. Esse tipo de assinatura permite ao usuário que se façam assinaturas aderentes a uma política de assinatura, por exemplo. Formatos de assinatura que atendem a esses requisitos são o CAdES e o XAdES. O detalhamento de como esses formatos são utilizados com políticas de assinatura é feito no Capítulo 3.

Em seguida, na Seção 2.8, é apresentada a proposta de formato PAdES. Esse formato, de maneira semelhante aos dois apresentados na seção anterior, adiciona ao PDF formas de incluir informações para estender a validade da assinatura por um longo prazo. Como exemplo das informações adicionadas podemos citar: dados de validação e carimbos do tempo. É interessante resaltar que embora esse formato seja análogo aos formatos CAdES e XAdES, ele não possui um formato próprio de política de assinatura bem estabelecido associado a ele, como acontece com os formatos CAdES e XAdES.

O Padrão Brasileiro de Assinatura Digital (PBAD) é na Seção 2.9. Esse é o padrão de assinatura digital atualmente em uso no Brasil. Assinaturas aderentes a esse formato atendem aos requisitos dos padrões internacionais CAdES e XAdES. Entretanto, o PBAD estabelece requisitos adicionais para suas assinaturas. Diferentemente dos padrões internacionais, o PBAD incluí a forma de distribuição de políticas de assinatura. Ferramentas feitas para esse padrão de assinatura digital foram utilizadas nos experimentos desse trabalho.

Na Seção 2.10 é discutida a relação entre assinaturas digitais e as-

sinaturas manuscritas. Embora assinaturas digitais sejam amplamente utilizadas, a percepção dos usuários mostra que assinaturas digitais não são encaradas de maneira equivalente a assinatura de próprio punho. Os usuários tendem a confiar menos na assinatura digital e acreditar que ela não será aceita. Políticas de assinatura são uma ferramenta que pode auxiliar nesse problema, pois formaliza o acordo entre as partes para a aceitação da assinatura digital.

2.2 ASSINATURA DE DOCUMENTOS

A prática de autenticar documentos através da escrita do nome do signatário ao documento começou a ser usada no Império Romano por volta do ano de 439 A.C, durante o reinado do Imperador Valentiniano III (22). A regra, conhecida como *subscripto*, consistia em adicionar ao final do documento uma sentença curta, estabelecendo que o signatário "subscrevia" o documento. Essa forma de assinar documento, através da escrita do nome do assinante ao final do documento, se espalhou pela civilização ocidental e permaneceu inalterada por mais de 1.400 anos.

Em todo esse período, os documentos eram suportados por algum material físico, como por exemplo, o papel. Este material de suporte provia algumas das propriedades que, em conjunto com a subscrição do nome do assinante, permitia provar a autenticidade do documento.

Entretanto, com o advento do telégrado em 1844, surgiu o problema de como autenticar documentos eletrônicos. Não havia mais o material físico para prover certas propriedades que permitiam estabelecer a autenticação do documento. Assim, era possível alterar partes do documento, sem deixar qualquer evidência de que fora alterado. Apesar disso, do ponto de vista legal, a assinatura transmitida pelo telégrafo foi considerada, em 1867, como tendo os mesmos requisitos das assinaturas de próprio punho (23).

Contudo, somente em meados da década de 1970, quando foi proposta a criptografia assimétrica por Diffie e Hellman (24), vislumbrou-se uma forma de se assinar e verificar a assinatura de documentos eletrônicos, com algumas caracterísitcas similares àquelas do documento em papel. Pela primeira vez era possível, usando somente a representação eletrônica, verificar-se a integridade da mensagem e imputar a sua

autoria. A assinatura digital, como ficou conhecida, consistia de um conjunto de bits, que além de poder ser usado para verificar a integridade do documento eletrônico, ou seja, se era o mesmo documento que foi produzido quando foi assinado, fornecia as informações relativas a quem o subscreveu.

Em seu classico artigo, Diffie e Hellman propuseram o uso de duas chaves criptográficas, distintas, para cifrar e decifrar mensagens eletrônicas. Uma das chaves era usada para cifrar a mensagem. E somente a outra, diferente da primeira, poderia ser usada para decifrar essa mensagem. A ideia era manter em sigilo uma das chaves e a outra torna-la pública. A chave criptográfica secreta ficou conhecida como chave privada e a tornada pública, como chave pública.

A autenticidade de uma mensagem eletrônica poderia ser verificada da seguinte forma. O signatário usava a sua chave privada para cifrar a mensagem. O destinatário da mensagem somente poderia decifrar essa mensagem, utilizando a chave pública do signatário. A mensagem decifrada era, então, comparada à mensagem original. Se fosse a mesma, teríamos a evidência da autoria, uma vez que, somente quem possuia a chave privada poderia ter produzido aquela mensagem cifrada. Além disso, essa comparação provia a evidência relativa a integridade da mensagem, ou seja, o fato da mensagem decifrada ser a mesma da mensagem original, constitui numa evidência de sua integridade.

Apesar da revolução que foi proposta por Diffie e Hellman, a prática mostrou que não seria simples a implementação em larga escala das ideias da criptografia assimétrica. Duas são as principais dificuldades. Primeiro era preciso gerar e manter secreta a chave privada. E, quando não fosse mais necessária, prover algum meio de destruí-la. Além disso, poderia ser necessário publicizar que essa não era mais a chave privada de um determinado usuário. A segunda dificuldade está relacionada a como a chave pública poderia ser vinculada a um determinado usuário e como poderia ser esse vínculo divulgado.

Para proteger a chave privada, costuma-se utilizar dispositivos criptográficos, tais como smartcards ou módulos de segurança criptográfica. Esse dispositivos são especialmente concebidos para gerir o ciclo de vida de chaves criptográficas, e para manter secreta a chave privada, através de proteções físicas (25, 26). Por exemplo, em tais dis-

positivos, é possível gerar a chave privada e usá-la, mas não é possível obter uma cópia da mesma. A destruição da chave, quando não mais necessária pode ser feita pela destruição do dispositivo.

Khonfelder, em sua dissertação de mestrado no Instituto de Tecnologia de Massachusetts (MIT), propôs tratar esses desafios através do uso de certificados digitais (27). Um certificado digital é um documento eletrônico, digitalmente assinado, que contém um conjunto de atributos. Uma vez que o certificado é assinado, tais atributos são associados um ao outro. Entre os atributos, destacam-se o identificador do titular do certificado e a sua chave pública.

O certificado digital pode ser auto-assinado, ou pode ser assinado por uma terceira parte, denominada de autoridade certificadora. A confiança num certificado digital depende da confiança que se tem do seu signatário. Assim, é preciso confiar na entidade responsável pela assinatura do certificado. Diz-se que um certificado auto-assinado é um certificado raiz.

A gestão do ciclo de vida de certificado digital, conforme proposto por Khonfelder, mostrou-se muito complexa. Para viabilizar a sua utilização, estabeleceu-se uma série de entidades de prestação de serviços, organizados na forma de uma infraestrutura de chaves públicas (ICP) (28).

Apesar das entidades componentes de uma ICP estarem bem definidas, a prática tem mostrado que não é simples a implantação de uma ICP para viabilizar o processo de assinatura digital de documentos eletrônicos (29–31). Entre as críticas, estão o alto custo associado a manutenção dos serviços da ICP (32–34), e do entendimento de que, mesmo diante dos insumos da ICP, a assinatura digital ainda não provê os requisitos de segurança e funcionalidade desejados (35, 36).

A assinatura digital deve prover as seguintes propriedades (37, pg. 415):

a) Deve verificar o autor e a data e hora de assinatura;

b) Deve autenticar o conteúdo do documento ao tempo da assinatura;

c) Deve ser verificável por terceiras partes, para resolver disputas.

Com base nessas propriedades gerais, pode-se listar os requisitos

para uma assinatura digital:

a) A assinatura deve ser um conjunto de bits que deve, de alguma forma, depender do documento que está sendo assinado;

b) A assinatura deve estar de alguma forma relacionado a um identificador do signatário, ou seja, deve ser possível conhecer a identidade do assinante do documento eletrônico;

c) Deve ser fácil produzir e verificar a assinatura;

d) Deve ser inviável forjar a assinatura, seja modificando o documento para uma dada assinatura, seja construindo uma assinatura falsa para um dado documento;

e) Deve ser fácil manter uma cópia da assinatura. Idealmente, a assinatura deveria ser pequena, se comparada ao tamanho do documento.

Da mesma forma que os documentos eletrônicos, as asssinaturas digitais precisam ser devidamente descritas. Linguagens especiais tem sido proposta para isso. Além de uma linguagem próprio, também tem sido propostos formatos padrões para imersão de todos os atributos da assinatura. Em geral, todos os formatos de assinatura digital precisam incluir alguns dados em sua mensagem para que a validação seja possível. A forma como esses dados são incluídos na mensagem varia de formato para formato, e também pode depender de outras tecnologias, mas devido a forma como a assinatura digital baseada em criptográfia assimétrica foi definida, algumas informações indispensáveis podem ser identificadas. Essas informações são as seguintes:

- referência ao arquivo assinado através de resumo criptográfico;
- identificação do par de algoritmos utilizados (criptografia assimétrica e resumo criptográfico);
- identificação do autor da assinatura digital (certificado digital, referência a chave pública ou somente um nome identificador).

De forma a manter a assinatura pequena, o que geralmente é feito é assinar o resumo criptográfico do documento. O resumo criptográfico possui um tamanho definido fixo e é utilizado para identificar unicamente o documento eletrônico. A cifra assimétrica é executada sobre esse valor e não sobre o documento eletrônico em si. O processo geral de assinatura digital pode ser observado na Figura 1.

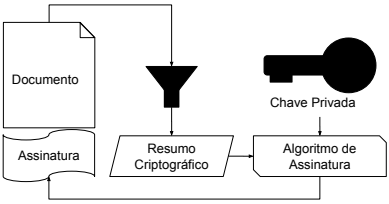


Figura 1 – Processo de assinatura digital. O elemento básico constituinte da assinatura digital é o resumo criptográfico do documento eletrônico, cifrado com a chave privada do signatário.

Neste trabalho, não é especificado um algoritmo criptográfico específico. Todas as análises e proposições desse trabalho são genéricas, e podem ser adotados quaisquer algoritmos de criptografia para produzir a assinatura. No entanto, de forma geral, é presumido a utilização de um algoritmo de criptografia assimétrica, associado a um algoritmo de resumo criptográfico tais como o RSA (38) ou ECDSA (39).

2.3 CERTIFICADOS DE CHAVE PÚBLICA E SUA INFRAESTRUTURA

Um formato bastante utilizado para identificar as chaves públicas das assinaturas digitais é o formato de certificado digital X.509 (40). Esse formato de certificado digital de chave pública é utilizado num sistema hierárquico de identificação.

Certificados digitais de chave pública nesse sistema hierárquico são emitidos por autoridades certificadoras. Sendo que a autoridade certificadora mais alta na hierarquia é especial, pois ela emite seu próprio certificado digital. Essa autoridade certificadora é conhecida como âncora de confiança.

Definição 2.1. Âncoras de confiança: A âncora de confiança representa a entidade a qual a confiança é assumida pelo usuário da ICP. Normalmente esse tipo de entidade tem um certificado auto-assinado.

As autoridades certificadoras podem emitir certificados digitais para outras autoridades certificadoras ou para entidades finais. O que

permite identificar se uma autoridade certificadora pode emitir é uma extensão chamada *KeyUsage* no seu próprio certificado digital. A representação de uma infraestrutura de chaves públicas (ICP) pode ser observada na Figura 2. Os nodos identificam as entidades, as setas contínuas identificam que existe um certificado emitido e as linhas pontilhadas indicam que aquela entidade assina uma LCR periodicamente.

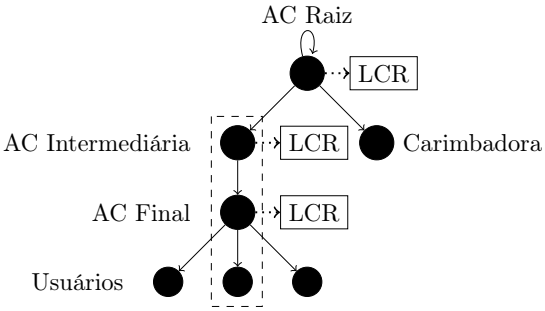


Figura 2 – Infraestrutura de Chaves Públicas.

Certificados digitais de chave pública são arquivos de assinatura digital. O assinante é o emissor do certificado, nesse caso, será sempre uma autoridade certificadora. A assinatura do certificado atrela as informações de identificação a chave pública. O padrão X.509 especifica o procedimento para obtenção do resumo criptográfico da chave pública e informações de identificação.

Todos os certificados emitidos dentro de uma ICP estão sujeitos a políticas de certificação. Essas políticas definem as práticas de certificação. Por práticas de certificação entende-se os procedimentos que uma autoridade certificadora atente para obtenção das informações de identificação postas nos certificados que emite. As políticas de certificação podem definir também quais informações serão fornecidas pelos certificados de chave pública emitidos.

Definição 2.2. Política de certificação: Política de certificação indica a aplicabilidade dos certificados emitidos para uma comunidade de usuários. Nela são expressados um conjunto de regras e requisitos de segurança que devem ser atendidos na obtenção dos dados e produção dos certificados.

2.3.1 Revogação de certificados de chave pública

Devido a problemas de gestão de par de chaves criptográficas fora do escopo deste trabalho, certificados digitais de chave pública possuem um período de validade. Entretanto, esse período não é absoluto. Certificados podem necessitar ser revogados antes que seu período de validade se encerre.

Para abordar tal problema autoridades certificadoras mantém uma lista de certificados revogados (LCR). Uma LCR é uma lista negra de certificados, ou seja, certificados presentes nessa lista não devem mais ser aceitos. Caso um certificado digital seja encontrado numa LCR, mesmo que a assinatura deste certificado seja válida ele não deve ser considerado válido e a sua chave pública não deve ser utilizada. É importante ressaltar que quando um certificado digital é incluído numa LCR ele é incluído com uma data de revogação, fornecida pela autoridade certificadora. Esta data, em geral, precede a data de emissão da LCR, que é emitida periodicamente. Há exceções onde uma LCR poderá ser emitida antes do previsto.

Toda LCR emitida por uma autoridade certificadora é assinada. A lista conterá os certificados que estariam vigentes no período mas que, por alguma razão, foram revogados. A razão de revogação também é codificada junto com a identificação de qual certificado foi revogado e a sua data de revogação. Os certificados só são mantidos em LCRs enquanto estiverem no seu período de validade, após esse período os certificados não aparecem mais nas LCRs emitidas.

Para verificar a validade de um certificado digital é necessário recuperar o seu caminho de certificação, ou seja, verificar as assinaturas dos certificados até a âncora de confiança da infraestrutura, isso pode ser visualizado na Figura 2. O tracejado indica quais as entidades pertencentes ao caminho de certificação. A âncora de confiança não é considerada parte do caminho, mas sim o alvo, ou seja, onde se quer chegar com esse caminho. Se o verificador do caminho de certificação conseguir encontrar um caminho onde todas as assinaturas são válidas e nenhum dos certificados está presente na LCR do seu emissor, o caminho pode ser considerado válido.

Nesse processo as LCRs dos certificados digitais envolvidos e seu período de validade devem ser verificadas também. Caso em alguma

dessas validações seja encontrada alguma discrepância, a chave pública do certificado digital que está sendo verificado não deve ser utilizada e o certificado digital deve ser considerado inválido. Caso não seja possível verificar alguma dessas informações, seja porque não foi possível obter uma LCR por questões de comunicação de rede ou algum certificado digital do caminho não foi encontrado a validação do certificado digital resultará em incerta e a chave pública em questão deve ser utilizada com cautela. O processo de validação do caminho de certificação pode ser visualizado na Figura 3.

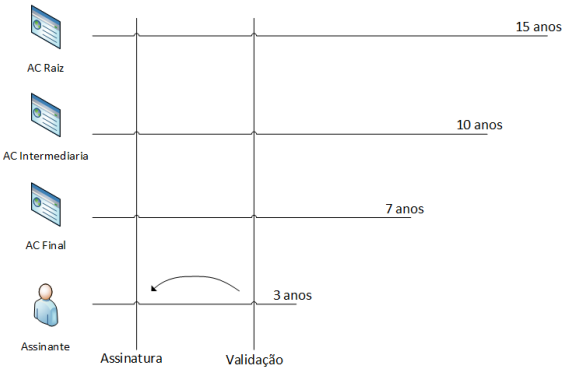


Figura 3 – Verificação do caminho de certificação.

2.3.2 Certificados de atributo

Da mesma forma que certificados digitais de chave pública são emitidos por autoridades certificadoras, certificados de atributo são emitidos por autoridades de atributos. Certificados de atributo são sempre associados à um certificado de chave pública. Enquanto o certificado de chave pública caracteriza a identidade associada a chave pública, certificados de atributo caracterizam atributos associados aquela identidade. É importante ressaltar que não existirá nenhuma chave pública num certificado de atributo, apenas uma referência ao certificado de chave pública do detentor dos atributos presentes no certificado.

O certificado de atributo também possui um caminho de certificação. Com exceção dele, todos os outros certificados desse caminho serão certificados de chave pública.

O certificado de atributo é necessário, pois as informações sobre atributo de uma identidade são bastante mais dinâmicas que o próprio certificado de chave pública e, ainda, pode ter requisitos de segurança diferentes.

Definição 2.3. Certificado de atributo: Um certificado de atributo é um certificado digital que associa atributos à identidade do detentor. Ele é emitido e assinado por uma autoridade de atributos.

2.3.3 Carimbos do tempo

Como muitas das informações fornecidas pela ICP são temporais, ou seja, válidas durante um período de tempo definido, o uso de ICPs geralmente necessita de atestados de tempo confiáveis. Essa fonte de tempo confiável pode ser incluída na ICP através de uma autoridade carimbadora. Essas autoridades emitem um tipo de informação especial, chamada carimbo do tempo, que possui uma marca de tempo confiável, pois a autoridade carimbadora é auditada dentro da ICP.

Carimbos do tempo são obtidos através de um protocolo de rede especificado pela RFC 3161 (41). O resultado desse processo, ou seja, o carimbo de tempo consiste de uma assinatura CMS. Essa assinatura é feita pela autoridade de carimbo de tempo sem conhecer o que foi carimbado por questões de sigilo que não são relevantes para esse trabalho. A assinatura CMS gerada pela autoridade de carimbo de tempo contém as informações sobre a autoridade de carimbo de tempo, um tipo especial de conteúdo assinado que inclui o resumo criptográfico carimbado e, possivelmente, informações sobre a precisão do relógio na carimbadora. Nessa assinatura CMS é incluído um atributo assinado que contém o momento que o carimbo foi gerado, conhecido pelo nome de *id-SigningTime*.

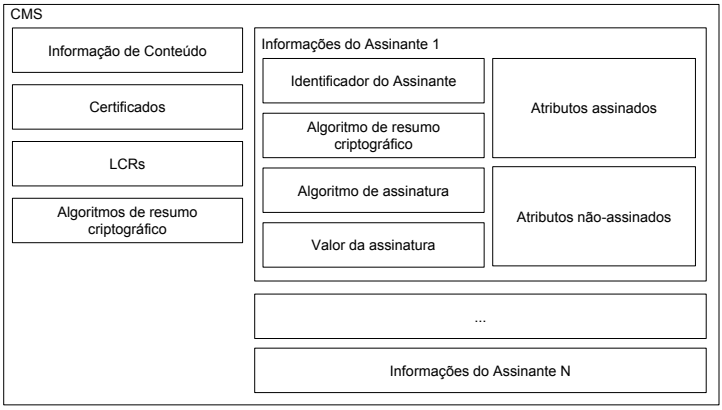
2.4 CRYPTOGRAPHIC MESSAGE SYNTAX

O padrão de mensagens CMS (42), embora não seja dedicado exclusivamente às assinaturas digitais, é amplamente utilizado para tal fim. Esse formato é descrito em linguagem ASN.1. Essa linguagem foi criada com o proposito de descrever estruturas de mensagens para protocolos. A forma como as mensagens descritas nessa linguagem são

codificadas pode variar, porém, mensagens criptográficas geralmente são codificadas no formato DER (43).

Como o formato CMS, representado na Figura 4, pode carregar variados tipos de mensagens criptográficas, existe um identificador na mensagem que indica o que a mensagem possui. Quando o CMS se trata de uma assinatura digital, este é identificado por um OID chamado *id-SignedData*.

Figura 4 – Formato de assinatura CMS.



Fonte: ICP-Brasil e PBAD (44)

O formato CMS permite que se inclua na mensagem mais de uma assinatura digital de um mesmo documento eletrônico, por isso existe uma lista de assinantes. Essa lista de assinantes caracteriza co-assinaturas.

Definição 2.4. Co-assinatura: Consiste em assinar, de forma independente, um documento independentemente se já foi assinado por um ou mais signatários. Co-assinaturas são disjuntas, no sentido que só se aplicam ao documento propriamente dito, ou seja, a produção da assinatura é feita usando somente os bytes que representam o documento, sem fazer uso dos bytes das outras possíveis assinaturas.

O campo *certificates* pode incluir uma lista de certificados utilizados para identificar as chaves públicas dos assinantes incluídos na

mensagem. Os valores incluídos nesse campo são certificados digitais no formato X.509 (45). Cada assinante pode também possuir alguns atributos em sua assinatura. Esses atributos podem ser divididos em assinados e não-assinados. Atributos assinados são incluídos no processo de obtenção do resumo criptográfico utilizado na assinatura digital, portanto devem ser concebidos antes da assinatura digital ser gerada.

Os atributos não-assinados não são incluídos nesse processo, por isso podem ser incluídos na assinatura em qualquer momento. Atributos em geral incluem informação útil para quem verificar a assinatura, seja com metadados sobre o documento eletrônico ou com informações adicionais não presentes no documento. O padrão CMS define alguns atributos mas não limita esse conjunto.

2.5 XML DIGITAL SIGNATURE

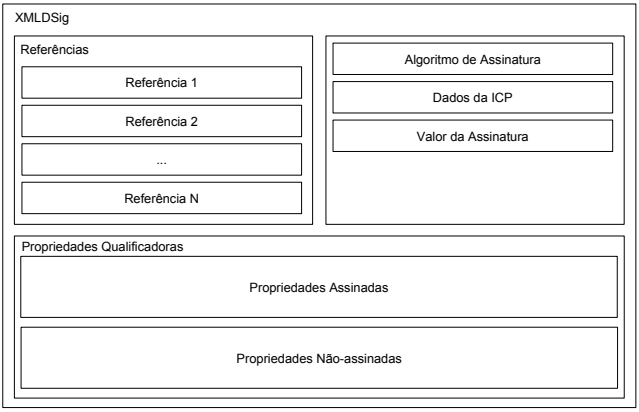
O padrão XMLDSig (46) possibilita a codificação de uma assinatura digital no formato de dados XML. Esse fato torna esse padrão bastante simples de se embarcar em tecnologias Web e, assim como o CMS, é amplamente utilizado.

Diferentemente do CMS, o formato XMLDsig, representado na Figura 5, permite que se assine um conjunto de arquivos, identificando cada um por um resumo criptográfico e um *Universal Resource Identifier* (URI). Mesmo que a assinatura XMLDSig permita que vários arquivos possam ser assinados numa única assinatura, é possível incluir apenas um assinante por mensagem XMLDsig.

URI é uma forma de identificar unicamente um documento na internet. URIs podem ser separadas em dois grandes grupos: *Universal Resource Locator* (URL) e *Universal Resource Name* (URN). Embora ambos possam ser utilizados na assinatura XMLDSig, a resolução de URNs não é amplamente difundida e padronizada como a resolução de URLs, tornado o uso da última a mais comum.

É possível incluir informações adicionais sobre a assinatura digital utilizando objetos. Objetos, assim como atributos na assinatura CMS, podem incluir metadados sobre a assinatura ou informações adicionais. Objetos podem ser assinados utilizando URLs. Estas podem identificar um elemento dentro de um documento XML através do *id*

Figura 5 – Formato XMLDSig.



Fonte: ICP-Brasil e PBAD (44)

deste elemento.

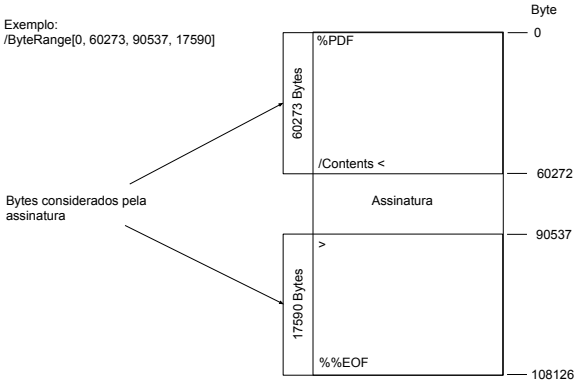
Na figura do formato XMLDSig está representado o objeto proposto para o formato XAdES, que será discutido a seguir. O objeto definido para o formato XAdES é chamado de *propriedades qualificadoras*. Esse objeto introduz no formato XMLDSig atributos assinados e não-assinados, necessários ao conceito de assinatura digital avançada.

Informações sobre a chave do assinante podem ser incluídas no elemento *ds:KeyInfo*. Essas informações podem variar bastante, mas é possível que nesse elemento sejam incluídos certificados de chave pública no formato X.509 codificados em *Base64*. Essa codificação é uma forma de mapear bytes para caracteres ASCII.

2.6 ASSINATURA PDF

De acordo com a ISO 32000 (7), documentos PDF incluem estruturas que suportam assinaturas digitais. Documentos PDF podem utilizar o formato CMS (42) dentro dessas estruturas para proteção e autenticação de documentos de forma geral. O padrão entretanto,

Figura 6 – Divisão do documento PDF em seções para processamento do resumo criptográfico.



Fonte: Perfis de assinatura avançada em PDF – Parte 1 (12)

limita as possibilidades do CMS a fim de evitar a repetição de informações de suas próprias estruturas com aquelas do CMS.

A assinatura CMS dentro de um documento PDF pode ser vista como uma assinatura *detached*. Entretanto a forma como o seu resumo criptográfico é obtido é própria do padrão de documentos PDF. Para obtenção do resumo criptográfico a aplicação deve primeiro alocar o espaço onde a assinatura será incluída, então a aplicação terá dividido o documento em três seções, uma que antecede a assinatura, outra onde a assinatura digital se encontra e a última a parte que sucede a assinatura digital.

O resumo criptográfico é obtido sobre a junção da parte que precede a assinatura digital com a que sucede. Isso é identificado no dicionário de assinatura do documento PDF através de quatro valores. Sendo dois pares, cada par indica onde começa o valor para o resumo criptográfico e qual o seu tamanho. Esse processo pode ser visualizado na Figura 6.

2.6.1 Seed Values

As assinaturas digitais são incluídas no documento PDF através de um dicionário chamado *SignatureDictionary*. Esse dicionário por sua vez é incluído num outro dicionário chamado *SignatureField*. Esse dicionário pode conter além da assinatura digital um dicionário chamado *SeedValueDictionary*. Esse dicionário tem uma função muito parecida com o de uma política de assinatura, porém seu uso é feito apenas no momento de assinar, sendo de responsabilidade do assinante somente cumprir as regras descritas no *seed values*. Após a assinatura ser feita esse campo não necessita mais ser verificado.

2.7 ASSINATURA DIGITAL AVANÇADA

Como as chaves utilizadas em ICPs tem perído de validade incerto devido a possibilidade de seu certificado digital ser revogado, ou em alguns casos, o período de validade ser muito curto para o uso que se quer dar a assinatura digital, foram criados atributos especiais para o CMS. O conjunto desses atributos com os procedimentos para seu uso é conhecido como CMS Advanced Electronic Signature(CAdES) (3, 8, 9).

O XMLDSig foi estendido de forma análoga, porém foi concebido um objeto especial que suporta os atributos assinados e não assinados de forma muito parecida com o CMS, essa especificação junto com a sua forma de uso é conhecida como XMLDSig Advanced Electronic Signature(XAdES) (1).

Assinaturas digitais avançadas adicionam alguns conceitos às assinaturas digitais. Além da possibilidade de inclusão de algumas informações adicionais a assinatura através de atributos, nesses padrões é criada a ideia de política de assinatura. Isso é feito através da possibilidade da inclusão de um atributo que pode indicar a política de assinatura. A política de assinatura pode ser referenciada de duas formas. A forma implícita, onde apenas indica-se que a assinatura está sujeita a uma política sem identificá-la. Ou a forma explícita, que identifica unicamente a política de assinatura através de um identificador único e, possivelmente, um resumo criptográfico da política de assinatura.

Outro conceito suportado por essas assinaturas digitais avança-

das é o de contra-assinatura. Essas assinaturas são incluídas como um atributo não-assinado na assinatura que contra-assinam.

Definição 2.5. Contra-assinatura: A contra-assinatura, diferentemente da co-assinautura, leva em consideração as assinaturas já realizadas no documento. Assim, ao contra-assinar um documento, um assinante estará assinando não somente o documento, mas as outras assinaturas.

Outra funcionalidade importante é a possibilidade de se proteger contra a revogação de certificados digitais ou a expiração dos mesmos através do uso de carimbos do tempo. Nesses padrões são definidos alguns tipos de atributos baseados em carimbos do tempo. Cada atributo define o que deve ser incluso no resumo criptográfico para obtenção do carimbo do tempo. O carimbo do tempo resultante é o valor do atributo.

O uso desses carimbos, em conjunto com outros atributos capazes de incluir informações sobre a ICP dentro da assinatura, tornam possível manter uma assinatura válida por um período maior que o da validade do certificado de chave pública utilizado para gerar a assinatura. Como, em geral, maior parte dessa informação é adicionada na forma de atributos não assinados, toda essa informação pode ser adicionada a assinatura após a sua geração e não depende do assinante.

O uso de carimbos de tempo na extensão da validade da assinatura digital pode ser visualizado na Figura 7. Como os carimbos utilizados atrelam o valor da assinatura digital e informações sobre a ICP a uma data confiável, é possível assumir que essa informação existia na data de emissão do carimbo e utilizar essa data para verificar essas informações.

2.8 ASSINATURA ELETRÔNICA AVANÇADA EM PDF

O formato de Assinatura Avançada em PDF (PAdES) (12), a exemplo dos padrões CAdES e XAdES, adiciona atributos assinados e não-assinados ao formado de assinatura para PDF. Esse formato define uma estrutura própria para inclusão de carimbos do tempo em documentos PDF.

Segundo a especificação técnica, as informações que podem ser adicionadas tanto no dicionário de assinatura, quanto em forma de

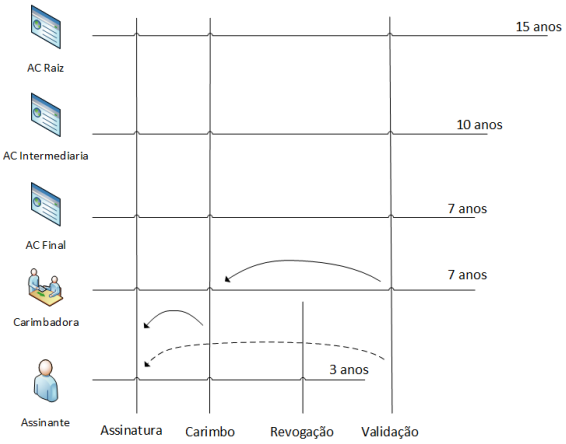


Figura 7 – Uso de carimbos de tempo em assinaturas digitais avançadas.

atributo no CMS, devem ser adicionadas no dicionário de assinatura obrigatoriamente. Isso resolve varias ambiguidades que estão presentes no formato de assinatura para documentos PDF.

O padrão contempla políticas de assinatura também, porém o único trabalho que comtempla formatos processáveis por máquina para esse padrão é o conjunto normativo para o padrão brasileiro de assinaturas digitais (20). É sugerido inclusive a possibilidade de incluir uma indicação de política de assinatura no dicionário *Seed Values*.

Alguns carimbos do tempo podem ser adicionados na estrutura CMS. Entretanto, os carimbos do tempo utilizados para extensão da validade da assinatura digital devem ser incluídos numa estrutura própria. Essa estrutura é um dicionário chamado *DocumentTimestamp*. Esses carimbos do tempo funcionam de forma muito parecida com a uma assinatura digital num documento PDF, protegendo todo o documento em questão.

Informações de certificação digital, contendo valores de certificado digital de chave pública, LCRs ou outras informações são adicionados também em uma estrutura adicional chamada *Dictionary Signature Store*(DSS), que fica fora do CMS embarcado no documento PDF.

2.9 PADRÃO BRASILEIRO DE ASSINATURA DIGITAL

O Padrão Brasileiro de Assinatura Digital (PBAD) é caracterizado por um conjunto de normativos que definem exatamente o que é entendido como assinatura digital e seus requisitos. Esse conjunto normativo é constituído por quatro documentos. O DOC-ICP-15 (47) que define os conceitos fundamentais do normativo. O DOC-ICP-15-01 (48), que define os requisitos para criação e verificação de assinaturas digitais no âmbito da ICP-Brasil, especificando as tecnologias a serem utilizadas e algoritmos. O DOC-ICP-15-02 (49), que estabelece um subconjunto dos atributos, definidos nos padrões internacionais assinatura digital, a serem utilizados, a fim de maximizar a interoperabilidade. E finalmente, o DOC-ICP-15-03 (20), que descreve as políticas de assinatura para os padrões CAdES, XAdES e PAdES. Esse documento define também a Lista de Políticas de Assinatura Aprovadas(LPA) e a gerência do ciclo de vida de políticas de assinatura dentro da ICP-Brasil.

Uma visão geral da assinatura digital é apresentada na Figura 8. Essa figura apresenta os elementos envolvidos no processo de geração e verificação de assinaturas digitais. As setas não representam as ordens em que as atividades ocorrem. As setas numeradas 1, 2, 3 e 4 indicam que essas entidades emitem certificados digitais para as entidades apontadas. A seta 6 indica que a carimbadora produz carimbos do tempo que são utilizados na assinatura. As informações utilizadas para gerar os carimbos do tempo proveem da assinatura digital. As setas 5 e 7 indicam o processo de geração da assinatura digital do documento e possivelmente atributos assinados. Finalmente, a seta 8 indica o uso da assinatura digital pelo assinante ou verificador para atestar autenticidade e integridade da assinatura digital.

2.9.1 Conjunto Normativo

O Conjunto Normativo DOC-ICP-15 define os requisitos que caracterizam uma assinatura digital na ICP-Brasil. Para caracterizar uma assinatura digital, a assinatura deve ser codifica em CAdES, XAdES ou PAdES e utilizar os atributos definidos no DOC-ICP-15-02. O uso de política de assinatura fica definido na ICP-Brasil e todos os implementadores devem respeitar seus requisitos. Todos os perfis de assinatura incluem um atributo em que o assinante identifica a política de assinatura utilizada na criação da assinatura. Essa referência a polí-

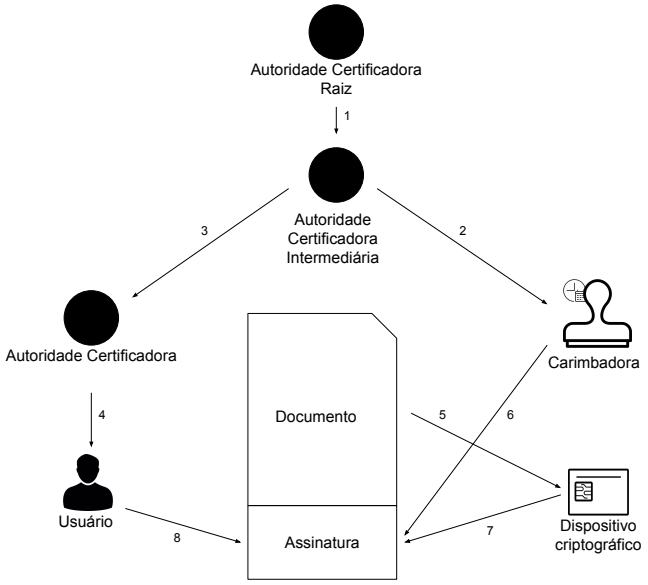


Figura 8 – Visão geral de assinaturas digitais no Padrão Brasileiro de Assinatura Digital (PBAD).

tica de assinatura deve ser explícita. O verificador então sabe quais os atributos de assinatura esperar e quais ele pode incluir na assinatura sem alterar o resultado de sua validação. O verificador e o assinante ainda tem a possibilidade de incluir os atributos que são considerados opcionais como definido no DOC-ICP-15-03 (20). Entretanto, as políticas em formatos ASN.1 ou XML desse conjunto normativo não possuem qualquer estrutura que auxilie os usuários a identificar quais são estes atributos. Portanto, a única forma de um usuário saber quais são os atributos opcionais que pode incluir na assinatura é consultando o DOC-ICP-15.03.

O Conjunto Normativo DOC-ICP-15 define os perfis de assinatura Referência Básica (RB), Referência de Tempo (RT), Referência de Validação (RV), Referência Completa (RC) e Referência de Arquivamento (RA). Esses perfis são baseados nos perfis sugeridos para os padrões CAdES e XAdES, detalhados no Capítulo 3. Para cada um desses perfis é definida uma política de assinatura no formato ASN.1 e outra no formato XML. Cada política de assinatura tem um campo

de aplicação descrito com a intenção de especificar para o usuário de assinatura digital qual a aplicação daquela política de assinatura.

2.9.2 Regras Definidas por uma Política de Assinatura

Segundo o DOC-ICP-15.03 e os padrões internacionais os agentes envolvidos na produção e uso de políticas de assinatura são:

1. Emissor de Lista de Políticas Aprovadas;
2. Emissores de Políticas de Assinatura;
3. Autoridades de Publicação da Políticas de Assinatura;
4. Desenvolvedores de Sistema de Geração e Verificação de Assinaturas.

Um documento de Política de Assinatura (PA) contém basicamente as seguintes informações:

1. Identificador de Objeto da Política (OID);
2. Informação sobre o Emissor da PA;
3. Campo de Aplicação da PA;
4. Regras para gerar e validar assinaturas;
5. Restrições para a geração e validação de assinaturas;
6. Tipos de comprometimento do assinante em relação aos dados assinados.

O DOC-ICP-15.03 contém a definição dos diversos perfis do PBAD. Cada perfil é formalizado através de uma política de assinatura descrita nesse documento. Entretanto, esse documento também contém algumas tabelas fora das políticas de assinatura determinando alguns atributos proibidos e outros opcionais.

Na Tabela 1 é possível observar a definição dos atributos não-assinados obrigatórios e opcionais de uma assinatura. A letra "O" indica que o atributo é obrigatório, "P" é opcional, ou seja, pode ser incluído na assinatura e "ND" que o atributo não deve ser incluído.

Tabela 1 – Atributos não-assinados obrigatórios (O), opcionais (P) e que os que não devem ser incluídos (ND) no PBAD.

Nome do atributo / Propriedade	**Identificação do atributo**	**Perfil AD**				
	Propriedade	**RB**	**RT**	**RV**	**RC**	**RA**
Contra-assinatura (*countersignature*)	id-countersignature	P	P	P	P	P
	CounterSignature					
Carimbo do tempo de assinatura (*signature time stamp*)	id-aa-signatureTimeStampToken	ND	O	O	O	ND
	SignatureTimeStamp					
Referências completas aos certificados (*complete certificate references*)	id-aa-ets-certificateRefs	P	P	O	O	O
	CompleteCertificateRefs					
Referências completas à revogação (*complete revocation references*)	id-aa-ets-revocationRefs	P	P	O	O	O
	CompleteRevocationRefs					
Referências aos certificados de atributo (*attribute certificate references*)	id-aa-ets-attrCertificateRefs	P	P	P	P	P
	AttributeCertificateRefs					
Referências à revogação de atributo (*attribute revogation references*)	id-aa-ets-attrRevocationRefs	P	P	P	P	P
	AttributeRevocationRefs					
Carimbo do tempo das referências (*time-stamped certificate crls references*)	id-aa-escTimeStamp	ND	P	O	O	ND
	SigAndRefsTimeStamp					
Valores dos certificados (*certificate values*)	id-aa-ets-certValues	P	P	P	O	O
	CertificateValues					
Valores de revogação (*revocation values*)	id-aa-ets-revocationValues	P	P	P	O	O
	RevocationValues					
Carimbo do tempo de arquivamento (*archive time-stamp*)	id-aa-ets-archiveTimestampV2	ND	ND	ND	ND	O
	ArchiveTimeStamp					

Fonte: DOC-ICP-15.03 (20)

As políticas de assinatura podem ser utilizadas em sistemas de duas principais maneiras. Uma de forma manual, onde os desenvolvedores dos sistemas de geração e verificação de assinaturas se responsabilizam por incluir no sistema as possibilidades de políticas de assinatura e manter esses sistemas atualizados.

Outra forma é o uso automático de políticas de assinatura. Nesse modelo é necessário que exista a versão da política de assinatura codificada em formato ASN.1 ou XML. Os sistemas de geração e verificação de assinaturas digitais devem ser preparados para interpretar as regras previstas na estrutura da política de assinatura e aplicá-las as assinaturas digitais que processam.

As políticas de assinatura devem estar disponíveis para a comunidade de interessados. Políticas de Assinatura possuem um período de validade descrito em seus dados. Quando o modelo escolhido é o automático, é necessário que as aplicações possam encontrar as versões de máquina das políticas de assinatura. Isso pode ser feito de variadas maneiras, uma vez que o ETSI (9, 12) não define como as políticas devem ser disponibilizadas.

No caso de estudo do PBAD, é definida uma estrutura adicional chamada Lista de Políticas de Assinatura Aprovadas (LPA) (20, veja o Anexo 3). A LPA tem um endereço fixo definido através do conjunto normativo. Os desenvolvedores de sistemas de geração e verificação de assinaturas digitais se comprometem a manter as aplicações atualizadas em relação à esse endereço. A LPA então aponta para as políticas de assinatura disponíveis no PBAD. Até o momento não é prevista a possibilidade de remoção de uma política de assinatura da LPA, uma vez que isso inviabilizaria a verificação de assinaturas digitais antigas.

No PBAD, o ITI é o responsável pela emissão e publicação das políticas de assinatura. Ele é quem mantém um repositório contendo todos os arquivos necessários às aplicações. É ele quem gerencia as emissões dos artefatos quando estes estão para expirar. Também é de responsabilidade do ITI verificar os algoritmos e informações necessárias a cada perfil de assinatura para que ele possa emitir as políticas de assinatura.

Se considerarmos o modelo manual de uso de políticas de assinatura, onde os desenvolvedores embarcam os requisitos estabelecidos por uma política de assinatura diretamente na aplicação, podemos verificar que o sistema produzido será muito mais vulnerável a alterações no ambiente, sendo assim menos estável. Outro ponto é que essa maneira de desenvolvimento de sistemas utilizando políticas acarreta uma maior carga sobre a entidade responsável pela manutenção das políticas, uma vez que essa deve ter um planejamento muito mais elaborado a fim de evitar qualquer alteração em políticas de assinatura, pois isso acarretaria em custos para atualização de todos os sistemas que utilizam assinaturas digitais com as suas políticas.

Entretanto, o modelo manual é mais simples de ser desenvolvido uma vez que as regras são aplicadas diretamente pelo desenvolvedor, não sendo necessário embarcar na aplicação a capacidade de interpretar uma política e aplicar regras descritas.

No modelo automático, os desenvolvedores devem tornar a aplicação capaz de interpretar as possíveis regras que podem vir a ser utilizadas numa política de assinatura. Entretanto, a carga sobre a entidade responsável pelas políticas de assinatura é diminuída, uma vez que após a emissão de uma nova política de assinatura as aplicações já estão prontas para criar e verificar assinaturas dentro seguindo o que é

estabelecido pelas novas políticas emitidas.

O desenvolvimento de sistemas capazes de interpretar políticas de assinatura de forma automática é mais custoso. Cabe aos desenvolvedores avaliar qual a abordagem devem seguir, pois o caminho a ser seguido somente pode ser justificado pelo contexto em que o sistema será utilizado. Por exemplo, uma aplicação onde sabe-se previamente que será necessário somente produzir assinaturas digitais seguindo uma única política de assinatura com poucas regras não justifica a produção de um sistema capaz de interpretar todas as regras.

É possível que um sistema tenha como premissa permitir o assinante julgar qual a política de assinatura que cabe para o documento que ele deseja assinar. Portanto, esse sistema idealmente, deveria ser capaz de interpretar qualquer política de assinatura de forma automática.

2.10 ACEITAÇÃO DA ASSINATURA DIGITAL

Apesar de amplamente utilizada, a assinatura digital de documentos eletrônicos ainda não é aceita como um substituto para a assinatura de próprio punho, no papel. Resultados de vários estudos mostram que, embora funcionalmente equivalente, as assinaturas digitais evocam reações psicológicas diferentes da assinatura manual. As pessoas tendem a acreditar que a chance de haver disputas sobre os documentos assinados digitalmente é maior que aqueles assinados no papel (50).

Acredita-se que isso se deve em parte, ao fato de que o documento eletrônico é assinado com o auxílio de uma plataforma computacional, enquanto que o documento papel é assinado pelo ser humano, usando uma caneta. Além disso, a assinatura no papel contém vestígios de aspectos biométricos do signatário. A assinatura manual, diferentemente da assinatura digital, depende de vários fatores, e tem ligeira variação, que está relacionado a aspectos emocionais do assinante (51).

A verificação da assinatura manual também é diferente da eletrônica. Cuidados adicionais são necessários à essa verificação, o que leva a um sentimento de maior confiança por parte do verificador da assinatura, quando comparado com a assinatura digital (52–56).

Acredita-se que o uso de políticas de assinatura podem diminuir as diferenças entre a assinatura manual no papel e a assinatura digital. Através das políticas de assinatura, tanto o signatário tente a acreditar mais que sua assinatura será aceita pelos destinatários, quanto os verificadores da assinatura terão mais dados e regras mais bem estabelecidas para a correta verificação da autenticidade dos documentos eletronicamente assinados.

2.11 CONCLUSÃO

Na Seção 2.2 desse capítulo foi apresentado um histórico comparando a assinatura manuscrita com a assinatura digital. Ficou identificado que assinaturas digitais devem satisfazer algumas propriedades, entre elas identificar o autor e momento da assinatura e ser verificável por terceiras partes para resolver disputas. Dessas e outras propriedades identificadas pode-se estabelecer requisitos para a assinatura digital. Desses requisitos podemos citar os principais: inviabilidade de forja e facilidade na geração e verificação da assinatura.

Ainda sobre essa seção, apresentou-se o processo básico de assinatura digital. Esse processo consiste em obter o resumo criptográfico do documento e cifrá-lo com uma cifra assimétrica utilizando a chave privada. Nenhum desses algoritmos em específico foram apresentados, pois podem ser vistos como blocos de construção para a assinatura digital, pois estes podem ser facilmente substituídos, sem afetar a proposta desse trabalho.

Na Seção 2.3, sobre certificados digitais e infraestrutura de chaves públicas, foram definidos os conceitos chave de âncora de confiança, política de certificação e certificado de atributo. Esses conceitos tem um papel especial nas políticas de assinatura que serão apresentadas no próximo capítulo. Ainda nessa seção, o caminho de certificação foi explicado. Esse caminho é bastante importante nos processo de validação da assinatura digital, uma vez que permite identificar com certo grau de confiança o assinante. Por último, mas não menos importante, foi apresentado o carimbo do tempo. Esses carimbos são fundamentais para extensão do prazo de validade de assinaturas digitais avançadas apresentadas mais a frente.

A partir dessa seção foram apresentados os formatos de assinatura digital de interesse para esse trabalho. Na Seção 2.4 foi apresentado o formato CMS. Esse formato foi utilizado para introduzir o conceito de co-assinaturas, idéia bastante utilizada em processos de assinatura digital. Ainda sobre o formato CMS, foi elucidado fatos sobre a sua estrutura, como a possibilidade de embarcar certificados digitais e atributos, sejam assinados ou não na assinatura.

Na Seção 2.5, foi apresentado o formato XMLDSig. Esse formato foi amplamente comparado com o formato CMS, pois as diferenças desse formato com o CMS são a razão de algumas diferenças entre os formatos CAdES e XAdES. Sua estrutura também foi apresentada, indicando as estruturas onde se pode armazenar certificados para auxiliar na validação das assinaturas e quais estruturas foram utilizadas para adicionar o conceito de atributos a esse formato.

Seguindo, na Seção 2.6, relatou-se as características de assinaturas digitais aplicadas a documentos PDF em específico. Foi exposto as diferenças entre o processamento de assinaturas CMS em geral e as especificidades do processamento do documento para quando a assinatura é embarcada no PDF. O dicionário *Seed Values* foi destacado nessa seção por entender-se que esse tem uma relação com políticas de assinatura.

Na Seção 2.7, foram explicadas características dos dois principais padrões de assinatura relacionados com esse trabalho. Esses dois padrões adicionam as assinaturas CMS (CAdES) e XMLDSig (XAdES) atributos assinados e não assinados. Desses atributos adicionados os mais relevantes são os atributos de carimbos do tempo, que permitem a extensão do prazo de validade da assinatura. Foi dado destaque nessa seção para um atributo não-assinado desses formatos que suporta o conceito de contra-assinatura. Esse tipo de assinatura é bastante relevante para processos gerais de assinatura digital onde são necessárias mais de uma assinatura.

A seguir, na Seção 2.8, é comentado o formato PAdES. A exemplo do CAdES e XAdES, esse formato adiciona atributos assinados e não-assinados a assinatura do PDF. A principal diferença desse formato para o CAdES e XAdES é que o carimbo de tempo utilizado para estender a válidade da assinatura é feito através de um dicionário e aposto fora do CMS embarcado no documento. A exemplo do carimbo, também é adicionada um dicionário para armazenar os dados de validação

da assinatura fora da mesma. Como o CMS também possui estruturas para armazenar dados de validação, o formato define que devem ser utilizados os dicionários sempre para evitar confusões.

Na Seção 2.9, é exposto o PBAD. São explicadas as relações entre o PBAD e os formatos CAdES, XAdES e PAdES. Partindo das relações entre os padrões de assinatura digital, são explicadas as características especiais do PBAD. Essas características especiais são a determinação de perfis de assinatura próprios e a obrigatoriedade do uso de políticas de assinatura. Como o uso de políticas é obrigatório, o PBAD tem uma forma exclusiva de distribuir as políticas de assinatura. Essa distribuição é feita através de uma LPA.

Finalmente é discutida a adoção de assinatura digital na Seção 2.10. A visão dos usuários quanto as assinaturas digitais ainda permanece diferente das assinaturas de próprio punho. Acredita-se que devido ao uso de computadores e outros equipamentos para sua confecção, em comparação com o uso da caneta para assinaturas de próprio punho, prejudica a confiança depositada na assinatura digital. Acredita-se que políticas de assinatura quando aplicadas ajudam o usuário a estabelecer sua confiança na assinatura.

3 POLÍTICAS DE ASSINATURA

3.1 INTRODUÇÃO

Neste capítulo são apresentados os principais trabalhos relacionados à definição de políticas de assinatura e seus usos. O material aqui descrito advém de várias fontes de informação. O levantamento bibliográfico nos permitiu encontrar material na forma de patentes, normas e padrões e artigos científicos. Também obteve-se material resultante da implementação prática dos códigos de referência do Padrão Brasileiro de Assinatura Digital (PBAD), do qual o nosso grupo de pesquisa tem participado.

A Seção 3.2 apresenta as definições dos principais conceitos necessários à compreensão da nossa proposta de mudança dinâmica de políticas de assinatura.

O estudo bibliográfico feito mostrou que a política de assinatura é, na verdade, derivada de uma análise dos requisitos impostos às implementações de assinaturas digitais, com foco num certo tipo de negócio ou num determinado domínio de aplicação. O resultado dessa análise produz um conjunto de regras relacionadas à criação, progressão e validação de uma ou mais assinaturas digitais para os quais o mesmo conjunto de regras se aplicam. Esse conjunto de regras pode ser aposto num documento de políticas. A Seção 3.3 descreve como é feita essa análise e como as regras constituintes de uma política de assinatura são encontradas.

A Seção 3.4 descreve a estrutura de políticas para formatos descritos em linguagem ASN.1 (57) e linguagem XSD (58). A Seção 3.5 descreve as duas principais especificações técnicas de assinatura digital nos formatos CAdES (8–11) e XAdES (1–3, 59). Ambos os formatos definem perfis de assinatura digital que servem como guia para uso de assinatura digital. Embora perfis não caracterizem políticas de assinatura mas podem ser vistos como uma base e princípio da mesma.

A Seção 3.6 mostra um exemplo de política de assinatura em formato XML. Essa política é para autenticação rápida de documentos eletrônicos. As partes anteriormente descritas na Seção 3.4 são apontadas através de figuras que representam o arquivo XML da política. As

regras estabelecidas pela política exposta como exemplo são discutidas de forma a esclarecer o contexto em que políticas de assinatura são utilizadas.

A Seção 3.7 apresenta um protocolo baseado no uso de políticas de assinatura. Um protocolo de troca justa tem como propriedade fundamental garantir que nenhuma das partes irá se comprometer sem que a outra parte também se comprometa, ou seja, se a execução do protocolo não for bem-sucedida nenhuma das partes deve possuir ou ser capaz de produzir uma prova que ateste que a outra parte está de acordo com a transação. Nesse protocolo a política de assinatura é utilizada para caracterizar as assinaturas utilizadas em diferentes momentos do protocolo de forma a garantir que a única assinatura que estabelece a transação realmente é a produzida no final da execução do protocolo. Tal uso de comprometimentos da política de assinatura auxilia o protocolo a satisfazer as propriedades para um protocolo de troca justa.

A Seção 3.8 apresenta um exemplo de modificação da estrutura de políticas de assinatura. Esse trabalho trata da adaptação de políticas de assinatura para representar a relação entre assinaturas, o que é uma necessidade bastante comuns em aplicações segundo o relatório técnico do ETSI 102 045 (60). Esse trabalho não mantém compatibilidade das políticas de assinatura com a estrutura proposta nos relatórios técnicos ETSI 102 038 (4) e ETSI 102 272 (21).

Patentes relacionadas ao uso e estrutura de políticas de assinatura são brevemente explicadas na Seção 3.9.

3.2 DEFINIÇÕES

Uma política de assinatura deve cobrir pelo menos um dos seguintes três conjuntos de regras para o gerenciamento do ciclo de vida de assinaturas:

1. Regras para criação de assinatura;
2. Regras para complementação de assinatura;
3. Regras para validação de assinatura.

Definição 3.1. Política de Criação de Assinatura: consiste de um conjunto de regras, aplicáveis a uma ou mais assinaturas, que definem os requisitos técnicos e procedimentais para sua criação, de forma a atender requisitos particulares de uma aplicação.

Definição 3.2. Política de Complementação de Assinatura: consiste de um conjunto de regras, aplicáveis a uma ou mais assinaturas digitais, que definem os requisitos técnicos e procedimentais para a progressão de assinaturas, de forma a atender requisitos de uma aplicação. A complementação da assinatura, por sua vez, é realizada através da inclusão de novos atributos a uma assinatura já existente.

Definição 3.3. Política de Validação de Assinatura: consiste de um conjunto de regras, aplicáveis a uma ou mais assinaturas digitais, que definem os requisitos para sua validação, de forma a atender requisitos de uma aplicação.

Definição 3.4. Autoridade de Política de Assinatura: É a entidade responsável por esboçar, registrar, manter, emitir e atualizar políticas de assinatura.

Definição 3.5. Política de Assinatura: consiste da política de criação de assinatura, política de complementação de assinatura, política de validação de assinatura ou qualquer combinação dessas, aplicável a uma assinatura ou a um conjunto de assinaturas. Trata-se, portanto, de um documento que especifica e expõe um acordo entre o assinante e o verificador dando significado e expondo quais as informações contidas na assinatura digital devem ser incluídas e verificadas.

Definição 3.6. Perfil de Assinatura: é um formato de assinatura, semelhante a uma política de assinatura. A diferença é que não existe uma referência a um documento de políticas. Um documento assinado num determinado perfil, contém os atributos assinados e não assinados, que o signatário estabelece. Entretanto, não há um acordo formal no qual o verificador da assinatura poderia utilizar para verificar a sua aderência a um determinado formato.

3.3 PROCESSO DE GERAÇÃO DE POLÍTICAS DE ASSINATURA

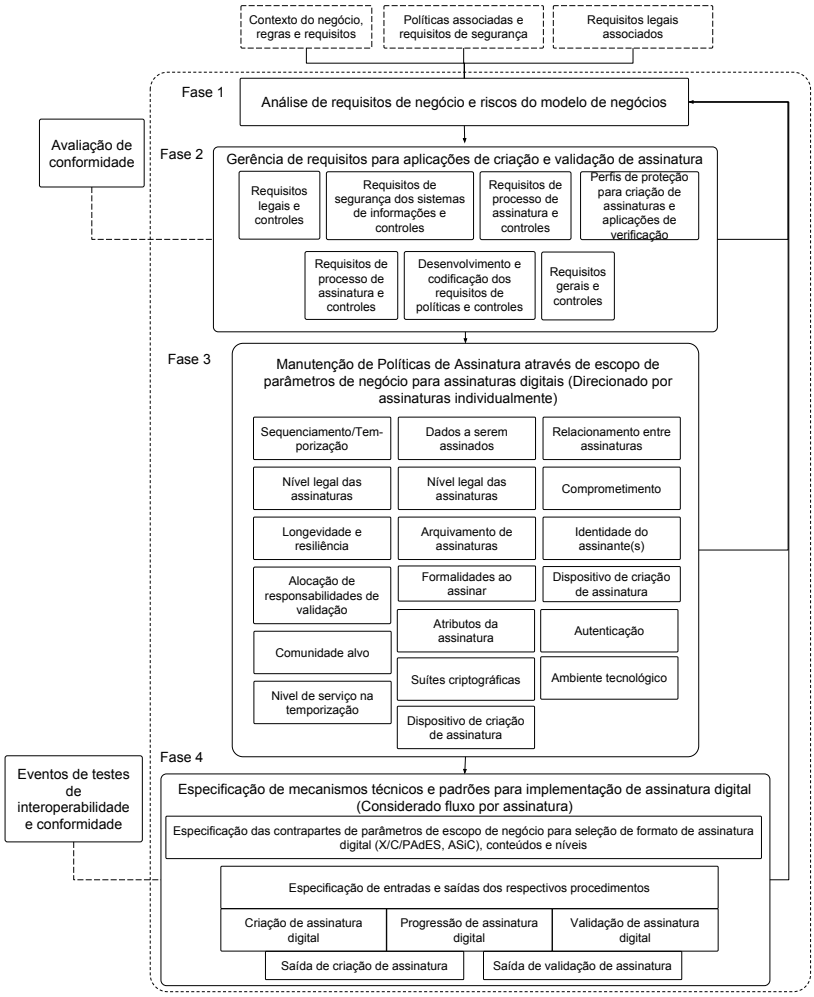
Não é uma tarefa simples identificar e descrever as regras que farão parte de uma política de assinatura. Em geral, o processo mais recomendado é estudar a aplicação alvo da assinatura, e através de um exercício exaustivo e recursivo, levantar todas as informações relevantes e proceder a sua análise. A Figura 9 apresenta uma visão ampla desse processo iterativo. Nesse processo, pode-se observar quatro fases.

A primeira fase consiste da obtenção de todas as informações relevantes para a implantação da assinatura digital numa determinada aplicação. Dentre essas informações podemos citar como exemplo questões sobre quais os relacionamentos entre assinaturas digitais e quais requisitos legais essas assinaturas digitais terão de se adequar. A identificação desses requisitos e informações é dependente da aplicação e do ambiente onde as assinaturas serão utilizadas e devem ser tratadas caso a caso.

A segunda fase trata da elaboração e transformação dos diferentes requisitos de segurança e de regras da aplicação em controles para serem implementados no sistema de assinatura. Nessa fase são obtidas várias das informações que serão acomodadas na política de assinatura. Ainda nessa fase, os interessados devem levantar requisitos para interface com o usuário, a fim de evitar confusão e mitigar erros na interação do usuário com as aplicações de assinatura digital. Também deve-se levantar quais os requisitos de segurança e questões legais caso a assinatura digital tenha que ter validade jurídica. Finalmente, devem ser estabelecidos os requisitos de completude, para evitar que as aplicações de assinatura digital implementem apenas parte dos requisitos necessários.

A terceira fase refere-se a todo o conjunto de informações da aplicação em que as assinaturas digitais serão utilizadas. Essa etapa deve condicionar como as assinaturas digitais serão implementadas, desde a sua instituição até sua manutenção. As informações que regem a utilização das assinaturas digitais podem ser oriundas de diversas fontes. Entre essas fontes podemos citar as regras da aplicação, que tem um papel forte no fluxo da assinatura digital, pois este ditará as particularidades na implementação da mesma. Outra fonte de informação importante são as questões legais a qual o negócio está sujeito. Informações sobre quem serão os atores que irão gerar as assinaturas digitais,

Figura 9 – Processo iterativo para implementação, geração e validação de assinaturas digitais.



Fonte: *Guidance on the use of standards for signature creation and validation* (61)

desde o tipo de agente, ou seja, se é uma pessoa física ou jurídica, até que tipos de dispositivos criptográficos serão utilizados.

As três fases descritas acima descrevem as condições e requisitos sob as quais as assinaturas digitais devem ser utilizadas no negócio. Dessas três fases pode-se obter todas as informações necessárias para se conceber as políticas de assinatura e a definição dos respectivos perfis de assinatura.

A quarta fase tem o propósito de angariar informações para auxiliar nas decisões técnicas a fim de atender os requisitos identificados nas fases anteriores. Essa última fase trata de informações necessárias a implementadores para que estes tenham informações suficientes para produzir ferramentas adequadas à aplicação em questão.

3.4 POLÍTICAS DE ASSINATURA

A estrutura de uma política de assinatura em ASN.1 é definida pela RFC 3125 (18). Essa RFC, por sua vez, foi baseada numa das primeiras versões da especificação técnica sobre assinaturas eletrônicas avançadas em CMS (versão 1.2.2) do ETSI (9). A RFC estabelece todas as informações que podem ser incluídas numa política de assinatura descrita em linguagem ASN.1. De forma análoga, a estrutura para políticas de assinatura para XML é definida pelo relatório técnico sobre políticas de assinatura em formato XML do ETSI (4). Essas estruturas em ASN.1 e XML, ilustradas na Figura 10, são bastante parecidas.

Conforme ilustra a figura, a política de assinatura é composta por três principais componentes: *algoritmo de resumo criptográfico e método de canonização*, *informações da política de assinatura* e o *valor do resumo criptográfico*. O *valor do resumo criptográfico* é calculado, utilizando o algoritmo identificado no componente *algoritmo de resumo criptográfico* através do processamento dos bytes do componente *informações da política de assinatura*.

O método de canonização do componente *algoritmo de resumo criptográfico e método de canonização* somente é utilizado em políticas de assinatura codificadas em XML. Isso ocorre porque a estrutura de um mesmo documento em XML pode ser representada, de forma de diferentes maneiras. Apesar da equivalência desses documentos, o resumo criptográfico é determinado a partir da representação do arquivo em bytes. Assim, mesmo em se tratando da mesma política, o resumo

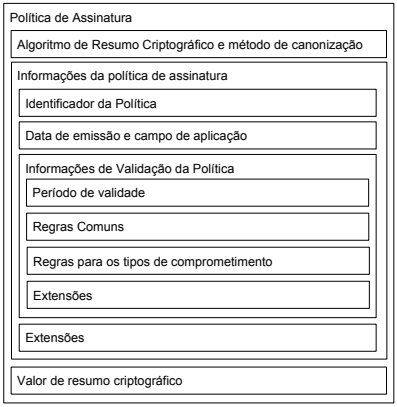


Figura 10 – Estrutura geral de uma política de assinatura para ASN.1 e XML.

criptográfico calculado é diferente. A canonização permite que se produza o mesmo conjunto de bytes a partir de diferentes mas equivalentes documentos de políticas descritos em XML (62).

O componente *informações da política de assinatura* é formado pelos campos *identificador da política*, *data de emissão e campo de aplicação*, *informações de validação da política* e possíveis extensões.

O componente *identificador da política* deve ser único e pode ser uma URI, para políticas em XML, ou um Identificador de Objeto (OID), para políticas em ASN.1. O componente *campo de aplicação* é um texto que descreve o contexto no qual a política é aplicável. Esse texto é uma descrição da política e serve para auxiliar a sua escolha, tanto pelo signatário, quanto pelo destinatário do documento, durante o processo de assinatura do documento. O componente *informações de validação da política* contém o *período de validade*, *regras comuns*, *regras para os tipos de comprometimento* e possíveis *extensões*. O componente *período de validade* determina a data inicial e final de utilização da política.

O campo *regras comuns* é representado na Figura 11. Esse campo é composto por *regras do assinante e do verificador*, *condições de confiabilidade do signatário*, *condições de confiabilidade para carimbos do tempo*, *condições de confiabilidade para certificados de atributos*,

restrições de algoritmos e possíveis *extensões*. A inclusão de outros componentes não previstos, na forma de extensões, pode ser combinado entre os envolvidos na assinatura.

As *regras do assinante e do verificador* são representadas na Figura 12. A componente *regras do assinante* contém *objetos externos a assinatura*, que estabelece se o documento a ser assinado estará embarcado na assinatura, se estará fora dela, ou ainda se isso é indiferente.

Ainda nas regras do assinante estão presentes as listas de atributos assinados e não assinados. Os atributos assinados contém a lista de atributos que devem ser incluídos pelo signatário na assinatura e devem ser obrigatoriamente verificados pelo destinatário do documento. Já os atributos não-assinados devem ser incluídos pelo assinante, mas verificados de forma opcional. Isso ocorre pois não há como se garantir a autenticidade desses atributos.

O campo *referências obrigatórias a certificados*, dentro ainda das *regras do assinante*, indica se o assinante deve fornecer uma referência ao seu certificado, a todo o caminho de certificação do seu certificado ou se isso não é necessário. O componente *dados de certificados obrigatórios* identifica se o assinante deve fornecer os certificados ou a toda a cadeia de certificação na assinatura. Finalmente, as regras do assinante possivelmente incluem um campo *extensões*.

O componente *regras do verificador* é composto pelos campos: *lista de atributos não-assinados* e possíveis *extensões*. De forma aná-

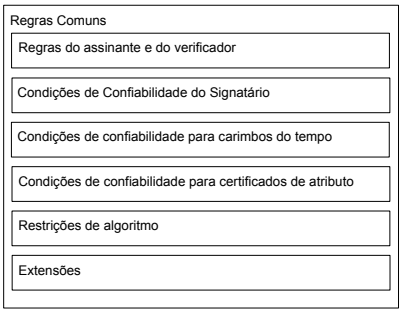


Figura 11 – Estrutura das regras comuns de uma política de assinatura

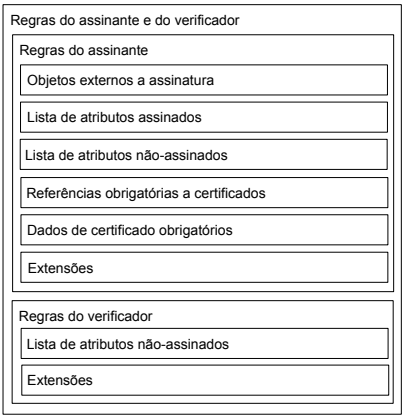


Figura 12 – Estrutura das regras do assinante e verificador

loga às *regras do assinante*, a *lista de atributos não-assinados* identifica quais os atributos não-assinados que competem ao verificador adicionar à assinatura do documento.

Os campos *condições de confiabilidade do signatário*, *condições de confiabilidade para carimbos do tempo* e *condições de confiabilidade para certificados de atributos* presentes nas *regras comuns* (ver Figura 11), estabelecem quais as âncoras de confiança, as condições sobre as políticas de certificação dos respectivos certificados e quais os métodos de revogação podem ser utilizados. Dessas estruturas a única obrigatória é a *condições de confiabilidade do signatário*. Esse componente *condições de confiabilidade do signatário* pode indicar a inclusão, não somente do certificado do signatário na assinatura, mas também, opcionalmente, outros certificados que por ventura poderiam ser necessários para proceder a validação da assinatura.

O componente *restrições de algoritmos* lista os algoritmos e respectivos parâmetros destes algoritmos que podem ser utilizados na geração da assinatura digital e seus atributos. Há ainda um espaço para *extensões* opcionais na estrutura de regras comuns.

O componente *regras para os tipos de comprometimentos* (ver Figura 10) é similar ao componente *regras comuns*, com a diferença de que cada *regra de comprometimento* contém uma lista dos tipos de

comprometimento para o qual as regras descritas se aplicam, representadas pelo campo *comprometimentos*. Essa estrutura está representada na Figura 13.

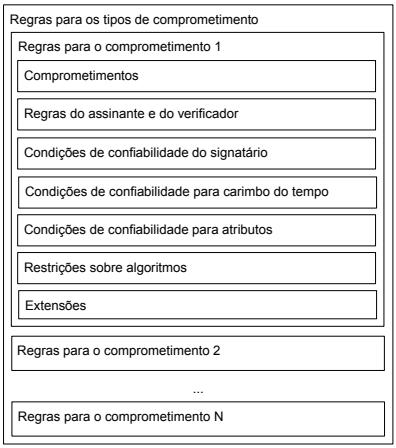


Figura 13 – Estrutura das regras para os tipos de comprometimento

O componente *regras para os tipos de comprometimento* é opcional. Ele somente é utilizado se há regras especiais para algum tipo de comprometimento, senão o componente *regras comuns* são utilizadas. Mesmo que o componente *regras para os tipos de comprometimento* esteja presente na política, este não limita quais os tipos de comprometimento que podem ser utilizados nas assinaturas.

3.5 POLÍTICAS DE ASSINATURA NO CADES E XADES

A RFC 5126 (8) define um conjunto de perfis para assinaturas CAdES. Essa RFC é baseada na especificação técnica sobre assinaturas avançadas em CMS do *European Telecommunications Standards Institute* (ETSI) (9). Uma assinatura CAdES é uma assinatura CMS acrescida de atributos assinados e não assinados que auxiliam na validação da assinatura.

No contexto de uma aplicação que faz uso de assinaturas digitais, existem vários tipos de usuários envolvidos. Em geral, esses são

os usuários típicos: assinante, verificador, emissor de políticas de assinatura, árbitro e provedor de serviços confiáveis.

O assinante é o responsável pela assinatura digital propriamente dita e respectiva política, provendo as evidências para o seu comprometimento com o documento assinado. Esse comprometimento pode ser referenciado na assinatura digital através de atributos.

O verificador deve seguir as regras de validação propostas pela política de assinatura para verificar a assinatura digital. Essas regras determinam as evidências que deveriam ter sido incluídas pelo assinante na assinatura do documento. Tais evidências são provas da validade da assinatura digital.

O árbitro é a entidade responsável pela negociação das eventuais disputas entre o verificador e o assinante. Para resolver uma disputa, ele também deve atuar como verificador e assim tomar a sua posição.

O provedor de serviços confiáveis é uma entidade ou um conjunto de entidades responsáveis por prover as relações de confiança entre o assinante e o verificador. Essas entidades, em geral, são os componentes de uma infraestrutura de chaves públicas (ICP), tal como as autoridades certificadoras.

Todos esses usuários, precisam conhecer as regras que deve ser utilizadas para gerar e verificar as assinaturas dos documentos. Essas regras podem ser listadas num documento de políticas de assinatura.

A política de assinatura pode ser referenciada de forma explícita ou ser reconhecida de forma implícita. Quando a referência é explícita, o documento de políticas é facilmente reconhecido. Entretanto, quando a política de assinatura é implícita, isso significa que essa deve ser inferida da aplicação alvo (onde o documento e sua assinatura fazem parte) ou de regras externas à assinatura relativas à semântica do documento assinado.

Tanto o CAdES, quanto o XAdES, não apresentam políticas de assinatura. Ao invés disso, eles definem um conjunto de perfis de assinatura. Perfis de assinatura, conforme a Definição 3.6 (veja página 63), consistem de formatos padrões sugeridos para assinaturas digitais.

O CAdES e o XAdES definem nove diferentes perfis de assinatura, conforme ilustra a Figura 14. Esses perfis são: assinatura eletrônica básica (BES), assinatura eletrônica com política explícita (EPES), assinatura eletrônica com carimbo do tempo (T), assinatura eletrônica com dados completos de validação (C), assinatura eletrônica estendida (X) tipo 1 e tipo 2, assinatura eletrônica estendida para longo prazo (XL) tipo 1 e tipo 2 e assinatura eletrônica de arquivamento (A). Cada um desses perfis representa um tipo distinto de assinatura digital com diferentes requisitos. Os propósitos desses perfis são enumerados na Tabela 2.

Tabela 2 – Perfis de Assinatura Digital.

Sigla	**Significado**	**Propósito**
BES	Assinatura eletrônica básica	Utililizado para assinar mensagem com pequeno prazo de validade.
EPES	assinatura eletrônica com política explícita	Utililizado para assinar mensagem com pequeno prazo de validade aderindo a uma política de assinatura.
T	assinatura eletrônica com carimbo do tempo	Utilizado para autenticar uma mensagem junto de uma data confiável.
C	assinatura eletrônica com dados completos de validação	Utilizado para autenticar mensagens que precisem ser verificadas utilizando dados de validação salvos de alguma forma pelo verificador.
X	assinatura eletrônica estendida	Utilizado para assinar mensagens com longo prazo de validade.
XL	assinatura eletrônica estendida para longo prazo	Utilizado para assinar mensagens com longo prazo de validade que precisam dos dados de validação embarcados na própria assinatura.
A	assinatura eletrônica de arquivamento	Utilizado para assinar mensagens que precisam ser arquivadas.

Todos esses perfis, à exceção do BES, podem incluir ou não uma referência a uma política de assinatura. No caso do EPES, essa referência é obrigatória.

Como pode ser visto na Figura 14, o perfil BES é o tipo mais simples de assinatura digital avançada. O EPES, por sua vez, é o BES adicionado de um identificador de política de assinatura. O perfil T, é o EPES adicionado de um carimbo de tempo sobre a assinatura. Esse carimbo protege somente o valor da assinatura, denotando assim apenas uma referência temporal à criação da assinatura. O perfil C é o T com a adição das referências aos certificados e aos dados de revogação. O

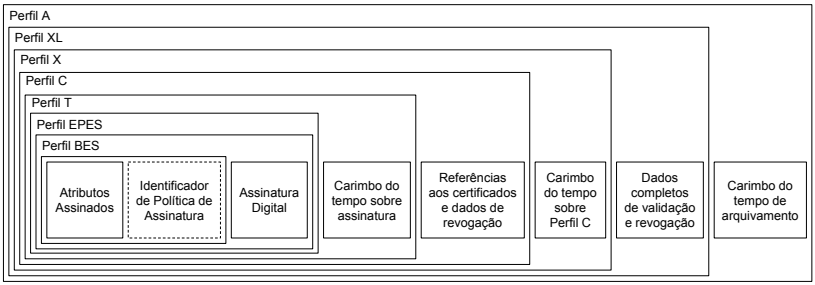


Figura 14 – Relação entre os perfis de assinatura digital avançada. O atributo "Identificador de Política de Assinatura" está representado tracejado uma vez que é opcional, mesmo para o perfil de assinatura T.

perfis X tipo 1 e 2, por sua vez, são o C adicionado de um carimbo do tempo sobre as referências. Os perfis XL tipos 1 e 2 são o perfil C adicionado dos dados completos de certificação e revogação e um carimbo do tempo sobre as referências. Nos perfis X e XL do tipo 1, o carimbo é sobre as referências e assinatura digital, atrelando assim os dois dados. Já nos perfis X e XL do tipo 2, o carimbo é somente sobre as referências dos dados de validação. Finalmente, o perfil A adiciona aos perfis XL tipo 1 ou 2 o carimbo de arquivamento. Esse carimbo de arquivamento é computado sobre todos os dados anteriores da assinatura, protegendo e fornecendo uma referência temporal à todos esses dados.

3.6 EXEMPLO DE POLÍTICA DE ASSINATURA

Uma política de assinatura é escolhida tal que a assinatura se adeque o melhor possível aos requisitos de uma aplicação em particular. Um exemplo de aplicação muito comum é a utilização de assinatura digital para fins de autenticação. Mensagens de autenticação são normalmente utilizadas uma única vez. Assim, o perfil de assinatura mais indicado é o EPES, uma vez que não há a necessidade de nenhum tipo de referência temporal para estender a validade por um período maior do que a validade do certificado do assinante. Nessa seção é apresentada uma política de assinatura em formato XML pela facilidade de leitura. Uma política em formato ASN.1 conteria informações análogas.

Na Figura 15 é ilustrada a forma como a estrutura geral de uma política de assinatura fica no formato XML. As partes omitidas serão demonstradas a seguir.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<pa:SignaturePolicy>
 <pa:SignPolicyDigestAlg Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
 <ds:Transforms>
  <ds:Transform Algorithm="http://www.w3.org/TR/xml-exc-c14n#" />
 </ds:Transforms>
 <pa:SignPolicyInfo>
  <pa:SignPolicyIdentifier>
   <XAdES:Identifier Qualifier="OIDAsURN">
    urn:oid:2.16.76.1.7.1.6.2.3
   </XAdES:Identifier>
  </pa:SignPolicyIdentifier>
  <pa:DateOfIssue>2016-04-27T00:00:00.000Z</pa:DateOfIssue>
  <pa:PolicyIssuerName>...</pa:PolicyIssuerName>
  <pa:FieldOfApplication>...</pa:FieldOfApplication>
  <pa:SignatureValidationPolicy>
   <pa:SigningPeriod>
    <pa:NotBefore>2016-04-27T00:00:00.000Z</pa:NotBefore>
    <pa:NotAfter>2029-03-02T00:00:00.000Z</pa:NotAfter>
   </pa:SigningPeriod>
   <pa:CommonRules>
    <pa:SignerAndVerifierRules> ... </pa:SignerAndVerifierRules>
    <pa:SigningCertTrustCondition> ... </pa:SigningCertTrustCondition>
    <pa:TimeStampTrustCondition />
    <pa:AlgorithmConstraintSet>
     ...
    </pa:AlgorithmConstraintSet>
   </pa:CommonRules>
   <pa:CommitmentRules>
   ...
   </pa:CommitmentRules>
  </pa:SignatureValidationPolicy>
 </pa:SignPolicyInfo>
 <pa:SignPolicyDigest>...</pa:SignPolicyDigest>
</pa:SignaturePolicy>
```

Figura 15 – Estrutura geral de uma política de assinatura em formato XML.

Adicionalmente, é desejavel nesse exemplo de aplicação, que haja uma referência assinada ao certificado do usuário sendo autenticado. Essa regra é prevista para o atributo assinado *SigningCertificate*. O propósito desse atributo é mitigar possíveis confusões com certificados do usuário emitidos para uma mesma chave pública. Por exemplo, sem

essa regra, o verificador de autenticação não teria como identificar inequivocamente o certificado do usuário sendo autenticado. O usuário poderia ter mais de um certificado com a mesma chave pública e possívelmente com status distintos. Um poderia estar válido e o outro revogado.

Para que o verificador de autenticação possa verificar a assinatura digital, é necessário que ele tenha o certificado do usuário e todo o seu caminho de certificação. De forma a facilitar o provimento desse certificado e do seu caminho de certificação, a política de assinatura poderia requerer a inclusão desses certificados na assinatura digital.

Observa-se, no entanto, que é comum que os certificados dos usuários possuam a extensão *Authority Information Access* (AIA) (45, veja seção 4.2.2.1, página 48). Com isso o verificador de autenticação teria dados de onde obter o caminho de certificação. Nesse caso, a política poderia unicamente requerer a inclusão do certificado do usuário sendo autenticado na assinatura.

Essa regra e a anteriormente citada pode ser vista na Figura 16. Nas regras apresentadas nessa figura também pode-se observar os atributos obrigatórios definidos pela política.

```
<pa:SignerAndVerifierRules>
 <pa:SignerRules>
  <pa:MandatedSignedQProperties>
   <pa:QPropertyID>SigningCertificate</pa:QPropertyID>
   <pa:QPropertyID>SignaturePolicyIdentifier</pa:QPropertyID>
  </pa:MandatedSignedQProperties>
  <pa:MandatedUnsignedQProperties />
  <pa:MandatedCertificateRef>signerOnly</pa:MandatedCertificateRef>
  <pa:MandatedCertificateInfo>signerOnly
  </pa:MandatedCertificateInfo>
 </pa:SignerRules>
 <pa:VerifierRules>
  <pa:MandatedQUnsignedProperties />
 </pa:VerifierRules>
</pa:SignerAndVerifierRules>
```

Figura 16 – Regras do assinante e do verificador.

Outra informação importante para o autenticador, é conhecer as âncoras de confiança, de forma a poder validar a cadeia de certificados do usuário sendo autenticado. O autenticador deve optar por aceitar ou

não essas âncoras de confiança. Para essa finalidade, a política de assinatura contém a lista de âncoras de confiança as quais os certificados utilizados para assinatura digital devem estar sujeitos. A política de assinatura pode, para cada âncora, limitar as políticas de certificação que podem ser utilizadas pelo assinante. Outra possibilidade da política de assinatura, é limitar o comprimento do caminho de certificação. Entretanto, isso é raramente utilizado, uma vez que essa limitação é melhor tratada pelos processos relacionados à própria ICP.

As âncoras de confiança na política de assinatura são segregadas em três grupos. O primeiro grupo contém as âncoras que devem ser utilizadas para certificados de assinantes. O segundo grupo para certificados de carimbadoras responsáveis pela emissão de carimbos do tempo apostos às assinaturas. E o terceiro grupo, as âncoras dos certificados de atributo. Como estamos tratando de uma política de autenticação rápida, o segundo grupo, de âncoras para carimbos do tempo, não é necessário, pois não se utilizam carimbos do tempo nesse contexto.

Entretanto, caso um carimbo do tempo seja afixado à assinatura, a âncora de confiança do certificado da carimbadora emissora deverá ser incluída, pelo menos, no grupo de âncoras para assinantes.

Nessa aplicação de autenticação, o terceiro grupo, de âncoras de confiança para certificados de atributos só deve ser incluído, caso sejam utilizados certificados de atributo, estabelecendo um tipo de comprometimento. Por exemplo, se o usuário sendo autenticado for um médico, e o autenticador precisar saber disso, o certificado de atributo poderia indicar tal comprometimento.

As condições de confiabilidade da política de exemplo podem ser observadas na Figura 17.

Os parâmetros sobre algoritmos criptográficos utilizados em assinaturas digitais também podem ser restringidos pela política de assinatura. Contudo, é preciso levar em conta que esses algoritmos também são estabelecidos pela política de certificação. Assim, a política deveria somente adicionar algum parâmetro extra, complementando aqueles da política de certificação.

Normalmente, a escolha do resumo criptográfico a ser utilizado numa assinatura, não é regida por regras gerais de uma ICP. Por exem-

```
<pa:SigningCertTrustCondition>
 <pa:SignerTrustTrees>
  <pa:CertificateTrustPoint>
   <pa:TrustPoint>
    <pa:X509Certificate>...
    </pa:X509Certificate>
   </pa:TrustPoint>
   <pa:AcceptablePolicySet>
    ...
   </pa:AcceptablePolicySet>
  </pa:CertificateTrustPoint>
  <pa:CertificateTrustPoint>
   <pa:TrustPoint>
    <pa:X509Certificate>...
    </pa:X509Certificate>
   </pa:TrustPoint>
   <pa:AcceptablePolicySet>
    ...
   </pa:AcceptablePolicySet>
  </pa:CertificateTrustPoint>
 </pa:SignerTrustTrees>
 <pa:SignerRevReq>
  <pa:EndRevReq>
   <pa:EnuRevReq>eithercheck</pa:EnuRevReq>
  </pa:EndRevReq>
  <pa:CACerts>
   <pa:EnuRevReq>eithercheck</pa:EnuRevReq>
  </pa:CACerts>
 </pa:SignerRevReq>
</pa:SigningCertTrustCondition>
```

Figura 17 – Condições de Confiabilidade para o assinante.

plo, não é comum a política de certificação determinar qual seria o algoritmo de resumo a ser utilizado nesse caso. Assim, a política de assinatura deveria incluir um ou mais algoritmos de resumo criptográfico e deixar que o assinante escolha o mais adequado.

A definição de quais algoritmos de resumo criptográfico farão parte de uma política de assinatura, deve levar em conta as estimativas computacionais de tempo de resistência desses algoritmos a colisões, para somente incluir aqueles que permanecerão válidos durante todo o período previsto para a vigência da política (63, 64). No nosso exemplo de política de assinatura para autenticação, como essa deve ser de curta duração, não há restrições quanto ao algoritmo a ser utilizado. Pode ser incluído qualquer algoritmo de resumo criptográfico válido. As regras definidas para o caso de exemplo podem ser vistas na Figura 18.

```
<pa:AlgorithmConstraintSet>
 <pa:SignerAlgConstraints>
  <pa:AlgAndLength>
   <pa:AlgId>http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
   </pa:AlgId>
   <pa:MinKeyLength>2048</pa:MinKeyLength>
  </pa:AlgAndLength>
  <pa:AlgAndLength>
   <pa:AlgId>http://www.w3.org/2001/04/xmldsig-more#rsa-sha512
   </pa:AlgId>
   <pa:MinKeyLength>2048</pa:MinKeyLength>
  </pa:AlgAndLength>
 </pa:SignerAlgConstraints>
</pa:AlgorithmConstraintSet>
```

Figura 18 – Regras sobre algoritmos.

Finalmente, as regras de comprometimento são usualmente utilizadas em contextos onde a política de assinatura é direcionada a uma aplicação específica. Por exemplo, no caso do PBAD, as políticas regem aplicações amplamente diferentes. Portanto, não são especificadas, nesse caso, regras de comprometimento. Entretanto, Ardieta et. al. (19) utilizam diversos tipos de comprometimento, para mensagens de autenticação.

3.7 PROTOCOLO DE TROCA JUSTA BASEADO EM POLÍTICA DE ASSINATURA

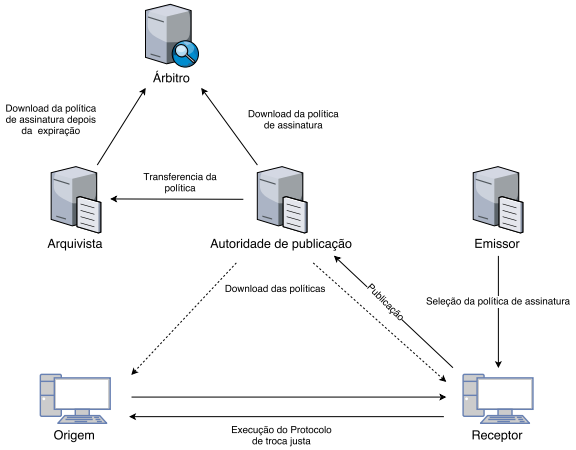
Ardieta et. al. (19) propuseram um protocolo de troca justa baseado em políticas de assinatura em formato XML. Protocolos de troca justa são utilizados para prevenir que um ou outro agente obtenha alguma vantagem indevida sobre os demais participantes. Podemos mencionar, como exemplo, a venda de um produto pela internet. Nesse caso, o protocolo de troca justa garante que nem o comprador e nem o vendedor obterão alguma evidência da compra se ambos não cumprirem seus papéis de forma correta. Se o protocolo não se completar da forma esperada, nenhuma das partes pode afirmar que a venda ocorreu.

Ardieta et. al. utilizam um conjunto de regras para criar e validar assinaturas digitais regida por políticas de assinatura de forma a evitar que se crie alguma situação de desvantagem tanto para o comprador, quanto para o vendedor. O protocolo proposto permite ao com-

prador de um produto na internet decidir se confia ou não nas regras que regem a transação eletrônica, melhorando a confiança dos usuários no comércio eletrônico.

Ardieta et. al definem um ciclo de vida para a gestão das políticas de assinatura utilizadas em seu protocolo, conforme ilustra a Figura 19. No referido trabalho, a política de assinatura é criada pela entidade *emissora*. A entidade, denominada de *autoridade de publicação*, é responsável pela distribuição da política de assinatura. A entidade, denomidada *arquivista*, é responsável por arquivar as políticas de assinatura. O arquivista deve manter as políticas de assinatura disponíveis para que o árbitro possa, mesmo depois que estas políticas não estejam mais publicamente disponíveis, utilizá-las na resolução de disputas. Os papel de *árbitro* é semelhante ao papel de um árbitro clássico num processo de assinatura digital. O *árbitro* age como um verificador quando houver conflitos em relação a validade da assinatura. As entidades *origem* e *receptor* atuam tanto como assinante ou verificador de uma assinatura digital em diferentes momentos da execução do protocolo.

Figura 19 – Relação entre as entidades envolvidas no protocolo de troca justa



Fonte: Ardieta et. al. (19)

A política de assinatura é utilizada para definir o tipo de comprometimento que a assinatura digital representa em diferentes momentos, de forma a tornar o protocolo justo para as partes envolvidas.

O protocolo de troca justa descrito por eles permite a criação de um registro da transação de compra utilizando diferentes tipos de comprometimento fornecidos pela política de assinatura. Assim, as assinaturas produzidas nas etapas intermediárias do processo não utilizam qualquer tipo de comprometimento que possa prejudicar algum dos envolvidos. Um comprometimento que representa a execução da transação como um todo, somente na conclusão do protocolo, garantindo assim, as propriedades almejadas.

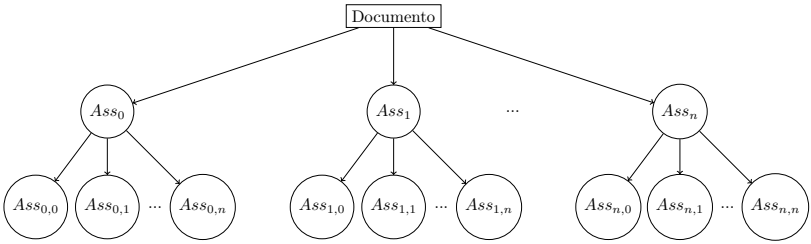
3.8 POLÍTICA DE ASSINATURA COM DEFINIÇÃO DE DEPENDÊNCIAS ENTRE ASSINATURAS

Adieta et. al. (65) propõem uma solução para o estabelecimento das relações entre as assinaturas de uma mesma transação eletrônica. Nesse trabalho, é proposta uma nova estrutura para política de assinatura em que as relações entre múltiplas assinaturas são representadas em forma de árvore. As justificativas para a proposição desse novo tipo de política são descritas no relatório técnico sobre políticas de assinatura para negócios publicado pelo ETSI (60).

Ardieta et. al. escolheram uma estrutura de árvore para a descrição da política de assinatura, que será utilizada para a geração de diferentes assinaturas, conforme ilustra a Figura 20. Essa forma de estrutura facilita a descrição da relação entre diferentes assinaturas. Na proposta deles, os nodos em mesmo nível representam co-assinaturas, e os filhos de um nodo representam contra-assinaturas. Cada um desses nodos contém as regras de validação das políticas de assinatura definidas em ASN.1.

Para a validação de uma assinatura é necessário identificar qual o nodo da política de assinatura contém as regras dessa assinatura. Para tal, é utilizado um algoritmo de busca em profundidade de forma a parear a assinatura em questão com o seu nodo correspondente na árvore da política de assinatura. Este algoritmo deve ser executado no início da validação da assinatura.

Figura 20 – Exemplo de árvore de relações entre assinaturas. Ass_x representam diferentes co-assinaturas x. $Ass_{x,y}$ representam diferentes contra-assinaturas y, para uma determinada co-assinatura x.



Fonte: Ardieta et. al. (65)

3.9 PATENTES RELACIONADAS A POLÍTICAS DE ASSINATURA

Mello e Dhalla (66) registraram uma patente em que propõem o uso de políticas de assinatura para permitir que documentos assinados possam ser modificados. Nesse trabalho, a política de assinatura é utilizada para definir quais partes podem e quais não podem ser modificadas. Essa patente não está relacionada com nenhum formato específico de documento. Entretanto, a política de assinatura é estruturada em árvore, como forma de gerenciamentos das partes de um documento. A árvore identifica quais partes do documento assinado podem ser alteradas.

Bowe (67) registrou uma patente onde é proposto um método que permite ao assinante assinar remotamente documentos eletrônicos, usando uma chave privada armazenada num servidor. Na patente dele, políticas de assinatura são utilizadas para reger o processo de assinatura a ser gerada no servidor. Essa patente está fortemente atrelada a assinaturas XMLDSig, uma vez que os processos do servidor utilizam esse formato. A principal inovação da sua patente é que o processo de criptografia assimétrica acontece do lado do servidor de aplicação, diferente dos métodos tradicionais onde esse processo ocorre ou no *hardware* criptográfico ou via *software*, ambos do lado do cliente. Também é descrito um processo de verificação remota da assinatura através de um protocolo.

3.10 CONCLUSÃO

Nesse capítulo são definidos os principais termos relacionados ao ciclo de vida de políticas de assinatura. Onde foi dado ênfase ao processo de determinação das regras que deverão ser incluídas numa política de assinatura motivada por uma determinada aplicação. Também é apresentado, tanto para ASN.1 como para XML, o formato comumente aceito para políticas. A apresentação desses formatos esclarece quais as regras que podem ser definidas por uma política. Em seguida, é esposto a relação entre prefis de asssinatura e políticas de assinatura em formatos de assinatura digital avançada.

Um exemplo de política de assinatura para autenticação então é apresentado. É discutido o motivo das informações presentes em cada parte da política. São apontados também as características da política em questão que se espera variar para outras aplicações.

Na parte final desse capítulo é apresentado um exemplo de onde uma política de assinatura pode ser utilizada. Essa seção apresenta um protocolo de troca justa baseado em políticas de assinatura. Nesse trabalho foram identificados papéis relativos ao ciclo de vida de políticas de assinatura. Em seguida, é apresentado uma mudança na política de assinatura para tratar relações entre assinaturas. O trabalho trata de um assunto que não é coberto pela proposta original de política de assinatura, mas que é bastante relevante para o uso de assinaturas digitais numa aplicação para negócios.

Por último, duas patentes são descritas. A primeira trata do uso de políticas para permitir a edição de documentos após esses terem sido assinados. A proposta permite que a edição de documentos assinados seja feita sem que a assinatura se torne inválida. A segunda patente é sobre um método para assinatura remota. A assinatura é feita num servidor de aplicação. A chave privada do assinante também fica nesse servidor. Políticas de assinatura são utilizadas para reger as assinaturas geradas por esse servidor de aplicação.

4 MÉTODO PARA ATUALIZAÇÃO DA POLÍTICA DE ASSINATURA

4.1 INTRODUÇÃO

Nesse capítulo é apresentada uma proposta para atualização dinâmica da política de assinatura. Esta proposta advém da constatação de que políticas de assinatura, da forma como são definidas atualmente, conflitam com o dinamismo necessário às assinaturas digitais. Esse dinamismo é observado nos diferentes requisitos que uma assinatura deve atender em diferentes situações.

As informações que motivam essa proposta são descritas na Seção 4.2. Nessa seção, são relacionadas as contradições encontradas na literatura relativa ao tema. Dessas contradições, a principal que motivou esse trabalho é a relação entre perfis e políticas de assinatura, visto que, embora cada um tenha as suas vantagens e desvantagens, o ideal seria combinar as capacidades de ambas para o uso nas aplicações.

A Seção 4.3 apresenta a proposta desse trabalho. Onde são explicadas as extensões propostas para políticas de assinatura nos formatos ASN.1 e XML, bem como os atributos não-assinados que acompanham essas extensões para os formatos de assinatura CAdES e XAdES. Ainda nessa seção, é exposto como o par extensão de política e atributo não-assinado pode ser utilizado pelo verificador da assinatura para atualizar dinamicamente a política de assinatura, sem invalidar a assinatura digital em questão.

Uma análise da proposta é apresentada na Seção 4.4. São listados os benefícios e malefícios causados pelo uso da nossa proposta. Foi adicionado um novo elemento no processo de assinatura digital. Esse elemento foi chamado de mantenedor. O mantenedor pode ser incorporado no processo como entidade com a responsabilidade de adequar a assinatura as necessidades do verificador, quando possível. Observou-se também, que a concepção de políticas de assinatura pela entidade emissora ficou mais complexa, já que está deve agora não só, identificar as diferentes políticas, como também, identificar as possíveis transições e garantir a compatibilidade entre essas transições. Finalmente, verificou-se que mesmo com as transições entre políticas ainda ocorrerão problemas relacionados ao arquivamento de assinaturas digitais

quando se utiliza políticas de assinatura.

4.2 PROBLEMAS COM O MÉTODO ATUAL

Observando os padrões CAdES e XAdES, pode-se verificar que os perfis propostos nos padrões são evolutivos, ou seja, uma assinatura poderia receber atributos adicionais e passar para outro perfil caso seja necessário. Já observando a política de assinatura, percebe-se que esta não é capaz de caracterizar essa transformação da assinatura. Quando uma assinatura digital é criada referenciando uma política de assinatura através de um identificador único, este não pode ser alterado, pois é identificado através de um atributo assinado. Assim, como consequência, os requisitos declarados da assinatura não podem ser alterados. Essa é uma grande limitação, pois os padrões avançados trazem a ideia de adaptação da assinatura à perfis mais completos desde a sua concepção. Por outro lado, ao utilizar uma assinatura digital sem política, perde-se usabilidade nas ferramentas, pois o software de verificação não tem como se configurar automaticamente, auxiliando o usuário, a não ser que este software verificador seja feito sob medida para alguma aplicação.

Outro ponto relevante do uso das políticas é que o assinante consegue expressar um comprometimento de maneira explícita com formalidade. No caso de perfis, embora o assinante possa expressar algum comprometimento, este estará sujeito a interpretação das partes e poderá incorrer em conflitos sobre o seu significado. A formalização de comprometimentos é um benefício bastante interessante para aplicações de assinatura digital como pode ser visto no protocolo de troca justa proposto por Ardieta et. al. (ver Seção 3.7, página 78).

Os formatos e informações relacionados para políticas de assinatura em ASN.1 e XML estabelecem os requisitos para assinatura digital apenas no momento da assinatura. Entende-se que por estarem intrinsecamente ligadas a todo o processo de assinatura digital, as políticas de assinatura também deveriam auxiliar no processo de complementação da assinatura digital. Entretanto percebe-se que nos formatos ASN.1 e XML de política de assinatura não há qualquer tipo de informação que possamos relacionar com essa parte do processo. Outro ponto, dada uma assinatura feita sob uma determinada política, se esta assinatura passou por um processo de complementação, ela pode ser idêntica a

uma assinatura feita sob outra política de assinatura com mais requisitos. Portanto, entende-se que existe uma possível descaracterização da política de assinatura dentro do processo de complementação.

4.3 PROPOSTA

Assinaturas digitais avançadas podem ser utilizadas sem políticas. Entretanto, se utilizadas sem políticas perde-se em usabilidade e expressividade pois a interpretação do comprometimento da assinatura digital fica subjetivo. Já se políticas de assinatura forem utilizadas, o processo de manutenção das assinaturas fica prejudicado pois a política pode passar a não representar com corretude os requisitos sobre uma determinada assinatura digital.

Portanto, o ideal seria possibilitar que políticas de assinatura fossem utilizadas para determinar o comprometimento, só que com a possibilidade de mudança da mesma para melhor representar os requisitos sobre aquela assinatura digital.

Para que isso seja possível, primeiramente é necessário ter alguns cuidados, pois esse processo não deve permitir a redução de requisitos sobre uma assinatura digital nem a mudança do comprometimento expressado pelo assinante. A redução de requisitos sobre uma assinatura digital não é interessante pois pode acarretar na perda de validade.

A redução de requisitos também não está de acordo com o que entende-se por processo de complementação da assinatura. A mudança de comprometimento do assinante permitiria a manipulação do mesmo e causaria problemas em protocolos como o de troca justa discutido anteriormente.

Observando como os perfis são propostos nos padrões CAdES e XAdES, pode-se notar que estes seguem um processo de complementação da assinatura digital que pode ser interessante para alguma aplicação, portanto, pode-se usar essa evolução de atributos como base de políticas de assinatura que possuem transições entre si.

As transições sugeridas podem ser visualizadas na Figura 21. Cada política formaliza um perfil de assinatura, definindo exatamente quais os atributos assinados, não-assinados e outras informações neces-

sárias a assinatura. As políticas começam a partir do perfil "EPES" pois o perfil "BES" não deve ter indicação de política de assinatura. A nomenclatura de cada política foi feita da seguinte forma: o nome PA EPES indica que está política de assinatura formaliza os requisitos do perfil EPES, o nome PA T formaliza os requisitos do perfil "T" e assim por diante. A figura não apresenta todas as transições da política, por exemplo a PA EPES tem transições para todas as outras políticas de assinatura, entretanto, essas transições estão representadas através de caminhos indiretos.

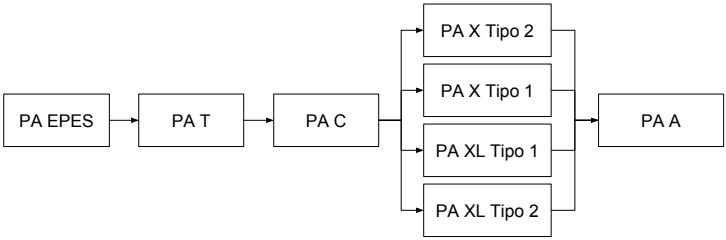


Figura 21 – Transições sugeridas para políticas de assinatura baseadas nos perfis.

A indicação das transições possíveis de uma política de assinatura pode ser feita através da inclusão de referências as outras políticas. Cada referência representa uma transição possível. A Figura 21 não representa exaustivamente as transições. Recomenda-se que todas as transições possíveis entre políticas de assinatura sejam representadas de maneira direta.

Por exemplo, consideremos as políticas A, B e C. Se existe uma transição da política A para a política B, e uma de B para C, podemos inferir que existe uma transição indireta da política A para a política C. Nesse trabalho, não foi identificado nenhum motivo para não tornar essa transição direta, ou seja, incluir uma referência da política C também na política A.

Ainda sobre as transições, para que uma transição não cause problemas com os comprometimentos da assinatura, as políticas entre as quais existem transições, devem definir os mesmos tipos de comprometimentos. O que pode variar entre essas políticas é apenas os requisitos sobre a assinatura digital.

As transições podem ser representadas por meio de uma extensão da política de assinatura. Extensões são previstas por políticas de assinatura (4, 21), dessa forma essas políticas ainda serão compatíveis com softwares que não implementem o suporte as transições. Entretanto, caso a assinatura já tenha sofrido uma transição de política de assinatura, os softwares que não suportam transições irão apresentar resultados de verificação diferentes dos que suportam. Isso se deve ao fato de que os softwares que não suportam transições irão verificar a assinatura de acordo com sua política de assinatura utilizada na geração da assinatura.

A especificação ASN.1 da extensão para políticas de assinatura em formato ASN.1 pode ser observada na Figura 22.

```
SignPolTransitions ::= SEQUENCE
         OF SignPolTransition

SignPolTransition ::= SEQUENCE {
    signPolicyIdentifier
            OBJECT IDENTIFIER,
    signPolicyHashAlg
        AlgorithmIdentifier,
    signPolicyHash
            SignPolicyHash
}
```

Figura 22 – Especificação da extensão de Políticas de assinatura para formato ASN.1.

A Figura 23 apresenta a extensão de políticas de assinatura em formato.

A extensão inclui os resumos criptográficos das políticas de assinatura que estão no conjunto de transições possíveis. Estes resumos representam as referências à transições possíveis. O valor desses resumos criptográficos deve ser igual aos valores encontrados no campo *valor de resumo criptográfico* das políticas referenciadas, descrito na seção 3.4.

Essa extensão deve ser incluída da estrutura *regras comuns* ou *regras para o tipo de comprometimento*. Essas estruturas também estão descritas na seção 3.4.

```
<xsd:element name="SignPolicyTransitions"
    type="SignPolicyTransitionsType"/>
<xsd:complexType
        name="SignPolicyTransitionsType">
    <xsd:sequence maxOccurs="unbounded">
        <xsd:element
                name="SignPolicyTransition"
                type="SignPolicyTransitionType"/>
    </xsd:sequence>
</xsd:complexType>

<xsd:element name="SignPolicyTransition"
    type="SignPolicyTransitionType"/>
<xsd:complexType name="SignPolicyTransitionType">
    <xsd:sequence>
        <xsd:element
                name="SignPolicyIdentifier"
                type="XAdES:ObjectIdentifierType"/>
        <xsd:element ref="ds:Transforms" minOccurs="0"/>
        <xsd:element name="SignPolicyDigestAlg"
            type="ds:DigestMethodType"/>
        <xsd:element
                name="SignPolicyDigest"
                type="ds:DigestValueType"/>
    </xsd:sequence>
</xsd:complexType>
```

Figura 23 – Especificação da extensão de políticas de assinatura para o formato XML.

Para que alguma entidade (iremos nos referenciar a essa entidade como mantenedor) atualize a política de assinatura numa assinatura que já foi gerada, esta deve incluir um atributo não-assinado que a referencia, através do OID e resumo criptográfico, a nova política de assinatura que deve ser utilizada para verificação. Esse atributo é muito parecido com o atributo assinado conhecido como *SignaturePolicyIdentifier* (1, 68), que identifica a política de assinatura com a qual a assinatura foi gerada, entretanto, este atributo não é assinado. Como o atributo proposto não é assinado, ele pode ser incluso por qualquer agente. A inclusão deste atributo na assinatura, caracteriza o papel do mantenedor.

Após a inclusão desse atributo, o processo de validação deve passar a considerar a política indicada por esse atributo para validação. Portanto, possivelmente o mantenedor também será responsável pela inclusão de novos atributos não-assinados na assinatura, sendo que

este, é o processo de complementação da assinatura. É importante notar aqui também, que esse novo atributo pode registrar a história de transições que a assinatura sofreu.

Entretanto, como qualquer transição possível entre políticas deve possuir uma referência direta, pode-se optar também por manter apenas a última versão desse atributo, excluído assim o histórico de transições. A estrutura do atributo pode ser verificada na Figura 24 para CAdES. Para o uso do atributo definido para CAdES, é necessário que este tenha um OID definido para si. Esse trabalho não define um OID para esse atributo.

```
SignPolicyTransition ::= {
    sigPolicyId         SigPolicyId,
    signPolicyHashAlg
        AlgorithmIdentifier,
    sigPolicyHash     SigPolicyHash,
    timeReference     Time OPTIONAL
    -- Time was imported from RFC 3852 (CMS)
}
```

Figura 24 – Especificação ASN.1 para o atributo de transição da política de assinatura para CAdES.

A Figura 25 apresenta a estrutura do atributo para XAdES.

```
<xsd:element name="SignPolicyTransition"
    type="SignPolicyTransitionType"/>
<xsd:complexType name="SignPolicyTransitionType">
    <xsd:sequence>
        <xsd:element name="signPolicyId"
                type="XAdES:ObjectIdentifierType"/>
        <xsd:element name="SignPolicyDigestAlg"
            type="ds:DigestMethodType"/>
        <xsd:element ref="ds:Transforms" minOccurs="0"/>
        <xsd:element name="signPolicyHash"
                type="ds:DigestValue"/>
        <xsd:element name="timeReference"
                type="xsd:dateTime" minOccurs="0"/>
    </xsd:sequence>
</xsd:complexType>
```

Figura 25 – Especificação do atributo de transição da política de assinatura para XAdES.

Com a adição desse novo atributo, é necessário uma alteração no processo de verificação de assinatura. A conferência das transições entre as políticas de assinatura deve ser feita no início da validação. O verificador pode ordenar as atualizações de políticas de assinatura indicadas através da referência temporal, se esta estiver presente. A partir do atributo assinado que identifica a política de assinatura com a qual a assinatura foi gerada, deve-se verificar se esta política possui a transição para a alguma política de assinatura indicada pelas atualizações.

De posse de uma nova política de assinatura, pode-se repetir o processo verificando as transições indicadas na assinatura e encontrando uma transição possível segundo a política atual. Esse processo deve ser repetido até que não se encontrem mais transições possíveis. A política de assinatura com a qual se termina deve ser utilizada para verificar o restante das regras da assinatura digital, de acordo com o processo tradicional.

4.4 ANÁLISE DO MÉTODO PROPOSTO

A utilização do método proposto para atualização da política de assinatura incorre em mudanças significativas nos processos que utilizam assinaturas digitais com políticas. A atualização de uma política para outra tem que ser planejada com cuidado. Um ponto a se observar é que a política de assinatura para a qual se pode migrar não deve alterar regras sobre atributos assinados. Caso aconteça a migração de uma política para outra que obriga a inclusão de mais informações assinadas, a assinatura seria invalidada e a atualização seria inviável, pois o mantenedor não tem como alterar informações assinadas.

Outro ponto é a indicação dos tipos de comprometimento especificados pelas políticas de assinatura. No processo de atualização não é interessante permitir a mudança do comprometimento do assinante, uma vez que isso abriria possibilidade para que o assinante fosse manipulado. Portanto, as transições entre políticas devem manter os mesmos tipos de comprometimento para evitar esse problema.

Se o mantenedor optar por manter as diversas versões do atributo que indica a transição de política numa assinatura digital, está

assinatura carregará consigo um histórico de atualizações. A autenticidade desse histórico não pode ser verificada, pois esses atributos não são de nenhuma forma atrelados a assinatura e qualquer um poderia incluir na assinatura qualquer histórico, desde que respeita-se as transições possíveis indicadas na política de assinatura. Entretanto, esse histórico pode ser útil se o verificador utilizar outros meios para garantir sua autenticidade.

O processo de complementação da assinatura fica explícito no método proposto. Pois a assinatura irá pelo menos indicar qual a última transição de política de assinatura que foi feita. Dessa forma não há mais descaracterização de política como verificado no modelo tradicional. Outro ponto que se deve ressaltar é que as transições não são definitivas enquanto não for feito um carimbo de arquivamento sobre a assinatura.

A possibilidade de alterar a política de assinatura sem invalidar a assinatura permite que agora consideremos um novo ator na manutenção de documentos eletrônicos. Antes, caso o verificador não aceitasse a política de assinatura utilizada pelo assinante, seria necessário que o assinante gerasse uma nova assinatura, como é representado na Figura 26.

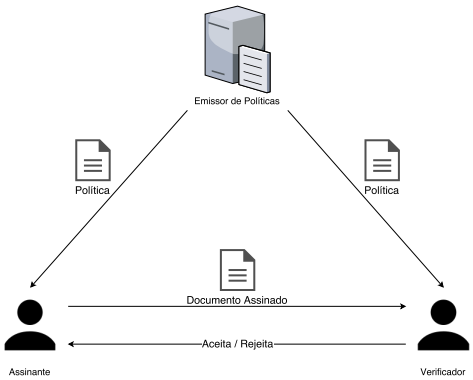


Figura 26 – Modelo atual de como a política de assinatura é utilizada.

Através do método proposto é possível que um terceiro, que pode oferecer um serviço de manutenção de documentos eletrônicos atualize a política de assinatura, ou até mesmo o próprio verificador, essa al-

teração na interação entre as entidades envolvidas é representada na Figura 27.

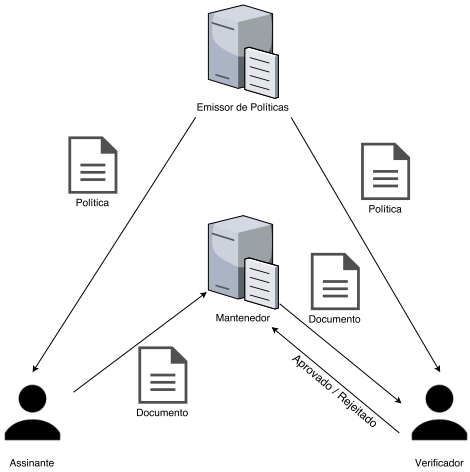


Figura 27 – Interação das entidades segundo o modelo proposto.

Considerando assinaturas em processo de arquivamento, caso alguma dessas assinaturas necessite mudanças nos seus requisitos para futuros carimbos de arquivamento, provavelmente a política na qual essas assinaturas se encontram não terão nenhuma transição possível. Essa limitação se da pois uma assinatura em processo de arquivamento precisará atender a alguma política que não existia no momento em que esta assinatura foi gerada. Portanto, essa limitação do modelo original permanece no modelo proposto. Quando a âncora de confiança embarcada numa política de assinatura expirar, não será mais possível validar as assinaturas feitas com ela.

4.5 CONCLUSÃO

Nesse capítulo foram apresentados os pontos em aberto ainda no uso de políticas de assinatura em processos de assinatura. Para esse trabalho, encarou-se como maior limitação a discrepância entre perfis de assinatura e políticas de assinatura, que impedia a política de assinatura de auxiliar os usuários no processo de complementação.

Para abordar tal problema foram propostas extensões para os formatos ASN.1 e XML de políticas de assinatura, bem como atributos não assinados para os formatos CAdES e XAdES de forma a possibilitar uma entidade, denominada mantenedor, atualizar a política de assinatura. A atualização da política de assinatura como foi definida nesse capítulo vai de encontro ao processo de complementação, resolvendo assim o problema abordado.

As implicações do uso do método proposto então são discutidas. Caracterizou-se um novo modelo de processo para assinaturas digitais que também inclui a figura do mantenedor. Verificou-se também que ainda uma limitação com relação ao uso de políticas em assinaturas em processo de arquivamento. A limitação identificada é que possivelmente a assinatura precisará referenciar uma política que não existia no momento de sua geração, isso não é possível nem através do modelo proposto.

5 AVALIAÇÃO

5.1 INTRODUÇÃO

Com o objetivo de avaliar a proposta apresentada no Capítulo 4, utilizou-se um conjunto de códigos de referência desenvolvido em nosso grupo de pesquisa. Esses códigos foram desenvolvidos para validar o padrão brasileiro de assinatura digital de documentos eletrônicos (PBAD). Conforme descrito na Seção 2.9 do Capítulo 2, o PBAD utiliza políticas de assinatura para guiar os geradores e verificadores de assinatura digital no âmbito da ICP-Brasil. Como o PBAD é baseado no XAdES e CAdES, ele sofre do mesmo problema de não permitir que a política de assinatura seja atualizada para atender novas condições que poderiam afetar a forma de validar as assinaturas digitais. Além disso, existe uma complexidade adicional no PBAD em relação as propostas internacionais. O PBAD estabelece atributos proibidos.

O conjunto dos códigos de referência foi modificado de forma a permitir a atualização dinâmica de políticas de assinatura conforme proposto nessa dissertação. Essa implementação foi utilizada para avaliar a nossa proposta.

Os códigos de referência são apresentados na Seção 5.2. Esses códigos servem de base para o desenvolvimento de softwares que assinam e verificam documentos eletrônicos. A modificação dos códigos de referência para se adequar a proposta dessa dissertação mostrou-se simples e de acordo com o esperado.

A Seção 5.3 apresenta o Gerenciador de Políticas utilizado para gerenciar o ciclo de vida de políticas de assinatura no PBAD. Essa ferramenta foi modificada para incluir a extensão da nossa proposta.

Por último, na Seção 5.4, são apresentadas simulações feitas com os novos códigos de referência e gerenciador de política. Com essas novas ferramentas foi possível avaliar o impacto da nova forma de gerenciar políticas de assinatura. Os resultados obtidos ficaram dentro do esperado com a proposta desse trabalho e atenderam as expectativas.

5.2 CÓDIGOS DE REFERÊNCIA

O projeto Códigos de Referência provê uma base de códigos que implementa os padrões CAdES e XAdES de forma adequada para uso no PBAD. Esse projeto é de código aberto. Esse código foi inicialmente desenvolvido na forma de uma biblioteca para que pudesse ser utilizado na mais variada gama de aplicações pela comunidade. Como produtos desse projeto produziu-se várias aplicações. Sendo elas um assinador e verificador de assinaturas digitais conformantes com o PBAD offline e outro acessível através da web, um verificador de conformidade de assinaturas offline e outro acessível através da web. Uma versão do verificador de conformidade pode ser acessada em verificador.iti.gov.br, esta ferramenta é amplamente utilizada pela comunidade.

Essa ferramenta foi desenvolvida para que pudesse ser utilizada unicamente com políticas de assinatura. A ferramenta é capaz de interpretrar dinamicamente as políticas de assinatura e se configurar para gerar e verificar as assinaturas de acordo.

A forma como a ferramenta foi desenvolvida também permite que o código da mesma seja integrado em outras aplicações, adaptando-se aos processos necessários. A forma de interação para gerar e verificar assinaturas foi definida e feita de forma que se possa tratar assinaturas XAdES ou CAdES de maneira transparente. Uma visão mais detalhada da arquitetura utilizada pode ser vista no trabalho Modelagem de um Software Orientado à Componentes para Assinatura Digital (69).

Os componentes da aplicação foram bastante isolados de forma que possam ser facilmente substituídos. A interação com os processos de assinatura digital são feitos através das interfaces *Signer* e *Verifier*. Destas a interface *Signer* não foi afetada pelas inclusões necessárias para essa proposta. Entretanto, a interface *Verifier* foi afetada pois foi necessário a adição de métodos para identificar as transições possíveis e executar uma transição.

A adição dos novos atributos requiridos pela nova política após uma transição pode ser feita utilizando o código já existente. O funcionamento interno do componente de assinatura também foi afetado, pois foi necessário adicionar a etapa inicial na validação para identificar qual a política que rege a assinatura que está sendo verificada. A implementação da decodificação da extensão da política de assinatura

e dos atributos não-assinados propostos foi simples e não teve grande impacto na ferramenta.

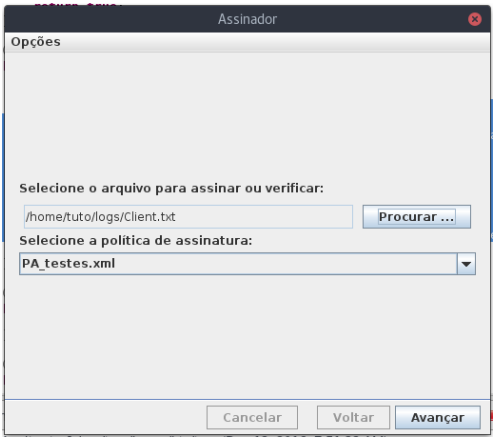


Figura 28 – Tela de seleção de documento para assinar ou verificar.

Na Figura 28 é possível ver a tela inicial do assinador. Se o usuário selecionar um documento eletrônico sem nenhuma assinatura, a ferramenta irá solicitar que o usuário selecione uma política de assinatura. Depois que a política foi selecionada a ferramenta sabe quais atributos deve incluir na assinatura e procede solicitando o desbloqueio da chave privada do assinante para proceder com a assinatura. Após o usuário informar seu PIN, a ferramenta completa o processo de assinatura e solicita ao usuário um local onde este deve salvar a assinatura digital recém gerada.

A Figura 29 mostra a interface caso o usuário selecione uma assinatura. Se esta assinatura digital não for válida, ou se a validação dela não for possível, o resultado será exibido e os botões para ações posteriores estarão bloqueados. Na figura é mostrado o exemplo onde a assinatura é válida e é possível contra-assinar a assinatura verificada ou atualizar sua política.

Esta última ação é decorrente da implementação desse trabalho. Se o usuário optar por contra-assinar ele será guiado um processo idêntico ao mencionado para a figura anterior, onde sua chave privada é solicitada. Caso ele opte por atualizar a política de assinatura, os atri-

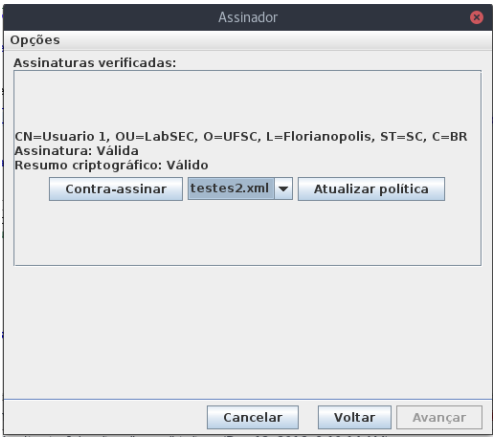


Figura 29 – Tela de status da assinatura digital.

butos novos serão incluídos na assinatura e a ferramenta solicitará que a assinatura seja salva em algum novo lugar.

5.3 GERENCIADOR DE POLÍTICAS DE ASSINATURA

O Gerenciador de Políticas de Assinatura é uma ferramenta criada para uso do ITI, capaz de gerar e editar políticas de assinatura para os formatos ASN.1 e XML. Esta ferramenta é atualmente utilizada pelo ITI para gerenciar as políticas de assinatura do PBAD e está em processo de manutenção. Ela foi desenvolvida pelo grupo de pesquisa do LabSEC.

Essa ferramenta permite ao usuário gerenciar o ciclo de vida das LPAs e PAs de acordo com o normativo do PBAD. O ciclo de vida desses artefatos envolve a atualização de políticas de assinatura e LPAs, criação de novas políticas e revogação das mesmas.

A tela inicial gerencia o estado geral de uma LPA. A lista à esquerda da interface, exposta na Figura 30, exibe as políticas de assinatura apontadas. O resto da interface apresenta informações sobre a LPA, sobre a PA selecionada na lista à esquerda e ações possíveis.

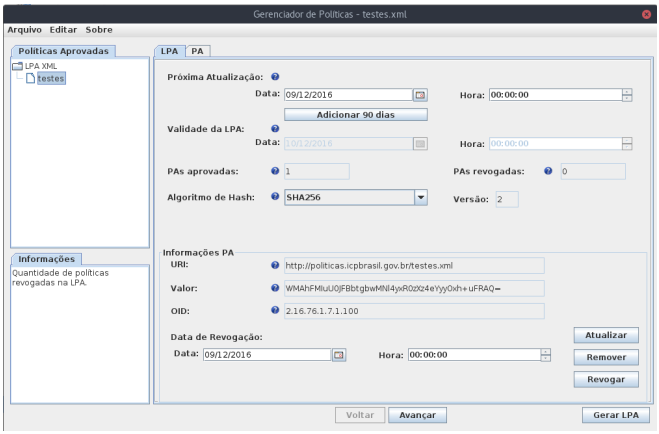


Figura 30 – Tela inicial do "Gerenciador de Políticas" exibindo dados de uma LPA.

Através do menu arquivo o usuário é capaz de criar uma nova política de assinatura para ser adicionada à LPA. A tela apresentada ao usuário após confirmar essa ação pode ser vista na Figura 31. A partir dessa parte da interface é possível editar o período da política, o

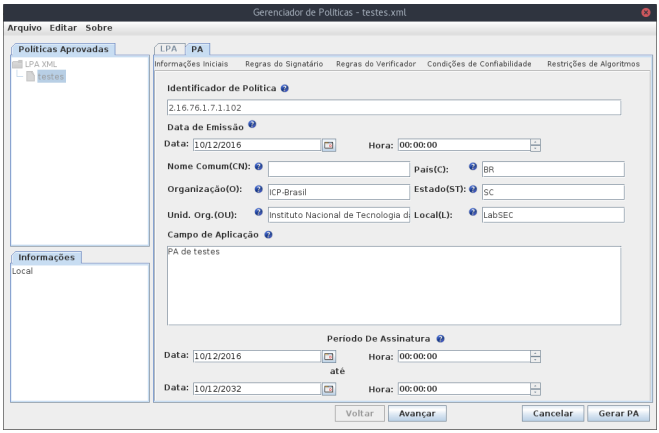


Figura 31 – Tela de edição de dados gerais de uma política de assinatura.

campo de aplicação e o identificador da política.

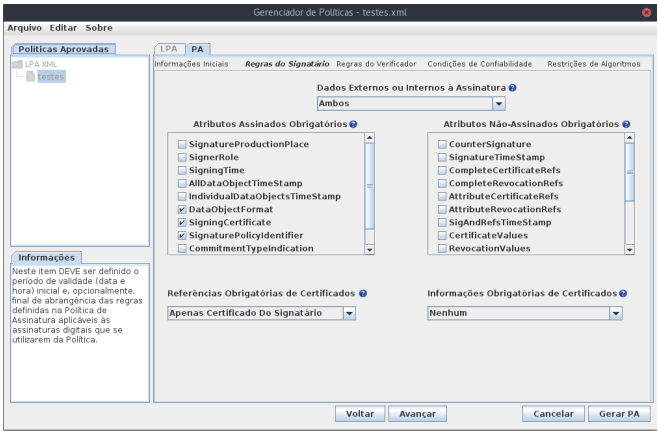


Figura 32 – Tela de edição das regras do assinante.

Após editar as informações gerais da política, pode-se editar as regras do assinante das regras comuns. A ferramenta não suporta a edição de regras de comprometimento, pois estas não são utilizadas no PBAD. Essa interface pode ser visualizada na Figura 32.

A opção para adição da extensão proposta foi adicionada na interface aberta pelo botão extensões dessa tela. Esse foi considerado o lugar mais propício para adição do suporte a extensão proposta. Entretanto, a extensão proposta não será adicionada as regras do assinante, mas sim no lugar reservado para extensões das regras comuns. Isso não deve afetar a usabilidade pois a maioria das extensões suportadas pela ferramenta são adicionadas nesse passo.

A seguir, as regras do verificados são definidas. Essa interface pode ser observada na Figura 33.

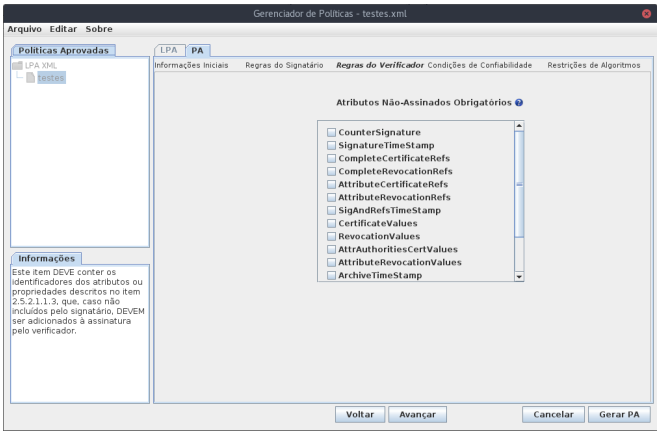


Figura 33 – Interface para edição das regras do verificador.

Na Figura 34, pode ser vista a interface que é utilizada para adicionar os conjuntos de âncoras de confiança para assinantes e carimbos do tempo. A ferramenta não suporta a adição de âncoras para certificados de atributo pois estes também não são utilizados no PBAD.

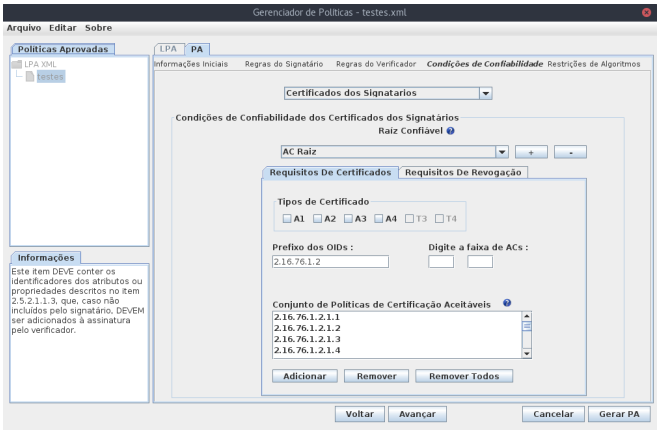


Figura 34 – Interface para edição dos conjuntos de âncoras de confiança.

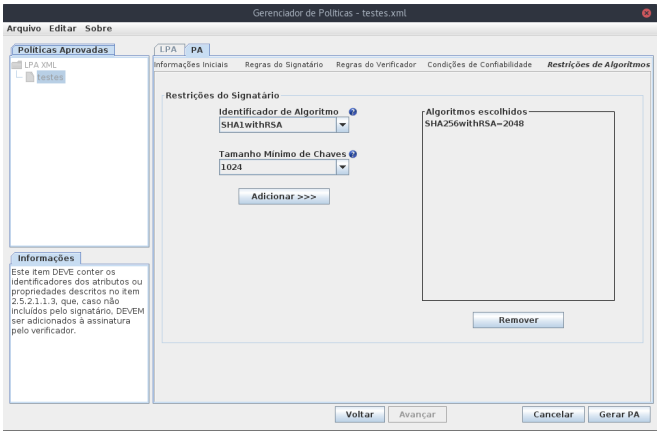


Figura 35 – Interface para edição das restrições sobre algoritmos.

Finalmente, na Figura 35, pode-se observar a tela para edição de restrições sobre algoritmos.

Um exemplo da extensão gerada pela ferramenta pode ser vista na Figura 36. A implementação de tal extensão foi mais simples do que inicialmente previsto. Ao implementar a extensão da política foi possível reutilizar código presente na ferramenta para criar as estruturas que a extensão utilizou. Isso não estava inicialmente previsto pois acreditava-se que existia um alto acoplamento entre essas estruturas uma vez que a ferramenta não foi planejada inicialmente para permitir o reuso de qualquer estrutura da política de assinatura. Entende-se que esse efeito inesperado se deve as bibliotecas utilizadas para implementar a codificação em XML e ASN.1 que foi adotada nessa ferramenta.

```
<pa:CommonRules>
 <pa:SignerAndVerifierRules>...</pa:SignerAndVerifierRules>
 <pa:SigningCertTrustCondition>...</pa:SigningCertTrustCondition>
 <pa:TimeStampTrustCondition/>
 <pa:AlgorithmConstraintSet>...</pa:AlgorithmConstraintSet>
 <pa:SignPolExtensions>
  <pa:SignPolExtension>
   <XAdES:policyTransitions>
    <ls:PolicyTransition>
     <pa:SignPolicyIdentifier>
      <XAdES:Identifier Qualifier="OIDAsURN">
       urn:oid:2.16.76.1.7.1.100
      </XAdES:Identifier>
     </pa:SignPolicyIdentifier>
     <ds:Transforms>
      <ds:Transform
         Algorithm="http://www.w3.org/TR/xml-exc-c14n#"/>
     </ds:Transforms>
     <pa:SignPolicyDigestAlg
        Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
     <pa:SignPolicyDigest>
      BkJSpoEEXWBofTtk9Op6sCksFzyaBOw0ecd+BsXIyRk=
     </pa:SignPolicyDigest>
    </ls:PolicyTransition>
   </XAdES:policyTransitions>
  </pa:SignPolExtension>
 </pa:SignPolExtensions>
</pa:CommonRules>
```

Figura 36 – Exemplo de extensão gerada com a ferramenta "Gerenciador de Políticas".

5.4 EXPERIMENTOS

Para verificar a proposta as extensões 22 e 23 foram implementadas no Gerenciador de Políticas de Assinatura. A adição dessas extensões não teve grande impacto na ferramenta e foi apenas necessário adicionar código para gerar e decodificar a extensão, além de criar uma interface para que o usuário possa selecionar para quais políticas a que ele está editando deve permitir a transição.

A implementação dos atributos propostos 24 e 25 causou um impacto maior no assinador de referência. O processo de validação teve de ser estendido para incorporar o uso dos atributos propostos. Algumas mudanças na arquitetura do software foi necessária para adicionar a possibilidade de um verificador atualizar a política de assinatura após

verificar a assinatura digital, entretanto boa parte do código para criar atributos pode ser reutilizado. A decodificação e geração dos atributos propostos foi de fácil implementação por serem bastante parecidos com os atributos identificadores de política de assinatura.

5.5 RESULTADOS OBTIDOS

Assinaturas XAdES foram geradas para todos os perfis disponíveis no PBAD. Os tamanhos obtidos foram: 3KB para AD-RB, 6KB para AD-RT, 13 KB para AD-RV, 33 KB para AD-RC e 47 KB para AD-RA. Assinaturas obtidas através de transições também possuem um tamanho semelhante e as diferenças não foram consideradas significativas. De posse desses dados fez-se uma simulação para avaliar qual o impacto da proposta em relação as questões de quantidade de dados necessária e quantidade de assinaturas perdida ao longo dos anos. Uma assinatura perdida é aquela em que não se pode manter evidências para a validade da mesma atendendo apenas aos requisitos da sua política de assinatura. A simulação abrange o período de 15 anos, por este ser o tempo de vida da AC-Raiz considerado, vale notar aqui que após esse período todas as assinaturas expirariam junto com sua respectiva AC-Raiz e outros métodos de preservação devem ser utilizados.

Primeiramente são apresentados os resultados da utilização de assinaturas digitais onde a obrigação dos participantes é garantir que a assinatura seja válida por pelo menos 10 anos (Ou seja, as assinaturas devem seguir o perfil AD-RV pelo menos). Utilizando as políticas em prática hoje, deve-se gerar inicialmente todas as assinaturas já aderentes ao perfil AD-RV. Após 10 anos, as assinaturas feitas no primeiro ano irão expirar e se tornaram inválidas. Para a simulação considerou-se que 1000 assinaturas novas seriam geradas todo ano. Esse número foi escolhido arbitrariamente, uma vez que o comportamento demonstrado com o gráfico é caracterizado por questões relativas as assinaturas individualmente. A representação gráfica dessa simulação pode ser vista na Figura 37.

Utilizando políticas de assinatura com transições e o mesmo número de assinaturas por ano, pode-se iniciar gerando assinaturas AD-RT, que garantem uma validade de pelo menos 5 anos com baixíssimo risco de expiração não esperada. No término desses cinco anos pode-se migrar as assinaturas que estão a ponto de expirar para o perfil AD-

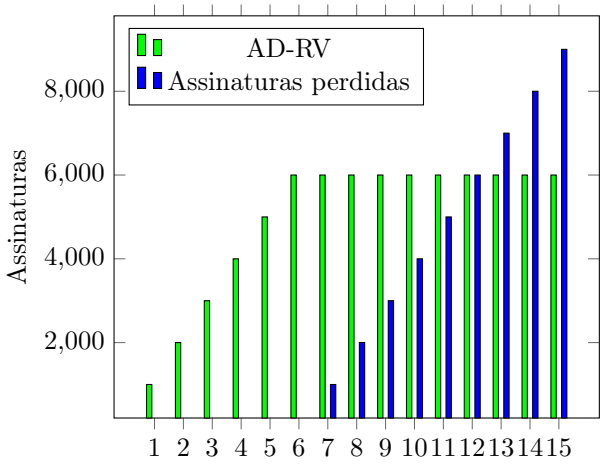


Figura 37 – Simulação de uso de assinatura durante 15 anos sob o modelo de políticas atuais.

RV, garantindo assim a validade destas por mais 5 anos, atingindo os 10 anos requeridos. Esse processo pode ser mantido até que a âncora de confiança expire, no nosso caso em 15 anos. Vale notar que as assinaturas geradas nos primeiros 3 anos tem seu perfil alterado para o AD-RA antes que seu algoritmo de resumo criptográfico seja quebrado, evitando assim a sua expiração. A representação gráfica dessa simulação pode ser vista na Figura 38.

5.6 CONCLUSÃO

Nesse capítulo foram apresentadas as ferramentas utilizadas e resultados obtidos com os experimentos feitos a fim de verificar a viabilidade das extensões propostas.

Na Seção 5.2, apresentou-se os códigos de referência desenvolvidos para o PBAD. Dentre as ferramentas geradas com esse código, destacou-se o assinador de verificador desktop, que teve sua interface estendida para suporte ao processo de transição de política de assinatura, bem como todo resto necessário para suportar o processo.

Na Seção 5.3 foi apresentada a ferramenta utilizada para geren-

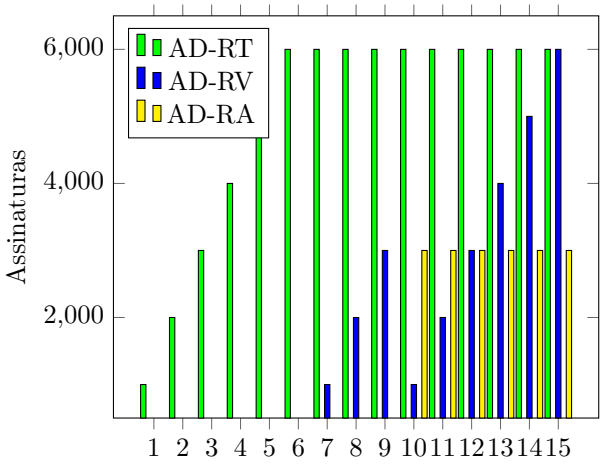


Figura 38 – Simulação de uso de assinatura durante 15 anos de acordo com o modelo de políticas proposto.

ciar o ciclo de vida das políticas de assinatura. Uma visão geral do processo de geração de uma política de assinatura foi dado e um exemplo da extensão gerada em XML é apresentada.

Os experimentos são descritos na Seção 5.4.

Finalmente, na Seção 5.5, são apresentados os resultados de simulações feitas com valores obtidos através de assinaturas geradas utilizando as ferramentas anteriormente apresentadas. Os valores apresentados são absolutos e espera-se que a proporção entre as quantidades se mantenha constante. Os números de assinaturas escolhidos não afetam de forma alguma as proporções obtidas nos resultados.

6 CONSIDERAÇÕS FINAIS

Neste trabalho mostramos que assinar documentos eletrônicos, diferentemente de assinar documentos papel, constitui-se de um esforço computacional e de comunicações de alta complexidade. Para assinar documentos eletrônicos é necessário o acesso a uma série de serviços providos de forma distribuída em rede, tais como primitivas criptográficas fornecidas por hardware especializados, carimbos do tempo fornecidos por autoridades de carimbo do tempo, certificados digitais emitidos por autoridades certificadoras e políticas de assinaturas emitidas por entidades emissoras de políticas.

Mostramos que, da mesma forma que os documentos eletrônicos, as assinaturas digitais são descritas por linguagens especiais. Nesse trabalho apresentamos as duas linguagens, e suas extensões, mais utilizadas para a descrição de assinaturas, ou seja, a Sintaxe de Mensagem Criptográfica (CMS) para assinaturas descritas em ASN.1 e a Assinatura Digital em XML (XMLDSig) para assinaturas em XML. Tecemos também comentários às assinaturas de documentos em formato PDF.

Nesse trabalho estamos interessados em dar sentido à assinatura digital. Entende-se como "dar sentido" o ato de mostrar os comprometimentos dos signatários às assinaturas digitais. A forma utilizada para que um receptor de um documento assinado digitalmente reconheça e aceite a assinatura é através da ferramenta política de assinatura. A política contém as regras que devem ser seguidas, tanto pelo assinante para produzir a assinatura, quanto pelo destinatário documento, que deve verificar se todas as regras apostas foram corretamente seguidas. Somente se isso ocorre é que a assinatura do documento pode ser considerada válida.

Apesar do grande apelo prático, existem poucos trabalhos científicos na literatura especializada sobre o tema principal desse trabalho. Há muitos trabalhos na camada mais básica do processo de assinatura, ou seja, propostas relacionadas a algoritmos criptográficos. Entretanto, há muito pouco nas camadas mais abstratas, tais como na definição de sentido às assinaturas e os respectivos comprometimentos dos signatários à mesma.

Em nosso levantamento bibliográfico, constatamos que os mai-

ores esforços e, portanto resultados nessa área estão sendo feitos por organismos de padronização, tais com o ETSI, a ISO, NIST, e no Brasil, o ITI. Em seguida, temos alguns trabalhos científicos, na forma de artigos. E finalmente, encontramos algumas patentes, que tratam de alguns desafios importantes da assinatura digital de documentos eletrônicos. Vários pesquisadores creditam a falta de pesquisas científicas relacionadas aos processos de assinatura digital à complexidade exagerada dos modelos de implementação de infraestrutura de chaves públicas.

Em termos de perfis e de políticas de assinatura, nesse trabalho, apresentamos as propostas XAdES para XML e CAdES para CMS. Tanto XAdES quanto CAdES apresentam um conjunto de perfis de assinatura digital, podendo ou não incluir uma referência a uma política de assinatura. O signatário escolhe, em acordo com o destinatário do documento eletrônico, um desses perfis e a política a ser adotada. Após isso, o signatário produz a assinatura e, portanto, os comprometimentos e respectivos artefatos que possibilitarão ao destinatário do documento, verificar a validade da assinatura.

Acontece que, após assinar o documento, pode ocorrer que haja a necessidade de se adicionar novos elementos à assinatura, não previstos quanto o documento foi assinado. Por exemplo, deseja-se preservar a assinatura por período superior ao previsto inicialmente. O uso de políticas, da forma como está definida na literatura científica e nos normativos nacionais e internacionais impossibilita que essa assinatura seja aprimorada. E isso, constatamos, é devido à amarração a uma determinada política de assinatura.

Neste trabalho, propomos um método para o aprimoramento dinâmico das assinaturas digitais, em termos de agregação de novos artefatos, visando garantir a preservação dos comprometimentos originalmente estabelecidos pelo signatário.

O método proposto permite que o processo de manutenção e proteção de uma assinatura digital fique explicitado em sua política de assinatura. O método baseou-se no uso de extensões dos padrões já estabelecidos de forma a garantir a compatibilidade com o que já existe. A característica adicionada à política de assinatura trouxe os seguintes benefícios:

- O assinante arca com uma menor preocupação ao produzir a assi-

natura, pois é esperado que este deva escolher num conjunto bem menor de possibilidades;

- Essa técnica vai evitar eventualmente a produção de assinaturas desnecessárias. Como o assinante deve escolher entre um conjunto menor de políticas é mais simples para o agente receptor da assinatura comunicar qual é a política correta evitando assim que o assinante acabe gerando uma assinatura que não será aceita devido o uso de uma política de assinatura incorreta;

- É possível a introdução de um outro agente especialista para mediar a atualização da assinatura, uma vez que se o assinante produziu uma assinatura que demonstra o comprometimento esperado ele pode delegar a responsabilidade de atualizar a assinatura para um terceiro.

6.1 TRABALHOS FUTUROS

Com a nossa proposta, é possível solucionar a questão de evolução da política de assinatura. Entretanto, alguns pontos relativos ao uso de políticas de assinatura ainda permanecem em aberto. Dentre esses pontos podemos citar os seguintes:

- A atualização para uma política que não existia quando a assinatura foi gerada não é possível mesmo com a técnica proposta. Essa funcionalidade é necessária em cenários onde se deseja efetuar o arquivamento da assinatura por longos períodos, por exemplo;

- A implicação da técnica proposta em cenários em que há mais de uma assinatura e estas tem relação entre si. Por exemplo, um documento é assinado por três agentes, sendo que um demonstra comprometimento com o documento e os outros dois se colocam como testemunhas. A atualização da política nas assinaturas não tratou de casos onde existem múltiplas assinaturas. Essa necessidade já havia sido levantada por Ardieta et. al. (65);

- Incluir na política de assinatura a possibilidade de partes do documento poderem ser alterados. Isso poderia ser muito útil para preservar a privacidade em documentos digitalmente assinados. Por exemplo, um documento da área médica poderia ser modificado para preservar a privacidade do nome do paciente. Já existem primitivas criptográficas que permitem a redação (70, 71)

ou sanitização (72–76) de documentos eletrônicos. Entretanto, ainda deve ser desenvolvido a metodologia e as regras para que essas primitivas possam ser aplicadas;

- A possibilidade de manter os vestígios que possibilitam provar a autenticidade de dados processados a partir de documentos eletrônicos assinados tem sido tratada recentemente na literatura especializada (77). A ideia é poder validar a assinatura de documentos que são resultados do processamento de documentos assinados. Nestes cenários, é necessário investigar como poderiam as políticas de assinatura digital preservadas e unificadas nos documentos processados;

- É possível que num cenário onde diferentes destinatários tenham requisitos de assinatura distintos. Deve-se investigar como poderiam ser produzidas as assinaturas e respectivas políticas de assinatura que atendam esses diferentes e possivelmentee, contraditórias requisitos;

- É necessário também investigar a preservação em longo prazo das políticas de assinatura. Na ocorrência, por exemplo, de que um ou mais primitivas criptográficas tenham que ser atualizadas, deve-se propor alternativas de como realizar a atualização das políticas, preservando a vontade original do signatário;

- A forma originalmente adotada para o PDF, impossibilita o uso pleno de políticas de assinatura. Conforme foi visto na Seção 2.8, está sendo desenvolvido o padrão PAdES que, em princípio, deveria prover formas de se trabalhar com políticas de assinatura. No entanto, até onde estudamos, o PADES possui uma série de deficiências que precisam ser devidamente tratatas. Como trabalho futuro, sugere-se redesenhar o PAdES, aos moldes do XAdES e CAdEs para que seja possível usar, em sua plenitude, políticas de assinatura.

- Notamos em nossos estudos que uma infraestrutura de chaves públicas é gerida por um documento de políticas, denominado de Políticas de Certificação (45, veja seção 6.1.2). Tal documento é materializado, para cada autoridade certificadora para um documento descrevendo como as políticas são implementadas para uma AC em particular. Tal documento é denominado de Declaração de Práticas de Certificação. Algumas regras de certificação

previstas na política de certificação podem ser instanciadas diretamente nos certificados digitais. A validação das políticas de certificação, onde cabível, é uma das tarefas que deve ser feita pelo verificador da assinatura, de forma a verificar se todas as ACs emissoras de certificados da cadeia de certificados, associada ao certificado digital do signatário, respeitam as regras definidas. Notamos que algumas regras de uma política de assinatura digital são as mesmas, ou muito semelhantes as regras de uma política de certificação. Como trabalho futuro, sugere-se investigar quais regras são comuns, de forma a propor uma forma de evitar a redundância, ou até mesmo a contradição de políticas.

REFERÊNCIAS

1 CRUELLAS, J. C. et al. *XML advanced electronic signatures (XAdES): W3C Note 20*. 2003.

2 ETSI. Especificação Técnica TS 119 132-1 v1.0.1, *Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures*. Sophia-Antipolis Cedex, France, 2015.

3 ETSI. Padrão Europeu EN 319 132-1 v1.1.1, *Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures*. Sophia-Antipolis Cedex, France, 2016.

4 ETSI. Relatório Técnico TR 102 038 v1.1.1, *TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies*. Sophia-Antipolis Cedex, France, 2002.

5 PAOLI, J. et al. Ecma-376 office open XML file formats. *URL http://www. ecmainternational. org/publications/standards/Ecma-376. htm*, 2006.

6 WEIR, R. Opendocument format: The standard for office documents. *IEEE Internet Computing*, IEEE, v. 13, n. 2, p. 83–87, 2009.

7 ISO. *Document management—Portable document format—Part 1: PDF 1.7*. Geneva, Switzerland, 2008.

8 PINKAS, D.; POPE, N.; ROSS, J. *CMS Advanced Electronic Signatures (CAdES)*. IETF, 2008. RFC 5126 (Informational). (Request for Comments, 5126). Disponível em: <http://www.ietf.org/rfc/rfc5126.txt>.

9 ETSI. Especificação Técnica TS 101 733 v2.2.1, *Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)*. Sophia-Antipolis Cedex, France, 2013.

10 ETSI. Padrão Europeu EN 319 122-1 v1.1.1, *Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures*. Sophia-Antipolis Cedex, France, 2016.

11 ETSI. Padrão Europeu EN 319 122-2 v1.1.1, *Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures*. Sophia-Antipolis Cedex, France, 2016.

12 ETSI. Especificação Técnica TS 102 778-1 v1.1.1, *Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES*. Sophia-Antipolis Cedex, France, 2009.

13 ETSI. Especificação Técnica TS 102 778-2 v1.2.1, *Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1*. Sophia-Antipolis Cedex, France, 2007.

14 ETSI. Especificação Técnica TS 102 778-3 v1.2.1, *Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles*. Sophia-Antipolis Cedex, France, 2010.

15 ETSI. Especificação Técnica TS 102 778-4 v1.1.2, *Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES LTV Profile*. Sophia-Antipolis Cedex, France, 2009.

16 ETSI. Especificação Técnica TS 102 778-5 v1.1.2, *Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures*. Sophia-Antipolis Cedex, France, 2009.

17 ETSI. Especificação Técnica TS 102 778-6 v1.1.1, *Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 6: Visual Representations of Electronic Signatures*. Sophia-Antipolis Cedex, France, 2010.

18 ROSS, J.; PINKAS, D.; POPE, N. *Electronic Signature Policies*. IETF, 2001. RFC 3125 (Experimental). (Request for Comments, 3125). Disponível em: <http://www.ietf.org/rfc/rfc3125.txt>.

19 HERNANDEZ-ARDIETA, J. L.; GONZALEZ-TABLAS, A. I.; ALVAREZ, B. R. An optimistic fair exchange protocol based on signature policies. *computers & security*, Elsevier, v. 27, n. 7, p. 309–322, 2008.

20 ICP-BRASIL. DOC-ICP 15-3, *Requisitos das Políticas de Assinatura Digital na ICP-Brasil - Versão 7.0*. Brasília, DF: [s.n.], 2015.

21 ETSI. Relatório Técnico TR 102 272 v1.1.1, *Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies*. Sophia-Antipolis Cedex, France, 2003.

22 FILLINGHAM, D. A comparison of digital and handwritten signatures. *Ethics and Law on the Electronic Frontier*, v. 6, 1997.

23 MASON, S. *Electronic signatures in law*. 4. ed. Londres: Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016. 418 p. ISBN 978-1-911507-01-7.

24 DIFFIE, W.; HELLMAN, M. New directions in cryptography. *IEEE Trans. Inf. Theor.*, IEEE Press, Piscataway, NJ, USA, v. 22, n. 6, p. 644–654, set. 2006. ISSN 0018-9448. Disponível em: <http://dx.doi.org/10.1109/TIT.1976.1055638>.

25 RAVI, S.; RAGHUNATHAN, A.; CHAKRADHAR, S. Tamper resistance mechanisms for secure embedded systems. In: IEEE. *VLSI Design, 2004. Proceedings. 17th International Conference on*. [S.l.], 2004. p. 605–611.

26 BRUGUIER, F. et al. Hardware security: From concept to application. In: IEEE. *Microelectronics Education (EWME), 2016 11th European Workshop on*. [S.l.], 2016. p. 1–6.

27 KOHNFELDER, L. M. *Towards a practical public-key cryptosystem*. Dissertação (B.S. Thesis) — Massachusetts Institute of Technology, 1978.

28 HOUSLEY, R.; POLK, T. *Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure*. 1st. ed. New York, NY, USA: John Wiley & Sons, Inc., 2001. 352 p. ISBN 0471397024.

29 ADAMS, C. et al. Which pki (public key infrastructure) is the right one?(panel session). In: ACM. *Proceedings of the 7th ACM conference on Computer and communications security*. [S.l.], 2000. p. 98–101.

30 ELLISON, C.; SCHNEIER, B. Ten risks of pki: What you're not being told about public key infrastructure. *Comput Secur J*, v. 16, n. 1, p. 1–7, 2000.

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

32 ADAMS, C.; JUST, M. Pki: Ten years later. In: CITESEER. *the 3rd Annual PKI R&D Workshop, NIST*. [S.l.], 2004. p. 255–270.

33 ARGYROUDIS, P.; MCADOO, R.; O'MAHONY, D. Comparing the costs of public key authentication infrastructures. In: *Proc. 1st Workshop on the Economics of Securing the Information Infrastructure (WESII'06)*. [S.l.: s.n.], 2006. p. 10.

34 OPPLIGER, R. Certification authorities under attack: A plea for certificate legitimation. *IEEE Internet Computing*, IEEE, v. 18, n. 1, p. 40–47, 2014.

35 WERLANG, F. C.; CUSTÓDIO, R. F.; VIGIL, M. A. G. A user-centric digital signature scheme. In: _____. *Public Key Infrastructures, Services and Applications: 10th European Workshop, EuroPKI 2013, Egham, UK, September 12-13, 2013, Revised Selected Papers*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014. p. 152–169. ISBN 978-3-642-53997-8. Disponível em: <http://dx.doi.org/10.1007/978-3-642-53997-8_10>.

36 GLADNEY, H. M. Trustworthy 100-year digital objects: Evidence after every witness is dead. *ACM Transactions on Information Systems (TOIS)*, ACM, v. 22, n. 3, p. 406–436, 2004.

37 STALLINGS, W. *Cryptography and network security: principles and practices*. 7. ed. Essex, Inglaterra: Pearson, 2016. 768 p. ISBN 0134444280.

38 RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, ACM, New York, NY, USA, v. 21, n. 2, p. 120–126, fev. 1978. ISSN 0001-0782. Disponível em: <http://doi.acm.org/10.1145/359340.359342>.

39 JOHNSON, D.; MENEZES, A.; VANSTONE, S. The elliptic curve digital signature algorithm (ecdsa). *Int. J. Inf. Secur.*, Springer-Verlag, Berlin, Heidelberg, v. 1, n. 1, p. 36–63, ago. 2001. ISSN 1615-5262. Disponível em: <http://dx.doi.org/10.1007/s102070100002>.

40 Internetional Telecomunication Union. Recommendation ITU-T X.509, *Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*. 2016.

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

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

43 International Telecomunication Union. Recommendation ITU-T X.690, *Information technology – ASN.1 encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*. 2015.

44 OLIVEIRA, M.; GARCIA, G. *ICP-Brasil e PBAD*. 2015.

45 COOPER, D. et al. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. IETF, 2008. RFC 5280 (Proposed Standard). (Request for Comments, 5280). Updated by RFC 6818. Disponível em: <http://www.ietf.org/rfc/rfc5280.txt>.

46 BARTEL, M. et al. *XML-Signature Syntax and Processing", W3C Recommendation xmldsig-core, October 2000*. 2008.

47 ICP-BRASIL. DOC-ICP 15, *Visão Geral Sobre Assinaturas Digitais na ICP-Brasil - Versão 3.0*. Brasília, DF, 2015.

48 ICP-BRASIL. DOC-ICP 15-1, *Requisitos Mínimos para Geração e Verificação de Assinaturas Digitais na ICP-Brasil – Versão 3.0*. Brasília, DF: [s.n.], 2015.

49 ICP-BRASIL. DOC-ICP 15-2, *Perfil de Uso Geral para Assinaturas Digitais na ICP-Brasil - Versão 3.0*. Brasília, DF: [s.n.], 2015.

50 CHOU, E. Y. Paperless and soulless e-signatures diminish the signer's presence and decrease acceptance. *Social Psychological and Personality Science*, SAGE Publications, v. 6, n. 3, p. 343–351, 2015.

51 ZALASIŃSKI, M.; CPAŁKA, K.; HAYASHI, Y. New fast algorithm for the dynamic signature verification using global features values. In: SPRINGER. *International Conference on Artificial Intelligence and Soft Computing*. [S.l.], 2015. p. 175–188.

52 ZULNARNAIN, Z. et al. Triangular geometric feature for offline signature verification. *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering*, v. 10, n. 3, p. 485–488, 2016.

53 GONÇALVES, R. P.; AUGUSTO, A. B.; CORREIA, M. E. Time/space based biometric handwritten signature verification. In: IEEE. *2015 10th Iberian Conference on Information Systems and Technologies (CISTI)*. [S.l.], 2015. p. 1–6.

54 GONÇALVES, R. M. P. Handwritten signature authentication using motion detection and qrcodes.

55 DOROZ, R.; PORWIK, P.; ORCZYK, T. Dynamic signature verification method based on association of features with similarity measures. *Neurocomputing*, Elsevier, v. 171, p. 921–931, 2016.

56 KAUR, M. R.; CHOUDHARY, M. P. Handwritten signature verification based on surf features using hmm. *International Journal of Computer Science Trends and Technology*, v. 3, p. 187–195, 2015.

57 International Telecomunication Union. Recommendation ITU-T X.680, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*. 2015.

58 GAO, S. et al. W3C XML schema definition language (XSD) 1.1 part 1: Structures. *W3C Candidate Recommendation*, v. 30, n. 7.2, 2009.

59 ETSI. Padrão Europeu EN 319 132-2 v1.1.1, *Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures*. Sophia-Antipolis Cedex, France, 2016.

60 ETSI. Especificação Técnica TS 102 045 v1.1.1, *Signature Policy for Extended Business Model*. Sophia-Antipolis Cedex, France, 2003.

61 ETSI. Relatório Técnico TR 119 100 v1.1.1, *Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for signature creation and validation*. Sophia-Antipolis Cedex, France, 2016.

62 BOYER, J. *Canonical XML Version 1.0 W3C:Recommendation 15 March 2001*. 2001.

63 BARKER, E. NIST Special Publication 800-57 Part 1 Revision 4, *Recommendation for Key Management–Part 1: General*. Gaithersburg, MD, 2016.

64 EPC. EPC342-08 versão 5.0, *Guidelines on cryptography algorithms usage and key manangement*. Cours Saint-Michel 30A – B 1040, Brussels, Bélgica, 2016.

65 HERNANDEZ-ARDIETA, J. L. et al. Extended electronic signature policies. In: *Proceedings of the 2nd International Conference on Security of Information and Networks*. New York, NY, USA: ACM, 2009. (SIN '09), p. 268–277. ISBN 978-1-60558-412-6. Disponível em: <http://doi.acm.org/10.1145/1626195.1626261>.

66 MELLO, M. D.; DHALLA, M. A. *Digital signing policy*. [S.l.]: Google Patents, 2013. US Patent 8,560,853.

67 BOWE, J. et al. *Server-side digital signature system*. [S.l.]: Google Patents, 2001. US Patent App. 09/840,472.

68 ETSI. Especificação Técnica TS 101 903 v1.4.2, *Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signature (XAdES)*. Sophia-Antipolis Cedex, France, 2010.

69 OLIVEIRA, M. Trabalho de Conclusão de Curso, *Modelagem de um Software Orientado à Componentes para Assinatura Digital*. 2012.

70 LIM, S.; LEE, H.-S. A short and efficient redactable signature based on rsa. *ETRI Journal*, Electronics and Telecommunications Research Institute, v. 33, n. 4, p. 621–628, 2011.

71 BRZUSKA, C. et al. Redactable signatures for tree-structured data: definitions and constructions. In: SPRINGER. *International Conference on Applied Cryptography and Network Security*. [S.l.], 2010. p. 87–104.

72 ATENIESE, G. et al. Sanitizable signatures. In: SPRINGER. *European Symposium on Research in Computer Security*. [S.l.], 2005. p. 159–177.

73 BRZUSKA, C. et al. Santizable signatures: How to partially delegate control for authenticated data. In: *BIOSIG 2009 - Proceedings*

of the Special Interest Group on Biometrics and Electronic Signatures. Darmstadt, Germany: GI, 2009. (LNI, v. 155), p. 117–128.

74 BRZUSKA, C. et al. Unlinkability of sanitizable signatures. In: SPRINGER. *International Workshop on Public Key Cryptography*. [S.l.], 2010. p. 444–461.

75 CANARD, S.; JAMBERT, A.; LESCUYER, R. Sanitizable signatures with several signers and sanitizers. In: SPRINGER. *International Conference on Cryptology in Africa*. [S.l.], 2012. p. 35–52.

76 FLEISCHHACKER, N. et al. Efficient unlinkable sanitizable signatures from signatures with re-randomizable keys. In: *Public-Key Cryptography–PKC 2016*. [S.l.]: Springer, 2016. p. 301–330.

77 AHN, J. H. et al. Computing on authenticated data. *Journal of Cryptology*, Springer, v. 28, n. 2, p. 351–395, 2015.