UNIVERSIDADE DE SÃO PAULO

ESCOLA POLITÉCNICA

MURILO RIVAU FERNANDES

SIPEX: Uma proposta de modelo de política de assinatura

São Paulo

2006

MURILO RIVAU FERNANDES

SIPEX: Uma proposta de modelo de política de assinatura

Dissertação apresentada a Escola Politécnica da
Universidade de São Paulo para obtenção do título de
Mestre em Engenharia Elétrica

Área de Concentração: Sistemas Eletrônicos
Orientador: Prof. Dr. João Antônio Zuffo

São Paulo

2006

Este exemplar foi revisado e alterado em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, 15 de dezembro de 2006.

Assinatura do autor _____

Assinatura do orientador _____

FICHA CATALOGRÁFICA

Rivau Fernandes, Murilo
SIPEX: Uma proposta de modelo de política de assinatura / M. Rivau Fernandes. -- ed.rev. -- São Paulo, 2006.
105 p.

Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.

1.Sistemas de informação (Segurança) 2. Documentos eletrônicos 3. Contrato eletrônico I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Sistemas Eletrônicos II.t.

DEDICATÓRIA

Ao meu pai José Marcos (em memória), à minha mãe Roseli e aos meus irmãos Heitor e Adriana.

AGRADECIMENTOS

Ao meu orientador, Prof. Dr. João Antônio Zuffo, por seu conhecimento, pela oportunidade dada, pela paciência e pelo incentivo.

Ao Doutor Volnys Borges Bernal, pela experiência, amizade e confiança depositada.

Aos amigos do Grupo NSRAV, pela ajuda e apoio em todos os momentos.

À Escola Politécnica da Universidade de São Paulo e ao Laboratório de Sistemas Integráveis por colocar a disposição sua infra-estrutura.

Ao Deus da minha vida, rocha eterna e minha salvação, acima de todas as coisas.

RESUMO

FERNANDES, M. R. **SIPEX: Uma proposta de modelo de política de assinatura**. 2006. 105 f. Dissertação (Mestrado em Engenharia Elétrica) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2006.

O processo conhecido como assinatura digital possui as características necessárias para prover autenticação, integridade e não repúdio de geração de documentos eletrônicos. No entanto, os requisitos que determinam a validade de uma assinatura digital podem variar de acordo com o contexto de negócio envolvido. Estes requisitos podem ser formalizados em um documento de políticas chamado de política de assinatura. Uma política de assinatura consiste em um conjunto de regras que determinam a validade de uma assinatura digital em um contexto legal ou de negócio. O Instituto Europeu de Padrões de Telecomunicações (ETSI) propôs um modelo de política de assinatura associado à validação de uma assinatura digital independente das outras assinaturas digitais existentes no documento. Porém, documentos com mais de uma assinatura podem apresentar requisitos de relacionamento entre si como, por exemplo, ordem de geração das assinaturas. Além disso, o emissor de uma política de assinatura deve assegurar sua integridade e autenticidade. A proposta do trabalho consiste na avaliação do modelo de política de assinatura proposto pelo ETSI e apresentar uma extensão deste modelo para contemplar o relacionamento entre as assinaturas de um documento e a autenticação da política de assinatura antes de ser utilizada para gerar ou verificar uma assinatura digital.

ABSTRACT

The process known as digital signature has the characteristics necessary to provide authentication, integrity and non repudiation of electronic documents. However, the requirements to determine the validity of a digital signature can vary the context of involved business in accordance with. These requirements can be written in a document of policies called signature policy. A signature policy consists of a set of rules to determine the validity of a digital signature in a legal or business context. The European Telecommunications Standards Institute (ETSI) presented the model of policies of signature associated with the validation of an individual signature. Documents with more than one signature can present requirements of relationship between the signatures as, for example, the order to generation of the signatures. Moreover, the issuer of the signature policies must assure its integrity and authenticity. The proposal of the work consists of the evaluation of the model of signature policy considered for the ETSI and to present an extension of this model to contemplate the relationship between the signatures of a document and the authentication of the signature policy.

SUMÁRIO

SUMÁRIO ..... **III**
LISTA DE FIGURAS ..... **V**
LISTA DE ABREVIATURAS ..... **VII**
1. INTRODUÇÃO **1**
1.1. Motivação 2
1.2. Objetivo 3
1.3. Trabalhos relacionados 4
1.4. Estrutura da dissertação 5
2. CONTRATOS **6**
2.1. Definição de contratos 6
2.1.1. Elementos para existência do contrato 7
2.2. O contrato eletrônico 8
2.3. Força probante de documentos 9
2.4. Exemplo de contrato 10
3. ASSINATURA MANUSCRITA VERSUS ASSINATURA ELETRÔNICA **12**
3.1. Assinatura manuscrita 12
3.1.1. Características da assinatura manuscrita 13
3.1.2. Propósitos de uma assinatura manuscrita 15
3.2. Assinatura eletrônica 17
3.2.1. Características da assinatura digital 19
3.2.2. Tipos de Propósitos 22
3.3. Diferenças entre Assinatura Digital e Assinatura Manuscrita 23
4. INFRA-ESTRUTURA DE CHAVES PÚBLICAS **26**
4.1. Cadeia de certificação 27
4.2. Política de Certificação Digital 27
4.3. Certificado Digital 28
4.4. Revogação do certificado digital 30
4.4.1. Lista de Certificados Revogados 31
4.4.2. Protocolo OCSP 33
4.5. Considerações Finais 33
5. ASSINATURA DIGITAL **35**
5.1. Geração da assinatura digital 35
5.2. Verificação da assinatura 37
5.2.1. Validade da assinatura digital 39
5.3. Invólucro de documento e assinatura 40
5.4. Formatos de invólucro de assinatura digital 42
5.5. Co-assinatura e contra-assinatura 44
5.6. Problema da verificação da validade do certificado 44
5.6.1. Carimbo de tempo 45
5.7. Considerações finais 47
6. POLÍTICA DE ASSINATURA DIGITAL **48**
6.1. Representação da política de assinatura 49
6.2. Atributos de uma política de assinatura 51
6.2.1. Geração e verificação da assinatura 57

6.2.2. Condições de confiança para o certificado do signatário 58
6.2.3. Condições de confiança para o carimbo de tempo 59
6.2.4. Condições de confiança para o certificado de atributo 60
6.2.5. Condições para algoritmos e tamanhos de chaves 61
6.3. Processo de uso da política de assinatura 61

7. PROPOSTA PARA POLÍTICA DE ASSINATURA 63
7.1. Extensão para relacionamento entre assinaturas 63
7.1.1. Proposta do modelo de política de relacionamento entre assinaturas 69
7.1.1.1. Atributo ordem de geração 70
7.1.1.2. Atributo vínculo temporal 72
7.2. Autenticação da política de assinatura 74
7.2.1. Ciclo de vida da política de assinatura autenticada 75

8. ESTUDO DE CASO 77
8.1. Política de assinatura para citação judicial 77
8.1.1. Propósito das assinaturas no mandado de citação 79
8.1.2. Política de assinatura para o mandado de citação eletrônico 80
8.2. Política de assinatura para contratos de câmbio 82

9. CONCLUSÃO 85
9.1. Trabalhos futuros 86

REFERÊNCIAS BIBLIOGRÁFICAS 87

APÊNDICE A – IMPLEMENTAÇÃO 92
Módulos do protótipo 92
Resultados 93

LISTA DE FIGURAS

Figura 1 - Contrato de prestação de serviço (adaptado de MILHOMENS; ALVES, 2006). ...11

Figura 2 - Assinatura digital como subclasse da assinatura eletrônica.....18

Figura 3 - Cadeia de certificação baseada no modelo hierárquico. 27

Figura 4 - Estrutura do certificado digital (Extraído de ARREBOLA, 2006).....28

Figura 5 - Uso permitido do certificado (Adaptado de BERNAL, 2005) 30

Figura 6 - Campos da LCR (Adaptado de ADAMS; LLOYD, 99).....31

Figura 7 - Período de tolerância (Adaptado de ETSI, 2003b). 32

Figura 8 - Processo de Geração da Assinatura Digital 37

Figura 9 - Processo de verificação da assinatura digital.....38

Figura 10 - Invólucro de documento e assinatura com documento incluído.....41

Figura 11 - Objetos do formato PKCS#7/CMS.....43

Figura 12 - Geração de assinatura com instante falso (Adaptado de BERNAL, 2005). 46

Figura 13 - Geração de assinatura com carimbo de tempo (Adaptado de BERNAL, 2005)....46

Figura 14 - Trecho da estrutura de política de assinatura em ASN.1. 50

Figura 15 - Atributos de uma política de assinatura. 51

Figura 16 - Política de assinatura e o atributo informações da política de assinatura. 53

Figura 17 - Política de assinatura e o atributo política de validação de assinatura. 54

Figura 18 - Política de assinatura e o atributo regras comuns. 56

Figura 19 - Conteúdo do atributo regra para propósito específico. 57

Figura 20 - Ordem de geração das assinaturas baseado em propósito de assinatura.....66

Figura 21 - Ordem de geração das assinaturas baseado em papéis e propósitos de assinatura 67

Figura 22 - Encapsulamento do atributo regras de relacionamento. 70

Figura 23 - Dependência de ordem entre as classes de signatários 71

Figura 24 - Conteúdo do atributo regras de relacionamento. 73

Figura 25 - Atributo assinatura da política. 75

Figura 26 - Diagrama de seqüência do mandado de citação 79

Figura 27 - Dependência de ordem entre as classes de signatários do mandado de citação 82

Figura 28 - Dependência de ordem entre as classes de signatários do contrato de câmbio. 84

LISTA DE ABREVIATURAS

AC	Autoridade Certificadora
AR	Autoridade de Registro
ASN.1	*Abstract Syntax Notation 1*
CA	Certificado de Atributos
HTTP	*Hypertext Transfer Protocol*
ICP	Infra-estrutura de Chaves Públicas
ITU-T	*International Telecommunications Union, Telecommunication Standardization Sector*
LCR	Lista de Certificados Revogados
SSL	*Secure Sockets Layer*
TLS	*Transport Layer Security*
XML	*eXtensible Markup Language*

1. INTRODUÇÃO

A atual tecnologia de assinatura digital já confere as propriedades suficientes para prover autenticação, integridade e irretratabilidade a documentos eletrônicos. No entanto, cada contexto específico de assinatura de documentos implica invariavelmente em um conjunto diferente de requisitos, tanto de negócio quanto tecnológicos, que determinam como as assinaturas devem ser agregadas ao documento, e posteriormente validadas, para que sirva adequadamente aos propósitos do negócio e tenham sua plena validade legal.

Como exemplo de requisitos pode-se citar a quantidade de assinaturas necessárias e a ordem em que as assinaturas devem ser apostas ao documento. Outros requisitos, que se aplicam exclusivamente aos documentos eletrônicos, dizem respeito, por exemplo, às regras para validação do estado de revogação, à necessidade ou não de carimbo de tempo, ao tamanho das chaves e algoritmos utilizados, etc.

Para prover clareza e pleno conhecimento das partes envolvidas, os requisitos são expressos em um documento denominado política de assinatura.

Essa documentação, nem sempre encontrada nos processos manuscritos, traz um imenso benefício, já que formaliza, de forma inequívoca, as condições em que um documento e suas assinaturas são consideradas válidas, tanto no momento da aposição das assinaturas quanto em uma verificação futura. Além disso, a utilização dos recursos da política de assinatura propicia maior flexibilidade, controle e segurança aos sistemas de gerenciamento e fluxo de documentos, já que permite, de uma forma padronizada, atender diferentes contextos de negócios.

O Instituto Europeu de Padrões de Telecomunicações (ETSI) e o *The Internet Engineering Task Force* (IETF) têm trabalhando em conjunto na definição de um modelo de política de assinatura. A proposta divulgada pelo ETSI (2003a) (2003b) é bastante completa

na abordagem dos requisitos exclusivos aos documentos eletrônicos. No entanto, o modelo de política do ETSI não apresenta elementos necessários para atender os requisitos de relacionamento entre as assinaturas. Além disso, o modelo também não contempla uma forma de prover a autoria de uma política de assinatura. O relacionamento entre assinaturas, dependendo do contexto, pode ser um requisito legal ou do negócio. A proposta deste trabalho estende o modelo de política para contemplar estes requisitos.

Essa complementação permite fazer com que a política de assinatura se torne mais aderente aos processos reais e, dessa forma, mais útil e relevante.

1.1. MOTIVAÇÃO

No cenário mundial, é crescente a adoção de assinatura digital em documentos eletrônicos tendo em vista a abundância de recursos de geração, armazenamento e transmissão de conteúdo digital, e os inegáveis ganhos de eficiência e redução de custos inerentes aos processos de gerenciamento eletrônico de documentos.

O Brasil, especificamente, já possui legislação pertinente à regulamentação da validade jurídica da assinatura digital em documento eletrônico. Esse fato cria incontáveis possibilidades de migração de processos manuais, que exigem assinaturas manuscritas, em processos completamente eletrônicos.

Somente para citar alguns exemplos, o mercado financeiro já celebra, desde 2004, contratos de câmbio assinados digitalmente. A Secretaria da Receita Federal já disponibiliza diversos serviços exclusivos aos contribuintes, tanto pessoa física como jurídica, que envolvem a assinatura digital, incluindo a declaração do imposto de renda. Em conjunto com

os governos estaduais, já sinalizou que os livros fiscais e contábeis serão assinados digitalmente pelas empresas e contadores, além do revolucionário processo de nota fiscal eletrônica, já em processo de piloto em vários estados, no qual todas as notas modelo “1” e “1A" serão assinadas digitalmente.

Dado que a demanda e expectativa de uso por parte do mercado são muito grandes, justificam-se a estruturação e evolução de todos os processos, padrões e tecnologia envolvendo o assunto. Nesse cenário se encaixa a grande motivação deste trabalho: contribuir para que os processos que envolvam assinatura digital de documentos eletrônicos se tornem mais claros, seguros e eficientes, promovendo o uso consciente da um recurso tão crítico quanto uma assinatura digital.

1.2. OBJETIVO

O objetivo principal deste trabalho é propor um modelo de política de assinatura digital de documentos eletrônicos – o SIPEX (*Signature Policy Extensions*). O SIPEX consiste na especificação de um modelo que estende o modelo proposto pelo ETSI para contemplar o relacionamento entre múltiplas assinaturas de um mesmo documento eletrônico, tratando os requisitos de quantidade de assinaturas, ordem de aposição das assinaturas e limites de tempo para aposição das assinaturas.

Como objetivos secundários o trabalho apresenta o desenvolvimento de um entendimento legal e tecnológico do cenário de assinaturas e documentos, a avaliação do modelo de política de assinatura proposto pelo ETSI e a aplicação do SIPEX em casos práticos que demonstrem a relevância das contribuições.

1.3. TRABALHOS RELACIONADOS

O *European Telecommunications Standards Institute* (ETSI) é um instituto independente, sem fins lucrativos, cuja responsabilidade é elaborar padrões de tecnologia da informação e telecomunicação para a comunidade européia. Seus objetivos são oficialmente reconhecidos pela Comissão Européia e pela "European Fair Trade Association" (EFTA – Associação Européia de Comércio). A proposta do ETSI estabeleceu uma estrutura padrão para o uso de assinaturas eletrônicas. Esta iniciativa conta com um conjunto de documentos que apresentam formatos de assinatura digital que visam complementar os atuais formatos de assinatura digital.

Em relação às especificações sobre assinatura digitais, o objetivo do ETSI é estabelecer uma padronização que permita a implementação de sistemas para assinaturas digitais que incorporem recursos para a sua verificação com segurança por longos períodos de tempo e guarde evidências de sua validade mesmo que o signatário ou o verificador tente negá-la mais tarde. Além disso, a proposta do ETSI apresenta o modelo de política de assinaturas que será discutido neste trabalho.

O trabalho de Leung e Hui (2000) apresenta a necessidade de explicitar o propósito de assinaturas para gerenciamento de sistemas de *workflow* e apresenta um conjunto de propósitos de assinatura. O propósito de assinatura é um elemento significativo para o modelo de política de assinaturas porque relaciona os requisitos técnicos necessários para realização da assinatura com o tipo de propósito.

Outros dois trabalhos (BERBECARU, 2004) e (SCHEIBELHOFER, 2001) também mencionam o modelo de política de assinaturas apresentado pelo ETSI, porém com enfoques

distintos deste trabalho. Enquanto o primeiro trata de formatos eletrônicos para assinatura digital, o segundo aborda um estudo sobre visualização segura de documentos. Assim, a proposta mais atual para o modelo de política de assinatura é apresentada pelo ETSI.

1.4. ESTRUTURA DA DISSERTAÇÃO

No capítulo 2 é apresentado o desenvolvimento de um entendimento legal sobre assinaturas e seu uso em documentos, dentre os quais os contratos se destacam por apresentarem uma diversificada gama de requisitos. O capítulo 3 desenvolve uma análise das características e implicações da assinatura manuscrita comparada com a assinatura digital.

Os capítulos 4 e 5 descrevem os conceitos da tecnologia que envolve a questão da assinatura digital. No capítulo 6 são apresentados o conceito de política de assinatura e o modelo proposto pelo ETSI.

O capítulo 7 descreve a proposta deste trabalho, detalhando as características e aplicações do SIPEX.

O capítulo 8 desenvolve dois estudos de caso utilizando o modelo proposto neste trabalho para demonstrar a relevância e aplicabilidade das contribuições. Por fim, o capítulo 9 apresenta as conclusões e os possíveis trabalhos futuros relacionados.

2. CONTRATOS

A assinatura pode ser utilizada para diversas finalidades. Uma das principais finalidades é a assinatura de contratos. Este capítulo faz uma breve apresentação sobre as principais características dos contratos e de que forma essas características são retratadas no formato eletrônico, quanto à sua eficácia jurídica e força probante. Não é objeto de estudo deste trabalho as necessidades relacionadas à adequação da legislação para questões inerentes à tecnologia.

2.1. DEFINIÇÃO DE CONTRATOS

Dentro da órbita jurídica, os fatos originados pela vontade humana, desde que lícitos e que tenham por fim imediato adquirir, resguardar, transferir, modificar ou extinguir direito são denominados atos jurídicos (MILHOMENS; ALVES, 2000). Neste gênero tem-se a definição de contrato: um contrato representa a vontade de duas ou mais pessoas.

O contrato possui diversas classificações. No que se refere a esse estudo, uma das classificações mais pertinentes é quanto à obrigatoriedade que está relacionada com o ato de assinar contrato. Esta classificação define dois tipos de contratos: os contratos unilaterais e os

contratos bilaterais. Em um contrato de compra e venda, por exemplo, uma das partes recebe o bem em troca de um valor financeiro. Este tipo de contrato dá o sentido de obrigatoriedade[1] entre as partes envolvidas e recebe a classificação de contrato bilateral. Já um contrato de doação de um bem, por exemplo, expressa a vontade das partes envolvidas, porém não é oneroso para uma das partes. No caso do exemplo, não existe nenhum tipo de obrigação para a parte aceitante. Este tipo de contrato recebe a classificação de contrato unilateral.

2.1.1. Elementos para existência do contrato

Segundo o artigo 104 do Código Civil Brasileiro, a validade de um contrato requer, enquanto negócio jurídico, agente capaz, objeto lícito e forma prescrita ou não defesa em lei. O agente é aquele que realiza o negócio jurídico, sendo exigida a capacidade civil que ocorre aos 18 anos completos[2]. O objeto é aquilo que se pretende realizar por meio do contrato, por exemplo, o objeto do contrato de locação é a locação. Quanto à licitude do objeto, significa que não haverá amparo legal para contratos que tenham como finalidade algo ilegal. Por fim, a forma prescrita significa que a forma de efetivação será de acordo com a determinação da lei sempre que esta existir, ou não contrária à lei, caso não haja previsão legal.

---

[1] Obrigação é um vínculo de direito pelo qual alguém pode ser constrangido a dar, fazer ou não fazer alguma coisa (MILHOMENS; ALVES, 2000 p. 3).

[2] O artigo 5º do Código Civil regula a capacidade civil da pessoa humana. O parágrafo único deste artigo, por seus incisos, prevê outras possibilidades de aquisição de capacidade, que não faz parte do escopo deste trabalho.

2.2. O CONTRATO ELETRÔNICO

O termo “documento” tem sua origem no latim “documentu” cujo significado mais genérico é a representação de um fato. De acordo com (MARCACINI, 2002), a maior parte das interpretações, na acepção jurídica da palavra, referem-se ao termo como a materialização de um fato em um meio tangível. Esta definição tradicional é aceitável considerando que a forma utilizada para registrar os fatos sempre se deu apegada a algo material. No entanto, segundo o autor, este conceito necessita ser expandido em função da evolução tecnológica no tocante ao modo pelo qual é possível registrar fatos em meios intangíveis. Para ele, o documento deve ser a representação do pensamento ou fato que se deseja perpetuar e não a coisa em que estes se materializam. Isso é justificável partindo do principio que um documento eletrônico consiste, tecnicamente, em uma seqüência de bits organizada segundo um determinado formato. Assim, independente do meio onde esteja armazenada esta seqüência, trata-se do mesmo documento.

Segundo CASTRO (2003, p. 6) “o documento eletrônico pode ser entendido como a representação de um fato concretizada por meio de um computador e armazenado em formato específico (organização singular de seqüência de bits), capaz de ser traduzido ou apreendido pelos sentidos mediante o emprego de programa (*software*) apropriado”. Pela definição apresentada, o contrato eletrônico não cria outro tipo de contrato senão aquele que é realizado através de um meio eletrônico. Na realidade continua sendo um contrato de compra e venda, locação ou escambo, por exemplo. A diferença reside na forma de materialização deste

contrato, ou seja, o documento eletrônico representa mais um meio, dentre outros, da representação de fatos [3] e vontades na órbita jurídica, as quais implicam em obrigações.

A título de distinção entre o formato tradicional e eletrônico, aquele continua a ser definido como a representação de um fato materializado em meio físico e a ele inseparavelmente ligado (MARCACINI, 2002). O formato eletrônico trata a representação do fato não como coisa, mas como uma seqüência de bits cuja inteligibilidade é obtida pela tradução através de um programa de computador.

2.3. FORÇA PROBANTE DE DOCUMENTOS

Uma questão importante e de relevância no tocante aos documentos eletrônicos é a sua validade quanto à sua autenticação e integridade (MARCACINI, 2002). Isto ocorre porque é possível alterar documentos digitais sem deixar vestígios. Para que seja atribuído um cunho de força probante ao documento tradicional ou eletrônico, é necessário que o documento possua características que tornem possíveis a identificação do signatário e a certeza de sua não modificação, ou indícios de tal.

Em documentos impressos em papel, a força probante é atestada normalmente por

---

[3] "Nos fatos jurídicos predomina a força da natureza; nos atos jurídicos, a vontade. Os atos jurídicos são fatos jurídicos mas a recíproca não é verdadeira. Os primeiros, atos jurídicos, são fatos jurídicos voluntários; são ações humanas que os produzem" (MILHOMENS; ALVES, 2000. p. 3).

meio da assinatura de próprio punho, utilização de selos e autenticações notariais, o uso de papéis timbrados ou com marcas d'água, entre outros.

Em documentos eletrônicos, a principal forma de atestação da força probante se dá por meio do uso de técnicas e algoritmos de criptografia combinadas com um conjunto de recursos e processos, como por exemplo, de uma infra-estrutura de chaves públicas, que serão detalhadas neste trabalho.

2.4. EXEMPLO DE CONTRATO

Um contrato não possui um formato específico, exceto quando é exigido por lei. No entanto, existem alguns modelos mais utilizados de acordo com o tipo de negócio. A Figura 1 a seguir ilustra um exemplo de contrato de prestação de serviços. Nele, é possível observar algumas características comuns em contratos como o objeto, as partes envolvidas, valores, prazo de entrega e a localidade onde é definido o foro para questões jurídicas. Como observado no exemplo, as partes envolvidas no negócio apõem as respectivas assinaturas representando um comprometimento com os termos definidos no texto do contrato. Além desta assinatura, o contrato também apresenta a necessidade da assinatura de testemunhas. Este tipo de assinatura, conforme será detalhado no próximo capítulo, não representa um propósito compromissivo com o contrato, ou seja, está relacionada com ato das assinaturas das partes e não com os termos do contrato.

CONTRATO DE PRESTAÇAO DE SERVIÇOS

.....que entre si fazem.....
empresa sediada à....(endereço).....
-cidade/SP, inscrita no CNPJ sob o nº.....
doravante denominada CONTRATANTE,.....
portador(a) do RG.....CPF.....
residente à.....,doravante denominado CONTRATADO:

Cláusula Primeira – Objeto
O presente contrato tem por objetivo e prestação de serviços profissionais de consultoria a ser desenvolvido de acordo com as especificações constantes deste contrato.

Cláusula Segunda: Prestação de Serviços
O CONTRATADO deverá, durante a vigência deste contrato e, em contrapartida do pagamento especificado na Cláusula Terceira, atender as solicitações de consultoria e assessoria da CONTRATANTE, compreendendo no que couber, os seguintes serviços:
....., em particular para o cliente da CONTRATANTE.

Cláusula Terceira: Remuneração dos Serviços
Pela prestação dos serviços indicados na Cláusula Segunda, o CONTRATADO será remunerado, conforme condições especificadas a seguir:
a) o valor mensal básico estipulado é de R$.....

Cláusula Quarta: Prazo
O prazo deste contrato é de....., podendo ser adiado a qualquer momento ou ser renovado por igual período.

Cláusula Quinta: Condições Gerais
1. O CONTRATADO prestará serviços à CONTRATANTE com ampla, total, irrestrita autonomia, sem qualquer tipo de subordinação jurídica.
2. Para o livre desempenho das tarefas, deverão ser dadas ao CONTRATADO as condições necessárias, sem as quais não se responsabilizará pela fiel execução dos serviços.
3. As despesas de viagens, estadas e alimentação, quando autorizadas e, que se tornarem necessárias por força do desempenho dos serviços contratados, correrão por conta da CONTRATANTE.
4. O CONTRATADO cumprirá rigorosamente seus deveres de observância de sigilo e da ética profissional, fazendo as recomendações oportunas e desenvolvendo todos os demais atos e funções, necessárias ou convenientes ao bom cumprimento das atribuições contratadas.

Cláusula sexta: Rescisão
1. Este contrato poderá ser rescindido por quaisquer uma das partes, desde que a outra parte seja cientificada, por escrito, com antecedência mínima de 10(dez) dias.
2. Ocorrendo a rescisão de contrato pura e simplesmente, ou seja, sem nenhuma infração legal das partes envolvidas, será pago a cada uma das mesmas, conforme o caso, a seguinte verba rescisória:
a) por parte do CONTRATADO: metade da remuneração mensal devida até o momento (dia útil) da rescisão
b) por parte da CONTRATANTE: o valor da remuneração mensal devida até o momento (dia útil) da rescisão.

Cláusula Sétima: Fôro
As partes elegem o fôro da cidade de São Paulo para dirimir quaisquer litígios oriundos do presente instrumento, com expressa renúncia a qualquer outro, por mais privilegiado que se apresente.
Justas e contratadas, firmam o presente em 2 (duas) vias de igual teor e forma.

São Paulo, ...

_____	_____
CONTRATANTE	CONTRATADO
Testemunhas:	
Nome:	Nome:
CPF:	CPF:

Figura 1 - Contrato de prestação de serviço (adaptado de MILHOMENS; ALVES, 2006).

3. ASSINATURA MANUSCRITA VERSUS ASSINATURA ELETRÔNICA

Os processos de assinatura utilizados tradicionalmente envolvem principalmente a assinatura manuscrita. Porém, esta não é aplicável em documentos eletrônicos. Este capítulo trata a respeito dos diferentes tipos de propósitos por parte do signatário quando realiza uma assinatura e compara a assinatura manuscrita com a assinatura eletrônica, ressaltando suas similaridades e diferenças.

3.1. ASSINATURA MANUSCRITA

No capítulo 2 foi apresentado o conceito de contratos e a assinatura como recurso para que o instrumento tenha força probante. Este capítulo irá tratar da assinatura de uma forma mais genérica, aposta a diversos tipos de documentos, como contratos, laudos, imagens, relatórios, documentos jurídicos, documentos específicos, etc.

Assinar um documento tem o sentido genérico de apor-lhe um sinal, marca ou símbolo pessoal com o fim de dar-lhe autenticidade[4] (MARCACINI, 2002). Assim, o autor de uma assinatura atesta sua identidade pessoal, vincula o documento e assume algum tipo de

[4] O termo autenticidade, aqui citado, refere-se a identificação do signatário.

compromisso sobre os termos expressos no documento, como será detalhado na seção 3.1.2.

3.1.1. Características da assinatura manuscrita

De acordo com (ZHOU, 2000), a assinatura manuscrita deve apresentar as seguintes características:

- **Dificuldade de reprodução por terceiros**. A assinatura deve ser difícil de ser forjada por uma outra entidade. No caso da assinatura manuscrita, considera-se que o ato da inscrição dos sinais gráficos que representam uma assinatura é de propriedade particular do signatário e o grau de complexidade de sua reprodução por outra entidade é elevado. Mesmo assim, existe a possibilidade de falsificação da assinatura. Em caso de suspeita de falsificação, o documento é encaminhado para um exame de perícia denominado exame grafotécnico, o qual permite identificar a assinatura com elevado nível de precisão;
- **Facilidade de verificação**. A assinatura deve ser de fácil verificação por uma terceira entidade. No caso da assinatura manuscrita, a técnica tradicional de verificação é baseada na inspeção visual. No entanto, esta verificação não é trivial de ser realizada por pessoas leigas e, também, pode não ser uma tarefa trivial verificar assinaturas de pessoas que não costumam manter um determinado padrão no momento de sua realização. Em função disso, e também da possibilidade de falsificação, em alguns casos costuma-se exigir o reconhecimento de firma por um notário. A titularidade da assinatura poderá ser reconhecida por autenticação, mediante sua realização na presença do notário, ou por semelhança, pela comparação com assinaturas previamente realizadas;

- **Não-reutilização**. A assinatura realizada em um documento não pode ser reutilizada em outro documento. A marca da assinatura manuscrita deixada em um documento está fortemente vinculada a este. Ela não pode ser "retirada" e "colada" em um outro documento: a marca não pode ser transferida para outro documento sem que as propriedades físicas do documento sejam comprometidas;

- **Inalterabilidade do documento**. Deve ser possível identificar a violação de integridade do documento. No caso da assinatura manuscrita, o documento assinado é considerado íntegro quando as propriedades físicas do papel permanecem originais. Considera-se neste caso as propriedades físicas do papel quanto à rasura ou vestígios de alteração da escrita do texto ou da própria assinatura. Observa-se que a assinatura manuscrita por si mesma não é capaz de prover a integridade do documento. A característica de integridade está associada à assinatura porque define o instante que poderá ser verificada a integridade do documento. Além disso, nota-se neste quesito uma limitação para documentos com mais de uma página. Normalmente a assinatura é realizada ao final do documento. Neste caso, recomenda-se a existência de um identificador, a numeração e a assinatura (ou rubrica) de todas as páginas do documento;

- **Irretratabilidade da geração**. Não deve ser possível ao signatário de um documento repudiar a geração da assinatura. Na assinatura manuscrita, supõe-se que a inscrição dos sinais gráficos que representam a assinatura seja de difícil geração por uma terceira entidade (falsificação) fazendo com que o signatário não possa repudiar a realização da assinatura.

3.1.2. Propósitos de uma assinatura manuscrita

Além das propriedades mencionadas, a realização de uma assinatura manuscrita pode assumir diferentes tipos de propósitos e conseqüentemente diferentes implicações. O propósito geralmente está associado ao uso comum dado àquela classe de documento ou explícito nos termos do documento assinado. Exemplos de propósitos decorrentes da realização de uma assinatura manuscrita são (ETSI, 2003a):

- **Compromissivo**[5]. Quando a assinatura tem o propósito de estabelecer o compromisso legal do signatário com os termos expressos no documento gerando obrigações sobre o objeto;
- **Ciente**. Quando a assinatura, algumas vezes chamada de rubrica ou visto, tem o propósito de informar que o signatário tomou conhecimento quanto ao conteúdo expresso em um documento;
- **Autoral**. Quando a assinatura tem o propósito de indicar que o signatário é o autor do documento, sem necessariamente assumir compromisso com os termos do documento.
- **Responsável**. Quando a assinatura tem o propósito de indicar que o signatário, embora não seja o autor do documento, é responsável pela sua confecção. Esta responsabilidade não implica um compromisso legal;

---

[5] Do Aurélio, Compromissivo. *Adj*. Em que há ou que envolve compromisso.

- **Protocolar**. Quando a assinatura tem o propósito de atestar o recebimento de um documento por uma determinada entidade, algumas vezes associando à assinatura o instante do recebimento e/ou uma identificação;

Além dos propósitos mencionados, existem alguns que são realizados utilizando uma contra-assinatura[6], que consiste em uma assinatura aposta sobre uma assinatura previamente realizada.

- **Procuração**. Quando a assinatura é realizada com o propósito de atribuir poderes para uma terceira entidade.
- **Autorização**. Quando a assinatura realizada tem o propósito de garantir direitos de acesso a um recurso para o requisitante. Este recurso pode ser o uso de um objeto ou a execução de alguma tarefa.
- **Testemunhal**[7]. Quando a assinatura realizada no documento tem o propósito de testemunhar o contexto associado ao documento. O exemplo mais típico é a assinatura de testemunhas em contratos. Este signatário pode ser levado a juízo para prestar depoimento em caso de disputa judicial para esclarecimentos relativos ao documento assinado;

---

[6] De acordo com a RFC2630 (HOUSLEY R, 1999), uma contra-assinatura é uma assinatura realizada sobre outra assinatura. Entretanto, como apresentado no trabalho, de acordo com o contexto de negócio onde é aplicada ela pode apresentar significados distintos, embora tecnicamente seja representada da mesma forma.

[7] Do Aurélio, Testemunhal. *Adj.* Relativo à testemunha.

- **Notarial**. Quando a assinatura tem o propósito de reconhecer, em caráter de fé pública, o documento assinado pela entidade;

3.2. ASSINATURA ELETRÔNICA

Conforme mencionado, a realização de uma assinatura sobre um documento tem como objetivo prover a autenticação e, por conseqüência, estabelecer um propósito em relação ao documento assinado. Do mesmo modo, o termo "assinatura eletrônica" pode ser aplicado ao ato de prover autenticação, porém utilizando meios eletrônicos para sua realização. Assim como na assinatura manuscrita, a assinatura eletrônica quando aplicada sobre o documento eletrônico também estabelece um propósito em relação ao documento assinado. Porém, a assinatura eletrônica é capaz de prover também, diferentemente da assinatura manuscrita, a integridade do documento, ou seja, o ato de realizar uma assinatura eletrônica sobre o documento provê a autenticação e a integridade do documento.

De acordo com o ETSI (2003b), a assinatura eletrônica é definida como um conjunto de dados no formato eletrônico os quais são anexados ou logicamente associados a um outro conjunto de dados no formato eletrônico que serve como método de autenticação[8]. O primeiro conjunto de dados representa a assinatura eletrônica enquanto o segundo representa o

[8] A definição do Instituto de Tecnologia da Informação (2002) foca diretamente a assinatura digital, e não a assinatura eletrônica, como faz o ETSI. Por essa razão foi utilizada a definição do ETSI. Maiores detalhes sobre assinatura digital e assinatura eletrônica serão vistos em capítulos subseqüentes.

documento assinado eletronicamente. Se comparado com a assinatura manuscrita, o primeiro conjunto de dados no formato eletrônico é análogo aos sinais gráficos que representam a assinatura manuscrita.

Tanto a assinatura manuscrita quanto a assinatura eletrônica possuem as características necessárias para prover autenticação em documentos. Por esta razão, é necessário dizer que uma assinatura manuscrita digitalizada em um equipamento tipo "scanner" não pode ser classificada como eletrônica. Isto porque a capacidade de prover a autenticação de uma assinatura digitalizada é fraca pelo fato de não existir uma associação inequívoca entre o subscritor e a assinatura digitalizada.

O termo "assinatura eletrônica" é utilizado para qualquer método que garanta a autenticação e integridade de documentos eletrônicos. Um dos principais métodos de geração da assinatura eletrônica é o método de assinatura digital, uma subclasse da assinatura eletrônica que utiliza a técnica de criptografia de chaves públicas, que será detalhado no capítulo 5. A Figura 2 ilustra a relação entre os termos "assinatura eletrônica" e "assinatura digital".

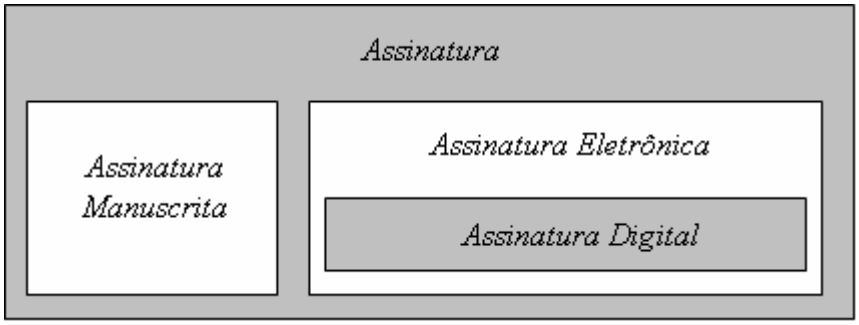

Figura 2 - Assinatura digital como subclasse da assinatura eletrônica.

O termo assinatura é usado com propósito de não vincular a técnica da assinatura digital como única forma de realizar uma assinatura em meio eletrônico, mantendo assim a utilização do termo para tecnologias futuras que garantam autenticação e integridade. Este

trabalho, no entanto, trata exclusivamente da assinatura digital, por ser o método mais difundido de assinatura eletrônica.

3.2.1. Características da assinatura digital

Assim como a assinatura manuscrita, a assinatura digital deve apresentar as seguintes propriedades:

- **Dificuldade de reprodução por terceiros**. A assinatura deve ser difícil de ser forjada por uma outra entidade. No caso da assinatura digital, o mecanismo utilizado para sua realização é baseado na utilização de algoritmos criptográficos de chaves assimétricas cuja chave privada é mantida sob sigilo pelo signatário. Desta forma, o grau de dificuldade para forjar uma assinatura digital por uma terceira entidade está restrito ao comprometimento da chave privada, já que a chave privada é secreta de cada entidade;
- **Facilidade de verificação**. A assinatura deve ser de fácil verificação por uma terceira entidade. No caso da assinatura digital a verificação[9] é realizada utilizando-se a chave pública da entidade signatária. Assim, é possível a verificação da assinatura por qualquer entidade que possua a chave pública do signatário;

[9] O processo de verificação da assinatura digital é detalhado na seção 5.2.

- **Não-reutilizável**. A assinatura realizada em um documento não pode ser reutilizada em outro documento. A assinatura digital utiliza como parâmetro para sua geração o documento eletrônico. Desta forma, qualquer alteração no documento é detectada no processo de verificação. Por esta razão, não é possível associar uma assinatura digital a um outro documento eletrônico senão àquele originalmente assinado sem que isso seja detectado;
- **Inalterabilidade do documento**. Deve ser possível identificar a violação de integridade do documento. No caso da assinatura digital, dado que todo o conteúdo do documento assinado digitalmente é compreendido como parte do cálculo no processo de geração da assinatura digital, qualquer alteração no documento pode ser detectada;
- **Irretratabilidade da geração**. Não deve ser possível ao signatário de um documento repudiar a geração da assinatura. No caso da assinatura digital, sua realização está vinculada à posse da chave privada, a qual deve ser mantida sob sigilo pelo signatário. Desta forma, a guarda da chave mantida sob proteção do signatário pode garantir a irretratabilidade de geração da assinatura.

Além das propriedades mencionadas, existem algumas situações que não ocorrem na assinatura manuscrita e que fazem parte do contexto da assinatura digital como, por exemplo:

- **Período de validade do certificado digital do signatário**. A titularidade do

portador do par de chaves é assegurada através do certificado digital[10], um documento assinado digitalmente por uma Autoridade Certificadora. Um dos atributos de um certificado digital é o seu período de validade que define o período de validade do par de chaves. Isto significa que uma assinatura para ser válida, deve ser realizada dentro do período de validade do certificado associado à chave privada utilizada na assinatura;

- **Revogação do certificado digital do signatário**[11]. O titular de um certificado digital pode solicitar a revogação do mesmo, ou seja, a anulação de seu efeito. Esse processo pode ocorrer em caso de perda ou comprometimento da chave privada associada a esse certificado. Dessa forma, assinaturas realizadas utilizando a chave privada associada a um certificado revogado não são mais válidas;

- **Retirada de assinatura**. Existem situações na qual é possível retirar uma assinatura digital de um documento eletrônico. No caso da assinatura manuscrita, a tentativa de remoção de uma assinatura do documento geralmente deixa vestígios. A assinatura digital, por ser representada por um conjunto de dados eletrônicos, pode ser removida do documento.

- **Junção de assinatura**. Diferentes assinaturas realizadas a um mesmo documento eletrônico podem ser reunidas em um mesmo invólucro. Esse processo permite a assinatura de um documento em paralelo por várias pessoas, sendo possível juntá-

[10] A definição de certificado digital é apresentada na seção 4.3.

[11] O conceito de revogação do certificado digital é apresentado no capítulo na seção 4.4.

las todas no mesmo documento em um momento posterior.

3.2.2. Tipos de Propósitos

Além dos propósitos apresentados na assinatura manuscrita, existem outros específicos da assinatura digital (LEUNG; HUI, 2000) (ETSI, 2003a) como, por exemplo:

- **Íntegro**[12]. O propósito é atestar a integridade das informações contidas no documento. Este tipo de comprometimento pode atestar a origem do documento pela identificação do signatário. Uma assinatura com este tipo de propósito pode ser importante para garantir a integridade do documento em um determinado processo ou fluxo no qual um documento deve ser visualizado e assinado por mais de um signatário paralelamente;
- **Tempestivo**. Quando a assinatura é realizada sobre o conteúdo do documento associando um vínculo temporal obtido a partir de uma entidade confiável de tempo;
- **Testante**. Quando a assinatura é realizada com o propósito de verificar o funcionamento de um sistema de geração de assinaturas.
- **Longevidade**. Quando a assinatura é realizada com o propósito de assegurar a

[12] Do Aurélio. Íntegro. *Adj*. Inteiro, completo.

validade de um documento assinado digitalmente por um longo período de tempo. Isto porque, no decorrer do tempo, o tamanho das chaves utilizadas ou ainda os algoritmos podem se tornar fracos e vulneráveis;

- **Desafio**. Quando a assinatura é realizada sobre uma mensagem cujo propósito é autenticar o usuário. Neste caso, a mensagem pode ser uma seqüência qualquer de bits pois não tem significado neste contexto.

3.3. DIFERENÇAS ENTRE ASSINATURA DIGITAL E ASSINATURA MANUSCRITA

Apesar da larga utilização da assinatura de próprio punho, a assinatura digital apresenta vantagens relacionadas às características de uma assinatura.

Com relação à geração da assinatura, o mecanismo da assinatura digital é baseado na utilização de algoritmos criptográficos de chaves assimétricas cuja chave privada é mantida sob sigilo pelo signatário. Desta forma, o grau de dificuldade para forjar uma assinatura digital está restrito ao comprometimento da chave privada, já que o custo computacional para a descoberta da chave é demasiadamente elevado.

Com relação à verificação de uma assinatura, a chave pública de verificação possibilita uma verificação mais apurada se comparada com a verificação visual utilizada para assinaturas de próprio punho. Além disso, dado que todo o documento assinado digitalmente é compreendido como parte do cálculo no processo de geração da assinatura digital, qualquer alteração no documento pode ser detectada de forma mais confiável e prática se comparada com a garantia de não rasura do documento em papel. Quanto ao não repúdio de geração, a assinatura digital somente pode ser gerada pelo portador da chave privada e desta forma o

processo pode assegurar a evidência para irretratabilidade de geração da assinatura.

Uma vantagem da assinatura digital que deve ser destacada é que ela permite que o receptor de um documento assinado digitalmente tenha condições de identificar e verificar a assinatura sem a necessidade de uma terceira entidade que valide a assinatura realizada sobre o documento, como no caso da assinatura manuscrita.

Com relação ao conceito de cópias de documentos, no caso da assinatura digital em documentos eletrônicos, a cópia é idêntica ao documento originalmente assinado. Se comparado com a assinatura manuscrita, para cada cópia do documento em papel é necessária a realização de uma nova assinatura.

Outra característica de diferença é com relação à realização de contra-assinaturas. Uma contra-assinatura é uma assinatura que faz referência a uma outra assinatura, como, por exemplo, a assinatura da testemunha em um documento. A assinatura da testemunha faz referência às assinaturas realizadas no documento e não ao texto do documento. Por esta razão, é comum que a assinatura de uma testemunha seja realizada após a assinatura das partes envolvidas no contexto do documento assinado. No caso da assinatura em papel, pode não ser possível assegurar que a assinatura de uma testemunha seja realizada somente após a assinatura das partes envolvidas no contexto do documento. No caso da assinatura digital, uma contra-assinatura somente pode ser realizada após a geração da assinatura que se pretende contra-assinar. Isto porque o parâmetro utilizado para a geração da contra-assinatura é a assinatura previamente realizada.

Por fim, outra diferença com relação à assinatura manuscrita é que a assinatura digital normalmente utiliza certificados digitais para identificação da entidade. O certificado digital possui um período de validade e a assinatura digital deve ser realizada durante esse período para ter validade[13]. Além disso, o certificado digital pode ser revogado em caso de desconfiança de comprometimento da chave privada a ele associado, o que implica na imediata diminuição do período de validade do certificado. Portanto, um dos requisitos para a validade de uma assinatura digital está relacionado ao período de validade do certificado digital e sua não revogação.

[13] O conceito e as características do certificado digital são apresentados na seção 4.3.

4. INFRA-ESTRUTURA DE CHAVES PÚBLICAS

Chama-se Infra-estrutura de Chaves Públicas (ICP) toda infra-estrutura de obtenção e uso de certificados digitais (ADAMS; LLOYD, 1999). Sua função básica é emitir certificados que vinculem uma chave pública a uma entidade, como um indivíduo, uma organização, ou um sistema. Os elementos que fazem parte de uma infra-estrutura de chaves públicas são:

- **Entidade final**. Termo utilizado para designar qualquer entidade que pode ser identificada como o sujeito para o qual um certificado de chave pública é emitido;
- **Autoridade Certificadora Raiz (AC-Raiz)**. Representa o início da cadeia de confiança. Uma AC-Raiz é responsável pela emissão dos certificados digitais de outras ACs, denominadas subordinadas.
- **Autoridade Certificadora (AC)**. Responsável pela emissão do certificado digital. Dentre as atividades de uma AC está o gerenciamento e publicação da lista de certificados revogados (LCR);
- **Autoridade de Registro (AR)**. Responsável por receber solicitações de emissão ou de revogação de certificados, pela identificação da entidade final e por disponibilizar os certificados emitidos pela AC aos seus respectivos solicitantes, servindo de intermediária entre o usuário e a AC;
- **Repositório de certificados e LCR**. Consiste em um repositório que pode ser acessado por todos os membros da ICP e onde ficam armazenados os certificados emitidos, bem como a lista dos certificados revogados.

4.1. CADEIA DE CERTIFICAÇÃO

Um certificado raiz determina o início de uma cadeia de certificação. A cadeia de certificação é formada pelo certificado da entidade final até o certificado raiz. Uma entidade final pode ter um certificado emitido diretamente por uma AC raiz ou por uma AC subordinada. Um dos modelos de cadeia de certificação é o modelo hierárquico. Este é o modelo praticado no contexto da ICP-Brasil, cujo objetivo é garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras (ICP, 2006).

A Autoridade Certificadora Raiz Brasileira emite certificados digitais para as autoridades certificadoras subordinadas, e não pode emitir diretamente às Entidades Finais. A Figura 3 ilustra o exemplo de uma cadeia de certificação baseada no modelo hierárquico.

Figura 3 - Cadeia de certificação baseada no modelo hierárquico.

4.2. POLÍTICA DE CERTIFICAÇÃO DIGITAL

Uma política de certificação digital define um conjunto de normas e práticas de uma AC para emissão e uso de certificados digitais. Uma política de certificação pode definir, por

exemplo, quais os tipos de certificados devem ser emitidos pela AC. No contexto da ICP-Brasil, por exemplo, toda autoridade certificadora subordinada à AC Raiz Brasileira deve contemplar, dentro da política de certificação, quais os tipos de certificados que emite, tanto para assinatura quanto para sigilo.

A Política de Certificação (PC) de um certificado deve ser disponibilizada para qualquer usuário através de uma URL identificada como atributo do certificado digital.

4.3. CERTIFICADO DIGITAL

O certificado digital é um documento assinado digitalmente cujo propósito é assegurar a integridade da chave pública associada à chave privada. Além disso, assegura a veracidade da ligação dessa chave a um determinado conjunto de dados que representam a identidade digital de seu titular. A Figura 4 ilustra os elementos que compõe um certificado digital.

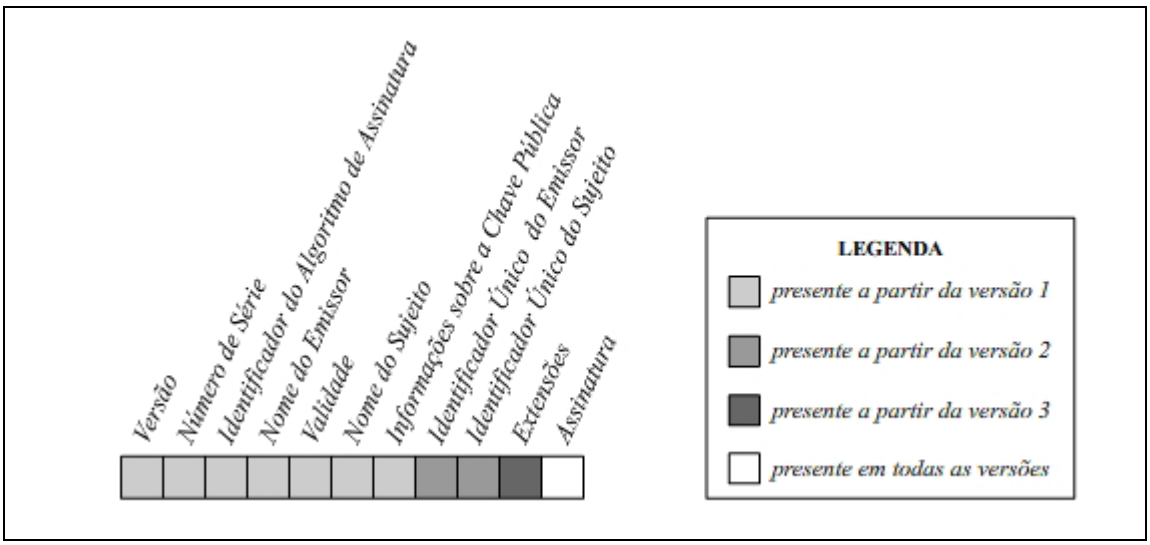

Figura 4 - Estrutura do certificado digital (Extraído de ARREBOLA, 2006).

O certificado digital de chave pública é formado por uma série de campos, a saber:

- **Versão**. Campo responsável por diferenciar as sucessivas versões do certificado;

- **Número de Série**. Identificador numérico único dentro de um domínio. Este identificador é atribuído pela entidade especificada no campo Nome do Emissor;
- **Identificador do Algoritmo de Assinatura**. Identificador do algoritmo utilizado para assinar digitalmente a estrutura;
- **Nome do Emissor**. Conjunto de caracteres que identifica a entidade emissora do certificado, aquela que assinou digitalmente a estrutura;
- **Validade**. Define o intervalo de tempo durante o qual o emissor do certificado atesta, inicialmente, sua validade;
- **Nome do Sujeito**. Identifica a entidade final à qual o certificado se refere, ou seja, a entidade que mantém a chave privada correspondente à chave encontrada no campo Informação sobre a Chave Pública.
- **Informação sobre a Chave Pública**. Contém a chave pública da entidade final (sujeito), o identificador do algoritmo utilizado e outros parâmetros associados;
- **Identificador Único do Emissor** e **Identificador Único do Sujeito**. Caso haja reutilização de nomes, esses campos servem como identificadores únicos para emissor e sujeito, respectivamente. De acordo com (HOUSLEY et al, 2002), o uso desses campos não é recomendado.
- **Extensões**. Presente na especificação a partir da versão 3, esse campo permite a criação atributos do certificado digital. Um dos mais notórios exemplos de extensão é o propósito da chave, ou *key usage*. Através dele uma AC pode impor restrições ao uso dos certificados emitidos.

4.4. REVOGAÇÃO DO CERTIFICADO DIGITAL

O certificado digital possui definido um período de validade que determina o intervalo de tempo no qual o certificado é válido para uso. Entretanto, em algumas situações o certificado digital pode perder a validade mesmo que não tenha expirado. Revogar o certificado digital significa invalidar o seu uso a partir do instante da revogação (ADAMS; LLOYD, 99). A Figura 5 ilustra o período de validade do certificado diminuído em função da revogação

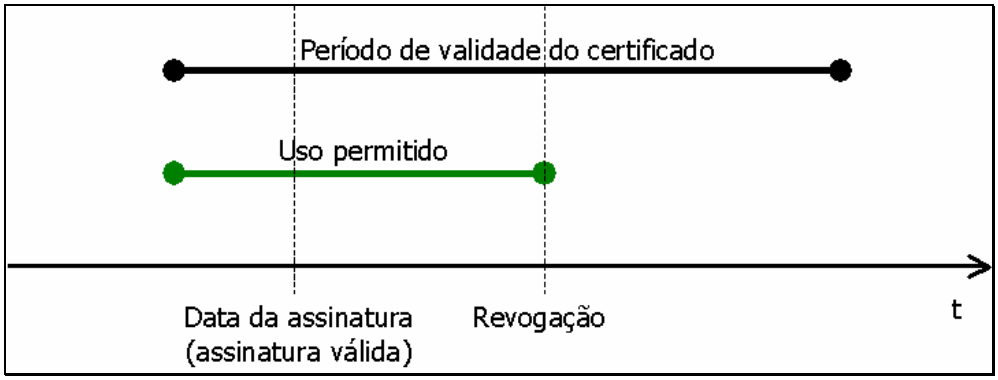

Figura 5 - Uso permitido do certificado (Adaptado de BERNAL, 2005).

Uma das principais razões para a revogação do certificado digital está relacionada com perda ou suspeita de comprometimento da chave privada. Neste caso, a entidade titular do certificado digital deve acionar os mecanismos da respectiva autoridade certificadora para a revogação do certificado digital. Normalmente o processo de revogação ocorre através da identificação da entidade titular do certificado, seguido de uma solicitação formal.

Para informar o estado de revogação do certificado digital é importante que exista algum mecanismo de publicação periódico. Dentre os mecanismos mais conhecidos estão a consulta à Lista de Certificados Revogados (LCR) e a verificação *on-line* através do *Online Certificate Status Protocol* (OCSP).

4.4.1. Lista de Certificados Revogados

Uma LCR é uma estrutura de dados assinada digitalmente que contém a lista da identificação dos certificados revogados (HOUSLEY; POLK; FORD; SOLO, 2004). A garantia de integridade e autenticidade da LCR é assegurada pela assinatura digital. Normalmente, a mesma AC que emite o certificado digital também assina a LCR.

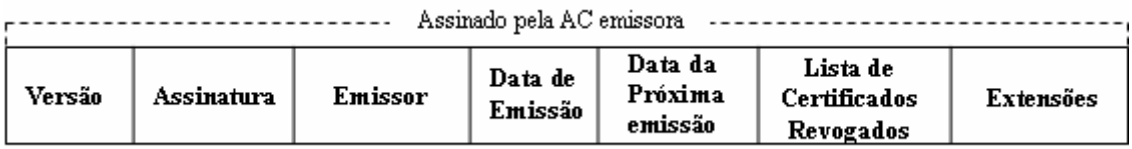

Figura 6 - Campos da LCR (Adaptado de ADAMS; LLOYD, 99).

Os campos ilustrados na Figura 6 são detalhados a seguir:

- **Versão**. Contém a versão da LCR, atualmente na versão 2;
- **Assinatura**. Contém a identificação dos algoritmos de resumo criptográfico e criptografia assimétrica para o cálculo da assinatura digital da LCR;
- **Emissor**. Contém a identificação (*Distinguished Name*) da entidade emissora da LCR;
- **Data de emissão**. Contém a data e hora de publicação da LCR;
- **Data da próxima Emissão**. Contém a data e hora de expiração da LCR;
- **Lista de Certificados revogados**. Contém o número de série e o instante de revogação dos certificados revogados. O instante da revogação é uma informação importante para a verificação futura de uma assinatura digital. O certificado digital revogado invalida a assinatura somente se esta for realizada depois do instante de

revogação. Caso contrário, se a assinatura for realizada antes da revogação, mesmo a identificação do certificado estando presente na LCR, a assinatura permanece válida;

- **Extensões**. Definido a partir da versão 2, este campo contém alguns atributos como, por exemplo, a razão pelo qual o certificado foi revogado. Este campo é opcional;

Uma questão importante com relação à LCR é quanto sua freqüência de publicação. Como descrito, os campos data de emissão e data da próxima emissão**,** definem o intervalo de tempo de uso da LCR. Devido à periodicidade da publicação, existe um intervalo de tempo entre o instante da revogação do certificado e o instante da publicação desta informação na LCR. Por esta razão, no caso da verificação uma assinatura, recomenda-se que a verificação do certificado quanto ao seu estado de revogação utilize uma LCR publicada posteriormente ao instante de realização da assinatura.

O período entre o instante de realização da assinatura e o instante de publicação da próxima LCR foi classificado pelo ETSI (2003b) como *Grace Period*, podendo ser traduzido como período de tolerância. A Figura 7 ilustra a situação do período de tolerância.

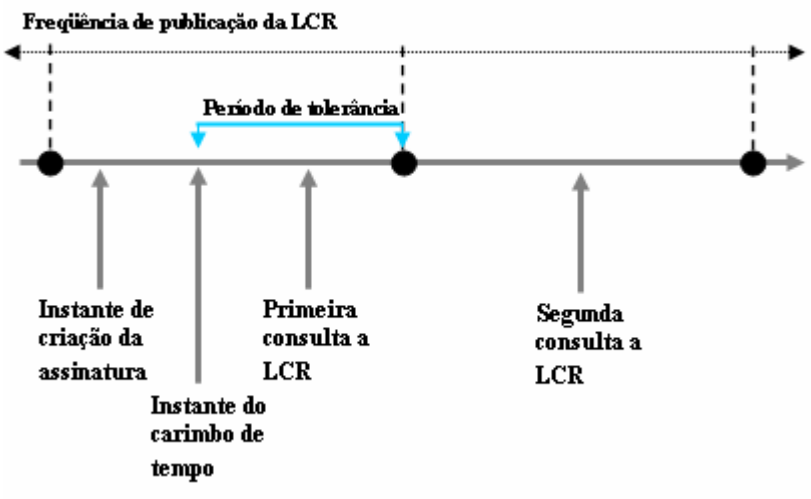

Figura 7 - Período de tolerância (Adaptado de ETSI, 2003b).

4.4.2. Protocolo OCSP

O protocolo *Online Certicate Status Protocol* (OCSP) permite a consulta em tempo real do estado de revogação do certificado digital (MYERS et al, 1999). O protocolo define uma requisição e uma resposta com os possíveis estados do certificado digital. Estes estados podem ser:

- **Válido**. O certificado digital não está revogado;
- **Revogado**. O certificado digital está revogado. Neste caso, informa também o instante de revogação e, opcionalmente, o motivo da revogação;
- **Desconhecido**. Não possui informações sobre o certificado solicitado.

As respostas são assinadas digitalmente pela entidade que emitiu o certificado para assegurar a integridade e autenticidade da informação contida na resposta.

4.5. CONSIDERAÇÕES FINAIS

Este capítulo apresentou os conceitos de infra-estruturas de chaves públicas e certificados digitais que serão usados no decorrer do texto. Com relação aos mecanismos de validação do estado de revogação, foram apresentados dois mais utilizados, a consulta a LCR e o protocolo OCSP.

O mecanismo de verificação por protocolo OCSP, se comparado com o mecanismo da LCR, apresenta como vantagem a resposta em tempo real do estado de revogação, evitando situações como o período de tolerância. Entretanto, como a resposta OCSP é assinada digitalmente, isso aumenta o ônus da autoridade certificadora pelo fato de ter que assinar cada

requisição realizada, necessitando de mais recursos computacionais. A Tabela 1 sumariza as características dos mecanismos.

Tabela 1 - Características dos mecanismos de publicação do estado de revogação.

Mecanismo	**Freqüência de publicação**	**Assinatura da AC emissora**	**Característica**
LCR	Periódica	Uma por período de publicação	Problema do período de tolerância.
OCSP	Tempo real	De acordo com o número de requisições	Aumenta o custo de infra-estrutura da AC emissora.

5. ASSINATURA DIGITAL

O processo de assinatura digital possui as características necessárias para prover autenticação, integridade e irretratabilidade (STALLINGS, 1998). Para realização de uma assinatura digital em documentos eletrônicos, no contexto de uma infra-estrutura de chaves públicas (ICP), o assinante deve possuir:

- Um certificado digital emitido por uma Autoridade Certificadora (AC) e sua chave privada correspondente;
- O documento eletrônico; e
- Um programa de computador capaz de realizar as operações criptográficas pertinentes ao processo de geração de uma assinatura digital (*software* de assinatura).

5.1. GERAÇÃO DA ASSINATURA DIGITAL

De acordo com Stallings (1998), o processamento para geração de uma assinatura digital divide-se em duas etapas. Na primeira etapa do processo, um valor de *hash*[14] do

[14] A função é utilizada com algum algoritmo de espalhamento para o cálculo do resumo criptográfico

documento, também conhecido como resumo criptográfico, é calculado utilizando um algoritmo, por exemplo, MD2, MD4, MD5, SHA1 ou outros. O valor do *hash* calculado de uma mensagem é uma seqüência de bits com um tamanho fixo. Todos os algoritmos confiáveis para o cálculo do valor do *hash* aplicam transformações matemáticas tais que, quando apenas um simples bit da mensagem de entrada é alterado, um valor de *hash* completamente diferente é obtido. Esta é a propriedade que garante a integridade do documento eletrônico assinado digitalmente. Estes algoritmos devem ser muito estáveis em ataques criptoanalíticos; ou seja, deve ser computacionalmente muito difícil, a partir de um valor de *hash*, encontrar a mensagem que originou tal valor. Esta inviabilidade para a recuperação da mensagem de entrada deve-se ao fato de que o valor de *hash* de uma mensagem pode ter o tamanho muitas vezes menor do que a mensagem de entrada. Há consenso atualmente que os recursos computacionais necessários para encontrar uma mensagem, dado seu valor de *hash,* são tão grandes que inviabilizam tal tarefa. É também importante saber que, teoricamente, é possível que duas mensagens inteiramente diferentes tenham o mesmo valor de *hash*, mas a probabilidade de isto acontecer é tão pequena que, na prática, é desconsiderada.

Em uma segunda etapa, o valor do resumo criptográfico da mensagem obtido no passo anterior, é cifrado com a chave privada do signatário. Este bloco cifrado é a assinatura digital da mensagem. Para este propósito, é utilizado um algoritmo criptográfico-matemático. Os algoritmos usados mais freqüentemente são RSA (baseado na teoria dos números), DSA

(MENEZES, 1996).

(baseado na teoria dos logaritmos discretos) e o ECDSA (baseado na teoria das curvas elípticas). Em geral, a assinatura digital obtida é anexada à mensagem assinada sob um formato especial para ser verificada posteriormente, se for necessário. A Figura 8 exibe as etapas do processamento para geração de uma assinatura digital.

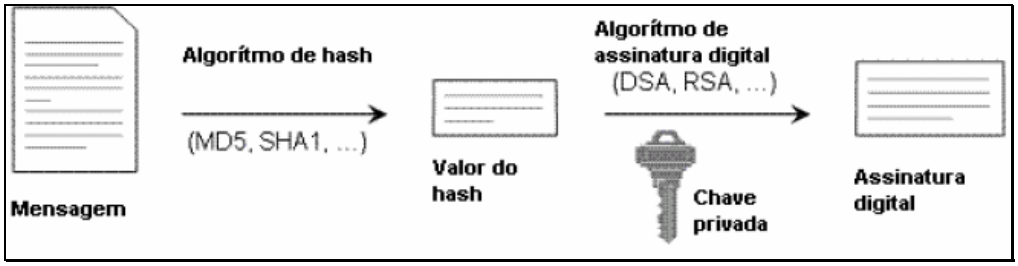

Figura 8 - Processo de Geração da Assinatura Digital.

5.2. VERIFICAÇÃO DA ASSINATURA

A tecnologia de assinatura digital permite ao receptor de uma dada mensagem assinada verificar sua autoria de geração e sua integridade. O processo de verificação da assinatura digital é proposto para determinar se uma dada mensagem foi assinada pela chave privada que corresponde a uma dada chave pública. No entanto, a verificação da assinatura digital não pode determinar se uma dada mensagem foi assinada por uma determinada entidade. Se há necessidade de verificar se uma entidade assinou uma dada mensagem, é necessário obter a sua chave pública de maneira segura, como, por exemplo, recebendo-a pessoalmente em um disquete ou um CD, ou no contexto de uma infra-estrutura de chaves públicas, utilizando um certificado digital. Sem ter um modo seguro de obter a chave pública de uma dada entidade não há a possibilidade de verificar se uma dada mensagem é realmente assinada pela mesma.

Do ponto de vista técnico, a verificação da assinatura digital é executada em três etapas. Na primeira etapa, o valor de *hash* da mensagem assinada é calculado. Para esse cálculo, utiliza-se o mesmo algoritmo de *hash* tal como foi usado durante o processo de geração da assinatura. O valor obtido é chamado de "valor de *hash* corrente" porque ele é calculado a partir da mensagem originalmente assinada.

Na segunda etapa, o bloco de assinatura digital é decifrado utilizando a chave pública associada à chave privada utilizada durante a etapa de assinatura da mensagem. Como resultado, é obtido o valor original do *hash* que foi calculado a partir da mensagem original durante a primeira etapa da criação da assinatura digital.

Finalmente, na terceira etapa, é comparado o valor corrente do *hash* obtido no primeiro passo da verificação com o valor original do *hash* obtido no segundo passo da verificação. Se os dois valores forem idênticos, a verificação é bem sucedida e prova que a mensagem foi assinada com a chave privada que corresponde à chave pública usada na verificação. Se forem diferentes, isto significa que a assinatura digital é inválida. A Figura 9 ilustra o processo de verificação da assinatura.

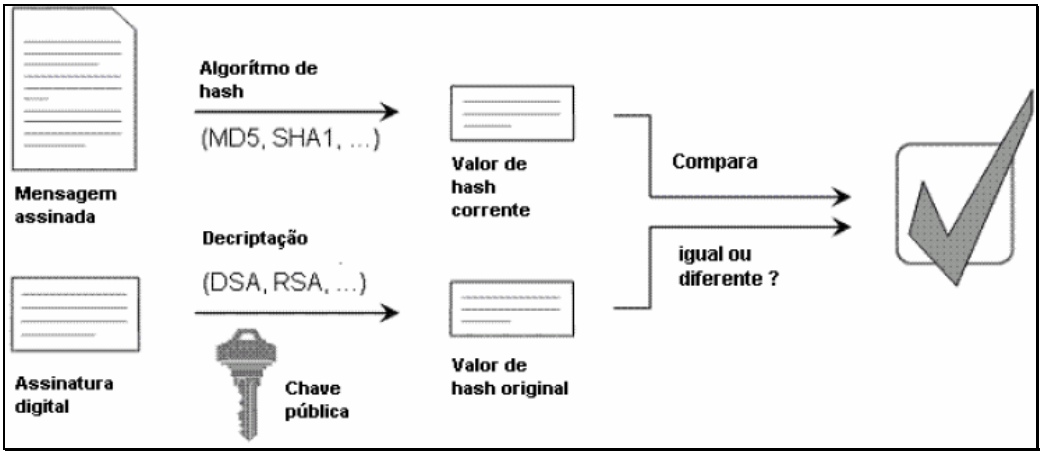

Figura 9 - Processo de verificação da assinatura digital.

5.2.1. Validade da assinatura digital

A validade da assinatura digital em um documento eletrônico consiste principalmente na verificação da integridade e autenticidade do documento e na validade do certificado do assinante. Com relação à validade do certificado, é necessário que:

- O propósito para o qual o par de chaves foi gerado inclua o campo *Digital Signature*, especificado no campo k*ey usage* do certificado;
- O período de validade do certificado não esteja expirado no instante de realização da assinatura;
- O certificado esteja dentro de um domínio de segurança confiável (certificado raiz confiável);
- O certificado não tenha sido revogado antes do instante da realização da assinatura.

Existem algumas razões para que assinatura digital seja considerada inválida sob a perspectiva do processamento criptográfico. Há pelo menos três possíveis razões para resultar em assinatura digital inválida:

- Se a assinatura digital é adulterada (ela não é verdadeira) e é decifrada com a chave pública verdadeira, o valor original obtido não será o valor de *hash* original da mensagem original, mas algum outro valor diferente;
- Se a mensagem foi alterada (adulterada) após a assinatura, o valor de *hash* corrente calculado dessa mensagem adulterada será diferente do valor de *hash* original porque as duas mensagens correspondem a valores de *hash* diferentes;
- Se a chave pública utilizada não corresponde à chave privada usada para efetuar a assinatura digital, o valor de *hash* obtido pela decifração da assinatura não será

igual ao valor de *hash* corrente obtido a partir da mensagem.

Se a verificação falhar, indica que a assinatura que está sendo verificada não foi obtida assinando a mensagem que está sendo verificada com a chave privada que corresponde à chave pública usada para a verificação. A verificação mal sucedida não significa necessariamente que uma tentativa de adulteração da assinatura digital foi detectada. Às vezes, a verificação pode falhar porque uma chave pública inválida é usada. Tal situação pode ser encontrada quando a mensagem não é emitida pela entidade que se esperou emiti-la ou quando o sistema de verificação da assinatura tem uma chave pública incorreta para esta entidade. É possível que uma mesma entidade possua diversos certificados válidos e o sistema tenha tentado verificar uma mensagem recebida com o certificado incorreto.

Para que tais problemas sejam evitados, o mais usual é que, quando um documento assinado é gerado, o bloco de assinatura e o certificado do signatário sejam anexados ao documento. Assim, durante a verificação, a chave pública contida no certificado recebido é usada para a verificação da assinatura. Se a verificação for bem sucedida, considera-se que o documento é assinado pela entidade que possui o certificado.

5.3. INVÓLUCRO DE DOCUMENTO E ASSINATURA

O resultado da assinatura digital de um documento eletrônico é uma seqüência de bits que possui obrigatoriamente:

- **Bloco de informações de assinatura**. Este objeto contém uma ou mais assinaturas realizadas sobre o documento. Cada assinatura contém um conjunto de dados criptografados que representam a assinatura digital propriamente dita.

Além dessa informação, outros objetos podem estar também presentes, como:

- **Certificados**. Este objeto pode conter os certificados das entidades signatárias do documento. Pode conter também os certificados das ACs da cadeia de certificação;
- **Lista de Certificados Revogados**. Este objeto pode conter as listas de certificados revogados relacionadas a cada certificado dos signatários.

Geralmente, estas informações são armazenadas em um único objeto que será denominado de "invólucro de documento e assinatura". Este invólucro pode ser apresentado de duas formas:

- **Invólucro com documento incluído**. Além do bloco de assinaturas e dos objetos opcionais, contém também o documento que foi assinado;
- **Invólucro com documento excluído**. Contém somente o bloco de assinaturas e os objetos opcionais, não incluindo o documento assinado.

A Figura 10 ilustra os objetos associados ao documento assinado digitalmente no invólucro com documento incluído.

Figura 10 - Invólucro de documento e assinatura com documento incluído.

5.4. FORMATOS DE INVÓLUCRO DE ASSINATURA DIGITAL

A especificação mais difundida para encapsular documentos eletrônicos e assinaturas digitais é o PKCS#7. Este formato, originalmente especificado pela RSA Laboratórios (RSA LABORATORIES, 1993), sofreu constantes evoluções (HOUSLEY, 1999) (HOUSLEY, 2002) até a versão mais atual conhecida como CMS3 (*Cryptographic Message Syntax version 3)* (HOUSLEY, 2004). Neste formato são definidos objetos descritos em *Abstract Syntax Notation 1* (ASN.1) e codificados em *Distinguished Encoding Rules* DER (ITU-T, 2002).

O CMS3 descreve uma sintaxe para armazenamento de conteúdo criptografado ou aberto, dentre eles o formato de assinatura digital. Relacionado ao conteúdo de assinatura digital, permite também a associação de atributos como, por exemplo, o carimbo de tempo (ADAMS et al, 2001) e contra-assinaturas. Além disso, a inserção de certificados e CRLs no pacote CMS permite a validação auto-contida da assinatura digital, ou seja, todos os elementos necessários à validação da assinatura estão presentes: o certificado do signatário, os certificados das ACs intermediárias (a cadeia de certificação) e a LCR. Quanto ao conteúdo assinado, não possui uma restrição de identificação do tipo de formatação do documento, sendo que qualquer seqüência de bits pode ser assinada e encapsulada no invólucro. A Figura 11 ilustra os objetos do formato PKCS#7/CMS.

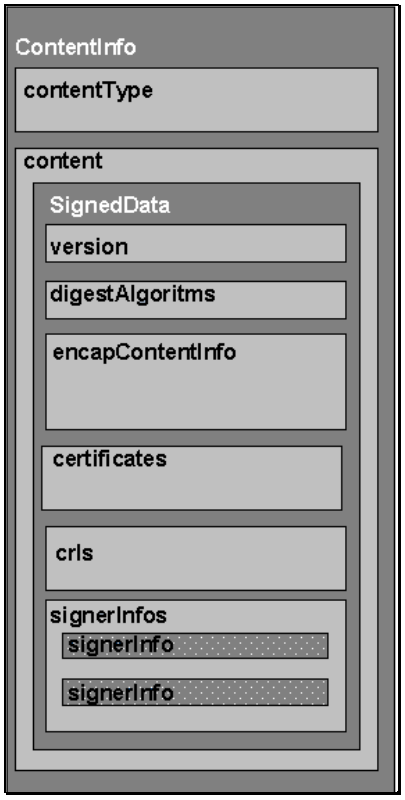

Figura 11 - Objetos do formato PKCS#7/CMS.

Outro formato utilizado para representação de assinaturas digitais é o *XMLSignature*, derivado da linguagem *Extensible Markup Language* (XML) (BRAY, 2004), cuja especificação é mantida pela organização *World Wide Web Consortium* (W3C) e *Internet Engineering Task Force* (IETF). Sua última especificação é dada pela RFC-3275 (EASTLAKE, 2002). Em comparação ao CMS, o *XMLSignature* apresenta as vantagens da própria linguagem XML, que é extensível, possibilitando a criação de *tags* de um modo arbitrário, desde que as regras de aninhamento sejam respeitadas. É bastante útil como meio de integração de diversas fontes de informação e apresentação de interface uniforme para esses dados (SOUZA, 2002).

O formato *XMLSignature* contempla assinatura de diversos tipos de conteúdo como, dados codificados em ASCII em diversos tipos de formatos, dados em código binário como, por exemplo, imagens em formato específico ou ainda dados formatados em XML. Com

relação ao conteúdo assinado, o formato *XMLSignature* permite identificar uma assinatura realizada sobre parte do documento.

Em nenhum dos dois formatos de assinatura apresentados existe um atributo que identifique o tipo do conteúdo assinado. Dessa forma, fica prejudicada a visualização do documento assinado, já que não se sabe, à priori, qual aplicativo utilizar para essa visualização.

5.5. CO-ASSINATURA E CONTRA-ASSINATURA

Co-assinar um documento tem o sentindo de apor ao documento uma nova assinatura. A contra-assinatura é aquela realizada sobre uma assinatura já existente (LEA, 2006). De acordo com ETSI (2003a), alguns exemplos de contra-assinatura são:

- Assinatura de testemunha;
- Assinatura de notário.

No meio eletrônico, a mensagem usada no cálculo para geração de uma contra-assinatura é o resumo criptográfico das assinaturas do documento previamente realizadas.

5.6. PROBLEMA DA VERIFICAÇÃO DA VALIDADE DO CERTIFICADO

Umas das diferenças marcantes da assinatura digital com relação à assinatura manuscrita é que a assinatura digital somente pode ser considerada válida se realizada durante

o período de validade do certificado digital, e se o mesmo não estiver revogado, conforme apresentado na seção 4.4. Por esta razão, é muito importante que haja, junto à assinatura, um registro confiável do instante de realização da mesma.

O trabalho de (ZHOU, 2000), apresenta quatro esquemas que podem ser usados como forma de assegurar a validade da assinatura digital gerada antes da revogação do par de chaves. Dentre os modelos apresentados, a utilização do carimbo de tempo (ADAMS; CAIN; PINKAS; ZUCCHERATO, 2001) é o mecanismo que oferece maior nível de segurança.

5.6.1. Carimbo de tempo

O parâmetro responsável por criar um vínculo temporal em uma assinatura digital é denominado de carimbo de tempo. Para garantir a lisura desse parâmetro, é recomendável que o mesmo seja emitido por uma terceira entidade confiável, chamada de "Autoridade de Carimbo de Tempo" (ACT) ou "*Time Stamping Authority*" (TSA).

O exemplo a seguir demonstra a importância do instante de realização de uma assinatura. Suponha que um atacante teve acesso à chave privada de uma entidade no instante T1. A entidade, após tomar conhecimento do comprometimento de sua chave privada, revoga o seu certificado digital no instante T2. No instante T3, o atacante realiza uma assinatura digital utilizando o certificado da entidade informando um instante falso de realização da assinatura. Por não existir um vínculo temporal confiável, no caso do exemplo, um atacante poderia realizar uma assinatura digital em nome da entidade e a assinatura poderia ser considerada como válida. A Figura 12 ilustra o exemplo mencionado.

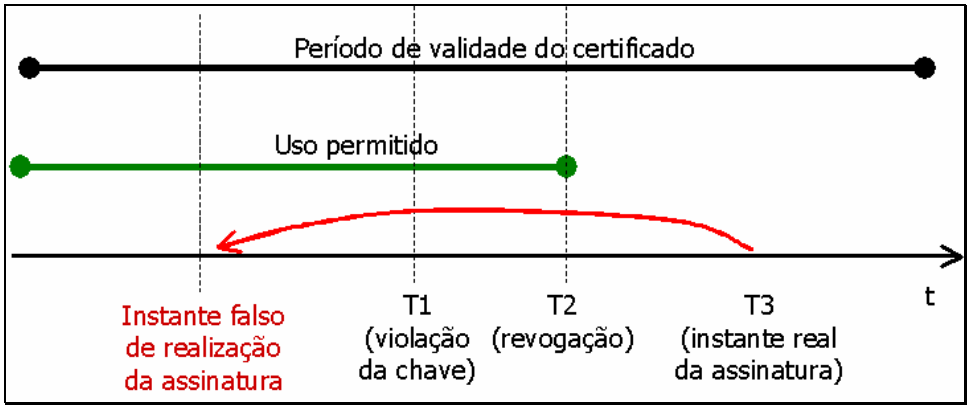

Figura 12 - Geração de assinatura com instante falso (Adaptado de BERNAL, 2005).

O uso do carimbo de tempo assegura um instante confiável de tempo. Assim, no caso do exemplo, o atacante não poderia informar um instante falso, pois o instante real de realização da assinatura estaria assegurado pelo carimbo de tempo. A Figura 13 representa a realização de uma assinatura com carimbo de tempo.

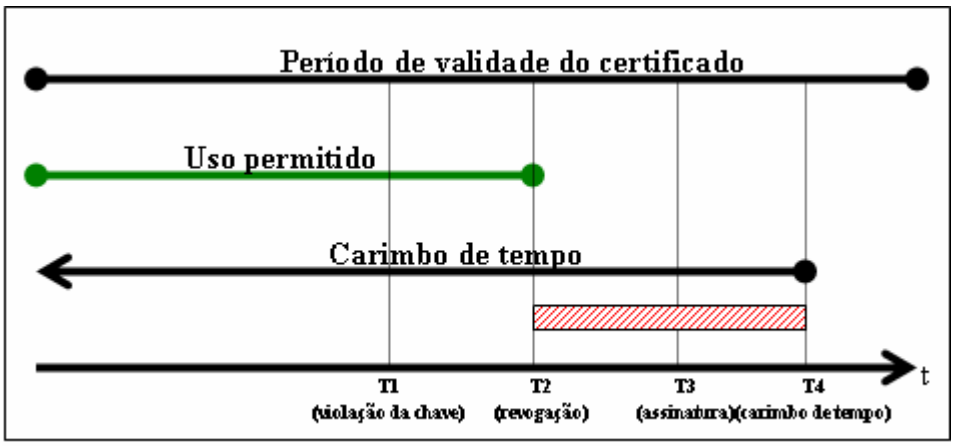

Figura 13 - Geração de assinatura com carimbo de tempo (Adaptado de BERNAL, 2005).

A presença do carimbo de tempo em um documento assinado digitalmente é importante para evitar o repúdio da assinatura, por parte das entidades signatárias, devido à revogação por violação de chaves criptográficas. Sua importância está relacionada à possibilidade de comprovar que a assinatura ocorreu antes de uma determinada data.

5.7. CONSIDERAÇÕES FINAIS

Este capítulo apresentou as principais características de uma assinatura digital e os elementos envolvidos no processo de geração e verificação. Os próximos capítulos, sempre que necessário, farão referências aos conceitos apresentados neste capítulo.

6. POLÍTICA DE ASSINATURA DIGITAL

No cenário do documento em papel, uma assinatura pode ser realizada em um determinado contexto específico e pode possuir diferentes tipos de propósitos, como apresentado no capítulo 3. Pode haver, ainda, múltiplas assinaturas de cada uma das partes interessadas e haver uma determinada ordem para que as mesmas ocorram, bem como pode haver a necessidade de apresentação anterior de determinado documento que comprove que um signatário tem realmente autoridade para assinar aquele tipo de documento.

O conjunto de requisitos para a geração e verificação de assinaturas pode variar de acordo com o contexto legal ou de negócio do documento. A política de assinatura expressa e formaliza justamente este conjunto de requisitos. Uma política de assinatura é um conjunto de regras que deve ser utilizada no momento de criação e verificação de uma assinatura eletrônica sob a qual a assinatura pode ser determinada como válida de acordo com o contexto (ETSI, 2003a). No momento de realizar a assinatura, o signatário deve aceitar essas regras, podendo então a política de assinatura estabelecer sob quais condições os signatários concordam em aceitar a assinatura para contexto aplicado.

Uma política de assinatura pode estar relacionada com a validação de uma assinatura individual ou de múltiplas assinaturas em um único documento, por exemplo, um contrato. Ela pode ser potencialmente muito complexa, gerenciando assinaturas que são requeridas em múltiplos estágios de uma transação comercial, por exemplo, transações de comércio internacional envolvendo controles de exportação e importação.

Além das características técnicas envolvidas no processo de realização de assinatura digital, uma política de assinatura pode incluir as formalidades e cerimônias para realização

de assinaturas do mundo em papel. Pode também incluir quem pode assinar, sob quais circunstâncias e o que pode ser assinado. Naturalmente essas regras poderiam ser estabelecidas entre as partes sem a necessidade do modelo de política de assinatura. Porém, isso exigiria que o usuário configurasse seu software de assinatura[15] (geração e verificação) para operar segundo determinado critério. A utilização do modelo de política de assinatura permite a configuração automática do software de acordo com as regras definidas.

Dentro do mesmo contexto de negócio, tais regras podem variar também de acordo com o propósito da assinatura e com o papel da entidade signatária no contexto aplicado.

6.1. REPRESENTAÇÃO DA POLÍTICA DE ASSINATURA

Segundo o ETSI (2003b), uma política de assinatura pode ser emitida no formato de um documento ou ainda em formato eletrônico. No caso do formato eletrônico, uma das vantagens de utilização de uma política de assinatura é a interoperabilidade entre softwares de geração de assinatura para gerar e validar uma assinatura de acordo com as regras estabelecidas na política. Com relação à notação do formato eletrônico, o ETSI (2002, 2003c) define o uso do ASN.1 (ITU-T, 2002) ou do XML (BRAY, 2005). Paralelamente aos formatos eletrônicos, a política pode ser expressa através de um documento descrevendo os

[15] Um software de assinatura é um programa de computador construído para realizar operações criptográficas, que faz uso de algum tipo de biblioteca criptográfica para assinar e verificar documentos eletrônicos.

itens da política de assinatura.

O uso do formato eletrônico é importante para o processamento automático de verificação da política, bem como sua utilização por *softwares* de geração e verificação de assinaturas digitais. Já o formato de documento tem sua relevância devido ao fato que o signatário do documento deve conhecer a política de assinatura que está sendo usada para gerar sua assinatura. Neste caso, é recomendável um sistema de visualização segura[16] do documento da política.

A Figura 14 ilustra o trecho de uma política de assinatura definida em formato eletrônico utilizando a notação ASN.1

```
SignaturePolicy ::= SEQUENCE {
    signPolicyHashAlg      AlgorithmIdentifier,
    signPolicyInfo         SignPolicyInfo,
    signPolicyHash         SignPolicyHash       OPTIONAL }

SignPolicyHash ::= OCTET STRING

SignPolicyInfo ::= SEQUENCE {
     signPolicyIdentifier          SignPolicyId
     dateOfIssue                   GeneralizedTime
     policyIssuerName              PolicyIssuerName
     fieldOfApplication            FieldOfApplication
     SignatureValidationPolicy     SinatureValidationPolicy
     signPolicyExtentions          SignPolExtentions       OPTIONAL
}
```

Figura 14 - Trecho da estrutura de política de assinatura em ASN.1.

[16] O trabalho de SCHEIBELHOFER (2001) apresenta uma proposta para visualização segura de documentos em meio eletrônico.

6.2. ATRIBUTOS DE UMA POLÍTICA DE ASSINATURA

Os atributos de uma política de assinatura, conforme definido pelo ETSI (2002c, 2003c) e mostrados na Figura 15, são:

- **Identificação do algoritmo de *hash***. Este atributo contém a identificação do algoritmo de *hash* usado;
- **Valor do *hash***. Este atributo contém o valor do *hash* calculado referente à política;
- **Informações da política de assinatura**. Este atributo contém efetivamente o conteúdo da política de assinatura e está detalhado a seguir.

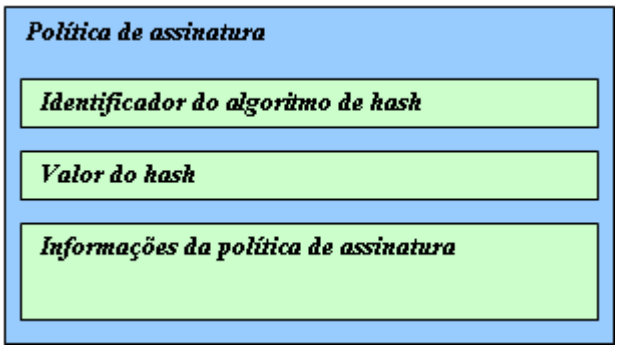

Figura 15 - Atributos de uma política de assinatura.

O identificador do algoritmo de *hash*, bem como seu valor, são parâmetros que são usados pelo signatário ou pelo verificador da assinatura para assegurar a integridade da política de assinatura.

O atributo informações da política de assinatura deve conter os seguintes atributos:

- **Identificador da política**. Este atributo contém um código de identificação da política de assinatura, por exemplo, um OID (*Object Identifier*), ou um número

inteiro que identifique uma versão da política de assinatura;

- **Data de emissão**. Este atributo contém a data de publicação da política de assinatura;
- **Nome do Emissor**. Este atributo contém a identificação da entidade geradora da política de assinatura, que pode ser usado pelo signatário ou verificador da assinatura para verificar a origem (procedência) da política de assinatura;
- **Contexto de aplicação**. Este atributo contém a informação do contexto do negócio para o qual a política está definida. Com este atributo, é possível determinar o contexto do documento para o qual a política está associada, por exemplo, documentos gerados em um contexto comercial ou em um contexto jurídico;
- **Política de validação de assinatura**. Este atributo contém as regras para geração e verificação de uma assinatura digital e está detalhado a seguir.

A Figura 16 ilustra os atributos de uma política de assinatura e os atributos que devem estar contidos no atributo informações da política de assinatura.

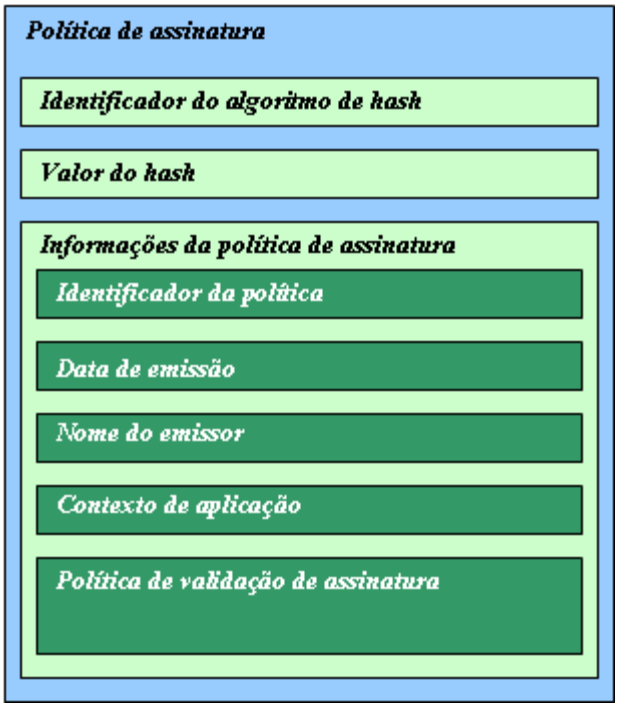

Figura 16 - Política de assinatura e o atributo informações da política de assinatura.

As regras que definem os requisitos técnicos para geração e verificação da assinatura são elementos do atributo política de validação de assinatura, o qual deve conter os seguintes atributos:

- **Período de validade**. Este atributo define a partir de que instante a política de assinatura poderá ser utilizada. Além disso, também define, opcionalmente, a partir de que instante a política não terá mais validade para utilização;
- **Regras comuns**. Este atributo define o conjunto de regras para geração e verificação de assinaturas digitais. Tais regras devem ser seguidas para qualquer tipo de assinatura que venha ser realizada neste contexto;
- **Regras para propósito específico**. Este atributo define uma seqüência do atributo regra para propósito específico. Os mesmos atributos contidos no atributo regras comuns estão presentes neste atributo, porém para um propósito de assinatura específico. Por esta razão, este objeto possui um elemento que define tal propósito,

chamado de propósito de assinatura. Alguns exemplos de propósitos de assinatura são apresentados no capítulo 3. Para o formato eletrônico do propósito, é necessário que cada tipo de propósito possua uma identificação. No o caso da notação ASN.1 esta identificação pode ser um OID (*Object Identifier*).

A Figura 17 ilustra o conteúdo do atributo política de validação.

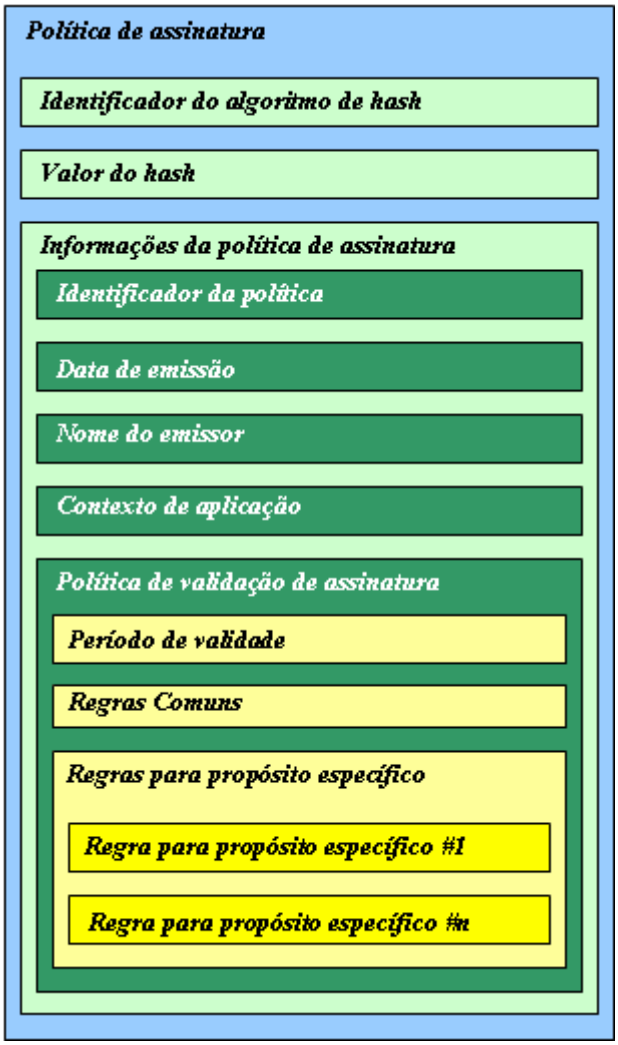

Figura 17 - Política de assinatura e o atributo política de validação de assinatura.

As regras definidas no atributo regras comuns não devem conflitar com as regras definidas no atributo regras para propósito específico. Por esta razão, deve existir uma atenção especial no momento de criação da política com intuito de não gerar regras conflitantes.

Os seguintes atributos devem estar contidos nos atributos regras comuns e regra para

propósito específico:

- Geração da assinatura e verificação da assinatura;
- Condições de confiança para o certificado do signatário;
- Condições de confiança para o carimbo de tempo;
- Condições de confiança para certificado de atributo[17];
- Regras para algoritmos e tamanhos de chaves permitidos;
- Extensões para definições futuras.

A Figura 18 ilustra o conteúdo do atributo regras comuns.

[17] Um certificado de atributo, segundo por Farrell e Housley (2002), é como um certificado digital que associa, de forma direta ou indireta, um conjunto de informações a uma entidade final. Este conjunto de informações contém atributos que determinam associações a grupos, papéis, privilégios de segurança ou qualquer outra informação associada ao proprietário do certificado.

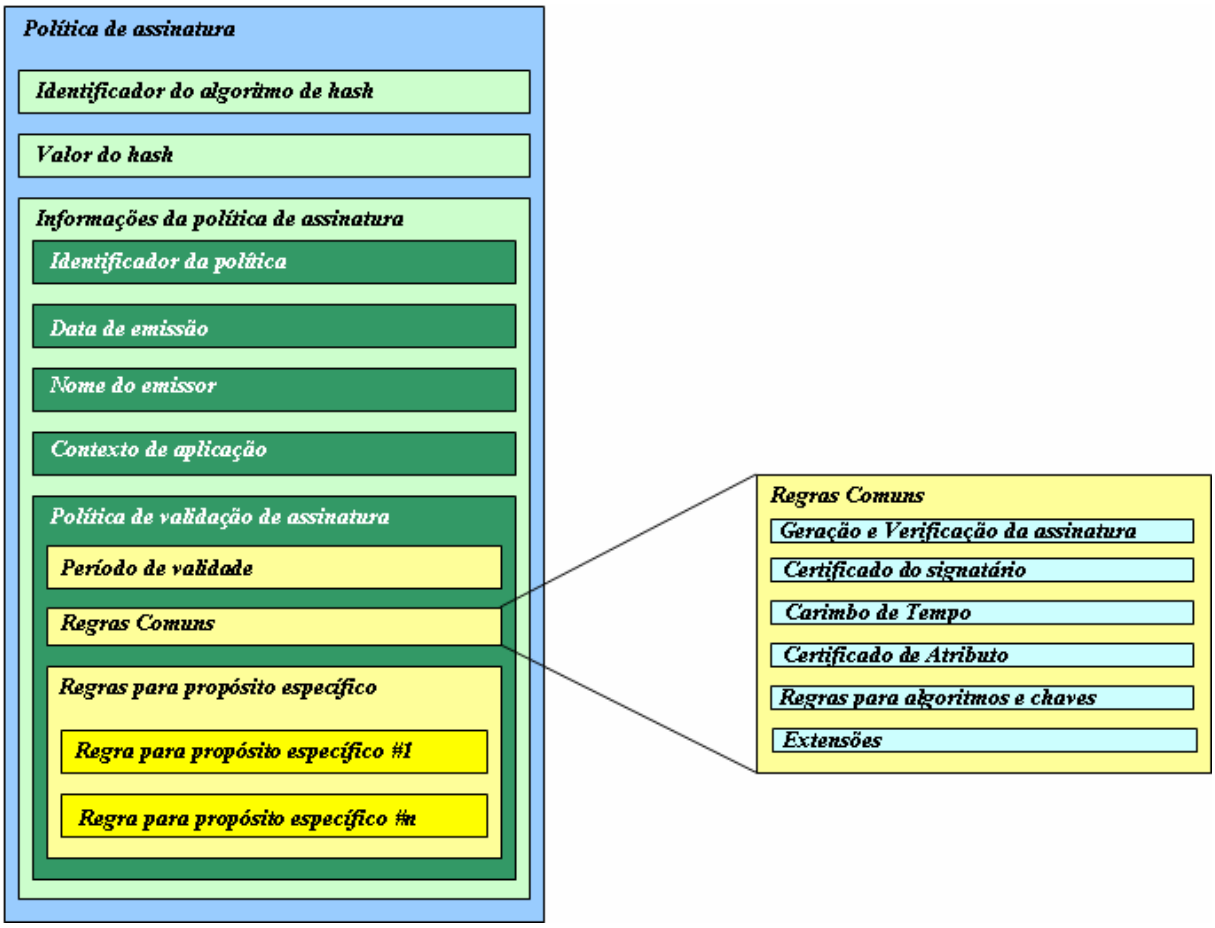

Figura 18 - Política de assinatura e o atributo regras comuns.

A Figura 19 ilustra o conteúdo do atributo regra para propósito específico, que possui um atributo especial para definição do propósito.

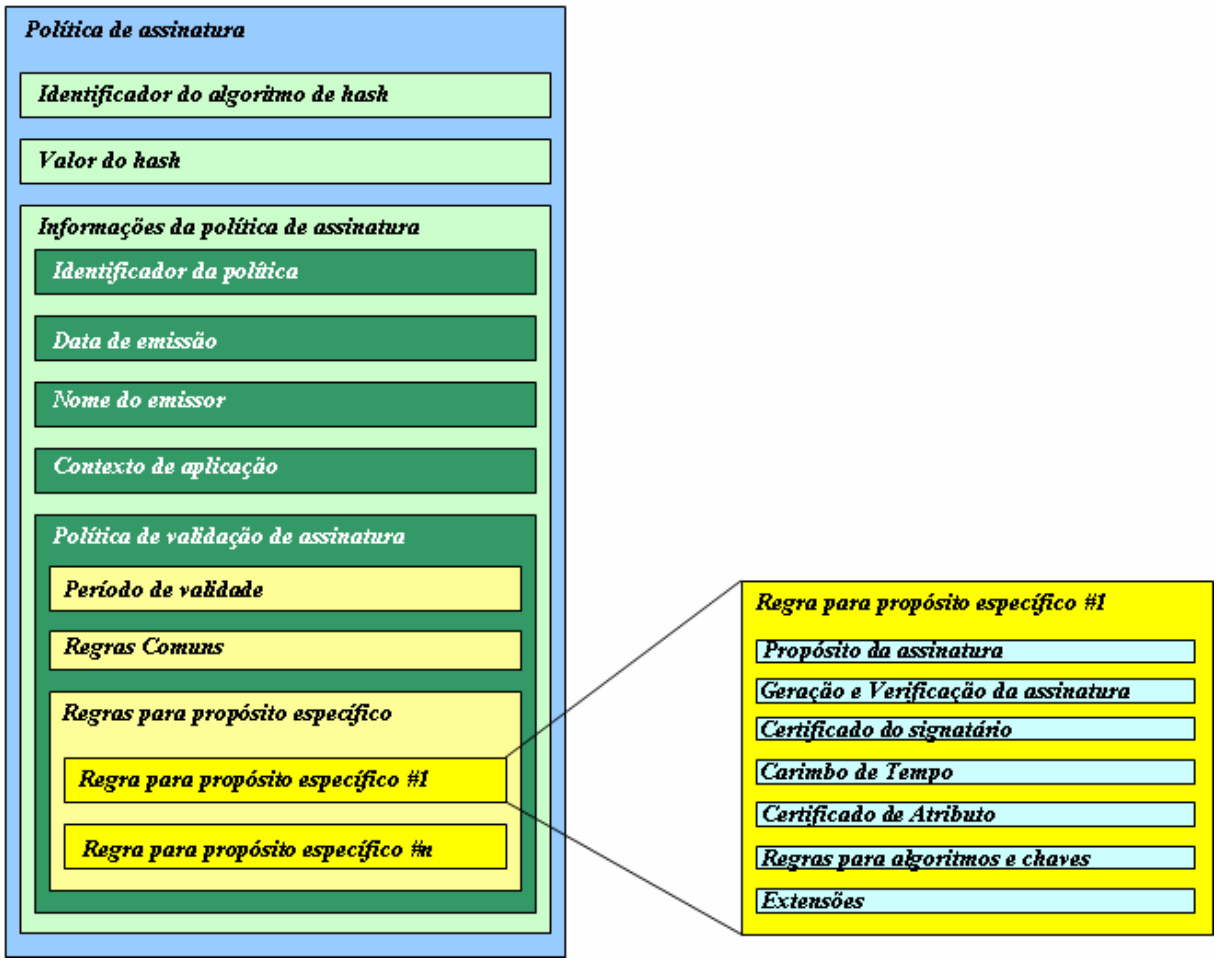

Figura 19 - Conteúdo do atributo regra para propósito específico.

A seguir são detalhados os atributos que devem estar contidos no atributo regras comuns e no atributo regra para propósito específico.

6.2.1. Geração e verificação da assinatura

Este atributo deve conter o atributo para geração e outro para verificação da assinatura. As regras para geração de assinatura digital são definidas através dos seguintes atributos:

- **Invólucro com documento incluído ou excluído**. Indica se o documento assinado digitalmente está incluído ou não no invólucro. (ver seção 5.3);

- **Conjunto de atributos autenticados**. Permite selecionar quais atributos autenticados são requeridos para geração da assinatura;
- **Conjunto de atributos não autenticados**. Permite selecionar quais atributos não autenticados são requeridos para a geração da assinatura;
- **Certificado do signatário**. Define quais os certificados ou referências de certificados devem ser incluídos no invólucro. É possível incluir o certificado do signatário, a cadeia de certificação completa ou nenhum certificado;
- **Extensões**. Permite definir regras futuras para geração de assinatura.

As regras para verificação da assinatura são definidas através dos seguintes atributos:

- **Conjunto de atributos não-autenticados**. Permite selecionar quais atributos não autenticados são requeridos caso não tenham sido adicionados ao invólucro no momento de geração da assinatura;
- **Extensões**. Permite definir regras futuras para geração de assinatura.

6.2.2. Condições de confiança para o certificado do signatário

As condições de confiança de um certificado digital dependem da validação da cadeia de certificação e do estado de revogação do certificado, e seus atributos são:

- **Condições de confiança quanto à cadeia de certificação**. Permite definir regras de confiança quanto ao certificado raiz, tamanho máximo do caminho de certificação, política de certificação.
- **Regras para verificação do estado de revogação do certificado**. Permite selecionar o mecanismo de verificação do estado de revogação[18] do certificado digital. As regras para verificação do estado de revogação podem ser divididas em duas partes: regras para o certificado da entidade final e regras para o certificado das ACs.

6.2.3. Condições de confiança para o carimbo de tempo

O carimbo de tempo é um selo de tempo adicionado como atributo não autenticado ao bloco de informação de assinatura digital, e seus atributos são:

- **Regras para verificação do certificado da ACT**. Este atributo contém as regras que permitem verificar as condições de confiança do certificado digital da Autoridade de Carimbo de Tempo. A seção 6.2.2 apresenta os atributos que são usados para verificar a cadeia de certificação do certificado da ACT;
- **Regras para verificação do estado de revogação do certificado da ACT**. Este atributo contém as regras que permitem verificar o estado de revogação do

[18] Alguns mecanismos de revogação são apresentados na seção 4.4

certificado digital da ACT. A seção 6.2.2 apresenta os atributos que são usados para verificar o estado de revogação do certificado da ACT;

- **Regras para o período de tolerância**. Este atributo permite definir quanto tempo deve ser aguardado, após o instante definido no carimbo de tempo, para obter a LCR e verificar o estado de revogação do certificado do signatário. A seção 4.4.1 apresenta a motivação para o uso deste atributo;
- **Intervalo máximo de tempo permitido entre os instantes de tempo definidos pelos atributos *SigningTime* e Carimbo de Tempo**. Este atributo, se definido, permite considerar o tempo informado pelo signatário para geração da assinatura (*SigningTime*) para compará-lo com o instante de tempo definido no atributo de carimbo de tempo. A assinatura pode ser considerada inválida se o intervalo tempo obtido ultrapassar o tempo máximo permitido neste atributo.

6.2.4. Condições de confiança para o certificado de atributo

Um certificado de atributo é usado para definir um papel de uma entidade, organização o grupo por um determinado período do tempo. A seguir são listados os atributos usados como parâmetros para validar um certificado de atributo.

- **Regras para verificação do certificado de atributo**. Este atributo contém as regras que permitem verificar as condições de confiança do certificado de atributo. A seção 6.2.2 apresenta os atributos que são usados para verificar a cadeia de certificação do certificado de atributo;
- **Regras para verificação do estado de revogação do certificado de atributo**.

Este atributo contém as regras que permitem verificar o estado de revogação do certificado do certificado de atributo. A seção 6.2.2 apresenta os atributos que são usados para verificar o estado de revogação do certificado de atributo;

6.2.5. Condições para algoritmos e tamanhos de chaves

A definição do algoritmo de criptografia e o tamanho de chave também são elementos definidos através de uma política de assinatura.

6.3. PROCESSO DE USO DA POLÍTICA DE ASSINATURA

A política de assinatura é utilizada no momento de geração da assinatura e no momento de verificação da assinatura.

No momento de geração da assinatura, o signatário deve selecionar a política emitida para o contexto do documento. Em seguida, o usuário deverá verificar o *hash* da política da assinatura para verificar a integridade da política. Além disso, o signatário poderá verificar a identificação da política e o nome da entidade emissora. Após a aceitação da política, o software de assinatura poderá interpretar a política codificada e gerar a assinatura de acordo com as regras definidas. Para isso, o usuário deverá também informar o propósito de sua assinatura a fim de que possam ser aplicadas as regras definidas na política de acordo com o propósito. O propósito da assinatura e o identificador da política devem ser assinados juntamente com o documento.

A mesma política utilizada para gerar a assinatura deve ser utilizada no momento de

verificar a assinatura. Da mesma forma que no momento da geração da assinatura, o usuário que fará a verificação da assinatura deve verificar a integridade e a entidade emissora da política. Em seguida, o software de assinatura digital deve interpretar a política codificada e a partir do conjunto de requisitos definidas verificar a assinatura digital.

7. PROPOSTA PARA POLÍTICA DE ASSINATURA

Este capítulo apresenta uma proposta que estende o modelo de política de assinatura proposto pelo ETSI, *o Signature Policy Extension* (SIPEX). No modelo que será apresentado, estão contemplados extensões para suportar requisitos de relacionamento entre assinaturas geradas no documento e autenticação de política de assinatura.

O relacionamento entre assinaturas pode ser usado com intuito de atender alguns requisitos para geração da assinatura digital, como por exemplo, a ordem de geração das assinaturas no documento.

A autenticação da política de assinatura pode ser usada para assegurar as informações contidas na política e a identificação da entidade que a gerou antes da sua utilização para gerar e verificar assinaturas digitais.

7.1. EXTENSÃO PARA RELACIONAMENTO ENTRE ASSINATURAS

O modelo proposto pelo ETSI contempla a definição de requisitos que devem ser seguidos durante a realização ou verificação de uma determinada assinatura digital, independentemente das outras assinaturas existentes, ou que serão realizadas em um documento. No entanto, existem alguns requisitos, relacionados à geração e à verificação da assinatura, que envolvem o relacionamento entre as assinaturas digitais presentes em um documento. São exemplos de requisitos:

- **Ordem de geração de assinaturas**. A ordem de realização das assinaturas em um documento pode ser um requisito necessário, dependendo do contexto.

Geralmente, as assinaturas em um documento podem ser realizadas em paralelo. Neste caso, não existe nenhum tipo de requisito para a ordem de realização da assinatura. Porém, podem existir situações nas quais seja importante exigir que a realização de uma determinada assinatura digital dependa de uma outra assinatura digital pré-existente no documento, ou seja, seja realizada somente após a geração de uma determinada assinatura. Por exemplo, no contexto de uma empresa, a assinatura de uma autorização pode ser precedida por uma outra assinatura referente ao pedido. A definição da ordem de geração da assinatura pode estar relacionada com os propósitos de assinatura requeridos ou ainda aos papéis[19] de cada entidade. Existem situações nas quais pode ser necessário estabelecer algum tipo de ordem para assinaturas com mesmo propósito, porém com os papéis distintos. Um papel pode ser definido como uma função que uma entidade pode assumir por um período de tempo;

- **Quantidade de assinaturas mínimas**. Para cada tipo de propósito pode ser necessária a realização de mais de uma assinatura. Existem situações, por exemplo, que são requeridas duas assinaturas de testemunhas. Além da quantidade de assinatura por propósito, pode ser necessária a realização de mais de uma assinatura com mesmo propósito, porém com papeis diferentes. Por exemplo, pode ser um requisito do negócio a assinatura de no mínimo dois procuradores de uma

[19] A atribuição de papel da entidade pode ser realizada através de um certificado de atributo associado ao certificado digital de chave pública.

empresa e uma assinatura de uma entidade mediadora do negócio. Neste caso, todas as assinaturas possuem propósito compromissivo, porém com papéis distintos;

- **Vínculo temporal entre as assinaturas**. De acordo com o contexto, pode ser um requisito que as assinaturas sejam realizadas dentro de um intervalo de tempo definido. Por exemplo, alguns tipos de contratos precisam ser assinados no mesmo dia.

Cada um dos exemplos mencionados acima define algum tipo de requisito relacionado ao relacionamento entre as assinaturas. Este relacionamento poderia ser modelado em um sistema de *workflow*[20] sem a necessidade específica de uma política de assinatura para o fluxo de geração das assinaturas. No entanto, a implementação destes controles em um sistema de *workflow* poderia torná-lo muito específico para um determinado contexto (LEUNG; HUI, 2000). Além disso, não seria possível, no momento futuro de verificação das assinaturas do documento, ter conhecimento de quais são as restrições que devem ser verificadas.

A proposta do modelo estendido para política de assinatura permitiria a um sistema de *workflow* utilizar o conjunto de regras definido na política de assinatura para execução do procedimento adequado definido no fluxo. Assim, seria possível implementar um sistema de controle de fluxo de documentos baseado em assinatura para tomada de decisão.

---

[20] Workflow é nome dado para automação de processos de negócio, onde as atividades são passadas de um participante para o outro de acordo com um conjunto de regras definidas.

Com relação à ordem de geração das assinaturas, podem ser geradas de regras simples até regras mais complexas como, por exemplo, ordem de assinatura baseada em propósitos e em papéis. A Figura 20 ilustra um exemplo de relacionamento entre assinaturas quanto à ordem de criação das assinaturas baseado no propósito da assinatura

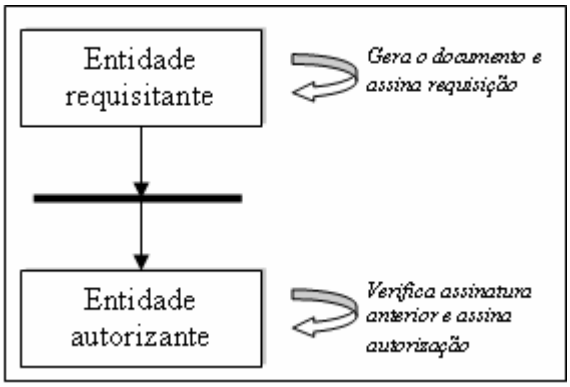

Figura 20 - Ordem de geração das assinaturas baseado em propósito de assinatura.

Outro exemplo quanto à ordem de criação pode estar baseado não somente nos propósitos de assinatura mas também nos papéis das entidades signatárias. A Figura 21 ilustra um exemplo de uma transação comercial com dependência de relacionamento entre as assinaturas quanto à ordem de criação, baseado tanto em propósito de assinatura quanto em papéis das entidades.

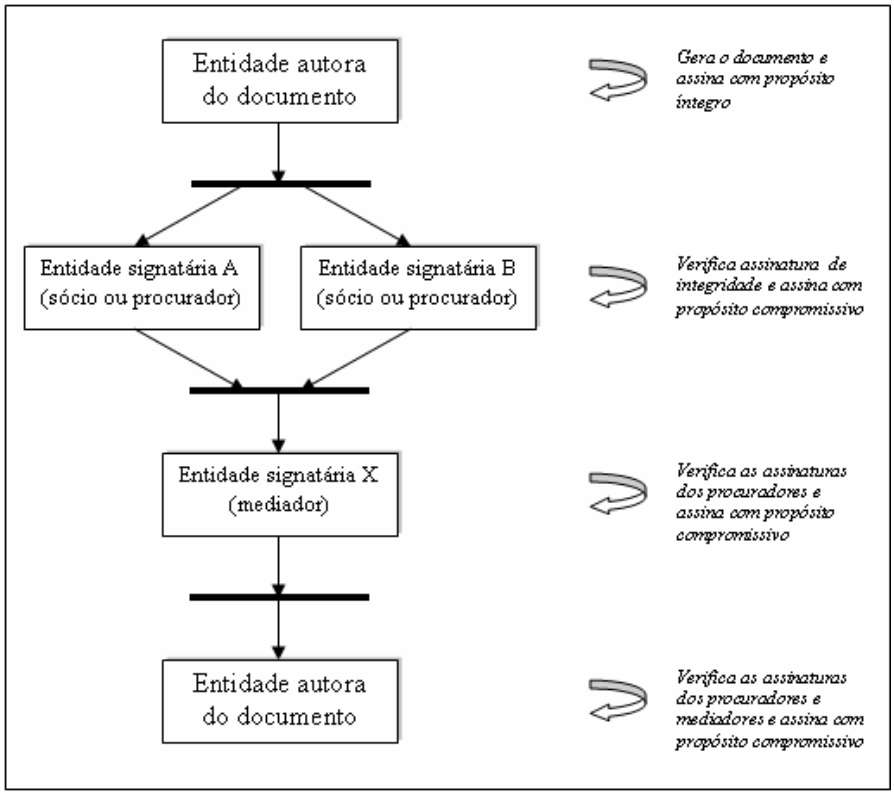

Figura 21 - Ordem de geração das assinaturas baseado em papéis e propósitos de assinatura.

A figura reflete um exemplo de transação comercial com os seguintes requisitos de negócio para geração da assinatura:

- O documento deve conter as assinaturas dos sócios ou procuradores das entidades assinantes, a assinatura de uma entidade mediadora da transação e a assinatura da entidade autora do documento;
- A entidade autora do documento deve disponibilizar o documento para os respectivos signatários;
- As assinaturas dos procuradores podem ser realizadas em paralelo, após a assinatura da entidade autora do documento;
- A assinatura da entidade mediadora somente pode ser realizada após a realização da assinatura dos procuradores das entidades signatárias;
- A assinatura da entidade autora do documento somente pode ser realizada após a

realização de todas as assinaturas.

De acordo com o exemplo, a entidade autora do documento gera a assinatura em dois momentos diferentes com propósitos diferentes. No primeiro momento, a assinatura gerada tem o propósito de garantir a integridade do documento[21]. Esta assinatura tem como objetivo assegurar a autenticidade, a origem e a integridade do documento perante para as entidades signatárias do documento. Esta assinatura poderia ser a assinatura compromissiva da entidade autora. No entanto, conforme descrito na regra de negócio, esta entidade somente poderá realizar sua assinatura ao final do processo.

Em seguida, as entidades signatárias do documento realizam a assinatura. Nota-se que a condição de realização de assinatura destas entidades depende do sucesso da verificação da assinatura com propósito íntegro da entidade autora do documento. A assinatura com propósito íntegro permite verificar não somente a integridade das informações que estão sendo assinadas, mas também a procedência destas informações.

A próxima etapa coincide com a assinatura da entidade mediadora da transação. A realização da assinatura, de acordo com os requisitos do negócio, depende da verificação das assinaturas dos procuradores das entidades signatárias A e B. Nota-se que existe uma condição de ordem de realização das assinaturas baseada nos papéis, ou seja, as assinaturas dos procuradores devem ser realizadas antes da assinatura do mediador. Neste caso, o propósito das três assinaturas é o mesmo.

---

[21] Propósito de assinatura íntegro (ver seção 3.2.2).

Finalmente, a entidade autora do documento, por condição do negócio, gera sua assinatura compromissiva, uma vez que todas as assinaturas necessárias para o documento foram realizadas.

A seguir será apresentada a proposta do que estende modelo de política de assinatura definido pelo ETSI para atender aos requisitos de relacionamento entre assinaturas quanto à sua geração.

7.1.1. Proposta do modelo de política de relacionamento entre assinaturas

De acordo com a modelo de política de assinatura do ETSI, discutido na seção 6.2, o atributo regras comuns contém entre seus elementos as condições de confiança para criação e verificação de uma assinatura, cadeia de certificação, estado de revogação, carimbo de tempo e algoritmos e tamanhos de chaves.

Visto que o atributo regras comuns define o conjunto de requisitos comuns para todas as assinaturas do documento, este atributo poderia conter também as regras para o relacionamento de geração de assinaturas do documento. Além disso, este atributo já possui definido em sua especificação original, um atributo reservado para extensões.

Este trabalho propõe a criação do atributo regras de relacionamento como extensão do atributo regras comuns. A Figura 22 ilustra o encapsulamento do atributo regras de relacionamento no modelo original de política de assinatura:

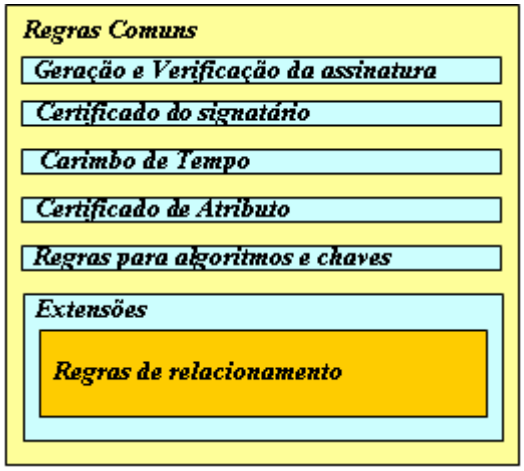

Figura 22 - Encapsulamento do atributo regras de relacionamento.

O atributo regras de relacionamento deve conter os seguintes atributos:

- **Ordem de geração**. Atributo que contém as regras para definição da ordem de geração de assinaturas por propósito e por papel definido por certificado de atributo;
- **Vínculo temporal**. Atributo que contém as regras para definição de vínculo temporal para geração das assinaturas.
- **Extensões**. Atributo definido para futuras regras de relacionamento entre assinaturas.

7.1.1.1. Atributo ordem de geração

A ordem de geração de assinatura define um conjunto de atributos que identificam uma classe de signatário. A relação de dependência é estabelecia entre as classes de signatários definida, ou seja, qual classe de signatário deve realizar a assinatura antes de uma outra classe. Uma classe de signatário é formada pelos papéis que uma entidade pode assumir, o propósito da assinatura e a quantidade mínima de assinaturas desta classe. Cada classe deve possuir uma identificação única a fim de possibilitar a criação das regras de dependência. O exemplo ilustrado na Figura 21 possui quatro classes de signatário. A Tabela 2 lista estas

classes e os respectivos atributos.

Tabela 2 – Atributos das classes de signatários.

Identificação da classe	Papel	Propósito	Quantidade de assinaturas
Classe A	Autora	Íntegro	1
Classe B	Sócio ou procurador	Compromissivo	2
Classe C	Mediador	Compromissivo	1
Classe D	Autora	Compromissivo	1

De acordo com as informações das classes de signatário é possível definir uma ordem de realização das assinaturas baseada na identificação das classes. A Figura 23 ilustra a relação de dependências entre as classes de acordo com o fluxo de negócio do exemplo.

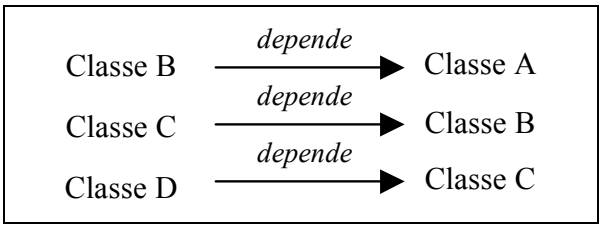

Figura 23 - Dependência de ordem entre as classes de signatários.

O atributo ordem de geração deve conter os seguintes atributos:

- **Classes de signatários**. Este atributo deve conter as classes de signatários possíveis para o documento. Uma classe de signatário é composta por:
  - **Identificação da classe**. Este atributo define uma identificação única para a classe de signatário na política;
  - **Papéis da entidade**. Este atributo identifica os papéis assumidos por uma entidade dentro da classe de signatário. Um papel pode ser definido, por

exemplo, através de um certificado de atributo;

- **Propósito da assinatura**. Este atributo identifica o propósito da assinatura da classe de signatário;
- **Quantidade de assinaturas**. Este atributo define a quantidade mínima e máxima de assinaturas dentro da classe de signatário.

- **Dependências**. Este atributo descreve as regras de dependência entre as classes de signatários. O atributo dependências deve conter:
  - **Identificação da classe.** Este atributo contém a identificação da classe definida no atributo de classe de signatário;
  - **Dependência.** Este atributo contém a identificação da classe de signatário dependente.

Na verificação da assinatura, se existir o atributo que define a ordem para geração das assinaturas, deverá ser considerado o instante de realização das assinaturas para verificar o cumprimento do requisito no momento da geração. A referência do instante de tempo deverá ser o carimbo de tempo ou o atributo *SigningTime,* nesta ordem.

7.1.1.2. Atributo vínculo temporal

O atributo vínculo temporal estabelece o instante de tempo máximo para a realização das assinaturas do documento. Para isso, este atributo contém uma referência de tempo para validar os instantes de realização da assinatura. O parâmetro para o instante de realização da assinatura pode ser obtido a partir do carimbo de tempo ou do atributo autenticado *SigningTime* de cada assinatura.

O atributo vínculo temporal contém os seguintes atributos:

- **Referência de tempo**. Este atributo define se a referência de tempo para o instante

de realização da assinatura será o atributo autenticado SigningTime ou o carimbo de tempo;

- **Instante máximo**. Este atributo define o instante máximo de tempo para realização das assinaturas.

A Figura 24 ilustra todos os atributos propostos para as regras de relacionamento.

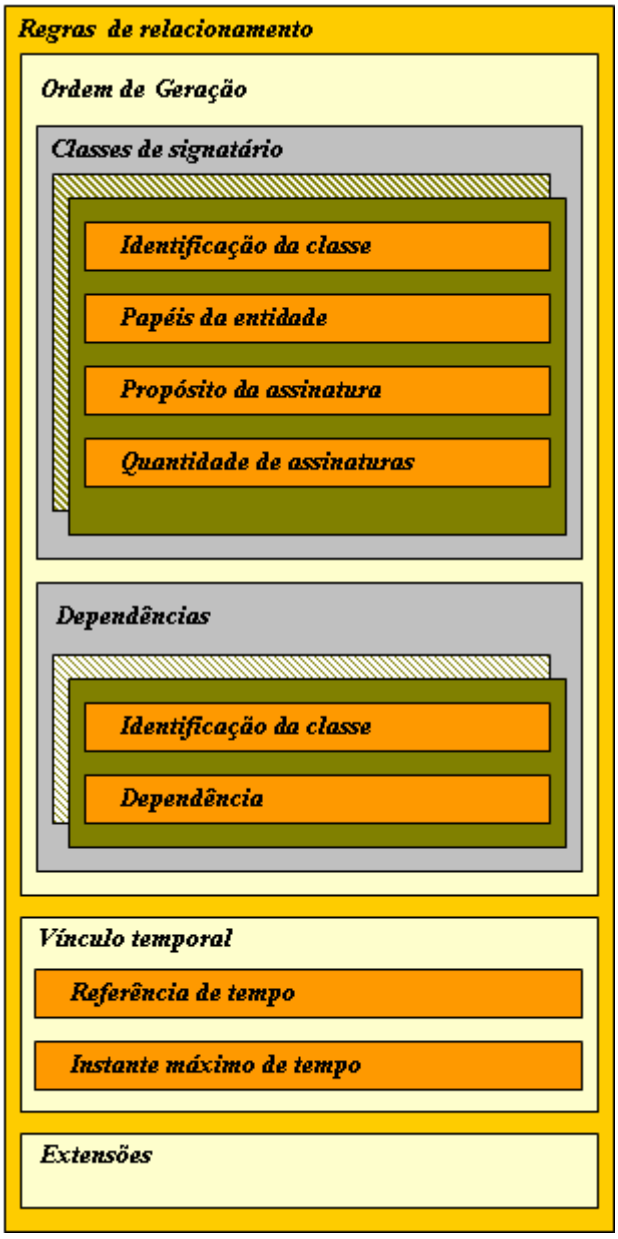

Figura 24 - Conteúdo do atributo regras de relacionamento.

7.2. AUTENTICAÇÃO DA POLÍTICA DE ASSINATURA

O modelo de política de assinatura proposto pelo ETSI, descrito no capítulo anterior, utiliza alguns atributos definidos na própria política para assegurar a integridade da política e a identificação da entidade que a gerou. Conforme apresentado no capítulo anterior, uma política de assinatura possui um atributo que define o resumo criptográfico da própria política. Além destes, uma política possui o atributo de identificação do seu emissor. Com estes elementos é possível para um usuário da política da assinatura verificar a integridade e a identificação da entidade emissora da política

Entretanto, este tipo de verificação não provê garantia quanto à autoria das informações contidas na política de assinatura. Uma alternativa para isso é adicionar um atributo ao modelo proposto pelo ETSI para contemplar a assinatura digital da política pela entidade emissora. A garantia da autoria pode ser um requisito importante para o uso de política de assinatura, afinal o usuário que gera ou verifica uma assinatura usando o modelo de políticas de assinatura, precisa concordar com as regras definidas na política. O signatário ao fazer uso da política da assinatura, também assina, como um atributo autenticado, a identificação da política de assinatura. Daí a importância da garantia de autoria da política. Além disso, a assinatura da política de assinatura permite para uma terceira entidade realizar a verificação das assinaturas no futuro com garantia de autenticidade quanto às regras definidas na política de assinatura utilizada para gerar a assinatura.

Com o objetivo de assegurar a autenticidade de uma política de assinatura, este trabalho estende o modelo proposto pelo ETSI e propõe a criação de um novo atributo no contexto da política de assinatura, a assinatura da política.

A Figura 25 ilustra a adição do atributo assinatura da política.

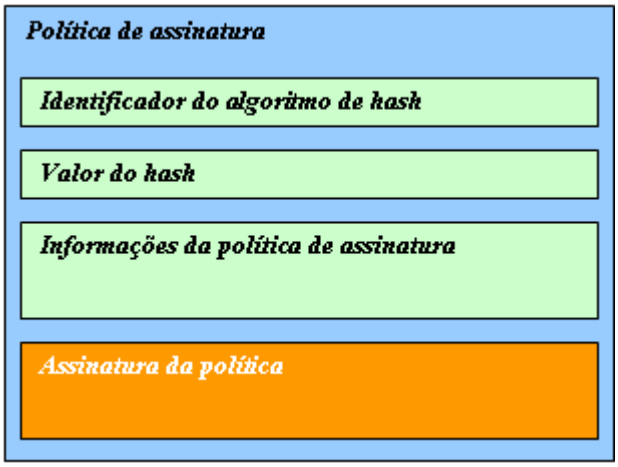

Figura 25 - Atributo assinatura da política.

A assinatura da política de assinatura deve ser realizada pela entidade que define a política de assinatura para o contexto do documento.

Além da adição do atributo de assinatura da política, pode ser necessário criar o atributo que define o conjunto de regras e condições para verificação da assinatura da política. Para isso, poderiam ser definidos, no conteúdo do atributo regras comuns, atributos para especificar o conjunto de requisitos para validar a assinatura da própria política.

7.2.1. Ciclo de vida da política de assinatura autenticada

O ciclo de vida da política de assinatura autenticada divide-se em três partes: a geração da política, o uso da política para geração da assinatura e o uso da política para verificação da assinatura. O signatário antes de usar uma política de assinatura para geração de uma assinatura, deve seguir as seguintes etapas:

- Verificar a assinatura da entidade emissora da política;
- Visualizar a política de assinatura;
- Aceitar o uso da política;

- Extrair os parâmetros para geração da assinatura;
- Gerar a assinatura do documento.

Para usar uma política de assinatura para verificar uma assinatura digital, o usuário deve seguir as seguintes etapas:

- Identificar a política de assinatura utilizada para geração da assinatura;
- Verificar a assinatura da entidade emissora da política;
- Extrair os parâmetros de verificação da assinatura.

8. ESTUDO DE CASO

Com o objetivo de avaliar a aderência do modelo de política de assinatura, foram selecionados dois contextos de assinatura de documentos distintos. O primeiro está relacionado com o contexto jurídico que, na órbita dos atos processuais, ocorre com certa freqüência, o mando de citação. Já o segundo, está inserido em contexto comercial, o contrato de câmbio.

Para ambos os contextos, serão apresentados os conceitos relacionados a cada tipo de documento e de que forma uma política de assinatura poderia ser utilizada para gerar e verificar as assinaturas nestes documentos.

8.1. POLÍTICA DE ASSINATURA PARA CITAÇÃO JUDICIAL

De acordo com o Código de Processo Civil, citação é o ato pelo qual se chama a juízo o réu ou o interessado a fim de se defender[22]. Dentre os tipos de citação existentes, a mais comum é a citação real ou pessoal.

Segundo RANGEL (2002), o mandado de citação é formado pelos seguintes

[22] Artigo 213 do Código do Processo Civil.

elementos:

- O nome do juiz e a indicação do juízo (tribunal responsável);
- Se a ação for iniciada por meio de queixa, o nome do querelante (vítima ou seu representante legal);
- O nome do citado ou, se desconhecido, os seus sinais identificadores; (alcunha, descrição física);
- Os endereços do citado, se conhecido;
- O juízo, o lugar, a data e a hora em que o citado deverá comparecer;
- A subscrição (geração do texto) pelo escrivão (gera e assina); e
- A assinatura do juiz (responsável pelas informações contidas no texto da citação).

Além destes, são considerados elementos extrínseco do mandado de citação a entrega da cópia de inteiro teor do mandado para o citado. O citado lê, assina e entrega a contrafé do mandado para o oficial de justiça. O oficial de justiça adiciona um texto no verso ou ao pé do mandado informando o cumprimento das formalidades, ou seja, a entrega do mandado para o citado. Após a adição do texto, o oficial de justiça assina a mensagem por ele gerada.

O fluxo representado pela Figura 26 ilustra as etapas de geração e entrega do mandado de citação.

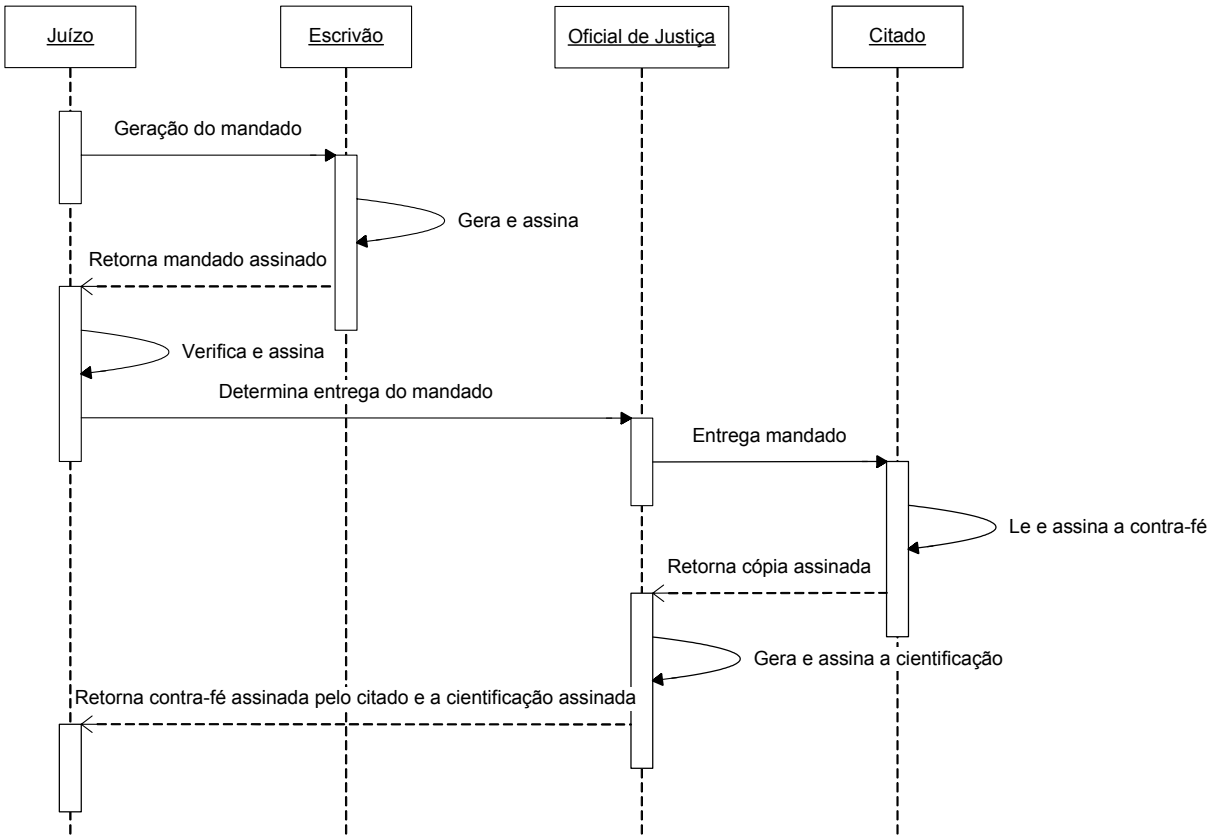

Figura 26 - Fluxo do mandado de citação

8.1.1. Propósito das assinaturas no mandado de citação

Cada assinatura realizada sobre o mandado possui um propósito distinto de acordo com o papel de cada signatário no documento, a saber:

- **Escrivão**. Assina o mandado de citação como responsável pela produção do documento. Esta assinatura pode ser classificada com o propósito autoral.
- **Juiz**. Assina o mandado após conferir o conteúdo do documento gerado pelo escrivão. O juiz assina como responsável pelo ato. Esta assinatura pode ser classificada com o propósito compromissivo.
- **Citado**. Assina o mandado após ler o conteúdo do documento e dá ciência. A

partir do instante da realização da assinatura do citado, inicia-se o prazo para apresentação da defesa. Esta assinatura pode ser classificada com propósito ciente.

- **Oficial de Justiça**. Assina o termo de ciência gerado no verso da contrafé assumindo responsabilidades sobre o cumprimento da formalidade. Esta assinatura pode ser classificada com o propósito compromissivo.

8.1.2. Política de assinatura para o mandado de citação eletrônico

A citação no formato eletrônico apresenta como vantagem a minimização da morosidade processual. Isto porque o processo de cumprimento de entrega do mandado no formato eletrônico pode ser mais ágil. No entanto, como se trata de um documento com validade legal, é necessário que o formato eletrônico para o mandado de citação apresente as características de integridade e autenticidade, do mesmo modo como apresentado em relação aos contratos no capítulo 2.

A assinatura digital possui as características necessárias para assegurar as características de integridade e autenticidade do mandado de citação. Apesar disso, é necessário que seja explicitado quais os elementos e requisitos técnicos são necessários para a geração das assinaturas necessárias no mandado de citação.

Aplicação do SIPEX para o mandado de citação eletrônico provê o meio para definir os requisitos técnicos para a realização das assinaturas do mandado. A Tabela 3 é um exemplo dos requisitos para definir uma política de assinatura para o mandado de citação eletrônico.

Tabela 3 - Exemplo de política de assinatura para o mandado de citação.

Atributo da política	**Valor**
Contexto de aplicação	Mandado de Citação
Emissor da política	Órgão jurídico competente
Documento incluído no invólucro	Sim
Atributo não autenticado obrigatório	Carimbo de tempo
Condições de confiança do certificado dos signatários	AC Raiz Brasileira
Mecanismo de verificação do estado de revogação dos certificados	Lista de certificados revogados
Algoritmos e tamanhos de chaves	Chave RSA com no mínimo 1024 bits de tamanho
Ordem de geração das assinaturas	Definida através das classes de signatários na seguinte ordem: Escrivão – Juiz – Citado – Oficial de justiça
Quantidade de assinaturas	No mínimo uma por classe de signatário
Vínculo temporal	As assinaturas devem ser realizadas 10 dias após a realização da primeira assinatura do mandado

Além, das regras definidas, o SIPEX provê uma forma de assegurar para os signatários do mandado de citação a autenticidade da política de assinatura. Desta forma, cada assinante, antes de usar a política em seu software de assinatura, verifica a assinatura da política.

De acordo com os signatários do mandado de citação, podem ser definidas quatro classes de signatários. A Tabela 4 lista os atributos das classes.

Tabela 4 - Classes de signatários do mandado de citação.

Identificação da classe	**Papel**	**Propósito**	**Quantidade de assinaturas**
Classe A	Juiz	Compromissivo	1
Classe B	Escrivão	Autoral	1
Classe C	Citado	Ciente	1
Classe D	Oficial de justiça	Compromissivo	1

De acordo com a ordem de geração das assinaturas, a relação de dependência para geração da assinatura é ilustrada na Figura 27.

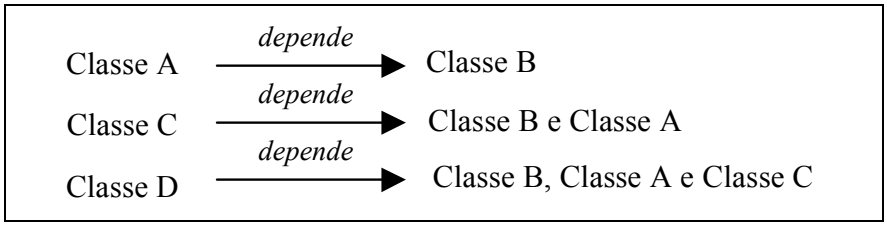

Figura 27 - Dependência de ordem entre as classes de signatários do mandado de citação.

8.2. POLÍTICA DE ASSINATURA PARA CONTRATOS DE CÂMBIO

Para o caso da assinatura digital em contratos de câmbio, é possível através de uma política de assinatura definir os requisitos legais e os requisitos do negócio.

Quanto ao requisito legal, é necessário que o documento eletrônico que representa o contrato de câmbio possua as assinaturas das partes envolvidas, que geralmente são um cliente, uma corretora e um banco interveniente da transação comercial de câmbio. Os requisitos técnicos de um contrato de câmbio assinado digitalmente devem estar de acordo com a carta circular definida pelo BANCO CENTRAL DO BRASIL (2004). Neste caso, não existe requisito legal para a ordem de geração das assinaturas.

Os requisitos de negócio podem variar de acordo com cada instituição. Um dos requisitos pode ser que a o banco seja a última parte para realizar a assinatura.

Em termos práticos, a entidade responsável pela geração do contrato, no caso o banco, envia o documento para os signatários responsáveis para assinatura. Opcionalmente, antes do envio do documento para os assinantes, o banco pode gerar uma assinatura com propósito íntegro sobre o contrato com o objetivo de assegurar a integridade e origem do contrato para

os signatários. Desta forma, os signatários do contrato, antes de gerarem as respectivas assinaturas, devem verificar a assinatura de integridade do banco. A ordem de geração de assinatura, neste caso, poderia ser baseada nos dois tipos de propósitos de assinatura existentes, ou seja, assinatura com propósito íntegro sendo realizada antes das assinaturas com propósito compromissivo. As assinaturas dos clientes podem ser realizadas em paralelo.

Tabela 5 - Exemplo de política de assinatura para contratos de câmbio.

Atributo da política	**Valor**
Contexto de aplicação	Contrato de câmbio eletrônico
Emissor da política	Instituição financeira
Documento incluído no invólucro	Não
Atributo não autenticado obrigatório	Carimbo de tempo
Condições de confiança do certificado dos signatários	AC Raiz Brasileira
Mecanismo de verificação do estado de revogação dos certificados	Lista de certificados revogados
Algoritmos e tamanhos de chaves	Chave RSA com no mínimo 1024 bits de tamanho
Ordem de geração das assinaturas	Definida através das classes de signatários na seguinte ordem: Clientes – Banco
Quantidade de assinaturas	No mínimo uma por classe de signatário
Vínculo temporal	As assinaturas devem ser realizadas no mesmo dia

De acordo com os signatários do contrato de câmbio, podem ser definidas quatro classes de signatários. A Tabela 6 lista os atributos das classes.

Tabela 6 - Classes de signatários do contrato de câmbio.

Identificação da classe	**Papel**	**Propósito**	**Quantidade de assinaturas**
Classe A	Banco	Íntegro	1
Classe B	Clientes	Compromissivo	1
Classe C	Corretoras	Compromissivo	1
Classe D	Banco	Compromissivo	2

De acordo com a ordem de geração das assinaturas, a relação de dependência para geração da assinatura é ilustrada na Figura 28.

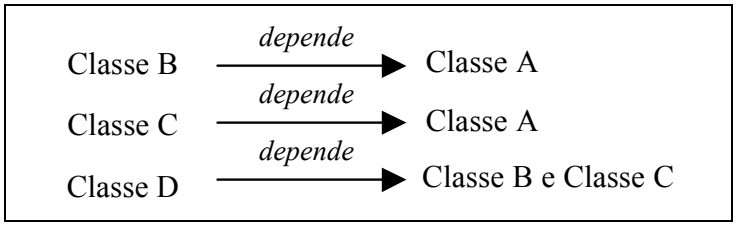

Figura 28 - Dependência de ordem entre as classes de signatários do contrato de câmbio.

9. CONCLUSÃO

A utilização do modelo de política de assinatura é importante porque estabelece um conjunto de requisitos técnicos para geração e verificação de assinaturas dentro de um contexto legal ou de negócio. O ETSI propôs um modelo de política que reflete os componentes envolvidos no processo de geração e verificação de uma assinatura. A partir da política de assinatura, os signatários envolvidos no contexto consideram a assinatura válida se esta estiver em conformidade com o conjunto de requisitos definidos na política.

No entanto, o modelo do ETSI não contempla requisitos de relacionamentos entre as assinaturas. Além disso, também não possui atributos que permitam para um usuário da política verificar a autoria da política de assinatura.

Este trabalho apresenta uma proposta de modelo de política de assinatura, o SIPEX, que consiste em uma extensão do modelo do ETSI para contemplar autenticação da política da assinatura e regras de relacionamento entre as assinaturas. A proposta do SIPEX define um conjunto de atributos que atendem os requisitos de ordem de geração de assinatura, quantidade mínima de assinaturas realizadas e limites de tempo para aposição das assinaturas. O SIPEX também define um atributo que atende o requisito de autenticação da política.

Além disso, o trabalho apresentou um sintético entendimento legal e tecnológico do cenário de assinaturas e documentos, clarificando os principais conceitos envolvidos no tema.

Além de proporcionar maior flexibilidade para os softwares de assinatura digital, o modelo proporciona a vantagem de registrar todas as regras utilizadas para gerar assinaturas baseadas no contexto do negócio. Desta forma, a política de assinatura pode ser usada como evidência a respeito das condições sob as quais a assinatura deve ser validada.

Uma outra vantagem oferecida pelo modelo é que as definições da política podem servir como regras de validação das transições nos diagramas de estado de um sistema de *workflow*.

Um problema relacionado com a política é que, dependendo do contexto, a sua criação pode ser muito complexa. Neste caso, seria interessante algum mecanismo que possibilite o gerenciamento de conflitos entres as regras definidas na política.

9.1. TRABALHOS FUTUROS

Com o objetivo de estender a aplicabilidade do modelo proposto e aprimorar algumas das funcionalidades oferecidas, diversos temas para trabalhos futuros podem ser abordados.

Relacionado ao ambiente de sistemas de *workflow*, um possível trabalho futuro é a definição de uma linguagem que complementasse linguagens formais de fluxo (como exemplo o YAWL, (AALST; HOFSTEDE, 2005)), de forma a proporcionar validade jurídica e outras exigências de negócios, como a tempestividade, para fluxos mais complexos. Nesse sentido a validade da transição entre estados poderia ser definida por uma política de assinatura.

No contexto da regulação da comunicação entre as instituições, também como trabalho futuro pode-se propor uma extensão dos padrões atuais de EDI como, por exemplo, o EDIFACT, de forma a contemplar o modelo de política de assinaturas.

REFERÊNCIAS BIBLIOGRÁFICAS

ADAMS, C.; LLOYD, S. Understanding Public-Key Infrastructure: Concepts, Standards and Deployment Considerations. Estados Unidos: Macmillan Technical Publishing, 1999. 296 p.

ADAMS C.; CAIN P.; PINKAS D.; ZUCCHERATO R. **RFC 3161:** Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), ago. 2001. Disponível em: <http://www.faqs.org/rfcs/rfc3161.html>. Acesso em: 12 dez. 2004.

ARREBOLA, F. V. **Um modelo de controle de acesso a recursos de rede baseado em Infra-estrutura de Chaves Públicas e Infra-estrutura de Gerenciamento de Privilégios**. 2006. 111 f. Dissertação (Mestrado em Engenharia Elétrica) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2006.

BANCO CENTRAL DO BRASIL, Carta Circular nº 3134, de 27 de abril de 2004.

BERBECARU Diana et al. **Towards concrete application of electronic signature.** Italy: Dip. Di Automatica e Informatica, Politecnico di Torino. Disponível em: <http://security.polito.it/doc/papers/e_sign.pdf >. Acesso em: 19 nov. 2004.

BERNAL, V. B. **Curso de Segurança em Redes de computadores**. São Paulo, 36 p. 2005.

BLUM, Renato Opice et al. **Direito Eletrônico:** A Internet e os Tribunais. Bauru: Editora EDIPRO, 2001, p. 44.

BRAY,Tim et al. **W3C Recommendation: Extensible Markup Language (XML)**, fev. 2004. Disponível em: <http://www.w3.org/TR/2004/REC-xml-20040204>. Acesso em: 23 jul. 2005.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002. Disponível em: <http://www.presidencia.gov.br/ccivil_03/LEIS/2002/L10406.htm>. Acesso em: 25 jul. 2005.

CASTRO, Aldemario Araujo Castro. **Revista Do Direito Eletronico**. São Paulo, ano 1, n. 1 p15, Julho a Agosto 2003. Disponível em: <http://www.ibde.org.br/revista>. Acesso em: 10 out. 2004

EASTLAKE D.; REAGLE J.; SOLO D. **RFC-3275:** XML-Signature Syntax and Processing, mar .2002. Disponível em: <http://www.faqs.org/rfcs/rfc3275.html>. Acesso em: 05 mar. 2005.

EUROPEAN PARLIAMENT AND THE COUNCIL OF EUROPEAN UNION, Directive 1999/93/EC, 13 de dezembro de 1999.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. **Electronic Signatures and Infrastructures (ESI)**: Signature policy for extended business model. France: ETSI, 2003a. 63 p. Disponível em: <http://webapp.etsi.org/exchangefolder/tr_102045v010101p.pdf >. Acesso em: 11 nov. 2004.

_____. **Eletronic Signatures and Infrastructures (ESI)**: Eletronic Signature Formats. France: ETSI, 2003b. 93 p. Disponível em: <http://webapp.etsi.org/exchangefolder/ts_101733v010501p.pdf>.Acesso em: 07 out. 2004.

_____. **Eletronic Signatures and Infrastructures (ESI)**: ASN.1 format for Signature Policies. France: ETSI, 2003c. 39 p. Disponível em: <http://webapp.etsi.org/exchangefolder/ts_102272v010101p.pdf>.Acesso em: 07 out. 2004.

_____. **Eletronic Signatures and Infrastructures (ESI)**: XML format for Signature Policies. France: ETSI, 2002a. 39 p. Disponível em: <http://webapp.etsi.org/exchangefolder/ts_102038v010101p.pdf>.Acesso em: 07 out. 2004.

_____. **Signature Policies Report**. France: ETSI, 2002b. 31 p. Disponível em: <http://webapp.etsi.org/exchangefolder/ts_102041v010101p.pdf>.Acesso em: 10 jan. 2006.

FARRELL, S.; HOUSLEY, R. RFC3281 - An Internet Attribute Certificate Profile for Authorization, 2002. Disponível em: <http://www.ietf.org/rfc/rfc3281.txt>. Acesso em: 4 jan. 2004.

FREIER, A. O.; KARLTON, P.; KOCHER, P. C. The SSL Protocol Version 3.0, 1996. Disponível em: <http://wp.netscape.com/eng/ssl3/draft302.txt>. Acesso em: 17 abr. 2004.

HOUSLEY R. **RFC 2630:** Cryptographic Message Syntax (CMS), jun. 1999. Disponível em: <http://www.faqs.org/rfcs/rfc3369.html>. Acesso em: 13 abr. 2005.

_____. **RFC 3369:** Cryptographic Message Syntax (CMS), aug. 2002. Disponível em: <http://www.faqs.org/rfcs/rfc3369.html>. Acesso em: 13 abr. 2005.

_____. **RFC-3852:** Cryptographic Message Syntax (CMS), jul. 2004. Disponível em: <http://www.faqs.org/rfcs/rfc3852.html>. Acesso em: 13 abr. 2005.

ICP Brasil: Infra-estrutura de Chaves Públicas Brasileira. Disponível em: <http://www.icpbrasil.gov.br>. Acesso em 12 jan. 2006.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. Declaração de práticas de certificação da AC-Raiz da ICP-Brasil. Brasil: ITI, 2001a. 26 p. Disponível em: <http://www.iti.gov.br/DPCacraiz.pdf> Acesso em: 06 jul. 2006

_____. Resolução nº 7: Aprova os requisitos mínimos para políticas de certificado na ICP-Brasil. Brasil: ITI, 2001b. 30 p. Disponível em: <http://www.iti.gov.br/resolucoes/RESOLU__O_7_DE_12_12_2001.PDF> Acesso em: 06 jul. 2006

_____. Definição de assinatura digital. Disponível em: <http://www.iti.br/twiki/bin/view/Main/PerguntaDois>. Acesso em: 06 jul. 2006.

ITU-T Recommendation X.690 Information technology -ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). 2002

LABORATÓRIO DE ENSAIOS E ANÁLISES. Manual de Condutas Técnicas Volume 4: Detalhamento dos Requisitos Técnicos para Softwares de Assinatura Digital, Sigilo e Autenticação no Âmbito da ICPBrasil. Brasil: LEA, 2006. 32 p. Disponível em: <http://www.lea.gov.br/download/LEA_MCT4-V1.pdf>. Acesso em: 06 jul. 2006.

LEUNG, K.R.P.H.; HUI, L.C.K., 2000. Multiple Signature Handling in Workflow Systems. In: Hawaii International Conference On System Sciences, 2000, Maui. **Proceedings…**USA: Computer Society Press, 2000. p.6033

MARCACINI, A. T. R. **Direito e Informática:** uma abordagem jurídica sobre criptografia. Rio de Janeiro: Forense, 2002.

MILHOMENS Jônatas; ALVES, Geraldo Magela. **Manual Prático dos Contratos:** Doutrina–Legislação–Jurisprudência–Formulários. 5 ed. Rio de Janeiro: Editora Forense, 2000, p. 5

MENEZES, A. J.; OORSCHOT, P. V.; VANSTONE, S. A. Handbook of Applied Cryptography. Estados Unidos: CRC Press, 1996. 816 p.

MYERS, M.; ANKNEY, R.; MALPANI, A.; GALPERIN, S.; ADAMS, C. RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP), 1999. Disponível em: <http://www.ietf.org/rfc/rfc2560.txt>. Acesso em: 12 out. 2004.

OASIS. eXtensible Access Control Markup Language (XACML) version 1.0. Disponível em: <http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf>. Acesso em: 13 ago. 2005.

PINKAS, D.; Ross, J.; Pope, N. **RFC 3126:** Eletronic Signature Formats for long term eletronic signatures, RFC 3126. Disponível em :<http://www.ietf.org/rfc/rfc3126.txt>. Acesso em: 15 mar. 2005.

RANGEL, Paulo. **Direito Processual Penal**. 6 ed. Rio de Janeiro: Lumes Júris. p 589-592. 2002

RSA LABORATORIES. **PKCS #7**: Cryptographic Message Syntax Standard v 1.5. USA: RSA Laboratories, 1993. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-doc>. Acesso em: 10 jun. 2005

RODRIGUES, S. Direito civil dos contratos e das declarações unilaterais de vontade. 28. ed. São Paulo: Saraiva, 2002. v. 3.

SCHEIBELHOFER, K. **Signing XML documents and the concept of "What You See Is what you sign"**. 2001. 118 f. Dissertação (Mestrado em Telemática) - Institute for Applied Information Processing and Communications, Graz University of Technology, Áustria, 2001.

SOUSA, Artur Afonso. **Base de Dados, Web e XML**. Lisboa: FCA Editora de Informática, 2002.

STALLINGS, W. **Cryptography and Network Security**. 2. ed. Prentice Hall, 1998

AALST, W.M.P.; HOFSTEDE, A.H.M. YAWL: Yet Another Workflow Language. Information Systems, 30(4):245-275, 2005.

ZHOU J.; DENG R. H. On the validity of digital signatures. In: ACM SIGCOMM Computer Communication Review, 2000, Singapura. **Proceedings…** Nova York: ACM Press, 2000. p 29-34

APÊNDICE A – IMPLEMENTAÇÃO

Para criar uma prova de conceito do modelo proposto, foi implementado um protótipo que inclui o modelo de política de assinatura no formato ASN.1. Este protótipo contempla o conjunto de atributos definidos pelo ETSI e as extensões apresentadas na proposta SIPEX. A implementação contempla os seguintes itens:

- Criação do modelo do conjunto de atributos da política de assinatura do ETSI;
- Associação de uma assinatura digital a uma política de assinatura;e
- Validação de uma assinatura de acordo com a política de assinatura.

Os atributos da política foram definidos como fixos e a validação da assinatura somente verifica as extensões propostas no modelo SIPEX.

MÓDULOS DO PROTÓTIPO

Os seguintes módulos foram desenvolvidos como parte da implementação do modelo proposto:

- **Gerador de política de assinatura**: desenvolvido em Java, este módulo permite a criação da estrutura ASN.1 da política de assinatura definida no SIPEX com os respectivos valores dos atributos da política. Para a codificação foi utilizada a biblioteca criptográfica Bouncy Castle.
- **Assinado**r: desenvolvido em C++ e baseado na biblioteca criptográfica CryptoAPI, este módulo gera assinaturas digitais em documentos eletrônicos e associa uma política de assinatura previamente definida com a assinatura gerada. Este módulo permite ao usuário signatário selecionar a política de assinatura de acordo com o contexto do negócio e o propósito da assinatura

- **Verificador**: desenvolvido em Java, este módulo permite a verificação da assinatura baseada no conjunto de regras definida na política.

RESULTADOS

Através do protótipo foi possível verificar a viabilidade da construção de componentes de software para validação de assinaturas digitais baseada em regras definidas em uma política de assinatura. Além disso, foi possível verificar a necessidade de uma evolução do modelo SIPEX com relação ao atributo vínculo temporal para que seja possível determinar a ordem de geração de assinaturas não somente no momento de criação das assinaturas mas também no instante de verificação das assinaturas.