REQUISITOS MÍNIMOS PARA

POLÍTICAS DE ASSINATURA DIGITAL

NA ICP-BRASIL

DOC-ICP-15.03

Versão 1.0

Índice

1 INFORMAÇÕES GERAIS

1.1 Este documento estabelece os requisitos mínimos a serem obrigatoriamente observados pelas entidades criadoras de Políticas de Assinatura Digital no âmbito da Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, em conformidade com a estrutura proposta pelos padrões ETSI TR 102 272 [6] e ETSI TR 102.038 [9].

1.2 Ele faz parte de um conjunto de normativos criados para regulamentar a geração e verificação de assinaturas digitais no âmbito da Infra-estrutura de Chaves Públicas Brasileira -ICP-Brasil. Tal conjunto se compõe de:

a) ASSINATURAS DIGITAIS NA ICP-BRASIL – DOC-ICP-15;

b) PERFIL PARA ASSINATURAS CADES ICP-BRASIL – DOC-ICP-15.01;

c) PERFIL PARA ASSINATURAS XADES ICP-BRASIL – DOC-ICP-15.02;

d) REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE ASSINATURA NA ICP-BRASIL – DOC-ICP-15.03;

e) POLÍTICA DE ASSINATURA ICP-BRASIL PADRÃO CADES – DOC-ICP-15.04;

f) POLÍTICA DE ASSINATURA ICP-BRASIL PADRÃO XADES – DOC-ICP-15.05.

1.3 Toda Política de Assinatura elaborada no âmbito da ICP-Brasil deve adotar a mesma sintaxe de estrutura empregada neste documento.

1.4 Esta estrutura prevê a criação de uma única assinatura digital (também conhecida como assinatura digital simples ou primária), a criação de assinaturas digitais em paralelo (também conhecidas como co-assinaturas) ou a criação de assinaturas digitais em série (também conhecidas como contra-assinaturas).

1.5 No documento DOC-ICP-15, item 6.2, foram definidos quatro formatos de assinatura digital no âmbito da ICP-Brasil.

a) sem carimbo de tempo (EPES);

b) com carimbo de tempo (EPES-T);

c) com informação completa para validação (EPES-C-X);

d) com informações para arquivamento (EPES-A); ou

e) uma combinação dos formatos citados nos subitens a) até d).

1.6 Salvo quando expressamente mencionado, este documento descreve os Requisitos Mínimos para Políticas de Assinatura aplicáveis a todos os formatos de assinatura.

1.7 Antes de entrar em utilização, uma Política de Assinatura criada no âmbito da ICP-Brasil deve ser submetida à AC-Raiz para fins de obtenção de um identificador único (Object Identifier), que a diferencie de outras políticas e permita seu correto processamento pelos sistemas. Após

esse procedimento, a política será reconhecida como Política de Assinatura Aprovada ICP-Brasil.

1.8 As Políticas de Assinatura Aprovadas ICP-Brasil são protegidas contra alterações indevidas por meio da publicação, no repositório da AC Raiz, de seu conteúdo assinado digitalmente por chave privada associada a certificado digital do Instituto Nacional de Tecnologia da Informação (ITI), utilizando algoritmo SHA256.

1.9 As Políticas de Assinatura Aprovadas ICP-Brasil devem ser escritas de uma forma inteligível por seres humanos e; opcionalmente, podem ser escritas de uma forma inteligível por sistemas de processamento.

1.10 No caso de políticas que sejam escritas com base no presente documento, a forma inteligível por sistemas de processamento deve ser ASN.1 ou XML.

2 CONTEÚDO DA POLÍTICA DE ASSINATURA

Os itens a seguir relacionam os conteúdos que devem, obrigatoriamente, fazer parte de uma Política de Assinatura Aprovada ICP-Brasil

2.1 Identificador da Política de Assinatura

2.1.1 Neste item deve ser identificada a Política de Assinatura e indicado o seu OID (*Object Identifier*).

2.1.2 No âmbito da ICP-Brasil, um OID – com o formato 2.16.76.1.5.n.n.n – será atribuído à Política de Assinatura na conclusão do processo de aprovação por parte ITI.

A composição do OID é feita de forma que o último número seja referente à versão da Política de Assinatura Aprovada.

2.1.3 Toda Política de Assinatura Aprovada ICP-Brasil deve estar disponível publicamente a todos interessados. Neste item deve ser indicada a URL onde a Política de Assinatura pode ser consultada.

2.1.4 Neste item deve ser mencionado que as Políticas de Assinatura Aprovadas estarão disponíveis para consulta também no repositório da AC-Raiz.

2.2 Data da Criação

Neste item deve ser informada a data de criação da Política de Assinatura.

2.3 Entidade Criadora da Política de Assinatura

Este item deve conter uma identificação da entidade responsável pela criação da Política de Assinatura e da comunidade que fará uso dela. No âmbito da ICP-Brasil, qualquer entidade - pessoa física ou jurídica, órgão de governo etc. – pode criar Políticas de Assinatura, conforme sua necessidade e conveniência.

2.4 Campo de Aplicação

2.4.1 Neste item deve ser definido, em termos gerais, o campo de aplicação da assinatura digital gerada conforme a Política de Assinatura, bem como os propósitos específicos para os quais a assinatura digital é aplicável.

2.4.2 Deverão estar relacionadas, quando cabível, as aplicações para as quais existam restrições ou proibições para o uso da PA.

2.5 Política de Validação da Assinatura

O campo Política de Validação estabelece as regras gerais e específicas aplicadas à Assinatura Digital e que devem ser observadas pelo assinante e pelo verificador da assinatura.

2.5.1 Período para Assinatura

2.5.1.1 Deve ser definido o período de validade (data e hora) inicial e final de abrangência das regras definidas na Política de Assinatura aplicáveis às assinaturas digitais que se utilizarem da Política.

2.5.1.2 O período de validade máximo admitido para uma Política de Assinatura no âmbito da ICP-Brasil é de 05 (cinco) anos.

2.5.2 Regras Comuns

Este campo define as regras comuns e gerais, tanto para o processo de assinatura pelo signatário, quanto para o processo de verificação pelo verificador.

Se um campo estiver presente nas Regras Comuns então ele NÃO DEVERÁ estar presente em nenhum campo de Regras para Propósitos Específicos de Assinatura.

2.5.2.1 Regras do Signatário e do Verificador

2.5.2.1.1 Regras do Signatário

Este campo define as regras que devem ser observadas e incluídas no pacote da assinatura pelo signatário, no momento da assinatura digital do documento eletrônico. Todas as assinaturas geradas segundo uma Política de Assinatura Aprovada ICP-Brasil devem estar em conformidade com o disposto no DOC-ICP-15, capítulo 6.

OBS.: Permite-se, adicionalmente, o uso de qualquer dos atributos e propriedades previstos nos padrões CMS, CADES, XMLDSIG e XADES, definidos respectivamente na RFC 3852 [14], no documento ETSI TR 102733 [7], na RFC 3275 [15] e no documento ETSI TS 102903 [10].

2.5.2.1.1.1 Dados Externos ou Internos a Assinatura

Neste item deve ser descrito se existe ou não a obrigatoriedade de inclusão do conteúdo assinado (documento eletrônico) na assinatura digital.

No caso de o conteúdo não ser incluído, ou seja, se ele ficar externo ao pacote de assinatura digital, deve ser descrita a forma de obter o conteúdo para verificação da assinatura.

2.5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

2.5.2.1.1.2.1 Neste item devem ser relacionados os atributos ou propriedades que devem constar, obrigatoriamente, no pacote da assinatura digital no âmbito desta Política de Assinatura e que são assinados juntamente com o documento eletrônico.

2.5.2.1.1.2.2 O documento DOC-ICP-15, item 6.2.3 define os atributos ou propriedades obrigatórios, para todos os formatos de assinatura digital ICP-Brasil.

2.5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios

2.5.2.1.1.3.1 Neste item devem ser relacionados os atributos ou propriedades que devem constar, obrigatoriamente, no pacote da assinatura digital no âmbito desta Política de Assinatura, e que não são assinados juntamente com o documento eletrônico.

2.5.2.1.1.3.2 O documento DOC-ICP-15 define, nos itens 6.2.4 a 6.2.6, os atributos ou propriedades obrigatórios, para todos os formatos de assinatura digital ICP-Brasil.

2.5.2.1.1.3.3 A inclusão desses atributos ou propriedades não assinados pode, opcionalmente, ser realizada pelo verificador ao invés do signatário. Nestes casos devem ser informados neste item apenas os atributos que devem ser incluídos pelo signatário. Os que devem ser incluídos pelo verificador devem ser relacionados no item 2.5.2.1.2.1.

2.5.2.1.1.4 Referências à Cadeia de Certificação

2.5.2.1.1.4.1 Neste item deve ser descrito que todas as assinaturas digitais criadas com base nesta Política de Assinatura devem conter obrigatoriamente a referência ao certificado do signatário, por meio do identificador Serial do Emissor.

2.5.2.1.1.4.2 Para os formatos EPES-C-X devem também ser incluídos identificadores (Serial do Emissor) de todos os certificados da cadeia de certificação, desde o certificado do signatário até a Autoridade Certificadora Raiz Brasileira,

2.5.2.1.1.5 Valores da Cadeia de Certificação

2.5.2.1.1.5.1 Para os formatos EPES e EPES-T e EPES-C-X não há necessidade de incluir os certificados da cadeia de certificação do signatário na assinatura digital.

2.5.2.1.1.5.2 Para os formatos e EPES-A deve ser descrito que todas as assinaturas digitais devem conter obrigatoriamente os certificados do signatário bem como de todos os certificados da cadeia de certificação, desde o certificado do signatário até a Autoridade Certificadora Raiz Brasileira.

2.5.2.1.1.5.3 Caso o verificador possa encontrar um ou mais certificados da cadeia de certificação através de alguma outra forma, poderá ser incluído na assinatura digital apenas o certificado do signatário ou até mesmo nenhum dos certificados. Nestes casos, deverá ser descrito de que forma os certificados estarão disponíveis e poderão ser utilizados para a verificação da assinatura.

2.5.2.1.1.6 Regras Adicionais do Signatário

Caso haja a necessidade de incluir regras adicionais relacionadas ao processo de Assinatura Digital executado pelo signatário, estas deverão ser incluídas neste item.

2.5.2.1.2 Regras do Verificador

Este item descreve as regras de validação da Assinatura Digital, aplicáveis a atributos ou propriedades não incluídos pelo signatário no momento da assinatura, os quais devem então ser incluídos pelo verificador.

2.5.2.1.2.1 Atributos Não-Assinados Obrigatórios

Este item deverá conter obrigatoriamente os atributos descritos no item 2.5.2.1.1.3 que não são incluídos pelo signatário.

2.5.2.1.2.2 Regras Adicionais do Verificador

Caso haja a necessidade de regras adicionais relacionadas ao verificador, essas deverão ser incluídas neste item.

2.5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

2.5.2.2.1 Validação da Cadeia de Certificação

Neste item deve constar que o processo de validação dos certificados da cadeia de certificação do signatário deverá ser realizado em conformidade com a RFC 3280 e com o disposto nesta Política de Assinatura.

2.5.2.2.1.1 Raiz Confiável

Neste item deverá constar que a validação deve ser feita tomando como ponto de confiança o certificado da AC-Raiz da ICP-Brasil, que se encontra disponível em http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt Para fins de conferência adicional, o certificado da AC-Raiz também se encontra publicado no Diário Oficial da União do dia 03.12.2001.

2.5.2.2.1.2 Restrição do Caminho de Certificação

Neste item deve constar que o número máximo de certificados de AC, no caminho de certificação entre o certificado do signatário e o da AC-Raiz é 2 (dois).

2.5.2.2.1.3 Conjunto de Políticas de Certificação Aceitáveis

Neste item devem constar os tipos de certificados ICP-Brasil, cujas chaves privadas associadas podem gerar assinaturas digitais segundo a Política de Assinatura. Entre os tipos aceitáveis, tem-se:

Tipo de Certificado	OID
A1	2.16.76.1.2.1.*n*
A2	2.16.76.1.2.2.*n*
A3	2.16.76.1.2.3.*n*
A4	2.16.76.1.2.4.*n*

2.5.2.2.1.4 Restrições de Nome

Neste item, caso existam, deverão constar os nomes (Subject Distinguished Name e/ou Subject Alternative Name) para os quais os certificados devem ser rejeitados.

2.5.2.2.1.5 Restrições de Políticas (Aceitável e Não-Aceitáveis)

2.5.2.2.1.5.1 Neste item poderão constar os indicadores relativos às Políticas de Certificado permitidas para garantir a aceitação dos certificados da cadeia de certificação. Opcionalmente poderão ser definidos os certificados da cadeia que devem ter suas Políticas verificadas.

2.5.2.2.1.5.2 Caso existam, também poderão constar os indicadores relativos às Políticas de Certificado correspondentes aos certificados que devem ser rejeitados. Opcionalmente poderão ser definidos os certificados da cadeia que devem ter suas Políticas verificadas.

2.5.2.2.2 Forma de Verificação do Estado da Cadeia de Certificação

2.5.2.2.2.1 Neste item deve constar se é ou não obrigatória a verificação do estado do certificado do signatário. Se for obrigatório, deve ser especificado o método a ser utilizado para essa verificação.

2.5.2.2.2.2 Também deve constar se é ou não obrigatória a verificação do estado dos certificados das Autoridades Certificadoras da cadeia de certificação do signatário. Se for obrigatório, deve ser especificado o método a ser utilizado para essa verificação.

2.5.2.2.2.3 Entre os métodos de verificação de estado estão a consulta a LCR (Lista de Certificados Revogados) em conformidade com a RFC 3280, a consulta OCSP (Online Certificate Status Protocol) em conformidade com a RFC 2560 ou algum outro método aprovado pela ICP-Brasil.

2.5.2.3 Condições de Confiabilidade do Carimbo de Tempo

NOTA: Este item não se aplica a assinaturas formato EPES

2.5.2.3.1 Validação da Cadeia de Certificação

Neste item deve constar que o processo de validação dos certificados da cadeia de certificação da Autoridade de Carimbo de Tempo deve ser realizado em conformidade com a RFC 3280 e

com o disposto nesta Política de Assinatura.

2.5.2.3.1.1 Raiz Confiável

Neste item deve constar que a validação deve ser feita tomando como ponto de confiança o certificado da AC-Raiz da ICP-Brasil, que se encontra disponível em http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt Para fins de conferência adicional, o certificado da AC-Raiz também se encontra publicado no Diário Oficial da União do dia 03.12.2001.

2.5.2.3.1.2 Restrição do Caminho de Certificação

Neste item deve constar o tamanho máximo do caminho de certificação, ou seja, número de Autoridades Certificadoras entre a Raiz confiável e o certificado da Autoridade de Carimbo de Tempo. No caso da ICP-Brasil, o máximo é 2 (dois).

2.5.2.3.1.3 Conjunto de Políticas de Certificação Aceitáveis

Neste item devem constar os tipos de certificados ICP-Brasil, cujas chaves privadas associadas podem gerar carimbos de tempo, aceitos segundo esta Política de Assinatura. Entre os tipos aceitáveis tem-se:

Tipo de Certificado	OID
T3	2.16.76.1.2.5.*n*
T4	2.16.76.1.2.6.*n*

2.5.2.3.1.4 Restrições de Nome

Neste item, caso existam, deverão constar os nomes (Subject Distinguished Name e/ou Subject Alternative Name) para os quais os certificados devem ser rejeitados.

2.5.2.3.1.5 Restrições de Políticas (Aceitável e Não-Aceitáveis)

2.5.2.2.3.1.5.1 Neste item poderão constar os indicadores relativos as Políticas de Certificado permitidos para garantir a aceitação dos certificados da cadeia de certificação da Autoridade de Carimbo de Tempo. Opcionalmente poderão ser definidos os certificados dessa cadeia de certificação que devem ter suas Políticas verificadas.

2.5.2.2.3.1.5.2 Caso existam, também poderão constar os indicadores relativos as Políticas de Certificado correspondentes aos certificados que devem ser rejeitados. Opcionalmente poderão ser definidos os certificados da cadeia que devem ter suas Políticas verificadas.

2.5.2.3.2 Forma de Verificação do Estado da Cadeia de Certificação

2.5.2.3.2.1 Neste item deve constar se é ou não obrigatória a verificação do estado do certificado da Autoridade de Carimbo de Tempo. Se for obrigatório, deve ser especificado o método a ser

utilizado para essa verificação.

2.5.2.3.2.2 Também deve constar se é ou não obrigatória a verificação do estado dos certificados das Autoridades Certificadoras da cadeia de certificação da Autoridade de Carimbo de Tempo. Se for obrigatório, deve ser especificado o método a ser utilizado para essa verificação

2.5.2.3.2.3 Entre os métodos de verificação de estado estão a consulta a LCR (Lista de Certificados Revogados) em conformidade com a RFC 3280, a consulta OCSP (Online Certificate Status Protocol) em conformidade com a RFC 2560 ou algum outro método aprovado pela ICP-Brasil.

2.5.2.3.3 Restrições de Nome

Neste item, caso existam, deverão constar as restrições dos nomes (Subject Distinguished Name e/ou Subject Alternative Name) aceitos para as Autoridades de Carimbo de Tempo que poderão atuar como tal no âmbito desta Política de Assinatura.

2.5.2.3.4 Período de Cautela

Opcionalmente, poderá ser informado neste item o período de tempo necessário após a data e hora do atributo assinado “Signing Time” para que seja realizada a validação da assinatura digital.

2.5.2.3.5 Atraso do Carimbo de Tempo

Nos casos de assinaturas digitais que incluem o atributo assinado “Signing Time”, opcionalmente poderá ser definido um período de tempo máximo permitido entre a data e hora do atributo assinado e a data e hora do carimbo de tempo. Este item determina o período de latência de data e hora entre a data e hora da máquina onde foi realizada a assinatura e a data e hora oficial dada pela ACT.

2.5.2.4 Condições de Confiabilidade dos Atributos

2.5.2.4.1 Atributos Obrigatórios

Item não aplicável.

2.5.2.4.2 Atributos Exigidos

Item não aplicável.

2.5.2.4.3 Validação da Cadeia de Certificação

2.5.2.4.3.1 Raiz Confiável

Item não aplicável.

2.5.2.4.3.2 Restrição do Caminho de Certificação

Item não aplicável.

2.5.2.4.3.3 Conjunto de Políticas de Certificação Aceitáveis

Item não aplicável.

2.5.2.4.3.4 Restrições de Nome

Item não aplicável.

2.5.2.4.3.5 Restrições de Políticas (Aceitável e Não-Aceitáveis)

Item não aplicável.

2.5.2.4.4 Forma de Verificação do Estado da Cadeia de Certificação

Item não aplicável.

2.5.4.5 Restrições de Atributos

Item não aplicável.

2.5.2.5 Conjunto de Restrições de Algoritmos

2.5.2.5.1 Caso existam restrições quanto aos algoritmos e tamanhos de chaves, associados a assinatura digital e às entidades que têm algum tipo de participação na assinatura digital, aceitos no âmbito desta Política de Assinatura, essas devem ser descritas neste item.

2.5.2.5.2 Podem ser incluídas restrições de aceitação do algoritmo utilizado pelo signatário para a realização da assinatura digital, do algoritmo do usado para assinar o certificado do signatário, dos certificados das Autoridades Certificadoras que compõe a cadeia de certificação do signatário, da Autoridade de Atributo e da Autoridade de Carimbo de Tempo, indicando para cada um desses tipos quais são as restrições quanto aos algoritmos (hash, chave pública, combinação do hash com chave pública) e quanto ao tamanho de chave mínimo exigido para esses algoritmos de assinatura.

2.5.2.5.3 Opcionalmente, podem também ser descritas quaisquer outras restrições de aceitação relacionadas a algoritmos.

2.5.2.5.4 Os algoritmos devem ser escolhidos entre os listados no documento Padrões e Algoritmos Criptográficos da ICP-Brasil - DOC-ICP-01.01.

2.5.2.6 Regras Adicionais

Caso haja a necessidade de incluir regras adicionais para geração ou verificação de assinaturas digitais, como por exemplo o ambiente mínimo exigido para assinatura digital, elas devem ser incluídas neste item.

2.5.3 Regras para Propósitos Específicos de Assinatura

Caso existam regras para propósitos específicos de assinatura, diferentes das regras definidas no item 2.5.2., essas devem ser detalhadas nos próximos itens.

2.5.3.1 Tipos de Propósitos Selecionados

Deve ser identificado o tipo de propósito para o qual a assinatura se destina, dentre aqueles definidos nos padrões ETSI TR 102 733 [7] e ETSI TS 101 903 [9].

2.5.3.2 Regras de Signatário e Verificador

Caso existam regras específicas para determinados tipos de compromisso, elas devem ser detalhadas neste item, usando a mesma estrutura definida em 2.5.2.1.

2.5.3.3 Condições de Confiabilidade dos Certificados dos Signatários

Caso existam regras específicas para determinados tipos de compromisso, elas devem ser detalhadas neste item, usando a mesma estrutura definida em 2.5.2.2.

2.5.3.4 Condições de Confiabilidade do Carimbo de Tempo

Caso existam regras específicas para determinados tipos de compromisso, elas devem ser detalhadas neste item, usando a mesma estrutura definida em 2.5.2.3.

2.5.3.5 Condições de Confiabilidade dos Atributos

Caso existam regras específicas para determinados tipos de compromisso, elas devem ser detalhadas neste item, usando a mesma estrutura definida em 2.5.2.4.

2.5.3.6 Conjunto de Restrições de Algoritmos

Caso existam regras específicas para determinados tipos de compromisso, elas devem ser detalhadas neste item, usando a mesma estrutura definida em 2.5.2.5.

2.5.3.7 Regras Adicionais

Caso haja a necessidade de regras adicionais para geração ou verificação de assinaturas digitais para determinado propósito específico, elas devem ser incluídas neste item.

2.5.4 Informações Adicionais sobre a Validação das Assinaturas

Caso haja a necessidade de informações adicionais quanto a validação das assinaturas digitais no âmbito desta Política de Assinatura, ela devem ser incluídas neste item.

2.6 Informações Adicionais sobre a Política de Assinatura

Caso haja a necessidade de informações adicionais sobre a Política de Assinatura, elas devem estar incluídas neste item.

3 BIBLIOGRAFIA

[1] ITI. Glossário ICP-Brasil. Instituto Nacional de Tecnologia da Informação. Versão 1.2; Brasília: ICP-Brasil, 2007.

[2] SCHNEIER, Bruce. Applied Cryptografy, Second Edition: protocols, algorithms, and source code in C. USA: Wiley, 1996.

[3] DOURNAEE, Blake. XML Security. Berkely: McGraw-Hill/Osborne, 2002.

[4] ETSI. Signature Policies Report. ETSI TR 102 041 (2002-02); European Telecomunications Standards Institute, 2002.

[5] ETSI. Eletronic Signature and Infraestructures (ESI); Signature policy for extended business model. ETSI TR 102 045 (2005-03); European Telecomunications Standards Institute, 2005.

[6] ETSI. Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies. ETSI TR 102 272 (2003-12); European Telecomunications Standards Institute, 2003.

[7] ETSI. Eletronic Signature and Infraestructures (ESI); CMS Advanced Eletronica Signatures (CadES). ETSI TR 102 733 (2007-01); European Telecomunications Standards Institute, 2007.

[8] ETSI. Electronic Signatures and Infrastructures; Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CadES); ETSI TS 102 734 (2007-02); European Telecomunications Standards Institute, 2007.

[9] ETSI. TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies; ETSI TR 102 038 (2002-04); European Telecomunications Standards Institute, 2002.

[10] ETSI. XML Advanced Electronic Signatures (XadES); ETSI TS 101 903 (2006-03); European Telecomunications Standards Institute, 2006.

[11] ETSI. Electronic Signatures and Infrastructures; Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XadES); ETSI TS 102 904 (2007-02); European Telecomunications Standards Institute, 2007.

[12] ETSI. Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms; ETSI TR 102 176 A (2005-07); European Telecomunications Standards Institute, 2005.

[13] ETSI.Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices; ETSI TR 102 176 B (2005-07); European Telecomunications Standards Institute, 2005.

[14] RFC 3852 Cryptographic Message Syntax (CMS) (2004-07);

[15] RFC 3275 (Extensible Markup Language) XML - Signature Syntax and Processing (2002-03);

[16] RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (1999-06);

[17] RFC 3126 Electronic Signature Formats for long term electronic signatures (2001-09);

[18] RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (2002-04);

[19] W3-IET-XML SIG XML- Signature Syntax and Processing W3C Recommendation (2002-02).

[20] REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL DOC-ICP-12 - V 1.0 – Documento em elaboração

[21] ITI. PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL. DOC-ICP-01.01 Instituto Nacional de Tecnologia da Informação. Versão 1.0; Brasília: ICP-Brasil, 2006.

[22] 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.