Infra-Estrutura de Chaves Públicas Brasileira

Manual de Condutas Técnicas 10 - Volume II

Procedimentos de Ensaios para Homologação de Equipamentos de Carimbo do Tempo no âmbito da ICP-Brasil

versão 1.0

Sumário

Listas de Ilustrações

Lista de Figuras

Lista de Tabelas

Glossário

Os termos utilizados neste MCT se referem àqueles definidos no Glossário ICP-Brasil conforme seção de referências normativas.

Lista de Acrônimos

AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
BIPM	*Bureau International des Poids et Mesures*
CT	Carimbo do Tempo
DPCT	Declaração de Práticas de Carimbo do Tempo
EAT	Entidade de Auditoria de Tempo
FCT	Fonte Confiável do Tempo
HLB	Hora Legal Brasileira
HSM	*Hardware Security Module*
HTTP	*Hypertext Transfer Protocol*
ICP	Infra-Estrutura de Chaves Públicas
ICP-Brasil	Infra-Estrutura de Chaves Públicas Brasileira
IRIG	Inter-Range Instrumentation Group
ITI	Instituto Nacional de Tecnologia da Informação
MSC	Módulo de Segurança Criptográfico
NTP	*Network Time Protocol*
OID	*Object Identifier*
ON	Observatório Nacional
PCT	Política de Carimbo do Tempo
PPS	*Pulse per Second*
PSS	Prestadores de Serviço de Suporte
RETEMP	Rede de Sincronismo Autenticado
RFC	*Request For Comments*
SAS	Sistema de Auditoria e Sincronismo
SCT	Servidor de Carimbo do Tempo
SHA	*Secure Hash Algorithm*
SINMETRO	Sistema Nacional de Metrologia
SNTP	*Simple Network Time Protocol*
TSP	*Time Stamp Protocol*
TST	*Time Stamping Token*

TSQ	*Time Stamp Query* (Solicitação de Carimbo do Tempo)
URL	*Uniform Resource Locator*
UTC	*Universal Time, Coordinated*

1 Introdução

Este documento descreve os procedimentos de ensaio aplicados ao processo de homologação de equipamento de Carimbo do Tempo no âmbito da Infra-Estrutura de Chaves Públicas Brasileira, a ICP-Brasil.

Os procedimentos de ensaio referem-se ao conjunto de métodos usados para avaliar se equipamentos de Carimbo do Tempo estão ou não em conformidade com os requisitos técnicos definidos pelo Manual de Condutas Técnicas 10 - Volume I.

Para uma melhor compreensão do disposto neste documento, as seguintes definições são aplicáveis:

- **Servidor de Carimbo do Tempo (SCT):** equipamento que opera na forma de solicitação e resposta, destinado a certificar que um determinado documento eletrônico existiu em um determinado instante. Como um componente de uma infra-estrutura de chaves públicas (ICP), o servidor de carimbo do tempo pode ter como propósito a certificação de que uma determinada assinatura foi realizada antes de um determinado instante, possibilitando assim, definir uma âncora temporal para ser utilizada como referência no processo de validação do certificado digital, seja para verificação de seu período de validade, seja para verificação do estado de revogação;
- **Autoridade de Carimbo do Tempo (ACT):** entidade na qual os usuários de serviços de carimbo do tempo (isto é, os subscritores e as terceiras partes) confiam para emitir carimbos do tempo. A ACT tem a responsabilidade geral pelo fornecimento do carimbo do tempo. É responsável pela a operação de um ou mais SCT, conectados à Rede de Carimbo do tempo da ICP-Brasil, que geram carimbos e assinam em nome da ACT;
- **Entidade de Auditoria do Tempo (EAT):** é a entidade responsável pela verificação da correta operação do Serviço de Carimbo do Tempo mantida pela Autoridade de Carimbo do Tempo;
- **Sistema de Auditoria e Sincronismo (SAS)**: hardware constituído por um MSC provido de relógio interno onde é executado software que audita e sincroniza SCTs e outros SAS. Como componentes;

- **Observatório Nacional (ON):** vinculado ao Ministério da Ciência e Tecnologia, integrante do Sistema Nacional de Metrologia (SINMETRO), o ON é o responsável legal pela geração, conservação e disseminação da Hora Legal Brasileira, com rastreabilidade metrológica ao BIPM (*Bureau International des Poids et Mesures*). Mantém e opera o Relógio Atômico, que é a Fonte Confiável do Tempo – FCT, a partir da qual se determina a Hora Legal Brasileira.

1.1 Organização deste documento

Cada seção deste documento contém um conjunto de requisitos que representam citações diretas do próprio texto do Manual de Condutas Técnicas 10 – Volume I. Os requisitos estão organizados da seguinte forma:

- *REQUISITO <número_do_requisito>.<número_de_seqüência_do_requisito>*
  - "número_do_requisito": corresponde ao número de área definido no Manual de Condutas Técnicas 10 – Volume I;
  - "número_de_seqüência_do_requisito": corresponde a um identificador seqüencial dos requisitos.

Os procedimentos de ensaio visam a orientar sobre como proceder nos testes elaborados sobre dispositivos. Os procedimentos de ensaio estão classificados e agrupados por Níveis de Segurança de Homologação da seguinte forma:

- NSH 1: Este nível não requer depósito e análise de código-fonte associado ao dispositivo em homologação;
- NSH 2: Este nível requer depósito e análise apenas de código-fonte de componentes específicos associados ao dispositivo em homologação. Por exemplo, código-fonte do algoritmo gerador de números aleatórios;
- NSH 3: Este nível requer depósito e análise de código-fonte completo associado ao dispositivo em homologação. Por exemplo, código-fonte de todo software e/ou *firmware* do módulo criptográfico.

Os procedimentos de ensaio (EN) que devem ser desempenhados pelo analista LEA estão organizados da seguinte forma:

- *EN.<número_do_requisito>.<número_de_seqüência_do_requisito>.<número_de_seqüência_do_ensaio>*
  - "número_do_requisito";

- “número_de_seqüência_do_requisito”;
- “número_de_seqüência_do_ensaio”: corresponde a um identificador seqüencial dos procedimentos que devem ser desempenhados.

Este documento (MCT 10 – Volume II) está estruturado da seguinte forma:

- Parte 1: Descreve os procedimentos de ensaio que devem ser verificados no processo de homologação de equipamentos de carimbo do tempo.

2 Parte 1

Procedimentos de Ensaios para Homologação de Equipamentos de Carimbo do Tempo no âmbito da ICP-Brasil

2.1 Requisitos gerais de carimbo do tempo

Esta seção descreve os requisitos gerais de carimbo do tempo que devem ser atendidos por Servidores de Carimbo do Tempo, Sistemas de Auditoria e Sincronismo e Autoridades de Carimbo do Tempo inseridos na estrutura de carimbo do tempo da ICP-Brasil.

Além dos componentes citados no item 1, também fazem parte da estrutura de carimbo do tempo da ICP-Brasil as seguintes entidades:

- **Comitê Gestor da ICP-Brasil** – Entidade responsável pela implantação da ICP-Brasil. Estabelece políticas, critérios e normas de funcionamento que devem ser seguidas pelas entidades integrantes da ICP-Brasil. Audita e fiscaliza a AC-Raiz;
- **AC-Raiz da ICP-Brasil (AC-Raiz)** – Credencia, audita e fiscaliza entidades da ICP-Brasil. Assina seu próprio certificado e os certificados das ACs imediatamente subordinadas;
- **Autoridade Certificadora (AC)** – Emite, renova ou revoga certificados digitais de outras ACs ou de titulares finais. Emite e publica LCR. Na estrutura de carimbo do tempo da ICP-Brasil emite os certificados digitais usados nos equipamentos das ACTs e da EAT e emite ainda os demais certificados utilizados nos processos relacionados aos carimbos do tempo;
- **Subscritor ou Cliente** – Pessoa física ou jurídica que solicita os serviços de uma Autoridade de Carimbo do Tempo (ACT), implícita ou explicitamente, concordando com os termos mediante os quais o serviço é oferecido;
- **Terceira Parte (*Relying Part*)** – Aquele que confia no teor, validade e aplicabilidade do carimbo do tempo produzido pela ACT.

A Figura 1 demonstra o modelo geral da estrutura de carimbo do tempo no âmbito da ICP-Brasil.

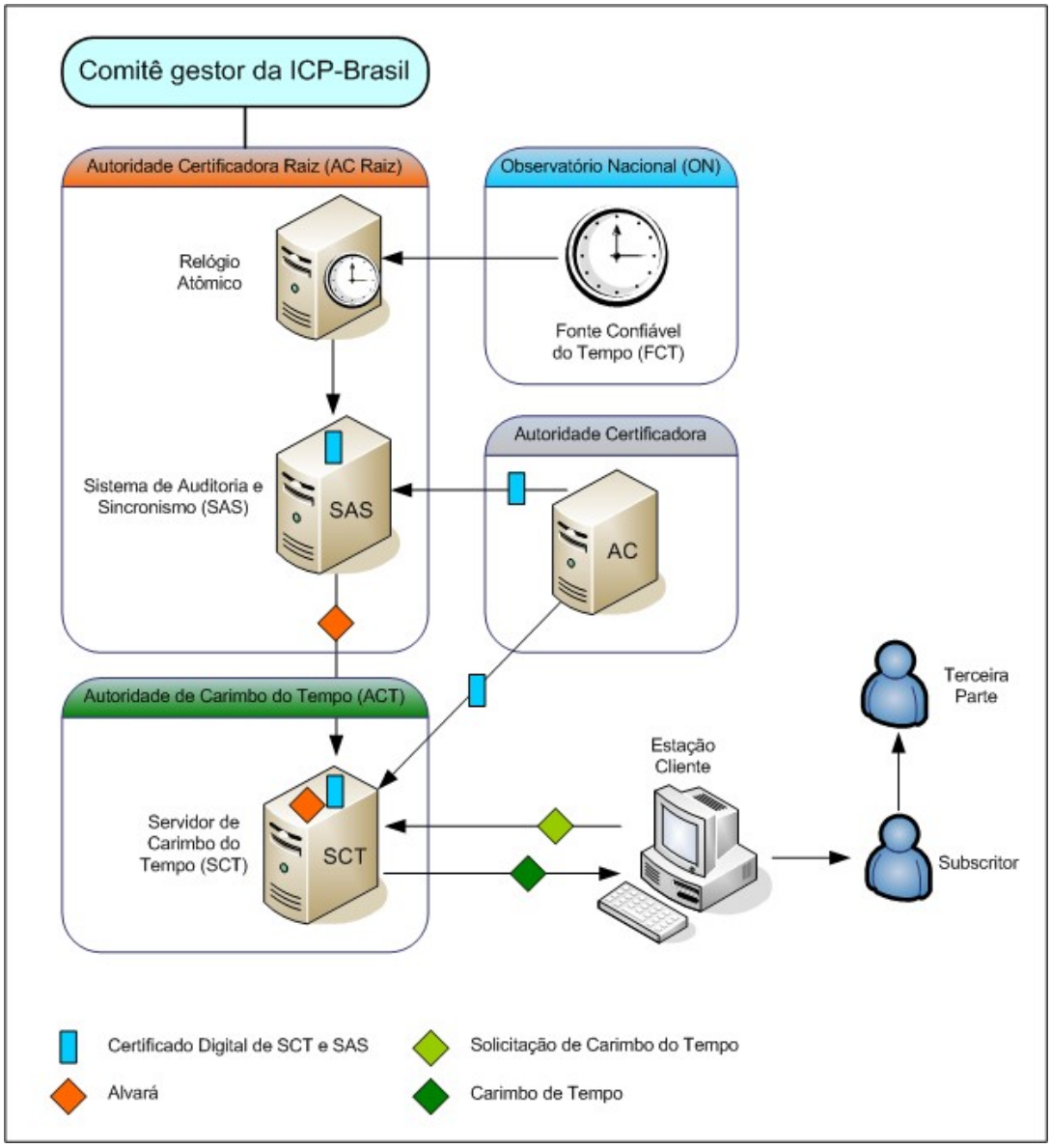

Figura 1: Modelo geral da estrutura de carimbo do tempo no âmbito da ICP-Brasil.

2.1.1 Requisitos de formato para solicitação e resposta de carimbo do tempo

2.1.1.1 Formato da solicitação

Conforme definido pela RFC 3161, mensagens de solicitação de carimbo do tempo possuem o seguinte formato:

TimeStampReq ::= SEQUENCE {

version Version,

```
        messageImprint      MessageImprint,
        reqPolicy           TSAPolicyId OPTIONAL,
        nonce               INTEGER OPTIONAL,
        certReq             BOOLEAN DEFAULT FALSE,
        extensions          [0] Extensions OPTIONAL
}
```

REQUISITO I.1: Uma solicitação de carimbo do tempo deve conter, no mínimo, os seguintes campos conforme definidos pela RFC 3161:

- "*version*": [OBRIGATÓRIO] versão da solicitação de carimbo do tempo;
- "*messageImprint*": [OBRIGATÓRIO] subdivide-se nos seguintes campos:
  - "*hashAlgorithm*": OID do algoritmo *hash* utilizado para gerar o conteúdo campo "*hashedMessage*";
  - "*hashedMessage*": *hash* dos dados a serem carimbados temporalmente.
- "*reqPolicy*": [OPCIONAL] quando presente, contém o OID da Política de Carimbo do Tempo (PCT) aplicável;
- "*nonce*": [OPCIONAL] quando presente, associa a solicitação do cliente à sua respectiva resposta, quando não existir uma referência de tempo local;
- "*certReq*": [OBRIGATÓRIO] campo utilizado para solicitar o envio do certificado da ACT na respectiva resposta;
- "*extensions*": [OPCIONAL] campo para inserir informações adicionais, conforme definido pela RFC 2459.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.01.01: Verificar se a documentação técnica do SCT descreve o formato de solicitações de carimbo do tempo suportado.

Nota: Os ensaios referentes ao formato de solicitação de carimbo do tempo são executados como parte da Seção 2.6.

2.1.1.2 Formato da resposta

Conforme a RFC 3161, mensagens de resposta à solicitações de carimbo do tempo possuem o seguinte formato:

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

A estrutura "*TimeStampToken*" é definida por:

```
TimeStampToken ::= SEQUENCE {
        contentType CONTENT.&id({Contents}),
        content [0]
        EXPLICIT CONTENT.&Type ({Contents}{@contentType})
}
```

Esta estrutura é utilizada para encapsular uma estrutura "*TSTInfo*", a qual é definida por:

```
TSTInfo ::= SEQUENCE {
        version                 Version,
        policy                  TSAPolicyId,
        messageImprint      MessageImprint,
        serialNumber        SerialNumber,
        genTime                 GeneralizedTime,
        accuracy                Accuracy OPTIONAL,
        ordering                BOOLEAN DEFAULT FALSE,
        nonce                   Nonce OPTIONAL,
        tsa                     [0] EXPLICIT GeneralName OPTIONAL,
        extensions              [1] Extensions OPTIONAL
}
```

REQUISITO I.2: Uma resposta à uma solicitação de carimbo do tempo deve conter, no mínimo, os seguintes campos conforme definidos pela RFC 3161:

- "*status*": [OBRIGATÓRIO] contém a estrutura "*PKIStatusInfo*" conforme definida na seção 3.2.3 da RFC 2510 pelos seguintes campos:
    - "*status*": indica a presença ou ausência de um carimbo do tempo na resposta da solicitação;
    - "*statusString*": campo opcional que descreve o motivo da ausência de um carimbo do tempo na resposta da solicitação;
    - "*failInfo*": indica o motivo da ausência de um carimbo do tempo na resposta da solicitação.
- "*timeStampToken*": [OPCIONAL] campo do tipo "*ContentInfo*" que encapsula um conteúdo do tipo "*SignedData*", conforme os seguintes campos:
    - "*TimeStampToken*": este campo possui o seguinte conteúdo:
        - "*eContentType*": contém o OID que especifica o tipo de conteúdo
        - "*eContent*": conteúdo propriamente dito em codificação DER
    - "*TSTInfo*": este campo possui o seguinte conteúdo:
        - "*version*": descreve a versão do carimbo do tempo (atualmente v1);
        - "*policy*": indica a política da ACT sob a qual esta resposta foi produzida;
        - "*messageImprint*": tamanho do *hash* conforme o algoritmo e o tamanho do *hash* indicado na solicitação;
        - "*serialNumber*": valor inteiro atribuído pela ACT para cada carimbo do tempo;
        - "*genTime*": instante em que o carimbo do tempo foi criado pela ACT.
        - "*accuracy*": desvio de tempo em relação ao UTC no formato *GeneralizedTime*;
        - "*ordering*": indica se existe uma ordem cronológica nos carimbos do tempo criados pela ACT;
        - "*nonce*": contém o mesmo valor do campo "*nonce*" da solicitação do carimbo do tempo;
        - "*tsa*": deve conter informações a respeito da ACT;

- "*extensions*": campo para inserir informações adicionais, conforme definido pela RFC 2459.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.02.01: Verificar se a documentação técnica do SCT descreve o formato de respostas de carimbo do tempo suportado.

Nota: Os ensaios referentes ao formato de resposta de carimbo do tempo são executados como parte da Seção 2.6.

2.1.2 Requisitos de Servidor de Carimbo do Tempo

REQUISITO I.3: Um Servidor de Carimbo do Tempo (SCT) deve ser compatível com o modelo geral da estrutura de carimbo do tempo da ICP-Brasil.

Nota: Este requisito é testado como parte da seção 2.1 à 2.7.

REQUISITO I.4: A documentação técnica deve especificar a versão, características e funcionalidades da aplicação de carimbo do tempo instalada no Servidor de Carimbo do Tempo.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.04.01: Verificar se a documentação técnica do SCT descreve a versão, características e funcionalidades da aplicação de carimbo do tempo instalada no Servidor de Carimbo do Tempo (SCT).

2.1.3 Requisitos de Sistema de Auditoria e Sincronismo

REQUISITO I.5: Um Sistema de Auditoria e Sincronismo (SAS) deve ser compatível com o modelo geral da estrutura de carimbo do tempo da ICP-Brasil.

Nota: Este requisito é testado como parte da seção 2.1 à 2.7.

REQUISITO I.6: A documentação técnica deve especificar a versão, características e funcionalidades da aplicação de auditoria e sincronismo instalada no Sistema de Auditoria e Sincronismo.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.06.01: Verificar se a documentação técnica do SAS descreve a versão, características e funcionalidades da aplicação de auditoria e sincronismo instalada no Sistema de Auditoria e Sincronismo (SAS).

REQUISITO I.7: Um SAS deve possuir mecanismos que permitam sua sincronização com a Fonte Confiável do Tempo conforme a estrutura de carimbo do tempo da ICP-Brasil.

Nota: Este requisito é testado como parte da seção 2.4.

2.1.4 Requisitos de certificação digital

Na estrutura de carimbo do tempo da ICP-Brasil, existem 3 tipos de Certificados digitais:

- Certificado digital ICP-Brasil de Servidor de Carimbo do Tempo;
- Certificado digital ICP-Brasil de Servidor de Auditoria e Sincronismo;
- Certificado digital de Atributo (também conhecido como alvará).

Exceto quando especificado, os requisitos gerais de certificação digital aplicam-se somente aos 2 primeiros tipos de certificados digitais.

REQUISITO I.8: Um SCT deve ser compatível com certificados digitais ICP-Brasil de equipamento, tipos T3 e T4.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.08.01: Verificar se a documentação técnica do SCT descreve a compatibilidade com certificados digitais ICP-Brasil de equipamentos, tipos T3 e T4.

EN.I.08.02: Por meio de inspeção direta, verificar se o SCT suporta certificados digitais ICP-Brasil de equipamentos, tipos T3 e T4.

REQUISITO I.9: Um SCT deve utilizar certificados digitais ICP-Brasil T3 ou T4 somente para fins de assinatura digital de carimbos do tempo.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.09.01: Verificar se a documentação técnica do SCT descreve a utilização de certificados digitais ICP-Brasil de equipamentos, tipos T3 e T4, para fins de assinatura digital de carimbo do tempo.

Nota: Os propósitos do certificado digital ICP-Brasil utilizado para fins de assinatura digital de carimbo do tempo são testados como parte do **REQUISITO VII.4**.

REQUISITO I.10: Uma aplicação de carimbo do tempo contida em um SCT deve ser capaz de manipular certificados digitais que implementam a versão 3 do padrão ITU-T X.509 (X.509v3). Especificamente para certificados digitais ICP-Brasil de SCT, designados somente para fins de assinatura digital de carimbos do tempo, as seguintes extensões são obrigatórias:

- "*Authority Key Identifier*": campo que deve conter o *hash* SHA-1 da chave pública da AC;
- "*Key Usage*": define o propósito da chave criptográfica contida no certificado digital. Dado que este é um certificado digital para fins de assinatura digital, somente os *bits digitalSignature* e *nonRepudiation* devem estar ativos;
- "*Extended Key Usage*": define uma extensão do propósito da chave criptográfica contida no certificado digital. Dado que este é um certificado digital para fins de assinatura digital de carimbo do tempo, deve conter o OID referente ao propósito *id-kp-timeStamping*. Esta extensão deve ser considerada como crítica e o OID correspondente é o 1.3.6.1.5.5.7.3.8;
- "*Certificate Policies*": deve conter o OID da PC correspondente e a URL da DPC da AC que emitiu o certificado digital;

- "*CRL Distribution Points*": deve conter a URL onde está publicada a LCR correspondente;
- "*Subject Alternative Name*": permite que identidades ou características adicionais sejam associadas ao proprietário de um certificado digital.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.10.1: Verificar se a documentação técnica do SCT descreve os mecanismos que manipulam certificados digitais que implementam a versão 3 do padrão ITU-T X.509 (X.509v3).

EN.I.10.2: Por meio de inspeção direta, verificar se o SCT é capaz de manipular certificados digitais que implementam a versão 3 do padrão ITU-T X.509 (X.509v3).

REQUISITO I.11: Um SAS deve ser compatível com certificados digitais ICP-Brasil de equipamento, tipos A3 e A4.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.11.01: Verificar se a documentação técnica do SAS descreve a compatibilidade com certificados digitais ICP-Brasil de equipamentos, tipos A3 e A4.

EN.I.11.02: Por meio de inspeção direta, verificar se o SAS suporta certificados digitais ICP-Brasil de equipamentos, tipos A3 e A4.

REQUISITO I.12: Um SAS deve utilizar certificados digitais ICP-Brasil A3 ou A4 somente para fins de assinatura digital de alvarás.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.12.1: Verificar se a documentação técnica do SAS descreve a utilização de certificados digitais ICP-Brasil de equipamentos, tipos A3 e A4, para fins de assinatura digital de alvarás.

Nota: Os propósitos do certificado digital ICP-Brasil utilizado para fins de assinatura digital de alvarás são testados como parte do **REQUISITO I.13**.

REQUISITO I.13: Uma aplicação de auditoria e sincronismo contida em um SAS deve ser capaz de manipular certificados digitais que implementam a versão 3 do padrão ITU-T X.509 (X.509v3). Especificamente para certificados digitais ICP-Brasil de SAS, designados somente para fins de assinatura digital de alvarás, as seguintes extensões são obrigatórias:

- "*Authority Key Identifier*": campo que deve conter o *hash* SHA-1 da chave pública da AC;
- "*Key Usage*": define o propósito da chave criptográfica contida no certificado digital. Dado que este é um certificado digital para fins de assinatura digital, somente os *bits digitalSignature* e *nonRepudiation* devem estar ativos;
- "*Certificate Policies*": deve conter o OID da PC correspondente e a URL da DPC da AC que emitiu o certificado digital;
- "*CRL Distribution Points*": deve conter a URL onde está publicada a LCR correspondente;
- "*Subject Alternative Name*": permite que identidades ou características adicionais sejam associadas ao proprietário de um certificado digital.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.13.1: Verificar se a documentação técnica do SAS descreve os mecanismos que manipulam certificados digitais que implementam a versão 3 do padrão ITU-T X.509 (X.509v3).

EN.I.13.2: Por meio de inspeção direta, verificar se o SAS é capaz de manipular certificados digitais que implementam a versão 3 do padrão ITU-T X.509 (X.509v3).

REQUISITO I.14: Todo certificado digital ICP-Brasil, antes de ser utilizado por um SCT ou SAS, deve ser verificado. A verificação de um certificado digital ICP-Brasil deve consistir em:

1. Realizar a validação criptográfica (verificação com a chave criptográfica assimétrica pública do assinante) da assinatura digital do certificado;
2. Verificar se o instante de seu uso está dentro do prazo de validade definido para o certificado digital;
3. Verificar se o instante de uso do certificado digital não é posterior a um instante de revogação. Caso a revogação do certificado digital não seja verificada, a aplicação do SCT ou SAS deve estar em conformidade ao **REQUISITO I.15**;
4. Verificar se o certificado digital é utilizado de acordo com seu propósito de uso definido nas extensões "*keyUsage*" e "*extendedKeyUsage*";
5. Verificar se o certificado digital é usado de acordo com a combinação entre seu propósito de uso e suas restrições básicas definidas na extensão "*Basic Constraints"*.
6. Validar o caminho de certificação conforme **REQUISITO I.16**.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.14.1: Verificar se a documentação técnica do SCT e SAS descrevem os mecanismos de verificação de certificados digitais ICP-Brasil antes da utilização.

EN.I.14.2 (Item 1 do REQUISITO I.14): Verificar se a aplicação de carimbo do tempo contida no SCT e a aplicação de auditoria e sincronismo contida em um SAS realizam a validação criptográfica da assinatura digital do certificado em duas situações distintas:

- Certificado digital íntegro;
- certificado digital não-íntegro, apresentando modificações em seu conteúdo original.

EN.I.14.3 (Item 2 do REQUISITO I.14): Verificar se a aplicação de carimbo do tempo contida no SCT e a aplicação de auditoria e sincronismo contida em um SAS realizam a verificação do instante de uso do certificado digital em relação ao seu prazo de validade em duas situações distintas:

- Certificado digital não-revogado e dentro de seu prazo de validade;
- certificado digital expirado (fora de seu prazo de validade).

EN.I.14.4 (Item 3 do REQUISITO I.14): Verificar se a aplicação de carimbo do tempo contida no SCT e a aplicação de auditoria e sincronismo contida em um SAS possibilitam validar o instante de uso do certificado digital em relação ao seu instante de revogação em duas situações distintas:

- Certificado digital não-revogado e dentro de seu prazo de validade;
- certificado digital revogado anteriormente ao seu instante de uso e dentro do seu prazo de validade.

EN.I.14.5 (Item 4 do REQUISITO I.14): Verificar se a aplicação de carimbo do tempo contida no SCT e a aplicação de auditoria e sincronismo contida em um SAS controlam a utilização do certificado digital em relação ao seu propósito de uso "*keyUsage"* nas seguintes condições:

- Certificado digital com propósitos de uso válidos para uma dada operação. Por exemplo, os propósitos *digitalSignature* e *nonRepudiation* para assinatura digital de carimbo do tempo (SCT) e alvará (SAS);
- certificado digital com propósitos de uso inválidos para uma dada operação. Por exemplo, os propósitos *keyEncipherment* e *dataEncipherment* para assinatura digital de carimbo do tempo (SCT) e alvará (SAS).

EN.I.14.6 (Item 5 do REQUISITO I.14): Verificar se os certificados digitais presentes nas aplicações de carimbos do tempo e nas aplicações de auditoria e sincronismo são usados de acordo com a combinação entre seu propósito de uso e suas restrições básicas definidas na extensão "*Basic Constraints"*.

EN.I.14.7 (Item 6 do REQUISITO I.14): Verificar se a aplicação de carimbo do tempo contida no SCT e a aplicação de auditoria e sincronismo contida em um SAS validam o caminho de certificação de seus certificados digitais conforme **REQUISITO I.16**..

REQUISITO I.15: Caso a verificação de revogação de certificados digitais não esteja habilitada, em qualquer processo de validação de certificado digital, a aplicação do SCT ou SAS deve emitir um alerta à entidade responsável indicando que a verificação de revogação não foi realizada e interromper a emissão de carimbos do tempo ou alvarás.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.15.1: Verificar se a documentação técnica do SCT e SAS descrevem os mecanismos que alertam a entidade responsável sobre a indisponibilidade de verificação de revogação de certificados digitais.

EN.I.15.2: Por meio de inspeção direta, verificar se SCT e SAS emitem alertas à entidade responsável indicando que a verificação de revogação não foi realizada e interrompendo a emissão de carimbos do tempo ou alvarás, caso a verificação de revogação de certificados digitais não esteja habilitada, em qualquer processo de validação de certificado digital.

REQUISITO I.16: Um caminho de certificação consiste em uma seqüência de “n” certificados digitais {1, ..., n}, sendo que o primeiro certificado corresponde ao da entidade considerada como “âncora de confiança”, ou seja, a AC Raiz. O n-ésimo certificado corresponde ao certificado que deve ser validado, neste caso, o de entidade final.
O processo de validação do caminho de certificação de um certificado digital deve satisfazer às seguintes condições:

- Para todo certificado digital “x” no intervalo {1, ..., n-1}, o proprietário do certificado digital “x” deve ser o emissor do certificado digital “x+1”;

- Os itens 1, 2, 3, 4 e 5 do **REQUISITO I.14** devem ser aplicados para cada certificado digital que forma o caminho de certificação avaliado, compreendendo desde o certificado digital da AC-Raiz até os certificados digitais das ACs intermediárias.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.16.1: Verificar se a documentação técnica do SCT e SAS descrevem os processos de verificação do caminho de certificação de um certificado digital.

EN.I.16.2: Verificar se a validação da relação entre o proprietário do certificado digital atual e o emissor do certificado digital subseqüente é realizado pela aplicação do SCT e SAS em duas situações distintas:

- Certificado digital com caminho de certificação completo;
- certificado digital com caminho de certificação incompleto.

EN.I.16.3: Para cada certificado digital que forma um caminho de certificação avaliado, verificar se a aplicação do SCT e SAS aplica os ensaios correspondentes aos itens 1, 2, 3, 4 e 5 do **REQUISITO I.14**.

REQUISITO I.17: Ao final do processo de verificação de um certificado digital, com relação aos requisitos constantes no **REQUISITO I.14**, a aplicação do SCT ou SAS deve ser capaz de informar à entidade responsável os problemas de não-conformidades encontrados, assim como impedir a emissão de carimbos do tempo ou alvarás respectivamente.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.17.1: Verificar se a documentação técnica do SCT e SAS descreve mecanismos de alerta à entidade responsável, devido a problemas de não conformidades encontrados no final do processo de verificação de um certificado digital.

EN.I.17.2: Por meio de inspeção direta, verificar se as aplicações do SCT e SAS emitem um alerta à entidade responsável, na presença de não conformidades em certificados digitais com relação aos requisitos constantes no **REQUISITO I.14**.

EN.I.17.3: Por meio de inspeção direta, verificar se as aplicações do SCT e SAS impede a emissão de carimbos do tempo ou alvarás, respectivamente, na presença de não conformidades em certificados digitais com relação aos requisitos constantes no **REQUISITO I.14**.

REQUISITO I.18: Uma aplicação de SCT ou SAS, deve ser capaz de identificar e mostrar à entidade responsável todos os campos específicos ICP-Brasil disponíveis em um certificado digital. Por campos específicos ICP-Brasil, ou simplesmente "campos ICP-Brasil" entende-se os seguintes campos "*otherName*" configurados no campo "*Subject Alternative Name*" do certificado digital de equipamento do SCT ou SAS:

- OID 2.16.76.1.3.8 = nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ), sem abreviações, se o certificado for de pessoa jurídica;
- OID 2.16.76.1.3.3 = Cadastro Nacional de Pessoa Jurídica (CNPJ), se o certificado for de pessoa jurídica;
- OID 2.16.76.1.3.2 = nome do responsável pelo certificado;
- OID 2.16.76.1.3.4 = nas primeiras 8 posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas onze posições subseqüentes, o Cadastro de Pessoa Física (CPF) do responsável; nas onze posições subseqüentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas quinze posições subseqüentes, o número do RG do responsável; nas 6 posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.18.1: Verificar se a documentação técnica do SCT e SAS descrevem a exibição dos campos específicos ICP-Brasil, de tal forma que permita à entidade usuária externa visualizar todos os respectivos campos especificados, por meio de parâmetros configurados no campo "*Subject Alternative Name*" do certificado digital.

EN.I.18.2: Por meio de inspeção direta, verificar se a aplicação do SCT e SAS, ao selecionar um certificado digital ICP-Brasil válido, possibilita apresentar à entidade usuária externa informações sobre todos os campos específicos ICP-Brasil, disponíveis neste certificado de acordo com o **REQUISITO I.18**.

2.2 Requisitos de segurança para SCT

Esta seção descreve requisitos relacionados à segurança de Servidores de Carimbo do Tempo (SCT). O SCT é o componente responsável por prover o serviço de carimbo do tempo, atendendo às solicitações recebidas.

De maneira geral, um SCT é constituído por um servidor (*Host*) que possui um Módulo de Segurança Criptográfico (MSC) instalado em seu interior. Como fonte de tempo para o SCT, utiliza-se um relógio de tempo real (*Real Time Clock* - RTC) localizado dentro da fronteira segura do MSC. Esta fonte de tempo é utilizada para emissão de carimbo do tempo. A Figura 2 apresenta um exemplo dos principais componentes de um SCT.

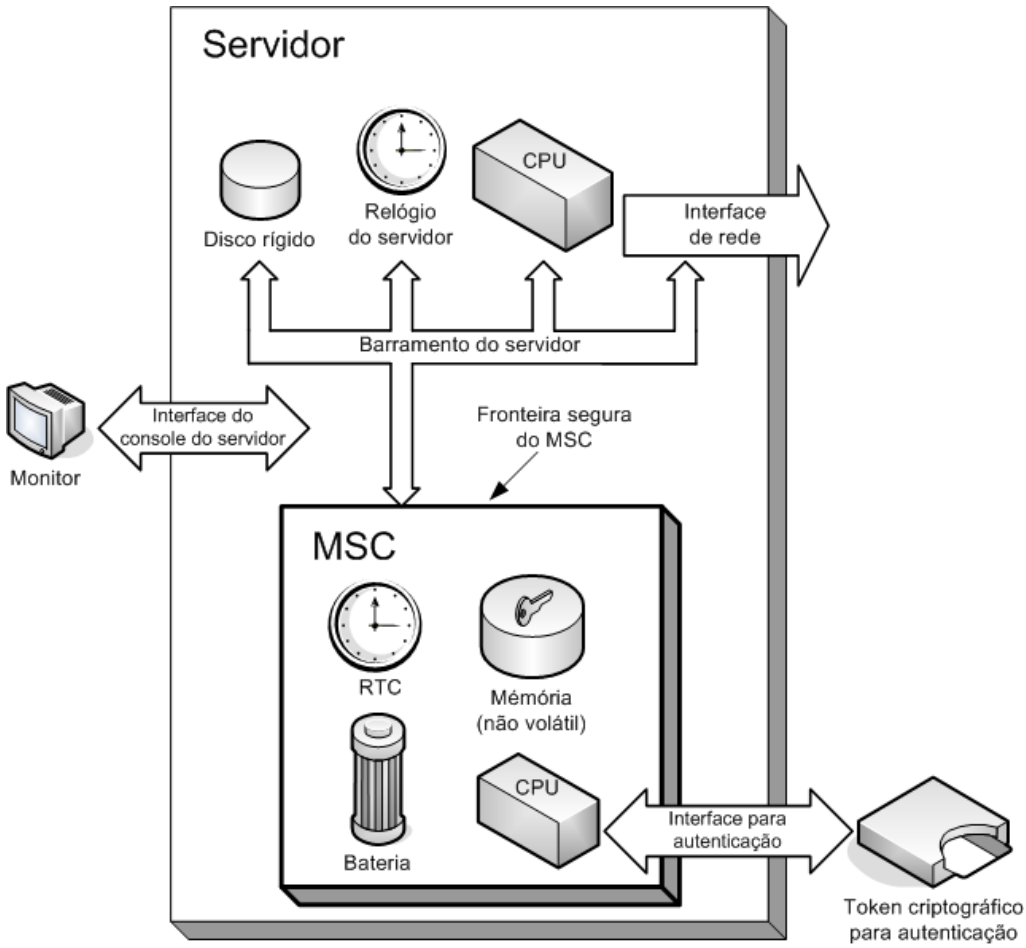

Figura 2: Principais componentes de um Servidor de Carimbo do Tempo

2.2.1 Requisitos gerais de segurança

REQUISITO II.1: Servidores de Carimbo do Tempo devem dispor de mecanismos que permitam a realização de auditorias periódicas por meio de um Servidor de Auditoria e Sincronismo (SAS).

Procedimentos de ensaio para NSH 1

EN.II.01.01: Analisar documentação técnica que descreve os mecanismos que realizam auditorias periódicas por meio de um SAS.

EN.II.01.02: Utilizando ferramenta específica, analisar a comunicação entre SCT e SAS verificando as informações de auditoria trocadas.

Procedimentos de ensaio para NSH 2 e 3:

EN.II.01.02: Analisar o código-fonte da aplicação do SCT que emite carimbo do tempo, verificando os mecanismos que realizam auditorias periódicas por meio de um SAS.

REQUISITO II.2: Um Módulo de Segurança Criptográfico (MSC) contido em um SCT deve atender aos seguintes requisitos, conforme definido no Manual de Condutas Técnicas 7 – Volume I:

- Especificação do módulo criptográfico;
- Portas e interfaces do módulo criptográfico;
- Papéis, serviços e autenticação;
- Modelo de estado finito;
- Segurança física do módulo criptográfico;
- Ambiente operacional;
- Gerenciamento de chaves criptográficas;
- Auto-testes;
- Mitigações de ataques;
- Gerenciamento.

Procedimentos de ensaio para NSH 1, 2 e 3

EN.II.02.01: Verificar se a documentação técnica sobre especificação do módulo criptográfico do MSC contido no SCT descreve a fronteira criptográfica e onde ela situa-se dentro do MSC. Por fronteira criptográfica, entende-se um perímetro que envolve qualquer hardware ou software responsável pela manipulação de parâmetros de segurança críticos que poderiam conduzir ao comprometimento de informações sensíveis se não controlados adequadamente.

EN.II.02.02: Verificar se a documentação técnica sobre serviços do MSC contido no SCT descreve as funções de segurança (incluindo a lista de funções não aprovadas pela família de padrões FIPS), operações criptográficas e modos de operação suportados.

EN.II.02.03: Verificar se a documentação técnica sobre papéis, serviços e autenticação do MSC contido no SCT descreve os papéis de acesso suportados pelo MSC, seus respectivos serviços associados e mecanismos de autenticação necessários para assumir tais papéis de acesso.

EN.II.02.04: Para cada papel de acesso suportado pelo MSC, realizar os seguintes procedimentos:

- Assumir o papel de acesso por meio dos mecanismos de autenticação solicitados;
- Executar todos os serviços associados ao papel de acesso;
- Quando aplicável, realizar tentativas de executar serviços que não são autorizados para o papel de acesso assumido;
- Efetuar o desligamento do SCT e verificar que a autenticação do papel de acesso previamente assumido foi perdida.

EN.II.02.05: Verificar se a documentação técnica sobre portas e interfaces do MSC contido no SCT descreve todas interfaces presentes no MSC, incluindo interfaces físicas e lógicas assim como os tipos de dados trafegados (dados em texto claro, chaves criptográficas e outras informações).

EN.II.02.06: Verificar se a documentação técnica sobre modelo de estado finito do MSC contido no SCT descreve todos os estados do módulo e as respectivas transições de estados. A descrição das transições de estados deve incluir condições internas do módulo, entradas de dados e controles que causam transições de um estado para outro e saídas de dados e estados resultantes das transições de um estado para outro.

EN.II.02.07: Verificar se a documentação técnica sobre segurança física do MSC contido no SCT descreve todos os mecanismos de segurança física presentes no MSC e seus respectivos componentes conforme as seguintes categorias de segurança física:

- Mecanismos mínimos de segurança física
  - Sensores de proteção para portas e interfaces físicas de manutenção que previnem contra acesso não autorizado aos componentes do MSC;
  - Obstruções em fendas de ventilação para prevenir observação/sondagem de componentes do MSC;
- Mecanismos de segurança física que evidenciam à violação
  - Coberturas e/ou camadas que evidenciem tentativas de acesso físico aos componentes do MSC;
  - Cadeados e/ou fechaduras resistentes às violações para portas e interfaces físicas de manutenção;
- Mecanismos de segurança física que resistem à violação
  - Coberturas e/ou camadas que resistem às tentativas de acesso físico aos componentes do MSC;
- Mecanismos de segurança física que detectam e respondem à violação
  - Mecanismos e/ou sensores que detectam tentativas de manipulação de componentes do módulo e respondem eliminando chaves e parâmetros críticos de segurança armazenados no MSC.

EN.II.02.08: Inspecionar o MSC contido no SCT verificando a presença e forma de atuação de cada mecanismo de segurança física.

EN.II.02.09: Realizar tentativas de penetração, sondagem, observação e manipulação de componentes do MSC contido no SCT avaliando a eficácia de cada mecanismos de segurança física, verificando se é possível extrair qualquer informação sem que o MSC se torne inoperante.

EN.II.02.10: Verificar se a documentação técnica sobre ambiente operacional do MSC contido no SCT descreve a especificação do sistema operacional (SO)

utilizado pelo MSC, assim como suas respectivas funcionalidades no que diz respeito à criação de ambientes seguros de operação.

EN.II.02.11: Realizar os procedimentos de criação de ambiente seguro conforme a documentação fornecida, observando mecanismos de segurança e controles envolvidos no processo.

EN.II.02.12: Verificar se a documentação técnica sobre gerenciamento de chaves criptográficas do MSC contido no SCT descreve como chaves criptográficas e PCSs são protegidos contra divulgação, modificação e substituição não autorizada.

EN.II.02.13: Realizar tentativas de obter acesso às chaves secretas, às chaves privadas e PCS para os quais um determinado papel de acesso não está autorizado, usando métodos específicos. O módulo deve negar o acesso ou permitir somente o acesso aos dados cifrados ou protegidos de outra forma.

EN.II.02.14: Verificar se a documentação técnica sobre auto-testes do MSC contido no SCT descreve os auto-testes realizados pelo módulo criptográfico, respectivos estados de erro, eventos que podem produzir tais estados e ações necessárias para retirar os estados de erro.

EN.II.02.15: Para cada auto-teste que puder ser invocado sob demanda, observar seus subseqüentes estados de execução com sucesso ou que levam a um estado de erro. Para auto-testes que levam a um estado de erro, observar os estados de erro alcançados e aplicar os respectivos procedimentos para remover o estado de erro e retomar a operação normal. Quando o módulo estiver em estado de erro causado por um auto-teste, verificar se é possível realizar operações criptográficas no MSC.

EN.II.02.16: Verificar se a documentação técnica sobre mitigações de ataques do MSC contido no SCT descreve proteções contra ataques não invasivos e outros tipos de ataques que possam expor informações críticas armazenadas no MSC.

EN.II.02.17: Verificar se a documentação técnica sobre gerenciamento do MSC contido no SCT descreve:

- Processos de atualização de *firmware*.
- Mecanismo de ativação do MSC;
- Utilitários de administração e diagnósticos suportados.

EN.II.02.18: Realizar os procedimentos de atualização de *firmware* conforme descrito na documentação fornecida, analisando mecanismos de segurança implementados pelo MSC para garantir a integridade do novo *firmware*.

EN.II.02.19: Realizar os procedimentos de ativação do MSC conforme descrito na documentação fornecida, verificando a aplicação de controles específicos, como por exemplo, por meio de segredo compartilhado M de N.

EN.II.02.20: Executar utilitários de administração e diagnósticos suportados pelo MSC, verificando as seguintes funcionalidades:

- Interface no idioma português do Brasil ou inglês;
- Geração e destruição de chaves criptográficas;
- Importação de chaves criptográficas;
- Visualização de certificados digitais ICP-Brasil apresentando os valores dos respectivos campos.

REQUISITO II.3: Servidores de carimbo do tempo devem possuir mecanismos que reagem contra o acesso físico não autorizado aos seus componentes internos, como por exemplo, proteções físicas instaladas em portas, tampas e outras interfaces de acesso físico. Tais mecanismos podem consistir em sensores acoplados às interfaces de acesso físico e ao interior do SCT e do MSC. Quando acionados, o SCT deve interromper a emissão de carimbos do tempo e destruir todas as chaves criptográficas armazenadas.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.03.01: Verificar se a documentação técnica do SCT descreve mecanismos que reagem contra o acesso físico não autorizado aos seus componentes internos.

EN.II.03.02: Realizar tentativas de acesso não autorizado no SCT por meio de portas, tampas e outras interfaces de acesso físico, verificando se a emissão de carimbos do tempo é interrompida e todas as chaves criptográficas armazenadas no MSC são destruídas.

REQUISITO II.4: A Parte Interessada deve fornecer documentação técnica específica que descreve a política de segurança não proprietária do MSC instalado no SCT.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.04.01: Verificar se a documentação técnica do MSC instalado no SCT descreve sua política de segurança não proprietária.

REQUISITO II.5: Após detectada uma intrusão pelo SCT, o mesmo deve entrar em um estado inoperante no qual não seja possível a emissão de carimbos do tempo. Para retirar o SCT deste estado, deve ser necessária a intervenção do super usuário ou administrador do sistema.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.05.01: Verificar se a documentação técnica do SCT descreve mecanismos que impedem a operação do SCT após a detecção de uma intrusão e suas respectivas ações para remover o SCT do estado inoperante.

EN.II.05.02: Realizar tentativas de intrusão no SCT de forma a torná-lo inoperante, observando quais ações foram necessárias para causar este efeito. Na sequência, aplicar as ações necessárias para remover o SCT do estado inoperante conforme

documentação fornecida, observando a eficácia do processo em não permitir que os mecanismos de segurança ativos sejam burlados.

REQUISITO II.6: Um SCT deve utilizar o relógio de tempo real (RTC) do MSC instalado em seu interior como fonte de tempo para emissão de carimbos do tempo. Os controles deste relógio devem ser acessados somente de forma restrita, portanto requerendo mecanismos de autenticação ou outras formas seguras de acesso.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.06.01: Verificar se a documentação técnica do SCT descreve o relógio de tempo real (RTC) do MSC instalado no interior do SCT, observando a descrição dos mecanismos que são utilizados para restringir o acesso aos controles do relógio.

EN.II.06.02: Realizar os procedimentos de alteração da hora do relógio do MSC instalado no interior do SCT por meio dos mecanismos e procedimentos descritos na documentação fornecida. Durante este processo, observar por meio de ferramenta específica a robustez dos mecanismos que restringem o acesso indevido aos controles do relógio.

REQUISITO II.7: A Parte Interessada deve fornecer documentação técnica que descreva qual o MTBF e MTRF para o SCT.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.07.01: Verificar se a documentação técnica do SCT descreve o MTBF e MTRF para o SCT.

2.2.2 Gerenciamento de chaves criptográficas

REQUISITO II.8: Chaves privadas para fins de assinatura digital de carimbos do tempo devem ser armazenadas no MSC do SCT de forma a garantir sua confidencialidade.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.08.01: Verificar se a documentação técnica do SCT descreve os mecanismos de manipulação de chaves privadas para fins de assinatura digital de carimbos do tempo.

EN.II.08.02: Por meio de ferramenta específica, observar os processos de manipulação de chaves privadas pelo SCT, verificando que somente são utilizadas as chaves privadas que estão armazenadas no MSC.

REQUISITO II.9: Cópia de segurança (*Backup*) da chave assimétrica privada de um SCT, não deve ser possível. Portanto, todo mecanismo que gera ou recupera cópias de segurança de chaves criptográficas no MSC do SCT deve estar desabilitado.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.09.01: Verificar se a documentação técnica do SCT descreve os mecanismos de gerenciamento de chaves privadas para fins de assinatura digital de carimbos do tempo.

EN.II.09.02: Por meio de inspeção direta na aplicação de gerenciamento de chaves privadas, verificar que esta não permite efetuar cópias de segurança de chaves criptográficas contidas no MSC do SCT.

2.2.3 Suporte a algoritmos

RECOMENDAÇÃO II.1: Para mitigar ataques de falsificação de carimbos do tempo, recomenda-se que um Servidor de Carimbo do Tempo utilize mecanismos de encadeamento de carimbos do tempo, como por exemplo, por meio de *Hash Tree* com base na função SHA-256.

Procedimentos de ensaio para NSH 1:

EN.REC.II.01.01: Verificar se a documentação técnica do SCT descreve os mecanismos de encadeamento de carimbos do tempo suportados pelo SCT.

Procedimentos de ensaio para NSH 2 e 3:

EN.REC.II.01.02: Por meio de inspeção direta do código-fonte da aplicação de carimbo do tempo do SCT, verificar a robustez do mecanismo de encadeamento de carimbos do tempo.

REQUISITO II.10: Para fins de assinatura digital de carimbos do tempo e resumos criptográficos (*hash*), um Servidor de Carimbo do Tempo deve oferecer suporte, no mínimo, mas não limitado aos seguintes algoritmos:

- Assinatura digital:
  - RSA/SHA-1, com tamanho de chave de 1024 e 2048 bits.
- Resumo criptográfico (*hash*):
  - SHA-1.

Procedimentos de ensaio para NSH 1:

EN.II.10.01: Verificar se a documentação técnica do SCT descreve os algoritmos de assinatura digital e resumos criptográficos suportados pelo MSC do SCT.

EN.II.10.02: Executar testes de criptografia de chave pública verificando o suporte pelo MSC do SCT ao algoritmo RSA. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas. O documento de testes de validação está organizado para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". Os testes de criptografia de chave pública consistem em:

- Teste de geração de assinaturas, que avalia a habilidade de um IUT em gerar a assinatura correta que pode ser validada pela chave pública associada.
- teste de verificação de assinaturas, que avalia a habilidade do IUT em reconhecer assinaturas válidas e inválidas;

EN.II.10.03: Executar testes de resumo criptográfico de dados verificando o suporte pelo MSC do SCT ao algoritmo SHA-1. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas. O documento de testes de validação está organizado para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". Os testes de resumo criptográfico de dados consistem em:

- Testes de mensagens curtas (*Short Message Test*), que avaliam a exatidão na geração do resumo criptográfico de dados com relação ao tamanho da mensagem de entrada;
- testes de mensagens longas selecionadas (*Selected Long Message Test*), que avaliam a exatidão na geração do resumo criptográfico para mensagens que contêm múltiplos blocos;
- testes de mensagens geradas pseudo-aleatoriamente (*Pseudorandomly generated messages test*), que verificam a exatidão dos resumos criptográficos de dados para mensagens geradas pseudo-aleatoriamente.

Procedimentos de ensaio para NSH 2 e 3:

EN.II.10.04: Executar testes de criptografia de chave pública verificando o suporte pelo MSC do SCT ao algoritmo RSA. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas. O documento de testes de validação está organizado para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". O teste de criptografia de chave pública consiste em testar a geração de chaves, avaliando a habilidade em gerar os valores corretos dos componentes do algoritmo.

2.3 Requisitos de segurança para SAS

Esta seção descreve requisitos relacionados à segurança de Sistemas de Auditoria e Sincronismo (SAS). O SAS é o componente responsável por auditar e sincronizar Servidores de Carimbo do Tempo (SCT), emitindo alvará de operação para SCTs.

De maneira geral, um SAS é constituído por um servidor (*Host*) que possui um Módulo de Segurança Criptográfica (MSC) instalado em seu interior. Como fonte de tempo para um SAS, pode-se utilizar um relógio de tempo real (*Real Time Clock* - RTC) localizado dentro da fronteira segura do MSC, ou em um módulo específico para sincronismo do tempo. Esta fonte de tempo é periodicamente sincronizada com um relógio atômico.

2.3.1 Requisitos gerais de segurança

REQUISITO III.1: Sistemas de Auditoria e Sincronismo devem dispor de mecanismos que permitam operar sincronizados periodicamente com uma Fonte Confiável do Tempo (FCT).

Procedimentos de ensaio para NSH 1

EN.III.01.01: Analisar documentação técnica do SAS que descreve os mecanismos que realizam sincronizações periódicas com uma Fonte Confiável do Tempo (FCT).

Procedimentos de ensaio para NSH 2 e 3:

EN.III.01.02: Analisar o código-fonte da aplicação do SAS que realiza auditoria e sincronismo, verificando os mecanismos que realizam sincronismos periódicos com uma Fonte Confiável do Tempo (FCT).

REQUISITO III.2: Sistemas de Auditoria e Sincronismo devem dispor de mecanismos que permitam auditar e sincronizar periodicamente Servidores de Carimbo do Tempo.

Procedimentos de ensaio para NSH 1

EN.III.02.01: Analisar documentação técnica do SAS que descreve os mecanismos que realizam auditorias e sincronizações periódicas em Servidores de Carimbo do Tempo.

Procedimentos de ensaio para NSH 2 e 3:

EN.III.02.02: Analisar o código-fonte da aplicação do SAS que realiza auditoria e sincronismo, verificando os mecanismos que realizam auditorias e sincronismos periódicos em Servidores de Carimbo do Tempo.

REQUISITO III.3: Um Módulo de Segurança Criptográfico (MSC) contido em um SAS deve atender aos seguintes requisitos, conforme definido no Manual de Condutas Técnicas 7 – Volume I:

- Especificação do módulo criptográfico;
- Portas e interfaces do módulo criptográfico;
- Papéis, serviços e autenticação;
- Modelo de estado finito;
- Segurança física do módulo criptográfico;
- Ambiente operacional;
- Gerenciamento de chaves criptográficas;
- Auto-testes;
- Mitigações de ataques;
- Gerenciamento.

Procedimentos de ensaio para NSH 1, 2 e 3

EN.III.03.01: Verificar se a documentação técnica sobre especificação do módulo criptográfico do MSC contido no SAS descreve a fronteira criptográfica e onde esta situa-se dentro do MSC. Por fronteira criptográfica, entende-se um perímetro que envolve qualquer hardware ou software responsável pela manipulação de parâmetros de segurança críticos que poderiam conduzir ao comprometimento de informações sensíveis se não controlados adequadamente.

EN.III.03.02: Verificar se a documentação técnica sobre serviços do MSC contido no SAS descreve as funções de segurança (incluindo a lista de funções não aprovadas

pela família de padrões FIPS), operações criptográficas e modos de operação suportados.

EN.III.03.03: Verificar se a documentação técnica sobre papéis, serviços e autenticação do MSC contido no SAS descreve os papéis de acesso suportados pelo MSC, seus respectivos serviços associados e mecanismos de autenticação necessários para assumir tais papéis de acesso.

EN.III.03.04: Para cada papel de acesso suportado pelo MSC, realizar os seguintes procedimentos:

- Assumir o papel de acesso por meio dos mecanismos de autenticação solicitados;
- Executar todos os serviços associados ao papel de acesso;
- Quando aplicável, realizar tentativas de executar serviços que não são autorizados para o papel de acesso assumido;
- Efetuar o desligamento do SAS e verificar que a autenticação do papel de acesso previamente assumido foi perdida.

EN.III.03.05: Verificar se a documentação técnica sobre portas e interfaces do MSC contido no SAS descreve todas interfaces presentes no MSC, incluindo interfaces físicas e lógicas assim como os tipos de dados trafegados (dados em texto claro, chaves criptográficas e outras informações).

EN.III.03.06: Verificar se a documentação técnica sobre modelo de estado finito do MSC contido no SAS descreve todos os estados do módulo e as respectivas transições de estados. A descrição das transições de estados deve incluir condições internas do módulo, entradas de dados e controles que causam transições de um estado para outro e saídas de dados e estados resultantes das transições de um estado para outro.

EN.III.03.07: Verificar se a documentação técnica sobre segurança física do MSC contido no SAS descreve todos os mecanismos de segurança física presentes no

MSC e seus respectivos componentes conforme as seguintes categorias de segurança física:

- Mecanismos mínimos de segurança física
  - Sensores de proteção para portas e interfaces físicas de manutenção que previnem contra acesso não autorizado aos componentes do MSC;
  - Obstruções em fendas de ventilação para prevenir observação/sondagem de componentes do MSC;
- Mecanismos de segurança física que evidenciam à violação
  - Coberturas e/ou camadas que evidenciem tentativas de acesso físico aos componentes do MSC;
  - Cadeados e/ou fechaduras resistentes às violações para portas e interfaces físicas de manutenção;
- Mecanismos de segurança física que resistem à violação
  - Coberturas e/ou camadas que resistem às tentativas de acesso físico aos componentes do MSC;
- Mecanismos de segurança física que detectam e respondem à violação
  - Mecanismos e/ou sensores que detectam tentativas de manipulação de componentes do módulo e respondem eliminando chaves e parâmetros críticos de segurança armazenados no MSC.

EN.III.03.08: Inspecionar o MSC contido no SAS verificando a presença e forma de atuação de cada mecanismo de segurança física.

EN.III.03.09: Realizar tentativas de penetração, sondagem, observação e manipulação de componentes do MSC contido no SAS avaliando a eficácia de cada mecanismo de segurança física, verificando se é possível extrair qualquer informação sem que o MSC se torne inoperante.

EN.III.03.10: Verificar se a documentação técnica sobre ambiente operacional do MSC contido no SAS descreve a especificação do sistema operacional (SO) utilizado pelo MSC, assim como suas respectivas funcionalidades no que diz respeito a criação de ambientes seguros de operação.

EN.III.03.11: Realizar os procedimentos de criação de ambiente seguro conforme a documentação fornecida, observando mecanismos de segurança e controles envolvidos no processo.

EN.III.03.12: Verificar se a documentação técnica sobre gerenciamento de chaves criptográficas do MSC contido no SAS descreve como chaves criptográficas e PCSs são protegidos contra divulgação, modificação e substituição não autorizada.

EN.III.03.13: Realizar tentativas de obter acesso às chaves secretas, às chaves privadas e PCS para os quais um determinado papel de acesso não está autorizado, usando métodos específicos. O módulo deve negar o acesso ou permitir somente o acesso aos dados cifrados ou protegidos de outra forma.

EN.III.03.14: Verificar se a documentação técnica sobre auto-testes do MSC contido no SAS descreve os auto-testes realizados pelo módulo criptográfico, respectivos estados de erro, eventos que podem produzir tais estados e ações necessárias para retirar os estados de erro.

EN.III.03.15: Para cada auto-teste que puder ser invocado sob demanda, observar seus subseqüentes estados de execução com sucesso ou que levam a um estado de erro. Para auto-testes que levam a um estado de erro, observar os estados de erro alcançados e aplicar os respectivos procedimentos para remover o estado de erro e retomar a operação normal. Quando o módulo estiver em estado de erro causado por um auto-teste, verificar se é possível realizar operações criptográficas no MSC.

EN.III.03.16: Verificar se a documentação técnica sobre mitigações de ataques do MSC contido no SAS descreve proteções contra ataques não invasivos e outros tipos de ataques que possam expor informações críticas armazenadas no MSC.

EN.III.03.17: Verificar se a documentação técnica sobre gerenciamento do MSC contido no SAS descreve:

- Processos de atualização de *firmware*.
- Mecanismo de ativação do MSC;
- Utilitários de administração e diagnósticos suportados.

EN.III.03.18: Realizar os procedimentos de atualização de *firmware* conforme descrito na documentação fornecida, analisando mecanismos de segurança implementados pelo MSC para garantir a integridade do novo *firmware*.

EN.III.03.19: Realizar os procedimentos de ativação do MSC conforme descrito na documentação fornecida, verificando a aplicação de controles específicos, como por exemplo, por meio de segredo compartilhado M de N.

EN.III.03.20: Executar utilitários de administração e diagnósticos suportados pelo MSC, verificando as seguintes funcionalidades:

- Interface no idioma português do Brasil ou inglês;
- Geração e destruição de chaves criptográficas;
- Importação de chaves criptográficas;
- Visualização de certificados digitais ICP-Brasil apresentando os valores dos respectivos campos.

REQUISITO III.4: Sistemas de Auditoria e Sincronismo devem possuir mecanismos que reagem contra o acesso físico não autorizado aos seus componentes internos, como por exemplo, proteções físicas instaladas em portas, tampas e outras interfaces de acesso físico. Tais mecanismos podem consistir em sensores acoplados às interfaces de acesso físico ao interior do SAS e do MSC. Quando acionados, o SAS deve interromper a realização de auditorias e sincronismo do tempo, destruindo todas as chaves criptográficas armazenadas.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.04.01: Verificar se a documentação técnica do SAS descreve mecanismos que reagem contra o acesso físico não autorizado aos seus componentes internos.

EN.III.04.02: Realizar tentativas de acesso não autorizado no SAS por meio de portas, tampas e outras interfaces de acesso físico, verificando se auditorias e sincronismo do tempo são interrompidas e todas as chaves criptográficas armazenadas no MSC são destruídas.

REQUISITO III.5: A Parte Interessada deve fornecer documentação técnica específica que descreva a política de segurança não proprietária do MSC instalado no SAS.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.05.01: Verificar se a documentação técnica do MSC instalado no SAS descreve sua política de segurança não proprietária.

REQUISITO III.6: Um Sistema de Auditoria e Sincronismo deve possuir um relógio de tempo real (RTC), seja ele interno ao MSC ou externo ao MSC situado em outro módulo mas de acesso restrito. Os controles deste relógio devem ser acessados somente de forma restrita, portanto requerendo mecanismos de autenticação ou outras formas seguras de acesso.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.06.01: Verificar se a documentação técnica do SAS descreve o relógio de tempo real (RTC), observando sua localização e a descrição dos mecanismos que são utilizados para restringir o acesso aos controles do relógio.

EN.III.06.02: Realizar os procedimentos de alteração da hora do relógio do SAS por meio dos mecanismos e procedimentos descritos na documentação fornecida.

Durante este processo, observar por meio de ferramenta específica a robustez dos mecanismos que restringem o acesso indevido aos controles do relógio.

REQUISITO III.7: Quando o relógio de tempo real do SAS se localizar em um módulo específico para sincronismo do tempo, porém interno ao SAS, a Parte Interessada deve fornecer documentação técnica específica que descreve este módulo. Esta documentação técnica específica deve contemplar tópicos sobre o acesso aos controles do relógio, segurança física contra violações, precisão e estabilidade temporal.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.06.01: Verificar se a documentação técnica do SAS descreve o relógio de tempo real (RTC) quando este consiste de um módulo interno específico, observando a descrição dos mecanismos que são utilizados para restringir o acesso aos controles do relógio, segurança física contra violações, precisão e estabilidade temporal.

REQUISITO III.8: A Parte Interessada deve fornecer documentação técnica que descreva qual o MTBF e MTRF para o SAS.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.08.01: Verificar se a documentação técnica do SAS descreve o MTBF e MTRF para o SAS.

2.3.2 Gerenciamento de chaves criptográficas

REQUISITO III.9: Cópias de segurança (*Backup*) da chave assimétrica privada de um SAS, não deve ser possível. Portanto, todo mecanismo que gera ou recupera cópias de segurança de chaves criptográficas no MSC do SAS deve estar desabilitado.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.09.01: Verificar se a documentação técnica do SAS descreve os mecanismos de gerenciamento de chaves privadas para fins de assinatura digital de alvarás.

EN.III.09.02: Por meio de inspeção direta na aplicação que gerencia chaves privadas para fins de assinatura digital de alvarás, verificar que esta não permite cópias de segurança de chaves criptográficas contidas no MSC do SAS.

2.3.3 Suporte a algoritmos

REQUISITO III.10: Para fins de assinatura digital de carimbos do tempo e resumos criptográficos (*hash*), um Servidor de Carimbo do Tempo deve oferecer suporte, no mínimo, mas não limitado aos seguintes algoritmos:

- Assinatura digital:
  - RSA/SHA-1, com tamanho de chave de 1024 e 2048 bits.
- Resumo criptográfico (*hash*):
  - SHA-1.

Procedimentos de ensaio para NSH 1:

EN.III.10.01: Verificar se a documentação técnica do SAS descreve os algoritmos de assinatura digital e resumos criptográficos suportados pelo MSC do SAS.

EN.II.10.02: Executar testes de criptografia de chave pública verificando o suporte pelo MSC do SAS ao algoritmo RSA. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas. O documento de testes de validação está organizado para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". Os testes de criptografia de chave pública consistem em:

- Teste de geração de assinaturas, que avalia a habilidade de um IUT em gerar a assinatura correta que pode ser validada pela chave pública associada.
- teste de verificação de assinaturas, que avalia a habilidade do IUT em reconhecer assinaturas válidas e inválidas;

EN.III.10.03: Executar testes de resumo criptográfico de dados verificando o suporte pelo MSC do SAS ao algoritmo SHA-1. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas. O documento de testes de validação está organizado para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". Os testes de resumo criptográfico de dados consistem em:

- Testes de mensagens curtas (*Short Message Test*), que avaliam a exatidão na geração do resumo criptográfico de dados com relação ao tamanho da mensagem de entrada;
- testes de mensagens longas selecionadas (*Selected Long Message Test*), que avaliam a exatidão na geração do resumo criptográfico para mensagens que contêm múltiplos blocos;
- testes de mensagens geradas pseudo-aleatoriamente (*Pseudorandomly generated messages test*), que verificam a exatidão dos resumos criptográficos de dados para mensagens geradas pseudo-aleatoriamente.

Procedimentos de ensaio para NSH 2 e 3:

EN.III.10.04: Executar testes de criptografia de chave pública verificando o suporte pelo MSC do SAS ao algoritmo RSA. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas. O documento de testes de validação está organizado para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". O teste de criptografia de chave pública consiste em testar a geração de chaves, avaliando a habilidade em gerar os valores corretos dos componentes do algoritmo.

2.4 Requisitos de Sincronismo do Tempo

Esta seção descreve requisitos que dizem respeito aos mecanismos de sincronismo do tempo entre um Servidor de Carimbo do Tempo (SCT) e um Sistema de Auditoria e Sincronismo (SAS). Na estrutura de carimbo do tempo da ICP-Brasil, o tempo é baseado na hora UTC difundida pelo Observatório Nacional, que representa a Fonte

Confiável do Tempo. Esta é difundida pela Autoridade Certificadora Raiz (AC-Raiz) por meio dos Sistemas de Auditoria e Sincronismo.

REQUISITO IV.1: No que diz respeito ao sincronismo do relógio dos SAS com a Fonte Confiável do Tempo baseada na hora UTC , devem existir controles para assegurar que:

- A ocorrência de perda de sincronização seja detectada pelos controles do sistema;
- O SAS deixe de emitir alvarás, caso seja constatado que seu relógio está fora da precisão estabelecida;

EN.IV.1.1: Verificar se a documentação técnica do SAS descreve controles que asseguram a detecção de perda de sincronismo do relógio e o cancelamento de emissão de alvarás, caso seja comprovado que o relógio está fora da precisão estabelecida.

EN.IV.1.2: Por meio de ferramenta específica, verificar se os controles detectam ocorrências de perda de sincronização do relógio do SAS.

EN.IV.1.3: Por meio de ferramenta específica, verificar se o SAS interrompe a emissão de alvarás ao detectar a perda de sincronismo do relógio fora da precisão estabelecida.

2.4.1 Protocolos de sincronismo do tempo

REQUISITO IV.2: A comunicação entre SAS e SCT para estabelecer um sincronismo do tempo, deve ser realizada por meio de um protocolo que prevê a autenticação mútua e o uso do protocolo NTPv3 (RFC 1305) para realizar o sincronismo do relógio do SCT com o SAS.

EN.IV.2.1: Verificar se a documentação técnica do SCT e SAS descreve o protocolo de sincronismo do tempo entre SAS e SCT e se o protocolo utilizado prevê mecanismos de autenticação mútua.

EN.IV.2.2: Por meio de ferramenta específica, verificar se o SCT e SAS suportam um protocolo que prevê autenticação mútua e o uso do protocolo NTPv3 (RFC 1305) para sincronismo do tempo.

REQUISITO IV.3: O formato de dados do protocolo de sincronismo do tempo utilizado deve ser semelhante ao descrito na RFC 1305 (NTPv3 sob protocolo UDP), contendo os campos descritos na tabela abaixo:

LI (2 bits)	***VN (3 bits)***	***Mode (3 bits)***	***Stratum (8 bits)***	***Poll (8 bits)***	***Precision (8 bits)***
Root Delay (32 bits)					
Root Dispersion (32 bits)					
Reference Identifier (32 bits)					
Reference Timestamp (64 bits)					
Originate Timestamp (64 bits)					
Receive Timestamp (64 bits)					
Transmit Timestamp (64 bits)					
Authenticator (optional) (96 bits)					

Tabela 1: Campos de dados que constituem o cabeçalho do protocolo de sincronismo NTPv3.

EN.IV.3.1: Verificar se a documentação técnica do SCT e SAS descreve o suporte ao protocolo de sincronismo NTPv3 e se este apresenta os campos de dados indicados na tabela 1.

EN.IV.3.2: Por meio de ferramenta específica, verificar se o SCT e SAS suportam o protocolo NTPv3 (RFC 1305) contendo os campos de dados indicados na tabela 1.

REQUISITO IV.4: O protocolo de sincronismo do tempo deve conter o campo LI (*Leap Indicator*), com tamanho de 2 bits, que indica a necessidade de inserção ou remoção de um *leap second* no último minuto do dia corrente por meio de bits 0 e 1, codificados da seguinte maneira:

00	Sem alerta
01	Último minuto teve 61 segundos
10	Último minuto teve 59 segundos
11	Condição de alerta (relógio não sincronizado)

Tabela 2: Códigos de resposta do campo LI definidos pela RFC 1305.

EN.IV.4.1: Verificar se a documentação técnica do SCT e SAS descreve a presença do campo LI (*Leap Indicator*) no protocolo de sincronismo suportado pelo equipamento e se está de acordo com a RFC 1305 quanto ao tamanho e os códigos de resposta do campo. Quando aplicável, a documentação técnica deve informar a utilização de tamanho ou códigos de resposta proprietários no campo LI.

EN.IV.4.2: Por meio de ferramenta específica, verificar a presença, tamanho e códigos de resposta do campo LI no protocolo de sincronismo suportado pelo equipamento, verificando a necessidade de inserção ou remoção de um *leap second* no último minuto do dia corrente.

REQUISITO IV.5: O protocolo de sincronismo do tempo deve conter o campo VN (*Version Number*), com tamanho de 3 bits (*integer*), que indica o número da versão do protocolo NTP utilizado.

EN.IV.5.1: Verificar se a documentação técnica do SCT e SAS descreve a presença do campo VN (*Version Number*) no protocolo de sincronismo suportado pelo equipamento e se está de acordo com a RFC 1305 quanto ao tamanho do campo. Quando aplicável, a documentação técnica deve informar a utilização de um tamanho proprietário no campo VN.

EN.IV.5.2: Por meio de ferramenta específica, verificar a presença e tamanho do campo VN no protocolo de sincronismo suportado pelo equipamento e se este indica a versão do protocolo NTP utilizado.

REQUISITO IV.6: O protocolo de sincronismo do tempo deve conter o campo *Mode,* com tamanho de 3 bits (*integer*), que indica o modo de operação do SAS de acordo com os seguintes valores definidos pela RFC 1305:

0	reservado
1	ativo simétrico
2	passivo simétrico
3	cliente
4	servidor
5	*broadcast*
6	reservado para mensagens de controle do NTP
7	reservado para uso privado

Tabela 3: Valores definidos pela RFC 1305 para o campo *Mode*.

EN.IV.6.1: Verificar se a documentação técnica do SCT e SAS descreve informações sobre a presença do campo *Mode* no protocolo de sincronismo suportado pelo equipamento e se está de acordo com a RFC 1305 quanto ao tamanho e aos valores do campo. Quando aplicável, a documentação técnica deve informar tamanho ou valores proprietários que identifiquem o modo de operação do SAS.

EN.IV.6.2: Por meio de ferramenta específica, verificar a presença, tamanho e valores do campo *Mode* no protocolo de sincronismo suportado pelo equipamento de modo a identificar o modo de operação do SAS.

REQUISITO IV.7: O protocolo de sincronismo do tempo deve conter o campo *Stratum*, com tamanho de 8 bits (*integer*), que indica o nível do *stratum* ao qual o SAS pertence de acordo com os valores definidos pela RFC 1305:

0	Não especificado
1	Referência primária
2 - 255	Referência secundária (via NTP)

Tabela 4: Valores definidos pela RFC 1305 para o campo *Stratum*.

EN.IV.7.1: Verificar se a documentação técnica do SCT e SAS descreve informações sobre a presença do campo *Stratum* no protocolo de sincronismo suportado pelo equipamento e se está de acordo com a RFC 1305 quanto ao tamanho e valores do campo. Quando aplicável, a documentação técnica deve informar tamanho ou valores proprietários que identifiquem o nível do s*tratum* ao qual o SAS pertence.

EN.IV.7.2: Por meio de ferramenta específica, verificar a presença, tamanho e valores do campo *Stratum* no protocolo de sincronismo suportado pelo equipamento de modo a identificar o *stratum* ao qual o SAS pertence.

REQUISITO IV.8: O protocolo de sincronismo do tempo deve conter o campo *Precision*, com tamanho de 8 bits (*integer*), que indica a precisão do relógio local.

EN.IV.8.1: Verificar se a documentação técnica do SCT e SAS descreve informações sobre a presença do campo *Precision* no protocolo de sincronismo suportado pelo equipamento e se está de acordo com a RFC 1305 quanto ao tamanho do campo. Quando aplicável, a documentação técnica deve informar tamanho ou valores proprietários que indiquem a precisão do relógio local.

EN.IV.8.2: Por meio de ferramenta específica, verificar a presença, tamanho e valores do campo *Precision* no protocolo de sincronismo suportado pelo equipamento.

REQUISITO IV.9: O protocolo de sincronismo do tempo deve conter o campo *Root Delay*, com tamanho de 32 bits (*fixed-point*), que indica o atraso total a partir da fonte de referência de tempo primária em segundos, indicando frações de tempo entre os bits 15 e 16.

Este campo pode conter valores positivos e negativos, dependendo da precisão do relógio.

EN.IV.9.1: Verificar se a documentação técnica do SCT e SAS descreve informações sobre a presença do campo *Root Delay* no protocolo de sincronismo suportado pelo equipamento e se está de acordo com a RFC 1305 quanto ao tamanho do campo. Quando aplicável, a documentação técnica deve informar tamanho ou valores proprietários que identifiquem o atraso total a partir da fonte de referência de tempo primária em segundos.

EN.IV.9.2: Por meio de ferramenta específica, verificar a presença, tamanho e valores do campo *Root Delay* no protocolo de sincronismo suportado pelo equipamento de modo a identificar o atraso total a partir da fonte de referência de tempo primária em segundos.

REQUISITO IV.10: O protocolo de sincronismo do tempo deve conter o campo *Root Dispersion*, com tamanho de 32 bits (*fixed-point*), que indica o erro máximo relativo à fonte de referência de tempo primária em segundos, indicando frações de tempo entre os bits 15 e 16. Apenas valores maiores que zero são possíveis de serem atribuídos a este campo.

EN.IV.10.1: Verificar se a documentação técnica do SCT e SAS descreve informações sobre a presença do campo *Root Dispersion* no protocolo de sincronismo suportado pelo equipamento e se está de acordo com a RFC 1305 quanto ao tamanho do campo. Quando aplicável, a documentação técnica deve informar tamanho ou valores proprietários que identifiquem o erro máximo relativo à fonte de referência de tempo primária em segundos.

EN.IV.10.2: Por meio de ferramenta específica, verificar a presença, tamanho e valores do campo *Root Dispersion* no protocolo de sincronismo suportado pelo equipamento de modo a identificar o erro máximo relativo à fonte de referência de tempo primária em segundos.

REQUISITO IV.11: O protocolo de sincronismo do tempo deve conter o campo *Reference Clock Identifier*, com tamanho de 32 bits, que identifica o relógio de referência de tempo.

EN.IV.11.1: Verificar se a documentação técnica do SCT e SAS descreve informações sobre a presença do campo *Reference Clock Identifier* no protocolo de sincronismo suportado pelo equipamento e se está de acordo com a RFC 1305 quanto ao tamanho do campo. Quando aplicável, a documentação técnica deve informar tamanho ou valores proprietários que identifiquem o relógio de referência de tempo.

EN.IV.11.2: Por meio de ferramenta específica, verificar a presença, tamanho e valores do campo *Reference Clock Identifier* no protocolo de sincronismo suportado pelo equipamento de modo a identificar o relógio de referência de tempo.

REQUISITO IV.12: O protocolo de sincronismo do tempo deve conter o campo *Reference Timestamp*, com tamanho de 64 bits, que indica a data e hora local na qual o relógio do SCT/SAS foi sincronizado pela última vez.

EN.IV.12.1: Verificar se a documentação técnica do SCT e SAS descreve informações sobre a presença do campo *Reference Timestamp* no protocolo de sincronismo suportado pelo equipamento e se está de acordo com a RFC 1305 quanto ao tamanho do campo. Quando aplicável, a documentação técnica deve informar tamanho ou valores proprietários que identifiquem a data e hora local na qual o relógio do SCT/SAS foi sincronizado pela última vez.

EN.IV.12.2: Por meio de ferramenta específica, verificar a presença, tamanho e valores do campo *Reference Timestamp* no protocolo de sincronismo suportado pelo equipamento de modo a identificar a data e hora local na qual o relógio do SCT/SAS foi sincronizado pela última vez.

REQUISITO IV.13: O protocolo de sincronismo do tempo deve conter o campo *Originate Timestamp*, com tamanho de 64 bits, que indica a data e hora local em que foi enviada a requisição de sincronismo do tempo a partir do *host* cliente para o *host* de sincronismo.

EN.IV.13.1: Verificar se a documentação técnica do SCT e SAS descreve informações sobre a presença do campo *Originate Timestamp* no protocolo de sincronismo suportado pelo equipamento e se está de acordo com a RFC 1305 quanto ao tamanho do campo. Quando aplicável, a documentação técnica deve informar tamanho ou valores proprietários que identifiquem a data e hora local em que foi enviada a requisição de sincronismo do tempo a partir do *host* cliente para o *host* de sincronismo.

EN.IV.13.2: Por meio de ferramenta específica, verificar a presença, tamanho e valores do campo *Originate Timestamp* no protocolo de sincronismo suportado pelo equipamento de modo a identificar a data e hora local em que foi enviada a requisição de sincronismo do tempo a partir do *host* cliente para o *host* de sincronismo.

REQUISITO IV.14: O protocolo de sincronismo do tempo deve conter o campo *Receive Timestamp*, com tamanho de 64 bits, que indica a data e hora local em que foi recebida a requisição de sincronismo no *host* de sincronismo.

EN.IV.14.1: Verificar se a documentação técnica do SCT e SAS descreve informações sobre a presença do campo *Receive Timestamp* no protocolo de sincronismo suportado pelo equipamento e se está de acordo com a RFC 1305 quanto ao tamanho do campo. Quando aplicável, a documentação técnica deve informar tamanho ou valores proprietários que identifiquem a data e hora local em que foi recebida a requisição de sincronismo no *host* de sincronismo.

EN.IV.14.2: Por meio de ferramenta específica, verificar a presença, tamanho e valores do campo *Receive Timestamp* no protocolo de sincronismo suportado pelo

equipamento de modo a identificar a data e hora local em que foi recebida a requisição de sincronismo no *host* de sincronismo.

REQUISITO IV.15: O protocolo de sincronismo do tempo deve conter o campo *Transmit Timestamp*, com tamanho de 64 bits, que indica a hora local em que foi enviada a resposta a partir do *host* de sincronismo para o cliente.

EN.IV.15.1: Verificar se a documentação técnica do SCT e SAS descreve informações sobre a presença do campo *Transmit Timestamp* no protocolo de sincronismo suportado pelo equipamento e se está de acordo com a RFC 1305 quanto ao tamanho do campo. Quando aplicável, a documentação técnica deve informar tamanho ou valores proprietários que identifiquem a hora local em que foi enviada a resposta a partir do *host* de sincronismo para o cliente.

EN.IV.15.2: Por meio de ferramenta específica, verificar a presença, tamanho e valores do campo *Transmit Timestamp* no protocolo de sincronismo suportado pelo equipamento de modo a identificar a hora local em que foi enviada a resposta a partir do *host* de sincronismo para o cliente.

2.4.2 Exatidão do relógio

REQUISITO IV.16: O fabricante deve informar a exatidão do relógio do SCT e SAS, indicando a incerteza associada.

EN.IV.16.1: Verificar se a documentação técnica do SCT e SAS descreve a exatidão do relógio indicando a incerteza associada.

2.5 Requisitos de gerenciamento e auditoria de ACTs

Esta seção descreve requisitos relacionados aos processos de gerenciamento das atividades de uma Autoridade de Carimbo do Tempo. Tais processos, são praticados por uma ACT para que sejam compiladas informações relevantes para os processos de auditoria.

Também são descritos requisitos relacionados ao Alvará emitido pela Entidade de Auditoria de Tempo (EAT), a qual é representada pela Autoridade Certificadora Raiz

(AC-Raiz) dentro da estrutura de carimbo do tempo da ICP-Brasil. A EAT realiza auditorias periódicas nos Servidores de Carimbo do Tempo (SCT) das ACTs, por meio de Sistemas de Auditoria e Sincronismo (SAS). A finalidade deste processo, além de garantir o sincronismo entre os relógios dos SCTs das ACTs e a Fonte Confiável do Tempo baseada na hora UTC (ON), também é a de garantir que os carimbos do tempo emitidos por um SCT estejam com a hora mais próxima possível da hora UTC.

Em suma, o processo de auditoria de SCTs consiste em duas etapas:

- Verificação de sincronismo entre o relógio do SCT e SAS;
- Emissão de um alvará, caso o relógio do SCT apresente um erro no tempo em relação ao SAS dentro do valor especificado na Política de Carimbo do Tempo. Caso contrário, o alvará não é emitido.

2.5.1 Registros

REQUISITO V.1: Qualquer atividade que corresponda aos procedimentos de auditoria e/ou sincronismo deve ser devidamente registrada pelo SCT e SAS simultaneamente e armazenada em arquivos (*log*) no formato UTF-8 ou ASCII, para posterior acesso pela EAT.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.1.1: Verificar se a documentação técnica do SCT e SAS descreve o suporte à geração simultânea de arquivos de registro (*log*) quando são executados procedimentos de auditoria e/ou sincronismo.

EN.V.1.2: Verificar se a documentação técnica do SCT e SAS descreve informações sobre o formato utilizado (UTF-8 ou ASCII) nos arquivos de registro (*log*), além de como e onde é feito seu armazenamento.

EN.V.1.3: Por meio de ferramenta específica, verificar se os arquivos de registro (*logs*) armazenados no SCT e SAS foram gerados simultaneamente com relação aos procedimentos de auditoria e/ou sincronismo.

REQUISITO V.2: Os arquivos de registro (*log*) armazenados no SAS, referentes à autenticação mútua com o SCT, devem conter no mínimo as seguintes informações:

- Data e hora de realização da autenticação;
- Erro do relógio do SCT;
- Retardo;
- Endereço de rede do SAS (auditor);
- Endereço de rede do SCT (auditado);
- Identificação do certificado digital do SCT;
- Identificação do alvará;
- Mensagem de aviso ou de erro.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.2.1: Verificar se a documentação técnica do SAS descreve quais informações são listadas nos arquivos de registro (*log*), armazenados no SAS, referentes à autenticação mútua com o SCT.

EN.V.2.2: Por meio de ferramenta específica, verificar se os arquivos de registro (*log*) armazenados pelo SAS, referentes à autenticação mútua com o SCT, contém as seguintes informações:

- Data e hora de realização da autenticação;
- Erro do relógio do SCT;
- Retardo;
- Endereço de rede do SAS (auditor);
- Endereço de rede do SCT (auditado);
- Identificação do certificado digital do SCT;
- Identificação do alvará;
- Mensagem de aviso ou de erro.

REQUISITO V.3: Os arquivos de registro (*log*) armazenados no SCT, referentes à autenticação mútua com o SAS, devem conter no mínimo as seguintes informações:

- Data e hora de realização da autenticação;

- Erro do relógio do SCT;
- Retardo;
- Endereço de rede do SAS (auditor);
- Endereço de rede do SCT (auditado);
- Identificação do certificado digital do SAS;
- Identificação do alvará;
- Mensagem de aviso ou de erro.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.3.1: Verificar se a documentação técnica do SCT descreve quais informações são listadas nos arquivos de registro (*log*), armazenados no SCT, referentes à autenticação mútua com o SAS.

EN.V.3.2: Por meio de ferramenta específica, verificar se os arquivos de registro (*log*) armazenados pelo SCT, referentes à autenticação mútua com o SAS, contém as seguintes informações:

- Data e hora de realização da autenticação;
- Erro do relógio do SCT;
- Retardo;
- Endereço de rede do SAS (auditor);
- Endereço de rede do SCT (auditado);
- Identificação do certificado digital do SAS;
- Identificação do alvará;
- Mensagem de aviso ou de erro.

REQUISITO V.4: Os arquivos de registro (*log*) armazenados no SCT e SAS, referentes ao processo de sincronismo, devem conter no mínimo as seguintes informações:

- Data e hora de realização do sincronismo;
- Erro do relógio do SCT;
- Retardo;

- Endereço de rede do SAS (auditor);
- Endereço de rede do SCT (auditado).

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.4.1: Verificar se a documentação técnica do SCT e SAS descreve quais informações são listadas nos arquivos de registro (*log*), armazenados no SCT e SAS, referentes ao processo de sincronismo.

EN.V.4.2: Por meio de ferramenta específica, verificar se os arquivos de registro (*log*) armazenados no SCT e SAS, referentes ao processo de sincronismo, contêm as seguintes informações:

- Data e hora de realização do sincronismo;
- Erro do relógio do SCT;
- Retardo;
- Endereço de rede do SAS (auditor);
- Endereço de rede do SCT (auditado).

REQUISITO V.5: A ACT deve prover uma interface para auditoria de seus SCTs, por meio de uma interface segura e autenticada. Esta interface deve possibilitar o acesso aos registros produzidos em eventos dos SCTs.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.5.1: Verificar se a documentação técnica do SCT descreve qual a interface disponibilizada para auditoria do equipamento, descrevendo as características e configurações de segurança e autenticação desta interface.

EN.V.5.2: Verificar, por meio de ferramenta específica, se a interface disponibilizada pelo SCT permite sua auditoria por meio de uma interface segura e autenticada.

REQUISITO V.6: A Parte Interessada deve fornecer documentação técnica que descreva qual o período de tempo para armazenamento dos logs dos eventos do SCT.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.6.1: Verificar se a documentação técnica do SCT descreve qual o período de tempo para armazenamento dos arquivos de log dos eventos do SCT.

REQUISITO V.7: A Parte Interessada deve fornecer documentação técnica que descreva qual o período de tempo para armazenamento dos logs dos eventos do SAS.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.7.1: Verificar se a documentação técnica do SAS descreve qual o período de tempo para armazenamento dos arquivos de log dos eventos do SAS.

2.5.2 Alvará

REQUISITO V.8: O alvará emitido por um SAS deve possuir campos de acordo com o seguinte formato, conforme definido pela RFC 3281:

A estrutura principal do alvará deve apresentar o seguinte formato:

```
AttributeCertificate ::= SEQUENCE {
        acinfo                AttributeCertificateInfo,
        signatureAlgorithm    AlgorithmIdentifier,
        signatureValue        BIT STRING
}
```

A estrutura *AttributeCertificateInfo* deve apresentar o seguinte conteúdo:

```
AttributeCertificateInfo ::= SEQUENCE {
        version                 AttCertVersion,
        holder                  Holder,
        issuer                  AttCertIssuer,
        signature               AlgorithmIdentifier,
```

```
        serialNumber            CertificateSerialNumber,
        attrCertValidityPeriod  AttCertValidityPeriod,
        attributes              SEQUENCE OF Attribute,
        issuerUniqueID          UniqueIdentifier OPTIONAL,
        extensions              Extensions OPTIONAL
}
```

Os campos *version*, *holder*, *issuer* e *attrCertValidityPeriod* devem apresentar o seguinte conteúdo, respectivamente:

```
AttCertVersion ::= INTEGER { v2(1) }
Holder ::= SEQUENCE {
        baseCertificateID   [0] IssuerSerial OPTIONAL,
        entityName          [1] GeneralNames OPTIONAL,
        objectDigestInfo    [2] ObjectDigestInfo OPTIONAL
}
AttCertIssuer ::= CHOICE {
        v1Form              GeneralNames,
        v2Form              [0] V2Form
}
AttCertValidityPeriod ::= SEQUENCE {
        notBeforeTime       GeneralizedTime,
        notAfterTime        GeneralizedTime
}
```

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.8.1: Verificar se a documentação técnica do SAS descreve os campos do alvará emitido por ele e se estes campos estão de acordo com a RFC 3281.

EN.V.8.2: Verificar, por meio de ferramenta específica, se os campos do alvará estão de acordo com a RFC 3281.

REQUISITO V.9: O campo *version* da estrutura *AttributeCertificateInfo* deve possuir o valor *v2* que indica que a versão do certificado de atributo é compatível com as definições do padrão x.509 (2000).

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.9.1: Verificar se a documentação técnica do SCT e SAS descreve o campo *version* da estrutura *AttributeCertificateInfo* do alvará.

EN.V.9.2: Por meio de ferramenta específica, verificar se o campo *version* da estrutura *AttributeCertificateInfo* do alvará possui o valor *v2*.

RECOMENDAÇÃO V.1: Para evitar problemas na interpretação do campo *holder* da estrutura *AttributeCertificateInfo* recomenda-se que este campo possua apenas a opção *baseCertificateID*. Esta opção deve conter o nome e o número de série do certificado digital do SCT.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.V.1.1: Verificar se a documentação técnica do SCT e SAS descreve o campo *holder* da estrutura *AttributeCertificateInfo* do alvará.

EN.REC.V.1.2: Por meio de ferramenta específica, verificar no alvará quais opções o campo *holder* da estrutura *AttributeCertificateInfo* disponibiliza e se este campo contém o nome e número de série do certificado digital do SCT.

REQUISITO V.10: O campo *issuer* da estrutura *AttributeCertificateInfo* deve conter a opção *V2Form*. Neste caso a opção *V2Form* deve conter os seguintes campos:

- *issuerName*: presente;
- *baseCertificateID*: obrigatoriamente ausente;
- *objectDigestInfo*: obrigatoriamente ausente.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.10.1: Verificar se a documentação técnica do SCT e SAS descreve o campo *issuer* da estrutura *AttributeCertificateInfo* do alvará.

EN.V.10.2: Por meio de ferramenta específica, verificar se o campo *issuer* da estrutura *AttributeCertificateInfo* possui a opção *V2Form* e se esta apresenta os campos:

- *issuerName*: presente;
- *baseCertificateID*: obrigatoriamente ausente;
- *objectDigestInfo*: obrigatoriamente ausente.

REQUISITO V.11: O campo *signature* da estrutura *AttributeCertificateInfo* deve conter um identificador do algoritmo utilizado para verificar a assinatura digital do certificado de atributo.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.11.1: Verificar se a documentação técnica do SAS e SCT descreve o campo *signature* da estrutura *AttributeCertificateInfo* do alvará.

EN.V.11.2: Por meio de ferramenta específica, verificar se o campo *signature* da estrutura *AttributeCertificateInfo* do alvará contém um identificador do algoritmo utilizado para verificar a assinatura digital do certificado de atributo.

REQUISITO V.12: O campo *serialNumber* da estrutura *AttributeCertificateInfo* deve conter o número de série do alvará, sendo este representado por valores inteiros positivos grandes, obtendo-se assim a unicidade deste valor. Este valor não deve ultrapassar um tamanho de 20 octetos.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.12.1: Verificar se a documentação técnica do SCT e SAS descreve o tamanho do campo *serialNumber* da estrutura *AttributeCertificateInfo* do alvará.

EN.V.12.2: Verificar, por meio de ferramenta específica, se o campo *serialNumber* da estrutura *AttributeCertificateInfo* contém o número de série do alvará.

REQUISITO V.13: O campo *attrCertValidityPeriod* da estrutura *AttributeCertificateInfo* deve possuir os campos *notBeforeTime* e *notAfterTime* a serem preenchidos com valores do tipo *GeneralizedTime*. Estes valores *GeneralizedTime* devem ser representados no formato UTC definido como YYYYMMDDHHMMSS onde as frações de segundo não devem ser indicadas.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.13.1: Verificar se a documentação técnica do SCT e SAS descreve o campo *attrCertValidityPeriod* da estrutura *AttributeCertificateInfo* do alvará.

EN.V.13.2: Por meio de ferramenta específica, verificar se o campo *attrCertValidityPeriod* da estrutura *AttributeCertificateInfo* possui os campos *notBeforeTime* e *notAfterTime* e se estão preenchidos com valores do tipo *GeneralizedTime*.

REQUISITO V.14: O campo *attributes* da estrutura *AttributeCertificateInfo*, deve conter no mínimo os seguintes atributos:

- *Delay*: Deve conter o tempo gasto no processo de comunicação com a EAT, neste caso representada pela AC-Raiz;
- *OffSet*: Deve conter a diferença de tempo entre o relógio do SCT e a EAT;
- *Max Offset*: Representa a máxima diferença permitida entre o relógio do SCT e a EAT;
- Status do processo de auditoria.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.14.1: Verificar se a documentação técnica do SCT e SAS descreve o campo *attributes* da estrutura *AttributeCertificateInfo* no que diz respeito aos atributos suportados.

EN.V.14.2: Verificar, por meio de ferramenta específica, se o campo *attributes* da estrutura *AttributeCertificateInfo* possui, no mínimo, os seguintes atributos:

- *Delay*: Deve conter o tempo gasto no processo de comunicação com a EAT, neste caso representada pela AC-Raiz;
- *OffSet*: Deve conter a diferença de tempo entre o relógio do SCT e a EAT;
- *Max Offset*: Representa a máxima diferença permitida entre o relógio do SCT e a EAT;
- Status do processo de auditoria.

RECOMENDAÇÃO V.2: Opcionalmente o campo *attributes* da estrutura *AttributeCertificateInfo*, pode conter os seguintes atributos:

- *Max Delay*: Representa o máximo atraso permitido no recebimento de uma auditoria;
- Agendamento do *leap second*: Quando aplicável, deve conter a data de agendamento do segundo adicionado ao UTC para compensar o atraso da rotação da Terra e manter a hora UTC em sincronismo com o tempo solar;

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.V.2.1: Verificar se a documentação técnica do SCT e SAS descreve o campo *attributes* da estrutura *AttributeCertificateInfo* no que diz respeito aos atributos recomendados pela **RECOMENDAÇÃO V.2**.

EN.REC.V.2.2: Por meio de ferramenta específica, verificar a presença dos atributos *Max Delay* e Agendamento do *leap second* no campo *attributes* da estrutura *AttributeCertificateInfo*.

REQUISITO V.15: Um SCT só pode emitir carimbos do tempo durante a vigência do alvará recebido.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.15.1: Verificar se a documentação técnica do SCT descreve os controles sobre a emissão de carimbos do tempo, no que diz respeito à vigência do alvará.

EN.V.15.2: Por meio de ferramenta específica, verificar se a emissão de carimbos do tempo é permitida apenas durante a vigência do alvará recebido.

REQUISITO V.16: Caso o alvará recebido por um SCT expire, o mesmo deve automaticamente interromper a emissão de carimbos do tempo, até o recebimento de um novo alvará válido.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.16.1: Verificar se a documentação técnica do SCT descreve os controles sobre a emissão de carimbos do tempo, no que diz respeito à data de expiração do alvará.

EN.V.16.2: Por meio de ferramenta específica, verificar se a emissão de carimbos do tempo é interrompida com o alvará expirado e se a emissão continua interrompida até o recebimento de um novo alvará válido.

REQUISITO V.17: Caso o alvará recebido por um SCT possua período de validade igual a zero, o SCT deve ser capaz de interpretar esta informação como uma indicação de que seu relógio está fora de sua precisão pré-estabelecida e deve interromper a emissão de carimbos do tempo.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.17.1: Verificar se a documentação técnica do SCT descreve os controles sobre a emissão de carimbos do tempo, no que diz respeito ao período de validade alvará.

EN.V.17.2: Por meio de ferramenta específica, verificar se o SCT ao receber um alvará com período de validade igual a zero interrompe a emissão de carimbos do tempo e identifica que está fora de sua precisão pré-estabelecida.

REQUISITO V.18: Um SAS deve emitir um alvará com período de validade não nulo somente se, no intervalo de tempo entre duas auditorias sucessivas, o relógio de um SCT não apresentar erro (*Offset*) acumulado que ultrapasse o valor especificado na Política de Carimbo do Tempo correspondente.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.18.1: Verificar se a documentação técnica do SAS descreve as condições para emissão de um alvará com período de validade não nulo.

EN.V.18.2: Por meio de ferramenta específica, verificar se o SAS emite alvarás com período de validade não nulo somente caso o relógio do SCT não apresentar erro (*Offset*) acumulado maior que o valor especificado na Política de Carimbo do Tempo.

EN.V.18.3: Por meio de ferramenta específica, verificar se o SAS emite alvarás com período de validade nulo caso o relógio do SCT apresentar erro (*Offset*) acumulado maior que o valor especificado na Política de Carimbo do Tempo.

REQUISITO V.19: Cada SCT deve ser capaz de ser auditado por pelo menos dois SAS distintos e situados em locais físicos diferentes.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.19.1: Verificar se a documentação técnica do SCT descreve a capacidade de ser auditado por pelo menos dois SAS distintos e quais as configurações que devem ser feitas para que esta auditoria seja suportada.

EN.V.19.2: Por meio de inspeção direta, verificar se o SCT suporta o recebimento de auditorias por dois SAS distintos.

REQUISITO V.20: Um SAS deve permitir a configuração da periodicidade de auditoria e sincronismo com um SCT.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.20.1: Verificar se a documentação técnica do SAS descreve configurações da periodicidade de auditoria e sincronismo com um SCT.

EN.V.20.2: Por meio de inspeção direta, verificar como é feita a configuração da periodicidade de auditoria e sincronismo com um SCT.

REQUISITO V.21: Um SCT deve permitir auditoria e sincronismo com um SAS das seguintes formas:

- Por intervenção direta do administrador, onde o SCT solicita ao SAS que se inicie o processo de auditoria e sincronismo;
- De forma automática, onde o SAS inicia o processo de auditoria e sincronismo de forma periódica conforme seus próprios controles.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.21.1: Verificar se a documentação técnica do SCT descreve os modos de auditoria permitidos de acordo com o **REQUISITO V.21**.

EN.V.21.2: Por meio de inspeção direta, verificar os modos de auditoria e sincronismo permitidos e suportados pelo SCT.

REQUISITO V.22: Um SAS deve permitir que se inicie o processo de auditoria e sincronismo sob demanda, como por exemplo, por meio da intervenção direta do administrador do SAS.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.22.1: Verificar se a documentação técnica do SAS descreve o processo de auditoria e sincronismo sob demanda.

EN.V.22.2: Por meio de inspeção direta, verificar se o SAS permite o processo de auditoria e sincronismo sob demanda.

REQUISITO V.23: Um SAS deve permitir a configuração dos parâmetros exatidão (*accuracy*) e atraso (*delay*) conforme a Política de Carimbo do Tempo vigente.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.23.1: Verificar se a documentação técnica do SAS descreve as configurações dos parâmetros exatidão (*accuracy*) e atraso (*delay*).

EN.V.23.2: Por meio de inspeção direta, verificar se o SAS permite configurar os parâmetros exatidão (*accuracy*) e atraso (*delay*) conforme a Política de Carimbo do Tempo vigente.

2.5.3 Requisitos específicos de auditoria de ACTs

REQUISITO V.24: SCT e SAS devem registrar em arquivos eletrônicos de auditoria todos os eventos relacionados à segurança destes sistemas. Entre outros, os seguintes eventos devem obrigatoriamente estar incluídos nos registros:

- Iniciação e desligamento do SCT;
- Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da ACT;
- Mudanças na configuração do SCT ou nas suas chaves;

- Mudanças nas políticas de criação de carimbos do tempo;
- Tentativas de acesso (*login*) e de saída do sistema (*logoff*);
- Tentativas não-autorizadas de acesso aos arquivos de sistema;
- Geração de chaves próprias do SCT e demais eventos relacionados com o ciclo de vida destes certificados;
- Emissão de carimbos do tempo;
- Tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas e de atualizar e recuperar suas chaves;
- Operações que resultem em falhas de escrita ou leitura, quando aplicável;
- Todos os eventos relacionados à sincronização dos relógios dos SCT com a FCT, incluindo no mínimo:
  - a própria sincronização;
  - desvio de tempo ou retardo de propagação acima de um valor especificado;
  - falta de sinal de sincronização;
  - tentativas de autenticação mal-sucedidas;
  - detecção da perda de sincronização.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.24.1: Verificar se a documentação técnica do SCT e SAS descreve como são feitos os registros em arquivos eletrônicos de todos os eventos relacionados à segurança destes sistemas, incluindo obrigatoriamente os eventos citados no **REQUISITO V.24**.

EN.V.24.2: Por meio de inspeção direta, verificar se todos os eventos de segurança, incluindo os obrigatórios descritos no **REQUISITO V.24**, são registrados em arquivos eletrônicos de auditoria.

REQUISITO V.25: Nos registros de auditoria, devem estar especificadas a identidade do agente que o causou, bem como a data e horário do evento. Registros de auditoria eletrônicos devem conter o respectivo horário UTC associado.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.25.1: Verificar se a documentação técnica do SCT e SAS descreve se os registros de auditora especificam a identidade do agente que o causou, bem como a data e horário do evento com o respectivo horário UTC associado.

EN.V.25.2: Por meio de inspeção direta, verificar se nos registros de auditoria estão especificadas a identidade do agente que o causou, bem como a data e horário do evento contendo o respectivo horário UTC associado.

REQUISITO V.26: Quanto à proteção de registros (*logs*) de auditoria, o SCT e SAS devem empregar mecanismos no sistema de registro de eventos para proteger registros e informações de auditoria contra acesso não autorizado, modificação e remoção.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.26.1: Verificar se a documentação técnica do SCT e SAS descreve como os registros de auditoria são protegidos contra acesso não autorizado, modificação e remoção.

EN.V.26.2: Por meio de ferramenta específica, verificar se os registros de auditoria são protegidos contra acesso não autorizado, modificação e remoção.

2.6 Requisitos de solicitação de carimbo do tempo

Esta seção descreve os requisitos relacionados à solicitação de carimbo do tempo que é submetida ao SCT quando se deseja carimbar temporalmente um documento eletrônico.

REQUISITO VI.1: Para o escopo definido por este documento, uma solicitação de carimbo do tempo deve apresentar o valor 1 no campo *version*.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VI.1.1: Verificar se a documentação técnica descreve o valor do campo *version*, na solicitação de carimbo do tempo.

EN.VI.1.2: Utilizando uma ferramenta específica, verificar se o campo *version* apresenta o valor 1, na solicitação de carimbo do tempo.

REQUISITO VI.2: Uma solicitação de carimbo do tempo deve apresentar no campo *hashAlgorithm* os parâmetros que identificam o algoritmo de *hash* utilizado para obter o campo *hashedMessage*. Por exemplo, o uso do algoritmo SHA-1 deve apresentar os seguintes valores:

- 1.3.14.3.2.26 que corresponde ao *Object Identifier* (OID) do algoritmo SHA-1;
- nulo (NULL) ou ausente que corresponde ao "*parameter*" do algoritmo SHA-1.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VI.02.01: Analisar a documentação técnica e identificar o algoritmo *hash* utilizado para obter o campo *hashedMessage* contido na solicitação de carimbo do tempo.

EN.VI.2.2: Utilizando uma ferramenta específica, verificar se o campo *hashAlgorithm* apresenta os parâmetros que identificam o algoritmo de *hash* utilizado para obter o campo *hashedMessage* presente na solicitação de carimbo do tempo.

EN.VI.2.3: Analisar se o algoritmo de *hash* identificado na documentação técnica por meio do ensaio **EN.VI.2.1** e os parâmetros que identificam o algoritmo de *hash* identificados por meio do ensaio **EN.VI.2.2** estão consistentes.

REQUISITO VI.3: O *hash* contido no campo *hashedMessage* de uma solicitação de carimbo do tempo deve ser representado por uma sequência de *bytes* cujo tamanho deve corresponder aquele associado ao respectivo algoritmo *hash*.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VI.3.1: Analisar a documentação técnica e identificar o tamanho do *hash* contido no campo *hashedMessage* presente na solicitação de carimbo do tempo.

EN.VI.3.2: Utilizando uma ferramenta específica, verificar o tamanho do *hash* contido no campo *hashedMessage* presente na solicitação de carimbo do tempo.

EN.VI.3.3: Analisar se o tamanho do *hash* identificado na documentação técnica por meio do ensaio **EN.VI.3.1** e o tamanho do *hash* identificado por meio do ensaio **EN.VI.3.2** estão consistentes.

REQUISITO VI.4: Caso a ACT não reconheça o algoritmo *hash* conforme especificado no campo *hashAlgorithm*, ou reconheça que o algoritmo especificado é fraco, a resposta da solicitação de carimbo do tempo não deve conter o carimbo do tempo e o campo *failInfo* desta mesma resposta deve conter o valor *bad_alg* especificado.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VI.4.1: Verificar a documentação técnica e analisar se o campo *failInfo* é preenchido com o valor *bad_alg* caso a ACT não reconheça o algoritmo de *hash* especificado no campo *hashAlgorithm*, ou reconheça que o algoritmo especificado é fraco.

EN.VI.4.2: Utilizando uma ferramenta específica, verificar se o campo *failInfo* é preenchido com o valor *bad_alg* caso a ACT não reconheça o algoritmo de *hash* especificado no campo *hashAlgorithm*, ou reconheça que o algoritmo especificado é fraco.

REQUISITO VI.5: O campo *reqPolicy*, quando presente em uma solicitação de carimbo do tempo, deve conter o *Object Identifier* (OID) da Política de Carimbo do Tempo (PCT) sob a qual a ACT deve emitir o carimbo do tempo solicitado.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VI.5.1: Verificar a documentação técnica e identificar se o campo *reqPolicy,* quando presente, contém o valor do *Object Identifier* (OID) da Política de Carimbo do Tempo (PCT) sob a qual a ACT deve emitir o carimbo do tempo solicitado.

EN.VI.5.2: Caso o campo *reqPolicy* esteja presente na solicitação de carimbo do tempo, utilizar uma ferramenta específica e analisar se o campo *reqPolicy* contém o valor do *Object Identifier* (OID) da Política de Carimbo do Tempo (PCT) sob a qual a ACT deve emitir o carimbo do tempo solicitado.

REQUISITO VI.6: O campo *nonce*, quando presente em uma solicitação de carimbo do tempo, deve conter um número aleatório grande, com alta probabilidade de ser gerado somente uma vez como, por exemplo, um número inteiro de 64 *bits*.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VI.6.1: Verificar a documentação técnica e identificar se o campo *nonce* está contido na solicitação de carimbo do tempo. Caso a documentação técnica descreva que o campo *nonce* está contido na solicitação de carimbo do tempo, avaliar os métodos de geração e o tamanho do número aleatório conforme **REQUISITO VI.6**.

REQUISITO VI.7: O valor do campo *nonce*, quando presente em uma solicitação de carimbo do tempo, deve ser incluído no campo "*nonce*" da resposta da solicitação.

Procedimentos de ensaio para NSH 1, 2 e 3:

Nota: A documentação referente a este requisito foi avaliada no **REQUISITO VI.6**.

EN.VI.7.1: Caso o ensaio **EN.VI.6.1** identifique a inclusão do campo *nonce* na solicitação de carimbo do tempo, utilizar uma ferramenta específica e analisar se o valor do campo *nonce* está contido no campo *"nonce"* da resposta de solicitação de carimbo do tempo.

REQUISITO VI.8: O campo *certReq*, quando presente em uma solicitação de carimbo do tempo, deve ser utilizado para solicitar o certificado da ACT na respectiva resposta da solicitação. O certificado solicitado é especificado pelo identificador *ESSCertID* dentro do atributo *SigningCertificate* da resposta desta solicitação e é fornecido pela ACT no campo *certificates* da estrutura *SignedData* da resposta.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VI.8.1: Verificar a documentação técnica e identificar se a solicitação de carimbo do tempo permite a inclusão do campo *certReq* e quais valores são aceitáveis.

EN.VI.8.2: Por meio de ferramenta específica, enviar uma solicitação de carimbo do tempo ao SCT contendo o campo *certReq.* Analisar na respectiva resposta se o campo *certificates* da estrutura *SignedData* contém o identificador *ESSCertID* dentro do atributo *SigningCertificate*.

REQUISITO VI.9: Caso o campo *certReq* não esteja presente em uma solicitação de carimbo do tempo ou contenha o valor *FALSE*, o campo *certificates* da estrutura *SignedData* não deve estar presente na resposta de carimbo do tempo solicitada.

Procedimentos de ensaio para NSH 1, 2 e 3:

Nota: A documentação referente a este requisito foi avaliada no **REQUISITO VI.8**.

EN.VI.9.1: Por meio de ferramenta específica, enviar uma solicitação de carimbo do tempo com o campo *certReq* contendo o valor FALSE. Analisar na respectiva resposta se o campo *certificates* da estrutura *SignedData* está ausente.

EN.VI.9.2: Por meio de ferramenta específica, enviar uma solicitação de carimbo do tempo ao SCT com o campo *certReq* ausente. Analisar na respectiva resposta se o campo *certificates* da estrutura *SignedData* está ausente.

REQUISITO VI.10: Se uma extensão é utilizada em uma solicitação de carimbo do tempo mas não é suportada ou reconhecida pelo Servidor de Carimbo do Tempo, o servidor não deve emitir o carimbo do tempo e deve retornar a indicação de falha *unacceptedExtension* por meio do campo *failInfo* da respectiva resposta.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VI.10.1: Analisar a documentação técnica e verificar se o Servidor de Carimbo do Tempo não emite o carimbo do tempo e retorna a indicação de falha *unacceptedExtension* por meio do campo *failInfo* da respectiva resposta, quando este recebe uma solicitação de carimbo do tempo contendo uma extensão não suportada.

EN.VI.10.2: Por meio de ferramenta específica, enviar uma solicitação de carimbo do tempo ao SCT contendo extensões não suportadas pelo SCT e verificar se o carimbo do tempo não será emitido e retornará a indicação de falha *unacceptedExtension* por meio do campo *failInfo* na respectiva resposta.

REQUISITO VI.11: Um Servidor de Carimbo do Tempo deve tratar ou considerar qualquer extensão como sendo não-crítica conforme o formato definido no padrão RFC 2459.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VI.11.1: Analisar a documentação técnica e verificar se o SCT considera ou trata qualquer extensão como sendo não-crítica conforme o formato definido no padrão RFC 2459.

EN.VI.11.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT contendo extensões suportadas e não suportadas pelo SCT e verificar como estas são tratadas por meio de análise das respectivas respostas.

REQUISITO VI.12: Extensões suportadas ou reconhecidas por um Servidor de Carimbo do Tempo que aparecerem na solicitação de carimbo do tempo devem aparecer também no respectivo carimbo do tempo.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VI.12.1: Verificar se a documentação técnica do SCT descreve quais extensões são suportadas ou reconhecidas nas solicitações de carimbo do tempo, e qual o tratamento aplicável para cada extensão.

EN.VI.12.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT contendo extensões suportadas ou reconhecidas e analisar se o carimbo do tempo é emitido contendo as respectivas extensões.

2.7 Requisitos de emissão de carimbo do tempo

Esta seção descreve os requisitos relacionados à emissão de carimbo do tempo, o qual é produzido pelo SCT após o recebimento de uma solicitação de carimbo do tempo.

2.7.1 Requisitos gerais de emissão de carimbo do tempo

REQUISITO VII.1: Um SCT deve somente realizar assinatura digital sobre o *hash* dos dados a serem carimbados temporalmente.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.1.1: Verificar se a documentação técnica do SCT descreve os mecanismos de assinatura digital do *hash* dos dados a serem carimbados.

EN.VII.1.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT contendo o *hash* dos dados a serem carimbados e verificar por meio de ferramenta específica se o carimbo do tempo contém a assinatura correta feita sobre o *hash* contido nas solicitações.

REQUISITO VII.2: Todo carimbo do tempo emitido por um SCT, deve apresentar informações suficientes para que a entidade solicitante possa realizar verificações a qualquer momento.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.2.1: Verificar se a documentação técnica do SCT descreve a apresentação de informações que possam ser utilizadas pela entidade solicitante para realizar verificações a partir do carimbo do tempo emitido, como por exemplo:

- Identificação do SCT responsável pela emissão do carimbo do tempo;
- identificação da organização responsável pelo servidor de carimbo do tempo;
- outras informações adicionais.

EN.VII.2.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT e verificar se os carimbos do tempo emitidos contêm informações para verificações, como por exemplo:

- Identificação do SCT responsável pela emissão do carimbo do tempo;
- identificação da organização responsável pelo servidor de carimbo do tempo;
- outras informações adicionais.

REQUISITO VII.3: Em resposta às solicitações de carimbo do tempo, um SCT não deve emitir qualquer informação que identifique o requisitor do carimbo do tempo.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.3.1: Verificar se a documentação técnica do SCT descreve a ausência de informações em carimbos do tempo que permitam identificar o requisitor do carimbo do tempo.

EN.VII.3.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT e verificar se este não apresenta nas respectivas respostas qualquer informação sobre o solicitante do carimbo do tempo.

REQUISITO VII.4: Para fins de assinatura digital de carimbos do tempo, um SCT deve somente utilizar o par de chaves criptográficas criado especificamente para este propósito.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.4.1: Verificar se a documentação técnica do SCT descreve o uso de par de chaves criptográficas.

EN.VII.4.2: Analisar o certificado digital ICP-Brasil utilizado pelo SCT para assinar carimbos do tempo e verificar se o campo "*Key Usage*" possui os valores *digitalSignature* e/ou *nonRepudiation* definidos como propósitos para o par de chaves criptográficas.

EN.VII.4.3: Analisar o comportamento do SCT perante o uso de certificados digitais ICP-Brasil com campos "*Key Usage*" que possuem valores inadequados para assinatura de carimbos do tempo.

REQUISITO VII.5: A Parte Interessada deve fornecer documentação técnica que descreva os métodos de assinatura digital de carimbo do tempo utilizados pelo SCT, indicando algoritmos e tamanhos de chaves suportadas.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.5.1: Verificar se a documentação técnica do SCT descreve os métodos de assinatura digital de carimbo do tempo utilizados, indicando algoritmos e tamanhos de chaves suportadas.

REQUISITO VII.6: Em resposta às solicitações de carimbo do tempo, quando concedido o carimbo do tempo, o certificado do SCT deve ser incluído no campo *TSTInfo* do carimbo do tempo.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.6.1: Verificar se a documentação técnica do SCT descreve a inclusão do certificado digital do SCT no campo *TSTInfo*, quando o carimbo do tempo é concedido.

EN.VII.6.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT e verificar se a resposta às solicitações de carimbo do tempo contêm o certificado digital do SCT no campo *TSTInfo*, quando o carimbo do tempo é concedido.

2.7.2 Requisitos de formato de carimbo do tempo

REQUISITO VII.7: Em uma resposta de uma solicitação de carimbo do tempo, o campo *status* da estrutura *PKIStatusInfo* contida no campo *status* deve indicar a presença ou ausência do carimbo do tempo por meio dos seguintes valores:

- *granted* (0);
- *grantedWithMods* (1);
- *rejection* (2);
- *waiting* (3)*;*
- *revocationWarning* (4);
- *revocationNotification* (5).

O carimbo do tempo somente deve estar presente na resposta caso o campo *status* seja igual a “0” ou “1”. Para os demais valores o carimbo do tempo não deve estar presente na resposta.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.7.1: Verificar se a documentação técnica do SCT descreve os valores utilizados no campo *status* da estrutura *PKIStatusInfo* contida no campo *status.*

EN.VII.7.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT e verificar o valor do campo *status* da estrutura *PKIStatusInfo* contida no campo *status* conforme a presença ou ausência do carimbo do tempo na resposta.

REQUISITO VII.8: Servidores de carimbo do tempo não devem produzir valores no campo *status* da estrutura *PKIStatusInfo* contida no campo *status* diferente daqueles especificados no **REQUISITO VII.7**.

Procedimentos de ensaio para NSH 1, 2 e 3:

Nota: A documentação referente a este requisito foi avaliada no **REQUISITO VII.7**.

EN.VII.8.1: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT e analisar se o valor do campo *status* da estrutura *PKIStatusInfo* contida no campo *status*, presente na reposta, está em consistência com o **REQUISITO VII.7.**

REQUISITO VII.9: Quando um carimbo do tempo não estiver presente em uma resposta de uma solicitação, o campo *failInfo* da estrutura *PKIStatusInfo* contida no campo *status*, deve indicar o motivo da ausência por meio, somente, dos seguintes valores:

- *badAlg* (0);
- *badRequest* (1);
- *badDataFormat* (5);
- *timeNotAvaliable* (14);

- *unacceptedPolicy* (15);
- *unacceptedExtension* (16);
- *addInfoNotAvaliable* (17);
- *systemFaliure* (25).

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.9.1: Verificar a documentação técnica e analisar se os valores utilizados no campo *failInfo* da estrutura *PKIStatusInfo* contida no campo *status*, para indicar o motivo da ausência do carimbo do tempo na resposta à solicitação de carimbo do tempo estão consistentes com os seguintes valores:

- *badAlg* (0);
- *badRequest* (1);
- *badDataFormat* (5);
- *timeNotAvaliable* (14);
- *unacceptedPolicy* (15);
- *unacceptedExtension* (16);
- *addInfoNotAvaliable* (17);
- *systemFaliure* (25).

EN.VII.9.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT e verificar caso o carimbo do tempo esteja incluído na resposta à solicitação, se o campo *failInfo* está ausente da estrutura *PKIStatusInfo* contida no campo *status*.

REQUISITO VII.10: Servidores de carimbo do tempo não devem produzir valores do campo *failInfo* da estrutura *PKIStatusInfo* contida no campo *status* diferente daqueles especificados no **REQUISITO VII.9**.

Procedimentos de ensaio para NSH 1, 2 e 3:

Nota: A documentação referente a este requisito foi avaliada no **REQUISITO VII.9**.

EN.VII.10.1: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT, verificar se os valores utilizados para preencher o conteúdo do campo *failInfo* da estrutura *PKIStatusInfo* contida no campo *status* estão consistentes com aqueles definidos no **REQUISITO VII.9.**

REQUISITO VII.11: Um carimbo do tempo não deve conter quaisquer outras assinaturas diferentes da assinatura da ACT.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.11.1: Verificar se a documentação técnica do SCT descreve quais assinaturas digitais estão presentes em carimbos do tempo emitidos pelo SCT.

EN.VII.11.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT e verificar se os carimbos do tempo emitidos contêm assinaturas digitais conforme a documentação fornecida.

REQUISITO VII.12: Servidores de carimbo do tempo devem ser capazes de fornecer carimbo do tempo versão 1.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.12.1: Verificar se a documentação técnica do SCT descreve versão dos carimbos do tempo que são emitidos.

EN.VII.12.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT e verificar se os carimbos do tempo emitidos apresentam a versão 1.

REQUISITO VII.13: Caso o campo *policy* esteja presente na solicitação de carimbo do tempo, o campo *policy* da resposta desta solicitação deve possuir o mesmo conteúdo, ou seja, mesmo OID da Política de Carimbo do Tempo (PCT) atribuído à

ACT que está atendendo a solicitação. Caso contrário, o Servidor de Carimbo do Tempo (SCT) da ACT deve emitir um erro (*unacceptedPolicy*) nesta resposta.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.13.1: Verificar se a documentação técnica do SCT descreve o conteúdo do campo *policy* presente em carimbos do tempo conforme as condições estabelecidas no **REQUISITO VII.13**.

EN.VII.13.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT e verificar a presença do campo *policy* e seu respectivo conteúdo conforme a documentação fornecida.

REQUISITO VII.14: O campo *serialNumber* da resposta de uma solicitação de carimbo do tempo, deve ser único para cada carimbo do tempo gerado por uma determinada ACT.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.14.1: Verificar se a documentação técnica do SCT descreve a unicidade valor contido no campo *serialNumber* da resposta à solicitação de carimbo do tempo.

EN.VII.14.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT e verificar se o campo *serialNumber* dos carimbos do tempo são preenchidos por valores únicos.

REQUISITO VII.15: Em caso de interrupção do serviço de um SCT, como por exemplo, devido a uma queda de força, a unicidade do valor do campo *serialNumber* deve ser preservada.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.15.1: Verificar se a documentação técnica do SCT descreve os métodos que garantem a unicidade dos valores contidos no campo *serialNumber* em caso de interrupção do serviço de um SCT.

EN.VII.15.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT, antes e após reinicialização do SCT e verificar se o campo *serialNumber* dos carimbos preserva a produção de valores únicos.

REQUISITO VII.16: O campo *genTime* da resposta de uma solicitação de carimbo do tempo, deve ser representado da seguinte forma:

- Seguir a hora UTC (*Coordinated Universal Time*), para evitar conflito com o fuso horário local em uso;
- Representar segundos;
- Quando a precisão for maior que 1 segundo, representar frações de segundo;
- Seguir a sintaxe: “AAAAMMDDhhmmss[.s...]Z”;
- A letra “Z”, que significa “Zulu” ou hora UTC, deve ser incluída no final;
- A representação do horário da meia-noite (GMT) deve ser “YYYYMMDD000000Z”, onde “YYYYMMDD” representa o dia seguinte à meia-noite.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.16.1: Verificar se a documentação técnica do SCT descreve o formato para o campo *genTime* contido em carimbos do tempo.

EN.VII.16.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT e verificar se carimbo do tempo contém o campo *genTime* no formato definido pelo **REQUISITO VII.16**.

REQUISITO VII.17: O campo *accuracy* (precisão) da resposta de uma solicitação de carimbo do tempo, deve consistir nos seguintes campos:

- *seconds*

- *millis* – valores entre 1 e 999
- *micros* – valores entre 1 e 999

Quando aplicável, a ausência de cada um destes valores deve ser representada por "0".

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.17.1: Verificar se a documentação técnica do SCT descreve a composição do campo *accuracy* (precisão) de um carimbo do tempo.

EN.VII.17.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT e verificar se a resposta à solicitação contém o campo *accuracy* composto conforme o **REQUISITO VII.17**.

REQUISITO VII.18: Caso o campo *nonce* esteja presente na solicitação de carimbo do tempo, o campo *nonce* da resposta desta solicitação deve possuir o mesmo valor.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.18.1: Verificar se a documentação técnica do SCT descreve o preenchimento do campo *nonce* presente em carimbos do tempo.

EN.VII.18.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT, contendo o campo *nonce* preenchido com valores conhecidos e verificar se as respostas às solicitações contêm os mesmos valores dos campos *nonce* enviados nas solicitações de carimbo do tempo.

REQUISITO VII.19: Quando o campo *tsa* da resposta de uma solicitação de carimbo do tempo estiver presente, ele deve corresponder à um dos valores *subject name* incluídos no certificado a ser utilizado para verificação do carimbo do tempo.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.19.1: Verificar se a documentação técnica do SCT descreve o preenchimento do campo *tsa* incluído em de carimbos do tempo.

EN.VII.19.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT e verificar o preenchimento do campo *tsa* conforme definido no **REQUISITO VII.19**.

REQUISITO VII.20: O identificador do certificado *ESSCertID* contido no certificado da ACT deve ser incluído como um atributo *signerInfo* dentro do atributo *SigningCertificate*.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.20.1: Verificar se a documentação técnica do SCT descreve o preenchimento do atributo *signerInfo* dentro do atributo *SigningCertificate* em carimbos do tempo.

EN.VII.20.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT e verificar se o atributo *signerInfo* dentro do atributo *SigningCertificate* é preenchido conforme o **REQUISITO VII.20**.

REQUISITO VII.21: Quando um SCT recebe solicitações de carimbo do tempo para dois documentos nos tempos T1 e T2, o SCT não deve gerar carimbo do tempo para o documento que chegou em T2 antes de gerar o carimbo do tempo para o documento que chegou em T1. Ou seja, a ordem da emissão de carimbo do tempo, deve corresponder à ordem de chegada das respectivas solicitações.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.21.1: Verificar se a documentação técnica do SCT descreve o tratamento de ordem de chegada de solicitações de carimbos do tempo.

EN.VII.21.2: Por meio de ferramenta específica, enviar solicitações de carimbo do tempo ao SCT e verificar por meio do campo *genTime* se a ordem dos carimbos do tempo segue a ordem especificada no **REQUISITO VII.21**.

3 Referências Normativas

COMITÊ GESTOR DA ICP-BRASIL. **Resolução N° 49, de 3 de junho de 2008: Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil.** Brasília: ICP-BRASIL, 2008. 23 p.

COMITÊ GESTOR DA ICP-BRASIL. **Resolução N° 41, de 18 de abril de 2006: Requisitos Mínimos para as Políticas de Certificados na Infra-estrutura de Chaves Públicas Brasileira (ICP-BRASIL).** Brasília: ICP-BRASIL, 2006. 20 p.

COMITÊ GESTOR DA ICP-BRASIL. **Resolução N° 58, de 28 de novembro de 2008: Visão geral do sistema de carimbos do tempo na ICP-Brasil.** Brasília: ICP-BRASIL, 2008. 11 p.

COMITÊ GESTOR DA ICP-BRASIL. **Resolução N° 59, de 28 de novembro de 2008: Requisitos mínimos para as declarações de práticas das autoridades de carimbo do tempo da ICP-Brasil.** Brasília: ICP-BRASIL, 2008. 30 p.

COMITÊ GESTOR DA ICP-BRASIL. **Resolução N° 60, de 28 de novembro de 2008: Requisitos mínimos para as políticas de carimbo do tempo da ICP-Brasil.** Brasília: ICP-BRASIL, 2008. 07 p.

COMITÊ GESTOR DA ICP-BRASIL. **Resolução N° 61, de 28 de novembro de 2008: Procedimentos para auditoria do tempo na ICP-Brasil.** Brasília: ICP-BRASIL, 2008. 08 p.

INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. **Glossário ICP-Brasil - Versão 1.2.** Brasília: ICP-Brasil, 2007. 49 p.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Information**

technology -- ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) – ISO/IEC 8825-1. Genève, Switzerland, Reference Number: ISO/IEC 8825-1:2002.

THE INTERNET ENGINEERING TASK FORCE. Freed, N. e Borenstein, N. **Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies.** RFC 2045, Category: Standards Track, November 1996. Disponível em <http://www.ietf.org/rfc/rfc2045.txt>. Acesso em: 30.jan.2006.

THE INTERNET ENGINEERING TASK FORCE. Linn, J. **Privacy Enhancement for Internet Electronic Mail:** Part I: Message Encryption and Authentication Procedures. RFC 1421, February 1993. Disponível em: <http://www.ietf.org/rfc/rfc1421.txt>. Acesso em: 30.jan.2006.

RSA LABORATORIES. PKCS #7: **Cryptographic Message Syntax Standard.** Version 1.5. 1993. 30p. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-7.doc>. Acesso em: 30.jan.2006.

THE INTERNET ENGINEERING TASK FORCE. Housley, R.; Polk, W.; Ford, W. e Solo, D. **Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile.** RFC 3280, Category: Standards Track, April 2002. Disponível em <http://www.ietf.org/rfc/rfc3280.txt>. Acesso em: 30.jan.2006.

THE INTERNET ENGINEERING TASK FORCE. Myers, M.; Ankney, R.; Malpani, A.; Galperin, S. e Adams, C. **X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.** RFC 2560, Category: Standards Track, June 1999. Disponível em <http://www.ietf.org/rfc/rfc2560.txt>. Acesso em: 30.jan.2006.

THE INTERNET ENGINEERING TASK FORCE. Housley, R. **Cryptographic Message Syntax (CMS).** RFC 3852, Category: Standards Track, July 2004. Disponível em <http://www.ietf.org/rfc/rfc3852.txt>. Acesso em: 30.jan.2006.

THE INTERNET ENGINEERING TASK FORCE. Farrell, S.; Housley, R. **An Internet Attribute Certificate Profile for Authorization.** RFC 3281, Category: Standards Track, April 2002. Disponível em <http://www.ietf.org/rfc/rfc3281.txt>. Acesso em: 10.set.2008.

THE INTERNET ENGINEERING TASK FORCE. Adams, C.; Cain, P.; Pinkas, D.; Zuccherato, R. **Internet X.509 Public Key Infraestructure Time-Stamp Protocol (TSP).** RFC 3161, Category: Standards Track, August 2001. Disponível em <http://www.ietf.org/rfc/rfc3161.txt>. Acesso em: 10.set.2008.

THE INTERNET ENGINEERING TASK FORCE. Pinkas, D.; Pope, N.; Ross, J. **Policy Requirements for Time-Stamping Authorities (TSAs).** RFC 3628, Category: Standards Track, November 2003. Disponível em <http://www.ietf.org/rfc/rfc3628.txt>. Acesso em: 10.set.2008.