Infraestrutura de Chaves Públicas Brasileira

Manual de Condutas Técnicas 10 – Volume II

Procedimentos de Ensaios para Avaliação de Conformidade de Carimbo do Tempo no âmbito da ICP-Brasil

versão 2.0

Brasília, 08 de maio de 2020

Sumário

LISTA DE ILUSTRAÇÕES

Lista de Figuras

GLOSSÁRIO

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

CONTROLE DE ALTERAÇÕES

Resolução que aprovou alteração	Item Alterado	Descrição da Alteração
		Novos Protocolos e Procedimentos para Auditoria e Sincronismo da Rede de Carimbo do Tempo
IN 09, de 07.12.2015 (Versão 1.1)	Item 2.4 vol. II	Disciplina A Utilização Da Hora Pelas Autoridades Certificadoras De Primeiro Nível Pertencentes À Infraestrutura De Chaves Públicas Brasileira – ICP-Brasil Por Meio Do Serviço *Network Time Protocol* – Ntp.
IN 04, de 23.04.2010 (Versão 1.0)		Aprova a versão 1.0 do documento Manual de Condutas Técnicas – Volume II.

Infraestrutura de Chaves Públicas Brasileira

TABELA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
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 do Tempo
FCT	Fonte Confiável de Tempo
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*
PCT	Política de Carimbo do Tempo
PPS	*Pulse per Second*
PSS	Prestadores de Serviço de Suporte
PTP	PRECISION TIME PROTOCOL
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 determina 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 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):
sistema onde é executado software que audita SCTs;
Árvore de Encadeamento do Tempo : Encadeamento de dados de carimbos do tempo e sincronismo, que emprega recursos criptográficos baseados em Árvores de Merkle.

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 entidades 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.

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.

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*": [OPCIONAL] campo utilizado para solicitar o envio do certificado da ACT na respectiva resposta;
"*extensions*": [OPCIONAL] campo para inserir informações adicionais, conforme definido pela RFC 5280.

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 para cada carimbo do tempo;

"*genTime*": instante em que o carimbo do tempo foi criado pelo SCT. Deve incluir frações de segundo ;

"*accuracy*": desvio de tempo em relação ao UTC no formato *GeneralizedTime*;

"*ordering*": indica se existe uma ordem cronológica nos carimbos do tempo criados pelo SCT;

"*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 5280.

"*encadeamento*": extensão não-crítica que deve ser aplicável quando o SCT suporta mecanismos de encadeamento de carimbos do tempo;

"alvará": extensão não-crítica que contém o alvará vigente para o SCT que emitiu o carimbo do tempo.

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 descrito no DOC-ICP-11.01.

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 Sistema de Auditoria e Sincronismo;
Certificado de atributo digital (no contexto da infra-estrutura de carimbo do tempo da ICP-Brasil também é conhecido como Alvará).

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

REQUISITO I.8: Um SCT deve ser compatível com certificados digitais ICP-Brasil de assinatura de carimbos do tempo 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 executada por um SCT deve ser capaz de manipular certificados digitais que implementam a versão 3 do padrão ITU-T X.509 (X.509v3). Por aplicação de carimbo do tempo, entende-se um aplicação que é executada no SCT, e responsável por atender solicitações de carimbo do tempo. 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 executada por um SAS deve ser capaz de manipular certificados digitais que implementam a versão 3 do padrão ITU-T X.509 (X.509v3). Por aplicação de auditoria e sincronismo, entende-se um aplicação que é executada no SAS, e responsável por auditar SCTs. 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 de 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 de 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 de 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) associado.
O MSC realiza operações criptográficas para geração de carimbos do tempo utilizando como fonte de tempo um relógio de tempo real (*Real Time Clock* - RTC) localizado dentro de sua fronteira segura.

A figura 2 apresenta um exemplo dos principais componentes de um SCT.

Infraestrutura de Chaves Públicas Brasileira

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 Sistema de Auditoria e Sincronismo (SAS).
O envio de dados para auditorias periódicas será realizado conforme descrito no DOC-ICP-11.01. ~~por comunicação por meio do Protocolo Websocket (RFC 6455 e atualizações) e do Protocolo Transport Layer Security (TLS) v 1.3 ou posterior (RFC 8446 e atualizações).~~
Os dados de auditoria seguem descritos neste documento nos itens 2.2.3 – Suporte a Algoritmos e 2.3.1 - Requisitos Gerais de Segurança.

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.01.03: 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) associado a um SCT deve atender aos requisitos definidos no Manual de Condutas Técnicas 7 – Volume I.

Procedimentos de ensaio para NSH 1, 2 e 3:

Os procedimentos de ensaio para o MSC contido em um SCT são aqueles definidos pelo Manual de Condutas Técnicas 7 – Volume II.

REQUISITO II.3: Um SCT deve utilizar o relógio de tempo real (RTC) do MSC associado 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.03.01: Verificar se a documentação técnica do SCT descreve o relógio de tempo real (RTC) do MSC associado ao SCT, observando a descrição dos mecanismos que são utilizados para restringir o acesso aos controles do relógio.

EN.II.03.02: Realizar os procedimentos de alteração da hora do relógio do MSC associado ao 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.

2.2.2. Gerenciamento de chaves criptográficas

REQUISITO II.4: Chaves privadas para fins de assinatura digital de carimbos do tempo devem ser geradas e armazenadas no MSC associado ao SCT de forma a garantir sua confidencialidade.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.04.01: Verificar se a documentação técnica do SCT descreve os mecanismos de manipulação de chaves privadas para fins de assinatura digital de carimbos de tempo.

EN.II.04.02: 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.5: 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 associado ao SCT deve estar desabilitado.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.05.01: Verificar se a documentação técnica do SCT descreve os mecanismos de gerenciamento de chaves privadas para fins de assinatura digital de carimbos de tempo.

EN.II.05.02: 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 associado ao SCT.

2.2.3. Suporte a algoritmos

REQUISITO II.06: Para mitigar ataques de falsificação de carimbos do tempo, um Servidor de Carimbo do Tempo deve utilizar uma árvore de encadeamento do tempo.
Os nós da árvore de encadeamento do tempo deverão ser construídas co~~**da seguinte forma:**~~**mo descrito no DOC-ICP-11.01**

~~- o SCT ao receber um novo alvará, calcula seu resumo criptográfico e inicia uma nova árvore;~~
~~- toda operação de sincronismo deverá ter seus dados de estampa de tempo no SCT (timestamp), desvio médio (offset) e atraso médio (delay), resumidos criptograficamente e registrados na árvore;~~
~~- carimbos do tempo emitidos pelo SCT devem ser resumidos criptograficamente e inseridos na árvore;~~

~~- os dados usados para gerar os resumos criptográficos da árvore deverão ser armazenados juntamente com indexador do bloco da árvore ao qual ele pertence;~~

Procedimentos de ensaio para NSH 1:

EN.II.06.01: Verificar se a documentação técnica do SCT descreve os mecanismos de encadeamento de carimbos de tempo suportados pelo SCT.

Procedimentos de ensaio para NSH 2 e 3:

EN.II.06.02: 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 de tempo.

REQUISITO II.7: Para fins de assinatura digital de carimbos do tempo e resumos criptográficos (*hash*), um Servidor de Carimbo do Tempo deve suportar os algoritmos criptográficos definidos conforme DOC-ICP-01.01 Seção 2 – tabela "Assinatura de Pedidos e Respostas de Carimbos do Tempo".

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.07.01: Verificar se a documentação técnica do SCT descreve os algoritmos de assinatura digital e resumos criptográficos suportados pelo MSC do SCT.

EN.II.07.02: Para os algoritmos suportados pelo MSC do SCT, executar testes de validação publicados pelo NIST. 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;
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.

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 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) associado. 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 uma escala de tempo.

2.3.1. Requisitos gerais de segurança

REQUISITO III.1: Sistemas de Auditoria e Sincronismo devem dispor de mecanismos que permitam operar sincronizados constantemente 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 de 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 de Tempo (FCT).

REQUISITO III.2: Sistemas de Auditoria e Sincronismo devem dispor de mecanismos que permitam auditar e sincronizar constantemente Servidores de Carimbo do Tempo.
O procedimento de auditoria deverá ser implementado pelo SAS conforme descrito no DOC-ICP-11.01 .
~~A auditoria é iniciada pelo SAS, que envia ao SCT um novo alvará, para que este encerre a árvore de encadeamento do tempo corrente e inicie uma nova. Em seguida, o SCT deverá enviar a árvore encerrada ao SAS.~~
~~Para este fluxo de dados deverá ser usado o protocolo Websocket com TLS, conforme item 2.2.3 – Suporte a Algoritmos.~~
O protocolo utilizado pelo SAS para auditar o SCT deverá ser descrito detalhadamente.
O protocolo utilizado pelo SAS para auditar um SCT deverá ser de uso livre.

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 requisitos definidos no Manual de Condutas Técnicas 7 – Volume I.

Procedimentos de ensaio para NSH 1, 2 e 3

Os procedimentos de ensaio para o MSC contido em um SAS são aqueles definidos pelo Manual de Condutas Técnicas 7 – Volume II.

REQUISITO III.4: 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.04.01: 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.04.02: 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.5: 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.05.01: 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.

2.3.2. Gerenciamento de chaves criptográficas

REQUISITO III.6: Chaves privadas para fins de assinatura digital de alvarás devem ser geradas e armazenadas no MSC do SAS de forma a garantir sua confidencialidade.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.06.01: Verificar se a documentação técnica do SAS descreve os mecanismos de manipulação de chaves privadas para fins de assinatura digital de carimbos de tempo.

EN.II.06.02: Por meio de ferramenta específica, observar os processos de manipulação de chaves privadas pelo SAS, verificando que somente são utilizadas as chaves privadas que estão armazenadas no MSC.

REQUISITO III.7: 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.07.01: Verificar se a documentação técnica do SAS descreve os mecanismos de gerenciamento de chaves privadas para fins de assinatura digital de alvarás.

EN.III.07.02: 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.8: Para fins de assinatura digital de alvarás e resumos criptográficos (*hash*), um Sistema de Auditoria e Sincronismo deve suportar os algoritmos criptográficos definidos conforme DOC-ICP-01.01 Seção 2 – tabela “Assinaturas Digitais ICP-Brasil CaDES e XaDES”.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.08.01: Verificar se a documentação técnica do SAS descreve os algoritmos de assinatura digital e resumos criptográficos suportados pelo MSC do SAS.

EN.II.08.02: Para os algoritmos suportados pelo MSC do SAS, executar testes de validação publicados pelo NIST. 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;
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.

2.4. Requisitos de Sincronismo de Tempo

Esta seção descreve requisitos que dizem respeito aos mecanismos de sincronismo do tempo em um Servidor de Carimbo do Tempo (SCT) e um Sistema de Auditoria e Sincronismo (SAS). Na estrutura de carimbo do tempo, a ICP-Brasil possui escala de tempo própria rastreável à hora UTC, denominada como Fonte Confiável do Tempo. difundida por meio dos Sistemas da Entidade de Auditoria do Tempo.

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;

Procedimentos de ensaio para NSH 1, 2 e 3:

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 de tempo

REQUISITO IV.2: A comunicação entre SAS e SCT para estabelecer um sincronismo do tempo deve seguir o descrito no DOC-ICP-11.01.~~:~~

- ~~Usar o protocolo PTPv2 – IEEE 1588v2-2008 - para realizar o sincronismo do relógio do SCT com o SAS.~~
  - ~~A fim de prover autenticação de dados no protocolo PTP deve-se associá-lo ao subprotocolo NTS-KE - "NTS Key Establishment", parte do protocolo para segurança do tempo em redes para o protocolo NTP (Network Time Security for the Network Time Protocol), servindo para iniciar a troca de chaves criptográficas e outros dados de segurança, por meio do protocolo TLS, entre servidor (SAS) e o cliente (SCT).~~

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.IV.2.1: Verificar se a documentação técnica do SCT e SAS descreve o uso de protocolo descrito no DOC-11.01 ~~PTPv2 – IEEE 1588v2-2008 -~~ para realizar o sincronismo do relógio

do SCT com o SAS., ~~empregando o subprotocolo NTS-KE - "NTS Key Establishment", parte do protocolo para segurança do tempo em redes para o protocolo NTP (Network Time Security for the Network Time Protocol), para iniciar a troca de chaves criptográficas e outros dados de segurança, por meio do protocolo TLS, entre o servidor (SAS) e o cliente (SCT).~~

EN.IV.2.2: Por meio de ferramenta específica, verificar se o SCT e SAS fazem uso de protocolo descrito no DOC-ICP-11.01 ~~PTPv2 – IEEE 1588v2-2008 -~~ para realizar o sincronismo do relógio do SCT com o SAS~~, empregando o subprotocolo NTS-KE - "NTS Key Establishment", parte do protocolo para segurança do tempo em redes para o protocolo NTP (Network Time Security for the Network Time Protocol), para iniciar a troca de chaves criptográficas e outros dados de segurança, por meio do protocolo TLS, entre cliente (SCT) e o servidor (SAS).~~

REQUISITO IV.3: O sincronismo entre a Fonte Confiável do Tempo e o SAS deve seguir o protocolo descrito no DOC-ICP-11.01. ~~empregar o protocolo PTPv2 – IEEE 1588v2-2008, com uso de estampas de tempo produzidas pelo hardware das interfaces de rede (hardware timestamping).~~

Procedimentos de ensaio para NSH 1

EN.IV.03.1: Analisar documentação técnica do SAS que descreve os mecanismos que realizam sincronizações periódicas com uma Fonte Confiável de Tempo (FCT), bem como inspecionar o hardware das interfaces de rede.

EN.IV.3.2: Por meio de ferramenta específica, verificar se o SAS suporta o protocolo descrito no DOC-ICP-11.01. ~~PTP com estampas de tempo de hardware para sincronismo com a Fonte Confiável do Tempo~~.

2.4.2. Exatidão do relógio

REQUISITO IV.4: O fabricante deve informar a exatidão do relógio do SCT e SAS, indicando a incerteza associada.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.IV.4.1: 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 processo de Autorização de Funcionamento

ou alvará, emitido pela Entidade de Auditoria do 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 de Tempo baseada na hora UTC , também é a de garantir que os carimbos de tempo emitidos por um SCT estejam com a hora mais próxima possível da hora UTC.

O processo de auditoria de SCT está descrito no DOC-ICP-11.01.
~~Em suma, o processo de auditoria de SCTs consiste nas etapas:~~

~~i. SAS envia Alvará ao SCT ;~~
~~ii. SCT recebe Alvará e inicia, com este Alvará, nova Árvore de Encadeamento do Tempo, encerrando a Árvore em uso;~~
~~iii. SAS solicita árvore de encadeamento e dados correlatos do SCT ;~~
~~iv. SCT envia dados para SAS.~~

~~Para mitigar ataques de falsificação de carimbos do tempo, o SCT deve utilizar uma árvore de encadeamento do tempo.~~
~~Os nós da árvore de encadeamento do tempo deverão ser construídas da seguinte forma:~~
~~i. o SCT, ao receber um novo alvará, calcula seu resumo criptográfico e inicia uma nova árvore;~~
~~ii. toda operação de sincronismo deverá ter seus dados de estampa de tempo no SCT (timestamp), desvio médio (offset) e atraso médio (delay), resumidos criptograficamente e registrados na árvore;~~
~~iii. carimbos do tempo emitidos pelo SCT devem ser resumidos criptograficamente e inseridos na árvore;~~
~~iv. os dados usados para gerar os resumos criptográficos da árvore deverão ser armazenados em registros de eventos (logs).~~

~~A auditoria no SAS é realizada pela avaliação estatística dos blocos de log de sicronismo recebidos.~~

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 armazenada em registros de eventos (*log*) no formato UTF-8 ou ASCII, para posterior acesso pela EAT.

O SCT deve utilizar árvores de encadeamento do tempo e registrar os eventos correspondentes a atividades de sincronismo e auditoria, construídas conforme descrito no DOC-ICP-11.01.
~~No SCT os nós da árvore de encadeamento do tempo deverão ser construídos da seguinte forma:~~

~~i. o SCT, ao receber um novo alvará do SAS, calcula seu resumo criptográfico e inicia uma nova árvore;~~
~~ii. toda operação de sincronismo deverá ter seus dados de estampa de tempo no SCT (timestamp), desvio médio (offset) e atraso médio (delay), resumidos criptograficamente e registrados na árvore;~~
~~iii. carimbos do tempo emitidos pelo SCT devem ser resumidos criptograficamente e inseridos na árvore;~~
~~iv. os dados usados para gerar os resumos criptográficos da árvore deverão ser armazenados em registros de eventos (logs) no formato UTF-8 ou ASCII, para posterior acesso pelo SAS.~~

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.1.1: Verificar se a documentação técnica do SCT descreve o suporte à geração da árvore de encadeamento do tempo e 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 descreve informações sobre o formato utilizado (UTF-8 ou ASCII) nos registros de eventos (*log*), bem como descreve o formato da árvore de encadeamento do tempo, além de como e onde é feito o armazenamento.

EN.V.1.3: Por meio de ferramenta específica, verificar se a árvore de encadeamento do tempo e os registros de eventos (*logs*) armazenados no SCT foram gerados nos procedimentos de auditoria e/ou sincronismo.

EN.V.1.4: Verificar se a documentação técnica do SAS descreve o suporte à árvore de encadeamento do tempo e de registros de eventos (*log*) quando são executados procedimentos de auditoria e/ou sincronismo.

EN.V.1.5: Verificar se a documentação técnica do SAS descreve informações sobre o formato utilizado (UTF-8 ou ASCII) nos registros de eventos (*log*), bem como descreve o formato da árvore de encadeamento do tempo, além de como e onde é feito seu armazenamento.

EN.V.1.6: Por meio de ferramenta específica, verificar se a árvore de encadeamento do tempo e os arquivos de registro (*logs*) armazenados no SAS foram gerados nos 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;
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;
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;
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;
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:

estampa de tempo (timestamp) no SCT;
desvio médio (offset) no SCT;
atraso médio (delay) no SCT;
endereço de rede do servidor de tempo;

~~Erro do relógio do SCT;~~
~~Retardo;~~
~~(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;
estampa de tempo (timestamp) no SCT;
desvio médio (offset) no SCT;
atraso médio (delay) no SCT;
endereço de rede do servidor de tempo;

~~Erro do relógio do SCT;~~
~~Retardo;~~
~~Endereço de rede do SAS (auditor);~~
Endereço de rede do SCT ~~(auditado)~~.

REQUISITO V.5: 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.05.1: 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.6: 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.06.1: 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

Um alvará consiste de um objeto de dados que contém uma estrutura de campos conforme os requisitos a seguir. No que diz repeito a codificação de um Alvará, este pode ser codificado em formato ASN.1 ou XML.

REQUISITO V.7: Todo Alvará, antes de sua emissão, deve ser assinado digitalmente utilizando certificados digitais de equipamento A3 ou A4. Este processo de assinatura deverá ser realizado por meio do MSC contido no SAS.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.07.1: Verificar se a documentação técnica do SAS descreve o processo de assinatura digital de Alvarás.

EN.V.07.1: Executar os processos de emissão do Alvará verificando se durante a operação de assinatura digital do Alvará é utilizada a chave privada contida no MSC do SAS referente ao certificado digital de equipamento A3 ou A4.

REQUISITO V.8: O alvará emitido por um SAS deve possuir campos de acordo com o seguinte formato, conforme definido pela RFC 5755:

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.08.1: 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 5755.

EN.V.08.2: Verificar, por meio de ferramenta específica, se os campos do alvará estão de acordo com a RFC 5755.

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

EN.V.09.2: 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.01.1: Verificar se a documentação técnica do SCT e SAS descreve o campo *holder* da estrutura *AttributeCertificateInfo* do alvará.

EN.REC.V.01.2: 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 de tempo, no que diz respeito à vigência do alvará.

EN.V.15.2: Por meio de ferramenta específica, verificar se a emissão de carimbos de 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 de 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 de 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, ou seja, data de início e término da validade são iguais, então 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 de 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 de 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 o relógio de um SCT não apresentar erro que ultrapasse o valor especificado na Política de Carimbo do Tempo correspondente.
O erro se refere a medida estatística de desvio do relógio.

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 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 maior que o valor especificado na Política de Carimbo do Tempo.

REQUISITO V.19: Cada SCT deve ser ser capaz de ser auditado por pelo menos 2 (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 com um SAS das seguintes formas:

Por intervenção direta do administrador, onde o SCT solicita ao SAS que se inicie o processo de auditoria;
De forma automática, onde o SAS inicia o processo de auditoria 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 permitidos e suportados pelo SCT.

REQUISITO V.22: Um SAS deve permitir que se inicie o processo de auditoria sob demanda, como por exemplo, por meio da intervenção direta do administrador do SAS, ou em períodos de tempo variáveis parametrizados por avaliação estatística do desempenho do relógio do SCT.

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 sob demanda e em períodos de tempo variáveis parametrizados por avaliação estatística do desempenho do relógio do SCT.

EN.V.22.2: Por meio de inspeção direta, verificar se o SAS permite o processo de auditoria sob demanda e em períodos de tempo variáveis parametrizados por avaliação estatística do desempenho do relógio do SCT.

REQUISITO V.23: Um SAS deve permitir a configuração dos parâmetros de erro 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 de erro.

EN.V.23.2: Por meio de inspeção direta, verificar se o SAS permite configurar os parâmetros de erro 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 a 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.

REQUISITO V.27: Quanto ao arquivamento perene das árvores de encadeamento do tempo, o SCT deve implementar mecanismo de envio para bases de registros distribuídos (blockchain) segundo o framework Hyperledger, de blocos com resumos criptográficos das árvores.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.27.1: Verificar se a documentação técnica do SCT descreve como é feito o envio de blocos referentes às árvores de encadeamento do tempo para bases segundo o framework referido acima.

EN.V.27.2: Por meio de ferramenta específica, verificar se a documentação técnica do SCT descreve como é feito o envio de blocos referentes às árvores de encadeamento do tempo para bases segundo o framework referido acima.

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.01.1: Verificar se a documentação técnica descreve o valor do campo *version*, na solicitação de Carimbo do Tempo.

EN.VI.01.2: 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.02.2: 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.02.3: Analisar se o algoritmo de *hash* identificado na documentação técnica por meio do ensaio **EN.VI.02.1** e os parâmetros que identificam o algoritmo de *hash* identificados por meio do ensaio **EN.VI.02.2** 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 àquele associado ao respectivo algoritmo *hash*.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VI.03.1: Analisar a documentação técnica e identificar o tamanho do *hash* contido no campo *hashedMessage* presente na solicitação de Carimbo do Tempo.

EN.VI.03.2: Utilizando uma ferramenta específica, verificar o tamanho do *hash* contido no campo *hashedMessage* presente na solicitação de Carimbo do Tempo.

EN.VI.03.3: Analisar se o tamanho do *hash* identificado na documentação técnica por meio do ensaio **EN.VI.03.1** e o tamanho do *hash* identificado por meio do ensaio **EN.VI.03.2** estão consistentes.

REQUISITO VI.4: Caso o SCT não reconheça o algoritmo *hash* conforme especificado no campo *hashAlgorithm*, 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. Os algoritmos de hash que devem ser utilizados em carimbos do tempo são aqueles definidos no DOC-ICP-01.01 Seção 2 – tabela "Assinatura de Pedidos e Respostas de Carimbos do Tempo".

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VI.04.1: 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*.

EN.VI.04.2: 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*.

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.05.1: 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.05.2: 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.06.1: 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.07.1: Caso o ensaio **EN.VI.06.1** 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.08.1: 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.08.2: 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.09.1: 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.09.2: 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 deve emitir o carimbo do tempo e 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 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 5280.

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 5280.

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 deverão 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.01.1: Verificar se a documentação técnica do SCT descreve os mecanismos de assinatura digital do *hash* dos dados a serem carimbados.

EN.VII.01.2: 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 sobre o mesmo a qualquer momento.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.02.1: 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.02.2: Por meio de ferramenta específica, enviar solicitações de Carimbo do Tempo ao SCT e verificar se os carimbos de 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.03.1: Verificar se a documentação técnica do SCT descreve a ausência de informações em carimbos de tempo que permitam identificar o requisitor do Carimbo do Tempo.

EN.VII.03.2: 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.04.1: Verificar se a documentação técnica do SCT descreve o uso de par de chaves criptográficas.

EN.VII.04.2: Analisar o certificado digital ICP-Brasil utilizado pelo SCT para assinar carimbos de 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.04.3: 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 de 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.05.1: 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, informações sobre o certificado do SCT não necessitam ser incluídas no campo *TSTInfo* do carimbo do tempo.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.06.1: 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.06.2: Por meio de ferramenta específica, enviar solicitações de Carimbo do Tempo ao SCT e verificar se a resposta às solicitações de Carimbo do Tempo contém 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.07.1: Verificar se a documentação técnica do SCT descreve os valores utilizados no campo *status* da estrutura *PKIStatusInfo* contida no campo *status*.

EN.VII.07.2: 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.08.1: 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.09.1: 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.09.2: 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 do SCT.

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 de 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 de 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 de 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 de 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 de 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 estar sempre presente e ser único para cada carimbo do tempo gerado por um determinado SCT.

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 de 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 escala de 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 de 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 [OPCIONAL]
millis – valores entre 1 e 999 [OPCIONAL]
micros – valores entre 1 e 999 [OPCIONAL]

A ausência de cada um destes campos deverá ser interpretando como valor 0 (zero). É importante ressaltar que isso não implica no suporte ao valor 0 (zero) para cada um destes campos.

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 de 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 de 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 do SCT 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 de 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**.

3. REFERÊNCIAS NORMATIVAS

INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. **Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil. DOC-ICP-01.** Versão 4.0. Brasília. Dezembro 2008.

INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. **Padrões e Algoritmos Criptográficos da ICP-Brasil. DOC-ICP-01.01.** Versão 2.0. Brasília. Junho 2009.

INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. **Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil. DOC-ICP-04.** Versão 3.0. Brasília. Dezembro 2008.

INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. **Visão geral do sistema de carimbos do tempo na ICP-Brasil. DOC-ICP-11.** Versão 1.1. Brasília. Outubro 2009.

INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. **Requisitos mínimos para as declarações de práticas das autoridades de carimbo do tempo da ICP-Brasil. DOC-ICP-12.** Versão 1.1. Brasília. Outubro 2009.

INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. **Requisitos mínimos para as políticas de carimbo do tempo da ICP-Brasil. DOC-ICP-13.** Versão 1.1. Brasília. Outubro 2009.

INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. **Procedimentos para**

auditoria do tempo na ICP-Brasil. DOC-ICP-14. Versão 1.1. Brasília. Outubro 2009.

INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. **Glossário ICP-Brasil.** Versão 1.3. Brasília. Outubro 2009.

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.

RSA LABORATORIES. PKCS #7: **Cryptographic Message Syntax Standard.** Version 1.5. 1993. 30p. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-7/pkcs-7v16.pdf>. Acesso em: 07.abr.2010.

THE INTERNET ENGINEERING TASK FORCE. Cooper, D.; Santesson, S.; Farrell, S.; Boeyen, S.; Housley, R.; Polk, W. **Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile.** RFC 5280, Category: Standards Track, May 2008. Disponível em <http://www.ietf.org/rfc/rfc5280.txt>. Acesso em: 06.mai.2020.

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: 07.abr.2010.

THE INTERNET ENGINEERING TASK FORCE. Housley, R. **Cryptographic Message Syntax (CMS).** RFC 3852, Category: Standards Track, September 2009. Disponível em <http://www.ietf.org/rfc/rfc5652.txt>. Acesso em: 07.abr.2010.

THE INTERNET ENGINEERING TASK FORCE. Farrell, S.; Housley, R.;Turner, S. **An Internet Attribute Certificate Profile for Authorization.** RFC 5755, Category: Standards Track, January 2010. Disponível em https://tools.ietf.org/html/rfc5755. Acesso em: 06.05.2020.

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: 07.abr.2010.

THE INTERNET ENGINEERING TASK FORCE. Pinkas, D.; Pope, N.; Ross, J. **Policy Requirements for Time-Stamping Authorities (TSAs).** RFC 3628, Category: Informational, November 2003. Disponível em <http://www.ietf.org/rfc/rfc3628.txt>. Acesso em: 07.abr.2010.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI). **Electronic Signatures and Infraestructures (ESI) – Policy requirements for time-**

stamping authorities. ETSI TS 102 023 v1.2.1. France. January 2003.