Infraestrutura de Chaves Públicas Brasileira

ANEXO I

Manual de Condutas Técnicas 10 – Volume I

Requisitos, Materiais e Documentos Técnicos para Homologação de Carimbo do Tempo no Âmbito da ICP-Brasil

Versão 3.0

10 de novembro de 2021

Infraestrutura de Chaves Públicas Brasileira

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

CONTROLE DE ALTERAÇÕES

Ato que aprovou alteração	Item Alterado	Descrição da Alteração
IN ITI nº 19, de 10.11.2021 Versão 3.0	Requisitos II.5, III.7 e III.8	Consolidação da implementação de novos protocolos para a rede de Carimbo do Tempo da ICP-Brasil. Aprova a versão 3.0 consolidada.
IN ITI nº 21, de 15.12.2020 Versão 2.0		Novos Protocolos e Procedimentos para Auditoria e Sincronismo da Rede de Carimbo do Tempo.
IN 09, de 07.12.2015 Versão 1.1	Item 1.3, parte I, vol. I	Disciplina a utilização da hora pelas ACs de primeiro nível pertencentes à 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 I.

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 do Tempo
HSM	*Hardware Security Module*
HTTP	*Hypertext Transfer Protocol*
ICP	Infraestrutura de Chaves Públicas
ICP-Brasil	Infraestrutura 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*

SIGLA	DESCRIÇÃO
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 requisitos técnicos observados no processo de homologação de equipamentos de carimbo do tempo no âmbito da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.

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 infraestrutura 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;
- **MSC associado**: MSC associado é aquele que, conectado de forma segura ao SCT ou SAS, seja situado internamente ou externamente a este, armazena as chaves criptográficas usadas para assinaturas digitais, como, por exemplo, em carimbos do tempo e alvarás. Pode-se associar múltiplos MSC a múltiplos SCT (relação M:N).

1.1 Objetivo da homologação

O objetivo do processo de homologação de equipamentos de carimbo do tempo é propiciar a interoperabilidade e operação segura do serviço de carimbo do tempo oferecido por um servidor de carimbo do tempo por meio da avaliação técnica de aderência aos requisitos técnicos definidos neste manual

1.2 Descrição do processo de homologação

O processo de homologação é baseado em um conjunto de requisitos técnicos definidos neste manual que devem ser atendidos por um Servidor de Carimbo do Tempo (SCT) e Sistema de Auditoria e Sincronismo (SAS).

Estes requisitos técnicos são avaliados pela execução de ensaios de aderência aos requisitos técnicos. Para a realização destes ensaios, a Parte Interessada deve submeter ao processo de homologação um conjunto de materiais requisitados, efetuando o depósito destes materiais no LEA.

1.3 Escopo deste manual

Equipamentos de carimbo do tempo, tais como servidores de carimbo do tempo e sistemas de auditoria e sincronismo fazem uso de subsistemas e outros componentes. Um servidor de carimbo do tempo, por exemplo, faz uso de um Módulo de Segurança Criptográfico (MSC) o qual é instalado em seu interior para fins de assinatura de carimbos do tempo.

Portanto, o escopo deste manual considera servidores de carimbo do tempo e sistemas de auditoria e sincronismo incluindo seus componentes.

O escopo dos requisitos técnicos e da avaliação de equipamentos de carimbo do tempo aplica-se aos seguintes componentes:

- Servidor de Carimbo do Tempo:
  - Módulo de Segurança Criptográfico (MSC);
  - softwares embarcados para emissão de carimbo do tempo;
  - interfaces de comunicação;
- Sistema de Auditoria e Sincronismo:
  - Módulo de Segurança Criptográfico (MSC);
  - softwares embarcados para sincronismo e auditoria;
  - interfaces de comunicação;

O resultado do processo de homologação de equipamentos de carimbo do tempo informa a aderência aos requisitos técnicos definidos neste manual

1.4 Estruturação do MCT 10 – Volume I

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

- Parte 1: Descreve os requisitos técnicos que devem ser verificados no processo de homologação de equipamentos de carimbo do tempo;

- Parte 2: Descreve os materiais que devem ser depositados para a execução do processo de homologação de equipamentos de carimbo do tempo;
- Referência Bibliográfica: Descreve as referências bibliográficas que foram utilizadas na elaboração deste manual.

2 PARTE 1 - REQUISITOS TÉCNICOS PARA HOMOLOGAÇÃO DE EQUIPAMENTOS DE CARIMBO DO TEMPO NO ÂMBITO DA ICP-BRASIL

2.1 Requisitos gerais de carimbo do tempo

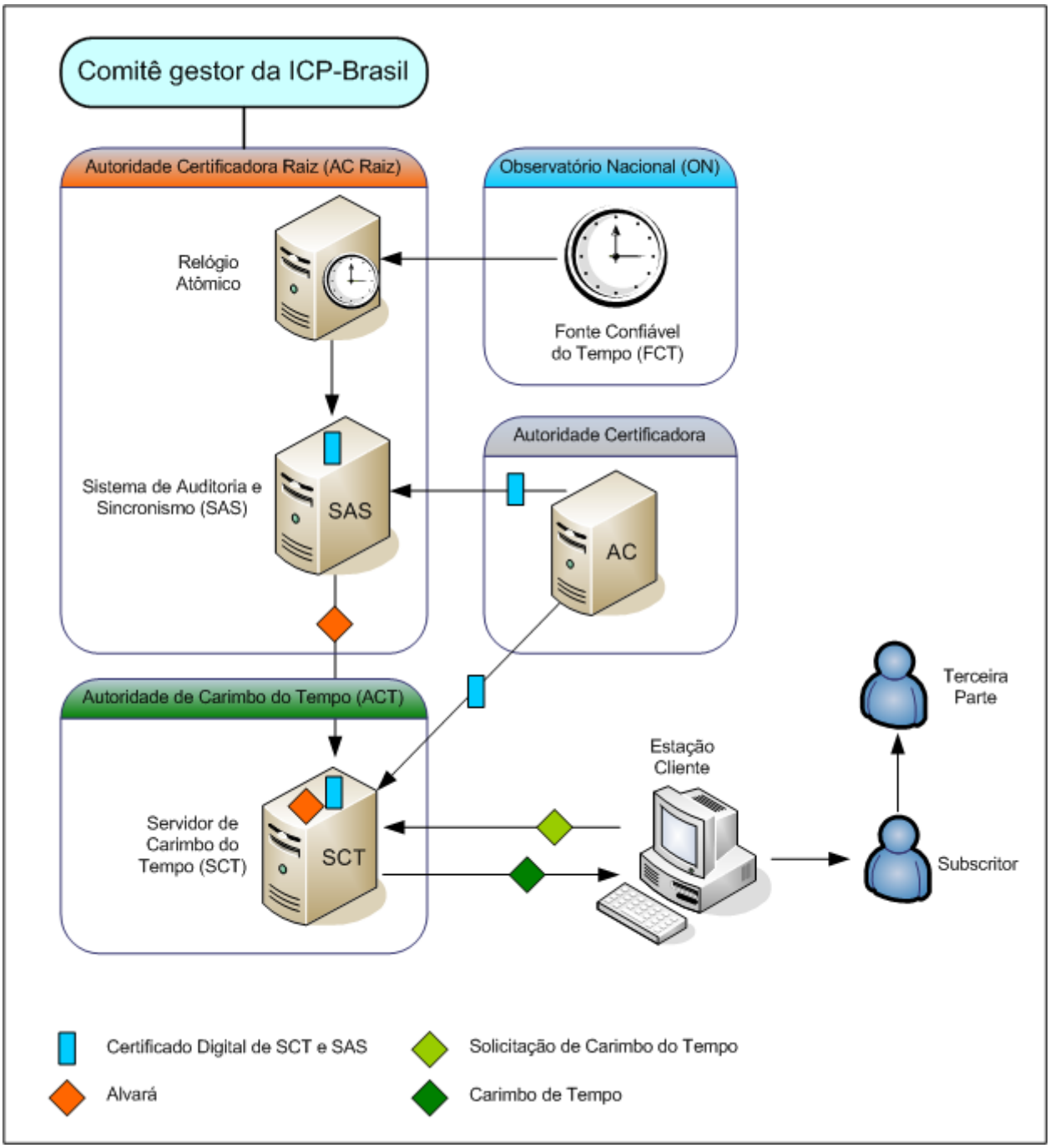
Esta seção descreve os requisitos gerais de carimbo do tempo que devem ser atendidos por Servidores de Carimbo do Tempo, Sistemas de Auditoria e Sincronismo e Autoridades de Carimbo do Tempo inseridos na estrutura de carimbo do tempo da ICP-Brasil.

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.

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



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

2.1.1.1 Formato da solicitação

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

TimeStampReq ::= SEQUENCE {

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

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

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

2.1.1.2 Formato de Resposta

Conforme a RFC 3161, mensagens de resposta a 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 a 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.

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.

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.

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.

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.

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.

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 infraestrutura 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.

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

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 uma 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.

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

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 uma 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.

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**.

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.

REQUISITO I.16: Um caminho de certificação consiste em uma sequência 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.

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.

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 subsequentes, o Cadastro de Pessoa

Física (CPF) do responsável; nas onze posições subsequentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas quinze posições subsequentes, o número do RG do responsável; nas 6 posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

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.

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. Os dados de auditoria seguem descritos neste documento nos itens 2.2.3 – Suporte a Algoritmos e 2.3.1 - Requisitos Gerais de Segurança.

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.

REQUISITO II.3: Um SCT deve utilizar o seu próprio relógio de tempo real (RTC) 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.

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.

REQUISITO II.5: Replicação de chaves assimétricas privadas de um SCT, mantidas em MSCs associados, deve ser permitida apenas para realização de cópia de segurança (*Backup*).

2.2.3 Suporte a Algoritmos

REQUISITO II.6: 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 construídos como descrito no DOC-ICP-11.01.

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).

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.

O protocolo utilizado pelo SAS para auditar o SCT deverá ser descrito detalhadamente.

REQUISITO III.3: Um Módulo de Segurança Criptográfico (MSC) associado a um SAS deve atender aos requisitos definidos no Manual de Condutas Técnicas 7 – Volume I.

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.

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.

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 associado ao SAS de forma a garantir sua confidencialidade.

REQUISITO III.7: Replicação de chaves assimétricas privadas de um SAS, mantidas em MSC associados, deve ser permitida apenas para realização de cópia de segurança (Backup).

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 um subconjunto dos algoritmos criptográficos definidos conforme DOC-ICP-01.01 item 2 – tabela "Assinaturas Digitais ICP-Brasil".

2.4 Requisitos de Sincronismo do 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.

2.4.1 Protocolos de sincronismo do 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.

REQUISITO IV.3: O sincronismo entre a Fonte Confiável do Tempo e o SAS deve seguir o protocolo descrito no DOC-ICP-11.

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.

2.5 Requisitos de gerenciamento e auditoria de ACTs

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

Também são descritos requisitos relacionados ao Alvará emitido pela Entidade de Auditoria de Tempo (EAT), a qual é representada pela Autoridade Certificadora Raiz (AC-Raiz) dentro da estrutura de carimbo do tempo da ICP-Brasil. A EAT realiza auditorias periódicas nos Servidores de Carimbo do Tempo (SCT) das ACTs, por meio de Sistemas de Auditoria e Sincronismo (SAS). A finalidade deste processo, além de garantir o sincronismo entre os relógios dos SCTs das ACTs e

a Fonte Confiável do Tempo baseada na hora UTC, também é a de garantir que os carimbos do 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.

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.

REQUISITO V.2: Os arquivos de registro (log) armazenados no SAS, referentes a 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.

REQUISITO V.3: Os arquivos de registro (log) armazenados no SCT, referentes a autenticação mútua com o SAS, 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 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;

- 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.

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.

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 respeito 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 associado ao SAS.

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}

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).

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.

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.

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.

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.

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.

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;

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;

REQUISITO V.15: Um SCT só pode emitir carimbos do tempo 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.

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.

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 deve representar uma medida estatística de desvio do relógio.

REQUISITO V.19: Cada SCT deve ser capaz de ser auditado por pelo menos 2 (dois) SAS distintos e situados em locais físicos diferentes.

REQUISITO V.20: Um SAS deve permitir 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.

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.

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

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.

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.

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.

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*.

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*.

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*.

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".

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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**.

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).

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**.

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

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

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.

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.

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

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

- A representação do horário da meia-noite (GMT) deve ser “YYYYMMDD000000Z”, onde “YYYYMMDD” representa o dia seguinte à meia-noite.

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.

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.

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.

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

3 PARTE 2 – MATERIAL E DOCUMENTAÇÃO TÉCNICA DEPOSITADOS PARA O PROCESSO DE HOMOLOGAÇÃO DE EQUIPAMENTOS DE CARIMBO DO TEMPO NO ÂMBITO DA ICP-BRASIL

3.1 INTRODUÇÃO

Esta parte detalha os materiais e a documentação técnica depositados pela Parte Interessada junto ao LEA para a execução dos processos de homologação de equipamentos de carimbo do tempo no âmbito da ICP-Brasil.

Os materiais e a documentação técnica referidos são classificados em três categorias:

- componentes físicos: correspondem às amostras dos equipamentos submetidos ao processo de homologação;
- documentação técnica: corresponde aos documentos de natureza técnica referentes aos dispositivos submetidos ao processo de homologação. Devem ser depositados em formato impresso ou em formato eletrônico. No caso de formato eletrônico, devem estar armazenados, preferencialmente, em mídia tipo “leitura-somente” (*read-only*). Devem estar, obrigatoriamente, escritos nas línguas portuguesa ou inglesa;
- componentes em softwares executáveis: correspondem aos CSPs, drivers, bibliotecas de software, ferramentas de gerenciamento de dispositivo e/ou outros softwares executáveis,

solicitados por este documento, referentes aos dispositivos submetidos ao processo de homologação. Devem ser depositados, obrigatoriamente, em formato eletrônico e armazenados, preferencialmente, em mídia tipo "leitura-somente" (*read-only*).

Três Níveis de Segurança de Homologação (NSH) diferentes foram estabelecidos para carimbos do tempo:

- 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 das aplicações de carimbo do tempo do SCT e sincronismo e auditoria do SAS;
- NSH 3: Este nível requer depósito e análise de código-fonte completo associado ao dispositivo em homologação.

Para os NSHs 2 e 3, a Parte Interessada pode depositar o código-fonte de duas maneiras diferentes:

- Linguagem de alto nível: Código-fonte deve ser depositado, por exemplo, em linguagem C, C++ ou Java. Se o código-fonte estiver escrito em linguagem proprietária ou mesmo em microcódigo, o respectivo manual desta linguagem deve estar contido na documentação bem como compiladores e simuladores para compilação e execução deste código-fonte;
- Linguagem de baixo nível: Código-fonte deve ser depositado em linguagem *assembly*, porém acompanhado do respectivo manual das instruções desta linguagem bem como compiladores e simuladores para compilação e execução deste código-fonte.

3.2 Materiais e documentação técnica depositados para SCT e SAS

3.2.1 Componentes físicos

Independentemente do NSH escolhido pela Parte Interessada, os seguintes componentes físicos devem ser depositados junto ao LEA:

- SCT: Amostras nas quantidades definidas por este documento.
- SAS: Amostras nas quantidades definidas por este documento e disponibilização de comunicação com dois SASs remotos e distintos que serão utilizados para realizar a auditoria e sincronismo do tempo do SCT objeto de homologação.
- Material de apoio: Caso o SCT e SAS submetidos necessitem de hardwares de apoio tais como cartão inteligente, leitora ou token, serão necessárias quantidades mínimas para operação do SCT e/ou SAS.

3.2.2 Documentação - Nível de Segurança de Homologação 1

Os seguintes documentos técnicos devem ser depositados junto ao LEA pela Parte Interessada:

- PIN e PUK padrão: Caso o SCT ou SAS necessitem de hardwares de apoio tais como cartão inteligente ou token para realização da autenticação de entidade usuária externa, o PIN e PUK padrão destes dispositivos devem ser fornecidos;
- Documentação que acompanha o produto: As seguintes informações devem estar descritas na documentação que acompanha o objeto de homologação na sua forma comercial:

- Manual de utilização do SCT e SAS;
- Manual de instalação do SCT e SAS;
- Especificações técnicas do SCT e SAS;
  - Certificados obtidos: Certificações e/ou licenças obtidas para o SCT e SAS emitidas por entidades independentes;
  - Certificados ICP-Brasil do MSC: Certificado referente ao processo de homologação ICP-Brasil do MSC contido no SCT e SAS. Quando desejável pela Parte Interessada os MSCs do SCT e SAS podem ser homologados em sequencialmente, e, portanto, neste caso não se aplica a entrega destes certificados;
  - Documentação técnica específica sobre SCT e SAS que descreve:
- componentes de hardware, software e firmware do SCT e SAS, incluindo suas respectivas versões;
- configuração física dos componentes do SCT e SAS;
- qualquer componente de hardware, software ou firmware que seja excluído dos requisitos de segurança deste Manual de Condutas Técnicas;
- características elétricas, lógicas e físicas aplicáveis ao SCT e SAS;
- papéis de acesso que são suportados pelo SCT e SAS;
- mecanismo de auditoria interna suportado pelo SCT e SAS;
- protocolo utilizado para sincronismo do tempo entre o SCT e SAS;
- mecanismo utilizado para sincronismo do tempo entre o SAS e a Fonte Confiável do Tempo;
- formato da requisição do carimbo do tempo suportado pelo SCT;
- formato de resposta do carimbo do tempo enviado pelo SCT;
- formato dos arquivos de logs do SCT e SAS;
- formato do certificado de atributo (Alvará) gerado pelo SAS e suportado pelo SCT.

- Serviços:

- serviços oferecidos pelo SCT e SAS: para cada serviço, indicar parâmetros de entrada e respectivas saídas, e os papéis de acesso autorizados para execução de cada serviço;

- Identificação e autenticação de entidade usuária externa:
  - mecanismos de autenticação de entidade usuária externa suportados pelo SCT e SAS;
  - tipos de dados de autenticação que são requisitados pelo SCT e SAS para cada mecanismo de autenticação suportado.

3.2.3 Documentação - Nível de Segurança de Homologação 2

Adicionalmente à documentação técnica solicitada no NSH 1, os seguintes itens devem ser depositados junto ao LEA pela Parte Interessada:

- Código-fonte da aplicação de um SCT que recebe solicitações e emite carimbos do tempo;
- Código-fonte da aplicação de um SAS que sincroniza e audita SCTs.

3.2.4 Documentação - Nível de Segurança de Homologação 3

Adicionalmente à documentação técnica solicitada nos NSHs 1 e 2, os seguintes itens devem ser depositados junto ao LEA pela Parte Interessada:

- Código-fonte dos SP (*Service Providers*), CSP (*Cryptographic Service Providers*) e ferramenta de gerenciamento do MSC para SCT e SAS.

3.2.5 Quantidade de materiais e documentação técnica depositados para SCT e SAS

A tabela 6 apresenta a quantidade de materiais e documentação técnica depositados pela Parte Interessada referente ao processo de homologação de equipamento de carimbo do tempo:

- Componentes físicos: amostras de cada modelo e/ou versão de SCT;
- documentação técnica:
  - documentos impressos: devem ser entregues cópias de igual teor;
  - documentos eletrônicos: devem ser entregues cópias de igual teor e armazenadas obrigatoriamente em mídias diferentes (por exemplo, dois CD-ROM com o mesmo conteúdo, apresentando como documentos técnicos, a política de segurança e código-fonte).

Tabela 1: Quantidade de material e documentação técnica depositados pela Parte Interessada junto ao LEA referentes ao processo de homologação de equipamento de carimbo do tempo

Requisito de depósito	**Material e documentos técnicos depositados pela Parte Interessada – NSH 1**	**Quantidade**
1	Servidor de Carimbo do Tempo (SCT)	1 unidade
2	Sistema de Auditoria e Sincronismo (SAS)	1 unidade
3	Acesso lógico a 2 (dois) SAS remotos	-
4	Login e senha para o SCT e SAS	-
5	Documentação que acompanha o produto	2 cópias
6	Relação de certificados obtidos	2 cópias
7	Documentação técnica específica sobre o SCT	2 cópias
8	Outros documentos que a Parte Interessada julgar relevante para o processo	2 cópias
Requisito de depósito	**Material e documentos técnicos depositados pela Parte Interessada – NSH 2**	**Quantidade**
9	Código-fonte da aplicação de um SCT que recebe solicitações e emite carimbos do tempo;	2 cópias
10	Código-fonte da aplicação de um SAS que sincroniza e audita SCTs.	2 cópias
Requisito de depósito	**Material e documentos técnicos depositados pela Parte Interessada – NSH 3**	**Quantidade**
11	Código-fonte dos SP (*Service Providers*), CSP (*Cryptographic Service Providers*) e ferramenta de gerenciamento do MSC para SCT e SAS.	2 cópias

4 REFERÊNCIAS BIBLIOGRÁFICAS

INFRAESTRUTURA 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.

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

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

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

INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. Rede de Carimbo do Tempo na ICP-Brasil – Recursos Técnicos. DOC-ICP-11.01. Versão 1.0. Brasília. Novembro 2020.

INFRAESTRUTURA 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.

INFRAESTRUTURA 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.

INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. Procedimentos para auditoria do tempo na ICP-Brasil. DOC-ICP-14. Versão 1.1. Brasília. Outubro 2009.

INFRAESTRUTURA 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. Housley, R.; Polk, W.; Ford, W. e Solo, D. 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: 07.abr.2010.

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. An Internet Attribute Certificate Profile for Authorization. RFC 3281, Category: Standards Track, April 2002. Disponível em <http://www.ietf.org/rfc/rfc3281.txt>. Acesso em: 07.abr.2010.

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.