Infra-Estrutura de Chaves Públicas Brasileira

Manual de Condutas Técnicas 10 - Volume I

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

versão 1.0

Sumário

Listas de Ilustrações

Lista de Figuras

Lista de Tabelas

Glossário

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

Lista de Acrônimos

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

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

1 Introdução

Este documento descreve os requisitos técnicos observados no processo de homologação de equipamentos de carimbo do tempo no âmbito da Infra-Estrutura 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 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 a operação de um ou mais SCT, conectados à Rede de Carimbo do tempo da ICP-Brasil, que geram carimbos e assinam em nome da ACT;
- **Entidade de Auditoria do Tempo (EAT):** é a entidade responsável pela verificação da correta operação do Serviço de Carimbo do Tempo mantida pela Autoridade de Carimbo do Tempo;
- **Sistema de Auditoria e Sincronismo (SAS)**: hardware constituído por um MSC provido de relógio interno onde é executado software que audita e sincroniza SCTs e outros SAS. Como componentes;
- **Observatório Nacional (ON):** vinculado ao Ministério da Ciência e Tecnologia, integrante do Sistema Nacional de Metrologia (SINMETRO), o

ON é o responsável legal pela geração, conservação e disseminação da Hora Legal Brasileira, com rastreabilidade metrológica ao BIPM (*Bureau International des Poids et Mesures*). Mantém e opera o Relógio Atômico, que é a Fonte Confiável do Tempo – FCT, a partir da qual se determina a Hora Legal Brasileira.

1.1 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 aplicam-se aos seguintes componentes:

- Servidor de Carimbo do Tempo:
  - Módulo de Segurança Criptográfico (MSC);

- softwares embarcado 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 titulares finais. Emite e publica LCR. Na estrutura de carimbo do tempo da ICP-Brasil emite os certificados digitais usados nos equipamentos das ACTs e da EAT e emite ainda os demais certificados utilizados nos processos relacionados aos carimbos do tempo;
- **Subscritor ou Cliente** – Pessoa física ou jurídica que solicita os serviços de uma Autoridade de Carimbo do Tempo (ACT), implícita ou explicitamente, concordando com os termos mediante os quais o serviço é oferecido;
- **Terceira Parte (*Relying Part*)** – Aquele que confia no teor, validade e aplicabilidade do carimbo do tempo produzido pela ACT.

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

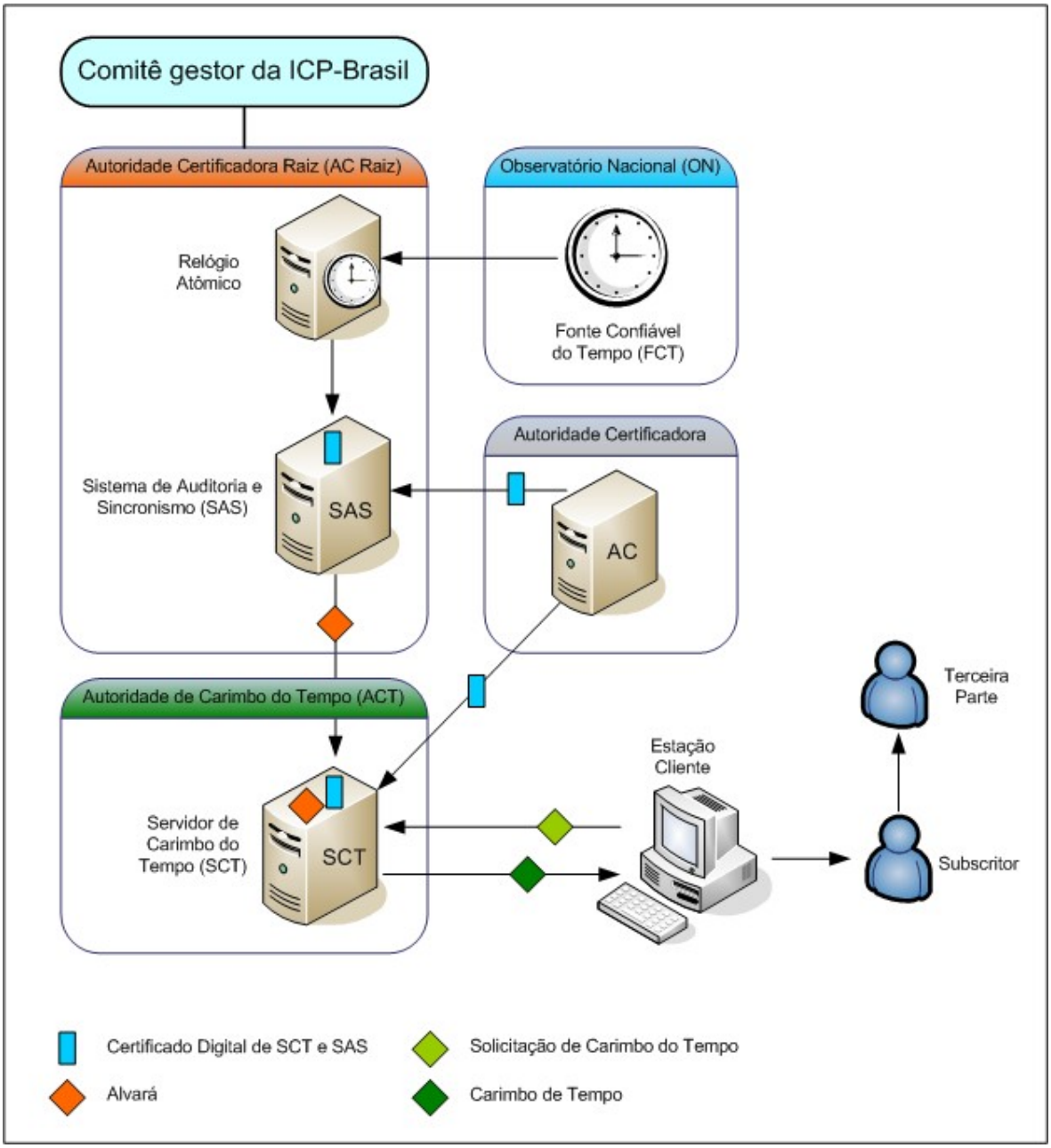

Figura 1: Modelo geral da estrutura de carimbo do tempo no âmbito da ICP-Brasil.

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

2.1.1.1 Formato da solicitação

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

TimeStampReq ::= SEQUENCE {

version Version,

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

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

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

2.1.1.2 Formato da 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 à uma solicitação de carimbo do tempo deve conter, no mínimo, os seguintes campos conforme definidos pela RFC 3161:

- "*status*": [OBRIGATÓRIO] contém a estrutura "*PKIStatusInfo*" conforme definida na seção 3.2.3 da RFC 2510 pelos seguintes campos:
    - "*status*": indica a presença ou ausência de um carimbo do tempo na resposta da solicitação;
    - "*statusString*": campo opcional que descreve o motivo da ausência de um carimbo do tempo na resposta da solicitação;
    - "*failInfo*": indica o motivo da ausência de um carimbo do tempo na resposta da solicitação.

- "*timeStampToken*": [OPCIONAL] campo do tipo "*ContentInfo*" que encapsula um conteúdo do tipo "*SignedData*", conforme os seguintes campos:
    - "*TimeStampToken*": este campo possui o seguinte conteúdo:
        - "*eContentType*": contém o OID que especifica o tipo de conteúdo
        - "*eContent*": conteúdo propriamente dito em codificação DER
    - "*TSTInfo*": este campo possui o seguinte conteúdo:
        - "*version*": descreve a versão do carimbo do tempo (atualmente v1);
        - "*policy*": indica a política da ACT sob a qual esta resposta foi produzida;
        - "*messageImprint*": tamanho do *hash* conforme o algoritmo e o tamanho do *hash* indicado na solicitação;
        - "*serialNumber*": valor inteiro atribuído pela ACT para cada carimbo do tempo;
        - "*genTime*": instante em que o carimbo do tempo foi criado pela ACT.
        - "*accuracy*": desvio de tempo em relação ao UTC no formato *GeneralizedTime*;
        - "*ordering*": indica se existe uma ordem cronológica nos carimbos do tempo criados pela ACT;
        - "*nonce*": contém o mesmo valor do campo "*nonce*" da solicitação do carimbo do tempo;
        - "*tsa*": deve conter informações a respeito da ACT;
        - "*extensions*": campo para inserir informações adicionais, conforme definido pela RFC 2459.

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 a estrutura de carimbo do tempo da ICP-Brasil.

2.1.4 Requisitos de certificação digital

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

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

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

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

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

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

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 contida em um SAS deve ser capaz de manipular certificados digitais que implementam a versão 3 do padrão ITU-T X.509 (X.509v3). Especificamente para certificados digitais ICP-Brasil

de SAS, designados somente para fins de assinatura digital de alvarás, as seguintes extensões são obrigatórias:

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

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 de 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.

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 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.

2.2 Requisitos de segurança para SCT

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

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

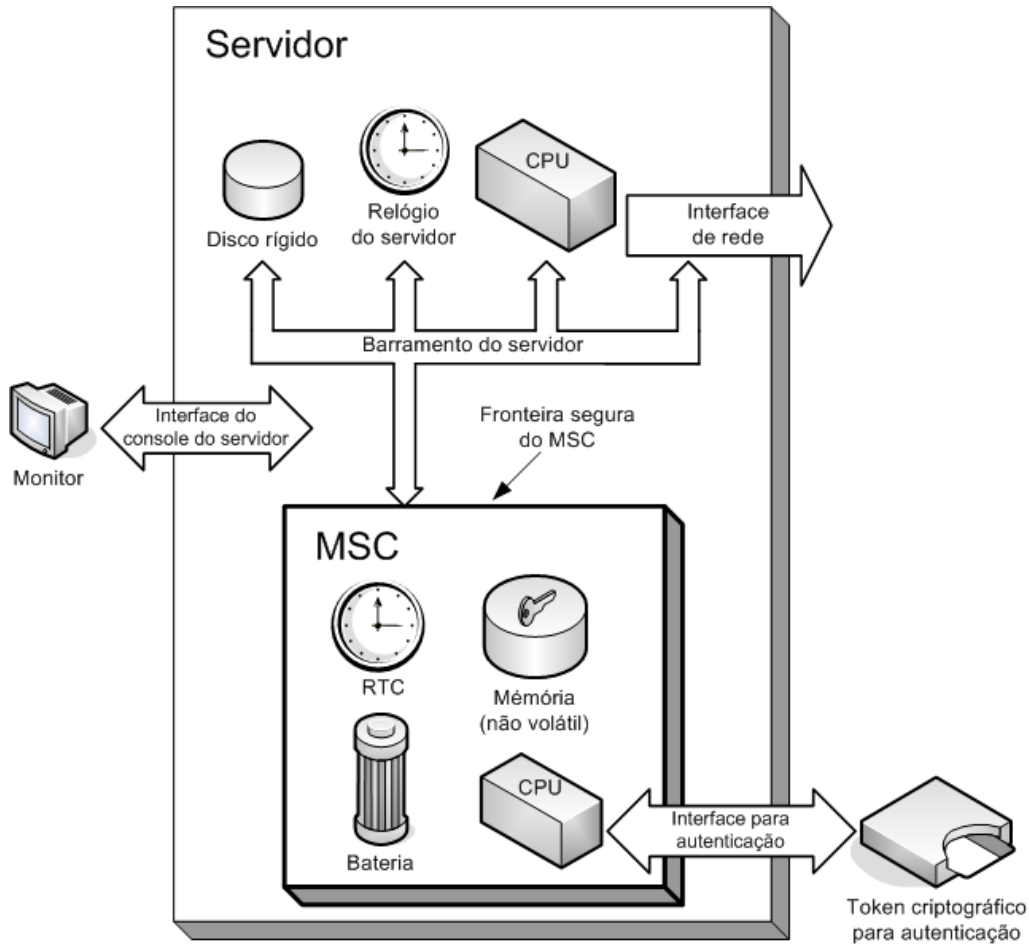

Figura 2: Principais componentes de um Servidor de Carimbo do Tempo

2.2.1 Requisitos gerais de segurança

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

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

- Especificação do módulo criptográfico;
- Portas e interfaces do módulo criptográfico;

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

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

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

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

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

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

2.2.2 Gerenciamento de chaves criptográficas

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

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

2.2.3 Suporte a algoritmos

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

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

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

2.3 Requisitos de segurança para SAS

Esta seção descreve requisitos relacionados à segurança de Sistemas de Auditoria e Sincronismo (SAS). O SAS é o componente responsável por auditar e sincronizar Servidores de Carimbo do Tempo (SCT), emitindo Alvará de operação para SCTs.
De maneira geral, um SAS é constituído por um servidor (*Host*) que possui um Módulo de Segurança Criptográfica (MSC) instalado em seu interior. Como fonte de tempo para um SAS, pode-se utilizar um relógio de tempo real (*Real Time Clock* -

RTC) localizado dentro da fronteira segura do MSC, ou em um módulo específico para sincronismo do tempo. Esta fonte de tempo é periodicamente sincronizada com um relógio atômico.

2.3.1 Requisitos gerais de segurança

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

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

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

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

REQUISITO III.4: Sistemas de Auditoria e Sincronismo devem possuir mecanismos que reagem contra o acesso físico não autorizado aos seus componentes internos, como por exemplo, proteções físicas instaladas em portas, tampas e outras interfaces de acesso físico. Tais mecanismos podem consistir em sensores acoplados às interfaces de acesso físico ao interior do SAS e do MSC. Quando

acionados, o SAS deve interromper a realização de auditorias e sincronismo do tempo, destruindo todas as chaves criptográficas armazenadas.

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

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

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

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

2.3.2 Gerenciamento de chaves criptográficas

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

2.3.3 Suporte a algoritmos

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

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

2.4 Requisitos de Sincronismo do Tempo

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

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

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

2.4.1 Protocolos de sincronismo do tempo

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

REQUISITO IV.10: O protocolo de sincronismo do tempo deve conter o campo *Root Dispersion*, com tamanho de 32 bits (*fixed-point*), que indica o erro máximo relativo à

fonte de referência de tempo primária em segundos, indicando frações de tempo entre os bits 15 e 16. Apenas valores maiores que zero são possíveis de serem atribuídos a este campo.

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

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

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

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

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

2.4.2 Exatidão do relógio

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

2.5 Requisitos de gerenciamento e auditoria de ACTs

Esta seção descreve requisitos relacionados aos processos de gerenciamento das atividades de uma Autoridade de Carimbo do Tempo. Tais processos, são

praticados por uma ACT para que sejam compiladas informações relevantes para os processos de auditoria.

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

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

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

2.5.1 Registros

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

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

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

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

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

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

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

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

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

2.5.2 Alvará

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

A estrutura principal do Alvará deve apresentar o seguinte formato:

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

A estrutura *AttributeCertificateInfo* deve apresentar o seguinte conteúdo:

```
AttributeCertificateInfo ::= SEQUENCE {
        version                 AttCertVersion,
        holder                  Holder,
        issuer                  AttCertIssuer,
        signature               AlgorithmIdentifier,
        serialNumber            CertificateSerialNumber,
        attrCertValidityPeriod  AttCertValidityPeriod,
        attributes              SEQUENCE OF Attribute,
        issuerUniqueID          UniqueIdentifier OPTIONAL,
        extensions              Extensions OPTIONAL
}
```

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

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

```
}
AttCertValidityPeriod ::= SEQUENCE {
        notBeforeTime       GeneralizedTime,
        notAfterTime        GeneralizedTime
}
```

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, 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, no intervalo de tempo entre duas auditorias sucessivas, o relógio de um SCT não apresentar erro (*Offset*) acumulado que ultrapasse o valor especificado na Política de Carimbo do Tempo correspondente.

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.

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 e sincronismo com um SAS das seguintes formas:

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

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

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

2.5.3 Requisitos específicos de auditoria de ACTs

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

- Iniciação e desligamento do SCT;
- Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da ACT;

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

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.

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*. 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.

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

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 não deve emitir o carimbo do tempo e deve 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 2459.

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, o certificado do SCT deve ser incluído 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 da ACT.

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 ser único para cada carimbo do tempo gerado por uma determinada ACT.

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

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

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 da ACT deve ser incluído como um atributo *signerInfo* dentro do atributo *SigningCertificate*.

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

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.

Adicionalmente aos Níveis de Segurança de Homologação, são estabelecidos dois Níveis de Segurança Física (NSF):

- NSF 1: Este nível requer que o módulo criptográfico suporte no mínimo os mecanismos de segurança física que evidenciam e resistem à violação.
- NSF 2: Além dos mecanismos de segurança física que são suportados no NSF 1, este nível requer que o módulo criptográfico suporte também mecanismos de segurança física que detectam e respondem à violação.

3.2 Materiais e documentação técnica depositados para MSC (aplicável para SCT e SAS)

3.2.1 Componentes físicos

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

- Módulo de segurança criptográfica operacional: Amostras de MSC operacionais nas quantidades definidas por este documento para cada modelo e/ou versão de MSC a ser submetido ao processo de homologação.
- Módulo de segurança criptográfica não operacional: Amostras de MSC não operacionais, com características idênticas, nas quantidades definidas por este documento para cada modelo e/ou versão de MSC a ser submetido ao processo de homologação.
- Componentes de segurança física: Amostras de cada componente responsável por garantir um determinado tipo de segurança física no módulo criptográfico, como por exemplo, micro *switches*, sensores ou outros dispositivos conforme o Nível de Segurança Física pretendido.

- Material de apoio: Caso o MSC submetido necessite de hardware de apoio como cartão inteligente, leitora ou *token*, serão necessárias quantidades mínimas para operação do módulo criptográfico.

3.2.2 Documentação - Nível de Segurança da Homologação 1

Manuais

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

- Instalação, configuração e operação
- Administrador (*Security Officer*)

Documentos Técnicos Específicos

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

- Documentação sobre especificação do MSC que descreve:
  - Componentes de hardware, software e *firmware*;
  - Fronteira criptográfica;
  - Configuração física do MSC;
  - Componentes de hardware, software ou *firmware* que estejam excluídos destes requisitos;
  - Características elétricas, lógicas e físicas;
  - Especificação das funções de segurança e operações criptográficas empregadas pelo MSC;
  - Diagrama de blocos detalhando todos os principais componentes de hardware e interconexões;
  - Local de armazenamento de PCSs e outros dados críticos nos componentes de hardware;
  - Política de segurança não proprietária do MSC;
  - Algoritmos criptográficos suportados.

- Documentação sobre portas e interfaces do MSC que descreve:
  - Interfaces lógicas;
  - Interface de entrada de dados;
  - Interface de saída de dados;

- Entrada de controle;
- Saída de estado.

- Documentação sobre papéis, serviços e autenticação no MSC que descreve:
  - Controle de acesso empregado pelo MSC;
  - Mecanismos de autenticação (baseado em papel ou identidade) e os tipos de dados de autenticação necessários;
  - Papéis autorizados suportados pelo MSC;
  - Funcionalidades atribuídas ao papel de acesso “Usuário”;
  - Funcionalidades atribuídas ao papel de acesso “Oficial de Segurança”;
  - Funcionalidades atribuídas ao papel de acesso “Manutenção”;
  - Funcionalidades que não requerem autenticação;
  - Força ou robustez dos mecanismos de autenticação suportados pelo MSC.

- Documentação sobre o modelo de estado finito do MSC que descreve:
  - Estados que o MSC pode assumir;
  - Diagrama de transição dos estados do MSC.

- Documentação sobre a segurança física do MSC que descreve:
  - Descrição de todos os componentes de hardware, software, *firmware* que estão contidos na fronteira criptográfica e protegidos pelos mecanismos de segurança física implementados;
  - Descrição dos mecanismos de segurança física implementados no MSC e seus respectivos componentes/circuitos associados;
  - Descrição de portas, tampas ou interfaces de acesso para manutenção no MSC;
  - Descrição dos mecanismos de destruição de chaves criptográficas simétricas e assimétricas privadas e PCSs ;
  - Descrição dos sensores para portas, tampas ou interfaces presentes no MSC.

- Documentação sobre o ambiente operacional do MSC que descreve:
  - Ambiente operacional utilizado pelo MSC;
  - Homologações prévias do ambiente operacional
  - Especificar o conjunto de papéis de acesso que podem:
    - Ativar a execução do software e do *firmware*;
    - Modificar componentes de software ou *firmware*;
    - Ler componentes armazenados no MSC;
    - Inserir chaves criptográficas e PCS.
  - Mecanismos de auditoria para registrar modificações, acessos, apagamentos e adições aos dados críticos e PCS;
  - Utilização de caminho confiável (*Trusted path*) pelo MSC.

- Documentação sobre gerenciamento de chaves criptográficas no MSC que descreve:
  - Chaves criptográficas, seus componentes e PCSs empregados pelo MSC;
  - Métodos utilizados pelo MSC para proteger chaves secretas, chaves privadas e PCS contra divulgação, modificação e substituição não autorizada;
  - Métodos utilizados pelo MSC criptográfico para proteger chaves públicas contra modificação e substituição não autorizada;
  - Métodos de geração de números aleatórios empregados pelo MSC (aprovado ou não pelo padrão FIPS);
  - Métodos de geração de chaves criptográficas empregados pelo MSC (aprovado ou não pelo padrão FIPS).
  - Métodos de atribuição de chaves empregados pelo MSC;
  - Métodos de importação e exportação de chaves criptográficas empregados pelo MSC (aprovados ou não pelo padrão FIPS);
  - Métodos de armazenamento de chaves criptográficas empregados pelo MSC;
  - Métodos de sobrescrita de chaves criptográficas com zeros binários que são empregados pelo MSC.

- Documentação sobre auto-testes do MSC que descreve:
  - Auto-testes realizados pelo MSC;
  - Estado que o módulo criptográfico pode assumir quando um auto-teste falha ou não;
  - Condições e ações necessárias para sair dos estados de erro e reiniciar a operação normal do módulo criptográfico.

- Documentação sobre mitigações de ataques no MSC que descreve:
  - Proteção contra ataques não invasivos;
  - Proteção contra outros tipos de ataques.

- Documentação sobre gerenciamento do MSC que descreve:
  - Processo de atualização de *firmware* do MSC;
  - Mecanismo de ativação do MSC;
  - Utilitários de administração e diagnósticos.

Documentação complementar

Os seguintes documentos técnicos podem ser depositados junto ao LEA pela Parte Interessada para complementar a documentação técnica específica descrita anteriormente:

- Política de segurança não proprietária: Política de segurança não proprietária (pública) de acordo com o programa de validação de módulos criptográficos mantido pelo NIST, especificamente quanto ao padrão FIPS 140-2;
- Relação de certificados obtidos: Relação de certificações e/ou licenças obtidas de entidades independentes para o módulo criptográfico;
- Outros documentos: Projetos técnicos e suas especificações que a Parte Interessada julgar necessários para completar toda documentação técnica exigida.

3.2.3 Documentação - Nível de Segurança da Homologação 2

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

- Código-fonte do componente PRNG *(Pseudo Random Number Generator);*

- Código-fonte do componente de geração de chaves;
- Código-fonte do componente de atribuição de chaves;
- Código-fonte do componente de sobrescrita de chaves;
- Código-fonte do componente de armazenamento de chaves;
- Código-fonte do componente de importação/exportação de chaves e sementes;

3.2.4 Documentação - Nível de Segurança da Homologação 3

Adicionalmente à documentação técnica solicitada no NSH 1 e NSH 2, os seguintes itens devem ser depositados junto ao LEA pela Parte Interessada:

- Código-fonte embarcado: Relação de todo código-fonte de software e/ou *firmware* embarcados no MSC;
- Código-fonte de apoio: Relação de todo código-fonte de apoio relacionado às interfaces de programação (API), SDK (*Software Development Kits*), SP (*Service Providers*), CSP, ferramenta de gerenciamento e bibliotecas de software suportadas pelo MSC.

3.2.5 Quantidade de materiais e documentação técnica depositados para MSC (aplicável a SCT e SAS)

Esta seção apresenta os materiais e os documentos técnicos depositados pela Parte Interessada junto ao LEA referente ao processo de homologação de MSC contidos no SCT e SAS.

As quantidades de material e documentos técnicos apresentados nesta seção devem seguir os seguintes critérios:

- Quanto aos componentes físicos: devem ser entregues ao LEA uma amostra operacional e duas amostras não operacionais para cada modelo e/ou versão de MSC contido em um SCT e SAS submetidos ao processo de homologação;
  - Componentes de segurança física: devem ser entregues ao LEA três amostras operacionais de cada tipo de componente utilizado na segurança física do MSC.

- Material de apoio: no contexto do MSC entregue deve incluir o seguinte material
  - Leitora de cartão inteligente: amostras necessárias para a utilização de mecanismos de controle de acesso implementados por meio de cartão inteligente;
  - Cartão inteligente: amostras necessárias para utilização de mecanismos de controle de acesso implementados por meio de cartão inteligente;
  - *Token* criptográfico: amostras necessárias para utilização de mecanismos de controle de acesso implementados por meio de *token* criptográfico;
- Quanto à documentação técnica:
  - Documentos impressos (Documentos técnicos): cópias de igual teor (por exemplo, três cópias impressas do manual de segurança do módulo criptográfico);
  - Documentos eletrônicos (Documentos técnicos): cópias de igual teor e armazenadas, obrigatoriamente, em mídias diferentes (por exemplo, dois CD-ROM com o mesmo conteúdo, apresentando como documentos técnicos o manual de usuário, a política de segurança não proprietária, o manual da ferramenta de gerenciamento e o código-fonte);
- Quanto aos componentes em softwares executáveis: cópias de igual teor e armazenadas, obrigatoriamente, em mídias diferentes (por exemplo, dois CD-ROM com o mesmo conteúdo, apresentando como componentes em softwares executáveis a ferramenta de gerenciamento do módulo criptográfico e o CSP do módulo criptográfico).

Tabela 5: Quantidade de materiais e documentos técnicos depositados para homologação de MSC contido em um SCT e SAS.

Requisito de depósito	**Materiais e documentos técnicos depositados pela Parte Interessada – NSH 1**	**Quant.**
1	MSC (Módulo de segurança criptográfica)	1
2	MSC não operacional	2
3	Componentes de segurança física (para cada tipo)	3
4	Cartão inteligente de acesso (conforme aplicável)	-
5	Leitora de cartão inteligente (conforme aplicável)	-
6	*Token* de acesso (conforme aplicável)	-
7	PIN padrão para os cartões inteligentes ou *tokens (conforme aplicável)*	-
8	Documentação técnica específica	2
9	Política de segurança não proprietária	2
10	Manual de usuário e manual de instalação	2
11	Relação de certificados obtidos	2
12	Outros documentos	2
Requisito de depósito	**Materiais e documentos técnicos depositados pela Parte Interessada – NSH 2**	
13	Código-fonte do componente PRNG *(Pseudo Random Number Generator*)	2
14	Código-fonte do componente de geração de chaves	2
15	Código-fonte do componente de atribuição de chaves	2
16	Código-fonte do componente de sobrescrita de chaves	2
17	Código-fonte do componente de armazenamento de chaves	2
18	Código-fonte do componente de importação/exportação de chaves e sementes	2
Requisito de depósito	**Materiais e documentos técnicos depositados pela Parte Interessada – NSH 3**	
19	Código-fonte embarcado	2
20	Código-fonte de apoio	2
Requisito de depósito	**Componentes em software executável depositados pela Parte Interessada – NSH 1, 2 e 3**	
21	Provedor(es) de serviço criptográfico	2
22	Ferramenta de gerenciamento do módulo criptográfico	2
23	Outras bibliotecas de software e/ou programas	2

3.3 Materiais e documentação técnica depositados para SCT e SAS

3.3.1 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: Disponibilização da comunicação e acesso físico direto dois SASs diferentes que serão utilizados para realizar a auditoria e sincronismo do tempo do SCT objeto de homologação.
- Componentes de segurança física: Amostras de cada componente responsável por garantir um determinado tipo de segurança física ao SCT e SAS.
- Material de apoio: Caso o SCT submetido necessite de hardware de apoio como cartão inteligente, leitora ou *token*, serão necessárias quantidades mínimas para operação do SCT e/ou SAS.

3.3.2 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 hardware de apoio como cartão inteligente ou *token* para realização da autenticação de entidade usuária externa;
- Documentação que acompanha o produto: As seguintes informações devem estar descritas na documentação que acompanha o objeto de homologação na sua forma comercial (produto):
  - Manual de utilização do SCT e SAS;
  - manual de instalação do SCT e SAS;
  - especificações técnicas do SCT e SAS;
- Relação de certificados obtidos: Relação de certificação e/ou licenças obtidas para o SCT e SAS emitidas por entidades independentes;
- 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 do SCT e SAS;
- qualquer componente de hardware, software ou *firmware* que seja excluído dos requisitos de segurança;
- características elétricas, lógicas e físicas aplicáveis ao SCT e SAS;
- projeto dos componentes de hardware, software e *firmware* do SCT e SAS;
- papéis de acesso que são suportados pelo SCT e SAS;
- métodos de verificação e validação do certificado digital usado no processo de carimbo do tempo pelo SCT;
- mecanismo de auditoria interna disponibilizados pelo SCT e SAS;
- mecanismos de segurança física adotados para mitigar ataques físicos ao SCT e SAS;
- tempo médio entre falhas para SCT e SAS;
- tempo médio para recuperação de falhas para SCT e SAS;
- protocolo utilizado para sincronismo do tempo entre o SCT e SAS;
- protocolo 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 e versão dos certificados digitais usados pelo SCT e SAS
- formato dos arquivos de *logs* do SCT e SAS;
- formato e versão do certificado de atributo (alvará) utilizado pelo SCT;
- formato do TST.

- Serviços:
  - Serviços oferecidos pelo SCT e SAS: para cada serviço suas entradas de serviço, suas correspondentes saídas de serviço e os papéis de acesso autorizados nos quais o serviço pode ser realizado;
  - demonstração de que para cada serviço oferecido pelo SCT e SAS, nos quais não é necessária a autenticação, a segurança do SCT e SAS não é afetada.
- Identificação e autenticação de entidade usuária externa:
  - Mecanismos de autenticação suportados pelo SCT e SAS;

- tipos de dados de autenticação que são requisitados pelo SCT e SAS para implementar os mecanismos de autenticação suportados;
- Exportação de *logs*:
  - Métodos de exportação de dados, como *log* de transações e algoritmos criptográficos utilizados nos métodos de exportação.

3.3.3 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.

3.3.4 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.

3.3.5 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 6: Quantidade de material e documentação técnica depositados pela Parte Interessada junto ao LEA referente 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	SCT	1 unidade
2	Acesso lógico e físico ao SAS	2 unidades
3	Login e senha padrão, para o SCT e SAS	-
4	Política de segurança	2 cópias
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	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 Normativas

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

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

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

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

COMITÊ GESTOR DA ICP-BRASIL. **Resolução N° 60, de 28 de novembro de 2008: Requisitos mínimos para as políticas de carimbo do tempo da ICP-Brasil.** Brasília: ICP-BRASIL, 2008. 7 p.

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

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

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Information technology -- ASN.1 encoding rules: Specification of Basic Encoding Rules**

(BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) – ISO/IEC 8825-1. Genève, Switzerland, Reference Number: ISO/IEC 8825-1:2002.

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

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

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

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

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

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

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

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

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