POLÍTICA DE CERTIFICADO DE ASSINATURA TIPO T4

PC T4 - AC SAFEWEB TIMESTAMPING

Versão 1.0
Julho 2020

AC SAFEWEB TIMESTAMPING
POLÍTICA DE CERTIFICADO DE ASSINATURA – TIPO T4

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou alteração	Item alterado
1.0	01/07/2020	N/A	Versão inicial

1 INTRODUÇÃO

A ICP-Brasil é uma plataforma criptográfica de confiança. Garante presunção de validade jurídica aos atos e negócios eletrônicos assinados e cifrados com certificados digitais e chaves emitidos pelas entidades credenciadas na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

1.1 VISÃO GERAL

1.1.1 O documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [5] estabelece requisitos mínimos a serem obrigatoriamente observados pelas Autoridades Certificadoras (AC), integrantes da ICP-Brasil, na elaboração de suas Políticas de Certificado (PC).

1.1.2 Esta Política de Certificado de Assinatura Digital tipo T4 da AC Safeweb Timestamping, a seguir designada simplesmente por "PC T4 da AC Safeweb Timestamping" adota a mesma estrutura empregada no documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [5].

1.1.3 O tipo de certificado de assinatura digital emitido sob essa PC é o Tipo T4.

1.1.4 Não se aplica.

1.1.5 Não se aplica.

1.1.6 Certificados do tipo T4 somente podem ser emitidos para equipamentos das Autoridades de Carimbo do Tempo (ACTs) credenciadas na ICP-Brasil. Os certificados do tipo T4 estão associados aos mesmos requisitos de segurança, exceto pelo tamanho das chaves criptográficas utilizadas.

1.1.7 Não se aplica.

1.1.8 Não se aplica

1.1.9 Não se aplica.

1.1.10 Não se aplica.

1.2 NOME DO DOCUMENTO E IDENTIFICAÇÃO

1.2.1 Esta Política de Certificado de Assinatura Digital é do tipo T4 da Autoridade Certificadora Safeweb Timestamping. O *Object Identifier* - OID da PC T4 da AC Safeweb Timestamping, atribuído para esta PC, na conclusão do processo de credenciamento da AC junto à ICP-Brasil, é **2.16.76.1.2.304.9.**

1.2.2 Não se aplica.

1.3 PARTICIPANTES DA ICP-BRASIL

1.3.1 AUTORIDADES CERTIFICADORAS

1.3.1.1. Esta PC se refere à AC Safeweb Timestamping, integrante da Infraestrutura de Chaves

Públicas Brasileira (ICP-Brasil), sob a hierarquia da Autoridade Certificadora Safeweb (AC Safeweb), que por sua vez está subordinada hierarquicamente à Autoridade Certificadora Raiz Brasileira (AC Raiz).

1.3.1.2 As práticas e procedimentos de certificação da AC Safeweb Timestamping estão descritos na Declaração de Práticas de Certificação da AC Safeweb Timestamping (DPC - AC Safeweb Timestamping).

1.3.2 AUTORIDADES DE REGISTRO

Os processos de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes são de competência das Autoridades de Registro (AR). As ARs vinculadas à AC Safeweb Timestamping estão relacionadas na página www.safeweb.com.br que contém:

a) Relação de todas as ARs credenciadas;

b) Relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento.

1.3.3 TITULARES DO CERTIFICADO

1.3.3.1 Os Titulares de Certificados desta PC T4 da AC Safeweb Timestamping são pessoas jurídicas, responsáveis por Autoridades de Carimbo do Tempo.

1.3.3.2 Em sendo o Titular do Certificado pessoa jurídica, será designado pessoa física como responsável pelo certificado, que será a detentora da chave privada. Preferencialmente será designado como responsável pelo certificado o representante legal da pessoa jurídica ou um de seus representantes legais.

1.3.4 PARTES CONFIÁVEIS

Considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do certificado digital e chaves emitidas pela ICP-Brasil.

1.3.5 OUTROS PARTICIPANTES

A relação de todos os Prestadores de Serviços de Suporte (PSS), Prestadores de Serviços Biométricos (PSBios) e Prestadores de Serviço de Confiança (PSC), vinculados à AC Safeweb Timestamping estão relacionados na página https://safeweb.com.br/repositorio.

1.4 USABILIDADE DO CERTIFICADO

1.4.1 USO APROPRIADO DO CERTIFICADO

1.4.1.1 Os certificados definidos por esta PC serão utilizados em aplicações mantidas por Autoridades de Carimbo do Tempo, credenciadas na ICP-Brasil, para assinatura de carimbos do tempo.

1.4.1.2 As aplicações e demais programas que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou superior, emitido por qualquer AC credenciada pela AC Raiz.

1.4.1.3 Na definição das aplicações para o certificado definido pela PC, a AC Safeweb Timestamping leva em conta o nível de segurança previsto para o tipo do certificado. Esse nível de segurança é caracterizado pelos requisitos mínimos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados (LCR) e extensão do período de validade do certificado.

1.4.1.4 Não se aplica.

1.4.1.5 Não se aplica.

1.4.1.6 Certificados de tipos T4 serão utilizados em aplicações mantidas por Autoridades de Carimbo do Tempo credenciadas na ICP-Brasil, para assinatura de carimbos do tempo.

1.4.1.7 Não se aplica.

1.4.1.8 Não se aplica.

1.4.2 USO PROIBITIVO DO CERTIFICADO

Não se aplica.

1.5 POLÍTICA DE ADMINISTRAÇÃO

1.5.1 ORGANIZAÇÃO ADMINISTRATIVA DO DOCUMENTO

Nome da AC: AC Safeweb Timestamping

1.5.2 CONTATOS

Endereço: Av. Princesa Isabel, 828, Santana, Porto Alegre/RS, CEP 90620-000.
Telefone: +55 (51) 3018-0300
Página web: https://www.safeweb.com.br
E-mail: compliance@safeweb.com.br

1.5.3 PESSOA QUE DETERMINA A ADEQUABILIDADE DA DPC COM A PC

Nome: Gisele Strey
Telefone: + 55 (51) 3018-0300
E-mail: compliance@safeweb.com.br
Outros: Setor de Compliance

1.5.4 PROCEDIMENTOS DE APROVAÇÃO DA PC

Esta PC é aprovada pela AC Safeweb e pelo ITI. Os procedimentos de aprovação da PC da AC Safeweb Timestamping são estabelecidos a critério do CG da ICP-Brasil.

1.6 DEFINIÇÕES E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	*Capability Maturity Model do Software Engineering Institute*
CMVP	*Cryptographic Module Validation Program*
CN	*Common Name*
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoa Jurídica
COBIT	*Control Objectives for Information and related Technology*
COSO	*Comitee of Sponsoring Organizations*
CONFAZ	Conselho Nacional de Política Fazendária
CPF	Cadastro de Pessoas Físicas
CS	*Code Signing*
DMZ	Zona Desmilitarizada
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
EV	*Extended Validation*
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	*Intrusion Detection System*
IEC	*International Electrotechnical Commission*
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	*International Organization for Standardization*
ITSEC	*European Information Technology Security Evaluation Criteria*
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados

NBR	Norma Brasileira
NIST	*National Institute of Standards and Technology*
NIS	Número de Identificação Social
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
OM-BR	Objetos Metrológicos ICP-Brasil
OU	*Organization Unit*
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	*Proof of Possession*
PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RFC	*Request For Comments*
RG	Registro Geral
SAT	Sistema de Autenticação e Transmissão
SNMP	*Simple Network Management Protocol*
SSL	*Secure Socket Layer*
TCSEC	*Trusted System Evaluation Criteria*
TSDM	*Trusted Software Development Methodology*
UF	Unidade de Federação
URL	*Uniform Resource Locator*

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

Os itens seguintes estão referidos em seus correspondentes na DPC - AC Safeweb Timestamping.

2.1 REPOSITÓRIOS

2.2 PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS

2.3 TEMPO OU FREQUÊNCIA DE PUBLICAÇÃO

2.4 CONTROLE DE ACESSO AOS REPOSITÓRIOS

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

Os itens seguintes estão referidos em seus correspondentes na DPC - AC Safeweb Timestamping.

3.1 NOMEAÇÃO

3.1.1 Tipos de nomes

Os itens seguintes estão referidos em seus correspondentes na DPC - AC Safeweb Timestamping.

4.10 SERVIÇOS DE STATUS DE CERTIFICADO

4.10.1 Características operacionais

4.10.2 Disponibilidade dos serviços

4.10.3 Funcionalidades operacionais

4.11 ENCERRAMENTO DE ATIVIDADES

4.12 CUSTÓDIA E RECUPERAÇÃO DE CHAVE

4.12.1 Política e práticas de custódia e recuperação de chave

4.12.2 Política e práticas de encapsulamento e recuperação de chave de sessão

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Os itens seguintes estão referidos em seus correspondentes na DPC - AC Safeweb Timestamping.

5.1 CONTROLES FÍSICOS

5.1.1 Construção e localização das instalações de AC

5.1.2 Acesso físico

5.1.3 Energia e ar condicionado

5.1.4 Exposição à água

5.1.5 Prevenção e proteção contra incêndio

5.1.6 Armazenamento de mídia

5.1.7 Destruição de lixo

5.1.8 Instalações de segurança (backup) externas (off-site) para AC

5.2 CONTROLES PROCEDIMENTAIS

5.2.1 Perfis qualificados

5.2.2 Número de pessoas necessário por tarefa

5.2.3 Identificação e autenticação para cada perfil

5.2.4 Funções que requerem separação de deveres

5.3 CONTROLES DE PESSOAL

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

5.3.2 Procedimentos de verificação de antecedentes

5.3.3 Requisitos de treinamento

5.3.4 Frequência e requisitos para reciclagem técnica

5.3.5 Frequência e sequência de rodízio de cargos

5.3.6 Sanções para ações não autorizadas

5.3.7 Requisitos para contratação de pessoal

5.3.8 Documentação fornecida ao pessoal

5.4 PROCEDIMENTOS DE LOG DE AUDITORIA

5.4.1 Tipos de eventos registrados

5.4.2 Frequência de auditoria de registros

5.4.3 Período de retenção para registros de auditoria

5.4.4 Proteção de registros de auditoria

5.4.5 Procedimentos para cópia de segurança (Backup) de registros de auditoria

5.4.6 Sistema de coleta de dados de auditoria (interno ou externo)

5.4.7 Notificação de agentes causadores de eventos

5.4.8 Avaliações de vulnerabilidade

5.5 ARQUIVAMENTO DE REGISTROS

5.5.1 Tipos de registros arquivados

5.5.2 Período de retenção para arquivo

5.5.3 Proteção de arquivo

5.5.4 Procedimentos de cópia de arquivo

5.5.5 Requisitos para datação de registros

5.5.6 Sistema de coleta de dados de arquivo (interno e externo)

5.5.7 Procedimentos para obter e verificar informação de arquivo

5.6 TROCA DE CHAVE

5.7 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

5.7.1 Procedimentos gerenciamento de incidente e comprometimento

5.7.2 Recursos computacionais, software, e/ou dados corrompidos

5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade

5.7.4 Capacidade de continuidade de negócio após desastre

5.8 EXTINÇÃO DA AC

6 CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a PC define as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo esta PC. São também definidos outros controles técnicos de segurança utilizados pela AC Safeweb Timestamping e pelas AR vinculadas na execução de suas funções operacionais.

6.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

6.1.1 GERAÇÃO DO PAR DE CHAVES

6.1.1.1 Sendo o titular de certificado uma pessoa jurídica, esta indica por seu(s) representante(s) legal(is), a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

6.1.1.1.1 Não se aplica.

6.1.1.1.2 Não se aplica.

6.1.1.2 O par de chaves criptográficos relativos aos certificados estabelecidos por esta PC é gerado pelo próprio Titular do Certificado, respeitando os seguintes critérios:

a) A geração da chave privada ocorre em hardware criptográfico aprovado pelo CG da ICP-Brasil ou com certificação INMETRO.

b) A entrega do certificado somente ocorre ao detentor da chave privada correspondente à chave pública constante do certificado.

6.1.1.3 O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados é o RSA, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.1.4 Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1]. As chaves privadas correspondentes aos certificados deverão ser armazenadas em hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO e com capacidade de geração de chave, sendo ativados e protegidos por senha e/ou identificação biométrica.

6.1.1.5 A chave privada trafega cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e o repositório utilizado para o seu armazenamento.

6.1.1.6 A mídia de armazenamento da chave privada assegura por meios técnicos e procedimentais adequados, no mínimo, que:

a) A chave privada é única e seu sigilo é suficientemente assegurado;

b) A chave privada não pode, com uma segurança razoável, ser deduzida e é protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e

c) A chave privada é eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

6.1.1.7 A mídia de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.

6.1.1.8 O armazenamento de chaves privadas de terceiros em hardware criptográfico só poderá ser realizada por entidade credenciada como PSC, nos termos do DOC-ICP-17 [4], ou no caso de soluções corporativas de armazenamento de chaves privadas de funcionários, em HSM de propriedade da instituição, mediante o conhecimento e concordância expressa do titular do certificado com a DPC da AC Safeweb Timestamping, que atendam as aplicações demandadas das organizações, com acesso exclusivo por meio da rede interna.

6.1.2 ENTREGA DA CHAVE PRIVADA À ENTIDADE

Item não aplicável.

6.1.3 ENTREGA DA CHAVE PÚBLICA PARA EMISSOR DE CERTIFICADO

A entrega da chave pública do solicitante do certificado é feita por meio eletrônico, em formato PKCS#10, através de uma sessão segura SSL - *Secure Socket Layer*.

6.1.4 ENTREGA DE CHAVE PÚBLICA DA AC SAFEWEB TIMESTAMPING ÀS TERCEIRAS PARTES

A AC Safeweb Timestamping disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, através dos endereços web:

a) Rep.1: http://repositorio.acsafeweb.com.br/ac-safewebts/ac-safewebts.p7b

b) Rep.2: http://repositorio2.acsafeweb.com.br/ac-safewebts/ac-safewebts.p7b

6.1.5 TAMANHOS DE CHAVE

6.1.5.1 O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC Safeweb Timestamping T4 é de 4096 bits.

6.1.5.2 Os algoritmos e os tamanhos de chaves a serem utilizados nos diferentes tipos de certificados da ICP-Brasil estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.6 GERAÇÃO DE PARÂMETROS DE CHAVES ASSIMÉTRICAS E VERIFICAÇÃO DA QUALIDADE DOS PARÂMETROS

6.1.6.1 Os parâmetros de geração e verificação de chaves assimétricas dos titulares de certificados atendem ao padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.6.2 Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.7 PROPÓSITOS DE USO DE CHAVE (CONFORME CAMPO “"KEY USAGE" NA X.509 V3)

Os pares de chaves correspondentes aos certificados emitidos pela AC Safeweb Timestamping são utilizados conforme descrito no item 1.4 desta Política de Certificação. Para isso, os certificados emitidos pela AC Safeweb Timestamping têm ativados os bits *digitalSignature, nonRepudiation e keyEncipherment.*

6.2 PROTEÇÃO DE CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO

A mídia de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) A chave privada é única e seu sigilo é suficientemente assegurado;

b) A chave privada não pode, com uma segurança razoável, ser deduzida e é protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e

c) A chave privada é eficazmente protegida pelo legítimo titular contra a utilização por terceiros, pois é gerada em HSM que segue o padrão de homologação ICP-Brasil ou com certificação INMETRO. Esses módulos criptográficos não permitem a exportação da chave privada e exigem senha para a sua utilização.

6.2.1 PADRÕES E CONTROLE PARA MÓDULO CRIPTOGRÁFICO

6.2.1.1 O módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão de homologação ICP-Brasil ou Certificação INMETRO.

6.2.1.2 Os requisitos aplicáveis ao módulo criptográfico utilizado para geração de chaves criptográficas dos titulares de certificado seguem os definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP BRASIL [1].

6.2.2 CONTROLE "N DE M" PARA CHAVE PRIVADA

Não se aplica.

6.2.3 CUSTÓDIA (*ESCROW*) DE CHAVE PRIVADA

6.2.3.1 A AC Safeweb Timestamping não realiza custódia (*escrow*) de chaves privadas emitidas conforme esta PC.

6.2.3.2 A AC Safeweb Timestamping não implementa a recuperação de chaves privadas.

6.2.4 CÓPIA DE SEGURANÇA DE CHAVE PRIVADA

6.2.4.1 Não é permitida a cópia de segurança da chave privada de certificados T4.

6.2.4.2 A AC Safeweb Timestamping não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido.

6.2.4.3 Não se aplica.

6.2.4.4 Não se aplica.

6.2.5 ARQUIVAMENTO DE CHAVE PRIVADA

6.2.5.1 As chaves privadas das entidades titulares de certificados emitidos por esta PC não são arquivadas.

6.2.5.2 Define-se arquivamento como o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente.

6.2.6 INSERÇÃO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO

Não se aplica, uma vez que a chave é gerada dentro do próprio módulo criptográfico.

6.2.7 ARMAZENAMENTO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO

Ver item 6.1.

6.2.8 MÉTODO DE ATIVAÇÃO DE CHAVE PRIVADA

O titular do certificado pode definir procedimentos necessários para a ativação de sua chave privada.

6.2.9 MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA

O titular do certificado pode definir procedimentos necessários para a desativação de sua chave privada.

6.2.10 MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA

O titular do certificado pode definir procedimentos necessários para a destruição de sua chave privada

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1 ARQUIVAMENTO DE CHAVE PÚBLICA

As chaves públicas da AC Safeweb Timestamping, dos titulares de certificados de assinatura digital e as LCRs por ela emitidas permanecem armazenadas após a expiração dos certificados correspondentes permanentemente para verificação de assinaturas geradas durante seu período de validade.

6.3.2 PERÍODOS DE OPERAÇÃO DO CERTIFICADO E PERÍODOS DE USO PARA AS CHAVES PÚBLICAS E PRIVADAS

6.3.2.1 As chaves privadas dos respectivos titulares são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2 Não se aplica.

6.3.2.3 O período máximo de validade admitido para certificados de assinatura digital Tipo T4 da AC Safeweb Timestamping é de 6 (seis) anos.

6.3.2.4 Não se aplica.

6.3.2.5 Não se aplica.

6.4 DADOS DE ATIVAÇÃO

Nos itens seguintes desta PC estão descritos os requisitos de segurança referentes aos dados de ativação. Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos.

6.4.1 GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO

Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são únicos e aleatórios.

6.4.2 PROTEÇÃO DOS DADOS DE ATIVAÇÃO

Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são protegidos contra uso não autorizado.

6.4.3 OUTROS ASPECTOS DOS DADOS DE ATIVAÇÃO

Não se aplica.

6.5 CONTROLES DE SEGURANÇA COMPUTACIONAL

6.5.1 REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURANÇA COMPUTACIONAL

6.5.1.1 Nos equipamentos onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC Safeweb Timestamping, recomenda-se o uso de mecanismos mínimos que garantam a segurança computacional, tais como:

a) Senha de *BIOS* ativada;

b) Controle de acesso lógico ao sistema operacional;

c) Exigência de uso de senhas fortes;

d) Diretivas de senha e de bloqueio de conta;

e) *Antivírus, antitrojan* e *antispyware*, instalados, atualizados e habilitados;

f) *Firewall* pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades;

g) Sistema operacional mantido atualizado, com aplicação de correções necessárias (*patches, hotfix*, etc.);

h) Proteção de tela acionada no máximo após 02 (dois) minutos de inatividade e exigindo senha do usuário para desbloqueio.

6.5.2 CLASSIFICAÇÃO DE SEGURANÇA COMPUTACIONAL

Não se aplica.

6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1 CONTROLES DE DESENVOLVIMENTO DO SISTEMA

Como descrito no item correspondente da DPC AC Safeweb Timestamping.

6.6.2 CONTROLES DE GERENCIAMENTO DE SEGURANÇA

Como descrito no item correspondente da DPC AC Safeweb Timestamping.

6.6.3 CONTROLES DE SEGURANÇA DE CICLO DE VIDA

Como descrito no item correspondente da DPC AC Safeweb Timestamping.

6.6.4 CONTROLES NA GERAÇÃO DE LCR

Antes de publicadas, todas as LCRs geradas pela AC Safeweb Timestamping são checadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação a número da LCR, data/hora de emissão e outras informações relevantes.

6.7 CONTROLES DE SEGURANÇA DE REDE

Não se aplica.

6.8 CARIMBO DO TEMPO

Em acordo com os REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL [5].

7 PERFIS DE CERTIFICADO E LCR

Os itens seguintes especificam os formatos dos certificados e das LCRs geradas segundo esta PC. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões. Os requisitos mínimos estabelecidos nos itens seguintes são atendidos em todos os tipos de certificados admitidos no âmbito da ICP-Brasil.

7.1 PERFIL DO CERTIFICADO

Todos os certificados emitidos pela AC Safeweb Timestamping, segundo esta PC, estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.1.1 NÚMERO DE VERSÃO

Os certificados emitidos pela AC Safeweb Timestamping, segundo esta PC, implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2 EXTENSÕES DE CERTIFICADO

7.1.2.1 Neste item, a PC descreve todas as extensões de certificado utilizadas e sua criticalidade.

7.1.2.2 A ICP-Brasil define como obrigatórias as seguintes extensões:

a) "***Authority Key Identifier***", não crítica: o campo *keyIdentifier* contém o *hash* SHA-1 da chave pública da AC Safeweb Timestamping;

b) ***"Key Usage***", crítica: configurados conforme disposto no item 7.1.2.7 deste documento;

c) "***Certificate Policies***", não crítica:

c.1) O campo *PolicyIdentifier* contém o OID desta PC: **2.16.76.1.2.304.9**;

c.2) O campo *PolicyQualifiers* contém o endereço *Web* onde se obtém a DPC AC Safeweb Timestamping: http://repositorio.acsafeweb.com.br/ac-safewebts/dpc-acsafewebts.pdf

d) "***CRL Distribution Points***", não crítica: contém o endereço na *Web* onde se obtém a LCR correspondente:

d.1) http://repositorio.acsafeweb.com.br/ac-safewebts/lcr-ac-safewebts.crl

d.2) http://repositorio2.acsafeweb.com.br/ac-safewebts/lcr-ac-safewebts.crl

e) "***Authority Information Access***", não crítica: a primeira entrada contém o método de acesso *id-ad-caIssuer*, utilizando o protocolo de acesso HTTP, para a recuperação da cadeia de certificação no seguinte endereço:

e.1) http://repositorio.acsafeweb.com.br/ac-safewebts/ac-safewebts.p7b

7.1.2.3 SUBJECT ALTERNATIVE NAME

A ICP-Brasil também define como obrigatória a extensão "*Subject Alternative Name*", não crítica, e com os seguintes formatos:

a) Não se aplica.

b) Não se aplica.

c) Para certificado de equipamento ou aplicação:

c.1) 4 (quatro) campos *otherName*, obrigatórios, contendo, nesta ordem:

i. OID = 2.16.76.1.3.8 e conteúdo = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, se o certificado for de pessoa jurídica;

ii. OID = 2.16.76.1.3.3 e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ), se o certificado for de pessoa jurídica;

iii. OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado;

iv. OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do RG do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF;

v. campo *rfc822Name* contendo o endereço e-mail do titular do certificado.

c.2) Não se aplica.

d) Não se aplica.

e) Não se aplica.

7.1.2.4 Os campos *otherName* definidos como obrigatórios pela ICP-Brasil devem estar de acordo com as seguintes especificações:

a) O conjunto de informações definido em cada campo *otherName* deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 *OCTET STRING* ou *PRINTABLE STRING*;

b) Quando os números de CPF, NIS (PIS, PASEP ou CI), RG, CNPJ, CEI, ou Título de Eleitor não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero";

c) Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF. O mesmo ocorre para o campo de município e UF, se não houver número de inscrição do Título de Eleitor;

d) Quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente. No caso de múltiplas habilitações profissionais, deverão ser inseridos e preenchidos os campos (OID) correspondentes às identidades profissionais apresentadas;

e) Todas informações de tamanho variável referentes a números, tais como RG, devem ser preenchidas com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível;

f) As 10 (dez) posições das informações sobre órgão expedidor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor;

g) Apenas os caracteres de A a Z e de 0 a 9, observado o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais.

h) Não se aplica.

7.1.2.5. Campos *otherName* adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidas pela AC Safeweb Timestamping, poderão ser utilizados com OID atribuídos ou aprovados pela AC Raiz.

7.1.2.6 Os outros campos que compõem a extensão *"Subject Alternative Name"* poderão ser utilizados, na forma e com os propósitos definidos na RFC 5280.

7.1.2.7 As extensões *"Key Usage"* e *"Extended Key Usage"* para os referidos tipos de certificado são obrigatórias e obedecem aos propósitos de uso e a criticalidade conforme descrição abaixo:

a) Não se aplica

b) Não se aplica

c) Para certificados de Assinatura de Carimbo do Tempo:

"Key Usage", crítica: somente os bits *digitalSignature, nonRepudiation e keyEncipherement* estão ativados;

"Extended Key Usage", crítica: somente o propósito *timeStamping* OID = 1.3.6.1.5.5.7.3.8 está presente nos certificados de equipamentos de carimbo do tempo de ACT credenciada na ICP-Brasil. Esse OID não deve ser empregado em qualquer outro tipo de certificado.

d) Não se aplica.

e) Não se aplica.

f) Não se aplica.

g) Não se aplica.

7.1.3 IDENTIFICADORES DE ALGORITMO

Os certificados emitidos pela AC Safeweb Timestamping às entidades titulares de certificado são assinados com o uso do algoritmo RSA com SHA-256 como função de *hash* (OID 1.2.840.113549.1.1.11) conforme o padrão PKCS#1.

7.1.4 FORMATOS DE NOME

7.1.4.1 Não se aplica.

7.1.4.2 O certificado digital emitido para equipamentos de carimbo do tempo de Autoridade de Carimbo do Tempo credenciada na ICP-Brasil deverá adotar o *"Distinguished Name"* (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = ICP-Brasil

OU = Safeweb Timestamping

CN = <nome do Servidor de Carimbo do Tempo (incluindo o serial do SCT)>

7.1.4.3 Não se aplica.

7.1.4.4 Não se aplica.

7.1.5 RESTRIÇÕES DE NOME

7.1.5.1 Neste item estão descritas as restrições aplicáveis para os nomes dos titulares de certificados.

7.1.5.2 As restrições aplicáveis para os nomes dos titulares de certificados emitidos pela AC Safeweb Timestamping são as seguintes:

a) não deverão ser utilizados sinais de acentuação, tremas ou cedilhas; e

b) além dos caracteres alfanuméricos, poderão ser utilizados somente os seguintes caracteres especiais:

Caractere	Código NBR9611 (hexadecimal)	Caractere	Código NBR9611 (hexadecimal)
Branco	20	+	2B
!	21	,	2C
“	22	-	2D
#	23	.	2E
$	24	/	2F
%	25	:	3A
&	26	;	3B
´	27	=	3D
(	28	?	3F
)	29	@	40
*	2A	\	5C

7.1.6 OID *(Object Identifier)* DA PC

O OID (*Object Identifier*) desta PC é **2.16.76.1.2.304.9**.

7.1.7 USO DA EXTENSÃO "*Policy Constraints*"

Não se aplica.

7.1.8 SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA

Nos certificados emitidos segundo esta PC, o campo *policyQualifiers* da *extensão “Certificate Policies”* contém o endereço *Web* da DPC AC Safeweb Timestamping: http://repositorio.acsafeweb.com.br/ac-safewebts/dpc-acsafewebts.pdf.

7.1.9 SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS DE PC

Extensões críticas são interpretadas conforme a RFC 5280.

7.2 PERFIL DE LCR

7.2.1 NÚMERO DE VERSÃO

As LCRs geradas pela AC Safeweb Timestamping implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2 EXTENSÕES DE LCR E DE SUAS ENTRADAS

7.2.2.1 Neste item são descritas todas as extensões de LCR utilizadas pela AC Safeweb Timestamping e sua criticalidade.

7.2.2.2 As LCRs da AC Safeweb Timestamping obedecem a ICP-Brasil que define como obrigatórias as seguintes extensões:

a) "***Authority Key Identifier***", não crítica: contém o *hash* SHA-1 da chave pública da AC Safeweb Timestamping que assina a LCR;

b) "***CRL Number***", não crítica: contém um número sequencial para cada LCR emitida pela AC Safeweb Timestamping.

7.3 PERFIL DE OCSP

7.3.1 NÚMERO DE VERSÃO

Não se aplica.

7.3.2 EXTENSÕES DE OCSP

Não se aplica.

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Os itens seguintes estão referidos em seus correspondentes na DPC - AC Safeweb Timestamping.

8.1 FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES

8.2 IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR

8.3 RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA

8.4 TÓPICOS COBERTOS PELA AVALIAÇÃO

8.5 AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA

8.6 COMUNICAÇÃO DOS RESULTADOS

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

Os itens seguintes estão referidos em seus correspondentes na DPC-AC Safeweb Timestamping.

9.1 TARIFAS

9.1.1 TARIFAS DE EMISSÃO E RENOVAÇÃO DE CERTIFICADOS

9.10 PRAZO E RESCISÃO

9.10.1 PRAZO

9.10.2 TÉRMINO

9.10.3 EFEITO DA RESCISÃO E SOBREVIVÊNCIA

9.11 AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES

9.12 ALTERAÇÕES

9.12.1 PROCEDIMENTO PARA EMENDAS

A AC Safeweb Timestamping segue um processo periódico de atualização de suas PCs, que contempla a revisão em duas etapas, a primeira realizada pela equipe de Compliance/Segurança da Informação e a segunda pela aprovação da Diretoria, visando a adequação dos documentos conforme as normas e procedimentos mais atuais da ICP-Brasil. Qualquer alteração nesta PC será submetida à aprovação da AC Raiz.

9.12.2 MECANISMO DE NOTIFICAÇÃO E PERÍODOS

A AC Safeweb Timestamping mantém a versão corrente desta PC para consulta pública em seu repositório *Web*, no endereço: http://repositorio.acsafeweb.com.br/ac-safewebts/pc-t4-acsafewebts.pdf.

9.12.3 CIRCUNSTÂNCIAS NA QUAL O OID DEVE SER ALTERADO

9.13 SOLUÇÃO DE CONFLITOS

9.14 LEI APLICÁVEL

9.15 CONFORMIDADE COM A LEI APLICÁVEL

9.16 DISPOSIÇÕES DIVERSAS

9.16.1 ACORDO COMPLETO

Esta PC representa as obrigações e deveres aplicáveis à AC Safeweb Timestamping e AR e outras entidades citadas. Havendo conflito entre esta PC e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

9.16.2 CESSÃO

9.16.3 INDEPENDÊNCIA DE DISPOSIÇÕES

9.16.4 EXECUÇÃO (HONORÁRIOS DOS ADVOGADOS E RENÚNCIA DE DIREITOS)

9.17 OUTRAS PROVISÕES

Esta PC foi submetida à aprovação, conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3]. Como parte desse processo, além da conformidade com este documento, é verificada a compatibilidade entre a PC e a DPC da AC Safeweb Timestamping.

10 DOCUMENTOS REFERENCIADOS

10.1 RESOLUÇÕES DO COMITÊ-GESTOR DA ICP-BRASIL

Os documentos abaixo são aprovados por Resoluções do Comitê-Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[4]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DEPRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇADA ICP-BRASIL	DOC-ICP-17
[5]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04

10.2 INSTRUÇÕES NORMATIVAS DA AC RAIZ

Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref.	Nome do documento	Código
[1]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL	DOC-ICP-01.01
[2]	ATRIBUIÇÃO DE OID NA ICP-BRASIL	DOC-ICP-04.01