POLÍTICA DE CARIMBO DO TEMPO

DA

AUTORIDADE DE CARIMBO DO TEMPO

ARPEN

(PCT ACT ARPEN)

Versão 1.0 de Fevereiro de 2021.

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Versão	Data	Responsável	Motivo	Descrição
1.0	Fevereiro/2021	Carlos Francisco Tatara	Versão Inicial	

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Este documento faz parte de um conjunto de normativos criados para regulamentar a geração e o uso de carimbos do tempo no âmbito da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil. Tal conjunto se compõe dos seguintes documentos:

a. VISÃO GERAL DO SISTEMA DE CARIMBO DO TEMPO NA ICP-BRASIL [1], documento aprovado pela Resolução nº 58, de 28 de novembro de 2008;

b. REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTIC AS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP- BRASIL [2], documento aprovado pela Resolução nº 59, de 28 de novembro de 2008;

c. REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL [11], este documento, aprovado pela Resolução nº 60, de 28 de novembro de 2008;

d. PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL [3], documento aprovado pela Resolução nº 61, de 28 de novembro de 2008.

1.1.2. Um carimbo do tempo aplicado a uma assinatura digital ou a um documento prova que ele já existia na data incluída no carimbo do tempo. Os carimbos de tempo são emitidos por terceiras partes confiáveis, as Autoridades Certificadoras do Tempo - ACT, cujas operações devem ser devidamente documentadas e periodicamente auditadas pela própria AC Raiz da ICP-Brasil.

1.1.3. A utilização de carimbos do tempo no âmbito da ICP-Brasil é facultativa. Documentos eletrônicos assinados digitalmente com chave privada correspondente a certificados ICP-Brasil são válidos com ou sem o carimbo do tempo.

1.1.4. O presente documento especifica os requisitos mínimos que devem constar de uma política de carimbo do tempo de uma ACT credenciada na ICP-Brasil. O subscritor e as terceiras partes devem consultar a Declaração de Práticas de Carimbo do Tempo (DPCT) da ACT ARPEN para obter detalhes adicionais sobre precisamente como esta Política de Carimbo do Tempo (PCT) é implementada pela ACT. De modo geral, a política de carimbo do tempo indica "o que deve ser cumprido" enquanto uma declaração de práticas da ACT indica "como cumprir", isto é, os processos que serão usados pela ACT para criar carimbos do tempo e manter a precisão do seu relógio.

1.1.5. Este documento foi elaborado com base nas normas da ICP-Brasil, nas RFC 3628 e 3161 do IETF e no documento TS 101861 do ETSI.

1.1.6. Este documento adota a mesma estrutura empregada em toda PCT elaborada no âmbito da ICP-Brasil.

1.1.7. Aplicam-se ainda à ACT ARPEN, no que couberem, os regulamentos dispostos nos demais documentos da ICP-Brasil, dentre os quais se destacam:

a. POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4], documento aprovado pela Resolução nº 02, de 25 de setembro de 2001;

b. CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5], documento aprovado pela Resolução nº 06, de 22 de novembro de 2001;

c. CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6], aprovado pela Resolução nº 24, de 29 de agosto de 2003;

d. CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [7], documento aprovado pela Resolução nº 25, de 24 de outubro de 2003;

e. POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [8], documento aprovado pela Resolução nº 10, de 14 de fevereiro de 2002; e

f. REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL [9], documento aprovado pela Resolução nº 36, de 21 de outubro de 2004.

1.2. Identificação

1.2.1. A Política de Carimbo do Tempo da Autoridade de Carimbo do Tempo ARPEN, a seguir designada simplesmente PCT ACT ARPEN, é identificada pelo OID (*Object Identifier*) 2.16.76.1.6.13.

1.2.2. Os carimbos do tempo emitidos pela ACT ARPEN, segundo esta PCT, seguem os procedimentos descritos na DECLARAÇÃO DE PRÁTICAS D E CARIMBO DO TEMPO DA AUTORIDADE DE CARIMBO DO TEMPO ARPEN (DPCT da ACT ARPEN), cujo OID dessa DPCT é 2.16.76.1.5.13.

1.3. Participantes da ICP-Brasil

1.3.1. Autoridade de Carimbo do Tempo.

Essa Política de Carimbo do Tempo se refere à Autoridade de Carimbo do Tempo da ARPEN.

1.3.2. Prestador de Serviço de Suporte

1.3.2.1. A ACT ARPEN mantém no endereço https://repositorio.bry.com.br/pss-act/ a lista atualizada dos seus prestadores de serviço de suporte.

1.3.2.2. PSS são entidades utilizadas pela ACT para desempenhar atividade descrita nesta DPCT ou na PCT e se classificam em três categorias, conforme o tipo de atividade prestada. ACT ARPEN utiliza como prestadores de serviço de suporte em suas operações:

- PSS BRy - Disponibilização de recursos humanos.
- PSS ARMAZEM - Disponibilização de infraestrutura física e lógica e de recursos humanos.

1.3.2.3. A ACT ARPEN mantém a lista de seus prestadores de serviço de suporte atualizada.

1.3.3. Subscritores

1.3.3.1. A solicitação de carimbos do tempo ocorre nos processos que demandam esse artefato e pode ser realizada por pessoas físicas e jurídicas.

1.3.4. Partes confiáveis

1.3.4.1. Considera-se terceira parte aquela que confia no teor, validade e aplicabilidade do carimbo do tempo.

1.4. Usabilidade do Carimbo do Tempo

1.4.1. Neste item estão relacionados abaixo as aplicações as quais são adequados os carimbos emitidos pela ACT ARPEN:

a. Os carimbos do tempo emitidos pela ACT ARPEN no âmbito desta PCT podem ser utilizados como referência temporal por aplicações ou processos de negócio que necessitem provar a existência de um determinado documento em relação a uma data específica;
b. Uma assinatura digital com carimbo do tempo emitido pela ACT ARPEN garante a irretratabilidade da sua geração, pois o carimbo do tempo serve como evidência de que o certificado do signatário não estava revogado ou expirado no momento da assinatura;
c. Não há proibição de uso de carimbo do tempo por sistemas aplicativos.

1.5. Política de Administração

1.5.1. Organização administrativa do documento

Nome da ACT: Autoridade de Carimbo do Tempo ARPEN.

1.5.2. Contatos

Unidade de Suporte
Nome: BRy Tecnologia SA
Endereço: Rua Lauro Linhares 2010 7º andar – Trindade – CEP: 88036-002 – Florianópolis/SC
Telefone: 48-3234-6696
E-mail: atendimento@bry.com.br

1.5.3. Pessoa responsável pela adequabilidade da DPCT e PCT

Nome: Carlos Francisco Tatara
Endereço: Rua Lauro Linhares 2010 7º andar – Trindade – CEP: 88036-002 – Florianópolis/SC
Telefone: 48-3234-6696
E-mail: tatara@bry.com.br

1.5.4. Procedimento de aprovação da PCT

1.5.4.1. Esta PCT foi submetida à aprovação, durante o processo de credenciamento da ACT responsável, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5].

1.6. Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC RAIZ	Autoridade Certificadora Raiz
ACT	Autoridade de Carimbo do Tempo
DPCT	Declarações de Práticas de Carimbo do Tempo
ETSI	*European Telecommunication Standard Institute*
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IETF	*Internet Engineering Task Force*
OID	*Object Identifiers*
PCT	Política de Carimbo do Tempo
PSS	Prestador de Serviço de Confiança
RFC	*Request For Comments*
SCT	Servidor de Carimbo do Tempo

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

Conforme descrito no item 2 da DPCT da ACT ARPEN.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Conforme descrito no item 3 da DPCT da ACT ARPEN.

4. REQUISITOS OPERACIONAIS

4.1. Solicitação de Carimbos do Tempo

Neste item da PCT estão descritos todos os requisitos e procedimentos operacionais estabelecidos pela ACT ARPEN para as solicitações de emissão carimbo do tempo. Estes requisitos e procedimentos, que deverão ser atendidos e executados pelos subscritores, compreendem:

a. Para solicitar um carimbo do tempo num documento digital, o subscritor deverá gerar uma requisição de carimbo do tempo (TSQ) contendo o hash a ser carimbado. As solicitações de carimbo do tempo serão realizadas através de sistema específico do subscritor ou através da integração de aplicações que utilizem assinatura digital de documentos;
b. O Servidor de Aplicativos da ACT ARPEN não aceitará as solicitações de emissão de carimbo do tempo cujo certificado do subscritor esteja expirado ou revogado
c. O Servidor de Aplicativos da ACT ARPEN não aceitará as solicitações de emissão de carimbo do tempo cujo certificado do subscritor esteja expirado ou revogado;
d. Para solicitações utilizando os protocolos HTTP ou HTTPs, a requisição de carimbo do tempo (Time Stamp Request) deverá conter em seu cabeçalho as credenciais de acesso do subscritor;
e. O Servidor de Aplicativos da ACT ARPEN disponibiliza o serviço de carimbo do tempo através dos protocolos TCP utilizando a porta 318, HTTP utilizando a porta 80 e HTTPs utilizando a porta 443, de acordo com a RFC 3161;
f. Os subscritores deverão utilizar o algoritmo de *hash* SHA-256 para efetuar as solicitações de carimbo do tempo.

4.1.1. Quem pode submeter uma solicitação de carimbo do tempo

Conforme item 4.1.1 da DPCT da ACT ARPEN.

4.1.2. Processo de registro e responsabilidades

Conforme item 4.1.2 da DPCT da ACT ARPEN.

4.2. Emissão de Carimbos do Tempo

Conforme item 4.2 da DPCT da ACT ARPEN.

4.3. Aceitação de Carimbos do Tempo

Os requisitos e procedimentos operacionais estabelecidos pela ACT ARPEN para verificação de um carimbo do tempo compreendem:

a. Verificar o valor do status indicado no campo PKIStatusInfo do carimbo do tempo. Caso nenhum erro estiver presente, isto é, o status estiver com o valor 0 (sucesso) ou 1 (sucesso com restrições), devem ser verificados os próximos itens;
b. Comparar se o hash presente no carimbo do tempo é igual ao da requisição (TSQ) que foi enviada para a ACT;
c. Comparar se o OID do algoritmo de hash no carimbo do tempo é igual ao da requisição (TSQ) que foi enviada para a ACT;
d. Comparar se o número de controle (valor do campo nonce) presente no carimbo do tempo é igual ao da requisição (TSQ) enviada para ACT;
e. Verificar a validade da assinatura digital do SCT que emitiu o carimbo do tempo;
f. Verificar se o certificado do SCT é válido e não está revogado;
g. Verificar se o certificado do SCT possui o uso adequado para este objetivo, isto é, o certificado deve possuir o valor id-kp-timeStamping com o OID definido pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [10].

4.4. Características do carimbo do tempo

a. a exatidão ou precisão mínima do tempo registrado no carimbo é de 500 ms;
b. o campo *genTime* será registrado até a unidade de microssegundos.

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Conforme item 5 da DPCT da ACT ARPEN.

6. CONTROLES TÉCNICOS DE SEGURANÇA

Conforme item 6 da DPCT da ACT ARPEN.

7. PERFIS DE CARIMBOS DO TEMPO

Conforme item 7 da DPCT da ACT ARPEN.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Conforme item 8 da DPCT da ACT ARPEN.

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

Conforme item 9 da DPCT da ACT ARPEN.

9.12. Alterações

9.12.1. Procedimento para emendas

9.12.1.1. Qualquer alteração nesta PCT deverá ser submetida à AC Raiz

9.12.2. Mecanismo de notificação e períodos

9.12.2.1. Mudança nesta PCT será publicada no site da ACT.

9.12.3. Circunstâncias na qual o OID deve ser alterado

Não se aplica.

10. DOCUMENTOS 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
[1]	VISÃO GERAL DO SISTEMA DE CARIMBO DO TEMPO NA ICP-BRASIL	DOC-ICP-11
[2]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-12
[3]	PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL	DOC-ICP-14
[2]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[5]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTOS DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[6]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[7]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[8]	POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06
[9]	REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL	DOC-ICP-10

11. REFERÊNCIAS

RFC 3161, IETF - Public Key Infrastructure Time Stamp Protocol (TSP), agosto de 2001.
RFC 3628, IETF - Policy Requirements for Time Stamping Authorities, November 2003.
RFC 3647, IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, november 2003.
ETSI TS 101.861 - v 1.2.1 Technical Specification / Time Stamping Profile, março de 2002.