IMPRENSA OFICIAL DO ESTADO SA IMESP
(ACT IMPRENSA OFICIAL)

POLÍTICA DE CARIMBO DO TEMPO

VERSÃO 1.0 –29/08/2019

Histórico de Versões

Data	*Versão*	*Observações*
29/08/2019	1.0	Redação Inicial

Conteúdo

SIGLAS

AC - Autoridade Certificadora
AC RAIZ - Autoridade Certificadora Raiz da ICP-Brasil ACT - Autoridade de Carimbo do tempo
BIPM - Bureau International des Poids et Mesures CT - Carimbo do tempo
DPCT - Declaração de Práticas de Carimbo do tempo EAT - Entidade de Auditoria do Tempo
FCT - Fonte Confiável do Tempo
HLB - Hora Legal do Brasil
ICP-Brasil - Infraestrutura de Chaves Públicas Brasileira
IETF - Internet Engineering Task Force
ISO – International Organization for Standardization NTP - Network Time Protocol
OID - Object Identifier
ON - Observatório Nacional
PC - Políticas de Certificado
PCT - Política de Carimbo do tempo
PS - Política de Segurança
PSS - Prestadores de Serviço de Suporte
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
TSP - Time Stamp Protocol
TSQ - Requisição de Carimbo do tempo (Timestamp-query – request)
TSR – Carimbo do tempo (Timestamp response)
UTC - Tempo Universal Coordenado

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Este documento descreve a Política de Carimbo do Tempo da Autoridade de Carimbo do Tempo da IMPRENSA OFICIAL - ACT IMPRENSA OFICIAL utilizada para regulamentar a geração e uso de carimbos do tempo no âmbito da ACT IMPRENSA OFICIAL. Ainda são observados os seguintes documentos:

a. VISÃO GERAL DO SISTEMA DE CARIMBO DO TEMPO NA IC P-BRASIL [1];
b. REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP- BRASIL [2];
c. REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBODO TEMPO NA ICP-BRASIL [11];
d. PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL [3].

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 IMPRENSA OFICIAL 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 IMPRENSA OFICIAL, 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];
b. CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5];
c. CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6];

d. CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [7];
e. POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [8];
f. REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL [9].

1.2. Identificação

1.2.1. A Política de Carimbo do Tempo da Autoridade de Carimbo do Tempo IMPRENSA OFICIAL, a seguir designada simplesmente PCT ACT IMPRENSA OFICIAL, é identificada pelo OID (Object Identifier) 2.16.76.1.6.10.

1.2.2. Os carimbos do tempo emitidos pela ACT IMPRENSA OFICIAL, segundo esta PCT, seguem os procedimentos descritos na DECLARAÇÃO DE PRÁTICAS D E CARIMBO DO TEMPO DA AUTORIDADE DE CARIMBO DO TEMPO IMPRENSA OFICIAL (DPCT da ACT IMPRENSA OFICIAL), cujo OID dessa DPCT é 2.16.76.1.5.10.

1.3. Declaração de conformidade

Todos os procedimentos usados pela ACT IMPRENSA OFICIAL para emissão dos carimbos do tempo descritos nesta PCT encontram-se em conformidade com as práticas declaradas na DPCT da ACT IMPRENSA OFICIAL.

1.4. Características do carimbo do tempo

Os carimbos do tempo emitidos segundo esta PCT implementam a versão 1 do padrão X.509, de acordo com perfil estabelecido na RFC 3161. Apresentam as seguintes características:

1 O campo accuracy apresenta a precisão do tempo presente no campo genTime do carimbo do tempo. A precisão mínima é determinada pelo Sistema de Auditoria e Sincronismo (SAS) que realiza periodicamente a auditoria e sincronismo dos relógios dos SCT desta ACT;
2 O campo genTime é representado até a unidade de microssegundos;
3 O campo policy indica o OID da política do SCT utilizada na geração do carimbo do tempo;
4 O campo ordering marcado como falso;
5 O campo nonce apresenta um valor que permite verificar se a resposta do SCT corresponde à requisição que foi enviada;
6 O campo serialNumber possui um número sequencial e único gerado para cada carimbo do tempo emitido por um SCT;
7 O campo messageImprint possui o hash do conteúdo carimbado;
8 O campo version apresenta a versão do timestamp token utilizado. O valor para este campo é 1;
9 O campo tsa apresenta os valores do Distinguished Name do certificado digital que assina os carimbos do tempo.

1.5. Comunidade e Aplicabilidade

1.5.1. Subscritores

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

1.5.2. Aplicabilidade

a. Os carimbos do tempo emitidos pela ACT IMPRENSA OFICIAL 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 IMPRENSA OFICIAL, depois de consultada a LCR, 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.

1.6. Dados de Contato

Imprensa Oficial do Estado SA IMESP.
Rua da Mooca, 1921 – Mooca – São Paulo, SP
Telefone: (55 11) 0800 0123401
Fax: (55 11) 2799 9887
Nome: Certificação Digital
Telefone: (55 11) 2799 9800
Email: certificacao@imprensaoficial.com.br

2. REQUISITOS OPERACIONAIS

2.1. Solicitação de Carimbos do Tempo

Neste item da PCT estão descritos todos os requisitos e procedimentos operacionais estabelecidos pela ACT IMPRENSA OFICIAL 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. Para solicitações utilizando o protocolo TCP, a requisição de carimbo do tempo TSQ (Time Stamp Request) deverá estar assinada pelo certificado do subscritor utilizando o padrão de assinatura CMS definido na RFC 3852;
c. O Servidor de Aplicativos da ACT IMPRENSA OFICIAL 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 credencias de acesso do subscritor.
e. O Servidor de Aplicativos da ACT IMPRENSA OFICIAL 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.

2.2. Aceitação de Carimbos do Tempo

Os requisitos e procedimentos operacionais estabelecidos pela ACT IMPRENSA OFICIAL 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 esteja presente, isto é, o status esteja 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].

2.3. Disponibilidade dos Serviços de Carimbo do Tempo

Os serviços de carimbo do tempo prestados pela ACT IMPRENSA OFICIAL serão oferecidos, no mínimo, 99,5% (noventa e nove e cinco décimos percentuais) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

3. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

Os itens seguintes definem como será mantida e administrada a PCT.

3.1. Procedimentos de mudança de especificação

Alterações nesta PCT podem ser solicitadas e/ou definidas pelos Gestores da ACT IMPRENSA OFICIAL, as quais deverão estar em conformidade com este documento e compatível com a DPCT da ACT IMPRENSA OFICIAL. A aprovação e a consequente adoção de nova versão estarão sujeitas à autorização da AC Raiz. Como parte desse processo, além da conformidade com este documento, deverá ser verificada a compatibilidade entre a PCT e a DPCT da ACT IMPRENSA OFICIAL.

3.2. Políticas de publicação e notificação

A ACT IMPRENSA OFICIAL mantém a versão corrente desta PCT para consulta pública, a qual está disponível no endereço **https://certificadodigital.imprensaoficial.com.br/repositorio/**.

3.3. Procedimentos de aprovação

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

4. 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
[10]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTICADOS NA ICP-BRASIL	DOC-ICP-04
[11]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL	DOC-ICP-13

5. REFERÊNCIAS

BRASIL, Lei nº 2.784, de 18 de junho de 1913 – determina a Hora Legal no Brasil.
BRASIL, Decreto nº 10.546, de 05 de novembro de 1918 – aprova o Regulamento da Lei nº 2.784. BRASIL, Decreto nº 4.264, de 10 de junho de 2002 – Restabelece e Modifica o Regulamento anterior.
BRASIL, Lei nº 9.933, de 20 de dezembro de 1999 – Dispõe sobre o Conselho Nacional de Metrologia, Normalização e Qualidade Industrial (CONMETRO) e sobre o Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (INMETRO).
RFC 1305, IETF – Network Time Protocol version 3.0.
RFC 2030, IETF – Simple Network Time Protocol (SNTP) version 4.0.
RFC 2527, IETF – Internet X-509 Public Key Infrastructure Certificate Policy and Certifications Practices Frame work, março de 1999.
RFC 3161, IETF – Public Key Infrastructure Time Stamp Protocol (TSP), agosto de 2001. RFC 3628, IETF – Policy Requirements for Time Stamping Authorities, November 2003. ETSI TS 101.861 – v 1.2.1 Technical Specification / Time Stamping Profile, março de 2002.
ETSI TS 102.023 – v 1.1.1 Technical Specification / Policy Requirements for Time Stamping Authorities, abril de 2002.