Infraestrutura de Chaves Públicas Brasileira

REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO DA ICP-BRASIL

DOC-ICP-13

versão 1.1

13 de outubro de 2009

Infraestrutura de Chaves Públicas Brasileira

Sumário

CONTROLE DE ALTERAÇÕES

Resolução ou IN que aprovou alteração	*Item Alterado*	*Descrição da Alteração*
Resolução nº 69, de 13/10/2009	2.2; 2.2.1; 2.2.2; 2.2.3.	Aprova a versão 1.1 dos documentos que regulamentam a geração e uso de carimbo do tempo no âmbito da ICP-Brasil:
Resolução nº 69, de 28/11/2008		Aprova a versão 1.0 do documento Requisitos mínimos para as políticas de carimbo do tempo da ICP-Brasil.

LISTA DE SIGLAS e ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC-RAIZ	Autoridade Certificadora Raiz
ACT	Autoridade de Carimbo de Tempo
CG	Comitê-Gestor
DPCT	Declarações de Práticas de Carimbo do tempo
ETSI	*European Telecommunication Standard Institute*
HSM	*Hardware Security Module*
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IETF	*Internet Engineering Task Force*
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ITI	Instituto Nacional de Tecnologia da Informação
OID	*Internet Engineering Task Force*
PCT	Política de Carimbo de Tempo
RFC	*Request For Comments*

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Este documento faz parte de um conjunto de normativos criados para regulamentar a geração e 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];**
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 CARIMBO DO TEMPO NA ICP-BRASIL** - este documento;
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 de Carimbo 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 um ACT credenciada na ICP-Brasil. O subscritor e as terceiras partes devem consultar a Declaração de Práticas de Carimbo do Tempo (DPCT) da ACT 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. Toda PCT elaborada no âmbito da ICP-Brasil deve obrigatoriamente adotar a mesma estrutura empregada neste documento.
1.1.7. Aplicam-se ainda às entidades que compõem a estrutura de carimbo do tempo na ICP-Brasil, no que couberem, os regulamentos dispostos nos demais documentos da ICP-Brasil, entre os quais destacamos:

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. Neste item deve ser identificada a PCT e indicado o seu Object Identifier (OID). No âmbito da ICP-Brasil, um OID no formato 2.16.76.1.6.n será atribuído à PCT na conclusão do processo de credenciamento da ACT responsável.
1.2.2. Neste item deve ser identificada a DPCT que estabelece os procedimentos adotados pela ACT para emissão de carimbos do tempo emitidos segundo a PCT. Deve também ser indicado o seu OID, no formato 2.16.76.1.5.n, o qual será atribuído à DPCT na conclusão do processo de credenciamento da ACT responsável.

1.3. Declaração de conformidade

Neste item, a ACT deve declarar que todos os procedimentos usados para emissão dos carimbos do tempo descritos na PCT encontram-se em conformidade com as práticas declaradas em sua DPCT.

1.4. Características do carimbo do tempo

Neste item devem ser informadas as características dos carimbos do tempo que serão emitidos segundo a PCT, contendo, no mínimo:

a) a exatidão ou precisão mínima do tempo registrado no carimbo;
b) a unidade utilizada no campo *genTime* do carimbo do tempo (segundos, milissegundos ou microssegundos).

1.5. Comunidade e Aplicabilidade

1.5.1. Subscritores

Neste item devem ser caracterizadas as entidades - pessoas físicas ou jurídicas - que poderão solicitar carimbos do tempo emitidos segundo esta PCT.

1.5.2. Aplicabilidade

Este item da PCT deve relacionar as aplicações para as quais são adequados os carimbos emitidos pela ACT e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses carimbos.

1.6. Dados de Contato

Neste item devem ser incluídos nome, endereço e outras informações da ACT responsável pela PCT. Devem ser também informados o nome, os números de telefone e endereço eletrônico de uma pessoa para contato.

2. REQUISITOS OPERACIONAIS

2.1. Solicitação de Carimbos do Tempo

Neste item da PCT devem ser descritos todos os requisitos e procedimentos operacionais estabelecidos pela ACT responsável para as solicitações de emissão carimbo do tempo. Esses requisitos e procedimentos, que deverão ser atendidos e executados pelos subscritores, deverão compreender, no mínimo:

a) o protocolo de solicitação do carimbo do tempo (http, email, etc.);

b) os algoritmos de *hash* que poderão ser utilizados pelos subscritores para solicitação do carimbo.

2.2. Aceitação de Carimbos do Tempo

Neste item da PCT devem ser descritos todos os requisitos e procedimentos operacionais estabelecidos pela ACT responsável para verificação de um carimbo do tempo. Esses requisitos e procedimentos deverão compreender, no mínimo:

a) forma de conferência do carimbo tempo, pelo subscritor e pela terceira parte, inclusive após a expiração do certificado que o assinou;

b) algoritmo do *hash* inserido no carimbo do tempo.

2.3. Disponibilidade dos Serviços de Carimbo do Tempo

Neste item da PCT deve ser descrita a disponibilidade dos serviços de carimbo do tempo prestados pela ACT. Devem ser informados, pelo menos, os dias e horários em que a ACT responsável estará em operação para emitir carimbos do tempo segundo a PCT.

3. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

Os itens seguintes devem definir como será mantida e administrada a PCT.

3.1. Procedimentos de mudança de especificação

Neste item devem ser descritos a política e os procedimentos utilizados para realizar alterações na PCT. Qualquer alteração na PCT deverá ser submetida à aprovação 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 responsável.

3.2. Políticas de publicação e notificação

Neste item devem ser descritos os mecanismos empregados para a distribuição da PCT à comunidade envolvida.

3.3. Procedimentos de aprovação

Toda PCT deverá ser 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].

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
[4]	**POLÍTICA DE SEGURANÇA DA ICP-BRASIL**	DOC-ICP-02
[5]	**CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO 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

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.