Infra-Estrutura de Chaves Públicas Brasileira

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

DOC-ICP-13 - versão 1.0

01 de dezembro de 2008

Sumário

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 - Infra-Estrutura 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 faz parte de um conjunto de normativos criados para regulamentar a geração e uso de carimbos do tempo no âmbito da Infra-estrutura 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	DOC-ICP-09

	ENTIDADES INTEGRANTES DA ICP-BRASIL	
[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.

6. GLOSSÁRIO

Alvará - Documento eletrônico assinado digitalmente pela Entidade Auditora, através de um sistema de auditoria e sincronismo. Consiste em um certificado de atributo no qual estarão expressos os dados referentes ao sincronismo e o parecer do auditor sobre a exatidão do relógio da entidade auditada.
Autenticação e Sincronização de Relógio (ASR) - Atividade periodicamente realizada pela EAT que resulta na habilitação ou não de um SAS ou de um SCT para operar sincronizado com a hora UTC. Essas operações devem ser efetuadas por intermédio de um conjunto de protocolos que garantam que o resultado final seja isento de fraudes.
Autoridade Certificadora (AC) – Entidade que emite, renova ou revoga certificados digitais de outras ACs ou de titulares finais. Além disso, emite e publica LCR. Na estrutura de carimbo do tempo da ICP-Brasil, emite os certificados digitais usados nos equipamentos e sistemas das ACTs e das EAT.
Autoridade Certificadora Raiz da ICP-Brasil (AC Raiz) – Entidade que credencia, audita e fiscaliza as demais entidades da ICP-Brasil. Assina seu próprio certificado e os certificados das ACs imediatamente abaixo dela. É também a Entidade de Auditoria do tempo da Rede de Carimbo do tempo da ICP-Brasil
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.
Carimbo do tempo (CT) - Documento eletrônico emitido pela ACT, que serve como evidência de que uma informação digital existia numa determinada data e hora no passado.
Certificado de Atributo - Estrutura de dados contendo um conjunto de atributos (características e

informações) sobre a entidade final, que é assinada digitalmente com a chave privada da entidade que o emitiu. Pode possuir um período de validade, durante o qual os atributos incluídos no certificado são considerados válidos.
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.
Compensação (Offset) - Correção necessária no relógio local para fazer com que indique o mesmo tempo indicado pelo relógio de referência.
Declaração de Práticas de Carimbo do tempo (DPCT) - Declaração das práticas e dos procedimentos empregados pela ACT para emitir Carimbos do Tempo.
Encadeamento - Ato de associar um carimbo do tempo a outro.
Entidade de Auditoria do Tempo (EAT) - Entidade que realiza as atividades de autenticação e sincronismo de Servidores de Carimbo do tempo (SCT) ou Sistemas de Auditoria e Sincronismo (SAS) instalados nas ACTs. Na estrutura de carimbo do tempo da ICP-Brasil, a EAT é a AC Raiz, que possui Sistemas de Auditoria e Sincronismo (SAS) ligados diretamente ao relógio atômico.
Erro - Diferença de tempo medida entre os relógios de um SAS e de um SCT.
Erro Máximo Acumulado - Erro máximo que pode ser acumulado pelo relógio interno do SCT, entre duas ASRs.
Estabilidade - Capacidade de um oscilador em manter a mesma freqüência em um determinado intervalo de tempo.
Exatidão - Afastamento máximo tolerado entre o valor indicado por um sistema de medição e o valor verdadeiro do tempo.
Fonte Confiável do Tempo (FCT) - É a denominação dada a um relógio sincronizado a hora UTC.
Hardware Security Module (HSM) – É um dispositivo baseado em hardware que gera, guarda e protege chaves criptográficas, além de ter a capacidade de executar operações criptográficas, como assinatura digital.
Incerteza - Dispersão dos valores que podem ser atribuídos a um mensurando, como resultado de uma sincronização.
Observatório Nacional (ON) – Unidade de pesquisa do Ministério da Ciência e Tecnologia (MCT), integrante do Sistema Nacional de Metrologia (Sinmetro). O ON é o responsável legal pela geração, conservação e disseminação da Hora Legal do Brasil.
Política de Carimbo do tempo (PCT) - Conjunto de normas que indicam a aplicabilidade de um carimbo do tempo para uma determinada comunidade e/ou classe de aplicação com requisitos comuns de segurança.
Precisão - Ver Exatidão
Prestador de Serviços de Suporte (PSS) - Entidade contratada pela ACT para realizar todas ou parte das atividades previstas na sua Declaração de Práticas de Carimbo do tempo.
Rastreabilidade - Relacionamento do resultado de uma medição de sincronismo com um valor de referência previamente estabelecido como padrão. A rastreabilidade se evidencia por intermédio de uma seqüência contínua de medidas, devidamente registradas e armazenadas e permite a verificação, direta ou indiretamente, do relacionamento entre o tempo informado e a fonte confiável do tempo.
Rede de Carimbo do tempo da ICP-Brasil – Rede criada e mantida pela AC Raiz da ICP-Brasil, que se liga ao Observatório Nacional para obter a hora UTC e a dissemina às ACT credenciadas na ICP-Brasil.
Resolução (Resolution) - Menor diferença entre indicações de um dispositivo mostrador que pode ser significativamente percebida. A resolução de um relógio é o menor incremento de tempo que o mesmo pode indicar.
Retardo (Delay) - Tempo de propagação na Internet entre o SCT e o SAS.
Segundo de Transição (leap second) - Ajuste ao UTC por meio da subtração ou adição de um segundo no último segundo de um mês do UTC. A primeira escolha é o fim de dezembro e de junho, e a segunda escolha é o fim de março e de setembro.
Servidor de Aplicativos (SAP) – Sistema que realiza a interface entre o subscritor e o SCT. Encaminha as solicitações de carimbo do tempo ao SCT e em seguida devolve ao subscritor os carimbos do tempo ou mensagens de erros recebidas em resposta.

Servidor de Carimbo do tempo (SCT) - Dispositivo único constituído por hardware e software que gera os carimbos do tempo, sob o gerenciamento da ACT. Deve possuir um HSM contendo um relógio a partir do qual são emitidos os carimbos do tempo. Nesse HSM devem ser também realizadas as funções criptográficas de geração de chaves e assinaturas digitais.
Sincronização de Relógio - Processo pelo qual dois ou mais relógios passam a indicar o mesmo tempo.
Sistema de Auditoria e Sincronismo (SAS) - Sistema constituído por hardware e software que audita e sincroniza SCT ou outros SASs. Deve possuir um HSM com relógio interno para a sincronização e capacidade de processamento criptográfico, para geração de chaves e realização de assinaturas digitais.
Subscritor - 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.
Tempo Universal Coordenado (UTC) - Escala do tempo adotada como padrão do Tempo Oficial Internacional, utilizada pelo sistema de Metrologia Internacional, Convenção do Metro, determinada e disseminada pelo BIPM.
Terceira Parte (Relying Part) - Aquele que confia no teor, validade e aplicabilidade do carimbo do tempo produzido pela ACT.