Infra-Estrutura de Chaves Públicas Brasileira

PROCEDIMENTOS PARA AUDITORIA DO TEMPO

NA ICP-BRASIL

DOC-ICP-14 – 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
ITI - Instituto Nacional de Tecnologia da Informação
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. 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 [3];

d) PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL - este documento.

1.2. Um carimbo do tempo aplicado a um documento eletrônico é uma evidência que ele foi criado antes da data incluída no carimbo do tempo. Os carimbos do tempo são emitidos por terceiras partes confiáveis, as Autoridades de Carimbo do Tempo (ACTs), cujas operações devem ser devidamente documentadas e periodicamente auditadas pela AC-Raiz da ICP-Brasil.

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.

1.4. Os relógios dos Sistemas de Carimbo do Tempo (SCTs), utilizados pelas ACTs devem ser auditados e sincronizados pela AC Raiz, que é a Entidade de Auditoria do Tempo (EAT), no âmbito da ICP-Brasil. Este documento trata desse processo de auditoria, realizado pela AC Raiz em todos os SCTs que pertencem às ACTs credenciadas junto à ICP-Brasil.

1.5. Ele tem como base as normas da ICP-Brasil, as RFC 3628 e 3161, do IETF, e o documento TS 101861 do ETSI.

1.6. Aplicam-se ainda às ACTs da ICP-Brasil e a seus Prestadores de Serviço de Suporte (PSS), 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].

2. PROCESSO DE AUDITORIA E SINCRONISMO

2.1. Descrição Sumária do Processo

2.1.1. A auditoria do relógio do SCT consiste na sua avaliação periódica pela AC Raiz, para verificar se ele está sincronizado com a Fonte Confiável de Tempo (FCT), ou se se encontra

dentro de um erro máximo pré-definido. Caso não esteja, serão realizadas tentativas de re-sincronizar o relógio do SCT.
2.1.2. Somente serão considerados sincronizados os equipamentos diretamente monitorados pela AC Raiz que se mantenham dentro dos padrões de comportamento previamente estabelecidos pela Política de Carimbo do Tempo (PCT) da Autoridade de Carimbo do Tempo (ACT).
2.1.3. O resultado final do processo de auditoria e sincronismo é a emissão, pela AC Raiz, de um alvará que permite ao SCT continuar operando por mais um período de tempo, se seu relógio estiver dentro dos padrões pré-definidos, ou, caso contrário, de um alvará com prazo de validade igual a zero, o que significa que o SCT não poderá emitir carimbos de tempo até ter seu relógio novamente sincronizado com a FCT.
2.1.4. A AC Raiz audita e sincroniza os relógios dos SCTs através de equipamentos denominados Sistemas de Auditoria e Sincronismo (SAS). A comunicação entre os SASs e os SCTs deve ser feita através de um protocolo que prevê a autenticação mútua baseada em certificados digitais e o uso de protocolos para o sincronismo do relógio tal como o Network Time Protocol (NTP).
2.1.5. Adicionalmente, a AC Raiz tem acesso a uma interface de auditoria dos SCTs para verificação dos registros produzidos.

2.2. Procedimentos da AC Raiz

2.2.1 Nesta seção são apresentados os procedimentos realizados pela AC Raiz para a auditoria e sincronismo dos relógios dos SCTs.
2.2.2. A AC Raiz manterá um relógio atômico sincronizado com o relógio atômico do Observatório Nacional. Ao relógio atômico da AC Raiz se ligam os equipamentos SAS, que realizarão as atividades de auditoria e sincronismo dos SCTs das ACTs. 2.2.3 Para cada SCT auditado, a AC Raiz proverá os serviços da Rede de Carimbo do Tempo da ICP-Brasil por meio de pelo menos 2 (dois) SAS, instalados em locais diferentes.
2.2.4. A AC Raiz disponibilizará às ACTs cópia dos certificados digitais de seus SAS, para permitir a autenticação mútua SAS-SCT.
2.2.5. Após a colocação do SCT em operação, a AC Raiz deverá:

a) auditar periodicamente o relógio dos SCTs, em período tal que o erro máximo acumulado não ultrapasse o valor especificado na PCT correspondente;
b) emitir alvarás, respeitando o período descrito no item a), habilitando o funcionamento dos SCTs;
c) informar à ACT, através de mensagem eletrônica, o motivo da impossibilidade da emissão de um alvará para um SCT;
d) analisar e emitir relatórios dos registros de auditoria e sincronismo do relógio do SCT, usando os dados registrados no SAS;
e) pelo menos 2 (dois) dias úteis antes da expiração do certificado do SAS, providenciar novo certificado e disponibilizá-lo às ACTs.

2.3. Procedimentos das Autoridades de Carimbo do Tempo

2.3.1. Nesta seção são apresentados os procedimentos que devem ser realizados pela ACT para permitir a auditoria e o sincronismo dos relógios de seus SCTs.
2.3.2. Antes colocar em operação seus SCTs, a ACT deve:

a) solicitar os serviços da Rede de Carimbo do Tempo da ICP-Brasil para cada relógio de SCT que emita carimbos de tempo no âmbito da ICP-Brasil;

b) contratar o fornecimento dos meios de comunicação e dos equipamentos necessários para ligar seus SCTs à rede Rede de Carimbo do Tempo da ICP-Brasil;
c) contratar, para cada SCT, no mínimo duas linhas de comunicação, de fornecedores diferentes, cada uma delas conectando-se a equipamentos SAS distintos, instalados em locais a serem indicados pela AC-Raiz;
d) utilizar somente equipamentos homologados pela ICP-Brasil ou por entidades por ela autorizadas;
e) enviar à AC Raiz cópia dos certificados digitais de seus SCTs, para permitir a autenticação mútua SAS-SCT.

2.3.3. Após a colocação do SCT em operação, a ACT deverá:
a) utilizar, em seus SCTs, somente certificados digitais ICP-Brasil específicos para equipamentos de carimbo do tempo;
b) pelo menos 2 (dois) dias úteis antes da expiração do certificado do SCT, providenciar novo certificado e enviá-lo à AC Raiz.

2.4. Auditoria e Sincronismo

2.4.1. A AC Raiz, por intermédio dos seus SASs, deverá realizar auditorias automáticas nos relógios dos SCTs, verificando o seu correto funcionamento. No final dessas auditorias, o SCT recebe um alvará que autorizará ou não o seu funcionamento.
2.4.2. O intervalo entre auditorias será fixado pela AC Raiz, de forma que o erro máximo acumulado pelo relógio do SCT não ultrapasse o valor máximo estabelecido na PCT da ACT. Se a correção ou o atraso de rede ultrapassar esse valor, o SCT não receberá permissão para funcionar.

3. REQUISITOS OPERACIONAIS

Esta seção trata dos requisitos de segurança que devem ser observados para as redes de comunicação de dados das ACTs, do nível de exatidão e estabilidade do sincronismo oferecido pela Rede de Carimbo do Tempo da ICP-Brasil, bem como do conteúdo dos arquivos que serão gerados durante a auditoria.

3.1. Proteção da Rede da Autoridade de Carimbo do Tempo

3.1.1. A ACT deve implementar, na rede onde estão conectados seus SCTs, os requisitos de segurança descritos na sua DPCT.
3.1.2. Os relógios dos SCTs devem estar protegidos contra ataques, incluindo violações e imprecisões causadas por sinais elétricos ou sinais de rádio, evitando que sejam descalibrados e permitindo que qualquer modificação possa ser detectada.
3.1.3. O acesso via rede aos SCTs deverá ser permitido somente para os seguintes serviços:
a) pela AC Raiz, para o sincronismo e auditoria de relógio;
b) pela ACT, para a administração dos SCTs a partir de equipamento conectado por rede interna;
c) pelo subscritor, para a solicitação e recebimento de carimbos do tempo.

3.2. Arquivos Gerados nas Auditorias

As operações de autenticação mútua e sincronismo gerarão arquivos codificados em UTF-8 (ou ASCII) nos SASs e SCTs, contendo dados resultantes destas operações.

3.3.1. Dados Referentes à Autenticação Mútua

3.3.1.1. Os arquivos de registro do SAS devem conter no mínimo as seguintes informações:
a) data e hora de realização da autenticação;
b) endereço de rede do SAS;
c) endereço de rede do SCT;
d) identificação do certificado digital do SCT;
e) identificação do alvará;
f) mensagem de aviso ou de erro.

3.3.1.2. Os arquivos de registro do SCT devem conter as seguintes informações:
a) data e hora de realização da autenticação;
b) endereço de rede do SAS;
c) endereço de rede do SCT;
d) identificação do certificado digital do SAS;
e) identificação do alvará;
f) mensagem de aviso ou de erro.

3.3.2. Dados Referentes ao Sincronismo

Os arquivos de registro do SAS e do SCT devem conter no mínimo as seguintes informações:
a) data e hora de realização do sincronismo;
b) erro do relógio do SCT;
c) retardo;
d) endereço de rede do SAS;
e) endereço de rede do SCT.

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]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL	DOC-ICP-13
[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.

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 EATs.
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 SCTs, 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 (SCTs) 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 ACTs 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.