Infraestrutura de Chaves Públicas Brasileira

REDE DE CARIMBO DO TEMPO NA ICP-BRASIL - RECURSOS TÉCNICOS

DOC-ICP-11 .01

versão 1.0

08 de maio de 2020

Sumário

CONTROLE DE ALTERAÇÕES

Ato Que Aprovou A Alteração	Item Alterado	Descrição Da Alteração
Resolução Nº , de XX.06.2020		Aprova a versão 1.0 do documento Rede de Carimbo do Tempo na ICP-Brasil – Recursos Técnicos.

LISTA DE SIGLAS e ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC-RAIZ	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AS	Sistemas Autônomos
CT	Carimbo do Tempo
DPCT	Declarações de Práticas de Carimbo do tempo
EAT	Entidade de Auditoria do Tempo
ETSI	*European Telecommunication Standard Institute*
FCT	Fonte Confiável de Tempo
HSM	*Hardware Security Module*
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IETF	*Internet Engineering Task Force*
MCT	Ministério da Ciência e Tecnologia
LCR	Lista de Certificados Revogados
PSS	Prestadores de Serviço de Suporte
RFC	*Request For Comments*
SAS	Sistemas de Auditoria e Sincronismo
SCT	Sistema de Carimbo do Tempo
SINMETRO	Sistema Nacional de Metrologia
PCT	Política de Carimbo do Tempo
UTC	*Universal Time Coordinated*

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 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 - este documento;
b) REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP- BRASIL [1];

c) REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL [2];
d) PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL [3].

1.2. 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.

1.3. Este documento define recursos técnicos adotados para a Rede de Carimbo do Tempo da ICP-Brasil - RCT, como protocolos para sincronismo, auditoria e outros aspectos de segurança.

2. Sincronismo de Tempo

2.1. Os recursos usados para manter o sincronismo dos relógios dos equipamentos que compõem a Rede de Carimbo do tempo da ICP-Brasil são os seguintes:

a) o sincronismo entre a FCT e o SAS deve empregar o protocolo PTPv2.1 – IEEE 1588v2-2008, com uso de estampas de tempo produzidas pelo hardware das interfaces de rede (hardware timestamping);
b) o sincronismo dos relógios dos SCT com o SAS deve ocorrer permanentemente, em períodos variáveis definidos e iniciados por equipamentos da EAT, utilizando o protocolo PTPv2 – IEEE 1588v2-2008. A fim de prover autenticação de dados no protocolo PTP deve-se associá-lo ao subprotocolo NTS-KE - "NTS Key Establishment", parte do protocolo para segurança do tempo em redes para o protocolo NTP (Network Time Security for the Network Time Protocol), servindo para iniciar a troca de chaves criptográficas e outros dados de segurança, por meio do protocolo TLS, entre servidor (SAS) e o cliente (SCT);

2.2 Os SCT devem gerar Árvores de Encadeamento do Tempo, que é uma estrutura de encadeamento de carimbos do tempo e dados sincronismo empregando recursos criptográficos baseados em Árvores de Merkle;

2.2.1 O SCT, ao receber um novo alvará, inicia uma nova Árvore;

2.2.2 Cada Árvore, indexada por 1 (um) alvará, formará um bloco, o qual no mínimo conterá:
i) a data e hora de finalização do bloco (alvará expirado), sincronizados com o EAT da ICP-Brasil.
ii) o número sequencial do bloco (bloco gênese terá o número 0);
iii) quantos nós (transações) aconteceram no bloco;
iv) tamanho em bits do bloco;
v) a raíz de Merkle da árvore;
vi) o resumo criptográfico do bloco anterior;
vii) o resumo criptográfico do bloco atual, resultado das alíneas 'i' a 'vi''.

2.2.3 Os nós da Árvore de Encadeamento do Tempo deverão ser construídos da seguinte forma:

i) cada operação de sincronismo deverá ter seus dados de estampa de tempo no SCT (timestamp), desvio médio (offset) e atraso médio (delay), resumidos criptograficamente e registrados em 1 (um) nó da árvore;

ii) cada carimbo do tempo emitido pelo SCT deve ser resumido criptograficamente e registrado em 1 (um) nó da árvore;

iii) os registros acontecem sequencialmente e os nós devem ter um indexador, também sequencial, com a localização do mesmo na Árvore de Merkle.

2.2.4 O algoritmo de resumo criptográfico deve ser SHA-256, descrito no DOC-ICP-01.01.

2.3 Os dados usados para gerar os resumos criptográficos da Árvore deverão ser armazenados em registros de eventos (logs), juntamente com indexador de cada nó da árvore ao qual ele pertence;

2.4 Expirado o alvará, o bloco é finalizado e consolidado, além de ser disponibilizado em uma rede permissionada de consenso e autorização, encadeada com outros blocos.

3. Auditoria

3.1. O processo de auditoria realizado pelo SAS deve ser composto das seguintes etapas:

a) O SAS envia alvará ao SCT;

b) O SCT recebe alvará e inicia, com este alvará, nova Árvore de Encadeamento do Tempo;

c) O SAS solicita os dados usados para gerar os resumos criptográficos que compõe a árvore de encadeamento encerrada pelo SCT;

d) O SCT envia os dados ao SAS para análise;

e) A análise realizada em uma auditoria do SAS deve considerar a avaliação estatística dos dados de sincronismo obtidos dos SCT, como desvios e atrasos médios;

f) O resultado final do processo de auditoria é a emissão pela EAT, através do SAS, 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. Os principais atributos do alvará são: ano, mês, dia, hora, minuto, segundo, compensação e retardo.

3.2. O envio de dados de auditoria será realizado com uso do Protocolo Websocket (RFC 6455 e atualizações) encapsulado pelo Protocolo Transport Layer Security (TLS) v 1.3 ou posterior (RFC 8446 e atualizações).

3.3 Os SCT deverão dispor de recurso para envio dos blocos descritos no item 2.4 à bases de registros distribuídos e permissionados de blocos.

4. ASPECTOS DE SEGURANÇA

4.1. Aspectos Gerais de Segurança da Entidade de Auditoria do Tempo

A AC-Raiz da ICP-Brasil, como Entidade de Auditoria do Tempo, obriga-se a:

a) adotar medidas de segurança física, lógica e de pessoal compatíveis, no mínimo, com as estabelecidas para as Autoridades de Carimbo do Tempo da ICP-BRASIL;
b) utilizar, para as operações de auditoria e sincronismo da Rede de Carimbo do Tempo da ICP-Brasil, SASs que possuam HSM com capacidade de processamento criptográfico, para geração de chaves e realização de assinaturas digitais;
c) manter os relógios de seus SASs sincronizados com a FCT;
d) garantir que a emissão dos alvarás seja feita em conformidade com o tempo constante do relógio interno do SAS e que a assinatura digital do alvará seja realizada dentro do HSM;
e) manter seus SASs com disponibilidade mínima de 99% do tempo;
f) analisar e emitir relatórios dos registros de auditoria e sincronismo dos SASs;
g) utilizar, em seus SAS, somente certificados digitais ICP-Brasil para assinatura de alvarás;
h) identificar e registrar as ações que executar, conforme as normas, práticas e regras estabelecidas pelo Comitê Gestor da ICP-Brasil;
i) dispor no mínimo de duas linhas de comunicação com a Internet, providas por diferentes sistemas autônomos (AS).

5. REFERÊNCIAS

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.