Política de Carimbo do Tempo da Autoridade de Carimbo do Tempo Safeweb

PCT – ACT SAFEWEB

Versão 1.0

Dezembro 2014

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Responsável	Descrição	Item alterado	Versão	Data
Compliance	Versão Inicial		1.0	16/12/2014

1 INTRODUÇÃO

1.1 VISÃO GERAL

1.1.1 Este documento descreve a Política de Carimbo do Tempo (PCT) da Autoridade de Carimbo do Tempo da Safeweb (ACT SAFEWEB) utilizada para regulamentar a geração e uso de carimbos do tempo no âmbito da ACT SAFEWEB. Ainda, são observados os 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 [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 do tempo são emitidos por terceiras partes confiáveis, as chamadas 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 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 SAFEWEB 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 SAFEWEB, 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 Safeweb, a seguir designada simplesmente PCT da ACT SAFEWEB, é identificada pelo OID (*Object Identifier*) **2.16.76.1.6.4.**
1.2.2 Os carimbos do tempo emitidos pela ACT SAFEWEB, segundo esta PCT, seguem os procedimentos descritos na DECLARAÇÃO DE PRÁTICAS DE CARIMBO DO TEMPO DA AUTORIDADE DE CARIMBO DO TEMPO SAFEWEB (DPCT da ACT SAFEWEB), cujo OID dessa DPCT é **2.16.76.1.5.4.**

1.3 DECLARAÇÃO DE CONFORMIDADE

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

1.4 CARACTERÍSTICAS DO CARIMBO DO TEMPO

1.4.1 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:

a) 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;
b) O campo *genTime* é representado até a unidade de microssegundos.
c) O campo *policy* indica o OID da política do SCT utilizada na geração do carimbo do tempo;
d) O campo *ordering* marcado como falso;
e) O campo *nounce* apresenta um valor que permite verificar se a resposta do SCT corresponde à requisição que foi enviada;
f) O campo *serialNumbe*r possui um número seqüencial e único gerado para cada carimbo do tempo emitido por um SCT;

g) O campo *messageImprint* possui o *hash* do conteúdo carimbado;
h) O campo *version* apresenta a versão do *timestamp token* utilizado. O valor para este campo é 1;
i) 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 solicitação de carimbos do tempo pode ser realizada por pessoas registradas no domínio www.actsafeweb.com.br mantido pela SAFEWEB.

1.5.2 APLICABILIDADE

1.5.2.1 Os carimbos do tempo emitidos pela ACT SAFEWEB 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.
1.5.2.2 Uma assinatura digital com carimbo do tempo emitido pela ACT SAFEWEB, após 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.

1.5 DADOS DE CONTATO

1.6.1 Dados da Instituição responsável pela ACT SAFEWEB
Nome: SAFEWEB SEGURANÇA DA INFORMAÇÃO LTDA.
Endereço: Avenida Princesa Isabel, 828, Santana, Porto Alegre/RS CEP: 90.620-000

1.6.2 Unidade para Suporte
Nome: SAFEWEB SEGURANÇA DA INFORMAÇÃO LTDA.
Endereço: Avenida Princesa Isabel, 828, Santana. Porto Alegre/RS CEP: 90.620-000
Pessoa da contato: Luiz Carlos Zancanella Junior
Telefone: (51) 3018-0300
E-mail: compliance@safeweb.com.br / junior@safeweb.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 SAFEWEB 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 através do endereço http://192.168.253.4/ACT, disponível apenas na Intranet;
b) O protocolo TSP é disponibilizado utilizando como meio de transporte o protocolo HTTP com autenticação através do controlador de domínio da acsafeweb.com.br;
c) O algoritmo de hash que será utilizado pelos subscritores para solicitação do carimbo será o SHA256.

2.2 ACEITAÇÃO DE CARIMBOS DO TEMPO

Os requisitos e procedimentos operacionais estabelecidos pela ACT SAFEWEB 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 estiver presente, isto é, o *status* estiver 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 *nounce*) 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 SAFEWEB 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.

2 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 realizadas pela ACT SAFEWEB, as quais deverão estar em conformidade com este documento e compatíveis com a DPCT da ACT SAFEWEB. 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 SAFEWEB.

3.2 POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO

A ACT SAFEWEB mantém a versão corrente desta PCT para consulta pública, a qual está disposta no endereço www.actsafeweb.com.br.

3.3 PROCEDIMENTOS DE APROVAÇÃO

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

3 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]	VISAO GERAL DO SISTEMA DE CARIMBO DO TEMPO NA ICP-BRASIL	DOC-ICP-11
[2]	REQUISITOS MINIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-12
[3]	PROCEDIMENTO PARA AUDITORIA DO TEMPO NA ICP-BRASIL	DOC-ICP-14
[4]	POLITICA 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]	POLITICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06
[9]	REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO AMBITO DA ICP-BRASIL	DOC-ICP-10
[10]	REQUISITOS MINIMOS PARA AS POLITICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[11]	REQUISITOS MINIMOS PARA AS POLITICAS DE CARIMBO DE 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.

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	*Timestamp-Query- Request* – (Requisição de Carimbo do tempo)
TSR	*Timestamp response* – (Carimbo do tempo)
UTC	Tempo Universal Coordenado