COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO- PRODESP

(ACT PRODESP)

POLÍTICA DE CARIMBO DO TEMPO

VERSÃO 1.0 –05/11/2021

Histórico de Versões

Data	*Versão*	*Observações*
05/11/2021	1.0	Redação Inicial

AVISO LEGAL

Sumário

1. INTRODUÇÃO

1.1 Visão Geral

1.1.1. Este documento descreve a Política de Carimbo do Tempo da Autoridade de Carimbo do Tempo da PRODESP- ACT PRODESP utilizada para regulamentar a geração e uso de carimbos do tempo no âmbito da ACT PRODESP. Ainda são observados os seguintes documentos:

a) VISÃO GERAL DO SISTEMA DE CARIMBO DO TEMPO NA IC P-BRASIL [1], documento aprovado pela Resolução nº 58, de 28 de novembro de 2008;
b) REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP- BRASIL [2], documento aprovado pela Resolução nº 59, de 28 de novembro de 2008;
c) REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL [11] - este documento, aprovado pela Resolução nº 60, de 28 de novembro de 2008;
d) PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL [3], documento aprovado pela Resolução nº 61, de 28 de novembro de 2008.

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 Autoridades Certificadoras 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 (PCT) da ACT PRODESP 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. Esta PCT foi elaborada no âmbito da ICP-Brasil e adota a mesma estrutura baseada no documento Requisitos Mínimos para as Políticas de Carimbo do Tempo da ICP-Brasil – DOC-ICP 13.

1.1.7. Aplicam-se ainda à ACT PRODESP, no que couberem, os regulamentos dispostos nos demais documentos da ICP-Brasil, dentre os quais destacamos:

a) POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4], documento aprovado pela resolução nº 02, de 25 de setembro de 2001;

b) CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5], documento aprovado pela resolução nº 06, de 22 de novembro de 2001;
c) CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6], documento aprovado pela Resolução nº 24, de 29 de agosto de 2003;
d) CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [7], documento aprovado pela resolução nº 25, de 24 de outubro de 2003;
e) POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [8], documento aprovado pela Resolução nº 10, de 14 de fevereiro de 2002; e
f) REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICPBRASIL [9], documento aprovado pela Resolução nº 36, de 21 de outubro de 2004.

1.2. Identificação

1.2.1. A Política de Carimbo do Tempo da Autoridade de Carimbo do Tempo PRODESP, a seguir designada simplesmente PCT ACT PRODESP, é identificada pelo OID (Object Identifier) 2.16.76.1.6.10.

1.2.2. Os carimbos do tempo emitidos pela ACT PRODESP, segundo esta PCT, seguem os procedimentos descritos na DECLARAÇÃO DE PRÁTICAS DE CARIMBO DO TEMPO DA AUTORIDADE DE CARIMBO DO TEMPO PRODESP(PCT da ACT PRODESP), cujo OID é 2.16.76.1.5.10.

1.3. Participantes da ICP Brasil

1.3.1. Autoridade de Carimbo do Tempo

Nome: ACT PRODESP

1.3.2. Prestador de Serviço de Suporte

1.3.2.1 São também publicados em serviço de diretório e/ou em página web da AC PRODESP a relação de todos os Prestadores de Serviço de Suporte – PSS;

http://certificadodigital.prodesp.sp.gov.br/repositorio/ac/act-prodesp

1.3.2.2 PSS são entidades utilizadas pela ACT para desempenhar atividade descrita neste documento e se classificam em três categorias, conforme o tipo de atividade prestada:

a) disponibilização de infraestrutura física e lógica;
b) disponibilização de recursos humanos especializados;
c) disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.3.2.3 A ACT mantém as informações acima sempre atualizadas.

1.3.3. Subscritores

1.3.3.1 A solicitação de carimbos do tempo ocorre nos processos que demandam esse artefato e pode ser realizada por pessoas físicas e jurídicas.

1.3.4. Partes Confiáveis

1.3.4.1. Considera-se terceira parte aquela que confia no teor, validade e aplicabilidade do carimbo do tempo.

1.4. Usabilidade do Certificado

1.4.1 Os carimbos do tempo emitidos pela ACT PRODESP 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;

1.4.2 Uma assinatura eletrônica com carimbo do tempo emitido pela ACT PRODESP garante a irretratabilidade da sua geração, pois o carimbo do tempo serve como evidência de que a assinatura foi realizada na data e hora do carimbo do tempo.

1.5. Política de Administração

1.5.1. Organização administrativa do documento

Nome da ACT: ACT PRODESP

1.5.2. Contatos

Rua da Mooca, 1921 – Mooca – São Paulo, SP

Telefone: (55 11) 0800 0123401

Fax: (55 11) 2799 9887

Nome: Certificação Digital

Telefone: (55 11) 2799 9800

Email: certificacao@imprensaoficial.com.br

1.5.3. Pessoa responsável pela adequabilidade da PCT e PCT

Nome: Roseli Ramalho de Jesus Caccaos

Telefone: (55 11) 2799 9805

E-mail: certificacao@sp.gov.br

1.5.4. Procedimentos de aprovação da PCT

1.5.4.1. Esta PCT é aprovada pelo ITI.

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

1.6. Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
PCT	Declaração de Práticas de Carimbo do Tempo
ETSI	*European Telecommunication Standard Institute*
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IETF	*Internet Engineering Task Force*
OID	*Object Identifier*
PCT	Política de Carimbo do Tempo
PSS	Pretador de Serviço de Suporte
RFC	*Request For Comments*
SCT	Servidor de Carimbo do Tempo

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1. Publicação de informações da ACT

2.1.1. A disponibilidade das informações publicadas pela ACT PRODESPna página da Internet http://certificadodigital.prodesp.sp.gov.br/repositorio/ac/act-prodesp é de 99,5% (noventa e nove e cinco décimos percentuais) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.1.2 As seguintes informações, no mínimo, são publicadas pela ACT PRODESP em sua página de Internet:

a) os certificados dos SCTs que opera;
b) esta PCT;
c) a PCT PRODESP;
d) as condições gerais mediante as quais são prestados os serviços de carimbo do tempo;
e) a exatidão do carimbo do tempo com relação ao UTC;
f) algoritmos de hash que poderão ser usados pelos subscritores e o algoritmo de hash utilizado pela ACT PRODESP;
g) uma relação, regularmente atualizada, dos PSS vinculados.

2.2 Frequência de publicação

2.2.1 Os certificados dos SCT são publicados imediatamente após a sua emissão. As versões ou alterações desta PCT e da PCT são atualizadas na página de Internet da ACT PRODESP após aprovação da AC Raiz da ICP-Brasil.

2.3 Controle de Acesso aos Repositórios

2.3.1 Não há qualquer restrição ao acesso para consulta a esta PCT e à PCT implementada. São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos por pessoal não autorizado pela gestão da ACT PRODESP.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 Para solicitações de carimbo do tempo que utilizem o protocolo TCP a requisição de carimbo do tempo TSQ (Time Stamp Request) deverá estar assinada pela chave privada do certificado do subscritor utilizando o padrão de assinatura CMS definido na RFC 3852. Este procedimento é necessário para que o Servidor de Aplicativos identifique o subscritor e qual a sua modalidade de contabilidade.

3.1.1 O padrão de assinatura é CMS do tipo Attached.

3.1.2 Após a identificação do subscritor, o TSQ é extraído da assinatura e é utilizado para dar andamento na emissão do carimbo de tempo.

4.REQUISITOS OPERACIONAIS

4.1 Solicitação de Carimbos do Tempo

Neste item da PCT estão descritos todos os requisitos e procedimentos operacionais estabelecidos pela ACT PRODESP 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. As solicitações de carimbo do tempo serão realizadas através de sistema específico do subscritor ou através da integração de aplicações que utilizem assinatura digital de documentos;
b) Para solicitações utilizando o protocolo TCP, a requisição de carimbo do tempo TSQ (Time Stamp Request) deverá estar assinada pelo certificado do subscritor utilizando o padrão de assinatura CMS definido na RFC 3852;
c) O Servidor de Aplicativos da ACT PRODESP não aceitará as solicitações de emissão de carimbo do tempo cujo certificado do subscritor esteja expirado ou revogado;
d) Para solicitações utilizando os protocolos HTTP ou HTTPs, a requisição de carimbo do tempo (Time Stamp Request) deverá conter em seu cabeçalho as credencias de acesso do subscritor;
e) O Servidor de Aplicativos da ACT PRODESP disponibiliza o serviço de carimbo do tempo através dos protocolos TCP utilizando a porta 318, HTTP utilizando a porta 80 e HTTPs utilizando a porta 443, de acordo com a RFC 3161.

4.1.1 Quem pode submeter uma solicitação de carimbo do tempo.

4.1.1.1 A solicitação de carimbos do tempo poderá ser realizada por pessoa física ou jurídica que seja previamente cadastrada como usuário da ACT PRODESP e realize as solicitações de carimbo do tempo de forma remota conforme especificado na RFC3161. As requisições de carimbo do tempo deverão utilizar encapsulamento CMS utilizando certificado digital conforme recomendado na RFC-3161 item 2.4.1.

4.1.2 Processo de registro e responsabilidades

4.1.2.1 A ACT PRODESP responde pelos danos a que der causa.

4.2 Emissão de Carimbos do Tempo

4.2.1 Nos itens abaixo são descritos todos os requisitos e procedimentos operacionais referentes à emissão de um carimbo do tempo e o protocolo a ser implementado, entre aqueles definidos na RFC 3161.

4.2.2 Como princípio geral, a ACT PRODESP dispõe aos subscritores o acesso a um Servidor de Aplicativos (SA), encaminha as TSQs recebidas ao SCT e em seguida devolve ao subscritor os carimbos do tempo recebidos em resposta às TSQs.

4.2.2 O Servidor de Aplicativos se constitui de:

a) sistema instalado no próprio equipamento que realiza as funções de SCT;

b) sistema instalado em equipamento da ACT distinto do SCT;

c) Não se aplica;

d) uma combinação das soluções anteriores.

4.2.3 O fornecimento e o correto funcionamento do Servidor de Aplicativos são de responsabilidade da ACT PRODESP.

4.2.4 O Servidor de Aplicativos executa as seguintes tarefas:

a) identificar e validar, se necessário, o usuário que está acessando o sistema;

b) receber os hashes que serão carimbados;

c) enviar ao SCT os hashes que serão carimbados;

d) receber de volta os hashes devidamente carimbados;

e) conferir a assinatura digital do SCT;

f) conferir o hash recebido de volta do SCT com o hash enviado ao SCT;

g) devolver ao usuário o hash devidamente carimbado;

h) comutar automaticamente para o SCT reserva, em caso de pane no SCT principal;

i) emitir alarmes por e-mail aos responsáveis quando ocorrerem problemas de acesso aos SCTs.

4.2.5 O SCT, ao receber a TSQ, deve realizar a seguinte sequência:

a) Verifica se a requisição está de acordo com as especificações da norma RFC 3161. Caso esteja de acordo, realizar as demais operações a seguir descritas. Se a requisição estiver fora das especificações, o SCT responde de acordo com o item 2.4.2 da RFC 3161, com um valor de status diferente de 0 ou 1, e indicar no campo "PKIFailureInfo" qual foi a falha ocorrida sem emitir, neste caso, um carimbo do tempo e encerrando, sem executar as demais etapas;

b) produzir carimbos do tempo apenas para solicitações válidas;

c) usar uma fonte confiável de tempo;

d) incluir um valor de tempo confiável para cada carimbo do tempo;

e) incluir na resposta um identificador único para cada carimbo do tempo emitido;

f) incluir em cada carimbo do tempo um identificador da política sob a qual o carimbo do tempo foi criado;

g) somente carimbar o resumo criptográfico (rash) dos dados, e não os próprios dados;

h) verificar se o tamanho do rash recebido está de acordo com a função rash utilizada;

i) não examinar o rash que está sendo carimbado, de nenhuma forma, exceto para verificar seu comprimento, conforme item anterior;

j) nunca incluir no carimbo do tempo algum tipo de informação que possa identificar o requisitante do carimbo do tempo;

k) assinar cada carimbo do tempo com uma chave própria gerada exclusivamente para esse objetivo;

l) a inclusão de informações adicionais solicitadas pelo requerente deve ser feita nos campos de extensão suportados; caso não seja possível, responder com mensagem de erro;

m) encadear o carimbo do tempo atual com o anterior, caso a ACT tenha adotado o mecanismo de encadeamento.

4.3 Aceitação de Carimbos do Tempo

Os requisitos e procedimentos operacionais estabelecidos pela ACT PRODESP 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 esteja presente, isto é, o status esteja 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 nonce) 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].

4.4 Características do carimbo do tempo

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 nonce apresenta um valor que permite verificar se a resposta do SCT corresponde à requisição que foi enviada;
f) O campo serialNumber possui um número sequencial 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.

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Os itens abaixo relacionados estão descritos na DPCT da ACT PRODESP.

5.1 Segurança Física

5.1.1 Construção e localização das instalações da ACT

5.1.2 Acesso físico nas instalações da ACT

5.1.3 Energia e ar condicionado do ambiente de nível 3 da ACT

5.1.4 Exposição à água nas instalações de ACT

5.1.5 Prevenção e proteção contra incêndio nas instalações da ACT

5.1.6 Armazenamento de mídia nas instalações da ACT

5.1.7 Destruição de lixo nas instalações da ACT

5.1.8 Sala externa de arquivos (off-site) para ACT

5.2 Controles Procedimentais

5.2.1 Perfis qualificados

6. CONTROLES TECNICOS DE SEGURANÇA

Os itens abaixo relacionados estão descritos na DPCT da ACT PRODESP.

8.6 Comunicação dos resultados

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

Os itens abaixo relacionados estão descritos na DPCT da ACT PRODESP.

9.1 Tarifas de Serviço

9.1.1 Tarifas de emissão de carimbos do tempo

9.1.2 Tarifas de acesso ao carimbo do tempo

9.1.3 Tarifas de revogação ou de acesso à informação de status

9.1.4 Tarifas para outros serviços

9.1.5 Política de reembolso

9.2 Responsabilidade Financeira

9.2.1 Cobertura do seguro

9.3 Confidencialidade da informação do negócio

9.3.1 Escopo de informações confidenciais

9.3.2 Informações fora do escopo de informações confidenciais

9.3.3 Responsabilidade em proteger a informação confidencial

9.4 Privacidade da informação pessoal

9.4.1 Plano de privacidade

9.4.2 Tratamento de informação como privadas

9.4.3 Informações não consideradas privadas

9.4.4 Responsabilidade para proteger a informação privadas

9.4.5 Aviso e consentimento para usar informações privadas

9.4.6 Divulgação em processo judicial ou administrativo

9.4.7 Outras circunstâncias de divulgação de informação

9.4.8 Informações a terceiros

9.5 Direitos de Propriedade Intelectual

9.6 Declarações e Garantias

9.6.1 Declarações e garantias das terceiras partes

9.7 Isenção de garantias

9.8 Limitações de responsabilidades

9.9 Indenizações

9.10 Prazo e Rescisão

9.10.1 Prazo

9.10.2 Término

9.10.3 Efeito da rescisão e sobrevivência

9.11 Avisos individuais e comunicações com os participantes

9.12 Alterações

9.12.1 Procedimento para emendas

9.12.2 Mecanismo de notificação e períodos

9.12.3 Circunstâncias na qual o OID deve ser alterado.

9.13 Solução de conflitos

9.14 Lei aplicável

9.15 Conformidade com a Lei aplicável

9.16 Disposições Diversas

9.16.1 Acordo completo

9.16.2 Cessão

9.16.3 Independência de disposições

10. 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 POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL	DOC-ICP-13
[3]	PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICPBRASIL	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 ICPBRASIL	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
[10]	PERFIL DO ALVARÁ DO CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP12.01
[11]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOCP-ICP-01.01

11. REFERÊNCIAS

RFC 3161, IETF - Public Key Infrastructure Time Stamp Protocol (TSP), agosto de 2001.

RFC 3628, IETF - Policy Requirements for Time Stamping Authorities, november 2003.

RFC 3647, IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, november 2003.

ETSI TS 101861 - v 1.2.1 Technical Specification / Time Stamping Profile, março de 2002.