POLÍTICA DE CARIMBO DO TEMPO DA

AUTORIDADE DE CARIMBO DO TEMPO QUICKSOFT

(PCT ACT QUICKSOFT)

Versão 2.1
Novembro/2022

Sumário

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item alterado	Descrição da alteração
1.0	Outubro/2014	-	Não há	Versão inicial
2.0	Outubro/2020	Resolução nº 173, de 17/08/2020	-	Revisão e consolidação do DOC-ICP-13, conforme Decreto nº 10.139, de 28 de novembro de 2019. Adequação da estrutura do documento à RFC 3647.
2.1	Novembro/2022		1.5	Alteração de endereço

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Este documento faz parte de um conjunto de normativos criados para regulamentar a geração e o 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 [1], documento aprovado pela Resolução nº 58, de 28 de novembro de 2008;
b. REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTIC AS 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 CARIMBODO 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 de 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 (DPCT) da ACT QUICKSOFT.

1.1.5. 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.

1.1.6. 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.

1.1.7. Este documento adota a mesma estrutura empregada em toda PCT elaborada no âmbito da ICP-Brasil.

1.1.8. Aplicam-se ainda à ACT QUICKSOFT, 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], 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], 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 ICP-BRASIL [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 QUICKSOFT, a seguir designada simplesmente PCT ACT QUICKSOFT, é identificada pelo OID (*Object Identifier*) 2.16.76.1.6.7.

1.2.2. Os carimbos do tempo emitidos pela ACT QUICKSOFT, segundo esta PCT, seguem os procedimentos descritos na DECLARAÇÃO DE PRÁTICAS D E CARIMBO DO TEMPO DA AUTORIDADE DE CARIMBO DO TEMPO QUICKSOFT (DPCT da ACT QUICKSOFT), cujo OID dessa DPCT é 2.16.76.1.5.7.

1.3. Participantes da ICP-Brasil

1.3.1. Autoridade de Carimbo do Tempo QUICKSOFT.

1.3.2. Prestador de Serviço de Suporte

1.3.2.1. A ACT QUICKSOFT mantém no endereço https://repositorio.bry.com.br/ a lista atualizada dos seus prestadores de serviço de suporte.

1.3.2.2. PSSs são entidades utilizadas pela ACT para desempenhar atividade descrita nesta PCT 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; ou

c. disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.3.2.3. A ACT QUICKSOFT 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 Carimbo do Tempo

1.4.1. Os carimbos do tempo emitidos pela ACT QUICKSOFT 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. Política de Administração

1.5.1. Organização administrativa do documento
Nome da ACT: Autoridade de Carimbo do Tempo QUICKSOFT.

1.5.2. Contatos
Unidade de Suporte
Nome: BRy Tecnologia SA
Endereço: Rua Lauro Linhares 2010 8º andar – Trindade – CEP: 88036-002 – Florianópolis/SC
Telefone: 48-3234-6696
E-mail: atendimento@bry.com.br

1.5.3. Pessoa responsável pela adequabilidade da DPCT e PCT
Nome: Carlos Francisco Tatara
Endereço: Rua Lauro Linhares 2010 8º andar – Trindade – CEP: 88036-002 – Florianópolis/SC
Telefone: 48-3234-6696
E-mail: tatara@bry.com.br

1.5.4. Procedimento de aprovação da PCT

1.5.4.1. Esta PCT foi submetida à aprovação, durante o processo de credenciamento da ACT QUICKSOFT, conforme o 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
ACT	Autoridade de Carimbo do Tempo
DPCT	Declarações 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 Identifiers*
PCT	Política de Carimbo do Tempo
PSS	Prestador 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

Conforme item 2.1 da DPCT da ACT QUICKSOFT.

2.2. Frequência de Publicação

Conforme item 2.2 da DPCT da ACT QUICKSOFT.

2.3. Controle de Acesso aos Repositórios

Conforme item 2.3 da DPCT da ACT QUICKSOFT.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Conforme item 3 da DPCT da ACT QUICKSOFT.

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 QUICKSOFT 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 QUICKSOFT 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 credenciais de acesso do subscritor;

e. O Servidor de Aplicativos da ACT QUICKSOFT 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;

f. Os subscritores deverão utilizar o algoritmo de *hash* SHA-256 para efetuar as solicitações de carimbo do tempo.

4.1.1. Quem pode submeter uma solicitação de carimbo do tempo

Conforme item 4.1.1 da DPCT da ACT QUICKSOFT.

4.1.2. Processo de registro e responsabilidades

Conforme item 4.1.2 da DPCT da ACT QUICKSOFT.

4.2. Emissão de Carimbos do Tempo

Conforme item 4.2 da DPCT da ACT QUICKSOFT.

4.3. Aceitação de Carimbos do Tempo

Os requisitos e procedimentos operacionais estabelecidos pela ACT QUICKSOFT 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 *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

a. a exatidão ou precisão mínima do tempo registrado no carimbo é de 500 ms;

b. o campo *genTime* será registrado até a unidade de microssegundos.

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Nos itens correspondentes à lista abaixo são ser referidos os itens correspondentes da DPCT da ACT QUICKSOFT ou detalhados aspectos específicos para a PCT, se houver.

6. CONTROLES TÉCNICOS DE SEGURANÇA

Conforme item 6 da DPCT da ACT QUICKSOFT.

7. PERFIS DE CARIMBOS DO TEMPO

Conforme item 7 da DPCT da ACT QUICKSOFT.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Nos itens correspondentes à lista abaixo são referidos os itens correspondentes da DPCT da ACT QUICKSOFT ou detalhados aspectos específicos para a PCT, se houver.

8.1. Frequência e circunstâncias das avaliações

8.2. Identificação/Qualificação do avaliador

8.3. Relação do avaliador com a entidade avaliada

8.4. Tópicos cobertos pela avaliação

8.5. Ações tomadas como resultado de uma deficiência

8.6. Comunicação dos resultados

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

Nos itens correspondentes à lista abaixo são referidos os itens correspondentes da DPCT da ACT QUICKSOFT ou detalhados aspectos específicos para a PCT, se houver.

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

9.13. Procedimentos de solução de disputa

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

9.12 Alterações

9.12.1 Procedimento para emendas

9.12.1.1. Qualquer alteração na PCT deverá ser submetida à aprovação da AC Raiz. Como parte desse processo, além da conformidade com este documento, será verificada a compatibilidade entre a PCT e a DPCT da ACT QUICKSOFT.

9.12.2 Mecanismo de notificação e períodos

9.12.2.1 A versão mais recente da PCT da ACT QUICKSOFT é disponibilizada em https://repositorio.bry.com.br/.

9.12.3 Circunstâncias na qual o OID deve ser alterado.

O OID da PCT da ACT QUICKSOFT será alterado pelo ITI em situações em que atualizações normativas ou tecnológicas afetem a compatibilidade entre os carimbos emitidos a partir das mudanças e os carimbos previamente emitidos.

10. DOCUMENTOS DA ICP-BRASIL

10.1. 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
[2]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[5]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTOS 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

11. REFERÊNCIAS

RFC 3161, IETF - *Public Key Infrastructure Time Stamp Protocol* (TSP), *August* 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 101.861 - v 1.2.1 *Technical Specification / Time Stamping Profile*, *March* 2002.