Infraestrutura de Chaves Públicas Brasileira

VISÃO GERAL DO SISTEMA DE CARIMBOS DO TEMPO NA ICP-BRASIL

DOC-ICP-11

versão 1.4

08 de maio de 2020

Infraestrutura de Chaves Públicas Brasileira

Sumário

CONTROLE DE ALTERAÇÕES

Ato Que Aprovou A Alteração	Item Alterado	Descrição Da Alteração
Resolução Nº 111, de 30.09.2015	2.1, 2.2.5, 2.4.2 e 5.	Aprova a Versão 1.3 do Documento Visão Geral do Sistema de Carimbos do Tempo na ICP-Brasil. com alteração da figura 1, exclusão do item 2.2.5 e 2.4.2, alínea b, e referências a Lei 2.784, de 18.06.1913, e Decreto 10.546, de 05.11.1918, da versão 1.2, e altera o item 2.4.2, alínea a.
Resolução Nº 78, de 31.03.2010	2.2.7: a, b, c, d, e.	Aprova A Versão 1.2 do Documento Visão Geral do Sistema de Carimbos do Tempo na ICP-Brasil.
Resolução Nº 69, de 13.10.2009	acrescenta-se a alínea “i”	Aprova a Versão 1.1 dos Documentos Que Regulamentam a Geração e Uso De Carimbo do Tempo no Âmbito da Infraestrutura de Chaves Públicas Brasileira ICP-Brasil.
Resolução Nº 58, de 28.11.2008		Aprova a versão 1.0 do documento Visão Geral do Sistema de Carimbos do Tempo na ICP-Brasil.

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. A criação desses documentos foi necessária porque as normas da ICP-Brasil até aqui existentes definiam regras para a criação e utilização de certificados digitais para permitir, entre outras aplicações, a assinatura digital de documentos eletrônicos, mas não regulamentavam o uso de mecanismos que permitissem determinar que uma informação digital existia num determinado instante do tempo no passado ou se uma assinatura digital foi aplicada antes da revogação ou expiração do certificado digital correspondente.

1.3. 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 de Carimbo do Tempo (ACTs), cujas operações devem ser devidamente documentadas e periodicamente auditadas pela própria AC-Raiz da ICP-Brasil. Os relógios dos SCTs devem ser auditados e sincronizados por Sistemas de Auditoria e Sincronismo (SASs).

1.4. 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.

1.5. 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.

1.6. Este documento define, exemplifica e explica o modelo adotado para a estrutura de carimbo do tempo da ICP-Brasil, estabelecendo quais são seus componentes e funções, bem como o motivo da adoção de cada um desses componentes.

1.7. Aplicam-se ainda às entidades que compõem a estrutura de carimbo do tempo na ICP-Brasil, no que couberem, os regulamentos dispostos nos demais documentos da ICP-Brasil, entre os quais destacam-se:

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]**.

1.8. Toda e qualquer organização que desejar filiar-se à ICP-Brasil como uma ACT deve implementar os ambientes, sistemas e procedimentos descritos nos documentos supracitados.

1.9 O ITI editará norma suplementar (DOC-ICP-11.01) com os recursos técnicos a serem observados na rede de carimbo de tempo da ICP-Brasil.

2. DESCRIÇÃO DO MODELO

2.1 Visão Esquemática do Modelo

O modelo geral de funcionamento está representado na Figura 1.

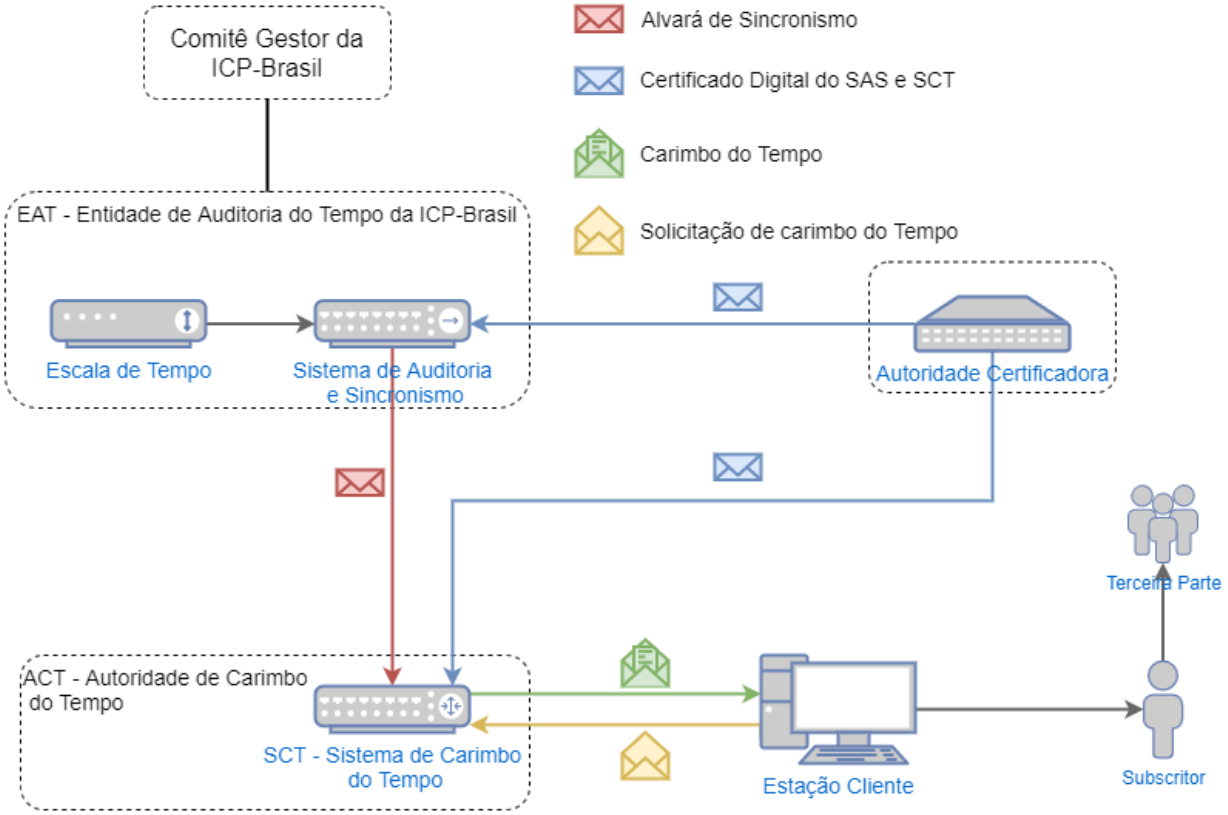

Figura 1 – Modelo de Funcionamento do Carimbo do Tempo da ICP-Brasil.

2.2. Entidades Integrantes e seu papel na estrutura

2.2.1. 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.

2.2.2. AC-Raiz da ICP-Brasil (AC-Raiz) – Credencia, audita e fiscaliza entidades da ICP-Brasil. Assina seu próprio certificado e os certificados das ACs imediatamente subordinadas. Atua também como Entidade de Auditoria do Tempo na Rede de Carimbo do Tempo ICP-Brasil.

2.2.3. Entidade de Auditoria do Tempo (EAT) – Faz a gestão da FCT, que mantém a escala de tempo da ICP-Brasil rastreável à escala de tempo UTC, bem como gere Sistemas de Auditoria e Sincronismo (SASs), para realizar as atividades de auditoria e sincronismo dos Servidores de Carimbo do tempo (SCTs), instalados nas ACTs.

2.2.4. Autoridade Certificadora (AC) - Emite, renova ou revoga certificados digitais de outras ACs ou de titulares finais. Emite e publica LCR. Na estrutura de carimbo do tempo da ICP-Brasil, emite os certificados digitais usados nos equipamentos das ACTs e da EAT e emite ainda os demais certificados utilizados nos processos relacionados aos carimbos do tempo.

2.2.5. 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. A ACT, mesmo utilizando-se de um PSS para executar suas atividades, é responsável pelos serviços por ele executados. Os PSSs classificam-se em três categorias, conforme o tipo de atividade prestada:

a) fornecedor de infraestrutura física e lógica;
b) fornecedor de recursos humanos especializados; ou
c) fornecedor de infraestrutura física, lógica e de recursos humanos especializados.

2.2.6. 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. Além disso, a ACT :

a) deve operar um ou mais Servidores de Carimbo do tempo (SCTs), conectados à Rede de Carimbo do tempo da ICP-Brasil, que geram carimbos em nome da ACT, utilizando um ou mais pares de chaves criptográficas específicas para essa finalidade;
b) deve manter disponível um serviço de páginas web onde é publicado, entre outras informações, sua Declaração de Práticas de Carimbo do Tempo (DPCT) e suas Políticas de Carimbo do Tempo (PCTs);
c) pode trabalhar com SCTs específicos, com características diferenciadas. Essas diferenças podem estar ligadas, por exemplo, aos algoritmos criptográficos utilizados, ao tamanho das chaves ou aos níveis de precisão de seu relógio. Um exemplo são as Autoridades de Carimbo do Tempo para Telecomunicações, que requerem um alto nível de precisão;

d) pode empregar PSS para fornecer partes dos serviços de carimbo do tempo. A ACT, no entanto, é a responsável e assegura que os requisitos identificados em sua PCT e DPCT sejam cumpridos. A chave ou as chaves privadas usadas para gerar o carimbo do tempo são identificadas como pertencendo à ACT responsável. Por exemplo, uma ACT pode subcontratar todos os componentes dos serviços, inclusive os serviços que geram o carimbo do tempo.

2.2.7. Subscritor ou Cliente - Pessoa física ou jurídica que solicita os serviços de uma Autoridade de Carimbo do Tempo implícita ou explicitamente concordando com os termos mediante os quais o serviço é oferecido.

2.2.8. Terceira Parte (Relying Part) - Aquele que confia no teor, validade e aplicabilidade do carimbo do tempo produzido pela ACT.

2.3. Credenciamento e manutenção de credenciamento das entidades na estrutura

2.3.1. A AC-Raiz da ICP-Brasil é a responsável pelo credenciamento das ACTs que desejam integrar a estrutura de carimbo do tempo da ICP-Brasil, com base em critérios estabelecidos nos documentos que regulamentam o assunto.

2.3.2. Uma vez credenciados, as ACTs podem solicitar às Autoridades Certificadoras da ICP-Brasil os certificados digitais para seus equipamentos.

2.3.3. Como forma de manter a segurança da estrutura, todas as entidades credenciadas devem obedecer à Política de Segurança da ICP-Brasil [4]. As ACTs e os PSSs são auditados previamente ao seu credenciamento e também anualmente, para verificar se os procedimentos operacionais e requisitos de segurança estabelecidos para essas entidades estão sendo cumpridos.

2.3.4. AC Raiz da ICP-Brasil pode, a qualquer momento, fiscalizar qualquer das entidades credenciadas.

2.4. Sincronismo e Auditoria do Tempo

2.4.1. A disseminação da escala de tempo da ICP-Brasil para as entidades que compõem a Rede de Carimbo do Tempo é realizada pela EAT, que utiliza mecanismos para garantir o sincronismo dos relógios dos equipamentos e a rastreabilidade do tempo informado .

2.4.2. Os recursos usados para auditoria e sincronismo dos relógios dos equipamentos que compõem a Rede de Carimbo do tempo da ICP-Brasil estão dispostos no DOC-ICP-11.01.

2.4.3. A garantia de que todos os equipamentos estejam sincronizados à hora UTC está baseada no fato de que os equipamentos que compõem a Rede de Carimbo do tempo da ICP-Brasil somente receberão os respectivos alvarás se estiverem adequadamente sincronizados

2.4.5. Os SASs e SCTs utilizam, para assinatura dos alvarás e carimbos do tempo e autenticação, chaves privadas vinculadas a certificados digitais ICP-Brasil, o que garante a autoria desses documentos.

2.6. Obtenção de um Carimbo do Tempo

2.6.1. Há duas formas de solicitar um carimbo do tempo na ICP-Brasil: solicitação presencial e solicitação remota. Caberá à ACT definir qual(is) dessas formas estará(ão) disponível(is) aos subscritores.

2.6.1.1. A solicitação presencial ocorre quando um subscritor dirige-se a uma ACT e entrega uma mídia contendo o arquivo ou o documento que deseja carimbar ao responsável pelo atendimento. Esse utiliza uma estação de trabalho, formata o pedido e o envia ao SCT. Recebe de volta o carimbo emitido, que é repassado ao subscritor.

2.6.1.2. A solicitação remota é feita a partir de um equipamento utilizando uma rede de comunicação de dados privada ou a Internet. O subscritor acessa a ACT, que dispõe de servidores atuando como interface de acesso ao SCT.

2.6.2. A ACT é responsável pela implementação, segurança e suporte desses servidores e pelo fornecimento e atualização dos aplicativos que sejam necessários para utilização do serviço.

2.6.3. O formato das solicitações e respostas de carimbo do tempo e os protocolos utilizados para o seu transporte devem atender ao disposto na RFC 3161.

2.6.4. Os procedimentos detalhados para solicitação e recebimento de carimbos do tempo devem constar nas Declarações de Práticas de Carimbo do Tempo da ACT.

2.7. Verificação de um carimbo do tempo

2.7.1. Tanto o subscritor que solicitou o carimbo do tempo, como a terceira parte, que irá receber o documento com esse carimbo, devem executar determinadas ações, antes de acreditar ou não na validade do carimbo. Como regras gerais devem ser verificadas: a identidade da ACT e do respectivo SCT; a validade dos certificados digitais; e o respeito à política sob a qual o carimbo foi emitido.

2.7.2. Os procedimentos detalhados para verificação de carimbos do tempo constam das Declarações de Práticas de Carimbo do Tempo e das Políticas de Carimbo do tempo (PCT), devem ser publicadas nos sítios de cada ACT.

2.8. Carimbos do tempo aceitos na ICP-Brasil

2.8.1. Cada ACT pode emitir carimbos do tempo para uso próprio ou por solicitação de terceiros, com base em diferentes Políticas de Carimbo do tempo que especificam o uso desses carimbos e a comunidade a que se aplicam.

2.8.2. Somente são aceitos na ICP-Brasil carimbos do tempo emitidos por SCT com alvarás fornecidos por Sistemas de Auditoria e Sincronismo.

3. ASPECTOS DE SEGURANÇA

3.1. Segurança da Autoridade de Carimbo do Tempo

3.1.1. Os requisitos de segurança e os procedimentos implementados nos ambientes das ACTs estão relacionados nos documentos citados na Seção 1 deste documento.

3.1.2. As características de segurança dos equipamentos que compõem a Rede de Carimbo do tempo da ICP-Brasil permitem o estabelecimento, para as ACTs, de ambientes físicos com requisitos menos rigorosos que os de uma Autoridade Certificadora da ICP-Brasil, dado que os SCTs:

a) somente podem operar sincronizados com a FCT;
b) utilizam HSM para geração de chaves criptográficas e assinatura de carimbos do tempo;
c) utilizam certificados digitais da ICP-Brasil com características específicas, o que traz a garantia de que o equipamento realmente pertence a uma ACT credenciada.

3.1.3. A ACT pode ainda utilizar mecanismos de segurança para determinar qual o último carimbo válido, caso ocorra comprometimento da chave privada do SCT. Entre esses mecanismos estão o encadeamento dos carimbos do tempo, o uso de trilhas de auditoria de todos os carimbos gerados pelo SCT ou ainda a emissão de carimbos do tempo por dois SCTs diferentes, para o mesmo documento.

3.2. Segurança da Entidade de Auditoria do Tempo

3.2.1. Aspectos Gerais da Entidade de Auditoria do Tempo da ICP-Brasil estão contidas no DOC-11.01.

3.2.2. Proteção da Rede de Carimbo do tempo da ICP-Brasil

3.2.2.1. A AC-Raiz implementa controles relativos à segurança de sua rede, observado o disposto na **POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]**.

3.2.2.2. Em especial, a AC-Raiz deve manter o segmento de rede que abriga os SASs protegidos contra acessos indevidos, de forma que apenas os serviços realmente necessários estejam disponíveis, entre os quais:

a) operações de sincronismo e auditoria dos SCTs;
b) administração dos SASs por pessoas autorizadas.

3.2.2.3. Todos os servidores e elementos de infraestrutura e proteção do segmento de rede que abriga os SASs, tais como roteadores, hubs, switches e firewalls devem:

a) operar em ambiente com segurança equivalente, no mínimo, ao nível 3 citado no documento **REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL [1]**
b) possuir acesso lógico restrito por meio de sistema de autenticação e autorização de acesso.

3.2.3. Proteção do Sistema de Auditoria e Sincronismo

3.2.3.1. A instalação e ativação dos HSM dos SASs devem ser feitas somente pelo pessoal formalmente designado, envolvendo mais de uma pessoa simultaneamente, em ambiente seguro.

3.2.3.2 Os relógios dos SASs devem ser sincronizados com a FCT, particularmente, deve-se garantir que:

a) os valores de tempo utilizados pelo SASs na emissão de alvarás sejam rastreáveis até a hora UTC;
b) o ajuste dos relógios dos SASs seja realizado de tal forma que não se afaste da precisão necessária para prover os parâmetros acordados com as ACTs;
c) os relógios dos SASs sejam 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;
d) a ocorrência de perda de sincronização seja detectada pelos controles do sistema;
e) o SAS deixe de emitir alvarás, caso seja constatado que seu relógio está fora da precisão estabelecida;
f) a sincronização dos relógios dos SASs seja realizada mesmo quando ocorrer a inserção de um segundo de transição (leap second).

4. DOCUMENTOS DA ICP-BRASIL

4.1. 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]	**REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS**	DOC-ICP-12

	DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	
[2]	**REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL**	DOC-ICP-13
[3]	**PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL**	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 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, 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.