

INSTRUÇÃO NORMATIVA ITI Nº 14, DE 11 DE NOVEMBRO DE 2020

Aprova a versão revisada e consolidada do documento Perfil do alvará do carimbo do tempo da ICP-Brasil DOC-ICP-12.01.

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe foram conferidas pelo inciso VI do art. 9º do anexo I do Decreto nº 8.985, de 8 de fevereiro de 2017, pelo art. 1º da Resolução nº 33 do Comitê Gestor da ICP-Brasil, de 21 de outubro de 2004, e pelo art. 2º da Resolução nº 163 do Comitê Gestor da ICP-Brasil, de 17 de abril de 2020,

CONSIDERANDO a determinação estabelecida pelo Decreto nº 10.139, de 28 de novembro de 2019, para revisão e consolidação dos atos normativos inferiores a decreto, editados por órgãos e entidades da administração pública federal direta, autárquica e fundacional,

RESOLVE:

Art. 1º Esta Instrução Normativa aprova a versão revisada e consolidada do documento Perfil do alvará do carimbo do tempo da ICP-Brasil DOC-ICP-12.01.

Art. 2º Fica aprovada a versão 2.0 do documento DOC-ICP-12.01 – Perfil do alvará do carimbo do tempo da ICP-Brasil, anexa a esta Instrução Normativa.

Art. 3º Esta Instrução Normativa entra em vigor em 1º de dezembro de 2020.

CARLOS ROBERTO FORTNER



ANEXO

Infraestrutura de Chaves Públicas Brasileira

**PERFIL DO ALVARÁ DO CARIMBO DO TEMPO
DA ICP-BRASIL**

DOC-ICP-12.01

Versão 2.0

11 de novembro de 2020



Infraestrutura de Chaves Públicas Brasileira

Sumário

CONTROLE DE ALTERAÇÕES.....	3
LISTA DE SIGLAS E ACRÔNIMOS.....	4
1. DEFINIÇÃO.....	5
2. LOCAL ADMITIDO.....	5
3. IDENTIFICAÇÃO E VALIDAÇÃO DO ALVARÁ.....	5
4. DOCUMENTOS DA ICP-BRASIL.....	7
5. REFERÊNCIAS.....	8



Infraestrutura de Chaves Públicas Brasileira

CONTROLE DE ALTERAÇÕES

Resolução ou IN que aprovou alteração	Item Alterado	Descrição da Alteração
Instrução Normativa ITI nº 14, de 11/11/2020 Versão 2.0		Revisão e consolidação, conforme Decreto nº 10.139, de 28 de novembro de 2019.
Resolução nº 155, de 03/12/2019 Versão 1.0		Aprova a versão 1.0 do Documento Perfil do Alvará do Carimbo do Tempo da ICP-Brasil.



Infraestrutura de Chaves Públicas Brasileira

LISTA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ASN.1	<i>Abstract Syntax Notation One</i>
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
MCT	Manual de Conduta Técnica
MSC	Módulo de Segurança Criptográfica
RFC	<i>Request For Comments</i>
SAS	Sistemas de Auditoria e Sincronismo
XML	<i>Extensible Markup Language</i>



Infraestrutura de Chaves Públicas Brasileira

1. DEFINIÇÃO

1.1 No contexto da infraestrutura de carimbo do tempo da ICP-Brasil um certificado de atributo digital também é conhecido como Alvará. Um alvará consiste de um objeto de dados que contém uma estrutura de campos que segue o formato definido pela RFC 5755, podendo ser codificado em formato ASN.1 ou XML.

1.2 Todo Alvará, antes de sua emissão, deve ser assinado digitalmente utilizando certificados digitais de equipamento por meio do MSC contido no SAS.

2. LOCAL ADMITIDO

2.1 O alvará, como limitador de autorização, tem seu uso admitido no TSTInfo, conforme previsto no MCT 10 da ICP-Brasil [3], e no *signingCertificate*, admitido pelas RFC 5035 e RFC 2634.

2.2 Quando presente no *signingCertificate* a validação do alvará deverá seguir, no mínimo, os procedimentos previstos no item 3.1.1. No TSTInfo essa validação não é obrigatória, sendo uma decisão do verificador realizá-la.

3. IDENTIFICAÇÃO E VALIDAÇÃO DO ALVARÁ

3.1 Os procedimentos descritos a seguir tem como objetivo identificar e validar o alvará quando estiver presente no *signingCertificate*, podendo ser utilizado para validação no TSTInfo.

3.1.1 Para identificar se um certificado de atributo, presente em um carimbo do tempo, é um alvará é necessário averiguar os seguintes fatores:

- a) O certificado de atributo tem o formato especificado no Manual de Condutas Técnicas (MCT) 10, Volume I [3];
- b) Checar a integridade da sua assinatura;



Infraestrutura de Chaves Públicas Brasileira

- c) O emissor deve ser um certificado considerado confiável para emissão de alvarás na ICP-Brasil;
- d) O alvará deverá estar válido no período do carimbo do tempo, conforme DOC-ICP 12 [1], item 9.6.1.2.c e atender ao procedimento de validação definido.

3.1.2 Recomenda-se, ainda, a validação completa do alvará, que pode ser feita acrescentando os itens abaixo, além daqueles descritos no item sobre validação de uma assinatura digital ICP-Brasil com referência de tempo, constante no DOC-ICP 15.01 [2], no processo de validação.

- a) O certificado do emissor do alvará não deve ser uma AC, ou seja, o valor de sua extensão *basicConstraints.cA* deve ser falso;
- b) O certificado do emissor precisa ter o bit de assinatura digital configurado como verdadeiro, ou 1, em sua extensão *keyUsage*;
- c) Validar o conteúdo do alvará conforme os requisitos V7 ao V14 e V17, do MCT 10, Volume I [3].



Infraestrutura de Chaves Públicas Brasileira

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 DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP- BRASIL Aprovado pela Resolução nº 59, de 28 de novembro de 2008	DOC-ICP-12

4.2 Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, 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 Instruções Normativas que os aprovaram.

<i>Ref.</i>	<i>Nome do documento</i>	<i>Código</i>
[2]	REQUISITOS PARA GERAÇÃO E VERIFICAÇÃO DE ASSINATURAS DIGITAIS NA ICP-BRASIL Aprovado pela Instrução Normativa nº 01, de 09 de janeiro de 2009	DOC-ICP-15.01
[3]	REQUISITOS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE CARIMBO DO TEMPO NO ÂMBITO DA ICP-BRASIL Aprovado pela Instrução Normativa nº 04, de 23 de abril de 2010	MCT10-VOLUME I E II



Infraestrutura de Chaves Públicas Brasileira

5. REFERÊNCIAS

RFC 5035, *Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility*, 2007.

RFC 5755, *An Internet Attribute Certificate Profile for Authorization*, 2010.

RFC 2634, *Enhanced Security Services for S/MIME*, 1999