Infraestrutura de Chaves Públicas Brasileira

PERFIL DO ALVARÁ DO CARIMBO DO TEMPO DA ICP-BRASIL

DOC-ICP-12.01

Versão 1.0

03 de dezembro de 2019

Sumário

CONTROLE DE ALTERAÇÕES

Resolução ou IN que aprovou alteração	*Item Alterado*	*Descrição da Alteração*
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.

LISTA DE SIGLAS e ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ASN.1	*Abstract Syntax Notation One*
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
MCT	Manual de Conduta Técnica
MSC	Módulos de Segurança Criptográfica
RFC	*Request For Comments*
SAS	Sistemas de Auditoria e Sincronismo
URL	*Uniform Resource Locator*
XML	*Extensible Markup Language*

1. Definição

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.

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

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

Quando presente no signingCertificate a validação do alvará deverá seguir, no mínimo, os procedimentos previstos no item 3.1. No TSTInfo essa validação não é obrigatória, sendo uma decisão do verificador realizá-la.

3. Identificação e Validação do Alvará

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

1. O certificado de atributo tem o formato especificado no Manual de Condutas Técnicas (MCT) 10, Volume I;
2. Checar a integridade da sua assinatura;

3. O emissor deve ser um certificado considerado confiável para emissão de alvarás na ICP-Brasil;
4. O alvará deverá estar válido no período do carimbo do tempo (ver DOC-ICP 12, item 2.1.3.3.c) e atender ao procedimento de validação definido no Perfil do Alvará do Carimbo do Tempo (anexo I).

3.2 Recomenda-se, ainda, a validação completa do alvará, que pode ser feita acrescentando os itens abaixo, além daqueles descritos no item 2.2.4.1, do DOC-ICP 15.01, no processo de validação.

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

4. REFERÊNCIAS

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

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