Florianópolis, 27 de Agosto de 2012

Aos(Às) Senhores(as) Conselheiros(as) do Comitê Gestor da ICP-Brasil

Prezados(as) Senhores(as), em relação ao quarto item da nossa última reunião do Comitê Gestor da ICP-Brasil, referente a regulamentação do Certificado de Atributo, gostaria de esclarecer nossa proposta:

a) Quanto a identificação do certificado de Pessoa Júridica da Entidade Emissora de Certificados de Atributos

Que a regulamentação aposte como fortemente **RECOMENDADO** o uso de certificados de pessoa jurídica exclusivos para o sistema de geração de certificados de atributos de uma entidade. Essa é uma boa prática de gestão de certificados digitais, e se seguida, pode facilitar o processo de auditoria dos sistemas emissores de atributos de uma Entidade Emissora de Atributos (EEA), principalmente se a mesma for uma entidade governamental ou uma empresa privada de médio e grande porte. O objetivo é que a chave privada da EEA seja mantido em hardware criptográfico, tal como um Módulo de Hardware Seguro (HSM), com um certificado emitido especialmente para esse fim. Assim, o sistema de gestão de certificados de atributos deveria usar somente essa chave para a geração de atributos, garantindo a rastreabilidade e facilitando os processos de auditoria por parte da entidade emissora de atributos ou auditores externos.

b) Quanto a criação de Identificadores de Atributos Padronizados (quando for conveniente)

Que seja fortemente **RECOMENDADO** que a entidades emissoras de certificados de atributos padronizem e identifiquem unicamente os seus atributos, principalmente aqueles de uso mais abrangentes, tais como o CPF e PIS. Isso pode ser feito através da atrbuição de um Identificador de Objeto (OID) para cada atributo. Sabe-se que campos em arquivos descritos na linguagem Abstract Sintaxe Notation 1 (ASN.1), o que é o caso de certificados digitais X.509, incluindo os certificados de atributos, podem conter duas entradas, um par, como em (oid, valor). Dessa forma, as aplicações que farão a leitura dos certificados de atributos reconhecerão o atributo a partir do OID e poderão processar a informação de forma correta. Além disso, isso garante também a interoperabilidade de sistemas, uma vez que sistemas diferentes, produzidos por empresas distintas, poderão transacionar com atributos de forma simples.

A entidade responsável por atribuir uma raiz de identificador de objetos para empresas públicas e privadas é a IANA (Internet Assigned Number Authority)[1]. O serviço é gratuito. Cabe a cada entidade registrada, organizar sua hierarquia de OIDs e publica-las da melhor forma possível.

Por exemplo, a raiz da UFSC é 7687

O atributo Número de Matrícula de um Aluno do UFSC é assim registrado.

(1.3.6.1.4.1.7687.1.1.1 , "8124148-0")

Qualquer aplicação, ao saber que o OID é 1.3.6.1.4.1.7687.1.1.1 saberá que o atributo "8124148-0" é o número de matrícula de um estudante da UFSC.

É claro que esse número de matrícula tem um significado, um codificação especial. O 81, por exemplo, significa que é um aluno que ingressou na UFSC em 1981. O algoritmo de "parser", ou seja, de análise do número de matrícula de alunos da UFSC, poderá ser invocado sempre que a aplicação detectar que se trata de um número de matrícula de um aluno da UFSC. Como o uso de OIDs isso fica fácil.

Atenciosamente

Prof. Ricardo Custódio
LabSEC/UFSC
Membro Representante da SBC

[1] www.iana.org