Infraestrutura de Chaves Públicas Brasileira

VISÃO GERAL SOBRE

CERTIFICADO DE ATRIBUTO

PARA A ICP-BRASIL

DOC-ICP-16

Versão 1.0

5 de julho de 2012

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Resolução que aprovou alteração	*Item Alterado*	*Descrição da Alteração*
Resolução Nº 93, de 5.7.2012 (Versão 1.0)	Novo	Criação do documento Visão Geral sobre Certificado de Atributo, versão 1.0 para a ICP-Brasil (DOC-ICP-16).

LISTA DE SIGLAS e ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AR	Autoridades de Registro
CA	Certificado de Atributo
CAA	Certificado de Atributo Autônomo
CAV	Certificado de Atributo Vinculado ao Certificado Digital
CD	Certificado de Atributo
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CPF	Cadastro de Pessoas Físicas
EEA	Entidade Emissora de Certificado de Atributo
GDE	Gestão de Documentos Eletronicos
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IANA	*Internet Assigned Number Authority*
IEC	*International Electotechinical Comission*
IETF	*Internet Engineering Task Force*
ISO	*International Organization for Standerdization*
ITU	*International Telecommunication Union*
LCR	Lista de Certificados Revogados
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
PJ	Pessoa Jurídica
RFC	*Request For Comments*
PJ	Pessoa Jurídica
RG	Registro Geral

1 INTRODUÇÃO

1.1 Este documento faz parte de um conjunto de normativos criados para regulamentar a adoção do Certificado de Atributos no âmbito da ICP-Brasil.

1.2 O certificado de atributo é, em suma, um documento eletrônico num formato específico, ou seja, no padrão ITU-T X.509 [1], assinado por certificado digital ICP-Brasil que permite agregar valor ao uso do certificado digital. Um certificado de atributo viabiliza o tratamento eletrônico de informações eletrônicas que requeiram a constatação jurídica de um fato.

1.3 O uso do certificado de atributo, de forma autônoma ou em conjunto ou diretamente vinculado ao certificado digital pode propiciar um maior fator de segurança para as aplicações, visto que agrega a possibilidade de verificação dos atributos de qualificação do titular do certificado digital. A responsabilidade para emissão de um certificado de atributos é da Entidade Emissora de Certificado de Atributo (EEA) que de fato possui o direito de qualificar o requerente do certificado. As qualificações são representadas por atributos que estão presentes em um certificado de atributos.

1.4 A premissa para que uma instituição, empresa ou entidade seja também uma EEA é que essa seja responsável pela gestão do ciclo de vida daqueles atributos e do respectivo certificado gerado a partir dos atributos escolhidos. Há inúmeros exemplos de atributos, assim como são inúmeras as entidades candidatas a emitirem certificados de atributos. A relação desta entidade com a ICP-Brasil se faz tão somente quando esta mesma entidade emissora assina o certificado de atributo com um certificado digital pertencente à cadeia de confiança da ICP-Brasil. O simples fato de assinar um certificado de atributos com um certificado digital padrão ICP-Brasil confere a esse todas as prerrogativas legais, já que um certificado de atributos é um documento eletrônico assinado num formato específico, neste caso no formato X.509.

1.5 Muito embora a geração e a consequente utilização de um certificado de atributos seja facultativa, a adoção sistemática desta tecnologia pode agregar inúmeras facilidades em termos de segurança e interoperabilidade na gestão de documentos eletrônicos (GDE) pela sociedade em geral, agregando não só a segurança técnica mas principalmente a segurança jurídica aos processos eletrônicos.

1.6 Além desta breve introdução sobre o tema, as demais seções estão organizadas da seguinte forma:

seção 2 - Motivações
seção 3 - Terminologia
seção 4 - Definições
seção 5 - Documentos sobre Certificado de Atributos para a ICP-Brasil
seção 6 - Gestão do Ciclo de Vida do Certificado de Atributo
seção 7 - Padrões de Certificado de Atributos
seção 8 - Referências Bibliográficas
seção 9 - Anexos

2 MOTIVAÇÕES

2.1 A ICP-Brasil instituiu uma infraestrutura de chaves públicas confiável, em âmbito nacional, cujo perfil dos certificados digitais contemplam em um único certificado, funções de identificação e qualificação de seu titular.

2.2 Em alguns casos, esta função de qualificação passa a ser múltipla em um mesmo certificado digital ocasionando incompatibilidade entre esses qualificadores, seja por descasamento de prazos de validade ou pela divergência entre autoridades responsáveis por esses qualificadores ou atributos. Adicionalmente, vários atributos uma vez inseridos no certificado digital passam a ser públicos, expondo informações pessoais e mesmo institucionais que noutras situações não seriam autorizadas ou ainda, seriam consideradas de cunho privado.

2.3 Em relação ao descasamento de prazo, a vigência de um certificado eventualmente se equipara à vigência do elemento identificador ou do(s) elemento(s) qualificador(es), ou até mesmo, entre os elementos qualificadores.

2.4 A questão quanto à vigência diz respeito à situação dos atributos incorporados ao certificado digital, que, posteriormente à sua emissão, podem expirar, ser suspensos, ou cancelados sem que isto reflita no uso desse certificado digital.

2.6 A implementação de certificado de atributo é simplificada tanto em sua infraestrutura quanto no seu conteúdo, que dispensa a existência de par de chaves.

2.7 Para propiciar a correção desses desvios e possibilitar larga utilização de certificado de atributos é necessário definir as diretrizes técnicas a serem adotadas para que os processos de geração e uso dos certificados de atributo sejam realizados de forma padronizada, responsável, interoperável e que atendam às necessidades do mercado, governo e da sociedade.

2.8 Nesse contexto, portanto, a criação do conjunto de normativos sobre certificado de atributo para a ICP-Brasil visa:

- auxiliar entidades na adoção de normas e condutas técnicas comuns que possam ser implementadas no processo de emissão e uso de certificado de atributo;
- consolidar e garantir a aplicação segura de certificados de atributo;
  promover a interoperabilidade entre sistemas que utilizam certificado de atributo para agilizar serviços e processos;
- uniformizar os esforços na definição dos requisitos técnicos de segurança e interoperabilidade para certificados de atributos e Entidade Emissora de Certificado de Atributo (EEA), possibilitando maior pragmatismo na implementação dos sistemas que utilizem certificado de atributo;
- promover a desmaterialização de processos;
- estabelece a competência técnica de entidades na utilização de certificados de atributos.

3 TERMINOLOGIA

3.1 Os termos abaixo, quando encontrados ao longo deste documento grafados em maiúsculas, DEVEM ser interpretados conforme descrito neste item:

3.1.1 DEVE (D) - Esta palavra, ou os termos "EXIGIDO" ou "OBRIGATÓRIO", significa que a definição é um requisito absoluto da especificação.

3.1.2 NÃO DEVE (ND) - Esta expressão, ou o termo "PROIBIDO¨ significa que a definição é uma proibição absoluta na especificação.

3.1.3 RECOMENDADO (R) - Esta expressão, ou o adjetivo "RECOMENDADO", significa que podem existir razões válidas, em circunstâncias particulares, para ignorar um ponto específico, mas as implicações completas precisam ser entendidas e ponderadas cuidadosamente antes de escolher um caminho diferente.

3.1.4 NÃO RECOMENDADO (NR) - Esta expressão significa que podem existir razões válidas, em circunstâncias particulares, em que o comportamento possa ser aceitável ou mesmo útil, mas as implicações completas devem ser entendidas e ponderadas cuidadosamente, antes de se realizar qualquer comportamento descrito com este rótulo.

3.1.5 PODE (P) - Esta palavra, ou o adjetivo "OPCIONAL", significa que é um item verdadeiramente opcional. Um implementador pode optar por incluir o item, enquanto outro pode omitir o mesmo item. Uma aplicação que não inclui uma determinada opção DEVE estar preparada para interoperar com outra aplicação que inclui aquela opção, embora talvez com funcionalidade reduzida. No mesmo espírito, uma aplicação que inclui uma determinada opção DEVE estar preparada para interoperar com outra aplicação que não a inclui (exceto, é claro, para o recurso que a opção oferece).

4 DEFINIÇÕES

4.1 Assinatura Digital ICP-Brasil é a assinatura eletrônica que:

a) esteja associada inequivocamente a um par de chaves criptográficas que permita identificar o signatário;
b) seja produzida por dispositivo seguro de criação de assinatura;
c) esteja vinculada ao documento eletrônico a que diz respeito, de tal modo que qualquer alteração subsequente neste seja plenamente detectável; e
d) esteja baseada em um certificado ICP-Brasil, válido à época da sua aposição.

4.2 Assinatura eletrônica é o conjunto de dados sob forma eletrônica, ligados ou logicamente associados a outros dados eletrônicos, utilizado como método de comprovação da autoria.

4.3. Atributo é aquilo que é próprio de alguém ou de algo. Na Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, é uma característica, sinal distintivo ou informação que acrescenta um sentido de qualidade ou qualificação associada a uma pessoa ou organização.

4.4 Certificado de Atributo (CA): é um documento eletrônico assinado no formato e na sintaxe

definida para um certificado padrão X.509 conforme orientações contidas na RFC5755 [2]. Possui estrutura similar ao Certificado Digital, exceto pelo fato de não conter a chave pública. O Certificado de Atributo contém qualificações atribuídas por uma EEA para uma pessoa, organização, aplicação ou equipamento. A entidade responsável pelos atributos contidos no certificado cria e assina o CA a partir de um certificado digital ICP-Brasil.

4.5 Certificado Digital (CD): Conjunto de dados de computador, gerados por uma Autoridade Certificadora, em observância à Recomendação Internacional ITU-T X.509, que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação.

4.6 Entidade Emissora de Certificado de Atributo (EEA): Instituição responsável pela emissão de Certificado de Atributo. É a entidade que detém prerrogativa legal na verificação e gestão do atributo conferido. Uma EEA para emitir um certificado de atributo deve dispor de um certificado digital padrão ICP-Brasil.

5 DOCUMENTOS SOBRE CERTIFICADO DE ATRIBUTOS PARA A ICP-BRASIL

Os normativos sobre Certificado de Atributo para a ICP-Brasil são listados na Tabela 5.1.

Código	Título	Conteúdo
DOC-ICP-16 (este documento)	Visão Geral sobre Certificados de Atributo para a ICP-Brasil	Define os principais conceitos e lista os demais documentos que compõem a visão da ICP-Brasil sobre o assunto.
DOC-ICP-16.01 [3]	Perfil de Uso Geral e Requisitos para Geração e Verificação de Certificados de Atributo na ICP-Brasil	Estabelece os requisitos obrigatórios a serem observados na criação e verificação de certificados de atributo para a ICP-Brasil.

Tabela 5.1: Organização dos documentos sobre Certificado de Atributo para a ICP-Brasil

6 GESTÃO DO CICLO DE VIDA DO CERTIFICADO DE ATRIBUTO

6.1 Entidades Envolvidas

6.1.1 A Entidade Emissora de Atributos – EEA é toda pessoa jurídica detentora da prerrogativa legal para emissão de determinado atributo e que emite Certificados de Atributo de acordo com as regras definidas neste documento (DOC-ICP-16) e demais documentos complementares mediante assinatura digital com um Certificado Digital ICP Brasil A3 ou A4 do tipo Pessoa-Jurídica.

6.1.2 Titular do Certificado de Atributo – é qualquer cidadão ou empresa titular ou não de um certificado digital, que passa a ser associado a um certificado de atributo emitido por uma EEA.

6.1.3 Autoridade Certificadora ICP-Brasil – é toda a instituição credenciada no âmbito da cadeia de confiança da ICP-Brasil capaz de emitir certificados digitais conforme políticas de certificados autorizadas.

6.1.4. Autoridade de Registro ICP-Brasil – Entidade responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC que tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC e identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota.

6.2 Do Certificado de Assinatura da EEA

6.2.1. Os certificados para assinatura de Certificados de Atributo serão de tipo Pessoa-Jurídica A3 ou A4.
6.2.2 É RECOMENDADO que a EEA reserve um determinado certificado de pessoa jurídica (PJ), preferencialmente do tipo A3 ou A4, para a finalidade de assinar certificados de atributos.
6.2.3. É RECOMENDADO que a EEA padronizem e identifiquem unicamente os seus atributos, principalmente aqueles de uso mais abrangentes, tais como o CPF e CNPJ. Isso pode ser feito através da atribuição de um Identificador de Objeto (OID) para cada atributo. Desta 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, garantirá 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*). O serviço é gratuito. Cabe a cada entidade registrada, organizar sua hierarquia de OIDs e publicá-las da melhor forma possível.

6.3 Tipos de vinculação de atributos em relação ao certificado digital

6.3.1 Vinculação direta: neste tipo de vinculação, as informações constantes do certificado de atributos fazem referência direta a um determinado certificado digital. Isso significa que toda vez que se fizer uso do certificado de atributos, o certificado digital deverá também estar presente ou acessível para verificação e validações dos dados.

6.3.2 Vinculação indireta: nesta vinculação, não há necessidade de verificação direta a um certificado digital. O simples fato de um certificado de atributos estar assinado por um certificado digital ICP-Brasil, e estar no prazo de validade, já constituem elementos suficientes para validação quanto a autenticidade e validade do certificado de atributos.

6.4 Tipos de Certificado de Atributos

6.4.1 Certificado de Atributos Autônomo (CAA) - este certificado tem como característica principal a possibilidade de ser emitido de forma independente da presença do titular. Não requer a necessidade de um certificado digital associado. O processo de emissão requer apenas que a EEA

seja a entidade gestora do atributo que será inserido no certificado de atributo assinado. Obviamente é necessário que o certificado de atributo guarde alguma relação direta ou referência com alguma informação relativa ao cidadão (RG, CPF, entre outros) ou a empresa (CNAE, CNPJ, entre outros). Como exemplo de potencial EEA para este tipo de certificado podemos citar as instituições públicas que emitem certidões e/ou declarações de forma "online" via Internet. Estas certidões ou declarações podem ser emitidas na forma de certificado de atributos. Entre os principais benefícios para estas instituições destacamos:

a) emissão de um documento eletrônico, neste caso uma certidão eletrônica, com valor probante;
b) a certidão eletrônica, na forma de um certificado de atributo, pode ser tratada (interpretada) eletronicamente, seja para aferir a autenticidade, seja ainda para dar a devido tratamento em um processo eletrônico;
c) interoperabilidade em operações eletrônicas seguras.

6.4.2 Certificado de Atributos Vinculado ao Certificado Digital (CAV) – este certificado se caracteriza por ter um vínculo direto com algum certificado digital ICP-Brasil previamente emitido. Isso garante maior segurança ao processo de autenticação e autorização associado ao uso da certificação digital. Enquanto o certificado digital permite a identificação de seu titular, o certificado de atributos qualifica este mesmo titular para um determinado ato. Para a emissão de um CAV, a EEA tem que necessariamente ter acesso ao certificado digital do titular para poder associar as informações constantes do certificado digital ao certificado de atributo a ser emitido. No caso de uma EEA, ser um banco, por exemplo, o certificado de atributo pode determinar acesso a determinadas operações diferenciadas além das operações permitidas para um cliente que tenha apenas um certificado digital.

6.5 Processo de emissão de Certificado de Atributo

6.5.1 O processo consiste basicamente em assinar um certificado de atributo por intermédio de um certificado digital.

6.5.2 Na Figura 1, do anexo I, observamos as principais etapas do processo de emissão do certificado de atributos, conforme descrito a seguir:

(1) a EEA, a partir de um banco de dados de sua propriedade, escolhe o conjunto de informações que irão fazer parte do certificado de atributos.
(2) a EEA, organiza os atributos que irão fazer parte do certificado de atributo no formato X.509, conforme orientações contidas no DOC-ICP-16.01 [3].
(3) a EEA, define se o certificado de atributo estará ou não associado, a um certificado digital. A vinculação pode ser direta ou indireta. No caso da vinculação direta, algumas das informações específicas do certificado digital (n.série, chave pública da AC, entre outras escolhidas) deverão ser necessariamente inseridas no certificado de atributo. Se a opção for por vinculação indireta ao certificado digital, haverá a necessidade de escolher um dos atributos (Nome, RG entre outros atributos de identificação) que façam alguma referência ao titular do certificado de atributos.
(3.1) caso a opção seja por vincular às informações específicas do certificado digital, há a necessidade ter essas informações previamente. O titular do certificado digital, o qual será o também o beneficiário do certificado de atributo deverá fornecer a EEA o certificado digital para registro das informações. A EEA de posse das informações sobre

o certificado digital e também das informações provenientes de seu banco de dados, providencia a assinatura do certificado no formato X.509.
(3.2) caso a opção seja por vincular de forma indireta a um certificado digital, a EEA deve apenas inserir os atributos escolhidos, e providenciar a assinatura do certificado de atributo do formato X.509.
(4) o certificado de atributos assinado deve ser então armazenado num repositório junto à EEA para futuras consultas via protocolo OCSP, e/ou ainda ser disponibilizado para armazenamento em mídia pertencente ao titular do certificado de atributos.

6.5.3 Na Figura 2, do Anexo I, temos as diferentes situações do processo de distribuição e uso do certificado de atributos para o titular do certificado.

(1) o certificado de atributos é armazenado num repositório da EEA;
(2) o titular do certificado de atributos interessado em armazenar o mesmo junto a mídia onde está o certificado digital, deve acessar o repositório da EEA, identificar-se com o certificado digital e solicitar da EEA o armazenamento na mídia correspondente;
(3) o certificado de atributos e o certificado digital são armazenados na mesma mídia (cartão ou token) e ficam disponíveis para uso pelo titular dos certificados;
(4) uma terceira parte autorizada que queira verificar a validade do certificado de atributo emitido pela EEA pode fazer um acesso ao repositório via protocolo OCSP.

6.6 Modelo de Emissão e Guarda de Certificados de Atributo

A EEA deve manter repositório de certificados de atributo, sua LCR ou OCSP, quando aplicável.

6.7 Responsabilidades e Obrigações da Entidade Emissora de Certificados de Atributo (EEA)

A EEA de um Certificado de Atributo deve observar as seguintes questões:

a) integridade e validade dos dados que farão parte do Certificado de Atributo;
b) assinatura digital do certificado digital por titular autorizado ou representante legal da entidade com poderes para tal;
c) reconhecimento e validação do titular do atributo
d) garantia quanto a integridade e autenticidade do atributo emitido

6.8 Verificação de Validade do Certificado de Atributo

Um certificado de atributos deve ser verificado com o uso de pelo menos uma prática a seguir quanto a validade:

1. Verificação via OCSP em repositório mantido pela EEA - Toda EEA deve manter um repositório de certificados de atributo emitidos de modo a permitir, sempre que necessário, a validação dos certificados por uma terceira parte interessada. No caso da revogação de um certificado de atributo, a informação deverá ser imediatamente atualizada no repositório. Esta recomendação aplica-se principalmente nos casos de certificados de atributo do tipo CAA.
2. Verificação por expiração do prazo de validade - Todo certificado de atributo deve ter o prazo de validade inserido de modo a permitir a validação pela própria aplicação que faz uso do certificado. Neste caso, não ha necessidade de consultar um repositório junto a EEA.

3. Verificação por consulta a LCR ou serviço OCSP, quando houver.

6.9 Verificação da Autenticidade do Certificado de Atributo

6.9.1. Um Certificado de Atributo é considerado válido quando atender a todos requisitos a seguir:

a) Validar a cadeia de certificação de confiança do certificado digital da EEA utilizado na assinatura do certificado de atributo.

b) o Certificado de Atributo não constar da LCR ou consulta OCSP da EEA emitente (quando aplicáveis);

c) o Certificado de Atributo não estiver expirado;

d) puder ser verificado com o uso de certificado digital válido da EEA emitente;

e) o Certificado Digital que o assinou não constar da LCR ou consulta OCSP da AC emitente.

6.9.2. Para validar o atributo vinculante é necessário realizar verificação da vinculação do certificado de atributo a um certificado digital, a partir da comparação direta dos atributos contidos em ambos os certificados.

7 PERFIL DE CERTIFICADO DE ATRIBUTO

Os certificados de atributo emitido pelas EEA deverão estar em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8 [4].

Todos os certificados emitidos pelas EEA deverão implementar a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5755.

8 ANEXOS

Anexo I – Figuras 1 e 2

BIBLIOGRAFIA

[1] ITU-T Rec. X.509 ISO/IEC 9594-8, The Directory: Public-key and attribute certificate framework, mar, 2000.
[2] FARREL, S. Et al. An Internet Attribute Certificate Profile for Authorization. IETF, 2010. RFC 5755 (Proposed Standard). (Request for Comments, 5755). Disponível em: <http://www.ietf.org/rfc/rfc5755.txt>.
[3] ITI. Perfil de Uso Geral e Requisitos para Geração e Verificação de Certificados de Atributo na ICP-Brasil. v.1.0. Brasília. DOC-ICP-16.01.
[4] ISO/IEC 9594-6: "Information technology; Open Systems Interconnection; The Directory: Selected attribute types".

ANEXO I

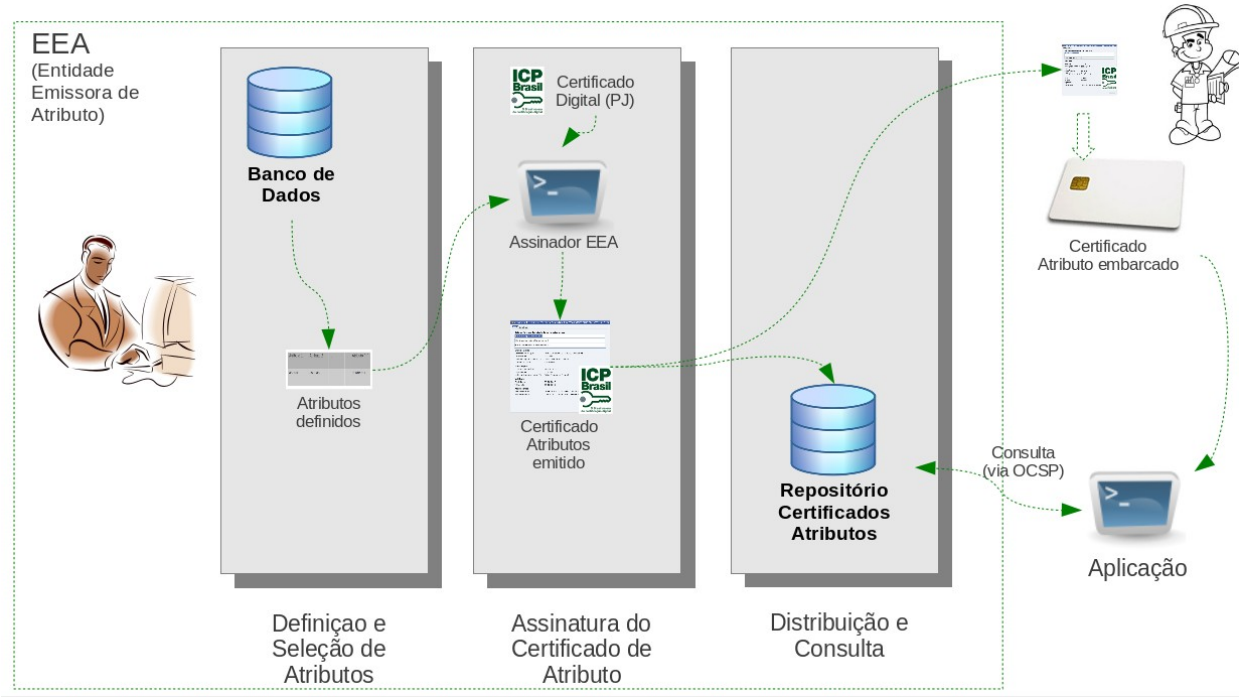

Figura 1 – Ciclo de vida do Certificado de Atributo

ANEXO I

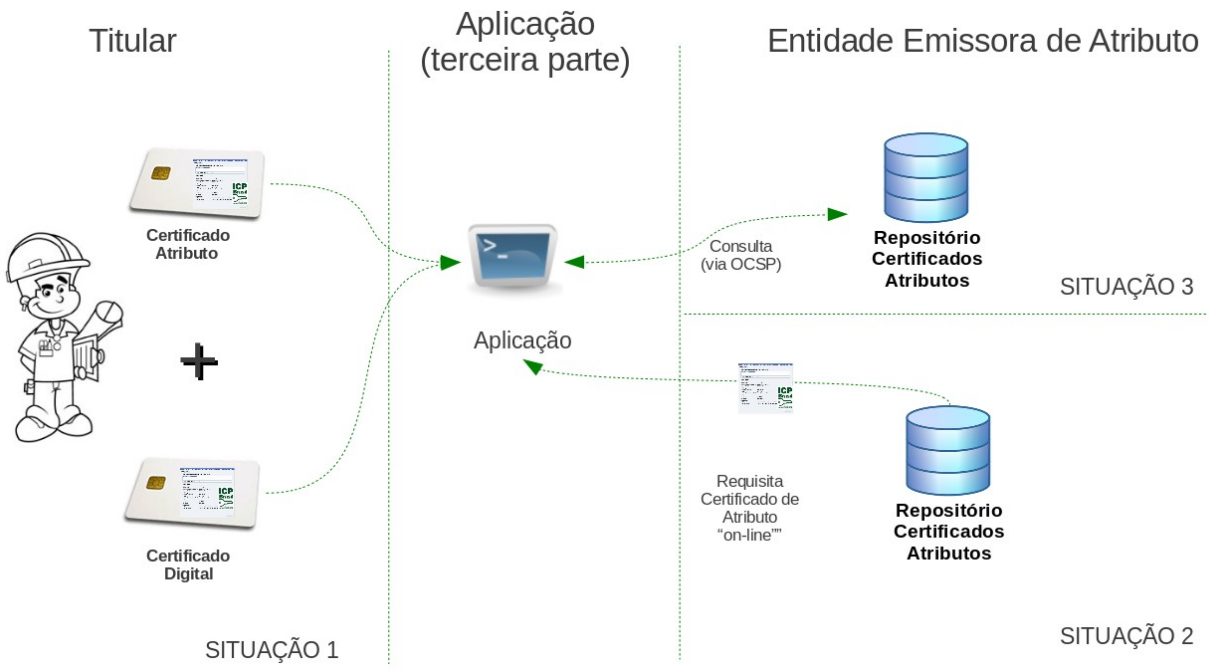

Figura 2 – Demonstração de distribuição e uso do Certificado de Atributo