

WHITE PAPER

# CERTIFICADO DE ATRIBUTO DIGITAL NA ICP-BRASIL



**Microsoft**<sup>®</sup>

## Conteúdo

1. Objetivo	2
2. Introdução	2
3. Certificado de Atributo Digital	3
4. Autoridade Certificadora de Atributo	3
5. Proposta de adequação do Certificado Digital da ICP-Brasil	4
6. Aplicação	5
7. Estudo de caso: Aplicação de fluxo de assinaturas	5
8. Conclusão	5
9. Trabalhos futuros	6
Bibliografia	6

## 1. Objetivo

O objetivo deste trabalho é analisar e propor modelos de uso do Certificado de Atributo Digital dentro das regras estabelecidas pela ICP-Brasil. Em linhas gerais, um Certificado de Atributo Digital é um documento eletrônico assinado digitalmente que apresenta qualidades associadas a uma pessoa ou organização identificada por meio de um Certificado Digital. A Serasa e a Microsoft realizaram um estudo de conceituação e aplicabilidade desta tecnologia e descrevem, neste trabalho, uma proposta de adequação das regras atuais de emissão de Certificados Digitais e a estruturação da emissão de Certificados de Atributo Digital para utilização no âmbito da ICP-Brasil.

## 2. Introdução

A ICP-Brasil – constituída pela MP 2200-2, em 2001 – estabeleceu, no Brasil, uma infra-estrutura de chaves públicas, centralizada em uma única raiz, com o propósito de emitir Certificados Digitais para assinatura digital e sigilo [ITI]. A disseminação do uso de Certificados Digitais é uma realidade devido às políticas governamentais e às iniciativas do setor privado. Este último, em particular, enxerga a

Certificação Digital como uma grande oportunidade para atender necessidades de segurança relacionadas à identificação e para acelerar processos de negócio, uma vez que as assinaturas digitais agilizam o trâmite de fechamento de transações entre partes.

Assim, são criados muitos sistemas de gerenciamento de assinaturas digitais, em que existem fluxos pré-definidos com segregação das partes. Esses sistemas devem analisar as assinaturas digitais e sua relação com o documento, ou seja, identificar se o documento admite uma assinatura digital de uma pessoa e qual o papel desta no processo. Toda essa arquitetura requer um conjunto de informações cadastrais sobre os signatários que deve ser obtido de outros sistemas. Geralmente, esses sistemas estão integrados por meio de tecnologias síncronas e assíncronas e estão sujeitos às intempéries operacionais inerentes a interdependência uns dos outros. Foi com base nesse cenário que estudamos o uso do Certificado de Atributo Digital e os principais desafios de sua implementação no contexto da ICP-Brasil.

Este trabalho está organizado da seguinte forma: Item 3 – Apresentação de uma breve conceituação de Certificado de Atributo Digital, sua estrutura aplicada às necessidades apresentadas no cenário acima e algumas sugestões para a sua normalização;

Item 4 – Introdução ao conceito da Autoridade Certificadora de Atributos (ACA) e sugestão de alguns pontos de reflexão na sua regulamentação pela ICP-Brasil;

Item 5 – Proposta de adequação da estrutura atual dos Certificados Digitais para que operem, adequadamente, com o conceito de Certificados de Atributo Digital;

Itens 6 e 7 – Apresentação das vantagens e dos desafios da utilização do Certificado de Atributo Digital em aplicações de assinatura digital;

Itens 8 e 9 – Conclusão e indicação de itens para os próximos estudos.

### 3. Certificado de Atributo Digital

O Certificado de Atributo Digital é um documento eletrônico assinado digitalmente que apresenta qualidades associadas a uma determinada entidade. Além dos atributos propriamente ditos, a temporalidade é outra característica importante, pois permite que uma informação seja confiável por um período de tempo pré-determinado [Network Working Group, 2002].

O Certificado de Atributo Digital, ao contrário do que o nome sugere, não possui todas as características de um Certificado Digital. Diferentemente do Certificado Digital, o Certificado de Atributo Digital não possui chave pública, embora alguns outros aspectos sejam semelhantes, como por exemplo:

- São assinados digitalmente por um Certificado Digital;
- Possuem um período de validade;
- Devem ser validados junto a uma Lista de Certificados Revogados (LCR).

Na sua essência, o Certificado de Atributo Digital é uma lista de parâmetros com valores que são associados a uma entidade (pessoa ou organização). Tecnicamente, os atributos são descritos por meio do modelo:

```
Attribute ::= SEQUENCE
{type      AttributeType,
 values    SET OF AttributeValue
 -- at least one value is required}
AttributeType ::= OBJECT IDENTIFIER
AttributeValue ::= ANY DEFINED BY AttributeType
```

Ou seja, de um modo simplificado, o atributo é escrito da seguinte forma: "OID=<valor>". É sobre esse aspecto que levantamos um ponto de discussão importante para a adequação ao modelo ICP-Brasil, qual seja, a normalização desses OIDs de modo a criar um conjunto de OIDs padrão. Assim, a ICP-Brasil teria mapeado um conjunto significativo de OIDs que poderia ser usado com um propósito bem definido e

as aplicações usufruiriam dessa padronização para interpretar os valores dos atributos. Ou seja, se a ICP-Brasil definir, por exemplo, que um determinado OID seja usado para descrever a identificação profissional de uma pessoa, todas as aplicações que entenderem o Certificado de Atributo Digital emitido sob as regras da ICP-Brasil saberiam onde procurar tais informações dentro da estrutura do certificado. Uma proposta, portanto, é definir um conjunto de OIDs, no âmbito da ICP-Brasil, para normalizar o seu uso e um outro de uso livre, pois sempre haverá casos específicos nos quais a normalização não é aplicável.

Desse modo, se tornaria possível a utilização ampla do Certificado de Atributo Digital e suas aplicações teriam condições de "confiar" e "obter" as informações sistematicamente.

Um Certificado de Atributo Digital deve ter validado os seguintes componentes:

- estrutura;
- período de validade; e
- atributos.

Além desses, o processo de validação pressupõe a validação do emissor do Certificado de Atributo Digital.

No próximo item, exploraremos os desafios e sugeriremos regras para a emissão de Certificados Digitais para as Autoridades Certificadoras de Atributos (ACA).

### 4. Autoridade Certificadora de Atributo (ACA)

Uma Autoridade Certificadora de Atributo (ACA) é uma entidade responsável por emitir Certificados de Atributo Digital assinados digitalmente. Sua principal função é oferecer credibilidade e temporalidade a uma determinada informação e é feito por intermédio da assinatura digital de uma informação que possui um determinado período de validade.

No seu núcleo, existe um Certificado Digital responsável pela assinatura. Como ocorre em uma Autoridade Certificadora da ICP-Brasil, assim, a

confiança está fortemente relacionada ao Certificado Digital da Autoridade Certificadora. Ou seja, a entidade emissora do Certificado de Atributo Digital deverá gozar de confiança para que os atributos por ela declarados sejam aceitos.

Dentro da estrutura da ICP-Brasil, o ciclo de confiança é estabelecido por meio da cadeia de certificados que possui uma raiz única (Autoridade Certificadora Raiz Brasileira) e das normalizações de operação, auditorias e fiscalizações que conferem credibilidade ao processo de emissão. Sendo assim, é natural que um certificado emitido dentro da cadeia ICP-Brasil seja confiável e que ele seja usado como Certificado Digital da ACA.

Um Certificado Digital de uma ACA, entretanto, deve ter características específicas que o caracterizem como tal, de modo que possam ser emitidos Certificados de Atributo Digital confiáveis. Para tanto, é necessário disciplinar a emissão e caracterizar o uso deste tipo de Certificado Digital. Antevemos a necessidade de criação de uma DPC/PC para regulamentar o processo de emissão e a adição de um "Object Identifier" (OID) na extensão "Extended Key Usage" informando que o Certificado Digital em questão é usado por uma ACA. Assim, um possível roteiro para o processo de validação de uma ACA ocorreria conforme apresentado abaixo:

1. Validação da cadeia: deve ser pela ICP-Brasil;
2. Validação do estado de revogação de cada Certificado Digital da cadeia: sempre em função de uma data;
3. Verificação da presença da extensão "Extended Key Usage" e do "flag" indicando emissão de Certificado de Atributo Digital;
4. Verificação da identidade da ACA, proprietária do Certificado Digital: pode ser feito por meio dos campos do próprio Certificado Digital (nome ou CNPJ, por exemplo).

Assim, realizando-se uma análise simples do Certificado Digital é possível determinar se a ACA é confiável ou não.

Desse modo, a ACA, de posse de um Certificado Digital

apropriado se torna apta a assinar Certificados de Atributo Digital.

Resumo:

- Criação de uma DPC/PC para emissão do certificado da ACA, contendo as regras para emissão desse tipo particular de Certificado Digital.
- Adição do OID na extensão "Extended Key Usage", indicando que o certificado será usado por uma ACA.

## 5. Proposta de adequação do Certificado Digital da ICP-Brasil

Ao analisar o conceito de Certificado Digital, tal como empregado pela ICP-Brasil, à luz do Certificado de Atributo Digital, surge, de imediato, a necessidade de atender a um requisito fundamental: a identificação única de uma pessoa ou organização, independentemente, do Certificado Digital que contém essa informação.

A importância desse elemento de identificação reside no fato de que o atributo é associado à pessoa ou à organização e não ao Certificado Digital, cuja função é meramente a de identificação.

Assim, mesmo que um Certificado Digital expire, seja renovado, ou mesmo que existam mais de um Certificado Digital associado a uma mesma pessoa ou organização, o vínculo desta com seus correspondentes atributos estaria assegurado, desde que, é claro, o Certificado de Atributo Digital seja válido.

Além disso, o padrão para vinculação de um Certificado de Atributo Digital e o(s) correspondente(s) Certificado(s) Digital(is) considera campos únicos como, por exemplo, um OID de tamanho fixo, contendo apenas o número do CFP de uma pessoa.

Não é o que ocorre atualmente na ICP-Brasil, já que, geralmente, os campos do Certificado Digital são compostos, ou seja, contém mais de uma informação.

Assim, para assegurar o atendimento aos requisitos de identificação única e a aderência ao padrão, consideramos relevante a criação de um OID na

extensão "Subject Alternative Name" (SAN) para conter a identificação única da pessoa ou da organização.

## 6. Aplicação

Existem muitos estudos de aplicação do Certificado de Atributo Digital em sistemas de controle de acesso, nos quais se discute seu papel em processos de autorização [Villar, Cunha, Diniz, & Souza, 2004] [Damiani, Vimercati, & Samarati, 2005]. O nosso estudo está focado em aplicações de controle de fluxo de assinaturas digitais baseadas na qualificação dos signatários e em suas respectivas alçadas e poderes. Esse tipo de aplicação está se tornando comum em empresas que adotam a assinatura digital dentro de um processo automatizado. O estudo [Guilhen & Reverbel, 2007] aborda a autorização em função da qualificação de usuários descritos em Certificados de Atributo Digital e representa também outra importante vertente da utilização dos certificados digitais, em conjunto com os de atributo, no universo corporativo.

O principal desafio endereçado pelo Certificado de Atributo Digital, neste contexto, é a delegação da responsabilidade sobre a atualização das informações. Ou seja, os sistemas devem "acreditar" na fonte da informação ao invés de manter modelos de integração que adicionam complexidade ao ambiente. Quando um sistema "acredita" numa determinada informação, ele está delegando responsabilidades sobre a veracidade da informação à origem dos dados e, dentro de um processo de confiança estabelecido, é possível construir uma rede de confiança e tornar o ambiente muito menos complexo, pelo menos no que diz respeito à manutenção da atualização de uma determinada informação.

É evidente que o Certificado de Atributo Digital não deve substituir completamente as integrações entre as aplicações. Em muitas situações, as bases de dados corporativas são a melhor solução. Contudo, quando a informação não é demasiadamente etérea e depende de entidades externas, como é o caso das entidades de classe que mantêm registros das situações de

seus afiliados, por exemplo, o uso do Certificado de Atributo Digital mostra-se bastante atraente.

## 7. Estudo de caso:

### Aplicação de fluxo de assinaturas

O estudo de caso criado para avaliar a utilização do Certificado de Atributo Digital é um controle de fluxo de assinatura num ambiente corporativo no qual documentos devem ser avaliados e, eventualmente assinados, por pessoas de diversas áreas de uma organização antes da assinatura final de um representante legal. A isso, adicionamos um controle de alçadas baseado em valores constantes do próprio documento.

Por meio da tecnologia OpenXML foi possível criar um modelo em que o fluxo da assinatura digital está descrito no próprio documento. Assim, a aplicação deve interpretar as assinaturas necessárias e validá-las quando apostas. A validação da assinatura passa por uma etapa estrutural (validade da integridade do documento e validade do Certificado Digital) e via validação semântica da assinatura, em que, por meio da apresentação do Certificado de Atributo Digital – que qualifica o signatário do documento – o sistema tem condições de verificar se pode ou não aceitar aquela assinatura. Desse modo, o sistema aceita ou rejeita a assinatura digital de acordo com os atributos apresentados pelo signatário.

Esse exemplo permitiu avaliar a utilização do Certificado de Atributo Digital e entender, na prática, os desafios que foram apresentados, resumidamente, neste trabalho.

## 8. Conclusão

A tecnologia de Certificado de Atributo Digital é um complemento importante para a certificação digital. Quando a ICP-Brasil foi instituída, a Certificação Digital – com as prerrogativas de validade jurídica – abriu caminho para que diversos tipos de documentos fossem assinados em formato digital. Sistemas foram

criados para coletar as assinaturas digitais e a todos se apresentou o desafio de validação semântica da assinatura digital. As aplicações tiveram que tratar informações (atributos) sobre os proprietários dos certificados digitais por meio de integrações e/ou replicações de dados.

O Certificado de Atributo Digital é uma tecnologia bastante estudada e documentada mundialmente, mas nunca foi usado num contexto tão grande como o criado pela ICP-Brasil. Levando-se em consideração as adequações nos Certificados Digitais e as regras para o estabelecimento da infra-estrutura de Certificados de Atributo Digital, notamos claramente os benefícios da sua adoção.

Acreditamos, com este trabalho, ter contribuído para revelar os principais desafios que a ICP-Brasil terá para tornar o Certificado de Atributo Digital uma realidade.

## 9. Trabalhos futuros

Este trabalho não esgota o estudo de adoção do Certificado de Atributo Digital no contexto brasileiro. Ele é um trabalho realizado pela Serasa e pela Microsoft e apresentou alguns aspectos essenciais na adoção da tecnologia.

Como trabalhos futuros, gostaríamos de propor:

- A. **Modelo de ACA Federativo:** criação de uma proposta de confiança federada de Autoridades Certificadoras de Atributo, no contexto brasileiro. Assim, as aplicações teriam condições de, sistemicamente, avaliar a fonte da informação.
- B. **Modelos de distribuição de certificados de atributo digital:** os dois principais modelos de distribuição de Certificados de Atributo Digital "PULL" e "PUSH" devem ser entendidos e adequados

aos nichos de aplicações existentes. O estudo deverá propor modelos – conceituais e reais – baseados em características de nichos de aplicações.

- C. **Tecnologias concorrentes:** SAML [OASIS, 2007].

## Bibliografia

- Damiani, E., Vimercati, S. D., & Samarati, P. (2005). New Paradigms for Access Control in Open Environments.  
Fonte: [citeseer.ist.psu.edu/damiani05new.html](http://citeseer.ist.psu.edu/damiani05new.html)
- Guilhen, S. N., & Reverbel, F. (2007). Um Serviço de Autorização Java EE Baseado em Certificados de Atributos X.509.  
Fonte: VII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais
- ITI. (2001). Medida Provisória. Fonte: <http://www.iti.gov.br/twiki/bin/view/Certificacao/MedidaProvisoria>
- Jordan C. N. Chongy, R. v. (s.d.). Security Attributes Based Digital Rights Management.
- Network Working Group. (abril de 2002). An Internet Attribute Certificate Profile for Authorization.  
Fonte: RFC: <http://www.ietf.org/rfc/rfc3281.txt>
- OASIS. (2007). OASIS Security Services (SAML).  
Fonte: OASIS: [http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=security](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security)
- Villar, M. V., Cunha, C. C., Diniz, A. L., & Souza, J. N. (2004). Segurança nos Processos de Autenticação e Autorização através de Certificados X.509. SSI.

