Classificação de Assinaturas Eletrônicas

Uma **assinatura eletrônica** é uma forma de garantir a autenticidade e integridade de um documento eletrônico. Ela fornece uma maneira de comprovar que um documento foi assinado por uma pessoa específica, e que o conteúdo do documento não foi alterado desde a assinatura.

Existem vários tipos de assinaturas eletrônicas, incluindo:

Assinatura eletrônica simples: é a mais básica e comum das assinaturas eletrônicas. Ela consiste em adicionar uma mensagem criptográfica ao documento eletrônico, que pode ser verificada com a chave pública do signatário.

A assinatura eletrônica simples poderá ser admitida nas interações com entre público de menor impacto e que não envolvam informações protegidas por grau de sigilo.

Assinatura eletrônica avançada: é uma forma mais segura de assinar documentos eletrônicos, pois inclui informações adicionais, como a data e hora da assinatura, além da assinatura simples.

A assinatura eletrônica avançada deverá ser usada em interações que envolvam informações protegidas por grau de sigilo.

Assinatura eletrônica qualificada: é considerada a mais segura e confiável de todas as assinaturas eletrônicas, pois inclui informações adicionais, como o certificado de um terceiro confiável e a data e hora da assinatura.

A assinatura eletrônica qualificada é admitida em qualquer interação eletrônica com ente público, independentemente de cadastramento prévio.

As assinaturas eletrônicas são ferramentas importantes para garantir a autenticidade e integridade de documentos eletrônicos, e existem vários tipos diferentes, cada um com suas próprias características e níveis de segurança. É importante entender as diferenças entre cada tipo de assinatura e escolher o que melhor atende às suas necessidades.

Certificados Digitais

No Brasil, existem dois tipos principais de certificados digitais utilizados: certificados A1 e certificados A3.

Certificados A1: são certificados digitais emitidos por Autoridades Certificadoras (ACs) credenciadas pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Eles geralmente são emitidos para pessoas físicas e jurídicas, e são utilizados para assinar documentos eletrônicos, acessar sistemas governamentais eletrônicos, e outras aplicações similares. Os certificados A1 são instalados diretamente no computador e geralmente possuem validade de até 1 ano.

Certificados A3: são certificados digitais emitidos por Autoridades Certificadoras (ACs) credenciadas pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Eles são utilizados para assinar documentos eletrônicos de forma mais segura, e geralmente são emitidos para usuários corporativos. Os certificados A3 são armazenados em dispositivos seguros, como tokens USB, smart cards ou hardware security module (HSM), e geralmente possuem validade de 2 ou 3 anos.

Certificado em Nuvem: é um tipo de certificado que pode ser armazenado, gerenciado e compartilhado totalmente online, sem a necessidade de utilizar uma mídia física (token ou cartão). Ele pode realizar todas as funções de um certificado tradicional diretamente na tela de múltiplos dispositivos conectado à rede, como smartphones e notebooks. As chaves do certificado são

armazenadas em ambiente seguro, auditado e de nível máximo de compliance. São gerados códigos de acesso individuais para cada usuário certificado e armazenado. Com esse modelo de certificado, as organizações podem emitir, revogar e gerenciar seus certificados de forma mais eficiente.

Certificado digital tipo A1	
	É instalado e armazenado diretamente em um computador e sua validade é sempre de um ano. **As vantagens dele são:**
✓ Pode ser instalado em diversos computadores simultaneamente; ✓ Pode ser importado por softwares de emissão de notas fiscais; ✓ Permite fazer o backup do certificado, então, o arquivo não é perdido se o computador for formatado; ✓ Agilidade no momento de assinar documentos, pois não depende de dispositivos externos; ✓ Não requer instalação de leitoras de cartão.	

Certificado digital tipo A3	
	É armazenado em token (que é parecido com um pendrive) ou em smartcard (cartão inteligente) que precisa de leitor específico, sendo que ambos podem ter validade de um, dois e três anos. **As vantagens são:**
✓ Pode ser levado para qualquer lugar onde possa ser necessário utilizar; ✓ É inviolável e tem um nível de segurança elevado, pois não pode ser extraído ou copiado para outra mídia; ✓ É pessoal e intransferível, somente o portador da senha pode usá-lo.	

É importante ressaltar que os certificados A1 são certificados digitais de nível de segurança básico, enquanto que os certificados A3 são de nível de segurança elevado, eles exigem uma validação mais rigorosa dos dados do titular e são utilizados para transações eletrônicas de maior valor, como transações financeiras e contratos.

Além desses dois tipos principais, também existem outros tipos de certificados digitais, como certificados de servidor, que são utilizados para proteger comunicações em websites e aplicativos, e certificados de e-mail, que são utilizados para proteger comunicações de e-mail.

A assinatura eletrônica e o certificado digital são dois conceitos diferentes, embora estejam relacionados.

A **assinatura eletrônica** é uma forma de garantir a autenticidade e integridade de um documento eletrônico. Ela fornece uma maneira de comprovar que um documento foi assinado por uma pessoa específica, e que o conteúdo do documento não foi alterado desde a assinatura. A assinatura eletrônica é realizada usando uma chave criptográfica, que pode ser verificada com a chave pública do signatário.

Já o **certificado digital** é um documento eletrônico que contém informações sobre a identidade de uma pessoa ou entidade, e é emitido por uma Autoridade Certificadora (AC) credenciada. Ele

contém informações como nome, endereço, número de identificação, e uma chave pública que pode ser usada para verificar assinaturas eletrônicas. Certificado digital é usado para garantir a identidade de uma pessoa ou entidade, e pode ser usado para acessar sistemas eletrônicos, assinar documentos eletrônicos, e outras aplicações similares.

Uso das Assinaturas Eletrônicas na UFLA

Assinatura de Diploma Digital: Utiliza certificado digital do tipo A3 de pessoa jurídica com o CNPJ da instituição + certificado digital do tipo A3 de pessoa física individual usado pelo diretor ou vice diretor da faculdade.

Acesso a Sistemas do Governo (SCDP, Workflow, ComprasNet, SiapeNet, SIAFI, etc.): Utiliza certificado digital do tipo A3 de pessoa física individual.

Assinatura Digital de Documentos: Pode ser feito gratuitamente através do certificado digital ICPEDU fornecido pela RNP ou através do certificado digital do portal GOV.BR.

Para saber mais, acesse a Lei 14.036 de 2020 que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos e o Decreto 10.543, de 13 de Novembro de 2020 que dispõe sobre o uso de assinaturas eletrônicas na administração pública federal e regulamenta o art. 5º da Lei nº 14.063, quanto ao nível mínimo exigido para a assinatura eletrônica em interações com o ente público.

Revisão #20
Criado Thu, Jan 26, 2023 11:55 AM por PLINIO MARCIO BRAGA TORRES
Atualizado Mon, Apr 3, 2023 1:53 PM por PLINIO MARCIO BRAGA TORRES