



Certificados Digitais utilizados no Sistema NF-e Security[®] v2



Produto:

**Certificados Digitais
utilizados no Sistema
NF-e Security[®] v2**

Release date: Mai 15, 2009



Certificados e Assinatura DIGITAL

O certificado digital é um documento eletrônico que possibilita comprovar a identidade de uma pessoa, de uma empresa ou um serviço de comércio eletrônico, para assegurar as transações on-line e a troca eletrônica de documentos, mensagens e dados. É um documento eletrônico que associa uma chave pública, fornecida por uma entidade confiável, a uma identidade (legítima o proprietário) e que assegura que o Documento não está com os dados comprometidos (íntegros).

Essa tecnologia permite assinar digitalmente, qualquer tipo de documento, conferindo-lhe a mesma validade jurídica dos equivalentes em papel assinados de próprio punho, além de propiciarem facilidades de serviços virtuais do Governo, Bancos e outras entidades que se utilizam de certificados para transações eletrônicas.

Os documentos assinados digitalmente atendem aos principais requisitos de segurança para a realização de negócios eletrônicos:

- Autenticidade: garante a identidade de todas as partes envolvidas.
- Integridade: fidelidade da informação com seu estado original intacto.
- Confidencialidade: técnica para manter a confidencialidade utilizando criptografia
- Não-repúdio: impede as partes de negarem a participação no negócio eletrônico.

Tipos de Certificados Digitais

Na ICP-Brasil estão previstos oito tipos de certificado, diferenciados pelo uso, pelo nível de segurança e pela validade. São duas séries de certificados, com quatro tipos cada.

A série A (A1, A2, A3 e 4) reúne os certificados de assinatura digital, utilizados na confirmação de identidade na Web, em e-mail, em redes privadas virtuais (VPN) e em documentos eletrônicos com verificação da integridade de suas informações. A série S (S1, S2, S3 e S4) reúne os certificados de sigilo, que são utilizados na codificação de documentos, de bases de dados, de mensagens e de outras informações eletrônicas sigilosas.

- Nos certificados do tipo A1 e S1, as chaves privadas ficam armazenadas no repositório do computador, em uma conta de usuário, de computador ou serviço.
- Nos tipos A2, A3, A4, S2, S3 e S4, as chaves privadas e as informações referentes ao seu certificado ficam armazenadas em um hardware criptográfico - cartão inteligente (*smartcard*) ou cartão de memória (*token USB* ou *pen drive*). Para acessar essas informações você usará uma senha pessoal determinada no momento da compra.

Os certificados utilizados para emissão de NF-e geralmente são do tipo A1 ou A3, ambos de classe 3, o que significa que validam indivíduos através do comparecimento pessoalmente dos mesmos perante um agente autorizado, além de outras comprovações específicas de identidade. Os certificados de classe 3 validam organizações através de bancos de dados de terceiros (como o Cadastro Nacional de Pessoas Jurídicas - CNPJ) e outros meios independentes. Veja na seqüência, o certificado mais indicado para sua empresa.



Qual Certificado?

Token, Cartão ou Arquivo?



Modelos mais utilizados:

A3 / S3 - é o certificado em que a geração e o armazenamento das chaves criptográficas são feitos em cartão inteligente (*smart card*) ou *token*, ambos com capacidade de geração de chaves e protegidos por senha ou hardware criptográfico aprovado pela ICP-Brasil. As chaves criptográficas têm no mínimo 1024 bits. A validade máxima do certificado é de três anos, sendo a frequência de publicação da Lista de Certificados Revogados no máximo de 24 horas e o prazo máximo admitido para conclusão do processo de revogação de 36 horas.

A cada acesso ao certificado A3 é necessário a autenticação, o que não é indicado para um modelo de assinatura digital de notas fiscais eletrônicas de um sistema instalado em um servidor, além de ficar exposto fisicamente no lado externo do computador. Em termos de política de segurança na área de TI, estes dispositivos, tokens ou smart cards, se removidos, paralisam a emissão de NF-e e podem comprometer a segurança.

A1 / S1 - É o certificado em que a geração das chaves criptográficas é feita por software e seu armazenamento pode ser feito em hardware ou repositório protegido por senha, cifrado por software, aprovado pela ICP-Brasil. Sua validade máxima é de um ano, sendo a frequência de publicação da Lista de Certificados Revogados no máximo de 48 horas e o prazo máximo admitido para conclusão do processo de revogação de 72 horas.

Estes certificados digitais são válidos por um ano e ficam armazenados no no repositório do computador, em uma conta de usuário, de computador ou serviço. Recomenda-se que seja feita uma cópia de segurança desse certificado (backup) em disquete, ou outra mídia portátil. A política de segurança de TI da empresa define em qual conta de usuário e/ou computador no domínio é que deverá ser instalado o certificado. Modelo comum para aplicações em servidores de NF-e.

→ BENEFIX utiliza certificados A1 no seu servidor de NF-e.

O uso do certificado A1 é mais prático e seguro quando gerenciado automaticamente pelo sistema de emissão de NF-e, independente de usuários e dispositivos. Para modelos integrados, o A3 não deverá ser utilizado e não é suportado na integração, até mesmo, porque é inviável em soluções ASP.

O modelo A3 é recomendado para uso individual e quando há a necessidade de mobilidade (usar em outros computadores), mas indesejável em soluções automatizadas. Imagine um local com processamento centralizado composto de vários CNPJ matriz usando certificados A3. O servidor teria vários "memory keys" e/ou "smartcards" conectados externamente, o que não seria seguro nem prático, pois a desconexão ou remoção acidental interromperia a emissão da respectiva matriz e filias, ainda, seria impossível caso a empresa tenha soluções hospedadas em um *Data Center*.

- **Recomendamos não adquirir certificados A3 para emissão automatizada de NF-e sob pena de necessitar comprar novos certificados A1.**



Portanto, ao adquirir o certificado digital para NF-e em sistemas automatizados, adquira o certificado **Tipo A1**.