Tipos de certificado digital - qual o melhor?

A Certificação Digital é a tecnologia que, por meio da criptografia de dados, garante autenticidade, confidencialidade, integridade e não repúdio às informações eletrônicas. Trata-se de um documento digital utilizado para identificar pessoas e empresas no mundo virtual.

Existem diferentes modelos e tipos de certificados digitais, cada um com aplicações específicas, de modo que, antes de adquirir um certificado digital, é importante compreender essas diferenças. Assim será possível fazer uma escolha informada e obter o certificado correto para atender às suas demandas.

Neste artigo você confere:

Tipos de certificados digitais

Tipo A – certificado de assinatura digital

Esse tipo de certificado é o mais utilizado, sendo indicado para profissionais liberais e empresas de qualquer área cujos processos de rotina exigem autenticação do autor.

O tipo A é utilizado para assinatura de documentos, transações eletrônicas, entre outras aplicações. Ele confere autenticidade a qualquer tipo de documento digital, sendo seu principal objetivo identificar quem assina o documento em questão e verificar que este documento não foi alterado após a assinatura.

Há diferentes modelos de certificado do tipo A (A1, A3, etc), os quais detalhamos mais abaixo.

Tipo S – certificado de sigilo/confidencialidade

O tipo S é capaz de conferir sigilo a uma determinada transação, pois ele criptografa os dados do documento assinado. Com isso, o documento só poderá ser acessado por meio de um certificado autorizado, o que evita o vazamento de informações.

Seu uso se aplica, por exemplo, para empresas que precisam trocar informações de cunho sigiloso, garantindo que os documentos assinados sejam inacessíveis para pessoas não autorizadas.

Tipo T – certificado de tempo

O tipo T se refere ao que conhecemos como carimbo de tempo ou protocolação digital. O objetivo deste certificado é atestar precisamente o momento em que um documento digital foi emitido, oferecendo garantia a respeito da data e a hora em que determinada informação digital passou a existir.

Para impedir que esses dados sofram adulterações, esse tipo de certificado utiliza um servidor externo de tempo para atestar o exato instante em que o carimbo de tempo foi aplicado em um documento.

O certificado de tempo pode ser utilizado em conjunto com outros tipos de certificados para acrescentar a característica da irretroatividade ao documento, conferindo ainda mais segurança às transações.

Certificado de assinatura digital: quais as opções?

Com esse tipo de certificado a pessoa ou empresa poderá fazer a assinatura digital de documentos para garantir sua autoria e conferir validade jurídica. Esses certificados podem ter diferentes níveis de segurança dependendo da forma de armazenamento do arquivo da chave criptográfica.

Certificado digital A1

Os certificados A1 são aqueles cuja chave privada é instalada diretamente no computador do usuário que fará a assinatura. Esse tipo de certificado não é compatível com dispositivos móveis (como celular e tablet) e fica acessível para cópias – o que pode ser útil para o usuário, mas também justifica por que o certificado A1 possui um nível de segurança inferior ao certificado A3.

De qualquer forma, os dados são protegidos por meio de uma senha de acesso, sendo que apenas por meio dela é possível acessar, mover e copiar a chave privada associada ao certificado.

O certificado A1 consiste em um arquivo digital, de extensão .PFX ou .P12, que o usuário recebe da Autoridade Certificadora (AC) para instalar em seu computador. É recomendado manter uma cópia de segurança do arquivo para casos de formatação ou avarias do equipamento – isso porque este certificado só pode ser emitido pela AC uma única vez, portanto perder o arquivo significa perder completamente o acesso à assinatura.

A validade máxima do certificado A1 é de 1 ano, devendo ser renovado anualmente.

Certificado digital A3

Os certificados A3 são gerados e armazenados em um hardware criptográfico, que pode ser um *smartcard* (cartão inteligente com chip, lido através de hardware específico) ou um *token* (artefato USB, semelhante a um pendrive).

O titular do Certificado A3 é o único que pode usar a chave privada, porque além da chave em meio físico, também é necessário estar em posse da senha de acesso. Além disso, também não é possível fazer cópia de segurança do certificado, como ocorre com o modelo A1.

Atualmente, há também certificados A3 armazenados em nuvem. Esses certificados continuam sendo gerados por hardware, mas são disponibilizados na nuvem pela Autoridade Certificadora para que o titular possa acessá-lo à distância. Neste caso, a pessoa depende de uma conexão com a internet para acessar e utilizar o certificado.

O certificado A3 é considerado o certificado padrão ouro e a opção mais segura para gerar assinaturas digitais, sendo, por isso, o mais recomendado para profissionais autônomos.

A validade do certificado A3 pode variar de 3 anos a 5 anos.

Outros modelos: e-CPF; e-CNPJ; NF-e; e-Saúde; Certificado Digital do CFM

Todos esses modelos são certificados dos tipos A1 ou A3, mas emitidos para fins e nichos específicos. Assim: o e-CPF é voltado para pessoas físicas; o e-CNPJ identifica pessoas jurídicas no meio eletrônico; o NF-e é voltado especificamente para a emissão de notas fiscais pelas empresas; o e-Saúde é direcionado aos diversos profissionais da área de saúde.

Há também, especificamente para os médicos, o Certificado Digital do CFM, disponibilizado gratuitamente pelo Conselho Federal de Medicina. Ele é um certificado do tipo A3 em nuvem que pode ser usado para assinar prescrições e outros documentos emitidos para os pacientes, assinar os prontuários eletrônicos, acessar os serviços digitais oferecidos pelo CFM e pelo governo, além de servir para os demais usos aos quais um certificado A3 se aplica.

Qual o melhor certificado digital para médicos?

O certificado A3, por ser mais seguro, é o recomendado pelo CFM para uso por médicos. Além disso, a validade mais longa também é um ponto a favor deste modelo, descartando a necessidade de renovação anual.

Se o médico atua como autônomo em consultório particular, um e-CPF atenderá às suas necessidades, bem como o e-Saúde e o Certificado Digital do CFM. Já para os profissionais que atuam com CNPJ, o e-CNPJ é a melhor opção.

Porém, não é necessário estar preso a estes modelos específicos. Na prática, o médico pode adquirir qualquer certificado A3, desde que emitido por uma Autoridade Certificadora credenciada junto à ICP-Brasil.

A lista atualizada das Autoridades Certificadoras pode ser conferida no site do Instituto Nacional de Tecnologia da Informação.

Os certificados digitais emitidos pela ICP-Brasil são os instrumentos mais confiáveis para uso nas transações e documentações eletrônicas, pois possuem amparo legal.

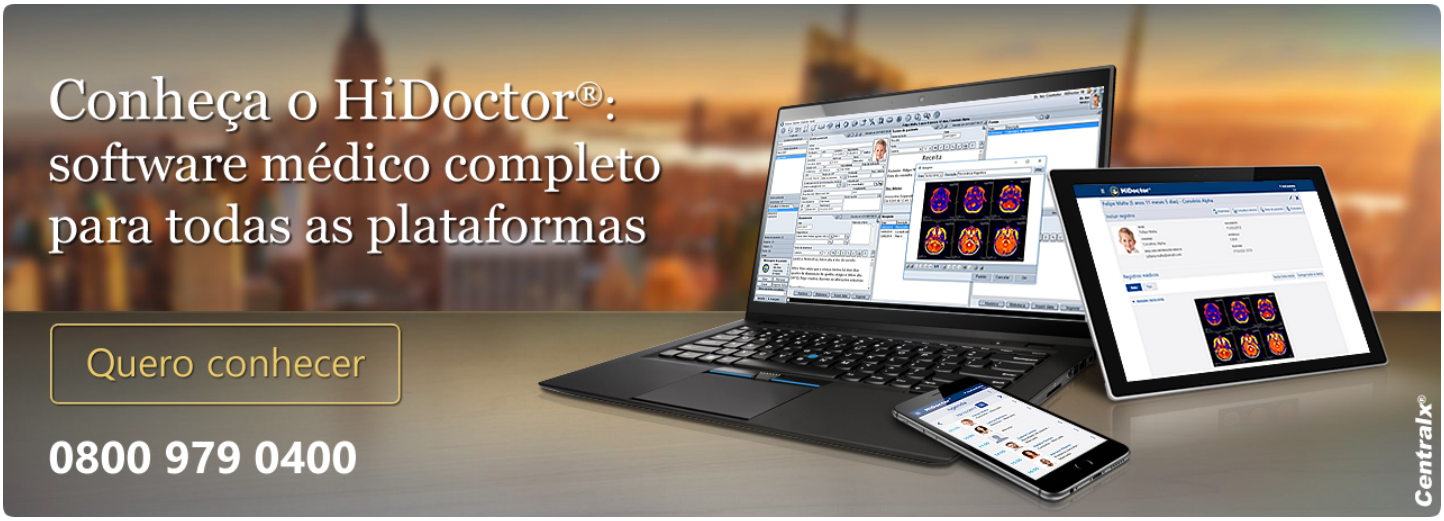
Além disso, na medicina, os certificados digitais são indispensáveis para o uso da telemedicina e também são requisito para assinar os prontuários eletrônicos, conforme regulamentado pelo CFM e pela legislação brasileira.

De posse de seu certificado digital, o HiDoctor® é a ferramenta certa para ajudá-lo a emitir documentos médicos e assinar seus prontuários com praticidade. Com funcionalidade de assinatura digital integrada ao software médico, esses processos podem ser feitos de forma descomplicada em

sua rotina de atendimentos.

O HiDoctor® é a única plataforma médica completa para seu consultório e o software mais utilizado por médicos e clínicas no Brasil. A Centralx® conta com mais de 30 anos de experiência no desenvolvimento de tecnologias para a área médica.

Experimente e conheça clicando abaixo!



Artigo original disponível em:

"Tipos de certificado digital - qual o melhor? " **- HiDoctor® Blog**

Centralx®