



## Certificado Digital Individual Profissional

Já reparou que a sua empresa, actualmente, lida com um alto volume de processos e transacções electrónicas? Porque é que ainda autoriza transacções de modo tradicional, com assinaturas manuscritas em papel, enquanto os processos automatizados poupam tempo e dinheiro?

Os certificados digitais da MULTICERT são imprescindíveis para uma utilização profissional e segura da Internet, uma vez que diminuem o risco de fraude e roubo de informação sensível (como por exemplo, espionagem industrial nos emails).

A MULTICERT dispõe de certificados que visam a autenticação em páginas e serviços web, através de SSL Client Side, assim como permitem o envio de mensagem de correio electrónicas assinadas digitalmente (através de clientes de email como o Microsoft Outlook, o Thunderbird, Mail.app, Entourage, entre outros) e a assinatura de documentos digitais em diversos formatos (PDF, Microsoft Word, Excel).

O Certificado Digital é um documento electrónico autenticado com uma assinatura digital, que certifica a titularidade de um par de chaves e a sua validade. Este documento é emitido por uma entidade certificadora de confiança, que associa inequivocamente a identidade de um indivíduo a uma chave criptográfica que lhe é exclusiva, assegurando com fiabilidade o seu valor probatório.

Os certificados digitais emitidos pela MULTICERT seguem o standard X.509v3 e são o elemento base de uma infra-estrutura de chaves públicas (PKI – Public Key Infrastructure), que se baseia na utilização de algoritmos de chaves assimétricas – uma chave pública e uma chave privada.

Uma forma de assegurar a autenticação de cada uma das partes pode ser alcançada através dos serviços de uma terceira parte que emita e regula os serviços de gestão de certificados digitais.

A necessidade de uma terceira entidade de confiança, denominada por Autoridade Certificadora ou Entidade Certificadora visa o reconhecimento de uma identidade com um par de chaves. Usando metodologias, processos e critérios bem definidos e públicos, a Entidade Certificadora regula a gestão dos certificados através da emissão, renovação e revogação dos mesmos, por aprovação individual.

Assim, um Certificado Digital pode ser utilizado como forma de identificação digital, como um BI por exemplo, podendo ser utilizado para efectuar transacções electrónicas em redes abertas com segurança e privacidade, assinar digitalmente documentos e disponibilizar outros mecanismos para fins de confidencialidade, como é o caso do envio de uma peça processual para um tribunal.

Se deseja identificar-se no mundo virtual, realizar trocas de informação confidenciais, assegurar-se que as mensagens que envia não são alteradas e declarar a autoria de mensagens, necessita de um Certificado Digital!

#### Contactos:

Estrada Casal do Canas, Lote 6  
Alfragide  
2729-092 Amadora - Portugal

Telefone: +351 217 123 010  
Fax: +351 217 123 011



WEB: [www.multicert.com](http://www.multicert.com)  
Email: [info@multicert.com](mailto:info@multicert.com)

Copyright © 2002/2008 MULTICERT - Todos os direitos reservados. A MULTICERT detém todos os direitos de propriedade intelectual neste documento ou foi devidamente autorizada para os utilizar. Todas as marcas incluídas neste documento são utilizadas apenas para identificar produtos e serviços e estão sujeitas a regras legais. O documento ou partes não pode ser copiado, reproduzido, arquivado, traduzido ou transmitido a terceiros por qualquer meio sem consentimento prévio da MULTICERT.

#### Autenticidade

Permite verificar que o documento teve proveniência no remetente que o reivindica.

#### Confidencialidade

Permite através da cifragem que duas pessoas/sistemas troquem dados sem poderem ser vistos por terceiros.

#### Integridade

Garante através da assinatura digital que duas pessoas/sistemas que trocam dados consigam ter a garantia de que não foram alterados, ou seja, garante que foram mesmo os dados originais transmitidos pela outra pessoa/sistema.

#### Não-Repúdio

Garante através da assinatura digital, que a pessoa que criou/assinou um certo conjunto de dados, não pode negar a sua autoria.

#### O que é?

- É uma assinatura electrónica de documentos, conferindo aos mesmos o valor legal equivalente a uma assinatura manuscrita em papel
- Identificação electrónica segura e unívoca de uma pessoa
- Autenticação electrónica segura
- Cifra de documentos electrónicos ou de correio electrónico para o titular
- Integridade de documentos electrónicos ou de correio electrónico
- Permite identificar o endereço de correio electrónico do seu titular
- Permite a identificação e a realização de autenticação segura perante servidores web
- É integrável e reconhecido automaticamente pelos principais browsers e aplicações de correio electrónico
- Pode funcionar em tokens criptográficos seguros

#### Como pode ser utilizado?

- Administração, autenticação e autorização
- Controle de acessos
- Gestão de identidades
- Segurança na Internet
- Segurança de redes
- PKI