

**Curso de Tecnologia em Redes de Computadores**  
**Disciplina: Tópicos Avançados II – 5º período**  
**Professor: José Maurício S. Pinheiro**

**AULA 4: Aspectos Legais da Certificação Digital**

Na sua essência, a certificação digital baseia-se em informação, a qual é compilada, organizada e atualizada em sistemas digitais, relativamente a pessoas físicas e jurídicas. Portanto, deve ser vista à luz da convergência do significado legal e social dessa informação (aspectos existentes), do significado técnico e eletrônico da mesma (aspectos inovadores).

A confiança em um documento eletrônico deve ser garantida por um tripé, que engloba: certificado digital confiável, algoritmo de criptografia, plataforma computacional e uma âncora temporal.

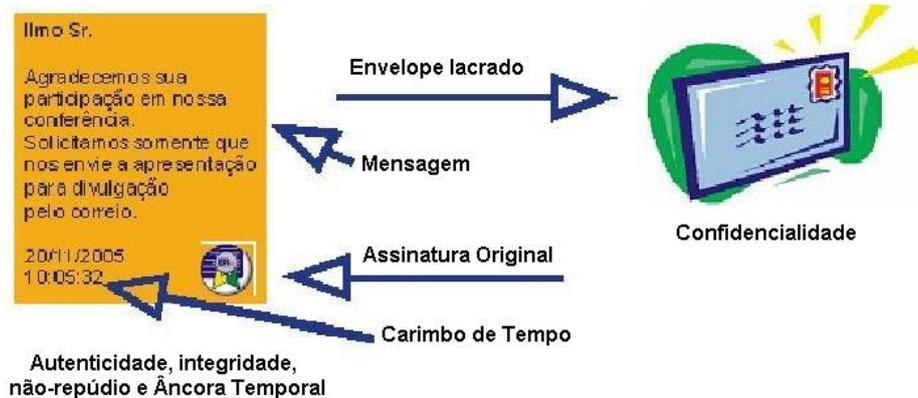
A garantia da confiança no documento eletrônico é resolvida tecnicamente com o processo de assinatura e âncora temporal. Estes processos demandam o uso de criptografia, cujos protocolos criptográficos garantem a impossibilidade de ação maliciosa.

Para a garantia da interoperabilidade entre sistemas operacionais, os padrões utilizados na criptografia são definidos por recomendações internacionais denominadas de RFC (documento que descreve os aspectos relacionados com a Internet, como padrões, protocolos, serviços, recomendações operacionais etc.).

**Documento Eletrônico**

A para eliminar fatores de risco, fez-se o uso de protocolos criptográficos, que é uma tarefa a ser realizada no início de qualquer sistema. Isto é feito através da análise dos requisitos de segurança que um sistema deve atender. Faz-se necessário saber quais requisitos de segurança um documento eletrônico deve apresentar.

Quando se fala em documento eletrônico seguro ocorre uma mudança no conceito de “documento”. Para entender melhor o que é um documento eletrônico seguro, é feita uma analogia entre o documento papel e eletrônico (figura 1). Esta analogia envolve os atributos de segurança.



**Figura 1 - Documento Digital x Documento em papel**

Para assinatura em papel, geralmente é usado algum tipo de marca física para identificação de autenticidade do documento, ou também para mostrar o acordo de um assinante com o que está dito em um documento. Para isso é feito uma assinatura manuscrita que tem validade jurídica, onde pode ser levada ao tabelião que faz o seu reconhecimento por semelhança sendo arquivada, podendo ser periciada por meios grafológicos.

Já no documento digital sua autenticidade é feita através de certificado digital é emitido por uma Autoridade Certificadora que faz a ligação entre o certificado e o assinante, garantindo assim o princípio da autenticidade. A integridade do documento feito em papel é feita pela inexistência de rasuras, mas no documento digital é feito através de criptografia.

A assinatura em papel também se caracteriza por ser irretroativa, ou seja, não se pode assinar um documento agora dizendo ser do passado, mas em documento digital as da criação do documento geralmente e a data do seu próprio terminal, data que pode ser facilmente alterada, dando uma característica de retroatividade a ele sem deixar pistas. Para resolver este problema foi criado o protocolo criptográfico de datação, que funciona como uma âncora temporal. Este protocolo é disponibilizado em um servidor, denominado de Protocolizador Digital de Documentos Eletrônicos (PDDE). A PDDE garante a irretroatividade a documentos eletrônicos.

Logo para dar ao documento digital a mesma confiabilidade que o em papel é necessário utilizar três componentes:

- O certificado digital (utilizado para assinar);
- Os algoritmos de criptografia e a plataforma computacional;
- Âncora Temporal (Temporalidade ou irretroatividade): garante a certeza e imparcialidade de quando o documento eletrônico foi criado e da relação de precedência com outros.

## Identidade Digital

A Identidade digital (ID) traduz a atribuição de propriedades a uma pessoa, as quais são imediata e operacionalmente acessíveis através de meios

técnicos. Engloba todos os dados relacionados com a pessoa, e que podem ser armazenados e automaticamente interligados por uma aplicação eletrônica.

A questão da identidade digital pertence ao universo dos sistemas de informação e alguns dos problemas que têm surgido no seu processo de digitalização derivam de percepções focadas na perspectiva tecnocrática. Não é recomendável tratar o assunto somente do ponto de vista tecnológico. É importante analisar também os aspectos sociais, culturais e legais relacionados à expressão da vontade do assinante num documento eletrônico. Na verdade, essa perspectiva faz parte dos pilares da via para a sociedade da informação, e em consequência, para a identidade digital: Sociedade; Legislação; Direito; Segurança e Tecnologia.

A Identidade Digital é parte integrante de vários outros processos críticos da sociedade da informação, tais como: votação eletrônica; controle de acessos, incluindo passagem de fronteiras (e-passaporte), digitalização de processos na administração pública e de saúde, comércio eletrônico, entre outros.

Dentre as vantagens, riscos e oportunidades oferecidas pela identidade digital se podem destacar:

- A robustez e segurança de assinatura ou identificação são uma vantagem, que pode ser amplificada pela fidelidade de outras tecnologias, por exemplo, a biometria;
- A fidedignidade de uma assinatura ou identificação no meio digital é uma desvantagem no caso (não desejável) de roubo de identidade e falsificação: é muito mais difícil provar uma assinatura falsificada (embora existam mecanismos efetivos que previnem a aceitação de assinaturas digitais após detecção do roubo de identidade);
- A possibilidade de um controle do cidadão na gestão da sua identidade, a facilidade de criação de pseudônimos preservadores da privacidade e/ou anonimato;
- A falsificação de uma identidade digital a partir de um documento físico falsificado é um risco que necessita de ser avaliado e enquadrado juridicamente, já que tal situação é possível existir na fase de transição do documento físico de identificação para a ID.

### **Confiança na Autoridade Certificadora**

A escolha de confiar em uma Autoridade Certificadora é similar ao que ocorre em transações convencionais, que não se utilizam o meio eletrônico. Por exemplo, uma empresa que vende parcelado, aceita determinados documentos para identificar o comprador antes de efetuar a transação. Estes documentos normalmente são emitidos pela Secretaria de Segurança de Pública e pela Secretaria da Receita Federal, como o RG e o CPF. Existe, aí, uma relação de confiança já estabelecida com esses órgãos. Da mesma forma, os usuários podem escolher uma AC à qual desejam confiar a emissão de seus certificados digitais.

## **Assinatura Digital**

No Brasil, a assinatura é considerada apenas uma identificação que possui alguns efeitos jurídicos, assim como está disposto nos artigos 21 e 22 do Código Comercial. Nos artigos 131 a 135 do Código Civil, a assinatura apenas presume a veracidade das declarações ou servem para provar um valor, porém na há nada disposto nos artigos em caso da ausência da assinatura. No Brasil, o importante é a declaração de vontade expressamente manifestada, demonstrada por qualquer meio permitido legalmente, e seus efeitos. Neste ponto, podemos atentar para os artigos 129, 136, 1289 e 1290 do Código Civil Brasileiro.

A assinatura simplesmente é uma das formas de declaração. Por exemplo: se uma pessoa possui uma assinatura eletrônica e outra pessoa tem acesso e utiliza essa assinatura contratando um serviço em seu nome, não necessariamente a pessoa prejudicada (desde que prove) deva cumprir o mesmo. O que acontecerá é que ela deverá ressarcir o contratante prejudicado com perdas e danos, mas não necessariamente deve cumprir a obrigação.

As leis sobre assinaturas eletrônicas têm como objeto a validade jurídica de documentos eletrônicos que são criadas e arquivadas eletronicamente. Documentos em geral, para serem legalmente válidos, precisam depender de confiança e credibilidade, que dependem de três características: integridade, genuinidade e a segurança. Para que seja autêntico, o documento não pode sofrer alterações, sejam por erros humanos (involuntários ou intencionais), falhas técnicas, fatores externos ou fraudes, e precisa ser seguro. Um documento é seguro quando é difícil de alterá-lo. Essas características visam manter o documento autêntico, íntegro e confidencial.

As assinaturas eletrônicas servem para dar essas qualidades aos documentos eletrônicos. Suas principais funções são a identificação da pessoa assinando, a indicação da intenção da pessoa assinando e a prova da integridade e autenticação do documento evitando alterações unilaterais. Com a rápida expansão da Internet e o crescimento na utilização de transações por meios eletrônicos, a necessidade em identificar a pessoa assinando e manter a integridade, autenticidade e confidencialidade dos documentos eletrônicos tornou-se necessário e essencial para permitir o funcionamento de transações comerciais no ciberespaço.

Diversos países já adotaram leis especiais tratando das transações eletrônicas, especialmente no que se refere à questão do documento eletrônico e da assinatura digital. Os objetivos de se ter legislação versando sobre assinaturas eletrônicas são para remover fronteiras ao comércio eletrônico e permitir e promover o comércio eletrônico ajudando em estabelecer a confiança e a integridade requeridas pelas partes transacionadas.

## **Cuidados na utilização do Certificado Digital**

A certificação digital traz diversas facilidades, porém seu uso não torna as transações realizadas isenta de responsabilidades. Ao mesmo tempo em que o uso da chave privada autentica uma transação ou um documento, ela

confere o atributo de não-repúdio à operação, ou seja, o usuário não pode negar posteriormente a realização daquela transação. Por isto, é importante que o usuário tenha condições de proteger de forma adequada a sua chave privada.

Em caso de suspeita de comprometimento da chave privada, seja por uma invasão sofrida no computador ou pelo surgimento de operações associadas ao uso da chave que não sejam de conhecimento do seu proprietário, a revogação do certificado deve ser solicitada o mais rapidamente possível à AC responsável pela sua emissão. Além disso, é necessário estar alerta às recomendações da DPC quanto aos procedimentos necessários a revogação do certificado.

Primeiramente, deve-se lembrar que o certificado digital representa a “identidade” da pessoa no mundo virtual. Assim, é necessária a adoção de alguns cuidados para se evitar que outra pessoa, possa praticar negócios jurídicos, acessar páginas na Internet e realizar transações bancárias em nome do titular do certificado.

Recomendações para o uso de um certificado digital:

1. A senha de acesso da chave privada e a própria chave privada não devem ser compartilhadas com ninguém;
2. Caso o computador onde foi gerado o par de chaves criptográficas seja compartilhado com outros usuários, não se recomenda que a chave privada seja armazenada no disco rígido, pois todos os usuários terão acesso a ela, sendo melhor o armazenamento em HSM (Hardware Security Module), Smart Card ou Token;
3. Caso a chave privada esteja armazenada no disco rígido de algum computador, deve-se protegê-lo de acesso não-autorizado, mantendo-o fisicamente seguro.
4. Nunca deixe a sala aberta quando sair e for necessário deixar o computador ligado. Utilize também um protetor de tela com senha. Cuidado com os vírus de computador, eles podem danificar sua chave privada;
5. Caso o software de geração do par de chaves permita optar entre ter ou não uma senha para proteger a chave privada, recomenda-se a escolha pelo acesso por meio de senha. Não usar uma senha significa que qualquer pessoa que tiver acesso ao computador poderá se passar pelo titular da chave privada, assinando contratos e movimentando contas bancárias. Em geral, é bem mais fácil usar uma senha do que proteger um computador fisicamente;
6. Utilize uma senha longa, uma vez que existem programas com a função de desvendar senhas. Deve-se evitar o uso de dados pessoais como nome de cônjuge ou de filhos, as datas de aniversários, endereços, telefones, ou outros elementos relacionados com a própria pessoa. A senha nunca deve ser anotada, sendo recomendável sua memorização.