diritto&diritti dal 1996
diritto.it
direttore Francesco Brugaletta

ISSN 1127-8579

Pubblicato dal 28/02/2017

All'indirizzo http://www.diritto.it/docs/39104-certificado-digital-um-estudo-explorat-rio

Autore: Veyzon Campos Muniz

Certificado digital: um estudo exploratório

CERTIFICADO DIGITAL: UM ESTUDO EXPLORATÓRIO.

DIGITAL CERTIFICATE: A EXPLORATORY STUDY.

Veyzon Campos Muniz[1]

Resumo: O presente artigo tem por escopo apresentar definições e aplicabilidade acerca dos certificados digitais e conceitos afins. Fundado em pesquisa bibliográfica e legislativa, o estudo é dividido em três seguimentos. No primeiro, é abordada a contextualização histórica do certificado digital. No segundo, centra-se na sua conceituação técnica e na exposição da tipologia existente. No terceiro, apresentam-se aplicações dos certificados digitais para a Administração Pública, bem como casos exemplificativos desses instrumentos na experiência comparada (da ONU, da União Europeia e do Mercosul). Por fim, assevera-se como positiva a implementação de certificados digitais como mecanismo de segurança em uma sociedade de conhecimento. **Palavras-chaves:** Certificado digital; conceituação; aplicação.

Abstract: This article presents the definitions and applicability about digital certificates and related concepts. Founded in literature and legal search, the study is divided into three parts. At first, we discuss the historical context of the digital certificate. In second, focuses on the technical concept and exposure of existing typology. In the third, we present applications of digital certificates for Public Administration, as weak as illustrative cases of these instruments in comparative experiences (UN, EU and Mercosul). Finally, it is asserted to be positive for implementing digital certificates as a security mechanism in a knowledge society. **Keywords:** Digital certificate; conceptualization; application.

Introdução

Castells (2002) assinala que a sociedade nas últimas décadas foi substancialmente transformada pela revolução operada no processamento de informações, na geração de conhecimento e nas tecnologias da informação. Esse novo cenário social passou a ser denominado, nessa linha de reflexão, como "sociedade do conhecimento" (knowledge society).

Característicos dessa sociedade, para além da rapidez em que dados são processados e informações são transmitidas, são os riscos a que se expõem os usuários dos meios de comunicação telemáticos. Em face disso, o certificado digital emerge como um

[1] Doutorando junto ao Programa de Doutoramento em Direito Público – Estado Social, Constituição e Pobreza do Instituto Jurídico da Universidade de Coimbra (Portugal). Mestre em Direito e bacharel em Ciências Jurídicas e Sociais pela PUCRS. Especialista em Direito Tributário pela UNIP e em Direito Público pela UCS/ESMAFE-RS. Professor no Curso de Direito das Faculdades Integradas de Taquara (FACCAT).

instrumento de maximização da segurança e da validade jurídica de atos e negócios realizados no âmbito digital.

Posto isto, o estudo teórico de definições e aplicações desses certificados é o que permite aos usuários acessar o conhecimento fundamental para a sua utilização prática. Assim, o presente artigo se ocupa da explicitação conceitual dos elementos que compõe o processo de certificação digital, uma vez que a garantia da confidencialidade e integridade de informações e verificação da autoria de documentos, lançados através da internet, se concretiza a partir dele.

1 Contextualização

Desde sua gênese, nos Estados Unidos, na década de 1990, os certificados digitais são sinônimos de inovação no processo de gestão. A adesão ao processo de certificação digital garante inúmeros benefícios a partir da validação de assinaturas realizada em meios eletrônicos. A troca de informações confidenciais via internet, o comércio eletrônico, os processos administrativos e judiciais eletrônicos, a assinatura de declarações de renda, a obtenção e envio de documentos sem a necessidade de mobilidade física e até mesmo a realização de transações bancárias foram possibilitadas pela implementação desse mecanismo inovador.

No Brasil, somente em 2001 esse processo teve início, com a constituição do ICP- BRASIL, isto é, a infraestrutura de chaves públicas brasileira que instituiu um sistema nacional de certificação digital. A estrutura composta de um ou mais certificadores denominados de autoridades certificadoras desenvolve-se a partir de pares de chaves criptografadas que asseguram o acesso das informações somente ao titular desta identidade virtual. Assim, uma vez que uma pessoa (física ou jurídica) solicita um certificado digital seus dados e transações estão totalmente asseguradas pela autoridade certificadora. É dessa forma que o certificado digital corresponde a uma identidade virtual que permite a verificação inequívoca e segura em alto grau do procedimento realizado eletronicamente.

2 Conceituação

O certificado digital é, assim, uma assinatura com validade jurídica que garante proteção às transações eletrônicas e outros serviços via internet, permitindo que pessoas e

empresas se identifiquem e assinem digitalmente de qualquer lugar do mundo com mais segurança e agilidade. Trata-se de um arquivo eletrônico que identifica quem é seu titular, um verdadeiro "documento eletrônico de identidade".

Exemplifica-se: quando se vai realizar uma transação, de forma presencial costuma-se solicitar um documento que comprove sua identidade. Na internet, como as transações são feitas eletronicamente, o certificado digital surge como forma de garantir a identidade das partes envolvidas. Para poder assinar um documento digitalmente é preciso inicialmente possuir um certificado digital validado por uma entidade homologada no âmbito da ICP-Brasil.

A utilização da certificação digital propicia grandes vantagens como agilidade, redução de custos e segurança, permitindo, assim, que processos sejam não mais realizados pessoalmente ou por meio de inúmeros documentos em papel,e sim feitos totalmente por via eletrônica. Com isso os processos tornam-se menos burocráticos, mais rápidos e por tanto, mais baratos. A certificação digital garante autenticidade e integridade, impedindo que o remetente negue posteriormente que tenha enviado uma mensagem ou autorizado determinada transação. O processo de certificação digital possui status e a validade de um documento propriamente dito.

Ademais, com o aumento progressivo das transações pela internet seja via e-mails, acesso remoto, assinatura eletrônica, entre outros, as preocupações com privacidade e segurança aumentam cada vez mais. Crescem também a quantidade de fraudes e de métodos para que informações sigilosas sejam furtadas e usadas de forma inadequada visando adquirir vantagens ilegais. A utilização do certificado digital é, frente a isso, uma maneira de sanar esta preocupação, pois é uma das ferramentas mais modernas de segurança para proteção pessoal e empresarial.

Os certificados digitais são, por conseguinte, dispositivos que incrementam e acrescentam uma série de recursos de segurança da informação. Qualidade essa que tem se tornado cada vez mais importante para qualquer pessoa que utilize a rede em seu cotidiano. O aperfeiçoamento desse mecanismo se torna cada vez mais essencial para que possamos usar a internet de forma eficaz e ao mesmo tempo segura.

3 Operacionalidade

Segundo Monteiro e Mignoni (2007), um certificado ou identidade digital é um arquivo digital de computador, que como os demais documentos tradicionais de identificação, além dos dados do indivíduo ou entidade possuem também uma chave pública do assinante. Estes documentos são chancelados digitalmente pela entidade emissora, conhecida como autoridade certificadora, com o objetivo de interligar a chave pública a uma pessoa física ou jurídica, possuindo o mesmo valor do documento físico (tal como uma carteira de identidade, um passaporte, cartões de créditos) e sendo utilizado da mesma forma. Esses documentos de identificação na rede, ao serem apresentados, servem como prova de identificação.

Um certificado digital é formado por um conjunto de campos padrões como, por exemplo, número da versão e número único de identificação do certificado. Além destes campos, um certificado também possui campos de extensões, eles são necessários para definir as funções do certificado, o personalizando. Na prática, o certificado digital funciona como uma carteira de identidade virtual que permite a identificação segura de uma mensagem ou transação em rede de computadores, mas também serve como um mecanismo para a divulgação da chave pública. Assim, em regra, contém os dados de seu titular (nome, e-mail, CPF), chave pública, nome e assinatura da autoridade certificadora que o emitiu.

Por fim, é possível utilizar o certificado digital pela internet, como por exemplo: pagar uma conta, fazer compras sem precisar se locomover, o meio de comunicação através de redes sociais, enviar/receber documentos importantes através de sistemas (que é o meio mais seguro). Assim funciona um certificado digital e são esses os principais benefícios oferecidos para aqueles que preferem e/ou precisam dessa tecnologia.

4 Aplicações

O certificado digital aplica-se aos meios administrativos dando passagem das atividades rotineiras administrativas manuais, com gastos altos e perda de um precioso tempo a uma forma segura, eficaz, econômica e com menor burocracia. É válido dizer que, a certificação digital comporta um leque extenso de pontos específicos passíveis de análise para cada exercício administrativo. Nesse contexto, será demonstrado de forma geral, mas não menos abrangente alguns cases, senão vejamos:

a) Agência Nacional de Saúde Suplementar: adotou a certificação digital em seu projeto de padronização de documentos, o TISS (sistema de troca de informação em saúde suplementar), obrigando todas as operadoras de saúde a usar certificados digitais.

b) Banco Central: se vale do sistema SISBACEN pelo qual o autocredenciamento se dá com certificados digitais próprios.

c) Comércio eletrônico: na compra e venda de produtos via internet, com garantias reais para vendedores e compradores, deve haver o cadastramento em sites com certificação digital.

d) Correio eletrônico (e-mail): o uso de certificados digitais garante a identificação do emissor e a integridade e inviolabilidade do conteúdo da mensagem enviada.

e) Justiça Federal: se utilizado do e-PROC, sistema que permite o envio eletrônico de documentos referentes aos processos, através da internet, sem a necessidade da apresentação posterior dos documentos originais; está implementando o SIMP, sistema integrado de mandado de prisão, mecanismo que possibilita a emissão e o envio de mandados de prisão de maneira; nas perícias judiciais, podem-se protocolar eletronicamente petições, laudos periciais, contestações e todos os tipos de medidas judiciais pertinentes.

f) Justiça do Trabalho: se utiliza do HOMOLOGNET, sistema de homologação das rescisões trabalhistas, projeto que prevê a ratificação das rescisões de contrato de trabalho de forma online e com o uso de certificação digital.

g) Ministério da Educação: no âmbito do Programa Universidade para Todos (PROUNI), a certificação digital é exigida na transação de informações com as instituições de ensino participantes.

h) Receita Federal: vale-se de certificados digitais nos sistemas de aprovação dos cadastros de pessoas físicas e jurídicas (CPF e CNPJ); igualmente, nos procedimentos de consulta à situação fiscal dessas pessoas e de obtenção de cópias e retificações dos documentos de arrecadação de receitas federais (DARFs), declarações do imposto de renda de pessoas jurídicas (DIPJs), declaração de créditos e débitos de tributos federais (DCTFs), e declarações de contribuições sociais (DACONs); no âmbito do SPED, sistema público de escrituração digital, prevê que os dados dos livros diários sejam assinados digitalmente pelo representante legal da empresa e seu responsável contábil; e no âmbito do SISCOMEX, sistema de comércio exterior, determina para as empresas que pretendem negociar

internacionalmente a habilitação e cadastramento de seu responsável legal, mediante uso de certificado digital.

i) Sistema registral: permite consultar ocorrências existentes no registro imobiliário, mediante autenticação com uso de certificados digitais; no registro de contratos sociais e alterações de sociedades simples, com utiliza integralmente certificação digital.

5 Experiências comparadas

Bertol (2009) afirma que a regulamentação sobre assinaturas e certificados digitais é um processo complexo, que envolve o desenvolvimento de normas e padronização, por órgãos oficiais ou independentes, até a incorporação dessas diretrizes na legislação dos países. Na experiência brasileira, se observa que o Decreto (presidencial) n. 3.505 institui, em 2000, a Política de Segurança da Informação na Administração Pública Federal, sendo assim um antecessor da já referida Medida Provisória n. 2.200-2 que, no ano seguinte, criou a infraestrutura de chaves públicas brasileira.

Entretanto, é importante destacar que experiências em âmbito internacional foram de grande influência na implementação da certificação digital no Brasil. O modelo jurídico de incremento de assinaturas eletrônicas (ONU, 2001) proposto pela Organização das Nações Unidas é exemplificativo.

A referida organização internacional, na qual seus Estados membros partilham de interesses a fim de enfrentar problemáticas socioeconômicas e relativas à segurança internacional, apresentou recomendações quanto ao processo de certificação digital. Conforme indica Garcia (2004), em 1996, a UNCITRAL (United Nations Commission On International Trade Law), comissão atinente ao Direito Comercial Internacional, visando estabelecer diretrizes para o uso dos meios eletrônicos de comunicação que pudessem ser adotados por países com diferentes sistemas jurídicos e socioeconômicos, instituiu a chamada Lei Modelo sobre Comércio Eletrônico.

O modelo foi marco legal importante tanto por estabelecer regras gerais de regulamentação das relações comerciais por via eletrônica, quanto por fomentar a aceitação, em plano mundial, dos certificados e assinaturas digitais. Na esteira do contributo das Nações Unidas, as uniões comerciais latu sensu, paulatinamente, passaram a adotar normas gerais de

padronização da certificação digitais, com o objetivo de facilitar o e-commerce entre seus países membros.

A União Europeia, enquanto gestão pública comunitária, na qual as decisões políticas e econômicas são compartilhadas pelos Estados membros, a aplicação dos certificados digitais, inicialmente, esbarrou no problema da ausência de padronização para o mercado comum. Nos anos 1980 e 1990, alguém que tivesse um certificado digital alemão não poderia contratar ou vendar com alguém, seja pessoa física ou jurídica, pública ou privada portuguesa ou belga, por exemplo. Assim, com a Diretiva n. 93/1999, o Conselho Geral e o Parlamento Europeu estabeleceu uma normatização legal para as assinaturas eletrônicas, em consonância com o modelo ONU.

Por sua vez, o Mercosul, união aduaneira que não apresenta uma gestão pública compartilhada, somente em 2006, apresentou uma diretiva normativa referente a certificação digital. Considerando o desenvolvimento contínuo de tecnologias de informação e comunicação a serviço da consolidação e desenvolvimento socioeconômico dos seus países membros editou a Resolução n. 37/2006, pela qual reconheceu a eficácia jurídica dos documentos eletrônicos, assinaturas eletrônicas e certificados digitais no âmbito do Mercosul, determinando a incorporação das normas nos ordenamentos nacionais.

Contudo, no Brasil ainda não há lei específica tratando dos documentos eletrônicos, assinaturas e certificados digitais. As normas existentes no país dão conta do processo de certificação em sede de normas infra-legais, guiando-se pelo marco regulatório da medida provisória relativa as chaves públicas.

Por conseguinte, mesmo sem legislar especificamente sobre a matéria, percebe-se que há uma crescente atenção à popularização das transações pela internet, fenômeno que impõe à Administração Pública a implementação de mecanismos de segurança, forte na confidencialidade e integridade das informações certificadas digitalmente.

6 Conclusões articuladas

1. Desde logo, cumpre referir que as vantagens do processo de certificação digital se referem à agilidade nas transações, a redução de custos, a diminuição de burocracia, melhoria de gestão de qualidade e, sobremania, a garantia de autenticidade e integridade dos documentos eletronicamente transmitidos.

2. O processo de criação do certificado digital como ferramenta para uso da rede é essencial para o aumento da informatização com segurança. Ao mesmo tempo, o estudo desse instrumento enquanto aperfeiçoamento é importante para que se possa usar a internet de forma cada vez mais segura e eficaz.

3. Conclui-se, ainda, que os certificados digitais funcionam de uma maneira segura e sigilosa, com dados, validade de documento e responsabilidade. O meio de reconhecer os dados é a criptografia, fazendo com que o certificado digital se torne um documento totalmente seguro. Sendo assim, em compensação, os benefícios que tem trazido são muitos, como: pagamento de contas, compra de produtos, envio de documentos importantes através de sistemas, comunicação e internet, facilitando a vida dos cidadãos que optam por essa tecnologia.

4. No tocante à gestão pública, a certificação digital corresponde àquela atividade de reconhecimento (em meio eletrônico) que facilita quase todas as transações administrativas. Na seara administrativa é preciso poupar o tempo empregado, com atenção a segurança e confiabilidade das operações, dentro de cada estrutura e frente a limitações operacionais e técnicas existentes. O certificado digital, nesse contexto, agrega qualidade a processos e organizações (como p.ex. Agência Nacional de Saúde Suplementar, Banco Central, comércio e correio eletrônicos, Justiças Federal e do Trabalho, Ministério da Educação, Receita Federal, e sistema registral), constituindo-se como instrumento relevante ao administrador, público e privado.

5. Percebe-se que o modelo de regulamentação de certificação digital proposto pela ONU na década de 1990 é, ainda hoje, a principal orientação sobre a matéria. A União Europeia apresenta norma, desde 1999, seguindo tal padrão. O Mercosul, ao seu turno, regulamentou o assunto em 2006. O Brasil, membro da ONU e integrante do Mercosul, entretanto, não adotou medida legislativa para tratar da certificação digital, valendo-se de normas infra-legais, do Executivo, que viabilizam o processo técnico de certificação digital no país.

Referências

BERTOL, Viviane Regina Lemos. **Uma proposta para regulamentação da certificação digital no Brasil.** Brasília: UnB, 2009. [tese de doutorado]

BRASIL. **Medida Provisória n. 2.200-2**, de 24 de agosto de 2001. Disponível em: [http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm]. Acesso em: 20 set. 2014.

CASTELLS, Manuel. **La dimensión cultural de la internet.** Barcelona: UOC, 2002. Disponível em: [http://www.uoc.edu/culturaxxi/esp/articles/castells0502/castells0502.html]. Acesso em: 29 set. 2014.

GARCIA, Flúvio Cardinelle Oliveira. **Da validade jurídica dos contratos eletrônicos.** Teresina: Jus Navigandi, 2004. Disponível em: [http://jus.com.br/artigos/4992]. Acesso em: 29 set. 2014.

LINK, Fábio. **Operações com certificados digitais.** Guaíba: UERGS**,** 2011**.** [trabalho de conclusão de curso].

MERCOSUL. **Resolução n. 37**, de 18 de julho de 2006. Disponível em: [http://www.sice.oas.org/trade/mrcsrs/resolutions/Res3706p.pdf]. Acesso em: 20 set. 2014.

MONTEIRO, Emiliano; MIGNONI, Maria Eloisa. **Certificados digitais: conceitos e práticas.** São Paulo: Brasport, 2007. [versão digital]

ONU. **Resolução n. 51/162**, de 16 de dezembro de 1996. Lei Modelo da UNCITRAL sobre comércio eletrônico. Disponível em: [http://www.lawinter.com/1uncitrallawinter.htm]. Acesso em: 20 set. 2014.

UNIÃO EUROPEIA. **Directiva n. 93**, de 13 de dezembro de 199. Disponível em: [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:ES:PDF]. Acesso em: 20 set. 2014.