ARTICLE:

# ELECTRONIC SIGNATURES AND COURT PROCEEDINGS IN BRAZIL

WRITTEN BY:
**PROFESSOR CARLOS ALBERTO ROHRMANN**

**Electronic and digital signatures are regulated by law in Brazil. Provisory Measure n. 2.200 of August 24, 2001, created the Brazilian Public Key Infrastructure – PKI Brazil. This article explores the concepts of digital and electronic signatures under a comparative analysis in order to present some of the most relevant points of the Brazilian Provisory Measure that regulates the issue. After setting out the law, the ongoing debate will be discussed about the use of electronic signatures for signing written documents that lawyers file in their everyday practice before the courts in Brazil.**

## Introduction

Brazilian law regulates electronic signatures and digital signatures through the Medida Provisória Nº 2.200-2, de 24 de Agosto de 2001 Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências (MP2.200-2), and this provisionary measure remains valid under the status of a federal statute until the Brazilian Congress rejects it or converts it into a federal statute.

It is assumed that 'electronic signature' is a term that refers to any technical method of legally identifying the parties in the on-line world, and the term digital signature refers to a type of electronic signature that is generated through the asymmetric encryption software. MP2.200-2 regulates both forms of signature.

This article analyses the most recent developments regarding the use of digital signatures for filing legal documents before courts in Brazil. The concept of digital signatures will be briefly reviewed within a comparative perspective (taking the U.S. law as a parameter), and a number of points relating to MP2.200-2 will be discussed. The article will finally address the use of electronic signatures before Brazilian courts, in which it is concluded that digital signatures in Brazil are as legally valid as a civil signature, but do not always work as traditional handwritten signatures. It is with this changing concept that the courts continue to struggle with.

## Digital signatures under a comparative perspective

The law often requires a document to be signed in Brazil. For example, in the United States, both physical commercial transactions and electronic commercial transactions that deal with the sale of goods must also comply with the Statute of Frauds.[1] As defined in article 2 of the U.C.C.,[2] the requirement that a contract must be in a written form was not created as a formality to make traders' lives more difficult. The idea is to provide security for all the parties involved in a commercial transaction. Once the contract has been written and signed, the record might be used afterwards as proof of the intention of both parties.

The concept of the digital signature can be drawn from the law or from the work of legal scholars. Digital signatures are defined as a seal affixed to an electronic document that is generated by a hash algorithm, which uses as an input the original electronic document and the signer's private signature key. The use of the key is capable of asserting that the person whose key it was, is the person that caused the digital signature to be affixed to the electronic document. Digital signatures are capable of guaranteeing the integrity of the data.

The method used to generate digital signatures is relatively simple. The sender encrypts the e-mail with their private key. An encrypted seal is generated and added to the message, which is then sent to the recipient. The recipient decrypts the message with the sender's public key. If the decryption process runs

[1] *U.C.C., Article 2, § 2-105.*
[2] *U.C.C., Article 2 - Sales - § 2-201.*

*The signer has a guarantee that the electronic document has not been altered, because if the statement is modified, then the public key will not work properly when verifying the digital signature.*

perfectly, then it can be said with certainty that a person who used the private key signed the message. In order to link the name of the sender with their private key, the system relies on a certificate issued by a trusted third party, a Certification Authority. Where the recipient receives both the message and the certificate issued by the Certification Authority, then the recipient can be certain that the electronic document is legally binding if the owner of the private key caused the key to be used to sign the document.

The Law entrusted the authority to issue a certificate to a third party, known as a Certification Authority – the CA, as we see, for example, from the Brazilian[3] Law, MP 2.200, article 6:

"Art. 6o Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações".

"Article 6. The CAs (the entities which are entitled to issue digital certificates which bind pairs of cryptographic keys to a respective holder) are to issue, dispatch, distribute, revoke and control the certificates, as well as to put at the disposition of the users lists of revoked certificates and other regarding information pertaining the matter. They should also keep records of their actions".

The signer has a guarantee that the electronic document has not been altered, because if the statement is modified, then the public key will not work properly when verifying the digital signature. In other words, any alteration of any character in the electronic document demonstrates that the content of the document has been altered since it was signed with a digital signature, and reduces the legal validity of the document.

## The Brazilian MP .200-2

MP 2.200-2 created the Brazilian Public-Key Infrastructure – PKI Brazil. Under the terms of the MP 2.200-2, the PKI Brazil has a Root Certification Authority (RCA). The RCA, among other tasks, is responsible for issuing digital certificates to certify the other certification authorities, the CAs. The cryptographic keys used by the Brazilian RCA can be as big as a 2048-bit key.[4] The RCA is the National Institute of Information Technology, the ITI, a federal agency that is subordinated to the Ministry of Science and Technology. The ITI is responsible for auditing the work of the CAs, and the MP 2.200-2 authorizes the ITI to apply fines to the CAs. The PKI Brazil is structured under a hierarchical model that has the Brazilian Federal Government at the top of the certification process. Those CAs that are certified by the RCA are legally considered to be CAs in the PKI Brazil.

CAs are the ones that issue digital certificates to the final user. MP 2.200-2 also created the register authorities – RAs that are responsible for identifying the final user. The RAs are operationally associated with the CAs, under the terms of article 6 of the MP 2.200-2:

"Art. 6o Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados,

[3] *See also Comitê Gestor da ICP Brasil, Resolução n. 21 de 29 de agosto de 2003 (http://www.icpbrasil.gov.br/), that "alters the Declaration of Practices of Certification of the CA – Root of ICP Brazil – also alters the Criteria and Proceedings to Entrust the Entities which Participate in the ICP Brazil, the Minimum Requisites for the Policy of Certification at the ICP – Brazil and the Minimum Requisites for the Declaration of Practices of Certification of the Certification Authorities of ICP - Brazil.": "Altera a Declaração de Práticas de Certificação da AC - Raiz da ICP - Brasil, os Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP - Brasil, os Requisitos Mínimos para as Políticas de Certificado na ICP - Brasil e os Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP - Brasil."*

[4] *FABIANO MENKE, ASSINATURA ELETRÔNICA NO DIREITO BRASILEIRO (SÃO PAULO: ED. RT, 20005, P. 47).*

bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento".

"Article 6. The CAs (the entities which are entitled to issue digital certificates which bind pairs of cryptographic keys to a respective holder) are to issue, dispatch, distribute, revoke and control the certificates, as well as to put at the disposition of the users lists of revoked certificates and other regarding information pertaining the matter. They should also keep records of their actions.

Paragraph – The owner will always generate the pair of cryptographic keys and its signing private key will be under his exclusive control, use and knowledge".

When the final user wishes to generate a pair of cryptographic keys, they must identify themselves with a valid form of identity (the identity card and the card that has the number of the person before the Brazilian Internal Revenue Service), in person, before a RA.[5] Once the RA is satisfied of their identity, the final user will be able to generate the pair of cryptographic keys. The final user will always keep the private key. It is for this reason that there is no private key escrow requirement in Brazil.

MP 2.200-2 allows that both forms of public electronic document (such as those issued by the government) and private electronic document can be accepted with an electronic signature. Public electronic documents, under the terms of article 11 of the MP 2.200-2, which reads as follows:

"Art. 11. A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei n 5.172, de 25 de outubro de 1966 - Código Tributário Nacional".

"Article 11 – The use of electronic document for tax purposes must comply with the terms of article 100 of Law nº 5.172, of 25 of October of 1966 – National Tax Code".

Electronic documents can also be used for tax purposes, providing the electronic document complies with the terms of the rules in the Código Tributário Nacional – the National Tax Code.[6] It is interesting to note that the Brazilian judiciary, even before the passing of MP 2.200-2, had ruled valid a tax document issued by the tax authorities in electronic format.[7] There is no specific topic in MP 2.200-2 regarding the filing of legal electronic documents before courts in Brazil, thus electronic filing of documents before courts are therefore not prohibited.

Article 10 of MP 2.200-2 regulates the effects of electronic signatures:

"Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 10 As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei n 3.071, de 1 de janeiro de 1916 - Código Civil.

§ 20 O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento".

"Article 10 –The electronic documents referred to by this Provisionary Measure are considered as public documents as well as private documents, for all legal purposes.

§ 1 Declarations made upon electronic documents produced within the ICP – Brazil's certification process are to be considered trustworthy as to the authenticity of the signer, in accordance with Article 131 of Law nº 3071, of January 1st, 1916 (Brazilian Civil Code).

§ 2 This Provisionary Measure does not prevent other means of proving the authorship and integrity of electronic documents. This Provisionary Measure also does not prevent the use of certificates that are not

[5] *Instituto Nacional de Tecnologia, ITI, for a list of the CAs and of the RAs that belong to the ICB-Brasil on 25. Oct. 2005: http://www.iti.gov.br/.*

[6] *Código Tributário Nacional, art. 100, about the complementary tax norms to the law, such as the acts of the tax authorities, decisions of the administrative tax authorities: "Art. 100. São normas complementares das leis, dos tratados e das convenções internacionais e dos decretos:*
*I - os atos normativos expedidos pelas autoridades administrativas;*
*II - as decisões dos órgãos singulares ou coletivos de jurisdição administrativa, a que a lei atribua eficácia normativa;*
*III - as práticas reiteradamente observadas pelas autoridades administrativas;*
*IV - os convênios que entre si celebrem a União, os Estados, o Distrito Federal e os Municípios.*
*Parágrafo único. A observância das normas referidas neste artigo exclui a imposição de penalidades, a cobrança de juros de mora e a atualização do valor monetário da base de cálculo do tributo."*

[7] *Tribunal de Justiça de São Paulo, TJSP, AgIn 105.464.4/7-SP, Rel. Des. Cesar Lacerda; j. 17 March 1999, 8a. Câmara de Direito Privado.*

issued by the ICP – Brazil, where their use is regarded as valid by both parties or accepted by the person to whom the document is supposed to be presented".

Section 1 of article 10 establishes that the declarations in electronic documents made under the certification model of the PKI Brazil are presumed valid in relation to the signer under the terms of the Brazilian Civil Code, article 219, which establishes that:

"Art. 219. As declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários".

"Art. 219. The declarations in documents signed are presumed to be valid in relation of the signers".

In other words, in Brazil, a digital signature with a digital certificate issued by a CA that belongs to the PKI Brazil (that has the Brazilian ITI as its root certification authority) brings about the same effects as a civil signature.

Section 2 of article 10 allows for the parties to use other forms of electronic signature and data integrity that are not within the PKI Brazil, such as using a CA that is not certified by the Brazilian Root Certification Authority. However, under the terms of section 2, the parties involved in the electronic transaction must agree that the chosen procedure is valid. Moreover, a third party that was not involved with the electronic document produced outside the PKI Brazil can repudiate the electronic document if they do not agree with the type of the electronic signature used.[8]

## Electronic signatures in court

The use of electronic documents by practitioners for filing legal documents before the judicial authorities in Brazil remains an ongoing debate. Even though there are many experienced in the so called "federal special civil courts" (Juizados Especiais Federais) – courts that only hear cases not worth more than 60 Brazilian Minimum Wages (R$18,000.00) – the use of electronic documents as an everyday practice before the courts is not common at present. The federal statute that regulates the Federal Special Courts is Lei n. 10.259 de 12 de julho de 2001, Dispõe sobre a instituição dos Juizados Especiais Cíveis e Criminais no âmbito da Justiça Federal. Article 8, section 2, allows that "Courts organize services to communicate with the parties and to receive petitions through electronic means".[9] What is done in practice, is to enroll lawyers in the electronic system of the court and to generate a password for the use of the lawyer. When lawyers want to file a petition, they log into the system with their username and password.[10] This is a solution that uses passwords and personal identification numbers as electronic signatures. This is a more simple way to implement electronic filing of legal documents before courts, but it is not as secure as using digital signatures.

The Brazilian Rules of Civil Procedure (Código de Processo Civil) adopts the principle of the liberty of forms for legal documents, but there are requirements regarding some acts of attorneys that must be in writing and signed with a manuscript signature. For example, Lei Nº 9.800, de 26 de Maio de 1999 "Permite às partes a utilização de sistema de transmissão de dados para a prática de atos processuais" introduced the legal possibility of the use of data communication systems (such as facsimile transmissions) to file legal documents related to judicial acts that must be performed in writing. Law n. 9.800/99 does not require courts to install the technical infrastructure in order to allow lawyers to file their documents electronically. Of course, that would be a process that would take time and demand public investment. Throughout the past six years, courts have invested in information technology in such a way that Law n. 9.800/99 has become increasingly used by lawyers (even though facsimile transmissions are still the most used resource in this field). As an example, in the case of EDAGA 389941/ SP, embargos de declaração no agravo n. 2001/0062036-2 decided by the Superior Tribunal de Justiça (Superior Court of Justice in Brasília), it was held that:

I – Article 1st of Law n. 9.800/99 allows the parties to use data transmission system such as facsimile or another for acts that require written document.

II – It is valid, as an act of the lawsuit, the petition that was sent through e-mail (Internet), when the original document, properly signed, is filed up to five days after the end of the term).[11]

[8] *CARLOS ALBERTO ROHRMANN, CURSO DE DIREITO VIRTUAL (BELO HORIZONTE: ED. DEL REY, 2005, P. 87).*

[9] *Lei n. 10.259/2001, art. 80, §2º: "Os tribunais poderão organizar serviço de intimação das partes e recepção de petições por meio eletrônico".*

[10] *Tribunal Regional Federal da Terceira Região available in electronic format at https://www.trf3.gov.br/upet2.php.*

[11] *Superior Tribunal de Justiça, EDAGA 389941/SP, embargos de declaração no agravo n. 2001/0062036-2. Published on DJ of 16 June 2003, p. 00263, Relator Min. Humberto Gomes de Barros:*
*"I - O art. 1º, da Lei 9.800/99, outorga às partes a faculdade de utilizar sistema de transmissão de dados e imagens tipo fac-símile ou outro similar, para a prática de atos processuais que dependam de petição escrita.*
*II - É plenamente eficaz, como ato processual, a petição remetida por correio eletrônico (Internet), quando os originais, devidamente assinados, são entregues até cinco dias da data do término do prazo recursal. Inteligência da Lei n.º 9.800/99."*

With the passing of MP 2.200-2, the debate about the use of digital signatures in court has gained much importance. There were some attempts to use digitalized signatures for filing legal documents that were rejected by the Brazilian Supreme Court.[12] In one case, a lawyer filed an appeal before the Brazilian Supreme Court using a digitalized signature. The Supreme Court Judge rejected the petition by deciding that that only when the lawyer has signed the document is it valid.[13] But, despite the decision in this case, more recently, the Brazilian Supreme Court implemented electronic filing models that require attorneys to fill in an application form before the court and then grant access through a PIN system.[14]

The Superior Court for Labour Cases (the "TST") has issued a regulation for filing electronic documents (Instrução Normativa n. 28 IN 28 – Normative Instruction n. 28 NI 28 that created the "e-Doc").[15] The TST requires attorneys to use digital certificates that are issued by a certification authority, which belongs to the PKI-Brazil (IN 28, art. 4: "Art. 4º O acesso ao e-DOC depende da utilização, pelo usuário, da sua identidade digital, a ser adquirida perante qualquer Autoridade Certificadora credenciada pela ICP-Brasil, e de seu prévio cadastramento perante os órgãos da Justiça do Trabalho." – "Access to the e-DOC depends upon the use, by the users, of their digital identity, to be acquired before any Certification Authority that belongs to the ICP-Brasil, and of their previous filing before the Labour Courts"). Even though this seems to be a safety requirement for the system, and complies with the terms of MP 2.200-2, the Brazilian Bar Association does not agree with the requirement. The Bar argues that the requirement for lawyers to have their digital identities issued by a CA within the ICP-Brasil, that has as its root Certification Authority a Federal Agency that is not the Bar is against articles 13 and 54, X of the law of the Bar, Federal Statute n. 8.906 (Lei n. 8.906, de 4 de julho de 1994 – Dispõe sobre o Estatuto da Advocacia e a Ordem Dos Advogados do Brasil – OAB). The Brazilian Bar Association claims it is the only legally entitled association to issue identity for attorneys. Therefore Brazilian lawyers would have to use digital certificates issued by the Brazilian Bar Certification Authority that is not subordinated to the ITI (the Root Certification Authority created by MP 2.200-2). The Brazilian Bar Certification Authority already exists and it is known as the ICP-OAB, and it is not within the PKI-Brasil, the ICP-Brasil.[16] The Brazilian Bar argues that it cannot be legal to require lawyers to buy digital certificates from other CAs rather than using the digital certificates of the ICP-OAB, as this would be an extra cost for lawyers who want to file electronic documents before the court.[17]

The Brazilian Bar Association has filed a complaint before the Brazilian Council of Justice, which has a fiscal rule over the judiciary, in order to challenge the requirement of the Normative Instruction n. 28 of the TST.[18] If the complaint prevails, courts will have to accept digital certificates issued by the separate Brazilian Bar Association CA, the ICP-OAB, which is outside the scope of the PKI Brazil.

## Conclusion

Digital signatures are being used more and more in Brazil. Both the public sector and private entities are moving towards the acceptance of the PKI – Brazil. The use of electronic signatures for signing documents that are filed before courts is likely to move towards the digital signature model. Some issues related to the Brazilian Bar Association's CA outside the PKI Brazil are still being addressed by the National Council of Justice and the answer is imminent. Other lower courts are likely to be waiting for that decision before accepting electronic petitions with digital signatures.



*Carlos Alberto Rohrmann is Professor of Law at Faculdade de Direito Milton Campos, FDMC (Brazil) and is the author of Curso de Direito Virtual, (Ed. Del Rey, 2005) 'Course of Cyberlaw', a book about cyberlaw in Brazil. Professor Rohrmann holds a Doctorate in the Science of Law (UC Berkeley, USA).*

**rohrmann@bis.com.br**
**http://www.mcampos.br**
**http://www.direitodarede.com.br**

[12] *RMS (AgR) 24.257-DF, rel. Min. Ellen Gracie, August 13, 2002.*

[13] *Id., Petição por Meio de Assinatura Digitalizada. A Turma negou provimento a agravo regimental em que se pretendia a reforma da decisão proferida pela Ministra Ellen Gracie, relatora, que negara seguimento a recurso ordinário em mandado de segurança, por haver sido ele interposto por meio de cópia reprográfica. Alegava-se, na espécie, que a petição constante dos autos não seria uma cópia reprográfica, mas sim uma petição com assinatura digitalizada, sustentando-se, assim, o processamento dos autos, com base no art. 1º, da Lei 9.800/99 ("É permitida às partes a utilização de sistema de transmissão de dados e imagens tipo fac-símile ou outro similar, para a prática de atos processuais que dependam de petição escrita."). A Turma, salientando que a jurisprudência firmada na Corte é no sentido de que apenas a petição em que o advogado tenha originalmente firmado a sua assinatura tem validade reconhecida, afastou a aplicação do mencionado art. 1º da Lei 9.800/99 à espécie, à consideração de que determinados meios decorrentes da modernidade, tal como a assinatura digitalizada, precisam ser normatizados antes de serem postos em prática.*

[14] *Brazilian Supreme Court, e-STF, Res. n. 287 of April 14, 2004.*

[15] *Tribunal Superior do Trabalho, TST, Instrução Normativa n. 28, http://www.trt4.gov.br/edoc/in28tst.htm.*

[16] *OAB, Infraestrutura de Chave Pública – ICP OAB http://cert.oab.org.br/.*

[17] *OAB, OAB pede a CNJ medida contra terceirização da certificação http://www.oab.org.br/noticia.asp?id=4954.*

[18] *Conselho Nacional de Justiça – CNJ, Pedido de providências n. 349, filed 05 Sep. 2005: http://www.cnj.gov.br/acompanhamentoprocessual/faces/jsf/consultarandamentoprocessual/ConsultarProcesso.jsp.*