Electronic Certification in Brazil and in the European Union

RICARDO BARRETTO FERREIRA DA SILVA AND JOSÉ LEÇA

This article seeks to combine the transnational context of electronic commerce with the need to extend security to electronic transactions supported by electronic documents. More specifically, we propose to evaluate the treatment given to electronic signatures by the European block, comparing it with the treatment afforded to the matter in Brazil, enabling us to evaluate how the different systems for the extension of the authenticity and validity of electronic documents can 'converse', to the effect of admitting their mutual validity.

The EU Directive [1]

On 13 December 1999, the European Community adopted Directive 1999/93/CE, which basically establishes the legal framework for according legal validity to electronic signatures in Europe.[2] The Directive came into force on 19 January 2000. This Directive regulates, among other things, (i) the electronic signature, (ii) the signature-creation device and (iii) the electronic certificate, establishing a system based on two forms of electronic signature and the concept of a 'qualified certificate'.

For each element, there are different regulatory levels and security requirements. A total technological 'exemption' policy is adopted and different security levels apply to the two forms of electronic signature.

■ Electronic Signature

The two forms of electronic signature are defined in article 2 as follows:

- **electronic signature** "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication"[3]
- **advanced electronic signature** "an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that."[4]

■ Electronic signature-creation devices

The Directive also regulates the way in which an electronic signature is created. In fact, if the electronic signature is a sequence of data that serves to give authenticity to a document, its creation method is relevant. There are two types:

- **Signature-creation device**, meaning a "configured software or hardware used to implement the signature-creation data".[5] and
- **Secure signature-creation device**, a "signature-creation device which meets the requirements laid down in Annex III;"[6]

■ Certificates

The Directive establishes that certificates aim to confirm the identity of the person who uses the electronic signature. There are two classes of certificates, which abide by different security requirements and regulations:

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ 19.1.2000 L13/12).
[2] This and other citations in connection with the Directive were based on the English version of this document, available from http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf (visited on 11.09.2004).
[3] Article 2(1).
[4] Article 2 (a), (b) and (c).
[5] Article 2(5).
[6] Article 2(6) (Annex III carries some objective criteria to guarantee that the way in which the electronic signature was created has a high security level.)

- **Certificate** "an electronic attestation which links signature-verification data to a person and confirms the identity of that person".[7]
- **Qualified certificate** "a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II".[8]

■ Legal Effects of electronic signatures

Let us then look at how the elements mentioned thus far (the electronic signature, the electronic certificate and signature-creation device) interrelate and the legal consequences of this.

The regime for extending legal validity to electronically signed documents is adopted by the Directive in a gradual manner, that is by using different mechanisms to create an electronic document will grant it a different legal status. This gradation commences with the electronic signature. Basically, its use will ensure the validity of the electronic document as evidence for procedural purposes; that is to say, its validity may not be denied due to the simple fact of (i) being presented in electronic form, or (ii) not being based on a qualified certificate, or (iii) not being based on a qualified certificate issued by a qualified certification service provider, or (iv) not having been created through a secure signature-creation device.[9]

The 'simple' electronic signature provides for the flexibility of the confirmation of authorship and integrity – it does not submit its validity to the condition of a given closed technology or methodology. By using any type of electronic signature, as defined in the Directive, the electronic document may be used in the courts as evidence. This authentication implies, it is true, the use of some kind of signature-creation data and some kind of signature-creation device – secure or not, since intrinsically related to the actual existence of the electronic signature. But nothing more: using any type of electronic signature, as defined in the Directive, the electronic document may be used in the courts as evidence.

But like any evidence, the electronic signature may be challenged: questions of the authorship, integrity, validity of declarations and all other circumstances that compromise legal acts in general may be challenged, whether through expert examination, or other evidence permitted by law and that refute the validity of the document. Therefore, depending on the transaction, it may be important to establish a solid method of procedures capable of conferring the authenticity of electronic documents: the weaker the system adopted, the easier it is for it to be disputed in court.[10]

If the validity of the electronic document as evidence is guaranteed, then, by the Directive, even to non-advanced electronic signatures, what is the difference of the legal regime assigned to advanced electronic signatures?

The difference is that, in accordance with article 5(1)(a) of the Directive, the adoption of a qualified electronic signature – based on a qualified certificate, and created through secure signature-creation devices – complies with the legal requirements of a signature as regards the data in digital form, as a hand written signature abides by the legal requirements in relation to hand written data. This provision of the Directive thus puts the digital signature on the same footing as the hand written signature, attributing it the same legal status. In addition, and as might be expected, the advanced electronic signature is also admitted as evidence in legal proceedings.

Hence, it is concluded that the electronic signature can have three security gradations, of which the electronic signature is the least sophisticated, followed by the advanced electronic signature, which has the attributes established in article 2(2) of the Directive. Finally, by adopting an advanced electronic signature that is confirmed by a qualified certificate and also produced by a secure signature-creation device, this signature will, broadly speaking, acquire the status of a hand written signature, which we could call the 'qualified' electronic signature.

■ Certification service providers

By and large, the Directive establishes that the Member States shall neither submit the provision of certification services to prior authorization and nor will there be limits on the number of providers. In addition, accreditation regimes are optional. Exception is made to the providers that issue qualified certificates, which are subject to tighter regulation and control.

This provision of the Directive thus puts the digital signature on the same footing as the hand written signature, attributing it the same legal status

[7] Article 2(9).
[8] Article 2(10).
[9] Article 5(2).
[10] Naturally the robustness of the system is directly associated to the type of transaction that the electronic signature supports. It would make no sense to use a system with a maximum level of sophistication and at an exorbitant cost for the simple purpose, for example, of making a purchase of a modestly priced product, or to obtain access to a given site on the internet.

It is important to mention that the service providers that issue qualified certificates (and only these) are subject to the control of the Member State in which the entity is established.[11] Thus, the Directive does not allow for the attribution of qualified certification entity status to providers that are not located in a Member State. The exception is in article 7 of the Directive, as commented below.

■ International Aspects

We have seen then that it is necessary for a qualified certification provider entity to be located in a Member State. We have also seen that the non-qualified certificates are valid, even if the certification entity that issued them is not located in a given Member State. But what about advanced certificates? How does one ensure their validity even when generated outside the region of the European block?

Article 7 of the Directive establishes that, unless based on an international bilateral or multilateral agreement, the certificates issued by qualified certification service provider entities that are not established in a Member State, or that have their certificates guaranteed by a service provider located (and accredited under an optional accreditation regime) in a Member State, will not be valid. Accordingly, the Directive admits cross validity of advanced certificates; but it depends on the existence of a specific international agreement.

MP 2.200-2, of August 24, 2001

■ Introduction

Prior to 2001 there were no specific rules in Brazil regulating the electronic signature, in the sense of a regulation that legally guaranteed the authorship and integrity of electronic documents. It was Provisional Executive Act 2.200-2, of August 24, 2001 (MP 2200) that regulated the matter. For this purpose, it created the Brazilian Public Keys Infrastructure – PKI Brazil, based on the use of public and private cryptographic keys issued within the scope of PKI-Brazil, without, however, dismissing the legal recognition of other electronic authorship and integrity control systems, albeit under a differentiated regime.

PKI-Brazil means the Brazilian Public Keys Infrastructure. MP 2200 establishes the basic framework for this infrastructure, creating the necessary conditions for the extensive regulation that followed it.[12]

When we analyzed the Directive we are able to identify, in accordance with the definitions and with the respective legal treatments, how the different necessary elements for the extension of legal validity interrelate – whether for the purposes of evidence, or for the purposes of the fulfillment of the manuscript signature requirements.

The Brazilian system also maintains a progressive regime for granting legal validity to electronic documents, but with a different focus – and with different consequences. While the European legislation refers to (i) the non-discrimination of the electronic document (in relation to the document on paper), and (ii) the fulfillment of the manuscript signature requirements through an electronic signature, Brazilian legislation focuses, essentially (i) on the legal assignment of authorship and integrity of documents and (ii) on the validity sphere of this assignment (only between the parties).

■ Legal treatment of the electronic signature

■ Article 10 of MP 2200

MP 2200 guarantees the legal validity of digitally signed documents in Brazil in two fields: (i) documents produced within PKI-Brazil and (ii) documents produced outside PKI Brazil. The legal basis for this differentiation is in article 10:

Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.	Art. 10. For all legal purposes, public or private documents are construed as the electronic documents referred to in this Provisional Executive Act.

[11] Article 3(3).

[12] There are presently already 31 Resolutions issued by the Management Committee of ICP-Brazil, as well as Ordinances, Orders and other administrative measures. The regulations establish the certification entity policies, security and quality standards, admissibility requirements, operating methodology of the entity members of ICP-Brazil, such as the certification authorities, registration entities, Root Certification Authority, security issues, and many others.

§ 1o 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.	Paragraph 1 The declarations contained in electronic documents produced with the use of the certification process provided by PKI-Brazil are presumed true in relation to the signatories, in the manner of art. 131 of Law 3.071, of January 1, 1916 – Civil Code.[13]
§ 2o 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.	Paragraph 2 The determinations in this Provisional Executive Act do not preclude the use of other evidence of the authorship and integrity of documents in electronic form, including those that use certificates not issued by PKI-Brazil, provided that admitted by the parties as valid or accepted by the person for whom the document is intended.

■ Common element: authorship and integrity

Paragraph 2 of article 10 establishes the minimum parameters for granting validity to an electronic document, even when PKI-Brazil is not adopted: authorship and integrity, provided that the parties accept it. The aim of MP 2200 was to afford flexibility to business transactions to the point of the parties electing the way in which they will ensure the authorship and integrity of electronic documents. Thus, even if a given transaction does not follow the PKI-Brazil methodology, MP 2200 admits the legal validity of the electronic documents that rely on other means of evidencing the authorship and integrity.

The minimum standard is the possibility of evidencing authorship and integrity, provided that admitted by the parties involved. But if it is true that the Law attributes the presumption of veracity relating to declarations contained in a signed document, such presumption will disappear if one of the parties challenges and proves that the signature is linked to a distinct person or entity, or that the document has been changed or altered.[14]

■ Reinforced Authorship and Integrity: PKI-Brazil

As stated previously, the difference between the legal recognition of electronic documents produced outside the sphere of PKI-Brazil and those produced within the mechanics of PKI-Brazil, is its restricted validity scope. Upon using PKI-Brazil, a legal presumption applies to the effect that the person whose signature was used is the author of the electronic document and it remains unchanged as regards its content before third parties.

We have seen above, briefly, that the purpose of Brazilian regulations concerning the electronic signature is different to that of the European Directive: while the Directive establishes (i) the non-discrimination of the electronic document, and (ii) the minimum requirements for the electronically signed document to have the same validity as the manually signed document, MP 2200 simply grants legal validity with respect to the authorship and integrity of the electronic document.

One reason for this difference is that the manifestation of will in Brazil, especially in connection with business and private transactions, as a rule, is not rigid. To this effect, legal transactions do not require a signature to be valid – so much so that many verbal contracts are valid and effective. The validity of a legal transaction is simply associated (i) to the capacity of the agent, (ii) the legality of the object and (iii) the possibility of the form adopted for the transaction.

[13] It is relevant to clarify that the reference made to the Civil Code is outdated, considering that, since 2002, Brazil has adopted a new Civil Code (Law 10.406, of January 10, 2002). The corresponding article in the prevailing code has the following wording: "Art. 219 The declarations contained in signed documents are presumed to be true in relation to the signatories."

[14] The fragility of the method of confirmation of authorship and integrity may thus give space for disputes even between the parties. This is why it is necessary to carefully evaluate the level of security of the document: a more sophisticated authorship and integrity system will be less susceptible to disputes.

Thus, because Brazilian law, as a rule,[15] does not require a manuscript signature for a private transaction to be valid, it would make no sense for the rules that regulate electronic transactions to deal with whether an electronic signature is obligatory. On the contrary, it makes more sense to carry out the validity of legal transactions, the extension of legal validity to authorship and integrity done electronically. All this to justify why Brazilian laws do not carry a provision similar to the one of the Directive (especially with respect to its article 5): the Brazilian digital certification system approved by MP 2200 does not place the existence of the signature itself (or the fulfillment of the manuscript signature requirements) as a validity requirement, but the way in which an electronic document is unchanged and associated to the person that produced it.

We will not be addressing the characteristics of the organic and hierarchical structure or the workings of PKI-Brazil, which subject would justify a separate article. What matters for the purposes of this article is that there is effectively a public key infrastructure in place in Brazil headed by a government entity that occupies the highest hierarchical level within PKI-Brazil, exercising the role of Root Certification Authority. It is the Information Technology Institute (ITI) associated to the President's Cabinet (Presidency of the Republic).

It is also important to mention that MP 2200 determines that a private key issued to users of PKI-Brazil (which permits the issuance of a document within the scope of PKI-Brazil) fully meets the requirements of the European Directive for the advanced electronic signature. Another important aspect of PKI-Brazil is that the Certification Authorities and Registration Authorities belong to PKI-Brazil, in the same way as the certification service providers in Europe, can be both public and private entities.

■ International Aspects

Lastly, it is also important to mention that article 4 of MP 2200 establishes that the Management Committee of PKI-Brazil has authority to identify and evaluate the external PKI policies, negotiate and approve bilateral certification, cross-border certification, interoperability rules and other forms of international cooperation, and to certify, when applicable, their compatibility with PKI-Brazil, observing the provisions in international treaties, agreements and acts; and that deal with international aspects. Thus, Brazilian law admits the validity of other Public Key Infrastructures, provided they are based on international agreements or acts.

Comparative analysis

Having described electronic signatures in Europe and Brazil, it is now possible to make an evaluation to identify to what extent the systems could 'converse' to the effect of mutually recognizing each other.

First, it is interesting to note that both the Brazilian and the European scheme are considered flexible. Indeed, even the less technologically sophisticated documents can have their legal validity guaranteed both in Europe and in Brazil, regardless of any other formality. This is why, in Brazil, any electronic document whose authorship and integrity confirmation system is accepted by the parties will have its legal validity ensured. These documents may be produced outside the country – in Europe, for example – regardless of any registration, certificate, evaluation, storage or any other procedure: between the parties the document will be valid.

On the European side, by and large, an electronic signature may not have its validity denied with basis solely on the fact of its signature being electronic. Thus, considering the electronic signature concept,[16] any authentication method is supposedly valid for the purposes of evidence in legal proceedings, also regardless of any registration, certificate, evaluation or any other procedure.

Both in Brazil and in Europe, the electronic signature in its simplest form requires a very similar security standard (both – in a general and flexible manner – require that there be an authentication confirmation method, except for 'simple' electronic signatures). The difference is in the legal consequence of their effects: in Brazil the electronic signature will guarantee the authorship and integrity of the document only in relation to the parties; in Europe, the consequence will be the non-discrimination of the electronic information –

[15] In Brazil, by and large there is no supremacy with regards to the legal effect, validity or force of documents written on paper with respect to other documents or means of reproduction of a fact or act. In fact, the principle of the liberty of forms prevails in the Brazilian Civil Law, according to which the parties may freely determine, provided that the law does not call for a special form; wherefore, even the manuscript signature may be dispensed with. Note, however, that there are exceptions to this assertion, and that are effectively cases wherein the form is essential for the validity of a document.

[16] Article 2(1) of the Directive 1999/93: Electronic signature – *the data in electronic form linked or logically associated to other electronic data, and that are used as a method of authentication.*

with respect to documents on paper – in legal proceedings.

In principle, this difference does not generate much concern, for if Brazilian law grants the presumption of validity – between the parties – of declarations contained in electronic documents, this means that the association of the signatory to the content may not, in principle, be challenged in court. Now, it is possible that there is a difference of scope of the use of an electronic documents in these two regions: while its use is unrestricted in Europe, in Brazil, electronic documents produced outside PKI-Brazil are only valid between the parties; this means to say that it is admissible for one Brazilian electronic document to be repudiated by a third party, even if there is an authorship and integrity confirmation system in the document. This does not mean that a court will necessarily not accept an electronic record as evidence; it may do so to the extent that the other party does not challenge this evidence – if it does, the normal evidence verification means (such as expert examination or investigation, for instance) will determine if the electronic record reflects a fact in a reliable manner or not.

As regards 'qualified signatures', they are also similar with respect to their requirements: the electronic signatures, associated to the certificates issued by PKI-Brazil and under the terms determined by the European Directive, seek to guarantee (i) their unequivocal association to the signatory, (ii) the identification of the signatory, (iii) that the signatory may maintain it under its exclusive control, and (iv) that it is linked to the data to which it refers, such that any subsequent alteration of the data is detectable. Also, the format of the certificates issued is regulated with the same level of security.

The difference here is that Brazil adopts a closed technology to extend the presumption of authorship to documents produced within the scope of PKI-Brazil, while the European Directive is apparently more flexible. This means to say that PKI-Brazil meets the security standards of the European 'qualified' signature, but the inverse may not be true.

As a matter of fact, it is the method of implementing the Directive into domestic law by the various Member States that will determine the possibility of verifying if all the requirements imposed by PKI-Brazil on the Brazilian Certification Authorities are complied with in the EU Members that adopt public key infrastructure systems similar to those of Brazil. In any event, in principle, under the terms of the current PKI-Brazil regulation in force, only the foreign electronic signature systems based on public key infrastructures could be considered for some type of cross-border certification arrangement with Brazil.

In this regard, even if there is technically a compatibility of the digital signature systems between a given country of the European block and PKI-Brazil, the mutual recognition of these systems is not automatic, as is the case with less sophisticated electronic signatures. As we have seen, both the Brazilian and European regulations require the execution of specific bilateral or multilateral agreements that establish the terms and conditions for the mutual recognition of qualified signatures. In Brazil to date, no kind of agreement has been signed to this effect, notwithstanding the intention already demonstrated by ITI in doing so.

Conclusion

The adoption of a flexible electronic authentication system both by Brazil and by the European block is an important initiative to reduce the barriers for the development of electronic commerce. This flexibility also permits the adaptation of the means of authentication in accordance with the transaction that it supports – simpler transactions or transactions of a lower value do not demand a sophisticated technological and certainly more expensive system; whereas for more relevant transactions, the use of a more robust system is justified, which gives more certainty to the identification and integrity of the documents and parties involved.

In Brazil, the most sophisticated electronic signature system adopted is the public key infrastructure system, which is regulated by PKI-Brazil, whose rules are issued by a government entity – the Management Committee, and based on a hierarchical certification system in which the root certification entity is also a government entity, the National Technology Institute. Notwithstanding, both public and private entities may qualify as certification and registration authorities. In Europe, the qualified electronic signature system is apparently more flexible, not necessarily requiring a public key infrastructure system, though the latter, in principle, meets the requirements of the Directive for the advanced electronic signatures certified by a qualified certificate and created by a secure signature-creation device.[17]

The compatibility between non-qualified electronic signatures is already possible between Brazil and Europe; however qualified electronic signatures will still depend on bilateral or multilateral agreements that guarantee a cross-border certification system between the two regions. ■

The authors are the Senior Partner and Associate Lawyer, respectively, of Barretto Ferreira, Kujawski, Brancher e Gonçalves Sociedade de Advogados, with international experience in electronic commerce and telecommunications, among other areas. They are president and vice president, respectively, of the legal committee of the Brazilian Electronic Commerce Chamber – Camara-e.net.

Ricardo Barretto Ferreira da Silva e-mail: **barretto@bkbg.com.br**
José Leça e-mail: **leca@bkbg.com.br**

[17] It is the so-called qualified electronic signature which, within the scheme of the Directive, fulfills the requirements for the manuscript signature in relation to documents printed on paper.