Sistema Económico
Latinoamericano y del Caribe

Latin American and Caribbean
Economic System

Sistema Econômico
Latino-Americano e do Caribe

Système Economique
Latinoaméricain et Caribéen

Fundamentals and state of the Art Digital Signature in Latin America and the Caribbean

XXXVIII Regular Meeting of the Latin American Council
Caracas, Venezuela
17 al 19 October 2012
SP/CL/XXXVIII.O/Di N°16-12

BANCO DE DESARROLLO DE AMÉRICA LATINA

Sistema Económico Latinoamericano y del Caribe

Latin American and Caribbean Economic System

Sistema Econômico Latino-Americano e do Caribe

Système Economique Latinoaméricain et Caribéen

Fundamentals and State of the Art of Digital Signature in Latin America and the Caribbean

Intra-regional Relations

Permanent Secretariat of SELA
Caracas, Venezuela
May 2012
SP/ Di N° 7-12

C O N T E N T S

F O R E W O R D

The Permanent Secretariat of SELA is pleased to submit the consultation document "Fundamentals and State of the Art of Digital Signature in Latin America and the Caribbean," prepared as an integral part of the pilot project of interoperability and harmonization of the International Trade Single Windows within the framework of the Latin American Pacific Arch, as set forth in the Agreement on Technical Cooperation between CAF-Development Bank of Latin America and SELA.

Thus, the Permanent Secretariat complies with the recommendations made by its Member States during the XXXVII Regular Meeting of the Latin American Council of SELA, held in Caracas from 19 to 21 October 2011, so as to contribute to the development of international trade facilitation, with an emphasis on Foreign Trade Single Windows as a tool of the utmost importance for the advancement of paperless trade, with transparency, simplification, legal and technical security, and efficiency.

In order to comply with these objectives, it was considered essential to analyze and systematize the different criteria that work as the base for the use of the advanced or qualified digital and/or electronic signature, the security inherent to them, the equivalent mechanisms, the probative capacity and, in general, how Certificate Authorities (CA) facilitate the implementation of electronic documents with legal validity.

Summarizing, the objective of this document is to serve as a useful consultation guide for government and private actors interested in the implementation of the advanced or qualified digital and/or electronic signature – conceived as a new tool for interoperability among countries – and in gaining knowledge about legal requirements to facilitate the flow of electronic documents in every national Single Window, and their potential to influence intra-regional and regional trade with the rest of the world.

Based on this analysis, the idea is to get some useful conclusions to think and act as regards the development of International Trade Single Windows and other related processes, such as the digital signature, in Latin American and Caribbean countries.

After the introduction, the study is divided into five sections. The first section deals with the technical and legal risks of electronic information. The second one analyzes the principles associated to electronic media, considering the functional equivalence, technological neutrality, the non-alterability of the pre-existing right, the good faith, and the contract freedom. Then, the third section focuses on the Manifestations of the functional equivalence, that is, the written, signature, original, file and preservation, and date and time functional equivalents. The fourth section presents a summary of the State of the Art of the advanced or qualified Digital and/or Electronic Signature in Latin America and the Caribbean, in which legal references containing specific subjects on the matter are provided by country.

Finally, some conclusions are offered and concrete actions are recommended for the countries of Latin America and the Caribbean. Emphasis is made on the need to have regional Single Windows with full probative guarantees, so as to mitigate the risks associated to electronic communications, and to jointly and decidedly establish, as a standard for legal and technical security, the mechanism of the advanced or qualified digital and/electronic signature, issued by a service provider or certification body, in order to facilitate the implementation of fully electronic functions and operations, contributing to the electronic government objectives and to paperless guidelines, as well as to prepare their system for interoperability as an essential phase in trade facilitation, from a perspective that emphasizes the importance of regional integration.

The Permanent Secretariat expresses its deepest appreciation to Dr. Marcela Bello Zuluaga, who prepared this document.

I. INTRODUCTION

The Permanent Secretariat of the Latin American and Caribbean Economic System (SELA), regional inter-governmental body promoting a consultation and coordination system to agree on common stances and strategies for Latin America and the Caribbean, has been supporting various projects on International Trade Single Windows as an essential strategy within the framework of trade facilitation in the region, in order to foster the exchange of experiences, and to facilitate the interoperability and harmonization to materialize the exchange of electronic information, and to make paperless trade a reality – technically and legally safe.

To that end, SELA has implemented various support mechanisms, in order to promote the effective application of Information and Communication Technologies (ICTs) in its Member States, emphasizing those aspects of special interest, such as technical and legal security of communications, specifically, in subjects related to Digital and/or Electronic Signatures, which, in accordance with the different legal guidelines, are key to guarantee the attributes required by the laws, and turn the electronic flow of documents of Single Windows into a reality in each of the countries and within the region.

These actions by the Permanent Secretariat of SELA include the creation of this consultation document, as part of the steps forward of the "Pilot Project for Interoperability and Harmonization of the International Trade Single Windows within the framework of the Latin American Pacific Arch", as set forth in the Technical Cooperation Agreement between CAF-Development Bank of Latin America and SELA.

Thus, the objective of the document entitled "Fundamentals and State of the Art of Digital Signature in Latin America and the Caribbean" is to serve as a useful consultation guide for government and private actors interested in the subject, providing them with detailed information about the use of electronic signatures, their level of security, equivalent mechanisms, probative capacity and, in general, how the digital certification services or the so-called Certificate Authorities (CA) provide a service that facilitates the implementation of electronic documents with legal validity

As an input for this consultation document, due account was taken of the main concerns raised on this matter during the last four meetings organized by SELA on the issue of Single Windows: "First Regional Latin American and Caribbean Meeting on International Trade Single Windows" (Bogota, 25 and 26 March 2010); "First Workshop on International Trade Single Windows: Considerations and proposals for regional actions in the framework of the Forum on the Latin American Pacific Arch " (Valparaíso, Chile, 30 November and 1 December 2010); "II Regional Latin American and Caribbean Meeting on International Trade Single Windows: Advances and pending challenges" (Valparaíso, Chile, 1 and 2 December 2010); and the "III Regional Latin American and Caribbean Meeting on International Trade Single Windows: Paperless foreign trade and risk management in trade operations" (Chamber of Commerce of Lima, 28 and 29 November 2011, Lima, Peru).

II. TECHNICAL AND LEGAL RISKS OF ELECTRONIC INFORMATION

The first aspect that needs to be tackled is the risks associated to the implementation of electronic channels, highlighting their probative incidence and legal validity. In this regard, six types of risks have been identified, which are defined below:

1. Impersonation

In the presence of electronic communication channels – for instance, the Internet public network – it refers to the possibly high risk that the person interacting with the system is not who he/she claims to be, an so it is essential to verify the authenticity and origin guarantees in electronic environments.

In this connection, the determination of authorship is necessary to verify, among other aspects, the capability and competence of the parties involved in an electronic communication; for instance, the legal representation or the power to represent of the legal or moral entity is the only one that can effectively and legally link such legal or moral entity to a certain action.

2. Alteration

Electronic media and, in general, electronic information contained in the different types of files, such as: Word, Excel, pdf, ppt, or any other type of word, image or video processor are susceptible to be modified or altered, which could compromise the integrity of the electronic information. In this regard, integrity refers to the attributes necessary to mitigate the risk of alteration, and consists of the confirmation that the data message or the electronic information received corresponds to the message sent, since in the electronic confirmation, such information or message can be modified or altered. For instance, a person with no previous knowledge of electronic systems can alter a received e-mail, just by writing on the text and sending it or saving it with content that is not the original content sent by the issuer.

Similarly, in the process of transmission or sending of electronic information there are activities and information prone to be handled in an unauthorized way, and possible modification of the messages of the activity, as well as the possibility of manipulation of the information during the process of preservation and filing, along the life cycle of the file.

3. Loss of confidentiality

The attribute of confidentiality implies that the information is only shared among the authorized persons or organizations. In the context of the Internet public network, security and confidentiality are a true challenge, considering that the information and the systems that facilitate their transmission and access to the Internet can be intercepted by unauthorized entities. The non-loss of confidentiality is an essential attribute for electronic communications, with important legal implications.

4. Rejection or repudiation

It refers to the rejection of the authorship or of the integrity of the information transmitted through electronic media.

5. Reception refusal

In most electronic information systems, especially text messaging through e-mail, the receiving of the message is tied to the actions of the addressee or recipient, which makes refusal possible.

In the case of e-mails, traditional acknowledgements of receipt depend on the recipient authorizing such proof to the sender. Nonetheless, these parameters can be easily changed, since these "acknowledgements of receipt" corresponds to a simple text, with no protection, and includes no information about the contents of the message sent. This can also happen in other data transmission systems, and so their probative capability and, thus, their legal validity, are very limited.

6. Date and time conflicts

Date and time in the generation, sending and reception of electronic information play a highly important role in probative matters.

The date and time of generation of a document in a text processor will link the date and the time of the computer of the sender, and that date might be mistaken, out of sync, or not be the same date and time of the country in which the legal effects of the transaction will be taking place. It is possible to draft and send e-mails without being connected to the Internet; nonetheless, such mail uses the sending date and time of the moment in which the button "send" was pushed, even if the mail remains in the sent mail tray.

In that sense, it is worth highlighting that the information system projects that intend to automate processes, procedures or administrative activities, such as International Trade Single Windows, should take into account the previous associated risks to electronic media, so as to analyze their impact and establish mechanisms that would mitigate them and guarantee their legal validity.

Also, added to the aforementioned risks, there is a series of challenges that should be tackled, related to traditional paper documents, such as:

- The contents of an electronic document are dispatched on an electronic base that cannot be sensed by the senses;

- The obsolescence of the technologies that participate in the generation and storage of these documents, equipments, and applications, and the fragility of the hardware/software in which they are preserved, considering the development and evolution of technology;

- The virtual nature of information, such as in the case of electronic mail, that can be easily eliminated, leaving behind no support for the transactions or operations with legal incidence;

- The location of the information used by several bodies sharing it, which prevents, in many cases, the identification of its creator or generator;

- The difficulties to identify the type and documentary form of these documents. The documentary format (original, copy) is closely related to the probative value of the documents or, which is the same, their legal validity.

Considering all these aspects, this consultation document intends to tackle several of the technical and legal mechanisms aimed at preventing the aforementioned risks, and, at the same time, promote the use of electronic media in a more reliable manner, which undoubtedly offers more technical and legal security for information than that offered by physical supports, adding more efficiency and efficacy to the processes.

III. PRINCIPLES ASSOCIATED TO ELECTRONIC MEDIA

Most Latin American and Caribbean countries have made important efforts in the design and instrumentation of public policies on paperless electronic government, with the objective of promoting transparency, security, efficiency, and administrative efficacy. In that connection, they have promoted the instrumentation of electronic operations, such as: i. The services that the State lends to citizens and companies through Single Electronic Windows, whose objective is to rationalize and simplify trade operations along the whole supply chain, ii. Provision of electronic billing service so as to facilitate tax evasion controls and increase company efficiency; and iii. All aspects related to contracting electronic services that tend to the transparency and democratization of public purchases, among other online government initiatives.

Effective instrumentation of paperless initiatives of electronic government depend on and unavoidably require legal frameworks of operation, and so over the past ten years, Latin American and Caribbean countries have made efforts to create laws and regulations to include the use of technologies, and, as a consequence, regulate the mechanisms that offer assurance and guarantees to the parties.

Considering the aforementioned, existing regional legal frameworks, and those in the process of issuing, shall involve and consider the following fundamental principles:

1. Functional Equivalence: "Considered to be the main principle of electronic media"

It is the principle that allows for everything that can be done through physical or traditional means to be made through electronic media, with the same legal and probative value.

In other words, the legal function of written and autographed instrumentation, with respect to every legal act, or their oral expression, is equally fulfilled by the electronic instrumentation via a data message (electronic information), regardless of the content, length, scope, and objective of the act.

From this point of view, functional equivalence implies the non-discrimination of electronic information (data messages) with respect to the traditional written media, which allows giving it the same treatment from the legal and probative point of view. The idea with this is, through Information and Communication Technologies (ICTs), to guarantee that the physical medium or traditional procedure demands or requirements are reproduced as a whole.

2. Technological Neutrality: "Principle that allows for giving durability to the regulations"

It is the principle that establishes that the law and its implementation cannot be tied to one single technology, but that it has to consider the technologies that will promote their development and regulation, as well as the technologies that are being developed or that are about to be developed.

3. Non-alterability of pre-existing law: "The current substantial law regime is not to be altered or modified"

Electronic commerce does not imply a modification of the substantiality of the current law of the obligations. This is the case because the electronic channel and its legal application to all types of transactions is in essence a new support and transmission mean of negotiable or pre-negotiable wills. This way, if there is a deceptive manoeuvre to

get some economic gain through swindling, using an electronic channel, the penal code of the corresponding country is applied, and the electronic channel would have no relevance whatsoever, only because it is electronic. In fact, the electronic channel does not produce any different effect or procedure in an action. When talking about administrative issues, the so-called administrative litigious code, if they are of the procedural type, the civil procedures code shall apply; and if they are commercial, the commercial code shall apply, and so on.

It is worth mentioning that the practice of this principle in the regional legal systems has been to facilitate, through special regulation instruments, the use of electronic channels on each branch of the law.

4. Good faith: "This principle is nothing but a reaffirmation of the fundamentals reporting the whole law in a general level."

Whenever the national or international exchange of goods and services is mentioned, or when we talk about e-commerce, this principle acquires special relevance because of the characteristics of the exchange taking place through the use of technological supports in which good faith, as the main principle of business, represents the main foundation in terms of equality, decent treatment, and trust.

5. Contract freedom

Contract freedom is the manifestation or necessary consequence of the principle of inalterability of the pre-existing right, in the framework of e-commerce. Contract freedom is a right that has to be set against the backdrop of free enterprise, of private autonomy, and free competition.

Next, we make special reference to the principle of functional equivalence and its manifestations, as it is considered of more relevance within the context of paperless commerce and electronic information.

IV. MANIFESTATIONS OF THE PRINCIPLE OF FUNCTIONAL EQUIVALENCE

Nowadays, it can be said that in most Latin American and Caribbean countries, no information is denied legal effects, validity or mandatory force, just for being in the form of data messages or as electronic information.

The laws or regulations in the region, although with differences in this regard, have used as a referential framework the law of the United Nations Commission for the Unification of International Trade Law (UNCITRAL) from 1996, which establishes as a mechanism for legal and technical assurance of communications, the so-called digital or electronic signature issued by a service provider or digital certification body. Later on, we will see to these concepts.

Until now, five (5) manifestations of the aforementioned functional equivalence principle have been mentioned, all of them present in the treatment of the phenomenon through electronic media:

1. The written functional equivalent

This principle establishes that whenever the information is required in writing, such requisite will be satisfied with a data message or electronic information, as long as the information contained in it is accessible for future consultation.

For this reason, in the area of electronic information, and with full validity, the electronic document procedural notion of document, understood as its support, for any case of instrumentation of information or virtualization systems, will be known as a data message, e.g. information contained in electronic media, which would allow access to it in the future.

2. The functional equivalent of signature

The laws or regulations in the matter establish the functional equivalent of the signature, when any regulation demands the presence of a signature, or sets forth certain consequences in the absence of such, in relation to a data message or electronic information. Such requirement will be considered satisfied if the following conditions are met:

- When a method that allows for the identification of the starter of a data message or electronic information is used, and to indicate that the contents have their approval.

- When the method is both reliable and appropriate for the objective of the message generated or conveyed.

Manuscript signatures exist in the Latin American and Caribbean legislation since about 65 years. Generally, they are contained in the code of commerce and correspond to the graphic representation of the only and exclusive will of every individual, and on probative matters, concepts of graphological specialist's reports for the analysis of its authenticity. The manuscript signature has been the legal mechanism par excellence in the physical or traditional context, as it guarantees two attributes that are inherent to their application: the authenticity, establishing that the person signing is who he/she claims to be, and the non-repudiation, which establishes that the person signing agreed to the commitments acquired, and undersigned the document acknowledging its contents. Thus, when in presence of a physical document signed in manuscript, such document is considered to be authentic and non-repudiated, granting probative capacity to the document.

It is worth mentioning that, in the search of the electronic equivalent of the manuscript signature, it was essential to think of a mechanism that, at least, would guarantee the attributes of the manuscript signature to be applied to electronic documents. That is how in the legislations of Latin America and the Caribbean they embraced the United Nations standards, and confirmed that such equivalence would take place in the presence of an advanced, certified or qualified digital or electronic signature, in accordance with the denomination of the corresponding country (the differences are only nominal), as from such digital or electronic signature would originate the attributes of the aforementioned manuscript signature, e.g.: the authenticity and the non-repudiation, and, additionally, thanks to the standards used by the same account with an attribute that supersedes the manuscript signature; the integrity, since when a document is electronically or digitally signed, it is possible to evidence in the verification process if the document has been altered or changed in any way, thus guaranteeing that the document has kept its integrity at all times.

In this connection, when in presence of hand-signed documentary proof, presented before a judicial authority, the counterpart in a judicial process might question the contents and the integrity, arguing that such physical document was altered, because, although that is their signature, the content is different. On the other hand, if the proof is electronic and the document has been electronically or digitally signed, the system

allows for the validation of the integrity of the content, through an operation that basically works in the following manner:

> i. When performing an advanced, certified or qualified digital and/or electronic signature procedure, the users sign by entering a unique password under their control, which allows them to access the storage media of their signature (cryptographic USB, a smart card or a logic medium in their computer).
> ii. Then, the system makes an encoding procedure of the content, generating a unique mathematical result by document, comprised by all its characters, regardless of the number of pages.
> iii. When trying to make a modification – however small, for instance, change a lower case for an upper case -, in the verification process, the system revalidates the mathematical result. If a change in a character is detected, the mathematical result will not be the same and it will alert about an alteration, and thus the signature will be invalidated.
> iv. If, on the contrary, the signed electronic document was not altered, the verification process will notify of the success, and will correspond to a completely whole document, which will never be questioned by the counterpart.

At any rate, for the digital and/or electronic signature to have the attributes of the manuscript signature, it shall meet the requirements imposed on them by the law, in order to guarantee its reliability and appropriateness. In this regard, in reference to the legal attributes of this signature, it is useful to remember the most relevant functions:

- Authenticity. The signature guarantees that the persons participating are indeed who they claim to be. In other words, the contents of the message are safeguarded by means of mathematical algorithms, thus safeguarding the authenticity of the initial message;

- Integrity. It is possible to verify that the message was not modified in the electronic communication process, thus guaranteeing that the message sent has not been manipulated. Since it is a digital and/or electronic signature, it is directly related to the document, and so any change to the text invalidates the signature;

- Confidentiality. The message is secret or confidential for the parties of the electronic communication, preventing third parties, foreign to the message, from knowing about it; and

- Non-repudiation. The doctrine has developed the non-repudiation function, which consists of the subscriber's impossibility of denying that they have electronically or digitally signed the corresponding message.

Now, in accordance with the Latin American and Caribbean legislations, it is important to explain the difference between the electronic signatures (simple), and the advanced, certified, or qualified digital and/or electronic signatures, depending on the denomination of each country. This way, the electronic signature (simple) is the type of authentication mechanisms that can be defined as any mechanism that allows for the identification of a person in an information system. It is a generic concept that can have multiple applications.

From the definition of electronic signature (simple), different elements may be extracted: i. It is a technical mechanism, ii. it allows for the identification of a person in an information system, and iii. it has to be reliable and appropriable.

This last characteristic – the reliability and the appropriability – is the most controversial in the operation of an electronic signature, as they are subjective technical concepts that do not have a clear legal reference, and that are normally formulated in previous agreements between the parties that use electronic communications. Let us think about bank contracts, in which, precisely, it is established that the PIN systems and passwords are technical mechanisms that allow for the authentication of the financial consumer before their Bank, and in the same contract it is pointed out that such mechanism is reliable and appropriable. Thus, the ATM keyword, the password, and a PIN are electronic signatures we use everyday. Electronic signatures, then, have full validity, and the determining factor in the model used, is that the parties of an electronic communication have set, through a previous agreement, the reliability and appropriability of such mechanism.

Once the electronic signature is defined in the authentication mechanisms recognized by the legislations of the region, both the existing ones and the ones to be issued, it will be possible to argue that the advanced electronic signature (which mainly uses PK technology, and a third reliable party for its issuing), is its most important type, as it enjoys a presumption of reliability and appropriability in all legislations. The advanced electronic signature denomination used in Mexico, to differentiate it from the simple electronic signature, originates form the model of the European Guideline on Electronic Commerce, but in the Latin American and Caribbean legislations it has been called differently. Thus, in countries such as Colombia and Chile, it is called digital signature, while others use the concept of certified digital signature, such is the case of Venezuela and Brazil; and yet others, such as Panama, call them qualified electronic signature. To add yet more elements to the possibilities of denomination of this mechanism in the region, there are legislations, such as the Ecuadorian, in which it is strictly defined as electronic signature, without any other adjectives.

Summarizing, an advanced, certified or qualified electronic signature may be defined as a mathematical procedure that allows for the suitable identification of a person in electronic media (authentication), and also to verify, on the side of the addressee of a data message, whether they have altered such message (integrity). This way, the attributes of legal security, inherent to the manuscript signature, such as authenticity and non-repudiation, are achieved.

In relation to the characteristics of legal and technical ensuring of the electronic and/or digital advanced, certified, or qualified signatures, legislators from Latin American and Caribbean countries adopted a presumption of reliability and appropriability in favour of these characteristics.

In other words, the difference between a digital and/or electronic advanced, certified, or qualified signature and a simple digital signature is that the former has more probative force, since it is not necessary to determine its reliability and appropriability, as it enjoys that presumption, not only because of the technology used, but also because it demands the intervention of a service provider of certification or of a digital certification body, which commits its responsibility to the unequivocal identification of a person in electronic media.

The service provider of certification or the digital certification body is precisely a reliable third party that guarantees - even at the level of patrimonial responsibility – the identity of the persons in electronic media. That is to say, it is a third party, which, through different

audited processes, verifies the identity of a person, so that they are able to develop operations and activities through electronic media.

In this context, the certification service provider or the certification body are entities authorized under the government requirements of each country, to issue electronic certificates related to third party's electronic signatures. Such bodies offer or facilitate the services of chronological registration or stamping in the transmissions of data messages or electronic information (Time digital seal or electronic dating, depending on the legislation), and perform other functions related to electronic signatures.

In virtue of this, it is worth mentioning some conclusions of the functional equivalent of a signature:

- The keywords of passwords, used by financial bodies or as means of access to information systems of the companies, are simple electronic signatures that have been issued or backed by a services provider or by a reliable third party, and thus their reliability and appropriability depend on the healthy criticism of the judge in probative cases.

- In other words, when in the presence of an electronic and/ or digital signature, advanced, certified or qualified by a reliable third party or by a digital certification service provider, such signature is presumed to be reliable and appropriable, and the load of proof is on the head of the digital certification body that issued the certificate, in which case such body inverted the probative load.

- By opposition, when in presence of a simple electronic signature, not backed by a reliable third party, the load of proof is on the head of the issuing body, and shall demonstrate that the mechanism properly ensured the transaction.

- A self-generated electronic signature (code or password) cannot have the same probative value of the type of signature in which the one proving the identity is a reliable third party, which at the same time has the professional duty to do so.

- The intervention of the third party (certification service provider) is essential, as it allows to guarantee the identity of the signing parties before any other party, not only between the ones establishing the communication, and thus considering the procedure for the generation of the signature, the laws have established in their favour three main attributes in the legal assurance of the electronic information, already explained, which are: i. Authenticity, as it is possible to verify the author of a data message, who in turn is legally bound; ii. Integrity, since the addressee of such data message will be able to determine whether the information has been altered in the electronic communication process; and iii. Non-repudiation, since the persons signing commit themselves to the corresponding subscription, and afterwards they cannot recant or refute such act. It is worth mentioning that Latin American and Caribbean legislators have granted advanced, certified, and qualified electronic and/or digital signatures these probative characteristics, precisely because in the issuing process, there is a third party backing the identity of the holder of the signature.

- In accordance with the abovementioned, it can be concluded that in the electronic legislation of Latin America and the Caribbean, both the simple electronic signature, and the advanced, certified and qualified electronic and/or digital signatures are recognized, depending on the corresponding denomination;

and that although both of them are capable of producing the same legal effects as authentication mechanisms, it is also true that there are deep differences in the probative load of the legal security attributes previously explained, thanks to the intervention of the third party, called digital certification service provider or certification body. The difference, then, is essentially probative, since although the automatically advanced, certified, or qualified electronic and/or digital signature incorporates the authenticity, the integrity, and the non-repudiation, the simple electronic signature has to be proven, and it is also necessary to determine that it is a reliable and appropriable mechanism.

- The advanced, certified, or qualified electronic and/or digital signature corresponds to an authentication mechanism that can be applied to mitigate the risks inherent to electronic communications, previously explained, such as: i. Supplanting risk; ii. Alteration risk; iii. Repudiation risk; and iv. Confidentiality risk.

- Finally, and considering the abovementioned, it can be said that the advanced, certified, or qualified electronic and/or digital signature, imposed through the use of a digital certificate previously issued by a digital certification service provider, duly authorized by the legislation of each country -, is considered to be the proper equivalent of the manuscript signature, as it is considered to be reliable and appropriable.

3. The functional equivalent of original

The concept of "original" in the field of electronic media establishes that when any rule requires that the information is presented and preserved in its original form, such requisite will be satisfied with a data message or electronic information, if the following conditions are met:

a) The existence of any reliable guarantee indicating that the integrity of the information has been preserved, starting at the moment of its creation in its definitive form as a data message or in any other form;

b) If the information has to be presented, if such information ca be shown to the person it has to be presented to.

This equivalent implies a change in paradigm in the matter of the originality from the point of view of the physical or traditional documents. What is understood as an original document in the physical world is the first document created, and what originates from it will be called the copies. Nonetheless, it is impossible to hold the same concept in electronic media, and this is the case because of the frequent reproduction of an electronic document. Let us use the example of a PDF document sent to a person who, at the same time, sends it to 100 other addressees, and those 100 addressees send it to another thousand. Which, then, is the first document? It is impossible to determine.

Because of this, the legislators have adopted the concept issued by UNCITRAL in the matter of the originality in the electronic media, considering that a document or data message is original in the electronic media if it is whole.

The originality is equal to the integrity, which, basically, indicates that the document has not suffered any alteration or change. It is unaltered since its creation, with the exception of the addition of an endorsement or of any change that is inherent to the communication, filing or presentation process.

This takes us to conclude that in the electronic channel there may be several originals of the same document, as long as from each of them their integrity can be derived.

The use of the digital and/or electronic signature guarantees the integrity of the information, as it was previously explained in the equivalent of manuscript signature. The digital and/or electronic signature of a document allows asserting that the information has remained whole since its subscription, and that it will remain like that at least while the signature preserves its uniqueness.

Every document that requires as a formal duty to be backed by the original, if digitally and/or electronically signed by the one who should be its issuer, complies with all the conditions to be an original.

4. The functional equivalent of file and preservation

In reference to the preservation of data messages and electronic documents, the laws clearly establish that when it is a legal requirement for certain documents, entries or information to be preserved, such requirement shall be deemed met as long as the following conditions are fulfilled in their electronic filing and preservation:

a) The information has to be accessible for future consultation.

b) The data message or preserved document shall be in the format in which it was generated, sent, or received, or in a format that allows verification that the preserved information has been accurately reproduced.

c) The preservation of the information that allows to determine the origin, destination of the message, the date and the time in which the document was sent or received, or when the document was reproduced.

When there is an electronic document as the law establishes, it is appropriate to have the possibility to file and preserve it in electronic format.

In accordance with the aforementioned, if the documents contained in such file are digitally and/or electronically signed, it will be possible to comply with the requirements of origin, authenticity, integrity, and, in the case of determination of date, we could resort to the service of chronological stamping, electronic dating, or time sealing (as later is detailed on the item on equivalent of date and time), through which the certainty of exact date and time in which an electronic document is generated, sent or received is granted, thus providing the temporal preservation extremes of the document.

5. The functional equivalent of date and time

The idea of "time" is presumed as an irreversible fact that globally affects all human activities, and is a key component for all causal relations between processes. The relations of dependence between some facts and others are a function of the order in which each one of them is performed, and usually are a manifestation of the causal relations that unite them.

The accuracy in time and the contents of the transactions are of vital importance in electronic commerce. Nonetheless, transactions in general are made using time sources from the computers themselves, and thus "time" is not reliable and can be easily manipulated and repudiated. This problematic situation can be corrected by applying chronological stamps, electronic dating, or time seals to the electronic documents, which guarantees that the transactions have taken place in a specific point in time, and that

their contents have not been altered since then, using a so-called “atomic clock” or the legal time provided by the public body in charge of it in the country.

A computer's clock can be easily manipulated, and the documents are easily edited. But if electronic commerce is to be a reality, and the idea is to digitalize an important chunk of human activities, the equivalent of physical security citizens are so used to, and that has been the foundation of the laws, has to be applied and socialized. This is the time when the digital dating systems appear, which correlate the existence of bits to the human events of general reference, and, in particular, to the agreement of absolute time guaranteed through a certification service provider, which on top of certifying digital and/or electronic signatures, offers this service of electronic time sealing globally known as T*ime Stamp Authority* (TSA).

With these description of the functional equivalents in terms of the use of electronic media, as well as by the large number of countries that have embraced laws, regulations, and procedures, or that are fostering legislation projects for the implementation of electronic channels, it is possible to conclude that we are very close to counting on implementations of advanced, certified, or qualified digital or electronic signature in most Latin American and Caribbean countries, in order to promote transparent commerce, legally and technically secure, and thus facilitate to a great extent the necessary interoperability of intraregional commerce.

Nonetheless, there are important challenges that need to be tackled and overcome, in order to really materialize the use and spreading of the mechanism of advanced, certified, or qualified electronic and/or digital signature, including subjects ranging from awareness raising, socialization, and training, to their practical use in projects, both public and private.

V. STATE OF THE ART OF DIGITAL AND/OR ELECTRONIC SIGNATURE IN LATIN AMERICA AND THE CARIBBEAN

Next, we make a correlation, country by country, of the law reference including specific subjects in the matter of Electronic Signature. Many countries in the region have adopted the model law of UNCITRAL in its structure and scope, but it is assimilated in each country based on their particular traits. Thus, there are nominal differences in terms of certified digital signature through a reliable third party. In any case, there is homogeneity in the general purposes and functional equivalences already mentioned throughout this basic consultation document.

All countries that presently have a law in the matter of legal and probative validity of data messages, or that regulate legal conditions for electronic commerce, have chosen to acknowledge through functional equivalence criteria the legal efficacy of certified electronic and/or digital signatures, as mechanisms to grant legal security to electronic transactions, promoting safe electronic commerce and the irrefutable identification of the individuals that perform electronic transactions.

The state of the art of digital and/or electronic signature in the region can be summarized as follows:

Country	Law or Regulation on Electronic Signature
1. Argentina	Law 25506 from 2001 – Law on Digital Signature Acknowledges the use of electronic signature and of the digital signature, and their legal efficacy.
2. Bahamas	Electronic Communications and Transactions Act, 2003 This law grants legal acknowledgement to electronic documents, contracts, signatures and information.
3. Barbados	Electronic Communications and Transactions Act, 2003 This law gives legal acknowledgement to electronic documents, contracts, signatures and information.
4. Belize	Electronic Communications and Transactions Act, 2003 This law grants legal acknowledgement to electronic documents, contracts, signatures and information.
5. Bolivia	080 Act from 2007 – Electronic Documents, Signatures, and Commerce from 2007. This law acknowledges the legal and probative value of: i. The legal acts held through electronic media, or others more technologically advanced, made by legal or natural entities collective or unipersonal companies, communities of goods, and other bodies that constitute an economic unit subject to rights and duties, ii. The use of electronic signatures, duly certified by a Certification Body, credited in accordance with the provisions of the law herein, iii. The civil and commercial acts that directly or indirectly use electronic media or others more technologically advanced to perform electronic commerce activities.
6. Brazil	Order in Council 3,996 from 2001 and Order in Council 4,414, from 2002. Regulates the provision of services of digital certification of electronic signature. Efforts have been made to promote projects related to electronic commerce legislation, but the country considers the current legislation to be enough in other regulations that have authorized the use of electronic signatures, they also count on specific decrees that regulate such services. Brazil is a country in the region that is recognized by the effective spreading of the use of advanced electronic signature, and it actually requires its use for tax purposes.
7. Chile	Act 19,799 from 2002 – Electronic Documents Act The act adopts the provisions related to electronic documents, electronic signatures, and certification services of the signatures.
8. Colombia	Act 527 from 1999. Legal and Probative Validity of data messages. By which the access to and use of data messages, electronic commerce, and of digital signatures is defined and regulated, and the certification bodies are established, and other provisions are set. Colombia has developed an endless number of authorization regulations that have allowed for paving the road towards the massive use of the instruments.

9. Costa Rica	Act 8454 from 2005 – Certificates, digital signatures, and electronic documents act It establishes the general legal framework for the secure use of electronic documents, and of the digital signature in public and private bodies.
10. Cuba	In Cuba there is no special legislation to control electronic commerce; nonetheless, there are regulations that authorize its use in different areas of the law.
11. Ecuador	Electronic Commerce, Electronic Signatures, and Data Messages Act from 2002 This act regulates data messages, electronic signatures, certification services, electronic and telematic contracting, the lending of electronic services through information networks, including electronic commerce, and the protection of the users of these systems.
12. El Salvador	In El Salvador there is no special legislation to control electronic commerce; nonetheless, there are regulations that authorize its use in different areas of the law.
13. Grenada	Electronic Transactions Act, 2008. This law gives legal recognition to electronic documents, contracts, signatures and information.
14. Guatemala	Law/Decree 47 from 2008 – Law to Acknowledge Electronic Communications and Signatures.
15. Guyana	No legislation antecedent was found in public sources of information.
16. Haiti	No legislation antecedent was found in public sources of information. Apparently, there is no special legislation regulating electronic commerce, nonetheless, there are certain regulations that authorize its use in different areas of the law.
17. Honduras	In the legal framework of Honduras, there is no special law regulating electronic commerce, or electronic contracting; however, some civil and commercial general regulations apply. The Financial System Law acknowledges, in its article 51, the legal effects of the electronic signature, which shall have, in reference to the data presented in electronic format, the same legal value of the manuscript signature.
18. Jamaica	Electronic Transactions Act, 2007 This law grants legal acknowledgement to electronic documents, contracts, signatures and information.
19. Mexico	Advanced Electronic Signature Act from 2012. Corresponds to a new Electronic Commerce Law including modifications to the Civil Code, and other laws that give legal framework to the electronic signature. Regulates the use of the advanced electronic signature in acts provided by the Law, and the issuing of digital certificates, services related to the advanced electronic signature and its standardization.

20. Nicaragua	Act 729 from 2010 – Electronic Signature Act Authorizes communications through electronic media, whenever it is possible to accurately establish, via reliable records, the identification of the issuer and of the receiver, the time, date, and contents of the message.
21. Panama	Act No. 51 from July 22, 2008, which defines and regulates the electronic documents, the electronic signatures, and the lending of technological storage of documents, and the certification of electronic signatures, and adopts other provisions for the development of electronic commerce. Presently, the country is processing a reform of this law.
22. Paraguay	The regulation of Act Nº 4017/10, "Of the legal validity of the electronic signature, the digital signature, the data messages, and the electronic file," through decree Nº 7.369. This decree specifies aspects such as the reproduction of original documents by electronic means, the digitalization of public files, as well as the certification of documents and requirements for their application. In terms of the service for the filing and preservation of documents and data messages, the decree indicates that the bodies performing the reproduction of original documents by electronic means, or that lend a service of storage, shall incorporate a stamping procedure that guarantees the effects of the electronic document. This is equal to the physical document stored.
23. Peru	Act No. 27269 from 2000 – Act on Digital Signatures and Certificates Regulates the use of Electronic Signatures, granting the same legal validity and efficacy of the use of manuscript signatures, or of any other similar, that leads to a manifestation of will.
24. Dominican Republic	Act 126 from 2002 – Act on Electronic commerce, Documents and Digital Signatures. This law applies to all kinds of information in the form of digital document o data message.
25. Suriname	No legislation antecedent was found in public sources of information. Apparently, there is no special legislation regulating electronic commerce. Instead, there are several general laws that apply to the subject. Online government strategies have been implemented, using mechanisms of technical assurance through simple electronic signatures, such as codes and passwords.
26. Trinidad and Tobago	Electronic Transactions Act 2011 This act acknowledges the legality of electronic transactions and introduces subjects related to digital signature.
27. Uruguay	Act 18,600 from 2009 – Electronic document and electronic signature act. This act acknowledges the legal admissibility, validity, and efficacy of the electronic document and of the electronic signature.

28. Venezuela	Order in council Nº 1204 de 2001, Data Messages and Electronic Signatures Act This order of council has the goal of granting and acknowledging legal efficacy and validity to the Electronic Signature, the Data Message, and to all intelligible information in electronic format, regardless of their material support, attributable to individuals or legal entities, public or private, as well as to regulate all aspects related to Certification Service Providers and Electronic Certificates.
29. Antigua and Barbuda	Electronic Transactions Act 2006 This act grants legal recognition to electronic documents, contracts, signatures, and information.
30. Dominica	No legislation antecedent was found in public sources of information.
31. Saint Kitts and Nevis	No legislation antecedent was found in public sources of information.
32. Saint Vincent and the Grenadines	Electronic Transactions Act 2007 This act grants legal recognition to electronic documents, contracts, signatures, and information.
33. Saint Lucia	Electronic Transactions Act 2007 This act gives legal recognition to electronic documents, contracts, signatures, and information.

VI. CONCLUSIONS AND RECOMMENDATIONS

a) In accordance with the aforementioned, it is important to evaluate the matter of digital and/or electronic signature in Latin America and the Caribbean, as a new phenomenon of interoperability between countries, which will allow for transparency, simplification, rationalization, and efficiency of intraregional commerce processes, and of the region with the rest of the world.

b) Similarly, it will be necessary for the countries of the region to incorporate authentication mechanisms in their public policies designed by each one of them in the matter of electronic government.

c) The main multipliers of the use of digital and/or electronic signatures or digital certification services are the government and their information systems. Thus, information systems called upon to multiply the electronic and/or digital signature as a mechanism to ensure and mitigate the risks of electronic communication and bring about the transactions and electronic processes are i. State tax bodies; ii. Social security and sanitary bodies; and iii. The financial sector.

d) The region should facilitate, through some kind of supranational regulatory instrument, the recognition of electronic and/or digital signatures in each country, under the laws and regulations of each country of origin of the signature. An example of this is the recognition project of the Latin America Integration Association (ALADI) for the digital certification system of origin, or the Federal Bridge Certification Authority, which gives validity to the digital signatures issued in the different legislations of the United States.

e) Integration of advanced, certified, or qualified digital and/or electronic signatures, according to how they are called in each country, issued by a certification service providing body, will guarantee:

- The authenticity of the origin;
- The integrity of the transactional information along its life cycle;
- The non-repudiation of transactions;

As a consequence, each country should evaluate the current state of the digital and/or electronic signature, paying attention to:

- whether there is a specific law and regulations, should they apply;
- whether there is a public or private digital certification service provider;
- whether there is any specific authorizing integration and/or Norms in multiplying systems, as commerce subjects in single windows, tax, government operations, social security, etcetera.

In accordance with the resulting answers to the previous questions by each country, it will be possible to know their current state and evaluate the application of the following recommendations:

a) The countries that have a law in the matter of electronic media, regardless of their denomination, and that have also regulated such regulations, and count on reliable third parties or on certification service providers for the issuing of certified digital and/or electronic signatures, shall focus all their efforts on the integration of certification services of digital certification of certified digital and/or electronic signatures in different transactional public systems, along with the issuing of the corresponding regulatory instruments that authorize their use in such actions, processes and public procedures. This way, the path towards the massive use and coverage of these instruments would be paved, extending plurality of providers, and improving prices and competition, the number of signature subscribers, and the number of systems using them. This would allow for the consolidation of fundamental aspects in the context of paperless electronic government.

b) It is important to highlight the need for Single Electronic Commerce Windows in the region, which by their very nature are usually systems managed by public bodies, and that require, in accordance with their legislations, to count on full probative guarantees, so as to mitigate the risks associated to electronic communication, jointly and decisively establish, as a legal and technical security standard, the mechanism of advanced or qualified digital and/or electronic signature issued by a service provider or certification body, in order to facilitate the implementation of fully electronic functionalities and transactions, thus contributing to the electronic government objectives, and the paperless guidelines, as well as to prepare their system for the interoperability as an essential phase for the facilitation of commerce.

c) It is recommended that in the matter of commerce facilitation, the projects in the process of design and implementation of Electronic Commerce Single Windows – considered to be of the highest relevance in the strategies of electronic government and paperless commerce – incorporate certified digital and/or electronic signature mechanisms, following the development pattern of the Single Windows, already consolidated in the region and in the world. Similarly, some

legislation that have implemented the electronic invoice have considered the need to force the use of electronic and/or digital signature to use the system in a more effective and safer manner.

d) The countries that have legislation for electronic media, but that still have not regulated specific subjects related to electronic signatures and service providers, should focus their efforts on issuing such regulations and building the proper environment that promotes the constitution of certification bodies, whether public or private. After such legislative effort, they would have to consider strategies for the use and spreading, as established in the previous paragraph, to guarantee the stability and sustainability of the service provider and, in general, of the registration system for certified electronic and/or digital signatures.

e) In order to facilitate the constitution of certification service providers, countries could use the infrastructure of other regional service providers as a base, so as to facilitate the implementation, and make viable the investment costs for the public or private bodies interested.

f) Lastly, the countries of the region that do not have any laws in the matter of the use of electronic media have several interesting regulative examples. The most frequently copied is the model act from 1996 of UNCITRAL, or the European guideline for electronic commerce from 1993, as well as the model act for electronic signatures from 2005. Also, there are regional regulations that have turned into regulating paradigms for other countries. Such is the case of the Colombian and Chilean laws, and the technical standards and developments from Brazil, experiences that have consolidated their leadership, as they were the first countries with certification service providers.

These challenges and recommendations are aimed at promoting the use and spreading of the digital and/or electronic signature, which will materialize the safe interoperability, and the paperless projects, both in commerce and in electronic government environments in Latin America and the Caribbean.