WORLD TRADE ORGANIZATION

JOB/GC/115, JOB/CTG/3
JOB/SERV/247, JOB/IP/20
JOB/DEV/41

21 December 2016

(16-6995)

General Council
Council for Trade in Goods
Council for Trade in Services
Council for Trade-Related Aspects of Intellectual Property Rights
Committee on Trade and Development

Original: English

WORK PROGRAMME ON ELECTRONIC COMMERCE

ELECTRONIC SIGNATURES

Communication from Argentina, Brazil and Paraguay

The following communication, dated 15 December 2016, is being circulated at the request of the delegations of Argentina, Brazil and Paraguay.

1.1 Electronic signature (e-signature) encompasses a broad range of digital solutions aiming to ensure the authenticity, integrity and privacy of online domestic and cross-border transactions and communications. An electronic signature uses electronic data to ascertain the identity of the sender of an email or the purchaser of an on-line service. In its basic format, an e-signature does not require an independent official third party for certification purposes.

1.2 In its more sophisticated version, an electronic signature, known as advanced electronic signature or digital signature, is based on an electronic file (an advanced digital certificate) that acts like a full digital identity, allowing safe and unequivocal identification of the author of an electronic message or a digital transaction. The digital certificate must be issued by a trustable third party – an official or accredited Certification Authority -, which will associate any natural person or any juridical person to a pair of cryptographic keys. A digital certificate not only enables clear identification of a person in the World Wide Web, but also ensures legal validity of any digital action using it. Digital certificates are becoming a fundamental tool for e-commerce, electronic contracts, bank operations, e-government initiatives, among other usages. For instance, an email sent with a digital certificate ensures the identity of the sender and the integrity of the message, ascertaining that its content has not been violated in any way.

1.3 The issue of e-signature and authentication has already been identified as a relevant issue in the discussions under the Work Programme on Electronic Commerce (documents JOB/GC/97/Rev.3 and JOB/GC/98).

1.4 In order to provide further input to the discussions, Argentina, Brazil and Paraguay would like to share with Members GMC Resolution 37/06, which deals with this issue within MERCOSUR. The co-sponsors are convinced that e-signature is a fundamental issue in any future consideration regarding electronic commerce in the WTO.

MERCOSUR (Resolution GMC 37/06)

Article 1 – Scope of application

The purpose of this Resolution is to recognize, subject to the conditions laid down hereunder, the legal value of electronic documents, of electronic signatures and advanced electronic signatures within MERCOSUR, thereby contributing to their utilization.

These provisions do not apply to other aspects relating to the conclusion or validity of legal instruments where formal requirements are laid down in national laws, nor do they affect the regulations and limits set forth in national legislation governing the use of documents.

This Resolution does not authorize the free movement of digital certification services within MERCOSUR. For the provision of digital certification services, the States Parties shall observe the disciplines set forth in the Protocol of Montevideo on Trade in Services in the MERCOSUR, and in their specific schedules of commitments.

Article 2 – Principles

The States Parties shall observe the following principles:

1. Operational autonomy and permanent coordination among national infrastructures;

2. Interoperability based on international standards;

3. Exchange between States Parties of digital information and documentation under safe technical conditions, with legal validity and probative value;

4. Transparency in the management of digital certification;

5. Neutral treatment by national laws of the different technologies used for the activities set forth in this Resolution in order to allow for adaptation to the pace of technological development inherent in such activities (technology neutrality);

6. Functional interpretation of the terms and concepts in order to ensure that a particular process or technology used by a State Party is not denied legal effect solely because it has been given a nomenclature different from that provided in this Resolution.

Article 3 – Definitions

For the purposes of this Resolution:

(1) **"Electronic signature"** shall mean data in electronic form attached to other electronic data or logically associated with such data, used by the signatory as a means of identification.

(2) **"Advanced electronic signature"** shall mean an electronic signature which meets the following conditions:

(a) It requires information known only to the signatory, so that the signatory can be uniquely identified.

(b) It is created by means that the signatory can maintain under his/her sole control.

(c) It is verifiable by third parties.

(d) It is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

(e) It is created using a signature creation device that is technically safe and reliable, and is based on a certificate that is qualified and valid at the time of signing.

(3) **"Digital signature"** shall be used interchangeably with "advanced electronic signature".

(4) **"Signatory"** shall mean a natural or legal person that legally uses an electronic signature creation device.

(5) **"Electronic document"** shall mean the digital representation of acts or facts regardless of the medium to which they are affixed, or in which they are saved or stored.

(6) **"Digital document"** shall be used interchangeably with "electronic document".

(7) **"Digital certificate"** shall mean a digitally signed electronic document that links signature verification data to the signatory and confirms the signatory's identity.

(8) **"Qualified certificate"** shall mean a digital certificate issued by an accredited service provider that meets the requirements laid down by national law.

(9) **"Advanced certificate"** shall be used interchangeably with "qualified certificate".

(10) **"Certification service provider"** shall mean the natural or legal person which, under national law, delivers certificates or provides other services relating to electronic signatures.

Article 4 – Legal effects of electronic documents and electronic signatures

The States Parties recognize that electronic documents meet the handwriting requirements. Consequently, in each one of the States Parties, electronic documents shall have the same legal effects as written documents, subject to the exceptions provided for in national laws.

The States Parties shall recognize the legal effects of electronic signatures where they are accepted as valid by the parties that use them or accepted by the persons to whom the document to which they are linked was presented.

The States Parties shall ensure that the evidentiary effects of an electronic document are not denied solely because it is not connected to an advanced electronic signature, if its authenticity and integrity can be unequivocally demonstrated.

The parties shall be free to agree mutually on the conditions under which they will accept electronic signatures, in accordance with their national laws.

Should one of the parties not recognize an electronic signature, it shall be up to the other party to prove its validity.

Article 5 – Advanced electronic signature: Mutual recognition

In order to ensure mutual recognition of advanced electronic signatures and digital certificates, the States Parties may conclude mutual recognition agreements with each other. The Common Market Group (GMC) shall adopt guidelines for that purpose. These guidelines shall reflect the state of affairs at the time of their adoption, and may be updated at the proposal of Working Subgroup (SGT) No. 13 in order to keep pace with the related technological developments.

Through mutual recognition agreements, advanced electronic signatures that meet the conditions set forth therein shall be accorded the same legal and probative value as is accorded to handwritten signatures.

The States Parties shall recognize the authenticity and integrity of an electronic document signed with an advanced electronic signature, accepting it as documentary evidence in a court of law in accordance with the provisions of the mutual recognition agreements.

In the framework of SGT No. 13, the States Parties shall indicate which bodies are authorized to sign the mutual recognition agreement.

Article 6 – Qualified digital certificates

The mutual recognition agreements shall establish the conditions under which digital certificates issued by a State Party to the agreement shall have the same legal validity in the other States Parties to the Agreement.

These conditions must require, at the minimum, that the digital certificates:

(a) are issued by a certification service provider that is accredited under the national accreditation and control system provided for in Article 7;

(b) respect the internationally recognized standard formats laid down by the implementing authority of each State Party;

(c) meet the minimum criteria set forth in the guidelines mentioned in Article 5;

(d) contain, at the minimum, sufficient data to:

1. identify beyond doubt the owner and the certification service provider that issued the certificate, indicating its period of validity and data by which its unique identity can be established;

2. be verifiable in terms of revocation status;

3. clearly differentiate between verified and unverified information included in the digital certificate;

4. be able to verify the signature;

5. identify the certification policy under which it was issued.

Article 7 – Provision of certification services

The States Parties shall not subject the provision of certification services to prior accreditation except in the case of those connected to an advanced electronic signature in accordance with the terms of this Resolution.

The States Parties shall create a suitable accreditation and control system for certification service providers established in their respective territories that issue qualified certificates by which advanced electronic signatures can be verified.

The States Parties may subject the use of electronic signatures and advanced electronic signatures in the public sector to possible additional requirements. These requirements shall be objective, transparent, proportionate, and non-discriminatory, and shall relate only to the specific characteristics of the application concerned. These requirements shall not act as an obstacle to cross-border services.

Article 8 – Liability

States Parties shall ensure, at the minimum, that a certification service provider accredited pursuant to Article 7 is liable for damage caused to any natural or legal person that had reasonable confidence in the digital certificate issued by that provider with respect to the following:

(a) all fields and data required by the respective national infrastructures for the qualified certificate are included and accurate at the time of issue;

(b) at the time the qualified certificate is issued by the accredited certification service provider, the signature identified therein reflects the signature creation data corresponding to the verification data contained in the provider's qualified certificate, in order to guarantee the chain of trust;

(c) any errors or omissions in the said qualified certificates or failure to follow the certification procedures established in the mutual recognition agreements;

(d) where appropriate, proper and timely registration of the revocation of the qualified certificates issued.

It is up to the accredited certification service provider to demonstrate that it acted neither negligently nor intentionally.

The States Parties shall ensure that the certification service provider accredited pursuant to Article 7 can indicate in a qualified certificate, in a manner that is identifiable by third parties, the limits of its utilization.

The certification service provider accredited pursuant to Article 7 shall not be liable for damage resulting from the utilization of a qualified certificate it has issued if such utilization exceeds the scope defined in its certification policy, nor shall it be liable for any inaccuracies in the qualified certificate resulting from verified information supplied by the owner, provided the accredited certification service provider can demonstrate that it has complied with all the conditions set forth in its certification policies and procedures.

Article 9 – Protection of personal data

The States Parties shall ensure that a certification service provider that issues qualified certificates for the public may only collect personal data directly from the person to which such data refer, after having obtained the express consent of that person and only to the extent that such data are necessary to issue and maintain the certificate. The data shall not be obtained or used for any other purpose without the express consent of the owner.

The States Parties shall guarantee the confidentiality of the other personal data required to issue the qualified certificate that do not appear therein, in accordance with the terms of this article.