Notes on E-signatures and Trade

Richard Hill[1], November 2017

In the WTO, some members have stated "that e-signature is a fundamental issue in any future consideration regarding electronic commerce in the WTO."[2] And some members have put forward proposals to discuss, and potentially negotiate binding rules, on the issue of e-signatures. Proponents have portrayed the issue of e-signatures as a technical issue under the broader concept of e-commerce. The issue has already been addressed by technical and legal experts through the United Nations Conference on International Trade Law (UNCITRAL). However, e-signatures may not be well understood by trade negotiators, and the proposals presented to WTO appear to have technical and legal implications, some of which may be unintended and may run counter to the UNCITRAL Model Law on Electronic Signatures which promotes a technology-neutral approach, pursuant to which a diversity of e-signature implementations already exist.

This note contains the following sections:

1. E-transactions and the role of e-signatures

In most jurisdictions, many contracts can be formed without any particular form requirement. In particular, they can be formed without signatures. It has long[3] been recognized that electronic exchanges are, for most commercial purposes, equivalent to electronic transactions.

Since signatures are generally not required for commerce, e-signatures are not generally required for e-commerce. However, signatures are generally required for payment orders. Any such signature requirements are based on national law. The figure below illustrates this situation.

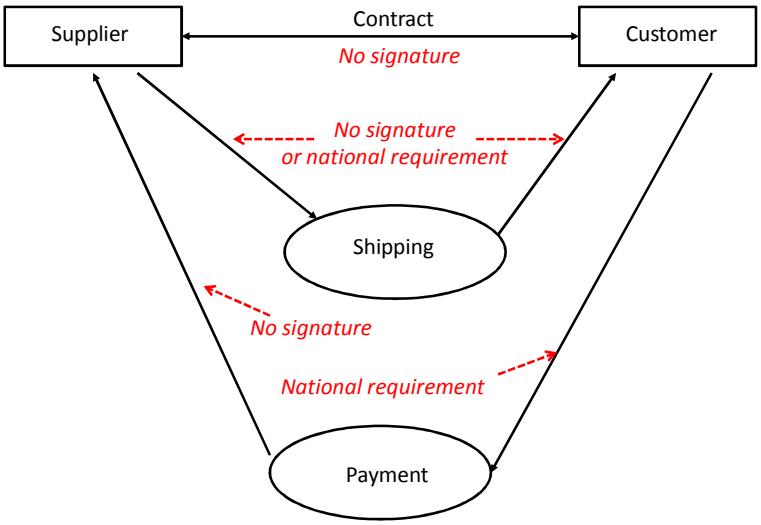
---

[1] Richard Hill, rhill@hill-a.ch, is a former official at the International Telecommunications Union.

[2] JOB/GC/115, JOB/CTG/3, JOB/SERV/247, JOB/IP/20, JOB/DEV/41 from Argentina, Brazil and Paraguay, 15 December 2016

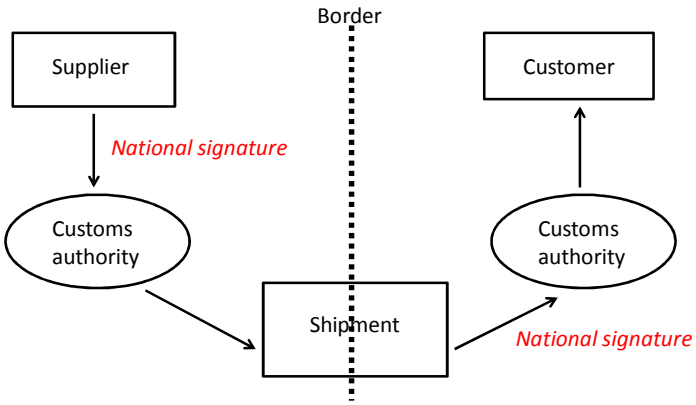
[3] An early US case, dating back to 1869, involved the formation of a contract by telegram: *Howley v. Whipple* 48 N.H. 487, 488, cited in Wright, B. (1991) *The Law of Electronic Commerce: EDI, FAX, and E-mail: Technology, Proof and Liability*, Little Brown and Company, page 284.

An international e-transaction
(without details of shipping)



In addition, in international trade, signatures may be required when goods are transferred from a supplier to a shipper and from a shipper to a customer, in particular for customs clearance purposes. The following figure illustrates the shipment process in more detail, in the case of international commerce. If the two concerned states have different standards for e-signature, then the e-signature of the supplier may not be recognized by the customs authority of the customer.

The international shipping process



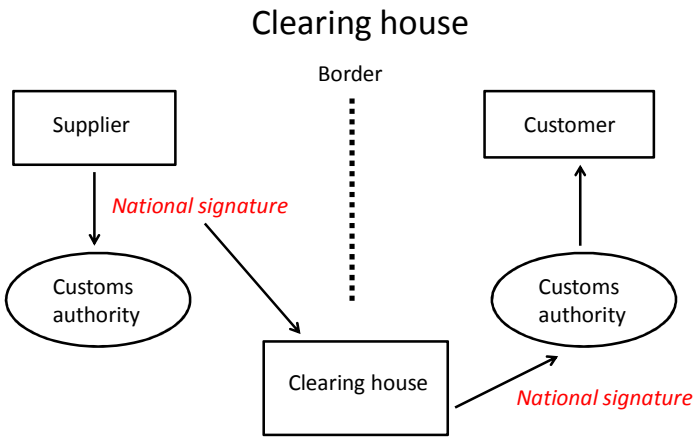
If the two national e-signature requirements are different, then the original e-signature cannot cross the border because it will not be recognized across the border

Solutions:

- International standard for e-signature for customs
- Clearing house

There are (at least) two solutions to the issues raised by the potential incompatibility of national e-signature standards. One is to agree on an international standard for e-signature. The second is to envisage a clearing house. The first solution is not practical: many states have implemented the UNICTRAL Model Law on Electronic Signatures, which promotes a technology-neutral approach, and therefore a diversity of e-signature implementations already exist.

The second solution would appear to be relatively straightforward to implement: a central organization could be able to recognize and authenticate the supplier's e-signature, and to convert it to the e-signature format required by the customer's customs authority. The slide below illustrates this solution.



The clearing house authenticates the original e-signature and generates a new e-signature in accordance with the norms of the other country

2. E-signature technologies

There are several security mechanisms or technologies that underlie e-signatures:

- Something you know (e.g. password)
- Biometrics (e.g. conventional personal signature)
- Encryption (e.g. which generally involves something you know, specifically, the encryption keys)
- Challenge-response (the remote system asks for something, e.g. a code, which only the authentic user can provide; commonly used challenge-response systems use the mobile network to transmit an SMS, or a specialized calculator to compute the response)
- Two factor
    - Something you have (e.g. a smart card, or a physical key) plus
    - Something you know (e.g. a password)
- Dual-channel communication (this is commonly used in order to counter the risk of a man-in-the-middle attack, that is, a situation where the user is communicating with an intruder and not with the desired remote system)
    - Personal Computer (used as one channel)
    - Mobile phone, post, etc. (used as the second channel, for example to send an SMS code used for challenge-response)

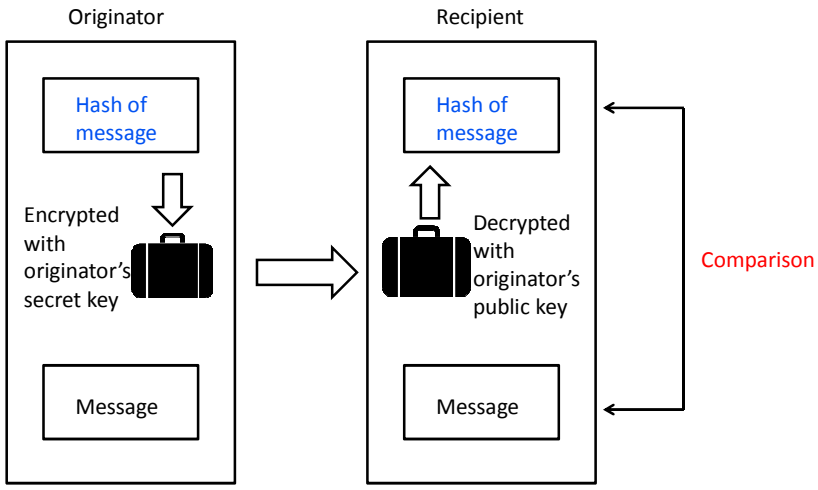
The above basic technologies can be combined in various ways to counter specific risks and to achieve an acceptable level of security.

For example, here are some specific technologies:

- Smartcard and PIN code (something you have plus something you know)
- Public Key Infrastructure (PKI)[4] – this is a set of protocols that permits encryption without requiring the exchange of secret keys via a secure channel: all communications take place over insecure channels.
    - Public-key encryption[5]
        - For web pages: this is in common use, with the HTTPS protocol[6]
        - As signature (see next slide)
    - Certificates: these are digital documents that certify that a given public key really is the public key of a given person.[7]
- Biometrics (e.g. signature, iris scan, fingerprints)
- Challenge-response via dual-channel (for example, in some e-banking systems the bank sends an SMS which the user must enter on the web site in order to authorize the payment order)

The next slide illustrates the functioning of signature via public key encryption. A "hash"[8] is a function that is applied to a message and that returns a code that (1) depends on every bit of the message and (2) is not likely to be the same as the hash for any other message.

Public key encryption used for e-signature



3. E-signature provisions proposed to WTO

---

[4] https://en.wikipedia.org/wiki/Public_key_infrastructure
[5] https://en.wikipedia.org/wiki/Public-key_cryptography
[6] https://en.wikipedia.org/wiki/HTTPS
[7] https://en.wikipedia.org/wiki/X.509#Certificates
[8] See https://en.wikipedia.org/wiki/Cryptographic_hash_function

The European Union has proposed that WTO members adopt the following provisions:

> 1. Members shall not deny the legal effect and admissibility as evidence in legal proceedings of electronic authentication and trust services solely on the basis that they are in electronic form.
>
> 2. Members shall not adopt or maintain measures for electronic authentication and trust services that would:
>
> (a) prohibit parties to an electronic transaction from mutually determining the appropriate electronic methods for that transaction; or
>
> (b) prevent parties from having the opportunity to prove to judicial or administrative authorities that their electronic transaction complies with any legal requirements with respect to electronic authentication and trust services.
>
> 3. Notwithstanding paragraph 1, a Member may require that, for a particular category of transactions, the method of electronic authentication or the trust service meet certain performance standards or be certified by an authority accredited in accordance with the Member's law.

Provision 2(a) above might be interpreted to allow dominant companies to impose insufficiently secure methods on consumers, via click-through contracts of adhesion. And it might be interpreted to invalidate national laws imposing certain consumer protection measures, such as minimum security requirements for contracts concluded with consumers.

It is important to recognize that e-signature is not just a technical or a trade issue: it involves national legal issues and social aspects of contract formation. That is, e-signature is a policy issue that has to be addressed by political instances that are accountable to their citizens in general, not just for international trade issues. Some non-technical, non-trade issues also arise with respect to proposals from China; and Argentina, Brazil and Paraguay; see below.

Provision 3 above might be used to create a technical barrier to trade if a state imposes specific technology (e.g. certification authority) for many transactions, for example all transactions over $100. That technical barrier to trade might result in an unfair advantage for national companies that provide the required technology or the required services. That is, this provision might provide a (no doubt unintended) method for creating barriers to open markets and it would thus negate the supposed advantages of such provisions for developing countries.

China has submitted a document[9] to WTO whose section 4.2 includes the following:

> If the parties enter into a contract in the form of letter or text in electronic data, a confirmation instrument may be required to be signed prior to the forming of a contract. The contract is formed at the time when the confirmation instrument is signed.

This provision would be contrary to current practices, in which signatures are typically not required for contract formation, whether by electronic or other means, and it would contradict the Vienna Convention on Contracts for the International Sale of Goods[10], whose Article 11 states: “A contract of sale need not be concluded in or evidenced by writing and is not subject to any other requirement as to form.”

---

[9] JOB/GC/142, JOB/CTG/9, JOB/SERV/271, JOB/DEV/49 of 19 October 2017.

[10] https://www.uncitral.org/pdf/english/texts/sales/cisg/V1056997-CISG-e-book.pdf

Argentina, Brazil and Paraguay have submitted to WTO a document (cited above) that appears to be more in the nature of an information note than a concrete proposal. The document contains a MERCOSUR Resolution, whose Article 4 contains the following provision:

> 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.

While this provision may be appropriate for the MERCOSUR countries, it could have unintended consequences elsewhere. In some jurisdictions, certain documents, for example last wills and testaments, have to be "in writing" and/or signed by hand not merely in order to authenticate the signer, but also to signify to the signer that he or she is agreeing to a document that has significant legal consequences. This motivation for a form requirement is referred to a *solemnitas*: it is a form requirement that makes the signer aware of the importance of his or her signature.

If the MERCOSUR proposal were adopted, then national parliaments would have to review their existing laws, and modify them so that documents for which *solemnitas* is required would be specified as exceptions to the general provision cited above. This does not appear to be a desirable way to proceed: why should a trade agreement trigger the need for a detailed review of national legislation not related to trade?

None of the proponents have identified any e-commerce transactions that are currently constrained because of the lack of these rules in the WTO.

In addition, in the October 2017 Statement by the African Group on The Work Programme on Electronic Commerce, this group, representing 42 members of the WTO, notes that:

> "we have already seen a number of submissions currently on the table that have been identified as international Internet public policy issues by the United Nations Commission on Science and Technology for Development in the Working Group on Enhanced Cooperation in November 2014. Several of these issues being brought into the WTO have been discussed at length by other international organisations that have policy authority over these issues, or they have been resolved in these international organisations. They include: … UNCITRAL Model Law on Electronic Signatures".

In sum, given that a fourth of the WTO membership oppose discussing e-signatures because the issue has already been resolved by UNCITRAL; proponents of new rules have failed to make a compelling case for new rules in the WTO; and proponents have also failed to acknowledge the important policy implications of their proposals, it seems quite premature to discuss rules on e-signatures in the WTO.