# RECOMMENDATION 14 REVISION WORKING GROUP

20TH UN/CEFACT FORUM MEETING, VIENNA, AUSTRIA

18 SEPTEMBER 2012

**Attendance**

**Present:**

Lance Thompson, Conex (FR) (Chair)
Gordon Cragge, TFAS UK (UK) (Editor)
Andrea Caccia, Hubzhub Anorc (IT)
Carlo Salomone, AITI-EACI (IT)
Christiaan Van Der Valk, Trust Weaver (SE)
Dominique Vankemmel, Normafret France (FR)
Eva Chan C.P., Djava Factory (MY)
Gérard Galler, EU Commission (EU)
Jae Sung Lee, UNCITRAL (AT)
Jari Salo, Tieke (FI)
Jean-Luc Champion, GS1 (BE)
Jean-Michel Kaliszewski, IATA (CH)
Marco Sorgetti, FIATA (CH)
Matti Olvukkamäki, Ministry of Employment and the Economy (FI)
Micahel Coffee, US Dept of State (US)
Nishio Shigetaka, JASTPRO (JP)
Peter Kustor, Federal Chancellery (AT)
Raffaella Migliorini, Ministry of Economy Consip (IT)
Siegfried Gruber, A-Trust (AT)
Soomin Park, KL-Net (KR)
SP Sahu, WCO (WCO)
Syed Tahir Hasnain, IATA (CH)

**Excused (absent but have shown interest):**

Nacho Alamillo (ES)
Hidetoshi Aramaki, NACCS (JP)
Josephine Baiamonte, CBP (US)
Steve Bisbee, ESRA (US)
Ervin Cano, Chamber of Commerce of Guatemala (GT)
Luca Catellani, UNCITRAL (KR)
Jina Choi, Cupia (KR)
Moudrick M. Dadashov, SSC (LT)
Ibrahima Diagne, Gainde (SN)
Christophe Hypolite, DGDDI (FR)
Hyun-Soo Kim, KLRI (KR)
Jonathon Koh, Crimson Logic (SG)
Luis Lahoz, Global Information Security
Jeong-Hyun Lee, KISA (KR)
Frédéric Leger, IATA (CH)
Jin-Soo Lim, KISA (KR)
Bill Luddy, UNCITRAL (US)
Stephen Mason, Lawyer (UK)
Charles Moore
Vitoriana Morais, ESRA (US)
Ken Moyle, ESRA (US)
Reinhard Posch, Austrian Government (AT)
JM Rietsch, FedISA (FR)
André Sceia, UNECE (CH)
Johan Stoopen, Dutch Customs (NL)
Gilles Taib, FedISA (FR)
Ivar Tallo, eGovernance Academy (EE)
Margo Tank, ESRA (US)
Nigel Taylor, GXS (UK)
Richard Triola, Settleware Secure Services Inc (US)

**General summary – overview**

As the first official meeting of the Working Group of the Revision of Recommendation 14, the day was planned around a series of presentations which were meant to provide a backdrop for considerations to be taken in the future work.
The presentations proved that there are a number of different implementations that exist around the world and that any future recommendation will need to remain technologically neutral and open to as many examples as possible, representing as many regions of the world as possible.
Some key points to be considered are presented in the last presentation “Next Steps Forward, group discussion” which takes some of the points that came out of the day’s discussions.

**Brief summary of each presentation (as it pertains to Rec-14 revision)**

**Rec-14 Overview of project & meeting schedule, Lance THOMPSON, Conex / group chair**

Brief reminder of the 1979 recommendation and elements which should be retained and others to be updated / modified / added to

- 1979 Rec14 seeks to encourage the use of electronic data transfer
- 1979 Rec14 seeks to eliminate a signature whenever possible
- 1979 Rec14 recommends to meet requirements (when a signature is deemed necessary) through authentication methods or guarantees that can be electronically transmitted

Scope of the present revision project was reminded

- removal of the requirement for a signature except where essential for the function of the document
- introduction of other methods to authenticate documents
- creation of a legal framework that permits and gives equal status to authentication methods other than signature
- regular review of documentation used for domestic and cross border trade, possibly by a joint public and private sector effort
- Guidelines (retracing much of the original format of the 1979 Rec14
- 2 Annexes (of case studies in legal enabling environments and technical solutions)

The relation with other UN/CEFACT projects

- The work of former proposed recommendation 37 can be encompassed in the first annex insofar as it reflects case studies & best practices
- Likewise, it is important to try to identify, again through actual implementations, the requirements for the creation of a "trusted/secure environment" for these alternative solutions (alternative to a manual signature).

**UNCITRAL documents and tools covering electronic signature, Mr. Jae Sung Lee, UNCITRAL**

Brief reminder of the organization of UNCITRAL and its workings.

E-Commerce is dealt with in Working Group 4. This group has an "Electronic transferable records" project since 2011.

The UNCITRAL texts covering e-commerce and electronic signatures were negotiated with universal participation reflecting a balance of regional, economical, legal and other interests and compatible with various legal traditions.

Basic principles in UNCITRAL documents covering electronic signatures:

- Non-discrimination (communication should not be denied validity on the sole grounds that it is in electronic form)
- Functional equivalence (purpose & function of paper- based requirements may be satisfied with electronic communications, provided certain criteria are met)
- Technology neutral (equal treatment of different technologies and does not favor one over the others)
- Party autonomy

Four documents cover electronic signature:

- Model Law on e-Commerce (MLEC), June 1996
    - Art.7:
    - (1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:
        - *(a)* a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
        - *(b)* that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

    - (2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.
- Model Law on e-Signatures (MLES), July 2001
    - Defines a signature, gives equal treatment of signature technologies, defines when an electronic signature is deemed reliable
- e-Commerce Convention (ECC), Nov 2005. Entry in force in 2013. Becomes binding for States that become a party to the Convention – 16 signatories.
    - Electronic communication method identifies a party and indicates that party's intent in respect to the information contained in the electronic communication
    - The method used is as reliable as appropriate for which the electronic communication was generated or proven to have fulfilled the function of identity and intention by itself or together with other evidence.
- Promoting Confidence in electronic commerce (2007)
    - Is more a manual for the general public to better understand the main legal issues regarding signatures and authentication methods and cross border use of electronic signatures and authentication methods

**Presentation of the proposal for a EU regulation on electronic identification and trust services for electronic transactions which is intended to replace the Electronic Signature Directive, Mr. Gérard Galler, European Commission**

12 years after the e-Signature directive, the EU Commission proposes this new law to aims at boosting trust and convenience in electronic transactions in order to encourage their usage and thus enhance the EU internal market. The proposed law intends to establish interoperability and ease usage of solutions across EU Member States

- It plans to ensure that electronic trust services have the same legal value as in traditional paper-based processes.
- It establishes mutual recognition of electronic identification schemes among the Member States as well as the recognition of essential trust services, namely electronic signatures electronic seals, time stamping, electronic delivery, electronic documents acceptability and website authentication
- The regulation is technology neutral.
- electronic signature can only be created by natural persons,
- eSeals are established for legal persons as document authentication instrument. It is technically similar to signature but its legal meaning is smaller than signature
- Establishes security assurance levels
    - Simple electronic signature
    - Advanced electronic signature
    - Qualified electronic signature (has equivalent legal affect to a handwritten signature)

**e-Signature State of Play in Austria, Peter Kustor, Austrian Chancellery**

Brief review of the application of the 1999 e-Signature Directive into Austrian Legislation.
Explanation on how a qualified signature is produced in Austria (advanced electronic signature + qualified certificate + Secure Signature Creation Device (SSCD)

- Advanced electronic signature = uniquely linked to signatory, capable of identifying the signatory, created using means under the signatory's sole control, linked to the data it relates to in such a manner that subsequent change of the data is detectable.
- Austrian Citizen Card concept is not necessarily a "smart-card"; example was given with cell phone SMS which provides a 5-minute token to 'sign' data
- Recognition of other Member States' / countries' signatures using their national signature cards (AT, BE, EE, FI, IS, IT, LT, PT, SP, SE, CH, Lichetenstein)

- Public authorities sign documents using an advanced signature; their logo and content of the official signature is then visualized on view of the data it is signing. This signature can then be verified on a third authority's website.
- Reminder that Member States of the EU are cooperating in some key policy areas (eID interoperability, eHealth, eJustice, Services Directive, eProcurement)

**Observation on the status of use and regulation of digital and other electronic signatures, Mr. Christiaan Van Der Valk, Trustweaver / ICC**

Electronic signatures and other types of evidence which enable the exchange of electronic information/documents is a multidisciplinary field. It involves not only technical competence but also regulatory. However lawyers are often being excluded from implementations… and technical people don't necessarily know what the purpose is…

Evidence is something that must be thought about while you are doing the transaction. It is not only about making it right at a certain date and time, but also being able to prove it in 5 or 10 years…

Complete absence of requirements of evidence breeds negligence; complete prescription is breed form over substance.

Past examples have proven that as the transaction becomes more complex or a harder control process, and the higher the legal and/or commercial value of the data or document… the stronger the types of proof (leading to a strong digital signature).

Three different levels of evidence assurance presented in this framework: e-commerce (with a process audit trail), e-business (with a medium electronic or digital signature), e-government (with strong digital signature).

**Experience in South-East Asia on trans-boundary trade, Eva Chan, Djava Factory**

(No slides available, but most information available on the Pan-Asian Alliance website).

The experience of the Pan-Asian, a group of service providers that are sometimes the national single window, sometimes major service providers for international trade.

Each member of the PAA agrees to use same standards for sharing data and common messaging for core document exchanges.

Documents exchanged do not necessarily need to be signed by the end-user as they are transiting a secure network of service providers (true for invoice, AWB, Seaway Bill…). In this case, the service provider (PAA member) must sign the envelope (ebXML).

Other documents (such as Certificate of Origin) will require a digital signature (often PKI), requirement of the destination regulatory authority. In this case, there is a network of PAA suggested certification authorities that can produce these digital signatures for the data transmission. The actual digital signature is between the service providers.

**e-AWB: the road to e-Freight, Syed Tahir Hasnain, IATA**

General presentation of IATA e-AWB and how it fits into the IATA e-Freight program (which aims at enabling the dematerialization of around 20 core supply chain documents).

In order to enable the dematerialization of the e-AWB for example, it is necessary for the departure and the destination countries to have signed either the Montreal Convention of 1999 or the Montreal Protocol of 2004 (both countries must have signed the same agreement). This effectively allows the data to be transmitted electronically and retain its legal effect.

Then the two partners (the one who is producing the e-AWB and the airline who will receive it) must sign a bilateral agreement to replace the Warsaw Convention Airway Bill (this document has on the front side the information relative to the goods to be transported and on the reverse side the terms and conditions of contract). This bilateral agreement will replace the reverse-side terms and conditions of contract and set down the details for the data transmissions.

Then the data can be sent using the industry defined standard, FWB (or xFWB) without any supplemental authentication. (There is a "signature" data-element which can be used, but which would only be a typed in name).

Other industry defined standard messages (Houseway Bill, Flight Manifest, etc.) do not need any authentication for their exchange.

**GS-1 Identification Keys, Jean-Luc Champion, GS-1**
General presentation of GS-1, its structure and its recommended standards.
Several GS1 Standards (here we spoke mainly of bar codes) allow for the identification (of companies, of places, of products), and allow to share these identification information with other actors on the Supply Chain. This is achieved through the first digits of the bar codes. The national GS1 agency attributes to companies that request (paying process) an identification number, they can then use this ID number as the beginning of all of their bar codes.
A project (Florida Flower Importers) was presented at the WCO IT Conference in Tallinn in May 2012 which foresees the reuse of the GTIN (Item/Product Identification code bar) for regulatory identification of the actors and the products. The US Health Department can in this way receive more specific information about the traders and the products allowing them to capture the more detailed information necessary for their regulatory procedures. Thus transfer of data without any authentication.

**A-Trust experience with electronic signatures in Austria, Mag. Siegfried Gruber, A-Trust**
Brief presentation of A-Trust and its history with electronic signatures.
A reminder of some of the points seen during the morning session with Mr. Kustor of the Austrian Chancellory.
A bit more detail on the different solutions that are available and that seem to go beyond the qualified signatures presented in the morning.
The citizen card solution is suggested as a good solution (as now there are only about 200,000 issued certificates issued (for 8 million population of Austria). If these citizen cards were obligatory, as they are in some other EU countries (BE, EE), it would be a good way to create e-ID for all citizens and promote interoperability with other existing solutions in the EU.
Signature of PDF documents and batch signatures (to sign multiple documents at the same time) were also described.
However, we are still far from interoperability within the EU since it is often not possible for recipients in other countries to verify the signatures of documents signed using the Austrian-defined solution, using standard software products.

**Electronic Signatures and the US Customs Single Window ACE, Lance Thompson for US CBP delegate unable to attend**
Very complete presentation of the legislative framework which enables electronic data exchange (and obliged government agencies to create electronic solution).

- Computer Security Act, 1987
    - Improve security and privacy of sensitive information; requires creation of computer security plans
- Paperwork Reduction Act, 1995
    - Requires Federal Agencies to study the requirements for information collected (aiming to reduce information collection burden on the public)
- Government Paperwork Elimintation Act (GPEA), 1998
    - Use of electronic process, when practicable, as a substitute for paper & use and acceptance of electronic signatures
    - The Office of Management and Budget (OMB) establishes levels of sensitivity of a transaction - low risk information processes may need only minimal safeguards while high risk processes may need more.
    - The OMB also provides some examples of what types of transactions are considered high risk processes.

    - Electronic records and their related electronic signatures are not to be denied legal effect, validity or enforceability merely because they are in electronic form.
    - Defines an electronic signature: identifies, authenticates, shows the "intent"
- Electronic Record and Signatures in Global and National Commerce Act (E-SIGN), 2000
    - Eliminates legal barriers to the use of electronic technology to form and sign contracts, collect and store documents, and send and receive notices and disclosures.
- Customs Modernization Act (Mod Act), 1993
    - Codification of automation, providing for an automated electronic system.
    - Gives same legally binding effect to electronic transmissions through EDI system as to signed documents

Example of implementation of these above regulations in the Customs and Border Protection (CBP) Single Window "Automated Commercial Environment (ACE)".
The trader or broker and CBP sign a series of agreements (ACE terms and conditions, Interchange agreement, etc.). Which then enable the transfer of data from the trader or broker to CBP using a VPN. The VPN is then the means of authentication of the trader or broker and guarantees the integrity of the data transmitted.

**Next steps forward, group discussion**
Three real deliverables are identified here:

- The recommendation – it is hoped to do most of the writing on this before the end of the year. Some points to be taken into consideration include
    - Levels of sensitivity / security assurance levels (wording to be worked) and recommended level of authentication corresponding to each level (EU defines three, US define at least two, UNCITRAL does not define levels but states that this should be taken into consideration)
    - It is essential as a proposed UNECE Recommendation that the work remains technology neutral.
    - Both technical aspects and legal aspects should be considered. Not to neglect retention periods and recuperation of data during those periods for example.
    - Definitions and functions should be as close to UNCITRAL document as possible; look if there are cases where these do not apply
- Annex 1 on legally enabling implementations
    - Establish a template for submission of data – to think about the key characteristics to be considered. (Perhaps find inspiration in the Rec 14 template for submissions)
    - It will then be important to try to deduce a common checklist for consideration as introduction to the annex.
- Annex 2 on technical implementations enabling electronic data transfer
    - Use typologies in UNCITRAL "Promoting Confidence…" document (page 17, point 24) to group similar solutions and allow an easier lecture for future readers of the recommendation.
    - Must consider other typologies for examples like the above IATA example or GS1 example…

First Conference call is planned for mid-October. Exact date to be decided by a general consensus. Three dates are tentatively planned as option: 17, 24 or 25 October (each would be planned at 13:00 in order to allow Asia and US to participate).

This summary is pending approval by the different speakers. It is intended to be finalized by Friday, Sept 21st, 2012.