Rec 14 Revision Working Group

UN/CEFACT 20th Forum, Vienna, AT
Tuesday, September 18th 2012
Lance THOMPSON, Chair
Gordon CRAGGE, Editor
The 1979 version of Rec-14

- Authentication of Trade Documents by Means other than Signature
- Approved and published in 1979
- Seeks to encourage the use of electronic data transfer in domestic & cross border trade
- Remove signatures where possible
- Meet requirements through authentication methods or guarantees that can be electronically transmitted
The 1979 version of Rec-14

RECOMMENDATION

Recommends to Governments and international organizations responsible for relevant intergovernmental agreements to study national and international texts which embody requirements for signature on documents needed in international trade and to give consideration to amending such provisions, where necessary, so that the information which the documents contain may be prepared and transmitted by electronic or other automatic means of data transfer, and the requirements of a signature may be met by authentication guaranteed by the means used in the transmission; and

Recommends to all organizations concerned with the facilitation of international trade procedures to examine current commercial documents, to identify those where signature could safely be eliminated and to mount an extensive programme of education and training in order to introduce the necessary changes in commercial practices.
The 1979 version of Rec-14

Structure of the original recommendation

- Recommendation
- Background to current requirements for a handwritten signature
  - Definition
  - Function
  - Requirement of signature
    - Commercial documents, Transport documents, Financial documents, Official documents
  - Signature and proof
- Alternative Methods
  - Methods available
  - Security of data
  - Responsibility for data transmission
- Conclusions
- Annex:
  - Definition
  - Jurisprudence from Belgium
  - Conventions & other recommendations
  - SWIFT
The 1979 version of Rec-14
Some problems with the 33 year old Rec.

• Vocabulary problems
  – “Signature” does not only imply “manual” signatures as it might have 33 years ago
  – Definition provided perhaps regional specific

• Technical problems
  – Some technical solutions are suggested in §18
  – ‘counter-signing’ and retention period need to be reviewed

• Updating content
  – Multiple references to customs should be opened up to all regulatory process
  – Annexes are dated. Need to bring in more recent examples.
Recommendation 14 Revision
Project Proposal

The scope of a revised Recommendation 14 could, based on the present recommendation, include the following content:

Recommendations

• 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
Recommendation 14 Revision
Project Proposal

Guidelines
• definition and function of signature
• requirement for signature on trade documentation
• signature and proof of authenticity, integrity and veracity
• other options than signature
• approval, registration and authorisation to use other authentication methods
• security of data, including transmission
• data transmission issues (who, what, when, where, how)
• conduct of trade document review process
• checklist for the creation of a legally enabling environment
• checklist for functional requirements of digital evidence (integration of the work of the previous draft Recommendation 37)

Annexes
• Case stories - a repository of practical examples of the removal of signature from trade documents
  — Both from a legal point of view and a functional point of view
• Examples of technological solutions for dematerialisation of trade documents.
Project Deliverables

- A revised recommendation text with recommendation and guidelines, possibly with a repository of case studies and a separate annex listing examples of existing technological solutions.
- A revised recommendation text aiming to be universal and durable in time
- Accompanied by two different types of annex to be updated in light of any future evolutions of legal framework or technical advances
  - Annex of checklists for the implementation of electronic signatures and other means of electronic authentication (legally enabling environment, functional requirements...)
  - Annex of a repository of case studies of existing technological solutions – either from their legal framework point of view or their functional implementation point of view – or ideally both (which would be one of the main basis of the previous annex)
Parallel work that has been conducted within UN/CEFACT concerning the functional aspects of a specific type of authentication – digital signatures – could be easily integrated, insofar as it reflects the reality of actual implementations, as it is closely related to the topic and the latest draft of the document (from December 2011) reads like a functional checklist.

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).

To note that these are examples of implementations that replace (manual) signatures by other technological alternatives; others will most likely be identified. Finally, all of these technical solutions available could be included in a repository (separate from the Recommendation itself) which could be easily updated as it evolves.
Sept 18th Working Group Meeting

Proposed Agenda

First morning session, begins at 9:00

• General presentation of Recommendation 14 and the proposed Revision Working Group
  – Lance THOMPSON, Conex / UN/CEFACT
• Presentation on base UNCITRAL documents and tools covering Electronic Signature
  – Mr. Jae Sung LEE, Legal Officer International Trade Law Division, UNCITRAL
• Break at 10:00
Sept 18th Working Group Meeting

Proposed Agenda

Second morning session, resumes at 10:30

• 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, Policy Officer, European Commission

• Austrian Electronic Signature solution
  — Mr. Peter KUSTOR, Head of eGovernment Legislation, Federal Chancellery, Austria

• Trustweaver
  — Mr. Christiaan VAN DER VALK, CEO

• Q&A, Comments, Discussions, Break at 12:15
Sept 18th Working Group Meeting

Proposed Agenda

First afternoon session, resumes at 14:00

• IATA e-AWB & e-Freight and authentication
  – Mr. Tahir Hasanain SYED, Manager Cargo Standards Electronic Messages

• GS1. Authentication in dematerialized exchanges.
  – Mr. Jean-Luc CHAMPION, GSMP eCom Process Manager

• A-Trust electronic signature experience in Austria
  – Mag. Siegfried Gruber, Consultant

• US CBP Electronic Signature in the Customs Single Window ACE
  – Presented by Lance THOMPSON for CBP expert, unable to attend

• Q&A, Comments, Discussion, Break at 15:30
Proposed Agenda

Second afternoon session, resumes at 16:00
• Compare the day’s presentations to the 1979 version of Recommendation 14
• Draft how future work will need to be split up & set calendar for conf. calls and work
• Set date for conference call
• End session at 17:00
Presentation on base UNCITRAL documents and tools covering Electronic Signature

Mr. Jae Sung LEE
Legal Officer International Trade Law Division, UNCITRAL

Sept. 18th Rec-14 WG Meeting
The work of UNCITRAL in electronic commerce

Jae Sung LEE
Legal Officer, UNCITRAL
Office of Legal Affairs
United Nations
When and why was UNCITRAL established?


The core legal body of the UN system in the field of private international trade/commercial law.

Mandate: Progressive harmonization and modernization of international trade law by preparing and promoting the use of legislative and non-legislative instruments in key areas of commercial law.
United Nations System

Office of Legal Affairs (OLA)

- Office of the Legal Counsel
- General Legal Division
- Treaty Section
- Codification Division
- International Trade Law Division
- Division for Ocean Affairs and the Law of the Sea

UNCITRAL
United Nations Commission on International Trade Law

Other UN Entities
- UNOPS United Nations Office for Project Services
- UNICEF United Nations Children’s Fund
- UNFPA United Nations Population Fund
- UNDP United Nations Development Programme
- UNHCR United Nations High Commissioner for Refugees
- ILO International Labour Organization
- UNESCO United Nations Educational, Scientific and Cultural Organization
- WHO World Health Organization
- IMF International Monetary Fund
- OECD Organisation for Economic Co-operation and Development
- ITU International Telecommunication Union
- WIPO World Intellectual Property Organization
- ILO International Labour Organization
- WTO World Trade Organization
- WMO World Meteorological Organization
- UNODA Office for Disarmament Affairs
- DPA Department of Political Affairs
- SDS Department of Safety and Security
- OCHA Office for the Coordination of Humanitarian Affairs
- DESA Department of Economic and Social Affairs
- DPI Department of Public Information
- OHRLLS Office of the High Representative for the Least Developed Countries, Landlocked Developing Countries and Small Island Developing States
- OHCHR Office of the United Nations High Commissioner for Human Rights
- UNDRC United Nations Registry Centre
- UMO United Nations Multimedia Office
- UNDOC United Nations Office on Drugs and Crime
- UNV United Nations Volunteers
- UNWFPA United Nations Women's Fund
- UNWTO World Tourism Organization
- ILO International Labour Organization
- UNESCO United Nations Educational, Scientific and Cultural Organization
- WHO World Health Organization
- IMF International Monetary Fund
- OECD Organisation for Economic Co-operation and Development
- ITU International Telecommunication Union
- WIPO World Intellectual Property Organization
- UNODA Office for Disarmament Affairs
- DPA Department of Political Affairs
- SDS Department of Safety and Security
- OCHA Office for the Coordination of Humanitarian Affairs
- DESA Department of Economic and Social Affairs
- DPI Department of Public Information
- OHRLLS Office of the High Representative for the Least Developed Countries, Landlocked Developing Countries and Small Island Developing States
- OHCHR Office of the United Nations High Commissioner for Human Rights
- UNDRC United Nations Registry Centre
- UMO United Nations Multimedia Office
- UNDOC United Nations Office on Drugs and Crime
- UNV United Nations Volunteers
- UNWFPA United Nations Women's Fund
- UNWTO World Tourism Organization
- OLA Office of Legal Affairs
Composition of UNCITRAL

• 60 member States elected by the General Assembly considering geographical regions and levels of economic development
• Non-member States participate as observer States and no difference in deliberation
• Term of 6 years with half (30) of the members reelected or replaced every 3 years (elections to be held on Nov 12, 2012)
Organization of work

- The Commission
- Working Groups
- The Secretariat
The Commission

- Annual sessions held alternately in New York and Vienna ('12 New York, '13 Vienna)

- Work at the sessions:
  - Finalization and adoption of draft text referred to the Commission by the working group
  - Consideration of progress reports of the working groups
  - Selection of topics for future work or research
  - Reporting on technical assistance activities
6 Working Groups

I. Procurement  
II. Arbitration  
III. Online Dispute Resolution  
IV. Electronic Commerce  
V. Insolvency Law  
VI. Security Interests

- Two sessions per year alternating between New York (spring) and Vienna (fall)
6 Working Groups

6 Working Groups

- WG IV (Electronic Commerce): Electronic transferable records (2011~)


The Secretariat

• 14 professional staff, mostly lawyers
• Director: Renaud Sorieul
• Main Tasks:
  - Preparation of reports and draft texts
  - Provision of technical assistance to States in need of law reform
  - Coordination with other relevant organizations
UNCITRAL Texts

- Negotiated with universal participation and reflect balance of national, regional, economic, legal and other interest
- Drafted with a view to ensure compatibility with the various legal traditions including Islamic law
- Methods operate at different levels and involve different types of compromise or acceptance
- Move from a hard law to soft law
UNCITRAL Texts

- **Conventions** - Designed to unify law by establishing binding legal obligations
- **Model Law** - A legislative text recommended to States for enactment as part of their *domestic* law
- **Legislative Guide** - A set of principles and legislative recommendations for legislators to consider in their enactment of *domestic* law
Convention on the Recognition and Enforcement of Foreign Arbitral Awards
(New York, 1958)

Convention pour la reconnaissance et l'exécution des sentences arbitrales étrangères
(New York, 1958)

Convención sobre el Reconocimiento y la Ejecución de las Sentencias Arbitrales Extranjeras
(Nueva York, 1958)


United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea
UNCITRAL Model Law on International Commercial Arbitration
1985
With amendments as adopted in 2006

UNCITRAL Model Law on International Commercial Conciliation
with Guide to Enactment and Use
2002

UNCITRAL Model Law on Electronic Commerce
with Guide to Enactment and Use
1996
with additional article 5 as adopted in 1998
Coordination

- Mandate to coordinate the work of organizations active in the field of international trade law both within and outside the United Nations' system, to encourage cooperation between them, avoid duplication of effort and promote efficiency, consistency and coherence

World Bank, OECD, WIPO, UNCTAD, UN-ESCAP, UN-ECE, UN-ESCWA, European Union, APEC, ASEAN as well as Unidroit and the Hague Conference
Electronic Commerce

- 2007 - Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods
- 2001 - UNCITRAL Model Law on Electronic Signatures with Guide to Enactment
- 1995 - UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, with additional article 5 bis as adopted in 1998
- 1985 - Recommendation on the Legal Value of Computer Records
UNCITRAL Texts on Electronic Commerce

- Provides comprehensive legal framework for electronic transactions
- Based on the following underlying principles:
  - Non-discrimination
  - Functional equivalence
  - Technological neutrality
  - Party autonomy
Non-discrimination

A communication shall not be denied validity on the sole ground that it is in electronic form.

Conclusion of contract
(Writing, Signature)
Functional equivalence

Purposes and functions of paper-based requirements may be satisfied with electronic communications, provided certain criteria are met.
Technological neutrality

- Equal treatment of different technologies (EDI, e-mail, Internet, instant messaging, fax, etc.)
- Possibility to have detailed provisions on technology requirement in the regulations implementing e-commerce legislation.
• Adopted by UNCITRAL on 12 June 1996.

• The UNCITRAL Model Law on Electronic Commerce (MLEC) is intended to facilitate commerce via the use of modern means of communications and storage of information.

• The MLEC is based on the establishment of a functional equivalence in electronic media for paper-based concepts such as "writing", "signature" and "original".

• The MLEC established rules for the formation and validity of contracts concluded with electronic means and for the attribution and retention of data messages.
Article 7. Signatures

(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.
• Adopted by UNCITRAL on 5 July 2001.

• The Model Law on Electronic Signatures (MLES) aims at bringing additional legal certainty to the use of electronic signatures.

• The MLES establishes criteria of technical reliability for the equivalence between electronic and hand-written signatures.

• The MLES follows a technology-neutral approach, which avoids favoring the use of any specific technical product.

• The MLES establishes basic rules of conduct that may serve as guidelines for assessing possible responsibilities and liabilities for the signatory, the relying party and trusted third parties intervening in the signature process.
Article 2. Definitions

(a) “Electronic signature” means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory’s approval of the information contained in the data message;

Article 3. Equal treatment of signature technologies

Nothing in this Law, except article 5, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in article 6, paragraph 1, or otherwise meets the requirements of applicable law.
Article 6. Compliance with a requirement for signature

1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, ....

3. An electronic signature is considered to be reliable ... if:
   (a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;
   (b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
   (c) Any alteration to the electronic signature, made after the time of signing, is detectable; and
   (d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.
Article 7. Satisfaction of article 6

Article 8. Conduct of the signatory

Article 9. Conduct of the certification service provider

Article 10. Trustworthiness

Article 11. Conduct of the relying party

Article 12. Recognition of foreign certificates and electronic signatures
• Adopted by the General Assembly on 23 November 2005.

• The Electronic Communications Convention (ECC) builds up and, in certain cases, updates the provisions of both Model Laws.

• The ECC aims at enhancing legal certainty and commercial predictability where electronic communications are used in relation to international contracts.
Article 9. Form requirements

3. Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if:

(a) A method is used to identify the party and to indicate that party’s intention in respect of the information contained in the electronic communication; and

(b) The method used is either:

   (i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or

   (ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.
Entry into force of the ECC

- Entry into force on 1 March 2013
- States parties: Dominican Republic, Honduras & Singapore
- 16 other signatories (Central African Republic, China, Colombia, Iran, Lebanon, Madagascar, Montenegro, Panama, Paraguay, Philippines, Republic of Korea, Russia, Saudi Arabia, Senegal, Sierra Leone, Sri Lanka)
- Australia, Thailand, Sri Lanka have declared intention to adopt
- Other States have adopted substantive provisions of the ECC domestically
Promoting confidence in electronic commerce (2007)

• Analyzes main legal issues regarding
  ✔ Signatures and authentication methods
  ✔ Cross-border use of electronic signatures and authentication methods
For more information, please visit the UNCITRAL web site @ http://www.uncitral.org/
or e-mail me at jaesung.lee@uncitral.org
Break

Discussions resume at 10:30
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, Policy Officer, European Commission

Sept. 18th Rec-14 WG Meeting
European Commission’s proposal for a Regulation on Electronic identification and trust services for electronic transactions in the internal market

Gérard GALLER
Policy Officer
European Commission - DG ConNECT
Gerard.galler@ec.europa.eu
Elisa, a Belgian student wants to enrol **online** to a University in Italy.

Albeit she has an eID card, **it does not work** because her Belgian eID **IS NOT RECOGNISED** in Italy.
Problem statement – example #2

- A French SME wants to do business electronically with an Italian counterpart.
- What about the respective requirements for trust services like e-signatures, seals, documents, time stamps, delivery?
- Are cross-border services technically feasible? May be…
- Will they be legally recognised?

Result:
Where do we stand in EU?

- **EU legal framework for eSignatures** (Directive 1999/93/EC)
- Excellent but incomplete EU standards framework on eSig. and related electronic trust services
- **No EU legal framework for related electronic trust services**
- **No EU legal framework for eID**
- Few widely accepted standards on eID (management)
- Large **EU Member States + industry investments** especially for eSignature and eID
After three years of feedback gathering...

- **Informal consultations and discussions:**
  - from Action Plan on eSig. & eID, 28.11.08, COM(2008)798
  - with **European Parliament**
  - with **EU Member States**
    - Multilateral meetings
    - Services Directive technical group on e-procedures
  - with **private and public stakeholders**
    - **FESA** (Forum of European Supervisory Authorities) meetings
    - **Public online consultation** Feb-Apr 2011
    - **SME survey** Oct-Dec 2011
    - Liaison with **large scale project**, especially **STORK**
    - Participation to **public conferences**
    - Numerous **bilateral meetings** with stakeholders

- **Studies** (IAS Study, Crobies, IDABC studies, ...)
- **12 years of** operation of eSig Directive
- Mandatory **“Impact Assessment”** report
What is the legislative proposal's ambition?

- To strengthen EU Single Market by boosting **TRUST** and **CONVENIENCE** in secure and seamless cross-border and cross-sector electronic **TRANSACTIONS**
Who will benefit from the proposal?

13 million EU citizens work in another EU country

21 millions of SMEs of which a significant part is working internationally

Some 150 million EU citizens shop online. However, only 20% of them buy goods and services from another EU state.
1. By ensuring that people and businesses can use their national eIDs to access online services in other EU countries.
2. By removing the barriers to the internal market for e-Signatures and related online trust services across borders

\[ \rightarrow \]

i.e. by ensuring that trust services have the same legal value as in traditional paper-based processes.
What is the scope of the proposed Regulation?

1. Mutual recognition of electronic identification

2. Electronic trust services:
   - Electronic signatures interoperability and usability
   - Electronic seals interoperability and usability
   - Cross-border dimension of:
     1. Time stamping,
     2. Electronic delivery service,
     3. Electronic documents admissibility,
     4. Website authentication.
How does it work for mutual recognition of eID?

A EU Member State:

1. May ‘notify’ the ‘national’ electronic identification scheme(s) used at home, at least, for access to public services;
2. Must recognise ‘notified’ eIDs of other Member States for cross-border access to its online services which require e-identification by its national laws;
3. Must provide online free ID data authentication facility;
4. Is liable for unambiguous identification of persons and for authentication;
5. Should allow the private sector to use ‘notified’ eID
6. Must take part to a coordination mechanism at EU level
What is foreseen for electronic trust services?

Common Principles:

• Technological neutrality
• Mutual recognition of «qualified» electronic trust services
• Strengthens and harmonises national supervision of qualified trust service providers and trust services
• Reinforces data protection + obligation for data minimisation
• Uses delegated and implementing acts as a mechanism to ensure flexibility vis-à-vis technological developments and best practice
What is foreseen for electronic trust services?

**eSignature**

- Builds on existing eSignature infrastructure and clarifies concepts related to eSig. (natural persons)
- Introduces eSeals (legal persons)
- Allows for full reference to standards
- Clarifies validation of qualified eSignatures
- Ensures long term preservation
- Allows «server / remote» and «mobile» signing
What is not covered?

- The proposal does not require / address / contain:
  - Member States to have an eID scheme
  - Member States to notify their eID scheme(s)
  - «soft ID» (ex. Facebook)
  - «Notified» eIDs are not necessarily ID cards
  - "EU database" of any kind
  - "EU eID«
  - Prior authorisation to start qualified service or accreditation
  - Details on trust services other than eSig / eSeals
  - Persons’ roles and/or attributes
  - Format of e-documents
  - Establishment of proof
  - Encryption
Why will it make a difference? (1/2)

- **Creates confidence in electronic trust services:**
  - Effective state supervision
  - Systematic usage of "trusted lists"
  - De facto world class «trustmark» for EU qualified services

- **Easy eSignature:**
  - Harmonisation power of Regulation
  - Full eSig specification via secondary legislation + standards

- **Related trust services:**
  - Address clear market needs: eSeals, eDelivery, eDocuments, …
  - Harmonise national legislation: time stamping, eDelivery
  - e-Document admissibility: « big bang » for de-materialisation
  - Website authentication is an implicit expectation of the citizens
Why will it make a difference? (2/2)

- Comprehensive “toolbox” of trust building instruments
  - One single legislation across EU
  - Harmonisation power of Regulation
- Foster eID usage (“world premiere”):
  - Leverage eID cards and mobile ID infrastructure
  - Reliable eID to allow cross border eBusiness and enable eGov services
  - Private sector is invited to build on «notified» eIDs
  - Leverage Large Scale Pilot project STORK
Indicative timeline

**Legislative process**
- Cyprus Presidency report
- Parliament + Council adoption

**Standardisation mandate m460**
- Standards
- Delegated/Implementing acts
- Commission Decisions

|------|------|------|------|------|------|

**NB. Dates are indicative**
For further information

- **Website:**

- **Draft Regulation:**
Provisions of the proposed Regulation

- **Ch 1: General Provisions**
- **Ch 2: Electronic identification**
- **Ch 3: Trust services**
  - **Sec 1: General Provisions**
  - **Sec 2: Supervision**
  - **Sec 3: Electronic signature**
  - **Sec 4: Electronic seals**
  - **Sec 5: Electronic time stamp**
  - **Sec 6: Electronic documents**
  - **Sec 7: Qualified electronic delivery service**
  - **Sec 8: Website authentication**
- **Ch 4: Delegated acts**
- **Ch 5: Implementing acts**
- **Ch 6: Final provisions**
- **Annexes I, III, IV: Qualified certificates**
- **Annex II: Qualified eSig creation devices**
Ch 1. General Provisions

- **Legal basis:** Art 114 TFEU (internal market)

- **Art 1, Art 2: Subject matter and scope**
  - Cover mutual recognition & acceptance of
    - "notified" eID
    - "electronic trust services" (eSig, eSeals, eDoc, time stamping, eSig/eSeal long term preservation service, certificates, website authentication)
  - « Toolbox » of trust services: usage is NOT mandatory

- **Art 3: Definitions**
  - Trust services do not encompass eID (subsidiarity)
  - **Qualified** = matching the requirements of the Regulation
  - Qualified trust service providers (QTSP) and trust services (QTS)
  - **eSig creation device:** SW or HW used to create an eSig

- **Art 4: Internal market**
  - Free “movement” of trust services and related products
  - Mutual recognition and acceptance of trust services
Ch 2. Electronic identification

- **Art 5:** **Legal effect:**
  - Mutual recognition and acceptance of “notified” e-identification schemes
  - Natural and legal persons

- **Art 6, Art 7:** **Notification mechanism:**
  **A Member State:**
  1. May ‘**notify**’ to Commission the ‘national’ electronic identification scheme(s) used at home, at least, for access to public services;
  2. **Must** recognise and accept ‘notified’ eIDs of other Member States for cross-border access to its online services requiring e-identification under its national laws;
  3. **Must** provide online free ID data **authentication** facility;
  4. **Is liable** for unambiguous identification of persons and for authentication;
  5. **May** allow the **private sector** to use ‘notified’ eID

- **Art 8:** **Coordination mechanism** between Member States to ensure eID means interoperability and enhance security
Ch. 3. Trust services (TS)  
Section 1. General provisions

- **Art 9: Liability:** TSP is liable for what it does (similar to e-sign Dir)

- **Art 10: International aspects:**
  - Mutual recognition of QTS and Q-certificates
  - Mutual recognition only via international agreements
  - 3rd country TS must comply with EU data protection, security and supervision levels

- **Art 11: Data processing and protection**
  - Stronger and unlimited reference to data protection directive
  - Obligation of data minimisation

- **Art 12: Accessibility for disabled persons**
  - Services and products «accessible» whenever possible

- **Generic three-pronged approach:**
  - Technologically neutral definition (non discrimination)
  - "Qualified" secure level (with legal effect)
  - Presumption of compliance (if voluntary standards are matched)
Ch. 3. Trust services
Section 2. TSP and TS Supervision (1/2)

- **Art 13, 14: Supervision**
  - National or «regional» supervision authority
  - Common essential supervision requirements of Q-TSPs
  - **Cooperation between Supervisors:**
    - Mutual supervision assistance
    - Yearly supervision report
    - Collection of market statistics from Q-TSPs and Supervisors
    - Exchange of good practices between Supervisors (↔ FESA)
  - **MS to ensure long term availability of trust data of Q-TSPs**
Art 15: Requirements on Q and non Q-TSPs:
- Obligation of security due diligence for Q and non Q-TSPs
- Security breach notification obligation for Q and non Q-TSPs
- Binding instructions by Supervisors to Q and non Q-TSPs

Art. 16: Supervision of Q-TSPs
- Q-TSP subject to at least yearly audit
- Supervisor can issue binding instructions to Q-TSP. Supervisor can remove “Qualified” status.

Art. 17: Initiation of Q-Trust services
- Mandatory notification to Supervisor
- No prior authorisation

Art. 18: Trusted Lists:
- EU trusted lists of Q-TSs and Q-TSPs (SD Decision 2009/767/EU)

Art. 19: Requirements for Q-TSPs:
- Issuance certificates: face-to-face OR remotely using «notified» eID
- Mandatory on-line standardised certificate status info (ex. OCSP)
- Other reliability and professionalism requirements similar to ex-Annex II
Ch. 3. Trust services
Section 3: eSignatures (1/2)

• **Art. 3 (definitions): eSignature:**
  - eSig. = “data in e-form attached to or logically associated with other e-data and which are used by the signatory to sign”
  - Natural persons only
  - Advanced eSig. (AeS): adapted to allow server signing and make « sole control » manageable

• **Art. 20: Legal effects and acceptance of eSignatures**
  - Qualified eSig. (QeS) has “equivalent legal effect” to handwritten signature
  - Mutual recognition and acceptance of QeS
  - Allows for classification of eSignatures with security assurance levels < QeS
  - Security of AeS may be defined via standards
  - Security assurance requirements higher than QeS are forbidden for public services
Ch. 3. Trust services  
Section 3: eSignatures (2/2)

- Art. 21 and Annex I: Qualified Certificates for eSignature
  - Fully defined in Annex I: exact mandatory content
- Art 3.17, 22-24: Qualified signature creation devices Q-SCD
  - Extended scope of creation devices: HW or SW to create an eSig.
  - Certification of Q-SCD (ex. ISO 15408 “Common criteria”)
  - European positive list of certified Q-SCD
- Art 25-26: Validation
  - Defines when a QeS is valid
  - Defines Q-validation service provider (new)
- Art 27: Preservation of eSignatures
  - Defines Q-long term preservation service (new)
- Art 34.4: eSig formats for public services:
  - Administrations to accept a minimum common set of standardised eSig formats (= SD Decision 2011/130/EU: CAdES, XAdES, PAdES)
Ch. 3. Trust services

- **Section 4. eSeals**
  - Legal persons only
  - Instrument for document authentication: “data in e-form attached to or logically associated with other e-data to ensure origin and integrity of the associated data”
  - «mutatis mutandis» like eSignature

- **Section 5. Time stamping**
  - Legal existence of time stamps
  - Defines qualified time stamps («date certaine»)

- **Section 6. eDocuments**
  - Non discrimination «paper vs e-documents»
  - Presumption of authenticity and integrity of Q-signed/sealed eDocuments
Ch. 3. Trust services

- **Section 7. eDelivery**
  - Legal effect: certainty of cross-border electronically delivery
  - Establishes qualified eDelivery services
  - NB. Assumes national legislation will establish equivalence of e-delivery and paper «lettre recommandée»

- **Section 8. Website authentication**
  - Only establishes legal existence of qualified website authentication certificates
Ch 4 and 5. Secondary legislation

- **Ch 4: Delegated acts**
  - Art. 38: Standard provision for delegated acts

- **Ch 5: Implementing acts**
  - Art. 39: Standard provision for implementing acts:
    - “Examination procedure”
    - Qualified majority
Ch 6. Final provisions

- **Art 40:** Reporting every four years
- **Art 41:** Repeal Directive 1999/93/EC
  - SSCDs already certified as SSCDs become QSCDs
  - Existing Q-Certificates will remain valid max. five years
- **Art 42:** Immediate entry into force
  - 20 days after official publication following adoption by European Parliament and Council by the «ordinary procedure» (ex-codecision)
eSignatures
State of Play in Austria

Mr. Peter KUSTOR,
Head of eGovernment Legislation,
Federal Chancellery, Austria

Sept. 18th Rec-14 WG Meeting
eSignatures
- State of Play in Austria

UN/CEFACT – Revision of Rec 14 WG

Peter Kustor
Vienna, 18 September 2012
Peter.Kustor@bka.gv.at
Agenda

- 1. eSignature in Austria – overview and legal frame
- 2. The Austrian Citizen Card
- 3. eDocuments from businesses and citizens
- 4. eDocuments issued by Public Authorities
- 5. EU interoperability outlook
eSignature – overview and legal frame

- EU Signature Directive (1999/93/EC)
  - AT Signature Ordinance 2008 (3/2008 replacing the Ordinance from 2000)
What is a “Qualified Signature”?

Qualified Signature = advanced el. signature
+ qualified certificate
+ SSCD
Advanced Electronic Signature

- is uniquely linked to the signatory
- it is capable of identifying the signatory
- it is created using means that the signatory can maintain under his sole control
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable
Advanced Electronic Signature

- is uniquely linked to the signatory
- it is capable of identifying the signatory
- it is created using means that the signatory can maintain under his sole control
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable
„is uniquely linked to the signatory“

- the signature-creation-data used for signature generation (and the corresponding signature verification data) can practically occur only once
Advanced Electronic Signature

- is uniquely linked to the signatory
- it is capable of identifying the signatory
- it is created using means that the signatory can maintain under his sole control
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable
„it is capable of identifying the signatory“

Authenticity

- practically impossible to create the same key pair twice
- ensured that a signature that is verifiable using signature verification data (public key in the certificate) has been created with the corresponding signature-creation data (private key)
- practically impossible that signature-creation data can be derived
Advanced Electronic Signature

- is uniquely linked to the signatory
- it is capable of identifying the signatory
  - it is created using means that the signatory can maintain under his sole control
  - it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable
„using means that the signatory can maintain under his sole control“

- Signature-creation authorised only by the signatory
- Multifactor authentication: knowledge and possession

Does “can maintain under sole control” mean that it must be ensured by hardware means? NO!

„…to be assumed that ‘sole control’ can be achieved with appropriate technical or organisational means even with software certificates […] … security measures need to be in place providing that the signatory can enforce his sole control…“ (RV 293 BlgNR 23. GP)

– see also FESA - working paper on advanced electronic signatures and “Public Statement on Server Based Signature Services”: “…FESA members believe that sole control at least of the signature creation data can be achieved and that advanced electronic signatures can be created by a server based signature service…“!
Advanced Electronic Signature

- is uniquely linked to the signatory
- it is capable of identifying the signatory
- it is created using means that the signatory can maintain under his sole control
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable
„it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable“

Integrity

- practically impossible that different electronic data result in the same signature or can be created from a given electronic signature.
Advanced Electronic Signature

- is uniquely linked to the signatory
- it is capable of identifying the signatory
- it is created using means that the signatory can maintain under his sole control
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable
Qualified Signature?

Qualified Signature = advanced el. signature

+ qualified certificate

+ SSCD
Qualified Certificate

Certificate content
Annex I
1999/93/EC

Requirements
Annex II
1999/93/EC

Annex I
1999/93/EC

Annex II
1999/93/EC
Certificate Content (Annex I)

- indication that the certificate is issued as a qualified certificate
- identification of the CSP and the State in which it is established
- name of the signatory (or a pseudonym identified as such)
- signature-verification data which correspond to signature-creation data under the control of the signatory
- beginning and end of the period of validity of the certificate
- identity code of the certificate
- advanced electronic signature of the CSP issuing it

Further options: limitations on scope, value of transaction, specific attributes of the signatory
Requirements on the CSP (Annex II)

- reliability necessary for providing certification services
- secure directory and a secure and immediate revocation service
- precise date and time when a certificate is issued or revoked
- verify identity and, if applicable, specific attributes of the signatory
- personnel with expert knowledge, experience, and qualifications (managerial level, electr. signature technology, security procedures)
- trustworthy systems and products - protected against modification and ensuring the technical and cryptographic security;
- measures against forgery of certificates, and, in cases where the CSP generates signature-creation data, guarantee its confidentiality
- sufficient financial resources (to bear the risk of liability for damages)
- etc.
Qualified Signature?

Qualified Signature = advanced el. signature + qualified certificate + SSCD
SSCD

- Confirmation by a designated body (Art. 3(4) of 1999/93/EC)
- According to Art. 3 para 4 second subpara of the Directive, these attestations ("determination of conformity with the requirements laid down in Annex III") are to be recognised by all Member States.
Qualified Signature?

Qualified Signature = advanced el. signature + qualified certificate + SSCD
Agenda

- 1. eSignature in Austria – overview and legal frame
- 2. The Austrian Citizen Card
- 3. eDocuments from businesses and citizens
- 4. eDocuments issued by Public Authorities
- 5. EU interoperability outlook
Citizen card concept

- The Austrian citizen card is a concept, not a specific technology

- The Citizen Card combines
  - Qual. electronic signature/declaration of intent → Authentication
  - Unique electronic identity → Identification
  - data on representation, mandates → Representation
Citizen “Cards”

Cards:
- Health insurance cards: 100% coverage, activation free of charge for citizens
- Official’s service card
- Certification service provider signature cards
- Student service cards, etc.

Mobile phone signatures:
- Started 2009 with support of the European Commission (part of the EU Large Scale Pilot “STORK”)
- Free of charge for citizens
eID citizen card function

Access to e-business:
- eSignature
- eBanking
- eBilling
- eProcurement
- CyberDoc
- Archivium
- eDelivery

Within administration:
- eSignature
- eRegisters
- eFile System

Access to e-gov:
- eForms
- eHealth
- eDelivery
- eDocument-Safe
- eUniversity
- eVoting
Server Side – Open Source Programme

- Basic modules for integration into applications
  - Open Source, free for public & private sector
- MOA – Module for On-line Applications
  - Identification (MOA-ID)
  - Signature validation / creation (MOA-SS/SP)
  - Electronic delivery (MOA-ZS)
  - Representation (MOA-VV)
  - Official signatures (MOA-AS)
Demo

Vergleichswert: urLM6Fosrh

Signaturdaten anzeigen
TAN: 2fs3n

Signieren

Log On at HELP ONLINE

Compare Value: urLM6Fosrh
Your TAN
(5min valid): 2fs3n

Aktuelle Angebote
- Geburt, Heirat, Alleinerziehung, Scheidung,
  Lebensgemeinschaften, etc.
- Sozialversicherungen
  Pension, Erbsen, Rodilfen,
  Arbeitnehmerveranlagung, etc.

Aktuell
- Aktuell Winterreifenfahrt November
- Aktuell Thermische Sat
mobile phone signature

- server-based citizen card solution for
- qualified electronic signatures via mobile phone
- familiar technology and comfortable alternative to the current smartcards
- important step towards usability and dissemination of modern eGovernment services because
  - no software installation on the local PC, just the browser,
  - no special computer skills and
  - no card readers are needed for use.
- No requirement on the mobile phone or SIM
  - Just receiving SMS
Mobile phone signature

- Core Aspects
  - Operated by a Certification Service Provider (CSP) for qualified certificates
  - Signature-creation data (cryptographic keys) kept at CSP but controlled by the signatory
    - 2-factor authentication (knowledge & possession) as known from smartcards
  - Secure Signature-Creation Device
    - 1999/93/EC Annex III, confirmed by a notified body
Registration possibilities

- „self registration“ using a qualified signature (existing citizen card):
  
  https://www.handy-signatur.at/

- Registration authorities/ registration officers at various institutions (expanding: finance authorities, post offices…)
  
  https://www.a-trust.at/Aktivierung/ro/OfficerData.aspx?t=mobile

- Using „trusted systems“ (currently e.g. FinanzOnline, registration via online banking in cooperation with telecom providers)
Agenda

- 1. eSignature in Austria – overview and legal frame
- 2. The Austrian Citizen Card
- 3. eDocuments from businesses and citizens
- 4. eDocuments issued by Public Authorities
- 5. EU interoperability outlook
eDocuments from businesses and citizens

- Citizen Card in all forms (card-based or Mobile Phone Signature) allows for qualified electronic signature of eDocuments
- The qualified signature satisfies the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data (Art. 5 Signature Directive)
- These – legally valid - authentic eDocuments are used for eGovernment as well as private purposes (eCommerce/ eBanking/ contracts/ eBilling/ eProcurement …)
Open source tools for using the citizen card

MOCCA
Modular Open Citizen Card Architecture

- Application – PDF-AS
  - Web server
- Server side integration
- Browser plus applet
  - Basis card-access functions
  - No local installation
  - Minimum footprint
MOCCA and non-AT signature cards

Currently integrates cards from
- Austria
- Belgium
- Estonia
- Finland
- Iceland
- Italy
- Liechtenstein
- Lithuania
- Portugal
- Spain
- Sweden
- Switzerland

Example for verification of a test document signed with a number of foreign cards
(Test verification instance including also the test certificates)
Open source signature tools

- **Online signature possibility**
  - E.g. https://www.buergerkarte.at/pdf-as/?locale=en

- **Local installation**
  - MOCCA
    http://webstart.buergerkarte.at/mocca/
  - PDF-OVER
    https://www.buergerkarte.at/pdf-signatur.en.php
  - Signature verification

- **All open source software:**
  - www.egovlabs.gv.at and NEW:
Open source tool for signature: e.g.: “PDF-OVER”
Agenda

- 1. eSignature in Austria – overview and legal frame
- 2. The Austrian Citizen Card
- 3. eDocuments from businesses and citizens
- 4. eDocuments issued by Public Authorities
- 5. EU interoperability outlook
The "Official signature" is an advanced el. signature of an authority.

It facilitates recognition of the fact that a document originates from an authority.

The signature certificate includes a specific attribute.

It has to be visualized with certain elements.
Different implementations regarding visualization of eSignatures

Minimum content:
- Logo of the authority
- Explicit information that it was “officially signed”
- Information needed for the verification of the electronic signature and the printout
Signature verification

Follow the link in the individual document for information or go directly to the signature verification service of the AT Supervisory Authority for electronic signatures

www.signature-verification.gv.at
The verification procedure and result

- Upload doc.
- See:
  - Signatory
  - Verification successful
  - Valid certificate chain
  - (Poss. manifest)
  - Link to detailed report
Detailed report (signed by RTR)

- Details on
  - Certificate
  - Signature type
  - Signature attribute „official signature“
  - ...

- Signed by Supervisory Authority
Documents issued by Public Authorities

- § 18 of the General Administrative Procedure Act 1991 foresees that (since 1.1.2011)
  - Official documents issued **electronically** have to bear an **official signature** (§ 19 E-GovG)
  - Official documents issued on **paper** have to be
    - **manually signed** by the official approving the document or
    - manually **certified** by the office, indicating that the document corresponds with the document approved by the responsible official UNLESS
    - the paper document is the printout of an electronic document which bears an **official signature**. In this case, no further requirements need to be met.
Agenda

- 1. eSignature in Austria – overview and legal frame
- 2. The Austrian Citizen Card
- 3. eDocuments from businesses and citizens
- 4. eDocuments issued by Public Authorities
- 5. EU interoperability outlook
EU outlook – the legal perspective

- June 2011: Proposal of the EC for a new EU Regulation on electronic identification and trust services for electronic transaction in the internal market
EU outlook – the interoperability perspective

- ICT Policy Support Programme
- 2007 – 2013, € 730 million budget
- Large Scale Pilots to support key policy areas
- Focus on cross-border aspects

- Next step: CEF
Member States cooperate in key policy areas

- eID interoperability
- eHealth
- eJustice
- Services Directive
- eProcurement
Interoperability across Europe...

ECAS:
~ 700 applications connected
~ 260,000 users
~ 200,000 logins/day
Thank you
for your attention!

Peter Kustor
Federal Chancellery of Austria
Department I/11 - E-Government –
Legal, Organisational and International Issues

Ballhausplatz 1
1014 Vienna
Peter.kustor@bka.gv.at
http://digitales.oesterreich.gv.at or
http://digital.austria.gv.at
Trustweaver
Electronic signature solutions

Mr. Christiaan VAN DER VALK
CEO

Sept. 18th Rec-14 WG Meeting
“e-Signatures”

Observations on the status of use and regulation of digital and other electronic signatures
ICC Commission on Digital Economy

- International Chamber of Commerce (ICC) ICC, the World Business Organization, promotes the market economy, cross border trade and investment, and entrepreneurship.
  - National Committees and groups in 140 countries
  - UN observership, long-standing relationship with UNCITRAL in many fields
  - Incoterms, UCP500, Court of Arbitration
- Digital Economy Commission
  - Business leaders and experts drawn from the ICC membership establish the key business positions, policies and practices on e-business, information technologies and telecommunications through the EBITT Commission and its task forces.
  - Members are from users and providers of information technology and electronic services from both developed and developing countries
  - UNCITRAL e-commerce, e-signature, e-contracting work contributions
  - GUIDEC: “e-signature” best practices since 1997
Multidisciplinarity = complexity

Recommendation 14 « If it is perfectly possible to envisage replacing the signature, why are people still so attached to it? The explanation may be found in the value of proof which a signature provides. »

Doing something well and subsequently proving that are two completely different things. This is hard to understand for the techies in the basement….where did the lawyers go?

Expressing consent, semantically, is a specific subcase of the previous statement. Doing it well vs proving that…

Data cannot be its own proof.

Complete freedom of evidence breeds negligence (if it isn’t required…); complete prescription breeds form over substance.
e-Signature law legacy

- Acknowledge that “paving the way” top-down legislation has produced mixed results
- Many assumptions have turned out to be somewhat off…some a little more
- You can have both legal certainty/interop and general freedom of evidence
« Evidence assurance »

Complex or hard to control process

Simple or highly controlled process

Legal and/or commercial value of data or document

Strong digital signature

Medium electronic or digital signature

Process /audit trail approach

E-commerce

E-business

E-Government
Q&A, Comments, Discussions
Lunch Break

Lunch & Learn for those interested
(12:30 to 13:00) on Confluence website

Discussions resume at 14:00
IATA e-AWB & e-Freight and authentication

Mr. Syed Tahir HASNAIY, Manager Cargo Standards Electronic Messages

Sept. 18th Rec-14 WG Meeting
e-AWB: the road to e-freight

UNCEFACT 20th Session, Vienna
18th Sept 2012
Agenda

1. The e-freight vision
2. What is the e-AWB?
3. Why doing e-AWB?
4. How does the e-AWB work?
5. The pre-requisites for e-AWB
6. Industry support
The e-freight program targets at modernizing the Air Cargo business

“e-freight aims to take the paper out of the air cargo supply chain and replace it with cheaper, more accurate and more reliable electronic messaging”
The e-freight scope encompasses the complete Air Cargo Supply Chain

1. Invoice
2. Packing List
3. Certificate of Origin
4. Letter of Instruction
6. CITES Certificate*
7. Air Waybill
8. House Waybill
9. House Manifest
10. Export Goods Declaration
11. Customs Release Export
12. Security Declaration*
13. Flight Manifest*
14. Freight Booked List*
15. Export Cargo Declaration
16. Import Cargo Declaration
17. Transfer Manifest
18. Transit Declaration*
19. Import Goods Declaration
20. Customs Release Import
What is the Air Waybill?

The Air Waybill (AWB) is the contract of carriage between the ‘shipper’ (e.g. forwarder) and the ‘carrier’ (airline).
e-AWB paves the way for e-freight

Benefits & Shipments

Number of documents & Complexity

Jan 2013: e-freight mandates e-AWB!
Cathay Pacific in Hong Kong shows that e-AWB was the first step to increase e-freight volumes.
Time has come for e-AWB

- The e-AWB is an electronic cargo contract that is an alternative to the paper AWB contract
- With e-AWB, the paper AWB is removed
- The electronic AWB (e-AWB) simplifies the air cargo process for all parties including Regulators
- The e-AWB is specified in the IATA Recommended Practice (RP) 1670
- The e-AWB was developed by the industry (airlines and forwarders) in 2008 and 2009
- The move to e-AWB is endorsed by the FIATA (International Association of Freight Forwarders Associations)
Many airlines have already implemented e-AWB
Some are achieving 100% penetration on their home market

100 to 70 %
- Cathay Pacific Cargo
- DRAGONAIR
- Emirates SkyCargo

70 to 20 %
- Airfrance KLM Cargo
- LAN Cargo

20 to 1 %
- Delta Cargo
- Korean Air Cargo
- Swiss WorldCargo
- Lufthansa Cargo
- cargolux
The airline industry set aggressive targets to move to e-AWB

- **2012**: 15% e-AWB where feasible*
- **2013**: 70% e-AWB where feasible*
- **2014**: 100% e-AWB where feasible*

* Feasible: On MC99 and MP4 routes
e-AWB current penetration status
All involved parties benefit from e-AWB

- Reduction in processing cost due to the removal of paper AWB
- Greater accuracy of AWB data
- Reduction in cargo handling delays due to missing or illegible paper AWB
- Elimination of the requirements to file paper AWB
- Real-time access to AWB information for all personnel from all locations
- First step towards a paper free air cargo
The e-AWB has two key components

Paper AWB

Front (600a)

Reverse (600b)

Electronic messages + Signed e-AWB agreement

e-AWB
Example for an e-AWB compatible process

**Freight Forwarders**
- Prepare Consol
- Resolve Issues (with airline if any)
- Deliver Freight

**Service Providers**
- FWB*
- FNA
- FMA
- FSU/RCS

**Airlines**
- Receive Information
- Identify Issues (with forwarder if any)
- Acknowledgement (with forwarder if any)
- Receive Freight
- Freight Acceptance (produce cargo receipt)

*: FWB and possibly FHL messages are sent
Pre-requisites for success with e-AWB

The following dimensions should be validated when embarking on the e-AWB journey:

- Origin and destination countries have signed the MP4 or MC99 convention
- National regulations applicable on the route allows for electronic contracts and transactions
- AWB related procedures set by local authorities create a favorable environment for e-AWB (no systematic request for paper AWB)
IATA Standards and Tools - Overview

Standard tools
- Functional specifications
- Model e-AWB agreement (RP1670)
- CIMP and CXML standards
- e-learning solution
- Presentations, FaQ, Glossary

Engagement
- FIATA communiqué
- Airline press releases e.g. CX, EK
- Engagement campaign results
- List of countries accepting e-AWB and plain paper AWB
- Reporting scorecards
- e-freight Matchmaker: e-AWB reports

Information at www.iata.org/e-awb

Questions at cargo@iata.org
e-Learning

http://www.iata.org/training/courses/Pages/tcgp72.aspx

IATA Electronic Airwaybill (e-AWB)

Read more in Arabic, English, French, Spanish, or Russian.

**Description**

This training is designed for staff of Airlines and freight forwarders, intending to adopt e-AWB at countries where MP4 or MS9 has been signed and local customs has e-Customs modernization program in place as well as another stakeholders - Shippers, Export & Import customs, Ground handling agents (GHA) and Customs agents/brokers.

**What you will learn**

Upon completing this course you will have the skills to:

- Acquire necessary knowledge of implementation of e-AWB, core concepts and terminology.
- Use the technology supporting e-AWB and understand how Standardized messages facilitate communication between the shipper/freight forwarder, carrier and other interested parties.
- Understand the necessary steps that carriers and shippers/freight forwarders are required to follow in order to successfully adopt e-AWB.
- Facilitate the steps for implementing e-AWB and ensure that access to resources that will help your organization in this area are available.

**Who should attend**

This course is recommended for:

- Freight forwarders
- Airlines
- Ground handling agents (GHA)
- Customs agents/brokers
Thanks!

More information
www.iata.org/e-AWB

Questions at cargo@iata.org

e-AWB on-line training

http://www.iata.org/training/courses/pages/tcgp72.aspx
GS1. Authentication in dematerialized exchanges

Mr. Jean-Luc CHAMPION
GSMP eCom Process Manager

Sept. 18th Rec-14 WG Meeting
GS1 Identification
Keys
A need for global standards...

What happens when there aren’t global standards?

- Inefficiencies
- Increased risk
- Lost opportunities
... to meet the needs of the supply chains in different sectors

- Efficiency
- Safety
- Collaboration
- Sustainability

- in Retail & Consumer Goods
- in Healthcare
- in Transport & Logistics
- and more...
GS1: The Global Language of Business

GS1 is a neutral not-for-profit organisation driven by its users, that facilitates collaboration amongst trading partners, to create more efficient, safer and sustainable value chains through global standards.
GS1 is both global and local

GS1 Global Office
Identification, creation, development and maintenance of standards and our foundational architecture, coordination with other international bodies, development of training programmes...

GS1 Member Organisations
Local offices in 111 countries around the globe
Implementation of standards, local regulatory adjustments, community management and relationship management with local governments and regulatory agencies...
Global reach, local presence

111 Member Organisations
1,500,000 member companies
150 countries served
2,000 people helping us
Some of the world’s best-known companies sit on our Board...just to name a few!
GS1: A global system of standards
GS1 System of standards

- Identify
- Capture
- Share
GS1 ID keys – The foundations of a common language in the supply chain

GS1 Identification Keys provide a common way to accurately identify anything in the supply chain

These globally-recognised numbers uniquely identify a product, pallet, assets or location, so that interested parties can get relevant information about them.
GS1 Identification Keys

Companies
- GS1 Company Prefix
- Global Location Number (GLN)
- Electronic Product Code (EPC) Manager Number

Product
- Global Trade Item Number (GTIN)
- Serialized Global Trade Item Number (SGTIN)

Pack, Case, Pallet
- Global Trade Item Number (GTIN)
- Serialized Global Trade Item Number (SGTIN)
- Serial Shipping Container Code (SSCC)

Location
- Global Location Number (GLN)
- Serialized Global Trade Item Number (SGTIN)

Services
- Global Service Relation Number (GSRN)
- Global Document Type Identifier (GDTI)

Assets
- Global Individual Asset Identifier (GIAI)
- Global Returnable Asset Identifier (GRAI)
GS1 System of standards

- Identify
- Capture
- Share
From barcodes to RFID, capturing supply chain data efficiently

GS1 Barcodes and GS1 EPC/RFID ensure automatic identification of products or assets along the supply chain.

Tracking product shipments, tracing medical devices in hospitals, managing inventory in stores, facilitating check-out... **GS1 data carrier standards** help companies improve many **critical business processes**.
GS1 System of standards

- Identify
- Capture
- Share
GS1 Standards help companies share different types of business data

Physical movement of goods throughout the supply chain

Business data shared between trading partners

- **Master data**: technical information about a product, such as weight and size of the product, case, pallet – synchronised with GS1 GDSN
- **Transaction data**: such as order, dispatch advice, invoice - exchanged automatically with GS1 eCom
- **Physical event data**: information about the movement of a trade item or logistical unit – shared with GS1 eCom or GS1 EPCIS
The three elements of global data synchronisation

When combined, they provide a powerful environment for secure and continuous synchronisation of reliable data on product information.

- Global Data Synchronisation Network
- Data Quality (Data Quality Framework)
- Product Classification (Global Product Catalogue)
GS1 Identification
Keys
GS1 Identifications Keys

- Keys administered by GS1 and fully under its control:
  1. GTIN - Global Trade Item Number
  2. GLN - Global Location Number
  3. SSCC - Serial Shipping Container Code
  4. GRAI - Global Returnable Asset Identifier
  5. GIAI - Global Individual Asset Identifier
  6. GSRN - Global Service Relation Number
  7. GDTI - Global Document Type Identifier
  8. GINC - Global Identification Number for Consignments
  9. GSIN - Global Shipment Identification Number
  10. GDCN – Global Digital Coupon Number
Global standards for business

• Developed by business users worldwide since 1973.

• Provide a common platform for trade and commerce in all countries and sectors.

• Designed to enable automatic identification systems throughout supply chains and to be used within e-business messages.

• Used by over a million organisations worldwide.
GS1 Identification Keys

• Identification is the foundation of the GS1 Core System

• GS1 Identification Keys are defined independently of carrier technology:
  • Technology never alters the meaning of the GS1 data.

• A GS1 Company Prefix assigned to a user company may be used to create any GS1 Identification Key
  • The single exception GS1 Identification Keys that are assigned one by one by a GS1 Member Organisation
What is a GS1 Identification Key?

A GS1 Key provides access to information – often master data - held in computer files.
GS1 Identification Keys

- **Item identifier = GTIN**
  - Global Trade Item Number
- **Logistics unit identifier = SSCC**
  - Serial Shipping Container Code
- **Location identifier = GLN**
  - Global Location Number

- **Unique**
- **Non-significant**
- **International**
- **Secure**
- **Foundational**
**GS1 Identification Key properties**

- **Unique**: every variant of an item is allocated a separate unique number.
- **Non-significant** structure: they identify an entity but provide no information about it.
- **International**: GS1 Identification Keys may be used in all countries and all sectors.
- **Secure**: GS1 Identification Keys have a defined structure and most include Check Digits.
- **Foundational**: to many business solutions: compliant bar coding; traceability; data synchronisation; etc.
What do GS1 Keys identify?

- Products and services (trade items)
- Physical locations and parties
- Logistics units
- Assets (including returnable transport items)
- Consignments
- Shipments
- Service recipients (customers, employees, etc.)
- Documents
- Coupons
GS1 Identification Keys in detail

• **Global Trade Item Number (GTIN)**
  - to identify any item (product or service) upon which there is a need to retrieve pre-defined information and that may be priced, or ordered, or invoiced at any point in any supply chain..

• **Global Location Number (GLN)**
  - to identify any physical location or party, such as a warehouse location or company using eCOM messages.

• **Serial Shipping Container Code (SSCC)**
  - to identify any logistics unit of any composition constructed for transport or storage.
Global Trade Item Number (GTIN)
• All GTINs may be recorded unambiguously if right-justified in a 14-digit field.

• Explicit leading zeroes may or may not be required depending upon the usage.

<table>
<thead>
<tr>
<th>Data structure</th>
<th>GTIN recorded in 14-digit field</th>
</tr>
</thead>
<tbody>
<tr>
<td>GTIN-14</td>
<td>$N_1 \ N_2 \ N_3 \ N_4 \ N_5 \ N_6 \ N_7 \ N_8 \ N_9 \ N_{10} \ N_{11} \ N_{12} \ N_{13} \ N_{14}$</td>
</tr>
<tr>
<td>GTIN-13</td>
<td>0 $N_1 \ N_2 \ N_3 \ N_4 \ N_5 \ N_6 \ N_7 \ N_8 \ N_9 \ N_{10} \ N_{11} \ N_{12} \ N_{13}$</td>
</tr>
<tr>
<td>GTIN-12</td>
<td>0 0 $N_1 \ N_2 \ N_3 \ N_4 \ N_5 \ N_6 \ N_7 \ N_8 \ N_9 \ N_{10} \ N_{11} \ N_{12}$</td>
</tr>
<tr>
<td>GTIN-8</td>
<td>0 0 0 0 0 0 0 $N_1 \ N_2 \ N_3 \ N_4 \ N_5 \ N_6 \ N_7 \ N_8$</td>
</tr>
</tbody>
</table>
Allocating the numbers

• Each GS1 Member Organisation assigns unique GS1 Company Prefixes to its members.

• GS1 ensures that each GS1 Member Organisation assigns unique blocks of numbers.

• Each GS1 Member Organisation will provide rules to help its members comply with the *GS1 General Specifications*. 
1 product = 1 GTIN
1 GTIN = 1 product
Global Location Number (GLN)
Global Location Number

- Used to identify physical locations and parties.

- Vital for GS1 eCom messaging so that all parties and locations may be uniquely identified.

- A pre-requisite for Global Data Synchronisation.
The identification of physical locations and parties (i.e. senders and receivers) involve throughout the supply chain enables an efficient flow of goods and information via:

- Party Data Synchronisation
- Physical location marking
- Routing information on logistic units
- ...
GLN structure

- GLNs have a similar structure to GTINs

<table>
<thead>
<tr>
<th>GS1 Company Prefix</th>
<th>Location Reference</th>
<th>Check Digit</th>
</tr>
</thead>
<tbody>
<tr>
<td>N₁ N₂ N₃ N₄ N₅ N₆ N₇ N₈ N₉ N₁₀ N₁₁ N₁₂</td>
<td>N₁₃</td>
<td></td>
</tr>
</tbody>
</table>
GLN Allocation

• General rule – A separate GLN is required to identify each different location (e.g. each store of a retail group)

• The owner of the organisation or location is responsible for communicating GLN changes throughout the supply chain.

• The sale of a single location requires change of its GLN.
GLNs Trading Partners Allocation

• Party responsible for a given location assigns the GLN.

• Although GLNs cannot be bought or sold, they may be used for third party trading partners who choose not to assign GLNs.
  • Example – Long-term lease of storage space. Leaseholder could use the GLN of the leasing company (property owner) with permission.
  • Use of the GLN for any other location type or trading partner is prohibited.
Serial Shipping Container Code (SSCC)
SSCC structure

<table>
<thead>
<tr>
<th>Extension Digit</th>
<th>GS1 Company Prefix</th>
<th>Serial Reference</th>
<th>Check Digit</th>
</tr>
</thead>
<tbody>
<tr>
<td>N₁</td>
<td>N₂ N₃ N₄ N₅ N₆ N₇ N₈ N₉ N₁₀ N₁₁ N₁₂ N₁₃ N₁₄ N₁₅ N₁₆ N₁₇</td>
<td></td>
<td>N₁₈</td>
</tr>
</tbody>
</table>

- The SSCC is assigned for the life time of the logistic unit and is a mandatory element of the GS1 Logistic Label.
Using SSCCs

• The SSCC is used to identify individual logistic units.

• Logistic units that are used to ship goods can take many physical forms: pallets; barrels; crates; ..

• The SSCC can be used by all parties in the supply chain as a key to the relevant information held on databases.
SSCC use in the supply chain

- The SSCC for each logistic unit can be quoted in GS1 eCom messages.

- Each party handling the logistic unit will know in advance what it is and will be able to scan the bar coded label that encodes the SSCC to confirm its arrival.

- An SSCC must not be re-issued for another logistic unit for at least a year.
SSCC: Key Identifier to track and trace through the supply chain

Supplier

Applies original SSCC

Transporter

Uses SSCC for internal controls & tracing

Distributor

Receives SSCC. Uses SSCC for internal controls and for outbound shipment

Transporter

Uses SSCC for internal controls

Customer

Receives original SSCC
GS1 Solutions

- B2C Trusted Source of Data
- Traceability
- Sustainability
- Upstream Integration
Providing digital product information consumers can trust

Digital information is driving consumer decisions

GS1 aims at developing a framework to communicate digital product information provided by brand owners to retailers, application providers and government for B2C purposes.
The vision of the GS1 B2C project is that:

- **Brand-owners** can share relevant product information easily, thus building trust with consumers.
- **Internet application providers** (IAPs) can ensure they are delivering authentic data.
- **Consumers** can feel confident that the digital product information they access is accurate, no matter how or where they shop.

At global level, the B2C project is governed by a multi-stakeholder project board chaired by Tesco and Coca Cola Company.
GS1 Solutions

- B2C Trusted Source of Data
- Traceability
- Sustainability
- Upstream Integration
Traceability – ensuring product and consumer safety

Can you identify the origin of a food safety outbreak? Can you trace defective products to the point of sale to recall them?

The GS1 Global Traceability Solution provides quality managers in the FMCG or food supply chain with an effective traceability process that complies with the multiple international regulatory requirements.
GS1 Solutions

- B2C Trusted Source of Data
- Traceability
- Sustainability
- Upstream
GS1 Sustainability

Enabling the sustainable supply chain – a common language for packaging sustainability

- **The Global Protocol on Packaging Sustainability** – an initiative of the Consumer Goods Forum with global retailers and manufacturers to develop a **common measurement system** for packaging sustainability

- **GS1 Sustainability Data Synchronisation** - global standards for the automated exchange of these sustainability-related metrics between trading partners. **Currently in early stages of development**
GS1 Solutions

• B2C Trusted Source of Data
• Traceability
• Sustainability
• Upstream Integration
Improved collaboration between manufacturers and their suppliers

GS1 Upstream Integration Solution
Designed to address the challenges in supply chain integration and collaboration between manufacturers and their suppliers.

GUSI: Global Upstream Supply Initiative
A Working Group of The Consumer Goods Forum with manufacturers from CPG/Retail and their suppliers. Collaborating together to develop an upstream solution based on common scenarios, common processes, common electronic messages – in order to reduce complexity and implementation costs and create an exchange platform.
Contact Details

GS1 Global Office
Avenue Louise 326, bte 10
B-1050 Brussels, Belgium
T + 32 2 788 78 00
W www.gs1.org
A-Trust experience with electronic signature

Mag. Siegfried Gruber
Consultant

Sept. 18th Rec-14 WG Meeting
A-Trust
Company Presentation
The Company

**A-Trust** Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH

- founded 2000
- privately owned company
- Owners: Chamber of commerce, chamber of lawyers and notaries, banks
- sole accredited service provider for qualified certificates in Austria, based on EU legislation and Austrian Signature Law
- providing certificates as well as hard- and software-products and services for secure data transactions
PRODUCTS I - signature

Certificates for individuals
- for authentication, digital signatures and encryption
- smartcard based certificates
- Software-certificates

Citizencard function
- unique identification of individuals for applications within the e-Government

Server-certifikates
- a.sign SSL certificate for proven identity of Web-Servers
- a.sign corporate signatur: server-based signing and encrypting of messages
PRODUCTS II - Software

\textit{a.sign} Client:
- middleware for usage of \textit{A}-Trust smartcards

\textit{A}-Trust citizencard-solution (BKU):
- unique identification within e-Government applications

\textit{a.sign} PDF:
- signing of single PDF-documents
- also available as COM-object for integration in various software products

\textit{a.sign} MultiSign:
- signing of multiple PDF-documents (batch-handling)
PRODUCTS III - Applications

e-TRESOR
Ihr persönlicher Datensafe

- web-based high-secure archive for electronic documents
- available 24h around the world
- sensible data protected by strong authentication and encryption

www.handy-signatur.at
Ihr Weg zur digitalen Signatur

- qualified signature without smartcards
- permanently available, also when travelling
- highest security level using mobile-phone
for your safety!
US CBP Electronic Signature in the Customs Single Window ACE

Presented by Lance THOMPSON for CBP expert, unable to attend

Sept. 18th Rec-14 WG Meeting
Electronic Signatures
U.S. Customs and Border Protection
Agenda

• Legislative framework
• Guidance for Federal Agencies
• Practical Applications
  • The Automated Commercial Environment
  • The Automated Broker Interface
Legislative Framework

- Paperwork Reduction Act of 1995
Legislative Framework
• Legislation passed to improve the security and privacy of sensitive information in Federal computer systems and to establish a minimum acceptable security practices for such systems.

• Requires the creation of computer security plans, and the appropriate training of system users or owners where the systems house sensitive information.
Paperwork Reduction Act of 1995

Required each Federal agency to:

1. Establish a process, independent of program responsibility, to evaluate proposed collections of information;

2. Manage information resources to reduce information collection burdens on the public; and

3. Ensure that the public has timely and equitable access to information products and services.
Government Paperwork Elimination Act (GPEA), 1998

• Required federal agencies to provide for
  1. The option of the electronic maintenance, submission, or disclosure of information, when practicable, as a substitute for paper; and
  2. The use and acceptance of electronic signatures when practicable

*Per guidance from the Office of Management and Budget (OMB), agency considerations of cost, risk and benefit, as well as any measures taken to minimize risks, should be commensurate with the level of sensitivity of the transaction (i.e., low risk information processes may need only minimal safeguards while high risk processes may need more).
• E-SIGN 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.

• E-SIGN applies broadly to Federal and state statutes and regulations governing private sector activities.

• Laws and regulations that are primarily governmental and do not relate to business, commercial or consumer transactions are not within the scope of this legislation; they are instead addressed by the Government Paperwork Elimination Act.

• * Certain laws and regulations involve both GPEA and E-SIGN, especially with respect to record retention requirements in agency regulations that govern business, consumer and commercial transactions.
Modernization Act, 1993

- One of the most sweeping regulatory reform legislations, amending the Tariff Act of 1930 and related laws.
- Introduced two new Customs concepts known as "informed compliance" and "shared responsibility." These concepts are premised on the idea that in order to maximize voluntary compliance with Customs laws and regulations, the trade community needs to be clearly and completely informed of its legal obligations.
- An overarching goal of the Mod Act was to place a greater responsibility upon the trade community to exercise “reasonable care” in complying with import requirements.
- The principal section of the Mod Act addressing automation was codified under 19 U.S.C. 1411-1414 (promulgated by CBP under the National Customs Automation Program (NCAP) testing provision, 19 CFR 101.9).
- **NCAP provides U.S. Customs and Border Protection with an automated electronic system to process commercial importations and facilitate business improvements with the trade community.**
The Mod Act amended Section 484 of the Tariff Act of 1930:

- Added provision (d)(1) providing that:
  Entries shall be signed by the importer of record, or his agent, unless filed pursuant to an electronic data interchange system. If electronically filed, each transmission of data shall be certified by an importer of record or his agent, one of whom shall be resident in the United States for purposes of receiving service of process, as being true and correct to the best of his knowledge and belief, and such transmission shall be binding in the same manner and to the same extent as a signed document. The entry shall set forth such facts in regard to the importation as the Secretary may require and shall be accompanied by such invoices, bills of lading, certificates, and documents, or their electronically submitted equivalents, as are required by regulation.
• The Mod Act was subsequently amended by the Trade Act of 2002 to include, among other things, the following change (2002—Subsec. (b). Pub. L. 107–210):
  – struck out a former second sentence which read as follows: “Participation in the Program is voluntary.”
  – Inserted a new second sentence which now reads: The Secretary may, by regulation, require the electronic submission of information described in subsection (a)...
Recent regulatory promulgations include:

- Section 343(a) of the Trade Act of 2002, as amended by the Maritime Transportation Security Act of 2002 (19 U.S.C. 2071 note) directed CBP to promulgate regulations providing for the mandatory transmission of electronic cargo information by way of a CBP approved electronic data interchange (EDI) system before the cargo is brought into or departs the United States by any mode of commercial transportation (ocean, air, rail or truck).

- Section 203 of the Security and Accountability for Every Port Act of 2006, Public Law 109–347, 120 Stat. 1884 (SAFE Port Act) directed the Secretary of Homeland Security, acting through the Commissioner of CBP, to promulgate regulations to require the electronic transmission to the Department of Homeland Security of additional data elements for improved high-risk targeting, including appropriate security elements of entry data, as determined by the Secretary. This additional data was to be provided as advanced information with respect to cargo destined for importation into the United States prior to loading of such cargo on vessels at foreign seaports. In 2008, pursuant to the Trade Act and the SAFE Port Act, CBP published an interim final rule in the Federal Register requiring importers and carriers to submit additional information pertaining to maritime cargo before the cargo is brought into the United States by means of a CBP approved electronic interchange system (commonly referred to as the “Importer Security Filing”).
• CBP, under NCAP, issued a number of Federal Register Notices announcing the transmission of required advance data through ACE.

• NCAP “testing” began for the truck mode of transportation until all land border ports mandated the transmission of advance truck manifest data through ACE (2005-2007).

• Most recently CBP conducted NCAP testing concerning the transmission of required advance ocean and rail data through ACE (2010-2011).

• After successful completion of that testing, CBP announced, effective September 29, 2012, ACE would be the only CBP-approved EDI for transmitting to CBP required advance information for ocean and rail cargo.
Guidance for Federal Agencies
Use of Electronic Signature Technology

- GPEA specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity or enforceability merely because they are in electronic form.
- Federal governments are encouraged to use a range of electronic signatures alternatives.
• Government agencies are to assess different security approaches in determining the appropriate balance between benefits accrued from electronic information transfer and the risk of harm if the information is compromised. Key approaches include:
  – Shared secrets (personal identification numbers or passwords)
  – Digitized signatures or biometric means of identification (e.g., fingerprints, retinal patterns, voice recognition)
  – Cryptographic digital signatures
  – A combination of approaches
What is an Electronic Signature?

• As defined by GPEA, an electronic signature is a method of signing an electronic message that:
  – Identifies and authenticates a particular person as the source of the electronic message; and
  – Indicates such person’s approval of the information contained in the electronic message (i.e., “intent”)

As defined by GPEA, an electronic signature is a method of signing an electronic message that:
– Identifies and authenticates a particular person as the source of the electronic message; and
– Indicates such person’s approval of the information contained in the electronic message (i.e., “intent”)

• Do policies and/or regulations support the use and enforceability of electronic signatures?
• Is it necessary to use a signed agreement between the entity submitting the electronically signed information and the Federal agency?
• Are mechanisms in place to tie transactions to an entity in a legally binding way?
• Are security measures in place to ensure no one is able to alter a transaction once it has been received by the agency?
• Is the “chain of custody” secure? That is, is there an electronic audit trail that provides for the chain of custody for the secure electronic transaction that identifies sending locations, sending entity, date and time stamp of receipt and any other needed measures to ensure the integrity of the document?
• Should the agency provide an acknowledgement of receipt?
Practical Applications
Technology:
The Automated Commercial Environment

• **ACE** is the commercial trade processing system being developed by CBP to become the “single window” through which international traders will electronically provide all information needed by federal agencies for the import of cargo.

• ACE is the enabler of further collaboration between the U.S. Government and the trade community to enhance the security, safety, compliance and flow of international trade.

• Although the trade cannot currently file entries using ACE, they can use the ACE Portal to access their account information. Depending on the functionality available for the specific account type (e.g., importer, broker, carrier etc.) additional capabilities may also be available.
ACE Portal Application and Program Participation

Sign up today to take advantage of the latest ACE Secure Data Portal capabilities. Benefits of establishing a Portal account include the following: file manifests electronically, make periodic payments on an interest-free monthly basis, file and process formal consumption entries and informal entries, including Automated Broker Interface (ABI) Census Warning Overrider, view and respond to certain CBP forms through the ACE Portal, and file and process AD/CVD entries (also know as type 03 entries) and track the lifecycle of your AD/CVD cases. Participating in ACE not only provides these tangible benefits, but also supports the U.S. Department of Homeland Security's (DHS) dual mission to facilitate legitimate trade and secure our nation's borders.

For questions on applying to ACE, e-mail us at ACENow@dhs.gov. This e-mail address is used only to facilitate establishing an ACE Account. If you are seeking employment opportunities within CBP or DHS, please visit the Careers section of the U.S. Customs and Border Protection website.

ACE Application Form
- 05/09/2012
To submit an application for an ACE Portal Account, complete, electronically sign and e-mail the ACE application form directly to CBP. Note: Please read instructions at the beginning of the application.

http://cbp.gov/xp/cgov/trade/automated/modernization/ace_app_info/
• Interested parties wishing to establish an ACE Portal Account must acquaint themselves with the ACE Portal “Terms and Conditions” (published as a Federal Register Notice).
• Once an ACE Secure Data Portal is established, the ACE Terms and Conditions also appears via a link on the log in page of the ACE Portal (https://ace.cbp.dhs.gov). Users must actively clink on the link to accept the “Terms and Conditions.”
• All ACE Accounts must have a designated Account Owner. The Account Owner must complete a “signed” ACE Application as proof of their designation as Account Owner for the Account and submit it to CBP. The “signature” can be digital. This document must also be signed by the Principal (any high ranking officer within the company structure).
• The Account Owner is the individual responsible for the daily administration of the ACE Portal account’s activities and will collect all the information required to populate the Account. Information that will be pre-populated in the Account must be verified by the Account Owner for each account type established for the Account and corrections must be made as appropriate.
• The Account Owner will receive the “shared secret” and their ACE User ID from CBP. The Account Owner will receive an e-mail from CBP that will provide a link where they can obtain their temporary password.
• The Account Owner will be prompted to change the initial password the first time he/she logs into the ACE Portal after selecting and answering five challenge questions.
• Once CBP reviews the data, any discrepancies will be provided to the Account Owner, and will require correction by the Account Owner. Once the data is complete, the Account Owner can access the ACE Portal and activate users.
• The Trade Community can currently file entries using either the Electronic Data Interchange (EDI) or via traditional paper filing.
• EDI is a mode of communication between computers that relies on machine-to-machine (point-to-point) transmission of structured data files, referred to as messages.
• Filers (Brokers and Importers) use EDI messages to provide import information to multiple agencies with import authority through ACE ("single window").
• The electronic message submission that filers participate in is referred to as the **ABI** program. ABI requirements are defined in the Customs and Trade Automated Interface Requirements (CATAIR).
ABI link on cbp.gov

http://cbp.gov/xp/cgov/trade/automated/automated_systems/abi/
Technology and Policy

- Largest trade sector submitting data to CBP is the broker community. Brokers are either self-filers or act as agents for the importer of record.
- From a policy perspective, CBP can reach the importer or the broker (NOTE: CBP regulates the broker community) by issuing civil penalties if there are violations.
- To use ABI, a brokerage or importer must request or already possess a “filer code.” This request is made in writing by a licensed broker or importer and is normally signed by the officer of the company. CBP will accept this application by mail, facsimile, or as scanned image file such as PDF. Only originally signed hard copies are acceptable.
- Once a filer code has been issued, the brokerage/importer must submit a Letter of Intent indicating an intent to transmit data via EDI. The Letter of Intent must be on company letter head, signed by the officer of the company and provide a description of the trading partner’s current or planned hardware, data communications, and entry processing system; and information regarding the brokerage/importer and the entries they expect to make through the system. CBP will accept this application by mail, facsimile, or as scanned image file such as PDF. (Note: CBP is currently exploring developing an automated utility to replace the hard copy letter of intent).
- Any party transmitting data with CBP must also sign an Interconnection Security Agreement (ISA). This agreement requires acknowledgment by the signatory that: both CBP and the signatory are expected to protect the data in accordance with the Privacy Act, Trade Secrets Act (18 U.S. Code 1905), and Unauthorized Access Act (18 U.S. Code 2701 & 2710); they are aware of the sensitivity of all data filed is Sensitive But Unclassified (SBU); that all CBP employees with access to the data are U. S. citizens with a valid and current CBP Background Investigation; they are aware of the policy documents that govern the protection of the data (CBP 1400-05D Security Policy Handbook and Department of Homeland Security 4300A Security Policy Handbook); and that CBP maintains an audit trail and employs intrusion detection measures to maintain security and system integrity.
• The filer is responsible for acquiring or developing the software that will be used to generate and transmit the ABI message set.

• This software is then tested to ensure that it can accurately and securely transmit messages using the chosen communication protocol. A filer also has the option of using a commercial service bureau (who has also completed certification testing) to prepare submissions.

• Data is transmitted using a Virtual Private Network (VPN), a means of communication from one computer to another over a public telecommunications network that relies on encryption to secure the content of transmissions.
CBP ISA link on cbp.gov

http://cbp.gov/xp/cgov/trade/automated/automated_systems/isa/
• ACE authenticates the electronic documents that it receives by comparing certain fields in the message to a user profile established at the time of registration. The profile includes, among other things, both the filer code and password chosen by the filer. This “trusted” profile is used during authentication (Port, Filer Code, password).

• CBP allows and expects the filer code and password to be shared by multiple people at the brokerage or importing company (whose responsibility it is to ensure their employees are meeting all requirements of their license). This is permitted because CBP can hold the broker-applicant and their brokerage civilly liable for false statements made using the shared credentials.

• No additional or individual credentials are issued to or used by those making submissions to ACE. If a violation should occur, CBP as the regulating agency for brokers, can ultimately revoke or suspend the broker license and where circumstances require, issue penalties against the broker.

• ACE confirms receipt of an electronic document by sending an outbound message to the filer from which the document was received. This message is received and stored by the same software that was used to generate the document whose receipt the message acknowledges.
• The EDI message set includes a field for electronic signature.
• An ACE Entry Summary is designated as *paperless* until such time (if any) that CBP requests that a paper document be submitted.
• The Electronic Signature indicator is MANDATORY if the 10-Record Summary Filing Action Request Code is an A (Add) or R (Replace).
• For ACE Entry Summaries, there is a one-byte field that permits the filer to indicate his “electronic signature.” *(See description from the 10 record of the ACE Entry Summary Create/Update CATAIR Chapter on the CBP website at:)*

ACE Entry Summary Create/Update CATAIR Chapter on cbp.gov

Entry Summary Create/Update

This chapter provides record formats and processing instructions to submit entry summary and related information to ACE.

The reader should be advised that this technical document is considered final. However, the document retains the DRAFT designation in the footer until such time that an official OPA (Office of Public Affairs) publication number has been assigned to the new “ACE ABI CATAIR” publication. For your information, subsequent revisions to this document will be controlled through the official CBP document amendment process.

• Data received through EDI messages transmitted by filers is written to a database and displayed to CBP employees through a graphic user interface.

• The database has an associated audit trail that records any changes made to data and includes the date in which the change was made and the identifier of the user making the change.

• Metadata associated with the message (such as date and time of receipt) are also written to the database.

• Records are stored in “the manner delivered to CBP.” Copies are stored at the filers’ location and must be provided to CBP by the filer upon request.
Q&A, Comments, Discussions
Break

Discussions resume at 16:00
Rec-14 Revision WG
Roadmap ahead

• Discussion on the days presentations in light of the 1979 recommendation

• Future work to be done:
  – Drafting a new recommendation text within the scope of the approved revision project
    • Is it reasonable to aim for December?
  – Organization of Annex
    • How should each annex be organized? Should they be completely integrated or as separate documents?
    • How should call for papers be sent out (limit length of contributions? Request in a certain format?...)

• Conference call schedule
Rec-14 Revision WG
Roadmap ahead – some ideas

• Definition of electronic signature:
  – UNCITRAL « Promoting Confidence », §20, p15

• Organization of the technical annex (Annex 2):
  – UNCITRAL « Promoting Confidence », §24/25, p16-17
    grouping them in these typologies

• Organization of the regulatory annex (Annex 1):
  – Around how legally enabling?
  – Establish a model outline for submissions
  – Try to deduce a common checklist for considerations as introduction to the annex
Rec-14 Revision WG
Roadmap ahead – sources to be considered

• Group suggestions

• First Telephone conference call mid-October:
  – Wednesday October 17th @ 13:00 C.E.T.
  – Wednesday October 24th @ 13:00 C.E.T.
  – Thursday October 25th @ 13:00 C.E.T.