# 3 Enabling a conducive technical framework

# 3.1 Digital identity

Establishing the identity of users electronically is necessary to promote confidence in interactions with and transactions within a paperless trade system. Electronic identification and authentication ascertain who is sending data to whom.

Identities that remain uncertain could compromise all actions taken based on that data. Few people will take actions with legal effect if they do not know who they are dealing with.

Identity is the ability to distinguish an entity in a context. Natural and legal persons may have both foundational and functional digital identities.

Foundational identities are unique identifiers, such as the name and date of birth of a natural person, or the registration number of a company issued by the business register of the country involved. Those identifiers are persistent and irreplaceable and may apply in many distinct contexts. Those identifiers are mainly a result of the country's history and designed for public law purposes and are not specifically meant for supporting the B2G and B2B processes of the international supply chain.

Functional identities are identifiers (issued by the public or private sector) that are used in specific contexts and they may acquire credibility by repeated use. Each entity may have multiple functional identities but should have only one foundational identity based on the national legislation of the country of origin.

In practice, information from foundational digital identity providers such as civil records and vital statistics offices, and company registries, is used by trust services to provide the identity attribute of clients for whom they offer assurance as to identification.

**"Establishing the identity of users electronically is necessary to establish confidence in user identities in interactions and transactions with a paperless trade system."**

Several methods can be used to identify a legal or natural person in information systems, ranging from a password and higher levels of security that utilize multi-factor authentication to possession of a certificate from a third-party certificate authority (i.e. trust service provider) that attests to its identity. Electronic identification and authentication may be a function of certain trust services, such as electronic signatures, to provide evidence whether a document or message may be attributed to a particular legal entity.

Along with digital identities of legal entities and natural persons, identification of physical and digital objects[1] is equally important. Digital identities of objects permit one to identify and trace the history, distribution,

location and use of containers, consignments, shipments, bills of lading, insurance certificates – not only physical products but also digital assets. Traceability and greater transparency of supply chain operations can play a key role in improving the ability to recall products, mitigating counterfeiting activities, and providing consumers with greater insights into the environmental footprint and social impacts of final and intermediate goods in global supply chains.

## International guidance and good practices

### Identification of legal entities

Identifiers play a key role as "data connectors" between systems (i.e. B2G, B2B, G2G). Both public and industry actors have developed identifiers to help to identify supply chain actors and to gain insights into who originated data messages (see Box 4).

**Box 4: Examples of identifiers**

**WCO's trade identification number**

The WCO, in collaboration with customs authorities and industry stakeholders, has developed technical standards and guidance for a trade identification number (TIN) to identify authorized economic operators (AEOs), which is now commonly used for reporting to customs authorities. The TIN is for B2G reporting only.

**Legal entity identifier**

The Financial Stability Board, established by the G20 in 2011, was mandated to develop the Global Legal Entity Identifier. Now administered by the Global Legal Entity Identifier Foundation, the legal entity identifier (LEI) is a 20-digit code to uniquely identify public and private-sector participants in financial transactions (B2G, B2B).

Each LEI contains business register data on the entity as registered in the country involved and mandatory information about the entity's ownership structure. It thus answers the questions of "who is who" and "who owns whom" with regard to corporate affiliation.

All the data are made available as a broad public good free of charge for any user on the Global Legal Entity Identifier Foundation website. The Foundation is subject to oversight by the LEI Regulatory Oversight Committee.

**Proprietary systems**

Proprietary systems, such as the Data Universal Numbering System (DUNS), developed and managed by Dun & Bradstreet, assign a unique numeric identifier (a DUNS number) to a single business entity.

**Decentralized Identifiers**

The Decentralized Identifiers (DIDs) protocol is a type of identifier that enables a verifiable, decentralized digital identity. A DID acts as a unique identifier. Verifiable credentials are then used to store and represent machine-readable credentials that are tied to that cryptographic identity. The World Wide Web Consortium (W3C) has developed the Verifiable Credentials Data Model, which provides a standard way to express identity credentials on the internet for any subject (i.e. a person, a company, a physical or digital good, or even a document). The United States Department of Homeland Security, for example, is funding the development of DID-based identity credentials as a standard that the United States Customs and Border Protection service can use for supply chain verification.

The UNCITRAL Model Law on Identity Management and Trust Services (expected to be adopted in 2022) will introduce a common model legal regime for identity management services to support their use and cross-border recognition.

### Identification of objects

In relation to objects, identifiers include product identifiers and asset identifiers for containers, ships and planes. A presentation of identifiers standards for objects is available in the *Standards Toolkit for Cross-border Paperless Trade* (ICC/WTO, 2022).

Tables 11 and 12 list some of the relevant sections on digital identity in the *Legal Readiness Assessment Guide*, the *Technical Readiness Assessment Guide* and the corresponding checklists.

**Table 11: Digital identity – relevant sections in the *ESCAP Technical Readiness Assessment Guide* and *Checklist***

| Questions in the *Guide* and *Checklist* | Section |
|---|---|
| Has your country implemented electronic customs (and other services that facilitate customs declarations in an electronic format)? If yes…,<br>Does it have the ability to authenticate users electronically? | A2.1.1<br>A2.1.1.3 |
| Has your country implemented electronic port systems (including air, sea, road, rail and inland ports)? If yes…,<br>Does it have the ability to authenticate users electronically? | A2.1.2<br>A2.1.2.3 |
| Has your country implemented any cross-border trade systems other than those specified above? If yes…,<br>Does it have the capability to authenticate users electronically? | A2.1.4<br>A2.1.4.3 |

**Table 12: Digital identity – relevant sections in the *ESCAP Legal Readiness Assessment Guide* and *Checklist***

| Questions in the *Guide* and *Checklist* | Section |
|---|---|
| Does the law address how electronic signatures, including for identification, authorization and authentication, are added in an electronic environment? Does it require the use of a specific technology or method for electronic signatures or is it technology neutral? | I.B.1 |
| Does the law recognize foreign electronic signatures? | I.B.4 |
| Does the law deal with trust services? | I.B.6 |

# 3.2 Electronic payments

The ability to make payments electronically can facilitate and accelerate trade. Electronic payments may be used within a paperless trade system for various purposes, such as the payment of customs duties and fees (B2G payment) and the settling of the purchase price of goods and services (B2B and C2B payments).

There are different types of electronic payment system and an increasing number of licensed third-party payment providers and platforms (i.e. independent of traditional banks). The types of system that can be used by a paperless trade system depends on the national payment system architecture.

The national bank or an association of domestic banks and financial institutions generally establish the rules and standards for electronic payment and settlement in domestic and cross-border funds transfers, for example by ordering a bank to transfer money (wire transfer) or through credit or debit cards.

Alternatively, or complementarily, certain commercial documents may be used to perform payment or give guarantee of payment. These documents include, for instance, bills of exchange, cheques, promissory notes and letters of credit, which can, in some jurisdictions, be used in electronic form.

Limitations often apply to the types of electronic payment accepted, for example by requiring the exclusive use of a payment service method or provider. In some jurisdictions, the use of electronic payments may be restricted to domestic transactions.

Moreover, diverging legal and technical standards have made it more difficult to connect different payment systems. The World Economic Forum (WEF, 2020) reports that domestic infrastructure requirements, forced data localization, and licensing and equity requirements on foreign firms have hindered the electronic payments service providers, thereby limiting services available to the domestic market and vice-versa. Divergent regulatory systems and infrastructures have created challenges for domestic firms.

## International guidance and good practices

When introducing a national legal framework for electronic payments, instruments such as model laws, treaties and guidelines can be used (see Box 5).

Payment should not present an unnecessary burden to users. Interoperability of payment systems is necessary to support all electronic payment transactions.

Electronic payment systems should use international standards to be able to communicate with different payment systems within and across borders, thereby providing traders fulfilling border formalities with a payment system that connects with their chosen payment method and financial institution. International standards (e.g. payment messaging standards such as SWIFT) play an important role in facilitating cross-border payment systems.

Many payment card networks use a common messaging standard.[2] Similarly, cross-border payments sent between banking customers (issuers) also use international standards and standardized messages between banks with instructions for payment transfers.[3]

Tables 13 and 14 list some of the relevant sections on integrating electronic payments in the *Legal Readiness Assessment Guide,* the *Technical Readiness Assessment Guide* and the corresponding checklists.

**Box 5: Examples of instruments**

**WTO's Trade Facilitation Agreement**

Article 7.2 of the WTO's Trade Facilitation Agreement deals specifically with e-payment in the form of a 'best-efforts' provision and states that members "to the extent practicable, adopt or maintain procedures allowing the option of electronic payment for duties, taxes, fees, and charges collected by customs".

**International Convention on the Simplification and Harmonization of Customs Procedures (as amended) (Revised Kyoto Convention)**

Standard 4.6 of the Revised Kyoto Convention requires national legislation to "specify the methods that may be used to pay the duties and taxes."* The Revised Kyoto Convention was developed by the WCO and is the main trade facilitation customs convention.

The guidelines to Standard 4.6 recommend that customs authorities "should accept payment of duties and taxes in forms other than cash, such as travellers cheques, money orders, certified cheques, uncertified cheques (in specified circumstances), bonds, credit cards, securities, etc."**

The guidelines encourage the use of electronic funds transfer, "allowing for quick and efficient payment." The WCO also provides practical implementation guidance on e-payment systems applied to single windows.+

**International Chamber of Commerce**

The ICC Customs Guidelines provides relevant business perspectives on electronic payments (ICC, 2012).

**Financial Stability Board**

The Financial Stability Board developed, in coordination with the Bank for International Settlements Committee on Payments and Market Infrastructures, the G20 Roadmap for Enhancing Cross-border Payments: First Consolidated Progress Report, which was endorsed by the G20 leaders at their November 2020 Summit.++

* See http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/conventions/pf_revised_kyoto_conv/~/link.aspx?_id=7D65110194D24C01AC00508F0CC4A329&_z=z.

** See http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/wto-atf/dev/rkc-guidelines-ch4.pdf?la=en.

+ See http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/single-window/compendium/swcompendiumvol2partiv.pdf.

++ See https://www.fsb.org/wp-content/uploads/P131021-1.pdf.

**Table 13: Integrating electronic payments – relevant sections in the *ESCAP Technical Readiness Assessment Guide* and *Checklist***

| Question in the *Guide* and *Checklist* | Section |
|---|---|
| Are the paperless trade systems integrated with an electronic payment system? | A2.1.1.2, A2.1.2.2, A2.1.4.2 |

**Table 14: Integrating electronic payments – relevant sections in the *ESCAP Legal Readiness Assessment Guide* and *Checklist***

| Questions in the *Guide* and *Checklist* | Section |
|---|---|
| Does the paperless trade system accept or initiate electronic payments? | IV.D.1 |
| Does the paperless trade system accept electronic transferable records? | IV.D.2 |

# 3.3 Data models and semantics

For parties to exchange and reuse fully electronic messages, all information needs to be clearly defined and unambiguous, both from a semantic and a syntax perspective. Data compatibility is one of the main issues that needs to be addressed in various connectivity projects.

A standardized data library is useful. For example, packaging material that is palletized can be described as slab, board and honeycomb slate, among others, before even taking into account differences between languages. In the context of paperless trade systems, data semantic and syntax standardization based on international standards can help to enable seamless data exchange without compatibility issues.

## International guidance and good practices

Streamlining documentary and data requirements relating to import, export and transit can facilitate data standardization. The United Nations Economic Commission for Europe (UNECE) and United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) suggest "an iterative process of capturing, defining, analyzing, and reconciling government information requirements … to eliminate redundancies and duplication" (UNECE and UN/CEFACT, 2013a).

Similarly, the United Nations Network of Experts for Paperless Trade and Transport in Asia and the Pacific (UNNExT), ESCAP and UNECE have developed the *Data Harmonization and Modelling Guide for Single Window Environment* (UNNExT *et al.*, 2012) "to assist governments and businesses in harmonizing and standardizing the international trade data required in fulfilling all import, export, and transit-related regulatory requirements." Both UN/CEFACT and the WCO have developed libraries of semantics and data models to standardize semantics and processes.

An overview of existing data standards (i.e. standards that define the core elements of an electronic record representing a trade document) and data format/exchange standards (i.e. standards that facilitate the exchange of data between different systems) is provided in the *Standards Toolkit for Cross-border Paperless Trade* (ICC/WTO, 2022), which maps existing standards, including:

- foundational and identifier standards;
- standards for commercial transaction documents;
- standards for transport, forwarding and cargo handling documents;
- standards for payment documents;
- standards for port and airport clearance documents;
- standards for real-time shipment tracking data;
- standards for official control documents at customs and other cross-border regulatory agencies;
- interoperable digitalization frameworks.

Table 15 lists the relevant sections on data models and semantics in the *ESCAP Technical Readiness Assessment Guide* and *Checklist*.

**Table 15: Data models and semantics – relevant sections in the *ESCAP Technical Readiness Assessment Guide* and *Checklist***

| Questions in the *Guide* and *Checklist* | Section |
|---|---|
| Has data harmonization and standardization been conducted for the data elements for paperless trade at the agency level? At the national level? | A6.1, A6.1.1, A6.1.2 |
| If yes, has a data model been adopted and is it based on international standards/guidelines? | A6.1.3, B4.1 |

# 3.4 Communication protocols

To enable the exchange of information within and across borders, IT networks underlying paperless trade systems should integrate various communication protocols. Protocols are rules (i.e. for e-communications purposes, languages implemented in the form of networking algorithms) that govern the way a particular system functions for communication. These rules define the syntax and semantics of communication to exchange information between two electronic devices.

Multiple communication protocols exist, including:

- multi-protocol label switching (MLPS)
- internet protocol (IP)
- virtual private network (VPN)
- secure hypertext transfer protocol (HTTPS)

The network infrastructure for paperless environment should support those communication protocols to enable connectivity with and interoperability between heterogeneous platforms. Otherwise, paperless trade systems will exist in silos unable to exchange information among themselves, thereby hindering the potential of cross-border exchange of electronic messages.

## International guidance and good practices

According to the ISO Open Systems Interconnection Model, data transmission (i.e. how data are sent and received) over a network can be described through seven layers or levels:[4]

- physical
- data link
- network
- transport
- session
- presentation
- application

A communication protocol should cover these layers and should be open (i.e. not proprietary) (see Box 6).

A mapping of data formats and exchange standards commonly used to facilitate the exchange of trade data between different systems is available in the *Standards Toolkit for Cross-border Paperless Trade* (ICC/WTO, 2022).

Table 16 lists the relevant sections on communication protocols in the *ESCAP Technical Readiness Assessment Guide* and *Checklist*.

**Box 6: Examples of protocols**

International well-known and open protocols include, *inter alia*:

**Internet protocol (IP)** is a communications protocol for routing packets of data over a network. IP does not handle packet ordering or error checking. Such functionality requires another protocol, typically the transmission control protocol (TCP).

**Hypertext transfer protocol (HTTP)** is used to request and transmit files, especially web pages and web page components, over the internet or other computer networks. HTTP can be implemented on top of any other protocol on the internet, or on other networks. Combined with the secure socket layer/transport layer security (SSL/TLS) protocol, the hypertext transfer protocol secure (HTTPS) provides encryption and secure identification.

**Extensible markup language (XML)**, developed by UN/CEFACT and the Organization for the Advancement of Structured Information Standards (OASIS), is a communication protocol supporting the exchange of electronic business data.

**Simple object access protocol (SOAP)**, maintained by the World Wide Web Consortium (W3C), provides a way to communicate between applications running on different operating systems, with different technologies and programming languages.

**JavaScript object notation (JSON)** is a standard file format designed for data interchange that is both human and machine-readable. It is commonly used for transmitting data in web applications.

**Table 16: Communication protocols – relevant sections in the *ESCAP Technical Readiness Assessment Guide* and *Checklist***

| Questions in the *Guide* and *Checklist* | Section |
|---|---|
| How does the single window system receive data electronically, i.e., what kind of user interface and communication channel is used (Internet-based network or dedicated/secured private network)? | A2.2.1 |
| Is the ICT network able to support various communication protocols? | A3.2.3 |
| Is the ICT network designed to take into account future requirements such as device and technology upgrades? | A3.2.5 |
| Is the single window system, if implemented, interoperable with other systems? | A3.3 |
| Is it able to integrate, interface and/or interoperate with other existing heterogeneous systems (i.e., with systems on a different platform)? | A3.3.1 |
| If it does support (i.e. is interoperable with) heterogeneous systems, what is the method of integration/ interfacing? | A3.3.2 |
| What kind of communication protocol is used for electronic data exchange currently? | A.4.4 |

# 3.5 Connectivity

Telecom infrastructure and network services should be available at all stations (communications points) supporting paperless trade systems. The lack of secure internet with proper speed or its cost when present can impede implementation of a paperless trade system.

Different network infrastructure options that are financially and technologically appropriate for different areas could be deployed (e.g. using fibre optics, wireless devices and satellites).

Moreover, the ICT infrastructure should be designed with possible future device and technology upgrades in mind. The potential future expansions that should be considered include, for example, increased numbers of users of the systems, increased number of ICT nodes of connectivity, and future requirements of higher performance and throughput of electronic services.

## International guidance and good practices

Connectivity can be improved by international commitments made (or that could be made) by governments, such as commitments under WTO agreements, for example:

- market access commitments in the telecommunications services sector;
- WTO Reference Paper[5] laying out key regulatory principles in the telecommunications services sector;
- WTO's Information Technology Agreement, eliminating tariff and non-tariff barriers applicable to IT products.

Technical standards have also been established in multiple international forums. The International Telecommunication Union (ITU) has developed international standards known as ITU-T Recommendations, which serve as defining elements in the global infrastructure of ICTs. The ITU also publishes case studies highlighting national practices (e.g. see ITU/UPU (2009) for the satellite strategy in Bhutan).

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) also deal with technical issues of telecommunication. The subcommittee which works on standardization in the field of telecommunications has published over 280 ISO/IEC standards. For instance, the quality characteristics in ISO/IEC 25010:2011 provide criteria to evaluate the properties of a software product, including, *inter alia*, functionality, performance, reliability, security and scalability.

Industry associations, such as the Telecommunication Industry Association, the European Telecommunications Standards Institute and the Internet Engineering Task Force have also developed telecommunications and internet standards.

Table 17 lists one relevant section on connectivity in the *ESCAP Technical Readiness Assessment Guide* and *Checklist*.

**Table 17: Connectivity – relevant section in the *ESCAP Technical Readiness Assessment Guide* and *Checklist***

| Question in the *Guide* and *Checklist* | Section |
|---|---|
| Is network service available at all border posts, including ports, airports and cargo clearance facilities, in your country? | A3.1 |

# 3.6 Data security

As discussed in Section 2.3, the confidence of users to replace paper-based documents with electronic information depends on the security, confidentiality and the privacy of personal and business information.

There are technical measures that should be adopted by the IT system underlying a paperless trade system to deserve this confidence.

## International guidance and good practices

The ISO/IEC 27000 family of standards provides requirements for an information security management system (ISMS), which describes and demonstrates an organization's approach to information security and privacy. There are several measures that can ensure such security, such as:

- dedicated network infrastructure separated from the open public network for some sensitive connectivity (e.g. G2G network connection);
- VPN to enable users to send and receive data over a public network as if their computing devices were directly connected to the private network;
- encryption protocols (e.g. SSL) and hardware and software keeping users' digital identities to provide additional encryption and authentication services;
- ring-based network zones.

**"The confidence of users to replace paper-based documents with electronic information depends on the security, confidentiality and the privacy of personal and business information."**

For the successful design and implementation of an ISMS in accordance with ISO/IEC 27001:2013, *Information Technology: Security Techniques – Information Security Management Systems – Requirements*, there are critical steps to follow. These steps are also detailed in ISO/IEC 27003:2017, *Information Technology: Security Techniques – Information Security Management Systems – Guidance*, with ISO/IEC 27001 being "what" and ISO/IEC 27003 "how".

The IEC 62443[6] series of standards was developed to secure industrial automation and control systems throughout their lifecycles. The Institute of Electrical and Electronics Engineers (IEEE) has also established standards on cybersecurity, such as IEEE 1686-2013, *IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities*. At the national level, the US National Institute of Standards and Technology has published the *Guide for Developing Security Plans for Federal Information Systems* (Swanson *et al*., 2006).

Table 18 lists some of the relevant sections on data security in the ESCAP *Technical Readiness Assessment Guide* and *Checklist*.

**Table 18: Data security – relevant sections in the *ESCAP Technical Readiness Assessment Guide* and *Checklist***

| Questions in the *Guide* and *Checklist* | Section |
|---|---|
| Do the paperless trade systems have the ability to authenticate users electronically? | A2.1.1.3, A2.1.2.3, A2.1.4.3 |
| Do the paperless trade systems ensure data/document security? | A2.1.1.4, A2.1.2.4, A2.1.4.4 |
| Is the ICT network able to provide secure information exchanges that ensure confidentiality and data integrity? | A3.2.4 |
| Is there a policy for the establishment of a disaster recovery plan at the agency level? | A3.5.1 |
| Is there a policy for the establishment of a disaster recovery plan at the national level? | A3.5.2 |
| Does your country have a business continuity plan for paperless trade systems? | A3.6 |
| Is there an information technology security policy for your country? | A4.1 |
| If any of the systems mentioned in A2.1, "Electronic systems", have been implemented, what kind of security measures are in place to protect them from unauthorized access? | A4.2 |
| What kind of authentication mechanism is used to ensure security of information transmitted electronically? | A4.3 |

## Endnotes

1 Unlike subjects, objects do not have rights nor obligations.

2 See ISO 8583-1:2003, *Financial Transaction Card Originated Messages: Interchange Message Specifications, Part 1. Messages, Data Elements and Code Values.*

3 See the ISO 20022:2013 set of standards,

4 See https://www.iso.org/cms/%20render/live/en/sites/isoorg/contents/data/ics/35.100/x/.

5 See https://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm.

6 See https://www.iec.ch/blog/understanding-iec-62443.