United Nations ECE/TRANS/WP.30/GE.2/2016/1

Economic and Social Council

Distr.: General
25 January 2016

Original: English

Economic Commission for Europe

Inland Transport Committee

Working Party on Customs Questions affecting Transport

Group of Experts on Legal Aspects of Computerization of the TIR Procedure

Second session
Geneva, 4-5 April 2016
Item 4 of the provisional agenda
Compatibility of the eTIR legal framework with national legal requirements

Results of the surveys conducted by the Informal Ad hoc Expert Group on Conceptual and Technical Aspects of Computerization of the TIR Procedure

Note by the secretariat

I. Background

1. At its previous session, the Group of Experts on Legal Aspects of Computerization of the TIR Procedure (GE.2) commenced considerations on the possibility that national legal requirements in some countries may not be compatible with the legal requirements of introducing eTIR. In this context, GE.2 may recall that the delegation of the Russian Federation informed GE.2 that the current proposal of mutual recognition of authentications performed at the country of departure would not be compatible with the legislation of the Russian Federation. Against this background, GE.2 had concluded that there would possibly be merit in conducting a survey to seek relevant information from all TIR Contracting Parties on this issue (see ECE/TRANS/WP.30.GE.2/2, para. 8(a)). As a first step, GE.2 requested the secretariat to provide, at the current session, the results of relevant surveys already undertaken by the Informal Ad hoc Expert Group on Conceptual and Technical Aspects of Computerization of the TIR Procedure (GE.1) in the framework of the eTIR project, in order to determine the appropriate next steps. In line with this request, the secretariat prepared this summary of the results of the surveys conducted by GE.1.

II. GE.1 surveys

2. At its sixth session (October 2004), GE.1 welcomed a proposal from the secretariat to undertake a survey to gather information from customs administrations on existing systems and on their needs and constraints regarding the eTIR system. To this end, the secretariat drafted a questionnaire, which was sent to Director-Generals of Customs (with a copy to the TIR Customs Focal Points. At its seventh session (May 2005), the Expert Group used the preliminary results of the questionnaire, contained in document ExG/COMP/2005/3, to finalize the first chapter of the eTIR Reference Model and to assess the future requirements of the eTIR project. The Expert Group also requested the secretariat to continue requesting answers to the questionnaire from those countries which had not yet replied, in particular countries from outside the European Union. At its eighth session (November 2005), the Group took note of the latest results of the eTIR questionnaire, contained in TRANS/WP.30/GE.1/2005/4, and welcomed the idea of receiving updated results at its ninth session, including the answer by the Russian Federation together, possibly, with other replies received by the secretariat before mid-February 2006. The final results of the questionnaire are contained in document ECE/TRANS/WP.30/GE.1/2006/2 and have been used by GE.1 in Chapters 1.1.7 and 1.1.8 if the eTIR Reference Model.

3. At its nineteenth session (September 2011), GE.1 reconsidered the proposal to include international declaration mechanisms in the scope of the eTIR project on the basis of document ECE/TRANS/WP.30/GE.1/2010/9, prepared by the secretariat in collaboration with experts from Czech customs. While highlighting the absence of global international agreements on electronic signatures, the Expert Group took note that some countries impose the use of national certification authorities when it comes to signing electronic documents intended for governmental agencies. The Expert Group felt that there was insufficient information to take a decision on the issue and requested the secretariat to launch a survey among both TIR and eTIR focal points, aimed at gathering information from all TIR Contracting Parties on the current and expected practice, rules and regulations on electronic signatures (ECE/TRANS/WP.30/2012/1, para. 10). The survey took place in March 2012 and the results of the survey, originally contained in Informal document GE.1 No. 3 (2012), are presented in Annex.

4. At its twentieth session (April 2012), GE.1 concluded that the survey on the use of electronic signatures in the framework of the eTIR project confirmed that most countries require the use of electronic signatures or other authentication mechanisms for the transmission of advance cargo information. In most countries, only national (or at best: regional) electronic signatures are accepted and, at present, only a few countries recognize foreign certification authorities (CA) for the issuance of legally binding electronic signatures. The Expert Group confirmed that, as long as internationally recognized CA's have not been developed and recognized, it will be extremely difficult to implement the cross-border use of electronically signed documents. The Expert Groups noted that 50 per cent of the respondents to the questionnaire indicated that an international CA could be used if recognized by an international agreement and half of those considered that the TIR Convention could be considered as providing an appropriate platform for that purpose. Consequently, the secretariat was requested to further explore the possibilities to include international declaration mechanisms, for example by means of trusted third party solutions and directly in the eTIR international system, possibly linked with the authorization procedure of TIR Carnet holders. Finally, the Expert Group requested the secretariat to redraft a proposal to include international declarations mechanisms in the eTIR Reference Model for its next meeting, underlining that a realistic proposal should be based on authentication mechanisms (e.g. user/password) and trusted system-to-system information exchanges (e.g. Virtual Private Network), rather than on electronic signatures. (ECE/TRANS/WP.30/2012/7, para. 10)

III. Considerations by the Group of Experts

5. GE.2 may wish to consider this document and determine whether or not to conduct a new survey.

Annex

Results of the survey on the use of electronic signatures in the framework of the eTIR project

I. Respondents

3. By 10 April 2012, the following 30 countries had replied to the questionnaire:

Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Montenegro, Mongolia, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Turkey, Ukraine, United Kingdom

II. Consolidated replies to the survey

Question 1: Bearing in mind that in the future eTIR system, the Customs declaration will be lodged and accepted at the moment when the holder (or his representative) presents the goods, the vehicle and a reference to the advance cargo information to Customs, do you consider it necessary that the holder authenticates himself at the time of the electronic submission of the advance cargo information by means of using an electronic signature or any other type of authentication mechanism.

Yes: 27 (90%)

Austria, Belgium, Bulgaria, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Mongolia, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, Ukraine, United Kingdom

No: 2 (7%)
Finland, Serbia

No reply: 1 (3%)
Cyprus

Question 2: In your country, do Customs authorities already have in place a legal mechanism for user authentication or the use of electronic signatures?

Yes: 25 (83%)
Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Italy, Latvia, Lithuania, Montenegro, Netherlands, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Turkey, Ukraine

No: 5 (17%)
Austria, Greece, Mongolia, Norway, United Kingdom

If no, are you aware of any plans in your country to introduce for Customs purposes the use of electronic signatures or any other form of authentication mechanism in the near future?

Yes: 3(60%)
Greece, Mongolia, United Kingdom

No: 2 (40%)
Austria, Norway

Question 3: In your country, do Customs authorities accept the use of signatures certified by foreign certification authorities?

Yes: 7 (24%)
Belgium, Czech Republic, Estonia, Lithuania, Portugal, Serbia, Turkey

No: 22 (76%)
Austria, Bulgaria, Denmark, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Mongolia, Montenegro, Netherlands, Norway, Poland, Romania, Slovakia, Slovenia, Spain, Sweden, Ukraine, United Kingdom

If no, are you aware of any intention to change this in the near future?

Yes: 7 (33%)
Bulgaria, Greece, Italy, Mongolia, Montenegro, Poland, Turkey

No: 9 (43%)
Austria, Germany, Latvia, Norway, Romania, Slovenia, Spain, Ukraine, United Kingdom

Not applicable: 5 (24%)
Finland, France, Hungary, Slovakia, Sweden;

Question 4: In your view, would it be possible that, in the future, the Customs authorities of your country could accept electronic signatures, if these were issued or certified by an internationally recognized certification authority (i.e. a certification authority that would be recognized by an international legal instrument, such as the TIR Convention)?

Yes: 15 (52%)
Belgium, Czech Republic, Estonia, Finland, Greece, Hungary, Lithuania, Mongolia, Montenegro, Poland, Serbia, Slovakia, Slovenia, Sweden, Turkey

No: 3 (10%)
Italy, Spain, Ukraine

No reply /
not applicable: 11 (38%)
Austria, Bulgaria, Cyprus, Denmark, Germany, France, Latvia, Netherlands, Norway, Romania, United Kingdom

If yes, would your government be interested that such certification authority would be developed within the legal framework of the TIR Convention?

Yes: 8 (53%)
Finland, Lithuania, Montenegro, Poland, Serbia, Slovakia, Slovenia, Turkey

No: 3 (20%)
Belgium, Mongolia, Sweden

No reply /
not applicable: 4 (27%)
Czech Republic, Estonia, Greece, Hungary

IV. Preliminary considerations by the secretariat

Question 1:

The vast majority of respondents consider it necessary that the holder authenticates himself at the time of submission of advance cargo information. Various replies refer to applicable EU legislation and the application of NCTS, others refer to applicable national legislation. The general opinion is that authentication is required to prevent fraudulent use of either the TIR Carnet holder's identity or of the TIR Carnet. Similar to the signature in the paper system, due authentication makes the holder responsible for the submitted data in the TIR Carnet as well as for all other responsibilities related to the use of the TIR system, including the payment of the Customs debt in case of infringement.

Question 2:

The majority of countries dispose already of some form of national legislation stipulating the conditions for authentication mechanisms or the use of electronic signatures. Out of the five countries where legislation is still absent, three inform that the introduction of legislation is under consideration.

Question 3:

Only seven countries report that they recognize electronic signatures certified by foreign certification authorities. The other twenty-eight countries report that either they do not recognize electronic signatures from abroad at all or, in some countries, only after prior registration with their national system.

Question 4:

Fourteen countries report that they could advocate some kind of existence an internationally recognized certification authority, but indicate, at the same time, that a firmer position on the issue would require further coordination at the national governmental level. Seven countries indicate that they would be interested to support such development within the framework of the TIR Convention.

Appendix

A. Individual answers[1]

Question 1: Bearing in mind that in the future eTIR system, the Customs declaration will be lodged and accepted at the moment when the holder (or his representative) presents the goods, the vehicle and a reference to the advance cargo information to Customs, do you consider it necessary that the holder authenticates himself at the time of the electronic submission of the advance cargo information by means of using an electronic signature or any other type of authentication mechanism.

Denmark: We handle transit declarations, including TIR) in NCTS. Communications with traders take place through NCTS by means of declarations sent in EDIFACT-format.

Estonia: Estonia considers it necessary that the TIR Carnet holder authenticates himself at the time of the electronic submission of the advance cargo information. The representative of the TIR Carnet holder had to authenticate himself as a natural person by means of accessing the electronic system of the Estonian Tax and Customs Board with an ID card, or digital ID. In the near future, a development of authentication on the basis of electronic signatures is not foreseen.

Germany: on paper, the holder authenticates himself with his signature. Thus, in an electronic environment, he has to authenticate himself by means of an electronic signature or another, similar mechanism.

Finland: it should be up to each individual Contracting Party to apply risk analysis also to pre-declarations [=advance cargo information] which will never be released for transit. Thus, it might be irrelevant to identify the holder from the pre-declaration which will never be released for transit. In any case, the holder will be identified upon handling the transit declaration at the Customs office. The same principle applies to the Common Transit system in the European Community – although the practice may vary in different EU countries.

France: Even if the eTIR project provides that a declaration will be considered as accepted only at the moment when the holder (or his representative) presents the goods, the vehicle and a reference to the advance cargo information to Customs, we must check if a (natural) person) who wants to use a TIR Carnet as a Customs declaration and who claims to represent a company, is actually authorized to act on behalf of the TIR Carnet holder. More precisely, the authentication mechanism is aimed at preventing fraudulent use of a holder ID or TIR Carnet number by a user who has not been granted access by the holder or his representative.

On the other hand, in a scenario where a declaration could be lodged by anyone, without any authentication, it seems possible that someone lodges a declaration, presents the vehicle, the goods and the reference to the declaration to a Customs office and conducts a transport using the ID number of a different TIR Carnet holder or another company's TIR guarantee. Checking consistency between the declaration and the vehicle / driver would only be possible at the Customs office if the link between holder, driver and vehicle was certain, which is not always the case, in particular in the event of subcontracting.

[1] Contributions have been edited by the secretariat for the sake of clarity and consistency.

Hungary: Hungary considers authentication or identification of a holder as essential and necessary during the transmission of electronic cargo data, especially when the TIR Carnet is accepted by Customs authorities. First of all, the holder is responsible for all the data elements of TIR Carnet. Second, a holder will be known by means of identification or his identity can be confirmed. Last but not least, he is also responsible for the TIR operation with regard to other issues such as time limit, prescibed itinerary or Customs debt.

Italy: the authentication of the TIR Carnet holder is considered as a mandatory step towards a paperless environment.

Latvia: In Latvia every person who submits a transit our TIR declaration, must be a registered as user with the national declaration system. The holder is provided with login and password for authentication. Without these, there is no method to submit declarations in Latvia. The national system could be connected with other systems, including those from other countries. In such case, the trader or organization signs an agreement with the State Revenue Service of Latvia concerning the use of electronic signatures as well as an agreement on the submission of electronic TIR Carnets to the transit control system and will obtain his own login and password. The organization could share its data with the users of its system.

Lithuania: Commission Regulation (EEC) No 2454/93, laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code, Article 184a (in the case of road traffic, the entry summary declaration shall be lodged at the Customs office of entry at least one hour prior to arrival at the Customs office of entry in the Customs territory of the Community).

Mongolia: The use of an e-signature is required due to the implementation of the “National Single Electronic Window”.

Netherlands: Customs need to know the person who is using their electronic declaration system and, therefore, authentication of the declarant is necessary.

Norway: Our national electronic system only accepts pre–registered users. Answers/messages are sent back to a centrally registered address.

Poland: Poland is of the opinion that even if electronically sent data are referred to as ' advance cargo information' rather than 'Customs declaration', authentication of the holder remains be required. In Community transit, there is no distinction between the two: the sent message (IE15) is actually treated as Customs declaration, even if it is accepted only after the presentation of goods, together with the reference to the electronic document.

Portugal: Any person, whether holder or his representative, has to be duly certified and recognized as such.

Serbia: Serbia believes that authentication is not necessary for the submission of the advance cargo declaration. Such approach would require the acceptance of large numbers of digital certificates issued by many different certification authorities (or companies) from all over the world. In addition, this could complicate holder’s job since he would probabily have to carry appropriate devices (tokens, cards, readers etc.) with him, which, of course, he first would have to buy.

Spain: Spain is of the opinion that electronic signature systems are necessary for security reasons.

Sweden: Sweden Customs has a security concept based on Public Key Infrastructure (PKI).

Turkey: In general, TIR Carnets are submitted by drivers to Custom offices, the holder or his representative not being physically present at Customs offices. For that reason, TIR Carnets are signed by drivers, although they are not authorized. If an electronic signatures

is used, TIR Carnets can be signed by the authorized holder or his representative. It is also important to know who submits the declaration and who is responsible.

Ukraine: Application of an electronic signature allows to identify clearly the document in the form of an electronic document as well the person who signed this electronic document.

United Kingdom: The system should be able to verify all messages and have an audit trail of who lodged them.

Question 2: In your country, do Customs authorities already have in place a legal mechanism for user authentication or the use of electronic signatures? If no, are you aware of any plans in your country to introduce for Customs purposes the use of electronic signatures or any other form of authentication mechanism in the near future?

Denmark: Citizens and companies in Denmark have been using on-line services, including electronic signatures, for years, but the full potential has not yet been reached.

At present, the government is working on an eGovernment Strategy for the years 2011-2015. More and more procedures in the public sector will be automated and digitalized. All companies will obtain a digital mail box and will be granted access to company information on the business portal. The system for electronic signatures is called NemID, a system where all citizens log in and communicate electronically with all public authorities, banks etc. The system is based on personal registers (CVR). As a consequence, it is not easy when foreign companies are not registered. Normally, companies can be registered through a representative in Denmark. In order for someone (person or company) to obtain the same rights, this could be achieved by means of certificates based on a X509 standard. Thus, theoretically, it should be possible.

France: Customs authorities already have in place a legal mechanism for user authentication, but it is not based on the use of electronic signatures. In fact, when declaration mechanisms were developed, the opportunity to use electronic signatures was assessed and the conclusion was that using electronic certificates could represent a real burden for traders. Different elements justified that conclusion, not only financial costs related to certificate purchasing, but also complexity implied by certificate management (necessity for each user of a company to get a separate certificate etc.). Moreover, France considered that it was possible to ensure authentication and to secure access to the system by other, simpler means. First of all, it should be underlined that the majority of electronic Customs declarations in France are lodged in EDI; in that case, a system to system exchange is realized (each system recognizes its partner) and no other authentication than the technical one is necessary. In DTI, the authentication process is taken into account in the Customs portal: users are authenticated by user / password (chosen by the user at registration). For more sensitive Customs applications, stricter security requirements can be added (registration can be "confirmed" by a manager of the company). Furthermore, most of the time, in DTI, user rights are given by Customs, at the request of the company, which contributes to securing the declaration mechanism.

Greece: There is a team studying the possible introduction of electronic signatures for Customs.

Poland: At present, Poland does not use electronic signatures in transit (NCTS). There is a verification of the declarant on the basis of the EORI number and e-mail address; the declarant must be registered in the relevant reference database. For other procedures (import, export), Poland has in place a mechanism called “key for safe transmission of data”; the key is issued/provided by a designated office within the Polish Customs administration (Safe Data Transmission Center).

Question 3: In your country, do Customs authorities accept the use of signatures certified by foreign certification authorities? If no, are you aware of any intention to change this in the near future?

Czech Republic: Customs authorities accept the use of signatures certified by foreign certification authorities. However, due to the fact that the certification policy of the foreign certification authority can be different from the requirements of the Czech Act, the acceptance of the signature is subject to individual assessment.

Estonia: The Estonian Tax and Customs Board can accept electronic signatures only from certification authorities approved by the Estonian Information System Authority, which coordinates the development and administration of national information systems, including public key infrastructure to enable secure digital authentication and signatures.

France: No definitive answer (neither yes nor no), because signatures based on electronic certificates are not used by French Customs within the framework of Customs online procedures. However, if this would be the case, it can be assumed that certificates delivered by foreign certification authorities could be accepted, like is the case today for certificates used for other purposes (certificates for servers, encryption of documents etc. where certificates delivered by foreign authorities can be used).

Montenegro: Recently, a national certified body has been created in order to give local keys for electronic submission of docs. At this moment, there does not seem to be a connection between our country and foreign certification institutions, but the awareness thereof seems positive for the future.

Netherlands: Netherlands does not accept electronic signatures certified by foreign certification authorities and does not see any change in that regard in the near future.

Poland: We will accept electronic signatures/ certificates issued by certification authorities of all other EU Member States, on the basis of so called Trusted-service Status List, conforming to the Decision of the European Commission 2009/767/EC of 16 October 2009, setting out measures facilitating the use of procedures by electronic means through the points of single contact under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market. The restriction is the requirement that the certificates as well as signature formats should be in accordance with a set of technical specifications.

Romania: According to the law in force, only electronic signatures issued by qualified certifying providers accredited with the Special Supervisory and Regulatory Authority in the field are accepted.

Serbia: Yes, some authorities accept electronic signature /certificates issues by foreigh certification authorities. We use the digital certificate issued by IRU for TIR EPD pre-declarations (advance cargo information). By this means, indirectly, all holders who use IRU's system for sending pre-declarations are authenticated for the Customs system. Also, in the near future, we will most probably exchange internally issued certificates within the Customs administration for the purpose of exchange certificates of origin.

Ukraine: No, because it is necessary to change not only Customs legislation but electronic signature legislation first.

Question 4: In your view, would it be possible that, in the future, the Customs authorities of your country could accept electronic signatures, if these were issued or certified by an internationally recognized certification authority (i.e. a certification authority that would be recognized by an international legal instrument, such as the TIR Convention)? If yes, would your government be interested that such certification authority would be developed within the legal framework of the TIR Convention?

Czech Republic: In the future, Czech Customs authorities could accept electronic signatures, if these were issued or certified by an internationally recognized certification authority. However, due to the fact that the certification policy of the foreign certification authority can be different from the requirements of the Czech Act, the acceptance of the signature is subject to individual assessment.
It depends on the assessment of the Ministry of Interior if such certification authority could be developed within the legal framework of the TIR Convention.

Estonia: In the future, this should be possible, if the certification authority will be approved for the cross-border recognition of electronic signatures by the Estonian Information System Authority.

Estonia is involved in the EU policy in the field of eGovernment, where the cross-border recognition of electronic signatures is under discussion in a number of ongoing projects, funded by the Information Society Directorate General or the Community Innovation Programme. It is crucial for EU member states to have a joint policy on the establishment of a certification authority within the framework of the TIR Convention.

Germany: an answer to this question would require extensive study.

France: As indicated above, French Customs are not opposed in principle to electronic signature and electronic certificates, even when issued by an international authority. But, for the moment, French Customs are not convinced that using signatures based on electronic certificates is practical and necessary to authenticate Customs systems users.

For information purposes, it should be noted that, apart from the specific needs of the eTIR project, France distinguishes two separate needs concerning authentication:

(a) authentication of a user in a system managed by the national administration; this requirement can be met by other means than a signature based on electronic certificates, because the system is under control of Customs (or a partner authority).

In DTI, a simpler level of authentication (login / password), combined with user profiles management, can be sufficient.

In EDI, a system-to-system exchange and mutual recognition of platforms are enough to accept the validity and authenticity of data.

From a conceptual point a view, it is assumed that the eTIR international declaration mechanism could be considered as EDI (as well as TIR-EPD, which allows transporters to send declarations Customs via the IRU); thus, a national system would accept the declaration like any other EDI declaration and would not check the identity or profile of the user, because that task would be performed upstream by the international system. To summarize, France is of the opinion that both DTI and EDI allow authentication without signature: in DTI, the system and its access are directly controlled by the administration; in EDI, access and authentication are controlled by the EDI platform (which can be an international one). Consequently, the electronic signature is only one of the various ways to address the need of authentication. Even though highly secure, it could, nevertheless, constitute a burden and slow down the deployment of the eTIR.

(b) authentication of documents issued by a third system; this requirement, which seems outside the scope of eTIR, refers to documents presented to Customs via a

system (e.g. documents received by email), which need to be checked: for instance: a certificate of origin signed by a Chamber of Commerce in a third country. Obviously, in such case, the only way to check the authenticity is to rely on a signature based on an electronic certificate. For the moment, that scenario is the only one where using electronic certificates is considered by French Customs for the near future. However, it seems possible that Contracting Parties have different views and practices about authentication and validation of declarations. Consequently, it would perhaps be better to allow flexibility and to accept that some countries require electronic certificates and other countries use different methods.

Further to the above remarks, it should be clear that France is neither opposed nor in favour of the development of a certification authority within the legal framework of the eTIR Convention.

At the same time, an important point should be looked at within the context of document ECE/TRANS/WP.30/GE.1/2011/9, paragraph 25, which states that "it would be easy to implement a mechanism that would allow national associations or Customs administrations to deliver internationally recognized electronic certificates together with the TIR Carnet holder's identification Number. If duly recognized in the TIR Convention, a certification authority could be created under international auspices and provide certificates for those transport companies that meet the requirements to use the TIR system." In our view, this paragraph suggests that a certificate could be given to a transport company as soon as authorization is granted. We agree with the simplicity of that scenario. However, supporters of the electronic signature solution must check if providing certificates to "transport companies" is sufficient. In this respect, EU Directive 1999/93/EC distinguishes "electronic signature" (with minimal requirements) from "advanced electronic signature" (which must be linked to a natural person, and is the only one that can really – and without any possible contestation – satisfy the legal requirements of a signature). When delivered to "transport companies", and not to natural persons working for these companies, such certificates could probably not be the basis of real legal signatures. The rules seem quite clear: if a certificate is delivered to a company, it is not possible to know who really uses that certificate or to know if that very individual has the authority to realize binding formalities on behalf of the company.

Hungary: According to IT experts, using electronic signatures for Customs procedures is possible but it will incur high costs, both for Customs authorities and holders/clients. At present, there is no legal basis.

Lithuania: According to the Law on electronic signature of the Republic of Lithuania, qualified certificates, issued by foreign state certification-service-providers shall be considered legally equivalent to the qualified-certificates issued by the Republic of Lithuania certification-service-providers, if:

(a) they are issued by a certification-service-provider, who is accredited in the Republic of Lithuania;

(b) they are issued by a certification-service-provider who is accredited in the European Union;

(c) the certificate is guaranteed by the certification-service-provider of the Republic of Lithuania, who corresponds to the requirements established by the Government or an institution authorized by it for certification-service-providers who issue qualified-certificates;

(d) the certificate is guaranteed by a certification-service-provider of a European Union Member State, corresponding to the equivalent requirements for certified-service-

providers who issue qualified-certificates, established by the Government of the Republic of Lithuania or an institution authorized by it.

Netherlands: Position is unknown, as discussions on the issue take place at governmental level.

Poland: Our law states that the certificates issued by certification authorities established outside Poland are recognized (and treated as those established in Poland) provided that one of several conditions is met, for instance:

- certificate or certification authority is recognized on the basis of an agreement between EU and third countries or between EU and international organizations, or
- certification authority is accredited in accreditation system of one of EU or EEA countries and fulfils the requirements set out by the law of that country.

Portugal: The reputation of the organization as such is not the real issue. What really counts is the liability of the Certification Authority issuing the certificate.

Romania: At present, we have no knowledge about the possibility to change to law so that it would provide the legal framework for using electronic signatures certified by foreign certification authorities in Romania.

Ukraine: In case of changes in the regulations, such a development under the TIR Convention would be acceptable for the Customs authorities of Ukraine.

B. Applicable legislation

Austria: no national legislation

Belgium: The use of the electronic signatures is based on a national law of 9 July 2001 and implemented via a 'KB' (Koninklijk Besluit = Order in Council);

Bulgaria: Law on Electronic Documents and Electronic Signatures, in force since 2011 and amended in December 2010;

Cyprus: Cyprus legislation, either by specific local laws or by international treaties and conventions that Cyprus has signed up to and ratified, recognizes certifications of signatures as follows:

In Cyprus: certifications made by the Authorized Certifying Officers.
In any other Country: certifications made by:

Any consular officer of the Republic of Cyprus or by

The authorities of other states which under International Treaties and Conventions to which Cyprus is signatory, are competent in such matters. Such Treaties are:

(a) Hague Convention Abolishing the Requirement of Legalization for Foreign Public Documents of 5th October 1961-Law 50/72 and 91/72. In Cyprus the competent authority in matters relating to this Convention is the Ministry of Justice. This certification is type APOSTILE.

(b) Treaty on Legal Co-operation between the Cyprus Republic and the Hellenic Republic on matters on civil, family, commercial and criminal law-Law 55/84. Under this Treaty, the Republic of Cyprus accepts all signatures certified by any public or officer of any police department in Greece. Also become acceptable certification from citizen's service centers of ministry of Interior in Greece.

(c) European Convention Abolishing the Legalization of Documents issued by Diplomatic Representatives or Consular Officers. Law 6/69. Under this Convention the Republic of Cyprus accepts all signatures certified in any country by consular officers of any state, member of the European Union

Czech Republic: Act on Electronic signatures No 227/2000

Estonia: Digital Signatures Act, which entered into force in 2000.

Germany: Customs and Tax Law and Electronic Signature Law

Finland: Commission Regulation (EEC) No 2452/93(implementing provisions) Article 199.2

France: France: Even if, at present, electronic signatures are not used by French Customs authorities for user authentication, we confirm that electronic signature complies with French law, which is based on EU law (Directive 1999/93/CE of 13 December 1999 on a Community framework for electronic signatures). Concerning the specific area of Customs formalities, the French national Customs code provides that "the transmission of an electronic declaration within the conditions settled by the ministry of budget entails the same legal effects as the lodgment of a written and signed declaration having the same object. Such transmission entails commitment concerning the accuracy of the content of the declaration and the authenticity for documents attached or stored." This article clearly states that, for French Customs, the value of a electronic Customs declaration can be recognized, regardless of the use of electronic certificates or not, since the conditions stated by the administration are met.

Hungary: According to Commission Regulation (EEC) No 2452/93 (implementing provisions), an identification process is defined in Article 4.

Italy: All legal aspects for all Italian Public Administrations are fixed by Digit PA, the national institution for the digitalization of Public Administrations.

Latvia: The use of electronic signatures is applicable by means of the "Law on Electronic Documents". Users have to sign an agreement with the State Revenue Service of Latvia concerning the use of electronic signatures. In order to submit Customs declarations (including Transit and TIR declarations), the user's login and password is used as electronic signature. There is no need to attach further specific files.

Lithuania: Law on electronic signature of the Republic of Lithuania and regulations of the Customs Department under the Ministry of Finance of the Republic of Lithuania.

Montenegro: Law on electronic signature (2003).

Mongolia: The law on e-signature was approved in 2011. This law will enter into force on 1 January 2013. As a consequence, accompanying rules and regulations as well as the establishment of a legal framework are at different levels of development. The Information, Communications, Technology and Post Authority of Mongolia is in charge of this issue.

Poland: The Act on electronic signature and The Act on computerization of the bodies fulfilling public services.

There are plans for changes in the future by means of a project to implement, in three years' time (full implementation), the verification of electronic signatures for all procedures, transit-NCTS included.

There will be actually three options available:

- use of key for safe transmission of data,
- use of electronic signatures/ certificates issued by certification authorities,

- use of trusted profile (e-PUAP) used for communication with public administration.

Portugal: Decreto-Lei No. 290-D/99, of 2 August 1999, amended by Decreto-Lei No. 62/2003 of 3 April 2003 and Portaria No. 767/2007 of 9 July 2007.

Romania: Law No. 455/2001.

Serbia: Law on electronic signature, Law on electronic document, Regulation on the e-administrative affairs of state administration, Regulation on the Customs approved treatment of goods, Law on general administrative procedures and the Law on administrative disputes.

Slovakia: National law relating to electronic signatures.

Slovenia: The Law on Electronic Commerce and Electronic Signatures.

Spain: Law 11/2007 of 22 June, The Citizens' Electronic Access to Public Services Act, refers to the forms of identification and authentication and sets forth the electronic signature systems that the public may use in their dealings with public authorities (including the Customs authorities) in line with what each authority decides.

Sweden: national laws;

Turkey: Law of Electronical Signature, Number 5070. This law covers the legal status of electronic signatures, activities of electronic certification service providers and procedures regarding the use of electronic signatures in all areas.

Ukraine: Law of Ukraine "On electronic digital signature" of 22.05.2003 № 852-IV;

Law of Ukraine "On electronic documents and electronic documents turnover" of 31.05.2005 № 2599-IV; Decree of the Cabinet of Ministers of Ukraine dated 28.10.2004 № 1452 "On approval of the application of digital signatures by public authorities, local authorities, enterprises, institutions and state-owned organizations"; Decree of the Cabinet of Ministers of Ukraine dated 28.10.2004 № 1453 "On approval of standard operating procedures of electronic documents turnover in the executive branch"; Decree of the Cabinet of Ministers of Ukraine dated 28.10.2004 № 1451 "On Approval of the central certification body"; Decree of the Cabinet of Ministers of Ukraine of 28.05.2010 № 680 "On approval of certification of the availability of electronic documents (electronic data) at a certain point in time".

United Kingdom: VAT, which is part of HMRC does have electronic signatures. For Customs declarations, the badge number (user authentication) could be used, but this could be one of several people. For Customs purposes, the use of electronic signatures or any other form of authentication mechanism in the near future is under consideration.