Informal document WP.30/GE.2 (2016) No. 1

Distr.: General
30 November 2016

English only

Economic Commission for Europe

Inland Transport Committee

Working Party on Customs Questions affecting Transport

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

Third session
Geneva, 12 and 13 December 2016
Item 2 of the provisional agenda
Compatibility of the eTIR legal framework
with national legal requirements

Compatibility of the eTIR legal framework with national legal requirements

Note by the secretariat

I. Introduction

1. At its second session, the Group of Experts on Legal Aspects of the Computerization of the TIR Procedure (GE.2) decided to conduct a survey with the objective of collecting information on (a) the various methods of authentication used at customs offices of departure, (b) the various specificities (implementation and processing) of the use of electronic signatures in particular, (c) on the legal status/validity of electronic communications (including electronic signatures) in domestic jurisdictions, such as, but not limited to, their admissibility as evidence in national court proceedings. Further to this, GE.2 had requested the secretariat to prepare the draft survey, circulate it to all participants of GE.2 electronically for comments and inputs as well as finalize and launch it prior to the next session of GE.2. In line with this request, the secretariat prepared and launched the survey electronically in September 2016, following electronic consultations and approval of GE.2, and has compiled the preliminary results of the survey, as received by the date of 15 November 2016, for discussion at the present session.

2. This document contains a preliminary analysis of the survey results by the secretariat and the statistics about the answers so far as an annex.

II. Analysis of the survey results[1]

A. General remarks

The survey was replied by thirty- three Contracting Parties by 15 November 2016. The respondents represented different national and regional backgrounds, as there were three Eurasian Economic Union (EEU), twenty-two European Union (EU) and twenty-seven NCTS countries among the respondents. Most of the questions were replied to, and additional information and comments were provided when necessary.

B. Analysis of individual sections

Section 1: General

This section, which consists of two sets of questions that look at computerization of procedures and electronic authentication by customs, received the highest number of replies from respondents, while Question 1 in this Section was replied to by all respondents of the survey. Results indicate that all respondents have IT infrastructure in place for processing Customs declarations and data- exchange and, furthermore, they carry a development agenda in both fields. There seems to be a requirement for authentication for electronic declarations in all countries and this is mostly done by “usernames and passwords” and/or “Public Key Infrastructure (PKI) electronic signature”.

Question 1

(i) In your country can a customs declaration be submitted electronically?

Almost all countries have electronic declaration, and for those three countries who replied “in some cases” there is some sort of infrastructure in place and according to their replies to Question 1/iii, they are planning to improve it.

(ii) Do customs authorities in your country exchange data contained in customs declarations electronically at the national and/or international level?

Almost all countries gave a clear “yes” reply to this question. Whereas six countries replied “in some cases” and “no”, it is observed from the comments section that these countries are also exchanging data both at the national and international level. So, other than a possible misunderstanding about this question, it is evident that all Customs authorities are capable of data exchange.

(iii) Are customs authorities in your country planning to move to a computerized environment that will allow electronic declaration and data exchange in the future?

All countries who did not give a “yes” answer to previous two items replied to this question positively which indicates a commitment to further improving existing infrastructure.

Question 2

(i) Does information/data submitted electronically (such as advance cargo information) need to be authenticated?

[1] This chapter is not numerated in order to avoid any overlap with survey numbering.

Almost all respondents indicated a requirement for authentication in this question. However, there are four countries that require authentication "in some cases" based on the type of declaration or the status of the declarant.

(ii) Please select the method or methods used by customs in your country for the authentication of the person sending electronic information (you can select more than one):

It is evident from this question that "usernames and passwords" and/or "Public Key Infrastructure (PKI) electronic signature" are the mostly applied methods of authentication, and it is very common that a customs authority uses more than one method.

Section 2: Public Key Infrastructure (PKI) Electronic signatures

This section searches for information on the legal validity of and the conditions for using the Public Key Infrastructure (PKI) electronic signature specifically, both within the customs context and in general. Questions in this section were responded to by almost all countries. Results indicate that PKI electronic signatures are widely used by customs. In most countries, PKI electronic signatures have a legal basis and benefit from acceptance at court proceedings. On the other hand, in only a limited number of countries the legal basis is broadly permissive; in most countries there is prescriptive legislation in force. Non-residents are also able to obtain signatures in most countries. As for the use of signatures generated using a certificate issued by foreign certification authorities, there is not a liberal practice in general. Such signatures are accepted only in a limited number of countries based on inter-governmental agreements (including customs unions) or the recognition of a certification authority.

Question 3

(i) Do the laws in your country currently allow for the use and legal validity of PKI electronic signatures in general?

Almost all countries replied to this question positively, indicating the legal validity of PKI electronic signatures in their countries. On the other hand, there are four countries, both EU and non-EU, where PKI electronic signatures are not valid.

(ii) Please select the type of legislation in force:

This question indicates that there is a limited number of countries where the legislation is broadly permissive on electronic signatures. Most countries replied that their legislation is prescriptive in the sense that it prescribes specific technical methods to electronically sign a document. There are only four countries who indicated a two-tier legislation in force.

Question 4

Are PKI electronic signatures in the context of customs and trade transactions between operators and public authorities admissible as evidence in court proceedings in your country?

All countries (except two) indicated that PKI electronic signatures are considered as evidence in court proceedings. In most of the replies, it was indicated as evidence with high relevance and having equal legal validity with a manual signature. In few cases, it may have lower value than manual signature depending on the case or technology used.

Question 5

(i) In your country, do Customs authorities accept the use of PKI electronic signatures generated using a certificate issued by foreign certification authorities?

This question reveals that in most countries customs authorities do not accept the use of PKI electronic signatures generated using a certificate issued by foreign certification authorities. Furthermore, in countries where it is allowed, it can be used under specific conditions.

(ii) Please select the applicable conditions/restrictions which apply to the acceptance of PKI electronic signatures generated using a certificate issued by foreign certification authorities:

With regard to conditions underlying the use of certificates issued by foreign certification authorities, although answers were divided among the options provided in close rates, it was clear that for the EU countries the legal framework was set by Regulation (EC) No 910/2014/EU (eIDAS Regulation). The respondents indicated that, according to this Regulation, the certificate has to be issued by a certification authority that is in the Trusted Services List (TSL), which is also published in accordance with the Regulation. As for non- EU countries, since they mostly indicated in the previous question that certificates issued by foreign certification authorities are not accepted, there were only two non-EU respondents to this question, namely Armenia and I.R. of Iran. Both of these countries required a bilateral or multilateral agreement with the country where the certificate is issued.

Question 6

In your country, can a non-resident obtain a certificate for a PKI electronic signature?

Most of the countries responded this question positively, hence allowing a non-resident obtain a certificate for a PKI electronic signature. Although some indicated this possibility only “under specific conditions”, these conditions mostly seem procedural, such as for example, verification of the person. It is also worth emphasizing that among those who replied to this question negatively, there are both EU and non-EU countries.

Section 3: Electronic authentication mechanisms for eTIR

This section aims to collect information on preferences and practicalities relating to electronic authentication in the eTIR context in particular. Most countries responded to the questions in this section, only slightly less than previous sections. This section indicates that countries consider it necessary that a person submitting data electronically is always authenticated, thus, the holder submitting advance cargo information in for eTIR needs to be authenticated each time. On the other hand, there is not a specific tool indicated as the necessary authentication mechanism. With regard to the use of PKI electronic signatures in eTIR, the number of countries who can accept an internationally recognized certification authority is slightly higher than the number of those not favourable towards this option. Countries with positive approach are also mostly interested in developing such a certification authority within the eTIR legal framework.

Question 7

Do you consider it necessary that the holder (or his representative) 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 electronic authentication mechanism), 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 the customs office of departure?

It is clear from the responses to this question that almost all countries will require the holder (or his representative) to authenticate himself at the time of the electronic submission of the advance cargo information in the future eTIR system. In terms of the mechanism to be used for authentication, most countries welcome mechanisms other than PKI electronic signatures as well.

Question 8

(i) In your view, would it be possible that the Customs authorities of your country could accept PKI electronic signatures for eTIR in particular, 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 eTIR legal framework)?

With regard to the use of PKI electronic signatures that are issued or certified by an internationally recognized certification authority in eTIR system, although the majority of countries replied positively, the rate of negative answers is close to the positive.

(ii) If yes, would your government be interested that such certification authority would be developed within the eTIR legal framework?

Almost all countries who declared they may accept the use of PKI electronic signatures generated by an internationally recognized certification authority, consider that such an authority can be developed within the eTIR legal framework.

III. Considerations by the Group of Experts

3. GE.2 is invited to reflect on whether the number of replies received is sufficiently representative for drawing accurate conclusions or if it would be necessary to mandate the secretariat to extend the deadline and send a reminder to Contracting Parties who have not yet replied.

4. As the survey reveals the diversity of methods used by TIR Contracting Parties for electronic authentication and the limitations on the use of signatures generated using a certificate issued by foreign/international certification authorities, GE.2 may wish to discuss alternative solutions to secure the electronic authentication in the eTIR system.

Annex

Section 1: General

Question 1

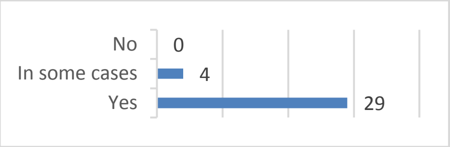
(i) In your country can a customs declaration be submitted electronically?

(a) Yes;

(b) In some cases;

Please specify (max 300 characters):

(c) No.



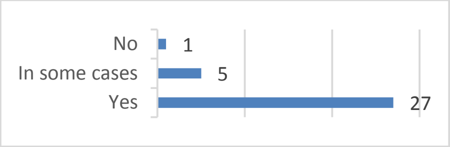
(ii) Do customs authorities in your country exchange data contained in customs declarations electronically at the national and/or international level?

(a) Yes;

(b) In some cases;

Please specify (max 300 characters):

(c) No.

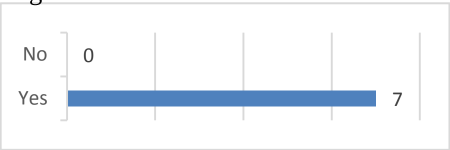


(iii) Are customs authorities in your country planning to move to a computerized environment that will allow electronic declaration and data exchange in the future?

(a) Yes;

(b) No.

Comment (max 300 characters):



Question 2

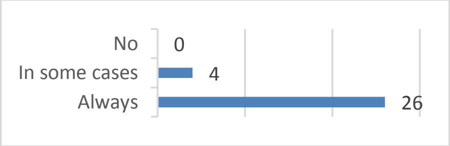
(i) Does information/data submitted electronically (such as advance cargo information) need to be authenticated?

(a) Always;

(b) In some cases;

Please specify (max 300 characters):

(c) No.



(ii) Please select the method or methods used by customs in your country for the authentication of the person sending electronic information (you can select more than one):

(a) Usernames and Passwords;

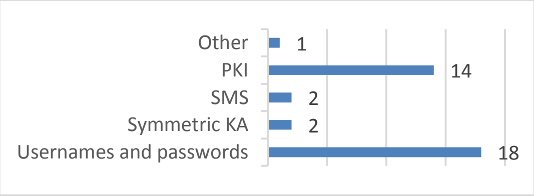
(b) Symmetric key authentication;

(c) SMS based;

(d) Public Key Infrastructure (PKI) electronic signature;

(e) Other.

If other, please specify (max 300 characters):



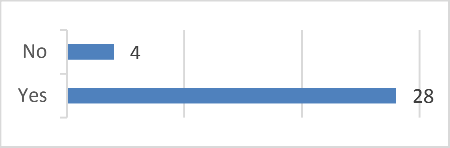
Section 2: Public Key Infrastructure (PKI) Electronic signatures

Question 3

(i) Do the laws in your country currently allow for the use and legal validity of PKI electronic signatures in general?

(a) Yes;

(b) No.

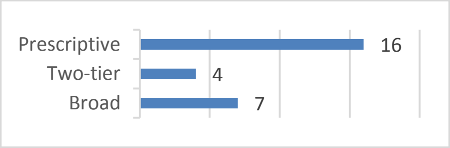


(ii) Please select the type of legislation in force:

(a) Broadly permissive (only few legal restrictions);

(b) "Two-tier" (generally permitted, but specific approved technologies are considered of higher security/legal value/reliability);

(c) Prescriptive (prescribes specific technical methods to electronically sign a document).



Question 4

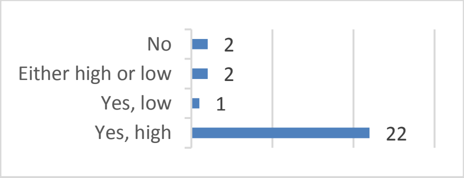
Are PKI electronic signatures in the context of customs and trade transactions between operators and public authorities admissible as evidence in court proceedings in your country?

(a) Yes, and they are considered as evidence with high relevance (and equal legal validity with manual signature) for the outcome of the case;

(b) Yes, but their value as evidence compared to manual signature is generally lower or determined on a case by case basis;

(c) Either high or low value as evidence depending specifically on the technology used;

(d) No, not accepted as evidence.



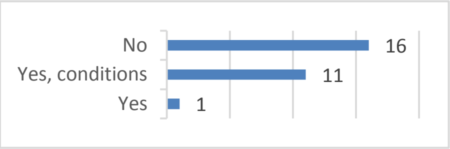
Question 5

(i) In your country, do Customs authorities accept the use of PKI electronic signatures generated using a certificate issued by foreign certification authorities?

(a) Yes;

(b) Yes, under specific conditions;

(c) No.



(ii) Please select the applicable conditions/restrictions which apply to the acceptance of PKI electronic signatures generated using a certificate issued by foreign certification authorities:

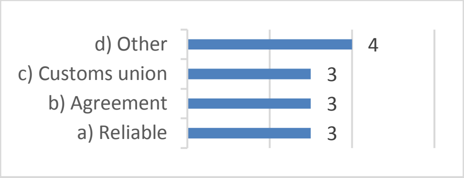
(a) The certificate has to be issued by a foreign certification authority that my country recognizes as reliable;

(b) The certificate has to be issued in a country with which my country has a relevant bilateral or multilateral agreement(s);

(c) The certificate has to be issued within the customs union of which my country is part;

(d) Other.

If other, please specify (max 300 characters):



Question 6

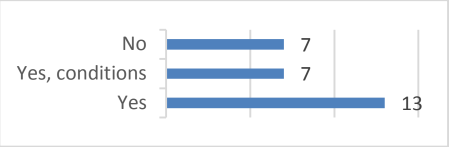
In your country, can a non-resident obtain a certificate for a PKI electronic signature?

(a) Yes;

(b) Yes, under specific conditions;

Please specify (max 300 characters):

(c) No.



Section 3: Electronic authentication mechanisms for eTIR

Question 7

Do you consider it necessary that the holder (or his representative) 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 electronic authentication mechanism), 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 the customs office of departure?

(a) Yes, a person submitting data electronically to customs needs to be always authenticated (by means of either a PKI electronic signature or any other type of electronic authentication mechanism)

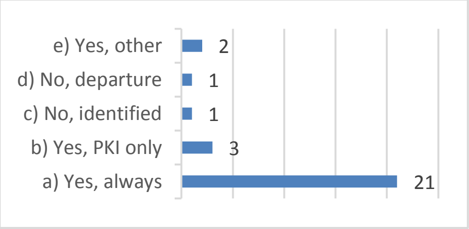
(b) Yes by means of PKI electronic -signature only;

(c) Yes, by means of other authentication mechanism(s);

Such as (please list) (max 300 characters):

(d) No, electronic authentication is not needed because the holder can always be identified in case of irregularity;

(e) No, electronic authentication is not needed because the holder (or his representative) can be authenticated when presenting the goods and the vehicle at the customs office of departure.

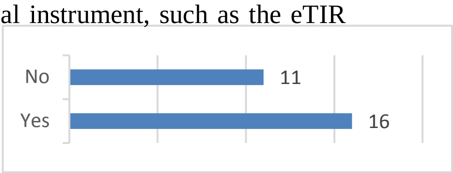


Question 8

(i) In your view, would it be possible that the Customs authorities of your country could accept PKI electronic signatures for eTIR in particular, 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 eTIR legal framework)?

(a) Yes;

(b) No.



(ii) If yes, would your government be interested that such certification authority would be developed within the eTIR legal framework?

(a) Yes;

(b) No.