Economic and Social Council

Economic Commission for Europe

Inland Transport Committee

Working Party on Customs Questions affecting Transport

148th session
Geneva, 6-9 February 2018
Item 4 (b) (iv) of the provisional agenda
**Customs Convention on the International Transport of Goods
under Cover of TIR Carnets (TIR Convention, 1975):
Revision of the Convention**

Draft Annex 11 to the TIR Convention

Note by the secretariat

I. Background and mandate

1.   At its fifth session (October 2017), the Group of Experts on the Legal Aspects of Computerization of the TIR Procedure (GE.2) considered the results of a survey on electronic authentication mechanisms. The Group of Experts welcomed the survey results and reiterated its findings from the survey, at previous sessions, that data submitted electronically required authentication in all countries, along with a variety of methods of authentication in use and differing specificities and legal status of electronic signatures. On the other hand, as it was not possible to discuss some issues arising from the survey results due to limited participation to its meetings, GE.2 concluded that it would be useful to discuss the authentication mechanisms to be used in the eTIR system at the Working Party on Customs Questions affecting Transport (WP.30), which is a well-attended body. To this end, the secretariat was requested to prepare a new document that summarized the results of the survey for the consideration of WP.30 at its next session.

2.   In line with the above, the secretariat has prepared the present document that includes the considerations by GE.2, a summary of survey findings and statistical data on results of the survey, in Annex I and replies to the survey, in Annex II.

II. Considerations by the Group of Experts

3.   At its second session (April 2016), the Group of Experts decided to conduct a survey with the objective of collecting information that will enable a realistic assessment of the

most suitable electronic authentication requirements for eTIR. Further to this, a survey was prepared by the secretariat 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. The secretariat launched the survey electronically in September 2016, following electronic consultations and approval of GE.2, and had compiled the preliminary results of the survey for discussion at the third session.

4.   At its third session (December 2016), GE.2 welcomed the preliminary results of the survey, as presented in Informal document WP.30/GE.2 (2016) No.1, and requested the secretariat to revise the document to indicate more details about the various replies. GE.2 was also of the view that the results would be more representative if more Contracting Parties, particularly outside of the European Union and the New Computerized Transit System (NCTS), would reply. Against this background, the Secretariat requested the Contracting Parties, who had not yet done so, to reply to the survey by the end of April 2017. Only two additional replies were received in that period. Subsequently, the secretariat prepared Informal document WP.30/GE.2 (2017) No. 1 which contained an updated analysis of the survey results and the statistics about the replies as an annex.

5.   At its fourth session (May 2017), GE.2 welcomed Informal document WP.30/GE.2 (2017) No. 1, and noted that only two additional replies had been received after the extension of the deadline, hence thirty-five received in total, and that those replies had not affected the conclusions derived from the survey as presented at the previous session. Furthermore, the secretariat informed GE.2 that the analysis of the survey results, in terms of different regions and transit systems, had revealed that there was a requirement for authentication in all countries, but a variety of methods of authentication were in use, with differing specificities of electronic signatures and legal status thereof. However, GE.2 did note, with concern, that a limited number of respondents had indicated that the only applicable authentication method in their countries is Public Key Infrastructure (PKI) electronic signature, issued by a domestic certification authority and, exclusively, to the residents of those countries. This appeared to imply that those countries would likely not be able to apply Annex 11 in its current form unless national legal reforms would be introduced. A number of delegations were of the view that the replies of those countries should be examined more closely at the next session, in order to assess the situation and discuss possible ways forward. To this end, the secretariat was requested to prepare a new document, focused on the above-described parameters, for consideration at the next session. At the same time, GE.2 agreed that the survey, as such, could be considered completed.

6.   At its fifth session (October 2017), GE.2 welcomed document ECE/TRANS/WP.30/GE.2/2017/3 that contained the replies of the thirty-five countries. GE.2 reiterated its findings from the survey that data submitted electronically required authentication in all countries, along with a variety of methods of authentication in use and differing specificities and legal status of electronic signatures. It was noted that a limited number of respondents had indicated that the only applicable authentication method in their countries was the PKI electronic signature that was issued by a domestic certification authority exclusively to the residents of the country. That raised a concern about the methods of authentication in draft Annex 11. GE.2 also noted with concern that it was not possible to consider the national requirements of the countries who wished to take part in eTIR pilot projects since they had not participated in the survey. GE.2 concluded that it would be useful to discuss the authentication mechanisms to be used in the eTIR system at WP.30, which is a well-attended body.

III.   Summary of survey findings[1]

7.   The survey was replied by following thirty- five Contracting Parties: Armenia, Austria, Azerbaijan, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Finland, France, Greece, Hungary, Iran (Islamic Republic of), Ireland, Italy, Kyrgyzstan, Latvia, Lithuania, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Russian Federation, Serbia, Slovenia, Sweden, Switzerland, the former Yugoslav Republic of Macedonia, Turkey and United Kingdom of Great Britain and Northern Ireland. Outcomes of each section of the questionnaire were as follows:

A.   Section 1: General

8.   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. 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".

B.   Section 2: Public Key Infrastructure (PKI) Electronic signatures

9.   This section searches for information on the legal validity of and the conditions for using the 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, only in 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.

C.   Section 3: Electronic authentication mechanisms for eTIR

10.   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 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 in favour of this option. Countries with positive approach to internationally recognized certification authority are also mostly interested in developing such a certification authority within the eTIR legal framework.

---

[1] Detailed survey findings are available in Informal document WP.30/GE.2 (2017) No.1.
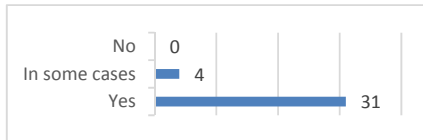
Annex I

## Results of the Survey[2]

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.

|	
No	0
In some cases	4
Yes	31

(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.

No	1
In some cases	5
Yes	29
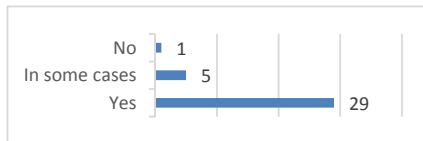
(iii) *Are customs authorities in your country planning to move to a computerized environment that will allow electronic declaration and data exchange in the future?*

  (a) Yes;

  (b) No.

  Comment (max 300 characters)

No	0
Yes	8

---
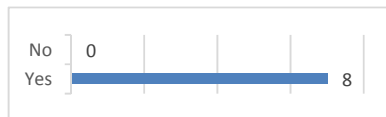
[2] Annex I is an update of the Annex to the Informal document WP.30/GE.2 (2017) No.1. This Annex includes the replies of the Russian Federation which were received after the release of mentioned document.

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.

No	0
In some cases	4
Always	28
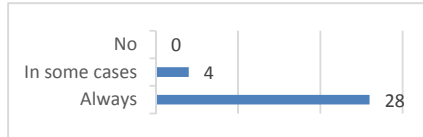
(ii)   *Please select the method or methods used by customs in your country for the authentication of the person sending electronic information (you can select more than one):*

　　　　(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)

Other	1
PKI	16
SMS	2
Symmetric KA	2
Usernames and passwords	18
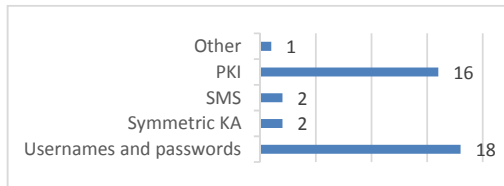
Section 2: Public Key Infrastructure (PKI) Electronic signatures

Question 3

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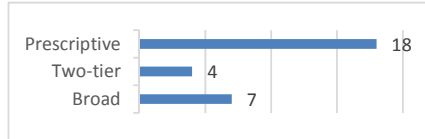
　　　　(a)　　Yes

　　　　(b)　　No

No	4
Yes	30
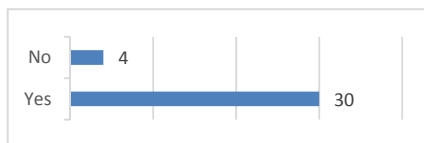
(ii)   *Please select the type of legislation in force:*

　　　　(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).

Prescriptive   18
Two-tier   4
Broad   7

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.

No   2
Either high or low   2
Yes, low   1
Yes, high   24
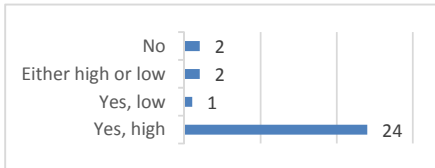
Question 5

(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.

No   17
Yes, conditions   12
Yes   1
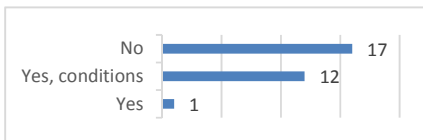
(ii)   Please select the applicable conditions/restrictions which apply to the acceptance of PKI electronic signatures generated using a certificate issued by foreign certification authorities:

(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):
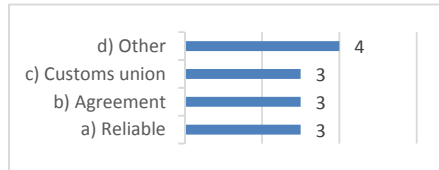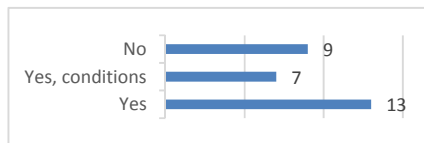

Question 6

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.

e) Yes, other	2
d) No, departure	1
c) No, identified	1
b) Yes, PKI only	4
a) Yes, always	22
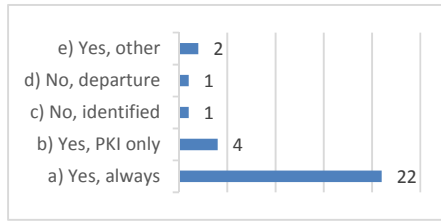
Question 8

(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.

No	12
Yes	17
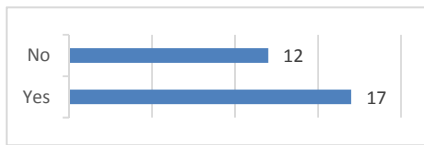
(ii)   If yes, would your government be interested that such certification authority would be developed within the eTIR legal framework?

(a)   Yes;

(b)   No.

No	1
Yes	12
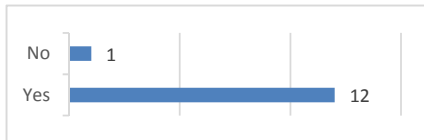
Annex II

Replies to the survey[3]

Country	Q/1/i	Q/1/ii	Q/1/iii	Q/2/i	Q/2/ii	Q/3/i	Q/3/ii	Q/4	Q/5/i	Q/5/ii	Q/6	Q/7	Q/8/i	Q/8/ii
Armenia	a	a	a	a	d	a	c	c	b	b	a	a		
Austria	a	a	b	a	a	b			c			a	b	
Azerbaijan	a	a	a	a	d	a	c	a	c		c	a	a	
Belarus	a	a	a	b	d	a	c	a	c	d	c	a	a	b
Belgium	b	b	a	b	e	a	b	a	a	a	a	a	a	
Bosnia and Herzegovina	b	b	a			b								
Bulgaria	a	b	a	a	d	a	c	b	b	c	c	b	b	
Croatia	a	a	b	a	d	a	a	a	c	d	a	a	b	
Cyprus	a	c	a	a	a	a	c	a	b	d	a	c	a	a
Czech Republic	a	a	b	a	d	a	c	a	b	d	a	a	a	b
Denmark	a	b	a	a	a	a	a	a	c	d	c	a	b	
Finland	a	a	a	a	d	a	a	a	c	d	b	a	a	a
France	a	a	a	a	a	a	c	a	b	c	b	a	a	a
Greece	a	a	a	a	a	a			c	d	a	a	b	
Hungary	a	a	a	a	a	a	b	a	b	d	b	c		
Iran (Islamic Republic of)	a	a	a	a	a	a	b	a	b	b	a		a	a
Ireland	a	a	b	a	d	a	c	a	c	d	a	a	b	
Italy	a	a	a	a	a	a	c	a	b	a	a	a	a	a
Kyrgyzstan	b	a	a	c	a	b		d	c		c	e	b	
Latvia	a	a	a	a	a	a	c	a	c		c	a	a	a
Lithuania	a	a	a	a	a	a	c	a	b	b	b	a	a	a
Montenegro	a	a	a	a	b	a	a	d	c	a	a	b	a	a
Netherlands	a	a	a	a		a								
Norway	a	a	a	c	a	b						a		
Poland	a	a		a	d	a	b	a	b	a	b	a	a	a
Portugal	a	a	a	a	a	b	c	a	c	d	b	a	b	
Romania	a	a	a	a	a	a	c	a	b	c	a	a	a	
Russian Federation	a	a		a	d	a	c	a	b	d	c	b	b	b
Serbia	a	a	a	a	d	a	c	a	c	d	c	a	a	a
Slovenia	a	a		a	d	a	a	a	c	d	a	a	a	a
Sweden	a	a	a	a	e	a	a	c	c	d	b	a	a	a

---

[3] This Annex is a reproduction of Chapter II of the document ECE/TRANS/WP.30/GE.2/2017/3. It is recommended that these replies are considered along with comments made by the respondents to the survey, as indicated in mentioned document.

Country	Q/1/i	Q/1/ii	Q/1/iii	Q/2/i	Q/2/ii	Q/3/i	Q/3/ii	Q/4	Q/5/i	Q/5/ii	Q/6	Q/7	Q/8/i	Q/8/ii
Switzerland	a	a	a	a	a	a	c	a	c		c	d	b	
The former Yugoslav Republic of Macedonia	b	a	a	b	d	a	a	a	c		c	b	b	
Turkey	a	b	a	a	a	a	c	a	c		a	a	a	
United Kingdom	a	a		b	c									