Distr.: General
17 September 2014

English only

Economic Commission for Europe

Inland Transport Committee

Working Party on Customs Questions affecting Transport

Informal Ad hoc Expert Group on Conceptual and Technical Aspects of Computerization of the TIR Procedure

Twenty-fourth session
Antalya, 25-26 September 2014
Item 3 of the provisional agenda
New information and communication technology developments in the TIR system

Ensuring mutual recognition of electronic signatures

Note by the secretariat

I. Background

1. At its twentieth session (19-20 April 2012), the Informal Ad hoc Expert Group on Conceptual and Technical Aspects of Computerization of the TIR Procedure (GE.1 or Expert Group) discussed results of the survey on the use of electronic signatures in the framework of the eTIR project, contained in Informal document GE.1 No. 3 (2012). 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 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).

2. In view of the above, the secretariat deems it appropriate to provide GE.1 with information about new concepts on the mutual recognition of electronic signatures, as presented below by Mr. Aleksandr Sazonov (deputy general director on development "National Certification Authority Rus" CJSC, UN/CEFACT Recommendation for ensuring legally significant trusted trans-boundary electronic interaction project leader).

II. New concepts

3. Electronic signature based on Public Key Infrastructure (PKI)-technology (hereafter electronic signature) is one of the means that can be used to ensure e-document genuineness (integrity + authenticity). This technology is widely used, as it is sufficiently secure and scalable. But it has peculiarities that cause some difficulties in the cross-border exchange of e-documents. Users who have electronic signature certificates (hereafter certificates) issued by one CA can verify electronic signatures of each other easily. But if users have certificates issued by different CA's they generally cannot mutually verify electronic signatures.

4. If user Anton wants to verify electronic signature of user Bertha he has to:

a) trust Bertha's CA that has issued the certificate for user Bertha

b) be able to technically verify Bertha's electronic signature.

Both of these points cause difficulties - especially in cross-border scenarios.

5. There are several approaches on implementing services of the verification and attestation of foreign electronic signatures, each having their pros and cons. The most applicable approach for providing such services is the usage of trusted services of a third party (or TTP services). The idea is not new - it is addressed in X.842 recommendations. The possibility to use other variants is severely limited.

6. Nowadays, steps on the establishment of TTP services infrastructure are being taken in the Russian Federation and the European Union (EU). In the EU, there are even several projects, where TTP services based on one or another technology are used (for example, PEPPOL and E-CODEX). But the TTP services within these projects can be used for the projects tasks only, not for general purposes.

7. Neither the Russian Federation nor the EU have a complete legal basis that would enable launching TTP services of verification and attestation of electronic signatures for a wide scope of tasks.

8. But the situation is improving:

- Electronic Identification and Signature (eIDAS) Regulation has been agreed in the European Union;
- Documents on TTP within the framework of Eurasian Economic Union, such as IISFMT (Integrated Information System of Foreign and Mutual Trade), are being developed. The Development Strategy will possibly include expansion of application scope of TTP services by 2020.

9. There can be different variants of TTP services infrastructure architecture:

a) There can be a single international TTP service that verifies electronic certificates issued by CA's in different countries.

b) There can be a single TTP service per country (so called National TTP service). And such National TTPs mutually forward the electronic verification requests to each other.

c) There can be several TTP services that bilaterally interact with each other in their own country as well as with TTP services in other countries.

10. In practice there can be a combination of all the variants a, b and c. For example, a few small countries agreed to establish a joint (international) TTP service that verifies electronic certificates issued by CA's in these countries. And this joint TTP service interacts with respective National TTP services of several other countries. For more details, please refer to the White Paper on Common trust infrastructure for legally significant transboundary electronic interaction[1].

11. Thus, the accumulated major experiences can be re-used in the framework of eTIR:

a) An architecture of TTP services as well as the related legal basis can be designed, respectively adopted, for the specific requirements of eTIR. An advantage of such an approach is that it can be practically implemented within a reasonable period. Its disadvantage is that it will be just another local solution for a particular area of application.

or

b) The principles of establishing and operating TTP services as well as of the necessary legal basis for the mutual cross-border recognition of the results of the TPP services can be laid down to enable trusted electronic interaction with reference to existing eIDAS and/or IISFMT documents. This variant is the best one from the point of view of reusability and further development / extension, as well as for the alignment of the eTIR framework with already existing frameworks on eIDAS and IISFMT. But it may take much time until the TTP services within eIDAS are launched and become operational.

III. Considerations by the Expert Group

12. The Expert Group may wish to take the above presented concepts into consideration and assess whether it seems appropriate to revisit the eTIR Reference Model in order to introduce such concepts or, alternatively, propose that they be put to the test in, for example, the framework of a future pilot project.

[1] For more information see the white paper available at http://www.en.rcc.org.ru/userdocs/docs/TTS_White_Paper.pdf