Note on electronic Signatures in CITES Permits

1. This document has been drafted by the Secretariat for discussion in the CITES Working Group on electronic Systems and Information Technologies

CITES documentary requirements

2. CITES Resolution Conf. 12.3 (Rev. CoP17)[1] provides a compilation of recommendations and standards relating to documentary requirements of CITES permits and certificates in paper and electronic format.

3. Resolution Conf. 12.3 (Rev. CoP17) states the **equivalence of paper and electronic CITES permits:**

> *RECOGNIZING that permits and certificates may be issued in paper, electronic or both formats;*
>
> *RECOGNIZING that there is no obligation on Parties to issue permits or certificates in electronic formats;*
>
> *2. AGREES that:*
>
> > *b) Permits and certificates may be issued in paper format or electronic format provided all Parties involved have agreed with the electronic format*
>
> *3. RECOMMENDS that:*
>
> > *k) all Parties consider the development and use of electronic permits and certificates;*

4. With regard to signatures and stamps Resolution Conf. 12.3 (Rev. CoP17) states the **functional equivalence of physical and electronic signatures:**

> *2. AGREES that:*
>
> > *e) if a permit or certificate form, whether issued in an electronic or paper format, includes a place for the signature of the applicant, the absence of the handwritten signature or in case of electronic forms any electronic equivalent should render the permit or certificate invalid;*
>
> *Annex 1 Information that should be included in CITES permits and certificates*
>
> > *l) The name of the signatory and his/her handwritten signature for paper permits and certificates or its electronic equivalent for electronic permits and certificates*

[1] https://cites.org/eng/res/12/12-03R17.php

m) The embossed seal or ink stamp of the Management Authority or its electronic equivalent

Concerns of Parties

5. Several Parties informed the Secretariat that the requirement for electronic signatures in Resolution Conf. 12.3 (Rev. CoP17) could cause practical problems in the implementation of electronic CITES permits.

6. In particular Parties were concerned that an electronic equivalent of a physical signature is often associated with asymmetric encryption technology such solutions using the RSA algorithm and Public Key Infrastructure (PKI).

7. As most countries do not have PKI and/or legislation that fully supports use of PKI for trade documents, the lack of PKI infrastructure would prevent the widespread adaption of electronic CITES permits.

International recommendations for use of electronic signatures in trade documents

8. The Nations Centre for Trade Facilitation and electronic Business (UN/CEFACT), an intergovernmental body of UNECE, is the UN focal point to develop international standards for trade facilitation and electronic Business.

9. CITES has a well-established liaison with UN/CEFACT. The CITES Permit is based on the UN Layout Key (UN/CEFACT Recommendation 1), and the CITES XML standard for electronic permits[2] is based on the eCERT standard of UN/CEFACT.

10. UN/CEFACT has issued Recommendation 14 on *Authentication of trade documents*[3], which provides recommendations to Governments and trade on the use of physical and electronic signatures in trade documents. In developing this Recommendation UN/CEFACT worked closely with the United Nations Commission on International Trade Law (UNCITRAL) and prepared Recommendation 14 in alignment with relevant work of UNCITRAL.

[2] CITES ePermitting Toolkit, https://oldsrv.cites.org/eng/prog/e/toolkit/index.htm

[3] https://www.unece.org/tradewelcome/un-centre-for-trade-facilitation-and-e-business-uncefact/outputs/cefactrecommendationsrec-index/list-of-trade-facilitation-recommendations-n-11-to-15.html

11. Recommendation 14 was revised in 2014 to meet the latest requirements of electronic document exchanges.

Guidance on use of electronic Signatures in UN/CEFACT Recommendation 14

12. UN/CEFACT and UN/CITRAL specifically distinguish between *electronic signatures* and *digital signatures*: An electronic signature does not call for a specific type of technology, rather it is a process that serves the same functions as a manual signature. An *electronic signature* is defined as

> *Data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's intention in respect of the information contained in the data message.*
>
> *In its broadest sense, a signature (manual-ink or its electronic equivalent) creates a link between a person (physical or legal) and the content (document, transaction, procedure, or other). This link can be considered as having three inherent functions: an identification function, an evidentiary function and an attribution function.*
>
> *In international business relations, one of the basic foundations[4] is trust between the parties; the requirements of a signature will, in many cases, most likely reflect that trust.*

13. By contrast, the term *digital signature* denotes the implementation of an electronic signature in a specific technology and is usually associated with signatures using asymmetric encryption and PKI technology. Thus a digital signature is a specific technology choice for the implementation of an electronic signature.

14. When implementing electronic signatures, UN/CEFACT recommends that Parties avoid adopting solutions that are more costly and burdensome than the manual signature process (UN/CEFACT Recommendation 14, para 38). Similarly, UNCITRAL recommends that the method of authentication should be "as reliable as was appropriate for the purpose for which the data message was generated"[5].

15. UN/CEFACT specifically notes that an electronic signature providing the required security level can be **implemented through different technologies** other than PKI.

16. The Recommendation states that, for example, an electronic signature could be implemented through a registration and verification process based on an ID/password for identification of the user and a secure connection between the user and the application.

17. The important criteria to qualify as an electronic signature is not the technology used but whether the electronic signature is a **functional equivalent to the paper signature,** i.e.

[4] For further discussion on the *Functions of a signature* see UN/CEFACT Recommendation 14, para 16

[5] UNCITRAL "Model Law on Electronic Commerce with Guide to Enactment 1996 with additional articles 5bis as adopted in 1998"

whether the chosen technology solution delivers the same level of reliability as the physical signature (UN/CEFACT Recommendation 14, para 66).

Relevance of Recommendation 14 for CITES electronic signatures

15. Resolution Conf. 12.3 (Rev. CoP17) establishes the functional equivalence of physical and electronic signatures in CITES permits and explicitly uses the term "*electronic signature*".

16. UN/CEFACT Recommendation 14 and UNCITRAL Model Law states that any electronic process that provides the functional equivalence of the physical signature constitutes an electronic signature.

17. If CITES follows advise of UN/CEFACT Recommendation 14 then Parties are not required to use digital (i.e. PKI type) signatures as electronic equivalent to the paper based signature. Instead Parties can use other forms of electronic signature, for example, by identifying exporters through ID and passwords when requesting CITES permits or by using secure document exchange for cross border permit exchanges with other Parties.

Guidance to Parties on electronic Signatures in CITES permits

18. Resolution Conf. 12.3 (Rev. CoP17) currently lacks clear guidance to Parties on which functionality the paper or electronic signature should provide, i.e. an explanation why a signature or a seal is required in the document.

Recommendation

19. It is therefore suggested that the ePermitting Working Group provides following recommendation to the Standing Committee for an update of Resolution Conf. 12.3 (Rev. CoP17):

RECOMMENDS that

a) Parties should consider UN/CEFACT Recommendation 14 as best practice when implementing the electronic equivalent of signatures and seals in electronic CITES permitting systems ;
b) Parties using electronic CITES systems should use username and passwords and/or similar technologies to authenticate all users that have access to the system;
c) electronic CITES systems must keep an audit trail, i.e. keep electronic records that enable the Management Authority to identify the person who requested, approved, processed or altered electronic CITES permits and certificates; and
d) archives of audit trials must be kept for no fewer than 5 years after the expiry date of the permit; and

AGREES that in electronic CITES systems that meet the above requirements, the electronic equivalent of a physical signature and a seal is provided through the identification of the permit applicant, the identification of the official that issued or authorized the document, and the identification of the issuing agency.