UNITED NATIONS **E**

Economic and Social Council

Distr.
GENERAL

ECE/TRADE/C/WP.7/GE.1/2007/7
20 April 2007

ENGLISH
Original: FRENCH

ECONOMIC COMMISSION FOR EUROPE

COMMITTEE ON TRADE

Working Party on Agricultural Quality Standards

Specialized Section on Standardization of Fresh Fruit and Vegetables

Fifty-third session
Geneva, 21-25 May 2007
Item 5 (a) of the provisional agenda

AMENDMENTS TO THE GENERAL TEXTS

CONFORMITY CERTIFICATE

Document submitted by France*

DEMATERIALIZATION OF EXPORT CERTIFICATES FOR FRUIT AND VEGETABLES

I. BACKGROUND

1. Prompted by the need to modernize export control operations (many companies have their own control system) and by the increasing use of information technology, States are looking for ways of reducing the time required for control operations and the related costs.

2. The dematerialization of control certificates is one solution that reflects the development of e-government in France.

* The present document has been submitted after the official documentation deadline by the Trade and Timber Division due to resource constraints.

II. TERMINOLOGY: SOME DEFINITIONS

Digital certificate
Electronic certification
Electronic export certificate
Digital signature
Digital certification

3. The vocabulary should be used carefully, as the terms cover several concepts which have a specific meaning for specialists in this area, a fact that could lead to misunderstandings.

A. Electronic or digital certification

4. This term refers to a process of certification by a recognized external body, which attests that the electronic system in place meets the four security criteria listed below:

- **Sender authentication**. All individuals must be able to identify themselves in a secure manner (for example, using a password or smart card) before sending a message to ensure their identity cannot be stolen by a third party;

- **Non-repudiation**. The person receiving the message must be able to know with certainty that the sender will not at some time in the future deny sending it;

- **Integrity of data exchange**. It must not be possible for the message to be modified between the time it is sent and the time it is received;

- **Data confidentiality**. It must not be possible for the message to be viewed by a third party during its transfer.

B. Digital certificate

5. This certificate is issued by a recognized certification authority, usually for a fee. It is the operator's "identity card" and makes the operator's electronic transactions legally binding.

C. Digital signature or electronic signature

6. Digital or electronic signatures authenticate the authorship of an electronic document and guarantee its integrity, in the same way as a manual signature on a paper document. A digital signature must have the following features:

- It must allow the reader of a document to identify the person or body that has signed it;

- It must serve as a guarantee that the document has not been modified between the time it was signed by the author and the time it was viewed by the reader.

7. To this end, the following conditions must be met:

- It must not be possible to alter the signature;
- It must not be possible to reuse the signature: it forms part of the signed document and cannot be moved to another document;
- It must not be possible to modify a signed document; once signed, a document cannot be altered.

8. It is only through the use of public-key cryptography that electronic signatures have been made possible. They differ from manual signatures in that they are not visual but correspond to a string of numbers. A scanned manual signature - or one that is reproduced in any other way - is not an electronic signature.

III. CONCLUSION

9. It is thus preferable to speak of “dematerialization” in a general manner, as States may choose different levels of dematerialization. For example:

- Certificates may be drafted on a laptop and printed out directly;
- The operator may send a certificate by e-mail to the control service and receive a signed copy in return by e-mail, fax or post.

IV. THE SYSTEM INSTITUTED IN FRANCE IN 2007

10. Export data (all information listed on the control certificate) are communicated by the operator on the Internet.

11. The certificate is checked by the inspector (risk analysis and consistency of declarations) in one of two ways:

- The certificate is printed out and checked manually;
- The certificate is authorized by the attachment of an “electronic signature” (special personal USB key used with a code - operates in the same manner as a credit card) and the signed certificate is sent back to the operator by e-mail.

12. Consequences of the electronic signature of a quality control certificate:

- No longer bears a manual signature;
- Box 13 (Observations) of the control certificate, contains a comment such as “This certificate was signed electronically”;
- Authenticity of the certificate can be checked on the website indicated on the certificate.
