

CONCOURS EXTERNE ET INTERNE DES 23, 24 ET 25 FEVRIER 2011

**POUR L'EMPLOI D'INSPECTEUR DES DOUANES ET DROITS INDIRECTS
DANS LA SPÉCIALITÉ « TRAITEMENT AUTOMATISÉ DE L'INFORMATION –
PROGRAMMEUR SYSTÈME D'EXPLOITATION »**

ÉPREUVE ÉCRITE D'ADMISSIBILITÉ N° 4 (FACULTATIVE)

(DURÉE : 2 HEURES - COEFFICIENT 3)

**TRADUCTION SANS DICTIONNAIRE D'UN TEXTE TECHNIQUE
RÉDIGÉ EN ANGLAIS**

AVERTISSEMENTS IMPORTANTS

L'usage de tout document autre que le support fourni est interdit.

L'usage de tout matériel autre que celui d'écriture est interdit.

Toute fraude ou tentative de fraude constatée par la commission de surveillance entraînera l'exclusion du concours.

Il vous est interdit de quitter définitivement la salle d'examen avant le terme de la première heure.

Le présent document comporte 3 pages numérotées.

National Single Windows (NSW)

Managing a new chain of trust for an end-to-end dematerialization

This project of dematerialization will only have limited effect if undertaken solely at a national level. To be more successful, the management of chain of trust should be addressed at a more global level.

For example, in the case of dematerialization of CITES, sanitary certificates, certificates of origin etc., until the connection between export and import authorities is available (eg. CITES), the import authority may have to formalize an understanding with the export authority to guarantee the authenticity of a electronically signed document circulating between export and import.

An e-doc is trusted if its digital signature is valid – i.e.:

- the e-doc has not been altered (integrity)
- the issuer of the e-doc is safely authenticated

It's easy to check the integrity of the e-doc, but a trust scheme is needed to authenticate the signer. As a mutual recognition of CA signature is still far away, an e-document by e-document / issuer by issuer approach using a Valid Certificate List (VCL) is proposed to answer the question: “who is allowed to sign what?”

Computerized checks, which would lead to reconsideration of time-costly (and often not carried out) controls of paper document:

- the signature is cryptographically correct
- the certificate used for the signature belongs to the VCL
- none of the certificates of the certification path are revoked (CRL)

This VCL - storing all the approved e-certificates - can be implemented on the export or the import side and used to certify the authenticity of the signatory.

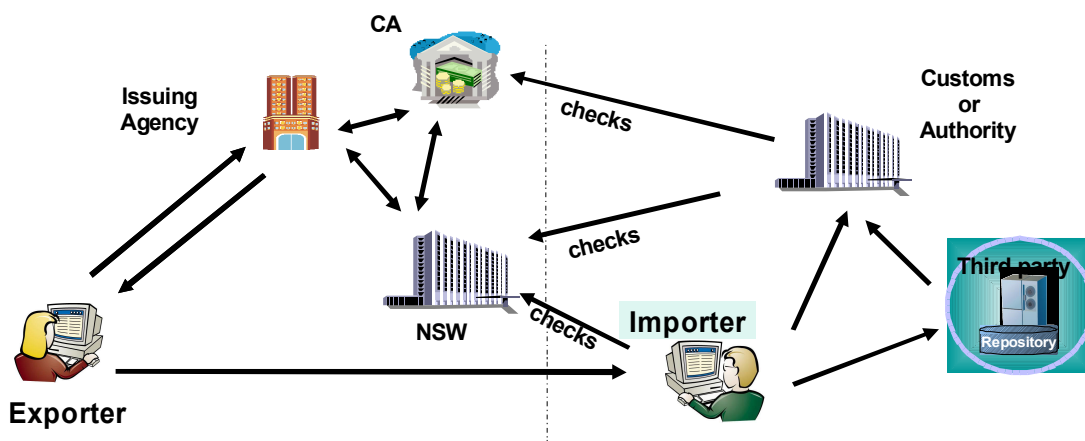


Fig: Import customs has access to e-doc and integrity/authenticity controls

Ground rules

The following ground rules should be kept in mind:

- E-documents will be referenced in customs declarations;
- These references will identify the permanent location of the e-document;
- Digital signatures are a means for maintaining authenticity and integrity of the data;
- The relying parties (origin and destination countries) agree on the limited question of accepting the national Certifying Authority's (CA) certificates issued to the e-document issuing authority;
- The signatures and the archived information are long-living and will be valid beyond the life-cycle of the certificate or the Certifying Authority;
- Customs can download e-doc information as and when it needs.