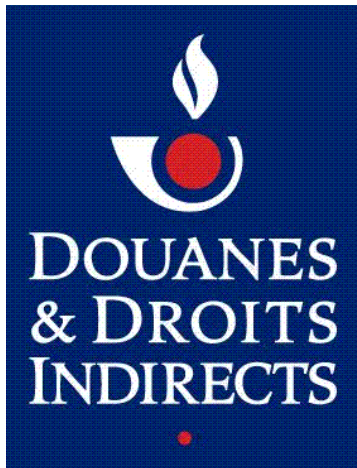




**MINISTÈRE  
DE L'ÉCONOMIE, DE L'INDUSTRIE  
ET DE L'EMPLOI**

**MINISTÈRE  
DU BUDGET, DES COMPTES PUBLICS  
ET DE LA FONCTION PUBLIQUE**



**Direction Générale des Douanes et Droits Indirects**

**Annales des épreuves**



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE

AP4X07V1

**CONCOURS EXTERNE ET INTERNE DES 27, 28 FÉVRIER ET 1<sup>ER</sup> MARS 2007**

**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.

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.

# 1.Public Key Infrastructure (PKI)

## Introduction

The Security Requirements expressed in the specifications indicate some areas where cryptographic controls, which are usually well served by a Public Key Infrastructure (PKI), are needed.

A PKI is the combination of software, encryption technologies, processes, and services that enable an organization to secure its communications and business transactions. A PKI solution usually meets the security requirements of authenticity (strong authentication), confidentiality (data encryption), integrity (digital signature), and non-repudiation.

For EMCS, the areas where cryptographic controls are needed concern :

- **Strong authentication** (i.e. certificate-based), which is required to securely authenticate Member State Administration (MSA) Users and National Excise Applications (NEA) applications accessing central services (SEED, CS/RD, CS/MIS) through the web services channel.

Strong authentication requirements that may be considered by MSA to securely authenticate Economic Operators accessing the NEA is a national matter, which is out of the scope of the technical specifications.

- **Cross-organisational Unique Identity.** An MSA Official who has already received an X.509 certificate from its administration to access national services could use this same certificate to access EMCS Central Services (and not a second certificate delivered by an accredited EC certification authority).

This means that a trust relationship has to be established between MSA PKIs and the EMCS Common Domain PKI (CDPKI).

- **Secure Audit Logs.** Every NEA shall produce cryptographically protected audit logs so as to be able to detect an illegitimate use of the system by EMCS users and applications.
- **Digital Signature.** Although not explicitly mentioned in the functional specifications, there is a need for MSAs to get the assurance that an excise movement agreed between two Economic Operators (i.e. the consignor and the consignee) will not basically lead to a fake movement.

A way to address this issue could consist in obtaining from the Economic Operators involved in an excise movement a document informing about the nature of the agreed movement (e.g. product, volumes, place of dispatch, place of destination, etc.) that would be digitally signed by both operators.

This document would be attached (in one way or another) to the draft electronic Administrative Accompanying Document (e-AAD) submitted by the consignor and checked by the MSA at Dispatch prior to deliver a valid e-AAD.

The verification of both consignor and consignee digital signatures could be achieved automatically by the NEA or even manually by an MSA official.

## Problem Statement

If MSAs wish to exploit their electronic capability for business-to-business applications e.g. to transparently access EMCS Central Services  *$n \times (n-1)$  trust relationships between national PKIs will be required.*

However, national domain PKIs may implement different architectures, security policies, and cryptographic suite, which make the interoperability between those PKIs almost impossible considering the high number of PKIs communities to interconnect. Therefore a flexible mechanism is needed to link these PKIs.

Within a PKI, a normalised data structure called *X.509 certificate* is used to bind a specific identity to a specific public key and information on how the public key can be used (e.g. SSL server certificate, e-mail signer certificate, etc.). *Certification Authorities (CA)* are trusted entities that issue certificates to users within a PKI and provide status information about the certificates the CA has issued.

Today, PKI architectures encountered in the MSAs (and Economic Operators) fall into one of the three configurations illustrated at the Figure 1 :

- A single CA (T1), or
- A hierarchy of CAs (T2), or
- A mesh of CAs (T3).

Each of the configurations is determined by fundamental attributes of the PKI : the number of CAs in the PKI, the links between CAs in a hierarchy of CAs (links labelled “B” on the figure), where users of the PKI place their trust (known as *user trust point*<sup>1</sup>), and the trust relationships between CAs within a multi-CA PKI (links labelled “C” on the figure).

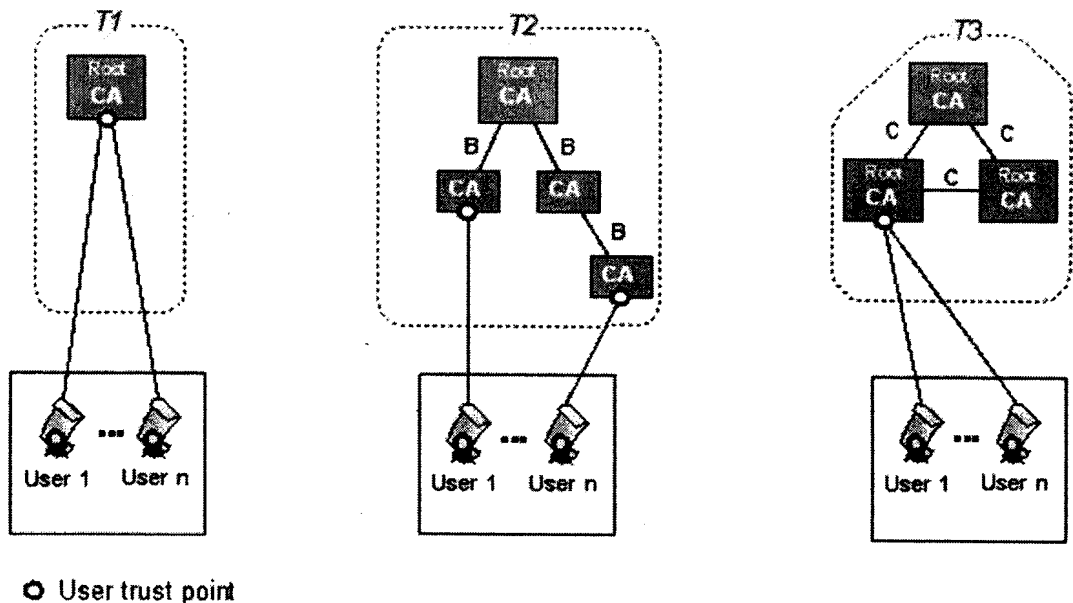


Figure 1 : PKI Architecture Types

<sup>1</sup> The user trust point corresponds to the CA that effectively signed the user certificate.

To allow interoperability between MSAs, isolated CAs shall be combined to form larger PKIs. The two basic ways to achieve this is using superior-subordinate relationships, or peer-to-peer relationships (Figure 2). In theory, any organisational structure can be realised using either of the two methods.

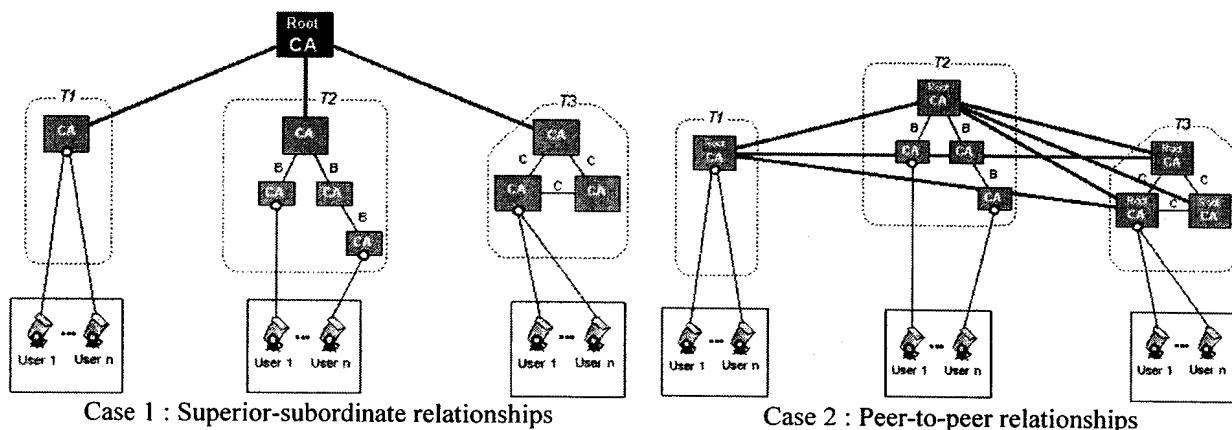


Figure 2 : CA Combinations

In practice, however, there are technical and political issues encountered when architecting organisational PKIs. Each method has its strengths and weaknesses. For large, more complex organisations such as the one encountered within EMCS, none of those methods can provide a satisfactory result.

Indeed, in a PKI constructed with superior-subordinate relationships (Case 1) provides a good scalability and easy to develop certification paths (unidirectional) but presents some drawbacks resulting from the reliance on a single trust point ; the compromise of a “root” CA, everyone’s trust point, results in a compromise of the entire PKI. Worse yet, there are no straightforward recovery techniques. The nature of a hierarchical PKI is that all trust is concentrated in the “root” CA and failure of that trust point is catastrophic. Another drawback is that agreement on a single “root” CA may be politically impractical because all MSAs must adjust their trust points.

PKI constructed with a peer-to-peer relationship (Case 2) presents the advantage of being very resilient (no single point of failure) : CAs issue certificates to each other and since the CAs have peer-to-peer relationships, they cannot impose conditions governing the types of certificates other CAs can issue. Moreover, mesh PKI can easily incorporate a new community of users ; any one of the CAs in the mesh simply establishes a trust relationship with that community’s CA. But mesh PKIs presents some drawbacks resulting from the bi-directional trust model : certification path development is more complex than in a hierarchy. This makes path discovery more difficult since there are multiple choices. Users in a mesh PKI must also determine which application a certificate may be used for (e.g. access to SEED database) based on the contents of the certificates rather than the CA’s location in the PKI. This requires larger and more complex certificates and more complicated certificate path processing.

## 2. Glossaire (ne pas traduire)

EMCS (Excise Movement and Control System) is a computerised system for monitoring movements of excise goods between Member States under duty suspension.