16 October 2015

Certification Policy – English Summary

Version : 1.0

	Name	Function (organization)	Date
Written by	Florent BACCI	Project owner assistance (ANTS)	29/01/2015

1. Document presentation

1.1 Versions

Version	Date	Author	History
1.0	29/01/2015	Florent BACCI	Document creation

1.2 Document objective

This document is a summary of the Certification Policy used by the Ministère de la Justice for its Public-Key Infrastructure.

1.3 Project summary

The Carte Justice project aims to provide strong authentication and trusted signature capabilities for public agents of the Ministère de la Justice, using X.509 certificates contained inside smartcards protected by PIN codes.

2. Organizational structure

2.1 Actors

The PKI is managed by mainly 3 actors:

- The Ministère de la Justice (MJ), which is the final client and user of the PKI. It holds authority on the PKI.
- The Agence Nationale des Titres Sécurisés (ANTS), which is the technical provider for the infrastructure supporting the PKI.
- The Imprimerie Nationale (IN), which is a subcontractor of the ANTS and is responsible for the physical production and delivery of the cards containing the certificates.

The final users of the certificates may belong to other organizations, but have always a strong relationship with the MJ.

2.2 Chain of trust

The Ministère de la Justice is the Certification Authority for the Justice PKI. It defines a chain of trust by designating public agents as registration authorities on different levels.

There are 4 levels in the chain: AE (Registration Authority), AEC (Central Registration Authority), AED (Delegated Registration Authority) and OC (Certification Agent). The top level is AE, which designates AEC for each branch of the ministry. Each AEC can then designate AED for each department under its supervision.

The AED are in direct contact with the final carriers of the certificates. They can designate others AED to help them in their task, or OC, which can assist their AED but do not have the authority to validate actions.

Each actor is given a perimeter to work on, and can only execute actions on people belonging to the perimeter.

3. Functional structuration

3.1 Identities management

The identities of all actors, including AE, AEC, AED, OC and final carriers are managed in a directory operated by the IT department of the ministry. All information about the actors is entered, checked and updated by the HR staff of their department. The profile and action perimeter of each actor is also set in this directory, following the chain of trust.

3.2 Cards and certificates lifecycle

The ASSCAP portal, managed by ANTS, allows authorized actors to request cards and / or certificates for a given carrier in their perimeter. It requires strong authentication. Only one card may be held at any time by a carrier. The card has a lifetime of 6 years, and contains two certificates, one for authentication and one for signature, each with a lifetime of 3 years. They are replaced by new certificates at the mid-life of the card.

3.3 Certificates delivery and activation

Carriers receive their card during a face to face meeting with their AED (or its OC). The AED performs an identity check of the carrier before handing the card. The card can only be activated using a PIN code mailed directly to the carrier. The carrier is required to configure PIN codes for the protection of each of his certificates.

For the certificates replacement at mid-life of the card, there is no face-to-face requirement. The carrier can directly update its card by authenticating himself with the previous certificates.

3.4 Revocation

A card and its certificates can be revoked at any time by either the carrier himself, using a password and secret questions, or by its AED. CRLs are published daily.

4. Technical structuration

4.1 Responsibilities

The technical responsibilities are separated between the following actors:

- Ministry's IT department : manage the directory, including identities, PKI rights and CRL publication
- ANTS: manage the certificate request portal, generating and revoking the certificates, managing the cards content and transmit physical orders.
- Imprimerie Nationale: produce, configure and send the smartcards, produce and send the activation PINs, according to the ANTS orders.

4.2 Certificates

All certificates are X.509 signed certificates. The root self-signed certificate of the CA is designated as "AC Justice" and has a lifetime of 12 years. It signs the effective CA certificates, designated as "AC Personnes n" (with n a number), which have a lifetime of 6 years each. All others certificates are signed by the "AC Personnes n" certificate, hosted in a Hardware Security Module. All certificates use 2048 bits keys and RSA + SHA2 algorithms.

5. Conformity

The PKI is audited and follows the French RGS *** PKI standard, and also follows the X.509 standard, RFC3647 and RFC5280