RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

**BACK TO BASICS**

# PUBLIC KEY INFRASTRUCTURE (PKI)

In twenty-one best practices, check out the French cybersecurity agency (ANSSI)'s essential resources for securing the implementation of a hierarchical public key infrastructure (PKI) to manage certificates for an entity's internal use.

## 1/ CONCEIVE

→ **Establish a Certificate Authority (CA) hierarchy tailored to the entity's needs:**

> create at least one root CA, and at least one intermediate CA for each root CA;

> dedicate each intermediate CA to issuing one or more certificate templates, organized by business or by use.

→ **Define, draw up, and comply with a Certificate Policy (CP) and a Certification Practice Statement (CPS)** - find the definitions in Appendix A2 of the French General Security Baseline (RGS, only available in French).

→ **Create certificate templates in line with the PKI's certification practices** (Web server authentication certificates, encryption certificates, code signing certificates, etc.). Strictly limit the fields of X.509 certificate extensions (Key Usage, Extended Key Usage, Authority Information Access, etc.) to the requirements of a given template.

→ **Ensure that certificates issued for a given user or process comply with the template(s) associated** with that user or process.

→ **Secure exchanges between the components of the PKI** (CA, registration authority, archiving entity, etc.) in terms of confidentiality, integrity, and authenticity.

→ **Secure exchanges between PKI components and end-users** in terms of confidentiality, integrity, and authenticity – particularly with regards to certificate request and issuance.

→ **Ensure key lifecycle management by:**

> generating private keys for certificates from a random number generator, in compliance with ANSSI's *Guide des mécanismes cryptographiques* (only available in French);

> generating private keys for algorithms, in compliance with the above-mentioned guide;

- RSA with a 4096-bit module or ECDSA with the P-384 curve, defined in FIPS 186-4 for a root CA;
- RSA with a 3072-bit module or ECDSA with the P-256 curve, defined in FIPS 186-4 for an intermediate CA or an end-entity certificate;

> defining a validity period for certificates, according to their sensitivity and exposure. For example: ten years for a root CA, a few years for an intermediate CA or a few months for an end-entity certificate.

> not reusing a private key for any purpose other than the one specified by the associated certificate.

**V1.0** (08/25)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

→ **Protect certificate private keys by:**

> storing root CA private keys off-line, ideally in secure element such as a secure hardware security module (HSM) ;

> storing intermediate CA private keys on-line in secure element such as a secure hardware security module (HSM) ;

> protecting end-entity certificate private keys with access control and, ideally, with encryption. Add hardware protection whenever the sensitivity level of the keys requires it.

→ **Retain an off-line escrow copy of the private keys of certificates dedicated to encryption.**

→ **Implement at least one certificate revocation management mechanism** (CRL and/or OCSP). Opt for two mechanisms to ensure redundancy.

→ **Anticipate the transition of the PKI to post-quantum cryptography** (investigate the implementation of hybrid certificates, performance impacts, etc.). Learn more : ANSSI's views on the Post-Quantum Cryptography transition.

## 2/ OPERATE

→ **Dedicate human resources to the operation, the maintenance in operational condition (MCO), and the maintenance in security condition (MCS) of the PKI according to pre-defined processes.**

→ **Verify the legitimacy of a certificate request.** In particular, check that the content of the request complies with the certificate policy, and that the applicant owns the private key associated with the public key contained in the certificate signing request (CSR).

→ **Configure certificate stores** (for browsers, products, etc.) **only with CAs that are strictly necessary.**

→ **Ensure that any equipment and software using certificates** (VPN concentrator, Web browser, document reading/signing tool, etc.) **verify the certification chain.** Each certificate within that chain must be verified. The elements to be taken into consideration include the certificate signature, the revocation status, and the validity period.

→ **Anticipate the renewal of certificates**, in particular the renewal of the root CA, for example as soon as the certificate reaches 2/3 of its lifetime. Regularly test certificate renewal processes.

→ **Renew the certificate's private key systematically when renewing a certificate.**

→ **Automate the generation, deployment, and renewal of certificates** through the secure implementation of dedicated protocols such as ACME. To find out more, see ANSSI's *Automatisation de la gestion des certificats avec ACME* (only available in French).

→ **Separate roles specific to the operation and administration of the PKI** (administrator, application manager, operator, etc.).

→ **Log and monitor events related to the PKI** (certificate issuance, HSM logs, CRLs, OCSP tokens, etc.).

→ **Carry out internal audits of the PKI, at a frequency that is adapted to the entity.** Consider calling on an external service provider to carry out these audits.