RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

INFRASTRUCTURE DE GESTION DE CLÉS (IGC)

Retrouvez, en une vingtaine de bonnes pratiques, les ressources essentielles de l'ANSSI pour la mise en œuvre sécurisée d'une infrastructure de gestion de clés (IGC) hiérarchique gérant les certificats à usage interne à une entité.

1/ CONCEVOIR

→ **Créer une hiérarchie d'autorités de certification (AC) adaptée au besoin de l'entité :**

> créer au minimum une AC racine, et au minimum une AC intermédiaire pour chaque AC racine ;

> dédier chaque AC intermédiaire à l'émission d'un ou plusieurs gabarit(s) de certificat, avec une répartition par métier ou par usage.

→ **Définir, rédiger et respecter une politique de certification (PC) et une déclaration des pratiques de certification (DPC).** Voir à ce sujet les définitions de l'annexe A2 du Référentiel général de sécurité (RGS).

→ **Définir des gabarits de certificats** conformes aux pratiques de certification de l'IGC (certificats d'authentification de serveur Web, certificats de chiffrement, certificats de signature de code, etc.). Limiter les champs des extensions de certificats X.509 (*Key Usage*, *Extended Key Usage*, *Authority Information Access*, etc.) aux stricts besoins d'un gabarit donné.

→ **S'assurer que les certificats émis pour un utilisateur ou un processus donné soient conformes au(x) gabarit(s) associé(s)** à cet utilisateur ou ce processus.

→ **Protéger les échanges entre les différentes composantes de l'IGC** (AC, autorité d'enregistrement, entité d'archivage, etc.) **en confidentialité, intégrité et authenticité.**

→ **Protéger les échanges entre les composantes de l'IGC et les entités finales en confidentialité, intégrité et authenticité,** en particulier les demandes et délivrances de certificats.

→ **Assurer une gestion du cycle de vie des clés :**

> générer les bi-clés des certificats à partir d'une source d'aléa conforme au Guide des mécanismes cryptographiques ;

> générer des bi-clés pour des algorithmes conformes au Guide des mécanismes cryptographiques ;

- RSA avec un module de 4096 bits ou ECDSA avec la courbe P-384 définie dans le FIPS 186-4 pour une AC racine ;
- RSA avec un module de 3072 bits ou ECDSA avec la courbe P-256 définie dans le FIPS 186-4 pour une AC intermédiaire ou un certificat d'entité finale ;

> définir une durée de validité des certificats en fonction de leur sensibilité et de leur exposition. Par exemple une dizaine d'années pour une AC racine, quelques années pour une AC intermédiaire ou quelques mois pour un certificat d'entité finale.

> ne pas réutiliser une bi-clé pour un autre usage que celui prévu par le certificat associé.

V1.0 (08/25)

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

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

→ **Protéger les clés privées des certificats :**

> stocker les clés privées des AC racine hors ligne, idéalement dans un équipement sécurisé de type HSM (*Hardware Security Module) ;*

> stocker les clés privées des AC intermédiaires en ligne dans un équipement sécurisé de type HSM ;

> protéger les clés privées des certificats d'entité finale par du contrôle d'accès et, idéalement, par du chiffrement. Ajouter une protection matérielle lorsque le niveau de sensibilité des clés le nécessite.

→ **Séquestrer hors ligne une copie des clés privées des certificats dédiés au chiffrement.**

→ **Mettre en œuvre au moins un mécanisme de gestion de la révocation des certificats (CRL et/ou OCSP).** Opter pour deux mécanismes afin d'assurer une redondance.

→ **Anticiper la migration de l'IGC vers la cryptographie post-quantique** (investiguer la mise en œuvre de l'hybridation sur les certificats, les impacts de performance, etc.). Voir à ce sujet l'Avis de l'ANSSI sur la migration vers la cryptographie post-quantique.

2/ EXPLOITER

→ **Dédier des ressources humaines à l'exploitation et au MCO/MCS de l'IGC selon des processus définis au préalable.**

→ **Vérifier la légitimité d'une demande de certificat.** En particulier, vérifier la conformité du contenu de la demande à la politique de certification et vérifier la possession, par le demandeur, de la clé privée associée à la clé publique contenue dans la demande de certificat.

→ **Configurer les magasins de certificats** (des navigateurs, des produits, etc.) **uniquement avec les AC strictement nécessaires.**

→ **S'assurer que les équipements et logiciels utilisant des certificats** (concentrateur VPN, navigateur Web, outil de lecture/signature de documents, etc.) **vérifient la chaîne de certification.** Chaque certificat de cette chaîne doit être vérifié. Les éléments à prendre en considération comprennent notamment la signature du certificat, le statut de révocation et la période de validité.

→ **Anticiper le renouvellement des certificats**, en particulier le renouvellement de l'AC racine, par exemple dès l'atteinte des 2/3 de la durée de vie du certificat. Tester régulièrement les processus de renouvellement des certificats.

→ **Renouveler systématiquement la bi-clé du certificat lors d'un renouvellement de certificat.**

→ **Automatiser la génération, le déploiement et le renouvellement des certificats** via la mise en œuvre sécurisée de protocoles dédiés comme ACME. Pour en savoir plus, consulter le guide « Les Fondamentaux » sur l'Automatisation de la gestion des certificats avec ACME.

→ **Distinguer des rôles propres à l'exploitation et à l'administration de l'IGC** (administrateur, responsable d'application, opérateur, etc.).

→ **Journaliser et surveiller les événements relatifs à l'IGC** (émission de certificats, journaux des HSM, CRL, jetons OCSP, etc.).

→ **Réaliser des audits internes de l'IGC** à une fréquence adaptée à l'entité. Envisager la réalisation d'audits par un prestataire externe.

Pour aller plus loin, consulter les annexes A du Référentiel général de sécurité.