Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
nationale

*Direction centrale de la sécurité
des systèmes d'information*

Paris, le 28 mars 2006

N° 724/SGDN/DCSSI/SDS/AsTeC

Gestion des clés cryptographiques

Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard

Version 1.0 du 13 mars 2006

Version	Modifications
Version 1.0 du 13 mars 2006	**Première version applicable.**
Version 0.11 du 28 juillet 2005	**Prise en compte des commentaires de la DGA et des remarques effectuées en séance lors de l'atelier DCSSI-Industriels du 7 juin 2005.**
Version 0.10 du 27 mai 2005	**Version présentée au cours de l'atelier DCSSI-Industriels du 7 juin 2005.**

Cellule d'Assistance Technique en
Conception de la DCSSI
SGDN/DCSSI/SDS/AsTeC
51 boulevard de La Tour-Maubourg,
75700 Paris 07 SP
AsTeC@sgdn.pm.gouv.fr

A. Table des matières

B. Introduction

B.1. Contexte

B.1.a. Objectif du document

La sécurité de la plupart des systèmes d'information repose pour partie sur l'utilisation de fonctions cryptographiques. Ces fonctions ont une sécurité de nature essentiellement mathématique qui repose sur des hypothèses importantes quant aux clés cryptographiques utilisées. Ces hypothèses peuvent être formalisées par des objectifs de sécurité qui doivent impérativement être respectés pour que les fonctions cryptographiques puissent remplir leur rôle.

Pour que les fonctions cryptographiques remplissent effectivement leur rôle, il est indispensable que leur gestion soit sûre au niveau du système d'information.

L'objectif de ce document est de présenter le cycle de vie d'une clé cryptographique et différentes architectures de gestion de clés possibles. Il vise aussi à aider à l'élaboration d'un système de gestion de clés.

B.1.b. Positionnement du document

Ce document complète le document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » édité par la DCSSI : il remplace notamment ses paragraphes « C.3.3 gestion de clés » et « F.3.3 gestion de clés », qui seront supprimés des éditions ultérieures.

Nous décrivons dans ce document des règles et des recommandations relatives à différents niveaux de robustesse cryptographique. Ces niveaux sont définis dans le paragraphe B.3 du document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques ».

- Note importante : la diffusion du présent document est calquée sur celle du document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » qui prévoit trois versions :
  - **La présente version, non classifiée, traite uniquement du premier niveau de robustesse, qualifié de « standard ». Ce document a pour vocation d'être largement diffusé, en particulier de manière électronique**.
  - Une deuxième version du document est également non classifiée mais n'est pas diffusée par voie électronique ; elle traite des deux premiers niveaux de robustesse, « standard » et « renforcé ».
  - Une troisième version traite de l'ensemble des trois niveaux de robustesse, niveau « élevé » compris.
- Les **règles** définissent des principes qui doivent *a priori* être suivis par tout mécanisme visant un niveau de robustesse donné. L'observation de ces règles est une condition généralement nécessaire, mais non suffisante, à la reconnaissance du niveau de robustesse visé par le mécanisme. Inversement, le fait de suivre l'ensemble des règles, qui sont par nature très génériques, ne garantit pas la robustesse ; seule une analyse spécifique permet de s'en assurer.
- En plus des règles, nous définissons également des recommandations. Elles ont pour but de guider dans le choix de certaines architectures de gestion de clés permettant un gain considérable en terme de sécurité. Il va de soi qu'en tant que recommandations, leur application peut être plus librement modulée en fonction d'autres impératifs tels que des contraintes de performance ou de coût.

Il importe de noter dès à présent que les règles et recommandations contenues dans ce document ne constituent pas un dogme imposé aux concepteurs de produits utilisant des mécanismes

cryptographiques. L'objectif est de contribuer à une amélioration constante de la qualité des produits de sécurité. A ce titre, le suivi des règles énoncées dans ce document doit être considéré comme une démarche saine permettant de se prémunir contre de nombreuses erreurs de conception ainsi que contre d'éventuelles faiblesses non décelées lors de l'évaluation des mécanismes cryptographiques.

Dans un souci de transparence, nous avons tenté de justifier chaque règle et recommandation contenues dans ce document. Le but est de convaincre que les choix ne sont pas faits de manière arbitraire mais au contraire en tenant compte le plus rigoureusement possible de l'état de l'art actuel en cryptographie ainsi que des contraintes pratiques liées à la mise en œuvre.

Le lecteur est invité à se référer également au document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » notamment pour les différentes limitations décrites qui s'appliquent aussi au présent document. Ainsi, il convient de rappeler que les notions, règles et recommandations contenues dans ce document s'adressent à un lecteur familier des concepts de gestion de clés.

B.1.c. Organisation du document

L'organisation de ce document est dans certains aspects similaire à celle du document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » :

- les concepts généraux relatifs à la gestion des clés cryptographiques sont présentés au paragraphe B.2 ;
- le cycle de vie d'une clé est défini au paragraphe B.3, ainsi que les différents types d'architectures fonctionnelles associées à la gestion des clés ;
- l'ensemble des règles et recommandations s'appliquant aux différentes étapes du cycle de vie sont ensuite regroupées dans le chapitre C, à partir de la page 15 ;
- les règles et recommandations sont repérées selon la codification suivante : les premières lettres (**Règle** ou *Recom*) indiquent si l'on à affaire à une règle ou une recommandation, l'indice suivant (S, R ou E) indique le niveau de robustesse standard, renforcé ou élevé correspondant, le domaine d'application est ensuite précisé et, finalement, un chiffre permet de distinguer les règles d'un même domaine d'application.

Ce document ne comporte volontairement aucun tableau récapitulatif. Les différentes règles et recommandations ne peuvent en effet être assimilées à une recette décrivant comment réaliser une architecture de gestion de clés, ce qui serait une grave source d'erreurs et de confusions.

B.1.d. Mise à jour du document

Comme pour le document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques », ce document a vocation à être révisé régulièrement pour tenir compte des évolutions constantes des menaces et des possibilités technologiques. La collecte de commentaires et la diffusion des révisions sont effectuées par la cellule d'assistance technique en conception de la DCSSI.

Adresse e-mail (non sécurisée) : `AsTeC@sgdn.pm.gouv.fr`

B.2. La gestion de clés cryptographiques

B.2.a. Définitions et concepts

L'objet de ce chapitre est de rappeler les définitions et concepts essentiels en matière de gestion de clés cryptographiques afin de bien comprendre les règles et recommandations émises dans ce document. Ces rappels couvrent le strict minimum. Ils sont bien évidemment sommaires et volontairement non mathématiques.

B.2.a.1. Clés secrètes symétriques

La gestion des clés peut être plus ou moins simple selon les applications. Dans le contexte de mécanismes symétriques, la principale difficulté réside dans la distribution, ou mise en accord, des clés afin de permettre aux correspondants de partager les mêmes secrets initiaux sans que des attaquants potentiels ne les aient interceptés. Ceci peut être réalisé au moyen de techniques asymétriques modernes mais peut également l'être via des méthodes non cryptographiques de nature organisationnelle.

Une durée de vie maximale, appelée crypto-période, est de plus en général associée à chaque clé. Une telle durée de vie peut être représentée par une date limite d'emploi ou par un compteur du nombre d'utilisations qui ne doit pas dépasser une certaine limite. Une telle limitation de la durée de vie des clés vise en général à réduire l'effet d'une éventuelle compromission des clés. Il est important de bien comprendre que dans un système cryptographiquement bien conçu il ne doit pas y avoir de phénomène « d'usure » des clés limitant leur durée d'utilisation.

Afin de protéger les clés lors de leur stockage, elles peuvent être elles-mêmes chiffrées avec une autre clé qui n'a généralement pas à être partagée. On désigne en général sous le terme de clé noire une clé ainsi chiffrée, par opposition aux clés rouges qui sont en clair. Dans l'acception courante, une clé noire est toutefois protégée avec un niveau de sécurité au moins identique à celui des données qu'elle protège. Or dans certains cas, la protection réalisée sur la clé n'atteint pas ce niveau cryptographique. Par exemple, si la clé est chiffrée à l'aide d'un mot de passe dont l'entropie est faible. On pourrait dans ce cas parler de clé camouflée pour distinguer ce type de cas de figure, même si cette terminologie n'est pas établie.

Notons enfin un cas particulier d'architecture, encore assez courant, utilisant un secret largement partagé entre un grand nombre d'utilisateurs. La divulgation de telles clés a en général des conséquences dramatiques en terme de sécurité, ce qui est contradictoire avec leur large diffusion. Dans certaines applications, l'usage exclusif de primitives symétriques rend nécessaire l'emploi de telles architectures ; ceci milite fortement en faveur d'une utilisation d'architectures asymétriques permettant de s'en passer.

A titre d'exemple, imaginons un groupe important de N individus souhaitant pouvoir s'authentifier mutuellement. En utilisant des techniques symétriques, on peut soit prévoir une clé secrète par paire d'individus, ce qui implique que chacun mémorise au moins $N-1$ clés, soit donner la même clé à tout le monde. Si l'on souhaite de plus pouvoir ajouter de nouveaux membres facilement, cette dernière solution devient la seule possible. Cependant, même si la clé est *a priori* protégée, sa large diffusion augmente le risque de compromission.

Une manière simple de résoudre ce problème avec une technique asymétrique est de faire choisir à chaque membre du groupe un bi-clé dont la partie publique est certifiée par une autorité. Chaque membre doit alors uniquement mémoriser son bi-clé et la clé publique de l'autorité.

B.2.a.2. Bi-clés asymétriques

La gestion des clés en cryptographie asymétrique est à la fois plus simple et plus complexe que dans le cas symétrique. Plus simple, mais également plus sûre, car il n'y a plus besoin de partager des secrets à plusieurs. Ainsi, la clé privée n'a besoin d'être connue que de son seul détenteur et certainement pas divulguée à d'autres. Par conséquent, il n'y a en théorie nul besoin de faire générer de telles clés par un tiers. On peut par exemple tout à fait concevoir qu'une clé privée soit générée par une carte à puce et qu'à aucun moment de la vie du système cette clé n'ait à quitter l'enceinte supposée sécurisée de la carte.

Le problème majeur qui se pose réside cependant dans la nécessité d'associer une clé publique à l'identité de son détenteur légitime. Une telle certification de clé publique peut être effectuée au moyen de la signature d'un certificat par une autorité qui certifie de ce fait que telle clé publique appartient bien à tel individu ou entité. Il se pose alors le problème de la vérification de cette signature qui va à son tour nécessiter la connaissance de la clé publique de l'autorité. Afin de certifier cette clé, on peut concevoir qu'une autorité supérieure génère un nouveau certificat, et ainsi de suite. On construit ainsi un chemin de confiance menant à une clé racine en laquelle il faut bien finir par avoir confiance. De telles constructions sont désignées sous le terme d'infrastructure de gestion de clés (IGC).

Notons enfin que dans de nombreuses applications pratiques, il est nécessaire de disposer d'une sorte de voie de secours permettant par exemple d'accéder à des données chiffrées sans être pour autant destinataire de ces informations. Les motivations de tels mécanismes de recouvrement peuvent être multiples mais il est important d'insister sur le fait qu'elles peuvent être parfaitement légales et légitimes. La méthode la plus simple est le séquestre de clé consistant à mettre sous scellé les clés privées ou secrètes tout en contrôlant les conditions d'accès à ces informations. Des travaux cryptographiques modernes proposent cependant de nombreuses autres solutions bien plus souples, sûres et efficaces.

B.2.b. Objectifs de sécurité minimaux

B.2.b.1. Définitions

B.2.b.1.1. Authenticité

Une clé cryptographique n'est qu'une valeur numérique. Le remplacement d'une clé par une autre peut permettre, s'il est possible, de contourner un mécanisme cryptographique. Les attaques dites « par le milieu » utilisent ce principe en usurpant l'identité du possesseur de la clé. Mais il peut aussi être très dangereux de pouvoir faire employer une clé par un algorithme cryptographique ou pour un usage pour lequel elle n'a pas été prévue.

Il est donc important que les clés utilisées soient non seulement intègres, c'est-à-dire non modifiées, mais encore correctement associées à une entité du système, un algorithme cryptographique et un usage. L'objectif de sécurité correspondant est appelé **authenticité** de la clé.

B.2.b.1.2. Clé secrète vs. privée

De façon systématique nous désignerons dans la suite par « clé secrète » une clé cryptographique utilisée dans un système symétrique, par « clé privée » la partie qui doit rester secrète d'un bi-clé asymétrique et par « clé publique » la partie qui est diffusée dans un système asymétrique.

B.2.b.1.3. Environnement de confiance

Nous appellerons par définition environnement de confiance l'environnement dans lequel est exploitée une clé d'un système cryptographique.

- La notion d'environnement de confiance que nous définissons est volontairement très générale. Une application cryptographique va forcément disposer au moins d'un environnement de confiance, de même que les différentes entités d'un système de gestion de clés. La forme physique de ces environnements peut être quelconque.
- Il est naturel d'imaginer que l'environnement de confiance est sécurisé. Toutefois, il peut exister des systèmes où l'environnement de confiance n'est pas sécurisé techniquement. Inversement, un équipement peut être sécurisé sans être de confiance. Le fait d'utiliser des clés cryptographiques implique obligatoirement que pour le niveau de sécurité visé, l'environnement d'utilisation est « suffisamment » de confiance, car cet environnement ayant accès aux clés cryptographiques peut les exploiter.
- Même si ne sont exploitées que des clés publiques, l'environnement qui les utilise doit être de confiance. En effet, si on prend l'exemple d'un outil de vérification de certificats de clés publiques, il ne va utiliser que des clés publiques permettant la vérification de la chaîne de certificats. Pour autant, il est indispensable pour la sécurité du système que cet outil de vérification soit de confiance et que le stockage des clés publiques qu'il utilise protège ces dernières en authenticité et en intégrité.
- Le document [IGI-501] « Recommandation pour l'intégration des fonctions cryptographiques dans les systèmes d'information » (version 1.0 n° 501/SGDN/DCSSI/DR du 20 septembre 2001) introduit dans son article 3 les objectifs de sécurité d'un « moyen de cryptologie ». Un tel moyen est dans le contexte du présent document un « environnement de confiance ». Dans l'article 4 - §1, il est ensuite proposé une méthode pour atteindre les objectifs de sécurité identifiés. Cette méthode consiste à distinguer un « domaine cryptographique » maîtrisé et autonome, du « domaine de confiance » dans lequel il est exploité. Par cette méthode, la sécurité du « domaine cryptographique » ne dépend pas de celle du « domaine de confiance ». L'architecture ainsi proposée permet donc de réduire l'environnement de confiance au seul « domaine cryptographique ». La notion d'environnement de confiance du présent document se veut donc générale et non liée à une architecture particulière de moyen cryptographique. Il n'en demeure pas moins que la définition précise d'un environnement de confiance et de ses interfaces avec les autres constituants du système d'information est, comme indiqué dans le document [IGI-501], de nature à faciliter la réalisation des objectifs de sécurité identifiés dans [IGI-501] et de satisfaire du même coup les exigences et recommandations du présent document.

B.2.b.1.4. Tiers de confiance

Nous appellerons par définition tiers de confiance toute entité qui effectue pour le compte d'utilisateurs finaux des opérations critiques pour la sécurité des clés.

- Cette définition inclut mais ne se limite pas à la notion de « tiers de confiance agréé » du décret n°98-102 du 24 février 1998 pris en application de l'article 28 de la loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications.
- Dans ce document, un tiers de confiance est typiquement une autorité de certification d'une IGC. La confiance dans cette autorité est en effet indispensable à la sécurité.

B.2.b.2. Cryptographie symétrique

La sécurité des systèmes de cryptographie symétriques repose sur la confidentialité, l'authenticité et l'intégrité d'une ou plusieurs clés secrètes partagées entre deux ou plusieurs entités. Toute atteinte à ces objectifs de sécurité est une atteinte directe à une ou plusieurs des fonctions de sécurité utilisant le système cryptographique.

B.2.b.3. Cryptographie asymétrique

La sécurité des systèmes de cryptographie asymétriques repose :

- sur la confidentialité, l'authenticité et l'intégrité d'une ou plusieurs clés privées et
- sur l'authenticité et l'intégrité des clés publiques utilisées.

Toute atteinte à ces objectifs de sécurité est une atteinte directe à une ou plusieurs des fonctions de sécurité utilisant le système cryptographique.

- Disons tout de suite que les objectifs d'authenticité et d'intégrité des clés publiques sont tout aussi importants et difficiles à réaliser que l'objectif de confidentialité d'une clé privée ou secrète.

B.2.b.4. Disponibilité

Outre ces objectifs liés à la nature cryptographique des mécanismes utilisés, le bon fonctionnement du système nécessite avant toute chose la disponibilité des clés.

Ce point peut s'avérer déterminant dans beaucoup d'aspects de la conception d'une architecture de gestion de clés.

B.3. Typologie des architectures de gestion de clés

B.3.a. Cycle de vie des clés cryptographiques

B.3.a.1. Demande de clé

Avant tout, une clé cryptographique n'est générée que suite à une demande, implicite ou explicite, qui permet d'identifier le début du cycle de vie d'une clé. Cette demande peut, dans certains cas, donner lieu à une formalisation utile au suivi de la clé dans son cycle de vie.

B.3.a.2. Génération

L'opération de génération de clés dépend des algorithmes cryptographiques utilisés. Dans tous les cas, une expertise cryptographique est indispensable à la validation de ce processus, crucial pour remplir les objectifs de sécurité énoncés ci-dessus. Les règles de l'état de l'art en matière de génération de clés pour un algorithme donné et de génération d'aléa ne sont toutefois pas l'objet de ce document.

B.3.a.2.1. Génération centralisée

La génération de clés peut être effectuée de façon centralisée. Dans ce cas, l'utilisateur final fait confiance à un tiers pour la génération de ses éléments secrets et privés.

Dans certains contextes, la génération de clés fait aussi apparaître la fabrication ou la personnalisation d'éléments matériels.

Dans la suite nous distinguerons deux cas :

- la génération centralisée de clé aléatoire consiste à utiliser un générateur d'aléa pour fabriquer selon un procédé cryptographique les clés secrètes ou privées ;
- la dérivation de clé à partir d'une clé maître consiste à utiliser un procédé cryptographique pour obtenir à partir d'une clé dite maître et d'éléments publics d'identification de l'utilisateur final une clé secrète ou privée.

B.3.a.2.2. Génération locale

La génération de clé peut aussi être effectuée de façon privative lorsque la génération intervient localement au niveau de l'utilisateur final.

- La génération peut être effectuée directement au sein de l'environnement de confiance. Il peut aussi y avoir injection de clé sous le contrôle de l'utilisateur local. Dans ce dernier cas, la génération de clé est supposée contrôlée par l'utilisateur local et sort du périmètre de ce document.

Dans la suite nous distinguerons trois cas :

- la génération locale de clé aléatoire consiste à utiliser localement un générateur d'aléa pour fabriquer selon un procédé cryptographique les clés secrètes ou privées ;
- la différentiation locale de clé consiste à utiliser un procédé cryptographique pour obtenir à partir d'une clé privée ou secrète locale et d'éléments de différenciation une autre clé secrète ou privée, généralement destinée à un usage différent ;
- l'échange de clé consiste, lors de l'ouverture d'une session entre deux ou plusieurs intervenants, à utiliser un protocole cryptographique dédié pour élaborer une clé secrète commune aux intervenants.

B.3.a.3. Affectation

Une fois une clé cryptographique générée, son admission dans le système d'information est une opération cruciale en terme de sécurité. C'est cette opération qui associe à une valeur numérique l'identité de l'utilisateur, de l'entité, du flux d'information, etc. auquel elle est affectée ainsi que l'usage qui lui est dévolu (signature, chiffrement, échange de clé, etc.). Cette opération existe que la cryptographie utilisée soit asymétrique ou non ; elle prend toutefois selon les systèmes des formes différentes. On peut définir cette opération comme celle qui fait passer une valeur numérique du statut de donnée brute au statut de clé cryptographique dans un système.

- Il ne faut pas confondre l'affectation avec l'injection d'une clé dans un équipement. Cette dernière opération est pour nous associée à l'étape d'introduction de la clé affectée dans le système applicatif (cf. §B.3.a.4).

L'opération d'affectation prend en outre un aspect encore plus crucial lorsqu'il s'agit de la première admission dans le système. Pour distinguer ce cas de figure, on parlera dans ce document du premier enrôlement d'un utilisateur ou d'un équipement dans un système. En effet, dans ce cas, la sécurité de l'opération ne peut résulter que de procédés non cryptographiques, de nature physique et organisationnels. C'est lors de ce premier enrôlement que seront affectés à l'utilisateur ou à l'équipement les premiers éléments cryptographiques permettant ultérieurement de le reconnaître de façon sûre et de lui affecter de nouvelles clés.

B.3.a.4. Introduction

Un autre aspect de la gestion d'une clé consiste à l'introduire physiquement ou logiquement dans l'ensemble du système applicatif une fois que son rôle a été correctement défini. Cet aspect recouvre la distribution et le transport de la clé jusqu'à l'utilisateur ou à l'équipement, puis son injection éventuelle dans l'environnement de confiance de l'utilisateur ou de l'équipement.

- L'introduction est l'opération qui fait passer la clé affectée du système de gestion de clés proprement dit au système applicatif qui va l'utiliser.

B.3.a.5. Utilisation

De par leur nature même, les éléments privés ou secrets ne peuvent être employés que dans un environnement de confiance. Cet environnement est en effet responsable du stockage des clés et de leur bonne gestion pendant la durée où elles sont utilisées. Il peut en découler notamment des exigences quant à la protection de l'environnement de confiance applicatif.

B.3.a.6. Fin de vie

La fin de vie d'une clé cryptographique donne lieu à une révocation, un retrait, voire une destruction. Ces opérations existent que la cryptographie utilisée soit asymétrique ou non.

- Révoquer une clé n'est pas synonyme de retrait en ce sens qu'une clé peut avoir été révoquée et continuer d'être utilisée pour des opérations de vérification ou de compatibilité ascendante. De même le retrait ne

signifie pas forcément que la clé ne sera plus jamais utilisée : elle peut être archivée pour permettre, par exemple, de mener une enquête postérieurement à son retrait.

B.3.a.7. Renouvellement

Le renouvellement d'une clé cryptographique est un processus à prévoir dès la conception d'un système d'information. Là encore cette opération existe que la cryptographie utilisée soit asymétrique ou non. Ce renouvellement peut intervenir de façon normale ou provoquée par des événements fortuits comme une compromission.

B.3.a.8. Recouvrement

Le recouvrement de clé est une opération qui peut avoir pour objectif d'assurer la disponibilité d'un service ou de répondre à des exigences légales. Ce type de fonctionnalité est d'autant plus difficile à mettre en œuvre que ses objectifs sont par nature contraires aux objectifs de sécurité visés par ailleurs. La définition précise de la fonctionnalité visée est indispensable de même qu'une expertise cryptographique globale.

- L'expertise cryptographique est indispensable car dans certains cas, un simple archivage des clés ne répond pas à l'objectif de recouvrement opérationnel du fait des propriétés des protocoles cryptographiques. Par exemple, dans un protocole d'échange de clé de type Diffie-Hellman aléatoire, l'ensemble des données échangées dans le protocole sont publiques et le secret utilisé lors de la session est à usage unique et n'est pas conservé au-delà de son temps d'utilisation. La connaissance de l'ensemble des échanges et des clés privées n'est d'aucune utilité pour retrouver le secret aléatoire choisi.

B.3.b. Architectures fonctionnelles des systèmes utilisateurs

B.3.b.1. Architecture répartie

Dans une architecture répartie, chaque utilisateur final est susceptible d'entrer en relation de façon cryptographiquement sécurisée avec tous les autres utilisateurs finaux du système d'information. Potentiellement, si le système comprend *N* utilisateurs, alors il existe *N(N-1)/2* flux d'information à protéger.

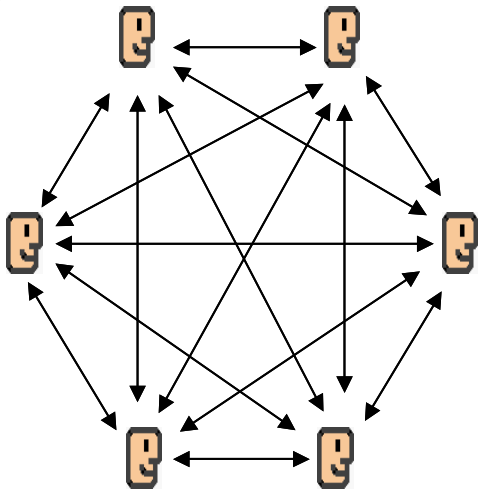

Figure 1 architecture fonctionnelle répartie

B.3.b.2. Architecture centralisée

Dans une architecture centralisée, les utilisateurs finaux sont susceptibles de n'entrer en relation qu'avec un ou plusieurs utilisateurs centraux identifiés. Si le système d'information comprend *n*

utilisateurs centraux et *N* utilisateurs, alors il existe *nN* flux d'information potentiels à protéger. En règle générale, *n* est très inférieur à *N*.

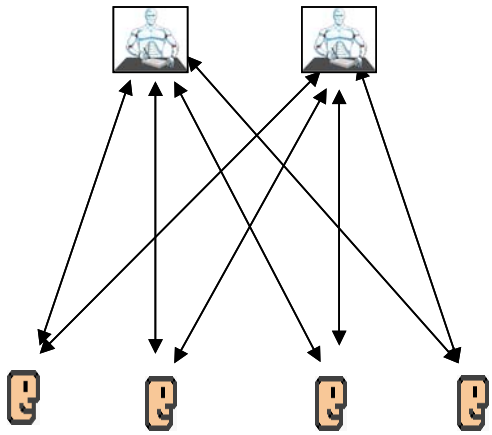

Figure 2 architecture fonctionnelle centralisée

B.3.c. Exemples illustratifs

B.3.c.1. Exemples d'architectures fonctionnelles

Un exemple typique d'architecture répartie est la messagerie sécurisée de bout en bout. Dans ce cas, chaque utilisateur du système peut envoyer un message à chacun des utilisateurs. Mais on observe ce même type d'architecture lorsque deux téléphones chiffrants ou deux chiffreurs IP sont amenés à communiquer.

Un exemple caractéristique d'architecture centralisée est la gestion de moyens de paiement. Dans ce cas, l'utilisateur final n'interagit qu'avec sa banque et n'a pas d'échanges directs avec un autre utilisateur final.

Bien entendu, les systèmes réels offrent souvent des situations intermédiaires entre ces deux architectures.

Il convient en outre de ne pas confondre ici une architecture fonctionnelle centralisée avec une génération de clés centralisée. En toute rigueur, ces deux problématiques sont indépendantes, même si dans la pratique, on utilisera souvent une génération de clés centralisée dans une architecture fonctionnelle centralisée. La réciproque n'est pas vraie. On trouve très souvent, notamment dans les infrastructures de gestion de clés, des générations de clés centralisées utilisées, par exemple, dans une messagerie typique des architectures fonctionnelles réparties.

B.3.c.2. Exemples de cycles de vie possibles

Les exemples ci-dessous se veulent purement illustratifs des notions définies ci-dessus. Ils ne présentent qu'une instanciation possible parmi la multitude des cycles de vie possibles dans chaque cas. Ils ne constituent en aucun cas une recommandation de réalisation.

B.3.c.2.1. Infrastructure de gestion de clés

Une infrastructure de gestion de clés offre principalement un service à une application cliente qui a besoin de clés cryptographiques pour fonctionner. En oubliant les clés propres aux services de l'IGC, le cycle de vie d'une clé d'utilisateur de l'application cliente pourrait être par exemple le suivant :

1. La demande de clé intervient auprès d'une autorité d'enregistrement.

2. La génération de la clé peut être locale, par exemple réalisée par un butineur ou une carte à puce.
3. Le premier enrôlement se fait auprès d'une autorité d'enregistrement.
4. Les affectations de clés ultérieures peuvent être effectuées en ligne.

Comme la génération est supposée locale dans notre exemple, l'introduction de la clé dans le système consiste uniquement en la certification de la clé.

5. Si l'application cliente est un contrôle d'accès, alors la clé est utilisée à chaque établissement d'une session sécurisée.
6. L'expiration du certificat, ou sa révocation à la demande de l'utilisateur ou sur compromission sont autant de cas de fin de vie de la clé.
7. La demande de renouvellement intervient à nouveau auprès de l'autorité d'enregistrement.
8. Enfin, le séquestre de clé peut être un service de recouvrement offert à l'utilisateur.

B.3.c.2.2. Système de paiement

Dans un système applicatif de paiement, le cycle de vie d'une clé du porteur de moyen de paiement peut être décrit par exemple comme suit :

1. La demande de clé se fait généralement sous la forme d'une demande de support électronique de paiement auprès de son guichet bancaire.
2. La génération de la clé intervient au moment de la personnalisation de la carte bancaire, de façon centralisée.
3. L'affectation de la clé intervient au même moment.
4. L'introduction de la clé dans le système se fait lors de la délivrance de la carte ou à l'aide d'un mécanisme d'activation téléphonique si l'organisme bancaire n'a pas de guichet.
5. L'utilisation de la clé est effective à chaque transaction financière.
6. La date de fin de validité de la carte ne constitue pas la fin de vie de la clé. Celle-ci peut ou non être reconduite dans la carte renouvelée. Par ailleurs, une carte volée est listée pour éviter sa possible utilisation frauduleuse, ce qui constitue un autre cas de fin de vie.
7. En cas de perte de carte, la clé est renouvelée lors du changement de carte.
8. Il n'y a pas à proprement parler de fonctionnalité de recouvrement.

B.3.c.2.3. Sécurité locale d'un poste de travail

Pour la sécurisation locale d'un poste de travail, le cycle de vie de la clé de sécurisation du poste peut par exemple être décrit succinctement de la façon suivante :

1. La demande de clé est effectuée par un administrateur qui souhaite donner des droits d'accès à un utilisateur.
2. La génération est locale au poste de travail et ne sert qu'à la protection de celui-ci.
3. L'affectation se fait localement en liaison avec la définition des droits d'accès du poste.
4. L'introduction de la clé intervient, par exemple, au moment du chiffrement du disque dur.
5. L'utilisation de la clé est permanente au cours de l'utilisation du poste de travail.
6. La fin de vie de la clé correspond à un reformatage ou à un transchiffrement du disque dur.

7. Lors du changement d'utilisateur, la clé de chiffrement est changée pour garantir que le nouvel utilisateur d'un matériel n'a pas accès aux données de son prédécesseur.
8. Il est enfin généralement fortement souhaitable que la clé de chiffrement du disque soit sauvegardée et accessible à un administrateur désigné pour pallier la perte de la clé utilisateur, mais la procédure d'accès à cette clé peut aussi être interdite à l'administrateur informatique et réservée à un rôle particulier.

C. Règles et recommandations

Dans toute la suite, nous cherchons à définir des règles et recommandations minimales pour des systèmes de gestion de clés de niveaux standard. Par raccourci, nous parlerons de clé de niveau standard lorsque ceci ne prêtera pas à confusion. Il est toutefois évident qu'une clé de niveau donné a vocation à être employée dans un système applicatif de même niveau.

C.1. Règles et recommandations générales

L'utilisation d'une clé cryptographique doit obligatoirement se faire dans un environnement de confiance. Que la clé soit publique, privée ou secrète, les objectifs de sécurité sur l'utilisation de celle-ci sont tels que toute atteinte à ces objectifs de sécurité remet en cause les fonctions de sécurité remplies par l'usage de la cryptographie. Ces objectifs ont été rappelés au paragraphe B.2.b.

L'impact d'une clé doit dans tous les cas être étudié. Il s'agit, pour un système donné, de mesurer l'impact de l'atteinte à l'un des objectifs de sécurité ci-dessus. Ceci ne doit pas se confondre avec l'analyse du risque de compromission. Il s'agit bien d'estimer, sous l'hypothèse que la compromission ou l'atteinte à l'intégrité de la clé a eu lieu, les conséquences pour le système cryptographique. C'est sur cette étude d'impact que l'analyse de risque peut ensuite s'appuyer pour estimer la robustesse du système.

- Dans beaucoup de systèmes cryptographiques, notamment ceux faisant intervenir des tiers de confiance, il existe une ou plusieurs clés dont la compromission ou l'atteinte à l'intégrité peut entraîner des atteintes aux objectifs de sécurité de tout ou d'une grande partie des acteurs du système. Il s'agit par exemple des clés maîtres d'un système de dérivation de clé, d'une clé de réseau ou de la clé privée d'une autorité de certification. Nous parlerons dans ce cas de clé présentant un risque d'impact systémique ou de façon plus concise de *clé à risque systémique*.

Niveau Standard

Règle$_s$Impact. Dans une architecture de gestion de clés de niveau standard l'impact de chaque clé du système doit être évalué.

Justification :

- L'expérience prouve qu'une étude systématique de l'impact de chaque clé apporte beaucoup pour l'amélioration de la robustesse du système.

Règle$_s$Durée. Dans une architecture de gestion de clés de niveau standard l'étude d'impact d'une clé doit prendre en compte les différentes durées associées à celle-ci.

Justification :

- Les différentes durées d'une clé ont une grande importance en terme d'analyse de risque :
  - Durée d'utilisation de la clé : c'est la période pendant laquelle la clé est active.
  - Crypto-période : c'est la durée au-delà de laquelle la clé est renouvelée.
  - Durée d'impact de la clé : c'est la période pendant laquelle une compromission de la clé a un impact sur le système.
  - Durée d'archivage : pour certaines clés, notamment de confidentialité, c'est la période durant laquelle la clé doit être archivée pour une utilisation ponctuelle ultérieure.

- Généralement la durée d'impact d'une clé est supérieure à sa durée d'utilisation, elle-même supérieure à sa crypto-période. L'estimation de ces différentes durées est l'un des éléments fondamentaux de l'étude d'impact.
- L'archivage des clés est dans un grand nombre de cas un besoin opérationnel, légal ou réglementaire. Les exigences quant à cet archivage dépendent fortement de l'étude d'impact.

Règle$_S$ImpactSystémique. Dans une architecture de gestion de clés de niveau standard les procédures de récupération du système en cas d'atteinte à la confidentialité à l'intégrité ou à l'authenticité d'une clé présentant un risque d'impact systémique doivent être étudiées et documentées.

Justification :

- Cette règle vise à sensibiliser les concepteurs au risque qu'il y aurait à faire reposer l'ensemble d'un système cryptographique sur une clé à risque systémique sans prévoir le cas où les objectifs de sécurité sur cette clé seraient remis en cause.
- Aucun dispositif purement technique n'est à même de protéger de façon satisfaisante une clé présentant un risque systémique.
- L'expérience prouve qu'une étude systématique de l'impact de chaque clé apporte beaucoup pour l'amélioration de la robustesse du système, notamment en identifiant justement les clés présentant un impact systémique.

Recom$_S$ImpactSystémique. Dans une architecture de gestion de clés de niveau standard il est recommandé d'éviter d'avoir recours à des clés présentant un risque systémique.

Justification :

- L'analyse d'impact peut conduire à proposer des solutions pour limiter l'impact de certaines clés ou organiser leur renouvellement de façon à éviter l'existence même de clés à risque systémique.
- Ceci n'est pas toujours possible : une clé racine dans une IGC par exemple présente toujours des risques systémiques.

C.2. Demande de clé

La demande de clé ne fait pas l'objet de règle ou de recommandation particulière. En effet, cette étape du cycle de vie est fortement tributaire du contexte opérationnel. On s'attachera toutefois à bien identifier cette étape et les procédures afférentes car c'est par leur correcte définition que pourront être satisfaites certaines des règles et des recommandations liées à l'affectation ultérieure des clés et relatives au contrôle de l'authenticité et de l'intégrité des clés.

C.3. Génération de clé

C.3.a. Génération locale de clé

C.3.a.1. Génération locale de clé aléatoire

Niveau Standard

Règle$_S$AléaLocal. La génération locale d'une clé cryptographique aléatoire de niveau standard doit faire appel à un générateur d'aléa de niveau standard.

Justification :

- La génération d'aléa utilisée pour générer des clés cryptographiques doit avoir un niveau de qualité cohérent avec le niveau de sécurité recherché. Les règles et recommandations sur la génération d'aléa feront l'objet d'un document séparé.

➢ Le document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » édité par la DCSSI contient d'ores et déjà un certain nombre de règles et de recommandations sur la génération d'aléa, notamment en matière de retraitement algorithmique.

C.3.a.2. Différentiation locale de clé

Niveau Standard

Règle$_s$Différentiation. La différentiation locale d'une clé cryptographique de niveau standard doit faire appel à un mécanisme cryptographique de niveau standard.

Justification :

- Le procédé cryptographique utilisé pour différencier localement une clé cryptographique doit avoir un niveau de qualité cohérent avec le niveau de sécurité recherché. Le document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » édité par la DCSSI contient d'ores et déjà un certain nombre de règles et de recommandations applicables.

C.3.a.3. Echange de clés

Niveau Standard

Règle$_s$EchangeClés. L'échange d'une clé cryptographique de niveau standard avec une entité homologue distante doit faire appel à un mécanisme cryptographique de niveau standard.

Justification :

- Le protocole cryptographique d'échange de clé utilisé doit avoir un niveau de qualité cohérent avec le niveau de sécurité recherché. Le document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » édité par la DCSSI contient d'ores et déjà un certain nombre de règles et de recommandations applicables.

C.3.b. Génération centralisée de clé

C.3.b.1. Génération centralisée de clé aléatoire

Niveau Standard

Règle$_s$AléaCentral. La génération centralisée d'une clé cryptographique aléatoire de niveau standard doit faire appel à un générateur d'aléa de niveau standard.

Justification :

- La génération d'aléa utilisée pour générer des clés cryptographiques doit avoir un niveau de qualité cohérent avec le niveau de sécurité recherché. Les règles et recommandations sur la génération d'aléa font l'objet d'un document séparé.

$Recom_s$AléaCentral. Il est recommandé que la génération centralisée d'une clé cryptographique aléatoire de niveau standard fasse appel à un générateur d'aléa de niveau renforcé.

Justification :

- Le caractère centralisé de cette opération rend celle-ci d'autant plus cruciale car une attaque sur le générateur d'aléa pourrait permettre de remonter à l'intégralité des clés générées. Il convient donc de chercher à élever le niveau d'exigence au niveau de la génération centralisée.

$Règle_s$GénérationCentralisée. La génération centralisée d'une clé cryptographique aléatoire de niveau standard doit intervenir dans un environnement de confiance de niveau standard.

Justification :

- La qualité intrinsèque du générateur d'aléa ne suffit pas à elle seule à garantir la sécurité de la génération. L'ensemble du dispositif technique et organisationnel qui intègre le générateur d'aléa doit être analysé.

$Recom_s$GénérationCentralisée. Il est recommandé que la génération centralisée d'une clé cryptographique aléatoire de niveau standard intervienne dans un environnement de confiance de niveau renforcé.

Justification :

- Si une vulnérabilité intervient au niveau de la génération centralisée des clés, c'est l'ensemble du système applicatif qui peut être compromis. Il est donc naturel d'attacher un soin plus grand aux règles de sécurité relatives à cette génération centralisée.

C.3.b.2. Dérivation de clés

Un mécanisme de dérivation de clé vise à remplacer un mécanisme de génération de clé purement aléatoire par un procédé déterministe dépendant de l'identité de l'utilisateur final.

Ce type de procédé peut présenter des avantages, notamment dans une architecture applicative centralisée utilisant des mécanismes cryptographiques symétriques. Il permet dans ce cas de réduire le besoin de stockage sécurisé des *n* utilisateurs centraux qui, pour s'adresser à leurs *N* utilisateurs rattachés, n'ont à mémoriser qu'un secret maître au lieu de *N* secrets individuels d'utilisateurs.

Il permet aussi de faciliter l'organisation d'un service de recouvrement de clés, ce qui peut constituer un besoin opérationnel et fonctionnel.

Par contre, la compromission d'une clé maître, qui permet à un attaquant potentiel de retrouver l'ensemble des clés dérivées à partir de cette clé, constitue un risque majeur pour ce type de procédé.

Niveau Standard

Règle$_s$Dérivation. La clé maître d'un mécanisme de dérivation de clé de niveau standard doit être exploitée dans un environnement de confiance de niveau minimal standard.

Recom$_s$Dérivation. Il est recommandé que la clé maître d'un mécanisme de dérivation de clé de niveau standard soit exploitée dans un environnement de confiance de niveau minimal renforcé.

Justification :

- Comme pour la génération de clé aléatoire centralisée les mécanismes de dérivation de clé présentent un risque systémique. La règle et la recommandation sont donc cohérentes avec celles de la génération centralisée de niveau standard.

Recom$_s$Dérivation. Les mécanismes de dérivation de clé ne devraient être utilisés que dans des architectures applicatives centralisées.

Justification :

- L'utilisation d'un mécanisme de dérivation de clés apporte un risque supplémentaire lié à sa cryptanalyse possible. Il est donc recommandé de n'utiliser ce type de mécanisme que si les objectifs de sécurité visés ne sont pas facilement atteignables par d'autres moyens. Dans le cas d'architectures applicatives réparties, il semble au contraire beaucoup plus aisé d'éviter le recours à des mécanismes de dérivation.

C.3.c. Génération de clé de signature

L'usage de signature implique le souhait d'assurer un objectif de non-répudiation directement au niveau cryptographique. Cet objectif est délicat à atteindre par des moyens purement techniques. On pourra donc avoir intérêt à viser un simple objectif d'authenticité et à le compléter par des mesures opérationnelles ou contractuelles.

Les règles et recommandations ci-dessous concernent la génération d'une clé destinée à un usage de signature. Elles complètent les règles et recommandations génériques proposées ci-dessus.

Niveau Standard

Recom$_s$DérivationSignature. Il est recommandé que la génération d'une clé de signature de niveau standard ne fasse pas intervenir de mécanisme de dérivation de clé.

Justification :

- La clé privée de signature doit être parfaitement maîtrisée par l'utilisateur pour que l'objectif de non répudiation puisse être atteint. L'utilisation d'un mécanisme de dérivation de clé est donc déconseillée puisque la connaissance de la clé maître permet d'usurper l'identité de tout utilisateur.

Recom$_s$GénérationAléatoireSignature-1. Il est recommandé que la génération d'une clé de signature aléatoire de niveau standard soit effectuée directement par l'utilisateur final dans son environnement de confiance.

Justification :

- Il est naturel que la génération d'une clé de signature soit locale. Toutefois, il peut être acceptable de générer cette clé de façon centralisée par un tiers de confiance.

$Recom_S$GénérationAléatoireSignature-2. Il est recommandé que la génération d'une clé de signature aléatoire de niveau standard fasse intervenir de l'aléa provenant d'une source maîtrisée par l'utilisateur final.

Justification :

- L'utilisation dans le processus de génération de l'aléa d'éléments fournis par l'utilisateur (mouvements de souris, frappes clavier, etc.) réduit les risques de possibilité de répudiation liés à une faiblesse éventuelle de la qualité de l'aléa utilisé.
- L'utilisation d'un dispositif technique évalué fournissant un aléa est envisageable. Toutefois, s'agissant d'une clé de signature, le fait d'y ajouter des éléments provenant de l'utilisateur contredit l'argument consistant à prétendre que le générateur d'aléa utilisé pourrait avoir reproduit la clé générée dans un autre contexte.

C.4. Affectation d'une clé

L'affectation d'une clé cryptographique dans un système applicatif est une opération qui est souvent mal comprise dans ses impacts en matière de sécurité. C'est cette opération qui occasionne le plus de problèmes notamment en terme d'initialisation. En effet, la problématique de premier enrôlement conduit souvent à un problème de « poule et d'œuf » : comment m'enrôler dans un système de façon sûre, alors que ce système ne me connaît pas.

L'affectation vise à garantir, pour les autres utilisateurs du système applicatif, que la clé générée est :

- d'une part bien définie dans son rôle à l'égard du système,
- d'autre part bien associée à l'identité de son utilisateur final, qu'il soit personne ou entité automatique du système.

L'opération varie notablement en fonction de l'existence ou non d'un tiers de confiance.

C.4.a. Usage d'une clé cryptographique

La cryptographie peut être employée pour réaliser beaucoup de fonctions de sécurité de natures différentes. Nous distinguerons dans ce document les usages de clés suivants :

- chiffrement : c'est l'usage le plus connu des algorithmes cryptographiques, visant à répondre à un objectif de confidentialité (par exemple AES en mode CBC) ;
- intégrité : c'est un usage spécifique de la cryptographie symétrique visant à garantir qu'un message n'a pas été modifié (par exemple CBC-MAC « retail ») ;
- authentification : c'est un usage visant à garantir l'identité d'une personne ou d'un équipement par un mécanisme cryptographique insensible au rejeu ;
- signature : c'est un usage spécifique de la cryptographie asymétrique visant à répondre à un triple objectif d'intégrité d'un message, d'authentification de son émetteur et garantissant la non-répudiation (par exemple ECDSA) ;
- transfert de clé : c'est un usage visant à transmettre de façon confidentielle une clé cryptographique utilisée dans un autre contexte, mais sans que l'authenticité soit

nécessaire (par exemple chiffrement CBC par une clé secrète de chiffrement de clé) ;

- échange de clé : c'est un usage visant à s'accorder de façon confidentielle sur une clé cryptographique utilisée dans un autre contexte, sans que l'authenticité soit nécessaire (par exemple Diffie-Hellman) ;
- dérivation de clé : c'est un usage visant à obtenir pour un ensemble d'utilisateurs, à partir d'une clé maître et d'un élément d'identité d'un utilisateur, une clé privée ou secrète spécifique de ce dernier ;
- différentiation locale de clé : c'est un usage visant à obtenir, à partir d'une clé privée ou secrète et d'éléments complémentaires, une ou plusieurs clés privées ou secrètes destinées à des usages différents ;
- source d'aléa : c'est l'usage consistant à introduire dans un générateur pseudo-aléatoire, une quantité d'information secrète aléatoire permettant de différencier ce générateur pour chaque équipement et de l'utiliser, bien qu'il reste purement déterministe, comme un générateur d'aléa.

L'usage d'une clé peut parfois être difficile à caractériser. Il nous semble toutefois, que l'on peut toujours se ramener aux cas ci-dessus. Il convient toutefois de ne pas confondre l'usage des clés et les services de sécurité qu'elles rendent.

- Par exemple, dans un défi Diffie-Hellman signé par une clé RSA le service rendu est un échange de clé authentifié. On peut toutefois distinguer l'élément d'aléa dont découle le challenge (qui est rarement désigné comme clé mais qui reste un élément secret) dont l'usage est de type « transfert de clé » et la clé RSA dont l'usage est de type « signature ».

Niveau Standard

Règle$_S$Usage. L'usage d'une clé de niveau standard doit être unique.

Justification :

- L'emploi d'une même clé à plus d'un usage, par exemple pour chiffrer avec un mécanisme de confidentialité et assurer l'intégrité avec un mécanisme différent, est source de nombreuses erreurs. Ceci n'interdit cependant pas de dériver deux clés à partir d'une même clé source à condition que le mécanisme de dérivation soit de niveau de robustesse cryptographique standard.
- L'emploi d'un même bi-clé à plus d'un usage, par exemple pour chiffrer et signer, est aussi une grave source d'erreurs.

C.4.b. Objectifs de sécurité de l'affectation

L'objectif intrinsèque à l'affectation d'une clé cryptographique à un utilisateur ou à un équipement est celui d'authenticité qui se décline en deux aspects :

- garantir à l'utilisateur ou à l'équipement l'authenticité de la clé qui lui est proposée et
- garantir pour le système, la possession effective de la clé par l'utilisateur ou l'équipement auquel elle est affectée.

Niveau Standard

Règle$_S$Affectation. Les mécanismes cryptographiques utilisés lors de l'affectation d'une clé cryptographique de niveau standard à un utilisateur ou à un équipement donné doivent être de niveau standard. Ces mécanismes doivent garantir la confidentialité, l'intégrité et l'authenticité de la clé.

Justification :

- Cette règle n'est applicable que pour les affectations postérieures au premier enrôlement effectué.
- Au cours du premier enrôlement, la (les) clé(s) affectées(s) lors de cette étape d'initialisation devra(ont) ensuite servir conformément à son (leurs) usage(s) identifié(s) pour garantir dans les affectations ultérieures de nouvelles clés les objectifs de sécurité requis.
- Il est naturel que les mécanismes cryptographiques utilisés soient d'un niveau de robustesse cohérent avec celui des clés qu'ils protègent.

Recom$_S$Affectation. Il est recommandé que les mécanismes cryptographiques utilisés lors de l'affectation d'une clé cryptographique de niveau standard à un utilisateur ou à un équipement donné garantissent la possession de la clé par l'utilisateur ou l'équipement auquel elle est affectée.

Justification :

- Au niveau standard, nous considérons que l'objectif de confidentialité sur la clé peut constituer un élément de preuve implicite de possession puisque seul l'utilisateur ou l'équipement destinataire est susceptible de disposer de la clé. Toutefois, il est préférable de disposer d'une preuve explicite de cette possession avant de considérer la clé comme affectée.
- Ne pas vérifier la possession de la clé lors de l'affectation présente des risques car dès que la clé est affectée, les autres entités du système peuvent commencer à l'utiliser. Il peut donc y avoir des atteintes à la disponibilité, par exemple si le message envoyé n'est pas déchiffrable par le destinataire. Il peut aussi y avoir des atteintes en confidentialité, par exemple si un attaquant empêche l'acheminement d'une nouvelle clé pour obliger un utilisateur ou un équipement à continuer d'utiliser une clé qu'il s'est procurée.

C.4.c. Objectifs sur le premier enrôlement

Nous considérons maintenant uniquement le premier enrôlement d'un utilisateur ou d'un équipement dans le système. Une fois cet enrôlement réalisé, nous considérons que les utilisateurs ou équipements finaux disposent des moyens cryptographiques permettant d'effectuer des affectations de clés ultérieures.

Les objectifs du premier enrôlement restent identiques et visent à garantir :

- l'authenticité de la clé proposée ;
- la possession de la clé par l'utilisateur.

Ces objectifs ne peuvent toutefois être remplis que par des mesures largement organisationnelles puisque les équipements en présence ne sont pas « à la clé ».

- Techniquement, ce premier enrôlement va donc, par exemple, consister en l'introduction d'une clé de base dans un équipement. Cette clé d'initialisation cryptographique servira ensuite à protéger les échanges liés à

l'affectation d'autres clés dans le système. C'est la raison pour laquelle le premier enrôlement revêt une importance cruciale, car c'est le seul qui ne peut pas reposer sur des moyens cryptographiques de protection et c'est pourtant celui sur lequel reposera dans beaucoup de cas la sécurité des affectations ultérieures.

- Mais il peut aussi ne pas y avoir d'affectation ultérieure : dans l'exemple de système de paiement du paragraphe B.3.c.2.2, la personnalisation est effectuée une fois pour la durée de vie de la carte et ce sont des mesures organisationnelles qui garantissent que c'est le bon usager qui reçoit sa carte et donc sa clé.
- Remarque : les règles et recommandations relatives à ce premier enrôlement dépendent du mode de génération de la clé affectée. Pour alléger la rédaction nous parlerons par exemple de « premier enrôlement d'une clé générée localement » pour désigner « l'affectation d'une clé générée localement lors du premier enrôlement de l'utilisateur ou de l'équipement auquel elle est affectée ».

C.4.c.1. Premier enrôlement d'une clé générée localement

C.4.c.1.1. Premier enrôlement d'une clé générée localement sans tiers de confiance

Niveau Standard

Règle$_s$EnrôlementPrivatif. Lors de son premier enrôlement, l'utilisateur final d'un système de niveau standard doit proposer à ses interlocuteurs un moyen de contrôler son identité, l'authenticité de la clé qu'il cherche à s'affecter et le fait qu'il possède bien cette clé.

Justification :

- Dans le cadre d'un premier enrôlement sans tiers de confiance, il est indispensable que les interlocuteurs échangent des moyens de contrôle de leurs identités respectives et de l'association de ces identités avec les clés échangées. Il est aussi nécessaire de s'assurer de la possession de la clé.

- À titre d'exemple, pour un premier enrôlement de clés de messagerie via l'internet, on peut imaginer utiliser le haché (souvent appelé empreinte) d'une clé publique et utiliser l'un des moyens suivants :
  - le publier sur son site personnel ;
  - l'envoyer par SMS (l'authentification découlant alors de la connaissance ou non du numéro de téléphone de l'appelant) ;
  - l'envoyer par courrier signé (l'authentification résultant de la signature manuscrite).
- La signature de la clé publique par la clé privée (auto-signature) ne constitue un élément de preuve de la possession de la clé que si la donnée signée dépend bien de l'interlocuteur. Dans le cas contraire, le rejeu est toujours possible.

Recom$_s$ControleIndépendant. Dans un système de niveau standard, il est recommandé que le moyen de contrôle proposé par l'utilisateur final lors de son premier enrôlement soit véhiculé de façon indépendante de sa clé.

Justification :

- Au niveau standard, nous ne souhaitons pas interdire l'enrôlement à distance dans un système.

- Sur l'exemple ci-dessus, des trois moyens proposés, seuls les deux derniers peuvent être considérés comme indépendants.

♦

C.4.c.1.2. Premier enrôlement d'une clé générée localement auprès d'un tiers de confiance

Il convient tout d'abord de noter que cette situation n'a de sens que dans le cas d'une infrastructure de gestion de clés (IGC), c'est-à-dire d'un système cryptographique asymétrique. En effet, dans un tel système la clé privée de l'utilisateur n'a pas besoin d'être communiquée au tiers de confiance et ne sort donc pas de l'environnement de confiance de l'utilisateur. Au contraire, pour un système symétrique, générer une clé de façon locale et l'affecter à un usage et une identité auprès d'un tiers de confiance va consister à l'acheminer vers ce dernier. On obtiendra au final une situation similaire à celle d'une génération de clé symétrique centralisée après acheminement de la clé vers son utilisateur final puisque les deux parties auront un secret partagé. Cette situation finale similaire aurait toutefois été obtenue de façon aberrante par une génération de la clé symétrique au niveau local.

L'utilisateur final qui a généré sa clé localement dans son environnement de confiance doit, préalablement à l'affectation de sa clé par le tiers de confiance, prouver à ce dernier :

- l'authenticité de la clé publique qu'il propose ;
- qu'il est bien en possession de la clé privée correspondante.

Pour cela, il est nécessaire que l'identité de l'utilisateur soit déjà connue du tiers de confiance.

Niveau Standard

Règle$_S$EnrôlementIGC. Dans un système avec tiers de confiance, pour assurer le premier enrôlement d'une clé de niveau standard générée localement, le tiers de confiance doit disposer d'un moyen de contrôler l'identité de l'utilisateur final, l'authenticité de sa clé et le fait qu'il possède bien cette clé. L'utilisateur final doit disposer de même d'un moyen de contrôler l'authenticité des éléments publics de l'IGC.

Justification :

- Cette règle est similaire à celle de l'enrôlement privatif. Toutefois, l'introduction d'un tiers de confiance rend la relation entre les deux parties dissymétrique au contraire de celle d'un enrôlement privatif où les deux parties sont des utilisateurs finaux.
- Un mécanisme de contrôle de l'identité annoncée par l'utilisateur doit être présent. Comme il s'agit du premier enrôlement, ce mécanisme est de nature non cryptographique. Par exemple, on peut utiliser un précédent enrôlement dans un autre système connu du tiers de confiance (numéro de téléphone, numéro GSM, etc.) pour acheminer l'empreinte de la clé affectée à un usage et une identité donnée. L'objectif de sécurité est là encore d'éviter les attaques par le milieu sur le processus d'enrôlement à distance.
- De même, l'utilisateur final doit être en mesure de contrôler l'authenticité du tiers de confiance. En l'occurrence, comme il s'agit d'une infrastructure de gestion de clés, il convient généralement d'être en mesure de contrôler par un moyen indépendant l'authenticité de la clé publique de l'autorité de certification racine. Ceci peut se faire, par exemple, par la publication de l'empreinte de cette clé par un moyen indépendant.

➢ Il est important notamment de ne pas reposer sur le seul mécanisme d'auto-signature du certificat de l'autorité racine. En effet, dans ce cas particulier, le fait que la clé soit auto-signée n'est pas une preuve d'authenticité mais un élément de preuve de possession de la clé privée. En effet, le certificat étant daté et signé, il n'est pas possible à un tiers de modifier la date du certificat ou les éléments de publication des listes de révocation sans invalider le certificat. Le mécanisme d'auto-signature est aussi important pour garantir l'intégrité de la donnée.

Recom$_s$ContrôleIndépendant. Il est recommandé que le premier enrôlement auprès d'un tiers de confiance d'un utilisateur final générant localement sa clé de niveau standard utilise un moyen d'acheminement indépendant du processus d'enregistrement pour tous les éléments de contrôle de l'identité de l'utilisateur, de l'authenticité de la clé et de celle des éléments publics de l'IGC.

Justification :

- Au niveau standard, nous ne souhaitons pas interdire l'enrôlement à distance dans un système qui ne disposerait pas de moyen d'acheminement indépendant pour les éléments de contrôle de l'identité de l'utilisateur et de l'authenticité de la clé.
- Il convient toutefois de noter que dans le cas d'un processus d'enrôlement automatisé auprès d'un tiers de confiance, l'application de cette recommandation est fortement recommandée dès le niveau standard pour contrer la menace d'attaque par le milieu.

C.4.c.2. Premier enrôlement d'une clé générée de façon centralisée

C.4.c.2.1. Premier enrôlement d'une clé générée de façon centralisée sans tiers de confiance

Cette situation n'a pas de sens car le centre de génération de clés est *de facto* un tiers de confiance.

C.4.c.2.2. Premier enrôlement d'une clé générée de façon centralisée avec tiers de confiance

Niveau Standard

Règle$_s$EnrôlementCentralSécuritéPhysique. Dans un système avec tiers de confiance, le premier enrôlement d'une clé de niveau standard générée de façon centralisée doit être réalisé dans un environnement de confiance et par un lien physique de confiance.

Justification :

- La problématique du premier enrôlement d'une clé générée de façon centralisée est aussi celle de son acheminement. En effet, comme il s'agit du premier enrôlement, l'utilisateur final ne dispose pas de moyens cryptographiques lui permettant de déchiffrer cette première clé qui doit lui être envoyée.
- Par voie de conséquence, l'environnement de confiance de l'utilisateur final doit être au plus près d'une entité de confiance contrôlée par le tiers de confiance. On peut penser par exemple aux autorités d'enregistrement d'une IGC ou à un centre de personnalisation. L'injection de l'élément secret doit se faire par un lien physique de confiance. On notera que ceci implique un enrôlement en vis-à-vis avec l'entité de confiance qui émane du tiers de confiance.
- Cette règle vise à assurer le même niveau de sécurité que lors d'une génération locale de clé. Rappelons qu'il s'agit ici de réaliser le premier enrôlement, c'est-à-dire de fournir à l'utilisateur final les premiers éléments cryptographiques qui vont asseoir ultérieurement toute la sécurité du système de gestion de clés. Il est donc naturel de prendre à ce moment et dès le niveau standard toutes les précautions nécessaires.

Règle$_s$EnrôlementCentral. Dans un système avec tiers de confiance, lors d'un premier enrôlement de niveau standard, le tiers de confiance doit disposer d'un moyen de contrôler l'identité de l'utilisateur final et l'utilisateur final doit avoir un moyen de vérifier l'authenticité de sa clé générée de façon centralisée par le tiers de confiance.

Justification :

- La sécurité physique de l'enrôlement ne diminue pas la nécessité de contrôle de l'identité de l'utilisateur et de l'authenticité de sa clé mais cette fois-ci c'est l'utilisateur final qui doit être en mesure de contrôler sa clé. Ce dernier point n'implique pas forcément des mesures techniques. En effet, la relation de confiance entre l'utilisateur final et son tiers de confiance, la procédure d'enrôlement en vis-à-vis, la mise à disposition d'un moyen cryptographique comme environnement de confiance sont autant de moyens pour l'utilisateur final de s'assurer de l'authenticité de son vis-à-vis.

C.4.c.2.3. Premier enrôlement d'une clé dérivée

Niveau Standard

Règle$_s$EnrôlementDérivationSécuritéPhysique. Le premier enrôlement d'une clé de niveau standard générée par un processus de dérivation à partir d'une clé maître doit être réalisé dans un environnement de confiance et par un lien physique de confiance.

Justification :

- La problématique du premier enrôlement d'une clé dérivée est la même que celle d'une clé générée de façon centralisée. En effet, l'objet de la dérivation de clé n'est pas d'introduire dans l'environnement de confiance de l'utilisateur la clé maître de la dérivation, mais bien sa clé dérivée.
- Comme il s'agit du premier enrôlement, l'utilisateur final ne dispose pas de moyens cryptographiques lui permettant de déchiffrer cette première clé. Cette dernière doit donc être introduite au plus près d'une entité de confiance contrôlée par le tiers de confiance, ce qui implique un enrôlement en vis-à-vis avec cette entité.
- Cette règle vise à assurer le même niveau de sécurité que lors d'une génération locale de clé. Rappelons qu'il s'agit ici de réaliser le premier enrôlement, c'est-à-dire de fournir à l'utilisateur final les premiers éléments cryptographiques qui vont asseoir ultérieurement toute la sécurité du système de gestion de clés. Il est donc naturel de prendre à ce moment et dès le niveau standard toutes les précautions nécessaires.

Règle$_s$EnrôlementDérivation. Lors d'un premier enrôlement de niveau standard, le tiers de confiance doit disposer d'un moyen de contrôler l'identité de l'utilisateur final et l'utilisateur final doit avoir un moyen de vérifier l'authenticité de sa clé générée par dérivation d'une clé maître contrôlée par le tiers de confiance.

Justification :

- La problématique du premier enrôlement d'une clé dérivée est la même que celle d'une clé générée de façon centralisée.

C.5. Introduction d'une clé

C.5.a. Acheminement de clé

La problématique d'acheminement d'une clé intervient par exemple lors d'une génération centralisée ou d'une génération par un procédé de dérivation à partir d'une clé maître.

- Note importante : Nous n'envisageons pas ici l'acheminement des éléments de premier enrôlement pour lesquels la protection ne peut s'appuyer sur des mécanismes cryptographiques. Cette opération de premier enrôlement a été envisagée au paragraphe .
- L'acheminement de clé peut aussi intervenir dans un processus de génération locale d'une clé secrète, par exemple au cours d'un processus d'échange de clé. Nous considérons dans ce cas, que le processus d'échange de clé est du niveau applicatif et ne fait pas partie de la gestion des clés. Il n'en demeure pas moins que les objectifs de sécurité sur ce mécanisme sont tout à fait similaires à ceux de l'acheminement d'une clé aléatoire générée de façon centralisée.

C.5.a.1. Acheminement de clé aléatoire générée de façon centralisée

Niveau Standard

Règle$_S$AcheminememententCléCentral. L'acheminement jusqu'à l'utilisateur final d'une clé cryptographique de niveau standard générée aléatoirement de façon centralisée doit bénéficier de moyens de protection de niveau standard. Ces moyens doivent garantir l'authenticité, l'intégrité et la confidentialité de la clé acheminée.

Justification :

- Lorsqu'une clé est générée de façon centralisée, il faut, une fois la clé générée, pouvoir l'acheminer de façon protégée jusqu'à l'utilisateur final. Ceci suppose, soit des moyens organisationnels, soit la présence dans le système d'un mécanisme spécifique ayant ses propres clés et mécanismes cryptographiques et destiné à protéger cet acheminement. Ce dernier doit avoir un niveau de sécurité cohérent avec celui recherché pour la clé.

Recom$_S$AcheminementNoirCentralBout-en-bout. Il est recommandé que l'acheminement jusqu'à l'utilisateur final d'une clé cryptographique de niveau standard générée aléatoirement de façon centralisée soit protégé cryptographiquement de bout en bout en authenticité, intégrité et confidentialité par des mécanismes de protection de niveau standard.

Justification :

- Il est recommandé dès le niveau standard que cet acheminement soit protégé de bout en bout, de façon cryptographique, c'est-à-dire que le système de génération de clé protège la clé générée de façon telle que seul le destinataire final, à l'exclusion de tout intermédiaire, puisse y avoir accès. On retrouve là le concept classique de clé noire de bout en bout. La clé cryptographique opérationnelle « rouge » ne devrait exister qu'au niveau de sa génération et de son utilisation.

- Cette recommandation ne s'applique pas, bien entendu, aux éléments de premier enrôlement pour lesquels la protection ne peut s'appuyer sur un mécanisme cryptographique.

C.5.a.2. Acheminement de clé générée par dérivation

Niveau Standard

Règle$_s$AcheminememententCléDérivée. L'acheminement jusqu'à l'utilisateur final d'une clé cryptographique de niveau standard générée par un procédé de dérivation à partir d'une clé maître doit bénéficier de moyens de protection de niveau standard. Ces moyens doivent garantir l'authenticité, l'intégrité et la confidentialité de la clé acheminée.

Recom$_s$AcheminementNoirDérivéeBout-en-bout. Il est recommandé que l'acheminement jusqu'à l'utilisateur final d'une clé cryptographique de niveau standard générée par un procédé de dérivation à partir d'une clé maître soit protégé cryptographiquement de bout en bout en authenticité, intégrité et confidentialité par des mécanismes de protection de niveau standard.

Justification :

- La problématique d'acheminement est la même que la clé soit générée aléatoirement de façon centralisée ou dérivée à partir d'une clé maître.

➢ Cette recommandation ne s'applique pas, bien entendu, aux éléments de premier enrôlement pour lesquels la protection ne peut s'appuyer sur un mécanisme cryptographique.

C.5.b. Injection de clé

C.5.b.1. Injection de clé générée localement

Il peut sembler curieux d'envisager l'injection d'une clé générée localement. Toutefois, dans certains cas, la génération d'une clé peut être effectuée par l'utilisateur dans un environnement de confiance distinct de l'environnement de confiance applicatif.

➢ Par exemple, un utilisateur averti pourrait employer un logiciel autonome pour générer sa clé privée de signature et vouloir ensuite l'injecter dans un logiciel de messagerie. Dans ce cas, la génération est locale mais l'environnement de confiance de l'utilisateur est scindé en deux parties relatives à la génération et à l'utilisation des clés.

Niveau Standard

Recom$_s$InjectionCléLocale. Il est recommandé que la génération locale d'une clé cryptographique de niveau standard ne donne pas lieu à un processus d'injection.

Justification :

- La génération locale de clé a pour principal objectif de donner une plus grande maîtrise à l'utilisateur final dans l'injection de ses clés. Toutefois, ceci ne doit pas se faire au prix des objectifs de sécurité premiers de protection des clés. Il semble difficile de séparer au niveau local l'environnement de confiance de l'utilisateur en deux.

Règle$_s$InjectionCléLocale. L'injection d'une clé cryptographique de niveau standard générée localement doit bénéficier de moyens de protection de niveau standard. Ces moyens doivent garantir l'authenticité, l'intégrité et la confidentialité de la clé injectée.

Justification :

- Comme nous ne souhaitons pas interdire au niveau standard de séparer la génération locale de l'utilisation des clés, il convient de prévoir les mesures techniques permettant de garantir le respect des objectifs de sécurité sur la clé générée.

➢ Les moyens requis peuvent être par exemple de prévoir la possibilité pour l'utilisateur de contrôler une empreinte cryptographique de la clé qu'il a introduite dans son environnement de confiance d'utilisation.

➢ En matière de confidentialité, la définition du périmètre exact de l'environnement de confiance peut notablement s'élargir si la génération locale est effectuée de façon indépendante de l'application utilisatrice.

C.5.b.2. Injection de clé générée de façon centralisée

C.5.b.2.1. Injection de clé aléatoire générée de façon centralisée

Niveau Standard

Règle$_s$InjectionCléCentral. L'injection dans l'environnement de confiance de l'utilisateur final d'une clé cryptographique de niveau standard générée aléatoirement de façon centralisée doit bénéficier de moyens de protection de niveau standard. Ces moyens doivent garantir l'authenticité, l'intégrité et la confidentialité de la clé injectée.

Justification :

- Cette règle est en cohérence avec celle liée à l'acheminement de cette même clé.
- Il s'agit ici d'attirer l'attention des concepteurs sur la sécurité de l'étape d'injection qui peut nécessiter d'être opérée par des mécanismes distincts de ceux utilisés lors de l'acheminement de la clé.

Recom$_s$InjectionCléCentral. Il est recommandé que l'injection dans l'environnement de confiance de l'utilisateur final d'une clé cryptographique de niveau standard générée aléatoirement de façon centralisée soit effectuée à partir d'une donnée protégée dès la génération en confidentialité, authenticité et intégrité par des mécanismes cryptographiques de niveau standard.

Justification :

- Il est recommandé dès le niveau standard que l'acheminement soit protégé de bout en bout de façon cryptographique. Cette recommandation est donc cohérente avec celle de l'acheminement.

➢ Cette recommandation ne s'applique pas, bien entendu, aux éléments de premier enrôlement pour lesquels la protection ne peut s'appuyer sur un mécanisme cryptographique.

C.5.b.2.2. Injection de clé générée par dérivation

Niveau Standard

Règle$_s$InjectionCléDérivée. L'injection dans l'environnement de confiance de l'utilisateur final d'une clé cryptographique de niveau standard générée par un processus de dérivation à partir d'une clé maître doit bénéficier de moyens de protection de niveau standard. Ces moyens doivent garantir l'authenticité, l'intégrité et la confidentialité de la clé injectée.

Recom$_s$InjectionCléDérivée. Il est recommandé que l'injection dans l'environnement de confiance de l'utilisateur final d'une clé cryptographique de niveau standard générée par un processus de dérivation à partir d'une clé maître soit effectuée à partir d'une donnée protégée dès la génération en confidentialité, authenticité et intégrité par des mécanismes cryptographiques de niveau standard.

Justification :

- La problématique d'acheminement est la même que la clé soit générée aléatoirement de façon centralisée ou dérivée à partir d'une clé maître.

➢ Cette recommandation ne s'applique pas, bien entendu, aux éléments de premier enrôlement pour lesquels la protection ne peut s'appuyer sur un mécanisme cryptographique.

C.6. Utilisation d'une clé

C.6.a. Diffusion d'une clé

La diffusion d'une clé dans un système est le nombre d'environnements de confiance qui sont susceptibles d'y accéder en clair. La diffusion augmente le risque de compromission d'une clé. La diffusion minimale d'une clé est :

- pour une clé privée limitée à un seul environnement de confiance ;
- pour une clé secrète limitée à deux environnements de confiance.

➢ Il existe d'un point de vue théorique des moyens de partager un secret entre plusieurs entités de telle façon que des calculs puissent être effectués à partir de ce secret sans le révéler. Ces méthodes mathématiques peuvent être utilisées mais ne sont pas envisagées ici. Elles vont plus loin que le simple partage de secret, qui permet, à partir de parts de secret distinctes, de reconstituer un secret dans un environnement de confiance et de l'utiliser.

Niveau Standard

Recom$_s$Diffusion. Il est recommandé que la diffusion d'une clé privée ou secrète de niveau standard soit limitée aux seuls environnements de confiance qui l'utilisent vraiment.

Justification :

- La limitation de la diffusion d'une clé est un moyen simple de réduire le risque de compromission.
- Toutefois, pour des systèmes de niveau standard, l'objectif de confidentialité sur la clé peut être assuré par des moyens techniques ou physiques. L'analyse de risque peut dans ce cas aboutir à la conclusion que le risque de compromission est acceptable, même si la diffusion de la clé est large. Il n'est donc pas nécessaire, au niveau standard, d'édicter en règle cette recommandation.
- Ceci est en cohérence avec la recommandation d'acheminement protégé en confidentialité de bout en bout.

C.6.b. Utilisation applicative d'une clé

Niveau Standard

Règle$_s$EnvironnementConfiance. L'utilisation d'une clé cryptographique dans un système applicatif de niveau standard doit obligatoirement se faire dans un environnement de confiance ayant un niveau de sécurité au minimum standard.

Justification :

- Que la clé soit publique, privée ou secrète, les objectifs de sécurité sur l'utilisation de celle-ci sont tels que toute atteinte à ces objectifs de sécurité remet en cause les fonctions de sécurité qui nécessitent l'emploi de la cryptographie.

Règle$_s$VérificationAuthenticité. Avant toute utilisation d'une clé dans un système applicatif de niveau standard, son authenticité doit être vérifiée par un mécanisme de sécurité de niveau minimum standard.

Justification :

- La vérification d'authenticité avant utilisation est une mesure simple qui bloque un grand nombre de chemins d'attaque cryptographique.
- Il convient de noter que cette vérification n'est pas forcément de nature cryptographique ; elle peut découler du processus d'enrôlement ou s'appuyer sur l'environnement de confiance.

Règle$_s$VérificationUtilisabilité. Avant toute utilisation d'une clé dans un système applicatif de niveau standard, il doit être vérifié par un mécanisme de sécurité de niveau minimum standard que la clé est toujours utilisable.

Justification :

- La fin de vie d'une clé est une opération qui doit être prévue par une architecture de gestion de clés pour gérer, notamment, les cas de compromissions.
- Pour être efficace, il convient que les informations de retrait ou de révocation soient exploitées.

C.7. Fin de vie d'une clé

Niveau Standard

Règle$_s$FinUtilisation. Une architecture de gestion de clés de niveau standard doit prévoir la fin de vie de l'ensemble des clés qu'elle gère ou utilise.

Justification :

- La fin de vie d'une clé, le dés-enrôlement d'un utilisateur ou la compromission d'une clé sont, par exemple, des événements tout à fait prévisibles qui doivent donner lieu à une procédure de révocation.
- Ces événements doivent être étudiés pour toutes les clés, y compris les éventuelles clés maîtres, clés racines, etc. dont la fin de vie a des impacts sur le système différents de la fin de vie d'une clé utilisateur.

Recom$_s$CauseFinUtilisation. Il est recommandé qu'une architecture de gestion de clés de niveau standard traite les différentes causes de fin de vie d'une clé de façon distincte.

Justification :

- Les procédures de révocation de clé prévues pour gérer une cryptopériode peuvent s'avérer non adaptées si la cause de la révocation est une compromission. Il convient donc de bien identifier les causes de révocation et de s'assurer que les procédures de révocation et éventuellement de renouvellement des clés sont adaptées à chaque cas de figure.
- Au niveau standard, les cas qui ne sont pas nominaux comme la compromission d'une clé peuvent être traités par des mesures non techniques.

Règle$_s$Effacement. Une clé de niveau standard dont la durée d'utilisation est dépassée doit être effacée des environnements de confiance où elle était utilisée par un moyen technique de niveau de sécurité standard.

Justification :

- Si la durée d'utilisation de la clé est dépassée, alors, hormis un éventuel archivage, aucun environnement de confiance de l'architecture de gestion de clés n'a besoin de conserver cette clé.
- Les règles et recommandations sur le procédé d'effacement feront l'objet d'un document séparé.

C.8. Renouvellement d'une clé

Niveau Standard

Règle$_s$Renouvellement. Une architecture de gestion de clés de niveau standard doit prévoir le renouvellement de l'ensemble des clés qu'elle gère ou utilise.

Justification :

- Au même titre que la fin de vie, le renouvellement de chaque clé du système doit être étudié.
- L'étude des procédures de renouvellement d'une clé permet d'affiner l'étude d'impact de chaque clé, notamment en identifiant celles qui présentent un risque systémique du fait de leur diffusion et/ou de la difficulté de leur renouvellement.

Règle$_s$RenouvellementEnrôlement. Une architecture de gestion de clés de niveau standard doit assurer que le renouvellement d'une clé ne puisse se faire qu'après vérification de l'authenticité de la nouvelle clé et de la possession de celle-ci par l'utilisateur. Les mécanismes utilisés pour cette vérification doivent être de niveau standard.

Justification :

- Cette règle est en cohérence avec celles relatives à l'enrôlement.

C.9. Recouvrement d'une clé

Niveau Standard

Règle$_s$Recouvrement. Une architecture de gestion de clés de niveau standard qui prévoit des fonctions de recouvrement de clés doit mettre en place des contrôles d'accès à cette fonctionnalité de niveau renforcé.

Justification :

- Le contrôle de la fonction de recouvrement est primordial pour éviter toute atteinte intempestive aux objectifs de sécurité principaux d'une architecture de gestion de clés.

Index des concepts