RÈGLES ET RECOMMANDATIONS CONCERNANT LA GESTION DES CLÉS CRYPTOGRAPHIQUES UTILISÉES DANS L'ENSEMBLE DES MÉCANISMES CRYPTOGRAPHIQUES

Annexe à l'Arrêté Ministériel n° 2018-637
du 2 juillet 2018

ANNEXE AU « JOURNAL DE MONACO » N° 8.390

DU 13 JUILLET 2018

TABLE DES MATIÈRES

1 Introduction

1.1. Contexte

1.1.1. Objectif de l'annexe

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 les caractéristiques des 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 la présente annexe 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.

1.1.2. Positionnement de l'annexe

La présente annexe vient en complément de l'annexe à l'arrêté ministériel n° 2018-635 du 2 juillet 2018 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée définissant le choix et le dimensionnement des mécanismes cryptographiques et concerne.

Elle définit les règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques.

1.1.3. Définition des règles et recommandations

Les **règles** définissent des principes qui doivent être suivis par tout mécanisme. L'observation de ces règles est une condition nécessaire à la sécurité du mécanisme. Cependant, le fait de suivre l'ensemble des règles, qui sont par nature très génériques, n'est pas suffisant pour garantir la robustesse du mécanisme cryptographique ; seule une analyse spécifique permet de s'en assurer.

À côté des règles, la présente annexe définit également des **recommandations**. Elles ont pour but de guider le choix de certaines architectures de gestion de clés permettant un gain considérable en termes de sécurité, pour un coût souvent modique. 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 est également nécessaire de se référer à l'annexe de l'arrêté ministériel n° 2018-635 du 2 juillet 2018, précité, définissant les « Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques », pour les différentes limitations décrites qui s'appliquent aussi à la présente annexe. Ainsi, il convient de rappeler que les notions, règles et recommandations contenues dans la présente annexe s'adressent à un lecteur familier des concepts de gestion de clés.

Les règles et recommandations sont repérées selon la codification suivante : les premières lettres (Règle ou Recom) indiquent si l'on a affaire à une règle ou une recommandation, le domaine d'application est ensuite précisé et, finalement, un chiffre permet de distinguer les règles d'un même domaine d'application.

1.1.4 Mise à jour de l'annexe

La mise à jour de la présente annexe est réalisée par l'Agence Monégasque de Sécurité Numérique en fonction des évolutions techniques, législatives et règlementaires en matière de sécurité des systèmes d'information. Ladite mise à jour est publiée par arrêté ministériel, lequel précise les modalités de transition et date d'effet.

1.2 La gestion de clés cryptographiques

1.2.1 Définitions et concepts

L'objet de ce point 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 la présente annexe.

1.2.1.1 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 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.

Enfin, il est à noter que dans 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 termes de sécurité. 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.

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

1.2.1.2 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 en aucun cas 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.

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 ou PKI en anglais).

De fait, 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 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.

1.2.2 Objectifs de sécurité minimaux

1.2.2.1 Définitions

« 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.

« Clé secrète versus. Privée » :

- une « *clé secrète* » désigne une clé cryptographique utilisée dans un système symétrique ;
- une « *clé privée* » désigne la partie qui doit rester secrète d'une bi-clé asymétrique ;
- une « *clé publique* » désigne la partie qui est diffusée dans un système asymétrique.

« Environnement de confiance » :

- désigne l'environnement dans lequel est exploitée une clé d'un système cryptographique.
- La notion d'environnement de confiance définie ici 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.

« Tiers de confiance » désigne toute entité qui effectue pour le compte d'utilisateurs finaux des opérations critiques pour la sécurité des clés. Dans la présente annexe, 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.

1.2.2.2 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.

1.2.2.3 Cryptographie asymétrique

La sécurité des systèmes de cryptographie asymétriques repose :

- sur la confidentialité, l'authenticité et l'intégrité d'une ou plusieurs clés privées ;

- 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.

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.

1.2.2.4 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.

1.3 Typologie des architectures de gestion de clés

1.3.1 Cycle de vie des clés cryptographiques

1.3.1.1 Demande de clé

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.

1.3.1.2 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 la présente annexe.

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 deux cas seront distingués :

- 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.

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 la présente annexe.

Dans la suite trois cas seront distingués :

- 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.

1.3.1.3 Affectation

Une fois une clé cryptographique générée, son admission dans le système d'information est une opération cruciale en termes 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), 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 associée dans la présente annexe à l'étape d'introduction de la clé affectée dans le système applicatif (cf. point 1.3.1.4).

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 la présente annexe 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.

1.3.1.4 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.

1.3.1.5 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.

1.3.1.6 Fin de vie

La fin de vie d'une clé cryptographique donne lieu à une révocation, un retrait, voire une destruction, 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 ou de déchiffrer un document postérieurement à son retrait.

1.3.1.7 Renouvellement

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

1.3.1.8 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.

1.3.2 Architectures fonctionnelles des systèmes utilisateurs

1.3.2.1 Architecture répartie

Dans une architecture répartie (voir figure 1), 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.

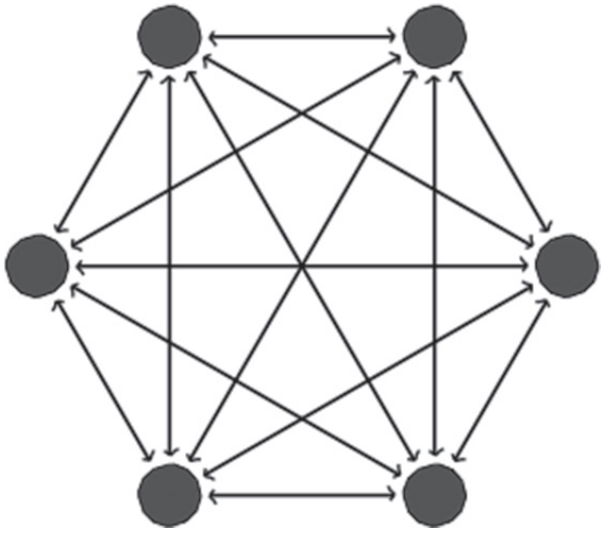

Figure 1 - Architecture fonctionnelle répartie

1.3.2.2 Architecture centralisée

Dans une architecture centralisée (voir figure 2), 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*.

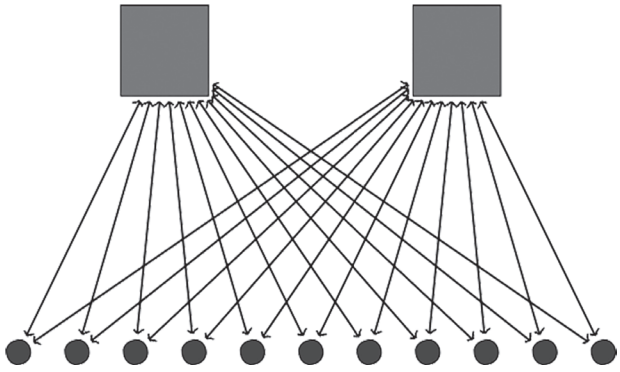

Figure 2 - Architecture fonctionnelle centralisée

2 Règles et recommandations

Dans toute la suite, des règles et recommandations minimales sont définies pour des systèmes de gestion de clés. Par raccourci, le terme de clé conforme au référentiel sera employé lorsque ceci ne prêtera pas à confusion.

2.1 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 point 1.2.2.

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 eue 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. Une telle clé sera qualifiée de clé présentant un risque d'impact systémique ou de façon plus concise de clé *à risque systémique*.

RègleImpact-1. Dans une architecture de gestion de clés l'impact de chaque clé du système doit être évalué.

RègleDurée-1. Dans une architecture de gestion de clés l'étude d'impact d'une clé doit prendre en compte les différentes durées associées à celle-ci.

RègleImpactSystémique-1. Dans une architecture de gestion de clés 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.

RecomImpactSystémique-1. Dans une architecture de gestion de clés il est recommandé d'éviter d'avoir recours à des clés présentant un risque systémique.

2.2 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.

2.3 Génération de clé

2.3.1 Génération locale de clé

2.3.1.1 Génération locale de clé aléatoire

RègleAléaLocal-1. La génération locale d'une clé cryptographique aléatoire doit faire appel à un générateur d'aléa conforme au référentiel.

2.3.1.2 Différentiation locale de clé

RègleDifférentiation-1. La différentiation locale d'une clé cryptographique doit faire appel à un mécanisme cryptographique conforme au référentiel.

2.3.1.3 Échange de clés

RègleÉchangeClés-1. L'échange d'une clé cryptographique avec une entité homologue distante doit faire appel à un mécanisme cryptographique conforme au référentiel.

2.3.2 Génération centralisée de clé

2.3.2.1 Génération centralisée de clé aléatoire

RègleAléaCentral-1. La génération centralisée d'une clé cryptographique aléatoire doit faire appel à un générateur d'aléa conforme au référentiel.

RecomAléaCentral-1. Il est recommandé que la génération centralisée d'une clé cryptographique aléatoire fasse appel à un générateur d'aléa conforme au référentiel et respectant de plus l'ensemble des recommandations associées.

RègleGénérationCentralisée-1. La génération centralisée d'une clé cryptographique aléatoire doit intervenir dans un environnement de confiance conforme au référentiel.

RecomGénérationCentralisée-1. Il est recommandé que la génération centralisée d'une clé cryptographique aléatoire intervienne dans un environnement de confiance conforme au référentiel et respectant de plus l'ensemble des recommandations associées.

2.3.2.2 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.

RègleDérivation-1. La clé Maître d'un mécanisme de dérivation de clé doit être exploitée dans un environnement de confiance conforme au référentiel.

RecomDérivation-1. Il est recommandé que la clé maître d'un mécanisme de dérivation de clé soit exploitée dans un environnement de confiance conforme au référentiel et respectant de plus l'ensemble des recommandations associées.

RecomDérivation-2. Les mécanismes de dérivation de clé ne devraient être utilisés que dans des architectures applicatives centralisées.

2.3.3 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.

RègleDérivationSignature-1. La génération d'une clé de signature ne doit pas faire intervenir de mécanisme de dérivation de clé.

RecomGénérationAléatoireSignature-1. Il est recommandé que la génération d'une clé de signature aléatoire soit effectuée directement par l'utilisateur final dans son environnement de confiance.

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

2.4 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 termes 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.

2.4.1 Usage d'une clé cryptographique

La cryptographie peut être employée pour réaliser beaucoup de fonctions de sécurité de natures différentes. Dans la présente annexe les usages de clés suivants seront distingués :

- 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 surchiffré) ;
- 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 et ECKCDSA) ;
- 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 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*.

RègleUsage-1. L'usage d'une clé doit être unique (sauf exception dument justifiée).

2.4.2 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 ;
- garantir pour le système, la possession effective de la clé par l'utilisateur ou l'équipement auquel elle est affectée.

RègleAffectation-1. Les mécanismes cryptographiques utilisés lors de l'affectation d'une clé cryptographique à un utilisateur ou à un équipement donné doivent être conformes au référentiel. Ces mécanismes doivent garantir la confidentialité, l'intégrité et l'authenticité de la clé.

RecomAffectation-1. Il est recommandé que les mécanismes cryptographiques utilisés lors de l'affectation d'une clé cryptographique à un utilisateur ou à un équipement donné garantissent la possession de la clé par l'utilisateur ou l'équipement auquel elle est affectée.

2.4.3 Objectifs sur le premier enrôlement

Seul le premier enrôlement d'un utilisateur ou d'un équipement dans le système est maintenant considéré. Une fois cet enrôlement réalisé, il est considéré 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 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.

Remarque :

Les règles et recommandations relatives à ce premier enrôlement dépendent du mode de génération de la clé affectée. Il sera question 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.

2.4.3.1 Premier enrôlement d'une clé générée localement

Premier enrôlement d'une clé générée localement sans tiers de confiance

RègleEnrôlementPrivatif-1. Lors de son premier enrôlement, l'utilisateur final d'un système 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.

Remarques :

Pour un premier enrôlement de clés de messagerie via l'internet, on peut utiliser le hache (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.

RecomContrôleIndépendant-1. Dans un système, 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.

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.

RègleEnrôlementIGC-1. Dans un système avec tiers de confiance, pour assurer le premier enrôlement d'une clé 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.

RecomContrôleIndépendant-1. Il est recommandé que le premier enrôlement auprès d'un tiers de confiance d'un utilisateur final générant localement sa clé 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.

2.4.3.2 Premier enrôlement d'une clé générée de façon centralisée

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.

Premier enrôlement d'une clé générée de façon centralisée avec tiers de confiance

RègleEnrôlementCentralSécuritéPhysique-1. Dans un système avec tiers de confiance, le premier enrôlement d'une clé générée de façon centralisée doit être réalisé dans un environnement de confiance et par un lien physique de confiance.

RègleEnrôlementCentral-1. Dans un système avec tiers de confiance, lors d'un premier enrôle- ment, 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.

Premier enrôlement d'une clé dérivée

RègleEnrôlementDérivationSécuritéPhysique-1. Le premier enrôlement d'une clé 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.

RègleEnrôlementDérivation-1. Lors d'un premier enrôlement, 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.

2.5 Introduction d'une clé

2.5.1 Acheminement de clé

Le problème 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.

L'acheminement des éléments de premier enrôlement, pour lesquels la protection ne peut s'appuyer sur des mécanismes cryptographiques, n'est pas envisageable. Cette opération de premier enrôlement a été traitée au point 2.4.3.

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. Il est considéré 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.

2.5.1.1 Acheminement de clé aléatoire générée de façon centralisée

RègleAcheminemementCléCentral-1.
L'acheminement jusqu'à l'utilisateur final d'une clé crypto- graphique générée aléatoirement de façon centralisée doit bénéficier de moyens de protection conformes au référentiel. Ces moyens doivent garantir l'authenticité, l'intégrité et la confidentialité de la clé acheminée.

RecomAcheminementNoirCentralBout-en-bout-1.
Il est recommandé que l'acheminement jusqu'à l'utilisateur final d'une clé cryptographique générée aléatoirement de façon centralisée soit protégé cryptographiquement de bout en bout en authenticité, intégrité et confidentialité par des mécanismes de protection conformes au référentiel.

2.5.1.2 Acheminement de clé générée par dérivation

RègleAcheminemementCléDérivée-1.
L'acheminement jusqu'à l'utilisateur final d'une clé cryptographique générée par un procédé de dérivation à partir d'une clé maître doit bénéficier de moyens de protection conformes au référentiels. Ces moyens doivent garantir l'authenticité, l'intégrité et la confidentialité de la clé acheminée.

RecomAcheminementNoirDérivéeBout-en-bout-1.
Il est recommandé que l'acheminement jusqu'à l'utilisateur final d'une clé cryptographique 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 conformes au référentiel.

2.5.2 Injection de clé

2.5.2.1 Injection de clé générée localement

Il est possible d'injecter 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.

RecomInjectionCléLocale-1. Il est recommandé que la génération locale d'une clé cryptographique ne donne pas lieu à un processus d'injection.

RègleInjectionCléLocale-1. L'injection d'une clé cryptographique générée localement doit bénéficier de moyens de protection conformes au référentiel. Ces moyens doivent garantir l'authenticité, l'intégrité et la confidentialité de la clé injectée.

2.5.2.2 Injection de clé aléatoire générée de façon centralisée

RègleInjectionCléCentral-1. L'injection dans l'environnement de confiance de l'utilisateur final d'une clé cryptographique générée aléatoirement de façon centralisée doit bénéficier de moyens de protection conformes au référentiel. Ces moyens doivent garantir l'authenticité, l'intégrité et la confidentialité de la clé injectée.

RecomInjectionCléCentral-1. Il est recommandé que l'injection dans l'environnement de confiance de l'utilisateur final d'une clé cryptographique 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 conformes au référentiel.

Remarque :

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

2.5.3 Injection de clé générée par dérivation

RègleInjectionCléDérivée-1. L'injection dans l'environnement de confiance de l'utilisateur final d'une clé cryptographique générée par un processus de dérivation à partir d'une clé maître doit bénéficier de moyens de protection conformes au référentiel. Ces moyens doivent garantir l'authenticité, l'intégrité et la confidentialité de la clé injectée.

RecomInjectionCléDérivée-1. Il est recommandé que l'injection dans l'environnement de confiance de l'utilisateur final d'une clé cryptographique 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 conformes au référentiel.

2.6 Utilisation d'une clé

2.6.1 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.

RecomDiffusion-1. Il est recommandé que la diffusion d'une clé privée ou secrète soit limitée aux seuls environnements de confiance qui l'utilisent vraiment.

2.6.2 Utilisation applicative d'une clé

RègleEnvironnementConfiance-1. L'utilisation d'une clé cryptographique dans un système applicatif doit obligatoirement se faire dans un environnement de confiance ayant un niveau de sécurité conforme au référentiel.

RègleVérificationAuthenticité-1. Avant toute utilisation d'une clé dans un système applicatif, son authenticité et son intégrité doivent être vérifiées par un mécanisme de sécurité conforme au référentiel.

RègleVérificationUtilisabilité-1. Avant toute utilisation d'une clé dans un système applicatif, il doit être vérifié par un mécanisme de sécurité conforme au référentiel que la clé est toujours utilisable.

2.7 Fin de vie d'une clé

RègleFinUtilisation-1. Une architecture de gestion de clés doit prévoir la fin de vie de l'ensemble des clés qu'elle gère ou utilise.

RecomCauseFinUtilisation-1. Il est recommandé qu'une architecture de gestion de clés traite les différentes causes de fin de vie d'une clé de façon distincte.

RègleEffacement-1. Une clé dont la durée d'utilisation est dépassée doit être effacée des environnements de confiance où elle était utilisée par un moyen technique conforme au référentiel.

2.8 Renouvellement d'une clé

RègleRenouvellement-1. Une architecture de gestion de clés doit prévoir le renouvellement de l'ensemble des clés qu'elle gère ou utilise.

RègleRenouvellementEnrôlement-1. Une architecture de gestion de clés 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 conformes au référentiel.

2.9 Recouvrement d'une clé

RègleRecouvrement-1. Une architecture de gestion de clés qui prévoit des fonctions de recouvrement de clés doit mettre en place des contrôles d'accès à cette fonctionnalité conformes au référentiel et respectant de plus l'ensemble des recommandations associées.

imprimé sur papier PEFC

IMPRIMERIE GRAPHIC SERVICE
GS COMMUNICATION S.A.M. MONACO