Federal Information Security Policy Guideline

Guide pour la cryptographie

21/11/2019

FISPDOC03 V1.1

Remarque importante : Le présent document est un guide qui résulte d'une collaboration entre des experts en sécurité de l'information des différents services fédéraux (SPF, OIP, IPSS). Les mesures présentées sont considérées comme des mesures minimales applicables raisonnablement de manière commune à tous les services fédéraux. Elles se basent sur des normes internationales et des bonnes pratiques en matière de sécurité de l'information ainsi que sur les expériences des participants au groupe de travail FISP.

Si des mesures plus strictes sont requises pour un service fédéral pour des raisons réglementaires ou autres raisons formelles et impérieuses, on peut supposer que ces mesures sont prioritaires sur les mesures prévues dans le présent guide.

Groupe de travail

.be

Table des matières

Contenu de ce document

Orientation du document

Le présent document fait partie intégrante de la méthodologie de sécurité de l'information au sein de l'administration fédérale (projet FISP). Chaque organisation fédérale doit disposer d'une politique et de processus en matière d'utilisation de mesures de gestion cryptographiques.

Cette politique doit être considérée comme un moyen de transposer la politique de sécurité de l'organisation en termes appropriés aux services cryptographiques utilisés dans l'exécution de tout ou partie de la politique de sécurité.

Objectif de sécurité du document

Cette politique a été rédigée pour proposer des mesures de sécurité de l'information relatives à la cryptographie, de manière à concrétiser la politique de sécurité.

Champ d'application

Cette politique ne constitue pas une description complète du processus de cryptage et ne contient pas de descriptions de produits, mais comporte une information suffisante pour poser des choix (stratégiques) appropriés et créer une prise de conscience en matière de cryptage et de Public Key Infrastructure (PKI).

Confidentialité du document

Distribution publique

Sauvegarde

Il s'agit d'une politique basée sur les pratiques internationales en matière de mesures cryptographiques. Si vous souhaitez appliquer cette directive à votre organisation, vous devez d'abord procéder à une évaluation et vérifier si d'autres restrictions, règles ou pratiques légales s'appliquent à votre organisation. Adaptez la politique de sécurité en fonction de votre organisation !

Lors du Conseil des ministres du 3 mai 2019, un avant-projet de loi a été soumis, à savoir la révision de la loi du 11/12/1998. Si cette loi est adoptée, la politique FISP sera mise à jour étant donné que la politique actuelle ne tient pas compte des évolutions légales futures.

Responsabilités

Le présent document est destiné au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de l'administration fédérale, aux responsables du traitement de l'information (y compris les sous-traitants des systèmes d'informations), à l'officier de sécurité et aux autres intervenants dans des domaines connexes (ex. le gestionnaire de documents).

Propriétaire

Le groupe de travail FISP est propriétaire du présent document.

Introduction

La présente politique propose des mesures de sécurité de l'information en matière de cryptographie pour les institutions fédérales (notamment cryptage et gestion de clés).

Le présent document contient une information suffisante pour poser des choix (stratégiques) appropriés et créer une prise de conscience. Les mesures proposées sont liées à la proposition de classification de l'information de la politique globale de sécurité de l'information (FISP) et aux différents contextes de données.

Un avis est également formulé à l'égard des mesures à prendre pour le cryptage. Des indications sont également données quant à la maîtrise tant des processus opérationnels que des processus de gestion qui sont importants dans l'application du cryptage.

Il ne s'agit toutefois pas d'une description complète de processus de cryptage ni d'une description de produit. Le présent document n'a pas été rédigé pour expliquer la cryptographie ni les mesures de sécurité de l'information en matière de cryptographie. Une description détaillée du principe de la cryptographie et des mesures correspondantes se retrouve dans le document FISP « Cryptographie - Explication ».

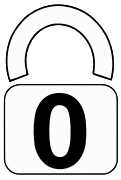
Classification de l'information - Cryptographie

La prise d'une décision concernant la question de savoir si une solution cryptographique est appropriée, doit être considérée comme un élément d'un processus plus large d'évaluation du risque. Cette évaluation peut ensuite être utilisée pour déterminer si une mesure cryptographique doit être prise et laquelle. Type, force et qualité doivent être pris en considération.

Mesures

Les mesures proposées sont liées à la proposition de classification de l'information de cette politique globale de sécurité de l'information (FISP) et aux différents contextes de données : data in use, data in motion, data at rest. Un exemple des différentes applications des contextes de données se trouve dans le document « Cryptographie - explication ».

Les mesures proposées sont des mesures superposées. Cela implique que les mesures de la classe d'information inférieure peuvent rester applicables aux classes supérieures, à l'exception de mesures techniques incompatibles. De plus, la complexité et la force des mesures évoluent avec la classe.

Catégorie[1]	
	Le cryptage s'effectue conformément aux pratiques communes et aux algorithmes et protocoles de cryptographie. **Data in motion :** • Cryptage au niveau du transport étant donné les objectifs d'intégrité (ex. extraction HTTPs de sites internet publics). • Terminaison au périmètre du réseau sécurisé. • Standard technique : ○ Protocole TLS : forward secrecy nécessaire si techniquement possible. **Data in use :** • Mesures d'atténuation après analyse des risques. **Data at rest :** • Le cryptage n'est pas nécessaire
 [2]	**Data in motion :** • Les solutions de cryptage doivent être réévaluées pour garantir non seulement les objectifs d'intégrité, mais également la confidentialité (ex. remplacement HTTS = one way SSL par un two ways SSL ou connexion IPSec,...) **Data in use :** • Le cryptage n'est pas nécessaire au sein de l'organisation. Cloisonnement au niveau de l'organisation par le biais de mesures d'accès physiques et/ou logiques. **Data in rest :** • Dans un environnement protégé : cloisonnement au niveau de l'organisation par le biais de mesures d'accès physiques et/ou logiques. • Dans un environnement non protégé : Seul le cryptage le plus simple est nécessaire (stockage, postes de travail, appareils mobiles, back-up,...).

[1] Cf. classification de l'information FISP
[2] Classe 1 = Classe 0 + mesures supplémentaires

	**Data in motion :** • Exportation sûre hors de l'application (application layer, database,...) : sécurité physique, sécurité d'accès logique (y compris transport interapp/intralayer). • Exportation sûre hors de l'organisation : cryptage au niveau du transport si on utilise un réseau non protégé et terminaison au niveau de la « trusted infrastructure » (ex. dans DMZ). • Standard technique : ○ Protocole de transport (TLS) (system-to-system) : authentification réciproque (2-way TLS) ○ Protocole de transport (TLS) (client-serveur) : authentification réciproque • 2-way TLS ou, • 1-way TLS + authentification substantielle eIDAS • Critères d'implémentation des certificats et clés : ○ contrôle de l'utilisation, ○ fort codage obligatoire **Data in use :** • pas de nécessité de mesures supplémentaires. **Data at rest :** • Dans un environnement non protégé : cloisonnement au niveau du besoin fonctionnel par le biais d'un cloisonnement physique, sécurité d'accès logique. Cryptage uniquement après analyse des risques. • Dans un environnement non protégé : cryptage pour l'ensemble de la chaîne de traitement (stockage, postes de travail, appareils mobiles, back-up,...).
	**Data in motion :** • Le cryptage est nécessaire indépendamment du contexte de transport (tant à l'intérieur qu'à l'extérieur de l'organisation) • Standard technique : ○ Obligation d'utiliser la version la plus récente de TLS et forward secrecy **Data in use :** • Pas de nécessité de mesures supplémentaires. **Data at rest :** • Le cryptage est nécessaire pour l'ensemble de la chaîne de traitement : stockage, DB ou middleware, postes de travail, appareils mobiles, back-up,...
 [3]	**Data in motion :** • Le cryptage est nécessaire et doit se faire au moyen d'un système de certification externe de l'autorité nationale (tant au niveau de la notification que du transport). **Data in use :** • Le cryptage est obligatoire au niveau de l'application si techniquement possible. **Data at rest :** • Le cryptage est obligatoire pour tout informatif au repos. L'organisation doit utiliser l'algorithme de cryptage le plus puissant et le plus récent disponible au moment de l'enregistrement.

[3] Pour cette classe, il faut également tenir compte d'autres exigences de sécurité sur la base de la loi du 11/12/1998.

Mesures pour le cryptage[4]

Mesures

Les règles et conditions d'utilisation suivantes peuvent servir d'exemples pour la gestion du cryptage des données. Il est également indiqué quelles mesures une organisation doit prendre pour réaliser cet objectif.

Rigueur durant le cryptage

Pour ce faire, une organisation doit veiller à ce que :

- le collaborateur dispose des outils et moyens nécessaires pour le cryptage de données ;
- le collaborateur dispose des procédures nécessaires pour le cryptage des données ;
- le collaborateur ait connaissance des procédures pour le cryptage des données.

Rigueur dans l'utilisation d'applications de cryptage

Pour ce faire, une organisation doit veiller à ce que :

- le collaborateur suive des formations pour l'utilisation des applications de cryptage ;
- le collaborateur dispose de manuels clairs pour les applications de cryptage ;
- les règles pour une utilisation rigoureuse soient acceptées et signées par les collaborateurs.

Connaissance de la cryptographie

Pour ce faire, une organisation doit veiller à ce que :

- lors de l'arrivée de nouveaux collaborateurs, une attention suffisante soit consacrée à la signification et à l'utilisation de la cryptographie, en ce compris les risques potentiels de la cryptographie qui pourraient, in fine, entraîner un effet néfaste sur son effectivité ;
- les applications cryptographiques soient régulièrement abordées dans les informations et les formations, quant à leur utilisation et leurs risques;
- la direction reconnaisse, soutienne et transmette l'importance du cryptage ;
- le collaborateur prenne part à un programme de prise de conscience.

Rigueur dans l'utilisation de la clé privée

Pour ce faire, une organisation doit veiller à ce que :

- le collaborateur soit sensibilisé aux négligences dans le traitement de sa clé privée. Par exemple, si le collaborateur laisse traîner sa smartcard avec sa clé privée sur son poste de travail.

Réaction rapide et adéquate lorsque la clé privée est compromise

Pour ce faire, une organisation doit veiller à ce que :

[4] Basé sur BIR - Politique de cryptage

- le collaborateur dispose de procédures décrivant la marche à suivre lorsque sa clé privée est compromise.

Le collaborateur est au courant et a connaissance des règles

Pour ce faire, une organisation doit veiller à ce que :

- les risques liés au cryptage soient mis en lumière dans le matériel de conscientisation et de training.

Autorisation et responsabilité durant le cryptage de l'information

L'organisation doit aussi être attentive à :

- l'autorisation implicite des utilisateurs, l'information qu'ils peuvent ou non voir en télétravail ;
- la clarté des rôles et responsabilités ;
- il doit également être clair que le collaborateur peut être appelé à se justifier a posteriori.

Mesures pour la gestion des clés[5]

Mesures

Les mesures présentées dans le présent chapitre sont des mesures minimales pour la gestion des clés. L'objectif est de contribuer à une politique de sécurité à l'échelle de l'organisation. La confidentialité, l'intégrité et l'authenticité des clés cryptographiques doivent être garanties durant la génération, l'utilisation, le transport et le stockage des clés. Les mesures minimales présentées sont liées aux activités suivantes :

- La détermination de la durée de vie des clés ;
- La génération et l'enregistrement des paires de clés et certificats ;
- Le retrait (« révocation ») de paires de clés ;
- L'archivage des clés ;
- La distribution des clés ;
- Le remplacement et à la mise à jour des clés ;
- La restauration des clés ;
- La destruction des clés.

La durée de vie des clés

L'organisation peut :

- tenir à jour toutes les paires de clés, le moment où les paires de clés sont émises et où elles expirent. C'est notamment nécessaire pour pouvoir déterminer quand une nouvelle paire de clés doit être générée.
- conserver toutes les paires de clés qui ont expiré afin de pouvoir garantir que toutes les données chiffrées au moyen de cette clé à présent invalide puissent de nouveau être déchiffrées.
- établir une procédure déterminant de quelle manière les utilisateurs sont informés du fait qu'une nouvelle paire de clés a été générée.

Générer (et enregistrer) des clés

L'organisation peut :

- enregistrer toutes les informations pertinentes, telles que les caractéristiques cryptographiques, la propriété et les phases de vie du matériel de cryptage dans un système d'enregistrement automatisé.
- fixer les tâches, responsabilités et compétences concernant la demande et la génération de clés et certificats. Un CISO peut jouer un rôle central en la matière. Le responsable :
    - collecte et vérifie les données d'identification du demandeur et autorise la demande.
    - sert d'autorité d'enregistrement (AE) interne pour les demandes de certificats. Pensons notamment aux activités suivantes : identification, authentification et autorisation de la demande, définir et compléter le contenu exact et agir en tant qu'intermédiaire à l'égard de l'autorité de certificat (AC) interne ou externe.
    - par application, définir dans un plan des clés, quand et comment les clés doivent être remplacées.
- définir où les incidents de sécurité doivent être notifiés, qui peut retirer une clé, comment communiquer, quelles sont les étapes à suivre et quelles clés retirées figurent sur une « revocation list ».
- conserver les clés cryptographiques de manière sûre.
- définir si des clés peuvent faire l'objet d'un back-up et, si oui, lesquelles. La raison d'un back-up est de continuer à pouvoir déchiffrer l'information après la perte de la clé originale. La raison de ne pas autoriser

[5] Basé sur BIR - Politique de cryptage

de back-up peut consister en des exigences que la loi sur la signature électronique (LSE) pose en matière d'authenticité et d'irréfutabilité.

Distribution des clés

L'organisation peut :

- enregistrer, dans un système d'enregistrement automatisé, toutes les clés en circulation, y compris le destinataire, sur la base d'une identité unique. Ce faisant, la partie compromettante est directement connue.
- définir comment les certificats et les codes d'accès correspondants sont émis.

Remplacement (et mise à jour) des clés

L'organisation peut :

- définir la fréquence à laquelle les paires de clés sont remplacées. Cette fréquence dépend du champ d'application. Les paires de clés utilisées pour le cryptage de données auront une durée de vie plus courte que les paires de clés utilisées pour créer une signature électronique.

Restauration des clés

L'organisation peut :

- définir dans quels cas spécifiques la restauration de clés peut être appliquée, pour quel type de clés, quelle méthode/solution est mise en place, qui peut introduire une demande et qui peut exécuter la procédure de restauration.

Retrait des clés

L'organisation peut :

- définir dans quels cas spécifiques le retrait de clés est appliqué, qui peut introduire une demande, qui peut exécuter la procédure et via quelle méthode l'aperçu des clés retirées est publiée (Certificate Revocation List (CRL) et/ou Online Certificate Status Protocol (OCSP)).

Archivage des clés

L'organisation peut :

- définir dans quels cas spécifiques l'archivage de clés est appliqué, qui peut introduire une demande de restauration et qui peut exécuter la procédure.
- définir comment les données cryptées sur demande peuvent être publiées de manière contrôlée.
- traiter les données cryptées selon les mêmes procédures de gestion (comme les procédures de back-up) que des données « normales ».
- dans le cas de données cryptées archivées, archiver également les clés et algorithmes afin de garantir la disponibilité des données.
- garantir le niveau de sécurité des données cryptées pendant le délai de disponibilité requis.

Destruction des clés

L'organisation peut :

- enregistrer, dans un système d'enregistrement automatisé, toutes les clés en circulation, qui utilise quelles clés et où, y compris les clés pour le back-up et l'archivage.
- définir quel type de clé peut être détruit et quand. A cet effet, il convient de tenir compte de la loi et de la réglementation, notamment les délais légaux de conservation.

Lien avec d'autres mesures[6]

L'application de la cryptographie ainsi qu'une gestion adéquate des clés sont essentielles pour garantir la confidentialité de l'information. Elles ne peuvent toutefois pas être instaurées en tant que mesures isolées. Il est préférable d'instaurer un ensemble de mesures. D'autres mesures sont déjà expliquées dans les autres documents FISP.

Lien avec l'IAM en tant que mesure

La vérification et la gestion des identités sont des éléments cruciaux du travail avec des certificats numériques. Les certificats numériques constituent d'ailleurs un mécanisme d'authentification repris dans les mesures minimales IAM.

Lien avec la séparation de fonctions en tant que mesure

La séparation des fonctions est une mesure de contrôle organisationnelle ayant pour but principal de prévenir fraudes et erreurs. Cet objectif est atteint par la répartition des tâches et droits correspondants pour un processus spécifique sur plusieurs organisations, rôles, personnes ou comptes.

Lien avec la journalisation en tant que mesure

Les mesures cryptographiques sont également appliquées pour protéger des données (sensibles) dans des fichiers journaux :

- Le cryptage peut alors être appliqué par garantir la confidentialité de cette information.
- Pour garantir l'intégrité de fichiers journaux, ils peuvent être sécurisés par le biais du hachage ou du placement d'une signature numérique.
- L'ajout d'un « time stamp » permet de réaliser une synchronisation de temps correcte. C'est notamment important pour l'analyse des journaux.

Lien avec les réseaux en tant que mesure

La cryptographie est souvent utilisée pour sécuriser des réseaux ; des données en transit ou « data in motion » (DIM) sont cryptées dans le cadre de :

〉 l'intégrité : le hachage ou la signature numérique permet d'éviter que des données en transit soient modifiées de manière incontrôlée ;

[6] Autorité flamande-classification de l'information - Cryptographie

〉 la confidentialité : par le biais du cryptage, par ex. de données non publiques sur un réseau public au moyen du « tunneling ».

Gestion du document

Historique

Date	*Auteur*	*Version*	*Description des modifications*
09/05/2019	BOSA	V.0.1	• First draft
15/05/2019	BOSA	V.0.2	• Texte complété et retravaillé • Contextes de données déplacées vers l'annexe • Explication technique introduite dans un document distinct
20/05/2019	FISP workgroup	V. 1	• Modification de l'introduction • Data in rest sous classe 1 modifiés • Référence à la loi pour la classe 4 • Déplacement de l'annexe « données en contexte » vers le document explicatif
21/11/2019	FISP workgroup	V.1.1	• Distribution publique

Approbations

Date	*Approbateur(s)*	*Version*
21/11/2019	FISP workgroup	V.1.1

Sources

Ce document a été rédigé à l'aide des sources suivantes :

- Autorité flamande -classification de l'information - Cryptographie
- BIR - Politique de cryptage
- IEC 27001/2

Lien avec une autre politique

Dépendance de documents internes

Réf.	*Titre*
FISPDOC05	*Guide pour la sécurisation et la gestion des identités et des accès de base (IAM), et des accès privilégiés (PAM)*

Positionnement de la politique par rapport à la norme ISO 27001

Section	*Objectifs et mesures de référence*	*En relation (X = Oui*
	Contexte de l'organisation	
	Leadership	
	Planification	
	Support	
	Opération	
	Évaluation du travail presté	
	Améliorations	

Positionnement de la politique par rapport à la norme ISO 27002

Section	**Objectifs et mesures de référence**	En Relation *(X = Oui)*	Objectifs/Mesures *(Détail)*
	Politique de sécurité de l'information		
	Organisation de la sécurité de l'information		
	Sécurité des ressources humaines		
	Asset management		
	Contrôle d'accès		
	Cryptographie	*X*	*10.1*
	Sécurité physique et écologique		
	Sécurité opérationnelle		
	Sécurité de la communication		
	Acquisition, développement et maintenance des systèmes d'information		
	Relations avec les fournisseurs		
	Gestion des incidents de sécurité de l'information		
	Sécurité de l'information dans le « Business Continuity Management »		
	Conformité		