Politique relative à la sécurité et la confidentialité de l'information

Chiffrement

(BLD CRYPT)

TABLE DES MATIERES

1. Introduction

Le présent document fait partie intégrante de la méthodologie relative à la sécurité et à la confidentialité de l'information dans la sécurité sociale. Il est destiné aux responsables, aux sous-traitants de l'information, au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de la sécurité sociale (IPSS).

Dans ce document sont décrites les responsabilités du collaborateur concernant la cryptographie : techniques permettant de cacher ou crypter des informations à envoyer, de telle manière qu'une personne qui a accès au canal entre l'expéditeur et le destinataire (et peut donc "écouter") ne puisse pas, moyennant un effort raisonnable, déduire des données véhiculées quelles informations ont été envoyées par l'expéditeur et quelles étaient les parties concernées.

La cryptographie est utilisée pour transférer des données qui ne peuvent pas être lisibles par d'autres parties. Seuls l'expéditeur et le destinataire disposent de la clé nécessaire pour rétablir les données dans leur forme originale.

2. Chiffrement

Toute institution souscrit à la politique suivante relative à la sécurité et à la confidentialité de l'information pour l'ensemble des informations et systèmes d'information placés sous sa responsabilité.

- L'institution doit établir, valider, communiquer et tenir à jour une politique formelle relative à l'utilisation de contrôles cryptographiques.
- L'institution doit établir, valider, communiquer et tenir à jour une politique formelle relative à l'utilisation, à la protection et à la durée de vie des clés cryptographiques pour tout le cycle de vie.

Annexe A : Gestion du document

Gestion des versions

Date	Auteur	Version	Description du changement	Date d'approbation	Date d'entrée en vigueur
2017		V2017	Première version et intégration EU GDPR	07/03/2017	07/03/2017

Erreurs et omissions

Si des erreurs ou des problèmes sont constatés à la lecture du présent document, vous êtes prié en tant que lecteur de transmettre au conseiller en sécurité de l'information (CISO) / délégué à la protection des données (DPO) de l'institution une brève description de l'erreur ou du problème ainsi que de sa place dans le document conjointement à vos données de contact.

Définitions

Dans un souci de cohérence de la terminologie et des concepts utilisés dans tous les documents de politique, toutes les définitions relatives à la sécurité et à la confidentialité de l'information sont centralisées dans un document intitulé "Définitions relatives à la sécurité et à la confidentialité de l'information".

Annexe B : Références

Ci-dessous figurent des documents qui ont servi d'inspiration au présent document.

- ISO, "ISO/IEC 27001:2013 Information Security Management System Requirements", septembre 2013, 23 pages
- ISO, "ISO/IEC 27002:2013 Code of Practice for Information Security Management", septembre 2013, 80 pages
- ISACA, "COBIT 5 for Information Security", mai 2012, 220 pages
- ENISA, "Study on cryptographic protocols", novembre 2014, 52 pages
- ENISA, "Recommended cryptographic measures: securing personal data", septembre 2013, 34 pages

Ci-dessous figurent des références aux sites web qui ont servi d'inspiration au présent document.

- https://www.iso.org/fr/isoiec-27001-information-security.html
- https://www.iso.org/fr/standard/54534.html
- https://www.iso.org/fr/standard/54533.html
- http://www.isaca.org/cobit
- http://www.ccb.belgium.be/fr
- https://www.safeonweb.be/fr
- https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data/cryptographic-protocols-and-tools
- https://www.enisa.europa.eu/publications
- https://www.esat.kuleuven.be/cosic/
- https://uclouvain.be/crypto/
- https://webstore.ansi.org/software/Encryption-Cryptography.aspx

Annexe C : Directives relatives à l'utilisation des contrôles cryptographiques

Ces directives s'appliquent aux données et aux systèmes d'information qui utilisent le cryptage symétrique et le cryptage asymétrique, les phrases secrètes et les clés cryptographiques.

Des mesures cryptographiques doivent être déterminées sur la base d'une analyse des risques formelle précise répondant aux questions suivantes :

- Comment sont gérées les données enregistrées sur des supports amovibles ?
- Où sont stockées ou traitées les données ?
- Comment la confidentialité, l'intégrité ou l'authenticité des données sont-elles garanties ?
- Comment est garantie l'irréfutabilité d'une activité ?

Lorsque la cryptographie est exigée, il faut toujours utiliser une mesure cryptographique qui soit la plus forte que possible.
L'institution doit tenir un aperçu indiquant où sont appliquées des mesures cryptographiques, quelles mesures cryptographiques sont appliquées et qui en est responsable.
Les mesures cryptographiques appliquées doivent être éprouvées par un expert indépendant fiable. Le responsable de la sécurité de l'information doit déterminer quelles mesures cryptographiques doivent être appliquées dans quels cas, suivant les bonnes pratiques actuelles.
L'application et l'opportunité des solutions et mesures cryptographiques doivent être évaluées périodiquement.
Les données cryptées de tiers qui arrivent sur le réseau de l'institution doivent d'abord être décryptées pour vérifier la présence de virus et autres malware.

Annexe D : Directives relatives à la gestion des clés

L'institution est responsable de la gestion des clés. Des procédures et des processus relatifs à la gestion des clés doivent être établis, validés, communiqués à tous les acteurs concernés et actualisés régulièrement.

La gestion des clés doit recouvrir au minimum les thèmes suivants :

- Demande/génération de clés
- Stockage de clés (privées)
- Transport de clés (privées)
- Utilisation de clés
- Remplacement et destruction de clés
- Archivage de clés
- Gestion des clés compromises

Les directives minimales suivantes doivent être d'application pour la demande/génération de clés :

- Il faut opter pour la plus forte mesure cryptographique applicable dans la pratique.
- Les clés doivent avoir une date d'activation et de validité.
- La durée de validité doit dépendre du but visé et du temps qu'il faudrait pour cracker la clé.
- Chaque clé doit être unique.
- Une clé doit être générée uniquement pour un but et un environnement précis.
- Les clés doivent être délivrées par une partie agréé qui travaille suivant une bonne pratique.

Les directives minimales suivantes doivent être d'application pour le stockage de clés (privées) :

- Le nombre de lieux de stockage des clés doit être limité à un minimum.
- Des systèmes doivent protéger les clés utilisées par le système pour les utilisateurs.
- Les clés doivent être protégées contre la perte ou la modification (ex. via une copie).
- L'accès aux clés doit être limité à un minimum (à leur responsable).
- Les clés sont accessibles uniquement aux experts techniques.

- Pour les données sensibles ou cruciales, il faut au minimum deux gestionnaires.
- Les clés doivent à tout le moins être protégées aussi bien que les données auxquelles elles se rapportent.

Les directives minimales suivantes doivent être d'application pour le transport de clés (privées) :

- Le transfert de clés sous forme lisible doit se faire en personne ou via un canal alternatif fiable.
- Ces moyens et méthodes de communication de clés doivent d'abord être approuvés par le conseiller en sécurité de l'information (CISO) / le délégué à la protection des données (DPO).
- Les directives minimales suivantes doivent être d'application pour l'utilisation des clés :
    - Chaque clé doit être utilisée uniquement pour le but et l'environnement visés.
    - Une clé utilisée dans des systèmes en production ne peut pas être utilisée dans des systèmes hors production.
    - Dans l'institution, la cryptographie s'impose majoritairement pour :
    - la sécurisation des données présentes sur les appareils mobiles
    - le stockage des mots de passe
    - la sécurisation des applications
    - la sécurisation de la communication de données non publiques sur des réseaux publics (comme les connexions VPN).
    - Le stockage et la sécurisation de la communication de données cruciales sur le réseau interne.

Les directives minimales suivantes doivent être d'application pour la demande et la destruction de clés :

- À la date d'expiration, toutes les clés doivent être supprimées partout où elles sont stockées ou appliquées.
- Au besoin, une clé répondant aux mêmes exigences sera générée.

Les directives minimales suivantes doivent être d'application pour l'archivage de clés :

- Les clés qui ont été utilisées par des utilisateurs ayant quitté l'institution doivent être cryptées et archivées.

Les directives minimales suivantes doivent être d'application pour les clés compromises :

- Chaque clé compromise ou supposée compromise doit directement être remplacée.
- Une procédure doit être définie pour chaque type de mesure indiquant comment agir lorsqu'une clé peut être compromise ou lorsqu'une vulnérabilité est connue.
- Une clé compromise ne peut pas procurer des données pouvant servir à déterminer la clé de remplacement.

Chaque clé doit être placée sous la responsabilité d'un collaborateur interne. Un aperçu de tous les responsables des clés doit être tenu.
Des mesures doivent être appliquées pour détecter les tentatives non autorisées de diffusion, de déchiffrement, d'accès, d'utilisation, de modification ou de remplacement de clés ou de données cryptées.
Ces directives doivent figurer dans des conventions avec les fournisseurs de services ou produits cryptographiques.
Des procédures indiquant comment gérer les demandes d'accès à des données cryptées (comme dans le cas d'un procès ou d'une plainte introduite auprès de l'institution) doivent être établies.
L'accès à des clés privées ou leur utilisation doivent être consignés suivant les procédures reprises dans le document "BLD Logbeheer".

Annexe E : Lien avec la norme ISO 27002:2013

Nous renvoyons ici à la (aux) clause(s) principale(s) de la norme ISO 27002:2013 relative à l'objet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	
Organisation de la sécurité de l'information	
Personnel sûr	
Gestion des moyens d'exploitation	
Sécurisation des accès	
Cryptographie	**Oui**
Sécurité physique et de l'environnement	
Sécurisation des processus	
Sécurité de la communication	
Achats, maintenance et développement de systèmes d'information	
Relations fournisseurs	
Gestion des incidents de sécurité	
Aspects de sécurité de l'information de la gestion de la continuité	
Respect	

***** FIN DU DOCUMENT *****