

Federal Information Security Policy Guideline

Guide de démarrage

21/11/2019

FISPD09 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 nécessaires à un service fédéral pour des raisons réglementaires ou pour d'autres raisons formelles et contraignantes, il va de soi que ces mesures prévalent sur celles décrites dans le présent guide.



TABLE DES MATIÈRES

I.	Contenu du document	4
	Orientation du document	4
	Objectif de sécurité du document	4
	Ce document est un guide pratique pour les différentes autorités fédérales, avec des conseils d'ordre général pour l'application et la mise en œuvre de FISP.	4
	Champ d'application	4
	Confidentialité du document	4
	Clause de non-responsabilité	4
	Responsabilités	4
	Propriétaire	4
II.	Introduction	5
III.	1.Stratégie de gestion	6
1.1.	Conseils :	6
IV.	2.Gestion des actifs	7
2.1.	Inventaire des actifs	7
2.2.	Catégorisation des actifs essentiels	7
2.3.	Conseils	7
V.	3.Évaluation du risque	7
3.1.	Conseils	8
VI.	4.Catégorisation de l'information	8
VII.	5.Exécution des mesures de sécurité spécifiques	8
5.1.	Guide pour le contrôle et la sécurité des accès physiques	9
5.2.	Guide pour la cryptographie	9
5.3.	Guide pour le logging et le monitoring	9
5.4.	Guide pour la sécurisation et la gestion des identités et des accès de base (IAM), et des accès privilégiés (PAM)	9
5.5.	Guide pour un usage sécurisé du cloud	9
5.6.	Guide pour la protection des données à caractère personnel	10
VIII.	6.Évaluation des mesures de sécurité	10
IX.	7.Annexe	11
7.1.	Cryptographie	11
	Cryptage	12
	Certificat numérique	13
	Public Key Infrastructure	15
	Gestion des clés	17
	Horodatage ('Time stamping')	18
	Les aspects de sécurité	19
	Contexte :	23
7.2.	Logging	25
	Le logging en tant que mesure	25
	Le monitoring en tant que mesure	27
	Monitoring sécurité	27
7.3.	Mesures IAM	29
	L'identification en tant que mesure	29
	L'authentification en tant que mesure	30
	L'autorisation en tant que mesure	33
7.4.	La mesure de sécurité de l'information PAM	35
	La gestion du changement (<i>change management</i>) en tant que mesure	35
	Identity & Access Management en tant que mesure	35

La gestion de la configuration en tant que mesure	35
La gestion des loggings en tant que mesure	36
La gestion des risques en tant que mesure	36
7.5. Types de données pour la protection des données à caractère personnel	37
Types de données de la catégorie d'information 0	37
Types de données de la catégorie d'information 1	37
Types de données de la catégorie d'information 2	38
Types de données de la catégorie d'information 3	40
Types de données de la catégorie d'information 4	44
X. Gestion du document	45
Historique	45
Approbations	45
Sources	45
XI. Lien avec une autre politique	46
Positionnement de la politique par rapport à la norme ISO 27001	46
Positionnement de la politique par rapport à la norme ISO 27002	46

Contenu du document

Orientation du document

Ce document fait partie intégrante de la méthodologie relative à la sécurité de l'information au sein de l'administration fédérale (projet FISP).

Objectif de sécurité du document

Ce document est un guide pratique pour les différentes autorités fédérales, avec des conseils d'ordre général pour l'application et la mise en œuvre de FISP.

Champ d'application

Cette politique de sécurité de l'information est applicable à toutes les informations qui circulent dans les organisations fédérales.

Confidentialité du document

Distribution publique

Clause de non-responsabilité

Ces informations ne peuvent pas être utilisées individuellement comme documentation de référence. Ce document ne peut pas servir de substitut à la législation ou à des normes, mais vise à guider le lecteur dans la prise de mesures de sécurité appropriées.

Responsabilités

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

Propriétaire

Le groupe de travail FISP est propriétaire du présent document.

Introduction

Le projet FISP comprend une politique de sécurité de l'information. Dans ce cadre, il existe des manuels spécifiques, notamment pour la cryptographie et le logging. Cependant, cette politique ne comprend pas la mise en œuvre effective des mesures de sécurité FISP. C'est la raison pour laquelle nous vous proposons ce starterkit. Dans ce starterkit, le groupe de travail FISP prévoit quelques conseils généraux pour les instances publiques afin de les aider au mieux dans l'application et la mise en œuvre des mesures de sécurité FISP. Dans ce cadre, nous prenons également en compte les étapes à parcourir avant l'application des mesures recommandées par FISP.

Les mesures recommandées par FISP tiennent compte des normes ISO 2700X existantes. Le paquet de mesures proposées en matière de sécurité de l'information n'est toutefois pas complet, étant donné qu'il y a des objectifs de sécurité qui ne sont pas encore traités de manière détaillée dans cette première version du FISP. Il est donc conseillé de se tourner vers ces normes dans le cas où des informations complémentaires sont nécessaires. Par ailleurs, nous vous conseillons également d'utiliser les BSG (Baseline Information Security Guidelines) fournies par le Centre pour la Cybersécurité Belgique (CCB) étant donné que FISP constitue un complément à cette politique.

1. Stratégie de gestion

L'implication des managers est très importante pour le succès de votre implémentation FISP. La politique de sécurité de l'information recommandée par FISP et le plan de sécurité de l'information qui en découle pour votre organisation fédérale nécessitent la validation et le support du management de l'organisation fédérale spécifique. La sécurité de l'information fait en effet partie d'une bonne gestion de l'organisation et sera en outre influencée par les besoins et les objectifs de l'organisation, les exigences en matière de sécurité, les processus utilisés dans cette organisation et la structure de l'organisation.

Impliquer le management favorise en outre le développement d'une culture de la sécurité et la mise en œuvre des mesures de sécurité proposées.

Il est important que le management crée d'abord un bon cadre pour la mise en œuvre du FISP. Cela peut se faire au moyen d'une stratégie de sécurité de l'information qui respecte la législation et les réglementations. Il est en outre indiqué d'intégrer la structure de la sécurité dès le début d'un projet.

Les instruments et le support nécessaires pour cette mise en œuvre devront être prévus par le management. Mais afin de pouvoir affecter les moyens de manière effective, ils doivent être communiqués à tous les intéressés au sein de votre organisation.

Enfin, il faudra organiser régulièrement des formations et des sensibilisations pour tous les collaborateurs internes et externes et pour l'organisation dans son ensemble. La communication avec toutes les parties intéressées de l'organisation fédérale est essentielle.

1.1. Conseils :

- Il est conseillé de faire concorder suffisamment le plan de sécurité de l'information avec la stratégie et les objectifs opérationnels de votre organisation fédérale de manière à éviter un rejet par le management.
- Soulignez la responsabilité du management (le responsable du traitement).
- Informez les managers en temps voulu.

2. Gestion des actifs

2.1. Inventaire des actifs

Nous devons d'abord examiner ce qui peut précisément être mis en péril, en d'autres termes ce que possède l'organisation fédérale ou la capacité de l'organisation fédérale. La gestion de la sécurité est basée sur des actifs clairement identifiés et valorisés. Il est donc indispensable de dresser un inventaire des actifs de l'organisation fédérale. L'objectif de la sécurité de l'information consiste à protéger l'organisation fédérale et ses actifs. Cela ne se limite toutefois pas à l'infrastructure IT ou aux actifs tangibles mais aussi aux personnes ou aux processus.

2.2. Catégorisation des actifs essentiels

Il est par conséquent conseillé de créer une hiérarchie dans les actifs inventoriés sur la base de la criticité de ces actifs. Il importe dès lors d'avoir une vision claire de la valeur et de l'importance des actifs et de comprendre dans quelle mesure ils sont importants pour le bon fonctionnement et la bonne organisation de l'instance fédérale. Il se peut donc qu'un processus en particulier soit plus important pour l'instance fédérale qu'un autre processus. Cette catégorisation permettra également de savoir plus clairement quels processus doivent être prioritaires sur le plan de la sécurité de l'information.

2.3. Conseils

- Définissez/identifiez les "actifs essentiels" en collaboration avec le management et les différents départements.
- Rencontrez si nécessaire les personnes responsables de ces différents actifs afin de mieux les identifier et les définir.
- Dressez-en une liste.
- Faites approuver formellement cette liste par le management, afin qu'il puisse être associé à votre processus (par exemple via un rapport d'approbation ou un document signé par le management).

Il est important d'améliorer ce processus en continu et donc de continuer à l'appliquer afin d'éviter de perdre de vue de nouveaux actifs.

3. Évaluation du risque

Nous examinons ensuite quelles menaces pèsent sur les actifs essentiels. Une analyse de risques vous permet d'identifier les menaces et les risques pour les actifs identifiés. Ces menaces peuvent être un incendie notamment, ou une intervention humaine (non) intentionnelle. Par exemple une personne qui oublie un document confidentiel. Il faut aussi tenir compte des maillons faibles de l'organisation fédérale, comme un logiciel mal installé qui permet à un pirate informatique de pénétrer plus facilement dans le système et d'avoir accès à des informations confidentielles. Il est donc conseillé de prendre en compte le plus d'incidents possible.

Pour l'évaluation des risques, il faudra faire une distinction entre les "risques inhérents" et les risques "résiduels". Alors que les risques "inhérents" sont ceux qui ont un impact négatif en l'absence de mesures de sécurité, les risques "résiduels" sont ceux qui pourraient avoir un impact négatif en dépit des mesures de sécurité prises.

Les résultats de l'analyse de risques aident le management à élaborer une stratégie qui tient compte de tous les coûts nécessaires pour protéger les actifs identifiés contre les menaces identifiées, et à développer une politique de sécurité pratique qui sert de fil conducteur pour les activités liées à la sécurité. Les risques résiduels élevés devront aussi être communiqués de manière suffisante à la direction afin de pouvoir décider si ceux-ci sont traités ou acceptés comme risques résiduels.

3.1. Conseils

- L'organisation doit, pour chaque processus, réaliser une évaluation des risques en matière de sécurité de l'information, la valider, la communiquer et la tenir à jour.
- Une analyse de risques se trouve dans la méthode optimisée d'analyse de risques 'Monarc'.¹ Une approche plus détaillée se trouve également dans la norme ISO 27005.
- L'organisation doit communiquer toutes les évaluations de risques présentant un risque résiduel élevé à la direction pour discussion et décision : traiter ou accepter.
- L'analyse de risques peut être très simple, mais elle peut aussi être détaillée.
- La complexité de l'analyse dépend de la taille de l'organisation fédérale, de la complexité des projets et de la sensibilité des données que vous traitez, de la disponibilité de l'expertise, du temps disponible et du budget.

4. Catégorisation de l'information

Avant de pouvoir appliquer des mesures de sécurité spécifiques, il est nécessaire de procéder à une catégorisation de l'information. Il est conseillé aux organisations fédérales, selon la sensibilité de l'information, de protéger l'information suivant une méthodologie afin de maîtriser et limiter les risques à certains niveaux de protection. Ces niveaux de protection s'expriment en niveaux de catégorisation. Selon la catégorie dont relève l'information, plusieurs mesures de sécurité sont proposées. Le groupe de travail FISP a établi un schéma pour la catégorisation de l'information. Il appartient à l'organisation fédérale de définir les procédures internes pour marquer ses informations suivant les catégories proposées par FISP.

Voir : FISP - catégorisation de l'information (lien à ajouter)

5. Exécution des mesures de sécurité spécifiques

Lorsque tous les actifs essentiels sont identifiés et évalués et que tous les risques pouvant représenter une menace pour l'instance fédérale sont connus, il est nécessaire de mettre en œuvre les mesures de sécurité conseillées par FISP. Cela permet de protéger les actifs essentiels contre les risques éventuels en matière d'intégrité, de confidentialité et d'accessibilité. Cependant, il restera toujours des risques résiduels après l'instauration des mesures de sécurité. Il est impossible d'éviter ces risques résiduels (par exemple des erreurs humaines) mais le but est de les maintenir au niveau le plus bas possible.

Le groupe de travail FISP a rédigé des documents détaillés sur plusieurs sujets. Dans la plupart de ces documents, vous pouvez retrouver des mesures de sécurité recommandées liées à la catégorisation de l'information proposée par FISP, à l'exception des mesures de sécurité physique et de la sécurité du Cloud.

¹ <https://www.monarc.lu/>

5.1. Guide pour le contrôle et la sécurité des accès physiques

Ce document décrit les mesures recommandées en vue d'empêcher tout accès physique, dommage et interférence non autorisés aux informations et aux systèmes de traitement des informations des organisations fédérales.

Voir : Guide pour le contrôle et la sécurité des accès physiques

5.2. Guide pour la cryptographie

Ce document décrit les mesures recommandées en matière de cryptographie. Il contient des informations suffisantes pour poser des choix (stratégiques) appropriés et créer une prise de conscience. Les mesures proposées sont liées à la proposition de catégorisation de l'information de FISP et aux différents contextes de données.

Voir : Guide pour la cryptographie

Pour de plus amples informations sur la cryptographie, voir l'annexe 7.1.

5.3. Guide pour le logging et le monitoring

Ce document décrit les mesures recommandées en matière de journalisation. Les mesures proposées sont liées à la catégorisation de l'information proposée par FISP. Le document comprend également des conseils pour les mesures à prendre pour la gestion du journal, des indications sur la rétention et la sécurité des enregistrements d'audit, sur la manière de gérer les erreurs dans les enregistrements d'audit et sur le suivi, l'analyse et le rapportage des audits.

Voir : Guide pour le logging et le monitoring

Si vous voulez de plus amples informations sur le logging et les mesures conseillées, voir l'annexe 7.2.

5.4. Guide pour la sécurisation et la gestion des identités et des accès de base (IAM), et des accès privilégiés (PAM)

Dans ce document, les mesures générales IAM sont organisées selon la catégorisation de l'information proposée par le groupe de travail FISP. Ce document fait également référence au "*Privileged Access Management*" (PAM).

Voir : Guide pour la sécurisation et la gestion des identités et des accès de base (IAM), et des accès privilégiés (PAM)

Si vous voulez de plus amples informations sur les mesures IAM, voir l'annexe 7.3. Pour de plus amples informations sur les mesures PAM, voir l'annexe 7.4.

5.5. Guide pour un usage sécurisé du cloud

Ce guide permet aux services publics d'identifier systématiquement les risques en matière de sécurité de l'information pour les services cloud, de les analyser et de les évaluer. Il décrit en outre les contrôles permettant de gérer ces risques de manière effective.

Voir : Guide pour un usage sécurisé du cloud

5.6. Guide pour la protection des données à caractère personnel

Ce document décrit les exigences en matière de sécurité de l'information telles que définies par le règlement général sur la protection des données (RGPD). Il contient également une catégorisation standardisée basée sur l'interprétation du groupe de travail FISP.

Voir : Guide pour la protection des données à caractère personnel

Si vous souhaitez de plus amples informations sur les différents types de données décrits dans le vade-mecum, voir l'annexe 7.5.

6. Évaluation des mesures de sécurité

Il est conseillé de procéder à une évaluation annuelle des mesures de sécurité. Cela permet de déterminer quelles sont les améliorations à apporter et d'évaluer le statut du plan de sécurité. La sécurité de l'instance fédérale doit être contrôlée constamment et doit pouvoir être adaptée et se développer, en tenant compte des besoins en termes de sécurité et des circonstances dans lesquelles l'instance fédérale existe et travaille.

Il est donc indispensable d'analyser régulièrement les menaces et les vulnérabilités (cycle d'amélioration continue : PDCA) et d'adapter aussi le plan de sécurité à la lumière de ces évaluations.

7. Annexe

7.1. Cryptographie

La cryptographie est la discipline scientifique visant à sécuriser des informations au moyen de techniques mathématiques. Les techniques cryptographiques peuvent être appliquées à des informations stockées (*'Data at Rest'* ou DAR), à des informations traitées par une application ou un système (*'Data in Use'* ou DIU) ou à des informations en circulation (*'Data in Motion'* ou DIM). Vous trouverez un exemple des différentes applications des contextes de données à l'annexe 1.

Appliquer des techniques cryptographiques permet d'assurer une série **d'aspects de sécurité** :

- **Confidentialité** : garantir que les informations peuvent uniquement être lues par ceux qui y sont autorisés.
- **Intégrité** : garantir que les informations ou fonctionnalités n'ont pas été modifiées par des personnes non autorisées.
- **Authentification d'entités** : vérifier l'identité d'une entité (entité = personne, organisation, processus, système...).
- **Authentification de données** : garantir l'origine et l'intégrité des informations. L'authentification de données se compose donc de deux éléments : vérifier que les données proviennent de la bonne entité et valider leur intégrité. L'authentification de données est plus complexe que la confidentialité.
- **Irréfutabilité** (*'non-repudation'*) : empêcher que des précédentes actions ou obligations puissent être niées.
- **Anonymat** : garantir la confidentialité des entités communicantes (c.-à-d. des métadonnées : qui communique avec qui) est également un service de sécurité pour lequel on peut avoir recours à des techniques cryptographiques.

La cryptographie comprend un éventail de techniques pour répondre aux aspects de sécurité ci-dessus. Vous trouverez ci-après un résumé des aspects de sécurité et des techniques qui les prennent en charge :

Confidentialité	Cryptage
Intégrité	Cryptage (hachage) et signature numérique
Irréfutabilité	Signature numérique avec certificat
Authentification	Signature numérique avec certificat (par ex. eID)

Techniques possibles pour des activités techniques – elles sont transparentes pour un utilisateur :

- La délivrance et la gestion de certificats numériques au moyen d'une PKI.
- La gestion de clés et le cycle de vie d'une clé ou d'une paire de clés.
- La confidentialité et l'intégrité des informations lors de la circulation sur un réseau – par ex. par la mise en place du VPN.
- Garantir l'origine du logiciel au moyen de la signature numérique.
- Garantir l'authenticité d'un site web au moyen d'un certificat (SSL).
- Authentification de système au moyen de certificats numériques.

Cryptage

Introduction

Le cryptage est un mécanisme visant à sécuriser des informations en les rendant illisibles aux personnes non autorisées. Il est réalisé par un algorithme mathématique et une clé cryptographique. En plus du contrôle d'accès comme mesure de sécurité, le cryptage permet d'assurer la confidentialité des informations. Il empêche une partie non autorisée de lire ou modifier des informations confidentielles. Il offre en outre la possibilité de contrôler si un message provient effectivement d'un certain expéditeur. Le cryptage peut aussi être utilisé pour rendre illisibles des données sur un ordinateur portable, un disque dur externe, une clé USB ou d'autres supports de stockage mobiles. En cas de perte ou de vol, personne ne peut alors lire les données cryptées.

Le cryptage d'informations est aussi appelé chiffrement ou codage ; le décryptage est appelé déchiffrement.

Il y a deux techniques de cryptage : symétrique et asymétrique.

Comment fonctionne le cryptage ?

Cryptage symétrique

Le cryptage symétrique utilise un algorithme mathématique qui se base sur la même clé secrète (symétrique) pour crypter et décrypter. Les deux parties doivent avoir la même clé secrète qui doit par conséquent être distribuée préalablement de façon sécurisée.

Les systèmes symétriques permettent aussi bien la confidentialité des informations que l'authentification des données, par exemple en réalisant d'abord le cryptage du document avec une clé symétrique pour ensuite calculer la valeur MAC (*Message Authentication Code* ou code d'authentification de message) du document crypté.

Le cryptage est non seulement utilisé pour sécuriser des informations envoyées contre des personnes non autorisées, mais aussi pour rendre illisibles des données sur un ordinateur portable, un disque dur externe, une clé USB ou d'autres supports de stockage mobiles. En cas de perte ou de vol, personne ne peut alors lire les données cryptées.

Le cryptage symétrique est rapide, mais peut devenir un processus complexe quand il y a beaucoup de parties communicantes actives. Par ailleurs, il est difficile d'obtenir la clé du destinataire sans qu'elle soit volée par des personnes non autorisées.

Exemples d'applications dans la pratique :

- **KMS** : un '*Key Management System*' – ou système de gestion de clés – gère les clés cryptographiques, y compris la génération de clés, l'échange, le stockage, l'utilisation, la destruction et le remplacement de ces clés.
- **Kerberos** : Kerberos est un système d'authentification pour des réseaux locaux avec une architecture client-serveur, se basant sur une *Trusted Third Party* (une partie en qui toutes les autres parties ont confiance). Il protège les serveurs contre toute utilisation par des parties non autorisées, et les clients contre toute interaction avec de faux serveurs. Il peut aussi générer une clé de session pour la communication entre le client et le serveur afin que des intrus ne puissent pas reprendre ou espionner les sessions en cours.
- DES et AES sont deux exemples bien connus d'algorithmes pour le cryptage symétrique.

Cryptage asymétrique (*Public key encryption*)

Le cryptage asymétrique répond à la question de savoir comment obtenir une clé secrète de cryptage du destinataire sans qu'elle soit volée par des personnes non autorisées. Là où le cryptage symétrique utilise un algorithme mathématique qui se base sur la même clé secrète (symétrique) pour crypter et décrypter, le cryptage asymétrique travaille avec une paire de clés. Le cryptage ou le décryptage ne dépend donc pas d'une seule clé mais de la paire complète.

La paire de clés se compose d'une clé publique et d'une clé privée. Une seule clé est secrète (privée) et l'autre est publique. La clé cryptographique pour crypter n'est donc pas la même que celle pour décrypter.

Un message est rendu illisible avec la clé publique du destinataire. Ce dernier peut ensuite déchiffrer le message avec sa clé privée. Il est indispensable que la clé privée ne soit pas divulguée par le propriétaire de la paire de clés. Le cryptage peut aussi servir à garantir qu'un message provient d'un certain expéditeur. Dans ce cas, l'expéditeur crypte un message avec sa clé privée. Si le destinataire peut ensuite rendre ce message lisible en le décryptant avec la clé publique, cela prouve que le message en question provient bel et bien de vous.

L'avantage du cryptage asymétrique est qu'il permet de fournir facilement la clé de décryptage au destinataire. La clé publique est publique et peut donc sans problème être partagée entre toutes les parties. Ainsi, on peut se concentrer sur la sécurité de la clé privée. C'est évidemment beaucoup plus simple.

Le cryptage asymétrique présente toutefois un inconvénient : le manque de rapidité. Pour résoudre ce problème, l'on combine souvent le cryptage asymétrique au cryptage symétrique. De cette manière, l'on peut crypter une clé de cryptage symétrique – nécessaire pour le cryptage d'une importante quantité d'informations – avec la clé publique du destinataire. Ensuite, le destinataire décryptera cette clé avec sa clé privée. Ceci permet de s'assurer que la clé peut être utilisée pour décrypter les informations en question.

Selon la clé utilisée pour crypter (publique ou privée), il est possible de réaliser d'autres services de sécurité :

- cryptage au moyen d'une clé publique → *confidentialité*
- cryptage au moyen d'une clé privée → intégrité et irréfutabilité (signature numérique)

Certificat numérique

Les clés publiques utilisées pour le cryptage asymétrique ont un inconvénient. Il est difficile pour le destinataire de contrôler si la clé publique provient du « vrai » expéditeur. Elle pourrait en effet aussi provenir de quelqu'un qui se fait passer pour l'expéditeur (ce que l'on appelle le '*spoofing*'). Un certificat numérique permet de résoudre ce problème. C'est une sorte de passeport ou de permis de conduire. Il est utilisé comme légitimation officielle, pour démontrer l'authenticité d'une entité et sa relation avec sa clé publique.

La partie qui délivre le certificat numérique détermine la crédibilité de ce certificat ainsi que les contrôles en amont qui y sont liés. Il est possible d'émettre soi-même un certificat, mais sa crédibilité est plutôt faible. Un certificat délivré par une autorité est considéré comme crédible et fiable. En règle générale, les organisations qui délivrent et gèrent des certificats sont des organisations commerciales et des organisations publiques.

Certificat SSL

Les organisations fédérales mettent de plus en plus de services et d'informations à disposition sur Internet. Il importe que l'utilisateur sache que le site web sur lequel il complète ses données appartient réellement à l'organisation fédérale et que la communication avec ce site est suffisamment sécurisée. Les certificats SSL permettent de garantir cette sécurité. Ils ajoutent un sceau unique à un site web. Ce sceau est ensuite disponible

sur les sites pour contrôler leur authenticité et leur sécurité. L'intégrité du site des pouvoirs publics est ainsi garantie. C'est l'un des types de certificats les plus courants.

Données stockées dans un certificat

Le certificat contient les données suivantes :

- le nom enregistré du propriétaire : le titulaire du certificat ;
- la clé publique du propriétaire ;
- la période de validité du certificat ;
- l'identité de l'émetteur du certificat : l'autorité de certification (AC) ;
- l'emplacement de la '*Certificate Revocation List*' (chez l'émetteur du certificat) ;
- un résumé des données ci-dessus, créé par une fonction de hachage et ensuite crypté avec une clé secrète de l'AC. Il s'agit de la signature numérique qui sert aussi à garantir l'authenticité et la validité des données susmentionnées.

Pour pouvoir être utilisés dans la plupart des applications, les certificats numériques sont créés selon une norme communément admise : X.509. Cette norme reconnue offre la possibilité de mener des contrôles d'identité simples à approfondis du titulaire du certificat.

La force du certificat

La force d'un tel certificat en termes de fiabilité repose sur deux critères :

1. Quel est le degré de fiabilité de l'émetteur du certificat ?
2. Dans quelle mesure l'identité du propriétaire de la paire de clés a-t-elle été vérifiée ?

Pour le premier point – l'émetteur du certificat – il est important de vérifier le certificat même :

- Le certificat n'a pas été délivré par le propriétaire même (il n'y a alors pas eu de contrôle de l'identité du propriétaire) ?
- Le certificat est-il toujours valable et n'est pas compromis (validité et annulation) ?
- Le certificat a-t-il été délivré par une partie fiable ?

Pour le deuxième point – le contrôle de l'identité du titulaire du certificat – il y a trois options lors de l'achat d'un certificat X.509 :

1. **Validation de domaine** : les certificats avec validation de domaine ne contiennent pas de données d'entreprise. L'on vérifie uniquement si le demandeur a le contrôle du domaine pour lequel le certificat est demandé. Le certificat est fiable pour tous les navigateurs et fournit une connexion sécurisée par cryptage. Pour les certificats SSL avec validation de domaine, le navigateur affiche une icône de cadenas verrouillé, par ex. :



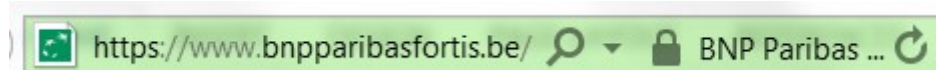
2. **Validation d'organisation** : les certificats avec validation d'organisation contiennent des données d'entreprise. Grâce à celles-ci, les visiteurs d'un site web peuvent vérifier s'ils se trouvent sur le site de la bonne entreprise. Les données d'entreprise figurent dans le certificat, mais ne sont pas mises en évidence comme c'est le cas avec les certificats EV. Ici aussi, le navigateur affiche une icône de cadenas verrouillé et

les données d'entreprise sont reprises dans le certificat, mais ne sont pas affichées en évidence sur le navigateur, par ex. :



En apparence, il n'y a pas de différences visibles avec la validation de domaine, mais le certificat fournit plus de détails.

3. **Validation étendue** (EV : '*extended validation*') : Outre la validation de domaine, où le demandeur montre qu'il a le contrôle du domaine pour lequel le certificat est demandé, il y a une vérification des données d'entreprise. Pour ce faire, l'on examine un registre public et l'organisation peut être appelée pour vérification. Il est parfois nécessaire de signer des documents supplémentaires. Un site web qui utilise des certificats SSL EV affiche une barre verte avec l'icône de cadenas verrouillé, par ex. :



En plus de la couleur verte et de l'icône de cadenas verrouillé, le navigateur affiche l'identification de l'organisation quand on clique sur l'icône de cadenas verrouillé. Ce type de validation est généralement utilisé par les institutions financières et les boutiques en ligne.

Spécifiquement pour la sécurité des sites web, il existe trois types différents de certificats SSL en plus des trois variantes de validation :

1. **Domaine unique** : ce type de certificats protège un seul nom de domaine, par ex. 'www.undomaine.com'.
2. **Multidomaine** : il est ici possible d'avoir plusieurs noms de domaine dans un seul certificat SSL.
3. **Certificats Wildcard** : avec un certificat Wildcard, tous les sous-domaines d'un domaine sont sécurisés. Ce type de certificats est uniquement disponible pour la validation de domaine et d'organisation ; pour la validation étendue (certificats EV), chaque sous-domaine doit avoir son propre certificat et l'on ne peut donc pas utiliser de certificats Wildcard.

Public Key Infrastructure

Une *Public Key Infrastructure* (PKI) – ou infrastructure à clés publiques (ICP) – est un ensemble de dispositions techniques et organisationnelles qui apportent une solution pour relier un propriétaire (personne ou organisation) à sa paire de clés cryptographiques au moyen du certificat numérique. De cette façon, des clés publiques peuvent être utilisées en combinaison avec les certificats correspondants pour authentifier et envoyer des informations (clés) secrètes sur un réseau moins sûr. Une PKI permet ainsi d'étendre la technique de cryptage asymétrique qui garantit que l'authentification et l'irréfutabilité peuvent être démontrées.

La délivrance et la gestion de ces certificats se font de manière formalisée, de sorte que le statut du certificat et du propriétaire est garanti. Un *Certificate Service Provider* (CSP) – ou prestataire de services de certification – est une partie (tierce) qui va délivrer les certificats pour le destinataire. Tant l'expéditeur que le destinataire doivent lui faire confiance. Il gère l'environnement PKI et garantit l'authenticité ainsi que l'origine des certificats.

Il doit également remplir des obligations de qualité. Les certificats peuvent être délivrés sous différentes formes. Les clés privées qui y sont liées doivent être protégées contre tout accès non autorisé et sont de préférence délivrées et stockées sur des objets sécurisés individuellement, comme des cartes à puce, des tokens USB et des *Hardware Security Modules* (HSM).

Plusieurs types de PKI sont utilisées, et elles sont associées à différents types de processus pour la délivrance de certificats par les CSP :

- Au sein d'une **organisation** : les certificats sont délivrés par un CSP propre.
- Au sein du **domaine public** : les processus de délivrance doivent se conformer à la 'loi eIDAS et archivage électronique'².
- **Toile de confiance** ('*web of trust*') : dans ce modèle, le contrôle de l'identité est effectué par les titulaires de certificat (les propriétaires des certificats). Ils sont responsables de l'authenticité de l'identité des autres titulaires de certificat. Citons comme exemples Thawte, CAcert et PGP.

² Loi du 21 juillet 2016 mettant en œuvre et complétant le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

Gestion des clés

Le degré de protection qu'offre la cryptographie dépend non seulement de l'algorithme ou du protocole utilisé, mais aussi de la confidentialité de la clé (clé secrète, clé privée) et de l'authenticité des clés publiques. La gestion des clés cryptographiques joue donc un rôle essentiel dans la sécurisation sur la base de techniques cryptographiques.

La gestion des clés porte sur toutes les activités liées aux clés, de la génération de clés jusqu'à leur destruction. Elle comprend la création, l'enregistrement, le stockage, la distribution, l'utilisation, l'annulation, l'archivage et la destruction de clés. En plus des mesures de sécurité techniques, il faudra prêter attention aux mesures de sécurité organisationnelles, physiques et procédurales. Citons comme exemples les mesures de sécurité pour la création et le stockage de clés, et la séparation des fonctions afin d'éviter et de détecter tout abus de clés.

Les thèmes suivants doivent être abordés dans les procédures de gestion des clés :

- comment demander une paire de clés ;
- qui peut générer les clés ;
- la façon dont les paires de clés doivent être transférées au propriétaire ;
- si le propriétaire doit s'identifier pendant le transfert de la paire de clés ;
- pendant combien de temps les clés seront valables ;
- qui peut retirer les clés ;
- comment les clés sont mises à jour.

La gestion des clés comprend les activités suivantes :

- déterminer la durée de vie des clés ;
- générer et enregistrer des paires de clés et des certificats ;
- annuler des paires de clés (*'revocation'*) ;
- archiver des clés ;
- distribuer des clés ;
- remplacer et mettre à jour des clés ;
- réparer des clés ;
- détruire des clés.

L'organisation de la gestion des clés repose principalement sur :

- le niveau de sécurité souhaité ;
- l'échelle ;
- les différentes façons dont le cryptage est appliqué ;
- l'importance des données cryptées.

L'importance des données cryptées est déterminée par l'échelle de classification des informations qui sont traitées. Plus la classification des informations est élevée, plus les procédures seront strictes et plus le degré de séparation des fonctions augmentera. Une analyse des risques peut aider à détecter les risques qui doivent être couverts par des mesures organisationnelles et/ou techniques.

Hiérarchie des clés

Il existe plusieurs façons de générer des clés cryptographiques, certaines sont *open source* (souvent gratuites), d'autres sont spécifiques au fournisseur (non gratuites). Mais une fois qu'une clé cryptographique a été générée et utilisée, elle doit être conservée en toute sécurité pour une utilisation ultérieure, ce qui n'est pas si simple. La hiérarchie des clés apporte une solution à ce problème.

La hiérarchie des clés est une technique qui utilise une clé principale (*roots*) pour crypter une clé cryptographique. Ainsi, elle met en place une méthode puissante pour sécuriser d'autres clés cryptographiques. Il suffit alors de très bien sécuriser cette clé principale pour garantir la fiabilité des autres clés. Malheureusement, cette solution n'exclut pas tous les risques car si la clé principale est piratée, toutes les clés sous-jacentes sont elles aussi compromises.

Cela signifie entre autres qu'il vaut mieux conserver cette clé principale dans un module HSM, par exemple homologué FIPS 140. Ce label de qualité garantit la bonne sécurité de la clé principale.

Les avantages de la hiérarchie des clés :

- le nombre de clés qui doivent être hautement sécurisées a été réduit pour ne viser que la sécurité de la clé principale ;
- l'utilisation d'une seule clé principale facilite l'utilisation de différentes clés pour sécuriser plusieurs éléments d'information ;
- seule la clé principale doit être traitée dans le HSM. Le cryptage et le décryptage ne doivent plus être effectués dans le HSM, ce qui signifie que le cryptage / décryptage en masse peut être réalisé plus rapidement.

Une hiérarchie plus approfondie de la gestion des clés est également possible : une clé principale sécurisée HSM sécurise une clé organisationnelle qui, à son tour, sécurise un certain nombre de clés de cryptage en masse qui sont utilisées dans toute l'organisation pour la protection des informations en masse.

Horodatage ('*Time stamping*')

La signature numérique s'accompagne d'un horodatage électronique. Les signatures numériques doivent tout d'abord être validées immédiatement après signature. Et ce, en raison d'une durée de validité limitée et du développement continu d'ordinateurs plus puissants. Cela rend les signatures numériques moins adaptées pour le long terme. Or, les factures numériques et autres documents d'archive, par exemple, nécessitent justement d'être validés à plus long terme.

La durée de validité d'une signature numérique dépend de la validité du certificat numérique utilisé. Si la validité dudit certificat est échuë, un message d'erreur apparaîtra à la signature numérique. Le certificat racine a lui aussi une validité à durée déterminée. Et une autorité de certification (AC) peut également cesser d'exister. Dans tous ces cas, il n'est plus possible de valider un document signé.

Pour éviter d'obtenir un message d'erreur, il faut combiner une signature électronique à un horodatage électronique. L'horodatage électronique prouve que le certificat était effectivement valable au moment de la signature. De cette manière, une signature numérique avec horodatage électronique ne sera jamais nulle. Cela permet aussi d'avoir une validation à long terme, même sans certificat valable, certificat racine valable ou AC active. L'horodatage électronique est également utilisé dans des techniques avancées de journalisation pour enregistrer la date et l'heure d'un événement de journalisation.

Il est essentiel d'utiliser une source fiable pour l'horodatage électronique. C'est pourquoi les horloges des serveurs sont souvent synchronisées avec une horloge fiable externe, par exemple une horloge atomique. Il est possible de s'inscrire à un service (AWS Amazon Time Sync Service, par exemple) qui fournit l'heure d'une telle horloge atomique et permet ainsi d'avoir des horloges internes fiables.

Les aspects de sécurité

Composants pour la confidentialité

Les messages et fichiers sont échangés de différentes façons via le ‘monde extérieur’ moins sûr :

- les utilisateurs finaux envoient des messages par e-mail sur Internet ;
- les utilisateurs finaux placent des fichiers sur des supports de stockage amovibles (clé USB, CD-ROM, DVD, carte SD...) qu’ils emportent avec eux hors de l’organisation ;
- des messages sont envoyés via des réseaux publics à un client peu fiable ou moyennement fiable, par exemple dans le cadre du télétravail ou du travail mobile ;
- lors de l’utilisation de connexions sans fil dans l’environnement de l’organisation, dont on suppose qu’elles sont aussi disponibles en dehors du bâtiment (comme le wifi) ;
- des messages sont échangés via des réseaux publics entre des systèmes de l’organisation à différents endroits ou avec ceux de partenaires fiables ;
- des messages et fichiers sont sauvegardés sur un portable (ordinateur portable, PDA, smartphone) qui est emporté hors de l’organisation.

Grâce au cryptage asymétrique, des entités qui communiquent peuvent s’envoyer des messages secrets sans devoir échanger au préalable des clés secrètes. De cette manière, vous pouvez en théorie crypter un message dans une communication en ligne à l’aide de la clé publique du destinataire. Le destinataire pourra décrypter le message crypté qu’il a reçu au moyen de la clé privée connexe. Mais dans la pratique, l’on fonctionne autrement car le cryptage asymétrique prend beaucoup de temps. À la place, l’on crypte le message avec une clé symétrique qui est à son tour cryptée avec la clé publique du destinataire. Ce dernier peut alors décrypter la clé symétrique avec sa clé privée et ainsi décrypter le message original à l’aide de la clé symétrique.

Le cryptage symétrique doit de préférence être transparent pour l’utilisateur final. Comme il a souvent lieu au niveau des connexions, réseaux et systèmes, c’est généralement le cas.

Lorsque le cryptage se déroule au niveau des applications, il faut la plupart du temps une interaction de l’utilisateur final. Citons comme exemples le cryptage d’e-mails et les logiciels distincts pour le cryptage de fichiers afin de sauvegarder ces fichiers sur des supports de stockage amovibles ou les envoyer en annexe d’e-mails. Le cryptage est au final aussi puissant que la mesure dans laquelle la clé cryptographique peut être gardée secrète pour les personnes non autorisées. Les facteurs suivants jouent un rôle crucial dans la force du cryptage :

- l’algorithme de cryptage ;
- la taille de la clé ;
- la distribution des clés ;
- la gestion du cycle de vie des clés.

Algorithme de cryptage et taille de la clé

L’algorithme de cryptage le plus courant et le plus robuste est AES. L’algorithme AES convient pour des tailles de clé de 128, 192 ou 256 bits. La taille et la qualité de la clé déterminent dans une large mesure le temps nécessaire pour ‘craquer’ le cryptage.

Distribution des clés

Pour la distribution des clés, on a souvent recours à des mécanismes de cryptage différents par clés. L'on distingue les clés de distribution et de gestion, ainsi que trois types de clés cryptographiques : les *Key Encryption Keys* (KEK) – ou clés de chiffrement de clés –, les clés séquentielles et les clés de session.

Propriété	<i>Key encryption key</i>	Clé séquentielle	Clé de session
But	Cryptage de la clé séquentielle ou de la clé de session	Cryptage symétrique des données sensibles	Cryptage symétrique des données sensibles
Catégorie	Clé publique ou clé secrète	Clé secrète	Clé secrète
Durée de vie	1 an	Période fixée	1 session
Distribution	Physique (carte à puce, CD-ROM, clé USB, papier) via une voie fiable	Sécurisée avec la KEK via la voie de communication elle-même ou via une autre voie moins sûre Physique via une voie fiable (pas de KEK)	Sécurisée avec la KEK via la voie de communication elle-même

Exemples de cryptage à des fins de confidentialité

- Cryptage d'e-mails : PGP, S/MIME
- Cryptage du trafic web : TLS
- VPN : IPsec
- Cryptage wifi : WPA, WPA2

Composants pour l'intégrité

Une fonction de hachage cryptographique, ou hachage, est un composant cryptographique qui assure l'intégrité. Bien que le hachage n'utilise pas de clés secrètes, il s'agit quand même de cryptage, à savoir du cryptage à sens unique.

Une fonction de hachage se base sur une donnée d'entrée – un message – de longueur arbitraire et génère un code – la valeur de hachage – qui est spécifique à ce message. Chaque modification du message entraîne une modification de la valeur de hachage. En outre, il n'est pas possible de constituer le message à partir d'une certaine valeur de hachage (« pas possible » signifie ici qu'il n'est pas arithmétiquement possible de le faire dans un délai raisonnable).

Une fonction de hachage peut garantir l'intégrité des informations à condition que la valeur de hachage soit correctement protégée contre toute manipulation. Ainsi, dans le contexte de DIM (*'Data in Motion'* = données en mouvement) par exemple, l'intégrité d'un message envoyé peut être démontrée en envoyant la valeur de hachage par un autre canal de communication ou en l'envoyant cryptée.

Les fonctions de hachage sont associées à des techniques de cryptage asymétrique pour créer une signature numérique (voir plus loin). Une signature numérique fournit les services de sécurité suivants : intégrité du message, authentification de l'expéditeur, authentification des données et irréfutabilité.

Un MAC (*Message Authentication Code* ou code d'authentification de message), parfois aussi appelé fonction de hachage chiffré, génère une valeur de hachage ou une valeur MAC sur la base d'une clé secrète. Outre l'intégrité du message, il y a une forme (limitée) d'authenticité des données (garanties sur la source du message envoyé). Il faut dans ce cas échanger la clé secrète au préalable.

Composants pour l'authentification

La signature numérique combinée à un certificat sert de base à l'authentification d'entités (personnes, équipements et organisations) en reliant la clé publique à une entité et en vérifiant son identité. Les techniques pour l'irréfutabilité et l'authentification vont donc de pair, à savoir qu'elles combinent la signature numérique et le certificat. La signature numérique associée à un certificat peut être comparée à une simple signature apposée à la main.

L'authentification au moyen d'un certificat fait partie des moyens d'authentification forts, à savoir l'authentification multifactorielle où au moins deux formes d'authentification sont imposées :

- quelque chose que vous connaissez, par exemple un mot de passe,
- quelque chose que vous possédez, par exemple un token, une clé USB ou un certificat,
- quelque chose que vous êtes (une caractéristique personnelle), par exemple une empreinte digitale ou une empreinte rétinienne.

La signature numérique doit répondre à une série d'exigences :

- la signature doit être unique pour pouvoir vérifier son auteur ;
- la signature doit permettre d'authentifier le contenu du message ;
- la signature doit pouvoir être contrôlée par des tiers afin de résoudre d'éventuels problèmes d'irréfutabilité.

Afin d'apporter les garanties nécessaires, une partie tierce devra apposer une sorte de cachet qui assure l'authenticité de la clé et permet de relier la clé à la bonne personne. Le passeport en est un exemple (de la vie réelle). Pour demander un passeport, il faut suivre une procédure définie par l'administration. Le passeport sert par exemple à prouver l'identité du voyageur lorsqu'il est à l'étranger.

L'on utilise souvent un certificat distinct pour l'authentification, l'intégrité et l'irréfutabilité. La carte d'identité électronique eID délivrée par l'administration fédérale belge fonctionne sur la base de deux certificats : un pour l'authentification (preuve au moyen d'une signature numérique) et un pour l'intégrité / l'irréfutabilité (au moyen d'une signature numérique légalement valable car qualifiée).

Les certificats numériques servent non seulement à authentifier des personnes, mais ils peuvent aussi être attribués à des sites web et des équipements, comme des serveurs, des routeurs, etc. Ils peuvent être divisés en deux catégories, les certificats de serveur et ceux de client :

1. un **certificat de serveur** est utilisé par un serveur, par exemple un serveur web, pour s'authentifier et pour créer une connexion cryptée entre le client et le serveur ;
2. un **certificat de client** est utilisé par un utilisateur final qui peut se servir de ce certificat pour s'authentifier à l'aide de ce certificat de client.

Pour être juridiquement valables en Belgique, les signatures numériques doivent respecter la loi du 21 juillet 2016, aussi appelée 'loi eIDAS et archivage électronique'. Cette loi transpose et met en œuvre le règlement européen eIDAS. Lorsqu'une signature numérique satisfait à certaines exigences, elle peut être « avancée » ou « qualifiée ».

Une signature numérique avancée :

- doit être liée au signataire de manière univoque ;
- doit permettre d'identifier le signataire ;

- a été créée à l'aide de données de création de signature numérique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ;
- est liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable (art. 26 du règlement eIDAS).

Une signature numérique est **qualifiée** si elle est avancée et qu'elle a été créée à l'aide d'un dispositif de création de signature numérique qualifié et qui repose sur un certificat qualifié de signature numérique.³ Les signatures électroniques qualifiées pour lesquelles un certificat qualifié a été utilisé, sont valables comme preuve et ont l'effet juridique équivalent à celui d'une signature manuscrite.⁴

Composants pour l'irréfutabilité

Un message peut être crypté au moyen de la clé privée et ensuite décrypté avec la clé publique connexe. C'est donc l'opération inverse du cryptage pour la confidentialité.

Vu que la clé privée est gardée secrète par son propriétaire, c'est sur le cryptage avec une clé privée que repose une signature numérique – c'est l'utilisation la plus connue de la cryptographie asymétrique. Comme seul le propriétaire dispose de la clé privée, il ne peut pas nier qu'il a crypté le message. L'irréfutabilité des données est donc garantie.

Si l'on combine la technique de cryptage asymétrique et l'utilisation d'un *message digest/hash* (empreinte numérique), l'on peut également garantir l'intégrité du message. Avant de crypter le message avec la clé privée, celui-ci est d'abord comprimé par une fonction de hachage cryptographique.

Une signature numérique peut être associée à un cryptage asymétrique afin de garantir la confidentialité des informations. Pour ce faire, il faut que :

1. l'expéditeur / le signataire appose sa signature numérique sur le document avec sa propre clé privée ;
2. l'ensemble (le document + la signature) soit crypté avec la clé publique du destinataire afin de le rendre illisible pour des tiers. Dans la pratique, l'on utilisera généralement le cryptage symétrique pour cette dernière étape vu que cette technique est plus rapide.

Lors du transfert et du stockage, toute modification apportée aux messages qui est passée inaperçue (ou toute modification apportée par des personnes non autorisées) représente un risque. Le destinataire n'a aucune garantie que le message est intègre et qu'il provient de l'identité indiquée comme signataire du message (irréfutabilité).

³ art. 3, § 12 du règlement eIDAS

⁴ art. 25 du règlement eIDAS

Le placement d'une signature numérique peut être divisé en deux parties.

1. Fixer les caractéristiques uniques du message (dans un hachage).
2. Lier l'identité unique de l'expéditeur au hachage.

Le niveau d'assurance résultant de la méthode appliquée est fortement influencé par la nature et la qualité des algorithmes et méthodes qui sont appliqués. Il s'agit ici surtout :

- de chiffres aléatoires ;
- de l'unicité et de la longueur des clés et des codes d'accès ;
- des moyens et processus de délivrance de clés, de distribution et de sauvegarde ;
- de la qualification de la délivrance des certificats.

Le tableau ci-dessous reprend les liens qui existent entre le niveau d'assurance, les clés utilisées et la confiance dans l'expéditeur et le destinataire.

Niveau d'assurance	Modèle de clé	Qualité du processus	Confiance dans l'expéditeur et le destinataire
1 : Faible, durée de conservation incertaine	Symétrique	Clés partagées	Propre organisation ou partenaire
2 : Moyen, durée de conservation incertaine	Asymétrique	Service PKI ou PKI privée	Propre organisation ou partenaire
3 : Élevé, durée de conservation garantie	Asymétrique	PKI certifiée	Pouvoirs publics ou partie certifiée

Contexte :

DIU ('data in use')

Données en stockage temporaire

Les données sensibles comme les mots de passe et les codes PIN sont cryptées au niveau des systèmes ou des applications. Cela permet de garantir que les valeurs de ces données seront uniquement lisibles pour les processus autorisés.

DIM ('data in motion')

Cryptage au niveau des applications

Ici, le cryptage est effectué par deux systèmes *end-to-end* communiquant entre eux. Seul le champ de données d'un ensemble est crypté. La technique de *secure HTTP*, qui est utilisée pour le cryptage des messages HTTP, est une forme bien connue de cryptage au niveau des applications.

Cryptage au niveau des sessions

Un exemple de cryptage au niveau des sessions est *Transport Layer Security* (TLS). Cette technique est utilisée avec des protocoles d'application tels que HTTP(s), FTP(s), IMAP(s), POP(s) et SMTP(s), reconnaissables par le S. Si TLS est appliqué à (HTTP), la communication web est cryptée (HTTPs) par session et une icône de cadenas verrouillé apparaît dans la barre d'état du navigateur.

Cryptage au niveau des réseaux

Un exemple de cryptage au niveau des réseaux est IPsec. Sur la base de ce protocole, des tunnels de communication cryptés sont mis en place entre les points d'extrémité du réseau, permettant ainsi une communication sécurisée. Ces tunnels peuvent servir à construire des *Virtual Private Networks* (VPN) – ou réseaux privés virtuels. Les réseaux sans fil sont cryptés avec des protocoles propres comme WPA (*Wi-Fi Protected Access*).

Le cryptage se termine au composant du réseau et n'est donc pas *end-to-end*. Si le point d'extrémité est un serveur proxy par exemple, la communication est alors cryptée jusqu'au serveur proxy, mais continue ensuite en texte clair jusqu'au PC de l'utilisateur.

Cryptage au niveau des liaisons de données

Le cryptage a lieu au 'niveau le plus bas' du réseau et est effectué entre deux nœuds de réseau. Toutes les données qui sont échangées – et donc y compris les informations de protocole – sont cryptées. Un exemple de cryptage d'une liaison de données est le protocole PPTP.

DAR ('data at rest')

Données stockées

Le cryptage d'informations sur des supports de données s'effectue sur trois niveaux :

1. Cryptage au niveau du stockage ('*storage*'), supports fixes et mobiles :
 - cryptage de supports de stockage mobiles, comme des disques durs d'ordinateurs portables, clés USB, CD-ROM, bandes ou modules de mémoire enfichables, mais aussi dans des mémoires de PDA et smartphones ;
 - cryptage de supports de stockage fixes, comme des matrices de disques durs de bases de données, bandes et supports optiques.
2. Cryptage au niveau des bases de données.
3. Cryptage au niveau des applications.

7.2. Logging

Le logging consiste à rassembler et tenir à jour l'information afin de détecter les activités système et utilisateur et les associer à des événements ('*events*'). Cette information est à son tour utilisée pour un suivi pertinent et sert d'input de contrôle pour la sécurisation et la gestion des risques. En utilisant les bons outils et les bonnes procédures, les journaux d'audit peuvent contribuer à détecter les violations en termes de sécurité de l'information et de l'ICT, les problèmes techniques et les situations de non-conformité aux lignes stratégiques.

Le monitoring va encore plus loin en assurant un suivi en temps (presque) réel des événements.

Le logging comprend les éléments suivants, classés par ordre de complexité :

- Journaux de bord (*logbooks*) manuels,
- Journaux d'audit (*audit logs*) automatisés,
- Pistes d'audit (*audit trails*).

Le logging manuel consiste à tenir à jour manuellement les activités et leur enregistrement dans un journal de bord. Cette méthode est la plus sensible aux erreurs, irrégularités et oublis d'activités. Le logging manuel est en effet basé sur la discipline et la capacité de l'exécutant. Le journal de bord du visiteur est un bon exemple de journalisation manuelle.

On reconnaît plusieurs journaux d'audit automatisés :

- Les journaux techniques ou journaux système : on y enregistre les événements (*events*) tels que l'utilisation de fonctions de gestion techniques et fonctionnelles, des activités liées à la gestion de la sécurité, les perturbations et les incidents (de sécurité).
- Journaux application : ils rassemblent les événements d'une application tels que les messages, exceptions et erreurs. Le format et le contenu de ces journaux sont déterminés durant la phase de design d'une application.

Le traitement de l'information du journal, toujours par ordre de complexité, comporte :

- L'analyse des loggings d'audit, de préférence à l'aide d'outils de filtrage,
- La corrélation de divers journaux d'audit, avec des sources externes ou non,
- le monitoring sécurité (en temps réel),
- le monitoring des informations et événements de sécurité : *Security incident & event monitoring* (SIEM).

Le logging en tant que mesure

Un journal d'audit est une compilation d'enregistrements chronologiques (un fichier plat, un fichier structuré, une base de données ou un journal de bord physique). Cette compilation apporte la preuve d'une activité ou d'un ensemble d'activités dans un traitement, une procédure ou un événement.

Une piste d'audit est une compilation sécurisée et automatisée d'enregistrements chronologiques. Cette compilation (un fichier plat, un fichier structuré, une base de données ou un journal de bord physique) permet de reconstituer une série d'événements selon le moment de leur survenance et en lien avec la création, la modification et la suppression d'enregistrements électroniques. Grâce à cette structure, l'information d'audit est plus accessible et plus facile à défricher grâce à l'utilisation d'outils d'analyse.

Il existe de nombreux types de mécanismes différents pour le logging des composants qui peuvent survenir simultanément. Exemples de ces mécanismes :

- SYSLOG est un standard de journalisation informatique. Le logging est scindé entre les systèmes qui génèrent le logging et les systèmes qui enregistrent le logging.
- SNMP signifie *Simple Network Management Protocol*. Ce protocole peut être utilisé pour gérer les appareils en réseau. Le protocole prévoit aussi des messages de statut (*traps*).
- Le journal *Windows Event* est présent par défaut dans les systèmes d'exploitation Windows et peut également être envoyé à un dispositif de journalisation centralisé.
- Les fichiers journaux individuels tels que les fichiers texte, les fichiers à valeurs séparées par des virgules (CSV) et autres variantes.
- À partir des applications et dans les bases de données, le logging se fait souvent dans la base de données même ou une base de données séparée. Cette journalisation est généralement structurée et doit être envoyée à un système de journalisation central.
- Le logging des systèmes de sécurité, tel que *Intrusion Detection Systems*.

Afin de pouvoir détecter efficacement les attaques, il est important d'enregistrer l'information de le logging en un point central unique, ce qui permet d'avoir une vue d'ensemble sur toutes les informations provenant de différents composants.

Les avantages du logging centralisé sont :

- La facilité d'utilisation : il ne faut regarder qu'en un seul endroit.
- La disponibilité : le logging est disponible, même si le système qui la réalise n'est pas disponible.
- La sécurité : le logging est aussi disponible lorsque le système-source a été piraté ou infecté.
- La sécurité : le logging peut être protégé contre les consultations et les modifications non autorisées, par exemple par une signature numérique.
- La simplicité : un journalisation centrale est plus simple à sécuriser sur un back-up par exemple.
- L'analyse automatique des fichiers journaux reflète plus rapidement la cohérence des incidents et permet de détecter des liens logiques entre des incidents isolés.

Mais le logging localisé reste intéressant. Elle permet en effet de garantir la cohérence et la consistance des informations du logging. Les informations du journal doivent alors être conservées jusqu'à l'obtention d'une confirmation de bonne réception des informations du journal par le système de stockage central.

Événements auditable

Il s'agit ici des activités identifiées pour le logging :

- succès et échec de la connexion,
- succès et échec de l'authentification,
- succès et échec dans l'autorisation,
- succès et échec dans l'exécution des activités privilégiées,
- succès et échec dans l'accès aux fichiers, dossiers, applications et outils système,
- succès et échec dans l'accès aux fonctions de gestion fonctionnelles et techniques,
- création, modification, suppression de comptes, fichiers, dossiers,
- création, modification, suppression de paramètres système (y compris base de données),
- création, modification, suppression dans les polices,
- création, modification, suppression dans les paramètres d'accès tels que les droits et privilèges,
- activités système et application telles que la fermeture, le redémarrage, les erreurs,
- modifications aux systèmes et applications.

Il faut par ailleurs définir les seuils nécessaires (*thresholds*) avec lesquels on détermine à partir de quelle limite un événement auditable est considéré comme un incident (potentiel).

Contenu des enregistrements d'audit (*audit records*)

Les enregistrements d'audit doivent comprendre suffisamment d'informations pour montrer quel événement a eu lieu, quelle en est la cause et quelles en sont les conséquences. Par ailleurs, il doit être possible d'identifier chaque intervention humaine liée à un événement.

Un journal correctement mis en œuvre doit pouvoir apporter une réponse aux questions suivantes :

- Que s'est-il passé ?
- Quand cela s'est-il produit ?
- Où cela s'est-il produit ?
- Qui était concerné ?
- D'où cela vient-il ?

Concrètement, cela signifie pour la mise en place d'une piste d'audit réussie :

- la date et l'heure,
- le nom d'utilisateur / domaine, réductible à une personne, un système, un lieu,
- la source IP ou application,
- l'application, l'URL ou le service utilisé(e)
- le module ou la fonction utilisé(e),
- l'action exécutée (création, modification, consultation, suppression),
- le champ de données modifié ou consulté.

Le monitoring en tant que mesure

Le monitoring sécurité consiste à compiler et analyser les informations afin de détecter les comportements suspects ou les accès et activités non autorisés, à générer des alarmes appropriées et à prendre des actions.

Le système SIEM constitue une forme particulière de monitoring sécurité : il s'agit ici de consulter différentes sources et, sur la base de ces informations et de leurs corrélations, de détecter les comportements suspects ou les accès et activités non autorisés, de générer des alarmes appropriées et de prendre des actions.

Ces mesures se distinguent du logging par le besoin d'outils et de connaissances spécialisés pour pouvoir mettre en œuvre le monitoring. Elles sont donc en tant que telles prévues comme mesures après l'analyse des risques.

Monitoring sécurité

Le monitoring sécurité est une conjonction de personnes, de processus et de techniques. Il faut de la technique pour rendre visible ce qui se passe en termes de sécurité de l'information. Il faut ensuite des analystes pour analyser les événements et leur réserver un suivi.

C'est en principe une analyse de risques qui détermine ce qui est précisément suivi par le monitoring sécurité. Cette analyse de risques permet de déterminer quels actifs sont critiques ou moins critiques. On peut, sur cette base, définir quels journaux ou quelles alarmes peuvent fournir des informations pertinentes sur ces actifs. Une fois l'analyse de risques terminée, on peut attribuer une qualification aux actifs et déterminer ce qui est permis

ou non à propos de ces actifs. Les journaux et les alarmes liés à ces actifs et ces mesures fournissent des informations pertinentes sur les événements qui ont lieu en lien avec ces actifs. Une compilation de mesures et d'actifs peut par exemple être : un *active directory*, un pare-feu, un système de détection des intrusions, le logiciel antivirus et le logging des actifs concernés.

Le monitoring sécurité consiste aussi à compiler, analyser et suivre les informations pertinentes. Cela permet de tenir à l'œil les vulnérabilités, les activités suspectes et les incidents de sécurité potentiels et effectifs, et de prendre des actions là où elles s'avèrent nécessaires. Il est possible également d'analyser et de rapporter des tendances afin d'identifier et de planifier des actions préventives.

SIEM

Une solution SIEM offre la possibilité d'utiliser des informations provenant d'autres sources, comme par exemple les journaux AD et e-mail, les journaux de périmètre de sécurité, etc. Ces informations sont utilisées pour détecter les incidents de sécurité. Extraire les incidents depuis les journaux de façon automatisée, c'est ce que promettent de faire les systèmes SIEM.

Une solution SIEM prévoit des loggings de bord continus et un monitoring en temps réel des mesures de sécurité et des alarmes causées par un comportement déviant. Par ailleurs, il y a également un enregistrement à long terme des informations des loggings et des analyses historiques/de tendances, en lien avec la gestion des incidents et la recherche légale (*forensics*).

SIEM se compose de plusieurs solutions de sécurité :

- Gestion des loggings (*log management*) : compilation et enregistrement des informations des loggings des systèmes et applications ;
- Gestion des événements de sécurité (*Security Event Management - SEM*) : monitoring en temps réel des événements en matière de sécurité de l'information ;
- Gestion de l'information de sécurité (*Security Information Management - SIM*) : enregistrement de l'information, analyse et rapportage ;
- Corrélation des événements de sécurité (*Security Event Correlation - SEC*) : corrélation des informations collectées.

Les informations sont collectées à partir de différents systèmes sources et traités par la solution SIEM :

- Des enregistrements d'audit sont collectés à partir de différents systèmes sources,
- Les enregistrements d'audit sont transposés dans un format déterminé pour traitement ultérieur,
- L'information est enrichie à partir d'autres sources (par ex. AD pour lier des comptes à des informations utilisateur comme le nom, le département, l'emplacement, ...),
- Les informations sont agrégées et mises en corrélation, Analyse et rapportage.

La mise en œuvre d'un SIEM présente la meilleure valeur ajoutée lorsque deux conditions sont remplies :

- Il doit y avoir une solide base de journalisation,
- Il faut avoir développé de bons cas d'utilisation (*use cases*).

7.3. Mesures IAM

L'identification en tant que mesure

Les processus d'identification sont des processus qui sont chargés de définir l'identité d'une personne. À titre d'exemple, la saisie du nom d'utilisateur pour identifier une personne par rapport à un ordinateur, ou l'envoi de l'adresse réseau de l'expéditeur d'un message électronique pour faire connaître l'identité de l'expéditeur à l'ordinateur récepteur.

Les processus d'identification peuvent être subdivisés en deux grands groupes sur la base des caractéristiques : identification faible ou forte.

Identification faible

La validation de l'identité d'une personne physique se fera sur la base d'un attribut d'identité qui ne relève pas du contrôle d'une source certifiée ou enregistrée par l'autorité. Il peut s'agir d'une adresse mail, d'un numéro de téléphone, etc. Les attributs d'identité utilisés proviennent généralement d'une organisation commerciale ou non. De cette manière, la procédure de vérification n'offre pas une garantie suffisante sur l'identité de l'individu concerné (risque d'usurpation d'identité ou *identity spoofing*).

Identification forte

L'identification se fera sur la base d'une source certifiée ou enregistrée par l'autorité fédérale belge (*Identity provider*). Aujourd'hui, seule l'autorité fédérale peut effectuer une validation forte d'une identité pour satisfaire aux caractéristiques d'une identification forte. Les labels d'identification unique d'une identité (personne physique) sont :

- Le numéro de registre national (NRN en abrégé)
- Le numéro BIS de registre national (numéro BIS)

L'identification d'identités étrangères

La compatibilité des identités des individus étrangers, au sein de l'UE également, est assurée par l'enregistrement de l'individu dans le Registre national BIS.

Sources dérivées reconnues pour une identification forte

L'autorité fédérale belge utilise une série de sources dérivées reconnues, telles que le NISS et ItsMe®.

L'authentification en tant que mesure

Il est cependant relativement facile de falsifier une identité. Il est donc nécessaire non seulement de déterminer l'identité, mais aussi de la vérifier. L'authentification, aussi appelée authentification de source, est la vérification de l'identité d'une personne. On utilise à cet effet une caractéristique unique, spécifiquement liée à l'identité qui est vérifiée.

Authentification de facteur

Qu'entend-on par facteurs ?

Dans l'authentification d'une personne, la caractéristique unique se compose d'une ou de plusieurs données liées à la personne (facteurs). Nous pouvons distinguer à cet égard les données suivantes, liées à la personne :

- Quelque chose que vous connaissez, un mot de passe ou un code PIN
- Quelque chose que vous avez, une carte bancaire ou une carte à puce
- Quelque chose que vous êtes, à savoir les données biométriques, comme votre empreinte digitale

Authentification à facteur simple

Dans sa forme la plus simple, nous utilisons l'authentification à facteur simple à peu près tous les jours, sous la forme d'un badge d'accès à notre bâtiment, mais aussi sous une forme plus sécurisée : notre accès à la station de travail en utilisant un identifiant et un mot de passe.

L'authentification à facteur simple se réfère à la manière unique qui permet de valider l'identité :

- Pour la validation de l'accès à un bâtiment, le système de contrôle d'accès ne validera que sur la base de quelque chose que détient l'utilisateur
- Pour l'accès à la station de travail au moyen d'un identifiant et d'un mot de passe, le contrôle ne sera validé que sur la base de quelque chose que l'utilisateur connaît.

Le problème dans l'utilisation de facteurs simples est que ceux-ci n'offrent pas toujours une garantie suffisante pour la vérification de l'identité. Afin de donner une meilleure garantie de protection de l'information, il est fortement conseillé de prendre au minimum des mesures supplémentaires permettant de réduire le risque d'abus.

Authentification multifactorielle

L'autorité fédérale belge met l'accent sur l'authentification multifactorielle.

Cette authentification à facteurs multiples est basée sur la validation d'une identité sur plusieurs facteurs en combinant ces facteurs dans le processus d'authentification. L'exemple le plus connu de l'application d'une authentification multifactorielle est la carte de crédit (quelque chose que vous avez) et le code pin correspondant (quelque chose que vous connaissez). Le processus d'authentification utilise ici deux facteurs pour constater l'identité d'un utilisateur.

L'un des concepts intéressants de cette authentification multifactorielle est que les deux facteurs sont indépendants l'un de l'autre. L'identifiant et le mot de passe se trouvent tous deux dans la même classe de facteurs (quelque chose que vous connaissez) et ne sont donc pas considérés comme facteurs multiples.

- L'authentification à double facteur est basée sur plusieurs facteurs.

- L'authentification à deux étapes se base sur deux étapes d'authentification à exécuter, avec un facteur similaire (par ex. deux fois quelque chose que l'on 'connaît').

L'authentification à double facteur est donc toujours une authentification à deux étapes (car il s'agit de deux étapes distinctes), mais à l'inverse, l'authentification à deux étapes n'est pas toujours une authentification à double facteur (car il est possible de n'utiliser qu'un seul facteur pour les deux étapes).

De l'identité au compte (*account*)

Pour prouver l'identité d'un individu, vous avez avant tout besoin d'une source authentique, un processus d'enregistrement d'identité fiable et contrôlé qui permet d'enregistrer l'identité d'un individu.

Les identités sont centralisées dans le registre national et le registre national BIS de l'autorité fédérale belge mais ces identités ne sont pas directement utilisables comme moyen d'authentification. Un utilisateur ne peut pas simplement se référer à ce processus d'enregistrement pour prouver son identité. C'est pourquoi l'individu reçoit un 'moyen', qui est reconnu en tant que tel comme référence d'identité par tout un chacun et par toute organisation. Il s'agit en l'occurrence d'une preuve d'identité (y compris les passeports, les certificats de naissance, ...). La carte d'identité belge (eID) est le moyen de référence pour le citoyen. Son utilisation comme moyen d'authentification est cependant limitée en ce qui concerne l'identification interactive entre des personnes physiques et l'interaction avec les services CSAM fédéraux.

Afin de supprimer les limites d'utilisation de notre preuve d'identité, l'autorité fédérale utilise un système de gestion d'accès, qui permet d'associer des moyens d'authentification adaptés à une identité, afin que l'utilisateur puisse avoir accès, de manière adéquate, aux applications et aux services. Ce moyen d'authentification s'appelle un compte (*account*). Le compte a toujours un lien avec l'identité d'une personne physique.

La forme sous laquelle un compte se présente dépend entièrement de la technologie utilisée. L'eID belge supporte à la fois les formes d'authentification électronique et les formes d'authentification physique.

Cycle de vie (*lifecycle*) d'un compte

Un cycle de vie décrit tous les processus, critères et objectifs de l'objet concerné, dans le cas présent l'objet compte.

Création de comptes

La création d'un compte est déterminée sur la base de la motivation présente d'un individu pour obtenir un accès. Il s'ensuit que les personnes qui ne sont pas censées avoir un accès aux services ou à l'information ne peuvent pas disposer d'un compte (actif).

Statut d'un compte

Un compte est actif lorsque, techniquement, il offre la possibilité d'être utilisé comme moyen d'authentification. Les critères pour considérer un compte actif dépendent de la forme dans laquelle le compte a été fourni. Un compte est cependant inactif lorsqu'il a été exclu comme compte actif sur la base de critères.

Mesure de contrôle

Après avoir fait l'inventaire de tous les comptes existants, en ce compris le type et la catégorie correspondante avec les indicateurs suivants, on peut contrôler les comptes :

- Compte dormant : le compte n'est plus motivé s'il n'a plus été utilisé au cours des 13 derniers mois. Le statut actif ou inactif n'a pas d'influence sur la situation 'dormante' du compte
- Compte non motivé : le compte n'est pas associé à une identité validée d'une personne physique.
 - Les applications et les systèmes peuvent aussi, techniquement parlant, être utilisés comme identités. Dans le contexte IAM, nous associons cependant toujours des comptes à une personne physique.
 - Il est autorisé de faire des associations via une application derrière laquelle un lien indirect se fait avec une personne physique, sous la forme d'un 'gestionnaire d'application'.
 - Compte inactif : le compte n'est techniquement pas en état de participer à un processus d'authentification.
 - Un compte peut par exemple être temporairement bloqué ou utilisé pendant certaines heures seulement (par ex. les heures de bureau).
 - Compte non contrôlé : le compte ne répond pas aux exigences techniques minimales de la politique de mots de passe attribuée au type ou à la catégorie de compte.
 - Âge du mot de passe
 - Complexité du mot de passe
 - Cryptage réversible du mot de passe
 - Pas de mot de passe
 - ...

Provisionnement (*provisioning*)

Le provisionnement est le sous-processus utilisé pour toutes les activités qui mènent à la fourniture d'un compte à une personne identifiée. Selon la mise en œuvre du processus, les comptes sont fournis au statut actif ou inactif à la personne légitime. Lors de la fourniture de comptes inactifs, le processus de provisionnement génère un (sous-)processus d'activation autorisé et documenté.

Déprovisionnement (*de-provisioning*)

Le déprovisionnement est le sous-processus qui fait qu'un compte n'est plus disponible pour un utilisateur final comme moyen d'authentification utilisable.

- Selon la forme du moyen d'authentification et/ou la méthodologie de déprovisionnement, on parle de suppression, désactivation (blocage), refus (*revoke*), ...

Le déprovisionnement peut être réalisé en une ou plusieurs étapes. Les processus de déprovisionnement par phases sont toujours supportés par des besoins identifiés dans le processus de cycle de vie du compte.

- Désactiver temporairement ou non un compte, avant de le supprimer effectivement, dépend du besoin de réactivation ultérieure de ce compte.
- Si des comptes ne peuvent pas être supprimés effectivement en vertu d'une réglementation identifiée, ce besoin sera explicitement repris dans la documentation descriptive du processus.

Fiabilité du processus d'authentification

Les mesures prises dans le processus d'enregistrement du compte sont élargies à une série de mesures techniques qui doivent empêcher la duplication et l'usage abusif d'un compte. On parle des degrés de confidentialité de l'authentification.

Plusieurs accords ont été conclus au plan européen concernant ces degrés de confidentialité de l'authentification. Les degrés de confidentialité de l'authentification eID.AS permettent à des plateformes d'authentification des États membres européens individuels d'indiquer de manière uniforme et standardisée quelles exigences elles posent en termes de qualité pour la confidentialité d'une demande d'authentification.

Ces degrés de confidentialité sont subdivisés en 3 échelles eID.AS LoA.

- '*High*' : confidentialité élevée du processus d'authentification, ou authentification forte
- '*Substantial*' : confidentialité substantielle du processus d'authentification, ou authentification fiable
- '*Low*' : confidentialité basse du processus d'authentification, ou authentification faible

Dans ce document, nous n'irons pas dans le détail des degrés de confidentialité de l'authentification eID.AS.

L'autorisation en tant que mesure

L'autorisation est l'octroi de droits à des personnes et aux processus initiés pour ces personnes. Ces droits donnent à la personne accès à certaines données et fonctions. Concrètement, il s'agit de l'autorisation d'utiliser un service ou une application. On fait une distinction entre :

- La gestion des accès (le processus) en tant que mesure organisationnelle.
- Le contrôle d'accès (la technique) en tant que mesure technique.
- La séparation des fonctions (le principe) en tant que mesure de contrôle organisationnelle.

La gestion des accès en tant que mesure

L'autorisation est basée sur les profils d'accès, qui précisent quelles personnes ont accès à quelles données et fonctions. Il s'agit donc ici d'une mesure organisationnelle qui repose sur une politique d'accès. Ce processus explique comment et dans quelles circonstances un individu obtient un accès aux moyens organisationnels. Les attributs suivants sont présents dans la gestion des accès pour garantir un processus auditable :

Information disponible lors du traitement d'un accès

- Attributs de base de la demande d'accès (date, heure, demandeur, numéro, ...)
- Sujet, comme référence à l'individu qui souhaite avoir l'accès
- Motivation de la demande et confirmation de la motivation
- Attributs de base de la validation de l'accès (date, heure, ...)
- Identité de la personne qui donne la ou les approbation(s)
- Échéance du droit d'accès, selon la catégorie de l'information traitée dans le service ou l'application
- (Re)validation périodique répétée d'un droit, selon la catégorie de l'information traitée dans le service ou l'application.

Le contrôle d'accès en tant que mesure

Le contrôle d'accès est un ensemble de mesures techniques qui reposent sur les spécifications techniques de la technologie appliquée. Lors de la connexion à une application ou un service, l'identité (l'authentification) sera validée, où le traitement technique de la demande de validation dépend de la technologie utilisée. Selon la méthode utilisée, la même plateforme d'authentification déterminera quelles autorisations sont accordées à l'individu concerné (sur la base de son compte ou droit associé).

Exemple(s) de plateformes d'authentification :

- L'authentification LDAP ne valide que le compte. Une application fera toujours, par code, une validation supplémentaire pour valider une adhésion de groupe.
- Une ACL (*Access Control List*) sur un fichier, un dossier ou un disque sera validée par le sous-système disque sur la base de l'ACE (*Access Control Entry*) sur l'objet concerné.

La mesure de contrôle d'accès doit cependant être en ligne avec le besoin d'accès du rôle spécifique, jusqu'à l'information traitée. Nous suggérons de suivre le principe de '*least access privilege*' et de scinder les accès pour les utilisateurs finaux des accès de gestion.

La séparation des fonctions en tant que mesure

La séparation des fonctions est une mesure de contrôle organisationnelle. Elle implémente un niveau adéquat de séparation des droits comme principe de sécurité. On va alors répartir les tâches et les droits correspondants pour un processus d'entreprise particulier sur plusieurs organisations, rôles, individus et/ou comptes.

Il y a plusieurs approches dans la séparation des fonctions :

- La séparation séquentielle (deux signatures en principe)
- La séparation individuelle (principe des quatre yeux)
- La séparation spatiale (droits distincts sur des comptes séparés)
- La séparation de faculté (plusieurs facteurs contribuent à l'accomplissement)

Quelques exemples dans la pratique :

- Gestion séparée des clés et mise en œuvre du cryptage
- Comptes séparés pour l'utilisateur final, accès application et gestion des comptes
- Rôles séparés gestion d'accès, demandes d'accès et (re)validation

7.4. La mesure de sécurité de l'information PAM

PAM ou '*Privileged Access Management*' est une application stricte et le suivi d'une série de processus de base. Ce document soulignera l'importance des différents processus pour le processus PAM. Il s'agit des processus de base suivants :

- Gestion des modifications dans le traitement de l'information ou '*Change management*'
- Gestion des configurations dans le traitement de l'information ou '*Configuration management*'
 - La gestion des configurations comprend aussi, outre la configuration du traitement de l'information, tous les détails des possibilités d'accès au traitement de l'information
- Identité et gestion des accès ou '*Identity & Access Management*' (IAM)
- Gestion du logging (*log management*)
- Gestion de risques (*risk management*) sur la base du rapportage de risques opérationnels sur la base d'informations historiques des processus ci-dessous ou de la gestion de risques opérationnels (*operational risk management - ORM*).

La gestion du changement (*change management*) en tant que mesure

Le processus de gestion du changement remplit les critères 'Motivation' et 'Approbation', qui sont importants pour le processus 'PAM'.

Le processus de gestion du changement rassemble tous les éléments des besoins à la fois organisationnels et techniques. Par ailleurs, ce processus motive le besoin d'accès privilégié aux composants techniques. Éventuellement, il peut s'agir aussi de l'accès à l'information traitée durant les tâches de gestion. Ce processus fournit donc la validation et l'autorisation nécessaires pour accompagner ces activités de gestion.

Concrètement, ce processus nous aide à préciser le qui/quand/pourquoi pour toute demande d'accès privilégié à un composant de traitement d'information, et qui a donné la ou les autorisation(s) nécessaire(s) et quand.

Identity & Access Management en tant que mesure

Le processus *Identity & Access Management* remplit les critères suivants, qui sont importants pour le processus 'PAM' :

- Gestion de l'Identité : identifie chaque personne physique qui participe à un processus PAM
- Gestion de l'accès :
 - contribue aux besoins en matière d'authentification.
 - contribue aux besoins pour la gestion d'accès.

La configuration de mesures sur le composant technique (contrôle d'accès) est assurée via le processus de gestion de configuration. L'implémentation '*least access*' se fait sur la base de comptes et des rôles associés.

La gestion de la configuration en tant que mesure

Le processus de gestion de la configuration contrôle l'implémentation de paramètres et comprend notamment :

- Les contrôles d'accès, présents dans une bonne gestion des accès :
 - Quelles sont les attentes fonctionnelles remplies par les contrôles d'accès concernés (le principe de '*least access*' est une nécessité) ?
 - Comment les différents rôles d'accès sont-ils élaborés techniquement ?
 - Comment l'implémentation de ces contrôles d'accès est-elle contrôlée ?
 - ...
- La configuration des loggings est utilisée comme élément de base dans le contexte de l'auditabilité du traitement de l'information opérationnel :
 - Quelles sont les attentes fonctionnelles remplies par la configuration des loggings concernée ?
 - Comment cette configuration est-elle élaborée techniquement ?
 - Suivi opérationnel sur la base de rapports ?
 - Suivi opérationnel sur la base d'alertes (possible en temps réel) ?
 - Quelles corrélations, interprétations de l'information de journalisation aboutissent à un contrôle démontrable ?

La gestion des loggings en tant que mesure

La gestion des loggings rassemble du matériel source, venant de sources à la fois techniques et opérationnelles. Ce matériel source sera alors utilisé pour permettre les mesures de contrôle nécessaires.

- Cela permet de combiner des informations des loggings de différentes sources afin d'avoir une vue sur les risques opérationnels (gestion des risques).
- Cela permet, en cas d'incident dans le traitement de l'information, de procéder à une reconstruction des activités de traitement.
- ...

Nous faisons la distinction entre les sources suivantes comme informations des loggings (l'énumération de mesures ci-dessous ne se limite pas à ces exemples) :

- Sources techniques
 - Le processus de gestion de la configuration garantit les bons paramètres de la configuration des loggings.
 - Les entrées de journaux dans les fichiers ou les bases de données provenant de systèmes, *middleware* et applications (par ex. *Security log Windows*)
 - Le contrôle automatisé (*4EYES*) des activités de gestion (*Session recording*) (les contrôles non automatisés sont considérés comme des mesures de contrôle organisationnelles)
 - Cela comprend également la garantie de la disponibilité de ces informations au moyen de l'archivage ou la rétention (élaboration technique du contrôle *4EYES*)
- Sources organisationnelles
- Gestion des changements : journal opérationnel de tous les enregistrements de changements dans le processus ou l'outil de gestion des changements
- Suivi opérationnel des activités : enregistrement de toutes les activités exécutées manuellement par une personne physique indépendante, dans le cadre d'une session de gestion
 - Ces journaux 'physiques' sont enregistrés et archivés conformément aux besoins d'un système automatisé à des fins d'audit potentiel.
- ...

Il est conseillé d'optimiser le traitement de la mesure de contrôle au moyen de la collecte automatique des loggings.

La gestion des risques en tant que mesure

Cette mesure est une partie de la gestion opérationnelle des risques liée au traitement de l'information. Le rapportage et le suivi opérationnel de ces rapports sont une source de preuves importante. L'organisation démontre ainsi qu'il y a un suivi effectif des activités de traitement de l'information et que toutes les mesures prises aboutissent à une limitation correcte des autres risques.

Rapportage opérationnel de base de la gestion des risques, utilisé dans PAM

Le rapportage type ci-dessous est présent dans le contexte générique du traitement de l'information et n'est pas spécifiquement repris dans le contexte PAM

- Disponibilité des sources (output de la gestion des loggings)
- Garantir la disponibilité des sources nécessaires, ces sources sont nécessaires pour garantir le rapportage et le suivi
- Interprétations d'informations techniques de journaux sur la base de critères techniques - Exemple : tentatives ratées de mot de passe, *lock-out* du compte, comptes dormants, réinitialisation du mot de passe, ...
- Interprétations d'informations organisationnelles de journaux sur la base de critères organisationnels - Exemple : validation du *workflow* par des non autorisés
- ...

Rapportage en fonction de PAM

Anomalies de processus

- Les anomalies de processus sont détectées sur la base des corrélations d'informations provenant de différents processus ou de leurs plateformes techniques de support.

Anomalies de configuration

- Les anomalies de configuration sont détectées sur la base des corrélations d'informations du processus PAM et du journal technique des composants du traitement de l'information.

7.5. Types de données pour la protection des données à caractère personnel

Types de données de la catégorie d'information 0



Aucun type de données courantes n'a été relié à des données à caractère personnel identifiées dans la catégorie d'information 0.

Types de données de la catégorie d'information 1



Données de contact

Cette catégorie de données à caractère personnel comprend uniquement des informations qui permettent de prendre contact avec un individu dans un contexte professionnel. Ces informations de contact se limitent à la relation directe et unique avec l'Autorité flamande.

- Nom et Prénom
- Adresse professionnelle (Bâtiment, rue, numéro, boîte, code postal et commune)
- L'organisation pour laquelle l'individu exerce son activité professionnelle
- La fonction au sein de l'organisation
- Numéro de téléphone (ligne fixe). Il n'y a pas de distinction opérée sur la base de la technologie (analogique/numérique) (y compris SolIP/VoIP/ToIP/Téléphonie mobile/Fax)
- Adresse e-mail
- Photo de contact
- Références de contact professionnelles (personnelles) sur les réseaux sociaux (Facebook, Google+, LinkedIn)

Types de données de la catégorie d'information 2



Coordonnées personnelles

Cette catégorie de données à caractère personnel comprend uniquement des informations, exclues par la catégorie 1, qui permettent de prendre contact avec un individu.

- Nom et Prénom
- Données d'adresse
(Bâtiment, rue, numéro, boîte, code postal et commune)
- Références de téléphonie : ligne fixe, GSM, fax
(y compris SoIP/VoIP)
- Adresse e-mail
- Références de contact personnelles sur les réseaux sociaux
(Facebook, Google+, LinkedIn)

Données d'identification

Cette catégorie de données à caractère personnel comprend uniquement des informations qui permettent d'identifier un individu de manière unique.

- Données d'identification émises par les services publics : numéro de carte d'identité, numéro de passeport, VoID, numéro de permis de conduire, numéro de pension, plaque minéralogique véhicule(s) personnel(s)
- Données d'identification émises par l'employeur : numéro du personnel
- Noms de comptes techniques, indépendamment de la forme dans laquelle ils apparaissent : numéro de badge, UserID, adresse mail, numéro de téléphone, ...
- Données d'identification électronique : adresses MAC, adresses IP, cookies et clés d'identification uniques d'appareils

Caractéristiques personnelles

Ce type de données comprend les caractéristiques personnelles de l'individu :

- Sexe, date de naissance et de décès et informations connexes
- Lieu de naissance et nationalité
- État civil

Habitudes de consommation

Cette catégorie de données à caractère personnel comprend les informations relatives à la consommation de biens et de services, proposés par l'administration fédérale.

- Demandes de prix personnelles, offres, commandes, factures, tickets d'achats et tickets
- Logging de l'utilisation des applications de l'administration fédérale.

Caractéristiques de l'habitation

Informations et caractéristiques liées aux propriétaires, aux habitants, aux informations fiscales y afférentes et aux caractéristiques physiques du bâtiment.

- Données de base cadastrales : adresse, nature de l'habitation
- Caractéristiques fiscales, dont le revenu cadastral
- Certificats de performance énergétique
- Âge de l'habitation
- Identité du propriétaire
- Durée du statut de séjour en relation avec l'habitation
- Personnes ayant accès à des bâtiments privés
- Relation d'utilisation des habitants (location / ... / achat)
- Type d'habitation (maison mitoyenne / ... / maison individuelle)
- État d'entretien (bon/mauvais/rénové)
- Caractéristiques physiques (taille du bâtiment / espaces intérieurs / plan)
- Activités administratives ouvertes

Études, expérience et formation

- Intérêt, information et caractéristiques de la formation et formation en relation avec un individu
- Carrière académique, aperçu des écoles concernées, établissements académiques et universités
- Aperçu des diplômes obtenus et aptitudes professionnelles et licences
- Attestations d'expérience (professionnelle et intérêts)
- Adhésion à des organisations professionnelles et fonctions exercées
- Publications
- Formation interne (à la fonction)

Profession et poste

- Emplois et professions actuels et historiques
- Relation actuelle historique à l'employeur, à savoir employeur, titre professionnel, description de fonction, fonctions exercées, grade, détails de l'engagement, lieu de travail, spécialisation et type d'entreprise
- Situation militaire
- Intérêt, information et caractéristiques de la profession et relations aux employeurs par rapport à un individu
- Mandats publics
- Toutes les autorités, communes, provinces, régions et fédéral
- Participation à des comités publics
- Participation à des groupes de travail et des groupes de réflexion

Loisirs et intérêts

Cette catégorie de données à caractère personnel comprend uniquement des informations qui permettent d'identifier les loisirs et intérêts de l'individu.

- Adhésion à une association sans connotation raciale, ethnique, religieuse ou politique
- Fonction au sein d'une association sans connotation raciale, ethnique, religieuse ou politique

Numéro de Registre national (BIS) / numéro d'identification de la sécurité sociale

L'utilisation du numéro de registre national (BIS) est classée **au minimum dans la catégorie d'information 2** en conséquence de son utilisation répandue comme clé unique pour le traitement de données à caractère personnel. Il s'ensuit que le numéro de registre national (BIS) peut être utilisé pour divulguer des informations sensibles (contexte) via une corrélation entre des ensembles de données.

Types de données de la catégorie d'information 3



Données financières et fiscales

Cet élément décrit les données financières et fiscales de l'individu :

- Données d'identification financière : numéros d'identification et de compte bancaire, numéros de cartes de crédit et de débit
- Charges, revenus, biens, investissements, pension et tous les détails et informations dérivées
- Dettes, dépenses, loyers, crédits (y compris emprunts et hypothèques) et tous les détails et informations dérivées
- Évaluations situation financière et statuts (y compris étude de solvabilité et évaluation)
- Allocations, aide, dons et subsides
- Produits d'assurances, y compris tous les détails et informations dérivées
- Transactions financières, y compris tous les détails et informations dérivées
- Conventions, arrangements et compensations, y compris tous les détails et informations dérivées
- Autorisations, y compris tous les détails et informations dérivées
- Terrains, propriétés et autres biens

Informations et caractéristiques des services fiscaux et financiers, avantages et biens en relation avec un individu

Mode de vie

- Consommation de stimulants (tabac, alcool, stupéfiants)
- Particularités concernant l'utilisation de biens et services proposés en dehors de l'Autorité flamande
- Particularités concernant les voyages et déplacements
- Contacts sociaux, relations autres que celles avec les parents proches
- Adhésion à une association autre que professionnelle, philosophique, politique ou syndicale
- Utilisation d'outils de communication et médias

Caractéristiques physiques, données et traitements physiques, médicaux et psychiques

➤ Caractéristiques et traitements généraux :

- Situations à risques
- Handicap et/ou déficience
- Régimes et autres modes de vie adaptés
- Exigences particulières concernant les traitements physiques, psychiques ou médicaux d'un déplacement ou d'une habitation

- Données génétiques dans le cadre d'une recherche familiale sur l'hérédité
- Données relatives aux soins, y compris les moyens et procédures utilisés pour les soins médicaux et paramédicaux

➤ Caractéristiques physiques :

- Données et traitements médicaux
- Données et traitements psychiques
- Taille, poids
- Couleur de peau, couleur de cheveux, couleur des yeux
- Signes particuliers

➤ Données psychiques :

- Examens, diagnostics et rapports
- Traitements et médication
- Traits de caractère
- Comportement à risques

➤ Données médicales :

- Examens, diagnostics et rapports
- Traitements et médication

Composition du ménage

- Formes de cohabitation
- Données relatives à la forme de cohabitation actuelle et historique (partenaire, date du mariage, date du contrat de vie commune et rupture de la forme de cohabitation)
- Relation avec d'autres parents directs (enfants, parents et descendants)
- Nombre d'enfants
- Particularités relatives aux parents en ligne collatérale et par adoption et aux parents adoptifs

Données juridiques et judiciaires

- Plaintes, incidents et accidents
- Informations détaillées concernant l'individu dans un contexte de plaintes, incidents, accidents
- Informations détaillées concernant les examens et conclusions judiciaires
- Soupçons et mise en accusation, suspicion d'infractions
- Collusion et relation entre individus suspects et condamnés
- Enquêtes, plaintes et actions en justice entreprises par et/ou contre un individu
- Condamnations et peines
- Mesures judiciaires en relation avec l'individu : tutelle, administrateur provisoire, internement et placement
- Sanctions administratives de nature purement disciplinaire
- Sanctions administratives imposées aux non-fonctionnaires qui prêtent leur collaboration à un service public (médecins, pharmaciens, paramédicaux, entrepreneurs de travaux publics)
- Sanctions administratives de nature purement disciplinaire pouvant être imposées aux utilisateurs de services publics
- Sanctions administratives de nature purement disciplinaire pouvant être imposées en raison du non-respect de dispositions légales et réglementaires (amendes SAC)

- Données génétiques et biométriques traitées dans le cadre de la loi du 22 mars 1999 relative à la procédure d'identification en matière pénale

Données raciales ou ethniques

- Informations concernant la race et l'origine ethnique

Données sur l'orientation sexuelle

- Informations concernant l'orientation sexuelle
- Données combinées permettant de déduire l'orientation sexuelle de l'individu

Relations et convictions politiques, philosophiques ou religieuses

- Convictions politiques, philosophiques et religieuses
- Fonctions, titres et reconnaissances politiques, philosophiques et religieux
- Adhésion à des organisations à connotation politique, philosophique et religieuse (syndicats compris)
- Adhésion à ou soutien de groupes d'intérêts et d'organisations militantes

Enregistrements audio et vidéo

Ces éléments portent sur l'individu :

- Ceux-ci sont applicables indépendamment du support d'enregistrement (physique, analogique ou numérique)
- Enregistrement d'images fixes ou animées, aussi en dehors du spectre visible
- Enregistrement audio

Données génétiques et biométriques

Ce type de données comprend toutes les données de référence à l'identité biologique d'un individu

- Données ADN et informations dérivées permettant d'identifier l'origine
- Empreintes digitales, reconnaissance vocale, faciale, rétinienne, de la paume de main et informations dérivées
- Enregistrement morphologique du corps, entièrement ou partiellement, y compris les informations dérivées
- Enregistrement motricité, y compris les informations dérivées (par ex. signature dynamique)

Données de localisation

Ce type de données comprend essentiellement des traces électroniques se référant au lieu et au moment auxquels un individu peut être relié. La liste ci-dessous n'est pas limitative, d'autres développements technologiques sont également compris dans ce type de données :

Généralités

- Enregistrement du temps de travail
- Enregistrement d'accès physique
- Images caméra (de contrôle)
- Données de localisation téléphonie mobile
- Données de localisation conversations téléphonie (mobile) (par ex. conversations internationales)
- Données de localisation IOT informations 'beacon' en combinaison (dérivable) avec l'individu
- Données de localisation systèmes GPS en combinaison (dérivable) avec l'individu

- Informations infractions routières (PV)
- Informations utilisation parc automobile/carte carburant en combinaison (dérivable) avec l'individu

Téléphonie mobile

➤ Disposition de localisation sur les réseaux

Cette technique basée sur le réseau utilise l'infrastructure du fournisseur de services pour déterminer la localisation de la téléphonie mobile (mesure triangulaire).

➤ Localisation sur la base du combiné (GPS compris)

Avec cette technique, il est nécessaire que le client (l'utilisateur) installe le logiciel sur son appareil mobile. Ce logiciel sera utilisé pour définir la position. Pour ce faire, le logiciel utilisera notamment les données cellulaires, IMEI, la force du signal entre l'appareil et l'antenne, les forces des signaux entre l'appareil et les appareils proches. E-OTD ou U-TDOA. Si l'appareil est encore équipé d'un GPS, la détermination du lieu peut être réalisée de façon encore plus précise.

➤ Localisation sur la base de Sim

En utilisant la carte Sim dans les appareils mobiles, il est possible de demander les données brutes du réseau. Par ex. l'information de l'appareil proche avec lequel l'appareil est en contact, les forces des signaux.

➤ Localisation sur la base de combinaisons d'ensembles de données (hybride)

Avec cette technique, on combine la méthode basée sur le réseau et la méthode basée sur le combiné pour obtenir une localisation plus précise. Citons pour exemple l'A-GPS. On utilise ici une combinaison entre des signaux GPS et des signaux provenant d'autres sources (par ex. wifi). Cette technique est aussi utilisée notamment par *Google Latitude, Buddyway, ...*

➤ Localisation sur la base de traceurs Wifi/Bluetooth/NFC

La localisation de téléphones mobiles peut aussi être effectuée à l'aide de traceurs basés sur la technologie. Cette technique est par exemple appliquée pour suivre des visiteurs dans des rues commerçantes et des bâtiments, lors d'événements, dans le trafic. On utilise ici l'adresse unique MAC qui est présente dans chaque appareil.

Global positioning systems

Données de localisation sur la base de la technologie GPS présentes dans d'autres appareils et applications

Systèmes GPS

- GPS /États-Unis
- GLONASS /Russie
- Galileo /Europe

Détails du contrat avec l'employeur

- Statut fonctionnaire et aperçu
- Statut militaire et aperçu
- Contrats de travail

Information évaluation et prestation

- Distinctions militaires, professionnelles, civiles, religieuses

- Récompenses sociales et professionnelles (financières) et sanctions sur la base des prestations
- Résultats et détail de la formation académique
- Résultats et détail de l'évaluation de la formation
- Résultats et détail de l'évaluation des prestations professionnelles

Données de sécurité sociale

- Données relatives au soutien social de l'individu
- Allocations, interventions et primes sociales
- Statut chômage et informations détaillées liées

Statuts et permis

- Permis, y compris permis de travail
- Visa, visa de voyage
- Statut immigrants et réfugiés
- Particularités liées au visa
- Restrictions de séjour et de déplacement
- Conditions particulières concernant le droit de séjour

Types de données de la catégorie d'information 4



Aucun type de données courantes n'a été relié à des données à caractère personnel identifiées dans la catégorie d'information 4.

Gestion du document

Historique

<i>Date</i>	<i>Auteur</i>	<i>Version</i>	<i>Description des modifications</i>
22/10/2019	BOSA	V0.1	Premier draft
05/11/2019	BOSA	V.1	Mise à jour sur la base de commentaires de membres du FISP, notamment : <ul style="list-style-type: none">• Mention des risques résiduels• Mise à jour de la description du guide pour la sécurisation du Cloud• Suppression du tableau concernant le lien avec d'autres documents
21/11/2019	FISP workgroup	V1.1	Distribution publique

Approbations

<i>Date</i>	<i>Approbateur(s)</i>	<i>Version</i>
21/11/2019	FISP FISP workgroup	V.1.1

Sources

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

- ISO/CEI 27001
- BSG (Baseline information Security Guidelines) fournies par le Centre pour la cybersécurité Belgique (CCB)

Lien avec une autre politique

Positionnement de la politique par rapport à la norme ISO 27001

Section	Objectifs et mesures de référence	En relation (X = Oui)
4	Contexte de l'organisation	
5	Leadership	X
6	Planification	
7	Support	
8	Fonctionnement	
9	Évaluation des performances	
10	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)
A5	Politique de sécurité de l'information		
A6	Organisation de la sécurité de l'information		
A7	Sécurité des ressources humaines		
A8	Gestion des actifs		
A9	Contrôle d'accès		
A10	Cryptographie		
A11	Sécurité physique et environnementale		
A12	Sécurité liée à l'exploitation		
A13	Sécurité des communications		
A14	Acquisition, développement et maintenance des systèmes d'information		
A15	Relations avec les fournisseurs		
A16	Gestion des incidents liés à la sécurité de l'information		
A17	Sécurité de l'information dans la gestion de la continuité de l'activité		
A18	Conformité		