



Classification

Pour plus de sécurité, adoptez les réflexes CASES !

Table des matières

1. Principes de classification
2. Schéma de classification
3. Règles de sécurité
4. Classification par défaut

Nous proposons dans ce dossier un schéma de classification selon trois dimensions (Confidentialité, Intégrité, Disponibilité) avec plusieurs classes par dimension et règles de sécurité pour ces classes.

SE	VIT	7
CO		6
RE	IMP	5
IN		4
PU	NOR	3
		2
		1

Ce schéma pourra servir de base pour un schéma de classification interne à une organisation.



Principes de classification

INVENTAIRE DES BIENS

Par définition, le terme « **bien** » fait référence à «tout élément représentant de la valeur pour l'organisme ».

Les biens incluent donc les données, informations et savoir-faire de l'organisation.

La classification est à considérer comme une approche générale couvrant l'**ensemble** des biens. Voilà pourquoi elle doit reposer sur un inventaire des biens et des informations, répertoriant l'ensemble des biens et données d'une organisation. La classification devra en particulier couvrir : les applications, les systèmes, les réseaux, les composants en production et ceux en développement.

PROPRIETE

Afin de clarifier les responsabilités, une organisation associe à chaque bien (ou à chaque type de biens) un propriétaire. Ainsi, c'est le manager qui a l'ultime responsabilité et autorité sur la gestion de ce bien et, de ce fait, sur sa sécurité. Il est en particulier responsable de la classification du bien et des règles de sécurité à lui appliquer.

Même si la responsabilité ultime ne peut pas être déléguée, le propriétaire peut confier la gestion et l'élaboration des règles à un conseiller. Au final, il devra tout de même valider les règles proposées.

UTILISATION CORRECTE DES BIENS

Le propriétaire assure l'identification, la documentation et la mise en œuvre des règles permettant une utilisation correcte de l'information. Afin d'éviter de devoir formuler une liste de règles pour chaque bien ou chaque type de bien, il doit utiliser une classification ; celle-ci proposant un schéma avec différentes classes et des règles de sécurité définies pour chacune.

REVISION REGULIERE

Le propriétaire a également la responsabilité de revoir régulièrement la classification de ses biens. En effet, certains documents perdent en criticité avec le temps, il convient donc de les déclasser ou de réduire les exigences de sécurité qui leur sont appliquées. De plus, certains biens peuvent éventuellement avoir été mal classés ou qu'il peut y avoir des inconsistances dans la classification, il convient de revoir une fois par année leur classification.

CLASSIFICATION EN 3 AXES : "CONFIDENTIALITE", "INTEGRITE", "DISPONIBILITE"

Le schéma proposé demande à ce qu'un bien soit classé selon trois axes distincts :

- Confidentialité,
- Intégrité,
- Disponibilité.

CLASSIFICATION EN FONCTION DE L'IMPACT

Le schéma proposé suggère que les biens soient classés en fonction de l'impact d'une violation de la sécurité :

- Plus l'impact d'une divulgation est important, plus la classification de confidentialité devra être élevée.
- Plus l'impact d'une perte en cas de manipulation d'un bien est important, plus la classification d'intégrité devra être élevée.
- Plus l'impact en cas de non-disponibilité prolongée est critique, plus la classification de disponibilité devra être élevée.

Remarque : Selon ce principe, la classification peut dépendre de la quantité de données. Un fichier évoquant la consommation électrique d'un seul ménage nommé et un fichier avec la consommation de chaque ménage au Luxembourg a le même besoin de protection selon la loi sur la protection des données personnelles. Le deuxième fichier sera néanmoins placé dans une classe plus élevée car l'impact d'une divulgation de celui-ci est nettement plus grand pour l'opérateur que pour le premier.

Attention : Le principe de la quantité doit être appliqué avec prudence. La divulgation d'informations personnelles concernant une personne publique peut créer nettement plus de dégâts que la divulgation de la même information sur un groupe de personnes inconnues.

Notez bien que le fait d'accorder une classification plus élevée à un bien réduit le **risque** car le fait d'imposer des exigences supplémentaires au niveau de la sécurité réduit la **probabilité d'occurrence** d'un incident.

HERITAGE DE LA CLASSIFICATION DE CONFIDENTIALITE

Afin de simplifier et d'optimiser la classification, nous recourons à des principes d'héritage qui évitent de devoir classer séparément chaque entité.

Ainsi:

- Une information a toujours la même classification, indépendamment de la forme sous laquelle elle se trouve,
- un bien contenant d'autres biens a au minimum la même classification que le bien le plus confidentiel qui y est intégré.

Remarque : Ce principe est limité à l'aspect confidentialité. Pour l'intégrité, la forme a une influence plus importante. Un document format PDF est mieux protégé contre la divulgation qu'un document Word.

Exemple : Si un incident est classé confidentiel, tant le rapport imprimé de l'incident, le fichier électronique de ce rapport, la base de donnée contenant l'incident, que la description de l'incident donné par téléphone ou discuté au repas de midi, sont considérés confidentiels. Par héritage, la liste de tous les incidents est, au minimum, classée confidentielle.

Exception : Ce principe n'est pas absolu, c'est plutôt une règle par défaut qui peut subir des exceptions.

Il est possible qu'une lettre physique passée dans de mauvaises mains présente un risque plus grand que le contenu de la lettre raconté oralement. Par prudence, nous recommandons cependant de ne pas faire trop d'exceptions, car l'information en tant que telle se retrouve aussi dans la communication orale, même si elle ne

CLASSIFICATION DES SUPPORTS

Le même schéma de classification est appliqué au support contenant les biens (et en particulier des informations), ceci pour simplifier les règles de gestion d'informations classées. Le terme support est ici à considérer au sens large ; il inclut les bureaux, les armoires, les systèmes informatiques, les répertoires, les bases de données, les canaux de communications.

Exemple : Si un répertoire est classé interne, on ne peut pas y déposer un fichier classé confidentiel. Si le disque dur d'un ordinateur est classé strictement confidentiel, on ne peut pas stocker une information secrète sur cet ordinateur.

Clarification: Il existe une nuance essentielle entre le principe d'héritage et la classification des supports.

Par exemple, un support comme notamment un ordinateur n'hérite pas de la classification de ses informations ; le support ordinateur est classé confidentiel, non pas parce que l'information la plus

Grâce à ce principe, les règles de sécurité peuvent être réduites à la règle suivante :

Règle : Il est interdit de mettre un bien dans un support ayant une classification inférieure à ce bien.

critique qu'il contient est confidentielle, mais parce que son propriétaire a jugé qu'il répond aux exigences pour pouvoir véhiculer des informations confidentielles, (et non des informations strictement confidentielles).

En pratique il se peut très bien qu'il ne contienne pas d'informations confidentielles, ou qu'il contienne illicitement des informations strictement confidentielles ; dans ce cas, il ne devient pas un ordinateur strictement confidentiel « par héritage ». Par contre, nous considérons le fichier d'archive du disque dur comme une donnée et non pas comme un support, il hérite donc d'office de la classification de l'élément le plus critique qu'il contient.

CLASSIFICATION PAR DEFAUT

Dans un organisme qui introduit une classification, il est difficile d'assurer que la classification est complète et cohérente en raison des différentes interprétations possibles des divers propriétaires. Voilà pourquoi nous proposons également une classification par défaut, en fonction de la nature des biens.

MARQUAGE

En pratique, tous les utilisateurs doivent connaître la classification des informations qu'ils traitent et les protections préconisées. Une politique de classification devra donc inclure les mécanismes sur la manière d'indiquer la classification et la signaler via un affichage adéquat.

Dans certains cas exceptionnels, il peut être utile de ne pas directement indiquer la classification à

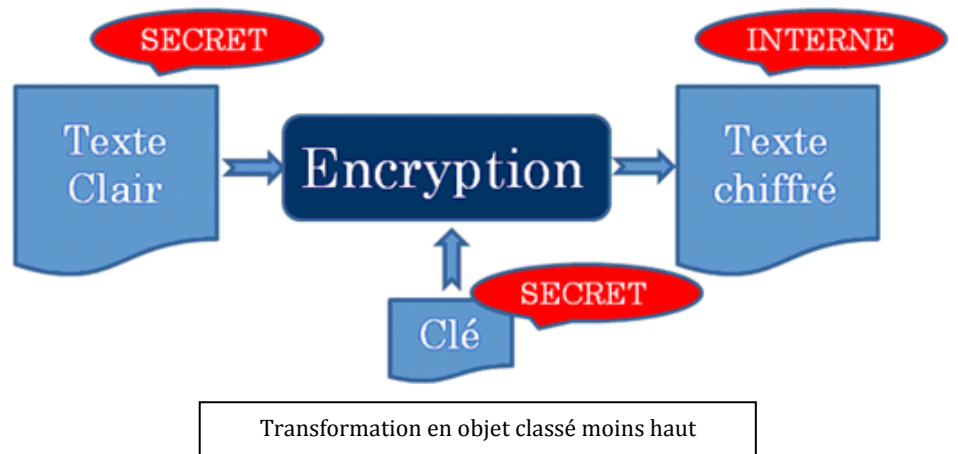
côté de l'information, ceci afin de ne pas attirer l'attention sur l'information. Il faut alors s'assurer par un autre moyen que ceux qui touchent à ces informations sont au courant de la classification. Nous recommandons d'appliquer ceci uniquement de façon occasionnelle, car d'expérience, le danger de divulgation par erreur suite à une inconscience sur la classification est plus grand que le danger de divulgation volontaire.

Dans les documents, nous faisons référence à une classe en utilisant la concaténation de l'acronyme de la classe de confidentialité, de l'acronyme d'intégrité et de celui de la disponibilité, séparé par « - ».

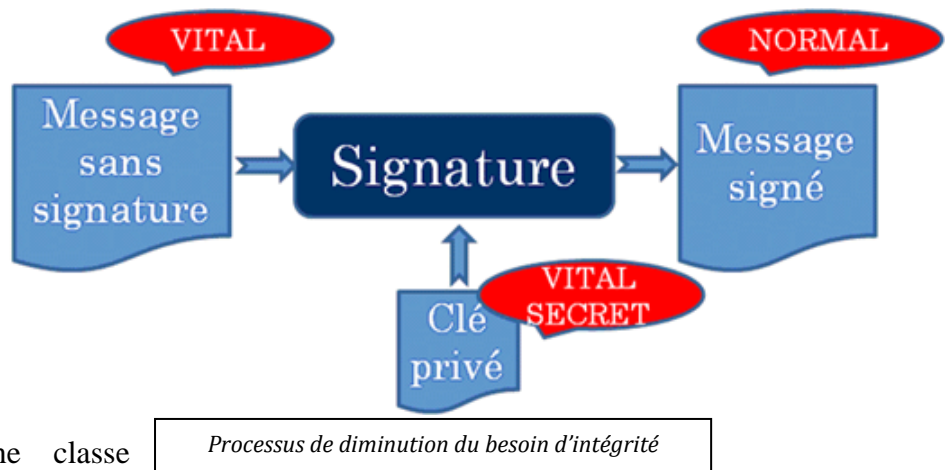
Par exemple "Co-Vit-D2" correspond à "Confidentiel" (Co = Confidentiel), Intégrité "Très important" (Vit = Vital) et disponibilité (D = Disponibilité) 2 respectivement 99 %.

UTILISATION DE LA CRYPTOGRAPHIE

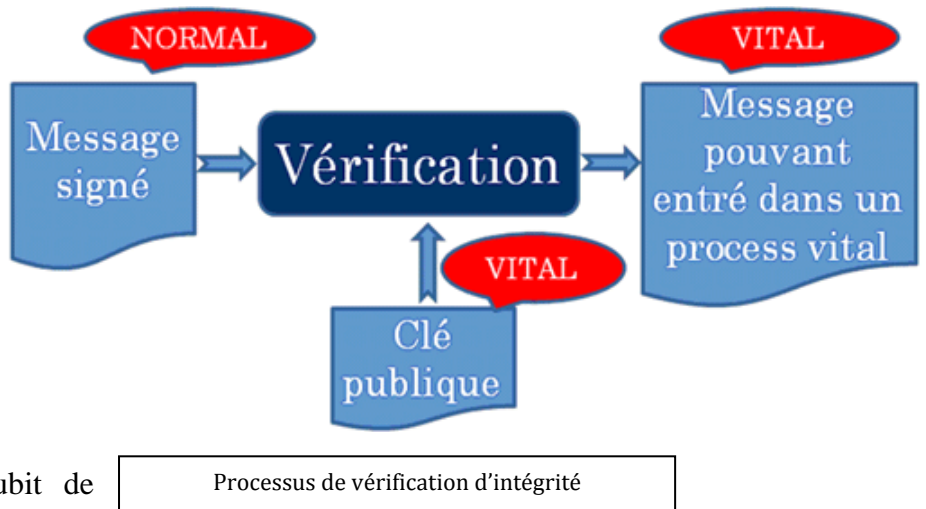
La cryptographie a mis à disposition des algorithmes permettant de transformer un texte clair, ayant un besoin de protection élevé, en un texte chiffré pouvant être traité comme texte sans besoin de protection. Ces algorithmes nécessitent l'utilisation de clés et chacune doit être protégée au même niveau que tous les messages clairs protégés par son entremise.



De même, la cryptographie a mis à disposition des algorithmes permettant de s'assurer de l'intégrité d'un message. Ces algorithmes nécessitent aussi l'utilisation de clés et chacune doit être protégée au même niveau que tous les messages protégés par son entremise. Les messages protégés en intégrité peuvent être classés dans une classe inférieure au message sans protection.



Le message protégé par une signature électronique par exemple, et classé « normal », peut être transformé dans un message non signé classé « vital » par le fait de vérifier et d'enlever la signature. Le message protégé par les règles de protection « vital » peut, par la suite, être entré dans un processus vital, alors qu'un message normal qui n'a pas subi de vérification n'est pas autorisé à entrer dans ce processus.



Au niveau des règles de sécurité, on spécifie quels algorithmes sont autorisés, sur quelles classes de données en clair et quelle est la classification des clés et des messages chiffrés.

CONFIDENTIALITE

Le schéma suivant indique l'abréviation officielle, le nom et une description des classes de confidentialité ainsi qu'une correspondance à la classe du **Traffic Light Protocol** défini par le CPNI (Center for the Protection of the National Infrastructure) qui fixe les règles de distribution des informations.

Abrév.	Classe	Description	Correspondance TLP
Se	Secret	Informations secrètes, gérées selon des procédures bien établies, stockées uniquement dans des emplacements chiffrés sous le contrôle exclusif du détenteur.	RED: Personal for named recipients only, mostly passed verbally or in person
Co	Confidential confidentiel	Informations gérées selon des procédures bien établies, accès restreint à des personnes ayant un motif approuvé.	AMBER: Limited distribution, within organisation, but only on a 'need-to-know' basis.
Re	Restricted Restreint	Documents confidentiels à l'organisation, peuvent être donnés à d'autres organisations sous base d'un NDA. Peuvent circuler librement dans les entités en charge du projet, mais pas à l'extérieur.	GREEN: Community wide. Circulation, may not be published or posted on the Internet, nor released outside of the community.
In	Internal Interne	Documents internes à l'organisation, peuvent être donnés à d'autres organisations de la même communauté, mais jamais à l'extérieur.	GREEN: Community wide. Circulation, may not be published or posted on the Internet, nor released outside of the community.
Pu	Public	Informations trouvées sur Internet, dans des conférences ouvertes, etc.	WHITE. Unlimited, subject to standard copyright rules, WHITE information may be distributed freely, without restriction.

INTEGRITE

Abrév.	Classe	Description
Vit	Vital	Informations qui peuvent en cas de modification engendrer des pertes importantes à l'organisme ou qui permettent à l'auteur de la modification de s'enrichir considérablement.
Imp	Important	Informations qui peuvent créer, en cas de modifications, des pertes d'efficacité ou des coûts de redressements notables.
Nor	Normal	Informations qui ne doivent pas disposer d'une protection d'intégrité en complément de la protection de confidentialité.

DISPONIBILITE

Au niveau de la classification des systèmes, la disponibilité souhaitée est souvent exprimée en pourcentage. La classe de la disponibilité est représentée par le nombre initial de 9 dans ce pourcentage. Par exemple une disponibilité de 99.9% est une disponibilité de classe 3, alors que la classe 1 correspond à 90% de disponibilité. 99.9% peut paraître élevé, mais correspond toujours à une perte de service de 500 minutes sur l'année, donc inconcevable pour certaines infrastructures critiques. Le réseau téléphonique est un bon exemple d'un service classe 5, 99.999% de disponibilité. Il a été conçu pour tolérer une panne de 2 heures toutes les 40 années. Dans la pratique, la disponibilité du réseau téléphonique obtenue s'avère plus faible.

En fait, il est plus parlant de définir le temps prévu de rétablissement d'une panne et d'attribuer la classification en fonction de ce temps. Une analogie avec la classification par classe de disponibilité est faite en spécifiant le nombre de pannes permises sur une année.

Nous utilisons souvent une abréviation qui indique le temps de rétablissement. Par exemple, 1h indique la classe pour laquelle il est prévu de rétablir le bien en une heure.

Le tableau suivant renseigne les classes utilisées dans notre schéma de classification et qualifie les classes selon la disponibilité et la durée tolérée de rétablissement.

Classe	Disponibilité en%	Perte de service (min/an)	Description	Abréviation	Explication	Nombre de pannes permises par an
1	90	50000	Non géré	1s	une semaine	5.09
2	99	5000	Géré	1j	un jour	3.56
3	99.9	500	Bien géré	4h	quatre heures	2.14
4	99.99	50	Tolérant des fautes	1h	une heure	0.85
5	99.999	5	Haute disponibilité	1min	une minute	5.13
6	99.9999	0.5	Très haute disponibilité	30sec	30 secondes	1.03
7	99.99999	0.05	Ultra-haute disponibilité	1sec	une second	3.08

Rappelons que la disponibilité indiquée dans la classe est la disponibilité visée au niveau de la conception, et non pas une disponibilité contractuellement garantie.

EXIGENCES DE BASE

Règle : Il est interdit de déposer un bien dans un contenant qui a une qualification inférieure à la classe du bien.

Règle : Chaque classe hérite d'office des règles de sécurité formulées pour les classes moins élevées.

Avec la première règle, la formulation de règles de sécurité pour les informations est remplacée par la qualification des contenants et la formulation de règles pour ces contenants. Avec la deuxième, nous évitons de répéter les règles des classes inférieures pour les classes supérieures.

EXIGENCES SUPPLEMENTAIRES SUR LES CLASSES

Abrév.	Classe	Exigences sécurité
Se	Secret	Informations gérées selon des procédures bien établies, sous le contrôle exclusif du détenteur ou d'un groupe de personnes.
Co	Confidentiel	Informations gérées selon des règles de sécurité stricte émises dans la politique de sécurité. Accès restreint à des personnes ayant un motif approuvé par le responsable hiérarchique et le responsable du bien. Si distribuées à l'extérieur, uniquement sur base d'un contrat avec clause de confidentialité et référence à une politique de sécurité adéquate.
Re	Restreint	Document confidentiel à l'organisation, peut être donné à d'autres organisations sous base d'un contrat avec clause de confidentialité, peut circuler librement dans les entités en charge du projet, mais pas à l'extérieur.
In	Interne	Document interne à l'organisation, peut être donné à d'autres organisations de la même communauté, mais jamais à l'extérieur.
Pu	Public	Informations trouvées sur Internet, dans des conférences ouvertes, etc.

CLASSIFICATION DES INFORMATIONS

Classe		Biens par défauts
Confidentialité		
Secret		Clés cryptographiques ; mots de passe personnels et sensibles, documents classifiés officiellement comme très secret ou secret (cf. LU-SEC) ; connaissances sur les évolutions de cours boursiers.
Confidentiel		Documents classifiés officiellement comme confidentiels (cf. LU-SEC), données protégées par loi CIP, secrets de direction, secrets bancaires, etc. ; secrets de fabrication, incidents de sécurité, données.
Restreint		Documents classifiés officiellement comme diffusion restreint (cf. LU-SEC), données privées protégé par la loi ; documentation du fonctionnement ; code source ; par défaut toutes autres informations.
Interne		Guide utilisateurs ; connaissances internes
Public		Livres, publications, etc.
Intégrité		
Vital		Flux financier important ; dispositifs de signature électronique permettant d'engager l'organisation, dispositifs de validation.
Important		Bases de données, informations sur le fonctionnement des systèmes, SCADA.
Normal		Classe d'intégrité par défaut.
Disponibilité		
7		Non utilisé ici
6		Non utilisé ici
5		Approvisionnement en électricité
4		Applications critiques importantes
3		Serveur WEB
2		Réseau bureautique
1		Système d'archivage, service ressources humaines

QUALIFICATION DES CONTENANTS

CONTENANTS INFORMATIQUES

Support	Classification	Justification Mesure de sécurité
Laptop PC	Co-Imp-D1	Administré par IT uniquement ; Mise à jour automatique, antivirus et firewall personnel à jour.
PDA	Re-Imp-D1	Administré par IT uniquement. Mise à jour automatique, antivirus et firewall personnel à jour. Echange e-mails cryptés, etc.
Serveurs	Co-Nor-D2	Serveurs gérés selon les bonnes pratiques de l'organisation. Certains serveurs spécifiques peuvent être classé Co si des règles supplémentaires sont appliquées, p.ex., pas d'accès aux techniciens externes, administration par des individus explicitement autorisés, etc.
Support Archivage	Co-Nor-D0	

Communication		
Courier DHL, etc.	Co-Vit-D3	Assurance, traçage.
Envoie postal recommandé marqué personnel	Co-Imp-D2	Le marquage personnel interdit l'ouverture par d'autres employés de l'entreprise. Garantie de livraison à la bonne adresse.
Courier normal	Re-Nor-D2	Protection par la loi sur les envois postaux.
Communication téléphonique	Co-Vit-D3	Protection par la loi sur les communications.
Communication en direct	Se-Vit-D5	Sous contrôle des participants.
Email crypté	Co-Nor-D0	Cf. consigne de config, AES 256 bits p.ex.
E-mail simple	Re-Nor-D0	Protection par la loi sur les communications.
FTP	In-Nor-D0	
https	Co-Nor-D0	Politique de certificat établie, certificat reconnaissable.
http	In-Nor-D1	

CONTENANTS PHYSIQUES

Physique		
Coffre fort	Se-Imp-D2	Coffre-fort de classe adéquate. Règles de l'administration des bâtiments publique. Procédure de gestion de clés avec responsabilité établie. Rapport d'ouverture, liste de contenus actualisés.
Armoire coupe-feu	Co-Imp-D1	Pas de protection, à part l'accès physique au bâtiment.
Armoire Tiroir de bureau	Re-Nor-D1	Clé sous contrôle personnel ; double de clé géré par procédure ; pas de clé cachée à des endroits connus ou évidents. Obligation de fermeture à clé le soir.
Armoire non fermé	In-Nor-D0	Pas de protection, à part l'accès physique au bâtiment.
Salle machine Salle archivage	Co-Imp-D2	Contrôle d'accès. Accès aux personnes devant y travailler régulièrement.
Salle de réunion publique	Pu-Nor-D2	Accessible à toute personne interne et à des visiteurs ; mauvaise isolation phonique.
Salle de réunion interne	In-Nor-D2	Accessible à toute personne interne et à des visiteurs accompagnés.
Bâtiment	In-Nor-D2	Gardiennage 27-7. Contrôle d'accès. Procédure d'accès.
Bâtiment back-up	Re-Imp-D3	
Bureaux	In-Nor-D0	Bureau ouvert, non fermé à clé.

Retrouvez les dossiers, fiches thématiques, alertes et actualités sur :

www.cases.lu