Security Guideline

Manuel pratique pour l'usage sécurisé des certificats électroniques dans le monde médical

eHealth. Réf : mibr/V1/V1/2012.E.068/Certificates.UserGuideLines/FR/1.0.

Version	Statut	Date	Auteur(s)	Nature des modifications
1.0	Final	10/09/2012	eHealth	

Plate-forme eHealth

Quai Willebroeck, 38

1000 Bruxelles

Web Site : https://www.ehealth.fgov.be/

Contents

1. Introduction

Afin que l'échange de données au sein du secteur médical soit sécurisé et ne permette pas l'interception de ces dernières par une personne non autorisée, des mécanismes de sécurité de haut niveau sont mis en œuvre.

Pour ce faire, ces mesures de sécurité mises en œuvre ont recours aux principes de cryptographie par le biais de l'utilisation des principes de chiffrements asymétrique et l'utilisation de couples de clés (clé privée/clé publique)[1].

1.1. Portée

Ce document a pour objectif de présenter un certain nombre de recommandations de sécurité liées à l'utilisation du certificat et des clés y associées permettant l'accès à des données confidentielles.

En plus des recommandations de sécurité décrites ci -après et en relation avec l'utilisation des certificats et des clés y associées, ce document contiendra également des recommandations de sécurité d'ordre général afin d'éviter qu'un incident puisse avoir un impact direct et/ou indirect.

De plus afin que le lecteur puisse comprendre les principes des certificats et des clés y associées, l'auteur du présent document propose au lecteur un certain nombre d'articles s'y référant :

- http://en.wikipedia.org/wiki/Public_key_certificate (EN) ;
- http://fr.wikipedia.org/wiki/Certificat_%C3%A9lectronique (FR)
- http://nl.wikipedia.org/wiki/Certificaat_%28PKI%29 (NL)
- http://www.pgpi.org/doc/pgpintro/ (EN)
- http://technet.microsoft.com/en-gb/library/aa998077%28v=exchg.65%29.aspx?wt.svl=2007resources+%3b (EN)
- http://technet.microsoft.com/fr-fr/library/aa998077%28EXCHG.65%29.aspx?wt.svl=2007resources%20; (FR)
- https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Certificate_System/8.0/html/Deployment_Guide/Introduction_to_Public_Key_Cryptography.html (EN)
- http://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-101.htm (FR)
- http://www.commentcamarche.net/contents/crypto/certificat.php3 ; (FR)

1.2. Présentation

Les certificats eHealth sont utilisés pour répondre à deux besoins principaux :

- l'authentification d'acteurs des soins de santé ;
- la base pour la création de la double clé de chiffrement (ETK) utilisée par le service de cryptage.

Lorsqu'un prestataire de soins souhaite avoir accès à certains services de base de la plate-forme eHealth en utilisant une connexion de système à système et non une application web, il doit disposer d'un certificat eHealth. Ce certificat permet d'identifier et d'authentifier le partenaire "système" tandis que l'eID ou le token citoyen permet d'identifier et d'authentifier l'utilisateur (la personne).

Ceci est valable tant pour l'utilisation de services de base que pour l'utilisation de services à valeur ajoutée proposés sous forme de services web. Les intégrateurs de logiciels (et non les prestataires de soins) peuvent par ailleurs demander des certificats de test. Ces certificats permettent aux collaborateurs IT de ces intégrateurs de logiciels qui sont actifs dans le secteur belge des soins de santé, de tester l'intégration de nos services de base.

[1] Une explication d'un chiffrement à clé symétrique est reprise dans la section 5 Annexe, au point 5.1

Le certificat d'authentification eHealth est un fichier contenant toutes les informations nécessaires pour identifier l'expéditeur. Le certificat est une déclaration officielle, signée par une autorité de confiance qui est compétente pour certifier le lien entre la clé électronique publique et l'identité du titulaire. Le certificat eHealth est certifié par la même « Autorité Certifiante » que la carte d'identité électronique (CA root : Fedict, CA opérationnel : Certipost).

Tout prestataire de soins, en tant qu'entité, pourra utiliser les certificats eHealth. Le certificat d'authentification eHealth certifie soit l'identité de personnes physiques connues dans la source authentique « Cadastre des professions de santé », soit l'identité d'institutions actives dans le secteur belge des soins de santé. Pour les acteurs qui n'exercent pas de profession médicale mais qui sont également actifs dans le secteur belge des soins de santé (comme les maisons de logiciels), un certificat de test eHealth officiel est prévu, permettant de tester les applications sans que des données médicales ne soient dévoilées à ce type d'utilisateurs.

Il est possible d'obtenir plusieurs certificats pour la même entité si l'institution le souhaite. Ceci peut se faire pour séparer les applications ou pour séparer l'environnement de production de l'environnement de test.

2. Principes d'identification, authentification et signature au sein de la plate-forme eHealth[2]

Dans le cadre du déploiement d'applications destinées au secteur soins de santé, par exemple (My)CareNet, Recip-e, la plate-forme eHealth a publié, sur son portail, un document décrivant les principes d'identification, authentification et signature .

Toute application qui souhaite utiliser un service électronique de la plate-forme eHealth, de (My)CareNet ou de Recip-e, doit s'authentifier au moyen d'une clé privée et du certificat d'authentification y afférent délivrés par la plate-forme eHealth.

Le certificat d'authentification de l'application contient l'identité du responsable de la gestion de l'application. La plate-forme eHealth prévoit des instructions précises pour l'obtention et l'installation de ce certificat d'authentification. L'installation et la gestion de ce certificat d'authentification relève de la responsabilité du responsable de la gestion de l'application.

Le service de base « Gestion des utilisateurs et des accès de la plate-forme eHealth » permet de vérifier si un utilisateur déterminé d'un service électronique de la plate-forme eHealth, de (My)CareNet ou de Recip-e possède certaines caractéristiques ou relations ; dans la négative, il permet de générer un message d'erreur. La plate-forme eHealth ne vérifie pas si un utilisateur déterminé peut utiliser une application locale déterminée. De plus, au vu du type de données traitées par ces applications locales, l'utilisation d'une authentification forte (eID, SmartCard, Secure Token, ….) est plus que recommandée.

[2] Cf. site web de la plate-forme eHealth : https://www.ehealth.fgov.be/fr/enregistrement-des-logiciels-medicaux, Recip-e : Mécanismes d'identification, d'authentification et de signature.

3. Principes généraux des certificats

3.1. Certificats eHealth

L'échange d'informations et même l'établissement d'une connexion avec la plate-forme eHealth va nécessiter la mise en place d'un certificat ainsi que les clés y associées. La plate-forme eHealth a mis à la disposition des utilisateurs une procédure et un utilitaire (ETK) permettant l'initialisation de la demande. Ces certificats permettront l'identification/authentification mais également l'encryption par le biais de l'utilisation des clés « publiques/privées ».

Le certificat eHealth permettra à l'entité de s'identifier et s'authentifier dans ses échanges avec ses partenaires. Qui plus est, ce dernier permettra également la non-répudiation de toutes transactions/actes signés par son biais.

L'utilisation du couple de clé « publique/privée » permet le chiffrement et déchiffrement (processus aussi appelé processus d'encryption et de décryption) nécessaire afin d'échanger des messages « confidentiel » entre partenaires au sein du secteur soins de santé.

La plate-forme eHealth laisse la liberté à chaque entité de commander et d'utiliser plusieurs certificats en fonction de l'activité professionnelle. Par exemple : certificat personnel, certificat de l'organisme, ….

Les certificats issus de la plate-forme eHealth sont la propriété du demandeur. Tout partage et transmission se fait sous l'entière responsabilité de ce dernier.

3.2. Gestion des mots de passe

Afin de protéger l'utilisation et donc l'accès à la clé privée d'un certificat, un mécanisme d'authentification basé sur l'introduction d'un code d'accès (mot de passe, code pin, …) est utilisé. Ce procédé est également implémenté dans le cadre de l'espace de stockage des certificats et clés y associées.

La gestion efficace des mots de passe est la première ligne de défense dans la sécurité électronique d'une organisation. A ce stade de l'utilisation d'outils électroniques où une authentification est nécessaire, voire obligatoire, celle-ci requiert régulièrement l'utilisation d'un code d'accès (code PIN), d'un mot de passe, d'une passphrase, etc … Et donc il n'est pas rare qu'un utilisateur lambda possède une multitude de ces preuves d'identité.

Par exemple :

- Le code pin de la carte d'identité électronique belge ;
- Le code pin de la carte de payement (débit/crédit) ;
- Le mot de passe de l'ordinateur ;
- Les codes d'accès aux applications, tant professionnelles que privées ;
- ….

Dès lors, l'utilisateur est contraint de retenir une multitude de ces codes et est tenté, pour des raisons de facilité, d'utiliser le même code d'accès, d'utiliser un code simple, de les inscrire à proximité (sous le clavier, dans le premier tiroir, …). Cela impacte le niveau de sécurité des données/applications protégées par ces codes.

Le mot de passe doit être facile à retenir et suffisamment complexe afin qu'il ne soit pas découvert facilement. Dès lors, les bonnes pratiques en la matière recommandent que :

- Le mot de passe ne doit pas être identique au nom de l'utilisatrice ou de l'utilisateur, même si on y ajoute un chiffre ou un symbole ;
- Le mot de passe ne doit pas contenir des informations personnelles, telles que le nom ou le numéro de la rue, le nom de l'entreprise, la date de naissance, etc… ;

- Le mot de passe ne doit jamais contenir de noms des membres de la famille, des animaux de compagnie, des amies et amis ou des collègues de travail ;
- Le mot de passe ne doit pas être une phrase commune suivie d'un chiffre qui change lorsque le mot de passe expire ;
- Le mot de passe utilisé pour une finalité, ne doit pas être réutilisé dans le cadre d'autres finalités ;
    - Le mot de passe ne doit être utilisé que pour un certain accès ;
    - Le mot de passe utilisé dans la génération d'une clé privée, ne doit pas être utilisé pour la génération d'autre clé privée ;
    - …

Mot de passe	Force	Raison
Vent	Faible	Trop court, trop facile à pirater/deviner
Laurent1	Faible	Utilisation du prénom de l'utilisateur, trop facile
2265	Faible	Identique au code pin de la carte bancaire personnelle de l'utilisateur. De plus ce choix constitue un apport de risques additionnels pour ce dernier
Hzc4uG	Bon	Six caractères, lettres majuscules et un chiffre
3zX2tRk4c+y	Très bon	Mot de passe généré par le système

Tableau 1 : Exemples force mot de passe

Il existe plusieurs procédés afin de construire un mot de passe suffisamment fort que pour ne pas être découvert facilement, tout en étant facile à retenir. Le procédé le plus utilisé est la génération d'une phrase assez longue tout en étant simple à retenir et y appliquer un procédé de sélection des caractères pouvant ainsi former un mot de passe. Le mot de passe ainsi généré est appelé « passphrase »

Exemple :

> En partant de la phrase suivante : « Bob a un cheval blanc qui court dans le pré d'Alice !», il est possible de générer une « passphrase » comportant tant des minuscules que des majuscules, mais également des chiffres et autres caractères spéciaux. A partir de la phrase simple précitée, il est possible de créer un mot de passe du style : « B@1cBqCdLpD@! ».

Tout comme le choix du mot de passe est important, son stockage l'est tout autant. Un mot de passe est, par définition, secret et doit le rester. Et donc placer ce dernier près de l'écran, sous le clavier, dans le premier tiroir n'est nullement une bonne idée !

Le mot de passe permettant l'identification/authentification et dans certains cas la signature, transmettre ce dernier n'est à faire qu'en cas de prévention afin de pallier à des problèmes potentiels importants. La responsabilité liée à l'utilisation de ce mot de passe reste celle du propriétaire initial de celui-ci.

Même en prenant toute les mesures de sécurité, la fiabilité d'un mot de passe ne pourra jamais être garantie dans le temps, dès lors, ce dernier devra être régulièrement modifié.

> *Dans le cadre du projet ETEE, la plate-forme eHealth met à disposition des utilisateurs un outil permettant la modification de ce mot de passe. Cet outil est disponible sur son portail[3]. ()*

3.3. Keystore[4]

Comme décrit dans la section « définitions », le keystore, ou magasin de clés, est un espace de stockage de l'ensemble des clés publiques et privées utilisées. En fonction de cela, une attention particulière au niveau de la sécurité doit être mise en place. Cette attention concerne tant l'accessibilité, la pérennité que la non-répudiation.

[3] https://www.ehealth.fgov.be/fr/application/applications/gestion_certificats_ehealth.htm

[4] Définition portant sur Keystore voir section 5.1 page 6

Afin de garantir une confidentialité des clés, cet espace de stockage ne doit être accessible qu'aux utilisateurs autorisés. Ces accès doivent être décrits dans les documents décrivant la mise en place de la sécurité au sein de l'entité. Ces documents sont généralement appelés « Politique de sécurité ».

Toute corruption du système d'information et donc potentiellement du contenu du keystore, entraîne que le degré de confiance envers les certificats et clés y associées ne permet plus leur utilisation dans le cadre de l'échange et l'accès à des données « sensibles ». Dès lors, le suivi de la procédure de révocation de ces certificats et clés y associées sera nécessaire. Toutefois, en cas d'incident physique à ce système d'information, il est admissible qu'une sauvegarde sécurisée[5] de cet espace de stockage soit utilisée afin de restaurer ledit système et les accès y réalisés.

La traçabilité des actions effectuées sur le keystore peut être assurée par la mise en place du système d'auditing interne au système d'exploitation. Cet auditing va permettre la consultation, via les traces systèmes, des actions réalisées par l'ensemble des utilisateurs ayant accès.

Les trois points développés ci-dessus doivent être décrits au sein d'un document décrivant les mesures de sécurité implémentées au sein de l'organisation.

3.4. Protection de la clé privée

Sauf pour des raisons de sauvegarde, comme mentionné dans le cas du keystore, la copie de la clé privée n'est pas recommandée.

Au vu des fonctionnalités offertes par la clé privée, tant la procédure de sauvegarde ou d'archivage implémentée que le support de stockage mais aussi la localisation de ce stockage doivent être protégés et sécurisés.

La destruction des clés, certificats ne peut être réalisée que par une personne habilitée au sein de l'entité. De plus, cette procédure doit faire partie des documents de sécurité généraux (politique de sécurité, plan de sécurité, …)

Afin de permettre la récupération d'anciens messages chiffrés[6] au-delà de la période de validité du certificat, la mise en place, par le biais de l'organisation du procédé d'archivage, de sauvegarde est nécessaire.

3.5. Gestion des certificats

Les certificats délivrés par la plate-forme eHealth ont une durée de validité limitée à 3 ans. La plate-forme eHealth notifiera le demandeur lors de l'échéance du certificat.

La plate-forme eHealth met à disposition sur son portail une procédure permettant de mandater un tiers pour la commande et la gestion des certificats délivrés par cette dernière.

Au vu du lien qui unit les certificats d'authentification et d'encryption, la procédure de renouvellement prévoit automatiquement le renouvellement de la paire.

Une fois la date d'expiration du certificat passé, son utilisation ne sera plus possible. Dès lors, afin d'éviter tout problème suite au dépassement de validité du certificat, une période de 2 mois est considérée comme souhaitable pour entamer la demande de renouvellement.

Afin de pouvoir relire des messages chiffrés au-delà de la durée du certificat, il est recommandé d'organiser un archivage sécurisé du répertoire des clés (keystore) et des mots de passe associés6.

La falsification, la fabrication de certificats eHealth est interdite. Qui plus est, l'utilisation de « faux » certificats rendra impossible toute communication au vu des contrôles de validités implémentés et de la non publication de la clé privée au sein de l'espace public dédié.

[5] Par sauvegarde sécurisée, on entend un espace de stockage physique séparé dont le niveau de sécurité appliqué est au moins égal au niveau de sécurité du keystore.

[6] Au moment de la rédaction du dit document, la plate-forme eHealth offre une solution d'échange de messages chiffrés, sans offrir une solution de stockage à long terme de ces messages chiffrés.

La plate-forme eHealth a décrit une procédure standard tant pour la demande que pour le renouvellement, et même dans le cas de révocation du certificat[7].

La demande de révocation de certificat ne peut être introduite que par le demandeur du certificat, le mandataire, le responsable accès entité (RAE)[8] ou, en dernier recours, par le conseiller en sécurité de la plate-forme eHealth. Toute demande de révocation doit s'accompagner d'une preuve d'identité, signature électronique (EID) ou une copie signée de la carte d'identité du demandeur.

3.6. Mandat

La plate-forme eHealth a publié sur son portail un formulaire permettant de donner un mandat à une personne interne ou externe à l'entité dans le but de gérer les certificats et les clés y associées[9].

3.7. Procédure de secours

Afin de permettre la continuité « business » de l'activité de l'entité dans le cas où l'identification et l'authentification par le biais de la carte d'identité électronique n'est plus possible (carte perdue, défectueuse, volée, …), la plate-forme eHealth propose une solution alternative par l'utilisation, lors de la connexion, du certificat personnel (différent du certificat système utilisé pour identifier et authentifier l'application). Cette solution alternative offrant un niveau de sécurité plus faible que l'utilisation de la carte d'identité électronique, son utilisation est limitée dans le temps (« fallback session »). C'est au sein du comité de pilotage de chaque projet qu'il convient de fixer, en collaboration avec la plate-forme eHealth, et après analyse des risques, la durée maximale autorisée et ce, en fonction du public cible et des nécessités opérationnelles.

Dans le cadre du projet Recip-E, il a été convenu que pour :

- les prescripteurs, la durée de session autorisée avant ré-identification est d'une heure (1h) ;
- les pharmaciens, la durée autorisée est de quatre heures (4h).

3.8. Révocation du certificat

Si vous ne pouvez plus vous connecter et échanger des données avec la plate-forme eHealth ou avec des tiers, il y a une forte présomption que votre certificat et vos clés y associées doivent être remplacés. Néanmoins avant de procéder à la révocation des certificats et clés y associées, une analyse de l'évolution de la situation peut vous apporter une première solution.

Par exemple :

- Le fichier comprenant la clé privée est-il toujours présent ? (fichier .P12 ou voir selon votre manuel d'utilisation du package médical)
- Le programme a-t-il été modifié récemment par une mise à jour ?
- …

Contactez le centre de contact au numéro 02/788 51 55 et suivez la procédure qui vous sera transmise pour générer une nouvelle clé secrète.

Il sera nécessaire de révoquer le certificat (selon la procédure publiée sur le site de la plate forme eHealth) et de commander un nouveau certificat.

[7] https://www.ehealth.fgov.be/fr/support/services-de-base/certificat-ehealth

[8] Définition portant sur Responsable Accès Entité (RAE)voir section 5.1 page 20

[9] https://www.ehealth.fgov.be/fr/support/services-de-base/certificat-ehealth

3.9. Principes de sécurité des certificats pour des cas spécifique

a) Utilisation dans un cadre partagé (ex : cabinet de garde médicale)

Certains environnements vont imposer le partage d'une même station de travail permettant l'accès aux services offerts par la plate-forme eHealth par plusieurs dispensateurs de soins (exemple : cabinet médical partagé par plusieurs médecins, ….). Certaines consignes supplémentaires à celles décrites précédemment doivent être respectées afin de garantir un bon niveau de sécurité.

L'identification et authentification à une application qui permet l'accès à des données « sensibles » au moyen de la carte d'identité électronique est préférable à l'installation en local d'un certificat personnel, surtout dans le cadre du partage de la station de travail. Comme mentionné précédemment, le code pin d'une carte d'identité électronique et le mot de passe d'un certificat personnel ne peuvent être transmis à un tiers.

Dans le cadre de l'utilisation du mot de passe associé à la clé privée utilisée pour l'identification de système à système, la transmission de cette dernière ne peut être réalisée qu'envers des personnes autorisées et suivant une procédure de sécurité définie et validée par le conseiller en sécurité de l'entité.

Au sein du projet permettant la réalisation de la prescription médicale, l'utilisation de la carte d'identité électronique est préférable à l'installation sur la station de travail du certificat personnel fourni par la plate-forme.

Afin de se prémunir contre l'utilisation non souhaitée par un tiers, l'utilisateur veillera à clôturer sa session à la fin de son service.

b) Utilisation dans une officine de pharmacien

L'utilisation de package médical au sein d'une officine faisant appel à des services électroniques (tels la prescription électronique,…) de la plate-forme eHealth implique qu'un certain nombre de consignes soient respectées afin de garantir un niveau de sécurité.

Afin que l'ensemble des postes de travail utilisés au sein de l'officine puissent avoir accès aux services électroniques de la plate-forme eHealth, l'installation du certificat d'authentification devra être réalisée sur chacun de ces postes de travail.

Pour protéger correctement la clé privée, le mot de passe y associé doit être suffisamment complexe et ne doit être communiqué qu'aux personnes autorisées à utiliser cette dite clé.

Dans le cas où le certificat et les clés y associées sont générés et installés par le fournisseur de l'application, il est nécessaire que les codes liés soient uniques à l'officine.

Le conseiller en sécurité du groupe pharmaceutique peut offrir ses services afin d'aider le responsable de la pharmacie dans ce cadre.

Tout problème doit faire l'objet d'une notification auprès du helpdesk desservant l'officine, car le risque de corruption du certificat et des clés y associées est présent. Et dans pareil cas, la révocation de ces derniers sera peut-être nécessaire.

4. Principes généraux de sécurité

Outre les points précités, ayant une relation directe avec le niveau de sécurité final des certificats et clés y associées dans le cadre de l'échange d'information au sein du réseau des acteurs de soins de santé, d'autres éléments liés à la sécurité de l'information peuvent avoir un impact indirect sur la sécurité de ces certificats et clés. Ces éléments, dont certains sont détaillés ci-dessous, devraient faire partie également du document de sécurité de l'information rédigé au sein de l'entité.

Etant donné la « sensibilité » des données utilisées par les différentes applications, la sécurisation du poste de travail de l'utilisateur final révèle toute son importance.

Différents évènements parus dans la presse prouvent que le niveau de sécurité du poste de travail de l'utilisateur final a un impact non négligeable sur la sécurité des données utilisées par cet utilisateur à travers différentes applications tant web que locales.

> Un exemple : En juin 2012, plus de 13.000 comptes bancaires belges ont été piratés pour une valeur estimée à 3 millions d'euros par le biais de l'infection du poste de travail par un logiciel malveillant téléchargé à partir des réseaux sociaux.

Dès lors, l'installation d'une suite applicative de sécurité continuellement mise à jour (comprenant lutte contre les virus, trojan, …) sur chaque poste de travail[10] n'est plus une recommandation, mais une obligation afin de protéger l'utilisateur et les données (tant professionnelles que privées) avec lesquelles il travaille.

4.1. Système d'exploitation

a) Droits / autorisations

Afin d'éviter tout risque au niveau de la sécurité des données traitées et accédées au moyen du certificat et des clés y associées par l'utilisation tant au niveau professionnel qu'au niveau privé, une séparation physique entre l'environnement professionnel et privé est recommandée.

Il y a lieu de limiter le nombre de comptes locaux sur un poste de travail. Il convient également de désactiver les comptes préinstallés.

L'implémentation d'une politique en matière de mots de passe est nécessaire, de manière à imposer des mots de passe forts ayant une longueur minimale. L'utilisation de la notion d'historique des mots de passe et un « account lockout threshold » permet d'éviter le risque de "brute force attack". La politique spécifique en matière de mots de passe sera déterminée en collaboration avec le conseiller en sécurité de l'information.

La réutilisation de mots de passe identiques sur différents comptes / différentes plateformes n'est pas conseillée (p.ex. mot de passe d'administrateur local différent des mots de passe domaine, database, …).

Configurer le poste de travail de telle manière qu'un code d'accès soit nécessaire tant pour le démarrage, qu'après un certain temps d'inactivé permet qu'un tiers non autorisé ne puisse pas utiliser le système à l'insu de son utilisateur/propriétaire.

En dehors d'un système spécialisé suffisamment sécurisé (SSO), évitez l'enregistrement automatique de mots de passe pour les connexions réseau et internet, les connexions vers les applications, …

b) Services

Sans pour autant bloquer l'utilisation des systèmes, les fonctions locales de sharing[11] doivent être évitées.

[10] Le terme « poste de travail » désigne tout système informatique permettant le traitement de données par le biais d'applications. (y inclus ordinateurs fixes et portables, tablettes, téléphones intelligents, …)

[11] "simple file sharing", "shared folders" et "internet connection sharing"

Désactivez les possibilités de « universal plug & play » pour éviter tout usage non autorisé de hardware supplémentaire.

Débranchez tous les canaux de communication[12] qui ne sont pas nécessaires dans le cadre des activités autorisées.

c) *Connexions*

Le firewall interne doit être activé. Ce firewall doit être actualisé en permanence et ne peut pas être mis hors service par l'utilisateur final. Ne laissez ouvert que quelques ports nécessaires à l'exécution des tâches professionnelles. Opérez une distinction entre les connexions nécessaires au réseau interne et les connexions externes.

En fonction des besoins, il y a lieu de prévoir la possibilité de créer différents profils (VPN sur portables, …).

4.2. Software hors système d'exploitation

a) *Navigateur*

Les paramètres internet du navigateur doivent être configurés afin d'éviter l'installation de malware à travers internet (limiter les fonctions comme active content, scripting, …).

Le navigateur doit, seul si possible, contrôler si chaque certificat numérique est toujours valide.

Les cookies doivent être limités au maximum.

L'utilisation d'un bloqueur de « Pop-Ups Windows » est recommandé.

b) *Anti-malware*

Le logiciel anti-malware doit être configuré afin qu'il effectue régulièrement et automatiquement un contrôle complet du système (tous les fichiers, également les fichiers startup, bios, boot records).

Les fonctions de contrôle en temps réel présentes au sein des logiciels anti-malware doivent être activées

La mise à jour du logiciel anti-malware doit être automatique et régulière.

c) *Autres logiciels*

Il convient de prendre des mesures maximales pour garantir l'intégrité des logiciels et éviter l'utilisation de logiciels dont la source n'est pas reconnue. L'utilisation de logiciels certifiés est un plus.

En cas d'installation de systèmes pouvant permettre la prise de contrôle à distance du poste de travail, cette prise de contrôle ne peut uniquement avoir lieu que moyennant l'accord de l'utilisateur final.

Des fichiers logs de sécurité générés lors de l'utilisation de l'application ne doivent pas être effacés. Ces fichiers peuvent servir en cas de difficultés d'utilisation : instabilité de l'application, impossibilité de se connecter, message d'erreur de l'application.

N'ouvrez pas des fichiers inconnus reçus - par exemple- par mail qui vous semblent suspects. Ils peuvent être utilisés pour attaquer votre système.

Ne connectez pas n'importe quoi à votre ordinateur ; par exemple une clé USB contenant des fichiers non contrôlés par un anti-virus.

4.3. Gestion des patches

En ce qui concerne la fréquence d'installation des mises à jour de sécurité, il convient de trouver un bon équilibre entre les besoins de sécurité et les objectifs opérationnels. Pour les mises à jour qui sont qualifiées d'urgentes par des organismes reconnus[13] il convient de prendre immédiatement les mesures adéquates.

[12] wireless network, firewire, bluetooth, infrared, serial, …

4.4. Messagerie électronique

À moins d'utiliser des techniques de chiffrage certifiées (encryption), le message électronique doit être considéré comme peu sûr. Le message envoyé peut être lu par une autre personne que votre destinataire final. Le message reçu peut provenir d'une personne se faisant passer pour une autre (duperie et usurpation) qui, elle, peut inspirer confiance, car des en-têtes de courrier sont facilement forgés. En conséquence, ne jamais rien révéler de confidentiel tel que mot de passe, code d'accès, données personnelles, etc, dans un message électronique.

Les menaces les plus courantes sont :

- le SPAM ;
- le phishing ;
- les chaînes de lettres ;
- les Hoax ;
- les trojans ;

[13] Sans, Secunia, ….

5. Annexe

5.1. Définitions

Authentification :

C'est le processus permettant de vérifier que l'identité que prétend posséder une entité, pour pouvoir utiliser un service électronique, correspond bien à l'identité qu'il prétend être.

L'authentification nécessite un élément de "preuve" d'une identité, le contrôle peut se faire sur base des facteurs suivants :

- des connaissances que l'utilisateur a (un mot de passe…);
- d'une possession (un certificat sur une carte lisible de manière électronique…);
- de caractéristiques biométriques (empreinte de la main…);
- ou bien, la combinaison de plusieurs de ces facteurs d'authentification.

Certificat

Un certificat de clé publique, généralement appelé simplement un certificat, est une instruction signée numériquement qui lie la valeur d'une clé publique à l'identité de la personne, de la machine ou du service qui contient la clé privée correspondante. La plupart des certificats communément utilisés sont basés sur la norme de certificat X.509v3.

Des certificats peuvent être émis pour une variété de fonctions telles que l'authentification d'utilisateurs Web, l'authentification de serveurs Web, la sécurisation d'une messagerie (Secure/Multipurpose Internet Mail Extensions ou S/MIME), la sécurité IP (IPSec), la sécurité TLS (Transport Layer Security) et la signature de code. Des certificats sont également délivrés par une Autorité de certification à une autre afin d'établir une hiérarchie de certification.

L'entité qui reçoit le certificat est appelée le *sujet* du certificat. L'émetteur et signataire du certificat est une Autorité de certification.

En général, les certificats contiennent les informations suivantes :

- La valeur de la clé publique du sujet.
- Des informations identifiant le sujet, par exemple son nom et son adresse de messagerie.
- La période de validité (durée pendant laquelle le certificat est valide).
- Des informations identifiant l'émetteur.
- La signature numérique de l'émetteur qui atteste la validité de la liaison entre la clé publique du sujet et les informations d'identification de ce dernier.

Un certificat n'est valide que pour la durée spécifiée, indiqué à l'intérieur de ce dernier par le biais de deux champs ; *Valide à partir du* et *Valide jusqu'au*. Une fois que la période de validité d'un certificat est dépassée, un nouveau certificat doit être demandé par le sujet du certificat expiré.

Dans le cas où il devient nécessaire de défaire la liaison déclarée dans un certificat, ce dernier peut être révoqué par l'émetteur. Chaque émetteur gère une liste de révocation de certificats qui peut être utilisée par des programmes lors de la vérification de la validité de n'importe quel certificat.

L'un des principaux avantages des certificats est que les hôtes n'ont plus besoin de gérer un jeu de mots de passe pour des sujets individuels qui doivent être authentifiés avant d'obtenir un accès. Il suffit désormais à l'hôte d'établir une relation d'approbation avec un émetteur des certificats.

Lorsqu'un hôte, tel qu'un serveur Web sécurisé, désigne un émetteur en tant qu'autorité racine approuvée, l'hôte approuve implicitement les stratégies que l'émetteur a utilisées pour établir les liaisons des certificats qu'il émet. En fait, l'hôte fait confiance à l'émetteur en ce qui concerne la vérification de l'identité du sujet du certificat. Un hôte désigne un émetteur en tant qu'autorité racine de confiance en

plaçant le certificat auto-signé de l'émetteur contenant sa clé publique dans le magasin de certificats de l'Autorité de certification racine de confiance de l'ordinateur hôte. Les Autorités de certification intermédiaires ou secondaires ne sont approuvées que si elles ont un chemin d'accès de certification valide à partir d'une Autorité de certification racine de confiance.

Entité

Une entité est une structure composée d'attributs, représentant un composant identifiable d'un domaine fonctionnel, et potentiellement en relation avec les autres entités de ce domaine.

Une entité est une personne physique, personne morale, un système ou assimilé

Hoax

En informatique, les canulars (appelés « hoax » en anglais) se trouvent souvent sous la forme de message électronique ou de simple lettre-chaîne. Dans ce dernier cas, Internet ne fait qu'amplifier un phénomène qui existait déjà à travers le courrier traditionnel. Le mot *hoax* est une simplification du premier mot de l'expression hocus pocus, signifiant « tromperie » ou « escroquerie ».

Identité

Une entité peut être identifiée de manière univoque sur base d'un ou plusieurs attributs d'identification.

Par exemple : le numéro de registre national, le numéro d'entreprise tel défini par la Banque Carrefour des Entreprise (BCE), numéro d'agrément délivré par l'Institut national d'assurance maladie invalidité, …

Une entité ne possède qu'une seule identité.

Keystore

Un keystore (magasin de clefs) est un fichier informatique qui stocke des certificats électroniques et éventuellement leurs clefs privées, le contenu de ce fichier sera utilisé par des applications de cryptographie à clef publique comme SSL

Malware

Le *malware* est la contraction de « malicious » (qui peut se traduire par « malicieux » dans le sens de « malveillant », et non celui de « porté à la plaisanterie ») et « software » (logiciel). C'est un terme désignant un logiciel malveillant ; un logiciel développé dans le but de nuire à un système informatique. Les virus et les vers sont les deux exemples les plus connus de logiciels malveillants.

Non-répudiation

La non répudiation est la propriété d'une action ou d'un événement d'avoir bien eu lieu et de ne pouvoir être niée ou nié ultérieurement.

Par exemple : Le fait de ne pas pouvoir nier une action

- l'expéditeur ne peut pas nier avoir envoyé le message ;
- le récepteur ne peut pas nier avoir reçu le message ;
- la signature d'un contrat (signature numérique) ;
- …

Phishing

Le *phishing*, est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. … — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale. Le phishing, ou hameçonnage, peut se faire par courrier électronique, par des sites web falsifiés ou par d'autres moyens électroniques.

Responsable Accès Entité (RAE)

Le Responsable Accès Entité est la personne désignée responsable de l'ensemble des applications sécurisées offertes par les administrations publiques pour l'ensemble de l'entreprise ou de l'organisation pour laquelle il est désigné. Le Responsable Accès Entité est le "root contact" de l'entreprise/organisation. Il est en mesure de gérer une ou plusieurs qualités.

SPAM

Le SPAM désigne une communication expédiée en masse à des fins publicitaires ou malhonnêtes, notamment du courrier électronique non sollicité par les destinataires. La perception du niveau de pertinence d'un message SPAM varie d'un utilisateur à l'autre.

Trojan (cheval de Troie)

Un cheval de Troie est un logiciel d'apparence légitime, mais conçu pour exécuter subrepticement (de façon cachée) des actions à l'insu de l'utilisateur. En général, un cheval de Troie tente d'utiliser les droits appartenant à son environnement pour détourner, diffuser ou détruire des informations, ou encore pour ouvrir une porte dérobée qui permettra à un attaquant de prendre, à distance, le contrôle de l'ordinateur.

Un cheval de Troie n'est pas un virus informatique, en ce sens qu'il ne se reproduit pas par lui-même, fonction essentielle pour qu'un logiciel puisse être considéré comme un virus. Un cheval de Troie est conçu pour être reproduit lors de téléchargements ou de copies par des utilisateurs naïfs, attirés par les fonctionnalités du programme. Les chevaux de Troie servent très fréquemment à introduire une porte dérobée sur un ordinateur. L'action nuisible à l'utilisateur est alors le fait qu'un pirate informatique peut à tout moment prendre à distance (par Internet) le contrôle de l'ordinateur.Un cheval de Troie se compose de deux parties distinctes : la partie "serveur" et la partie "client". La partie client est le composant envoyé à la victime tandis que la partie serveur reste sur l'ordinateur du pirate. La partie client est envoyée par courriel et se présente sous la forme d'une amélioration d'un logiciel (ex : MSN, Adobe Photoshop, Safari ...). Elle peut aussi se présenter sous la forme d'un test de QI ou d'un jeu à but lucratif. Bref, les formes sont multiples. Le cheval de Troie se glisse donc dans l'ordinateur et s'installe dans l'éditeur du registre. Là, il ouvre une porte dérobée (backdoor) de l'ordinateur et établit une connexion avec l'ordinateur pirate. La partie serveur, elle, s'occupe d'envoyer les informations. Le pirate peut contrôler la totalité des commandes exécutables sur un PC (il peut contrôler la souris, le clavier mais aussi imprimer, formater le disque dur, activer une webcam, etc..).

La distinction entre un cheval de Troie, un spyware, un keylogger, et une porte dérobée n'est donc souvent qu'une question de mot ou de contexte.

Vers (WORM)

Un ver, contrairement à un virus informatique, n'a pas besoin d'un « programme hôte » pour se reproduire. Il exploite les différentes ressources existantes ou disponibles afin d'assurer sa reproduction. La définition d'un ver s'apparente à la manière dont il se propage de machine en machine. Le véritable but de tels programmes peut aller bien au-delà du simple fait de se reproduire, notamment espionner, offrir un point d'accès caché (porte dérobée), détruire des données, faire des dégâts, envoyer de multiples requêtes vers un site internet dans le but de le saturer, etc

Virus

Au sens strict, un virus informatique est un programme informatique écrit dans le but de se propager à d'autres ordinateurs en s'insérant dans des programmes ou données légitimes appelés « hôtes ». Il peut aussi avoir comme effet, recherché ou non, de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme l'internet, mais aussi les disquettes, les cédéroms, les clefs USB, etc. Les virus informatiques ne doivent pas être confondus avec les vers qui sont des programmes capables de se propager et de se dupliquer par leurs propres moyens sans contaminer un « programme hôte ».

5.2. Bibliographie

1. *Wikipeadia.* [En ligne] Wikimedia Foundation, Inc. http://fr.wikipedia.org.