Manuel pratique pour l'usage sécurisé des certificats électroniques dans le monde médical
Version 2.0

This document is provided to you, free of charge, by the

eHealth platform

Willebroekkaai 38 – 1000 Brussel

38, Quai de Willebroek – 1000 Bruxelles

Table of contents

1. Document management

1.1 Historique

Version	Date	Auteur	Modifications/Remarques
1.0	10/09/2012	eHealth platform	Version intiale
2.0	17/01/2023	Information Security	Version adaptée

2. Introduction

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

Pour ce faire, ces mesures de sécurité mises en œuvre ont recours aux principes de cryptage par le biais de l'utilisation de paires de clés asymétriques(clé privée/clé publique)[1]

2.1 Scope

Ce document a pour objectif de présenter une série de recommandations en matière de sécurité en ce qui concerne 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, ce document contient également des recommandations de sécurité d'ordre général en ce qui concerne l'utilisation des certificats et des clés 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 une série articles à ce sujet :

- ***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.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-101.htm*** (FR)
- ***http://www.commentcamarche.net/contents/crypto/certificat.php3*** ; (FR)

2.2 Présentation

Les certificats eHealth sont utilisés pour répondre à deux besoins:

- l'authentification d'acteurs des soins de santé ;
- comme 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.

Les prestataires de soins et les établissements de soins agréés peuvent obtenir un certificat eHealth pour signer des appels et des messages sans avoir chaque fois besoin de l'eID.

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 au personnel IT de ces intégrateurs de logiciels actifs dans le secteur belge des soins de santé, de tester l'intégration de nos services de base.

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 publique électronique et l'identité du titulaire. Le certificat eHealth est certifié par la même « Autorité Certifiante » que la carte d'identité électronique (CA racine : BOSA, CA opérationnel : Zetes, Quovadis, Certipost).

La liste des identités numériques auxquelles on peut faire confiance pour chaque finalité est publiée par eHealth. Les clients peuvent établir la confiance en filtrant les TSL publiées pour chaque finalité. eHealth suit la

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

norme ETSI pour distribuer sa propre liste de certificats de confiance et assure le rôle de gestionnaire de schéma avec son propre ensemble de règles que les fournisseurs de services de confiance doivent suivre.

Les CA de confiance actuels sont publiés par la Plate-forme eHealth sur ***http://tsl.ehealth.fgov.be***.

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 soins 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 sociétés 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.

Si l'institution le souhaite, elle peut obtenir plusieurs certificats pour la même entité dans le but de séparer les applications ou de séparer l'environnement de production de l'environnement de test.

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

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

Toute application qui souhaite utiliser un service électronique de la Plate-forme eHealth, de MyCareNet 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 a élaboré des instructions précises pour l'obtention et l'installation de ce certificat d'authentification. L'installation et la gestion de ce certificat d'authentification relèvent 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 MyCareNet ou de Recip-e possède certaines caractéristiques ou relations ; dans la négative, un message d'erreur est généré. Compte tenu du type de données traitées par ces applications locales, l'utilisation d'une authentification forte est recommandée.

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

4. Principes généraux des certificats

4.1 Certificats eHealth

L'échange d'informations et l'établissement d'une connexion avec la Plate-forme eHealth requièrent la mise en place d'un certificat et des 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 et également le chiffrement par le biais de l'utilisation des clés publiques/privées.

Le certificat eHealth permet à l'entité de s'identifier et de s'authentifier dans le cadre des échanges avec ses partenaires. Il permet par ailleurs la non-répudiation de toutes les transactions/actions signées par le biais de ce certificat.

L'utilisation de la paire de clé publique/privée permet le chiffrement et déchiffrement (cryptage et décryptage) nécessaires pour l'échange de messages « confidentiels » entre partenaires au sein du secteur soins de santé.

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

Les certificats délivrés par la Plate-forme eHealth sont la propriété du demandeur. Tout échange et communication s'effectuent sous l'entière responsabilité de ce dernier.

4.2 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 appliqué 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. Lors de l'utilisation d'outils électroniques qui requièrent une authentification, il est généralement fait usage d'un code d'accès (code PIN, mot de passe, etc.). Il n'est dès lors pas rare qu'un utilisateur 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 partout ou d'utiliser un code facile à retenir, de les noter et de les conserver à proximité (sous le clavier, dans le premier tiroir du bureau, …). Ceci à un impact sur le niveau de sécurité des données/applications protégées par ces codes.

Le mot de passe doit être facile à retenir et en même temps suffisamment complexe pour ne pas être décelé. Les bonnes pratiques en la matière sont les suivantes :

- Le mot de passe ne peut pas être le nom de l'utilisateur, même pas en y ajoutant un chiffre ou un symbole ;
- Le mot de passe ne peut pas contenir d'informations personnelles, telles que le nom de la rue ou le numéro de maison, le nom de l'entreprise, la date de naissance, etc… ;
- Le mot de passe ne doit jamais contenir de noms de membres de la famille, d'animaux de compagnie, d'amis ou collègues de travail ;
- Le mot de passe ne peut pas être une phrase populaire ou un mot suivi d'un chiffre qui change lorsque le mot de passe expire ;

- Un mot de passe utilisé pour une finalité déterminée ne peut pas être réutilisé pour d'autres finalités ;
- Le mot de passe peut uniquement être utilisé dans le cadre d'un accès déterminé ;
- Le mot de passe utilisé pour la création d'une clé privée ne peut pas être utilisé pour la création d'autres clés privées ;
- ….

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

Tableau 1 : Exemples force mot de passe

Il existe plusieurs méthodes pour créer un mot de passe suffisamment fort pour ne pas être décelé, tout en étant facile à retenir. Le procédé le plus utilisé consiste à générer une phrase assez longue tout en étant simple à retenir et à y appliquer un procédé de sélection des caractères qui constituent 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@! ».

Si 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. Conserver le mot de passe près de l'écran, sous le clavier, dans le premier tiroir du bureau n'est donc nullement une bonne idée !

Le mot de passe étant utilisé pour l'identification/authentification et éventuellement la signature, il peut uniquement être communiqué dans un but de prévention afin d'éviter des problèmes potentiels importants. Le titulaire du mot de passe reste responsable de son utilisation.

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, il devra être régulièrement modifié.

Dans le cadre du projet ETEE, la Plate-forme eHealth propose un outil pour la modification de mots de passe. Cet outil est disponible sur son portail. [3].

[3] ***https://www.ehealth.fgov.be/ehealthplatform/nl/service-ehealth-certificaten***

4.3 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. Le niveau de sécurité mérite dès lors une attention particulière, tant au niveau de l'accessibilité, de la pérennité et de la non-répudiation.

Afin de garantir la confidentialité des clés, cet espace de stockage est uniquement accessible aux utilisateurs autorisés. Le Responsable des accès (généralement le DPO, le coordinateur ICT ou le CEO) doit accorder les droits d'accès et les documenter selon les règles d'accès applicables au sein de l'organisation. Ces documents sont généralement appelés « Politique de sécurité ».

Toute violation du système d'information et donc potentiellement du contenu du keystore compromet la confidentialité des certificats et des clés y associées, ce qui rend impossible leur utilisation dans le cadre de l'accès aux données « sensibles » et leur échange. Dès lors, une procédure de révocation des certificats et des clés y associées sera mise en œuvre. Toutefois, en cas d'incident physique au niveau du système d'information, il est possible de réaliser une sauvegarde sécurisée[5] de cet espace de stockage en vue de restaurer le système et l'accès au système.

La traçabilité des actions effectuées sur le keystore est assurée par la mise en place d'un système d'audit interne au sein du système d'exploitation. Ce système d'audit permet de vérifier, via les journaux système, les actions réalisées par l'ensemble des utilisateurs ayant eu accès.

Les trois points développés ci-dessus doivent être décrits dans un document relatif aux mesures de sécurité implémentées au sein de l'organisation

4.4 Protection de la clé privée

Hormis pour des finalités de sauvegarde, comme décrit ci-dessus en ce qui concerne le keystore, il n'est pas judicieux de prendre une copie de la clé privée.

Compte tenu des fonctionnalités de la clé privée, tant la procédure de sauvegarde ou d'archivage que l'espace de stockage et sa localisation doivent être protégés et sécurisés.

La destruction des clés et des certificats peut uniquement être effectuée par une personne habilitée au sein de l'entité. De plus, cette procédure doit être reprise dans les documents de sécurité généraux (politique de sécurité, plan de sécurité, …)

Pour pouvoir consulter à nouveau d'anciens messages chiffrés[6] à l'issue de la période de validité du certificat, la mise en place d'une copie de sauvegarde, par le biais d'une procédure d'archivage, est nécessaire.

4.5 Gestion des certificats

Les certificats délivrés par la Plate-forme eHealth ont une durée de validité de maximum 3 ans. La Plate-forme eHealth avertira l'intéressé par mail[7] 3 mois avant l'expiration 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 la Plate-forme eHealth.

---

[4] Définition du "Keystore" voir section 6.1

[5] Sauvegarde sécurisée : espace de stockage physiquement séparé avec un niveau de sécurité au moins aussi élevé que le niveau de sécurité du keystore

[6] Au moment de la rédaction du présent document, la Plate-forme eHealth offre une solution pour l'échange de messages cryptés, mais pas encore de solution pour le stockage à long terme de ces messages cryptés.

[7] A l'adresse e-mail saisie par l'utilisateur lors de la demande du certificat. Un rappel est envoyé mensuellement, à partir de 3 mois avant l'expiration et tant que le certificat n'a pas été renouvelé.

Compte tenu du lien entre les certificats d'authentification et les certificats de chiffrement, la procédure de renouvellement est automatiquement valable pour les deux.

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 la durée de validité du certificat, un délai de 3 mois est prévu pour la demande de renouvellement.

Afin de pouvoir reconsulter des messages chiffrés après l'expiration du certificat, il est recommandé d'organiser un archivage sécurisé du keystore et des mots de passe associés.

La falsification de certificats eHealth est interdite. Il ne sera d'ailleurs pas possible de communiquer à l'aide de « faux » certificats compte tenu des contrôles de validité appliqués et du fait que la clé privée n'est pas publiée dans l'espace public.

La Plate-forme eHealth a élaboré une procédure standard à la fois pour la demande et pour le renouvellement, ainsi que pour la révocation du certificat[8].

La demande de révocation du certificat ne peut être introduite que par le demandeur du certificat, son mandataire, le responsable accès entité (RAE)[9] ou, en dernier recours, par le conseiller en sécurité ou DPO de la Plate-forme eHealth. Toute demande de révocation doit être accompagnée d'une preuve d'identité valide.

4.6 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 pour la gestion des certificats et des clés y associées [10].

4.7 Procédure de secours (fallback)

Pour garantir la continuité des activités 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 qui consiste à utiliser , lors de la connexion, le certificat personnel (différent du certificat système utilisé pour identifier et authentifier l'application). Cette solution alternative offre un niveau de sécurité plus faible que l'utilisation de la carte d'identité électronique et 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 besoins 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 limitée à quatre heures (4h).

4.8 Révocation du certificat

Si vous ne pouvez plus vous connecter et échanger des données sur base de votre certificat, votre certificat/vos certificats et les clés y associées doivent probablement 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.

[8] ***https://www.ehealth.fgov.be/ehealthplatform/fr/service-certificats-ehealth***

[9] Pour la définition de responsable d'accès principal, voir la section 6.1.

[10] ***https://www.ehealth.fgov.be/ehealthplatform/fr/service-certificats-ehealth***

Par exemple :

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

Contactez le centre de contact de la Plate-forme eHealth 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 web de la Plate-forme eHealth) et de commander un nouveau certificat.

4.9 Principes de sécurité des certificats pour des cas spécifiques

4.9.1 Usage partagé (ex : poste de garde)

Dans certains contextes, un même ordinateur offrant accès aux services de la Plate-forme eHealth est partagé par plusieurs prestataires de soins (exemple : cabinet médical partagé par plusieurs médecins, ….). Dans ce cas, il convient de respecter certaines règles supplémentaires afin de garantir un niveau de sécurité adéquat.

L'identification et authentification à l'égard d'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 pas être transmis à des tiers.

Dans le cadre de l'utilisation d'un mot de passe associé à la clé privée pour l'identification de système à système, la transmission de cette dernière n'est possible qu'envers des personnes autorisées et suivant une procédure de sécurité définie et validée par le conseiller en sécurité de l'entité.

Dans le cadre 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 eHealth.

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

4.9.2 Utilisation dans une officine de pharmacien

L'utilisation de logiciels médicaux au sein d'une officine qui ont recours à des services électroniques (tels la prescription électronique,…) de la Plate-forme eHealth implique le respect d'une série de règles afin de garantir un niveau de sécurité adéquat.

Pour permettre à l'ensemble des postes de travail utilisés au sein de l'officine d'avoir accès aux services électroniques de la Plate-forme eHealth, le certificat d'authentification devra être installé 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 peut être communiqué qu'aux personnes autorisées à utiliser cette clé.

Dans le cas où le certificat et les clés y associées sont générés et installés par le fournisseur de l'application, il faut que les codes en question 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 être signalé au helpdesk en charge de l'officine, étant donné le risque de corruption du certificat et des clés y associées. Dans ce cas, une révocation est nécessaire.

5. Principes de sécurité généraux

Outre les points précités, qui concernent directement le niveau de sécurité 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 être repris intégralement dans le document de sécurité de l'information rédigé au sein de l'entité.

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

Différents évènements qui ont fait écho 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 dans 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 suite à l'infection des postes de travail par un logiciel malveillant téléchargé à partir des réseaux sociaux.

Dès lors, l'installation d'une solution anti-malware sur chaque poste de travail est obligatoire.

5.1 Système d'exploitation

5.1.1 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 dans le cadre de l'utilisation tant professionnelle que privée, 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 d'un historique des mots de passe et d'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 est déconseillée (p.ex. mot de passe d'administrateur local différent des mots de passe domaine, data base, …).

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

Mis à part un système spécialement sécurisé (SSO), un enregistrement automatique de mots de passe pour les connexions réseau et internet, les connexions vers les applications, … est à éviter

5.1.2 Connections

Le firewall interne doit être activé. Il doit être mis à jour en permanence et ne peut pas être désactivé par l'utilisateur. Seuls les ports nécessaires aux activités professionnelles doivent être laissés ouverts. Il convient de distinguer les connexions nécessaires au réseau interne et les connexions externes.

Selon les besoins, il y a lieu de prévoir la possibilité de créer différents profils (VPN sur les ordinateurs portables, etc.).

5.2 Logiciels externes au système d'exploitation

5.2.1 Navigateur (web browser)

Les paramètres des navigateurs web doivent être configurés de manière à garantir un niveau de sécurité adéquat.

5.2.2 Anti-malware

Le logiciel anti-malware doit être configuré pour effectuer régulièrement et automatiquement une vérification complète du système (tous les fichiers, y compris les fichiers de démarrage, bios, boot records).

Les fonctions de vérification en temps réel disponibles dans le logiciel anti-malware doivent être activées.

Ce logiciel doit être mis à jour régulièrement et automatiquement.

5.2.3 Autres logiciels

Des mesures adéquates doivent être prises pour garantir l'intégrité des logiciels et éviter l'utilisation de logiciels d'origine inconnue. L'utilisation de logiciels certifiés est un plus.

En cas d'installation de systèmes capables de prendre le contrôle du poste de travail à distance, cette prise de contrôle ne doit se faire qu'avec le consentement de l'utilisateur final.

Les fichiers journaux de sécurité créés lors de l'utilisation de l'application ne doivent pas être supprimés. Ces fichiers peuvent être utiles en cas de difficultés d'utilisation : instabilité de l'application, impossibilité d'établir une connexion, message d'erreur de l'application.

N'ouvrez pas les fichiers communiqués via un courrier suspect. Ces fichiers peuvent être utilisés pour lancer une attaque sur le système.

Ne connectez rien au PC, par exemple une clé USB contenant des fichiers qui n'ont pas été vérifiés par un antivirus.

5.3 Gestion des patches

En ce qui concerne la fréquence d'installation des correctifs de sécurité, un équilibre doit être trouvé entre les besoins de sécurité et les objectifs opérationnels. Pour les mises à jour qualifiées d'urgentes par des organismes reconnus tels que CERT.be, CERT-EU, CERT-FR, les mesures appropriées doivent être prises immédiatement.[11]

5.4 Messagerie électronique

À moins d'utiliser des techniques de chiffrement reconnues (cryptage), un courrier électronique n'est pas considéré comme très sûr. Le message envoyé peut être lu par une personne autre que le destinataire. Le message reçu peut provenir d'une personne qui se fait passer pour quelqu'un d'autre (tromperie, spoofing) et qui inspire confiance en utilisant des logos contrefaits. Par conséquent, l'utilisateur ne devrait jamais partager des informations confidentielles dans un e-mail, telles qu'un mot de passe, un code d'accès, des données personnelles, etc.

Si des mots de passe doivent quand même être partagés, utilisez un lien temporaire pour transmettre un mot de passe.

[11] ***https://www.cert.ssi.gouv.fr/***

https://www.cert.be/nl/nieuws

https://cert.europa.eu/cert/clusteredition/en/latest.html

Si vous envoyez le mot de passe par courrier électronique, il est stocké pour toujours dans la boîte aux lettres électronique du destinataire et dans les différents serveurs de courrier électronique qui transmettent le message au destinataire.

Voici un exemple d'une alternative pour le partage sécurisé des mots de passe : ***https://pwpush.com***

Les menaces les plus courantes sont:

- le phishing
- les mails en chaîne
- ingénierie sociale
- cheval de Troie.

6. Annexe

6.1 Définitions

6.1.1 Authentification

Il s'agit de la vérification de l'identité que l'entité prétend posséder et sur base de laquelle cette entité souhaite utiliser un service électronique.

L'authentification nécessite une preuve d'identité. La vérification peut être basée sur les éléments suivants :

- les connaissances que l'utilisateur possède (un mot de passe, etc.) ;
- possession (par exemple, un certificat sur une carte lisible électroniquement) ;
- caractéristiques biométriques (empreinte de la main, ...) ;
- ou une combinaison de différents éléments

6.1.2 Certificat

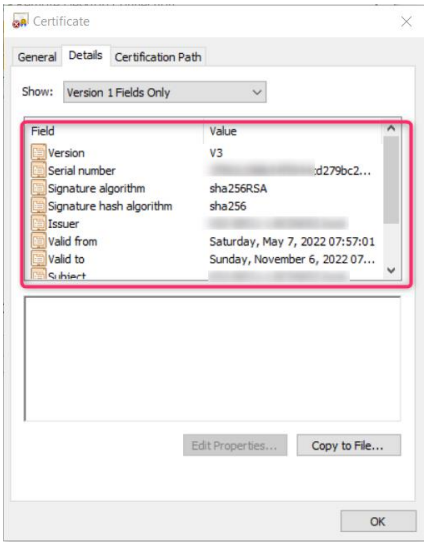
Un certificat à clé publique est généralement appelé "certificat" en abrégé. Il s'agit d'une déclaration signée numériquement qui relie la valeur d'une clé publique à l'identité de la personne, du dispositif ou du service possédant la clé privée correspondante. De nombreux certificats courants sont basés sur la norme de certificat X.509v3.

Les certificats peuvent être émis à des fins diverses, par exemple pour l'authentification des utilisateurs du web, l'authentification des serveurs web, le courrier électronique sécurisé (S/MIME (Secure/Multipurpose Internet Mail Extensions)), la sécurité IP (IPSec, Internet Protocol Security), TLS (Transport Layer Security) et les signatures de code de programme. Une autorité de certification (CA) délivre également des certificats à d'autres autorités de certification. Cela crée une hiérarchie de certification.

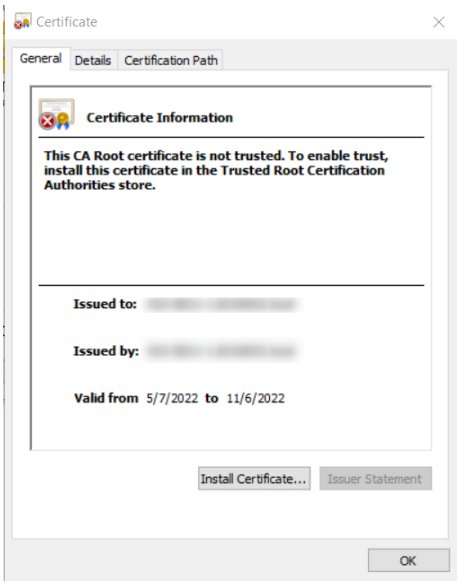
L'entité qui reçoit le certificat est le titulaire du certificat. L'autorité de certification est l'émetteur et le signataire du certificat.

Les certificats contiennent généralement les informations suivantes :

- La valeur de la clé publique du titulaire du certificat.
- Les données d'identification du titulaire du certificat, telles que son nom et son adresse électronique.
- La période de validité (la période pour laquelle le certificat est valide).
- Les données d'identification de l'émetteur.
- La signature numérique de l'émetteur. Cette signature ratifie la validité de la relation entre la clé publique et les données d'identification du titulaire du certificat.



La validité d'un certificat est limitée à la période spécifiée dans le certificat. Chaque certificat contient les dates "Valable du" et "Valable jusqu'au". Lorsque la période de validité d'un certificat a expiré, le titulaire du certificat expiré doit demander un nouveau certificat.



Dans certains cas, il peut être nécessaire d'annuler la relation déclarée dans un certificat. Le certificat est alors révoqué par l'émetteur. Chaque émetteur tient une liste de révocation de certificats. Cette liste permet de vérifier la validité d'un certificat.

L'un des principaux avantages des certificats est qu'il n'est plus nécessaire de stocker une collection de mots de passe sur les hôtes pour les titulaires individuels qui doivent être authentifiés avant de leur accorder accès. Il suffit désormais à l'hôte d'établir une relation de confiance avec un émetteur de certificats.

Lorsqu'un émetteur est désigné comme autorité racine de confiance sur un hôte, tel qu'un serveur web sécurisé, il est implicitement fait confiance aux règles sur base desquelles l'émetteur a établi les relations dans les certificats émis. Cela signifie qu'il faut croire que l'émetteur a vérifié l'identité du titulaire du certificat. Lorsqu'un émetteur de certificats est défini comme autorité racine de confiance par un ordinateur hôte, le certificat auto-signé de l'émetteur, qui contient la clé publique de l'émetteur, est placé dans les archives des

autorités de certification racine de l'hôte. Les autorités de certification intermédiaires ou sous-jacentes ne sont fiables que si elles disposent d'un chemin de certificat valide provenant d'une autorité de certification racine fiable.

6.1.3 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 équivalent.

6.1.4 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 attribué 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.

6.1.5 Keystore

Un keystore (magasin de clefs) est un fichier informatique dans lequel sont stockés les certificats électroniques et éventuellement leurs clefs privées ; le contenu de ce fichier sera utilisé par des applications de chiffrement à clef publique comme SSL.

6.1.6 Malware

Le malware est la contraction de « malicious » (malveillant) 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..

6.1.7 Non-répudiation

La non-répudiation implique qu'une action ou un événement ont bien eu lieu et ne peuvent être niés ni maintenant ni 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) ;
- …

6.1.8 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.

6.1.9 Responsable Accès Entité

Le « Gestionnaire d'accès principal » est la personne qui est désignée, pour l'ensemble de l'entreprise ou de l'organisation, comme responsable de l'ensemble des applications sécurisées offertes par les administrations publiques . Le Responsable Accès Entité est le "root contact" de l'entreprise/organisation. Il peut gérer une ou plusieurs qualités.

6.1.10 SPAM

Le terme « 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.

6.1.11 Trojan (Cheval de Troie)

Un cheval de Troie est un logiciel qui paraît légitime mais qui a en réalité été développé pour effectuer secrètement (de manière dissimulée) des actions à l'insu de l'utilisateur. En général, un cheval de Troie tente d'utiliser les droits de son environnement pour voler, diffuser ou détruire des données, ou pour ouvrir une porte dérobée permettant à un pirate de prendre le contrôle de l'ordinateur à distance.

6.1.12 Ver

Contrairement à un virus informatique, un ver n'a pas besoin d'un "programme hôte" pour se reproduire. Un ver utilise les différentes ressources existantes ou disponibles pour se reproduire. La définition d'un ver ne fait référence qu'à la façon dont le ver se propage d'un ordinateur à l'autre. L'objectif réel de ces programmes peut être bien plus que la simple reproduction. L'objectif d'un ver peut être d'espionner, d'ouvrir une porte dérobée, de détruire des données, de causer des dommages, d'inonder un site web de requêtes de sorte que le site tombe en panne, etc..

6.1.13 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 données ou des programmes légitimes, appelés "hôtes". Un virus informatique peut également causer des dommages en interférant avec le fonctionnement de l'ordinateur infecté. Le virus peut se propager via tout outil permettant l'échange de données numériques, comme Internet, les disquettes, les CD-ROM, les clés USB, etc.