Ontario Health

Norme sur la cryptographie

Version: 1.8

N° de document : 3537

Gestion du document

Fréquence de révision : Une fois par année ou selon la règle établie par le Comité ConnexionSécurité.

Historique des approbations

APPROBATEURS (S)	DATE D'APPROBATION
Comité ConnexionSécurité	2017-02-21
Comité ConnexionSécurité	2018-03-26
Comité ConnexionSécurité	2021-03-18

Historique des révisions

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
1.0	2013-12-20	Adoption de la version de novembre 2013 du groupe de travail sur la protection de la vie privée et la sécurité de ConnexionRGT.	Mark Carter
1.1	2014-12-04	Révision en fonction des commentaires reçus des membres du Comité ConnexionSécurité. Ajout de la définition de « mandataire », de « terminal d'envoi de données » et de « service de gestion d'identité ». Modification de la durée de vie maximale des certificats à cinq ans. Ajout de TLS 1.1+ aux protocoles cryptographiques acceptés.	Mark Carter
1.2	2014-12-12	Révision à la suite de la réunion du Comité ConnexionSécurité du 11 décembre. Établissement de la durée de vie à sept ans aux fins d'harmonisation avec le cycle de renouvellement des infrastructures aux points 1.28 et 2.44; ajout de l'attribution des tâches aux responsables de clés par le dirigeant principal de l'information ou son délégué aux points 1.33 et 2.49; révision pour obliger le traitement des clés comme un élément de catégorie restreinte conformément à la Politique sur la gestion de l'information et des éléments d'actif aux points 1.34 et 2.50.	Mark Carter
1.3	2015-01-22	Politique déposée devant les comités régionaux de protection de la vie privée et de sécurité et approuvée par tous les membres du Comité ConnexionSécurité en date du 22 janvier 2015.	Mark Carter

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
1.4	2015-10-19	Mise à jour des politiques pour refléter le changement de gouvernance. Le Comité directeur a été remplacé par l'organisme de surveillance compétent. Le Comité régional de protection de la vie privée et de sécurité ne participe plus au processus de décision en matière de dérogation.	Mark Carter
1.5	2017-02-21	Mise à jour des politiques afin d'incorporer les changements mis en œuvre lors du rafraîchissement 2017. La définition de « solution de DSE » a été ajustée. Plusieurs contrôles ont été reformulés afin d'inclure « participant » dans la solution de DSE.	Ravi Addepalli
1.6	2018-03-16	Mise à jour de la norme afin d'inclure l'accès au DSE par les patients.	Geovanny Diaz
1.7	2020-03-16	Mise à jour avec FIPS 140-3 qui a remplacer FIPS 140-2. Revision et mis à jour du tableau des algorithmes cryptographiques approuvés.	Ana Fukushima
1.8	2021-01-04	Examen du document avec des modifications mineures, mise à jour du cycle de révision tous les deux ans	Ana Fukushima

Norme sur la cryptographie

Objet

La présente norme a pour but de définir les contrôles de protection des renseignements nécessaires à la mise en place et à la gestion de solutions cryptographiques.

Portée

La présente norme s'applique à l'ensemble des composants de [la solution de DSE].

Elle vise les éléments suivants dans le cas des dépositaires de renseignements sur la santé (DRS) qui utilisent [la solution de DSE] pour voir, traiter ou autrement manipuler des renseignements personnels sur la santé (RPS) à l'aide d'une **technologie de gestion d'identité locale** :

- le système de contrôle de l'accès et de gestion d'identité du DRS (les « services de gestion d'identité ») qui gère les processus d'authentification et d'autorisation donnant accès à [la solution de DSE] (solution de service d'émission de jetons de sécurité de [la solution de DSE], Active Directory Federation Services 2.0 de Microsoft ou autre);

- toute connexion directe au portail du fournisseur de [la solution de DSE] et aux fonctions administratives de cette dernière, ce qui comprend les composants connectés (pare-feu, serveur mandataire, etc.);

- l'intégration du portail du fournisseur de [la solution de DSE] au système d'information local du DRS ou à l'application de gestion des dossiers médicaux électroniques.

Elle vise plutôt les éléments suivants dans le cas des DRS qui utilisent [la solution de DSE] pour voir, traiter ou autrement manipuler des RPS à l'aide du **service ONE ID de cyberSanté Ontario** :

- toute connexion directe aux fonctions administratives de [la solution de DSE], ce qui comprend les composants connectés (pare-feu, serveur mandataire, etc.).

Dans le cas des DRS qui créent et versent des RPS dans le dépôt de données cliniques de [la solution de DSE], la présente norme, en plus de ce qui est prévu pour les sites qui ne font que consulter les données, s'applique aux éléments suivants :

- les terminaux d'envoi de données qui fournissent des RPS au dépôt de données cliniques de [la solution de DSE];

- les technologies de l'information et les processus qui assurent la qualité des données envoyées (la mise en correspondance de la terminologie, par exemple).

La norme ne s'applique pas aux DRS, à leurs mandataires et à leurs fournisseurs de services électroniques qui ne créent pas, ne versent pas et ne consultent pas de données dans [la solution de DSE] et qui n'accèdent pas à cette dernière.

Définitions

[la solution de DSE] : Solution utilisée, y compris les systèmes connexes, pour stocker et rendre accessibles les renseignements personnels sur la santé contenus dans les systèmes de renseignements électroniques sur la santé des dépositaires de renseignements sur la santé.

[La solution de DSE] inclut les portails et les applications pour les patients (affiliés ou non à un dépositaire de renseignements sur la santé) qui facilitent l'accès du patient au DSE. Ces applications peuvent être :

- Commandées par le fournisseur (le fournisseur facilite la communication avec le patient)
- Fournies directement au patient (le patient a un accès direct au DSE)
- Commandées par le patient (le patient délègue l'accès à un mandataire spécial ou à d'autres délégués, p. ex., un membre de la famille ou un médecin).

Équipe de [la solution de DSE] : également appelée bureau de l'équipe; comprend des agents et des fournisseurs de services électroniques qui soutiennent [la solution de DSE], y compris les activités, les initiatives et les processus associés à la protection de la vie privée et à la sécurité.

Code d'authentification de message (MAC) : Somme de contrôle cryptographique de données faisant appel à une clé de session pour détecter des modifications accidentelles ou intentionnelles des données. Le MAC emploie un message et une clé de session pour générer un bloc authentificateur difficile à générer pour un message donné sans connaissance de la clé.

Connaissance répartie : Principe exigeant le traitement de l'information sous forme d'éléments distincts du moment de la production de l'information jusqu'à la combinaison des éléments en vue de leur utilisation. Un élément à lui seul ne permet pas de décoder le message.

Devrait/devraient : S'utilisent lorsqu'il y a des raisons, selon les circonstances, de ne pas exécuter ce qui est proposé. La personne doit cependant comprendre les conséquences de ses actes si elle décide de ne pas adhérer à ce qui est écrit et songer à mettre en œuvre des mesures de contrôle en guise de compensation.

Doit/doivent : S'utilisent dans le cas des exigences absolues où il n'y a aucune autre option possible.

Double contrôle : Principe de contrôle exigeant l'apport de deux personnes pour effectuer une tâche donnée.

Fournisseur de services électroniques : Personne ou entité qui fournit des biens ou des services dans le but de permettre à un dépositaire de renseignements sur la santé d'employer des moyens électroniques de recueillir, d'utiliser, de modifier, de diffuser, de conserver ou d'éliminer des renseignements personnels sur la santé et qui comprend un fournisseur de réseau d'information sur la santé.

Mandataire : Dans le contexte des dépositaires de renseignements sur la santé, personne qui, sous réserve de l'approbation du dépositaire, s'occupe de tout ce qui est lié aux renseignements personnels sur la santé de ce dernier, et ce, dans l'intérêt du dépositaire et non dans son propre intérêt, qu'il ait ou non le pouvoir d'engager le dépositaire, qu'il soit employé ou non par le dépositaire et qu'il soit rémunéré ou non. Par exemple, le mandataire peut être une organisation, un employé ou un entrepreneur qui valide l'identité des utilisateurs du dossier de santé électronique au nom d'un dépositaire de renseignements sur la santé. Un mandataire peut aussi assurer des services de correction de données d'un dépositaire de renseignements sur la santé à partir de son terminal d'envoi de données.

Organisme de surveillance compétent : L'organisme de surveillance compétent est formé de cadres supérieurs qui supervisent tous les aspects de la [solution DSE]. Voir la section intitulée Structure de la politique de gouvernance dans le document Politique de sécurité de l'information.

Peut/peuvent : S'utilisent lorsque ce qui est proposé n'est qu'une recommandation ou ne sert que d'exemple qui ne se veut pas exhaustif.

Responsable de clé : Mandataire ou fournisseur de services électroniques qui a l'autorisation de traiter en entier ou en partie une clé cryptographique tout au long de la durée de vie de cette dernière, de sa génération à sa destruction.

Service de gestion d'identité : Technologies et services, politiques, processus et procédures connexes servant à créer, à conserver, à mettre en sécurité, à valider, à affirmer et à gérer des identités électroniques pour [la solution de DSE].

Système d'information : Ensemble autonome de technologies de l'information organisées de manière à recueillir, à traiter, à conserver, à utiliser, à divulguer, à détruire ou à éliminer l'information.

Technologie de l'information : Tout élément (matériel ou électronique) utilisé pour l'acquisition, le stockage, la manipulation, la gestion, le déplacement, le contrôle, l'affichage, l'échange, l'envoi ou la réception automatiques de données ou d'information. Comprend, sans s'y limiter, le matériel informatique, les logiciels, les microprogrammes, le matériel auxiliaire et les ressources connexes.

Terminal d'envoi de données : Technologies et processus connexes qui alimentent le dépôt de données cliniques et font l'objet des recherches de données par l'utilisateur en milieu clinique. Comprend habituellement le système d'information (système d'information hospitalier, système d'information de laboratoire, système d'information clinique, moteur d'interface HL7, etc.) qui se branche automatiquement à [la solution de DSE] pour rendre les données cliniques accessibles.

Exigences de la norme

1. Exigences pour les dépositaires de renseignements sur la santé

1.1. Les dépositaires de renseignements sur la santé (DRS) ne doivent utiliser que les algorithmes cryptographiques approuvés pour [la solution de DSE]. La liste des algorithmes cryptographiques approuvés se trouve à l'annexe A intitulée *Algorithmes cryptographiques approuvés*.

1.2. Les DRS doivent évaluer toute proposition de solution cryptographique à mettre en place dans leurs services de gestion d'identité et leurs terminaux d'envoi de données.

1.3. Les DRS doivent veiller à ce que les solutions cryptographiques en place dans leurs services de gestion d'identité et leurs terminaux d'envoi de données refusent tout accès en cas de panne.

1.4. Les DRS devraient utiliser un chiffrement pour matériel (au lieu d'un chiffrement pour logiciel) dans leurs services de gestion d'identité et leurs terminaux d'envoi de données.

1.5. Lorsque les DRS emploient des appareils matériels cryptographiques (p. ex., RSA Token) pour leurs services de gestion d'identité et leurs terminaux d'envoi de données, ils doivent veiller à ce que les appareils respectent au minimum les exigences de boîtier anti-sabotage de la norme de troisième niveau 140.2 des Federal Information Processing Standards (FIPS) des États-Unis.

1.6. Les DRS ne devraient utiliser de solutions cryptographiques logicielles pour leurs services de gestion d'identité et leurs terminaux d'envoi de données qu'aux fins suivantes :

1.6.1. les fonctions cryptographiques unidirectionnelles (ou irréversibles);

1.6.2. les logiciels côté client en situation d'accès à distance;

1.6.3. les produits de chiffrement des données stockés du côté client, par exemple les produits de chiffrement intégraux;

1.6.4. les certificats numériques côté client ou côté serveur.

1.7. En cas de mise en place d'une solution cryptographique logicielle, les DRS doivent veiller à ce que le mot de passe ne soit pas stocké dans un programme, un fichier séquentiel ou un fichier script, à l'exception des certificats numériques SSL sur serveur, dans lequel cas des mesures strictes de contrôle de l'accès doivent être en place pour le fichier qui contient le mot de passe.

Certificats numériques dans les services de gestion d'identité et les terminaux d'envoi de données

1.8. Les DRS doivent veiller à ce que tous les certificats numériques soient révocables avec un système de liste des certificats révoqués protégé de manière cryptographique.

1.9. Les DRS doivent veiller à ce qu'un certificat numérique ne soit considéré comme fiable qu'une fois la validation cryptographique effectuée et que s'il ne figure pas sur une liste de certificats fiables révoqués.

Gestion des clés

1.10. Les DRS doivent protéger les clés cryptographiques pour leurs services de gestion d'identité et leurs terminaux d'envoi de données contre tout accès (dans le cas des clés secrètes et privées), toute modification, toute perte et toute destruction accidentelle ou intentionnelle non autorisés.

1.11. Les DRS doivent veiller à ce que l'équipement utilisé pour générer, charger, stocker et archiver des clés cryptographiques pour leurs services de gestion d'identité et leurs terminaux d'envoi de données soit physiquement protégé contre tout accès ou toute modification non autorisés.

1.12. Les DRS devraient élaborer une méthode pour gérer les clés cryptographiques de leurs services de gestion d'identité et de leurs terminaux d'envoi de données, méthode qui inclut les points suivants :

1.12.1. la génération, la distribution, le chargement, le stockage, le rétablissement, le remplacement, la révocation et la destruction de clés cryptographiques en toute sécurité;

1.12.2. la sauvegarde et l'archivage des clés cryptographiques en toute sécurité.

1.13. Les DRS doivent conserver un registre des clés cryptographiques et des éléments de clé associés à leurs services de gestion d'identité et à leurs terminaux d'envoi de données. Ce registre devrait comprendre les éléments suivants :

1.13.1. le nom de la clé et son but ou son utilisation;

1.13.2. le type de clé;

1.13.3. la date de génération de la clé;

1.13.4. le numéro de chaque élément et la quantité totale d'éléments;

1.13.5. le lieu de stockage;

1.13.6. tous les responsables de la clé depuis sa génération, y compris les dates de changement de responsable;

1.13.7. la date à laquelle la clé a été détruite et la preuve de la destruction.

1.14. Les DRS devraient passer en revue le registre des clés associées à leurs services de gestion d'identité et à leurs terminaux d'envoi de données une fois par année.

1.15. Les DRS devraient conserver des journaux de tout cas où des clés, des éléments de clé ou d'autres éléments connexes associés à leurs services de gestion d'identité et à leurs terminaux d'envoi de données sont générés, supprimés du stockage ou chargés sur un appareil cryptographique. Ces journaux peuvent comprendre les éléments suivants :

1.15.1. le nom de la clé et son but ou son utilisation;

1.15.2. la date et l'heure;

1.15.3. le numéro de l'élément;

1.15.4. le but de l'accès;

1.15.5. le nom et la signature du responsable qui accède à l'élément;

1.15.6. le numéro de l'emballage inviolable avant la suppression (s'il y a lieu).

1.16. Les DRS doivent restreindre l'accès aux clés cryptographiques ou aux éléments de clé et aux dispositifs contenant les clés de leurs services de gestion d'identité et de leurs terminaux d'envoi de données aux responsables désignés ou à leurs remplaçants.

1.17. Les DRS devraient stocker les clés de leurs services de gestion d'identité et de leurs terminaux d'envoi de données au moins d'endroits et sous le moins de formes possible.

Génération des clés

1.18. Les DRS doivent veiller à ce que les clés et les éléments de clé associés à leurs services de gestion d'identité et à leurs terminaux d'envoi de données soient tous générés à l'aide d'un générateur de nombres aléatoires ou pseudo-aléatoires qui effectue tous les tests de base assurant le caractère statistiquement aléatoire des nombres comme le définit la publication spéciale du National Institute of Standards and Technology (NIST) 800-22, révision 1a.

1.19. Pour assurer la confidentialité des clés secrètes associées à leurs services de gestion d'identité et à leurs terminaux d'envoi de données, les DRS doivent veiller à ce que ces dernières n'existent que sous les formes suivantes :

1.19.1. texte en clair à l'intérieur de la mémoire protégée d'un module de sécurité inviolable;

1.19.2. cryptogramme à l'extérieur de la mémoire protégée d'un module de sécurité inviolable;

1.19.3. deux éléments ou plus, conservés selon les principes de connaissance répartie et de double contrôle.

1.20. Les DRS devraient exiger qu'au moins deux mandataires ou fournisseurs de services électroniques autorisés surveillent le résultat du processus de génération de clés associées à leurs services de gestion d'identité et à leurs terminaux d'envoi de données.

1.21. Les DRS doivent veiller à ce qu'aucun système informatique multiutilisateur ou multifonctionnel ne serve à la génération de clés lorsqu'il y a des risques que des clés secrètes ou des éléments de clés secrètes en texte clair se trouvent dans une mémoire non protégée.

Chargement des clés

1.22. Les DRS doivent veiller à ce que les clés ou les éléments de clé associés à leurs services de gestion d'identité et à leurs terminaux d'envoi de données ne soient jamais chargés (ou rechargés) lorsqu'on soupçonne que la clé, l'élément de clé ou le dispositif cryptographique sont étés compromis.

Utilisation des clés

1.23. Les DRS ne doivent utiliser de clés cryptographiques dans leurs services de gestion d'identité et leurs terminaux d'envoi de données que pour une seule fin et ne doivent jamais faire passer les mêmes clés d'environnements de production à d'autres environnements.

Durée de vie et destruction des clés

1.24. La durée de vie d'une clé ne doit pas dépasser sept ans.

1.25. Les DRS doivent remplacer une clé non compromise utilisée pour leurs services de gestion d'identité et leurs terminaux d'envoi de données à la date de fin de la durée de vie ou avant.

1.26. Si une clé ou un élément de clé associé aux services de gestion d'identité et aux terminaux d'envoi de données d'un DRS a été compromis ou qu'on soupçonne une compromission, le DRS doit faire ce qui suit :

1.26.1. remplacer la clé compromise ou dont on soupçonne la compromission le plus tôt possible. La clé de remplacement ne doit pas être une variante de la clé d'origine;

1.26.2. inspecter le dispositif cryptographique pour voir s'il y a eu des modifications non autorisées avant l'installation d'une nouvelle clé ou d'un nouvel élément de clé.

1.27. Les DRS doivent rapidement révoquer toutes les clés et tous les éléments de clés associés à leurs services de gestion d'identité et à leurs terminaux d'envoi de données lorsqu'elles ne sont plus nécessaires et veiller à ce que les clés ou les éléments de clé soient détruits de manière sécuritaire.

1.28. Les DRS devraient exiger la présence des responsables de clés à titre de témoins lors de la destruction des clés ou des éléments de clé associés à leurs services de gestion d'identité et à leurs terminaux d'envoi de données et l'enregistrement de l'information relative à la destruction aux fins d'audit. Le registre ainsi créé peut comprendre les éléments suivants :

1.28.1. la date et l'heure de la destruction;

1.28.2. la raison de la destruction;

1.28.3. le nom complet et la signature de la personne qui a autorisé la destruction;

1.28.4. le nom complet et la signature de la personne qui a effectué la destruction;

1.28.5. le nom complet et la signature des personnes ayant assisté à la destruction.

Responsables de clés

1.29. Le dirigeant principal de l'information ou son délégué doit nommer un responsable pour chaque clé.

1.30. Les DRS doivent veiller à ce que les responsables de clés associées à leurs services de gestion d'identité et à leurs terminaux d'envoi de données traitent la clé ou l'élément de clé sous leur garde comme un élément de catégorie restreinte conformément à la Norme sur la gestion de l'information et des éléments d'actif.

1.31. Les DRS doivent veiller à ce que chaque clé cryptographique ou élément de clé ait le moins de responsables possible selon les besoins.

1.32. Les DRS doivent veiller à ce que les responsables de clés connaissent leur devoir de ne jamais divulguer la clé ou l'élément de clé sous leur garde à quiconque, pas même à un gestionnaire ou à un auditeur, sauf à un autre responsable autorisé pour cette même clé ou ce même élément de clé.

2. Exigences pour l'équipe de [la solution de DSE]

2.1. Seuls les algorithmes cryptographiques approuvés par l'équipe de [la solution de DSE] doivent être utilisés dans [la solution de DSE]. La liste des algorithmes cryptographiques approuvés se trouve à l'annexe A intitulée *Algorithmes cryptographiques approuvés*.

2.2. L'équipe de [la solution de DSE] doit veiller à ce que chaque proposition de solution cryptographique à mettre en place dans [la solution de DSE] soit évaluée par un spécialiste de sécurité de l'information.

2.3. L'équipe de [la solution de DSE] ne doit implanter que des solutions cryptographiques qui refusent tout accès en cas de panne.

2.4. L'équipe de [la solution de DSE] doit veiller à ce que des procédures officielles en cas d'imprévu soient rédigées avant la mise en œuvre d'une solution cryptographique dans un environnement de production. Ces procédures doivent être rendues accessibles à tous les intervenants concernés.

2.5. L'équipe de [la solution de DSE] devrait utiliser un chiffrement pour matériel (au lieu d'un chiffrement pour logiciel, p. ex., RSA Token) dans des environnements de stockage ou de traitement de renseignements personnels sur la santé.

2.6. Lorsque l'équipe de [la solution de DSE] emploie des appareils matériels cryptographiques, elle doit veiller à ce que les appareils respectent au minimum les exigences de boîtier anti-sabotage de la norme de troisième niveau 140.2 des Federal Information Processing Standards (FIPS) des États-Unis.

1.33. L'équipe de [la solution de DSE] ne doit permettre d'utiliser des solutions cryptographiques logicielles qu'aux fins suivantes :

2.6.1. les fonctions cryptographiques unidirectionnelles (ou irréversibles);

2.6.2. les logiciels côté client en situation d'accès à distance;

2.6.3. les produits de chiffrement des données stockés du côté client, par exemple les produits de chiffrement intégraux;

2.6.4. les certificats numériques côté client ou côté serveur;

2.6.5. le stockage de données dans des centres de données.

2.7. En cas de mise en place d'une solution cryptographique logicielle, l'équipe de [la solution de DSE] doit veiller à ce que le mot de passe ne soit pas stocké dans un programme, un fichier séquentiel ou un fichier script, à l'exception des certificats numériques SSL sur serveur, dans lequel cas des mesures strictes de contrôle de l'accès doivent être en place pour le fichier qui contient le mot de passe.

2.8. L'équipe de [la solution de DSE] doit protéger par voie cryptographique l'intégrité des clés, surtout lorsque ces dernières sont situées à un endroit accessible au public (sur un serveur Web branché à Internet, par exemple).

Certificats numériques

2.9. L'équipe de [la solution de DSE] doit veiller à ce que tous les certificats numériques soient révocables.

2.10. L'équipe de [la solution de DSE] doit veiller à ce qu'un certificat numérique ne soit considéré comme fiable qu'une fois la validation cryptographique effectuée et que s'il ne figure pas sur une liste de certificats fiables révoqués.

Gestion des clés

2.11. L'équipe de [la solution de DSE] doit protéger ses clés cryptographiques contre tout accès (dans le cas des clés secrètes et privées), toute modification, toute perte et toute suppression accidentelle ou intentionnelle non autorisés.

2.12. L'équipe de [la solution de DSE] doit veiller à ce que l'équipement utilisé pour générer, charger, stocker et archiver des clés cryptographiques soit physiquement protégé contre tout accès ou toute modification non autorisés.

1.34. L'équipe de [la solution de DSE] doit élaborer une méthode de gestion des clés cryptographiques, méthode qui inclut les points suivants :

2.12.1. la génération, la distribution, le chargement, le stockage, le rétablissement, le remplacement, la révocation et la destruction de clés cryptographiques en toute sécurité;

2.12.2. la sauvegarde et l'archivage des clés cryptographiques en toute sécurité.

Ces procédures doivent être rendues accessibles à tous les intervenants concernés.

1.35. L'équipe de [la solution de DSE] doit conserver un registre de toutes ses clés cryptographiques et de tous ses éléments de clé. Ce registre devrait comprendre les éléments suivants :

2.12.3. le nom de la clé et son but ou son utilisation;

2.12.4. le type de clé;

2.12.5. la date de génération de la clé;

2.12.6. le numéro de chaque élément et la quantité totale d'éléments;

2.12.7. le lieu de stockage;

2.12.8. tous les responsables de la clé depuis sa génération, y compris les dates de changement de responsable;

2.12.9. la date à laquelle la clé a été détruite et la preuve de la destruction.

2.13. L'équipe de [la solution de DSE] devrait passer en revue le registre de ses clés cryptographiques une fois par année.

1.36. L'équipe de [la solution de DSE] doit conserver des journaux de tout cas où des clés, des éléments de clé ou d'autres éléments connexes sont générés, supprimés du stockage ou chargés sur un appareil cryptographique. Ces journaux devraient inclure les éléments suivants :

2.13.1. le nom de la clé et son but ou son utilisation;

2.13.2. la date et l'heure;

2.13.3. le numéro de l'élément;

2.13.4. le but de l'accès;

2.13.5. le nom et la signature du responsable qui accède à l'élément;

2.13.6. le numéro de l'emballage inviolable avant la suppression (s'il y a lieu).

2.14. L'équipe de [la solution de DSE] devrait passer en revue les journaux d'audit de leurs clés une fois par année.

2.15. L'équipe de [la solution de DSE] doit restreindre l'accès aux clés secrètes ou aux éléments de clés secrètes, aux dispositifs contenant les clés et aux documents associés aux responsables désignés et à leurs remplaçants. Il suffit habituellement de désigner un responsable principal et un remplaçant pour chaque clé ou élément de clé.

2.16. L'équipe de [la solution de DSE] doit stocker les clés au moins d'endroits et sous le moins de formes possible.

2.17. L'équipe de [la solution de DSE] doit veiller à ce que les copies de sauvegarde de clés secrètes ne servent qu'à rétablir des clés accidentellement détruites ou autrement inaccessibles. Les sauvegardes ne doivent prendre que l'une des formes permises pour le stockage pour les clés en question.

2.18. L'équipe de [la solution de DSE] doit veiller à ce que les copies de sauvegarde de clés secrètes soient stockées avec des mesures strictes de contrôle de l'accès selon le principe de double contrôle et qu'elles fassent l'objet au moins du même degré de contrôle que les clés opérationnelles.

2.19. L'équipe de [la solution de DSE] doit veiller à ce que la création des copies de sauvegarde (y compris par clonage) ne se fasse que par au moins deux personnes autorisées. Toutes les exigences applicables aux clés originales s'appliquent aussi à toute copie de sauvegarde des clés et de leurs éléments.

2.20. L'équipe de [la solution de DSE] doit veiller à ce que les clés secrètes et les éléments de clés secrètes qui ne servent plus ou qui ont été remplacés soient révoqués et détruits de manière sécuritaire.

Génération des clés

2.21. L'équipe de [la solution de DSE] ne doit permettre la génération d'une clé que par la personne qui en est responsable.

2.22. L'équipe de [la solution de DSE] doit veiller à ce que les clés et les éléments de clé soient tous générés à l'aide d'un générateur de nombres aléatoires ou pseudo-aléatoires qui effectue tous les tests de base assurant le caractère statistiquement aléatoire des nombres comme le définit la publication spéciale du National Institute of Standards and Technology (NIST) 800-22, révision 1a.

1.37. Pour assurer la confidentialité de ses clés secrètes, l'équipe de [la solution de DSE] doit veiller à ce que ces dernières n'existent que sous les formes suivantes :

1.37.1. texte en clair à l'intérieur de la mémoire protégée d'un module de sécurité inviolable;

1.37.2. cryptogramme à l'extérieur de la mémoire protégée d'un module de sécurité inviolable;

1.37.3. deux éléments ou plus, conservés selon les principes de connaissance répartie et de double contrôle.

2.23. L'équipe de [la solution de DSE] devrait exiger qu'au moins deux mandataires ou fournisseurs de services électroniques autorisés surveillent le résultat du processus de génération de clés.

2.24. L'équipe de [la solution de DSE] doit veiller à ce qu'aucun système informatique multiutilisateur ou multifonctionnel ne serve à la génération de clés lorsqu'il y a des risques que des clés secrètes ou des éléments de clés secrètes en texte clair se trouvent dans une mémoire non protégée.

Distribution des clés

2.25. L'équipe de [la solution de DSE] doit veiller à ce que toute clé de chiffrement de clés soit transférée par envoi physique des composants de la clé séparément les uns des autres par divers moyens de communication ou par voie électronique sous forme de cryptogramme.

2.26. L'équipe de [la solution de DSE] doit veiller à ce que tout signe d'altération de l'emballage entraîne la destruction et le remplacement des éléments de clé ainsi que des clés chiffrées faisant partie de la clé combinée.

2.27. L'équipe de [la solution de DSE] doit veiller à ce que des mécanismes soient en place pour que seuls les responsables de clés autorisés puissent mettre des éléments de clé dans un emballage inviolable aux fins de transmission et que seuls les responsables autorisés ouvrent à leur réception les emballages inviolables contenant les éléments de clé.

Chargement des clés

2.28. L'équipe de [la solution de DSE] doit veiller à ce que les clés ou les éléments de clé ne soient jamais chargés (ou rechargés) lorsqu'on soupçonne que la clé, l'élément de clé ou le dispositif cryptographique a été compromis.

2.29. L'équipe de [la solution de DSE] doit veiller à ce que les clés secrètes non chiffrées soient intégrées aux dispositifs cryptographiques suivant les principes de double contrôle et de connaissance répartie. Dans les cas où on utilise un dispositif de chargement de clés sécurisé, seul le principe de double contrôle est à respecter.

2.30. L'équipe de [la solution de DSE] doit veiller à ce que tout matériel informatique utilisé pour le chargement de clés fasse l'objet d'un contrôle et soit conservé dans un environnement sécuritaire selon le principe de double contrôle.

2.31. L'équipe de [la solution de DSE] devrait exiger des responsables de clés qu'ils examinent tous les branchements de câbles avant le chargement de clés pour s'assurer qu'ils n'ont pas été altérés ou compromis.

Utilisation des clés

2.32. L'équipe de [la solution de DSE] doit définir et implanter des procédures qui préviennent ou détectent les substitutions non autorisées d'une clé pour une autre ou d'un élément de clé pour un autre ou le fonctionnement de tout dispositif cryptographique sans clés ou éléments de clé valables.

2.33. L'équipe de [la solution de DSE] doit veiller à ce que les clés cryptographiques ne soient utilisées que pour une seule fin et ne doivent jamais faire passer les mêmes clés d'environnements de production à d'autres environnements.

2.34. L'équipe de [la solution de DSE] doit veiller à ce que toutes les clés secrètes utilisées pour toute fonction soient propres au dispositif concerné, sauf si le contraire arrive par pur hasard.

Durée de vie et destruction des clés

2.35. La durée de vie d'une clé ne doit pas dépasser sept ans.

2.36. L'équipe de [la solution de DSE] doit veiller à ce que soit remplacée une clé non compromise à la date de fin de la durée de vie ou avant.

1.38. Si une clé ou un élément de clé a été compromis ou qu'on soupçonne une compromission, l'équipe de [la solution de DSE] doit faire ce qui suit :

1.38.1. remplacer la clé compromise ou dont on soupçonne la compromission le plus tôt possible. La clé de remplacement ne doit pas être une variante de la clé d'origine;

1.38.2. inspecter le dispositif cryptographique pour voir s'il y a eu des modifications non autorisées avant l'installation d'une nouvelle clé ou d'un nouvel élément de clé.

2.37. L'équipe de [la solution de DSE] doit veiller à ce que ses clés soient rapidement révoquées lorsqu'elles ne sont plus utiles et à ce que toute clé soit détruite conformément à la Norme sur la gestion de l'information et des éléments d'actif.

1.39. L'équipe de [la solution de DSE] doit veiller à ce qu'il y ait présence des responsables de clés à titre de témoins lors de la destruction des clés ou des éléments de clé et enregistrement de l'information relative à la destruction aux fins d'audit. Le registre ainsi créé peut comprendre les éléments suivants :

1.39.1. la date et l'heure de la destruction;

1.39.2. la raison de la destruction;

1.39.3. le nom complet et la signature de la personne qui a autorisé la destruction;

1.39.4. le nom complet et la signature de la personne qui a effectué la destruction;

1.39.5. le nom complet et la signature des personnes ayant assisté à la destruction.

Responsables de clés

2.38. Le dirigeant principal de l'information ou son délégué doit nommer un responsable pour chaque clé.

2.39. L'équipe de [la solution de DSE] doit veiller à ce que les responsables de clés traitent la clé ou l'élément de clé sous leur garde comme un élément de catégorie restreinte conformément à la Norme sur la gestion de l'information et des éléments d'actif.

2.40. L'équipe de [la solution de DSE] doit veiller à ce que chaque clé cryptographique ou élément de clé ait le moins de responsables possible selon les besoins.

2.41. L'équipe de [la solution de DSE] doit veiller à ce que les responsables de clés connaissent leur devoir de ne jamais divulguer la clé sous leur garde à quiconque, pas même à un gestionnaire ou à un auditeur, sauf à un autre responsable autorisé pour cette même clé.

2.42. L'équipe de [la solution de DSE] ne doit jamais permettre à un responsable de clés d'avoir sous sa garde plus d'un élément de clé pour la même clé même si la garde des éléments ne se fait pas au même moment.

Dérogations Toute dérogation à la norme doit être approuvée par l'organisme de surveillance compétent, lequel l'autorisera uniquement lorsque la situation le justifie et au degré minimal nécessaire pour la justification apportée.

Application Tous les cas de non-respect seront examinés par l'organisme de surveillance compétent. L'organisme de surveillance compétent a le pouvoir d'imposer les sanctions appropriées, ce qui peut inclure la cessation des ententes avec le DRS ou les fournisseurs de services électroniques ou la cessation des privilèges d'accès des mandataires, et de demander des mesures correctives.

References

Lois

- LPRPS, art. 12 et 13 et partie V.1
- O. Reg. 329/04, art. 6

Normes internationales

- ISO/IEC 27001:2005 – Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences
- ISO/IEC 27002:2005 – Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information
- ISO/IEC 27005:2008 – Technologies de l'information – Techniques de sécurité – Gestion des risques en sécurité de l'information
- ISO 27799:2008 – Informatique de santé – Management de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002
- Publication spéciale du NIST 800-22, révision 1a – A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
- FIPS 140-2 – Security Requirements for Cryptographic Modules

Documents de politiques et de normes sur les DSE de Santé Ontario

- Politique de sécurité de l'information
- Norme d'utilisation acceptable des données et des technologies de l'information
- Norme sur le contrôle de l'accès aux systèmes et les processus de gestion d'identité connexes
- Norme sur les pratiques d'inscription des autorités locales d'enregistrement (en anglais)
- Norme de cyberSanté Ontario au sujet des prestataires qui assurent la gestion fédérée de l'identité (en anglais)
- Norme sur la cryptographie
- Norme sur les fournisseurs de services électroniques
- Norme sur la gestion des incidents de sécurité de l'information
- Norme sur la gestion de l'information et des éléments d'actif
- Norme sur les réseaux et les opérations
- Norme sur la journalisation de sécurité et la surveillance
- Norme sur le cycle de développement de systèmes
- Norme sur la sécurité matérielle

- Norme sur la gestion des menaces et des risquesPolitiques harmonisées sur la protection de la vie privée (en anglais)

Référence à Inforoute Santé du Canada

- Exigences en matière de protection de la confidentialité et de sécurité d'Inforoute Santé du Canada (version 1.1 révisée le 7 février 2005)

Autre

- Directives concernant la sécurité des transmissions par télécopieur du commissaire à l'information et à la protection de la vie privée de l'Ontario (janvier 2003)

Annexe A : Algorithmes cryptographiques approuvés

Algorithme	Longueur minimale de la clé	À quelle utilisation conviennent-ils?
Algorithmes symétriques		
AES	AES 256	Chiffrement des données : • Session • Stockage o Sauvegarde o Archives Chiffrement des clés : • Session • Stockage o Sauvegarde o Archives
Skipjack	80 bits avec 32 itérations	o Chiffrement des données : Rejetée o Décryptage: Systèmes hérités autorisés.
Triple DES	112 bits	Chiffrement des données : • Session • Stockage o Sauvegarde o Archives Chiffrement des clés : • Session • Stockage o Sauvegarde o Archives
scrypt	256 bits	Chiffrement des données : • Session • Stockage o Sauvegarde. o Archives
Algorithmes asymétriques		
À courbe elliptique	160 bits	Chiffrement des données : • Session • Stockage o Sauvegarde o Archives Signature numérique Chiffrement des clés : • Session • Stockage o Sauvegarde o Archives Création d'une clé de session
RSA	2048 bits	Chiffrement des données : • Session • Stockage o Sauvegarde o Archives Signature numérique Chiffrement des clés : • Session • Stockage o Sauvegarde o Archives Création d'une clé de session
MAC et algorithmes de hachage		
AES MAC	128 bits	Authentification de message
MD5[1]	128 bits avec 16 itérations	Authentification de message et condensé de message
SHA-1[2]	Sans objet	Authentification de message et condensé de message
SHA-2	Sans objet	Authentification de message et condensé de message
TDES (triple DES) MAC	112 bits	Authentification de message
Argon2	128 bits	Authentification de message
Signatures numériques		
Signature numérique	1024 bits	Signature numérique
Signature numérique à courbe elliptique	160 bits	Signature numérique
Signature numérique RSA	2048 bits	Signature numérique

[1] Tout *nouveau* MAC ou algorithme de hachage ne doit pas être fondé sur l'algorithme Md5.
[2] Tout *nouveau* MAC ou algorithme de hachage ne doit pas être fondé sur l'algorithme SHA-1.

Algorithme	Longueur minimale de la clé	À quelle utilisation conviennent-ils?
Certificats numériques		
Conformes à la norme X.509 v3	Sans objet	Mise en relation d'une clé publique avec une identité précise
Algorithmes de transport et algorithmes convenus		
Diffie-Hellman	1024 bits	Création d'une clé de session numérique
Diffie-Hellman à courbe elliptique	160 bits	Création d'une clé de session numérique
Protocoles cryptographiques		
TLS 1.1 et versions ultérieures	Sans objet	Protocole d'authentification et de chiffrement des communications entre parties authentifiées