Agence nationale de sécurité du médicament et des produits de santé

Compte-rendu de séance

Date du document : 29/06/2018

Direction des dispositifs médicaux de diagnostic et des plateaux techniques
Pôle Dispositifs Médicaux médicaux radiogènes, injection, aide patient, logiciels
Sophie Nogaret

Comité Scientifique Spécialisé Temporaire

« Cyber sécurité des logiciels dispositifs médicaux »

Séance du Vendredi 13 avril 2018 de 13h30 à 16h30 en salle A014

Programme de séance		
1.	**Introduction**	
1.1	Présentation rapide des intervenants	
1.2	Adoption de l'ordre du jour	
2.	**Point Etape**	
2.1	Rappel de la feuille de route	
2.2	Bilan des précédentes réunions → état des lieux de l'avancement du projet	
3.	**Projet de recommandations à l'attention des fabricants de Dispositifs Médicaux**	
3.1	Discussion et travail de fond sur le document	
4.	**Conclusion**	

Noms des participants	Membres/ secrétaire	Présent	Absent/ excusé
Vincent ARCHER	Membre	Présent	
Bruno BLANCHET	Membre	Présent	
Luc CHAUSSON	Membre	Présent	
Alain ESPINOUX	Membre		Excusé
Régis GUILLEMAUD	Membre		Excusé
Alain MERLE	Membre	Présent (Téléconférence)	
Cédric CARTAU	Membre	Présent (Téléconférence)	
Benjamin MORIN	Membre	Présent	
Stéphane PASQUIER	Membre	Présent	
Vincent LOUIS	Membre	Présent (Téléconférence)	
Philippe LOUDENOT	Membre		Excusé
Bernard CASSOU MOUNAT	Membre		Excusé
Thierry SIRDEY	ANSM Secrétaire de séance	Présent	
Gwennaelle EVEN	ANSM	Présent	
Hélène BRUYERE	ANSM	Présent	
Sophie NOGARET	ANSM	Présent	

1. Introduction

1.1.Présentation des intervenants

Il est rappelé aux intervenants que la séance est enregistrée puis un tour de table est effectué : les différents membres du CSST et les personnes internes à l'Agence se sont présentés. La présente séance est composée de 8 experts (dont 3 par téléconférence) et de 4 personnes de l'ANSM.

Aucune situation de conflit d'intérêt majeur n'a été déclarée, ni retenue au cours de la séance du 13 avril 2018.

L'ANSM rappelle aux experts que suite au départ de la personne en charge du projet, un nouvel évaluateur a repris le sujet depuis janvier 2018. Pour cette raison, le calendrier a été modifié et la troisième séance a été décalée au mois d'avril 2018.
Il est rappelé que la seconde séance a consisté à la prise en compte des commentaires des experts sur le projet de document et l'élaboration de son plan.

Suite au précédent CSST, la structure du document a changé. Le texte a été transmis aux experts en amont de la réunion. L'ANSM remercie les experts pour leurs nombreuses remarques qui vont alimenter la discussion en séance.

<u>3 documents ont été fournis aux experts en séance :</u>

-Une présentation PowerPoint d'introduction.
-Un tableau Excel récapitulant l'ensemble des remarques des experts.
-Une version du document en mode suivi des corrections dans lequel l'ensemble des commentaires des experts ont été combinés.

1.2.Adoption de l'ordre du jour

L'ordre du jour est adopté à l'unanimité.

2. Point Etape

2.1. Rappel de la feuille de route

L'ANSM rappelle que le CSST a été créée en juin 2017. Les experts sont nommés jusqu'en juin 2018. Au regard de l'avancement du projet, il est proposé aux experts prolonger le CSST pour 1 année supplémentaire sous réserve de leur accord de participation. L'objectif est de publier les recommandations pour la fin de l'année 2018.

Réponse des experts : accord de principe pour une participation au CSST une année supplémentaire.

Compte tenu de l'état de l'art et de la complexité du sujet, il est décidé de rédiger une première version des recommandations comportant les points critiques/essentiels. Ce document sera amené à évoluer et à s'enrichir dans le futur.

De plus, les experts sont informés qu'un groupe de travail « software » se réunit depuis 2010 au sein de la commission européenne. L'objectif de ce groupe est d'établir des référentiels autour de la règlementation des DM appliquée aux logiciels. L'initiative française autour de la « Cyber » a contribué à la création d'un sous-groupe de travail sur ce thème dont l'objectif à terme est de rédiger des recommandations uniformisées au sein de la communauté européenne.

La première étape reste la réalisation d'un document à portée nationale. Et dans le contexte de marquage CE, le document en cours d'élaboration au niveau national pourrait servir de base à la rédaction de recommandations européennes.

Pour conclure, l'ANSM rappelle brièvement les éléments discutés lors des 2 CSST précédents :
-CSST du 26/06/2017 : Présentation des objectifs du groupe et discussion sur les définitions
-CSST du 11/10/2017 : Travail sur le plan du document et premières discussions sur les recommandations
Il avait été décidé de structurer les recommandations autour du cycle de vie du logiciel.

2.2.Bilan des commentaires reçus

Avant d'entamer la discussion sur le fond du document, l'ANSM fait un bilan général des commentaires transmis par les experts.

Au total, 180 commentaires ont été rédigés par les experts suite à la revue du document.
Plusieurs experts s'interrogent notamment sur la partie analyse de risques et la manière de l'aborder. Ce point sera discuté en séance.
De plus, l'ANSM indique qu'elle souhaite avoir l'expertise des membres sur certaines parties spécifiques et techniques telles que :
- l'utilisation de disques et supports amovibles,
- la cryptographie
- la définition des attaques.
-les dispositifs implantables : la question se pose de rédiger des recommandations adaptées spécifiquement à ce type de DM.

Plusieurs experts ont également fait les remarques générales suivantes :
- parler du règlement DM plutôt que des directives
- préciser la terminologie : terme générique pour désigner l'ensemble des cibles du document
- définir la sureté de fonctionnement
- aborder la notion de cyber défense.

Tous ces éléments seront discutés en cours de séance lorsque les échanges porteront sur les parties du texte correspondantes.
Les 180 commentaires reçus ont été regroupés en 44 items dont 25 prioritaires qui seront abordés en séance.

3. Projet de recommandations à l'attention des fabricants de Dispositifs Médicaux

3.1.Terminologie

Les recommandations concernent les logiciels DM et les logiciels intégrés dans un DM, qu'ils soient connectés ou non. Cependant, afin de ne pas alourdir le texte, il est décidé de définir au début du document une formulation simple définissant l'ensemble des produits concernés.
Plusieurs formulations sont proposées et le terme DM intégrant du logiciel est choisi.
Il est également décidé de systématiser l'emploi du terme cybersécurité pour plus de lisibilité.

3.2.Définition des critères prioritaires

Beaucoup de remarques portent sur la définition des critères prioritaires.
Une proposition de reformulation basée sur la combinaison de plusieurs sources bibliographiques a été rédigée. Cette proposition est validée en séance.

Les experts indiquent que l'emploi du terme traçabilité peut porter à confusion car il peut avoir une autre signification, notamment dans le mode du DM. Il a donc été choisi de parler d'auditabilité comme critère prioritaire.

3.3. Distinction entre sécurité et sûreté

Les experts rappellent que la question de la dangerosité pour le patient se place sur un autre plan et que l'innocuité du DM sur le plan médical est un prérequis ; les mesures de sûreté et de sécurité mises en place doivent garantir que ce prérequis reste vrai tout au long de la vie du DM.
Ils rappellent également que la sureté prend en compte les erreurs d'utilisation.

3.4. Attaque de dispositifs médicaux intégrant du logiciel

L'ANSM indique que les attaques de DM sont abordées de différentes manières selon les sources bibliographiques. Cependant, le regroupement des différentes définitions alourdi le texte.
Les experts proposent de faire référence aux critères prioritaires pour définir les attaques. Il est décidé de ne pas tenir compte des motivations des attaques et de ne prendre en compte que leurs conséquences.

Les experts rappellent qu'il peut être nécessaire d'avoir un accès physique au dispositif pour mener une attaque : ce point devra être intégré au niveau des définitions des critères.

3.5.Analyse de risques

L'ANSM s'interroge sur la manière d'aborder l'analyse de risque car l'approche dans le mode du dispositif médical n'est pas superposable avec une problématique de cybersécurité.

Dans un premier temps, il est décidé de définir l'analyse de risque et de rappeler ce que l'on attend de cette analyse de risque avant de donner les méthodes.

Les experts proposent de repartir de la norme 14971. Cette dernière ne prenant pas en compte la notion d'attaque, d'usage malveillant ni la notion de vulnérabilité, le document devra la compléter selon 3 axes :

- Définir les actifs et biens essentiels
- Préciser la notion de vulnérabilité
- Préciser les analyses d'impact sur les aspects intégrité, critères prioritaires

En complément, il est proposé de prendre en compte dans le document d'autres aspects tels que le DM au travers du système d'information et le DM dans son environnement. Ces éléments ne sont pas encadrés directement par la norme NF EN ISO14971.

Selon la norme NF EN ISO 14971, il revient au fabricant de définir les risques acceptables et de les documenter. Il est décidé de mentionner cette notion et de renvoyer à la norme NF EN ISO 14971.

La méthode EBIOS doit également être citée comme une méthode d'analyse de risque parmi d'autres, en exemple. Il est également proposé de mentionner d'autres méthodes et d'indiquer leurs avantages et inconvénients.

Un expert soulève la problématique des architectures complexes. En effet, les systèmes étant de plus en plus imbriqués/interconnectés, il apparait insuffisant de réaliser, d'une part, les analyses de risques système par système et, d'autre part, une analyse de risque sur leurs interactions. Ce schéma d'évaluation apparait limitant. Dans ce cas, l'utilisation d'outils informatiques permettrait de faciliter la démarche via des systèmes de modélisation. Après discussion, il apparait prématuré d'aborder cette notion : une proposition de modélisation obligatoire ne peut pas rentrer dans le scope des recommandations compte tenu des pratiques actuelles.

L'idée est d'évaluer le risque de propagation des menaces dans un système et de rendre le système robuste face à une défaillance. Les fabricants devront avoir une vue compositionnelle de leur système qui sera formalisée dans un langage informatique. Le groupe souligne qu'il ne s'agit pas de l'imposer mais de la recommander. Il est également proposé de citer les méthodes s'appliquant aux systèmes complexes tels que l'interaction entre 2 serveurs d'un système. L'idée est d'évaluer l'impact d'une attaque sur ce type de système.

Le réseau informatique d'un hôpital n'étant pas un DM, la gestion des risques d'un SIH est à côté hors du champ du document. Par contre, il faut parler prendre en compte le fait que le DM sera intégré dans un SIH. Les experts soulignent qu'aucune norme ne prend en compte cet aspect. Il existe un paragraphe dans la norme IEC80001 qui traite de la gestion des risques pour les SIH.
Le groupe décide évoquer le cas des DM intégrés dans un SIH à ce niveau-là. Ce point pourrait être illustré avec des exemples.

En résumé, les experts proposent d'identifier une situation de cybersécurité et de voir comment la traiter dans la cadre de la NF EN ISO 14971 et de la compléter avec les éléments manquants.
Exemple choisi : Firmware
Les experts indiquent qu'il faudra citer les éléments de fonctions de sécurité à appliquer.

L'ANSM demande aux experts de détailler la manière de l'aborder. Ils proposent de reprendre la trame de la NF EN ISO 14971 pour analyser et décrire une situation dangereuse puis d'estimer la probabilité d'occurrence, la criticité et enfin choisir les options de réduction des risques.
Il est proposé de prendre l'exemple du logiciel malveillant Wannacry et de demander à un ou plusieurs fabricants de nous fournir son analyse pour illustrer ce point.

3.6. Introduction des recommandations

Selon les experts, la partie recommandation est abordée trop tardivement dans le document et devrait être rattachée à l'analyse de risques. Après discussion, le groupe souhaite que l'analyse de risque soit la première recommandation et que de cette analyse de risque découle le reste des recommandations.
L'ANSM demande l'avis aux experts sur la définition des biens à protéger a minima. Ils proposent de remplacer le terme « a minima » par « exemple ».
Ils indiquent que les biens à protéger doivent être identifiés par le fabricant lors de la réalisation de l'analyse de risque. Ils souhaitent également que soit rappelé ce qui est attendu de l'analyse de risque du fabricant.

Il est donc décidé en séance de modifier la structure du document en intégrant l'analyse de risque ainsi que la définition des biens à protéger, dans la partie recommandations.

Discussion concernant l'exemple proposé :
Si le fabricant identifie le Firmware comme un bien à protéger, il devra dire pourquoi en définissant les biens essentiels et les mesures à prendre pour le protéger.
L'ANSM peut demander l'analyse de risque au fabricant lorsque le dispositif a été victime d'une attaque et ce dernier doit être en mesure de la présenter.
Si la confidentialité n'est pas identifiée comme un bien à protéger, en revanche, l'intégrité et l'authenticité représentent des biens essentiels. Le fabricant doit avoir mis en place l'ensemble des mesures permettant de les préserver. Un des moyens peut être par exemple les clés cryptographiques. Il est proposé de détailler la démarche et de citer les différents outils disponibles. Quelques exemples peuvent être donnés afin d'illustrer ce point.

Afin de rendre le document plus lisible, il est décidé, suite aux échanges, que les principales recommandations soient indexées dans la version finale. L'opportunité de lister l'ensemble des recommandations dans une fiche récapitulative introductive est également abordée.
Les experts citent en exemple les guides ASIPsanté et HAS comme modèles.

Les experts pensent que le document pourrait contenir une centaine de recommandations en fonction du niveau de granularité retenu. Néanmoins, l'ANSM indique que le document ne devra pas être trop technique, au risque de devenir rapidement obsolète au regard des évolutions constantes du domaine.

Suite aux discussions, le groupe a décidé de rédiger dans un premier temps un document rappelant les grands principes, constitué d'une liste de recommandations fondamentales qui découleront de l'analyse de risque. Le document sera prescriptif pour les fabricants. Dans un second temps, l'élaboration d'un document plus technique pourrait être envisagée.

3.7.Activité de conception du logiciel

Les experts confirment que le principe de minimisation des risques est essentiel. Par contre, les experts indiquent qu'il ne peut pas être appliqué à l'ensemble du logiciel. C'est la raison pour laquelle la définition « des biens » à protéger est primordiale.
En aéronautique, ce principe est appliqué à la partie sécuritaire mais il ne peut être appliqué aux systèmes complexes.
La mention « Limiter l'accès par authentification » ne doit pas être mentionnée dans les dispositions générales mais doit disposer d'une section dédiée.

3.8.Faire un état des lieux des biens à protéger

Selon le groupe, cette partie s'inscrit dans l'analyse des risques et doit être déplacée au début de la partie 3.

3.9.La cryptographie

L'ANSM sollicite la contribution des experts pour la rédaction de cette partie technique.
Les experts indiquent que la cryptographe ne doit pas être définies comme une recommandation mais comme un moyen/un outil de protection des biens à la disposition des développeurs. La cryptographie est une réponse à un risque.
Il faudra lister les standards établis et recommander au fabricant d'utiliser des bibliothèques reconnues et robustes. La cryptographie ne sera mentionnée qu'en exemple dans le document principal et un paragraphe dédié à la cryptographie pourrait être proposé en annexe du document. Il renverra vers un document de référence dans le domaine tel que le Référentiel Général de Sécurité (par exemple).

Les experts informent l'ANSM qu'il existe une initiative comparable en EU. Il faudra chercher le texte et le citer en exemple.

3.10.Gestion des droits

Les experts ont identifié une confusion entre gestion des authentifications et contrôles des accès. Ces deux sections doivent être séparées.

L'authentification préalable va dépendre du dispositif. L'utilisation de certains DM pourra se faire sans authentification préalable. Par contre, toute opération de maintenance nécessitera une authentification en amont.

L'ANSM aborde la question des dispositifs implantables et la possibilité de rédiger une partie dédiée à ce type de DM. Après discussion, il est décidé de rédiger un document le plus générique possible, applicable à l'ensemble des dispositifs médicaux. Le cas des DM implantables sera développé en annexe avec une liste des points applicables ou non et des éléments spécifiques sous la forme d'un tableau récapitulatif.
Il est également proposé de choisir un exemple de DM comme fil conducteur du document.

3.11.Hébergement

L'hébergement est dans le scope des recommandations. Il faut l'aborder comme une mesure de maitrise des risques et renvoyer vers la réglementation hébergeurs de données de santé (HDS) comme un niveau d'exigence minimum à atteindre pour la sécurisation des données. Un lien vers le guide ANSSI « recommandations/exigences d'un prestataire de cloud » pourra être ajouté.
La réglementation sur l'hébergement des données de santé est une réglementation de certification, il est important de préciser que c'est au fabricant de fixer les conditions minimales d'hébergement de son logiciel.

Exemple discuté en séance :
Si un fabricant de DM veut stocker les données dans le cloud, le document lui rappellera qu'il doit être vigilant au moyen de stockage des données et renverra vers la règlementation en la matière ou à des documents qui fixent la sécurité du cloud.
Si un fabricant vend un ensemble de services associés à un DM, il doit respecter les réglementations en lien avec ces services : dans le cas d'une prestation d'hébergement des données de santé, le fabricant doit respecter la réglementation HDS.
Dans le cas où le logiciel fournit des données, le fabricant doit indiquer les exigences minimales pour héberger ce logiciel.

3.12.Environnement d'utilisation

Le fabricant doit définir les compatibilités entre logiciels et matériels, Il s'agit d'une exigence fonctionnelle. Les problèmes de compatibilité ne peuvent pas être un prétexte pour ne pas appliquer la sécurité.

Par exemple, le fonctionnement du logiciel non garanti sur une nouvelle version n'est pas acceptable.
Après discussion, il est décidé de dire que les incompatibilités entre logiciel et matériel doivent être gérées et maitrisées. Une incompatibilité même documentée est potentiellement un frein à la sécurité.
Un autre point est abordé, le fabricant d'un logiciel ne peut pas imposer à l'environnement d'être sécurisé. Le DM doit être le plus autonome possible dans sa sécurité. Il faut minimiser le nombre d'hypothèses dans l'environnement (Exigence de performance 17.4 du règlement).
Il faut plusieurs couches de sécurité mais le fabricant doit penser sa sécurité en amont. Un DM ne peut pas être autonome, le fabricant doit donc faire des hypothèses d'environnement et les documenter.
Par contre, il apparait impossible d'imposer un réseau wifi avec une clé sécurisée. L'ANSM indique que c'est au fabricant de rechercher l'environnement prévisible de son DM et de prescrire un niveau minimal d'exigence en termes de compatibilité.

3.13. Communication

Suite aux discussions, il est décidé de proposer une recommandation très macro sur la confidentialité des données. Cette exigence macro va se décliner en plusieurs points tels que le stockage et le transport. Le cas des DM connectés peut être abordé dans la section sur la confidentialité des données.
Ces notions doivent être abordées dès la partie conception.

3.14.Gestion des supports amovibles

Le groupe s'interroge sur la manière d'assurer la sécurité des interfaces externes à un DM, notamment une interface de débug matériel ou un virus présent dans une clé usb.
La configuration sécurisée du système d'exploitation fait partie de la responsabilité du fabricant, en conséquence, celui-ci ne peut pas interdire d'utiliser une clé usb sur son DM. Il doit mettre en œuvre les actions permettant une utilisation sécurisée de son DM.
Il est décidé d'aborder ce point dans une section sur la validation des données importées dans le DM et de proposer une recommandation générique sur le filtrage des données importées sur le DM (innocuité des données importées dans le DM).

3.15.Activité de développement du logiciel

La notion de choix de langage de connexion a fait l'objet d'un échange en séance. Le document ne peut pas recommander l'utilisation d'un langage en particulier. Par contre, il peut recommander d'utiliser les outils et méthodes appropriés qui permettent de vérifier les vulnérabilités d'un logiciel. Ce point sera illustré par un exemple (analyse statique de codes sans désigner un produit en particulier). .

3.16.Auto surveillance du DM – Mode dégradé

L'ANSM demande des précisions sur la protection physique des équipements, notamment les notions d'auto surveillance et de vérification d'intégrité.
Les experts soulignent un problème de définition entre la notion d'auto surveillance du DM et celle du mode dégradé.
Une section « mécanisme de protection du DM » devra être proposée dans laquelle l'auto surveillance du DM sera développée. L'auto surveillance inclue les contrôles d'activité mémoire, le security boot. Elle n'est pas forcément réalisée au démarrage. Il s'agit d'une vérification récurrente faite au cours de la vie du système. Le mécanisme d'auto surveillance doit avoir plus de privilèges que l'attaquant.

Le mode dégradé doit également être défini. Les experts précisent que la détection d'une attaque n'est pas forcément l'attaque elle-même. Cela peut être également la détection de l'effet de l'attaque. Dans les deux cas, le mode dégradé du DM doit se déclencher.
Une section « mécanisme de détection des attaques et des défauts » devra être ajoutée.
Il faudra définir quels sont les éléments déclencheurs qui permettent de rentrer dans le mode dégradé et définir le processus qui se met alors en place.

3.17.Vérification et validation

Ces 2 points doivent être développés dans des sections distinctes.
Les experts proposent de décrire les techniques de vérification envisageables.
Concernant la notion de validation, le document pourra aborder les tests de pénétration comme un moyen de gérer la sécurité du dispositif dans son environnement (Proposer des méthodes d'évaluation déjà éprouvées : par exemple, un tiers qui essaie de rentrer sur le produit).

3.18.Mise en service et qualification opérationnelle

Les experts font remarquer que cette section peut laisser entendre qu'il revient au fabricant de régler les menaces grâce à des recommandations d'usage. Il faudra souligner qu'il doit mettre en place des mesures pour contrer les menaces.
Il doit également intégrer dans son plan de développement l'aptitude à l'utilisation (les mesures de sécurité doivent être adaptées à des utilisateurs non sensibilités à la sécurité).
Il sera précisé que le fabricant doit prendre en compte l'utilisation du DM en situation d'urgence même en cas de menace

3.19.Démarrage

Les experts indiquent que l'intitulé « démarrage » n'est pas satisfaisant. Ils proposent la section suivante : « dispositif de protection de l'intégrité du DM » dans laquelle les éléments suivants seront décrits : la vérification d'intégrité des mises à jour, la vérification de l'intégrité au démarrage.

3.20.Identification des incidents

Cette partie pourrait être déplacée dans la prochaine version des recommandations.

Les experts proposent qu'une fiche rappelant la conduite à tenir en cas d'attaque soit ajoutée en annexe du document. Il s'agit bien d'une recommandation fabricant. En cas d'attaque, c'est l'utilisateur qui va agir

mais le fabricant doit l'avoir prévu. Ce cas de figure doit être documenté/explicité par le fabricant. L'utilisateur ne doit pas se retrouver devant un message et ne pas savoir quoi faire. Le titre suivant est proposé : « Recommandation en cas d'alerte de sécurité ».

De même, une vulnérabilité est un risque d'incident. Quand le fabricant a connaissance d'un risque d'incident (combinaison d'une vulnérabilité et d'une menace), il y a toujours un risque que la vulnérabilité pourra être exploitée.
Actuellement, les fabricants attendent de découvrir la faille et son exploitation pour déterminer les actions à mettre en place. Or, idéalement, les fabricants devraient consulter les alertes, suivre la mise à disposition des patchs identifiant les vulnérabilités (ceux de microsoft notamment). L'anticipation via un système de veille apparait essentielle.

Selon la norme 62304, un processus de gestion des anomalies des SOUP doit être effectif pour rattraper les vulnérabilités publiées par les éditeurs des SOUP.

Cette partie doit être reprise et sera discutée lors d'une prochaine séance.

3.21.Sortie des données

Les experts indiquent qu'il manque une recommandation sur la sortie des données. Le mécanisme d'extraction des données vers un autre système doit être sécurisé. Cette partie pourrait être rattachée à la partie fin de vie du logiciel (en changeant l'intitulé de la section).

Il est rappelé que conformément au RGPD, le droit à la portabilité s'inscrit comme un principe de base.
Pour les éléments couverts par le RGPD, il est décidé de faire référence au texte.
L'ANSM demande aux experts si les solutions de restitution s'inscrivent dans l'idée de garantir le fonctionnement en cas d'attaque. Les experts indiquent qu'il s'agit d'un moyen de réduction des risques

3.22.Télémaintenance

L'ANSM se demande si la télémaintenance fait partie du scope des recommandations. La maintenance étant une obligation incombant à l'utilisateur, il s'agirait plutôt d'une recommandation utilisateur.

Les experts indiquent que le fabricant doit définir les modalités de réalisation de la maintenance. Elle ne doit pas être une porte d'entrée pour les attaques. La maintenance doit être particulièrement sécurisée notamment au niveau des droits d'accès (exigence de cloisonnement). Idéalement, la maintenance ne devrait pas donner accès aux données médicales, personnelles des patients stockées.

3.23. Fin de vie des composants

Les experts demandent à l'ANSM d'ajouter un exemple parlant pour illustrer ce point.

3.24. Effacement des clés cryptographiques

La question de pose de l'efficacité de l'effacement des données. Les experts indiquent qu'un chiffrement des données en amont sur le support de stockage pourrait être recommandé. Dans ce cas, il faut uniquement oublier la clé qui sert à chiffrer ce qui ne représente que quelques octets.

3.25.Gestion des données sur le Cloud

Les experts proposent de renvoyer aux documents de référence dans le domaine (HDS et ANSSI) et de rappeler les grands principes.

4. Conclusion

Les 25 points prioritaires identifiés suite aux commentaires des experts ont été discutés lors de cette 3ième séance. L'ANSM va intégrer les éléments dans le projet de document et faire des propositions de correction sur les autres commentaires émis par les experts.

Le document leur sera transmis avant le prochain CSST dont la date sera définie ultérieurement. L'ANSM va engager la procédure de renouvellement du CSST pour une année supplémentaire.
En parallèle, l'agence va présenter le projet de document au niveau du groupe Européen « Cybersécurité des logiciels ». Certains membres du CSST pourraient être sollicités afin d'apporter leur expertise au sein de ce groupe.

L'ANSM tient à remercier tous les experts pour leur participation active aux discussions.
Levée de séance.