Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TELECOMMUNICATIONS
DE L'UIT

H.812

(11/2017)

SERIE H: SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

Services et applications multimédias de cybersanté – Systèmes de santé individuels

Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels: Interface pour les services

Recommandation UIT-T H.812

RECOMMANDATIONS UIT-T DE LA SERIE H

SYSTÈMES AUDIOVISUELS ET MULTIMEDIAS

CARACTERISTIQUES DES SYSTÈMES VISIOPHONIQUES	H.100–H.199
INFRASTRUCTURE DES SERVICES AUDIOVISUELS	
Généralités	H.200–H.219
Multiplexage et synchronisation en transmission	H.220–H.229
Aspects système	H.230–H.239
Procédures de communication	H.240–H.259
Codage des images vidéo animées	H.260–H.279
Aspects liés aux systèmes	H.280–H.299
Systèmes et équipements terminaux pour les services audiovisuels	H.300–H.349
Architecture des services d'annuaire pour les services audiovisuels et multimédias	H.350–H.359
Architecture de la qualité de service pour les services audiovisuels et multimédias	H.360–H.369
Services complémentaires en multimédia	H.450–H.499
PROCEDURES DE MOBILITE ET DE COLLABORATION	
Aperçu général de la mobilité et de la collaboration, définitions, protocoles et procédures	H.500–H.509
Mobilité pour les systèmes et services multimédias de la série H	H.510–H.519
Applications et services de collaboration multimédia mobile	H.520–H.529
Sécurité pour les systèmes et services multimédias mobiles	H.530–H.539
Sécurité pour les applications et services de collaboration multimédia mobile	H.540–H.549
Procédures d'interfonctionnement de la mobilité	H.550–H.559
Procédures d'interfonctionnement de collaboration multimédia mobile	H.560–H.569
SERVICES MULTIMEDIAS À LARGE BANDE, TRI-SERVICES MULTIMEDIAS ET SERVICES MULTIMEDIAS EVOLUES	
Services multimédias à large bande sur VDSL	H.610–H.619
Services et applications multimédias évolués	H.620–H.629
Applications des réseaux de capteurs ubiquitaires et Internet des objets	H.640–H.649
SERVICES MULTIMEDIAS ET APPLICATIONS DE TELEVISION PAR RESEAU IP	
Aspects généraux	H.700–H.719
Terminaux pour la télévision par réseau IP	H.720–H.729
Intergiciels pour la télévision par réseau IP	H.730–H.739
Traitement d'évènements dans les applications de télévision par réseau IP	H.740–H.749
Métadonnées pour la télévision par réseau IP	H.750–H.759
Cadres généraux des applications multimédias pour la télévision par réseau IP	H.760–H.769
Exploration des services jusqu'au point de consommation dans la télévision par réseau IP	H.770–H.779
Affichage numérique	H.780–H.789
SERVICES ET APPLICATIONS MULTIMEDIAS DE CYBERSANTE	
Systèmes de santé individuels	**H.810-H.819**
Tests de conformité des systèmes de santé individuels aux normes d'interopérabilité (HRN, PAN, LAN et WAN)	H.820–H.849
Services d'échange de données multimédias concernant la cybersanté	H.860–H.869

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T H.812

Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels: Interface pour les services

Résumé

Les directives de conception de Continua définissent un cadre pour les normes sous-jacentes et les critères nécessaires pour assurer l'interopérabilité des dispositifs et des données utilisés pour les services de santé connectée individuels. Elles contiennent en outre d'autres directives de conception qui donnent des précisions supplémentaires concernant les normes ou spécifications sous-jacentes, qui consistent à réduire les options ou à ajouter des caractéristiques manquantes pour améliorer l'interopérabilité.

La Recommandation UIT-T H.812 contient un aperçu de l'interface pour les services (Services-IF), les directives de conception communes à toutes les classes de capacité homologuée (CCC) à cette interface et les directives de conception concernant les classes CCC pour la passerelle de santé individuelle (PHG) et les services employant le consentement.

Les directives de conception concernant les classes de capacité homologuée (CCC) indiquées ci-après sont définies dans des documents distincts, comme suit:

– UIT-T H.812.1 (2017) pour le chargement des observations

– UIT-T H.812.2 (2017) pour les questionnaires

– UIT-T H.812.3 (2017) pour l'échange de capacités

– UIT-T H.812.4 (2017) pour la session authentifiée persistante

La Recommandation UIT-T H.812 fait partie de la sous-série "UIT-T H.810 – Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels", qui couvre les sujets suivants:

– UIT-T H.810 – Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels: Introduction

– UIT-T H.811 – Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels: Interface avec les dispositifs de santé individuels

– UIT-T H.812 – Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels: Interface pour les services (le présent document)

– UIT-T H.812.1 – Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels: Interface pour les services: Chargement des observations

– UIT-T H.812.2 – Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels: Interface pour les services: Questionnaires

– UIT-T H.812.3 – Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels: Interface pour les services: Echange de capacités

– UIT-T H.812.4 – Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels: Interface pour les services: Session authentifiée persistante

– UIT-T H.813 – Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels: Interface avec le système d'information sanitaire

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T H.812	29-11-2015	16	11.1002/1000/12653
2.0	UIT-T H.812	14-07-2016	16	11.1002/1000/12913
3.0	UIT-T H.812	29-11-2017	16	11.1002/1000/13415

Mots clés

CDG, directives de conception de Continua, système d'information sanitaire, systèmes de santé connectée individuels, dispositifs de santé individuels, services.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIETE INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en oeuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en oeuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Liste des Tableaux

Liste des Figures

0 Introduction

Les directives de conception de Continua définissent un cadre pour les normes sous-jacentes et les critères nécessaires pour assurer l'interopérabilité des dispositifs et des données utilisés pour les services de santé connectée individuels. Elles contiennent en outre d'autres directives de conception qui donnent des précisions supplémentaires concernant les normes ou spécifications sous-jacentes, qui consistent à réduire les options ou à ajouter des caractéristiques manquantes pour améliorer l'interopérabilité.

Le présent document contient d'autres directives de conception concernant l'interopérabilité qui donnent des précisions supplémentaires concernant les normes ou spécifications sous-jacentes, réduisent les options qui y sont proposées ou ajoutent des caractéristiques manquantes.

Il contient une présentation générale de l'interface Services-IF, les directives de conception communes à toutes les classes de capacité homologuée (CCC) à cette interface ainsi que les directives de conception concernant les classes CCC pour une passerelle de santé individuelle (PHG) et un service de santé et de forme physique employant le consentement.

Les directives de conception concernant les classes de capacité homologuée (CCC) indiquées ci-après sont définies dans des documents distincts, comme suit:

– [UIT-T H.812.1] – *Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels: Interface pour les services: Chargement des observations*.

– [UIT-T H.812.2] – *Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels: Interface pour les services: Questionnaires*.

– [UIT-T H.812.3] – *Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels: Interface pour les services: Echange de capacités*.

– [UIT-T H.812.4] – *Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels: Interface pour les services: Session authentifiée persistante*.

Le présent document fait partie de la sous-série "UIT-T H.810 – Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels". Voir la Recommandation [UIT-T H.810] pour plus d'informations.

0.1 Structure

Le présent document est structuré de la manière suivante.

Paragraphes 0 à 5: Introduction et terminologie – Ces paragraphes contiennent des informations concernant l'interface Services-IF permettant de mieux comprendre la structure des spécifications de conception.

Paragraphe 6: Présentation générale de l'interface Services-IF – Ce paragraphe fournit une présentation générale des classes CCC à l'interface Services-IF.

Paragraphe 7: Cas d'utilisation – Ce paragraphe décrit des exemples pratiques.

Paragraphe 8: Modèle de comportement – Ce paragraphe donne un aperçu des séquences d'interactions dans le cadre des classes CCC communes à l'interface pour les services et résume les interactions, contraintes et exceptions habituelles.

Paragraphe 9: Mise en oeuvre – Ce paragraphe décrit en détail l'utilisation du contenu commun de la charge utile et du protocole simple d'accès aux objets (SOAP), en comparaison avec la méthode de transport fondée sur le transfert d'état représentationnel (REST), dans les classes de capacité homologuée communes à l'interface Services-IF.

0.2 Publication et versions des directives

Voir le paragraphe 0.2 de la Recommandation [UIT-T H.810] pour obtenir des informations relatives à la publication et aux versions des directives.

0.3 Nouveautés

Voir le paragraphe 0.3 de la Recommandation [UIT-T H.810] pour connaître les nouveautés exposées dans le présent document.

Recommandation UIT-T H.812

Directives de conception visant à assurer l'interopérabilité des systèmes de santé individuels: Interface pour les services

1 Domaine d'application

Le présent document porte sur l'interface ci-après:

– **Services-IF –** Interface entre une passerelle de santé individuelle (PHG) et des services.

Cette interface est définie dans l'architecture Continua, telle que décrite dans le paragraphe 6 de la Recommandation [UIT-T H.810] et illustrée dans la Figure 1-1.

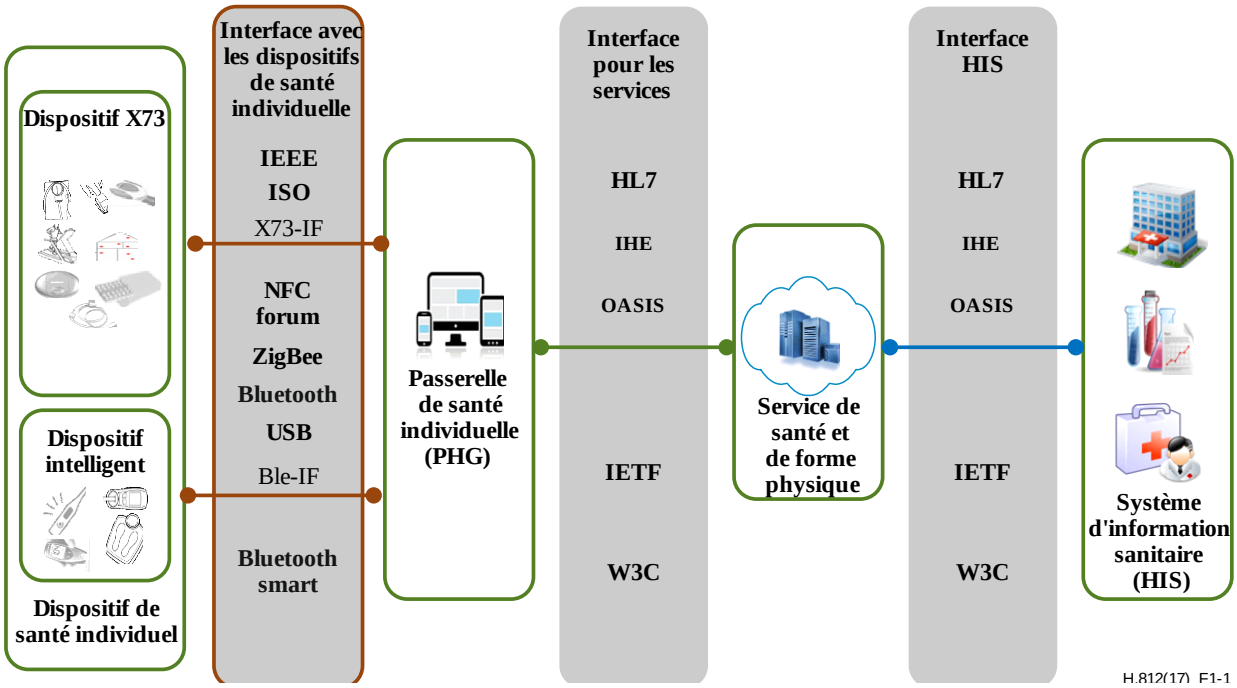

Figure 1-1 – Interface pour les services dans l'architecture Continua

Un certain nombre de classes de capacité homologuée (CCC) sont relatives à l'interface Services-IF. Le présent document contient des directives de conception visant à assurer l'interopérabilité, applicables à plusieurs classes CCC. Il contient notamment des directives de conception visant à assurer l'interopérabilité relative à la sécurité. En outre, le présent document contient les directives de conception concernant les classes CCC à l'interface entre la passerelle PHG et les services employant le consentement. Ces classes CCC peuvent être regroupées avec de nombreuses autres classes CCC relatives à l'interface Services-IF telles que, par exemple, les classes CCC relatives au chargement des observations ou aux questionnaires.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T H.810] Recommandation UIT-T H.810 (2017), *Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels: Introduction*.

Les autres documents cités sont disponibles dans le paragraphe 2 de la Recommandation [UIT-T H.810].

3 Définitions

Le présent document emploie les termes définis dans la Recommandation [UIT-T H.810].

4 Abréviations et acronymes

Le présent document emploie les abréviations et les acronymes définis dans la Recommandation [UIT-T H.810].

5 Conventions

Le présent document suit les conventions définies dans la Recommandation [UIT-T H.810].

6 Architecture

Dans cette architecture de référence de bout en bout, l'interface pour les services (Services-IF) relie une passerelle de santé individuelle (PHG) à un service de santé et de forme physique (HFS). La Figure 6-1 illustre l'interface pour les services dans l'architecture Continua de bout en bout et la Figure 6-2 montre un exemple de l'interface Services-IF.

Les directives de conception de l'interface Services-IF visent principalement à assurer l'interopérabilité des échanges d'informations par l'intermédiaire d'une interface pour les services. Un ensemble de classes de capacité homologuée relatives à l'interface pour les services est défini pour la passerelle PHG et le service de santé et de forme physique, afin d'assurer l'interopérabilité pour un certain nombre de cas d'utilisation différents, qui consistent notamment à charger des données de mesure, à remplir des questionnaires et à exécuter des commandes.

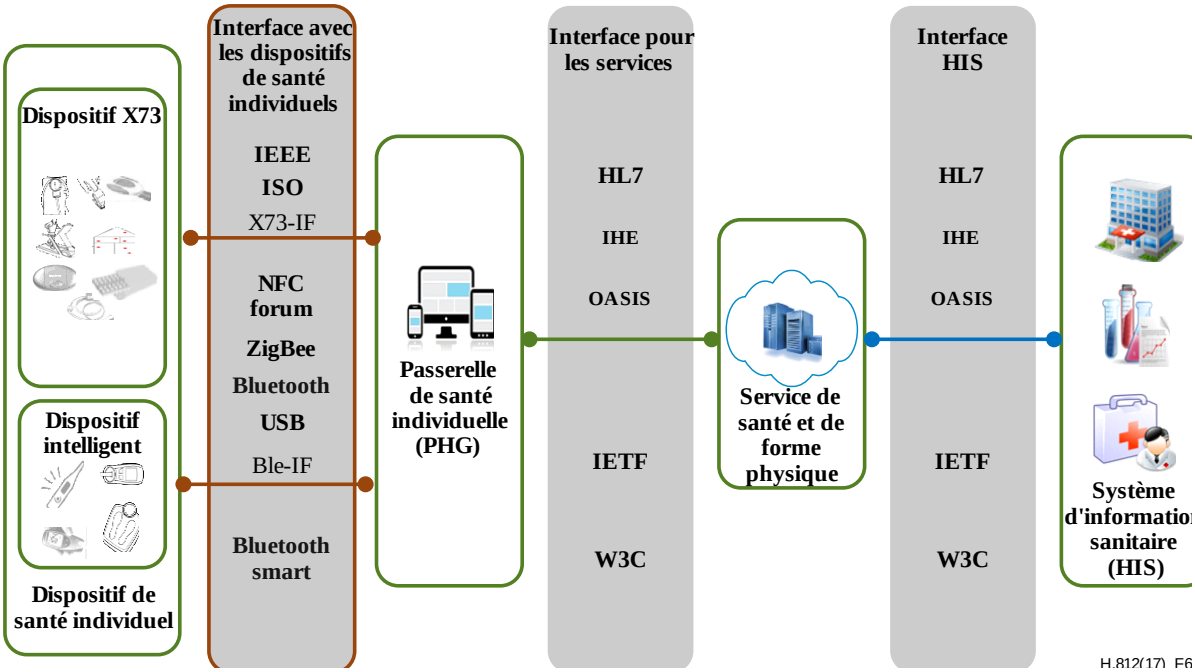

Figure 6-1 – Interface pour les services dans l'architecture Continua de bout en bout

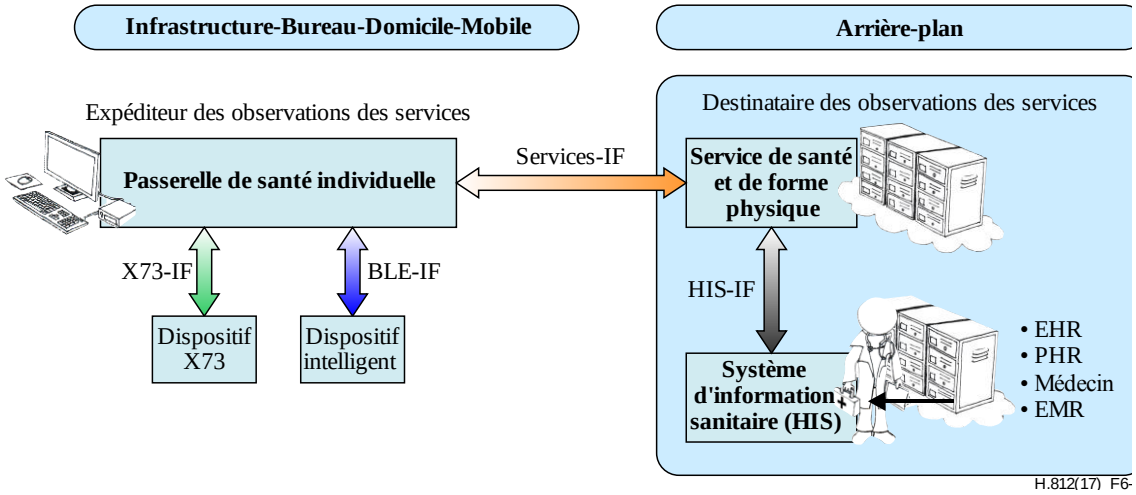

Figure 6-2 – Exemple d'une interface Services-IF

Outre l'interface Services-IF, l'architecture de référence de bout en bout définit aussi l'interface avec le système d'information sanitaire (HIS-IF). L'interface Services-IF est conçue pour garantir la granularité de l'échange d'informations entre une passerelle PHG (en général, un PC, un ordinateur portable, une tablette, un téléphone mobile ou un autre type de dispositif intégré), dispositif proche de l'utilisateur/du patient, et un service de santé et de forme physique (en général, un service d'arrière-plan basé sur le nuage), qui recueille les informations relatives aux utilisateurs et met ces informations à disposition en vue d'une utilisation ultérieure. En revanche, l'interface HIS-IF est conçue pour permettre l'échange d'informations compilées entre deux systèmes d'arrière-plan, par

exemple, un système de gestion des maladies et un dossier informatisé de santé (EHR)[1]. L'interface HIS-IF est définie dans la Recommandation [UIT-T H.813].

Il est aussi prévu qu'une passerelle PHG puisse être déployée dans des applications utilisées au domicile ou installées sur un dispositif mobile porté par l'utilisateur, ce qui impose un certain nombre de contraintes sur la conception de l'interface Services-IF. En raison de la difficulté à assurer la maintenance et/ou la mise à niveau de ces dispositifs "sur le terrain", une passerelle PHG devrait être solide et autonome, et suffisamment simple pour que les coûts restent bas et que les besoins en matière d'expérience ou de compétences techniques et opérationnelles soient minimaux. En raison de ces exigences, l'interface Services-IF est conçue de sorte que la plupart des métadonnées contextuelles associées aux échanges d'observations soient situées hors de la passerelle PHG.

D'autre part, il est prévu qu'un service de santé et de forme physique soit hébergé sur un système disposant de plus de capacités, comme un serveur ou un ordinateur personnel. La conception de l'interface Services-IF vise donc à ce que les problèmes de complexité et de maintenance soient déplacés au niveau du service de santé et de forme physique, de manière à éviter les problèmes au niveau de la passerelle PHG.

L'interface Services-IF est un canal abstrait composé d'une ou plusieurs paires de classes CCC qui relient une application PHG avec l'application d'un service de santé et de forme physique. Chaque paire de classes CCC est constituée d'un composant au niveau de l'application du service de santé et de forme physique et d'un composant situé dans l'application PHG. Continua définit des classes de capacité homologuée de part et d'autre de l'interface Services-IF.

La présente version des directives relatives à l'interface Services-IF permet la mise en oeuvre des classes de capacité homologuée suivantes:

– le chargement d'observations de la passerelle PHG vers le service de santé et de forme physique selon deux méthodes différentes: les services web (SOAP) et le transfert REST (données) [UIT-T H.812.1];
– le chargement d'informations relatives au consentement de la passerelle PHG vers le service de santé et de forme physique selon deux méthodes différentes: les services web (SOAP) et le transfert REST (données) [UIT-T H.812];
– le chargement de questionnaires à compléter du service de santé et de forme physique vers la passerelle PHG, ainsi que le chargement des questionnaires complétés de la passerelle PHG vers le service de santé et de forme physique [UIT-T H.812.2];
– l'échange d'informations (par exemple, des commandes non sollicitées) entre le service de santé et de forme physique et la passerelle PHG, au cours d'une session authentifiée persistante [UIT-T H.812.4];
– l'échange d'informations relatives aux classes de capacité homologuée prises en charge (échange de capacités) entre la passerelle PHG et le service de santé et de forme physique, en tant qu'outil permettant la réalisation des autres cas d'utilisation [UIT-T H.812.3].

Une passerelle PHG peut prendre en charge une ou plusieurs applications, chacune mettant en oeuvre une ou plusieurs classes de capacité homologuée Continua. La Figure 6-3 illustre l'interface Services-IF Continua, avec une application PHG et l'application d'un service de santé et de forme physique dans lesquelles toutes les classes de capacité homologuée possibles à l'interface Services-IF sont mises en oeuvre.

---

[1] NOTE – Dans l'architecture de bout en bout, l'interface pour les services et l'interface avec le système d'information sanitaire (HIS) peuvent toutes deux être mises en œuvre dans un dispositif proche de l'utilisateur/du patient (un PC, un ordinateur portable, un téléphone mobile, etc.) afin d'échanger des informations avec des entités qui sont géographiquement éloignées dudit dispositif. Les directives ne fixent aucune restriction quant au déploiement des classes de capacité homologuée sur un matériel particulier.

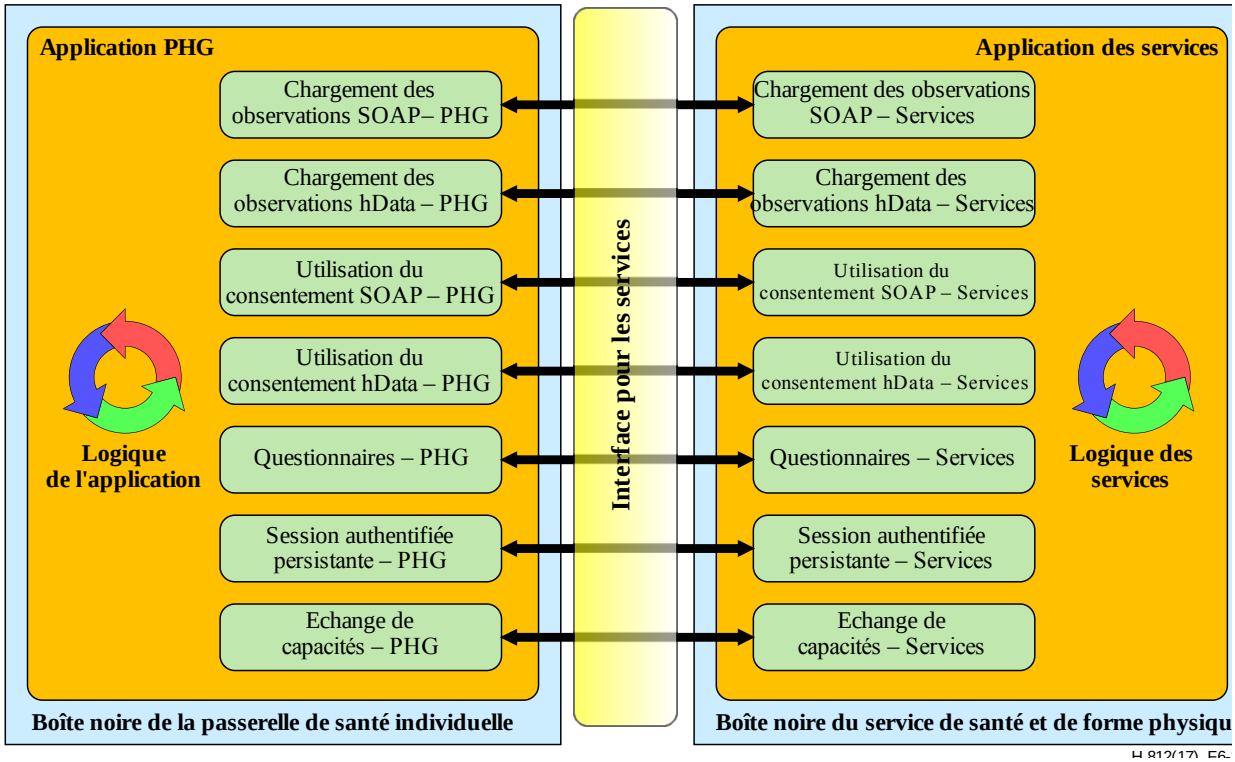

Figure 6-3 – Interface Services-IF Continua illustrant les classes de capacité homologuée à l'interface Services-IF

Les présentes directives ont pour objet d'indiquer le comportement du système avec suffisamment de détails pour atteindre un niveau d'interopérabilité acceptable dans un cas d'utilisation particulier. Un cas d'utilisation est encapsulé dans une classe de capacité homologuée (CCC). Les directives contiennent des déclarations normatives concernant le fonctionnement de l'interface réseau des composants de la classe CCC. Pour l'interface Services-IF, ces composants existent dans le contexte d'applications ou de services situés dans une passerelle PHG ou un service de santé et de forme physique.

Les plates-formes communes imposent souvent des restrictions quant à la façon dont les applications peuvent communiquer les unes avec les autres, afin de garantir la stabilité de la plate-forme dans son ensemble. On utilise l'expression "bac à sable" *(sandbox)* pour parler de cette restriction des interactions entre les applications. Afin de prendre en charge les applications soumises à ce fonctionnement, la version de l'interface Services-IF décrite dans le présent document utilise un modèle de référence qui définit une application comme un conteneur comportant un ou plusieurs composants CCC. Les interactions des composants situés dans le conteneur constitué par l'application ne sont pas soumises à des exigences normatives et sont entièrement laissées au soin du développeur de l'application. Les interactions à l'interface Services-IF entre les classes CCC de l'application de la passerelle PHG et les classes CCC correspondantes du service de santé et de forme physique sont visibles et sont, quant à elles, soumises à des exigences normatives qu'elles doivent respecter pour obtenir la certification.

Le modèle de référence permet à une passerelle PHG ou à un service de santé et de forme physique de comporter plusieurs applications, mais celles-ci doivent interagir entre elles exclusivement par l'intermédiaire des interfaces réseau. Dans les directives décrites dans le présent document, les applications qui s'exécutent au niveau d'un service de santé et de forme physique sont souvent appelées "services", étant donné que les services de santé et de forme physique sont généralement des plates-formes de services web. Sur le plan théorique, un service de santé et de forme physique est similaire à une application PHG.

Ces directives décrivent les mécanismes par lesquels les composants peuvent communiquer les uns avec les autres, par l'intermédiaire d'une interface de programmation d'application (API) interne. Les versions ultérieures de l'interface Services-IF pourront utiliser ces mécanismes pour assurer l'interopérabilité entre les différents composants d'une application.

Dans la Figure 6-4, les concepts relatifs au modèle de référence de l'interface Services-IF sont utilisés pour décrire une passerelle PHG comportant deux applications indépendantes, qui communiquent avec une application de services. L'une des applications PHG prend en charge trois classes CCC et l'autre, une seule. Des exigences normatives sont formulées au sujet des interfaces réseau entre la passerelle PHG et le service de santé et de forme physique. Les interactions entre les composants CCC contenus dans une même application ne sont pas normatives et sont indiquées par des traits discontinus rouges. Elles sont coordonnées par un traitement interne à l'application et ne relèvent pas du domaine d'application des directives décrites dans le présent document.

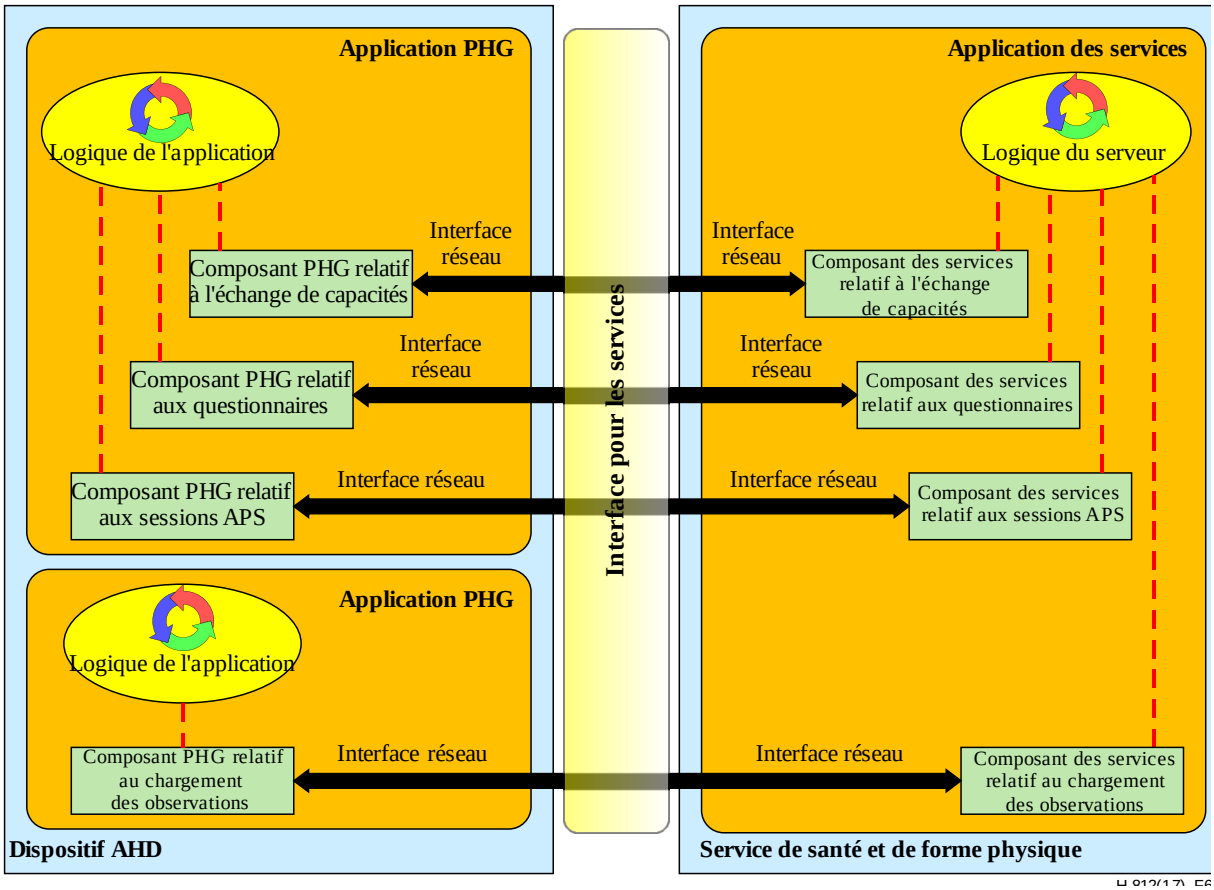

Figure 6-4 – Modèle de référence de l'interface Services-IF

Les communications qui utilisent l'interface Service-IF commencent avec le composant PHG relatif à l'échange de capacités. Ce composant envoie une demande à son homologue du service de santé et de forme physique, afin de s'informer sur les différentes classes de capacité homologuée que ce service prend en charge. En langage commun, l'application PHG demande: "Que peux-tu faire?" L'application du service de santé et de forme physique répond à cette question en indiquant les classes CCC qu'elle prend en charge. Dans le cas de la Figure 6-4, cette application répondrait: "Je prends en charge l'échange de capacités, les questionnaires, le chargement des observations au moyen du protocole SOAP ainsi que les sessions authentifiées persistantes (APS)". Lorsque le composant relatif à l'échange de capacités de l'application des services répond à l'application PHG, il fournira généralement à la passerelle PHG des informations supplémentaires, telles qu'une adresse URL, permettant à l'application PHG de passer à l'étape suivante, qui consiste à communiquer avec une

classe CCC particulière. Une passerelle PHG qui ne prend en charge que le chargement des observations au moyen du protocole SOAP ne doit pas forcément mettre en oeuvre l'échange de capacités. Cette fonctionnalité ne doit pas nécessairement être invoquée si la passerelle PHG a déjà connaissance des capacités prises en charge par le service de santé et de forme physique.

7 Cas d'utilisation

7.1 Cas d'utilisation de la gestion des consentements

Une directive en matière de consentement est la consigne de la politique de garantie de la protection de la vie privée d'un bénéficiaire de soins de santé, en vertu de laquelle l'accès aux informations d'identification personnelle sur la santé (IIHI) est accordé ou refusé [HL7 CDA IG].

La prescription relative au consentement de l'utilisateur repose sur différents règlements tels que la *Health Information and Portability Accountability Act* (HIPAA), les Directives UE 95/46, etc. Ces lois en matière de protection de la vie privée définissent et accordent des droits spécifiques aux patients en ce qui concerne la collecte, l'accès, l'utilisation et la divulgation d'informations sur leur santé. Ces lois stipulent que le consentement du patient doit être obtenu avant qu'il ne soit accédé aux informations sur sa santé et avant que celles-ci ne soient utilisées ou partagées. Par exemple, un patient peut, lors de son immatriculation auprès d'un organisme de gestion des maladies (DMO), être prié de remplir un formulaire de consentement. Ce formulaire de consentement contient l'accord et/ou la signature du patient en ce qui concerne un ensemble de politiques prédéfinies qui spécifient les personnes qui sont autorisées à accéder à ses informations IIHI, à quelles fins elles peuvent le faire et comment elles peuvent les utiliser. Le présent paragraphe décrit la saisie et le transfert de la politique de consentement sous forme électronique par l'intermédiaire de l'interface Services-IF. Le consentement numérique contribue à une autonomisation accrue du patient et à une gestion efficace du consentement. Des exemples de consentement du patient sont notamment l'accord ou le refus de l'accès aux informations IIHI, pouvant être outrepassé en cas d'urgence, la restriction de l'accès selon les rôles fonctionnels (par exemple, le personnel soignant), l'emploi de documents spécifiques pour des projets de recherche spécifiques, etc.

Dans un scénario de base, le patient donne son consentement lors de son immatriculation sur l'application du service de santé et de forme physique ou après celle-ci. La manière dont il spécifie ce consentement sort du cadre des directives décrites dans le présent document, mais il pourrait s'agir du choix d'une politique par défaut ou de son éventuelle adaptation, grâce à une interface utilisateur sur sa passerelle PHG, qui la convertirait en une version de la politique de consentement lisible par une machine. De telles politiques contiennent généralement une référence aux parties concernées, aux données et aux actions qui sont autorisées ou non. L'application d'un service de santé et de forme physique qui reçoit un consentement concernant un patient particulier l'entrepose et le met en application pour les données sur la santé dudit patient qu'il reçoit.

Les cas d'utilisation ci-après portent principalement sur les besoins mis en évidence en ce qui concerne la gestion des consentements du patient.

7.1.1 Chargement du consentement sur le serveur

Georges Tout-le-monde réalise une demande d'immatriculation auprès d'un organisme, par exemple, un organisme de gestion des maladies (DMO), assurant le suivi à distance de patients situés à leur domicile, qui recueille des informations sur la santé au moyen de dispositifs de mesure installés au domicile de Georges. Au moment de l'immatriculation, Georges remplit un formulaire de consentement électronique sur l'application de la passerelle de santé individuelle (PHG). Ce formulaire contient des options permettant de déterminer qui aura accès aux différents types de signes vitaux recueillis par le système de suivi à distance des patients, qui pourra les utiliser, les mettre à jour et les divulguer. Lorsqu'il a indiqué ses préférences, Georges clique ensuite sur le bouton "envoyer" sur son dispositif central de télésanté. Ce dispositif réunit ses préférences au sein d'un

document contenant les directives en matière de consentement et de protection de la vie privée, fondé sur la norme HL7 CDA R2. Ce document est ensuite envoyé de la passerelle PHG de Georges vers l'organisme DMO qui fournit un service de suivi à distance des patients. Les directives en matière de consentement vont ensuite conditionner l'accès aux données du patient dans l'organisme DMO. Parmi les données de Georges qui pourront être envoyées à des parties tierces, dans la mesure où cette opération est autorisée, on trouvera notamment le dossier personnel de santé (PHR), les dossiers informatisés de santé (EHR) et les dossiers médicaux informatisés (EMR) du patient. Les directives en matière de consentement et de protection de la vie privée de Georges seront associées aux données au moyen de l'identificateur de patient.

7.1.2 Récupération sur le serveur du formulaire de consentement du patient déjà complété

Georges peut vouloir mettre à jour ses préférences en matière de protection de la vie privée, par exemple, en autorisant l'accès à ses données à son entraineur sportif, étant donné qu'il a récemment souscrit à un service de forme physique, sur les conseils d'un infirmier de l'organisme DMO. Il trouvera un lien sur sa passerelle PHG conduisant à la version la plus récente du document contenant ses directives en matière de consentement et de protection de la vie privée. Georges clique sur ce lien; la passerelle PHG va alors récupérer sur le serveur la version la plus récente du document contenant les directives en matière de consentement et de protection de la vie privée de Georges et la lui remettre.

7.1.3 Chargement sur le serveur du consentement mis à jour

Georges consulte ses préférences en matière de consentement et de protection de la vie privée et les met à jour si son entraineur sportif n'a pas accès à ses données. Après avoir mis à jour ses préférences en matière de consentement, il clique sur le bouton "envoyer" sur sa passerelle PHG. Celle-ci les réunit au sein d'un document contenant les directives en matière de consentement et de protection de la vie privée, qui est envoyé à l'organisme DMO. Ce dernier remplace l'ancien consentement par le document mis à jour.

7.2 Cas d'utilisation de la mise en application du consentement

La mise en application du consentement par chiffrement assure de façon efficace la protection de la vie privée à laquelle a droit le patient et garantit que le contenu (par exemple, les observations ou les réponses à un questionnaire) n'est vu que par le destinataire auquel il s'adresse. Cela évite que ce contenu ne soit vu par d'autres personnes travaillant dans le même organisme, par exemple le personnel administratif. Un service de santé et de forme physique employant le consentement devrait évaluer le consentement avant de déchiffrer le contenu. Le consentement est évalué afin de déterminer si le destinataire a le droit de voir le contenu. Ainsi, le processus d'évaluation du consentement conduit par exemple à "Success-1" ou "Failure-0". Un service de santé et de forme physique employant le consentement devrait appliquer les préférences en matière de consentement exprimées dans le document de consentement.

7.2.1 Chiffrement du contenu avant le chargement

Georges Tout-le-monde réalise une demande d'immatriculation auprès d'un organisme DMO qui assure son suivi à distance et recueille des informations sur sa santé au moyen de dispositifs de mesure installés à son domicile. Il a aussi recours aux services d'un entraineur sportif, sur les conseils d'un infirmier de l'organisme DMO. Georges souhaite que son entraineur sportif puisse consulter les données relatives à son activités, mais pas celles qui proviennent d'autres dispositifs de mesure tels que son tensiomètre artériel. Il configure sa passerelle PHG de sorte que, désormais, seul l'infirmier de l'organisme DMO ait accès aux données provenant du tensiomètre et des dispositifs de suivi de l'activité, et que l'entraineur sportif n'ait accès qu'aux données provenant de ces dispositifs. Cette fonctionnalité est mise en oeuvre au moyen d'un chiffrement.

7.3 Cas d'utilisation des autres classes CCC

Voir le paragraphe 6 des directives de conception suivantes pour les cas d'utilisation de leur classe CCC respective:

– [UIT-T H.812.1] Chargement des observations

– [UIT-T H.812.2] Questionnaires

– [UIT-T H.812.3] Echange de capacités

– [UIT-T H.812.4] Session authentifiée persistante

8 Modèles de comportement

Le présent paragraphe porte sur:

– Le comportement de l'interface Services-IF en matière d'échange de messages.

– Le comportement des classes CCC fondées sur le transfert REST en matière de sécurité.

– Le comportement des classes CCC en ce qui concerne la gestion des consentements et leur mise en application.

8.1 Comportement commun de l'interface Services-IF en matière d'échange de messages

En raison de problèmes de sécurité et de protection de la vie privée, ainsi que de la faisabilité sur le plan technique de l'ensemble du système, l'interface Services-IF nécessite que toutes les connexions soient initiées par la passerelle PHG, comme indiqué dans la Figure 8-1. Les différentes directives de conception contiennent des informations concernant la charge utile des messages ainsi que d'autres détails.

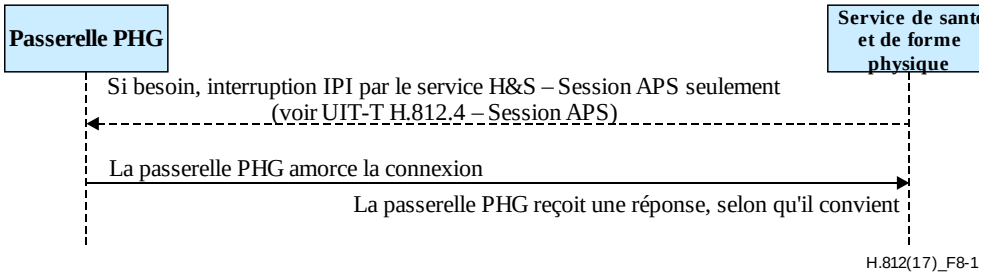

Figure 8-1 – Toutes les connexions sont initiées par la passerelle PHG

Lorsque la sécurité au niveau du transport (TLS) est nécessaire pour assurer la sécurité du contenu point à point, l'utilisation de la validation mutuelle des certificats lors de la prise de contact TLS dépend de la politique de sécurité du service de santé et de forme physique.

Lorsqu'une authentification est nécessaire:

– dans le cas du protocole SOAP, l'authentification est réalisée par un jeton SAML 2.0; et

– dans le cas de données, par un jeton du porteur OAuth 2.0.

Les directives décrites dans le présent document n'indiquent pas comment la passerelle PHG se procure ces jetons, étant donné que cela dépend de la relation de confiance établie entre les parties. L'application du service de santé et de forme physique peut prendre en charge une ou plusieurs options WS-Trust afin d'obtenir des jetons SAML 2.0 ou un serveur du cadre d'autorisation OAuth 2.0 utilisant un ou plusieurs types de justificatifs, par exemple, l'information de mot de passe du propriétaire des ressources. Le service de santé et de forme physique peut prendre en charge les deux services s'il prend en charge tant les chargements par données que ceux employant le protocole SOAP. Dans les deux cas de figure, une opération hors bande doit être réalisée lorsque l'utilisateur de la passerelle PHG crée un certain type de compte sur l'application du service de santé et de forme

physique, permettant au client de se procurer ces jetons. Le service de jeton du service de santé et de forme physique génère ces jetons en les adaptant au destinataire, validé lors de la réception du contenu. D'autre part, le service de santé et de forme physique peut exiger que ces jetons soient obtenus auprès du service d'autorisation d'une tierce partie (telle qu'une autorité de certification) avec laquelle la passerelle PHG a établi une relation de confiance. Dans ce cas, le service de santé et de forme physique laisse au service d'autorisation de la tierce partie le soin de valider le client. Le service de santé et de forme physique peut alors choisir d'accepter tout jeton provenant du service de cette tierce partie, ou encore de transférer les jetons reçus au service d'autorisation de la tierce partie pour obtenir une confirmation de sa part avant qu'ils ne soient acceptés. Les détails de la relation de confiance sont déterminés par la politique de sécurité du service de santé et de forme physique.

8.2 Modèle commun de sécurité pour les mises en oeuvre des classes CCC fondées sur le transfert REST

La Figure 8-2 présente un diagramme d'interaction pour les transactions REST fondées sur des données (REST) transmises sur HTTP. L'autorisation est accordée conformément au cadre d'autorisation OAuth 2.0 avec, comme type de justificatif d'autorisation, l'information de mot de passe du propriétaire des ressources. Cette information est généralement utilisée lorsque le degré de confiance entre le propriétaire des ressources (le patient) et le client (par exemple, une application de confiance exécutée sur le dispositif hébergeant des applications) est élevé. Dans des versions ultérieures des directives de conception, d'autres types de justificatifs pourront être nécessaires pour les cas d'utilisation dans lesquels des applications de tierces parties (disposant de moins de privilèges) peuvent être utilisées pour accéder aux données du patient. Le justificatif du propriétaire des ressources est utilisé pour une seule demande et est échangé contre un jeton d'accès. Ce jeton est ensuite utilisé pour réaliser une transaction REST sur une ressource. Toutes les interactions avec le serveur d'autorisation et le serveur de ressources sont réalisées au sein d'une session sécurisée, conformément à [IETF RFC 4346].

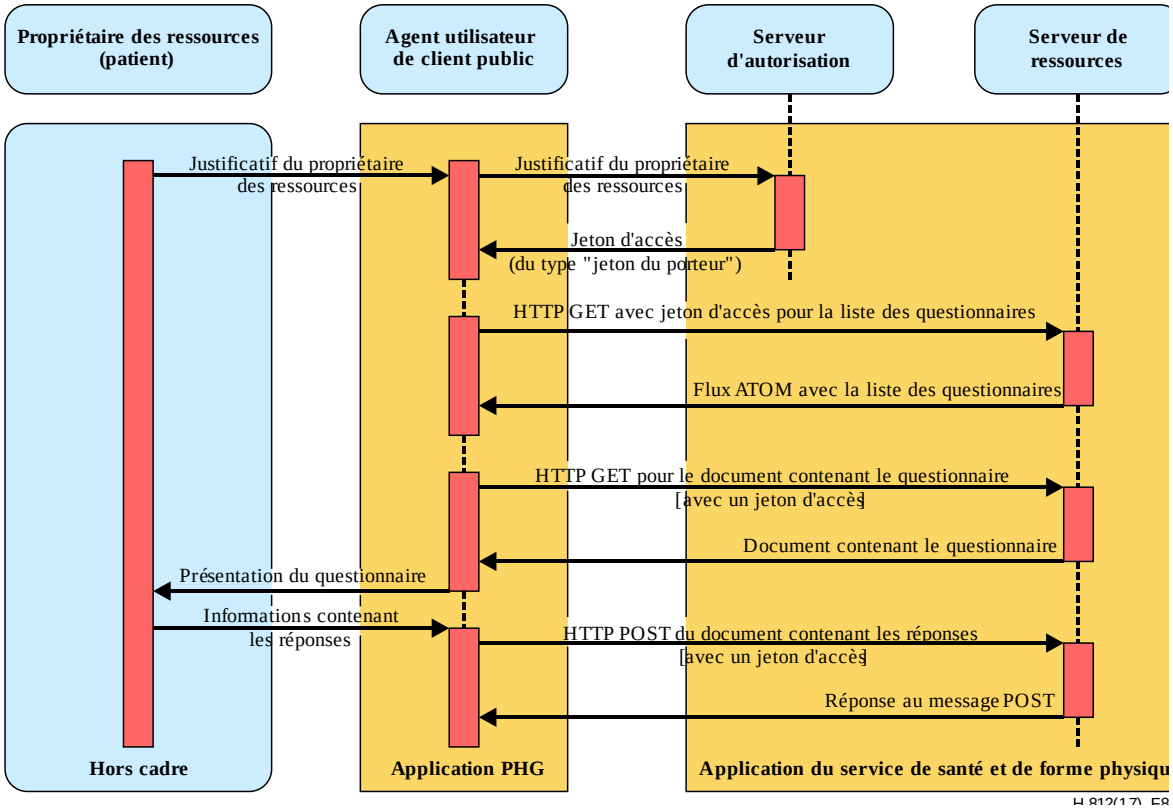

Figure 8-2 – Comportement des classes CCC autorisées utilisant le transfert REST en matière de sécurité (Le cas d'utilisation relatif aux questionnaires est utilisé comme exemple)

Les directives relatives à la sécurité des classes CCC fondées sur le transfert REST figurent dans les Tableaux B.1 et B.2.

8.3 Modèle de comportement relatif à la gestion des consentements

Les mécanismes d'échange suivants sont définis pour le service de gestion des consentements:

– Créer un *nouveau* document de consentement sur le serveur.

– Récupérer un document de consentement *déjà* établi sur le serveur.

– Charger un document de consentement *mis à jour* sur le serveur.

La Figure 8-3 illustre les transactions relatives aux cas d'utilisation de gestion des consentements décrits dans ce profil de contenu.

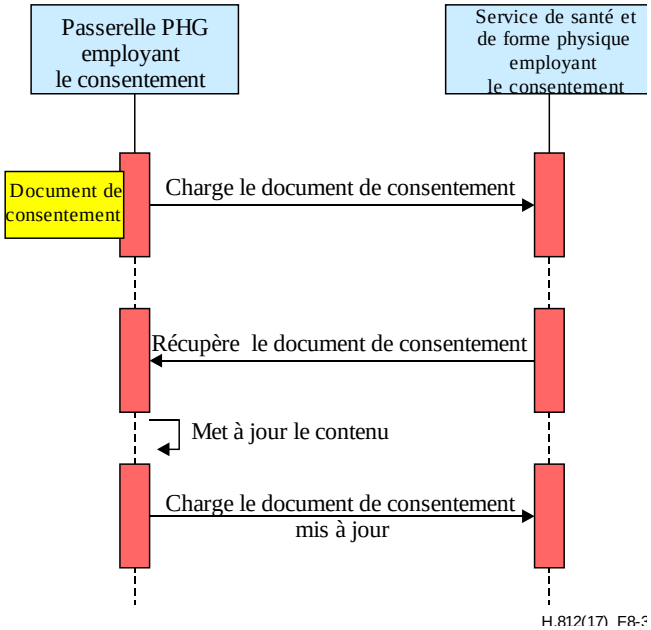

Figure 8-3 – Transactions relatives à la gestion des consentements entre la passerelle PHG et le service de santé et de forme physique

Les directives relatives à la gestion des consentements figurent dans les Tableaux C.1 et C.2.

8.4 Modèle de comportement relatif à la mise en application du consentement

La fonction suivante est définie pour la mise en application du consentement:

– Chiffrer le contenu à charger

La Figure 8-4 illustre la fonctionnalité relative à la mise en application du consentement.

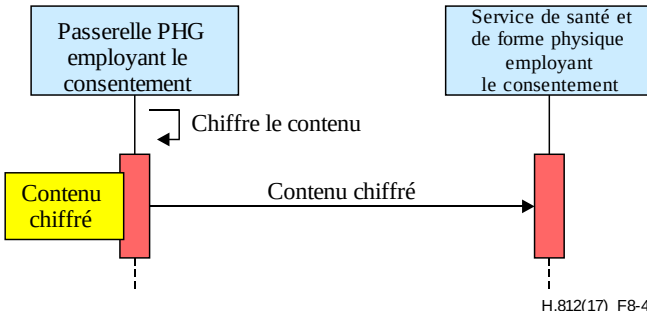

Figure 8-4 – Mise en application du consentement au niveau de l'interface Services-IF

Les directives relatives à la mise en application du consentement figurent dans les Tableaux C.3 et C.4.

9 Mise en oeuvre

9.1 Représentation du consentement

Les préférences en matière de consentement sont représentées conformément au guide *HL7 Implementation Guide for CDA Release 2.0: Consent Directive*, dans [HL7 CDA IG].

Les fichiers présentant des exemples de documents de consentement sont disponibles dans la documentation de la norme susmentionnée.

9.2 Protocoles de transport

9.2.1 Protocole de transport utilisant des données sur HTTP

Dans ce cas de figure, le protocole de transport utilisé pour l'échange de documents de consentement au niveau de l'interface Services-IF consiste à utiliser des données sur HTTP. Ce protocole prend en charge tous les cas d'utilisation mentionnés dans les paragraphes 7.1 et 7.2. Les exigences détaillées applicables à l'utilisation de ce protocole pour les communications entre la passerelle PHG et les services de santé et de forme physique figurent dans l'Annexe A ainsi que dans les Tableaux C.1, C.2, C.3 et C.4.

9.2.2 Protocole de transport utilisant le profil XDR IHE

Dans ce cas de figure, le protocole de transport utilisé pour l'échange de documents de consentement au niveau de l'interface Services-IF repose sur [IHE ITI TFS XDR]. Ce protocole ne prend en charge que le cas d'utilisation correspondant au chargement du consentement sur le serveur. Les documents de consentement sont associés aux informations sur la santé (message PCD-01) à l'aide de l'identificateur de patient. Ainsi, le consentement est associé aux informations sur la santé et conditionne leur utilisation.

9.3 Mise en application du consentement

9.3.1 Mise en application du consentement au moyen du chiffrement XML

Dans le cas du protocole de transport reposant sur [IHE ITI TFS XDR], la mise en application du consentement est réalisée au moyen du chiffrement XML défini par la norme [W3C XMLENC]. Cette norme permet le chiffrement de la charge utile de la transaction PCD-01 envoyée à un destinataire spécifique (par exemple, un médecin ou un infirmier) au service de santé et de forme physique employant le consentement.

La norme de chiffrement en langage XML est employée pour permettre la mise en application du consentement au moyen du chiffrement.

9.3.2 Mise en application du consentement au moyen du profil DEN IHE

Dans le cas du protocole de transport utilisant des données sur HTTP, la mise en application du consentement est réalisée au moyen du profil DEN IHE [IHE ITI DEN].

Annexe A

Aperçu des directives normatives

(Cette annexe fait partie intégrante de la présente Recommandation.)

Les classes de capacité homologuée sont énumérées dans le Tableau A.1.

Tableau A.1 – Classes de capacité homologuée

Nom de la classe de capacité homologuée	Classes de capacité homologuée	Classes de capacités à logo
Chargement des observations SOAP – PHG	Oui	Oui
Chargement des observations SOAP – Service de santé et de forme physique	Oui	Oui
Chargement des observations par données – PHG	Oui	Oui
Chargement des observations par données – Service de santé et de forme physique	Oui	Oui
Utilisation du consentement SOAP – PHG	Oui	Oui
Utilisation du consentement SOAP – Service de santé et de forme physique	Oui	Oui
Utilisation du consentement par données – PHG	Oui	Oui
Utilisation du consentement par données – Service de santé et de forme physique	Oui	Oui
Questionnaires – PHG	Oui	Oui
Questionnaires – Service de santé et de forme physique	Oui	Oui
Echange de capacités – PHG	Oui	Oui
Echange de capacités – Service de santé et de forme physique	Oui	Oui
Session authentifiée persistante – PHG	Oui	*
Session authentifiée persistante – Service de santé et de forme physique	Oui	*[2]

Les directives qui s'appliquent à chacune des classes de capacité homologuée sont indiquées dans le Tableau A.2 ci-dessous.

[2] * Ces cellules sont délibérément vides.

Tableau A.2 – Directives pour les classes de capacité homologuée

Classes de capacité homologuée	Directives pertinentes
Chargement des observations SOAP – PHG	Voir la Rec. [UIT-T H.812.1] et les Tableaux A.3 et B.3 de la Rec. [UIT-T H.812]
Chargement des observations SOAP – Service de santé et de forme physique	Voir la Rec. [UIT-T H.812.1] et les Tableaux A.3 et B.3 de la Rec. [UIT-T H.812]
Chargement des observations par données – PHG	Voir la Rec. [UIT-T H.812.1] et les Tableaux A.3 et B.1 de la Rec. [UIT-T H.812]
Chargement des observations par données – Service de santé et de forme physique	Voir la Rec. [UIT-T H.812.1] et les Tableaux A.3 et B.2 de la Rec. [UIT-T H.812]
Utilisation du consentement SOAP – PHG	Voir la Rec. [UIT-T H.812.1] et les Tableaux A.3, B.3, C.5 et C.7 de la Rec. [UIT-T H.812]
Utilisation du consentement SOAP – Service de santé et de forme physique	Voir la Rec. [UIT-T H.812.1] et les Tableaux A.3, B.3, C.6 et C.8 de la Rec. [UIT-T H.812]
Utilisation du consentement par données – PHG	Voir les Tableaux A.3, C.1, C.3 et B.1 de la Rec. [UIT-T H.812]
Utilisation du consentement par données – Service de santé et de forme physique	Voir les Tableaux A.3, C.2, C.4 et B.2 de la Rec. [UIT-T H.812]
Questionnaires – PHG	Voir le Tableau A.1 de la Rec. [UIT-T H.812.2] et les Tableaux A.3 et B.1 de la Rec. [UIT-T H.812]
Questionnaires – Service de santé et de forme physique	Voir le Tableau A.2 de la Rec. [UIT-T H.812.2] et les Tableaux A.3 et B.2 de la Rec. [UIT-T H.812]
Echange de capacités – PHG	Voir le Tableau A.2 de la Rec. [UIT-T H.812.3] et les Tableaux A.3 et B.1 de la Rec. [UIT-T H.812]
Echange de capacités – Service de santé et de forme physique	Voir le Tableau A.1 de la Rec. [UIT-T H.812.3], et les Tableaux A.3 et B.2 de la Rec. [UIT-T H.812]
Session authentifiée persistante – PHG	Voir les Tableaux A.1, A.2, A.3 et A.5 de la Rec. [UIT-T H.812.4] et les Tableaux A.3 et B.1 de la Rec. [UIT-T H.812]
Session authentifiée persistante – Service de santé et de forme physique	Voir les Tableaux A.1, A.4 et A.6 de la Rec. [UIT-T H.812.4] et les Tableaux A.3 et B.2 de la Rec. [UIT-T H.812]

Tableau A.3 – Exigences communes à toutes les classes CCC

Nom	Description	Observations
CapX-HFS-Universality	Tous les services de santé et de forme physique **doivent** prendre en charge l'échange de capacités, excepté pour les classes CCC de chargement des observations au moyen du protocole SOAP ou de service de santé et de forme physique employant le consentement.	Un service de santé et de forme physique qui met en oeuvre uniquement des classes CCC de chargement des observations au moyen du protocole SOAP ou de service de santé et de forme physique employant le consentement ne doit pas nécessairement prendre en charge la classe CCC d'échange de capacités d'un service de santé et de forme physique.
HFS-Transport_ Connection_Initiation	Toutes les connexions du service de santé et de forme physique **doivent** être initiées par l'application PHG du service de santé et de forme physique et **ne doivent pas** être initiées par le service de santé et de forme physique.	

Annexe B

Directives générales en matière de sécurité pour les classes CCC à l'interface Services-IF

(Cette annexe fait partie intégrante de la présente Recommandation.)

Tableau B.1 – Directives en matière de sécurité pour les passerelles PHG utilisant le transfert REST

Nom	Description	Observations
PHG-Grant_Type	Une passerelle PHG peut utiliser l'information de mot de passe du propriétaire des ressources comme type de justificatif d'autorisation, tel que défini dans la section 1.3.3 d'OAuth v2.0 [IETF RFC 6749].	Une passerelle PHG peut utiliser d'autres méthodes pour se procurer un jeton d'autorisation auprès du serveur d'autorisation.
PHG-authorization_request	Une passerelle PHG peut se procurer un jeton d'autorisation auprès du serveur d'autorisation, conformément aux sections 4.3 et 4.3.2 d'OAuth v2.0 [IETF RFC 6749].	Des exemples pour le format de la demande d'autorisation figurent dans l'Appendice III. En ce qui concerne la réponse, voir la directive associée HFS-authorization_ request_response.
PHG-bearer_token	Une passerelle PHG **doit** utiliser un jeton "du porteur" (*bearer*), conformément à [IETF RFC 6750], lorsqu'elle effectue une demande d'accès à une ressource protégée du service de santé et de forme physique [IETF RFC 6750].	Voir la directive associée HFS-authorization_request_ response.
PHG-Token_Transmit	Une passerelle PHG **doit** utiliser la méthode du champ d'en-tête de la demande d'autorisation lorsqu'elle envoie le jeton du porteur, comme défini dans la section 2.1 de [IETF RFC 6750].	
PHG-Confidentiality	Une passerelle PHG **doit** utiliser, au minimum, le protocole TLS v1.1 pour les communications sécurisées point à point avec le serveur d'autorisation et le service de santé et de forme physique [IETF RFC 4346].	
PHG-Cipher	Une passerelle PHG **devrait** employer une suite de chiffrement TLS_RSA_WITH_AES_128_ CBC_SHA.	

Tableau B.2 – Directives en matière de sécurité pour les services de santé et de forme physique utilisant le transfert REST

Nom	Description	Observations
HFS-authorization_ request_response	Un service de santé et de forme physique mettant en oeuvre le serveur d'autorisation **doit** retourner un jeton d'autorisation du type "du porteur" (*bearer*) après la validation de la demande de jeton d'accès, conformément à la section 4.3.3 d'OAuth v2.0 [IETF RFC 6749].	Voir la directive PHG-authorization_request pour le format de la demande. L'autorisation peut être constituée d'une entité distincte et ne doit pas nécessairement faire partie du service de santé et de forme physique.
HFS-refresh_token	Un service de santé et de forme physique mettant en oeuvre le serveur d'autorisation **doit** retourner un jeton d'actualisation.	
HFS-Token_Evaluation	Un service de santé et de forme physique **doit** évaluer le jeton d'autorisation et les droits qu'il ouvre avant d'autoriser l'accès à un enregistrement du service de santé et de forme physique.	

Tableau B.3 – Directives en matière de sécurité pour le transport au niveau de l'interface Services-IF

Nom	Description	Observations
HFS-Security_Transport	L'application d'un service de santé et de forme physique et les applications PHG **doivent**, au minimum, prendre en charge le protocole TLS v1.1 [IETF RFC 4346] du profil WS-I BSP v1.0 pour les communications sécurisées.	Cette directive est cohérente avec le profil ATNA IHE lorsque le chiffrement est effectué. Les directives Continua dépendent de l'indication du protocole TLS v1.1 [IETF RFC 4346] pour l'authentification mutuelle.
HFS-Security_ Transport_Cipher	L'application d'un service de santé et de forme physique et les applications PHG **doivent**, au minimum, prendre en charge le chiffrement AES, comme indiqué dans [IETF RFC 3268].	Le profil ATNA IHE prescrit l'utilisation à titre facultatif de la suite de chiffrement suivante: TLS_RSA_WITH_ AES_128_CBC_SHA. Les directives HIS emploient la suite de chiffrement suivante: TLS_RSA_WITH_ AES_128_CBC_SHA. D'autres suites de chiffrement sont admises mais elles devraient être négociées entre la passerelle PHG et le service de santé et de forme physique.
HFS-Confidentiality	Un service de santé et de forme physique **doit** utiliser le protocole TLS v1.1 pour les communications sécurisées point à point avec le serveur d'autorisation et un service de santé et de forme physique prenant en charge les questionnaires [IETF RFC 4346].	
HFS-Cipher	Un service de santé et de forme physique **devrait** prendre en charge la suite de chiffrement TLS_RSA_WITH_AES_128_CBC_SHA.	

Annexe C

Directives normatives applicables à la gestion des consentements

(Cette annexe fait partie intégrante de la présente Recommandation.)

Tableau C.1 – Directives de gestion des consentements au moyen du transfert REST pour une passerelle PHG employant le consentement

Nom	Description	Observations
PHG-Consent_Enabled	Une passerelle PHG employant le consentement doit être conforme à la norme contenant la directive relative au consentement HL7 CDA R2 en ce qui concerne la représentation des préférences du patient en matière de consentement [HL7 CDA IG].	
PHG-Consent_Enabled_ Transport_Standards	Une passerelle PHG employant le consentement doit être conforme aux normes de transport suivantes: HL7 Version 3 Specification: data Record Format, Release 1 [HL7 hRF] OMG data REST Binding for RLUS [OMG/data BIND] OMG Retrieve, Locate, and Update Service (RLUS) Specification 1.0.1 [OMG/data RLUS]	
PHG-Post_Consent	Une passerelle PHG employant le consentement doit utiliser la fonction HTTP POST avec l'URL suivant pour envoyer le consentement au service de santé et de forme physique: *baseURL/continua/consent*	Voir le cas d'utilisation du paragraphe 7.1. Le service d'extraction, de localisation et de mise à jour (RLUS) des données au moyen du transport REST est réalisé par une requête HTTP POST sans paramètre à cette URL avec le document de consentement et de protection de la vie privée dans le corps de la requête.
Consent_Enabled-PHG-Observation_Association	Le document de consentement transmis par la passerelle PHG employant le consentement doit contenir le même identificateur de patient que le ou les messages contenant les mesures faites lors des observations du service de santé et de forme physique.	Cela permet d'associer le document de consentement aux messages contenant les mesures faites lors des observations du service de santé et de forme physique.
Consent_Enabled-PHG-Observation-Association_ Value	Le champ "Patient ID" dans l'en-tête du document de consentement doit être fixé à la valeur PID-3. Les sous-champs CX-1 et CX-4 doivent être présents et le sous-champ CX-5 ne doit pas être présent.	

Tableau C.1 – Directives de gestion des consentements au moyen du transfert REST pour une passerelle PHG employant le consentement

Nom	Description	Observations
Consent_Enabled-PHG-Questionnaire Response_Confidentiality	Une passerelle PHG employant le consentement doit fixer la valeur du code de confidentialité à "R" dans l'en-tête du document contenant les réponses à un questionnaire.	
Consent_Enabled-PHG-Questionnaire Response_Association_Value	Pour associer le ou les documents contenant les réponses à un questionnaire avec le document de consentement du patient, une passerelle PHG employant le consentement doit utiliser l'élément de conversion du système de code de confidentialité, comme défini dans le Tableau IV.3.	Voir les Tableaux IV.1, IV.2 et IV.4.
Retrieving_Consent	Une passerelle PHG employant le consentement doit utiliser la fonction HTTP GET avec l'URL suivant pour récupérer le consentement auprès du service de santé et de forme physique: *baseURL/continua/consent*. Une passerelle PHG employant le consentement doit utiliser la fonction HTTP GET avec la valeur de l'élément de lien de l'entrée du flux ATOM pour récupérer le document de consentement actuel auprès du service de santé et de forme physique et doit valider qu'il s'agit d'un document conforme à la directive relative au consentement R2 CDA HL7 [HL7 CDA IG].	Voir le cas d'utilisation du paragraphe 7.1. Le service RLUS de données utilisant le transport REST est réalisé par une requête HTTP GET sans paramètre à l'URL correspondant au chemin de la section contenant les données relatives au consentement du patient. Cette requête retourne l'entrée du flux ATOM. Se référer au Tableau I.1 pour plus de renseignements au sujet de l'entrée du flux ATOM.

Tableau C.2 – Directives de gestion des consentements au moyen du transfert REST pour un service de santé et de forme physique employant le consentement

Nom	Description	Observations
Consent_Enabled-Health-&-Fitness-Service	Un service de santé et de forme physique employant le consentement doit être en mesure de recevoir le ou les documents de consentement du patient conformes à la directive relative au consentement HL7 CDA R2 [HL7 CDA IG].	

Tableau C.2 – Directives de gestion des consentements au moyen du transfert REST pour un service de santé et de forme physique employant le consentement

Nom	Description	Observations
Health-&-Fitness Service-Consent_Enabled_Transport_Standards	Une passerelle PHG employant le consentement doit se conformer aux normes de transport suivantes: HL7 Version 3 Specification: data Record Format, Release 1 [HL7 hRF] OMG data REST Binding for RLUS [OMG/data BIND] OMG Retrieve, Locate, and Update Service (RLUS) Specification 1.0.1 [OMG/data RLUS]	
HFS-Consent_Root	Un service de santé et de forme physique employant le consentement doit inclure les éléments suivants dans le fichier root.xml pour le contenu des questionnaires: 1) profile a) id="consent" b) reference="http://handle.itu.int/11.1002/3000/hData/Consent/2017/01/H.812.pdf" 2) section a) path="consent" b) profileID= "consent" c) resourceTypeId="consent" 3) resourceType a) resourceTypeId="consent" b) reference="http://www.hl7.org/dstucomments/showdetail.cfm?dstuid=63" c) representation d) mediaType="application/xml2"	Note: L'URL fourni en référence au point 1.b a seulement valeur d'exemple.
HFS-Consent_Validate	Un service de santé et de forme physique employant le consentement doit valider que le document de consentement est conforme à la directive relative au consentement HL7 CDA R2 et envoyer le message HTTP 200 en tant que réponse si le document est valide.	
HFS-Post_Consent-Response	Un service de santé et de forme physique employant le consentement doit créer un enregistrement contenant le document de consentement après la réception du message POST de la passerelle PHG employant le consentement et envoyer le message HTTP 201 en tant que réponse.	Voir *PHG-Post_Consent* ci-dessus

Tableau C.2 – Directives de gestion des consentements au moyen du transfert REST pour un service de santé et de forme physique employant le consentement

Nom	Description	Observations
PHG-Delete_Consent_Response	Un service de santé et de forme physique employant le consentement n'est pas tenu de prendre en charge la suppression d'un enregistrement contenant un document de consentement existant et doit retourner un message HTTP 405 "Méthode non autorisée" en tant que réponse à une requête HTTP DELETE portant sur l'URL d'un consentement.	

Tableau C.3 – Directives relatives à la mise en application du consentement au moyen de données pour une passerelle PHG employant le consentement

Nom	Description	Observations
Consent_Enabled-PHG-Content-Encryption_Actor	Une passerelle PHG employant le consentement doit chiffrer le contenu conformément au profil de chiffrement de document (DEN) IHE.	Ici, le contenu peut être la charge utile de la transaction PCD-01 ou le document contenant les réponses à un questionnaire.
Consent_Enabled-PHG-Questionnaire-Response_MIMEtype_	Une passerelle PHG employant le consentement doit fixer le type MIME à la valeur "application/xml" dans le cas où le contenu chiffré correspond aux réponses à un questionnaire.	Le but est d'indiquer le type de charge utile qui est chiffrée.
Consent_Enabled-PHG-Observation - Upload_MIMEtype_	Une passerelle PHG employant le consentement doit fixer le type MIME à la valeur "application/txt" dans le cas où le contenu chiffré correspond au chargement d'observations.	Le but est d'indiquer le type de charge utile qui est chiffrée.
Consent_Enabled-PHG-Content-Encryption_Algorithm	Une passerelle PHG employant le consentement doit utiliser l'algorithme AES-128 CBC pour le chiffrement du contenu.	L'algorithme utilisé est identifié au moyen de l'identificateur ContentEncryptionAlgorithmIdentifier dans la syntaxe cryptographique de message (CMS), décrite de manière plus détaillée dans le profil DEN IHE.
Consent_Enabled-PHG-Encryption-Recipient_Binding_PKI	Une passerelle PHG employant le consentement doit utiliser la méthode de gestion des clés fondée sur l'infrastructure PKI du profil DEN IHE [IHE ITI DEN].	La méthode de gestion des clés de contenu fondée sur l'infrastructure PKI emploie l'information KeyTransRecipientInfo comme type RecipientInfoType de la syntaxe CMS. Cela renvoie vers la clé publique ou vers le certificat x.509 v3 du destinataire.

Tableau C.4 – Directives de gestion des consentements au moyen du protocole SOAP pour une passerelle PHG employant le consentement

Nom	Description	Observations
HFS-Device_HTTP_Ack	Un service de santé et de forme physique employant le consentement doit envoyer le message HTTP 202 en tant que réponse après avoir bien reçu le contenu chiffré.	
Consent_Enabled-HFS-Content-Decryption_Actor_XDR	Un service de santé et de forme physique employant le consentement doit être conforme au profil DEN IHE pour déchiffrer le contenu chiffré [IHE ITI DEN].	
Consent_EnabledKey_Management	Un service de santé et de forme physique employant le consentement doit utiliser la méthode de gestion des clés fondée sur l'infrastructure PKI, comme indiqué dans le profil DEN IHE [IHE ITI DEN].	
Consent_Enabled-HFS-Decryption-Algorithm	Un service de santé et de forme physique employant le consentement doit utiliser l'algorithme de déchiffrement AES.128 CBC pour déchiffrer la charge utile.	L'algorithme utilisé est identifié au moyen de l'identificateur ContentEncryptionAlgorithmIdentifier dans la syntaxe cryptographique de message (CMS).
Consent_Enabled-HFS-Consent_Enforcement_	Un service de santé et de forme physique employant le consentement doit mettre en application les préférences en matière de consentement exprimées dans le document de consentement.	Cela évite par exemple la divulgation ultérieure du contenu à des entités non autorisées.

Tableau C.5 – Directives de gestion des consentements au moyen du protocole SOAP pour un service de santé et de forme physique employant le consentement

Nom	Description	Observations
Services-Observation-PHG-Consent	Une passerelle PHG pour la transmission des observations aux services employant le consentement **doit** être conforme à la directive relative au consentement [HL7 CDA IG] en ce qui concerne la représentation du consentement du patient dans un document de consentement.	
Services-Observation-PHG-Consent-Transport	Une passerelle PHG pour la transmission des observations aux services employant le consentement **doit** mettre en oeuvre l'acteur source de documents de l'échange XDR IHE pour envoyer un document de consentement au moyen de la transaction de fourniture et d'enregistrement du lot de documents-b ITI 41.	

Tableau C.5 – Directives de gestion des consentements au moyen du protocole SOAP pour un service de santé et de forme physique employant le consentement

Nom	Description	Observations
Services-Observation-PHG-Consent-Frequency	Une passerelle PHG pour la transmission des observations aux services employant le consentement **doit** envoyer le document de consentement au moins une fois au service de santé et de forme physique fondé sur des observations.	Le document de consentement est par exemple d'abord envoyé au cours de l'immatriculation auprès du service. Il est recommandé d'envoyer, pendant la durée de la connexion, au moins une fois le consentement au service de santé et de forme physique fondé sur des observations. Les cas d'utilisation tels que la mise à jour des préférences en matière de consentement doivent aussi être pris en charge. Le document de consentement mis à jour remplace le document de consentement existant au niveau du service de santé et de forme physique fondé sur des observations et employant le consentement.
HFS-Observation_ Measurement_ Consent_Document_ Association	Le document de consentement transmis par la passerelle PHG pour la transmission des observations aux services employant le consentement **doit** contenir le même identificateur de patient que le ou les messages contenant les mesures faites lors des observations des services.	Cela permet d'associer le document de consentement aux messages contenant les mesures faites lors des observations des services de santé et de forme physique.
HFS-Observation_ Measurement_Consent_ Document_Association_Value	Le champ "Patient ID" dans l'en-tête du document de consentement **doit** être fixé à la valeur PID-3. Les sous-champs CX-1 et CX-4 **doivent** être présents et le sous-champ CX-5 **ne doit pas** être présent.	

Tableau C.6 – Directives de gestion des consentements au moyen du protocole SOAP pour un service de santé et de forme physique employant le consentement

Nom	Description	Observations
Observation-Health-&-Fitness-Service-Consent	Un service de santé et de forme physique fondé sur des observations et employant le consentement **doit** pouvoir recevoir le ou les documents de consentement du patient conformes à la directive relative au consentement [HL7 CDA IG].	
Observation-HFS-Consent_Transport	Un service de santé et de forme physique fondé sur des observations et employant le consentement **doit** mettre en oeuvre l'acteur destinataire de documents de l'échange XDR IHE pour pouvoir recevoir un document de consentement au moyen de la transaction de fourniture et d'enregistrement du lot de documents-b ITI 41.	Le service de santé et de forme physique fondé sur des observations remplace le document de consentement existant lors de la réception d'une nouvelle version, comme indiqué par les métadonnées XDS du document de consentement.

Tableau C.7 – Directives de mise en application du consentement au moyen du protocole SOAP pour une passerelle PHG employant le consentement

Nom	Description	Observations
HFS-PHG-Content_ Encryption_Actor	Une passerelle PHG pour la transmission des observations aux services de santé et de forme physique employant le consentement **doit** chiffrer la charge utile (Annexe D de la Rec. [UIT-T H.812.1]) de la transaction PCD-01 en conformité avec les règles de chiffrement définies au § 4.1 de la spécification XML Encryption Specification [W3C XMLENC].	
HFS-PHG-Content_ Encryption_MIMEtype	Une passerelle PHG pour la transmission des observations aux services de santé et de forme physique employant le consentement **doit** fixer le type MIME à "application/hl7-v2+xml".	Le but est d'indiquer le type de charge utile qui est chiffrée.
HFS-Services-PHG-Content_ Encryption_Algorithm	Une passerelle PHG pour la transmission des observations aux services de santé et de forme physique employant le consentement doit utiliser l'algorithme AES-128 CBC de la spécification XML Encryption Specification pour le chiffrement de la charge utile.	L'algorithme AES-128 CBC est identifié au moyen de l'identificateur suivant: http://www.w3.org/2001/04/xmlenc#aes128-cbc [W3C XMLENC].

Tableau C.7 – Directives de mise en application du consentement au moyen du protocole SOAP pour une passerelle PHG employant le consentement

Nom	Description	Observations
HFS-PHG-Encryption_ Recipient_Binding_PKI	Pour le transport de la clé de contenu, une passerelle PHG pour la transmission des observations aux services de santé et de forme physique employant le consentement **doit** prendre en charge la Version 1.5 de la norme RSA figurant dans la spécification XML Encryption Specification.	Le transport de la clé fondé sur la norme RSA v1.5 est identifié au moyen de l'identificateur suivant [W3C XMLENC]: http://www.w3.org/2001/04/xmlenc#rsa-1_5. Pour des informations détaillées sur ladite norme, consulter la référence [b-RFC 2437]. Le transport de la clé fondé sur la norme RSA v1.5 est aussi employé dans la norme traitant de la syntaxe cryptographique de message (CMS), qui est employée sur l'interface HIS-IF. Pour plus de détails, consulter la référence [b-RFC 3370] et les directives relatives à la mise en application du consentement pour l'interface HIS-IF.
HFS-PHG-Encryption_ Recipient_Binding_ Symmetric	Pour le transport de la clé de contenu, une passerelle PHG pour la transmission des observations aux services de santé et de forme physique employant le consentement **devrait** employer l'algorithme d'emballage de clés symétriques AES-128 de la spécification XML Encryption Specification. Dans le cas d'un chiffrement employant un mot de passe, une passerelle PHG pour la transmission des observations aux services de santé et de forme physique employant le consentement peut employer l'algorithme PBKDF2 de la référence [IETF RFC 3211] pour obtenir la clé.	L'identificateur employé pour l'emballage de clés symétriques AES-128 est http://www.w3.org/2001/04/xmlenc#kw-aes128 [W3C XMLENC]. La clé utilisée dans l'emballage est nommée KEK et peut être obtenue au moyen d'un mot de passe ou d'une clé secrète partagée sur une longue période.
HFS-PHG-Integrity_ Payload_PCD-01_Create	Une passerelle PHG pour la transmission des observations aux services de santé et de forme physique employant le consentement **doit** calculer le condensé de la charge utile chiffrée au moyen de l'algorithme SHA256 (§ 5.7.2), conformément à la spécification XML Encryption Specification.	L'algorithme SHA256 est identifié au moyen de l'adresse URL suivante: http://www.w3.org/2001/04/xmlenc#sha256 [W3C XMLENC].

Tableau C.7 – Directives de mise en application du consentement au moyen du protocole SOAP pour une passerelle PHG employant le consentement

Nom	Description	Observations
HFS-Encrypted_ Payload_PCD-01_ transaction	Une passerelle PHG pour la transmission des observations aux services de santé et de forme physique employant le consentement **doit** emballer la charge utile chiffrée dans l'élément <CommunicateEncPCDData xmlns= "urn:ihe:continua:enc:pcd:dec:2012">.	Dans le cas d'une charge utile non chiffrée, le contenu est emballé dans l'élément <CommunicatePCDData xmlns= "urn:ihe:pcd:dec:2010">. Voir l'exemple dans la Figure II.1.
HFS-Encrypted_ Payload_PCD-01_Transaction_Header	Dans le cas d'une charge utile chiffrée, l'en-tête SOAP **doit** contenir la séquence "urn:ihe:continua:enc:pcd:dec:2012:CommunicateEncPCDData" au lieu de la séquence "urn:ihe: pcd:dec:2010: CommunicatePCDData".	Une transaction PCD-01 simple contient la séquence "urn:ihe: pcd:dec:2010:CommunicatePCDData". Voir les exemples dans les Figures II.1, II.2 et II.3.

Tableau C.8 – Directives de mise en application du consentement au moyen du protocole SOAP pour un service de santé et de forme physique employant le consentement

Nom	Description	Observations
HFS-HTTP-Ack	Un service de santé et de forme physique fondé sur des observations et employant le consentement **doit** envoyer une réponse HTTP SOAP contenant un code d'état égal à 202 après avoir bien reçu le message chiffré. Un service de santé et de forme physique fondé sur des observations et employant le consentement **ne devrait pas** envoyer d'accusé de réception au niveau de l'application PCD-01.	Il se pourrait en effet que le service de santé et de forme physique fondé sur des observations ne soit pas en possession de la clé de déchiffrement, le contenu pouvant être chiffré pour un destinataire particulier au niveau du service de santé et de forme physique.
HFS-Payload-PCD-01-Verify-Integrity	Un service de santé et de forme physique fondé sur des observations et employant le consentement **doit** vérifier le condensé de la charge utile chiffrée dans le message.	
HFS-Payload-PCD-01-Verify-Integrity-Algorithm	Un service de santé et de forme physique fondé sur des observations et employant le consentement **doit** prendre en charge l'algorithme SHA 256.	
HFS-Content-Decryption-Actor	Un service de santé et de forme physique fondé sur des observations et employant le consentement **doit** être conforme aux règles de déchiffrement indiquées au § 4.2 de la spécification XML Encryption Specification [W3C XMLENC].	

Tableau C.8 – Directives de mise en application du consentement au moyen du protocole SOAP pour un service de santé et de forme physique employant le consentement

Nom	Description	Observations
HFS-Key-Transport-RSA	Un service de santé et de forme physique fondé sur des observations et employant le consentement **doit** prendre en charge la Version 1.5 de la norme RSA figurant dans la spécification XML Encryption Specification [W3C XMLENC].	
HFS-Key-Transport-Symmetric	Un service de santé et de forme physique fondé sur des observations et employant le consentement **doit** prendre en charge l'algorithme d'emballage de clés symétriques AES-128 de la spécification XML Encryption Specification [W3C XMLENC]. Un service de santé et de forme physique fondé sur des observations et employant le consentement **doit** prendre en charge l'algorithme PBKDF2 d'obtention de la clé figurant dans la référence [IETF RFC 3211].	L'identificateur employé pour l'emballage de clés symétriques AES-128 est http://www.w3.org/2001/04/xmlenc#kw-aes128 [W3C XMLENC]. La clé utilisée dans l'emballage est nommée KEK et peut être obtenue au moyen d'un mot de passe ou d'une clé secrète partagée sur une longue période.
HFS-Content-Decryption-Algorithm	Un service de santé et de forme physique fondé sur des observations et employant le consentement **doit** utiliser l'algorithme de déchiffrement AES-128 CBC de la spécification XML Encryption Specification [W3C XMLENC].	L'algorithme AES-128 CBC est identifié au moyen de l'identificateur suivant: http://www.w3.org/2001/04/xmlenc#aes128-cbc [W3C XMLENC].

Appendice I

Eléments du flux ATOM relatifs à la gestion des consentements

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

Les éléments enfants suivants du flux ATOM de l'élément d'entrée ont une utilité particulière dans le cadre des documents de consentement.

Tableau I.1 – Eléments enfants du flux ATOM relatifs à la gestion des consentements

Elément	Utilité
Auteur	Construction relative à une personne indiquant qui a fourni les informations présentes dans le document de consentement, autrement dit, la personne ayant complété le formulaire de consentement.
Titre	Titre du document de consentement du patient (par exemple, autorisation et consentement de Georges).
Lien	Référence au document contenant les directives en matière de consentement de Georges. Ce document doit être conforme au guide de mise en oeuvre de la directive relative au consentement HL7 CDA R2. Le lien doit être relatif et le document de consentement et de protection de la vie privée doit se trouver dans la section de l'enregistrement de données dédiée au consentement.
Publication	Cet élément doit contenir la date et l'heure de la publication du document de consentement et de protection de la vie privée sur le serveur.

I.1 Informations relatives au consentement dans le fichier root.xml

```
<profile>
   <id>consent</id>

<reference><http://handle.itu.int/11.1002/3000/hData/Consent/2017/01/H.812.pdf></reference>
</profile>
<section>
  <path>consent</path>
  <profileID>consentId</profileID>
  <resourceTypeID>consent</resourceTypeID>
</section>
<resourceType>
  <resourceTypeID>consent</resourceTypeID>
  <reference>
    http://www.hl7.org/dstucomments/showdetail.cfm?dstuid=63
  </reference>
  <representation>
     <mediaType>application/xml</mediaType>
  </representation>
</resourceType>
```

Appendice II

Exemples de gestion des consentements utilisant le protocole SOAP

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

```
<html version="1.0" encoding="UTF-8" ?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
   <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing" >
      <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
soapenv:mustUnderstand="true" >
      <wsa:To
soapenv:mustUnderstand="true">
https://localhost:8443/WanReceiver/services/DeviceObservationConsumer_Service>/wsa:To>
      <wsa:ReplyTo soapenv:mustUnderstand="true">
         <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
      </wsa:ReplyTo>
      <wsa:MessageID
soapenv:mustUnderstand="true">urn:uuid:BC4B55779CD53E3F0C1333967505413</wsa:MessageID>
      <wsa:Action soapenv:mustUnderstand="true">urn:ihe:pcd:2010:CommunicatePCDData</wsa:Action>
      </soapenv:Header>
      <soapenv:Body>
         <CommunicatePCDData xmls="urn:ihe:pcd:dec:2010">
            MSH|^~\&|AT4_PHG^123456789ABCDEF^EUI-
            64|||20120409103145+0000||ORU^R01^ORU_R01|MSGID2848518|P|2.6|||NE|AL|||||IHE PCD ORU-
            R012006^HL7^2.16.840.1.113883.9.n.m^HL7 PID|||789567^^^Imaginary
            Hospital^PI||Doe^John^Joseph^^^^L
            OBR|1|POTest^AT4_PHG^1234567890ABCDEF^EUI-64|POTest^AT4_PHG*1234567890ABCDEF^EUI-
            64|182777000^monitoring of patient^SNOMED-CT|||20100903124015+0000
            OBX|1|CWE|68220^MDC_TIME_SYNC_PROTOCOL^MDC|0.0.0.1|532224^MDC_Time_SYNC_NONE^MDC||||||
            R
            OBX|2|CWE|68220^MDC_REG_CERT_DATA_AUTH_BODY^MDC|0.0.0.2|1^auth-body-continua(2)||||||R
            OBX|3|ST|588800^MDC_REG_CERT_DATA_CONTINUA_VERSION^MDC|0.0.0.3|1.5||||||R
            OBX|4||528388^MDC_DEV_SPEC_PROFILE_PULS_OXIM^MDC|1||||||X||||||1234567890ABCDEF^EUI-64
            OBX|5|ST|531696^MDC_ID_MODEL_NUMBER^MDC|PulseOx v1.5||||||R
            OBX|6|ST|531970^MDC_ID_MANUFACTURER^MDC|1.0.0.2|AT4 Wireless||||||R
            OBX|7|DTM|67975|^MDC_ATTR_TIME_ABS^MDC|1.0.0.3|20100903124015+0000||||||R2010090312401
            5+0000
            OBX|8|CWE|68218^MDC_CERT_DATA_AUTH_BODY^MDC|1.0.0.4|1^auth-body-continua(2)||||||R
            OBX|9|ST|588800^MDC_REG_CERT_DATA_CONTINUA_VERSION^MDC|1.0.0.5||||||R
            OBX|10|NA|588801^MDC_REG_CERT_DATA_CONTINUA_CERT_DEV_LIST^MDC|1.0.0.6|16388||||||R
            OBX|11|CWE|588802^MDC_REG_CERT_DATA_CONTINUA_REG_STATUS^MDC|1.0.0.7|0^unregulated-
            device(0)||||||R
            OBX|12|NM|150456^MDC_DIM_PERCENT^MDC|||||R|||20100903124015+0000
            OBX|13|NM|149520^MDC_PULS_OXIM_RATE^MDC|1.0.0.9|71|264864^MDC_DIM_BEAT_PER_MIN^MDC||||
            |R|||20100903124015+0000
         </soapenv:Body>
      </soapenv:Envelop>
```

Figure II.1 – Transaction PCD-01 avec une charge utile non chiffrée

```
<html version="1.0" encoding="UTF-8" ?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
   <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing" >
      <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
   soapenv:mustUnderstand="true">
<wsa:To
soapenv:mustUnderstand="true"
>https://localhost:8443/WanReceiver/services/DeviceObservationConsumer_Services/DeviceObservationC
onsumer_Service</wsa:To>
      <wsa:ReplyTo soapenv:mustUnderstand="true">
         <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
      </wsa:ReplyTo>
      <wsa:MessageID
soapenv:mustUnderstand="true">urn:uuid:BC4B55779CD53E3F0C1333967505413</wsa:MessageID>
      <wsa:Action soapenv:mustUnderstand="true">urn:ihe:pcd:2010:CommunicatePCDData</wsa:Action>
      </soapenv:Header>
      <soapenv:Body>
         <CommunicateEncPCDData xmlns="urn:ihe:continuacenc:pcd:dec:2012">
<EncryptedData xmlns=http://www.w3.org/2001/04/xmlenc#    MimeType="applicationhl7-v2+xml">
      <EncryptionMethod Algorithm=http://www.w3.org/2001/04/xmlenc#aes128-cbc/>
      <KeyInfo xmlns+"http://www.w3.org/2000/09/xmldsig#">
            <EncryptedKey xmlns=http://www.w3.org/2001/04/xmlenc#">
<Encryption Method Algorithm=http://www.w3.org/2001/04/xmlenc#rsa-1_5/>
                     <KeyInfo xmlns=http://www.w3.org/2000/09/xmldsig#>
                        <KeyName>John Smith</KeyName>
                     </KeyInfo>
                     <CipherData>
                        <CipherValue>Encrypted Key…</CipherValue>
                     </CipherData>
                  </EncryptedKey>
            </KeyInfo>
            <CipherData>
                     <CipherValu>Enc.OBX Message goes here…</CipherValue>
            </CipherData>
            </EncrptedData>
         </CommunicateEncPCDData>
      </soapenv:Body>
   </soapenv:Envelop>
```

Figure II.2 – Transaction PCD-01 chiffrée sur la base d'une clé publique

La Figure II.2 présente une transaction PCD-01 avec une charge utile chiffrée à l'aide de la norme de chiffrement XML. La clé de contenu est chiffrée à l'aide de la clé publique du destinataire.

```
<html version=”1.0” encoding=”UTF-8” ?>
<soapenv:Envelope xmlns:soapenv=”http://www.w3.org/2003/05/soap-envelope”>
   <soapenv:Header xmlns:wsa=”http://www.w3.org/2005/08/addressing” >
      <wsse:Security xmlns:wsse=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd”
   soapenv:mustUnderstand=”true”>
<wsa:To
soapenv:mustUnderstand=”true”
>https://localhost:8443/WanReceiver/services/DeviceObservationConsumer_Services/DeviceObservationC
onsumer_Service</wsa:To>
      <wsa:ReplyTo soapenv:mustUnderstand=”true”>
         <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
      </wsa:ReplyTo>
      <wsa:MessageID
soapenv:mustUnderstand=”true”>urn:uuid:BC4B55779CD53E3F0C1333967505413</wsa:MessageID>
      <wsa:Action soapenv:mustUnderstand=”true”>urn:ihe:pcd:2010:CommunicatePCDData</wsa:Action>
      </soapenv:Header>
      <soapenv:Body>
         <CommunicateEncPCDData xmlns=”urn:ihe:continuacenc:pcd:dec:2012”>
<EncryptedData xmlns=http://www.w3.org/2001/04/xmlenc#    MimeType=”applicationhl7-v2+xml”>
      <EncryptionMethod Algorithm=http://www.w3.org/2001/04/xmlenc#aes128-cbc/>
      <KeyInfo xmlns+”http://www.w3.org/2000/09/xmldsig#”>
            <EncryptedKey xmlns=http://www.w3.org/2001/04/xmlenc#”>
<Encryption Method Algorithm=http://www.w3.org/2001/04/xmlenc #rsa-1_5/>
                     <KeyInfo xmlns=http://www.w3.org/2000/09/xmldsig#>
                        <KeyName>John Smith</KeyName>
                     </KeyInfo>
                     <CipherData>
                        <CipherValue>Encrypted Key…</CipherValue>
                     </CipherData>
                  </EncryptedKey>
            </KeyInfo>
            <CipherData>
                     <CipherValu>Enc.OBX Message goes here…</CipherValue>
            </CipherData>
            </EncrptedData>
         </CommunicateEncPCDData>
      </soapenv:Body>
   </soapenv:Envelop>
```

Figure II.3 – Transaction PCD-01 chiffrée sur la base d'une clé symétrique

La Figure II.3 présente une transaction PCD-01 avec une charge utile chiffrée à l'aide de la norme de chiffrement XML. Dans cet exemple, on considère que la clé de contenu est connue de l'expéditeur et du destinataire et qu'elle est en lecture seule.

Appendice III

Exemple d'OAuth

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

Exemple 1:

– Demande de jeton d'accès

Afin d'obtenir un jeton d'accès, une passerelle PHG prenant en charge les questionnaires envoie la requête HTTP POST suivante au serveur d'autorisation.

```
POST http://localhost:3000/oauth2/token HTTP/1.1
User-Agent: Fiddler
Host: localhost:3000
Authorization: Basic
MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl
Content-Type: application/x-www-form-urlencoded
Content-Length: 59

grant_type=password&username=john@example.com&password=test
```

Où:

- http://localhost:3000/oauth2/token est l'URL du serveur d'autorisation et doit être connu par la passerelle PHG prenant en charge les questionnaires.
- Authorization: Basic MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl
- Il s'agit de l'en-tête de base d'une autorisation HTTP, générée par une passerelle PHG prenant en charge les questionnaires au moyen de l'identificateur qui lui a été attribué et du mot secret, en chiffrant ces données à l'aide d'une chaine de hachage de type Base64: Base64("120094574673767:b54dc82476af2814e620b86776c42c0e") =
- "MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl"
- *grand_type* indique le code de l'autorisation, qui, dans ce cas, comprend le nom d'utilisateur (*username*) et le mot de passe (*password*).
- Réponse contenant le jeton d'accès

Le serveur d'autorisation valide la demande de jeton d'accès et, le cas échéant, génère un jeton d'accès du type jeton "du porteur" (*bearer*) ainsi qu'un jeton d'actualisation facultatif.

```
HTTP/1.1 200 OK
Content-Length: 141
Content-Type: application/json
X-Ua-Compatible: IE=Edge
X-Runtime: 0.273027
Server: WEBrick/1.3.1 (Ruby/1.9.3/2013-02-22)
Date: Wed, 03 Apr 2013 08:54:57 GMT
Connection: Keep-Alive

{"access_token":"f779da766bfd1b9164b0fd6d280d52f1","refresh_token":"789f3daf81
a302e0636325114113e4b4","token_type":"bearer","expires_in":899}
```

Où:

- "f779da766bfd1b9164b0fd6d280d52f1" est le jeton d'accès qui sera utilisé par la passerelle PHG lorsqu'elle accèdera à une ressource sur le serveur.
- "789f3daf81a302e0636325114113e4b4" est le jeton d'actualisation qui peut être utilisé pour obtenir un nouveau jeton.
- Dans l'exemple ci-dessus, le jeton est du type jeton "du porteur".
- Le jeton a une durée de vie de 899 secondes.

– Demande d'accès à une ressource à l'aide d'un jeton d'accès du type jeton "du porteur"

Exemple 2:

Dans l'exemple ci-dessous, la passerelle PHG utilise un jeton du porteur pour demander l'accès à une ressource protégée, par exemple, un questionnaire.

```
GET http://localhost:3000/hdata/root.xml HTTP/1.1
User-Agent: Fiddler
Host: localhost:3000
Authorization: Bearer f779da766bfd1b9164b0fd6d280d52f1
```

Appendice IV

Association entre un questionnaire et des réponses dans une passerelle PHG employant le consentement

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

Tableau IV.1 – Eléments du système de code de confidentialité

Nom	Valeur	Remarques
Code	"R"	
codeSystem	2.16.840.1.113883.5.25	
codeSystemName	"Confidentiality" (confidentialité)	
displayName	"Restricted" (restreint)	

Tableau IV.2 – Eléments du système de code des directives Continua en matière de consentement

Nom	Valeur	Remarques
Code	La valeur **doit** être identique à celle spécifiée dans [HL7 CDA IG].	
codeSystem	2.16.840.1.113883.3.1817.1.2.1	
codeSystemName	"Continua Consent Directive" (directive Continua en matière de consentement)	
displayName	Identifiant du document de consentement	

Tableau IV.3 – Correspondances entre le système de code de confidentialité et le système de code des directives Continua en matière de consentement

Nom	Valeur	Remarques
Code	"R"	
codeSystem	2.16.840.1.113883.5.25	
codeSystemName	"Confidentiality" (confidentialité)	
displayName	"Restricted" (restreint)	
translation	code="<ID of the consent document>" codeSystem=2.16.840.1.113883.3.1817.1.2.1 codeSystemName="Continua Consent Directive" displayName= identifiant du document de consentement	"<>" est un emplacement réservé (*placeholder*) destiné à recevoir l'identifiant du document de consentement. Se reporter au Tableau IV.2 pour les éléments du système de code des directives Continua en matière de consentement.

Tableau IV.4 – Répartition des OID pour la Personal Connected Health Alliance

OID	Description	Remarques
2.16.840.1.113883.3.1817	OID de l'organisation: Personal Connected Health Alliance	
2.16.840.1.113883.3.1817.1	OID racine pour l'architecture Continua de bout en bout v1.0	
2.16.840.1.113883.3.1817.1.2	OID racine pour la sécurité et la protection de la vie privée de bout en bout	
2.16.840.1.113883.3.1817.1.3	OID racine pour l'interface PHD-IF	
2.16.840.1.113883.3.1817.1.4	OID racine pour l'interface ZigBee PHD-IF	
2.16.840.1.113883.3.1817.1.5	OID racine pour l'interface NFC PHD-IF	
2.16.840.1.113883.3.1817.1.6	OID racine pour l'interface Services-IF	
2.16.840.1.113883.3.1817.1.7	OID racine pour l'interface HIS-IF	
2.16.840.1.113883.3.1817.1.2.1	Sécurité et protection de la vie privée de bout en bout: OID pour le système de code des directives Continua en matière de consentement	

Bibliographie

On trouvera dans la Recommandation [UIT-T H.810] une liste de publications et documents de référence non normatifs contenant des informations générales complémentaires.

SERIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	**Systèmes audiovisuels et multimédias**
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2019