AGENCE
DU NUMÉRIQUE
EN SANTÉ

Pro Santé Connect

Référentiel Communauté PSC et Communauté PSC - Extension Espace de Confiance

Statut : Terminé | *Classification : Publique* | *Version : 1.0*

Agence du Numérique en Santé
2-10 Rue d'Oradour-sur-Glane – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

Historique du document

Version	Date de publication	Motif et nature de la modification
1.0	Octobre 2024	- Document modifié pour prise en compte des retours suite à la concertation de juin 2024

SOMMAIRE

ILLUSTRATIONS

1 INTRODUCTION

1.1 Qu'est-ce que Pro Santé Connect ?

Pro Santé Connect (PSC) est le fédérateur d'identité des professionnels des secteurs sanitaire, médico-social et social enregistrés au *Répertoire Partagé des Professionnels de Santé* (RPPS). Ce service socle est proposé par l'*Agence du Numérique en Santé* (ANS).

Il leur offre une manière simple, sécurisée et unifiée de se connecter à tous leurs services numériques, en pouvant passer de l'un à l'autre de manière particulièrement fluide.

Les *Fournisseurs de Services* (FS) numériques peuvent implémenter ce service socle basé sur des technologies standardisées. PSC leur permet :

- Une sécurisation de l'identification électronique des professionnels, protégeant les données de santé éventuellement traitées, et garantissant une conformité réglementaire sur le niveau de garantie de l'identification électronique de leurs Utilisateurs ;
- Un engagement de leurs Utilisateurs, familiers de ce mode d'identification électronique commun à de nombreux services ;
- De récupérer les traits d'identité des professionnels, ainsi que le cas échéant des données sectorielles associées (profession, situation d'exercice, activités, …).
- L'échange de données entre les FS et :
    - Les *Fournisseurs de Données* au niveau *Communauté Pro Santé Connect* ;
    - Les *interfaces de programmation d'application (API) Pro Santé Connectées* au niveau *Pro Santé Connect – Extension Espace de confiance.*

Depuis le 1er janvier 2023, l'implémentation de PSC est obligatoire pour les services numériques dits « sensibles » au sens défini dans la PGSSI-S[1].

PSC a fait l'objet d'une homologation au Référentiel Général de Sécurité (RGS).

PSC est un service de haute disponibilité, redondé sur plusieurs environnements. Des plans de continuité d'activité et de reprise d'activité à forts niveaux d'exigences sont définis.

1.2 Définitions

API Pro Santé Connectée

La notion d'*API Pro Santé Connectée*, mentionnée dans le présent référentiel, désigne une interface de programmation d'application, fournie par un *Fournisseur de Données* au sens de l'*Espace De Confiance PSC* (EDC), qui se réfère au *Cadre d'Interopérabilité des Systèmes d'Information de Santé* (CI-SIS) Volet Transport et qui doit être conforme aux spécifications de PSC.

Communauté Pro Santé Connect (Communauté PSC)

La *Communauté PSC* désigne l'ensemble des *Fournisseurs de Services* qui utilisent Pro Santé Connect pour l'authentification de leurs *Utilisateurs*.

Éditeur de Logiciel Proxy e-Santé

Désigne toute personne morale immatriculée dans l'Union européenne, qui conçoit, développe, distribue et assure le support et la maintenance d'un logiciel proxy de l'*Espace de Confiance PSC*, constitué uniquement du serveur intermédiaire *Proxy e-Santé*, destiné à être utilisé par un *OpS Proxy*.

[1] https://esante.gouv.fr/offres-services/pgssi-s/espace-de-publication

Éditeur de Logiciel Utilisateur

L'*Éditeur de Logiciel Utilisateur* désigne toute personne morale immatriculée dans l'Union européenne, qui conçoit, développe, distribue et assure le support et la maintenance d'un logiciel, habilité à utiliser PSC, destiné à être utilisé par un *OpS Utilisateur*.

Fournisseur de Données (FD)

Le *Fournisseur de Données (FD)* désigne toute personne morale immatriculée dans l'Union européenne, fournissant à des *Fournisseurs de Service*, via un mécanisme impliquant PSC, des données ou services supplémentaires à celles du jeton d'authentification au standard OAuth 2.0 fourni par PSC, conformément aux Conditions Générales d'Utilisation PSC.

Fournisseur de Service (FS)

Le *Fournisseur de Service* désigne toute personne morale immatriculée dans l'Union européenne, fournissant un Service Numérique et habilitée à utiliser PSC conformément aux Conditions Générales d'Utilisation PSC. Selon les sections du référentiel, la notion de *Fournisseur de Service* est déclinée en *Fournisseur de Données*, *Opérateur de Service Utilisateur*, *Éditeur de Logiciel Utilisateur*, *Opérateur de Service Proxy e-Santé* ou *Éditeur de Logiciel Proxy e-Santé*.

Opérateur de Service Proxy e-Santé (OpS Proxy)

Le *Opérateur de Service Proxy* désigne toute personne morale immatriculé dans l'Union européenne, fournissant en production un *Service Numérique* constitué uniquement du serveur intermédiaire *Proxy e-Santé*, à destination de l'*OpS Utilisateur*.

Opérateur de Service Utilisateur (OpS Utilisateur)

Le *Opérateur de Service Utilisateur* (OpS Utilisateur) désigne toute personne morale immatriculée dans l'Union européenne, fournissant un Service Numérique dans un environnement de production à des Utilisateurs et habilitée à utiliser PSC conformément aux Conditions Générales d'Utilisation PSC.

Proxy

La notion de Proxy, mentionnée dans le présent document, se réfère à la définition du CI-SIS Volet Transport. Les composants nommés « proxy » dans le présent référentiel sont des intermédiaires fonctionnels et techniques permettant le dialogue entre les services numériques et les *API Pro Santé Connectées* en garantissant par leur rôle, un niveau de sécurité conforme à la PGSSI-S dans le cadre de l'utilisation de Pro Santé Connect. Ils peuvent être intégrés aux serveurs applicatifs, être mutualisés et/ou externalisés entre plusieurs applicatifs voire plusieurs éditeurs.

Proxy e-Santé

Par *Proxy e-Santé* est désigné tout service de type Proxy ayant adhéré au niveau *Pro Santé Connect – Extension Espace de Confiance*. Ce serveur intermédiaire, ne disposant pas d'interface *Utilisateur*, est destiné à sécuriser les échanges de données entre l'*OpS Utilisateur*, ayant permis l'authentification de l'*Utilisateur* par PSC et l'*API Pro Santé Connectée*.

Proxy PSC

Par *Proxy PSC* est désigné tout Proxy ayant adhéré uniquement au niveau *Communauté Pro Santé Connect*.

Un *Proxy PSC* n'est pas habilité à fournir des jetons PSC à un composant de l'EDC contrairement à un *Proxy e-Santé*.

Service Numérique

Le *Service Numérique* désigne un service proposé par un *Opérateur de Service Utilisateur* et nécessitant l'authentification en ligne des *Utilisateurs*.

Utilisateur

L'*Utilisateur* désigne un professionnel des secteurs sanitaire, médico-social et social enregistré au répertoire santé qui s'authentifie avec *Pro Santé Connect* pour accéder au(x) *Service(s) Numérique(s)*.

1.3 Espace de Confiance Pro Santé Connect

L'Espace de Confiance (EDC) est un environnement dédié aux *Services Numériques* conformes au CI-SIS Volet Transport[2] permettant aux utilisateurs d'accéder à l'ensemble des *Services Numériques* nécessaires à l'exercice de leur activité, de façon fluide et sécurisée.

Au sein de *l'Espace de Confiance* PSC, un *Service Numérique* peut se connecter, par *API Pro Santé Connectée***,** à l'ensemble des autres services numériques de l'EDC, dans le cadre d'une relation de confiance entre ses différents acteurs afin, notamment, de garantir les niveaux de sécurité attendus.

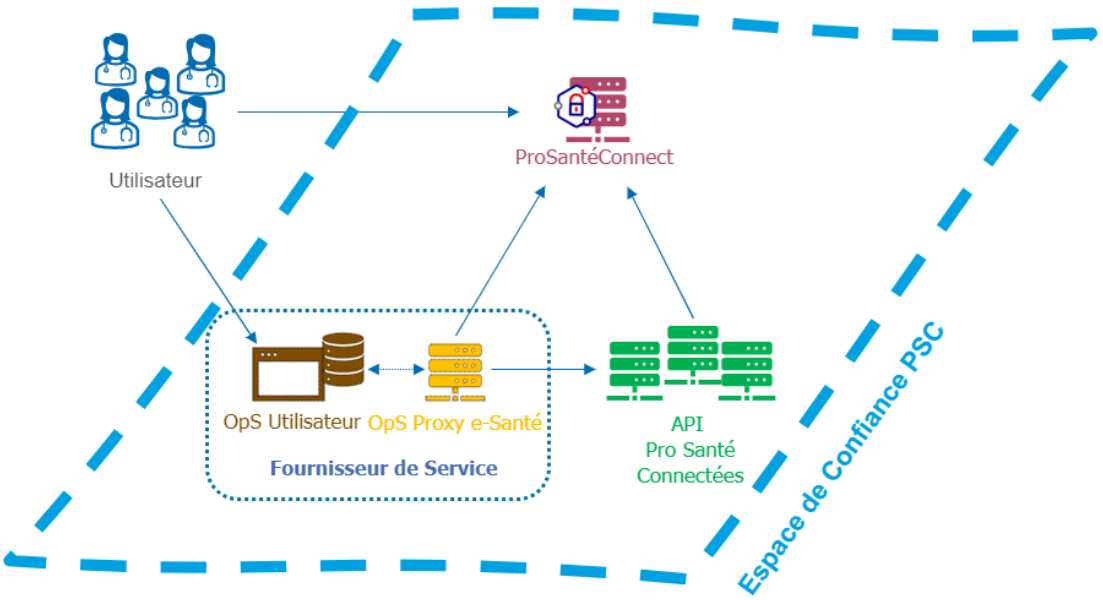

Figure 1 - Schématisation de l'Espace de Confiance

NB : l'environnement technique de l'utilisateur, incluant le navigateur, le système d'exploitation et les composants réseau lui permettant de contacter l'*Opérateur de Service Utilisateur*, sont considérés comme ne faisant pas partie de l'*Espace de Confiance*.

[2] https://esante.gouv.fr/services/referentiels/ci-sis/espace-publication/couche-transport

1.4 Destinataires et niveaux du référentiel

Ce référentiel décrit l'ensemble des exigences et recommandations qui doivent être respectées par les *Fournisseurs de Services* (FS) qui souhaitent implémenter PSC, d'une part comme fournisseur d'identité, d'autre part pour implémenter l'appel à une *API Pro Santé Connectée*.

La partie "*Référentiel Communauté PSC*" décrit les exigences qui s'appliquent aux *Fournisseurs de Services* qui souhaitent implémenter PSC comme fournisseur d'identité. Dans cette partie, la notion de *Fournisseur de Service* utilisée dans la rédaction des exigences regroupe :

- L'*Opérateur de Service Utilisateur* (*OpS Utilisateur*) ;
- Le *Fournisseur de Données* (FD).

L'applicabilité ou "portée" de l'exigence à l'égard de ces deux types d'acteurs est précisée en regard de chaque exigence.

La partie "*Référentiel Extension Espace de Confiance*" décrit les exigences supplémentaires qui s'appliquent aux *Fournisseurs de Services* qui souhaitent faire appel à une *API Pro Santé Connectée*. Dans cette partie, la notion de *Fournisseur de Service* utilisée dans la rédaction des exigences regroupe :

- *L'Opérateur de Service Utilisateur (OpS Utilisateur) ;*
- *L'Éditeur de Logiciel Utilisateur ;*
- *L'Opérateur de Service Proxy e-Santé (OpS Proxy e-santé) ;*
- *L'Éditeur de Logiciel Proxy e-Santé.*

L'applicabilité ou "portée" de l'exigence à l'égard de ces quatre types d'acteurs est précisée en regard de chaque exigence.

Lors de leur raccordement à PSC, les FS doivent indiquer à quel niveau du référentiel ils souhaitent adhérer :

Référentiel Communauté PSC	Le niveau *Communauté PSC* est le niveau minimum obligatoire. Il est destiné à l'ensemble des FS souhaitant implémenter PSC en tant que Fournisseur d'Identité, lui déléguant ainsi l'identification et l'authentification de leurs *Utilisateurs*. L'atteinte de ce niveau nécessite de répondre aux exigences du référentiel *Communauté PSC* permettant le bon fonctionnement de PSC. Le niveau communauté ne requière pas d'habilitation. Le FS doit réaliser des tests et valider le raccordement de sa solution à PSC sur le Bac à Sable.
Référentiel Extension Espace de confiance PSC	Le niveau *Extension Espace de Confiance PSC* est une extension du niveau *Communauté PSC*. Il est destiné aux FS souhaitant partager des données dans le cadre de l'appel aux *API Pro Santé Connectées*. L'atteinte de ce niveau nécessite de répondre aux exigences des 2 niveaux du référentiel : *Communauté PSC* et *Extension Espace de Confiance PSC*. Le niveau *Espace de Confiance* requière une habilitation dont les modalités sont expliquées dans les sections suivantes.

Les documents relatifs à PSC sont, par ordre de priorité décroissant :

- Le présent référentiel, incluant les sections « *Référentiel Communauté PSC* » et « *Référentiel Extension Espace de confiance PSC* » ;
- Les Conditions Générales d'Utilisation de *Pro Santé Connect*.

La numérotation des exigences du présent référentiel est faite de manière à garantir l'absence de renumérotation. Ainsi, en cas de publication d'une nouvelle version du référentiel et de l'ajout de nouvelles exigences, ces dernières seront numérotées de manière incrémentale par rapport aux exigences préexistantes.

1.5 Documentation et liens utiles

Documentation juridique	Article L.1470-3 du code de la santé publique : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043497483?init=true&page=1&query=Article+L.1470-3+&searchField=ALL&tab_selection=all Règlement eIDAS : https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/
Plateforme API.Gouv	https://www.data.gouv.fr/fr/dataservices/api-pro-sante-connect/
Référentiels PGSSI-S sur l'identification électronique	https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
Référentiel d'interopérabilité	https://esante.gouv.fr/services/referentiels/ci-sis/espace-publication/couche-transport
MOS-NOS	https://esante.gouv.fr/interoperabilite/mos-nos
Plateforme IGC-Santé	https://pfc.eservices.esante.gouv.fr/
Documentation technique de PSC	https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/documentation-technique
Conditions Générales d'Utilisation de PSC	https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/conditions-generale-d-utilisation-pro-sante-connect
Charte graphique de PSC	https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/charte-graphique-pro-sante-connect
Services raccordés à PSC	https://esante.gouv.fr/securite/e-cps/services-raccordes-a-pro-sante-connect
OpenID	https://openid.net/connect/
Implémentations OIDC	https://openid.net/developers/certified/
Client-Initiated Backchannel Authentication	https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1_0.html
CI-SIS Volet Transport	https://esante.gouv.fr/services/referentiels/ci-sis/espace-publication/couche-transport
Documents de conformité	Lien à venir + autres docs de référence (niveaux de contrôle, TI …)
Norme JWS	https://datatracker.ietf.org/doc/html/draft-ietf-jose-json-web-signature

RFC 8705	https://www.rfc-editor.org/rfc/rfc8705

2 HABILITATIONS A L'ESPACE DE CONFIANCE

L'habilitation des différents types d'acteurs dans l'EDC présente des caractéristiques différentes quant aux conditions et à l'environnement dans lequel la vérification des exigences est effectuée. De plus, une chaîne d'habilitation doit être respectée, puisque l'habilitation d'un type d'acteur peut dépendre de l'habilitation préalable d'un autre, étant entendu que, selon les configurations, chaque type d'acteur peut être constitué par une même personne morale ou par des personnes morales distinctes, disposant entre elles des accords contractuels adéquats.

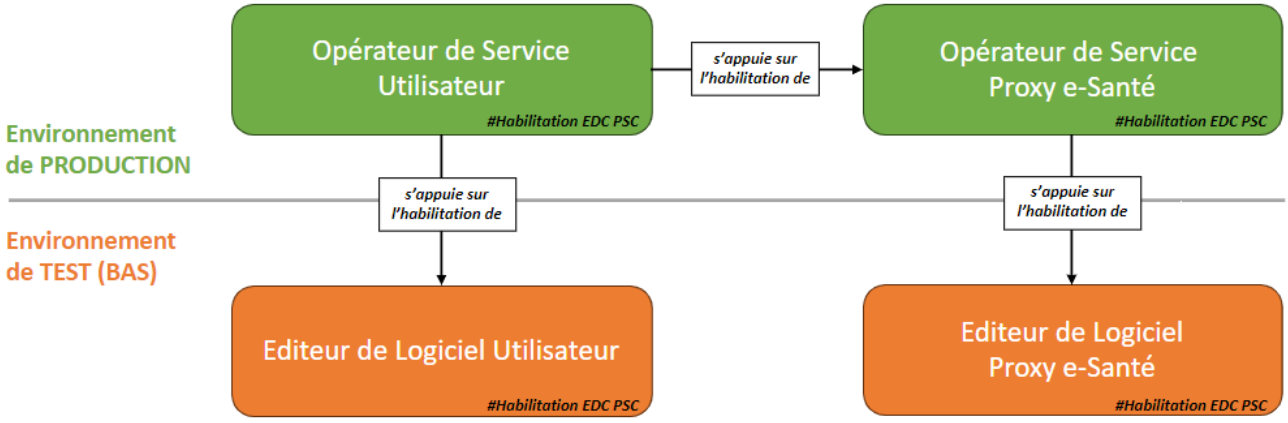

Figure 2 - Schématisation de la chaîne d'habilitation

2.1 Conditions d'habilitation

Le tableau ci-après présente les conditions de vérification des exigences qui s'appliquent à chaque type d'acteur ainsi que les dépendances entre eux du point de vue de ce référentiel.

Type d'acteur	Conditions de vérification des exigences	Dépendances
Éditeur de logiciel Utilisateur	L'habilitation à l'EDC de l'*Éditeur de Logiciel Utilisateur* repose sur la vérification par l'ANS, ou un tiers désigné par cette dernière, de la conformité du logiciel concerné au regard des exigences du référentiel identifiées comme lui étant applicables dans un l'environnement Bac à Sable (BAS) de PSC, le plus proche possible des conditions de production des *OpS Utilisateur* utilisant le logiciel. L'*Éditeur de Logiciel Utilisateur* doit : • Être conforme aux référentiels PSC sur le périmètre de son habilitation en tant qu'*Éditeur de Logiciel Utilisateur* ; • Fournir des directives à l'*OpS Utilisateur* pour lui permettre d'être conforme aux référentiels PSC, notamment en fournissant un document de conformité (EXI EDC PSC 102) ; • S'engager à ce que son logiciel utilisateur permette à l'*OpS Utilisateur* d'être conforme aux référentiels PSC, lorsque l'*OpS Utilisateur* suit ses directives.	Aucune.
Éditeur de logiciel Proxy e-Santé	L'habilitation à l'EDC de *l'Éditeur de Logiciel Proxy e-Santé* repose sur la vérification par l'ANS, ou un tiers désigné par	Aucune.

	cette dernière, de la conformité du logiciel concerné au regard des exigences du référentiel identifiées comme lui étant applicables dans un l'environnement Bac à Sable (BAS) de PSC, le plus proche possible des conditions de production des OpS *Proxy e-Santé* utilisant le logiciel. L'*Éditeur de Logiciel Proxy e-santé* doit : • Être conforme aux référentiels PSC sur le périmètre de son habilitation en tant qu'*Éditeur de Logiciel Proxy e-santé* ; • Fournir des directives à l'*OpS Proxy e-Santé* pour lui permettre d'être conforme aux référentiels PSC, notamment en fournissant un document de conformité (EXI EDC PSC 102) ; • S'engager à ce que son logiciel proxy permette à l'*OpS Proxy e-Santé* d'être conforme aux référentiels PSC, lorsque l'*OpS Proxy e-Santé* suit ses directives.	
OpS Utilisateur	L'habilitation à l'EDC de l'OpS *Utilisateur* repose sur la vérification par l'ANS, ou un tiers désigné par cette dernière, de la conformité du service aux exigences applicables à l'*Ops Utilisateur*. L'*OpS Utilisateur* pourra être audité, après son entrée dans l'*Espace de Confiance*, afin de vérifier le respect des exigences dans l'environnement de production du service. Dans le cadre d'un audit, les exigences vérifiées intègrent les exigences applicables à l'*OpS Utilisateur*, à *l'Éditeur de Logiciel Utilisateur* et à l'*OpS Proxy e-santé*. L'*OpS Utilisateur*, dès la mise en production doit : • Être conforme aux référentiels PSC sur le périmètre de son habilitation en tant qu'*OpS Utilisateur*, s'appuyant sur la conformité aux exigences applicables à l'*Éditeur de Logiciel Utilisateur* et à l'*OpS Proxy e-santé* ; • Demander et suivre les directives de l'*Éditeur de Logiciel Utilisateur* et de l'*OpS Proxy e-Santé*, notamment en respectant le document de conformité fournis par l'*Éditeur de Logiciel Utilisateur* et l'*OpS Proxy e-Santé* (EXI EDC PSC 102).	Communication obligatoire des numéros d'habilitation de l'EDC de l'*Éditeur de logiciel Utilisateur et* de l'*OpS Proxy e-santé*.
OpS Proxy e-Santé	L'habilitation à l'EDC de l'*OpS Proxy e-santé* repose sur la vérification par l'ANS, ou un tiers désigné par cette dernière, de la conformité du logiciel concerné au regard des exigences du référentiel identifiées comme lui étant applicables. L'*OpS Proxy e-Santé* pourra être audité, après son entrée dans l'*Espace de Confiance*, afin de vérifier le respect des exigences dans l'environnement de production du service. Dans le cadre d'un audit, les exigences vérifiées intègrent les exigences applicables à l'*OpS Proxy e-Santé* et à l'*Éditeur de Logiciel Proxy e-Santé*. L'*OpS Proxy e-Santé,* dès la mise en production doit : • Être conforme aux référentiels PSC sur le périmètre de son habilitation en tant qu'*OpS Proxy,* s'appuyant sur la	Communication obligatoire du numéro d'habilitation de l'EDC de *l'Éditeur de logiciel Proxy e-Santé* pour le(s) logiciel(s) concerné(s).

	conformité aux exigences applicables à l'*Éditeur de Logiciel Proxy e-santé ;* • Fournir des directives à l'*OpS Utilisateur* pour lui permettre d'être conforme aux référentiels PSC, notamment en fournissant un document de conformité (EXI EDC PSC 102) ; • Demander et suivre les directives de l'*Éditeur de Logiciel Proxy e-santé*, notamment en respectant le document de conformité fournis par l'*Éditeur de Logiciel Proxy e-santé* (EXI EDC PSC 102).	

2.2 Audits

Dans le cadre des dispositifs de vérification de conformité prévus par le référentiel *Extension Espace de Confiance PSC*, des audits des FS seront réalisés à la discrétion de l'ANS.

Conséquences d'une non-conformité :

L'accès à PSC d'un *OpS Utilisateur* peut être désactivé, si la non-conformité est due au non-respect des exigences qui lui sont applicables et/ou des directives des acteurs sur lesquels s'appuie son habilitation lors de la mise en production du service (*Éditeur de Logiciel Utilisateur* et/ou *OpS Proxy e-Santé* selon les cas).

L'accès à PSC d'un *OpS Proxy e-Santé* peut être désactivé, si la non-conformité est due au non-respect des exigences qui lui sont applicables et/ou des directives des acteurs sur lesquels s'appuie son habilitation lors de la mise en production du service (*Éditeur de Logiciel Proxy e-Santé*), et/ou s'il n'a pas fourni de directives permettant à un *OpS Utilisateur* d'être conforme au référentiel. La désactivation de l'accès à PSC d'un *OpS Proxy* peut entrainer de fait la désactivation des accès des *OpS Utilisateur* qui s'appuient sur son habilitation.

L'accès à PSC d'un *Éditeur de Logiciel Utilisateur,* resp. *Éditeurs de Logiciel Proxy e-Santé*, peut être désactivé si la non-conformité est dû au non-respect des exigences qui lui sont applicables et/ou s'il n'a pas fourni de directives permettant à un *OpS Utilisateur,* resp. *OpS Proxy e-Santé* d'être conforme au référentiel.

La désactivation de l'accès à PSC d'un *Éditeur de Logiciel Utilisateur* peut entrainer de fait la désactivation des accès des *OpS Utilisateur* qui s'appuient sur son habilitation.

La désactivation de l'accès à PSC d'un *Éditeur de Logiciel Proxy e-Santé* peut entrainer de fait la désactivation des accès des *OpS Proxy e-Santé* et des *OpS Utilisateur* qui s'appuient directement ou indirectement sur son habilitation.

Lorsqu'un *FS* fait appel à un sous-traitant pour la fourniture de tout ou partie sa solution, la relation entre ces acteurs doit être encadrée contractuellement afin de déterminer le partage de responsabilité et les obligations de chacune des parties en regard du présent référentiel.

Mise en demeure et notification en cas de désactivation de l'accès à PSC :

La désactivation de l'accès à PSC par l'ANS peut intervenir après un délai d'un mois à compter de la réception, d'une mise en demeure préalable de se mettre en conformité avec le référentiel. La mise en demeure précise les non-conformités constatées ainsi que le délai dont ils disposent pour se mettre en conformité.

Une fois notifié, le FS concerné peut adresser à l'ANS une demande, qui doit être justifiée, de délai supplémentaire. L'ANS, après évaluation du risque, notifie sa décision d'acceptation ou de refus de délai supplémentaire.

L'ANS se réserve le droit de désactiver l'accès à PSC, sans délai après l'envoi d'une notification, dès la constatation d'une défaillance de sécurité d'une gravité majeure issue d'une utilisation frauduleuse de PSC, et ce, pour faire cesser tout trouble perturbant gravement son bon fonctionnement et sa sécurité.

Dans ce cas la réactivation de l'accès à PSC ne pourra être réouvert qu'avec l'accord de l'ANS après instruction des mesures mises en place par le FS concerné.

3 REFERENTIEL COMMUNAUTE PSC

PORTEE	La présence d'un acteur dans l'encadré indique qu'il a une responsabilité et qu'il doit respecter l'exigence.	
Opérateur de Service Utilisateur		**Fournisseur de Données**
EXI PSC XXX	L'ensemble des exigences sont identifiables par un encadré gris.	

Opérateur de Service Utilisateur		**Fournisseur de Données**
RECO PSC XXX	L'ensemble des recommandations sont identifiables par un encadré blanc	

3.1 Portée des exigences et recommandations du référentiel

Le tableau ci-dessous, établi par l'ANS, définit les périmètres des exigences à respecter par les différents acteurs visés dans le présent référentiel.

Pour chaque colonne du tableau, lorsqu'une case est remplie par la mention « OUI », cela implique que l'acteur doit traiter, gérer et assurer le suivi de l'exigence associée. Dans le cas contraire, si l'acteur n'est pas concerné par une exigence, sa case correspondante sera complétée par la mention « NON ».

Communauté PSC		
EXIGENCE	**OpS Utilisateur**	**FD**
EXI PSC 01	OUI	OUI
EXI PSC 02	OUI	OUI
EXI PSC 03	OUI	NON
EXI PSC 04	OUI	OUI
EXI PSC 05	OUI	OUI
EXI PSC 06	OUI	OUI
EXI PSC 07	OUI	OUI
EXI PSC 08	OUI	OUI
EXI PSC 09	OUI	OUI
EXI PSC 10	OUI	OUI
EXI PSC 11	OUI	NON
EXI PSC 12	OUI	OUI
EXI PSC 13	OUI	OUI
EXI PSC 14	OUI	OUI
EXI PSC 15	OUI	OUI
EXI PSC 16	OUI	OUI
EXI PSC 17	OUI	OUI
EXI PSC 18	OUI	NON

Communauté PSC		
EXIGENCE	**OpS Utilisateur**	**FD**
EXI PSC 19	OUI	NON
EXI PSC 20	OUI	NON
EXI PSC 21	OUI	OUI
EXI PSC 23	OUI	OUI
EXI PSC 24	OUI	OUI
EXI PSC 25	OUI	OUI
EXI PSC 26	OUI	OUI
EXI PSC 27	OUI	OUI
EXI PSC 28	OUI	NON
EXI PSC 29	OUI	NON
EXI PSC 30	OUI	NON
EXI PSC 31	OUI	NON
EXI PSC 32	OUI	NON
EXI PSC 33	OUI	OUI
EXI PSC 34	NON	OUI
EXI PSC 35	OUI	OUI
EXI PSC 36	OUI	OUI
EXI PSC 37	OUI	OUI
EXI PSC 44	OUI	OUI
RECO PSC 38	OUI	OUI
RECO PSC 39	OUI	OUI
RECO PSC 40	OUI	OUI
RECO PSC 41	OUI	NON
RECO PSC 42	OUI	NON
RECO PSC 43	OUI	NON

3.2 Eligibilité à PSC et procédure de candidature

Pour intégrer PSC, le FS et le service doivent satisfaire plusieurs prérequis, détaillés ci-après.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 01	Le *Fournisseur de Service* DOIT être une personne morale (entreprise, association, groupement d'intérêt économique, etc.) de droit privé ou public, immatriculée dans l'Union Européenne.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 02	Le *Fournisseur de Service* DOIT s'engager à ne pas prononcer des propos ou proposer des contenus contrevenant aux droits d'autrui ou à caractère diffamatoire, injurieux, obscène, offensant, violent ou incitant à la violence, politique, raciste ou xénophobe et de manière générale tous propos ou contenus contraires à l'objet du service, aux lois et règlements en vigueur, aux droits des personnes ou aux bonnes mœurs.

Opérateur de Service Utilisateur	
EXI PSC 03	Le service DOIT être proposé en langue française.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 04	Le service DOIT proposer à des utilisateurs intervenant dans les secteurs sanitaires, médico-social et social, des fonctionnalités qui nécessitent leur identification électronique.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 05	Le *Fournisseur de Service* DOIT respecter la loi du 6 janvier 1978, dite « Informatique et Libertés », ainsi que le Règlement Général sur la Protection des Données (RGPD) en particulier en ce qui concerne l'information des utilisateurs.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 06	Le service DOIT, lorsqu'il traite de données de santé collectées à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, assurer leur confidentialité et leur intégrité, tout en assurant leur hébergement par un hébergeur certifié Hébergeur de Données de Santé (HDS).

Pour candidater, le FS remplit un dossier, dans le cadre d'un parcours qui commence sur API.gouv.fr où il fournit plusieurs documents, en particulier :

- Un extrait KBIS de la personne morale portant le service, responsable du traitement de données du service, ou toute pièce justifiant l'identité de l'organisme demandeur et son immatriculation au niveau européen ou international ;
- Un descriptif du service, indiquant le nom du traitement de données, ses finalités, ainsi qu'une description du type d'utilisateurs par codes (nomenclatures NOS – TRE_G15, TRE_R94, TRE_R95, TRE_R291), ainsi que les modalités prévues en termes de gestion des contrôles d'accès ;
- Le nom public du service, le logo du service et un descriptif d'une ligne du service, en vue de leur mention sur les pages de l'ANS et de l'application mobile e-CPS listant l'ensemble des services habilités à intégrer

Pro Santé Connect[3] et de l'application mobile e-CPS. Cette mention est obligatoire pour implémenter le service PSC ;

- Une adresse générique du délégué à la protection des données du FS, ainsi que le nom actuel du titulaire du poste ;
- Une adresse générique du contact opérationnel pour tout besoin d'échange entre le FS et les équipes en charge de la mise en œuvre de PSC, ainsi que le nom actuel du titulaire du poste.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 07	Le *Fournisseur de Service* DOIT prévenir l'*Agence du Numérique en Santé* dans le cas où le service ne serait plus conforme à une des exigences du présent Référentiel et/ou en cas de changement dans les informations qui ont été déclarées lors de la candidature au raccordement à Pro Santé Connect.

Le FS pourra s'appuyer sur les parcours de support mis à sa disposition par l'ANS tels que les formulaires en ligne ou l'adresse électronique dédiée aux éditeurs de PSC.

En cas de modifications ayant pour impact de ne plus respecter les exigences du présent référentiel, PSC se réserve le droit de bloquer l'accès du FS à PSC.

L'ANS se réserve le droit d'auditer les FS selon les conditions énoncées dans les CGU.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 44	Le *Fournisseur de Service* DOIT s'appuyer sur les versions en vigueur de moins de trois (3) ans ou sur la dernière version publiée de chaque document et standard mentionné dans ce référentiel.

En cas de prise en compte de nouvelles versions plus à jour, une communication de l'ANS sera transmise à l'ensemble des acteurs ; un délai de prévenance sera systématiquement appliqué, sauf en cas de force majeure.

[3] https://esante.gouv.fr/securite/e-cps/services-raccordes-a-pro-sante-connect

3.3 Modalités de raccordement technique

Pour être raccordé, le FS remplit un dossier, dans le cadre d'un parcours qui commence sur API.gouv.fr où il fournit, en particulier :

- Une URL de redirection (callback endpoint) et une URL de déconnexion (logout endpoint) de test ;
- Une URL de redirection (callback endpoint) et une URL de déconnexion (logout endpoint) de production ;
- Un certificat AUTH_CLI de l'offre ORG de l'IGC-Santé.

Dans le cas où le service n'utiliserait que le protocole CIBA, les URL pourront être omises.

Le protocole OpenID Connect (OIDC)[4] est au cœur du fonctionnement de PSC. C'est une surcouche d'identification au protocole OAuth 2.0[5]. Il permet à des Clients (ici, les FS) d'accéder à l'identité des utilisateurs par l'intermédiaire d'un fédérateur de fournisseur d'identité, PSC.

Un FS est considéré comme un client OpenID Connect s'il implémente le standard OpenID. Il est préférable d'utiliser une implémentation proposée dans une librairie certifiée par la fondation OpenID plutôt que d'en développer une spécifiquement pour le service.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 08	Le *Fournisseur de Service* DOIT être client OpenID Connect.

La liste des implémentations certifiées par la fondation OpenID Connect est disponible sur le site officiel.

Opérateur de Service Utilisateur	Fournisseur de Données
RECO PSC 38	Le *Fournisseur de Service* DEVRAIT utiliser une implémentation parmi celles qui sont certifiées par la fondation OpenID Connect.

Le protocole OpenID Connect définit 3 appels REST faits par le FS, et 5 endpoints, un du côté FS, et quatre du côté PSC.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 09	Le *Fournisseur de Service* DOIT respecter les flux standards OpenID.

PSC implémente le flux standard OpenID « flux code d'autorisation ». Lorsque l'utilisateur clique sur le bouton d'authentification du FS, le flux est le suivant :

- Le FS fait une redirection vers le endpoint d'autorisation de PSC avec ses informations de raccordement à Pro Santé Connect fournies par l'*Agence du Numérique en Santé* et son url de redirection. PSC redirige alors l'utilisateur vers sa mire d'authentification. Si l'utilisateur se connecte correctement, PSC renvoie un code d'autorisation au FS.
- Le FS fait un appel vers le token endpoint du provider avec le code d'autorisation reçu, et authentifie cette requête avec ses informations de raccordement à PSC fournies par l'*Agence du Numérique en Santé*. PSC retourne un token d'accès (une chaîne de caractères encodés en base64), un token id (sous la forme d'un Json Web Token), et un token de rafraichissement (une chaîne de caractères en base64).
- Le FS fait un appel vers l'endpoint 'UserInfo' de PSC avec le token d'accès reçu, et PSC renvoie les informations de l'utilisateur au FS.

[4] https://openid.net/connect/
[5] https://oauth.net/2/

Au cours de l'année 2022, PSC a implémenté le flux OpenID "Client Initiated Backchannel Authentication" (CIBA). Lorsque l'utilisateur clique sur le bouton d'authentification du FS, le flux est le suivant :

- Le FS demande à PSC de réaliser une authentification via le endpoint CIBA avec ses informations de raccordement à PSC fournies par l'*Agence du Numérique en Santé*. PSC identifie et authentifie l'utilisateur. Si l'utilisateur s'authentifie correctement, PSC met à disposition du FS un code d'autorisation.
- Le FS demande à PSC le résultat de l'authentification et reçoit en échange le code d'autorisation mis à disposition.
- Le FS fait un appel vers le token endpoint du provider avec le code d'autorisation reçu, et authentifie cette requête avec ses informations de raccordement à PSC fournies par l'*Agence du Numérique en Santé*. PSC retourne un token d'accès (une chaîne de caractères encodés en base64), un token id (sous la forme d'un Json Web Token), et un token de rafraichissement (une chaîne de caractères en base64).
- Le FS fait un appel vers l'endpoint 'UserInfo' de PSC avec le token d'accès reçu, et PSC renvoie les informations de l'utilisateur au FS.

Opérateur de Service Utilisateur	**Fournisseur de Données**
EXI PSC 10	Le *Fournisseur de Service* DOIT utiliser les flux OpenID définis par Pro Santé Connect.

Dans le cadre de la gestion de session PSC il est offert au FS la possibilité de rafraichir son jeton d'accès grâce au endpoint refresh, conformément à la norme OpenID, afin de maintenir la validité du jeton d'accès pendant toute la période où l'utilisateur est actif sur le service.

Opérateur de Service Utilisateur	
EXI PSC 11	Le *Fournisseur de Service* DOIT rafraîchir périodiquement les informations d'authentification auprès de Pro Santé Connect uniquement lorsque l'utilisateur utilise activement son service.

3.4 Bac à Sable

Les tests sur l'environnement PSC dit « Bac à Sable » permettent de valider le bon déroulé de la cinématique d'authentification à l'aide d'identités de test basée sur le flux standard OpenID.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 12	Le *Fournisseur de Service* DOIT avoir testé avec succès son service avec les endpoints de Pro Santé Connect Bac à Sable, préalablement à toute connexion à la production.

La vérification de cette exigence conditionne la délivrance des éléments nécessaires à l'accès à PSC Production.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 13	Le *Fournisseur de Service* DOIT donner accès à l'*Agence du Numérique en Santé* à son service de test.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 37	Le *Fournisseur de Service* DOIT uniquement utiliser des jeux de données de test, en opposition avec des données réelles, dans le cadre de ses travaux sur un environnement de test.

Il est entendu qu'aucune donnée réelle, notamment d'identité professionnelle et de santé, ne doit figurer dans les jeux de test.

3.5 Production

Sur l'environnement de Production, la cinématique d'authentification doit également respecter le flux standard OpenID.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 14	Le *Fournisseur de Service* DOIT contacter les endpoints de Pro Santé Connect Production

3.6 Paramétrage des requêtes

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 15	Le *Fournisseur de Service* DOIT paramétrer ses requêtes de token (token ID, token d'accès, token UserInfo) suivant le standard OpenID.

Comme la norme ne prévoit pas aujourd'hui de mesures techniques particulières pour préciser le niveau d'authentification souhaité, PSC utilise le claim optionnel « acr »[6] de la norme OpenID Connect. Pour le FS, cela veut dire remplir acr_values lors de la demande d'authentification.

Au sujet de acr_values, on notera que c'est, selon la norme, un « voluntary claim » qui théoriquement traduit une préférence et non une exigence. Cependant, ce champ est nécessaire à l'utilisation de PSC.

Actuellement, PSC n'accepte que « eidas1 ».

Dans le cadre d'évolution future, il est envisagé que PSC acceptera aussi « eidas2 ». Actuellement, PSC est conforme à la réglementation en vigueur (référentiel PGSSI-S sur l'identification électronique des acteurs de santé personnes physiques).

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 16	Le *Fournisseur de Service* DOIT utiliser le paramètre acr_values lors de la demande d'authentification avec la valeur « eidas1 ».

L'identité de l'utilisateur, fournie dans l'ensemble des scopes retournant le SubjectNameID, est issue du répertoire sectoriel de référence RPPS. Chaque utilisateur y est enregistré avec un identifiant national unique, l'idNat_PS[7], qui sera bientôt quasi exclusivement sous le format chiffre 8 + N° RPPS. Le numéro RPPS est un identifiant pérenne, constitué de 11 caractères non significatifs (numéro d'ordre sur 10 caractères + clé de Luhn sur 1 caractère).

L'ensemble des scopes retournant le SubjectNameID sont référencés dans la documentation technique de PSC[8].

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 17	Le *Fournisseur de Service* DOIT paramétrer ses requêtes d'autorisation avec le scope « openid » et l'un des scopes retournant le SubjectNameID.

Si un FS envoie une valeur de scope autre que les scopes attendus, PSC retournera un message d'erreur.

[6] https://openid.net/specs/openid-connect-basic-1_0.html#RequestParameters
[7] https://mos.esante.gouv.fr/2.html#_8f7f21e6-0c8e-44f4-b77d-35c58b2e12cf
[8] https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/documentation-technique

3.7 Utilisation des données du jeton

Opérateur de Service Utilisateur	
EXI PSC 18	Le *Fournisseur de Service* DOIT utiliser le champ SubjectNameID pour récupérer l'identifiant unique de l'identité, et référencer cet identifiant dans sa traçabilité interne.

PSC propose un service d'identification électronique des utilisateurs. Il ne constitue pas un fournisseur d'autorisations d'accès à tel ou tel service, ou telles ou telles données.

Il appartient à chaque FS, sous sa propre responsabilité, de mettre en place des contrôles d'accès pour ses utilisateurs. Ces derniers peuvent par exemple être gérés par des administrateurs locaux ou les personnes directement concernées par les données (patients, professionnels, etc.). Ils peuvent également être automatisés sur la base d'attributs de l'identité sectorielle (profession, savoir-faire, situation d'exercice, …) fournis par PSC.

Opérateur de Service Utilisateur	Fournisseur de Données
RECO PSC 39	Le *Fournisseur de Service* DEVRAIT mettre en place un contrôle d'accès sur des attributs de l'identification électronique (profession, secteur d'activité, etc.) issus du jeton Pro Santé Connect

À toutes fins utiles, il est fréquent que des services utilisent la profession ou le rôle professionnel (nomenclatures NOS – TRE_G15, TRE_R94, TRE_R95, TRE_R291) ou d'autres éléments de la nomenclature MOS-NOS[9] utilisée par l'ANS et véhiculée dans le scope_all.

Pour gérer les cas de mésusages éventuels, il est fortement recommandé que le service mette en œuvre un mécanisme de blocage des utilisateurs malveillants.

Opérateur de Service Utilisateur	Fournisseur de Données
RECO PSC 40	Le *Fournisseur de Service* DEVRAIT mettre en place un mécanisme de blocage des utilisateurs malveillants.

L'appel au endpoint d'introspection nécessite la présentation par le FS d'un jeton d'accès dès sa réception.

	Fournisseur de Données
EXI PSC 34	Lorsque le *Fournisseur de Service* reçoit un jeton Pro Santé Connect dont il n'est pas à l'origine de la demande d'authentification, il DOIT en vérifier la validité par un appel au endpoint d'introspection dès sa réception.

[9] https://mos.esante.gouv.fr/

3.8 Gestion et fusion des comptes avec d'autres systèmes d'authentification électronique

Un FS dispose généralement de systèmes d'identification électroniques préexistants et/ou complémentaires à PSC. Il peut les maintenir s'ils sont conformes aux référentiels sur l'identification électroniques. La fusion des comptes doit alors être effectuée.

Opérateur de Service Utilisateur	
RECO PSC 41	Le *Fournisseur de Service* DEVRAIT utiliser d'autres systèmes d'identification électronique que Pro Santé Connect, notamment pour permettre à des utilisateurs non encore enregistrés au Répertoire Partagé des Professionnels de Santé (RPPS) d'accéder au service, et/ou de pallier des indisponibilités de Pro Santé Connect ou de connexion réseau.

Opérateur de Service Utilisateur	
EXI PSC 19	Le *Fournisseur de Service* DOIT alors fusionner ses comptes autour de l'identifiant pivot Répertoire Partagé des Professionnels de Santé (RPPS), afin de permettre à ses utilisateurs de ne garder qu'un seul compte dans l'outil, quel que soit leur modalité de connexion.

Opérateur de Service Utilisateur	
RECO PSC 42	Pour les cas où le compte utilisateur ne disposaient pas auparavant du numéro RPPS enregistré, le *Fournisseur de Service* DEVRAIT demander à l'utilisateur de se connecter d'abord avec Pro Santé Connect, puis avec une des autres modalités de connexion disponibles afin d'effectuer l'appariement autour de l'identifiant pivot Répertoire Partagé des Professionnels de Santé (RPPS).

3.9 Déconnexion

Déconnexions par l'utilisateur au service et à PSC

PSC implémente la section sur la déconnexion en cours de spécification dans la norme OpenID Connect[10]. En flux code d'autorisation, la cinématique globale est la suivante :

1. L'utilisateur clique sur un lien de déconnexion présenté par le FS ;
2. Le FS doit déconnecter l'utilisateur de son application et de sa session PSC, en utilisant l'URL de déconnexion dédiée ;
3. L'utilisateur est redirigé vers la page de retour du FS.

Opérateur de Service Utilisateur	
EXI PSC 20	Le *Fournisseur de Service* DOIT offrir à l'utilisateur la possibilité de se déconnecter, quel que soit le moyen de connexion utilisé au préalable. S'il s'agit de Pro Santé Connect, le *Fournisseur de Service* doit déconnecter l'utilisateur à la fois du service et de Pro Santé Connect.

Par ailleurs, PSC ne gère pas la déconnexion de l'utilisateur au service PSC à la fermeture du navigateur tant qu'une session est active.

De son côté, le FS peut avoir un mécanisme pour détecter cette fermeture du navigateur. Dans ce cas, il ne doit pas propager cette déconnexion à PSC au cas où l'utilisateur utiliserait d'autres services, par exemple dans d'autres navigateurs, sur cette même session.

Opérateur de Service Utilisateur	
RECO PSC 43	Le *Fournisseur de Service* DEVRAIT déconnecter l'utilisateur du service à la fermeture du navigateur ou du client lourd, sans clôturer la session propre à Pro Santé Connect.

Déconnexion automatique de l'utilisateur du service et de PSC

PSC dispose d'un mécanisme de déconnexion automatique de la session PSC au bout d'une certaine durée sans rafraîchissement de la part du ou des FS de cette session[11].

Par ailleurs, le FS doit avoir un mécanisme similaire, sans néanmoins propager cette déconnexion à PSC au cas où l'utilisateur utiliserait d'autres services, par exemple dans d'autres onglets, sur cette même session.

Opérateur de Service Utilisateur	
EXI PSC 32	Le *Fournisseur de Service* DOIT déconnecter l'utilisateur automatiquement de son service après une période d'inactivité, sans clôturer la session propre à Pro Santé Connect.

3.10 Sécurité

Après approbation d'une demande de raccordement par PSC, les différentes informations du FS afin qu'il puisse communiquer avec PSC sont :

- Un client ID, information fournie par l'ANS ;
- Un Secret, information sensible qui peut être fournie par l'ANS ;
- Un certificat AUTH_CLI déclaré par le FS à l'ANS et une clé privée information sensible détenue par le FS seul.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 21	Le *Fournisseur de Service* DOIT utiliser les informations client ID et Secret fournis par Pro Santé Connect.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 35	Le *Fournisseur de Service* DOIT être en mesure de fournir son certificat AUTH_CLI de l'offre ORG de l'IGC-Santé à l'*Agence du Numérique en Santé*.

Afin d'assurer la sécurité des informations de raccordement précédemment citées, elles ne doivent jamais être conservées sur l'appareil de l'utilisateur.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 36	Le *Fournisseur de Service* DOIT conserver les informations sensibles fournies par l'*Agence du Numérique en Santé* au niveau d'un serveur.

Quel que soit la solution implémentée par l'industriel, PSC ne sera en contact qu'avec un seul serveur, jamais avec un client local.

[10] http://openid.net/specs/openid-connect-session-1_0.html#RPLogout
[11] https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/documentation-technique

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 23	Le *Fournisseur de Service* DOIT proposer un unique point de contact à Pro Santé Connect.

Les paramètres de sécurité de la protection des flux entre le FS et PSC suivent les préconisations de l'ANSSI : TLS1.2 au minimum, et nécessite l'obtention d'un certificat de AUTH_CLI de l'offre ORG de l'IGC-Santé[12]. Un certificat de l'IGC-Santé peut être obtenu en utilisant la Plateforme IGC-Santé (https://pfc.eservices.esante.gouv.fr/).

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 24	Le *Fournisseur de Service* DOIT communiquer avec Pro Santé Connect via une connexion sécurisée au minimum via TLS 1.2 par un certificat AUTH_CLI de l'offre ORG de l'IGC-Santé.

Dans la suite du document, un 'client lourd' est défini comme une application native ne s'appuyant pas sur un navigateur internet de l'appareil de l'utilisateur. A titre d'exemple, les applications installées sur l'appareil de l'utilisateur ou les applications mobiles déployées par les magasins logiciels des systèmes d'exploitation sont considérées, dans le cadre de référentiel *Communauté PSC* comme des clients lourds.

PSC permet aux FS client lourds de se raccorder en flux de redirection web ou en flux CIBA.

L'utilisation de composants de visualisation du navigateur web intégrés nativement dans une application (e.g. « webviews ») n'est pas suffisamment sécurisée, en raison de :

- L'absence de visibilité sur la maintenance des noyaux concernés ;
- La nécessité d'une mise à jour immédiate du parc complet des clients lourds concernés en cas de faille de sécurité du ou des noyaux concernés ;
- L'absence de visibilité sur un réel blocage opérationnel des clients lourds non suivis par une maintenance de sécurité.

Il est admis que l'utilisation de navigateurs grand public induit :

- Une visibilité sur la maintenance des noyaux concernées, grâce à une publication officielle et publique ;
- Des mises à jour automatiques configurées par défaut ;
- Une politique d'obsolescence des anciennes versions, publique et appliquée.

Une tolérance pourra être accordée aux solutions ayant une base applicative hybride, intégrant une application proposant un navigateur ayant les qualités de ceux du grand public.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 25	Le *Fournisseur de Service* de type client lourd DOIT utiliser une autre méthode que l'intégration native d'un composant navigateur à l'intérieur de son applicatif pour le déroulé de la cinématique de connexion Pro Santé Connect.

Le FS pourra ouvrir un navigateur extérieur et implémenter un mécanisme d'échange entre le serveur et son service client lourd.

Opérateur de Service Utilisateur	Fournisseur de Données
EXI PSC 26	Le *Fournisseur de Service* de type client lourd DOIT utiliser un navigateur extérieur à son application pour la cinématique « flux code d'autorisation » de Pro Santé Connect.

L'ANS se laisse le droit de faire évoluer les modalités techniques du service PSC, notamment vis à vis d'améliorations de sécurité liées aux préconisations de la PGSSI-S[13].

[12] https://industriels.esante.gouv.fr/produits-et-services/igc-sante-certificats-personnes-morales-et-serveurs
[13] https://esante.gouv.fr/offres-services/pgssi-s/espace-de-publication

Opérateur de Service Utilisateur		Fournisseur de Données
EXI PSC 33	Le *Fournisseur de Service* DOIT se maintenir conforme aux préconisations sécuritaires du service Pro Santé Connect prononcées et signifiées par l'*Agence du Numérique en Santé* auprès du responsable technique du *Fournisseur de Service*.	

L'ANS publiera les préconisations sécuritaires du service PSC sur son site institutionnel dans les sections destinées aux industriels intégrant PSC. De plus, l'ANS communiquera directement aux contacts fournis lors du raccordement en cas de modifications critiques de ces préconisations.

Par ailleurs, en cas d'incident de sécurité sur son service, en particulier si cet incident a un lien avec PSC, le FS doit le signaler à l'ANS.

Opérateur de Service Utilisateur		Fournisseur de Données
EXI PSC 27	Le *Fournisseur de Service* DOIT prévenir l'*Agence du Numérique en Santé* sous 12h en cas de détection d'un incident de sécurité et/ou impliquant une violation de données à caractère personnel.	

En cas d'incident de sécurité et/ou impliquant une violation de données à caractère personnel, l'ANS doit être prévenue sur l'adresse : prosanteconnect.editeurs@esante.gouv.fr.

3.11 Identité visuelle

PSC peut être proposé aux côtés d'autres modalités d'identification électronique. Dans ce cas, il est obligatoire d'intégrer les boutons officiels de PSC au même niveau que les autres méthodes de connexion proposées par le service : dans une même zone graphique, l'ensemble des moyens d'authentification doit être visible et mis sur un pied d'égalité.

Opérateur de Service Utilisateur		
EXI PSC 28	Le *Fournisseur de Service* DOIT intégrer l'identification électronique par Pro Santé Connect au même niveau que les autres modalités d'identification électronique proposées aux utilisateurs.	

PSC propose des boutons officiels à destination des FS. Il n'est pas permis d'utiliser d'autres boutons que ceux proposés. Ce référentiel met à disposition cette charte graphique (https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/charte-graphique-pro-sante-connect).

Opérateur de Service Utilisateur	
EXI PSC 29	Le *Fournisseur de Service* DOIT utiliser l'un des éléments graphiques de type boutons fournis par Pro Santé Connect pour l'intégration Pro Santé Connect conformément à la charte graphique de l'*Agence du Numérique en Santé*.

Opérateur de Service Utilisateur	
EXI PSC 30	Le *Fournisseur de Service* DOIT respecter la charte graphique Pro Santé Connect.

Opérateur de Service Utilisateur	
EXI PSC 31	Le *Fournisseur de Service* DOIT disposer de conditions générales d'utilisation et y insérer le paragraphe type sur Pro Santé Connect (Identification électronique par Pro Santé Connect)

Identification électronique par Pro Santé Connect

Pro Santé Connect est un téléservice mis en œuvre par l'*Agence du Numérique en Santé* (ANS) contribuant à simplifier l'identification électronique des professionnels intervenant en santé.

L'utilisateur peut se connecter grâce à l'ensemble des Moyens d'Identification Electronique reconnus par Pro Santé Connect définis à date par l'ANS sur le site esante.gouv.fr.

4 REFERENTIEL COMMUNAUTE PSC – EXTENSION ESPACE DE CONFIANCE

PORTÉE	La présence d'un acteur de l'*Espace de Confiance* dans l'encadré indique qu'il a une responsabilité et doit respecter l'exigence.		
Opérateur de Service Utilisateur	**Éditeur de Logiciel Utilisateur**	**Opérateur de Service Proxy e-santé**	**Éditeur de Logiciel Proxy e-santé**
EXI EDC PSC XXX	L'ensemble des exigences du référentiel sont identifiables par un encadré gris.		

Opérateur de Service Utilisateur	**Éditeur de Logiciel Utilisateur**	**Opérateur de Service Proxy e-santé**	**Éditeur de Logiciel Proxy e-santé**
RECO EDC PSC XXX	L'ensemble des recommandations du référentiel sont identifiables par un encadré blanc.		

4.1 Portée des exigences et recommandations du référentiel

Le tableau ci-dessous, établi par l'ANS, définit les périmètres des exigences à respecter par les différents acteurs visés dans le présent référentiel.

Pour chaque colonne du tableau, lorsqu'une case est remplie par la mention « OUI », cela implique que l'acteur doit traiter, gérer et assurer le suivi de l'exigence associée. Dans le cas contraire, si l'acteur n'est pas concerné par une exigence, sa case correspondante sera complétée par la mention « NON ».

		Opérateur de Service Utilisateur	Éditeur de Logiciel Utilisateur	Opérateur de Service Proxy e-Santé	Éditeur de Logiciel Proxy e-Santé
Référentiel Communauté Pro Santé Connect	**EXI PSC 01**	OUI	OUI	OUI	OUI
	EXI PSC 02	OUI	OUI	OUI	OUI
	EXI PSC 03	OUI	OUI	OUI	OUI
	EXI PSC 04	OUI	OUI	OUI	OUI
	EXI PSC 05	OUI	OUI	OUI	OUI
	EXI PSC 06	OUI	OUI	OUI	OUI
	EXI PSC 07	OUI	OUI	OUI	OUI
	EXI PSC 08	NON	NON	OUI	OUI
	EXI PSC 09	NON	NON	OUI	OUI
	EXI PSC 10	NON	NON	OUI	OUI
	EXI PSC 11	NON	NON	OUI	OUI
	EXI PSC 12	NON	OUI	NON	OUI
	EXI PSC 13	NON	OUI	NON	OUI
	EXI PSC 14	NON	NON	OUI	NON
	EXI PSC 15	NON	NON	OUI	OUI
	EXI PSC 16	NON	NON	OUI	OUI
	EXI PSC 17	NON	NON	OUI	OUI

		Opérateur de Service Utilisateur	Éditeur de Logiciel Utilisateur	Opérateur de Service Proxy e-Santé	Éditeur de Logiciel Proxy e-Santé
	EXI PSC 18	NON	NON	OUI	OUI
	EXI PSC 19	OUI	OUI	OUI	OUI
	EXI PSC 20	OUI	OUI	OUI	OUI
	EXI PSC 21	NON	NON	OUI	OUI
	EXI PSC 23	OUI	OUI	OUI	OUI
	EXI PSC 24	NON	NON	OUI	OUI
	EXI PSC 25	OUI	OUI	NON	NON
	EXI PSC 26	OUI	OUI	NON	NON
	EXI PSC 27	OUI	OUI	OUI	OUI
	EXI PSC 28	OUI	OUI	NON	NON
	EXI PSC 29	OUI	OUI	NON	NON
	EXI PSC 30	OUI	OUI	NON	NON
	EXI PSC 31	OUI	OUI	OUI	OUI
	EXI PSC 32	OUI	OUI	NON	NON
	EXI PSC 33	OUI	OUI	OUI	OUI
	EXI PSC 34	NON	NON	OUI	OUI
	EXI PSC 35	NON	NON	OUI	OUI
	EXI PSC 36	OUI	OUI	OUI	OUI
	EXI PSC 37	OUI	OUI	OUI	OUI
	EXI PSC 44	OUI	OUI	OUI	OUI
	RECO PSC 38	NON	NON	NON	OUI
	RECO PSC 39	OUI	OUI	OUI	OUI
	RECO PSC 40	OUI	OUI	OUI	OUI
	RECO PSC 41	OUI	OUI	OUI	OUI
	RECO PSC 42	OUI	OUI	OUI	OUI
	RECO PSC 43	OUI	OUI	NON	NON
Référentiel Communauté Pro Santé Connect – Extension Espace de Confiance	**EXI EDC PSC 101**	OUI	OUI	OUI	OUI
	EXI EDC PSC 102	OUI	OUI	OUI	OUI
	EXI EDC PSC 103	OUI	OUI	OUI	OUI
	EXI EDC PSC 104	NON	OUI	NON	OUI
	EXI EDC PSC 105	NON	NON	NON	OUI
	EXI EDC PSC 106	NON	NON	OUI	NON
	EXI EDC PSC 107	OUI	NON	OUI	NON
	EXI EDC PSC 108	OUI	NON	OUI	NON
	EXI EDC PSC 109	NON	OUI	OUI	OUI
	EXI EDC PSC 110	NON	NON	OUI	NON
	EXI EDC PSC 111	NON	NON	OUI	OUI
	EXI EDC PSC 112	OUI	NON	OUI	NON
	EXI EDC PSC 113	OUI	NON	OUI	NON
	EXI EDC PSC 114	NON	OUI	NON	OUI

		Opérateur de Service Utilisateur	Éditeur de Logiciel Utilisateur	Opérateur de Service Proxy e-Santé	Éditeur de Logiciel Proxy e-Santé
	EXI EDC PSC 115	NON	OUI	NON	OUI
	EXI EDC PSC 116	NON	OUI	NON	NON
	EXI EDC PSC 117	NON	OUI	NON	OUI
	EXI EDC PSC 118	OUI	NON	OUI	NON
	EXI EDC PSC 119	NON	OUI	NON	OUI
	EXI EDC PSC 120	OUI	NON	OUI	NON
	EXI EDC PSC 121	NON	NON	OUI	NON
	EXI EDC PSC 122	NON	NON	NON	OUI
	EXI EDC PSC 123	NON	NON	OUI	NON
	EXI EDC PSC 124	NON	NON	OUI	NON
	EXI EDC PSC 125	NON	NON	NON	OUI
	EXI EDC PSC 126	NON	NON	OUI	NON
	EXI EDC PSC 127	OUI	OUI	OUI	OUI
	EXI EDC PSC 128	OUI	NON	OUI	NON
	EXI EDC PSC 129	NON	OUI	NON	OUI
	EXI EDC PSC 130	OUI	NON	OUI	NON
	EXI EDC PSC 131	NON	OUI	NON	OUI
	EXI EDC PSC 138	OUI	OUI	OUI	OUI
	RECO EDC PSC 132	NON	NON	OUI	OUI
	RECO EDC PSC 133	NON	OUI	NON	OUI
	RECO EDC PSC 134	OUI	NON	OUI	NON
	RECO EDC PSC 135	NON	NON	NON	OUI
	RECO EDC PSC 136	OUI	OUI	OUI	OUI
	RECO EDC PSC 137	OUI	NON	OUI	NON

L'ANS pourra étudier à titre d'exception la levée de ces certaines exigences dans le cadre de demandes et de situations justifiées.

4.2 Eligibilité à l'Espace de Confiance

Avant d'intégrer l'EDC, le FS devra se conformer au Référentiel *Communauté PSC* et se référer au CI-SIS volet de transport Pro Santé Connect.

		Opérateur de Service Proxy e-santé	Éditeur de Logiciel Proxy e-santé
RECO EDC PSC 132	Le *Fournisseur de Service* DEVRAIT se conformer au CI-SIS volet de transport Pro Santé Connect.		

Opérateur de Service Utilisateur	Éditeur de Logiciel Utilisateur	Opérateur de Service Proxy e-santé	Éditeur de Logiciel Proxy e-santé
EXI EDC PSC 101	Le *Fournisseur de Service* DOIT respecter le référentiel *Communauté Pro Santé Connect*.		

Le respect du référentiel *PSC Communauté – Extension EDC* nécessite, par défaut, de répondre aux exigences du référentiel *Communauté Pro Santé Connect*.

4.3 Documentation et processus de conformité

Le document de conformité a pour objectif de rassembler toute information relative à l'exploitation du système telle que le paramétrage ou la configuration du système par défaut, son fonctionnement et son utilisation ainsi que les directives à adopter pour assurer une utilisation fiable, optimisée et sécurisée chez l'Opérateur.

Opérateur de Service Utilisateur	Éditeur de Logiciel Utilisateur	Opérateur de Service Proxy e-santé	Éditeur de Logiciel Proxy e-santé
EXI EDC PSC 102	Le *Fournisseur de Service* DOIT décrire dans le document de conformité, dédié et régulièrement mis à jour, les mesures qu'il met en œuvre afin de se conformer aux exigences du présent référentiel.		

Ce document de conformité explicitera également la liste des standards et spécifications auxquels le FS doit se conformer :

- [API REST] Volet Transport Synchrone - API Rest - CI-SIS ;
- [PSC] Pro Santé Connect - Référentiel PSC ;
- [OIDC] OpenID Connect ;
- [CIBA] OpenID Connect MODRNA Client initiated Backchannel Authentication Flow ;
- [RFC7235] HTTP Authentication ;
- [RFC7519] JSON Web Token (JWT) ;
- [RFC6749] OAuth 2.0 Authorization Framework, pour tous les aspects liés à l'obtention d'autorisation via le processus "Authorization Code Grant" ;
- [RFC6750] OAuth 2.0 Bearer Token Usage ;
- [RFC7009] OAuth 2.0 Token Revocation ;
- [RFC7662] OAuth 2.0 Token Introspection ;
- [RFC8693] OAuth 2.0 Token Exchange ;
- [RFC8705] OAuth 2.0 mTLS Client Authentication and Certificate-Bound Access Tokens.

Il est attendu que le FS maintienne conforme le document de conformité en précisant les éléments suivants :

- Des justifications concernant la façon dont sont sécurisées les communications entre les composants du système et avec les composants externes choisis, et plus particulièrement quand ils sont logiquement ou physiquement séparés ;
- Les éventuels protocoles ou flux de communication ne pouvant pas être chiffrés ainsi que les raisons et les risques résiduels induits et acceptés ;

- Les composants tiers sélectionnés en prenant en considération le respect de bonnes pratiques similaires de la part de ces derniers ;
- Les outils, processus et la documentation détaillée des mesures mises en place afin d'assurer la qualité, la sécurité du code et la gestion de l'obsolescence des bibliothèques.

Le FS pourra mettre en place une revue systématique de ses codes par un autre pair, avant toute mise en production.

Il est attendu que le document de conformité fasse apparaître l'obligation de :

- Paramétrer et personnaliser la configuration par défaut ;
- Activer uniquement les fonctionnalités et services essentiels à la mise en œuvre du logiciel ;
- Mettre en application le principe de moindre privilège ;
- Revoir régulièrement les mesures de sécurité mises en place concernant les sous-systèmes sensibles (c'est-à-dire les serveurs de stockage, les bases de données des clés privées, les identifiants, les jetons etc.)

D'autres éléments devant être inclus dans ce document de conformité seront précisés dans les exigences suivantes.

Le document de conformité devra être mis à jour en cas de publication d'une nouvelle version de ce référentiel ou d'une modification majeure du système, de son environnement ou des processus et mesures de sécurité applicables.

Opérateur de Service Utilisateur	**Éditeur de Logiciel Utilisateur**	**Opérateur de Service Proxy e-santé**	**Éditeur de Logiciel Proxy e-santé**
EXI EDC PSC 103	Le *Fournisseur de Service* DOIT utiliser le modèle fourni par l'*Agence du Numérique en Santé* pour rédiger le document de conformité.		

Le FS est ainsi invité à consulter le modèle fourni par l'ANS.

Dans le cas où le FS ferait le choix de ne pas s'appuyer sur le modèle de document de conformité fourni par l'ANS, le document de conformité qu'il rédigera devra alors à minima présenter les mêmes éléments que ceux qui sont attendu dans le modèle.

	Éditeur de Logiciel Utilisateur		**Éditeur de Logiciel Proxy e-santé**
EXI EDC PSC 104	Le *Fournisseur de Service* DOIT fournir l'inventaire des composants techniques, des flux applicatifs, des requêtes, des protocoles et des services nécessaires à l'utilisation du système dans une version supportée à date.		

L'inventaire est attendu dans le document de conformité dans son intégralité. L'obligation de revue régulière de la configuration par défaut, notamment à l'occasion des montées de version de tout composant, doit également être précisée dans le document de conformité.
Cet inventaire doit comprendre :

- Les composants qui constituent le système, les numéros de version et les dates de fin de support pour les composants fournis par des tiers ;
- Les flux applicatifs (précisant les protocoles, ports réseau, etc.) de ce système ;
- Les requêtes considérées comme nécessaires pour le fonctionnement du système ;
- Les protocoles utilisés ;
- Les services essentiels à activer lors du déploiement de la solution en production (par exemple, une application web classique peut comprendre un service de base de données, un serveur applicatif, un reverse proxy http etc…).

	Éditeur de Logiciel Utilisateur		**Éditeur de Logiciel Proxy e-santé**

RECO EDC PSC 133	Le *Fournisseur de Service* DEVRAIT utiliser, lorsqu'ils sont disponibles, des outils pour auditer l'ensemble des composants du système à chaque modification.

Ces outils peuvent varier selon la nature des différents composants intégrés dans le système tels que des bibliothèques, logiciels et dépendances de l'application. Ils peuvent prendre la forme d'outils de recherche de vulnérabilité, d'analyses de code sources automatisés ou non, bibliothèques etc.

La liste détaillée des outils utilisés pour auditer l'ensemble des composants du système sera à inclure dans le document de conformité.

			Éditeur de Logiciel Proxy e-santé
EXI EDC PSC 105	Le *Fournisseur de Service* DOIT être en mesure de fournir à l'*Agence du Numérique Santé* une analyse de risques à jour.		

Une analyse de risque doit être réalisée afin d'identifier les sous-systèmes sensibles. Cette analyse doit porter sur l'ensemble des composants permettant le stockage des secrets c'est-à-dire, les serveurs de stockage, les bases de données de clés privées, les composants participant à la gestion des jetons, etc.

		Opérateur de Service Proxy e-santé	
EXI EDC PSC 106	Le *Fournisseur de Service* DOIT appliquer des mesures issues de l'analyse de risques.		

Il est attendu que le FS :

- Identifie des mesures palliatives de sécurisation et stockage des secrets en se basant sur les résultats de l'analyse de risques effectuée ;
- Applique des mesures organisationnelles et techniques renforcées de sécurisation et stockage des secrets dans le but de protéger les actifs sensibles.

Les résultats de l'analyse de risques ainsi que les mesures de mitigation seront à inclure dans le document de conformité.

Opérateur de Service Utilisateur	**Éditeur de Logiciel Utilisateur**	**Opérateur de Service Proxy e-santé**	**Éditeur de Logiciel Proxy e-santé**
EXI EDC PSC 138	Le *Fournisseur de Service* DOIT s'appuyer sur les versions en vigueur de moins de trois (3) ans ou sur la dernière version publiée de chaque document et standards mentionnés dans ce référentiel.		

En cas de prise en compte de nouvelles versions plus à jour, une communication de l'ANS sera transmise à l'ensemble des acteurs ; un délai de prévenance sera systématiquement appliqué, sauf en cas de force majeure.

4.4 Chiffrement et sécurisation des canaux d'échanges

Afin de sécuriser les canaux d'échanges, il est attendu que le FS intègre des mécanismes s'appuyant sur des réglementations et protocoles de communication en vigueur, notamment dans le cadre de la gestion des certificats et jetons.

Par canaux d'échanges est entendu tout moyen mis en place permettant l'échange de données entre un FS de l'EDC et les autres acteurs de l'EDC, notamment PSC et l'*API Pro Santé Connectée*. Leurs chiffrement et sécurisation ont pour but de protéger les actifs sensibles notamment les jetons.

Opérateur de Service Utilisateur		**Opérateur de Service Proxy e-santé**	
EXI EDC PSC 107	Le *Fournisseur de Service* DOIT maintenir à jour les mécanismes cryptographiques utilisés et les tailles de clés correspondantes conformément aux recommandations de l'ANSSI.		

Les mécanismes cryptographiques correspondent par exemple aux algorithmes de chiffrement, de hachage, de vérification d'intégrité et d'authenticité etc.

Il est attendu que ces mécanismes soient conformes aux règles énoncées par le RGS (en particulier ses annexes B1 et B2), par le guide des mécanismes cryptographiques, par le guide de sélection d'algorithmes cryptographiques et le cas échéant par les Recommandations de sécurité relatives au TLS, publiés par l'ANSSI.

Opérateur de Service Utilisateur		**Opérateur de Service Proxy e-santé**	
EXI EDC PSC 108	Le *Fournisseur de Service* DOIT appliquer la politique de gestion des clés cryptographiques de l'IGC-Santé publiée par l'*Agence du Numérique en Santé*.		

Il est attendu du FS qu'il respecte les conditions générales d'utilisation des moyens d'identification électronique délivrés par l'ANS.

Pour appliquer la politique de gestion des clés cryptographiques de l'IGC-santé, le *Fournisseur de Service* devra notamment respecter les paragraphes ci-dessous des conditions générales d'utilisation des moyens d'identification électronique délivrés par l'ANS :

- 5.3.2 qui mentionne les engagements des propriétaires de certificat, le devoir de veiller à limiter l'accès aux clés privées uniquement aux personnes dûment autorisées et d'empêcher la duplication ou l'installation des clés dans de multiples équipements ;
- 5.4 qui aborde la durée de validité des certificats, leur renouvellement automatique ainsi que le devoir de prévenir par mail le propriétaire de la fin de validité du certificat 2 mois avant son échéance ;
- 5.5.1 qui évoque les modalités de révocation des certificats logiciels et les cas d'usage.

	Éditeur de Logiciel Utilisateur	**Opérateur de Service Proxy e-santé**	**Éditeur de Logiciel Proxy e-santé**
EXI EDC PSC 109	Le *Fournisseur de Service* DOIT mettre en place une communication chiffrée et authentifiée entre le *Service Utilisateur* et le *Service Proxy e-Santé*, adossée à l'authentification de l'utilisateur sur le *Service Utilisateur* et par l'authentification du *Service Proxy e-Santé.*		

Il est attendu que le FS intègre des mécanismes de protection adaptés aux risques tels que l'utilisation de VPN, du TLS ou de tunnels SSH.

Il est attendu que l'*OpS Proxy e-santé* assure la configuration permettant l'authentification du *Service Proxy e-Santé* auprès du logiciel utilisateur.

Il est attendu que l'*Éditeur de Logiciel Utilisateur* et l'*Éditeur de Logiciel Proxy e-santé* assurent l'adossement à l'authentification de l'utilisateur auprès de PSC.

Dans le cas d'un *Opérateur de Service Utilisateur* Client WEB où l'utilisateur opère avec des équipements (écran, clavier, souris…) distants du milieu d'exécution du service, il est attendu qu'une session de communication sécurisée

entre le terminal d'affichage de l'utilisateur et l'environnement d'exécution de l'*Opérateur de Service Utilisateur* WEB soit établie.

La figure ci-dessous explicite les différents flux TLS et mTLS lors d'une session de communication entre le client (de type Navigateur Web ou Client Lourd) et le serveur.

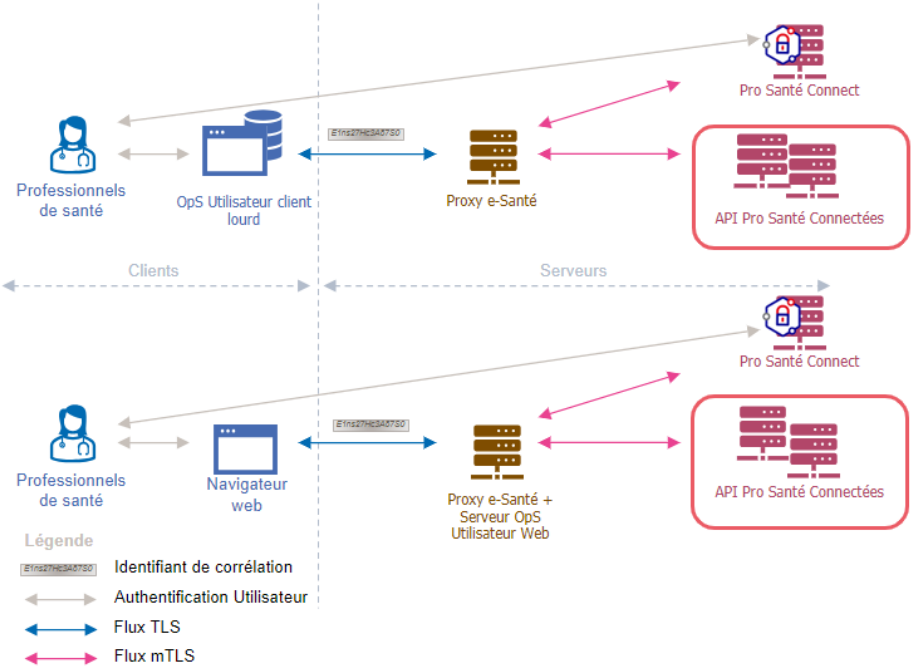

Figure 3 - Etablissement d'une session de communication Client-Serveur

Le diagramme suivant issu du CI-SIS Volet Transport illustre l'ensemble des étapes d'un appel d'une *API Pro Santé Connectée* depuis une application web.

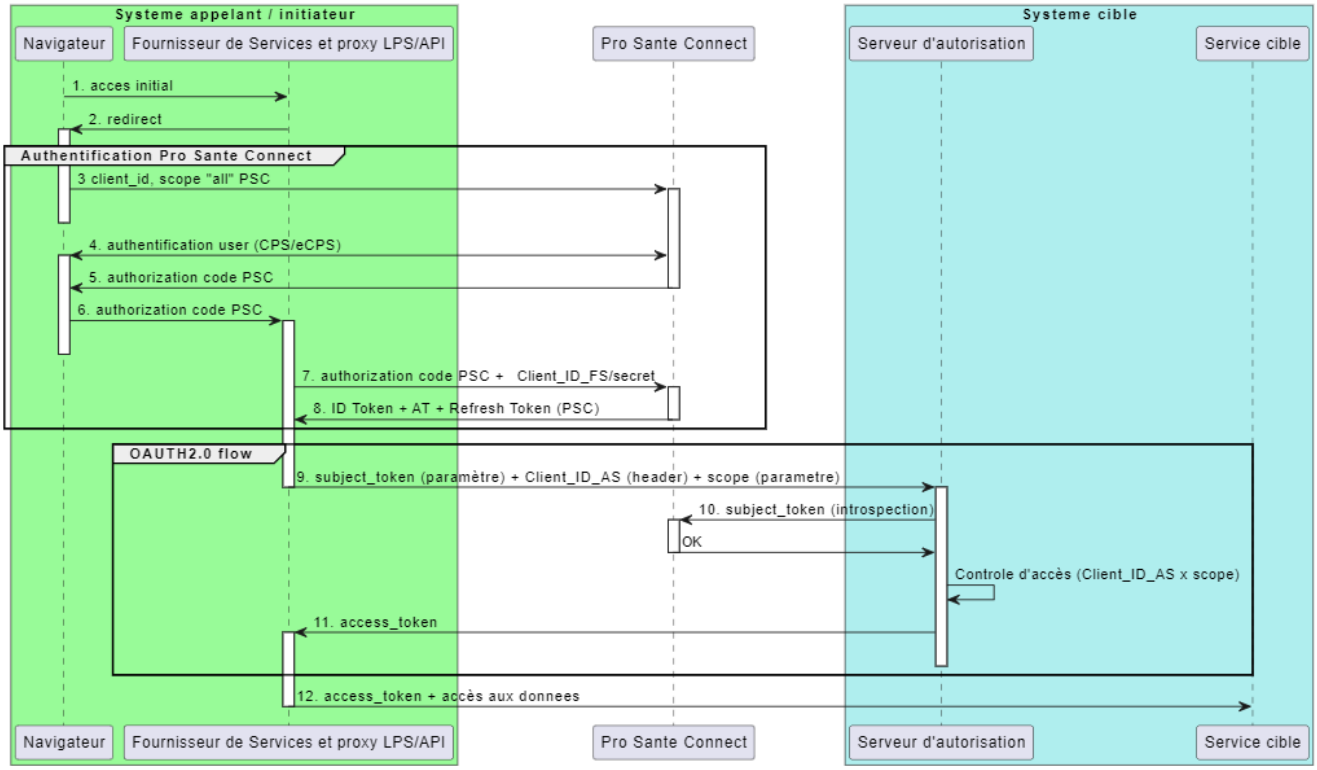

Figure 4 - Diagramme de séquence d'un appel d'une API ProSantéConnectée

		Opérateur de Service Proxy e-santé	
EXI EDC PSC 110	Le *Fournisseur de Service* DOIT mettre en place une communication chiffrée et sécurisée par authentification mutuelle de type TLS 1.2 minimum par un certificat électronique AUTH_CLI de l'offre ORG de l'IGC-Santé entre *Services Proxy e-santé* et *API Pro Santé Connectée.*		

La *Figure 5 - Principaux échanges au sein de l'espace de confiance* schématise les différents échanges de requêtes et flux au sein de l'*Espace de Confiance*.

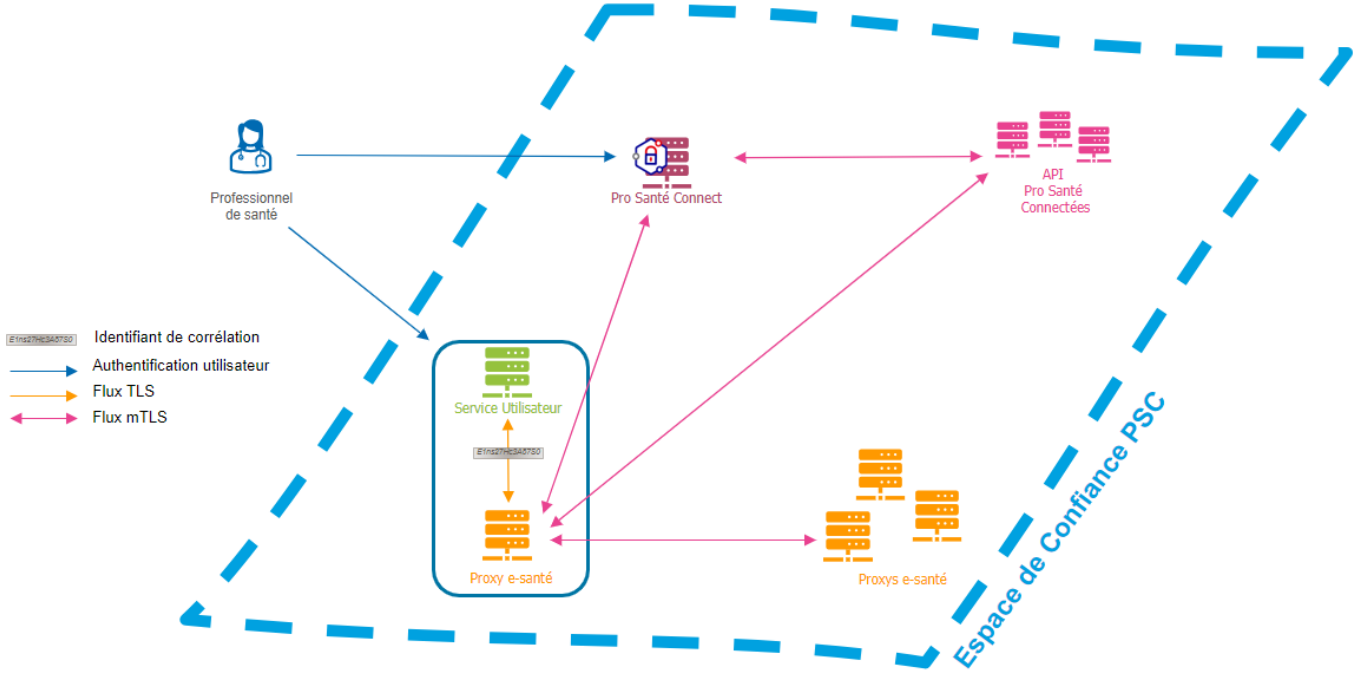

Figure 5 - Principaux échanges au sein de l'espace de confiance

Il est attendu que le FS n'utilise qu'un seul et unique type de certificat pour contacter et communiquer avec l'ensemble des composants de l'EDC.

L'utilisation de certificats électroniques côté "client TLS" peut être omise lors de l'établissement de la communication TLS entre un Serveur d'application *Service utilisateur* (en tant que "client TLS") et un *Proxy e-Santé* (en tant que "serveur TLS") à condition que ces deux systèmes soient sous la responsabilité du même Opérateur et que la

communication se fasse exclusivement via des réseaux privés (réseaux locaux ou VPN entre réseaux locaux) sous la responsabilité du même Opérateur. À l'exception de ce cas, toute autre tentative de connexion devra être refusée.

Champ	Valeur
cn=	Valeur libre correspondant au ClientID de l'*OpS Utilisateur.*
ou=	L'identifiant de la structure porteuse du fournisseur de services (idStructure) issu du référentiel d'identité utilisé par l'IGC Santé.

		Opérateur de Service Proxy e-santé	Éditeur de Logiciel Proxy e-santé
EXI EDC PSC 111	Le *Fournisseur de Service* DOIT garantir que le client ID, déclaré dans le Distinguished Name du certificat, qu'il présente aux autres acteurs de l'*Espace de Confiance* fait référence à un unique *Fournisseur de Service*, directement en contact avec l'utilisateur authentifié.		

Dans le cas d'un proxy mutualisé, l'*OpS Utilisateur* au contact de l'utilisateur transmet son client id au *Proxy e-Santé*. Le *Proxy e-Santé* communique ensuite avec l'*API Pro Santé Connectée* en lui communiquant son propre idStructure

(DN du certificat du *Proxy e-Santé*) ainsi que le client id du FS en contact avec l'utilisateur (dans le CN de son certificat).

Champ	Valeur	Champ	Valeur
cn=	Client ID de l'OpS 1	cn=	Client ID de l'OpS 2
ou=	idStructure de l'opérateur du Proxy e-Santé mutualisé	ou=	idStructure de l'opérateur du Proxy e-Santé mutualisé

Le *Proxy e-Santé* dispose d'un certificat ORG_CLI pour chaque *OpS Utilisateur* pour lequel il réalise des authentifications mutuelles. Ceci permet d'identifier et de tracer les différents services *OpS Utilisateur*.

Il est attendu que :

- L'*API Pro Santé Connectée* reçoive toujours le client id du FS directement en contact avec l'utilisateur ;
- Tout FS appelant une *API Pro Santé Connectée* utilise le certificat de l'*OpS Utilisateur* pour respecter la règle explicitant la nécessité de n'avoir qu'un certificat associé à un identifiant et une instance de l'application. Dans le cas où l'*OpS Utilisateur* et le *Proxy e-Santé* sont les mêmes acteurs alors c'est le certificat de l'*OpS Utilisateur* qui doit être utilisé et non celui du *Proxy e-Santé*.

Deux types d'architectures non autorisées dans le cadre de l'EDC sont présentées ci-dessous :

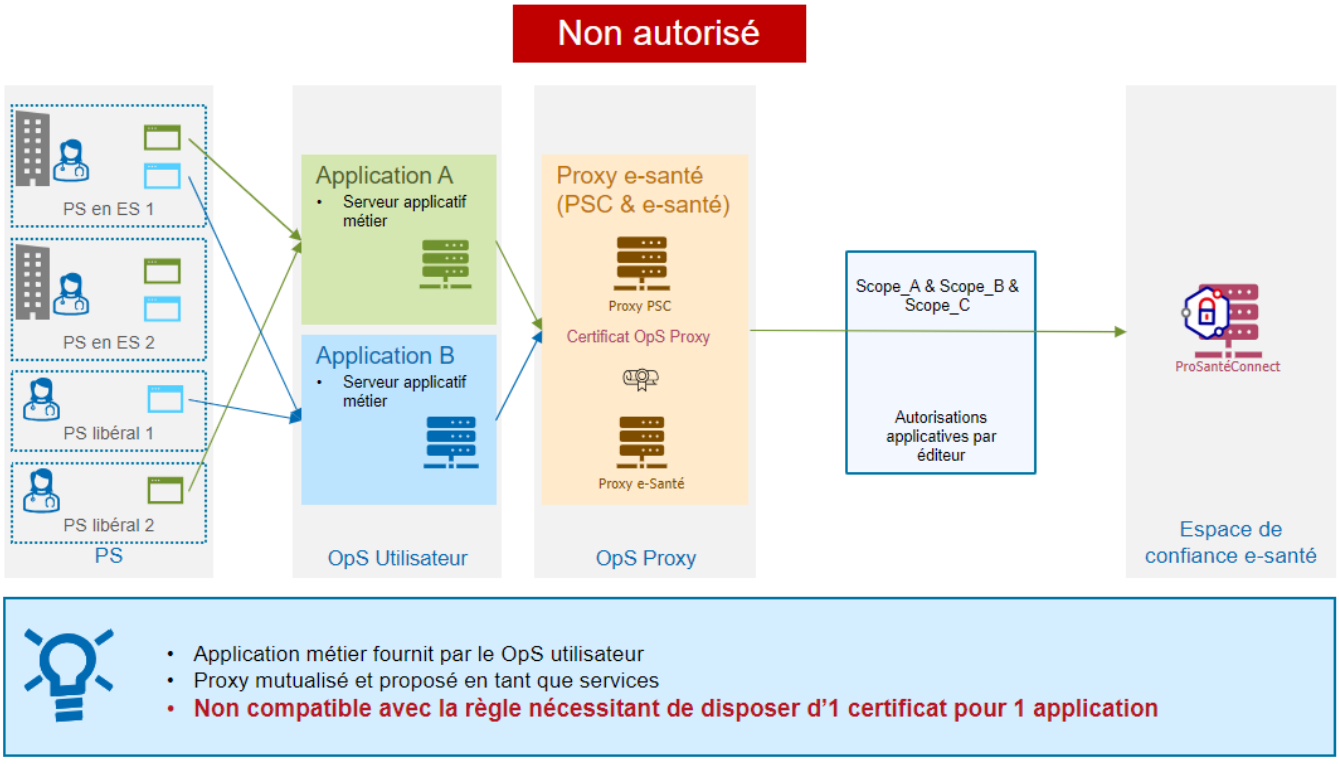

Figure 6 - Exemple 1 d'architecture non acceptée

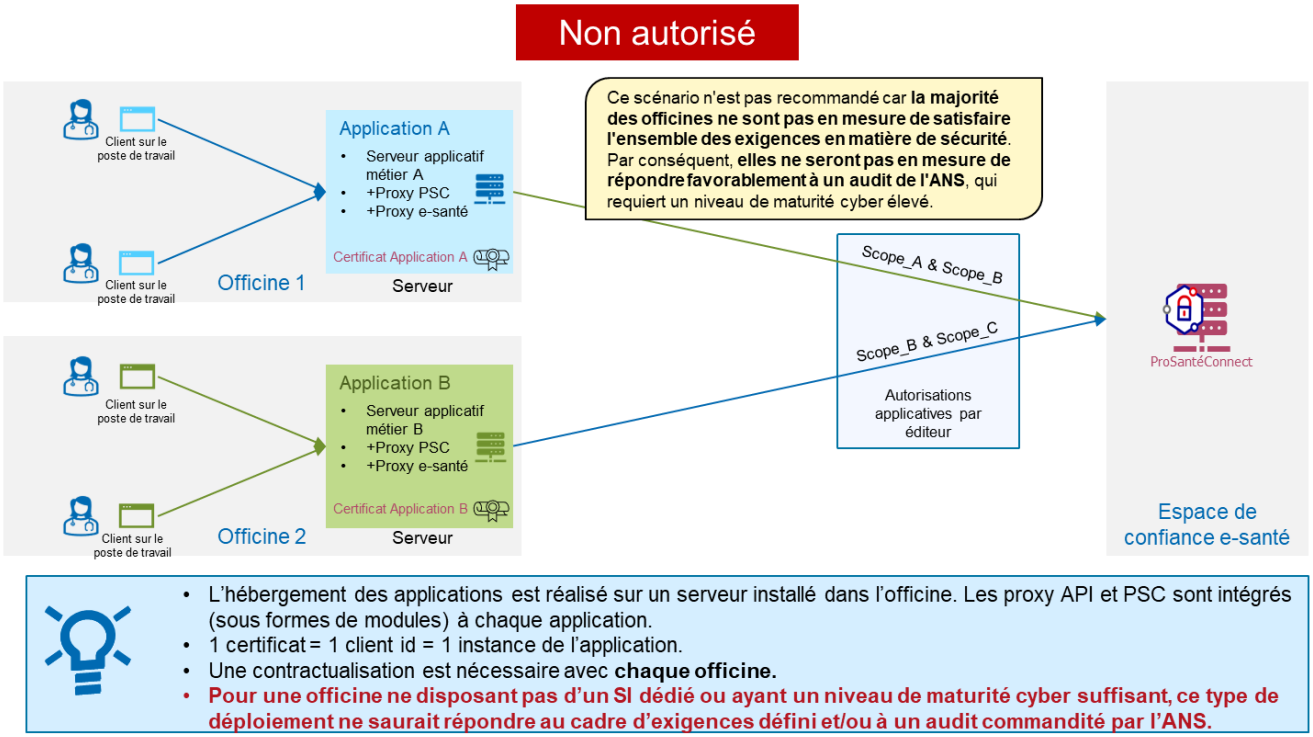

Figure 7 - Exemple 2 d'architecture non acceptée

Opérateur de Service Utilisateur		**Opérateur de Service Proxy e-santé**	
EXI EDC PSC 112	Le *Fournisseur de Service* DOIT vérifier la validité d'un certificat avant l'établissement de tout canal sécurisé sur la base de ce dernier.		

Les vérifications correspondent au contrôle de la validité et de la non-révocation du certificat prévus par les standards, incluant la vérification de validité de l'ensemble de la chaîne de certificats à laquelle est rattaché le certificat concerné.

Opérateur de Service Utilisateur		**Opérateur de Service Proxy e-santé**	
EXI EDC PSC 113	Le *Fournisseur de Service* DOIT garantir l'association, la protection et la continuité des flux HTTP entre les points de terminaison TLS.		

Le FS pourra s'appuyer sur le guide d'interconnexion d'un système d'information à internet de l'ANSSI.

En cas de terminaison des connexions TLS assurée par un dispositif différent du service, comme un Reverse Proxy, l'architecture système et réseau ainsi que la configuration des dispositifs doivent garantir la bonne association du flux HTTP ainsi que le service associé au certificat utilisé.

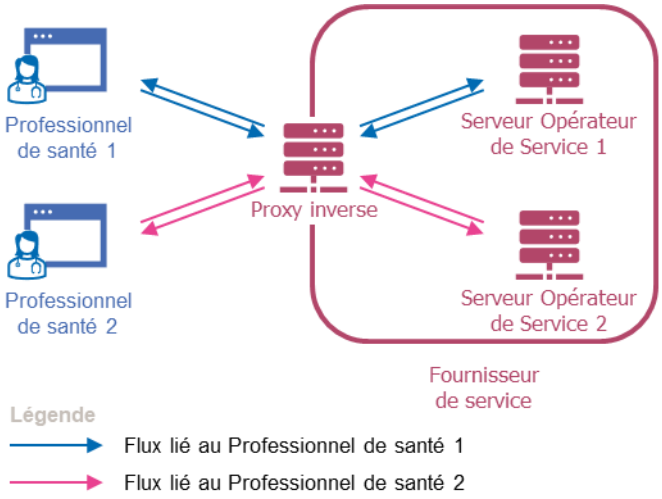

Figure 8 - Illustration d'un cas d'usage d'association des flux

La figure ci-dessus donne un exemple d'association des flux : le professionnel de santé 1 (respectivement 2) requérant une information détenue par le serveur fournisseur de donnée 1 (resp. 2), il est de la responsabilité du fournisseur de service de s'assurer que l'architecture et la configuration de son service assure le flux HTTP contenant la réponse attendue par le professionnel de santé 1 (resp. 2) est bien reçu par ce dernier.

Exemple de recommandations du guide d'interconnexion d'un système d'information à internet de l'ANSSI :

- Étudier la mise en place d'une interception TLS maîtrisée pour analyser les contenus échangés avec des sites malveillants accessibles en HTTPS ;
- Eviter la mise en place de mécanismes de déchiffrement HTTPS en raison d'une potentielle rupture de canal sécurisé pouvant exposer des données sensibles ;
- Gérer les cas d'exception des connexions directes pour garantir l'absence de communication entre les pares-feux internes et externes, sans passer par la zone de services relais.

4.5 Gestion des identifiants de corrélation

Cette section aborde la création, gestion, stockage et les règles de sécurisation des identifiants de corrélation lors des échanges entre le FS et les différents acteurs de l'EDC.

	Éditeur de Logiciel Utilisateur		**Éditeur de Logiciel Proxy e-santé**
EXI EDC PSC 114	Le *Fournisseur de Service* DOIT définir un identifiant de corrélation utilisateur partagé avec les autres composants de l'*Espace de Confiance* à la suite de l'authentification de l'utilisateur.		

Il est attendu que l'établissement de la session de communication sécurisée soit faite préalablement au démarrage du processus d'authentification de l'utilisateur via PSC.

L'identifiant de corrélation permettra d'assurer la traçabilité de bout en bout en prouvant l'état d'authentification de l'utilisateur obtenu de PSC, et en identifiant quelles sont les interactions réalisées par le *Proxy e-Santé* avec PSC et avec des *API Pro Santé Connectée* au nom d'un utilisateur donné.

L'authentification de l'extrémité côté *OpS Utilisateur* Client Lourd de la communication sécurisée peut être omise une fois le *Proxy e-Santé* authentifié via la communication sécurisée et l'utilisateur authentifié via l'utilisation de PSC dans le cadre de la même communication sécurisée respectant des recommandations de l'ANSSI. La *Figure 3 - Etablissement d'une session de communication Client-Serveur*, qui est présentée précédemment dans le document, indique quels flux doivent être protégés par TLS ou mTLS dans le cas d'un Client *OpS Utilisateur* Lourd.

	Éditeur de Logiciel Utilisateur		**Éditeur de Logiciel Proxy e-santé**
EXI EDC PSC 115	Le *Fournisseur de Service* DOIT définir un identifiant de corrélation non prédictif et résistant à toute collision construit à l'aide d'algorithmes générateur d'aléas et/ou de condensats conformes aux recommandations de l'ANSSI.		

Les recommandations sont décrites dans le guide des mécanismes cryptographiques. Il est également attendu que l'identifiant de corrélation possède au moins 128 bits d'entropie.

L'identifiant de corrélation produit par le logiciel *Proxy e-santé* doit être changé à chaque nouvelle connexion.

	Éditeur de Logiciel Utilisateur		
EXI EDC PSC 116	Le *Fournisseur de Service* DOIT s'assurer que les identifiants de corrélation sont masqués à l'utilisateur.		

Il est attendu que les identifiants de corrélation n'apparaissent pas dans les URL, les paramètres d'URL ou les messages d'erreur. Le FS doit utiliser exclusivement les méthodes HTTP POST plutôt que les méthodes GET pour envoyer des données.

4.6 Gestion des informations de raccordement

On appelle *informations de raccordement* les différentes informations utilisées par le FS et nécessaires pour son fonctionnement avec Pro Santé Connect telles que le client ID, le client secret, le certificat AUTH_CLI et la clé privée associée, mais aussi les secrets utilisés lors des échanges tels que codes PIN et jetons.

	Éditeur de Logiciel Utilisateur		**Éditeur de Logiciel Proxy e-santé**
EXI EDC PSC 117	Le *Fournisseur de Service* DOIT s'assurer qu'aucune information de raccordement ne soit présente dans le code source.		

Opérateur de Service Utilisateur		**Opérateur de Service Proxy e-santé**	
EXI EDC PSC 118	Le *Fournisseur de Service* DOIT s'assurer que les informations de raccordement persistantes soient stockées de façon sécurisée et jamais conservées au-delà de leur durée de validité.		

Une solution de gestion des clés (Key Management System ou KMS) est un exemple d'espace de stockage sécurisé des informations de raccordement afin d'éviter l'intégration de clés dans le code provenant des logiciels mis en œuvre.

Quand des informations de raccordement de sécurité sont transmises, les fonctionnalités adéquates des protocoles de communication utilisées doivent être mises en œuvre pour signaler que ces informations de raccordement de sécurité ne doivent pas être mises en cache par un navigateur, par un client lourd, ou par un éventuel système intermédiaire.
Les informations utilisées par le système pour assurer l'authentification de ses utilisateurs (personnes ou autres systèmes) ou pour vérifier leur état d'authentification doivent être stockées sous une forme qui interdit définitivement d'accéder à leur valeur en clair, tout en permettant leur comparaison avec une information de raccordement à tester.

Des fonctions de hachage cryptographique peuvent être employées afin d'obfusquer les informations de raccordement. L'obfuscation doit toujours permettre la bonne vérification d'une information de raccordement à tester lors de l'authentification. Si besoin, le haché de l'information peut être utilisé comme index pour retrouver les informations contextuelles liées à l'information mais qui ne constituent pas elles-mêmes des informations de raccordement de sécurité, et qui peuvent être nécessaires à des validations de sécurité (e.g. date d'expiration de l'état d'authentification matérialisé par l'information de raccordement , état de révocation ou non de l'information de raccordement, identifiant du système autorisé à utiliser l'information de raccordement) ou aux fonctions métiers assurées par le système (e.g. informations relatives à l'utilisateur).

Pour le cas des identifiants de corrélation, le stockage dans le navigateur est considéré comme étant sûr tant que les cookies sont correctement sécurisés lorsqu'un navigateur web est utilisé côté utilisateur. Dans le cas de l'utilisation du protocole HTTP(S), cette exigence se traduit notamment par le fait que le champ d'en-tête de réponse HTTP "Cache-Control" doit être inclus avec la valeur "no-store" et que le champ d'en-tête de réponse HTTP "Pragma" doit être inclus avec la valeur "no-cache".

	Éditeur de Logiciel Utilisateur		**Éditeur de Logiciel Proxy e-santé**
EXI EDC PSC 119	Le *Fournisseur de Service* DOIT s'assurer que les informations de raccordement éphémères ne soient stockées qu'en mémoire volatile et jamais conservées au-delà de leur durée de validité.		

Les informations de raccordement éphémères incluent en particulier les jetons délivrés par PSC. Les informations liées aux jetons d'accès ou jetons PSC lorsqu'elles sont connues, et à l'exclusion des jetons eux-mêmes, peuvent être stockées en tenant compte des contraintes de sécurité applicables aux informations contenues.

Une empreinte non réversible obtenue à l'aide d'une fonction de hachage cryptographique appliquée à ces jetons peut être stockée et utilisée à des fin d'indexation d'informations ou de liaison entre des traces.
Par exemple, dans le cadre de partage de charge ou de redondance à des fins de disponibilité du service, les jetons peuvent être transmis de façon sécurisée à un sous-système de cache partagé intégré à la solution ou être stockés temporairement en mémoire volatile par ce sous-système afin d'être partagés à nouveau. Dans ce cas, les différents serveurs manipulant ces secrets devront respecter chacune des exigences applicables au système lui-même.

Opérateur de Service Utilisateur		**Opérateur de Service Proxy e-santé**	
RECO EDC PSC 134	Le *Fournisseur de Service* DEVRAIT interdire l'envoi de jetons Pro Santé Connect jusqu'à un client lourd.		

Dans certains cas d'usages particuliers en raison de standards d'architectures imposés ou de référentiels existants, les jetons peuvent être amenés à transiter jusqu'à un poste client.

Opérateur de Service Utilisateur		Opérateur de Service Proxy e-santé	
EXI EDC PSC 120	Le *Fournisseur de Service* DOIT garantir que les jetons Pro Santé Connect initiés dans le cadre de l'*Espace de Confiance* ne sont échangés qu'avec d'autres acteurs de l'*Espace de Confiance*.		

Etant donné que les systèmes de navigations sont exclus du périmètre, il n'est pas exigé du FS de mettre en place des mesures de durcissement au niveau du navigateur de l'utilisateur visant à empêcher une éventuelle fuite de jeton depuis ce dernier.

4.7 Surveillance et gestion des alertes

La détection de mésusages ou de flux non conformes est obligatoire dans le cadre de l'EDC. Par conséquent, des mécanismes avancés de supervision du fonctionnement et de la sécurité du système, qui déclencheront des alertes en cas d'usage anormal ou mésusage du système, doivent être mis en place.

		Opérateur de Service Proxy e-santé	
EXI EDC PSC 121	Le *Fournisseur de Service* DOIT uniquement autoriser les flux applicatifs nécessaires à l'utilisation du système en intégrant des dispositifs de filtrage, de rupture de protocole et de détection d'intrusion couvrant l'intégralité du système afin de limiter ces flux.		

Le *Fournisseur de Service* devra s'appuyer sur les recommandations de l'ANSSI en termes de détection de rupture protocolaire et analyses de flux au sein du guide d'interconnexion d'un système d'information à internet.

Les dispositifs attendus, qui sont à intégrer dans le système ou l'environnement d'hébergement via Internet ou via une liaison directe avec un tiers, sont par exemple des dispositifs de :

- Filtrage (WAF) ;
- Rupture de protocoles (reverse proxy, serveur mandataire/proxy etc.) ;
- Routeurs filtrants, Firewall… ;
- IDS (système de détection d'intrusion) avec des règles de détection adaptées et maintenues à jour.

			Éditeur de Logiciel Proxy e-santé
EXI EDC PSC 122	Le *Fournisseur de Service* DOIT interrompre toute requête non conforme au fonctionnement prévu par le service en déclenchant une alerte.		

Une requête est considérée comme étant conforme si elle est incluse dans la description des requêtes fournies par l'inventaire.

		Opérateur de Service Proxy e-santé	
EXI EDC PSC 123	Le *Fournisseur de Service* DOIT mettre en œuvre une procédure de traitement des alertes qui est décrite dans un document dédié et régulièrement mis à jour.		

Il est attendu que le FS mette en place des mécanismes de supervision du fonctionnement et de la sécurité du système qui déclencheront des alertes en cas d'usage anormal ou mésusage du système. Pour la mise en place de la procédure, le *Fournisseur de Service* pourra s'appuyer sur les recommandations de l'ANSSI.

Le FS a pour obligation de préciser tous les détails de sa procédure de traitement des alertes dans le document de conformité.

Parmi les mésusages pris en compte figurent le dépassement de toute limite fixée sur des quantités non maîtrisées par les systèmes (e.g. délai maximal d'établissement de connexion TCP, fréquence maximale de requête, taille maximale des entêtes et requêtes http, durée maximale de requête HTTP, taille maximale de contenu reçu).

Les mésusages pris en compte dans la procédure d'alertes doivent également inclure toute non-conformité détectée dans les vérifications prévues par les spécifications des standards cités dans l'exigence EDC PSC 102 :

- [API REST] Volet Transport Synchrone- API Rest - CI-SIS ;
- [PSC] Pro Santé Connect - Référentiel PSC ;
- [OIDC] OpenID Connect ;
- [CIBA] OpenID Connect MODRNA Client initiated Backchannel Authentication Flow ;
- [RFC7235] HTTP Authentication ;
- [RFC7519] JSON Web Token (JWT) ;
- [RFC6749] OAuth 2.0 Authorization Framework, pour tous les aspects liés à l'obtention d'autorisation via le processus "Authorization Code Grant" ;
- [RFC6750] OAuth 2.0 Bearer Token Usage ;
- [RFC7009] OAuth 2.0 Token Revocation ;
- [RFC7662] OAuth 2.0 Token Introspection ;
- [RFC8693] OAuth 2.0 Token Exchange ;
- [RFC8705] OAuth 2.0 mTLS Client Authentication and Certificate-Bound Access Tokens.

Il est attendu que le FS interdise toute poursuite de requête en cas de non-conformité détectée aux spécifications de mise en œuvre des standards cités précédemment, ou encore aux spécifications des requêtes nécessaires au fonctionnement du service telles que décrite dans l'inventaire. Dans ce cas, après avoir interrompu la requête HTTP, le système devra retourner un code erreur approprié et les éventuelles informations complémentaires.

4.8 Mise en place d'une politique de gestion de traçabilité

Dans le cadre de l'EDC les flux échangés entre les composants serveurs, l'*API Pro Santé Connectée* et le FS doivent être tracés.

		Opérateur de Service Proxy e-santé	
EXI EDC PSC 124	Le *Fournisseur de Service* DOIT mettre en œuvre une politique de traçabilité qui est décrite dans un document dédié et régulièrement mis à jour.		

Il est attendu que le FS décrive une politique de traçabilité au sein du document de conformité basée sur une analyse des risques du système et sur ses besoins métiers.

La politique doit inclure les éléments suivants :

- Les types, contenus, formats et la finalité des traces produites par le système ;
- Les règles de conservation des traces, les informations nécessaires à leur utilisation (telles que l'adresse réseau IP et le port source) et les obligations de sécurité ;
- Le périmètre des composants et opérations devant générer les traces ;

- Des éléments garantissant la sécurité, la conservation des journaux d'audit et la traçabilité de ses données de journalisation. En particulier il est attendu :
    - Une journalisation d'un identifiant de corrélation entre le *Logiciel Utilisateur* et le *Proxy e-Santé*, permettant ainsi la traçabilité de la session de communication entre le *Logiciel Utilisateur* et le *Proxy e-Santé ;*
    - Une journalisation du paramètre SID, défini par la fondation OpenID Connect, comme correspondant à l'identifiant de corrélation dans le jeton d'accès fourni par le système PSC, permettant ainsi la traçabilité de la session de communication entre le *Proxy e-Santé* et le système PSC ;
- Le processus établissant les rôles et responsabilités du personnel en charge de la gestion de traces produites par le système PSC.

La politique doit préciser les règles suivantes :

- Une trace doit comporter toute information utile à son exploitation et ne pas comporter de secret de sécurité en clair ou d'information de nature confidentielle (comme cela est le cas des données liées à la sécurité du système ou des données à caractère personnelles) ;
- A titre d'exception, la trace peut comporter des informations limitées d'identification permettant d'identifier les personnes physiques liées au mésusage ;
- Une trace générée doit être facilement accessible à tout outil de collecte de traces mis en place à des fins d'alerte ou d'analyse ;
- Les sous-systèmes qui assurent la gestion des traces sont considérés comme étant des sous-systèmes sensibles. Les exigences définies dans ce document comme applicables aux sous-systèmes sensibles devront leurs être appliquées ;
- Les traces relatives aux activités des utilisateurs doivent être accessibles par les personnes qui y sont autorisées par la structure utilisatrice, et ce de manière autonome, interactive et en flux pour une récupération en temps réel ou différé ;
- Les traces sont conservées au minimum 1 an et respectent le RGPD.

Sur demande peut être fourni la liste des personnes habilitées à consulter les traces, le détail de leur profil au sein de l'entreprise ainsi que l'historique des identités des personnes habilitées.

			Éditeur de Logiciel Proxy e-santé
EXI EDC PSC 125	Le *Fournisseur de Service* DOIT inclure au minimum dans ses traces la date, l'heure, l'IP, le port, l'ID de session et le paramètre SID.		

Il est attendu que les événements de sécurité côté serveur soient journalisés (avec à minima l'authentification erronée, le refus d'accès à une ressource, l'obtention de jeton, le renouvellement etc.).

Tous les événements de sécurité, et plus particulièrement toutes les tentatives d'authentification à PSC ou à une *API Pro Santé Connectée* par un utilisateur, seront enregistrées avec au moins, pour chaque événement d'authentification : un horodatage en UTC, issu d'une source de temps fiable, et un élément permettant d'identifier la source de la tentative telle qu'une adresse IP locale.

Dans le cas où une trace doit être produite mais que certains éléments comme le SID ne sont pas définis car l'utilisateur ne s'est pas encore authentifié auprès de PSC, il n'est pas attendu que ces éléments non définis fassent partie des traces.

Sauf exception justifiée liée à la réglementation, aucun secret n'est journalisé par défaut. Dans le cas contraire, la confidentialité des données doit être garantie dans les traces (hash, etc.)

			Éditeur de Logiciel Proxy e-santé
RECO EDC PSC 135	Le *Fournisseur de Service* DEVRAIT inclure dans ses traces l'action réalisée par l'utilisateur, le résultat, la sensibilité de l'action et des données manipulées définies par leur importance métier.		

Cette recommandation complète l'exigence précédente, dans le cas où il est possible pour le *Logiciel Proxy e-Santé* d'accéder à des informations détaillées sur les actions métier de l'utilisateur. Il est alors attendu que les traces incluent dans une certaine mesure ces informations pour faciliter la corrélation entre une session réseau et le contenu des échanges de ladite session.

		Opérateur de Service Proxy e-santé	
EXI EDC PSC 126	Le *Fournisseur de Service* DOIT pouvoir fournir à l'*Agence du Numérique en Santé* les données de journalisation, pour une durée d'au moins un an, d'authentification et d'octroi d'accès aux ressources protégées par Pro Santé Connect.		

4.9 Bonnes pratiques de développement logiciel sécurisés

Cette section concerne l'engagement du FS à se mettre en conformité vis-à-vis des publications de l'*Open Web Application Security Project* (OWASP) en matière de sécurité des applications web.

Opérateur de Service Utilisateur	**Éditeur de Logiciel Utilisateur**	**Opérateur de Service Proxy e-santé**	**Éditeur de Logiciel Proxy e-santé**
RECO EDC PSC 136	Le *Fournisseur de Service* DEVRAIT se conformer à la publication "OWASP Top 10" et à la publication "FAPI 2.0 Security Profile" publiée par l'OpenID Foundation (OIDF) à chaque fois qu'il est concerné.		

A court terme, lors des vérifications, le système devrait atteindre au moins le niveau 1 spécifié par le standard ASVS publié par l'OWASP puis le niveau 2 à moyen ou long terme.

Concernant l'OWASP Top 10, il faudra prendre en compte à la fois la publication relative aux applications Web mais aussi les API. Le FS devra se renseigner sur les risques qui lui sont applicables et, à minima considérer les mesures de mitigation de risques qui seraient pertinentes pour sa situation.

Opérateur de Service Utilisateur	**Éditeur de Logiciel Utilisateur**	**Opérateur de Service Proxy e-santé**	**Éditeur de Logiciel Proxy e-santé**
EXI EDC PSC 127	Le *Fournisseur de Service* DOIT documenter toutes les mesures prises pour se conformer à la publication "OWASP Top 10" à chaque fois qu'il est concerné.		

Cette documentation sera incluse dans le document de conformité.

Dans le cas où une mesure ne peut pas être mise en œuvre, il est attendu que le document prenne en compte les justifications, les risques qui en découlent ainsi que les mesures palliatives proposées.

4.10 Contractualisation avec l'ensemble de la chaîne des éditeurs

Cette section aborde le devoir de formaliser un accord avec les sous-traitants dans le cadre de l'utilisation de PSC du FS.

Opérateur de Service Utilisateur		**Opérateur de Service Proxy e-santé**	
EXI EDC PSC 128	Le *Fournisseur de Service* DOIT inclure dans ses contrats avec ses sous-traitants impactant le service, une clause d'engagement de respect des versions actuelles du *Référentiel Communauté Pro Santé Connect – Extension Espace de Confiance* et des Conditions Générales d'Utilisation Pro Santé Connect.		

La liste des caractéristiques des sous-traitants a été détaillée par la Commission Nationale de l'Informatique et des Libertés.

4.11 Sécurité du système

La sécurité du système sera justifiée et maintenue à jour dans le plan d'assurance sécurité ainsi que par les résultats des futurs tests d'intrusions et plan de continuité d'activité effectuées.

	Éditeur de Logiciel Utilisateur		**Éditeur de Logiciel Proxy e-santé**
EXI EDC PSC 129	Le *Fournisseur de Service* DOIT maintenir à jour un plan d'assurance sécurité.		

Il est attendu du Plan d'Assurance Sécurité (PAS) qu'il spécifie l'ensemble des mesures permettant un hébergement et un traitement sécurisé du système chez un opérateur externe. Ce PAS devra être fourni dans le document de conformité.

Il doit inclure les éléments suivants :

- Les paramètres système devant obligatoirement être positionnés à certaines valeurs, les services annexes, les composants requis sur le système et ne devant pas être désactivés ou supprimés lors des opérations de durcissement ;
- Les mesures et procédures de sécurité retenues et mises en place pour protéger le système hébergé (ex : contrôles d'accès, la protection des données, etc.) ;
- Les résultats de l'analyse de risque et les retours d'expérience d'incident sous forme de compte rendu ;
- Les références légales, règlementations contractuelles liées à l'hébergement du système avec les responsabilités et droits des parties impliquées ;
- Les engagements entre l'hébergeur et la structure utilisatrice notamment des garanties de disponibilité, des délais de réponse en cas de problème, des mesures de résilience en cas de panne, etc ;
- L'environnement technique et opérationnel dans lequel le système doit être déployé (ex : configuration réseau, connectivité, etc.).

Il est attendu que le PAS (notamment les exigences et mesures de sécurité) soit mis à jour à chaque évolution majeure du produit grâce aux résultats d'analyse de risques ou de retours d'expérience d'incident.

Opérateur de Service Utilisateur		**Opérateur de Service Proxy e-santé**	

EXI EDC PSC 130	Le *Fournisseur de Service* DOIT appliquer le plan d'assurance sécurité.

	Éditeur de Logiciel Utilisateur		**Éditeur de Logiciel Proxy e-santé**
EXI EDC PSC 131	Le *Fournisseur de Service* DOIT faire réaliser par un auditeur d'un organisme qualifié PASSI, à intervalles réguliers, le test d'intrusion défini par l'*Agence du Numérique en Santé*.		

Il est attendu que le FS maintienne à jour le test d'intrusion par un auditeur d'un organisme qualifié PASSI, c'est-à-dire qu'il soit renouvelé avant chaque expiration des certificats, conformément aux préconisations de l'ANS.

Ce test d'intrusion permettra de vérifier le bon respect de certaines des exigences de ce présent référentiel et son résultat sera demandé dans le parcours de raccordement à PSC.

Opérateur de Service Utilisateur		**Opérateur de Service Proxy e-santé**	
RECO EDC PSC 137	Le *Fournisseur de Service* DEVRAIT tester régulièrement un Plan de Continuité d'Activité et le maintenir à jour.		

Le Plan de Continuité d'Activité doit être revu régulièrement (i.e. a minima annuellement) et être mis à jour à chaque évolution majeure du produit grâce aux résultats d'analyse de risques ou de retours d'expérience d'incident.
L'ANS prévoit dans de futures versions du présent référentiel que certaines recommandations puissent devenir des exigences. Ces changements feront l'objet des modalités de publication d'un nouveau référentiel.

5 GLOSSAIRE

ANS	Agence du Numérique en Santé
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API Pro Santé Connectée	Interface de Programmation d'Application référencée dans PSC
ASVS	Application Security Verification Standard
BAS	Bac À Sable
CIBA	Client Initiated Backchannel Authentication
CI-SIS	Cadre d'Interopérabilité des Systèmes d'Information de Santé
CGU	Conditions Générales d'Utilisation
DN	Distinguished Name
EDC	Espace De Confiance
eIDAS	electronic IDentification, Authentication and trust Services
Endpoint	Point d'entrée
ESMS	Etablissements et Services Médico-Sociaux
FAPI	Financial-Grade API
FD	Fournisseur de Données
FS	Fournisseur de Service
HDS	Hébergeur de Données de Santé
HTTP	HyperText Transmission Protocol
HTTPS	HyperText Transmission Protocol Secure
IGC-Santé	Infrastructure de Gestion de la Confiance du secteur santé-social
IP	Internet Protocol
JSON	JavaScript Object Notation
JWS	JSON Web Signature
MOS-NOS	Modèle et Nomenclature des Objets de Santé
mTLS	mutual Transport Layer Security
OIDC	OpenID Connect
OIDF	OpenID Foundation

OpS	Opérateur de Service
OWASP	Open Web Application Security Project
PAS	Plan d'Assurance Sécurité
PASSI	Prestataire d'Audit de la Sécurité des Systèmes d'Information
PGSSI-S	Politique Générale de Sécurité du Système d'Information de Santé
PS	Professionnel de Santé
PSC	Pro Santé Connect
REST	REpresentational State Transfer
RFC	Request For Comments
RGPD	Règlement Général sur la Protection des Données
RPPS	Répertoire Partagé des Professionnels de Santé
RGS	Référentiel Général de Sécurité
SID	Session ID (paramètre tel que défini par la fondation Open ID Connect)
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UTC	Universal Time Coordinated
WAF	Web Application Firewall