

Pro Santé Connect

Référentiel PSC

Statut : Validé | Classification : Publique | Version : 1.8.4



Historique du document

Version	Date de publication	Motif et nature de la modification
1.8	Juin 2021	- Création du document
1.8.4	Avril 2022	<ul style="list-style-type: none"> - Ajout de la notion de Fournisseur de Données ainsi que sa portée ; - [EXI PSC 05] Mention du respect de la loi du 6 janvier 1978 dite « Informatique et Libertés » ; - [EXI PSC 11] Besoin de rafraîchissement du jeton PSC uniquement lorsque l'utilisateur est actif ; - [EXI PSC 31] Mise à jour du paragraphe « Identification électronique par Pro Santé Connect » ; - [EXI PSC 32] Ajout d'une exigence de nécessité de déconnexion automatique de l'utilisateur du service suite à une période d'inactivité ; - [EXI PSC 33] Ajout d'une exigence de nécessité de maintien de la conformité des FS/FD suite aux évolutions techniques de PSC ; - [RECO PSC 05] Ajout d'une recommandation de blocage des utilisateurs indéclicats ; - [RECO PSC 06] Ajout d'une recommandation de déconnexion de l'utilisateur du service lors de la fermeture du navigateur ; - Correction de coquilles et mise à jour des liens expirés.

SOMMAIRE

1	Pro Santé Connect	3
1.1	Qu'est-ce que PSC ?	3
1.2	Qu'est-ce qu'un Fournisseur de service et un Fournisseur de données ?	3
1.3	Documentation et liens utiles	4
2	Le référentiel PSC.....	5
2.1	Objet du référentiel.....	5
2.2	Destinataires du document	5
2.3	Portée des exigences et recommandations du référentiel	5
2.4	Eligibilité à PSC et procédure de candidature	7
2.5	Modalités de raccordement technique.....	8
2.6	Bac à Sable	9
2.7	Production.....	9
2.8	Paramétrage des requêtes.....	10
2.9	Utilisation des données du jeton	10
2.10	Gestion et fusion des comptes avec d'autres systèmes d'authentification électronique	12
2.11	Déconnexion	12
2.12	Sécurité.....	13
2.13	Identité visuelle.....	14
3	Glossaire	16

EXI PSC XX	L'ensemble des exigences du référentiel est identifiable par un encadré gris
-------------------	--

Il est à noter que la numérotation des exigences du référentiel PSC 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 PRO SANTE CONNECT

1.1 Qu'est-ce que PSC ?

Pro Santé Connect (PSC) est le fédérateur d'identités 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 santé, en pouvant passer de l'un à l'autre de manière particulièrement fluide.

Ces derniers peuvent implémenter gratuitement 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 leur garantissant une conformité réglementaire sur le niveau de garantie de l'identification électronique de leurs usagers professionnels ;
- Un engagement de leurs utilisateurs, familiers de ce mode d'identification électronique communs à de nombreux services ;
- De récupérer les attributs de l'identité sectorielle (profession, savoir-faire, situation d'exercice, ...) ce qui leur permet notamment :
 - o De les référencer dans leur version la plus récente, en certifiant au passage l'identité professionnelle nationale dans le compte de l'utilisateur professionnel de leur service ;
 - o D'automatiser leur contrôle d'accès sur certains attributs professionnels (profession, activités, etc.) ;
- L'échange de données entre fournisseurs de données et fournisseurs de service, au travers des interfaces de programmation d'application (API) Pro Santé Connectées.

À compter du 1er janvier 2023, l'implémentation de PSC sera obligatoire pour les services numériques en santé nationaux, territoriaux, ainsi que pour les services locaux qui y sont fortement intégrés.

PSC a fait l'objet d'une homologation 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. L'hébergement est assuré par un Organisme d'Importance Vitale qui est en mesure d'apporter les réponses à cette contrainte aussi bien en ce qui concerne l'architecture technique qu'au niveau organisationnel.

1.2 Qu'est-ce qu'un Fournisseur de service et un Fournisseur de données ?

Par Fournisseur de Service (FS) est désignée toute personne morale immatriculée dans l'Union européenne, fournissant un service numérique à des utilisateurs professionnels intervenant dans les secteurs sanitaire, médico-social et social, et habilitée à utiliser Pro Santé Connect conformément aux CGU.

Par Fournisseur de Données (FD) est désignée toute personne morale immatriculée dans l'Union européenne, fournissant à des FS, via un mécanisme impliquant Pro Santé Connect, des données supplémentaires à celles du jeton Pro Santé Connect, relatives à des utilisateurs professionnels intervenant dans les secteurs sanitaire, médico-social et social, et habilitée à utiliser Pro Santé Connect conformément aux CGU.

1.3 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://api.gouv.fr/les-api/api-pro-sante-connect
Référentiels PGSSI-S sur l'identification électronique	https://esante.gouv.fr/offres-services/pgssi-s/espace-de-publication
Référentiel d'interopérabilité	https://esante.gouv.fr/services/referentiels/ci-sis/espace-publication/couche-transport
MOS/NOS	https://esante.gouv.fr/interopabilite/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

2 LE REFERENTIEL PSC

2.1 Objet du référentiel

Le référentiel PSC décrit les exigences à respecter et apporte des préconisations pour un fournisseur de service (FS) ou un fournisseur de données (FD) souhaitant implémenter PSC.

2.2 Destinataires du document

Le référentiel PSC s'adresse aux FS et aux FD voulant implémenter le fédérateur de moyens d'identité électroniques PSC.

2.3 Portée des exigences et recommandations du référentiel

EXIGENCE	Applicable aux FS	Applicable aux 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

EXIGENCE	Applicable aux FS	Applicable aux FD
EXI PSC 19	Oui	Non
EXI PSC 20	Oui	Non
EXI PSC 21	Oui	Oui
EXI PSC 22	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
RECO PSC 01	Oui	Oui
RECO PSC 02	Oui	Oui
RECO PSC 03	Oui	Non
RECO PSC 04	Oui	Non
RECO PSC 05	Oui	Oui
RECO PSC 06	Oui	Non

2.4 Eligibilité à PSC et procédure de candidature

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

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
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
EXI PSC 03	Le service DOIT être proposé en langue française
EXI PSC 04	Le service DOIT proposer à des utilisateurs professionnels intervenant dans les secteurs sanitaire, médico-social et social, des fonctionnalités qui nécessitent leur identification électronique
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
EXI PSC 06	Le service DOIT, lorsqu'il traite de données de santé, assurer leur confidentialité et leur intégrité, tout en assurant leur hébergement par un hébergeur agréé ou certifié 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 professionnels 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 ;
- Fournir 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'ANS¹ et de l'application mobile e-CPS listant les FS raccordés à PSC. Cette mention est obligatoire pour implémenter le service PSC ;
- Fournir une adresse générique du délégué à la protection des données du FS, ainsi que le nom actuel du titulaire du poste ;
- Fournir une adresse générique du contact opérationnel pour tout besoin d'échange entre le FS et PSC, ainsi que le nom actuel du titulaire du poste.

EXI PSC 07	Le Fournisseur de Service DOIT prévenir l'ANS 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
-------------------	--

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.

2.5 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.

Le protocole OpenID Connect (OIDC)² est au cœur du fonctionnement de PSC. C'est une surcouche d'identification au protocole OAuth 2.0³. Il permet à des Clients (ici, les FS) d'accéder à l'identité des utilisateurs finaux (les professionnels intervenant en santé) 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.

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](#).

RECO PSC 01	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.

EXI PSC 09	Le Fournisseur de Service DOIT respecter les flux standards OpenID
-------------------	--

PSC implémente [le flux standard OpenID « flux code d'autorisation »](#). Lorsque le professionnel de santé 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 son client id et son url de redirection. PSC redirige alors le professionnel intervenant en santé 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 son client id et son client secret. 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.

¹ <https://esante.gouv.fr/securite/e-cps/services-raccordes-a-pro-sante-connect>

² <https://openid.net/connect/>

³ <https://oauth.net/2/>

Au cours de l'année 2022, PSC implémentera le flux OpenID "Client Initiated Backchannel Authentication" (CIBA).

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.

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
-------------------	--

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

2.6 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.

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
-------------------	---

EXI PSC 13	Le Fournisseur de Service DOIT donner accès à l'ANS à son service de test
-------------------	---

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

2.7 Production

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

EXI PSC 14	Le Fournisseur de Service DOIT contacter les endpoints de Pro Santé Connect Production
-------------------	--

2.8 Paramétrage des requêtes

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"⁴ 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).

EXI PSC 16	Le Fournisseur de Service DOIT utiliser le paramètre acr_values lors de la demande d'authentification avec la valeur «eidas1»
-------------------	---

PSC propose au FS un ensemble d'informations professionnelles de référence sur l'utilisateur identifié électroniquement. Afin de simplifier son usage par un FS, PSC propose ces traits dans un scope : scope_all

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

EXI PSC 17	Le Fournisseur de Service DOIT paramétrer ses requêtes d'autorisation avec les scopes "openid" et "scope_all"
-------------------	---

2.9 Utilisation des données du jeton

L'identité du professionnel intervenant en santé fournie dans scope_all est issue du répertoire sectoriel de référence RPPS. Chaque professionnel y est enregistré avec un identifiant national unique, l'idNat_PS⁵, 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).

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 professionnels. 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 dernières peuvent par exemple être gérées par des administrateurs locaux ou les personnes

⁴ https://openid.net/specs/openid-connect-basic-1_0.html#RequestParameters

⁵ https://mos.esante.gouv.fr/2.html#_8f7f21e6-0c8e-44f4-b77d-35c58b2e12cf

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.

RECO PSC 02	Le Fournisseur de Service PEUT 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 MOS⁶/NOS 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 indécents.

RECO PSC 05	Le Fournisseur de Service PEUT mettre en place un mécanisme de blocage des utilisateurs indécents
--------------------	---

⁶ <https://mos.esante.gouv.fr/>

2.10 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.

RECO PSC 03	Le Fournisseur de Service PEUT utiliser d'autres systèmes d'identification électronique que Pro Santé Connect, notamment pour permettre à des utilisateurs professionnels non encore enregistrés au RPPS d'accéder au service, et/ou de palier à des indisponibilités de Pro Santé Connect ou de connexion réseau
--------------------	---

EXI PSC 19	Le Fournisseur de Service DOIT alors fusionner ses comptes autour de l'identifiant pivot RPPS, afin de permettre à ses utilisateurs de ne garder qu'un seul compte dans l'outil, quel que soit leur modalité de connexion
-------------------	---

RECO PSC 04	Pour les cas où la gestion du compte utilisateur ne disposaient pas auparavant du numéro RPPS enregistré, le Fournisseur de Service PEUT demander à l'utilisateur final de se connecter avec Pro Santé Connect et une des autres modalités de connexion disponibles successivement afin d'effectuer l'appariement autour de l'identifiant pivot RPPS
--------------------	--

L'identifiant Adeli peut également être utilisé en transitoire pour les professionnels qui n'ont pas encore migré sur un identifiant RPPS.

2.11 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 Connect⁷. 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.

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.

RECO PSC 06	Le Fournisseur de Service PEUT 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 session⁸.

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.

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
-------------------	---

2.12 Sécurité

Après approbation d'une demande de raccordement par PSC, un *client ID* et un *Secret* sont fournis au FS afin qu'il puisse communiquer avec PSC.

EXI PSC 21	Le Fournisseur de Service DOIT utiliser les informations de raccordement : client ID et Secret fournis par Pro Santé Connect
-------------------	--

Pour des questions de sécurité, le client ID et le Secret ne doivent jamais être localisé sur l'appareil de l'utilisateur final.

EXI PSC 22	Le Fournisseur de Service DOIT conserver le client ID et le Secret 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.

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-Santé⁹. Un certificat de l'IGC-Santé peut être obtenu en utilisant la Plateforme IGC-Santé (<https://pfc.eservices.esante.gouv.fr/>).

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 considérés dans le cadre de référentiel PSC comme des clients lourds.

⁷ http://openid.net/specs/openid-connect-session-1_0.html#RPLLogout

⁸ <https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/documentation-technique>

⁹ <https://industriels.esante.gouv.fr/produits-et-services/igc-sante-certificats-personnes-morales-et-serveurs>

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

L'utilisation de composants tels que les "webviews" (visualisation du navigateur web dans une application) n'est pas suffisamment sécurisée.

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.

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-S¹⁰.

EXI PSC 33	Le Fournisseur de Service DOIT se maintenir conforme aux préconisations sécuritaires du service Pro Santé Connect prononcées et signifiées par l'ANS auprès du responsable technique du Fournisseur de Service
-------------------	--

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.

EXI PSC 27	Le Fournisseur de Service DOIT prévenir l'ANS sous 12h en cas de détection d'un incident de sécurité et/ou impliquant une violation de données à caractère personnel
-------------------	--

2.13 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 connexions 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.

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 professionnels
-------------------	---

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>).

¹⁰ <https://esante.gouv.fr/offres-services/pgssi-s/espace-de-publication>

EXI PSC 29	Le Fournisseur de Service DOIT utiliser l'un des éléments graphiques fournis par Pro Santé Connect pour l'intégration Pro Santé Connect conformément à la charte graphique de l'ANS
EXI PSC 30	Le Fournisseur de Service DOIT respecter la charte graphique Pro Santé Connect
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 son application mobile e-CPS ou sa carte CPS, avec un lecteur de cartes et les composants nécessaires.

3 GLOSSAIRE

ANS	Agence du Numérique en Santé
API PSCconnectée	Interface de Programmation d'Application référencée dans PSC
CIBA	Client Initiated Backchannel Authentication
CGU	Conditions Générales d'Utilisation
Endpoint	Point d'entrée
FD	Fournisseur de Données
FS	Fournisseur de Service
JSON	JavaScript Object Notation
PGSSI-S	Politique Générale de Sécurité du Système d'Information de Santé
PS	Professionnel de Santé
PSC	Pro Santé Connect
REST	REpresentational State Transfer
RPPS	Répertoire Partagé des Professionnels de Santé