AGENCE
DU NUMÉRIQUE
EN SANTÉ

Pro Santé Connect

Référentiel PSC

Statut : Concertation | Classification : Restreinte | Version : 1.5

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

SOMMAIRE

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

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 professionnels pour en faire la vérification et éventuellement automatiser leur contrôle d'accès sur cette base.

À compter du 1er janvier 2022, 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 Documentation et liens utiles

Documentation juridique	Article L.1470-3 : https://www.dalloz-actualite.fr/sites/dallozactualite.fr/files/resources/2021/05/2021-581.pdf 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
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://integrateurs-cps.asipsante.fr/pages/prosanteconnect/documentation-fs
Conditions Générales d'Utilisation de PSC	https://integrateurs-cps.asipsante.fr/pages/prosanteconnect/cgu

Chartre graphique de PSC	https://integrateurs-cps.asipsante.fr/pages/charte-graphique-psc
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/

2 LE REFERENTIEL PSC

2.1 Objet du référentiel

Le référentiel PSC, décrit les exigences à respecter pour un fournisseur de service (FS) souhaitant implémenter PSC, en apportant certaines préconisations.

Le présent document a vocation à être publié pour concertation sur la plateforme participez.esante.gouv.fr du 31 mai au 11 juin 2021, et à être rendu opposable réglementairement.

2.2 Destinataires du document

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

2.3 Eligibilité à PSC et procédure de candidature

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

EX 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

EX PSC 02	Le service DOIT être proposé en langue française

EX PSC 03	Le service DOIT proposer à des utilisateurs professionnels intervenant dans les secteurs sanitaires, médico-social et social des fonctionnalités qui nécessitent leur identification électronique

EX PSC 04	Le service DOIT respecter le règlement général sur la protection des données (RGPD) et en particulier en ce qui concerne l'information des utilisateurs professionnels

EX PSC 05	Le service DOIT, lorsqu'il traite de données de santé, assurer leur confidentialité et leur intégrité, tout en assurant leur hébergement dans des infrastructures certifiées à cet effet

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 ;
- 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 l'ANS[1] et de l'application mobile e-CPS listant les FS raccordés à PSC. Cette mention est obligatoire pour implémenter le service PSC ;

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

- 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.

EX PSC 06	Le service DOIT prévenir Pro Santé Connect en cas de changement dans les informations qui ont été déclarées à Pro Santé Connect en vue à la candidature au raccordement

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.

2.4 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.

EX PSC 07	Le Fournisseur de Service DOIT être client OpenID Connect

La liste des implémentations certifiées par la fondation OpenID Connect est disponible ici.

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.

EX PSC 08	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

[2] https://openid.net/connect/
[3] https://oauth.net/2/

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.
- Prochainement, PSC implémentera le flux OpenID "Client Initiated Backchannel Authentication" (CIBA).

EX PSC 09	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.

EX PSC 10	Le Fournisseur de Service DOIT rafraichir les informations d'authentification auprès de Pro Santé Connect tant que l'utilisateur utilise son service

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

2.5 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.

EX PSC 11	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

EX PSC 12	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.

2.6 Production

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

EX PSC 13	Le Fournisseur de Service DOIT contacter les endpoints de Pro Santé Connect Production

2.7 Paramétrage des requêtes

EX PSC 14	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).

EX PSC 15	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.

EX PSC 16	Le Fournisseur de Service DOIT paramétrer ses requêtes d'autorisation avec les scopes "openid" et "scope_all"

2.8 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_PS[5], 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).

EX PSC 17	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

Un service gère ses autorisations d'accès sous sa propre responsabilité, en conformité avec les référentiels de sécurité existant sur ce sujet.

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.)

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[6]/NOS utilisée par l'ANS et véhiculée dans le scope_all.

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

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

Un FS dispose généralement de systèmes d'identification électroniques préexistants à PSC. Il peut les maintenir s'ils sont conformes aux référentiels de sécurité. 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

EX PSC 18	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

2.10 Déconnexion

PSC ne gère pas la déconnexion de l'usager au service PSC à la fermeture du navigateur.

En revanche, PSC implémente la section sur la déconnexion en cours de spécification dans la norme OpenID Connect[7]. 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.

EX PSC 19	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

2.11 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.

EX PSC 20	Le Fournisseur de Service DOIT utiliser les informations de raccordement : client ID et Secret fournis par Pro Santé Connect

[7] http://openid.net/specs/openid-connect-session-1_0.html#RPLogout

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

EX PSC 21	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.

EX PSC 22	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 SERV_SSL_SERV de l'IGC-Santé[8]. Un certificat de l'IGC-Santé peut être obtenu en utilisant la Plateforme IGC-Santé (https://pfc.eservices.esante.gouv.fr/).

EX PSC 23	Le Fournisseur de Service DOIT communiquer avec Pro Santé Connect via une connexion sécurisée au minimum via TLS 1.2 par un certificat SERV_SSL_SERV 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.

PSC permet aux FS client lourds de se raccorder en flux de redirection web, comme méthode alternative à l'utilisation du flux CIBA.

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

EX PSC 24	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.

EX PSC 25	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

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

EX PSC 26	Le Fournisseur de Service DOIT prévenir l'ANS sous 12h en cas de détection d'un incident de sécurité

2.12 Identité visuelle

[8] https://integrateurs-cps.asipsante.fr/IGC-Sante

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.

EX PSC 27	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://integrateurs-cps.asipsante.fr/pages/charte-graphique-psc).

EX PSC 28	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

EX PSC 29	Le Fournisseur de Service DOIT respecter la charte graphique Pro Santé Connect

EX PSC 30	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.

Consulter les conditions générales d'utilisation de Pro Santé Connect sur le site https://integrateurs-cps.asipsante.fr/pages/prosanteconnect/cgu.

3 GLOSSAIRE

ANS	Agence du Numérique en Santé
PSC	Pro Santé Connect
RPPS	Répertoire Partagé des Professionnels de Santé
FS	Fournisseur de Service
PS	Professionnel de Santé
Endpoint	Point d'entrée
CIBA	Client Initiated Backchannel Authentication
JSON	JavaScript Object Notation
REST	REpresentational State Transfer
CGU	Conditions Générales d'Utilisation