

Agence du Numérique en Santé

2-10 Rue d'Oradour-sur-Glane – 75015 Paris

T. 01 58 45 32 50

esante.gouv.fr

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Pro Santé Connect | | | | |
| Document de conformité – [nom du Fournisseur de Service – Numéro d’habilitation] | | | | |
| Statut : En cours | | | Classification : Publique | | | Version :1.0 |

Historique du document

| **Version** | **Date de publication** | **Motif et nature de la modification** |
| --- | --- | --- |
| **0.1** | Juin 2024 | * Création du document |

**SOMMAIRE**

[1 Description du document de conformité 4](#_Toc165970163)

[1.1 Rappel 4](#_Toc165970164)

[1.2 Qu’est-ce que le document de conformité ? 4](#_Toc165970165)

[1.3 Attendus vis-à-vis des Editeurs de Logiciel et Fournisseurs de Services 4](#_Toc165970166)

[1.4 Documentation et liens utiles 6](#_Toc165970167)

[2 Structure du document 8](#_Toc165970168)

[2.1 Architecture 8](#_Toc165970169)

[2.1.1 Obligations 8](#_Toc165970170)

[2.1.2 Règles de développement 8](#_Toc165970171)

[2.2 Dispositifs et éléments de configuration 9](#_Toc165970172)

[2.2.1 Inventaire 9](#_Toc165970173)

[2.2.2 Configuration 9](#_Toc165970174)

[2.3 Établissement de session 9](#_Toc165970175)

[2.3.1 Protocoles de communication / Flux 9](#_Toc165970176)

[2.3.2 Conformité aux standards 10](#_Toc165970177)

[2.3.3 Gestion des identifiants 12](#_Toc165970178)

[2.4 Mécanismes cryptographiques 13](#_Toc165970179)

[2.4.1 Conformité règlementaire 13](#_Toc165970180)

[2.4.2 Chiffrement 13](#_Toc165970181)

[2.4.3 Gestion des secrets 13](#_Toc165970182)

[2.4.4 Gestion des jetons 14](#_Toc165970183)

[2.5 Filtrage et alertes 15](#_Toc165970184)

[2.5.1 Filtrage de flux 15](#_Toc165970185)

[2.5.2 Procédure de traitement des alertes 15](#_Toc165970186)

[2.6 Politique de traçabilité 16](#_Toc165970187)

[2.7 Plan d’assurance sécurité 17](#_Toc165970188)

[2.8 Intégration de la sécurité dans le logiciel 18](#_Toc165970189)

[2.8.1 Analyse de risque 18](#_Toc165970190)

[2.8.2 Test d’intrusion 19](#_Toc165970191)

[2.9 Mises à jour 20](#_Toc165970192)

[3 Glossaire 21](#_Toc165970193)

# Description du document de conformité

## Rappel

Pour rappel, le référentiel *Communauté PSC - Extension Espace de* Confiance est le référentiel décrivant les exigences à respecter et apportant des préconisations pour un Fournisseur de Service (FS) et un Editeur de Logiciel souhaitant implémenter l’appel à une API Pro Santé Connectée.

Bien que ce document de conformité ne soit pas directement associé au référentiel d'exigences, il servira de référence pour le *Fournisseur de Service* et l'*Editeur de Logiciel* dans l'élaboration de ce livrable. En revanche, le *Fournisseur de Service* et l’*Editeur de Logiciel* devront s’appuyer sur le référentiel pour la rédaction de ce livrable.

## Qu’est-ce que le document de conformité ?

Le document de conformité est un guide rédigé par les *Editeurs de Logiciel* à destination des *Fournisseurs de Service*. Par conséquent, il est attendu que *l’Editeur de Logiciel* partage ce document prérempli au *Fournisseur de Service*, ainsi qu'à l'*ANS* pour contrôle, puis le *Fournisseur de Service* devra à son tour compléter le document de conformité et le rendre à *l’ANS*.

Ce document a pour objectif de rassembler toute information relative à l’exploitation du système fourni par l’*Editeur de Logiciel* notamment le paramétrage ou la configuration du système par défaut, son fonctionnement et son utilisation ainsi que les préconisations à adopter pour assurer une utilisation fiable, optimisée et sécurisée chez le Fournisseur de Service.

De plus, ce document permettra à l’ANS d’évaluer le *Fournisseur de Service* et plus précisément la mise en conformité de son système vis-à-vis des différents documents introduits par *l’ANS*.

Il est obligatoire d’utiliser ce modèle de document de conformité, mais il est possible de référer à des documents annexes dans les différentes zones de texte à remplir de ce document.

## Attendus vis-à-vis des Editeurs de Logiciel et Fournisseurs de Services

Il est de la responsabilité des *Editeurs de Logiciel* et *Fournisseurs de Service* de remplir ce document de conformité. Toutes les informations et les illustrations feront l’objet de points de contrôles de l’Agence du Numérique en Santé. Des zones de texte grises ont été placées à cet effet dans chaque section de la partie [Structure du document](#_Structure_du_document).

Le rôle de l’*Editeur de Logiciel* est de préremplir et préciser toute information pertinente telle que des bonnes pratiques de développement et des conseils de configuration du système fourni. L’*Editeur de Logiciel* sera ainsi apte à démontrer sa conformité et expliquer l’architecture sélectionnée ainsi que les prérequis en matière de sécurité grâce à des schémas d’architecture, justifications des choix de composants, préconisations etc.

Concernant le *Fournisseur de Service*, ce dernier doit reprendre ce document prérempli par l’*Editeur de Logiciel* et le compléter avec ses propres informations concernant les implémentations, infrastructures, solutions choisies etc. *L’ANS*, ou tout autre tiers désigné par cette dernière, se réserve le droit d’évaluer le niveau de conformité du Fournisseur de Service à partir des informations et justifications fournies.

Pour illustration, les zones de textes à remplir sont indiquées comme il suit :

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC XXX** | | | |
|  | **Editeur de Logiciel Utilisateur** |  |  |
| *[Il est attendu que le Fournisseur de Service supprime les instructions présentes dans chaque champ de texte ainsi grisé de ce document, à l'exception de cet exemple, puis les remplisse conformément aux dites instructions*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

Pour cet exemple de portée :

* Le document de conformité fourni par l’*Editeur de Logiciel Utilisateur* à l’ANS et à son (ses) *Fournisseur(s) de Service Utilisateur* devra avoir le champ de texte rempli, car l’*Editeur de Logiciel Utilisateur* est responsable de prouver sa conformité à l’exigence mentionnée ;
* Le document de conformité final fourni par le *Fournisseur de Service Utilisateur* à l’ANS devra avoir le champ de texte rempli, car le *Fournisseur de Service Utilisateur* doit reprendre le document fourni par l’*Editeur de Logiciel Utilisateur,* sans modifier substantiellement ce champ de texte, qui ne le concerne pas.
* Le document de conformité fourni par l’*Editeur de Logiciel Proxy e-Santé* à l’ANS et à son (ses) *Fournisseur(s) de Service Proxy e-Santé* devra avoir le champ de texte vide, car l’exigence ne le concerne pas ;
* Le document de conformité fourni par le *Fournisseur de Service Proxy e-Santé* à l’ANS devra avoir le champ de texte vide, car l’exigence ne le concerne pas ;

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC XXX** | | | |
| **Fournisseur de Service Utilisateur** | **Editeur de Logiciel Utilisateur** | **Fournisseur de Service Proxy e-santé** | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service supprime les instructions présentes dans chaque champ de texte ainsi grisé de ce document, à l'exception de cet exemple, puis les remplisse conformément aux dites instructions*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

Pour cet exemple de portée :

* Le document de conformité fourni par l’*Editeur de Logiciel Utilisateur* à l’ANS et à son (ses) Fournisseur(s) de Service Utilisateur devra avoir le champ de texte rempli, car l’*Editeur de Logiciel Utilisateur* est responsable de prouver sa conformité à l’exigence mentionnée, sur son périmètre ;
* Le document de conformité final fourni par le *Fournisseur de Service Utilisateur* à l’ANS devra avoir le champ de texte rempli, car le *Fournisseur de Service Utilisateur* doit reprendre le document fourni par l’*Editeur de Logiciel Utilisateur,* et le compléter avec des informations permettant de prouver sa conformité sur son propre périmètre.
* Le document de conformité fourni par l’*Editeur de Logiciel Proxy e-santé* à l’ANS et à son (ses) *Fournisseur*(s) *de Service Proxy e-santé* devra avoir le champ de texte rempli, car l’*Editeur de Logiciel Proxy e-santé* est responsable de prouver sa conformité à l’exigence mentionnée, sur son périmètre ;
* Le document de conformité final fourni par le *Fournisseur de Service Proxy e-santé* à l’ANS devra avoir le champ de texte rempli, car le *Fournisseur de Service Proxy e-santé* doit reprendre le document fourni par l’*Editeur de Logiciel Proxy e-santé,* et le compléter avec des informations permettant de prouver sa conformité sur son propre périmètre.

Certaines sections peuvent requérir de la part du *Fournisseur de Service* une mention du numéro d’habilitation de *l’Editeur de Logiciel* auquel il a fait appel pour répondre à l’exigence.

Dans les prochaines sections du présent document, le terme *Fournisseur de Service* (FS) couvrira l’ensemble des notions *d’Editeur de Logiciel Utilisateur, Fournisseur de Service Utilisateur, Editeur de Logiciel**Proxy e-santé et Fournisseur de Service Proxy e-santé* pour des raisons d’uniformisation.

## 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/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> |
| Référentiel Communauté Pro Santé Connect | <https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/referentiel-psc> |
| Référentiesl Communauté et Communauté PSC extension Espace de Confiance | Lien à venir |
| Norme JWS | <https://datatracker.ietf.org/doc/html/draft-ietf-jose-json-web-signature> |
| RFC 8705 | <https://www.rfc-editor.org/rfc/rfc8705> |

# Structure du document

Les informations et explications données permettront à *l’ANS* de réaliser les points de contrôles nécessaires à l’intégration du système dans l’EDC mais aussi à son amélioration continue. La structure de ce document est divisée en plusieurs sections.

## Intégration de la sécurité dans le logiciel

Dans l’optique d’améliorer la sécurité du logiciel en continu et conformément aux [exigences 104, 105 et 130 du référentiel EDC PSC,](https://esantegouv.sharepoint.com/sites/GRP-CommunautPSC-Contractualisation/Documents%20partages/General/En%20cours-%20Fichiers%20de%20travail/En%20cours%20-%20Livrables%20éditeurs/ANS_PSC_REFERENTIEL_ESPACE_CONFIANCE_PSC_V1.1_v0.4.docx) cette section présentera les mesures prises pour sécuriser la chaîne de développement logiciel, et inclura en particulier les résultats des tests d’intrusions et analyses de risques effectuées.

### Règles de développement

En tant que FS, je dois intégrer dans mon process de développement logiciel des outils permettant de vérifier le respect des règles de développement et décrire les outils mis en place. Tout outil de qualimétrie, vérification de l’obsolescence des librairies, outils de vérification de la sécurisation de la plateforme système devraient être considérés pour adoption dans le système. Je devrais considérer la mise en place d’une revue systématique de mes codes par un autre pair, avant toute mise en production.

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 102** | | | |
|  | **Editeur de Logiciel Utilisateur** |  | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service détaille son process de développement logiciel et les outils utilisés pour auditer ce dernier.*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

Je dois également me conformer à la publication "OWASP Top 10" et documenter les mesures mises en place. Dans le cas où une mesure préconisée ne peut pas être mise en œuvre, la documentation présente une justification, explicite les risques qui en découlent et propose des mesures palliatives à l'attention des opérateurs du système.

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 127** | | | |
| **Fournisseur de Service Utilisateur** | **Editeur de Logiciel Utilisateur** | **Fournisseur de Service Proxy e-santé** | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service décrive les actions mises en place pour faire face aux risques le concernant présentés dans la dernière publication « OWASP Top 10 ». Il devra le faire à l’aide d’un tableau comprenant pour chaque risque mentionné par les standards une colonne dédiée à chaque élément suivant :*   * *La description du risque ;* * *Les mesures mises en place (pour donner suite aux recommandations du standards) ;* * *La date de mise en place ou de mise à jour ;* * *Dans le cas où les mesures ne peuvent pas être mises en place, les risques induits et acceptés ;* * *Dans le cas où les mesures ne peuvent pas être mises en place, les mesures palliatives proposées.*   *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

### Sous-traitants

Concernant les sous-traitants intervenant dans mon processus de développement logiciel, j’ai pour obligation de m’assurer que le respect du référentiel et des Conditions Générales d’Utilisation Pro Santé Connect est maintenu.

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 128** | | | |
| **Fournisseur de Service Utilisateur** |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service détaille la clause incluse dans les contrats avec les sous-traitants, engageant ces derniers à respecter les versions actuelles du référentiel et des Conditions Générales d'Utilisation Pro Santé Connect (via extrait ou une capture d’écran) ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

### Analyse de risque

À la suite des résultats de l’analyse de risques effectuée par *l’Editeur de Logiciel*, en tant que FS, j’ai l’obligation :

* D’identifier des mesures palliatives à propos de la sécurisation et le stockage des secrets ;
* D’appliquer des mesures organisationnelles et techniques renforcées de sécurisation de sécurité.

Ces mesures de mitigation peuvent prendre la forme de mécanismes de protection adaptés aux risques tels que des VPN, des communications TLS, des tunnels SSH, etc.

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 105** | | | |
|  |  |  | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service récapitule les résultats de l’analyse en présentant les risques identifiés ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira.*  *]* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 106** | | | |
|  |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service récapitule les mesures de mitigation associées aux risques identifiés à l’aide d’un tableau comprenant pour chaque risque une colonne dédiée à chaque élément suivant :*   * *La description du risque ;* * *Les mesures organisationnelles mises en place ;* * *Les mesures techniques mises en place ;* * *La date de mise en place ou de mise à jour ;*   *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira.*  *]* | | | |

### Test d’intrusion

Si le cas se présente, j’ai l’obligation d’implémenter des mesures palliatives de sécurité à la suite d’un test d’intrusion ayant relevé des failles de sécurité.

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 131** | | | |
|  | **Editeur de Logiciel Utilisateur** |  | **Editeur de Logiciel Proxy e-santé** |
| [*Il est attendu que le Fournisseur de Service récapitule les résultats du test d’intrusion en présentant les vulnérabilités identifiées et les mesures associées à l’aide d’un tableau comprenant pour chaque vulnérabilité une colonne dédiée à chaque élément suivant :*   * *La description de la vulnérabilité ;* * *Le risque associé ;* * *Les mesures mises en place ;* * *La date de mise en place ou de mise à jour ;*   *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

## Architecture

### Inventaire

En tant que FS, je m’engage à fournir à l’ANS une liste des principaux composants nécessaires au fonctionnement de mon système et des flux les reliant sous la forme d’un inventaire :

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 104** | | | |
|  | **Editeur de Logiciel Utilisateur** |  | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service fournisse un inventaire recensant l’ensemble des composants techniques y compris issus de tiers, des flux applicatifs, des requêtes, des protocoles et* des services *nécessaires à l’utilisation du système dans une version supportée à date ; et qu’il détaille sa configuration actuelle ainsi que la version des composants, la date de revue et les outils utilisés*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 102** | | | |
| **Fournisseur de Service Utilisateur** |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service détaille la liste des comptes, incluant leur type (compte générique, de service, built-in) qui sont utilisés pour exécuter les services nécessaires au bon fonctionnement du système*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

### Sécurisation de l’architecture

Par ailleurs, je m’engage à mettre en place ces composants au sein d’une architecture sécurisée, ce qui implique entre autres de :

* Mettre en place le principe de moindre privilège ;
* Activer uniquement les services essentiels à la mise en œuvre du Service Utilisateur ou Proxy e-santé ;
* Revoir régulièrement les mesures de sécurité mises en place concernant les sous-systèmes sensibles de son architecture (en particulier les serveurs de stockage dont les bases de données des clés privées et autres secrets, les systèmes servant à l’administration etc.).

|  |  |  |  |
| --- | --- | --- | --- |
| **RECO EDC PSC 132** | | | |
|  |  | **Fournisseur de Service Proxy e-santé** | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service décrive son architecture*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC 102** | | | |
| **Fournisseur de Service Utilisateur** |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service détaille la manière dont il revoit régulièrement les mesures de sécurité mises en place concernant les sous-systèmes sensibles de son architecture*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

## Dispositifs et éléments de configuration

### Configuration

En tant que FS, j’ai pour obligation de m’approprier et paramétrer à un niveau de sécurité satisfaisant toute configuration par défaut le nécessitant, et d’effectuer une revue régulière de ces configurations notamment à l’occasion des montées de version des composants.

Lorsqu’ils sont disponibles, je devrais utiliser des outils pour auditer l’ensemble des composants du système à chaque modification.

Les composants issus de tiers doivent être sélectionnés en tenant compte du respect de bonnes pratiques similaires par ces tiers.

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC 102** | | | |
| **Fournisseur de Service Utilisateur** | **Editeur de Logiciel Utilisateur** | **Fournisseur de Service Proxy e-santé** | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service détaille quels fichiers de configuration (de librairies, services, systèmes…) ont été personnalisés et quelles bonnes pratiques ont été mises en place pour garantir la sécurisation globale du système, en particulier lorsqu’il s’agit de sous-systèmes sensibles ou issus de tiers*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **RECO EDC PSC 133** | | | |
|  | **Editeur de Logiciel Utilisateur** |  | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service détaille la liste des outils* *pour auditer l’ensemble des composants du système*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

### Conformité aux standards

Les standards et spécifications auquel je dois me conformer en tant que FS quand j’intègre les technologies dont elles traitent sont présentés ci-dessous :

* [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 ;
* [RFC 7636] Proof Key for Code Exchange by OAuth Public Clients Chapitres 4.1 "Code Verifier" et 4.2 "Code Challenge".

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 102** | | | |
|  | **Editeur de Logiciel Utilisateur** |  | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service fournisse une description de l’implémentation choisie (solution prête à l'emploi, solution sur mesure etc.) pour les standards cités ci-dessus*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

## Sécurisation des communications et mécanismes cryptographiques

### Protocoles de communication / Flux

En tant que FS, je m’engage à m’assurer que toutes les communications au sein de mon système sont sécurisées au niveau adapté.

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 102** | | | |
| **Fournisseur de Service Utilisateur** |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service spécifie comment la sécurisation des communications entre les composants du système et avec les composants externes choisis est réalisée, et plus particulièrement quand ils sont logiquement ou physiquement séparés ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 102** | | | |
| **Fournisseur de Service Utilisateur** | **Editeur de Logiciel Utilisateur** | **Fournisseur de Service Proxy e-santé** | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service spécifie la liste des éventuels protocoles ou flux de communications ne pouvant pas être chiffrés ainsi que les raisons et les risques résiduels induits et acceptés ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 121** | | | |
|  |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service fournisse la liste complète des dispositifs de filtrage, de rupture de protocole et de détection d’intrusion mis en place au niveau des flux applicatifs et leurs paramétrages au sein du système ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 113** | | | |
| **Fournisseur de Service Utilisateur** |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service fournisse une description des mécanismes mis en place afin d'assurer l'association, la protection et la continuité des flux HTTP conformément aux recommandations du guide d'interconnexion d'un système d'information à internet de l'ANSSI ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

### Conformité règlementaire

Dans cette section, en tant que FS, je m’engage à ce que les algorithmes de chiffrement, de hachage, de vérification d'intégrité et d'authenticité, et plus généralement les mécanismes cryptographiques utilisés et les tailles de clés correspondantes soient conformes aux règlementations ci-dessous dans leurs dernières versions en vigueur :

* Le [RGS de l’ANSSI (en particulier les annexes B1 et B2)](https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents) ;
* Le guide des mécanismes cryptographiques ;
* Le guide de sélection d'algorithmes cryptographiques et le cas échéant les Recommandations de sécurité relatives à TLS, publiés par l'ANSSI ;
* La politique de gestion des clés cryptographiques de l’IGC-Santé publiée par l’ANS.

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 107 & 108** | | | |
| **Fournisseur de Service Utilisateur** |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service liste l’intégralité des algorithmes cryptographiques utilisés, justifie leur intégration dans le système et les versions des protocoles ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

### Chiffrement

Cette section introduit les mécanismes de chiffrement et sécurisation des communications, les certificats et les mécanismes de protection sélectionnés.

En tant que FS, je m’engage à suivre et prouver le respect des points suivants :

* Mettre en place des contrôles de traces et de certificats, à faire correspondre la partie publique du certificat à celle du certificat AUTH\_CLI de l’offre ORG de l’IGC-Santé ;
* Associer au proxy un certificat ORG\_CLI pour chaque FS Utilisateur pour lequel il réalise des authentifications mutuelles ;
* N’avoir qu’un certificat associé à un identifiant et une instance de l’application à chaque appel de l’API PSC utilisant le certificat du FS Utilisateur ;
* Ne pas adopter d’architecture considérée interdite de l'EDC ;

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 110** | | | |
|  |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service détaille :*   * *Une preuve de la commande de certificat ;* * *La liste des API Pro Santé Connectées et des serveurs proxy e-santé avec lesquels des sessions de communication peuvent être ouvertes, le cas échéant en TLS mutuel ;*   *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 109** | | | |
|  | **Editeur de Logiciel Utilisateur** |  |  |
| *[Il est attendu que le Fournisseur de Service indique quel composant technique (navigateur, client logiciel via librairie tierce, client logiciel via implémentation maison, etc.) porte la vérification de validité du certificat utilisé pour authentifier le composant serveur du Service Utilisateur ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 109** | | | |
|  |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service détaille les mécanismes assurant l’authentification du proxy auprès du logiciel utilisateur ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 109** | | | |
|  | **Editeur de Logiciel Utilisateur** |  | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service détaille les mécanismes assurant l’adossement à l’authentification de l’utilisateur auprès de PSC ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

### Gestion des informations de raccordement

En tant que FS, je dois garantir que la forme de stockage des secrets de sécurité utilisés lors de l'authentification des utilisateurs (personnes ou autres systèmes) interdise définitivement d'accéder à leur valeur en clair tout en permettant leur comparaison avec un secret à tester. Je peux avoir recours à des fonctions de hachage cryptographique à cette fin.

Si besoin, le haché du secret peut être utilisé comme index pour retrouver les informations contextuelles liées au secret mais qui ne constituent pas elles-mêmes des secrets de sécurité, et qui peuvent être nécessaires à des validations de sécurité (ex: date d'expiration de l'état d'authentification matérialisé par le secret, état de révocation ou non du secret, identifiant du système autorisé à utiliser le secret...) ou aux fonctions métiers assurées par le système (ex: informations relatives à l'utilisateur...)

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC 117** | | | |
|  | **Editeur de Logiciel Utilisateur** |  | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service précise les mesures mises en place pour empêcher tout stockage d*’*information de raccordement dans le code source ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC 118** | | | |
| **Fournisseur de Service Utilisateur** |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service décrive la gestion du stockage des information de raccordement persistantes et des mécanismes utilisés ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC 119** | | | |
|  | **Editeur de Logiciel Utilisateur** |  | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service décrive le paramétrage de la solution garantissant que toute information de raccordement éphémère ne soient stockées qu'en mémoire volatile ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

Il est primordial que l’Editeur de Logiciel s’assure que les jetons et autres informations de raccordement éphémères ne soient pas stockés, même temporairement, sous quelque forme que ce soit, sur quelque support ou système de stockage que ce soit autre que la mémoire volatile du système, ni conservés dans des traces, ni imprimés, ni affichés.

A titre d'exception, ces jetons peuvent être transmis de façon sécurisée à un sous-système de cache partagé intégré à la solution, et stockés temporairement en mémoire volatile par ce sous-système afin que ces secrets puissent être partagés par différents serveurs dans le cadre, par exemple, de partage de charge ou de redondance à la fin de disponibilité du service.

Ce sous-système de cache doit au minimum respecter les exigences applicables au système lui-même ainsi que la règle de stocker les jetons uniquement en mémoire volatile.

En tant que FS, je devrais interdire l’envoi de jetons Pro Santé Connect jusqu’à un client lourd et 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.

De plus, l'accès à ce sous-système de cache doit faire l'objet d'une authentification conforme aux bonnes pratiques et aux exigences fixées par [l'analyse de risques du système](#_Analyse_de_risque).

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 120** | | | |
| **Fournisseur de Service Utilisateur** |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service liste* les *partenaires d'échanges de jetons Pro Santé Connect issus de l’Espace de Confiance ou une description des mesures techniques prises pour s'assurer que les partenaires d'échanges sont bien dans l'Espace de Confiance ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

## Filtrage et alertes

### Filtrage de flux

En tant que FS, je dois prendre les mesures nécessaires pour m’assurer que seuls les flux applicatifs définis dans mes matrices de flux sont autorisés au sein de l’environnement se trouvant sous mon contrôle.

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 121** | | | |
|  |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service documente les méthodes de filtrage adoptées afin d’autoriser uniquement les flux applicatifs nécessaires à l’utilisation du système*;  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

### Procédure de traitement des alertes

Concernant la procédure de traitement des alertes, tout écart aux documents techniques est à traiter comme un mésusage, et je dois faire apparaître ici une liste des ces cas considérés comme « mésusage ou usage anormal ».

Cette liste pourrait contenir, entre autres, les cas de dépassements du délai maximal d'établissement de connexion TCP, de la fréquence maximale de requêtes, de la taille maximale des en-têtes et des requêtes HTTP, de la durée maximale des requêtes HTTP, ainsi que de la taille maximale du contenu reçu.

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 122** | | | |
|  |  |  | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service précise :*   * *L’ensemble des cas considérés comme « mésusage ou usage anormal » menant à une interruption de requête ;* * *La procédure d'interruption de requête en cas de non-conformité*   *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 123** | | | |
|  |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service précise :*   * *La procédure de traitement des alertes*; * *Les mécanismes de supervision du fonctionnement et de la sécurité du système qui déclencheront des alertes en cas d’usage anormal ou mésusage du système*; * *Un exemple complet de réaction à une requête conforme et une requête non conforme*;   *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

## Traçabilité

### Politique de traçabilité

En tant que FS, je dois faire apparaître dans cette section :

* Les types, contenus, formats et finalités des traces produites par le système   
  Pour la description des traces, je ferai apparaître un tableau récapitulatif. Ce tableau contiendra une première colonne avec les informations contenues dans la trace (date, heure, IP, port, id sessions, etc.), une deuxième colonne avec le champ de la trace correspondant puis toute information complémentaire.

J’introduirai également un exemple de trace ;

* 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 (telles que l'authentification, la demande d'accès à une ressource, l’obtention de jeton, le renouvellement etc.) ;
* Des éléments garantissant la sécurité et la conservation des journaux d’audit et la traçabilité de ses données de journalisation ;*;*
* Le processus établissant les rôles et responsabilités du personnel en charge de la gestion de traces produites par le système PSC.

En tant que FS je m’engage à respecter les règles suivantes :

* Une trace doit comporter toute information utile à son exploitation telle que l’identifiant de session et le paramètre session\_state et ne pas comporter de secret de sécurité en clair ou d'information de nature confidentielle (au titre de la sécurité du système ni au titre des données à caractère personnel)

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 trace mis en place à fin 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 autorisées de la structure utilisatrice de manière autonome d'une part de façon interactive et d'autre part en flux pour récupération en temps réel ou différé ;
* Les traces sont conservées au minimum 1 an et respectent le RGPD ;
* Sur demande peut être fournie 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 habilités.

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 124** | | | |
|  |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service décrive les types, contenus et formats des traces produites par le système et illustre les éléments inclus dans une trace via un tableau et un exemple. En particulier, il est attendu de préciser qu’un identifiant de session, ainsi que le paramètre session\_state font bien partie des données journalisées ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]*  *[Il est également attendu que le Fournisseur de Service décrive :*   * *Les évènements tracés ;* * *Les règles de conservation et consultations des traces ;* * *Les informations nécessaires à leur utilisation ;* * *Les obligations de sécurité ;* * *Le périmètre des composants et opérations sensibles devant générer les traces ;* * *La finalité des traces ;* * *Les méthodes garantissant la sécurité et la conservation des journaux d’audit et la traçabilité de ses données de journalisation ;* * *Les règles et devoirs à respecter ;* * *Les processus établissant les rôles et responsabilités du personnel en charge de la gestion de traces produites par le système ;*   *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 125** | | | |
|  |  |  | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service fournisse une liste des éléments inclus dans les traces produites incluant les éléments minimums attendus et un exemple ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

### Gestion des identifiants de session

Cette section décrit la gestion des identifiants de session tout au long de leur cycle de vie.

Je dois aussi m’assurer que ces identifiants de session n’apparaissent pas auprès de l’utilisateur final.

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 114 & 115** | | | |
|  | **Editeur de Logiciel Utilisateur** |  | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service décrive le processus de génération des identifiants, le processus de gestion des traces d’identifiants, le déroulement théorique de l’authentification et les types de contrôles de bac à sable applicables (avec des liens de test) ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

## Plan d’assurance sécurité

En tant que FS, je m’engage à inclure dans le Plan d'Assurance Sécurité des justifications du respect des exigences et la planification des mesures de sécurité essentielles à l’utilisation de l’API Pro Santé Connectée. De plus, le Plan d’Assurance Sécurité sera mis à jour à chaque évolution majeure du produit grâce aux résultats d'analyse de risques ou de retours d'expérience d'incident.

Toute préconisation et information de configuration du système devant être prise en compte pour le durcissement du système (système hôte y compris) sera documentée dans l’encadré ci-dessous.

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 129** | | | |
|  | **Editeur de Logiciel Utilisateur** |  | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service décrive et justifie sous forme de catégorie les points 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.) ;*   *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

Si le système est susceptible d'être opéré par des acteurs autres que son Editeur de Logiciel, des exigences de sécurité et des propositions de mesures de sécurité correspondantes seront également à définir pour la mise en œuvre du produit et pour son environnement de mise en œuvre.

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC PSC 130** | | | |
| **Fournisseur de Service Utilisateur** |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service définisse des exigences de sécurité et des propositions de mesures de sécurité correspondantes ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

Je devrais également définir et tester régulièrement un plan de continuité d’activité et le maintenir à jour.

|  |  |  |  |
| --- | --- | --- | --- |
| **RECO EDC PSC 137** | | | |
| **Fournisseur de Service Utilisateur** |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service définisse son plan de continuité d’activité*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

## Mises à jour de ce document

En tant que FS, l’ANS attend de moi que je m’investisse tant dans la création du système que dans l'implémentation de nouvelles fonctionnalités.

Par conséquent, j’ai l’obligation de mettre à jour régulièrement ce document de conformité en se référant à l’Editeur de Logiciel lors d’implémentation de nouvelles fonctionnalités ou de mises à jour.

|  |  |  |  |
| --- | --- | --- | --- |
| **Fournisseur de Service Utilisateur** |  | **Fournisseur de Service Proxy e-santé** |  |
| *[Il est attendu que le Fournisseur de Service complète le tableau d’historique de ce document situé page 1 et récapitule dans ce champ de texte à chaque nouvelle mise à jour l’ensemble des travaux effectués notamment la liste des composants mis à jour, les nouvelles fonctionnalités, la date de révision et les potentiels ajouts à venir dans les prochaines mises à jour du système*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |

# Glossaire

|  |  |
| --- | --- |
| **ANS** | Agence du Numérique en Santé |
| **ANSSI** | Agence Nationale de la Sécurité des Systèmes d'Information |
| **API PSC Connectée** | Interface de Programmation d’Application référencée dans PSC |
| **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 |
| **FAPI** | Financial-Grade API |
| **FD** | Fournisseur de Données |
| **FS** | Fournisseur de Service |
| **IGC-Santé** | Infrastructure de Gestion de la Confiance du secteur santé-social |
| **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 |
| **OWASP** | Open Web Application Security Project |
| **PGSSI-S** | Politique Générale de Sécurité du Système d'Information de Santé |
| **PKCE** | Proof Key for Code Exchange |
| **PS** | Professionnel de Santé |
| **PSC** | Pro Santé Connect |
| **REST** | REpresentational State Transfer |
| **RFC** | Request For Comments |
| **RPPS** | Répertoire Partagé des Professionnels de Santé |
| **TLS** | Transport Layer Security |