AGENCE
DU NUMÉRIQUE
EN SANTÉ

POC Ouverture API eSignSante

Sous-titre

Statut : En cours | *Classification : Restreinte* | *Version : v1.0*

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

Destinataires

Prénom / Nom	Entité / Direction
Patrick MORTAS	Henix
Erick RIEGEL	Henix

Documents de référence

Historique du document

Version	Rédigé par		Vérifié par		Validé par	
0.1	C.CRIMETZ	Le 03/06/2021	P.NOM	Le JJ/MM/AA	P.NOM	Le JJ/MM/AA
	Motif et nature de la modification : **Création du document**					
1.0	C.SOPHIE	Le 07/06/2021	C.CRIMETZ	Le 10/06/2021	J.METZGER	Le 10/06/2021
	Motif et nature de la modification : Ajout d'exigences					
	Motif et nature de la modification :					
	Motif et nature de la modification :					
	Motif et nature de la modification :					
	Motif et nature de la modification :					
	Motif et nature de la modification :					
	Motif et nature de la modification :					

SOMMAIRE

1. INTRODUCTION 3
1.1. Objet du document 3
1.2. Terminologie 3
2. CONTEXTE 3
3. SERVICE CIBLE 4
3.1. Présentation du service cible 4
3.1.1. Processus de signature 4
3.1.2. Preuves 4
3.1.3. Déploiement et éléments techniques 4
3.2. Impacts utilisateurs 4
3.3. Présentation des processus détaillés 5
3.3.1. Cas d'utilisation « signature d'un document par délégation » 5
3.3.2. Cas d'utilisation « vérifier jeton d'authentification » 5
3.3.3. Cas d'utilisation « double signature » 5
4. EXIGENCES 6
5. PILOTAGE ET GOUVERNANCE 8
5.1. Planning prévisionnel 8
5.2. Gouvernance 8

1. INTRODUCTION

1.1. Objet du document

L'ANS souhaite ouvrir son API eSignSanté à l'extérieur. Dans un premier temps, un POC doit être réalisé à destination de la CNAM. Ce POC doit permettre l'appel de l'API eSignSanté, de l'extérieur, à la suite d'une authentification via un fournisseur d'identité OIDC. Ce document décrit les fonctionnalités demandées et les exigences pour la réalisation de ce POC.

1.2. Terminologie

[Lister et définir les termes techniques, sigles et acronymes employés dans la présente définition du besoin]

Terme, sigle, acronyme	Définition
eSignSante	API de signature et de vérification de signature électronique
XAdES	XML Advanced Electronic Signatures
PAdES	PDF Advanced Electronic Signatures
ANS	Agence du Numérique e Santé
PRO Santé Connect	Fournisseur public d'identité dédié à la santé qui réalise l'authentification à la place des services, avec le protocole OpenID Connect
CNAM	Caisse National d'Assurance Maladie
API	Application Programming Interface
OpenId Connect (OIDC)	Protocole d'authentification basé sur les spécifications OAuth 2.0
OAuth 2.0	
POC	Proof Of Concept : projet permettant de valider la faisabilité technique de a mise en œuvre d'une fonctionnalité

2. CONTEXTE

Pro Santé Connect est une solution complète qui répond au besoin de Fournisseurs de Service du monde de la santé d'authentifier et d'identifier les professionnels et intervenants en santé. La prochaine étape est de pouvoir proposer un service de signature lié à une authentification Pro Santé Connect.

La CNAM a exprimé son intérêt pour un tel service.

L'ANS souhaite réaliser un POC s'appuyant sur eSignSanté et permettant de répondre à cette demande.

3. SERVICE CIBLE

3.1. Présentation du service cible

3.1.1. Processus de signature

Le POC doit permettre l'appel de l'API eSignSanté à la suite d'une authentification OIDC.

Le token OIDC doit donc être :

1. Présent dans la requête d'appel du Client
2. Vérifié par l'API eSignSanté auprès du fournisseur OIDC
3. Valide

Si le token n'est pas valide, le POC eSignSanté doit retourner un message d'erreur au Client.

3.1.2. Preuves

Le POC doit permettre de vérifier à posteriori que chaque appel de l'API eSignSanté était bien lié à une authentification OIDC.

Chaque appel à l'API eSignSanté doit être lié à l'identité de la personne authentifiée.

Cela peut être fait, par exemple, en enrichissant la preuve émis par le POC API eSignSanté avec des éléments permettant de prouver que la vérification du jeton a bien été effectuée et son résultat.

La signature effectuée est faite pour le compte d'une personne ou d'un organisme :

La signature doit être enrichi pour indiquer pour qui cette signature a été faite.

Dans la norme PADES l'attribut « Reason » semble adapté pour cela (cf https://www.etsi.org/deliver/etsi_ts/119100_119199/11914403/01.01.01_60/ts_11914403v010101p.pdf). Pour la norme XADES, il faut voir si on peut utiliser l'attribut SignerRole (cf https://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf)

3.1.3. Déploiement et éléments techniques

Le POC doit pouvoir être déployé sur la plateforme conteneur ANS.

Le déploiement du POC doit être automatisé.

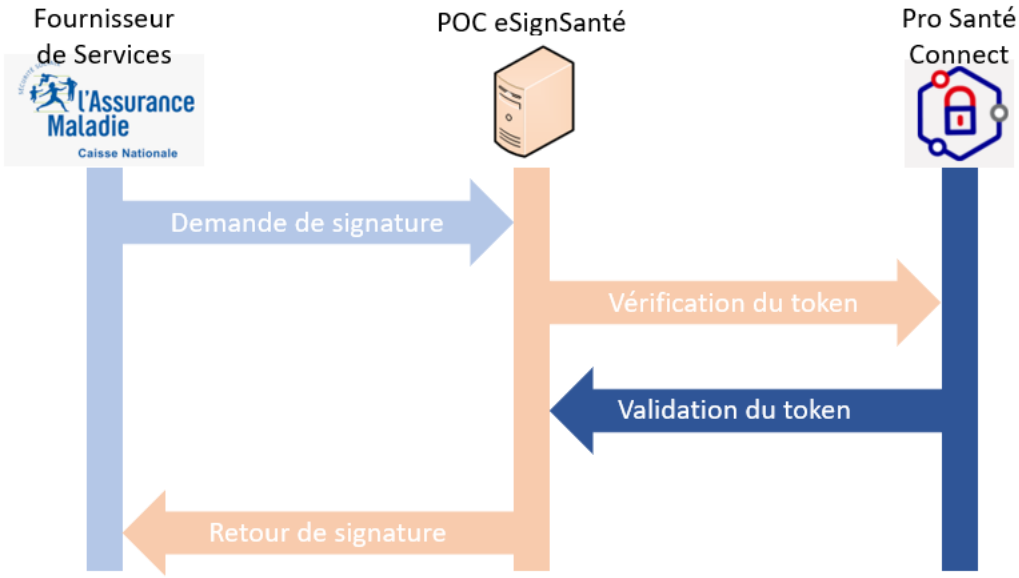
Le POC doit respecter les principes d'une application Cloud Native.

Le POC doit respecter au moins le niveau 2 du modèle de maturité Richardson

3.2. Impacts utilisateurs

Les évolutions effectuées sur le composant eSignSanté, doivent être transparentes pour les utilisateurs actuels de l'API en production (RPPS, TOMWS, Enreg).

3.3. Présentation des processus détaillés



3.3.1. Cas d'utilisation « signature d'un document par délégation »

L'utilisateur doit pouvoir signer un document en XADES.

L'utilisateur doit pouvoir signer un document en PADES.

Pour les documents PADES, la mention « signé pour le compte de <nom de l'utilisateur > » doit être indiqué dans l'attribut « reason ».

Pour les documents XADES, l'attribut « signerRole » doit contenir un rôle dans l'attribut « claimedRole » avec la valeur « délégataire de signature pour <nom personne> »

Le POC eSignSanté retourne le document signé et stocke la preuve générée par eSignSanté

La preuve doit contenir :

- Les éléments permettant de prouver la vérification du jeton
- Le résultat de cette vérification

3.3.2. Cas d'utilisation « vérifier jeton d'authentification »

Pour pouvoir faire signer par l'ANS un document, l'utilisateur doit s'authentifier via Pro Santé Connect.

Le jeton Pro Santé Connect est transmis au POC eSignSanté.

Le POC eSignSanté doit vérifier le jeton auprès de Pro Santé Connect.

Une fois la validité confirmée, eSignSanté doit utiliser les informations du jeton.

3.3.3. Cas d'utilisation « double signature »

Un document peut devoir être signé par deux personnes

Le POC doit permettre la double signature.

Le POC doit pouvoir vérifier la validité des deux jetons qui lui sont transmis auprès de Fournisseurs d'identité OIDC.

La preuve doit fonctionner de la même manière peu importe le nombre de signataires :

- Constitution de la preuve
- Conservation de la preuve

> ***Ce point pourra faire l'objet d'une pré-étude dans le cadre du projet.***

4. EXIGENCES

N° identifiant	Date de création	Type	Description	Critère d'adéquation	Émetteur	Priorité
PSC_esignsante_01	08/06/2021	Fonctionnel	Le POC doit permettre l'appel de l'API eSignSanté à la suite d'une authentification OIDC	l'API eSignSanté est capable de traiter les requêtes contenant un token d'identification OIDC	ANS	300
PSC_esignsante_02	08/06/2021	Technique	Le POC eSignSanté doit vérifier la validité du token auprès du FI OIDC	La validité du token est vérifié auprès du FI concerné	ANS	300
PSC_esignsante_03	08/06/2021	Fonctionnel	Le POC eSignSanté doit retourner un message d'erreur au Client si le token n'est pas valide	Si le token n'est pas valide, le POC eSignSanté retourne un message d'erreur	ANS	250
PSC_esignsante_04	08/06/2021	Fonctionnel	Le POC eSignSanté doit permettre de vérifier à posteriori que chaque appel de l'API eSignSanté était bien lié à une authentification OIDC.	Le POC eSignSanté permet de consulter les preuves générées	ANS	220
PSC_esignsante_05	08/06/2021	Fonctionnel	Chaque appel à l'API eSignSanté doit être lié à l'identité de la personne authentifiée	eSignSanté lie chaque appel fait à l'identité de la personne authentifiée	ANS	290
PSC_esignsante_06	08/06/2021	Fonctionnel	La signature doit être enrichi pour indiquer pour qui cette signature a été faite	la signature d'eSignSanté indique pour qui cette signature a été faite	ANS	280
PSC_esignsante_07	08/06/2021	Technique	Le POC doit pouvoir être déployé sur la plateforme conteneur ANS		ANS	200
PSC_esignsante_08	08/06/2021	Technique	Le déploiement du POC doit être automatisé.		ANS	200
PSC_esignsante_09	08/06/2021	Technique	Le POC doit respecter les principes d'une application Cloud Native.		ANS	300

PSC_esignsante_10	08/06/2021	Technique	Le POC doit respecter au moins le niveau 2 du modèle de maturité Richardson		ANS	300
PSC_esignsante_11	08/06/2021	Fonctionnel	Les évolutions effectuées sur le composant eSignSanté, doivent être transparentes pour les utilisateurs actuels de l'API en production	Aucun impact sur les utilisateurs actuels de l'API eSignSanté	ANS	300
PSC_esignsante_12	08/06/2021	Fonctionnel	L'utilisateur doit pouvoir signer un document en XADES	Un utilisateur peut signer un document en XADES	ANS	280
PSC_esignsante_13	08/06/2021	Fonctionnel	L'utilisateur doit pouvoir signer un document en PADES.	Un utilisateur peut signer un document en PADES	ANS	280
PSC_esignsante_14	08/06/2021	Fonctionnel	Pour les documents PADES, la mention « signé pour le compte de <nom de l'utilisateur > » doit être indiqué dans l'attribut « reason ».	Les attributs de signature contiennent bien le nom du demandeur	ANS	270
PSC_esignsante_15	08/06/2021	Fonctionnel	Pour les documents XADES, l'attribut « signerRole » doit contenir un rôle dans l'attribut « claimedRole » avec la valeur « délégataire de signature pour <nom personne> »	Les attributs de signature contiennent bien le nom du demandeur	ANS	270
PSC_esignsante_16	08/06/2021	Fonctionnel	Le POC eSignSanté retourne le document signé	Si le token est valide, le document signé est retourné	ANS	290
PSC_esignsante_17	08/06/2021	Fonctionnel	Le POC eSignSanté stocke la preuve générée	La preuve générée est stockée	ANS	250
PSC_esignsante_18	08/06/2021	Fonctionnel	La preuve contient les éléments permettant de prouver la vérification du jeton	la preuve de la vérification du jeton est présent dans la preuve	ANS	250
PSC_esignsante_19	08/06/2021	Fonctionnel	La preuve contient le résultat de la vérification du jeton	le résultat de la vérification du jeton est présent dans la preuve	ANS	250
PSC_esignsante_20	08/06/2021	Fonctionnel	Une fois la validité confirmée, le POC eSignSanté doit utiliser les informations du jeton.	Les informations du jeton sont utilisées pour consituter la preuve	ANS	270
PSC_esignsante_21	08/06/2021	Fonctionnel	Le POC doit permettre la double signature.	La double signature est possible	ANS	150
PSC_esignsante_22	08/06/2021	Fonctionnel	Le POC doit pouvoir vérifier la validité des deux jetons qui lui sont transmis auprès de Fournisseurs d'identité OIDC.	les jetons peuvent être vérifiés	ANS	150
PSC_esignsante_23	08/06/2021	Fonctionnel	La preuve doit fonctionner de la même manière peu importe le nombre de signataires : Constitution de la preuve	la constitution de la preuve est similaire peu importe le nombre de signataires	ANS	100
PSC_esignsante_24	08/06/2021	Fonctionnel	La preuve doit fonctionner de la même manière peu importe le nombre de signataires : Conservation de la preuve	la conservation de la preuve est similaire peu importe le nombre de signataires	ANS	100

5. PILOTAGE ET GOUVERNANCE

5.1. Planning prévisionnel

Le POC doit être finalisé pour mi-septembre.

5.2. Gouvernance

Le POC doit être réalisé en suivant une méthode agile (SCRUM). Les cérémonies suivantes devront être mises en place :

- Daily
- Retrospective
- Sprint Planning
- Sprint review (demo)

De plus un comité projet devra être planifié une fois par semaine.

Le suivi sera réalisé par Christian CRIMETZ.