AGENCE
DU NUMÉRIQUE
EN SANTÉ

Projet plateforme numérique SAS

Sécurisation des échanges par mTLS

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

SOMMAIRE

Page de révisions

Historique des versions

Version	Date	Auteur	Description des modifications
V1.0	02/11/2021	ANS	Version initialisée pour le Pilote
V2.0	19/05/2022	ANS	Version finalisée pour la phase de généralisation
V2.1	09/06/2022	ANS	Correction des liens de redirection
V2.2	03/11/2022	ANS	Correction nommage technique
V3.0	31/01/2023	ANS	Version avec la description de la liaison mTLS où la plateforme numérique SAS joue le rôle de client et serveur
V3.1	04/05/2023	ANS	Modification des IP et ajout d'exemples de configuration
V3.2	24/05/2024	ANS	Mise à jour des contrôles attendus sur les certificats

Références associées

Référence*	Nom du livrable	Description
(1)	SAS_SPEC INT_R01_Agrégateur de disponibilités SAS_SPEC INT_R04_Agrégateur de disponibilités CPTS SAS_SPEC INT_SOS1_Agrégateur de disponibilités SOS Médecins	Spécifications d'interopérabilité du flux d'agrégation des créneaux de disponibilités
(2)	SAS_SPEC INT_R02_Gestion des comptes régulateurs	Spécifications d'interopérabilité du flux de gestion des comptes régulateurs
(3)	SAS_SPEC INT_R03_Récupération des données du RDV	Spécifications d'interopérabilité du flux de récupération des données du RDV
(4)	SAS_Annexe Processus de génération et obtention d'un certificat IGC Santé	Annexe de support à la démarche de contractualisation avec l'ANS et la demande de cartes CPA et de certificats IGC Santé par l'éditeur

** La référence est utilisée par la suite dans ce document afin d'indiquer les renvois vers les documents identifiés ci-dessus.*

1. OBJET DU DOCUMENT

Le présent document constitue le livrable recensant les informations nécessaires à l'implémentation du mTLS pour la sécurisation des échanges avec la plateforme numérique SAS. Il a pour objectif de décrire le format des échanges entre la plateforme numérique SAS et les différentes solutions logiciels concernées.

Le chapitre 2 est consacré à la description détaillée de la sécurisation des échanges.

Le chapitre 3 décrit l'ensemble des informations nécessaires à l'implémentation du mTLS dans le cadre des requêtes émises par la plateforme numérique SAS vers la solution logicielle.

Le chapitre 4 décrit l'ensemble des informations nécessaires à l'implémentation du mTLS dans le cadre des requêtes émises par la solution logicielle éditeur vers la plateforme numérique SAS.

2. SÉCURISATION DES ÉCHANGES

2.1. TLS

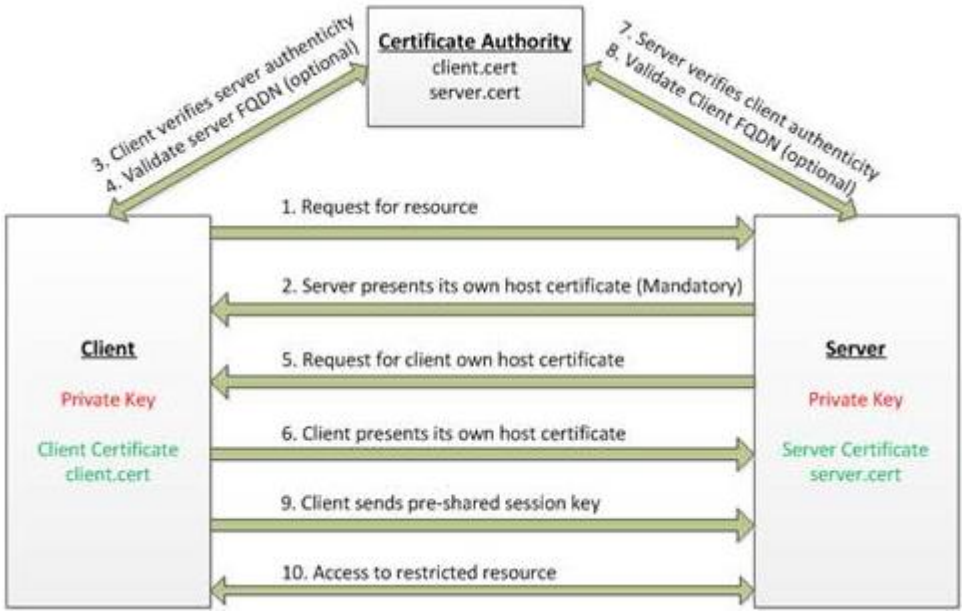
Les solutions logicielles devront être accessibles en HTTPS version TLS 1.2. Elles devront également indiquer la méthode de révocation des certificats utilisés.

Les solutions logicielles peuvent présenter des certificats issus d'une AC de leur choix. Toutefois cette AC devra être reconnue par la communauté informatique.

La plateforme numérique SAS sera accessible en HTTPS version TLS 1.2.

2.2. Mutual TLS (MTLS)

Le contrôle d'accès aux solutions logicielles s'effectue par la vérification de la validité du certificat présenté par le client. Il s'agit d'une version du protocole TLS appelée « Mutual TLS » (MTLS).



Mutual TLS Handshake

Le certificat présenté par le client doit être issu de l'IGC Santé. Il est de type AUTH_CLI de la gamme élémentaire et du domaine organisation. Ces certificats sont à installer dans les trust-stores des solutions logicielles.

- Autorités IGC Santé certifiant l'environnement de PRODUCTION : http://igc-sante.esante.gouv.fr/PC/#ca :
- ACR-EL.cer (http://igc-sante.esante.gouv.fr/AC/ACR-EL.cer)
- ACI-EL-ORG.cer (http://igc-sante.esante.gouv.fr/AC/ACI-EL-ORG.cer)

- Autorités IGC Santé certifiant les environnements de RECETTE et PREPRODUCTION : http://igc-sante.esante.gouv.fr/PC%20TEST/ :
- ACR-EL-TEST.cer (http://igc-sante.esante.gouv.fr/AC%20TEST/ACR-EL-TEST.cer)
- ACI-EL-ORG-TEST.cer (http://igc-sante.esante.gouv.fr/AC%20TEST/ACI-EL-ORG-TEST.cer)

Il est également demandé d'ajouter un **second niveau de contrôle lors de l'authentification du client sur le Common Name (CN) et Organizational Unit (OU) du certificat**.

Ce contrôle permet également de rejeter un certificat compromis dans le cas où les protocoles de révocation ont pu être mis en place.

2.3. TLS et révocation

Afin de parer à toutes compromissions de certificats clients, ceux-ci peuvent être révoqués à tout moment. Nous recommandons aux solutions logicielles d'implémenter une méthode de vérification des révocations de ces certificats.

L'IGC Santé prend en charge deux méthodes de révocations TLS : CRL et OCSP. Vous trouverez ci-dessous les liens vers la documentation IGC associée :

- https://integrateurs-cps.asipsante.fr/node/179
- https://integrateurs-cps.asipsante.fr/sites/default/files/170719_Guide_pratiques_verification_etat_certificats.pdf

À noter qu'en cas d'impossibilité de mettre à jour les listes CRL, un mécanisme de débrayage pourrait être mis en place.

2.3.1. Certificate Revocation List (CRL)

Ce protocole est basé sur la consultation de liste de certificats révoqués (CRL) : https://datatracker.ietf.org/doc/html/rfc5280#section-5

Tous les matins à partir de 7h les listes de révocations CRL sont mises à jour par l'IGC Santé.

2.3.2. Online Certificate Status Protocol (OCSP)

Ce protocole est une alternative aux CRL et permet d'effectuer une vérification « à la demande » : https://datatracker.ietf.org/doc/html/rfc2560

L'ANS met à disposition des utilisateurs des certificats produits par l'IGC Santé (uniquement) un service OCSP à l'adresse : http://ocsp.esante.gouv.fr

2.4. Healthcheck

Afin de vérifier l'état du service, il est souhaité dans la mesure du possible que les solutions logicielles éditeurs fournissent un endpoint retournant une réponse facilement analysable.

Le format souhaité est le suivant :

- Endpoint : <base_url>/check
- Méthode : GET
- Content-type de la réponse : application/json
- Code HTTP :
- OK :
- 200
- KO :
- 403 : échec de l'authentification
- 5XX : erreur, à préciser
- Tout autre code

Le contenu de la réponse doit être un object JSON avec à minima la variable « status » :

- OK : available
- KO : tout autre message

3. MODALITÉS DE SÉCURISATION DES ÉCHANGES AVEC LA SOLUTION ÉDITEUR DANS LE RÔLE « SERVEUR »

La plateforme numérique SAS (client) utilise un certificat IGC Santé qui est contrôlé par la solution logicielle éditeur (serveur).

3.1. Flux concernés

Les flux concernés par les modalités de sécurisation des échanges entre la plateforme numérique SAS et les solutions logicielles éditeurs dans le rôle « serveur » sont précisées ci-dessous :

Flux concernés	Nom de la spécification de référence
Agrégation des créneaux de disponibilités *(1)*	SAS_SPEC INT_R01_Agrégateur de disponibilités SAS_SPEC INT_R04_Agrégateur de disponibilités CPTS SAS_SPEC INT_SOS1_Agrégateur de disponibilités SOS Médecins
Gestion des comptes régulateurs *(2)*	SAS_SPEC INT_R02_Gestion des comptes régulateurs

3.2. Modalités de raccordement

Dans le cadre de la recette connectée avec la plateforme numérique SAS, nous avons trois environnements qui sont mis à disposition : Recette, PPRD, PROD.

En fonction du nombre d'environnements identifiés côté éditeur nous pouvons avoir les configurations suivantes :

- Soit en raccordement un pour un si l'éditeur propose également trois environnements :
- Recette <> Recette
- PPRD <> PPRD
- PRD <> PRD
- Soit en raccordement simplifié si l'éditeur propose deux environnements :
- Recette ANS <> PPRD éditeur
- PPRD ANS <> PPRD éditeur
- PRD <> PRD

Il est attendu de la part de l'éditeur de communiquer les endpoints correspondants à l'ANS.

3.3. Contrôles attendus sur les certificats et Common Name

Comme présenté dans le chapitre précédent, de manière schématique, nous allons effectuer des appels HTTPS classiques (TLS 1.2) en y ajoutant un certificat « TLS client » (mTLS).

Côté éditeur, il est attendu de :

- Configurer le « terminateur HTTPS » pour qu'il vérifie que l'appel se fasse bien avec un **certificat signé par les Autorité de Certifications (CA) de l'IGC Santé.**
- Ajouter un second niveau de sécurité dans votre application en **vérifiant le Common Name (CN) et Organizational Unit (OU) du certificat** pour chaque client et environnement.

Ci-dessous les informations utiles pour chacun des environnements ANS :

- Recette ANS
- Certificat MTLS (http://igc-sante.esante.gouv.fr/PC%20TEST/) :
- Racines : ACR-EL-TEST.cer (http://igc-sante.esante.gouv.fr/AC%20TEST/ACR-EL-TEST.cer)
- Intermédiaires : ACI-EL-ORG-TEST.cer (http://igc-sante.esante.gouv.fr/AC%20TEST/ACI-EL-ORG-TEST.cer)
- C = FR, ST = Paris (75), O = CABINET MLLE DENTISTE0023419, **OU = 499700234190004, CN = sas-agregateur-recette**

- Préproduction ANS
- Certificat MTLS (http://igc-sante.esante.gouv.fr/PC%20TEST/) :
- Racines : ACR-EL-TEST.cer (http://igc-sante.esante.gouv.fr/AC%20TEST/ACR-EL-TEST.cer)
- Intermédiaires : ACI-EL-ORG-TEST.cer (http://igc-sante.esante.gouv.fr/AC%20TEST/ACI-EL-ORG-TEST.cer)
- C = FR, ST = Paris (75), O = CABINET M. MASSEUR0034394, **OU = 499700343942006, CN = sas-aggregator-preproduction**

- Production ANS
- Certificat MTLS (http://igc-sante.esante.gouv.fr/PC/#ca) :
- Racines : ACR-EL.cer (http://igc-sante.esante.gouv.fr/AC/ACR-EL.cer)
- Intermédiaires : ACI-EL-ORG.cer (http://igc-sante.esante.gouv.fr/AC/ACI-EL-ORG.cer)
- C = FR, ST = Paris (75), O = AGENCE DU NUMERIQUE EN SANTE, **OU = 318751275100020, CN = sas-aggregator-production**

Tout un ensemble de tests seront ensuite réalisés par les équipes projet afin de vérifier et valider la conformité de l'implémentation.

3.4. Filtrage par adresse IP

Pour des raisons de sécurité, il arrive que certains éditeurs souhaitent mettre en place un filtrage IP supplémentaire. Vous trouverez ainsi les informations nécessaires ci-dessous :

- Recette ANS
- IP Publique : 51.91.149.173
- Préproduction ANS
- IP Publique : 37.59.26.69
- Production ANS
- IP Publique : 51.68.88.222

4. MODALITÉS DE SÉCURISATION DES ÉCHANGES AVEC LA SOLUTION ÉDITEUR DANS LE RÔLE « CLIENT »

Les solutions logicielles vont effectuer des appels HTTPS classiques (TLS 1.2) vers la plateforme numérique SAS en y ajoutant un certificat « TLS client » (mTLS).

Afin d'établir la double authentification, la solution logicielle éditeur (client) utilise le certificat émis par IGC Santé et devra le présenter lors de chaque requête transmise à la plateforme numérique SAS (serveur).

4.1. Flux concernés

Les flux concernés par les modalités de sécurisation des échanges entre la plateforme numérique SAS et les solutions logicielles éditeurs dans le rôle « client » sont précisées ci-dessous :

Flux concernés	Nom de la spécification de référence
Récupération des données du RDV *(3)*	SAS_SPEC INT_R03_Récupération des données du RDV

4.2. Modalités de raccordement

Dans le cadre de la recette connectée avec la plateforme numérique SAS, nous avons trois environnements qui sont mis à disposition : Recette, Préproduction, Production.

Le tableau ci-dessous présente les endpoints de la plateforme numérique SAS par environnement à renseigner pour les échanges.

Dans la suite de cette section, **<ENV_AGREG>** doit être remplacé par la ligne correspondante de ce tableau en fonction de l'environnement concerné.

Environnements	URL serveur plateforme numérique SAS
Recette	https://sas-agregateur.integration.santefr.esante.gouv.fr/
Préproduction	https://sas-agregateur.preproduction.santefr.esante.gouv.fr/
Production	https://sas-agregateur.production.santefr.esante.gouv.fr/

En fonction du nombre d'environnements identifiés côté éditeur nous pouvons avoir les configurations suivantes :

- Soit en raccordement un pour un si l'éditeur propose également trois environnements :
- Recette <> Recette
- PPRD <> PPRD
- PRD <> PRD
- Soit en raccordement simplifié si l'éditeur propose deux environnements :
- Recette ANS <> PPRD éditeur
- PPRD ANS <> PPRD éditeur
- PRD <> PRD

4.3. Démarche pour l'obtention d'un certificat IGC Santé et son implémentation

Le certificat présenté par les solutions logicielles éditeurs doit être issu de l'IGC Santé avec un Common Name (CN) prédéfini et un Organizational Unit (OU) correspondant à l'identifiant national de la structure.

Cette section détaille les différentes étapes à réaliser par les éditeurs pour obtenir un certificat IGC Santé conforme et implémenter les modalités de sécurisation nécessaires aux échanges avec la plateforme numérique SAS :

- Génération des CSR pour les différents environnements
- Génération et obtention d'un certificat IGC Santé
- Soit en autonomie par le biais des outils et formulaires mis à disposition
- Soit par le biais d'une demande spécifique à réaliser auprès de l'ANS
- Implémentation d'un certificat IGC Santé
- Contrôles réalisés par la plateforme numérique SAS

4.3.1. Génération des CSR pour les différents environnements

Un certificat ad-hoc pourra être utilisé pour l'ensemble des environnements hors-production et un second pour l'environnement de production. Il sera nécessaire de générer un CSR pour chaque demande de certificat IGC Santé.

Le CSR et la clé privée doivent être générés directement depuis les solutions logicielles, sans mot de passe ni email, uniquement avec un CNAME prédéfini.

Le format du CNAME attendu devra être le suivant :

NB : ci-dessous <EDITEUR> correspond au nom de la solution logicielle

- Pour les environnements hors-production :

```
sas-agregateur-test-<EDITEUR>
```

- Pour l'environnement de production :

```
sas-agregateur-prod-<EDITEUR>
```

La création du couple clé privée/CSR devra ainsi être réalisée pour chacun des environnements :

- Pour les environnements hors-production (le même certificat pourra être utilisé) :

```
openssl req -nodes -passout pass:"" -newkey rsa:2048 -sha256 -subj "/CN=sas-agregateur-test-<EDITEUR>" -keyout <EDITEUR>_test.key -out <EDITEUR>_test.csr
```

- Pour l'environnement de production :

```
openssl req -nodes -passout pass:"" -newkey rsa:2048 -sha256 -subj "/CN=sas-agregateur-prod-<EDITEUR>" -keyout <EDITEUR>_prod.key -out <EDITEUR>_prod.csr
```

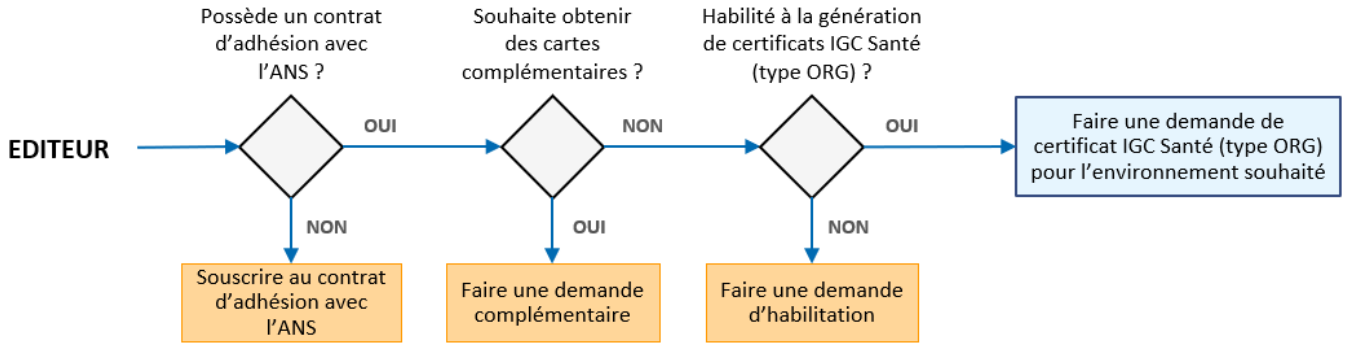
Point d'attention : Les clés privées ne doivent pas quitter les environnements où elles ont été générées, elles ne devront pas être communiquées, versionnées ni sauvegardées de manière classique.

4.3.2. Génération et obtention d'un certificat IGC Santé

Les éditeurs ont la possibilité de générer les différents certificats IGC Santé en toute autonomie en suivant les étapes détaillées dans la section suivante et en se rapportant à l'Annexe correspondante ***(4)***. En cas de difficultés rencontrées, l'ANS pourra prendre en charge la génération des certificats IGC Santé mais déclinera toute responsabilité quant à la gestion de leur cycle de vie et d'expiration qui resteront à la charge de l'éditeur.

4.3.2.1. En autonomie par l'éditeur

L'arbre de décision ci-dessous représente les actions à réaliser par les éditeurs pour réaliser une demande de certificat IGC Santé en toute autonomie :



Point d'attention : Les certificats concernant les environnements hors-production et production s'appuient sur des Autorités de Certification (AC) différentes et l'habilitation s'effectue au niveau de l'identification de la structure. Certaines étapes du processus devront donc être réalisées plusieurs fois.

Dans cette section, les liens pour réaliser chaque demande en ligne sur le service des démarches simplifiées sont cliquables et accessibles directement dans la colonne « Démarche en ligne ». Les demandes peuvent également être réalisées en complétant les formulaires PDF mis à disposition dans la colonne « Démarche par formulaire ».

Pour plus de détails sur le service des démarches simplifiées ou les étapes de complétion de chaque demande, une référence à la section correspondante de l'Annexe ***(4)*** est précisée.

4.3.2.1.1. Prérequis : Souscription au contrat d'adhésion avec l'ANS

Cette section détaille la souscription au contrat d'adhésion avec l'ANS. La démarche de contractualisation en ligne regroupe la demande d'adhésion, la commande de carte pour le représentant légal et le questionnaire relatif à l'attribution de carte.

Cette étape est préalable pour toute demande d'un certificat IGC Santé (pour les environnements hors-production ou de production).

	Démarche en ligne	Démarche par formulaire
Prérequis	► Être le représentant légal de la structure (identifiée par son SIRET) pour faire la demande	
Liens pour la demande	► Contrat d'adhésion et déclaration du représentant légal	► Contrat d'adhésion avec l'ANS ► Demande de carte pour le représentant légal ► Questionnaire d'attribution de carte
Section correspondante dans l'Annexe ***(4)***	► Section 2.2	► Section 3.1 et 3.2

4.3.2.1.2. Certificat IGC Santé pour les environnements hors-production

Cette section détaille les actions à réaliser pour chaque étape de complétion du processus à la demande d'un certificat IGC Santé pour les environnements hors-production.

- Réaliser une demande de cartes de tests et leurs habilitations à la génération de certificats IGC Santé (type ORG) sur les environnements hors-production. Il est possible et recommandé de commander un kit de test composé de 5 cartes CPx dont une CPA.

	Démarche en ligne	Démarche par formulaire
Prérequis	► Avoir souscrit au contrat d'adhésion avec l'ANS	
Liens pour la demande	► Commande des cartes de tests avec habilitations associées	► Formulaire de commande des cartes de tests et de leurs habilitations
Section correspondante dans l'Annexe ***(4)***	► Section 2.5	► Section 3.5

- Faire une demande de certificats IGC Santé pour les environnements souhaités

	Démarche en ligne
Prérequis	► Avoir une carte CPx habilitée à la génération de certificats type ORG pour la structure en hors-production
Lien pour la demande	► Téléservice de gestion et commande des certificats
Section correspondante dans l'Annexe ***(4)***	► Section 4

4.3.2.1.3. Certificat IGC Santé pour l'environnement de production

Cette section détaille les actions à réaliser pour chaque étape de complétion du processus à la demande d'un certificat IGC Santé pour les environnements production.

- Réaliser une demande de cartes complémentaires et permettre au représentant légal de déléguer la gestion des cartes et/ou habilitations (non nécessaire si le représentant légal ne souhaite pas déléguer la gestion)

	Démarche en ligne		Démarche par formulaire
	Formulaire Téléservice	Démarche via le support ANS	
Prérequis	► Avoir souscrit au contrat d'adhésion avec l'ANS et avoir demandé une carte principale (carte de directeur de structure autorisée)		
Liens pour la demande	► Service en ligne pour la gestion et la demande de cartes	► Démarche en ligne passant par le support de l'ANS	► Formulaire de commande de carte de personnel de structure
Section correspondante dans l'Annexe ***(4)***		► Section 2.3	► Section 3.3

- Faire une demande d'habilitation à la génération de certificats IGC Santé de type ORG pour la structure

	Démarche en ligne	Démarche par formulaire
Prérequis	► Être le représentant légal ou avoir été désigné mandataire préalablement	
Liens pour la demande	► Déclaration des administrateurs autorisés à commander des certificats logiciels	► Formulaire de déclaration des administrateurs autorisés à commander des certificats logiciels
Section correspondante dans l'Annexe ***(4)***	► Section 2.4	► Section 3.4

- Faire une demande de certificats IGC Santé pour l'environnement de production

	Démarche en ligne
Prérequis	► Avoir une carte CPx habilitée à la génération de certificats type ORG pour la structure en production
Lien pour la demande	► Téléservice de gestion et de commande des certificats
Section correspondante dans l'Annexe ***(4)***	► Section 4

4.3.2.2. En passant par une demande spécifique auprès de l'ANS

En cas de difficultés rencontrées par l'éditeur, l'ANS pourra prendre en charge la génération des certificats IGC Santé. Cette section se découpe en deux étapes et détaille les actions à réaliser ainsi que les modalités d'échanges des différents éléments :

- Transmission du CSR généré par l'éditeur à l'ANS :

Le CSR généré doit être transmis par l'éditeur par courriel de manière chiffré avec communication du mot de passe via un autre canal aux contacts préalablement identifiés. Seul le retour obtenu à la suite de l'exécution de la commande pour demander un CSR est à transmettre à l'ANS pour l'obtention du certificat IGC Santé

- Génération du certificat par l'ANS et transmission à l'éditeur :

L'ANS réalise les opérations nécessaires à la génération du certificat IGC Santé pour les environnements de production et hors-production au nom de l'éditeur. Les certificats générés par l'ANS seront transmis par courriel de manière chiffré avec communication du mot de passe via un autre canal aux contacts préalablement identifiés sous le format suivant :

- Pour les environnements hors-production : <EDITEUR>_TEST.crt
- Pour l'environnement de production : <EDITEUR>_PROD.crt

Point d'attention : Le certificat transmis est valable 3 ans et aura le champ OU valorisé avec l'identifiant de structure ANS (SIRET). Il est rappelé que l'ANS décline toute responsabilité quant à la gestion du cycle de vie, d'expiration et de révocation des certificats qui restent à la charge de l'éditeur.

4.3.3. Implémentation d'un certificat IGC Santé

À la suite de la génération des différents certificats IGC Santé (par l'éditeur ou par l'ANS), la solution logicielle éditeur devra les implémenter et les transmettre au sein d'un fichier PEM lors des appels vers la plateforme numérique SAS. Cette section détaille et précise la démarche d'implémentation d'un certificat IGC Santé et la génération du fichier PEM :

Lorsque les éditeurs auront un certificat IGC Santé, ils devront le mettre en forme au format « .PEM » (concaténation des sources : clé privée, publique, ACs).

- Pour les environnements hors-production, le même fichier pourra être utilisé :

```
# Convert it to pem
openssl x509 -inform der -in <EDITEUR>_TEST.crt -out <EDITEUR>_TEST.crt.pem

# Generate one PEM key
cp <EDITEUR>_TEST.key <EDITEUR>_TEST.key.crt.ca.pem
cat <EDITEUR>_TEST.crt.pem >> <EDITEUR>_TEST.key.crt.ca.pem
cat ACI-EL-ORG-TEST.cer.pem >> <EDITEUR>_TEST.key.crt.ca.pem

# Show Info
openssl x509 -text -noout -in <EDITEUR>_TEST.key.crt.ca.pem
```

- Pour l'environnement de production :

```
# Convert it to pem
openssl x509 -inform der -in <EDITEUR>_PROD.crt -out <EDITEUR>_PROD.crt.pem

# Generate one PEM key
cp <EDITEUR>_PROD.key <EDITEUR>_PROD.key.crt.ca.pem
cat <EDITEUR>_PROD.crt.pem >> <EDITEUR>_PROD.key.crt.ca.pem
cat ACI-EL-ORG.cer.pem >> <EDITEUR>_PROD.key.crt.ca.pem

# Show Info
openssl x509 -text -noout -in <EDITEUR>_PROD.key.crt.ca.pem
```

Pour chaque requête envoyée par la solution logicielle éditeur à la plateforme numérique SAS, les éditeurs (client) devront ajouter le fichier PEM généré dans l'appel. (cf. annexe 5.5).

4.3.4. Contrôles réalisés par la plateforme numérique SAS

La plateforme numérique SAS met en place différents contrôles afin de garantir la sécurisation des échanges. Cette section détaille les différents contrôles réalisés par la plateforme numérique SAS lors des échanges avec les solutions logicielles éditeurs (client) :

- Lors de chaque transmission du fichier PEM par la solution logicielle éditeur, la plateforme numérique SAS contrôle que le certificat est authentique et IGC Santé
  - Dans le cas où le certificat n'a pas été émis par l'autorité IGC Santé, un code http 401 Unautorized est renvoyé
- Un contrôle est réalisé sur la non-révocation du certificat présenté par la solution logicielle éditeur
- Un contrôle est réalisé sur le Common Name (CN) et Organizational Unit (OU) du certificat présenté par la solution logicielle éditeur. Il s'agit respectivement d'une chaîne de caractères unique définie lors de la génération du certificat et de l'identifiant national de la structure cliente pour chacune des solutions logicielles éditeurs et par environnement
  - Dans le cas d'un couple CN et OU non reconnu, un code http 403 Forbidden est renvoyé.

5. ANNEXES

5.1. Exemple d'implémentation des Autorités de Certification

Il peut être nécessaire de convertir les certificats .cer au format PEM :

```
openssl x509 -inform der -in ACR-EL.cer -out ACR-EL.cer.pem
```

A noter que ces fichiers peuvent être concaténés au sein d'un seul fichier.

HaProxy

```
Bind 0.0.0.0:8090 ssl crt /etc/haproxy/ssl/ ca-file /etc/haproxy/ssl/mtls/ca.crt verify required no-sslv3
```

Traefik (docker)

```
# Dynamic configuration
config_name:
  options:
    # MTLS
    mtls:
      clientAuth:
        # in PEM format. each file can contain multiple CAs.
        caFiles:
          - /traefik-ca/ca.crt
        clientAuthType: RequireAndVerifyClientCert
```

5.2. Exemple d'implémentation CRL dans Apache

Les chemins sont à adapter en fonction de votre configuration.

Configuration d'apache /etc/httpd/httpd.conf

```
SSLCARevocationCheck chain
SSLCARevocationPath /etc/apache2/conf/ssl.crl/
```

Cron journalier de mise à jour

Installation de make :

```
sudo apt install build-essential
```

Création du fichier make :

cf. : https://opensource.apple.com/source/apache_mod_ssl/apache_mod_ssl-689/mod_ssl/pkg.sslcfg/Makefile.crl.auto.html

```
cd /etc/apache2/conf/ssl.crl
vi Makefile


##
##  Makefile to keep the hash symlinks in SSLCARevocationPath up to date
##  Copyright (c) 1998-2001 Ralf S. Engelschall, All Rights Reserved.
##
SSL_PROGRAM="openssl"
update: clean
    -@ssl_program="$(SSL_PROGRAM)"; \
```

```
  if [ ".$$ssl_program" = . ]; then \
    for dir in . `echo $$PATH | sed -e 's/:/ /g'`; do \
      for program in openssl ssleay; do \
        if [ -f "$$dir/$$program" ]; then \
          if [ -x "$$dir/$$program" ]; then \
            ssl_program="$$dir/$$program"; \
            break; \
          fi; \
        fi; \
      done; \
      if [ ".$$ssl_program" != . ]; then \
        break; \
      fi; \
    done; \
  fi; \
  if [ ".$$ssl_program" = . ]; then \
    echo "Error: neither 'openssl' nor 'ssleay' program found" 1>&2; \
    exit 1; \
  fi; \
  for file in *.crl; do \
    [ "x$$file" = "x*.crl" ] && continue; \
    if [ ".`grep SKIPME $$file`" != . ]; then \
      echo dummy |\
      awk '{ printf("%-15s ... Skipped\n", file); }' \
      "file=$$file"; \
    else \
      n=0; \
      while [ 1 ]; do \
        hash="`$$ssl_program crl -noout -hash <$$file`"; \
        if [ -r "$$hash.r$$n" ]; then \
          n=`expr $$n + 1`; \
        else \
          echo dummy |\
          awk '{ printf("%-15s ... %s\n", file, hash); }' \
          "file=$$file" "hash=$$hash.r$$n"; \
          ln -s $$file $$hash.r$$n; \
          break; \
        fi; \
      done; \
    fi; \
  done
clean:
  -@rm -f [0-9a-fA-F]*.r[0-9]*
```

Création d'un fichier shell pour la tache planifiée :

```
vi /<cron_folder>/crl.sh

cd /etc/apache2/conf/ssl.crl
curl -s http://igc-sante.esante.gouv.fr/CRL/ACR-EL.crl | openssl crl -inform DER -out ACR-EL.crl
curl -s http://igc-sante.esante.gouv.fr/CRL/ACI-EL-ORG.crl | openssl crl -inform DER -out ACI-EL-ORG.crl
# Test certificats
curl -s http://igc-sante.esante.gouv.fr/CRL/ACR-EL-TEST.crl | openssl crl -inform DER -out ACR-EL-TEST.crl
curl -s http://igc-sante.esante.gouv.fr/CRL/ACI-EL-ORG-TEST.crl | openssl crl -inform DER -out ACI-EL-ORG-TEST.crl
# Rebuild links
make clean
make
```

Mise en place de la tache planifiée :

```
Crontab -e
0 8 * * * bash /<cron_folder>/crl.sh > /tmp/log-sas-plannedtask.log
```

5.3. Exemple d'implémentation CRL pour Apache ou Nginx

- Listes de révocation Production : ACR-ACI-EL-ORG.crl.pem

```
wget http://igc-sante.esante.gouv.fr/CRL/ACR-EL.crl
wget http://igc-sante.esante.gouv.fr/CRL/ACI-EL-ORG.crl
openssl crl -inform der -in ACR-EL.crl -out ACR-EL.crl.pem
openssl crl -inform der -in ACI-EL-ORG.crl -out ACI-EL-ORG.crl.pem
# Concatenate the chain into one file
cat ACR-EL.crl.pem ACI-EL-ORG.crl.pem > ACR-ACI-EL-ORG.crl.pem
```

- Listes de révocation PréProduction : ACR-ACI-EL-ORG-TEST.crl.pem

```
wget http://igc-sante.esante.gouv.fr/CRL/ACR-EL-TEST.crl
wget http://igc-sante.esante.gouv.fr/CRL/ACI-EL-ORG-TEST.crl
openssl crl -inform der -in ACR-EL-TEST.crl -out ACR-EL-TEST.crl.pem
openssl crl -inform der -in ACI-EL-ORG-TEST.crl -out ACI-EL-ORG-TEST.crl.pem
# Concatenate the chain into one file
cat ACR-EL-TEST.crl.pem ACI-EL-ORG-TEST.crl.pem > ACR-ACI-EL-ORG-TEST.crl.pem
```

Configuration Apache

Paramètre pour Apache indiquant l'emplacement du CRL :

```
SSLCARevocationPath /etc/ssl/certs/ACR-ACI-EL-ORG-TEST.crl.pem
```

Configuration Nginx

Paramètre pour Nginx indiquant l'emplacement du CRL :

```
ssl_crl /etc/nginx/certs/ACR-ACI-EL-ORG-TEST.crl.pem;
```

5.4. Exemple d'implémentation OCSP dans Apache

Voici les directives à mettre en place dans votre fichier de configuration Apache :

```
  # https://httpd.apache.org/docs/2.4/fr/mod/mod_ssl.html
  SSLVerifyClient require
  SSLOCSPEnable on
```

Il faut également activer l'OCSP Stapling pour fournir directement une attestation de validité à la connexion. L'OCSP Stapling est supporté à partir de la version 2.4+ d'Apache. Voici un exemple de configuration de l'OCSP Stapling :

```
SSLUseStapling on
SSLStaplingCache "shmcb:logs/stapling_cache(128000)"
```

5.5. Exemple d'implémentation OCSP dans Nginx

Voici les directives à mettre en place dans votre fichier de configuration Nginx :

```
ssl_ocsp leaf; # Permettre uniquement le contrôle sur des appels entrant.
resolver 8.8.8.8; # Renseignement d'un DNS valide.
```

5.6. Exemple de retour d'erreur par le serveur

Exemple de retour 401 :

```
curl -k -I <ENV_AGREG>/fhir/v1/Appointment
HTTP/1.1 401 UnauthorizedServer: nginx
Date: Mon, 19 Dec 2022 16:50:32 GMT
Content-Type: application/octet-stream
Content-Length: 57
Connection: keep-alive
```

5.7. Exemple de transmission du fichier PEM lors d'une requête éditeur

```
curl --location --request POST '<ENV_AGREG>/fhir/v1/Appointment' \
--cert /path/to/certificat/<EDITEUR>_PROD.key.crt.ca.pem
--header 'Content-Type: application/json' \
--data-raw '{
      "resourceType": "Appointment",
      "id": "32165461032",
      "meta": {
         "profile": [
            "http://interopsante.org/fhir/StructureDefinition/FrAppointment"
         ]
      },
      "identifier": [
         {
            "system": "urn:oid:1.1.111.1.11.1.1.1",
            "value": "2"
         }
      ],
      "extension": [
         {
            "url": "http://interopsante.org/fhir/StructureDefinition/FrAppointmentOperator",
            "valueReference": {
               "identifier": {
                  "type": {
                     "coding": [
                        {
                           "system": "http://interopsante.org/fhir/CodeSystem/fr-v2-0203",
                           "code": "IDNPS"
                        }
                     ]
                  },
                  "system": "urn:oid:1.2.250.1.71.4.2.1",
                  "value": "49b66567-5406-482e-9f6e-9d8dc2017f6c"
               }
            }
         }
      ],
      "status": "booked",
      "start": "2022-09-04T14:00:00+01:00",
      "end": "2022-09-04T14:15:00+01:00",
      "participant": [
         {
            "actor": {
               "identifier": {
                  "type": {
                     "coding": [
                        {
                           "system": "http://interopsante.org/fhir/CodeSystem/fr-v2-0203",
                           "code": "IDNPS"
```

```
                        }
                    ]
                },
                "system": "urn:oid:1.2.250.1.71.4.2.1",
                "value": "810100050075"
            }
        },
        "status": "accepted"
    }
  ]
}'
```

5.8. Exemple de configuration pour Apache

Activation et configuration des modules apache suivants :

```
...
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
LoadModule ssl_module modules/mod_ssl.so
...

# Secure (SSL/TLS) connections
Include conf/extra/httpd-ssl.conf
#
# Note: The following must must be present to support
#       starting without SSL on platforms with no /dev/random equivalent
#       but a statically compiled-in mod_ssl.
#
<IfModule ssl_module>
  SSLRandomSeed startup builtin
  SSLRandomSeed connect builtin
</IfModule>
...
```

Exemple Virtualhost

```
<VirtualHost *:443>

  DocumentRoot /var/www/html
  ServerName  localhost

  SSLEngine on
  SSLCertificateFile /usr/local/apache2/conf/server.crt
  SSLCertificateKeyFile /usr/local/apache2/conf/server.key

  # Certificate IGC-Santé :
  SSLCACertificateFile /etc/ssl/certs/ACI-ACR-EL-TEST.cer.pem

  # Revocation Method 1 : Works with CRL control
  SSLCARevocationPath /etc/ssl/certs/ACR-ACI-EL-ORG-TEST.crl.pem

  # Revocation Method 2 : Working with OCSP
  SSLVerifyClient require
  SSLOCSPEnable on
  SSLUseStapling on
  SSLStaplingCache "shmcb:logs/stapling_cache(128000)"

  <Directory /var/www/html >
    Options -Indexes +FollowSymLinks +MultiViews
    AllowOverride none
    Require all granted
```

```
    SSLVerifyClient      require
    SSLVerifyDepth       10

    SSLRequireSSL
    SSLRequire   (%{SSL_CLIENT_S_DN_CN} eq "sas-agregateur-recette")

  </Directory>

</VirtualHost>
```

5.9. Exemple de configuration pour Nginx

```
map  $ssl_client_s_dn  $ssl_client_s_dn_cn {
  default "";
  ~CN=(?<CN>[^,]+) $CN;
}
server {
  listen               80;
  listen               443 ssl;
  server_name          localhost;
  root                 /var/www/html;

  # Server TLS configuration :
  # TLS configuration is required to enable TLS module and granted access to
  # mTLS features.
  ssl_certificate        /etc/nginx/ssl/server.crt;
  ssl_certificate_key    /etc/nginx/ssl/server.key;
  ssl_protocols          TLSv1.1 TLSv1.2;

  # Mtls configuration
  ssl_verify_client      optional;
  ssl_verify_depth       10;

  # Certificate IGC-Santé :
  ssl_client_certificate /etc/nginx/certs/ACI-ACR-EL-ORG-TEST.cer.pem;

  # Revocation Method 1 : Works with CRL control
  ssl_crl              /etc/nginx/certs/ACR-ACI-EL-ORG-TEST.crl.pem;

  # Revocation Method 2 : Working with OCSP
  ssl_ocsp             leaf;
  resolver             8.8.8.8;

  location / {
    try_files $uri /index.html$is_args$args;
  }

  # Application of mTLS configuration for a given path.
  location /mtls-protect/ {
    try_files $uri /index.html$is_args$args;
    if ($ssl_client_verify != SUCCESS) {
      return 401 '{"status": "KO:Unauthorized", "verify": "$ssl_client_verify", "CN": "$ssl_client_s_dn_cn"}';
    }
    if ($ssl_client_s_dn_cn !~ "sas-agregateur-recette") {
      return 403 '{"status": "KO:Forbidden", "verify": "$ssl_client_verify", "CN": "$ssl_client_s_dn_cn"}';
    }
  }
}
```

Paramètre SSL

```
ssl_verify_client optional; # Permettre de faire une vérification en fonction d'une `location`spécifique.
ssl_verify_depth  10; # Paramètre en fonction du nombre de certificat dans la chaîne situé au dessus de l'application.
```

Définition de la route qui sera protégé par mTLS

```
location /mtls-protect/ {
  ...
}
```

Vérification du certificat

```
if ($ssl_client_verify != SUCCESS) {
  return 401 '{"status": "KO:Unauthorized", "verify": "$ssl_client_verify", "CN": "$ssl_client_s_dn_cn"}';
}
```

Vérification du CN en fonction de l'environnement

```
if ($ssl_client_s_dn_cn !~ "sas-agregateur-recette") {
  return 403 '{"status": "KO:Forbidden", "verify": "$ssl_client_verify", "CN": "$ssl_client_s_dn_cn"}';
}
```