NOTICE D'AIDE

PARTIE 1 : GENERALITES

> Envoi du formulaire

Par courrier :

ASIP Santé
Service Relations Clients – BP 80210
86963 FUTUROSCOPE CHASSENEUIL CEDEX

Par email :

monserviceclient.certificats@asipsante.fr

Si vous rencontrez des difficultés techniques, vous pouvez nous solliciter au
0 825 852 000 Service 0,06 € / min + prix appel
Du lundi au vendredi de 8h00 à 20h00
Et le samedi de 8h00 à 14h00

> Définition

Un certificat logiciel est un fichier informatique contenant des informations sur son propriétaire et qui sont certifiées par un tiers de confiance appelé Autorité de Certification.
Il fait fonction de pièce d'identité numérique.

L'ASIP Santé est l'Autorité de Certification du domaine de la santé. Elle délivre des certificats électroniques d'une validité de 3 ans pour sécuriser les échanges de données de santé informatisées.

> Commande de certificats avec le formulaire 413

Pour obtenir les certificats suivants, il est nécessaire de renseigner le formulaire 413 de commande de certificat logiciel qui est destiné à la déclaration d'habilitation.

OFFRE	USAGE	CODE PRODUIT	DESCRIPTIF DE L'USAGE CRYPTOGRAPHIQUE
CERTIFICAT DE PERSONNE MORALE **SERVEUR**	CERTIFICAT LOGICIEL SERVEUR USAGE SSL[6]_SERV	SERV_SSL	Il permet à un serveur appartenant à une structure de s'authentifier vis-à-vis d'un tiers, d'un module client ou d'une personne physique, voire en tant que client à un autre serveur distant.
	CERTIFICAT LOGICIEL SERVEUR USAGE SMIME[7] / SIGN / CONF	SERV_S/MIME	Il permet à un serveur de signer des objets et de déchiffrer les données qui lui sont destinées, sous la responsabilité de la structure concernée.
		SERV_SIGN (cachet)	Il permet à un serveur associé à une structure de signer électroniquement des objets.
		SERV_CONF	Il permet à un utilisateur de chiffrer sous la responsabilité de la structure concernée des données à destination d'un serveur qui est le seul à pouvoir déchiffrer les données qui lui sont destinées.
CERTIFICAT DE PERSONNE MORALE **ORGANISATION**	CERTIFICAT LOGICIEL OFFRE ORG	ORG_AUTH_CLI	Il permet aux applications associées à une structure de s'authentifier vis-à-vis d'un tiers, un serveur ou une application.
		ORG_SIGN (cachet)	Il permet à une application, sous la responsabilité d'une structure, de signer électroniquement des objets (documents, courriers électroniques,…)
		ORG_CONF	Il permet à un utilisateur de chiffrer des données à destination de cette structure, qui est la seule à pouvoir déchiffrer les données qui lui sont destinées.

OFFRE	USAGE	CODE PRODUIT	DESCRIPTIF DE L'USAGE CRYPTOGRAPHIQUE
CERTIFICAT DE PERSONNE PHYSIQUE **PRO**. Professionnel exerçant dans une structure qui l'emploie (demande faite par un mandataire).	CERTIFICAT LOGICIEL OFFRE PRO	PRO_AUTH	Il permet à un professionnel de santé (PS), à un personnel d'établissement (PE) ou à un personnel autorisé (PA) dans le cadre d'une structure identifiée, de s'authentifier vis-à-vis d'un tiers (serveur, application ou autre personne physique).
		PRO_SIGN	Il permet à un professionnel de santé (PS), à un personnel d'établissement (PE) ou à un personnel autorisé (PA) dans le cadre d'une structure identifiée, de signer des objets (documents électroniques,…).
		PRO_CONF	Il permet à un utilisateur de chiffrer des données à destination du porteur* de ce certificat de confidentialité, qui est le seul à pouvoir déchiffrer les données qui lui sont destinées. *le porteur est un professionnel de santé (PS), un personnel d'établissement (PE) ou un personnel autorisé (PA) dans le cadre d'une structure identifiée.

> Commande de certificats sans formulaire

Il n'est pas nécessaire de remplir et valider le formulaire 413 de commande de certificat logiciel pour les certificats de l'offre Professionnel de Santé (PS_AUTH, PS_SIGN, PS_CONF) présentés ci-dessous. Ils peuvent être commandés et générés directement en utilisant une carte CPS[1] sur la Plateforme de Confiance Nouvelle Génération (https://pfc.eservices.esante.gouv.fr).

OFFRE	USAGE	CODE PRODUIT	DESCRIPTIF DE L'USAGE CRYPTOGRAPHIQUE
CERTIFICAT DE PERSONNE PHYSIQUE **PROFESSIONNEL DE SANTE (PS)** (demande directe du PS)	CERTIFICAT LOGICIEL OFFRE PS	PS_AUTH	Il permet à un professionnel de santé de s'authentifier vis-à-vis d'un tiers (serveur, application ou autre personne physique).
		PS_SIGN	Il permet à un professionnel de santé de signer des objets (documents électroniques,…).
		PS_CONF	Il permet à un utilisateur des chiffrer des données à destination du professionnel de santé porteur de ce certificat de confidentialité, qui est le seul à pouvoir déchiffrer les données qui lui sont destinées.

PARTIE 2 : AIDE AU REMPLISSAGE DU FORMULAIRE 413

> Commande d'un certificat

Prérequis :

- Un **contrat** de commande de produit de certification en cours;
- Une **carte CPS, CDE, CPE nominative, CDA ou CPA**[1] valide pour l'administrateur technique (les cartes de service ne sont pas éligibles).

Modalité :

- Un **formulaire** n°413 de commande de certificat logiciel à l'ASIP Santé complété et signé par le représentant légal ou son mandataire.

> Notice d'aide au remplissage du formulaire

1. IDENTIFICATION DE LA STRUCTURE BENEFICIAIRE

Les champs marqué d'une * sont obligatoires.

Dénomination de la structure :
Dénomination ou raison sociale présente sur le KBIS de la structure qui souhaite obtenir le certificat.

N°SIRET (14 caractères attendus) :
Le numéro SIRET est un code Insee, permettant l'identification d'un établissement ou d'une entreprise française, présent sur le KBIS.

N°FINESS[5] géographique (9 caractères attendus) :
Le numéro FINESS[5] (Fichier National des Etablissement Sanitaires et Sociaux) géographique est un numéro attribué à chaque établissement et à chaque entité juridique.
Les FINESS[5] géographique sont disponibles sur le site :
http://finess.sante.gouv.fr/finess/jsp/rechercheSimple.jsp

Code postal et Commune :
Le code postal de la structure titulaire du contrat sur 5 caractères et la commune associée.

3. VISA ET CACHET

Les champs marqué d'une * sont obligatoires.

Compléter l'ensemble des champs présents relatifs à l'identité du représentant légal ou de son mandataire puis dater, signer et apposer le cachet de la structure sur ce formulaire.

Le numéro de carte attendu est le numéro de la carte CPS du représentant légal ou de son mandataire.

4. DETAILS DE LA DEMANDE DE CERTIFICAT LOGICIEL

Les champs marqué d'une * sont obligatoires.

Ces parties techniques peuvent être complétées par l'éditeur ou le distributeur de la solution logicielle que vous utilisez, sous votre responsabilité.

4.1 Usage des certificats et solution utilisée

Pour connaître le ou les produit(s) dont vous pouvez bénéficier, vous êtes invité à vous renseigner auprès de votre éditeur de solution logicielle.

Vous trouverez ci-dessous des exemples d'usages :

Authentification :
Permettre à un serveur de s'authentifier.
Permettre à une application de s'authentifier.
Permettre à un professionnel de santé (PS), à un personnel d'établissement (PE) ou à un personnel autorisé (PA) de s'authentifier.

Signature électronique :
Permettre à un serveur de signer électroniquement des documents (Ou cachet électronique).
Permettre à un serveur de signer des courriers électroniques.
Permettre à une application de signer électroniquement des documents.
Permettre à un professionnel de santé (PS), à un personnel d'établissement (PE) ou à un personnel autorisé (PA) de signer électroniquement des documents.

Sécurisation / chiffrement des données :
Permettre à un serveur de déchiffrer les données qui lui sont envoyées.
Permettre à une application de votre structure de déchiffrer les données qui lui sont envoyées.
Permettre des échanges sécurisés d'un utilisateur vers le serveur de votre structure.
Permettre des échanges sécurisés d'un utilisateur vers une application de votre structure.
Permettre des échanges sécurisés d'un utilisateur vers un professionnel de santé (PS), à un personnel d'établissement (PE) ou à un personnel autorisé (PA).

4.2 Offre de certificat souhaitée

Dans le cas où la structure n'est pas **propriétaire du nom de domaine ou sous domaine :**
Elle doit faire parvenir un courrier à l'adresse mentionnée au début de cette notice d'aide, signé par le détenteur, avec copie de sa carte d'identité.
Dans ce courrier le détenteur déclare accorder le droit d'usage du nom de domaine à l'établissement pour un usage particulier (par exemple DMP[2], MS Santé, messagerie, …) ou pour tout usage sans restriction.

Offre Certificat logiciel SERVEUR usage SSL[6]_SERVEUR

Le nom de domaine est obligatoire.

Le nom de domaine est nécessaire à la construction de l'identifiant unique.

Si vous souhaitez étendre les habilitations sur tous les serveurs et tous les sous-domaines, alors renseignez uniquement le nom de domaine.

Si vous voulez restreindre les habilitations à un sous-domaine spécifique, saisissez le nom de ce sous-domaine associé à votre nom de domaine. Par exemple sous_domaine.mon_domaine.fr.

Si vous voulez restreindre les habilitations à un serveur spécifique, saisissez le nom de ce serveur (FQDN[8]) associé à votre nom de domaine. Par exemple mon_serveur.mon_domaine.fr.

Si vous ne disposez pas de cette information, vous pouvez l'obtenir auprès de l'administrateur technique qui est en charge de l'installer sur le serveur.

Exemples d'usages : sécurisation d'un serveur Web, utilisation du web service PUSH de la PFLAU[3], utilisation du connecteur MS Santé par un opérateur MS Santé.

Offre Certificat logiciel SERVEUR usage SMIME[7] SIGN CONF

Le nom de domaine de messagerie est obligatoire.

Si vous souhaitez étendre les habilitations à l'ensemble des sous-domaines de votre domaine ou sous-domaine de messagerie, renseignez le nom de domaine ou de sous domaine de messagerie (exemple @mon_domaine.fr ou @sous_domaine.mon_domaine.fr) et ne cochez pas la case ☐ « *A cocher pour les cas de restriction* ».
Par exemple, si vous renseignez « @mon_domaine.fr » sans restriction les certificats pourront référencer des adresses de messagerie de la forme « xxx.yyy@mon_domaine.fr », « xxx.yyy@sous_domaine1.mon_domaine.fr », « xxx.yyy@sous_domaine2.mon_domaine.fr »…

Si vous voulez habiliter le(s) administrateur(s) technique(s) à un domaine ou sous domaine de messagerie spécifique, saisissez ce nom de domaine ou sous domaine de messagerie (exemple @mon_domaine.fr ou @sous_domaine.mon_domaine.fr) et cocher la case ☒ « *A cocher pour les cas de restriction* ».
Par exemple, si vous renseignez « @mon_domaine.fr » avec restriction, alors les certificats référenceront uniquement des adresses de messagerie de la forme « xxx.yyy@mon_domaine.fr ».

Exemple d'usages : signature dans le cadre de l'alimentation du DMP[2]

Offre Certificat logiciel offre ORG

Exemples d'usages : authentification dans le cadre de l'alimentation du DMP[2], signature, authentification sur la fonctionnalité de rétrocession de médicament sur le Dossier Pharmaceutique, Authentification sur le web service PULL[4] de la PFLAU[3].

Offre Certificat logiciel offre PRO

Le nom de domaine de messagerie est obligatoire.

Si vous souhaitez étendre les habilitations à l'ensemble des sous-domaines de votre domaine ou sous-domaine de messagerie, renseignez le nom de domaine ou de sous domaine de messagerie (exemple @mon_domaine.fr ou @sous_domaine.mon_domaine.fr) et ne cochez pas la case ☐ « *A cocher pour les cas de restriction* ».
Par exemple, si vous renseignez « @mon_domaine.fr » sans restriction les certificats pourront référencer des adresses de messagerie de la forme « xxx.yyy@mon_domaine.fr », « xxx.yyy@sous_domaine1.mon_domaine.fr », « xxx.yyy@sous_domaine2.mon_domaine.fr »…

Si vous voulez habiliter le(s) administrateur(s) technique(s) à un domaine ou sous domaine de messagerie spécifique, saisissez ce nom de domaine ou sous domaine de messagerie (exemple @mon_domaine.fr ou @sous_domaine.mon_domaine.fr) et cocher la case ☒ « *A cocher pour les cas de restriction* ».
Par exemple, si vous renseignez « @mon_domaine.fr » avec restriction, alors les certificats référenceront uniquement des adresses de messagerie de la forme « xxx.yyy@mon_domaine.fr ».

Exemples d'usages : chiffrement des messages, authentification par certificat logiciel, etc…

4.3 Désignation des personnes ayant le rôle d'administrateur technique

Remplir l'ensemble des champs présents relatifs à l'identité du ou des administrateur(s) technique(s). Le numéro de téléphone ainsi que l'adresse email sont utilisés en cas de problème.

Pour le numéro de carte, il s'agit du numéro présent sur la 3ème ligne (celle sous le nom/prénom) de la carte CPS, CDE, CPE nominative, CDA ou CPA[1].

PARTIE 3 : GLOSSAIRE

[1]Carte CPS, CDE, CPE, CDA ou CPA :
Carte Professionnel de Santé, Carte de Directeur d'Etablissement, Carte de Personnel d'Etablissement, Carte de Directeur Administratif, Carte de Personnel Administratif.

[2]DMP :
Dossier Médical Partagé

[3]PFLAU :
PlateForme de Localisation des Appels d'Urgence

[4]PULL :
Webservice dit « PULL » permettant aux centres de réception des appels d'urgence, après authentification par certificat logiciel client, de requêter les serveurs de la PFLAU[3] afin d'obtenir les coordonnées de l'abonné de la ligne de téléphone fixe.

[5]FINESS :
Fichier National des Etablissement Sanitaires et Sociaux

[6]SSL :
Secure Sockets Layer, est un protocole de sécurisation des échanges sur Internet.

[7]S/MIME :
Secure/Multipurpose Internet Mail Extensions est une norme de cryptographie et de signature numérique de courriels encapsulés au format MIME. Elle assure l'intégrité, l'authentification, la non-répudiation et la confidentialité des données.

[8]FQDN :
Dans le DNS[9], un fully qualified domain name (FQDN, ou nom de domaine complètement qualifié) est un nom de domaine qui révèle la position absolue d'un nœud dans l'arborescence DNS[9] en indiquant tous les domaines de niveau supérieur jusqu'à la racine. On parle également de domaine absolu, par opposition aux domaines relatifs. Par convention, le FQDN est ponctué par un point final.

[9]DNS :
Domain Name System (système de noms de domaine) est un service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom.