



L'offre Certificats logiciels

Les certificats logiciels : au service de la protection des données de santé

Un certificat logiciel est un fichier informatique faisant fonction de pièce d'identité numérique. Il permet de garantir à distance l'identité d'une personne physique (un professionnel de santé par exemple) et/ou d'une personne morale (une structure de santé par exemple).

Un certificat logiciel contient des informations sur son propriétaire, certifiées par un tiers de confiance appelé "autorité de certification". Il permet 3 fonctionnalités principales :

- L'authentification
- La signature électronique
- La sécurisation / le chiffrement des données

L'ASIP Santé est l'autorité de certification du domaine de la santé. Elle délivre des certificats logiciels pour sécuriser les échanges de données de santé informatisées entre les professionnels de santé exerçant en ville, à l'hôpital et dans les établissements médico-sociaux.

L'ASIP Santé propose actuellement 4 offres de certificats logiciels :

- Certificat de personne morale **Serveur**
- Certificat de personne morale **Organisation**
- Certificat de personne physique **Professionnel**
- Certificat de personne physique **Professionnel de Santé (PS)**

Matrice des offres à commander en fonction des projets / usages :

Projet / Usage	Offre Certificat Logiciel
DMP	ORG AUTH_CLI
	ORG SIGN
MS Santé	SERV SSL
ROR (<i>Répertoire Opérationnel des Ressources</i>)	ORG AUTH_CLI
	OU SERV SSL
PFLAU (<i>Plateforme de Localisation des Appels d'Urgence</i>)	SERV SSL
	ORG AUTH_CLI
Annuaire AMC (<i>Assurance Maladie Complémentaire</i>)	ORG AUTH_CLI
RPPS (partenaires)	ORG AUTH_CLI
	ORG SIGN
Annuaire Santé (<i>RASS</i>)	ORG AUTH_CLI
PRATIC	ORG AUTH_CLI
Dossier Pharmaceutique (<i>DP</i>)	ORG AUTH_CLI
Diapason	SERV SSL
	ORG AUTH_CLI
ROC	SERV SSL
	ORG AUTH_CLI
PSIG (<i>Portail des Signalements Sanitaires</i>)	SERV SSL
	ORG AUTH_CLI

Cas d'usages des certificats :

- Pour le dossier médical partagé (DMP), des structures souhaitent garantir leur identité et signer des éléments demandés par le DMP.
- Pour les messageries sécurisées MSSanté, par les opérateurs MSSanté qui doivent sécuriser les échanges entre eux.
- Pour l'authentification d'un système pour l'accès aux données du Répertoire partagé des professionnels de santé (RPPS).
- Pour l'accès sécurisé par les SAMU-Centre 15 à la plateforme de localisation des appels d'urgence (PFLAU).
- Pour sécuriser la connexion entre un logiciel de rétrocession de médicament utilisé en établissement de santé et le Dossier Pharmaceutique.
- Pour sécuriser les échanges entre les Répertoires Opérationnels de Ressources (ROR)

Détails des différents certificats :

1. Certificats logiciels pour les établissements ou industriels du domaine de la santé

OFFRE	USAGE	CODE PRODUIT	DESCRIPTIF DE L'USAGE CRYPTOGRAPHIQUE
Certificat de personne morale Serveur	CERTIFICAT LOGICIEL SERVEUR USAGE SSL_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 / 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.

OFFRE	USAGE	CODE PRODUIT	DESCRIPTIF DE L'USAGE CRYPTOGRAPHIQUE
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 Professionnel <i>Professionnel exerçant dans une structure qui l'emploie (demande faite par un mandataire)</i>	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.

2. Certificat de personne physique Professionnel de santé (PS) (demande directe du PS)

OFFRE	USAGE	CODE PRODUIT	DESCRIPTIF DE L'USAGE CRYPTOGRAPHIQUE
Certificat de personne physique Professionnel de santé (PS) <i>(demande directe du PS)</i>	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.

Exemples d'usages pour l'offre de certificat de personne physique professionnel de santé (PS) :

- Un médecin souhaite gérer des authentifications ou signatures électroniques depuis sa tablette numérique.
- Un professionnel de santé souhaite permettre le chiffrement (ou cryptage) des données dans le cadre des échanges par messagerie sécurisée.