Référentiel d'Homologation Outils de Sécurisation de Messagerie avec la Carte CPS

GIP Carte de Professionnel de Santé

Version 2.3 du 16 juin 2006

Mise à jour de la version 1.3 du 21 octobre 2004

Version approuvée par le

Comité d'Homologation du 15 juin 2006

TABLE DES MATIERES

1. Objet du Référentiel

1.1 Portée du référentiel

Ce document constitue un Référentiel destiné aux Industriels souhaitant développer une solution pour sécuriser des messageries utilisées par les porteurs de la carte CPS, appelée tout simplement « Solution » dans la suite du document. Ce Référentiel doit être utilisé dans le cadre du Processus d'Homologation défini par le GIP-CPS comme décrit dans le document de référence [CPS-01].

Note : 1. Dans le présent référentiel, le terme « CPS » se réfère aux cartes CPS2bis et CPS2ter.
2. Dans l'IGC CPS2ter, il existe plusieurs autorités racine.

1.2 Contenu du référentiel

Le Référentiel est constitué de plusieurs chapitres :

- Chapitre 1 : Objet du référentiel
- Chapitre 2 : Rappel du contexte
- Chapitre 3 : Démarche d'Homologation
- Chapitre 4 : Exigences fonctionnelles de la Solution
- Chapitre 5 : Exigences d'interopérabilité de la Solution
- Chapitre 6 : Exigences légales de la Solution
- Chapitre 7 : Cahier de recette de la Solution

Sont fournis en annexe les éléments suivants :

- Annexe A : Dossier de Produit type, permettant aux industriels d'effectuer une description de leur Produit en vue de son Homologation.
- Annexe B : Profil cryptographique d'une Solution de messagerie utilisant la carte CPS.

1.3 Terminologie et sigles

Abréviation	Signification
AES	*Advanced Encryption Standard*
API	*Application Programming Interface*
CAST	*Algorithme symétrique développé par Entrust*
CBC	*Cipher Block Chaining (chiffrement en mode chaîné)*
CPS	*Carte de Professionnel de Santé* *Dans ce document "CPS" désigne n'importe quelle carte de la famille CPS et par extension tout support, autre que la carte CPS, autorisé à embarquer les clés privées associées aux certificats CPS.*
CRL	*Certificate Revocation List (liste de révocation de certificats)*
DES	*Data Encryption Standard*
3DES	*Triple – Data Encryption Standard*
DH	*Diffie Hellman*
DSA	*Digital Signature Algorithm*
IDEA	*International Data Encryption Algorithm*
IHM	*Interface Homme Machine*
LDAP	*Lightweight Directory Access Protocol*
MD5	*Message Digest v5*
MIME	*Multipurpose Internet Mail Extensions*
POP3	*Post Office Protocol V3*
PS	*Professionnel de Santé*
RC2	*Rivest's Code V2*
RSA	*Algorithme asymétrique développé par Rivest, Shamir et Adleman*
S/MIME	*Secure/Multipurpose Internet Mail Extensions*
SHA-1	*Secure Hash Algorithm v1*
SHA-256	*Secure Hash Algorithm v2*
SMTP	*Simple Mail Transfer Protocol*
ESMTP	*SMTP service extension*

1.4 Références documentaires

Documents GIP-CPS

Référence	Documents GIP-CPS	Date et version
CPS-01	Plan d'Assurance Qualité du Processus d'Homologation des Outils de Sécurisation de Messageries .	Version 1.0 22 juin 2006
CPS-02	Politique de Certification l'IGC CPS *(disponible sur site WEB du GIP)*	
	Concernant les certificats de signature et d'authentification CPS2bis	Version 4 1er novembre 2001
	Concernant les certificats de signature et d'authentification CPS2ter	Version 1.0 11 octobre 2004
	Concernant les certificats de confidentialité	Version 1.3 19 mars 2002
CPS-03	Les certificats X.509 et les CRLs du Système CPS2bis	Version 2.1 14 septembre 2001
	Les certificats X.509 et les CRLs du Système CPS2ter	Version 1.4 17 septembre 2004
CPS-04	Charte d'Accès de l'Annuaire CPS *(disponible sur site WEB du GIP)*	Version 1.6 16 octobre 2003
CPS-05	DIT de l'Annuaire CPS	Version 2.1a 24 mars 2003
CPS-06	Guide d'intégration du Kit CPS2bis et CPS2ter (version V5.03)	Version 5.1 09 décembre 2003
CPS-07	ICP de Confidentialité GIP-CPS Spécification de l'interface client de demande de certificat.	Édition 12 16 décembre 2002

Standards et normes

Références	Sujets
FIPS 74	Mise en œuvre de l'algorithme DES
FIPS 180-1	Mise en œuvre de l'algorithme SHA-1
FIPS 180-2	Mise en œuvre des algorithmes SHA-256
FIPS 186	Mise en œuvre de l'algorithme DSA
FIPS 197	Mise en œuvre de l'algorithme AES
RFC 822	Format des adresses e-mail
RFC 3121	Mise en œuvre de l'algorithme MD5
RFC 2045 à 2049	Conformité MIME
RFC 2144	Mise en œuvre de l'algorithme CAST-128
RFC 2251 à 2255	Conformité LDAP V3
RFC 2268	Mise en œuvre de l'algorithme RC2
RFC 2311 à 2315	Conformité S/MIME V2
RFC 2479	APIs IDUP-GSS (APIs sécurisation de messages)
RFC 2554	SMTP Service Extension for Authentication
RFC 2630	Conformité CMS (Cryptographic Message Syntax)
RFC 2631	Mise en œuvre de l'algorithme Diffie-Hellman
RFC 2632 et 2633	Conformité S/MIME V3
RFC 2984	Mise en œuvre de l'algorithme CAST-128 dans CMS
RFC 3058	Mise en œuvre de l'algorithme IDEA dans CMS
RFC 3280	X.509 : profils des certificats et des listes de révocation *(annule et remplace RFC 2459)*
PKCS#1	Mise en œuvre de RSA-Encryption

2. Rappel du contexte

2.1 Le GIP-CPS

Le Groupement d'Intérêt Public « Carte de Professionnel de Santé » (GIP-CPS) a pour objet de créer les conditions garantissant l'indépendance et la responsabilité des différents acteurs du secteur sanitaire et social dans l'utilisation des cartes électroniques.
Pour ce faire, il assurera « (…) l'émission, la gestion et la promotion d'une carte de professionnel de santé, d'une carte de professionnel de santé en formation et d'une carte de personnel d'établissement destinée au personnel non professionnel de santé des établissements sanitaires et sociaux ou aux personnes qualifiées ayant une activité dans le secteur sanitaire et social et ne relevant pas des critères d'attribution de la CPS (…) ».
« Professionnel de santé » s'entend au sens des catégories réglementées par le code de la santé publique, c'est à dire les professions médicales (médecins, chirurgiens-dentistes, sages-femmes), les pharmaciens et les auxiliaires médicaux (professions paramédicales) (…) » **(Extrait Art. 2 de la « Convention constitutive du Groupement d'Intérêt public « Carte de Professionnel de Santé » » : Arrêté du 28 janvier 1993 modifié par l'Assemblée Générale du 17 décembre 1998)**.

Le groupement d'intérêt public « carte de professionnel de santé » émet, délivre et gère les cartes de professionnels de santé. Il veille à leur bon usage et assure la fiabilité des mécanismes et la protection des clés sur lesquelles reposent la confidentialité des données chiffrées et la validité des signatures électroniques produites à l'aide de ces cartes. » **(Art. R. 161-54 du Décret 98-271 du 9 avril 1998 relatif à la carte de professionnel de santé et modifiant le code de la sécurité sociale et le code de la santé publique)**.

Le rôle du GIP-CPS est articulé autour de trois axes fondamentaux :

- Spécification et développement du système « CPS » et des services associés,
- Exploitation du système « CPS » et des services associés,
- Promotion du système « CPS » en vue de son intégration.

En tant qu'Autorité de Certification, le GIP-CPS gère trois types de certificats :

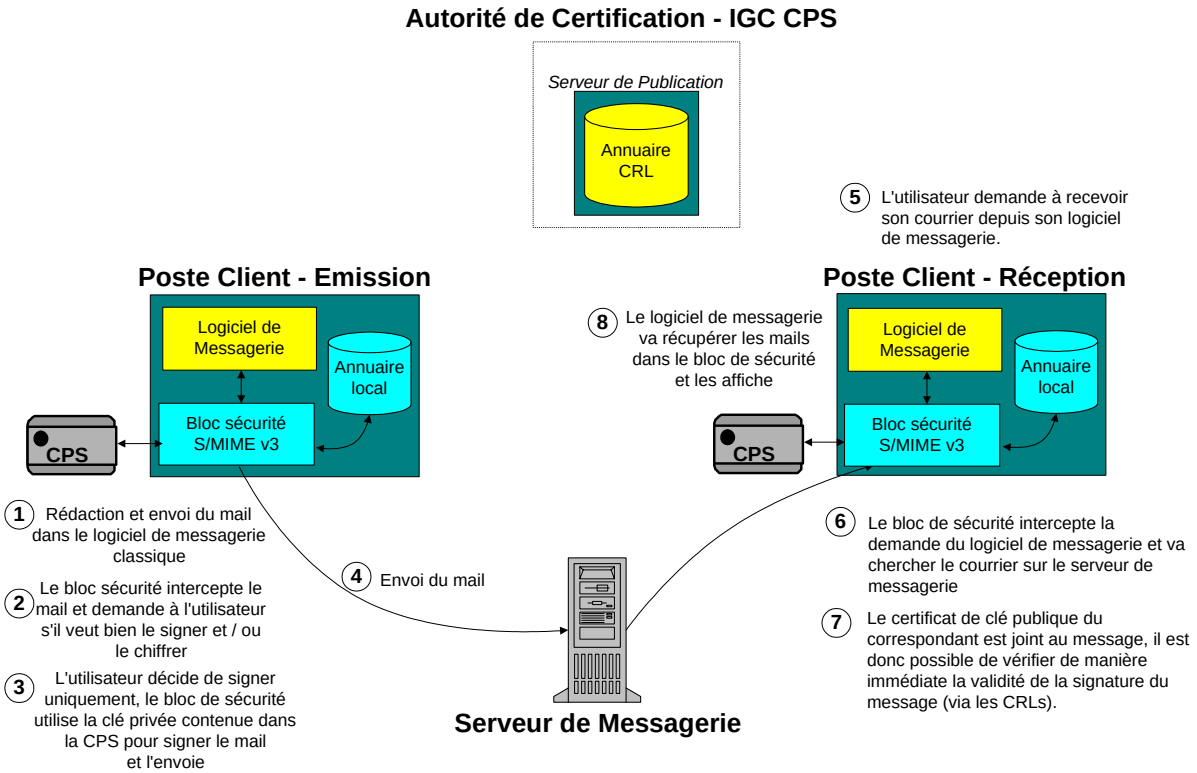
- Les certificats de clés de signature (utilisés pour signer les messages),
- Les certificats de clés d'authentification (pour des contrôles d'accès),
- Les certificats de clés de confidentialité (servant à échanger les clés de chiffrement).

2.2 La sécurisation des échanges

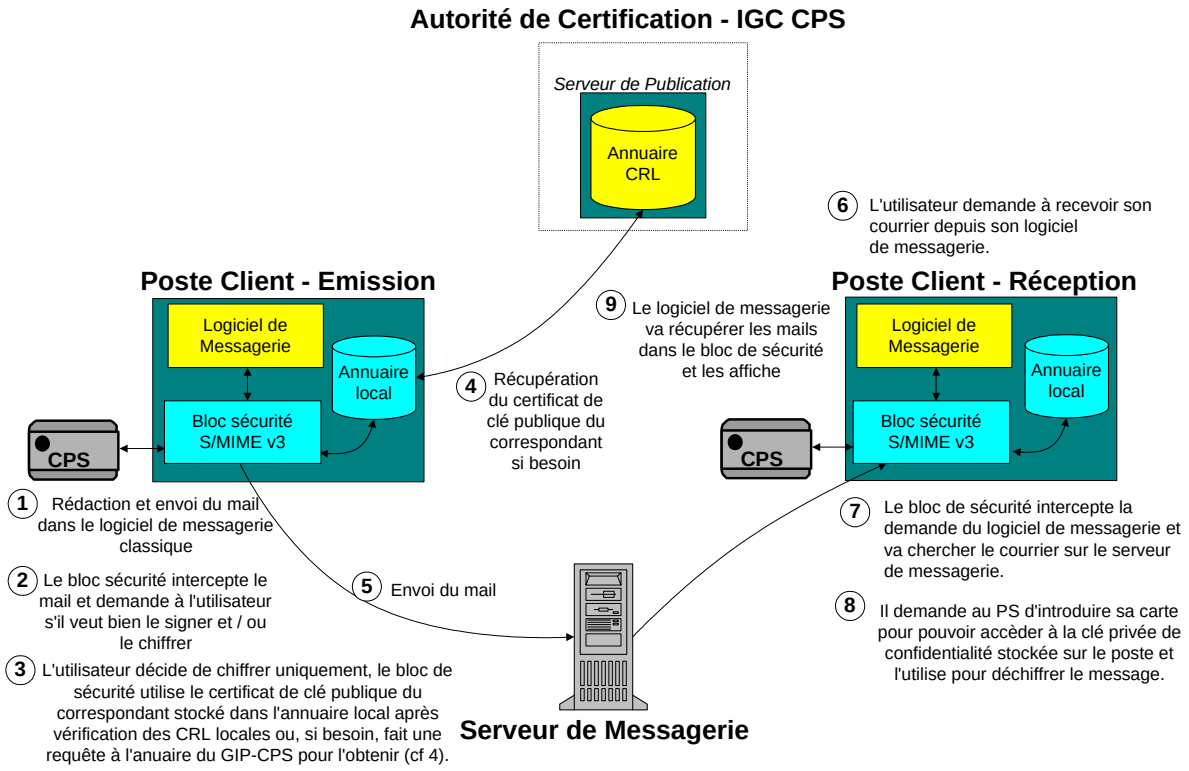
Le système de santé est aujourd'hui de plus en plus informatisé (télétransmission des feuilles de soins, gestion électronique des dossiers médicaux, …). Cette informatisation nécessite de mettre en place des mesures de sécurité permettant de maintenir les garanties de confidentialité et d'intégrité propres à l'activité médicale (secret médical) et spécifiques aux nouvelles technologies (respect de la loi informatique et libertés).

Dans le cadre de la mise en place de ces nouvelles technologies, la sécurisation des échanges requiert une attention particulière. En effet, l'ensemble des porteurs de cartes de la famille CPS doit pouvoir échanger des messages et des dossiers signés et/ou chiffrés.

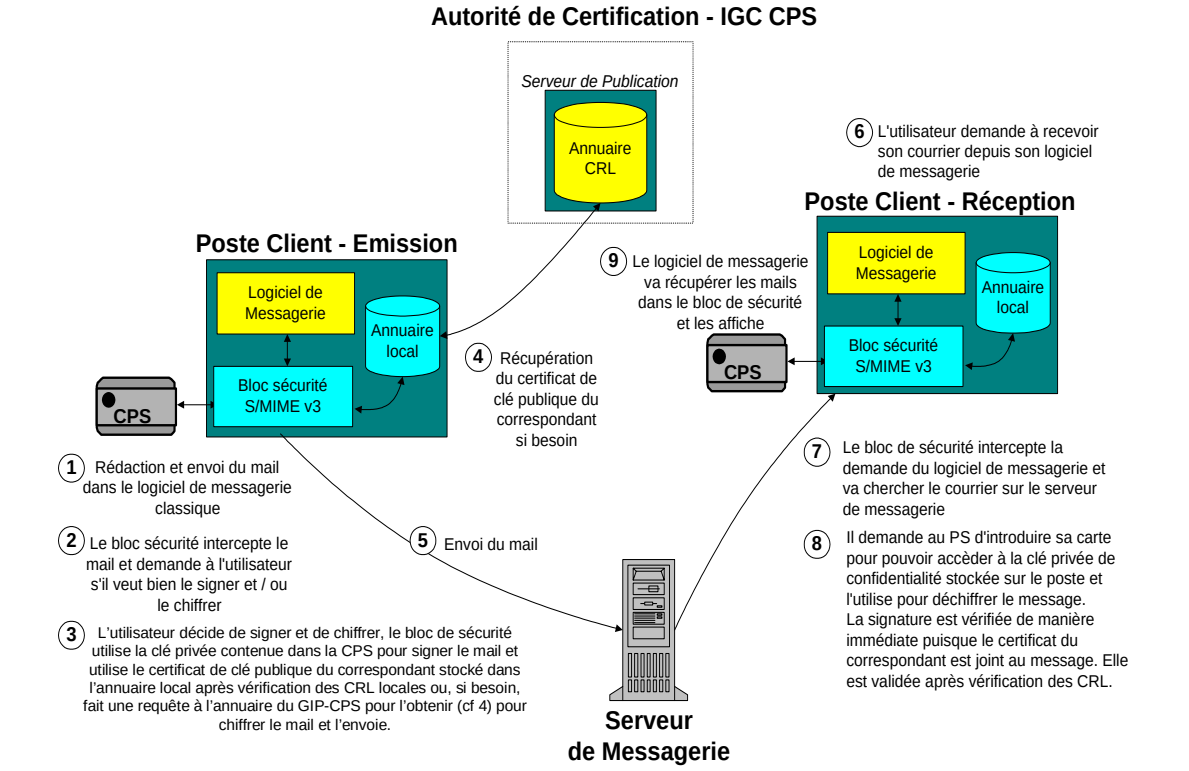
Les séquences des échanges sécurisés entre deux utilisateurs de la CPS, sont décrites dans les schémas ci-après :



Envoi d'un message signé

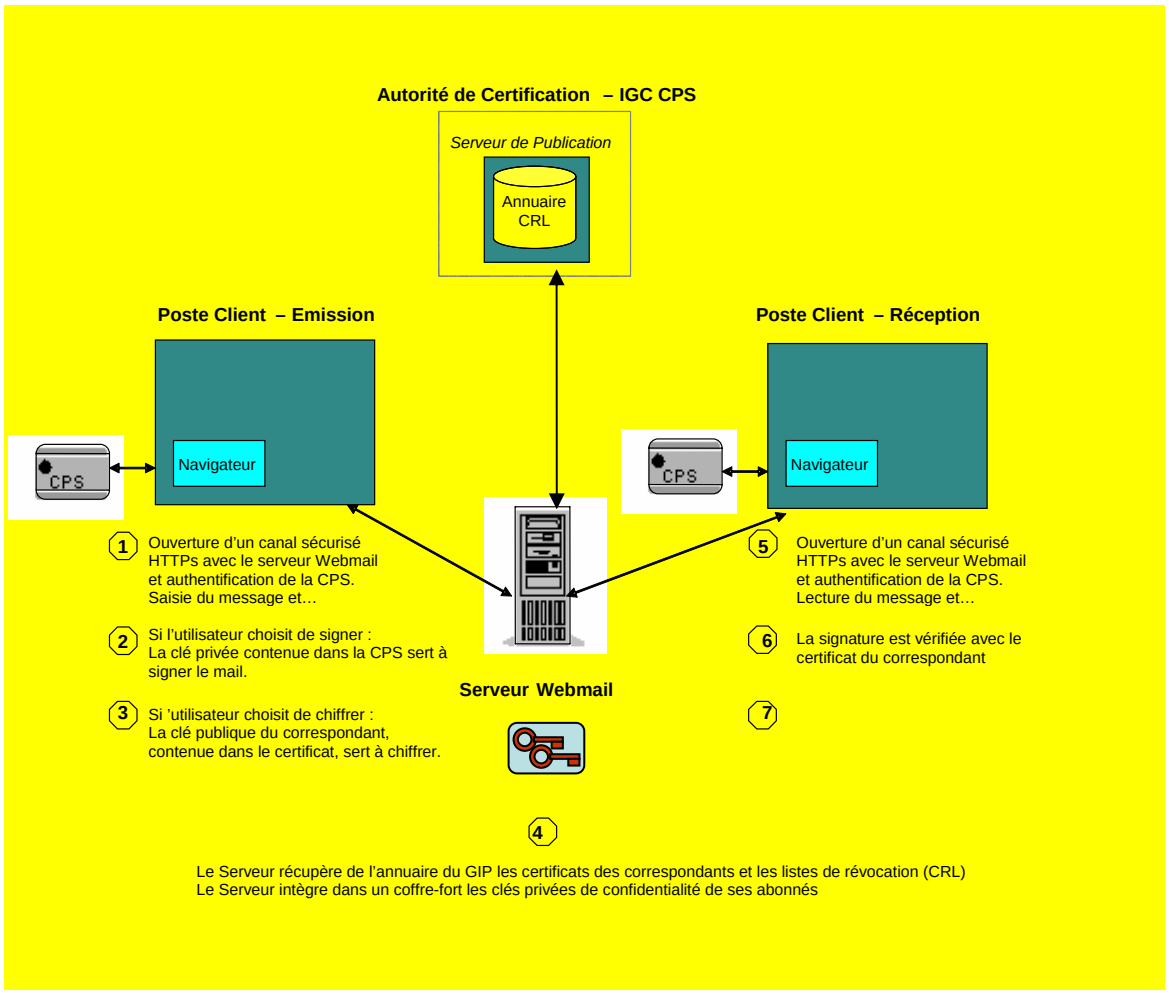


Envoi d'un message chiffré



Envoi d'un message signé, puis chiffré

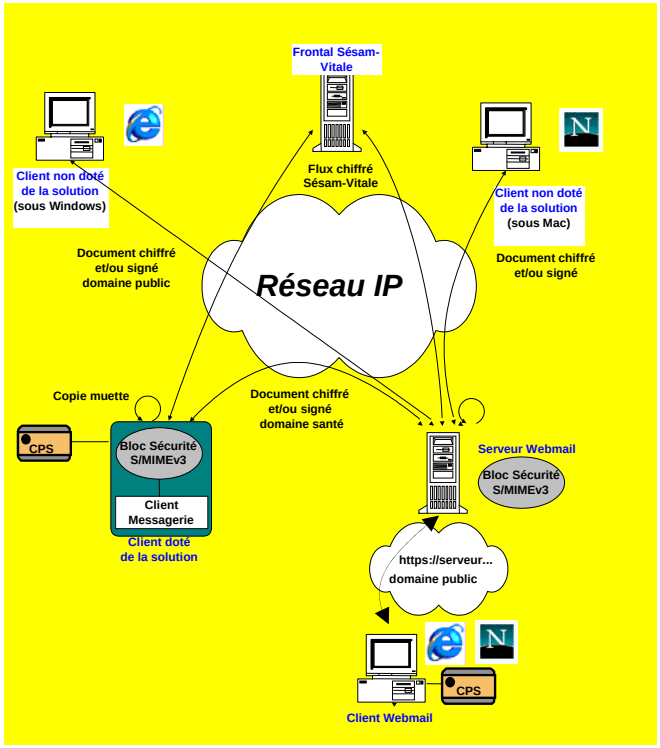
Les séquences des échanges sécurisés entre deux utilisateurs de la CPS et d'une Solution de type Webmail, sont décrites dans le schéma ci-après :



Il est important pour la suite du document de préciser que la carte CPS est entièrement compatible avec la norme X.509. Ceci permet d'être interopérable avec les infrastructures de gestion de clé du commerce et de pouvoir signer et chiffrer des messages pour la plupart des logiciels de messagerie.

Les messages sécurisés sont au format S/MIME et peuvent être échangés :

- ✓ A l'intérieur du domaine de la santé (les deux correspondants sont dotés d'une Solution et équipés de cartes CPS) ;
- ✓ Depuis le domaine de la santé (l'émetteur est doté d'une Solution et équipé d'une carte CPS) vers l'extérieur avec la limitation suivante :
  - ◊ Les messages signés par des CPS peuvent donner lieu à des messages d'alerte liés à l'absence d'adresse e-mail dans le certificat de signature[1].
- ✓ Depuis l'extérieur (le destinataire est non doté de la Solution) vers le domaine de la santé ;
- ✓ Entre un émetteur doté d'une Solution et équipé d'une carte CPS et un frontal SESAM-Vitale et inversement.



[1] *La présence d'une adresse e-mail dans les certificats est vérifiée par beaucoup de produits du marché.*

3. Démarche de l'homologation

3.1 Avant-propos

Parmi les applications de la CPS, l'Outil de Sécurisation de Messagerie (OSM) sera sans aucun doute un des plus utilisés et un des plus stratégiques pour la promotion de ce système. Le GIP-CPS n'ayant pas pour vocation de définir et de développer une application de messagerie spécifique à la CPS, il a été décidé de fournir à des industriels les moyens de développer eux-mêmes des produits qu'ils pourront proposer aux professionnels de la santé.

3.2 Objectifs et avantages du processus déclaratif

L'objectif principal d'un processus d'homologation de type « déclaratif » est de permettre aux industriels de développer leur propre solution, sans contrainte de technologie ou d'ergonomie, tout en offrant l'avantage d'un cadre « réglementaire » permettant de spécifier des exigences particulières au domaine de la santé en terme de fonctionnalité et d'interopérabilité.
Le but est donc de fournir aux futurs clients les moyens de choisir en toute confiance des produits de sécurisation pour leur messagerie professionnelle en garantissant :

- Le fonctionnement de la Solution dans certains environnements,
- La robustesse des mécanismes de sécurité implantés dans la Solution,
- La présence des fonctionnalités propres à l'utilisation de la CPS.

C'est la concurrence entre les industriels qui doit par la suite faire évoluer les solutions et les technologies et également promouvoir l'utilisation de la CPS dans le cadre de la messagerie professionnelle.

3.2.1 Les acteurs du processus d'homologation

Le GIP-CPS définit, publie et met à jour le Référentiel d'Homologation pour permettre aux Industriels de fournir des Produits conformes. Il agrée des auditeurs afin de vérifier que les Produits fournis par les Industriels sont conformes aux exigences du Référentiel. Il veille en particulier à la compétence des auditeurs ainsi qu'à leur objectivité, leur impartialité et à la répétabilité des résultats.

Le Comité d'Homologation est garant du Processus d'Homologation en particulier sur les aspects : objectivité, impartialité et répétabilité de l'audit réalisé. Le comité valide l'audit et rend un verdict sur l'Homologation du Produit.

L'Auditeur agréé par le GIP-CPS, il réalise un audit de vérification du produit selon le cahier de recette proposé dans le Référentiel.

L'Industriel réalise et teste le Produit candidat à l'Homologation. Il se conforme au Référentiel pour la réalisation des fonctionnalités du Produit et réalise les tests d'interopérabilité exigés. Il établit et dépose une Déclaration de Conformité et un Dossier Produit auprès du GIP-CPS en vue de son Homologation.

3.2.2 Homologation d'un Produit

La démarche d'homologation d'une Solution s'effectue selon le document « Plan d'Assurance Qualité. Processus d'Homologation des OSM ».

Ce processus, rappelé ici, s'effectue en plusieurs étapes :

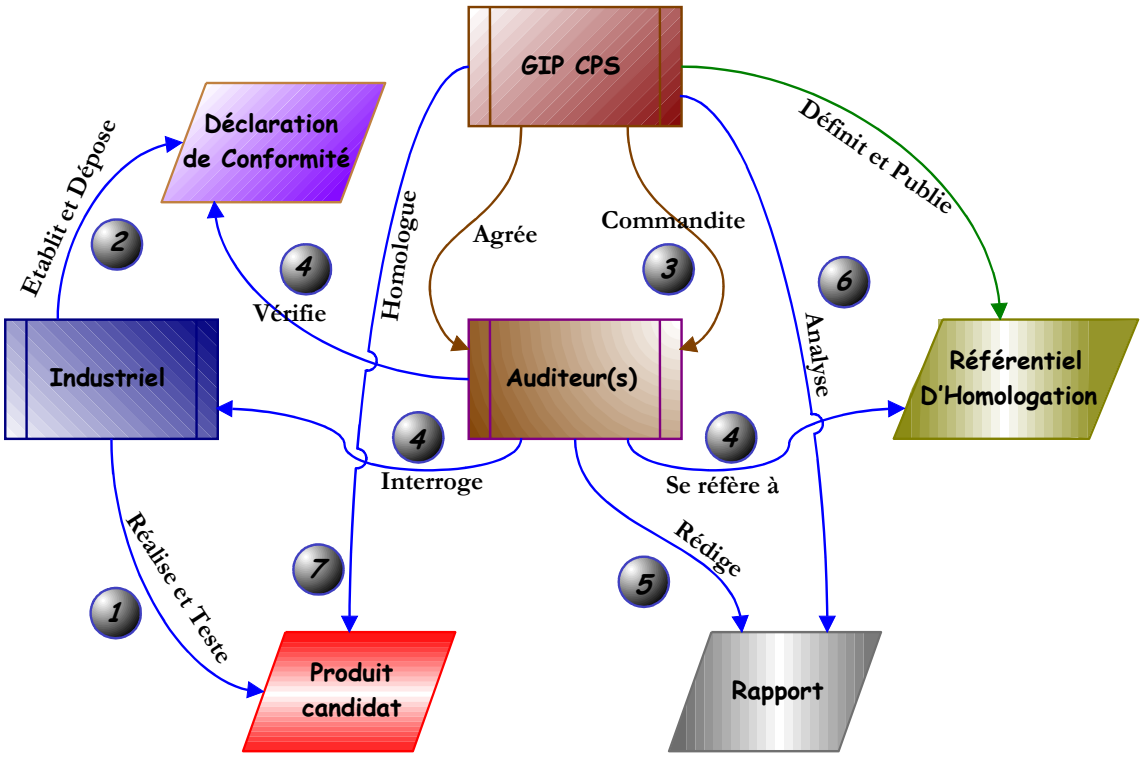
Lorsqu'un industriel souhaite faire homologuer son Produit, il présente au GIP-CPS une Déclaration de Conformité et un Dossier Produit basés sur les exigences du présent document et précisant :

- pour chaque clause obligatoire comment elle est respectée et, si applicable, la configuration de son Produit,
- pour chaque clause optionnelle, si elle est respectée ou non, comment elle est respectée et, si applicable, la configuration de son Produit.

Le comité désignera un Auditeur afin de vérifier le respect du Cahier de Recette ainsi que l'exactitude du "dossier produit".

A la suite de cet audit, il produira un rapport qui sera présenté au Comité d'Homologation qui décidera d'homologuer ou non le Produit.

La liste des Produits homologués sera publiée sur le site Web du GIP-CPS.



4. Exigences fonctionnelles de la Solution

Les exigences suivantes permettent de s'assurer que la Solution est compatible avec les orientations et les spécificités du domaine de la CPS.

Dans le tableau ci-après les exigences sont caractérisées selon trois catégories :

- Obligatoires : le champ « Option » est vide. L'exigence doit être réalisée par le Produit.
- Optionnelle : le champ « Option » est renseigné par l'abréviation OPT. L'exigence peut être réalisée par le Produit. L'Industriel est libre d'implémenter l'exigence.
- Conditionnelle : le champ « Option » est renseigné par l'abréviation COND. L'exigence est obligatoire si le Produit est d'un type particulier, ou qu'il présente une fonctionnalité particulière (ex : fonctionnement en mode proxy).

N°	Option	Libellé
F-1		Le produit doit permettre d'envoyer et de recevoir des messages signés (garantie d'origine et d'intégrité) et/ou chiffrés (garantie de confidentialité), conformément au standard S/MIME version 3. La signature se fera toujours par la CPS (RSA-Encryption), l'algorithme de condensation est obligatoirement le SHA-1. Le chiffrement des messages à envoyer sera effectué avec une clé de session de 128 bits en mode 3DES-CBC.
F-2		Le produit doit permettre l'envoi et la réception de messages non sécurisés (format MIME).
F-3		*Absente.*
F-4		Le code porteur de la carte est demandé la première fois qu'on a besoin d'accéder à la clé privée de signature et reste valide tant que la carte est dans le lecteur et qu'une durée de temps paramétrable n'est pas dépassée.
F-5		Le produit doit garantir que le porteur de la carte ne signe jamais un message à son insu. La responsabilité du produit n'est pas engagée dans les cas suivants : 1. Pré-configuration de traitements automatiques définis sous la responsabilité de l'utilisateur (F-22 et F-23) 2. Traitements automatiques par des applications s'appuyant sur les API du produit (cf. Dossier Produit). En installant/activant ces applications sur son poste, l'utilisateur assume cette responsabilité.
F-6		La signature d'un message doit s'effectuer au plus près de sa création, de préférence dès sa création. Elle peut s'effectuer juste avant l'envoi s'il y a possibilité de revoir le message avant de le signer.
F-7		Lorsque l'utilisateur du produit désire signer et chiffrer un message, le produit doit effectuer ces opérations dans l'ordre suivant : signature puis chiffrement.
F-8	OPT	Le produit peut permettre la conservation des messages signés (messages émis et reçus).

N°	Option	Libellé
F-9		Le produit doit être capable à la réception d'un message signé, de vérifier le certificat de clé publique de signature, conformément aux clauses I-9 à I-13.
F-10		La clé de confidentialité « partageable » doit être stockée de manière protégée dans le poste ou dans le serveur dans le cas d'un produit Webmail (chiffrée avec un mécanisme dont la force est au moins équivalent à un chiffrement avec une clé symétrique de 128 bits) [2].
F-11		*Absent (report vers F-16).*
F-12		Lorsqu'un élément du système est défaillant (lecteur, carte,…), il doit exister un mode de secours dans le produit, permettant à l'utilisateur d'accéder à la clé privée de confidentialité « partageable » pour déchiffrer des messages chiffrés reçus. Le déblocage du produit doit pouvoir être effectué par l'utilisateur du produit. Afin de limiter l'utilisation de ce mode de fonctionnement, son activation doit être suffisamment contraignante pour l'utilisateur afin qu'il ne devienne pas le mode nominal. Il pourra, par exemple, être activé par un mot de passe de secours composé au minimum de 8 caractères.
F-12b	OPT	En mode de secours il est possible d'émettre des messages chiffrés.
F-13		*Absente.*
F-14		Les clés privées de confidentialité « partageable » doivent pouvoir être importées et exportées au format PKCS#12 pour permettre de sauvegarder et d'installer les clés sur un autre poste équipé du même ou d'un autre produit OSM. L'exportation peut être faite uniquement par son détenteur légitime et après authentification de sa carte.
F-15		Le bi-clé de confidentialité « partageable » doit pouvoir être partagé sous la responsabilité du détenteur légitime (en fait, le sujet du certificat de clé publique de confidentialité). Il ne peut y avoir qu'un unique niveau de délégation.
F-16		L'accès à la clé privée de confidentialité « partageable » et son utilisation doivent être protégés par une authentification carte. Pour protéger l'accès au bi-clé de confidentialité « partageable », l'authentification de la carte est obligatoire avant le premier accès à la clé privée de confidentialité (avec, si besoin, la présentation du Code Porteur au préalable). Cette authentification reste valide tant que la carte est présente dans le lecteur et qu'une durée de temps paramétrable n'est pas dépassée.
F-17		*Absente.*
F-18		A chaque émission d'un message chiffré, le produit doit vérifier le certificat de clé publique de confidentialité de chaque destinataire, conformément aux clauses I-9, I-10 et I-12.
F-19	OPT	La Solution est multi-utilisateurs (détenteurs de leur propre clé de confidentialité « partageable ») au sens multi-boîtes-aux-lettres sur un poste unique.
F-20		Le produit doit pouvoir accéder à l'annuaire CPS pour récupérer les certificats de clés publiques des correspondants et les CRL et les delta-CRL correspondantes (la récupération des delta-CRL pour un produit de type Webmail est optionnelle si la gestion des listes est effectuée par le serveur Webmail).

[2] Cette clause, ne pouvant pas faire l'objet de spécifications de tests explicites, ne sera pas vérifiée par l'Auditeur, sa conformité est sous la responsabilité de l'industriel.
Toutefois, le GIP-CPS se réserve le droit de faire contrôler cette conformité en faisant appel à un laboratoire spécialisé pour expertise.

N°	Option	Libellé
F-21		Le produit doit être capable de gérer des listes et des delta-listes de révocation de certificat (la gestion des delta-CRL pour un produit de type Webmail est optionnelle si la gestion des listes est effectuée par le serveur Webmail). Le chargement d'une nouvelle CRL doit se faire au plus tard à la date/heure indiquée dans le champ "nextUpdate" de la CRL en cours. Si, la solution consolide les CRL et delta-CRL dans des fichiers locaux, elle doit protéger l'intégrité de ces fichiers. Le produit est capable de gérer la publication de minimum 25 delta-listes de révocation simultanées.
F-22		Le produit doit permettre, selon une configuration préalable, de signer et/ou de chiffrer automatiquement les messages émis. L'utilisateur est averti si le niveau de sécurité des différents destinataires n'est pas homogène.
F-23	OPT	La configuration préalable (F-22) pour sécuriser des messages de manière automatique peut se faire au travers d'un paramétrage sur critère via une interface homme-machine (IHM) par l'utilisateur (exemples critères : identifiant destinataire, adresse e-mail).
F-24		Le produit doit fonctionner avec un annuaire local de certificats (ou propre à l'utilisateur pour un produit de type Webmail). Cet annuaire local peut être propre à la Solution ou s'appuyer sur un annuaire externe.
F-25	OPT	L'annuaire local du produit permet l'exportation de certificats vers les logiciels de messagerie standard. De même, le produit peut importer des certificats en provenance d'un logiciel de messagerie.
F-26		Le produit doit assurer la fonction « client » auprès du service d'inscription (on-line et/ou par messagerie) mis en place par l'autorité de certification CPS (cf. [CPS-07]).
F-27	COND	**Obligatoire dans le cas d'une solution de type « proxy »**, la Solution doit pouvoir sécuriser les flux SMTP provenant d'autres applications que la messagerie habituelle de l'utilisateur. Dans le cas nominal, à la réception d'un message provenant de la messagerie ou d'une autre application, la Solution demande à l'utilisateur, au travers d'un POP-UP, le traitement sécuritaire à appliquer. Afin qu'une application puisse décider (selon ses propres critères applicatifs et en fonction du type de message) du traitement sécuritaire à appliquer (de façon automatique), elle peut communiquer des paramètres selon la convention suivante : **Convention** : Pour indiquer le traitement à appliquer sur un message SMTP, l'application fait précéder l'objet du message par : **$[Sign]\|[Sign+Chif]\|[Chif]$** [3] **(Sans "$" en première position : traitement habituel du produit)** **Exemples** : • $Sign$: signature ; • $Chif$: chiffrement « partageable » ; • $Sign+Chif$: signature et chiffrement « partageable » ; • $$: pas de traitement (pas de POP-UP). **Après sécurisation, la séquence "$-----$" sera supprimée de l'objet du message (respect F-33).** **Attention**, cette sécurisation automatique prime sur la clause F-22. L'intervention de l'utilisateur se limite à la validation des messages à signer (respect de F-4 et F-5).

[3] *[info] : information optionnelle,*
(info1|info2) : choix obligatoire entre info1 et info2.

N°	Option	Libellé
F-28	COND	**Obligatoire dans le cas d'une solution de type « proxy »**, si la Solution observe qu'un flux S/MIME provient du logiciel de messagerie et que ce flux est déjà sécurisé (cf. RFC 2633 §3.8 "Identifying an S/MIME message"), il le laisse passer tel quel. Ce comportement permet d'éviter que des personnes signent un message chiffré ou sur-chiffrent un message déjà chiffré. Dans le cas où le produit ne peut pas respecter cette clause, l'Industriel doit indiquer dans son "Dossier Produit", son « Manuel d'Installation » et dans son « Manuel d'Utilisation », la configuration du poste PS ou la procédure permettant d'éviter ce problème de double sécurisation.
F-29		La Solution doit informer l'utilisateur du niveau de sécurité des messages sécurisés reçus (chiffré et/ou signé).
F-30		En cas de message signé, l'utilisateur doit être informé du résultat de la vérification (signature message, validité certificat de signature, …) ainsi que de l'identité et la qualité du signataire avec affichage du contenu certificat si souhaitée.
F-31	OPT	Le "point de confiance CPS" peut être pré-chargé lors de l'installation du produit sur le poste du PS.
F-32		Après installation, l'intégration d'un "point de confiance" (AC-Racine-Exploit) doit être validée consciemment par l'utilisateur du produit (l'AC-Racine-TEST ne doit jamais figurer dans la base de confiance du poste).
F-33		La Solution ne doit jamais altérer l'objet du message – ni à l'émission, ni à la réception (risque de perturber des traitements automatiques basés sur le contenu de l'objet).
F-34		NOUVELLE Les désactivation et réactivation de la Solution doivent être possibles afin de permettre les mises à jour des logiciels et matériels sur le poste (ex : lecteur de carte). Le mode opératoire doit être décrit dans la documentation de la Solution.

5. Exigences d'interopérabilité de la Solution

Les exigences suivantes permettent de s'assurer que la Solution est compatible d'une part avec d'autres solutions homologuées et d'autre part est utilisable par les outils de messagerie standard.

Dans le tableau ci-après les exigences sont caractérisées selon trois catégories :

- Obligatoires : le champ « Option » est vide. L'exigence doit être réalisée par le Produit.
- Optionnelle : le champ « Option » est renseigné par l'abréviation OPT. L'exigence peut être réalisée par le Produit. L'Industriel est libre d'implémenter l'exigence.
- Conditionnelle : le champ « Option » est renseigné par l'abréviation COND. L'exigence est obligatoire si le Produit est d'un type particulier, ou qu'il présente une fonctionnalité particulière (ex : fonctionnement en mode proxy).

N°	Option	Libellé
I-1a		Afin de vérifier un premier niveau d'interopérabilité de son produit avec d'autres produits du marché, l'industriel passera des procédures de tests croisés avec au minimum les produits suivants : ◊ Outlook versions 2000, et 2003, ◊ Outlook Express version 6.0, ◊ Mozilla Thunderbird version 1.5, ◊ Lotus Notes version 6, ◊ Les produits déjà homologués par le GIP-CPS. [4]
I-1b	OPT	**Recommandé pour les Solutions Webmail.** Les Solutions Webmail qui s'appuient sur un navigateur web doivent être compatibles avec au moins deux navigateurs (natif + usuel) par système d'exploitation du poste du PS.
I-2		L'utilisateur doit pouvoir recevoir un message sécurisé d'un tiers non doté de la Solution si ce dernier a un logiciel de messagerie compatible S/MIME V2 ou V3 (hors algorithmes – couvert par I-4 et I-5).
I-3		*Absente*
I-4		Le produit doit supporter l'ensemble des algorithmes obligatoires définis dans le profil cryptographique proposé en annexe B du présent document.
I-5	OPT	Le produit peut supporter un ou plusieurs algorithmes optionnels définis dans le profil cryptographique proposé en annexe B du présent document.
I-6	OPT	La Solution peut accéder à d'autres annuaires de façon paramétrable, accessibles via LDAP pour récupérer automatiquement les certificats de clés publiques de confidentialité des correspondants et des listes et des delta-listes de révocation de certificats.
I-7		Si la Solution (installée chez le PS) peut fonctionner dans le mode "test", il ne devra exister aucune ambiguïté pour le destinataire du message. En "mode réel", toute vérification de certificats de test doit donner lieu à des messages d'avertissements explicites. C'est l'extension GipCardCategorie dans le certificat qui le type comme certificat de test. *(Il s'agit d'une carte de test quand le bit de poids fort = '1'.)*
I-8		*Absente*
I-9		Le produit doit être conforme à la RFC 3280 concernant la reconstruction et la vérification du chemin de confiance.
I-10		Le produit doit être conforme à la RFC 3280 concernant la vérification des signatures, des périodes de validité et de la non-révocation des certificats « utilisateur ».

[4] L'auditeur vérifiera en plus l'interopérabilité entre les produits dont l'homologation se fait en parallèle.

N°	Option	Libellé
I-11		Le produit doit détecter et afficher toute erreur concernant la vérification d'une signature.
I-12		Le produit doit afficher au minimum en fin de traitement d'un fichier signé : ◊ reconstruction du chemin de confiance jusqu'à un point de confiance (autorité de racine, CA-RACINE, pour l'IGC CPS) ; ◊ vérification des signatures, des périodes de validité et de la non-révocation des certificats "utilisateur" et "autorités des classes". La procédure doit s'interrompre en cas d'erreur. ◊ affichage à l'utilisateur du résultat de la vérification, avec : - l'état du certificat (révoqué ou non - la Solution doit clairement indiquer si les listes de révocation ont pu être consultées ou si la vérification s'est faite avec des listes périmées qui n'ont pu être mises à jour) + date d'expiration de la CRL, - le DN complet de l'émetteur du certificat, - le DN complet du porteur (sujet) du certificat, - sur demande de l'utilisateur, le détail de tous les champs du certificat doit pouvoir être affiché à l'utilisateur.
I-13	COND	**Obligatoire dans le mode « proxy » et dans le cas où la solution intègre un client de messagerie :** la Solution doit être capable de relayer les données d'authentification (identifiant + mot de passe) via le protocole ESMTP (cf. RFC 2554 SMTP Service Extension for Authentication).

6. Exigences légales de la Solution

N°	Option	Libellé
L-1		Le Produit doit être conforme à la législation française sur la cryptographie.
L-2		L'émetteur de messages chiffrés doit être capable de déchiffrer tout message émis, sur requête des autorités de l'Etat. Et de la même manière, le destinataire de messages chiffrés doit être capable de déchiffrer tout message qui lui est destiné, sur requête des autorités de l'Etat.
L-3	COND	NOUVELLE **Obligatoire pour une Solution de type Webmail.** L'éditeur de la solution Webmail doit informer l'exploitant de la nécessité de déposer une déclaration, ou une demande d'autorisation selon le contexte, auprès de la CNIL.

7. Cahier de Recette de la Solution

La section suivante décrit les différentes étapes que l'Auditeur doit suivre dans le cadre du Processus d'Homologation d'un Produit.

7.1 Environnement nécessaire à la réalisation de l'audit.

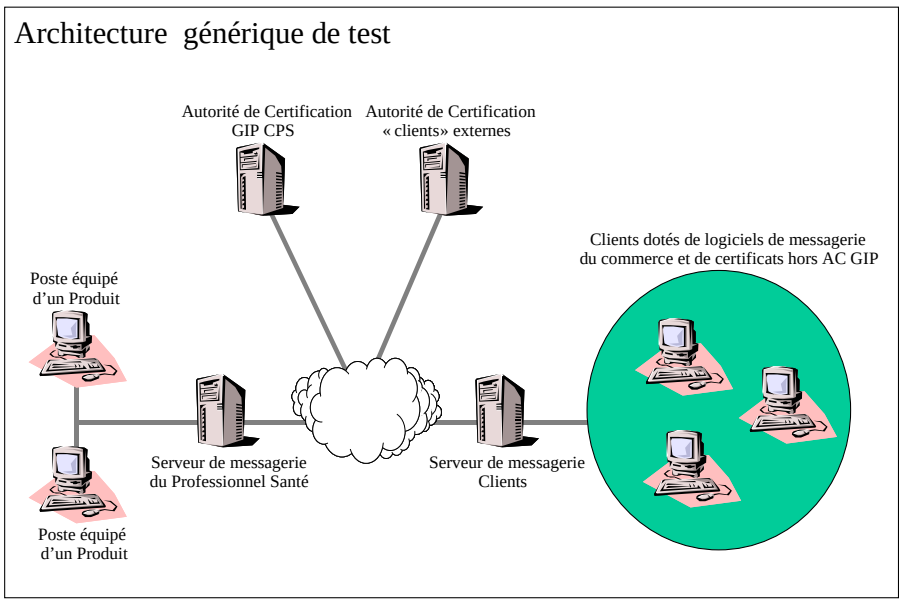
L'Auditeur doit disposer de certains éléments matériels et logiciels pour réaliser l'ensemble des tests. Les éléments fournis par l'Industriel sont les suivants :

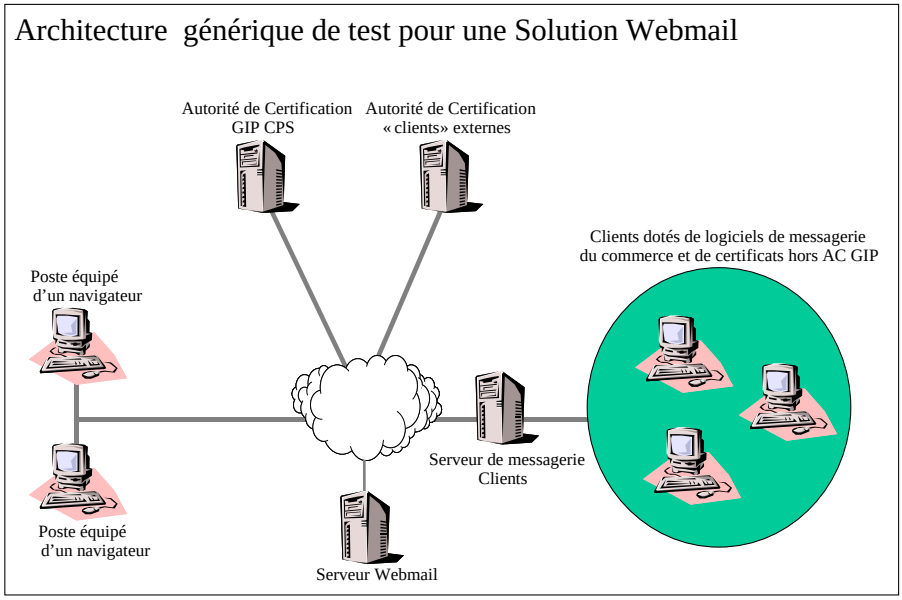
- Deux machines disposant d'un Produit installé par l'Industriel. L'une de ces machines devra être totalement réinstallée lors de la recette. (non applicable dans le cas d'un produit Webmail s'appuyant uniquement sur un navigateur web).
- La plate-forme de test de l'Industriel permettant de reproduire les tests d'interopérabilité avec les différents logiciels de messagerie compatibles avec le Produit qui sont répertoriés dans le Dossier Produit. La plate-forme devra obligatoirement disposer des éléments logiciels permettant d'envoyer des messages électroniques et de dialoguer avec l'Autorité de Certification du GIP-CPS (Annuaire et Serveur d'Inscription), ainsi que l'Autorité de Certification permettant de vérifier les certificats hors CPS utilisés lors des tests.
- Les éléments logiciels nécessaires pour effectuer une réinstallation complète d'un poste (système(s) d'exploitation(s), logiciel(s), Produit). (Non applicable dans le cas d'un produit Webmail).

Les éléments fournis par le GIP-CPS sont les suivants :

- Un jeu de cartes CPS (au moins deux valides et une dont le délai de validité est expiré).
- Un jeu de certificats de confidentialité (dont certains sont révoqués ou périmés) permettant d'effectuer des tests de compatibilité avec les logiciels de messagerie S/MIME V3.

L'architecture utilisée lors des tests peut être issue du schéma ci-après qui expose les différents éléments d'architecture nécessaires à la réalisation des tests. Certains éléments peuvent être situés sur une même machine tant que cela ne nuit pas aux résultats des tests.





7.2 Processus général

7.2.1 Enchaînement des étapes

Le processus général de vérification du Dossier Produit et des exigences du Référentiel que l'Auditeur doit suivre est décomposé en plusieurs étapes :

- Consultation du Dossier Produit fourni par l'Industriel
- Consultation de la documentation du Produit
- Installation et configuration du Produit (par l'Industriel)
- Tests fonctionnels
- Tests d'interopérabilité
- Tests d'installation (non obligatoires dans le cas d'un produit Webmail s'appuyant uniquement sur un navigateur web) et configuration du Produit

Il est important que l'étape de test d'installation et de configuration du Produit s'effectue en dernier. En effet, les tests fonctionnels et d'interopérabilité doivent s'effectuer sur des plates-formes fonctionnant parfaitement. A la suite de ces tests, l'Auditeur devra effectuer une réinstallation complète du poste afin de vérifier le processus d'installation et de configuration du Produit. Quelques tests (fonctionnels et d'interopérabilité) devront être à nouveau effectués pour vérifier que le Produit reste conforme après son installation par l'Auditeur (l'Auditeur peut reprendre certains tests déjà effectués).

7.2.2 Documents réalisés par l'Auditeur

L'Auditeur doit remettre un document présentant l'ensemble des tests effectués et pour chaque test les informations suivantes :

- Référence du test
- Conditions d'exécution
- Résultats obtenus
- Verdict sur le test

Le Cahier de Recette conduit en particulier à l'élaboration d'un tableau de compatibilité de la Solution avec les produits de messagerie standard du marché. Ce tableau est défini dans le dossier produit (voir annexe A).

7.3 Etapes à suivre par l'Auditeur

Les sections suivantes décrivent les tests minima à effectuer par l'Auditeur. Chaque test est constitué d'un paragraphe dont le formalisme est le suivant :

Texte normal : ce test est obligatoire et correspond à une exigence ou à un élément du Dossier Produit obligatoire.
Texte en italique : ce test n'est réalisé que si une exigence ou un élément du Dossier Produit est optionnel.
Référence en [exposant] : le test décrit la vérification d'une exigence du Référentiel.

7.3.1 Consultation du Dossier Produit

T-1. Vérifier que le Dossier Produit est complet et qu'il correspond au Produit à auditer (nom, version).

T-2. Vérifier que la description générale du Produit contient un schéma précisant l'intégration du Produit dans la chaîne de certification et dans le système d'information du client final.

T-3. Vérifier que les exigences obligatoires du Référentiel sont respectées.

T-4. Vérifier l'explication fournie pour le non respect d'une exigence obligatoire. Obtenir de l'Industriel son engagement pour se mettre en conformité et le délai nécessaire.

T-5. Vérifier que les exigences optionnelles du Référentiel suivies par le Produit sont effectivement réalisées.

7.3.2 Consultation de la documentation

T-6. Vérifier l'existence d'un guide de mise en route rapide. Ce guide doit permettre à un utilisateur d'installer et de configurer son produit dans les plus brefs délais. Vérifier qu'il contient au minimum les informations permettant de s'inscrire auprès du Serveur d'Inscription CPS et d'envoyer et de recevoir ses premiers messages.

T-7. Vérifier l'existence d'un manuel utilisateur. Ce manuel doit décrire les procédures d'installation plus fines ainsi que les méthodes de configuration plus élaborées, permettant à un utilisateur plus chevronné de personnaliser son produit et d'exploiter des fonctionnalités avancées (ex : sauvegarde des messages, migration vers un nouveau logiciel de messagerie).

T-8. Vérifier l'existence d'un système d'aide en ligne. L'aide en ligne doit permettre à l'utilisateur d'obtenir des informations contextuelles sur la fonctionnalité qu'il est en train de mettre en œuvre dans le Produit.

T-9. Vérifier que l'ensemble de la documentation fournie est suffisant pour permettre à l'utilisateur final d'obtenir facilement des informations concernant :

- L'installation du produit,
- L'inscription de l'utilisateur,
- L'interopérabilité avec les logiciels de messagerie du commerce.

T-10. Vérifier que la documentation expose les risques liées à l'emploi du Produit (ex : procédures automatisées) et qu'elle contient un guide de bonne pratique sur l'utilisation du produit, qui expose à l'utilisateur quelles précautions il doit prendre (anti-virus, sauvegardes des clés, …) pour utiliser de manière sûre son Produit.

T-11. Vérifier qu'il n'existe pas de mode de fonctionnement automatique permettant au Produit de signer des messages sans prévenir l'utilisateur (sauf paramétrisation sous la responsabilité de l'Utilisateur). [F-5]

7.3.3 Tests fonctionnels

T-12. Supprimé (doublon avec T-13, suite à la suppression de la CPS2).

T-13. Envoyer et recevoir des messages signés et/ou chiffrés, conformément au standard S/MIME version 3 avec une carte CPS. [F-1 + F-29]

T-14. Envoyer à partir du Produit un message non chiffré et non signé vers un correspondant. [F-2]

T-15. Émettre à destination du Produit un message non chiffré et non signé. [F-2]

T-16. Si le Produit ne demande pas systématiquement la saisie du code porteur lors de la signature d'un message, vérifier que le code porteur est invalidé lorsque la carte est retirée du lecteur. Si le Produit propose une durée de validité pour le code porteur, vérifier cette durée en tentant d'émettre deux messages signés dont le deuxième se situe après la période de validité. Vérifier que le Produit demande à nouveau le code porteur. [F-4]

T-17. Effectuer la signature d'un message. Vérifier qu'il n'est pas possible de le modifier avant son envoi définitif sans que l'utilisateur puisse à nouveau en contrôler le contenu ou que le produit prévienne l'utilisateur que le contenu a été modifié. [F-6]

T-18. En chiffrant un message vérifier que le Produit empêche par la suite la signature du message. [F-7]

T-19. Archiver les messages précédemment signés et chiffrés (reçus et émis) en utilisant la fonction fournie par le produit. Effectuer une restauration de ces messages et vérifier à nouveau les signatures. [F-8]

T-20. Émettre vers le Produit un message signé. A réception du message, vérifier le certificat de clé publique de signature du correspondant. [F-9]

T-21. Sauvegarder le fichier contenant la clé de confidentialité sans passer par les fonctionnalités du Produit (prendre le fichier directement). Exporter ce fichier vers un autre poste disposant d'un autre ou du même Produit et vérifier que ce fichier n'est pas directement exploitable. [F-14]

T-22. Vérifier qu'il est impossible de déchiffrer un message chiffré sans qu'une carte CPS soit présente dans le lecteur et sans activer le mode secours. [F-16]

T-23. Sur le poste disposant du Produit, tester la réception d'un message chiffré sans utilisation de la carte CPS ayant servi à générer la clé de confidentialité et vérifier que la clé est inutilisable sans une carte CPS d'un tiers autorisé (et sans mettre en œuvre le mode de secours). [F-12]

T-24. Retirer la CPS du poste disposant du Produit, puis activer le mode de secours avec un mot de passe correct et vérifier que les messages reçus peuvent être déchiffrés. [F-12]

T-25. Vérifier que le mode de secours permet l'envoi d'un message chiffré, mais exclut l'utilisation de la signature. [F-12b]

T-26. Sur le poste disposant du Produit, activer le mode de secours et vérifier que la clé de confidentialité peut être directement exploitée sans CPS et qu'il existe un mécanisme de protection d'utilisation de ce mode (ex : mot de passe de secours composé au minimum de 8 caractères). [F-12]

T-27. Exporter une clé de confidentialité depuis un poste disposant du Produit vers un autre poste disposant également du Produit. Vérifier que l'exportation puisse s'effectuer uniquement après authentification de la carte du détenteur légitime.
Essayer une exportation, notamment en mode secours et avec une carte de délégué, en vérifiant que l'exportation est rejetée. [F-14]

T-28. Vérifier que le bi-clé de confidentialité « partageable » peut être partagé (un seul niveau autorisé) et que la documentation est correcte. Effectuer un test d'émission et de réception de message dans ce mode. [F-15]

T-29. Démarrer le produit en ayant retiré la carte du lecteur. Vérifier que le produit refuse de se lancer et propose éventuellement le mode de secours. [F-16]

T-30. Émettre un message chiffré vers le poste disposant du Produit en ayant retiré préalablement la carte CPS du lecteur. Vérifier qu'il est impossible de déchiffrer le message sans carte (et sans avoir recours au mode secours). [F-16]

T-31. Émettre depuis le poste disposant du Produit un message chiffré vers plusieurs destinataires dont un ou plusieurs ont un certificat révoqué. Vérifier que le Produit refuse d'émettre le message vers le destinataire dont le certificat est révoqué et qu'il prévient l'utilisateur par un message d'erreur. [F-18 + I-12]

T-32. Vérifier que le produit gère correctement les CRL et delta-CRL (la récupération des delta-CRL pour un produit de type Webmail est optionnelle si la gestion des listes est effectuée par le serveur Webmail) en utilisant des certificats révoqués (vérification du certificat de confidentialité avant chiffrement, vérification du certificat de signature lors du contrôle de la signature d'un message reçu). [F-20 + F-21]

T-33. Mettre en œuvre l'automatisation de l'envoi de messages vers un destinataire particulier. Vérifier que les certificats de confidentialité sont toujours vérifiés en utilisant des destinataires dont le certificat est révoqué ou périmé. [F-22]

T-34. Vérification de l'automatisation de l'envoi de message par IHM. [F-23]

T-35. Vérifier l'existence d'un annuaire local. [F-24]

T-36. Exporter un certificat de confidentialité d'un logiciel de messagerie standard, puis l'importer dans l'annuaire local du produit audité. Vérifier l'importation en émettant un message chiffré vers le destinataire dont le certificat a été importé. [F-25]

T-37. Exporter un certificat de l'annuaire local du Produit vers un logiciel de messagerie standard. Vérifier l'exportation en émettant un message chiffré à l'aide de la clé de confidentialité d'un destinataire dont le profil a été importé. [F-25]

T-38. Vérification de l'automatisation de l'envoi de message par une application de test fournie par l'Industriel. [F-27 COND]

T-39. Émettre un message avec le Produit de type proxy vers un poste équipé d'un logiciel de messagerie standard. Vérifie que le format du message est conforme à l'exigence conditionnelle F-27. Vérifier que lors de l'envoi du message, l'utilisateur est informé du traitement effectué par le proxy. [F-27 COND]

T-40. Émettre un message déjà signé par le logiciel de messagerie vers le Produit de type proxy. Vérifier que le Produit n'effectue pas une autre opération de signature. Vérifier ce fonctionnement avec un message chiffré, avec un message signé/chiffré. [F-28 COND]

T-41. Émettre un message signé/chiffré vers un poste disposant d'un Produit. Vérifier que le Produit informe l'utilisateur que le message est signé et chiffré. Vérifier que le Produit informe l'utilisateur sur la validité de la signature et qu'il indique le nom et la qualité de l'émetteur. Vérifier que le Produit propose à l'utilisateur de visualiser le certificat. [F-30]

T-42. Émettre un message depuis un poste disposant d'un Produit en inscrivant dans l'objet du message un texte quelconque d'au moins une trentaine de caractères. Vérifier que l'objet du message n'est pas altéré sur le poste qui reçoit le message. Renvoyer vers le poste disposant du Produit le message reçu et vérifier que le Produit n'altère pas l'objet du message en réception. [F-33]

T-43. Vérifier qu'il existe un moyen de désactiver le Produit pour permettre la mise à jour du poste et que son mode opératoire est décrit dans la documentation du Produit. [F-34]

T-44. Vérifier qu'il est possible de réactiver le Produit suite à une désactivation [F-34]

7.3.4 Tests d'interopérabilité

T-45. Vérifier que le mode de récupération des CRL et delta-CRL est conforme à celui annoncé dans le Dossier Produit.

T-46. Vérifier que le fonctionnement du mode de récupération des CRL et delta-CRL est exposé dans la documentation utilisateur (la récupération des delta-CRL pour un produit de type Webmail est optionnelle si la gestion des listes est effectuée par le serveur Webmail).

T-47. Effectuer un test de réception d'un message dont le certificat de signature est révoqué. Vérifier que le produit informe l'utilisateur d'une erreur. [I-10 + I-12]

T-48. Vérifier qu'à la réception d'un message, l'utilisateur est capable d'effectuer une vérification du chemin de confiance. [I-9]

T-49. Vérifier qu'à la réception d'un message, l'utilisateur est capable d'effectuer une vérification de la signature. [I-11]

T-50. Vérifier que les mécanismes cryptographiques obligatoires inscrits dans le profil cryptographique du Dossier Produit sont effectivement réalisés. Effectuer des tests de mise en œuvre de ces mécanismes (voir tests suivants). [I-4]

T-51. Tester que les mécanismes cryptographiques optionnels réalisés par le Produit le sont effectivement. Effectuer des tests de mise en œuvre de ces mécanismes (voir tests suivants). [I-5]

Tests sur les mécanismes cryptographiques [I-2]

T-52. Pour chaque logiciel de messagerie décrit comme compatible dans le Dossier Produit, émettre un message signé depuis le Produit. Vérifier les résultats obtenus par rapport au tableau de compatibilité du Produit.

T-53. Pour chaque logiciel de messagerie décrit comme compatible dans le Dossier Produit, émettre un message chiffré depuis le Produit. Vérifier les résultats obtenus par rapport au tableau de compatibilité du Produit. Effectuer ce test pour l'ensemble des algorithmes fournis par le Produit.

T-54. Pour chaque logiciel de messagerie décrit comme compatible dans le Dossier Produit, émettre un message signé et chiffré depuis le Produit. Vérifier les résultats obtenus par rapport au tableau de compatibilité du Produit. Effectuer ce test pour l'ensemble des algorithmes fournis par le Produit.

T-55. Pour chaque logiciel de messagerie décrit comme compatible dans le Dossier Produit, recevoir un message signé écrit depuis le Produit. Vérifier les résultats obtenus par rapport au tableau de compatibilité du Produit. Effectuer ce test pour l'ensemble des algorithmes fournis par le Produit.

T-56. Pour chaque logiciel de messagerie décrit comme compatible dans le Dossier Produit, recevoir un message chiffré écrit depuis le Produit. Vérifier les résultats obtenus par rapport au tableau de compatibilité du Produit. Effectuer ce test pour l'ensemble des algorithmes fournis par le Produit.

T-57. Pour chaque logiciel de messagerie décrit comme compatible dans le Dossier Produit, recevoir un message signé et chiffré écrit depuis le Produit. Vérifier les résultats obtenus par rapport au tableau de compatibilité du Produit. Effectuer ce test pour l'ensemble des algorithmes fournis par le Produit.

Tests sur la compatibilité MIME. [F-2]

T-58. Pour chaque logiciel de messagerie décrit comme compatible dans le Dossier Produit, émettre un message au format texte depuis le Produit. Vérifier que le contenu n'est pas altéré et qu'il est compréhensible pour l'utilisateur. Effectuer à nouveau ce test en réception vers le Produit.

T-59. Pour chaque logiciel de messagerie décrit comme compatible dans le Dossier Produit, émettre un message au format texte accompagné d'une pièce jointe depuis le Produit. Vérifier que le contenu n'est pas altéré, qu'il est compréhensible pour l'utilisateur et que la pièce jointe est exploitable. Effectuer à nouveau ce test en réception vers le Produit.

T-60. Pour chaque logiciel de messagerie décrit comme compatible dans le Dossier Produit, émettre un message au format HTML accompagné d'une pièce jointe depuis le Produit. Vérifier que le contenu n'est pas altéré, qu'il est compréhensible pour l'utilisateur et que la pièce jointe est exploitable. Effectuer à nouveau ce test en réception vers le Produit.

7.3.5 Tests d'installation et configuration du Produit

T-61. Effacer l'intégralité d'un poste disposant d'un produit (système d'exploitation, logiciels, Produit). Installer à nouveau le système d'exploitation et les logiciels nécessaires aux tests, puis passer au test suivant pour valider la procédure d'installation du Produit. (non applicable dans le cas d'un produit Webmail s'appuyant uniquement sur un navigateur web).

T-62. Vérifier que la procédure d'installation exposée dans la documentation est conforme en rejouant les différentes étapes qui y sont décrites. (non applicable dans le cas d'un produit Webmail s'appuyant uniquement sur un navigateur web).

T-63. Vérifier que la procédure d'installation est réussie. [F-31] (non applicable dans le cas d'un produit Webmail s'appuyant uniquement sur un navigateur web).

T-64. Vérifier que la procédure d'inscription d'un utilisateur exposée dans la documentation est conforme en rejouant les différentes étapes qui y sont décrites. [F-26]

T-65. Vérifier que l'inscription de l'utilisateur a réussi. [F-26]

T-66. Vérifier que l'intégration du « point de confiance » AC-Racine-Exploit n'est faite qu'après validation de la part de l'utilisateur. [F-32]

T-67. Vérifier que la documentation décrit le mode de récupération des clés publiques de correspondants CPS ou non.

T-68. Effectuer un test de récupération d'un certificat de clé publique d'un correspondant disposant d'une CPS. [F-20]

T-69. Effectuer un test de récupération d'une CRL et d'une delta-CRL (la récupération des delta-listes pour un produit de type Webmail est optionnelle si la gestion des listes est effectuée par le serveur Webmail) pour chaque autorité racine et chaque autorité intermédiaire de l'IGC CPS. [F-21]

T-70. Effectuer un test de récupération d'une clé publique d'un correspondant ne disposant pas d'une CPS (test d'accès à d'autres annuaires que celui du GIP). [I-6]

T-71. Vérifier que le Produit permet la configuration de plusieurs utilisateurs ayant chacun leur propre clé de confidentialité. Tester l'envoi et la réception d'un message pour chaque utilisateur. [F-19]

T-72. Vérifier que le Produit accepte la configuration de plusieurs boîtes aux lettres. Tester l'envoi et la réception d'un message pour chaque boîte aux lettres. *[F-19]*

T-73. Récupérer un message signé avec une carte de test et vérifier que l'utilisateur soit averti par un message sans aucune ambiguïté. [I-7]

T-74. Vérifier, à partir d'un poste disposant d'un produit, la possibilité d'émettre et de recevoir des messages avec un Internet Service Provider qui authentifie ses clients au travers du protocole ESMTP « client authentication », en utilisant par exemple le serveur "smtp.mail.yahoo.fr". [I-13 COND]

ANNEXE A – Dossier Produit Type

Cette annexe décrit le dossier qui doit être rempli par l'industriel pour présenter sa solution au processus d'homologation. Ce dossier permet à l'Auditeur d'effectuer une pré-évaluation de la conformité de la Solution par rapport au référentiel.

Partie Administrative

Nom du produit : …….

Version du produit : …….

Remplir un Dossier Produit par version de produit et par système d'exploitation.

Renseignements administratifs de la société

Société : ……

Adresse :

……

……

Téléphone : …… Fax : ……

SIRET : …….

Personne chargée du dossier

Nom : …….

Téléphone : …….

E-mail : …….

Nature de la demande

- ❑ Initiale
- ❑ Suite à évolution du Référentiel d'Homologation
- ❑ Suite à changement de version
- ❑ Suite à mise à jour du produit
  - Nature de la mise à jour : ……

Autorisation de fourniture de produits cryptographiques

N° et date d'autorisation DCSSI : …….

Partie technique

Fonctionnement général du Produit

Description générale du fonctionnement du produit[5].

Quel critère est utilisé par le produit afin d'authentifier la carte ?

- ❑ N° carte physique.
- ❑ DN du porteur du certificat de signature.
- ❑ DN du porteur du certificat de confidentialité.

Décrire l'enchaînement des tâches pour créer et signer un message. En particulier, décrire les opérations effectuées sur le message entre sa création, sa signature et son envoi effectif. Décrire le(s) mécanisme(s) qui empêche(nt) un message d'être altéré entre sa création et sa signature, et notamment dans une situation Proxy, avec l'option « envoi différé » activée. Si besoin, décrire la configuration du poste nécessaire.

[5] Cette description doit s'agrémenter d'un schéma expliquant l'intégration du Produit dans la chaîne de certification et dans le système d'information du client.

Indiquer comment l'utilisateur peut conserver ses messages signés (reçus et émis). Si besoin, décrire la configuration du poste nécessaire.

Existe-t'il un moyen de sécuriser de manière automatique des messages ? ❑ OUI ❑ NON

Si oui, décrire les différentes configurations possibles. Et indiquer comment le Produit réagit lorsque le niveau de sécurité n'est pas homogène entre plusieurs destinataires d'un message émis automatiquement.

Décrire comment le Produit informe l'utilisateur du résultat de la vérification à la réception d'un message sécurisé.

Décrire comment l'utilisateur peut re-vérifier une signature sur un ancien message.

Décrire le fonctionnement général de l'annuaire local, en particulier son interconnexion avec les carnets d'adresses des logiciels de messageries classiques. Indiquer combien de correspondants peuvent être gérés.

Décrire quel est le mode d'intégration des « points de confiance » et notamment les « AC-Racine-Exploitation » de l'IGC CPS.

Quel est le mode d'enregistrement auprès du serveur d'inscription ?

- ❑ Messagerie
- ❑ En ligne

Décrire comment le Produit récupère les certificats de clés publiques de confidentialité de ses correspondants. En particulier, préciser à quel moment le Produit récupère et vérifie ces certificats et comment ils sont stockés dans l'annuaire local du Produit.
Indiquer combien de certificats peuvent être stockés dans l'annuaire local.

Pour la vérification des certificats révoqués le produit utilise :

- ❑ Des CRL
- ❑ Des delta-CRL

Description du mode de récupération des listes et des delta-listes de révocation. Préciser le mécanisme utilisé, son caractère manuel ou automatique, sa périodicité, ses différentes configurations possibles pour l'utilisateur.

Description de la procédure de partage de la clé de confidentialité (y compris la procédure d'annulation de ce partage).

Décrire la procédure de secours, suite à une panne de lecteur ou autre incident (activation et désactivation de ce mode).

Décrire comment le porteur effectue la « reprise » d'une clé de confidentialité « partageable » en cas de remplacement d'une carte suite à son expiration et en cas de remplacement anticipé (vol ou perte de la carte).

Le Produit propose-t-il un mode de test ? ❑ OUI ❑ NON

Si oui, décrire la procédure d'activation et de désactivation de ce mode. Décrire comment l'utilisateur est informé du mode de fonctionnement en cours.

Description de l'accès aux autres annuaires accessibles en LDAP (mode de configuration et ordre ?) pour les certificats de clés publiques, les CRL et les delta-CRL.

Documentation & support technique

Existe-t-il une documentation du produit : ❑ OUI ❑ NON

Si oui, cette documentation concerne :

- ❑ L'installation et la configuration rapide du produit,
- ❑ L'utilisation du produit.

La documentation est-elle sous forme :

- ❑ Papier,
- ❑ En ligne,
- ❑ Électronique (CD-Rom).

La documentation contient-elle des conseils d'utilisation du Produit, en particulier sur l'environnement de fonctionnement (ex : précautions d'emploi) : ❑ OUI ❑ NON

Si oui, décrire les hypothèses d'environnement (anti-virus, sauvegardes, ...).

Un support technique est-il proposé au client final ? ❑ OUI ❑ NON

Si oui, de quelle nature : ……..

Quelle est la politique de mise à jour du produit ?

- ❑ Patches, hotfix à télécharger
- ❑ Mise à jour de version par cédérom
- ❑ Autre : ……..

Est-ce que le Produit offre des interfaces programmatiques (API) ? : ❑ OUI ❑ NON

Si oui, annexer au présent Dossier Produit la description technique de ces APIs.

Garantissez-vous la compatibilité ascendante de ces interfaces programmatiques (API) ? :

❑ OUI ❑ NON

Quelle est la politique de mise à jour de l'Industriel en cas de changement de génération de la carte CPS ?

Le Dossier Produit de la Solution contient obligatoirement un tableau précisant :

- pour **chaque clause obligatoire**, comment elle est respectée et, si applicable, la configuration du Produit,
- pour **chaque clause optionnelle**, si elle est respectée ou non, comment elle est respectée et, si applicable, la configuration du Produit.

Ce tableau est défini comme suit :

	Exigence	Respectée	Commentaire
Exigences obligatoires	F-1	OUI	
	F-4	OUI	
	I-6	NON	La Solution utilise une technologie ne permettant pas de respecter intégralement l'exigence. Les utilisateurs sont avertis de ce fait dans la documentation commerciale et dans la documentation d'exploitation.
Exigences optionnelles	F-2	NON	
	I-3	NON	
	I-5	OUI	
Exigences conditionnelles	F-27	OUI	

Les exigences du tableau ci-dessus ne sont données qu'à titre d'exemple. Se reporter aux exigences d'interopérabilité et de fonctionnalité pour établir le tableau réel.

Les exigences non optionnelles doivent être accompagnées d'un commentaire permettant à l'Industriel d'expliquer la non-couverture de l'exigence.

Le Dossier Produit doit comporter des tableaux d'interopérabilité, permettant de garantir à l'Utilisateur quels sont les logiciels de messagerie classiques (en version française) avec lesquels le Produit est capable d'émettre et/ou de recevoir des messages signés et/ou chiffrés.

Les tableaux sont définis comme suit :

Logiciel	Signé		Chiffré		Signé + Chiffré	
Outlook (version 2000)	E		E		E	
	R		R		R	
Outlook (version 2003)	E		E		E	
	R		R		R	
Outlook Express (version 6.0)	E		E		E	
	R		R		R	
Mozilla Thunderbird (version 1.0)	E		E		E	
	R		R		R	
Lotus Notes (version 6)	E		E		E	
	R		R		R	
Autre(s) logiciels de messagerie	E		E		E	
	R		R		R	

Légende : E = Emission (envoi du Produit vers le logiciel testé)

R = Réception (envoi du logiciel testé vers le Produit)

Dans le cas de Solutions de type Webmail s'appuyant sur un navigateur web, le Dossier Produit indiquera la compatibilité de la solution avec les navigateurs web (natifs et usuels) :

Navigateur	Système d'exploitation
Internet Explorer	Windows
Safari	Mac OS-X
Mozilla Firefox	Windows, Mac OS X, Linux
Autres ?	

Ces tests seront effectués avec des cartes CPS réelles.

Le dossier contient le profil cryptographique du Produit qui doit être conforme à celui donné en annexe B, augmenté éventuellement d'autres mécanismes propres à la Solution développée.

Mécanismes cryptographiques		Produit		Système CPS	
		Emission	Réception	Emission	Réception
Algorithmes de condensation					
- SHA-1	(FIPS 180-1)			OBL	OBL
- SHA-256	(FIPS 180-2)			OPT[6]	OBL[7]
- MD5	(RFC 1321)			OPT	OBL
Algorithmes de signature					
- DSA	(FIPS 186)			NA	OPT
- RSA-Encryption	(PKCS#1)			OBL	OBL
Algorithmes de gestion de clés					
Algorithmes d'échange de clés					
- Diffie-Hellman	(RFC 2631)			OPT	NE
- RSA-Encryption	(PKCS#1)			OBL	OBL
Algorithmes de chiffrement de clés					
- 3DES pour clés 3DES	(FIPS 74)			OPT	NE
- RC2 pour clés RC2	(RFC 2268)			OPT	NE
- mixte				OPT	NE
Algorithmes de chiffrement de données					
- Triple DES	(3DES CBC – FIPS 74)			OBL	OBL
- RC2	(RC2 CBC - RFC 2268)			OPT	OPT
- CAST-128	(RFC 2144)			OPT	OPT
- IDEA	(RFC 3058)			OPT	OPT
- AES	(FIPS 197)			OPT[8]	OPT

OBL : Obligatoire
OPT : Optionnelle
NA : Non applicable
NE : Non Exigé (et non testé, car hors champ d'application)

[6] L'algorithme SHA-256 ne doit pas être utilisé, pour cette version du référentiel, en émission par défaut
[7] Attention : SHA-256 peut être utilisé sur les messages et sur les certificats X.509
[8] L'algorithme AES ne doit pas être utilisé, pour cette version du référentiel, en émission par défaut

ANNEXE B – Profil cryptographique d'une Solution de messagerie utilisant la carte CPS

Mécanismes cryptographiques		S/MIME V3	Système CPS	
			Emission	Réception
Algorithmes de condensation				
- SHA-1	(FIPS 180-1)	OBL	OBL	OBL
- MD5	(RFC 1321)	OPT	OPT	OBL
Algorithmes de signature				
- DSA	(FIPS 186)	OBL	NA (1)	OPT
- RSA-Encryption	(PKCS#1)	OPT	OBL (6)	OBL (2)
Algorithmes de gestion de clés				
Algorithmes d'échange de clés				
- Diffie-Hellman	(RFC 2631)	OBL	OPT	NE (3)
- RSA-Encryption	(PKCS#1)	OPT	OBL (7)	OBL (8)
Algorithmes de chiffrement de clés				
- 3DES pour clés 3DES	(FIPS 74)	OBL	OPT	NE (3)
- RC2 pour clés RC2	(RFC 2268)	OPT	OPT	NE (3)
- mixte		OPT	OPT	NE (3)
Algorithmes de chiffrement de données				
- Triple DES	(3DES CBC - FIPS 74)	OBL	OBL (4)	OBL (5)
- RC2	(RC2 CBC - RFC 2268)	OPT	OPT	OPT
- CAST-128	(RFC 2144)	OPT	OPT	OPT
- IDEA	(RFC3058)	OPT	OPT	OPT

OBL : Obligatoire
OPT : Optionnelle
NA : Non applicable
NE : Non Exigé (et non testé, car hors champ d'application)

Renvois du tableau :

1. La CPS ne supporte pas l'algorithme DSA (et l'IGC CPS ne certifie pas des clés de ce type).
2. Longueur de la clé de signature de 512 à 4.096 bits.
3. Non applicable, la CPS ne supporte pas l'algorithme DH.
4. Longueur des clés de confidentialité de 128 bits (112 bits effectifs).
5. Longueur des clés de session de 128 ou 192 bits (112 ou 168 bits effectifs).
6. RSA-Encryption avec la CPS, longueur des clés de 768 (CPS2bis) ou 2.048 bits (CPS2ter).
7. Longueur des clés de confidentialité de 512 à 4.096 bits.
8. Confidentialité « partageable », longueur des clés de 1.024 bits.