AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

Prorogation IGC-CPS2ter

Impacts sur les applications CPS

Note de présentation destinée aux éditeurs d'applications CPS

« ASIP-Santé »

Identification du document	
Référence	ASIPSanté - Prorogation IGC-CPS2ter - Impacts applications CPS - V 1.0 .doc
Date de la dernière mise à jour	**29/06/2012**
Etat	Validé
Version	**V 1.0**
Classification	Non sensible - public
Nombre de pages	**20**

Historique du document			
Version	Date	Auteur	Commentaires
V1.0	29/06/2012	ASIP	Première version publiée sur site web de l'ASIP-Santé dans l'Espace Intégrateurs CPS

Sommaire

1 Objet du document

Cette note a pour objet de présenter, aux éditeurs d'applications mettant en œuvre la carte CPS, le **projet de l'ASIP-Santé de proroger la durée de vie de l'Infrastructure de Gestion de Clés des cartes CPS** (l'IGC-CPS2ter).

La présentation de ce document sera l'occasion de recueillir les commentaires sur les impacts terrain identifiés et les schémas de migration proposés pour assurer la continuité des services.

En substance :

- L'IGC-CPS2ter est l'infrastructure de gestion de clés dont le rôle est d'émettre les certificats d'authentification et de signature confinés dans les cartes CPS2ter et CPS3.
  Pour rappel, les certificats serveurs relèvent d'une IGC distincte (IGC-CPS2bis) ;

- L'IGC-CPS2ter expire normalement fin 2014.
  Ce document présente en quoi cette prorogation de la durée de vie de l'infrastructure de gestion de clés CPS2ter requiert le déploiement de nouveaux certificats racine de l'IGC-CPS2ter sur le terrain (Postes PS et/ou Serveurs applicatifs) ;

- Le document :
  - décrit la problématique de la prorogation de l'IGC-CPS2ter,
  - présente une analyse des impacts identifiés sur les usages de la CPS,
  - propose des solutions permettant une migration contrôlée en assurant la continuité des services ;

- Le document propose un planning prenant en compte les contraintes des migrations terrain.

1.1 Vocabulaire

Dans la suite de ce document,

CPS ou **carte CPS**	désigne une carte de la « Famille CPS »,
Chaîne-2014	désigne la chaîne de confiance actuelle qui va expirer,
Chaîne-2020	désigne la nouvelle chaîne de confiance,
ACR	désigne : Autorité de Certification Racine,
ACI	désigne : Autorité de Certification Intermédiaire.

2 Problématique

A ce jour, l'ASIP-Santé gère deux IGC :

- L'**IGC-CPS2ter** qui délivre l'ensemble des certificats (signature et authentification) confinés en carte CPS (CPS2ter et CPS3) :
  - personnel « indirectement nominatif », porteurs de CPE (Classe-0),
  - professionnels de santé, porteurs de CPS ou CPF (Classe-1),
  - directeurs de structures, porteurs de CDE ou CDA (Classe-2),
  - personnel nominatif de structures, porteurs de CPE ou CPA (Classe-3).

  Les clés cryptographiques (de signature et d'authentification) ainsi que leurs certificats correspondants sont inscrits en double dans la CPS3 : 1 jeu dans le volet CPS2ter et une copie dans le volet IAS.
- L'**IGC-CPS2bis** qui délivre des certificats « logiciels » :
  - les certificats pour les serveurs applicatifs - SSL et Signature (Classe-4),
  - les certificats de confidentialité réservés aux porteurs des CPS (Classe-5),
  - les certificats pour les Frontaux de l'Assurance Maladie (Classe-6).

Afin d'accompagner la mise en œuvre de la stratégie d'urbanisation des systèmes d'information partagés de l'ASIP-Santé et notamment sa dimension sécuritaire, une adaptation de l'offre de produits de certification est en cours de préparation à l'ASIP-Santé.

Une nouvelle IGC, « **l'IGC-Santé »,** doit prendre, à moyen terme, la relève des IGC-CPS2bis et IGC-CPS2ter.

En attendant, l'IGC-CPS2ter arrive bientôt en fin de vie (fin 2014) et sera donc prorogée afin :

- de pouvoir réémettre des CPS3 avec une durée de vie nominale de 3 ans,
- d'attendre la disponibilité de l'IGC-Santé,
- d'offrir aux éditeurs d'applications CPS le temps nécessaire pour adapter leurs logiciels afin d'être compatibles avec l'IGC-Santé.

Cette prorogation consiste à re-certifier les clés ACR et ACI :

- les données des certificats ACR et ACI suivantes sont mises à jour :
  - les périodes de validité deviennent : 11/10/2004 – 31/12/2020,
  - des nouveaux n° de série sont attribués,
- les autres données des certificats ACR et ACI ne changent pas, notamment :
  - les bi-clés ; les anciennes clés publiques et privées sont conservées,
  - les gabarits des certificats ACR et ACI (identifiants, …),

La prorogation de l'IGC-CPS2ter ne change rien au contenu applicatif des cartes CPS.

Elle permet juste de rétablir la durée de vie nominale des cartes et d'assurer la continuité de service durant la construction de la nouvelle offre de certification de l'ASIP-Santé.

La date de début d'émission de CPS avec une date fin de vie dépassant la date de fin de vie de l'IGC-CPS2ter actuelle est fin novembre 2012.

3 Impacts terrain de la prorogation

Les cartes CPS embarquent des clés cryptographiques associées à des certificats électroniques qui sont mis en œuvre dans les mécanismes de sécurité d'accès à des applications locales ou en ligne (authentification) et dans les mécanismes de signature électronique.

Les applications doivent vérifier la validité des certificats CPS. Pour cela, elles ont besoin de la chaîne de confiance de l'IGC-CPS2ter (cf. Annexe 1 qui décrit l'architecture de l'IGC).

La prorogation de l'IGC-CPS2ter a pour conséquence de modifier sa chaîne de confiance.

Les applications qui s'appuient sur les cartes CPS comme dispositif de sécurité pour l'authentification de leurs porteurs ou pour la vérification de leurs signatures électroniques doivent prendre en compte cette nouvelle chaîne de confiance

L'impact terrain concerne essentiellement :

- les applications serveur qui authentifient des CPS de porteurs distants ou qui vérifient des signatures électroniques générées par des CPS,
- les applications clientes mettant en œuvre la CPS et notamment celles qui exploitent les chaînes de confiance des CPS : soit en vérifiant la chaîne lors d'une authentification locale sur un Poste PS, soit en les transmettant lors d'une procédure d'authentification ou associé à un objet signé par CPS,
- les logiciels de messagerie qui échangent des messages signés entre Postes PS.

Les CRL sont publiées tous les jours avec la date du jour. Un vérificateur doit forcément utiliser une chaîne de confiance valide. Il acceptera donc toutes les CRL du jour, qu'il utilise la Chaîne-2014 ou la Chaîne-2020. Les gabarits des CRL restent inchangés.

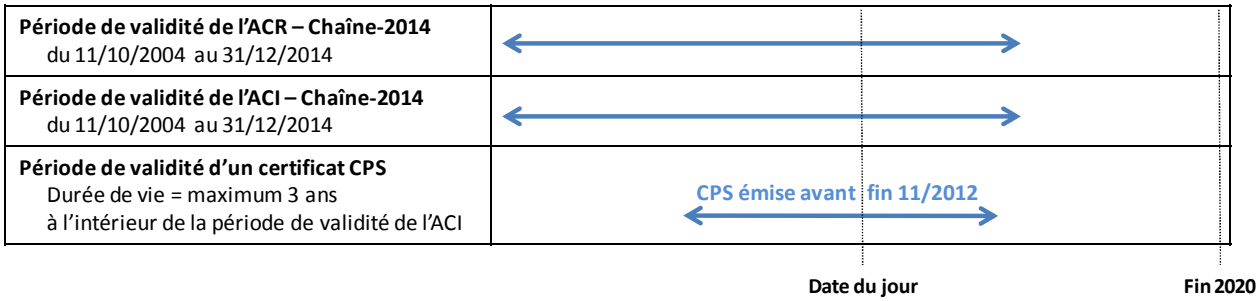
Le changement de chaîne de confiance n'a donc aucun impact sur la gestion des CRL.

3.1 Principe de vérification temporelle d'un certificat

Lors de la réception d'un certificat CPS, le vérificateur contrôle la validité du certificat CPS. Cette vérification consiste notamment à vérifier que le certificat a bien été signé par une Autorité de Certification (ACR et ACI) de confiance.

Les applications actuellement sur le terrain exploitent la Chaîne-2014.

Lors de la vérification d'un certificat, le vérificateur (re)construit d'abord la chaîne de confiance correspondante (Autorités de Certification Racine et Intermédiaire) et vérifie qu'elle est « de confiance ». Il vérifie ensuite si tous les certificats de la chaîne sont valides à la date du jour et qu'ils ne sont pas révoqués en analysant les CRL correspondantes.



- **Une CPS émise avant fin novembre 2012** à une durée de vie qui ne dépasse jamais la fin de la période de validité de la Chaîne-2014 (fin 2014).
- Par contre, **une CPS émise après fin novembre 2012** à une durée de vie qui dépassera systématiquement la fin de la période de validité de la Chaîne-2014 mais qui ne dépassera jamais la fin de la période de validité de la Chaîne-2020 (fin 2020).

Principe de l'emboîtement

Les règles des IGCs imposent le principe que les certificats des 3 niveaux (ACR, ACI et end-user) « s'emboîtent » : un certificat donné doit avoir une période de validité à l'intérieur de la période de validité du certificat de son autorité supérieure dans la chaîne de confiance.

> **Le respect de cette règle est du ressort de l'IGC.**
>
> **La vérification du « bon emboîtement » par une application est inutile.**

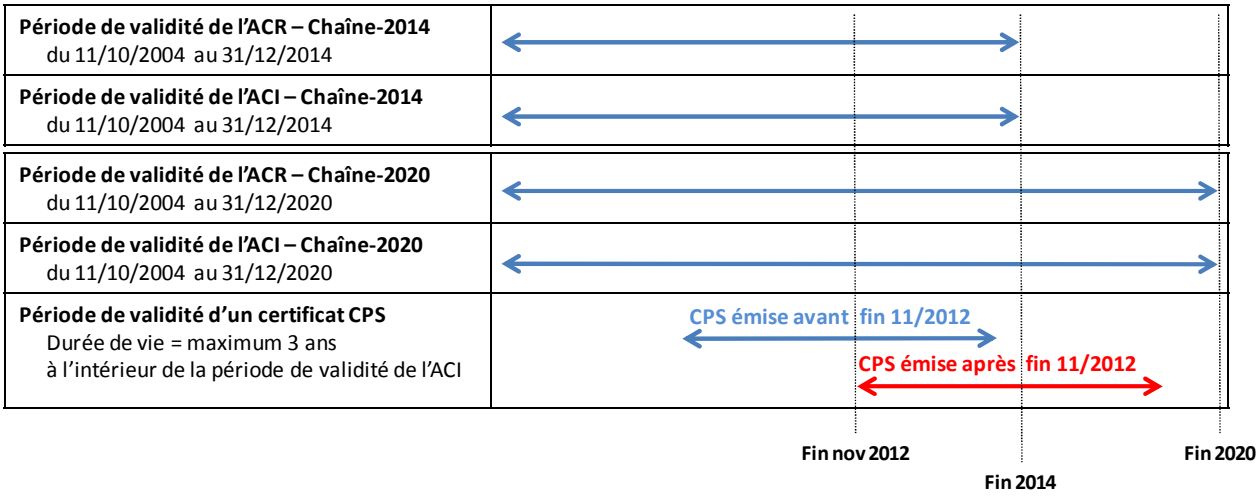
Toutefois, certaines applications vérifient le « bon emboîtement ». Leurs éditeurs doivent particulièrement bien vérifier si leurs applications ne sont pas concernées par la prorogation de l'IGC-CPS2ter. Il est conseillé, pour éviter d'éventuels impacts applicatifs, de supprimer cette vérification.

Impact de la prorogation sur la vérification temporelle d'un certificat

La prorogation de l'IGC-CPS2ter implique que, pendant la période de migration – fin novembre 2012 à fin 2014 – les vérificateurs de certificats CPS sont potentiellement confrontés à des certificats CPS émis tantôt avec la Chaîne-2014, tantôt avec la Chaîne-2020.

En outre, pour les CPS émises après fin novembre 2012, un vérificateur peut être confronté à un certificat CPS dont la date d'expiration dépasse fin 2014 mais qui est quand même présenté avec la Chaîne-2014 (cas où un Poste PS n'a pas encore été mis à jour).

Dans ces différents cas, il y un risque potentiel de refus du certificat par les applications vérificateurs et, par conséquent, de refus du service demandé.



Une CPS émise <u>avant</u> fin novembre 2012 a une durée de vie qui ne dépasse jamais la fin de la période de validité de la Chaîne-2014.
Ses certificats ne posent pas de problème d'emboîtement quelle que soit la chaîne de confiance utilisée par le vérificateur.

Une CPS émise <u>après</u> fin novembre 2012 a une durée de vie qui dépasse la fin de la période de validité de la Chaîne-2014 mais qui ne dépassera jamais la fin de la période de validité de la Chaîne-2020.

Un service applicatif de vérification doit remplacer la Chaîne-2014 par la Chaîne-2020 :

- **avant fin novembre 2012** pour les applications qui vérifient l'emboîtement,
- **avant fin 2014** (fin validité de la Chaîne-2014) pour les applications qui n'utilisent que la date du jour et ne vérifient pas cet emboîtement.

4 Configurations et Usages de la CPS

Les paragraphes suivants listent, pour chaque configuration et les usages de la CPS identifiés, les impacts potentiels sur les Postes PS et les Serveurs applicatifs.

Les solutions pour les impacts « faciles » à traiter sont indiquées dans les tableaux de ce chapitre. Des renvois dans les tableaux pointent vers des paragraphes ad hoc du chapitre suivant pour les cas exigeant des prérequis spécifiques.

Attention : La migration des Postes PS et des serveurs doit respecter les solutions décrites ci-dessous.
Dans certains cas, le serveur doit migrer **avant** la mise à jour des Poste PS au risque de refuser tout certificat CPS (d'authentification ou de signature) envoyé par des postes ayant déjà migré.

Les paragraphes suivants décrivent les configurations techniques suivantes :

- Poste avec un Navigateur communiquant avec un serveur distant,
- Poste avec LPS communiquant avec un serveur distant,
- Echange d'objets signés entre des Postes PS,
- Poste léger communiquant avec un serveur de structure,
- Authentification locale par CPS sur Poste PS,
- Authentification sans contact d'un « Support CPS ».

Dans les tableaux ci-dessous, l'expression « mis(e) à jour » désigne l'opération d'installation de la Chaîne-2020 (en remplaçant généralement la Chaîne-2014) et d'éventuelles adaptations pour la prise en compte des prérequis référencés.

4.1 Configuration : Poste avec un Navigateur communiquant avec un serveur distant

Usages	Configuration	Impacts	Solution
Authentification par CPS	Poste avec un navigateur en utilisation « native »	**Serveur** : Remplacement Chaîne-2014 par Chaîne-2020	Il est fortement conseillé de remplacer la Chaîne-2014 par la Chaîne-2020 sur le serveur dès sa publication. Si le serveur vérifie « l'emboîtement » le remplacement doit se faire **avant** fin novembre 2012.
		Poste PS : Non impacté	NA
Authentification par CPS + Signature d'un objet par une CPS	Poste avec un navigateur et utilisation d'une Applet ou un ActiveX	**Serveur** : Remplacement Chaîne-2014 par Chaîne-2020 + Eventuelle adaptation de l'Applet ou de l'ActiveX	Il est fortement conseillé de remplacer la Chaîne-2014 par la Chaîne-2020 sur le serveur dès sa publication. Si le serveur vérifie « l'emboîtement » le remplacement doit se faire **avant** fin novembre 2012.
			Les Applets et les ActiveX sont, en général, envoyés lors de chaque connexion par le serveur applicatif. Si les Applets et les ActiveX exploitent eux-mêmes la Chaîne-2014 ou s'ils remontent cette chaîne au serveur (lors d'une procédure d'authentification ou associé à un objet signé par CPS) ils doivent être mis à jour afin de prendre en compte la Chaîne-2020. La mise en œuvre des Applets et des ActiveX adaptés doit se faire dès la mise à jour du serveur pour éviter des conflits de gestion des chaînes coté serveur. Si les Applets et les ActiveX sont gardés en cache sur le poste, il faudra rafraîchir les caches pour que le poste prenne en compte la nouvelle version.
		Poste PS : Non impacté	NA

Usages	Configuration	Impacts	Solution
Authentification par CPS + Signature d'un objet par une CPS	Poste avec un navigateur et utilisation d'un exécutable sur le poste	**Serveur** : Installation Chaîne-2020, éventuellement en plus de la Chaîne-2014	1. Si l'exécutable sur le Poste PS n'exploite pas la Chaîne-2014 et qu'il ne la remonte jamais vers le serveur : • Il est fortement conseillé de remplacer la Chaîne-2014 par la Chaîne-2020 sur le serveur dès sa publication. Si le serveur vérifie « l'emboîtement » le remplacement doit se faire **avant** fin novembre 2012. 2. Si l'exécutable sur le Poste PS exploite la Chaîne-2014 ou s'il la remonte vers le serveur lors d'une procédure d'authentification ou associé à un objet signé par CPS : • La mise à jour de l'exécutable sur tous les postes est nécessaire. Dans la mesure où la mise à jour de tous les Postes PS déployés sur le terrain semble difficile à effectuer avant fin 2014 (délai trop court), le serveur doit être capable de gérer les 2 chaînes simultanément pour garantir la continuité de service. **Cf. § 5.1 « Prérequis serveurs applicatifs » qui détaille la solution à appliquer.**
		Poste PS : Le poste PS est impacté si l'exécutable exploite la Chaîne-2014 ou s'il remonte cette chaîne au serveur	1. Si l'exécutable sur le Poste PS n'exploite pas la Chaîne-2014 et qu'il ne la remonte jamais vers le serveur : le Poste PS n'est pas impacté 2. Si l'exécutable sur le Poste PS exploite la Chaîne-2014 ou s'il la remonte vers le serveur lors d'une procédure d'authentification ou associé à un objet signé par CPS : • Le serveur doit respecter les prérequis référencés ci-dessus. • La mise à jour de l'exécutable sur tous les postes est nécessaire. Cette mise à jour doit se faire **après** que le serveur ait été mis à jour et : o **avant** fin novembre 2012 si le LPS vérifie l'emboîtement, o sinon, **avant** l'expiration de la Chaîne-2014 si le LPS se limite à vérifier la validité du certificat PS et de sa chaîne de confiance à la date du jour.

Notes : Lors d'une procédure d'authentification, les navigateurs (I.E., Firefox, Safari, …) ne remontent jamais la chaîne de confiance correspondant au certificat client (de la CPS ou d'un autre outil crypto) vers le serveur distant.

Dans la majorité des configurations citées dans ce paragraphe, l'authentification est réciproque : le Navigateur authentifie également le Serveur applicatif. Pour cet usage, le Poste PS n'est pas impacté car le certificat serveur a été délivré par une autre IGC (l'IGC-CPS2bis ou une IGC commerciale ou publique).

4.2 Configuration : Poste avec LPS communiquant avec un serveur distant

Usages	Configuration	Impacts	Solution
Authentification par CPS + Signature d'un objet par une CPS	Poste PS avec un LPS	**Serveur** : Installation Chaîne-2020, éventuellement en plus de la Chaîne-2014	1. Si le LPS sur le Poste PS n'exploite pas la Chaîne-2014 et s'il ne la remonte jamais vers le serveur : • Il est fortement conseillé de remplacer la Chaîne-2014 par la Chaîne-2020 sur le serveur dès sa publication. Si le serveur vérifie « l'emboîtement » le remplacement doit se faire **avant** fin novembre 2012. 2. Si le LPS sur le Poste PS exploite la Chaîne-2014 ou s'il la remonte vers le serveur lors d'une procédure d'authentification ou associé à un objet signé par CPS : • La mise à jour du LPS sur tous les postes est nécessaire. Dans la mesure où la mise à jour de tous les Postes PS déployés sur le terrain semble difficile à effectuer avant fin 2014 (délai trop court), le serveur doit être capable de gérer les 2 chaînes simultanément pour garantir la continuité de service. **Cf. § 5.1 « Prérequis serveurs applicatifs » qui détaille la solution à appliquer.**
		Poste PS : Le poste PS est impacté si l'exécutable exploite la Chaîne-2014 ou s'il remonte cette chaîne au serveur	1. Si le LPS sur le Poste PS n'exploite pas la Chaîne-2014 et qu'il ne la remonte jamais vers le serveur : le Poste PS n'est pas impacté 2. Si le LPS sur le Poste PS exploite la Chaîne-2014 ou s'il la remonte vers le serveur lors d'une procédure d'authentification ou associé à un objet signé par CPS : • Le serveur doit respecter les prérequis énoncés en § 5.1. • La mise à jour du LPS sur tous les postes est nécessaire. Cette mise à jour doit se faire **après** que le serveur ait été mis à jour et : o **avant** fin novembre 2012 si le LPS vérifie l'emboîtement, o sinon, **avant** l'expiration de la Chaîne-2014 si le LPS se limite à vérifier la validité du certificat PS et de sa chaîne de confiance à la date du jour.

4.3 Configuration – Echange d'objets signés entre des Postes PS

Certaines applications échangent des objets signés entre des Postes PS.

Ces objets signés peuvent respecter différents formats tels que XADES (signature d'objets XML) ou S/MIME. Ce dernier format est utilisé par des produits de messagerie sécurisée et notamment par les OSM (Outils de Sécurisation de Messagerie).

Usage	Configuration	Impacts	Solution
Signature d'un objet par une CPS	Poste PS avec logiciel de signature (fonction génération de signatures)	**Poste PS de signature** : Selon les vérifications effectuées par le logiciel.	1. Si le logiciel de signature n'exploite pas la Chaîne-2014 et ne l'inclue pas dans l'objet signé : le logiciel de signature n'est pas impacté 2. Si le logiciel de signature exploite la Chaîne-2014 ou l'inclue dans l'objet signé : • La mise à jour du logiciel de signature sur tous les postes est nécessaire et doit se faire : o **avant** fin novembre 2012 si le logiciel de signature vérifie l'emboîtement avant signature, o sinon, **avant** l'expiration de la Chaîne-2014 si le logiciel se limite à vérifier la validité du certificat PS et de sa chaîne de confiance à la date du jour. Dans les 2 cas, la mise à jour du logiciel doit prendre en compte les prérequis énoncés en **§ 5.2 « Prérequis pour les logiciels qui échangent des objets signés entre des Postes PS »**.
Vérification d'un objet signé par un logiciel sur un autre Poste PS	Poste PS avec logiciel de signature (fonction vérification de signatures)	**Poste PS de vérification** : Selon les vérifications effectuées par le logiciel.	Le logiciel de vérification utilise forcément une chaîne de confiance pour vérifier la signature de l'objet. • La mise à jour du logiciel de vérification sur tous les postes est nécessaire et doit se faire : o **avant** fin novembre 2012 si le logiciel vérifie l'emboîtement, o sinon, **avant** l'expiration de la Chaîne-2014 si le logiciel se limite à vérifier la validité du certificat PS et de sa chaîne de confiance à la date du jour. Dans les 2 cas, la mise à jour du logiciel doit prendre en compte les prérequis énoncés en **§ 5.2 « Prérequis pour les logiciels qui échangent des objets signés entre des Postes PS »**.

Note : Pour le chiffrement des objets échangés, les Postes PS ne sont pas impactés car les certificats de chiffrement sont délivrés par une autre IGC (IGC-CPS2bis dans le cadre des produits OSM ou une autre IGC commerciale ou publique).

4.4 Configuration : « Poste léger » communiquant avec un serveur de structure

Usages	Configuration	Impacts	Solution
Authentification par CPS	Poste avec SmartCardLogon et serveur ActivDirectory ou Poste léger avec serveur TSE (exemple : Citrix)	**Serveur** : Remplacement Chaîne-2014 par Chaîne-2020	Il est fortement conseillé de remplacer la Chaîne-2014 par la Chaîne-2020 sur le serveur dès sa publication. Si le serveur vérifie « l'emboîtement » le remplacement doit se faire **avant** fin novembre 2012.
		Poste PS : Non impacté	NA

4.5 Configuration - Authentification locale par CPS sur Poste PS

Certaines applications locales à un Poste PS authentifient les porteurs de CPS pour contrôler les droits d'accès à l'application elle-même et/ou à des ressources qu'elle gère (base de données patients, coffre-fort de clés, …).

Usage	Configuration	Impacts	Commentaires
Authentification locale par CPS	Poste PS avec application locale	**Poste PS** : Selon les vérifications effectuées par le LPS.	L'éditeur doit analyser l'impact sur son application afin de la mettre éventuellement à jour. Si la mise à jour d'une application sur les postes équipés est nécessaire, elle doit se faire : o **avant** fin novembre 2012 si le LPS vérifie l'emboîtement, o sinon, **avant** l'expiration de la Chaîne-2014 si le LPS se limite à vérifier la validité du certificat PS et de sa chaîne de confiance à la date du jour.

4.6 Configuration – Authentification sans contact d'un « Support CPS »

L'authentification sans contact du support CPS authentifie uniquement le support, aucune donnée personnelle (nom, identité, …) n'est présente dans le certificat utilisé.

Usages	Configuration	Impacts	Solution
Authentification sans contact d'un Support CPS	Lecteur sans contact, soit branché sur un Poste PS, soit faisant partie d'un système de contrôle d'accès physique d'une structure.	**Poste PS** : Non impacté	Usage non impacté car le certificat du Support CPS a été délivré par une autre IGC (l'IGC-Technique).

5 Prérequis supplémentaires

5.1 Prérequis serveurs applicatifs

Dans le chapitre précédent on a constaté que lors de certains échanges (authentification CPS et objets signés par CPS), le logiciel sur le Poste PS peut envoyer la Chaîne-CPS avec le certificat CPS vers le serveur distant.

Les logiciels sur le terrain doivent être mis à jour afin d'envoyer la Chaîne-2020 à la place de la Chaîne-2014.

Dès lors, les serveurs et les applications centraux peuvent être confrontés à des échanges avec des clients distants (procédures d'authentification ou réception d'objets signés) qui présentent leur certificat CPS accompagné soit de l'ancienne chaîne (Chaîne-2014) soit de la nouvelle chaîne (Chaîne-2020).

Cette situation ne doit pas perturber les serveurs et les applications centraux et, par conséquent, une adaptation/contournement pourrait être nécessaire lors de l'installation de la chaîne de l'IGC-CPS2ter prorogée afin d'accepter indifféremment les Chaînes-2014 et 2020.

Les serveurs et applications centraux doivent respecter les prérequis suivants pour éviter une migration de postes client sur le terrain dans un délai inatteignable :

- Les serveurs et les applications centraux doivent être capables (ou mis en capacité) de réaliser des procédures d'authentification de CPS et de vérification de signatures CPS dans lesquelles les certificats CPS sont présentés indifféremment avec l'ancienne chaîne de l'IGC-CPS2ter (expirant fin 2014) ou avec la nouvelle chaîne (expirant fin 2020). »
- Il faudrait, tant que possible, supprimer les tests d'emboîtement sur les serveurs et les applications centraux.
- Le serveur doit mettre en œuvre ces prérequis **avant** toute installation de la Chaîne-2020 sur ses postes clients.

5.2 Prérequis pour les logiciels qui échangent des objets signés entre des Postes PS

Le présent prérequis s'applique aux logiciels qui émettent et reçoivent des objets signés entre des Postes PS.

Le problème dans ces échanges d'objets signés est qu'un même poste est tantôt émetteur d'objets signés et tantôt récepteur et vérificateur de d'objets signés.

Par ailleurs, certains logiciels vérifient l'emboîtement de la chaîne de confiance ce qui, dans les configurations actuelles, provoquera des rejets d'objets signés par une CPS dont la date de validité dépasse fin 2014.

5.2.1 Logiciels qui ne vérifient pas l'emboîtement de la chaîne de confiance CPS

La majorité des logiciels ne vérifient pas l'emboîtement de la chaîne de confiance CPS ; ils vérifient uniquement que le certificat de signature et ceux de la chaîne de confiance sont valides à la date du jour.

Pour ces logiciels Poste PS, les prérequis suivants doivent être respectés <u>avant</u> fin 2014 :

- Les logiciels émetteurs doivent :
  - joindre la Chaîne-2014 aux objets signés jusqu'à sa date d'expiration. *Jusqu'à cette date (fin 2014), ils sont compatibles avec les logiciels récepteurs actuellement sur le terrain.*
  - Dés que la Chaîne-2014 expire (fin 2014), les logiciels émetteurs doivent joindre la Chaîne-2020 aux objets signés. *Ils sont alors compatibles avec les Postes PS disposant des logiciels mis à jour ainsi qu'avec les logiciels récepteurs actuellement sur le terrain qui ne vérifient pas l'emboîtement et les logiciels.*
- Les logiciels récepteurs doivent :
  - être capables (ou être mis en capacité) de réaliser des procédures de vérification de signatures CPS dans lesquelles les certificats CPS sont présentés indifféremment avec l'ancienne chaîne de l'IGC-CPS2ter (Chaîne-2014 expirant fin 2014) ou avec la nouvelle chaîne (Chaîne-2020 expirant fin 2020). »

5.2.2 Logiciels qui vérifient l'emboîtement de la chaîne de confiance CPS

Certains logiciels d'émission et réception d'objets signés vérifient l'emboîtement de la chaîne de confiance CPS. Pour ces logiciels il est indispensable :

- de supprimer cette vérification **<u>avant</u>** fin novembre 2012, faute de quoi ces logiciels ne pourront plus accepter aucun objet signé par une CPS émise après fin novembre 2012.
- de respecter le prérequis énoncé dans le paragraphe §5.2.1 ci-dessus.

6 Macro-planning

Etape	Actions	**Echéances** (date fin des actions)	Acteurs
Préparation technique	Publication de la nouvelle chaîne de confiance	fin juin 2012	ASIP-Santé
	Mise à disposition des outils d'accompagnement sur l'Espace Intégrateur CPS : • le présent document et ses éventuelles versions successives ; • les nouvelles CryptoLib-CPS2ter + les installeurs dédiés à la Chaîne-2020. Cf. tableau en Annexe 2.	fin juin 2012	
	Lancement d'un mailing d'information à tous les éditeurs recensés par l'ASIP-Santé.	fin juin 2012	
Migration des serveurs applicatifs sur le terrain	L'administrateur des Serveurs doit installer la Chaîne-2020 pour la vérification de certificats CPS distants et, simultanément si besoin, mettre à jour le serveur en respectant les prérequis énoncés en § 5.1. **Rappel** : Pour certains Serveurs il est indispensable d'être mis à jour avant la 1ère installation d'un logiciel poste client mis à jour.	au plus tôt	Editeurs et exploitants
Migration des logiciels sur les Postes PS terrain	Adaptation et déploiement selon le contexte de chaque application.	soit avant fin nov 2012, soit avant fin 2014	Editeurs avec support technique de l'ASIP-Santé
Bascule de la chaîne de production	Retour à une émission des cartes CPS3 avec leur durée de vie nominale (3 ans).	fin nov 2012	ASIP-Santé

7 Dispositif d'accompagnement

En plus du présent document, l'ASIP-Santé propose le dispositif d'accompagnement suivant :

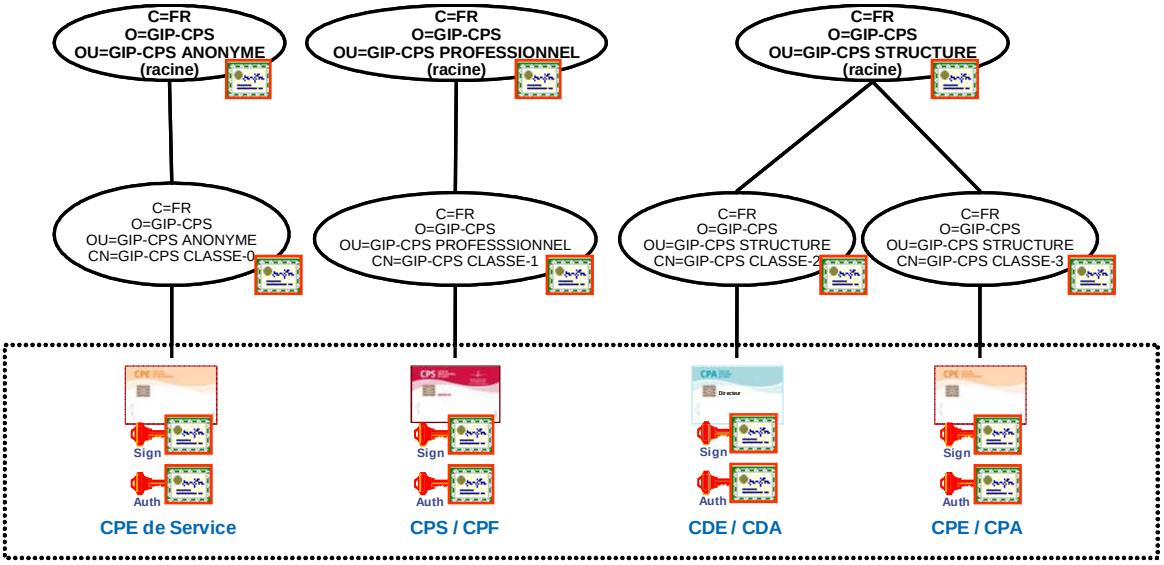
1. Publication dans l'Espace Intégrateur CPS :
   - d'un guide d'installation de certificats à l'attention des administrateurs de serveurs avec les préconisations techniques pour le déploiement (et suppression) de chaînes de confiance sur des serveurs Apache et IIS ;
   - des utilitaires dédiés à l'installation de la chaîne de l'IGC-CPS2ter prorogée dans les coffres forts de Windows, MacOS et Mozilla Firefox (avec la suppression de l'ancienne chaîne) ;
   - des nouveaux Kits d'installation des Librairies Crypto CPS intégrant l'installation de la chaîne de l'IGC-CPS2ter prorogée dans les coffres forts de Windows, MacOS et Mozilla Firefox (avec la suppression de l'ancienne chaîne) ;
2. Mise en place d'un support technique par l'ASIP-Santé pour les éditeurs de LPS et les promoteurs d'applications mettant en œuvre la CPS.

La mise à jour de la CryptoLib-CPS2ter sur un poste PS n'est utile que pour les logiciels CPS qui exploitent directement le coffre-fort du système pour le stockage des chaînes de confiance des CPS (systèmes Windows ou MacOS).

8 Annexe 1 - Architecture de l'IGC-CPS2ter

La chaîne de certification de l'IGC-CPS2ter compte :

- 3 Autorités de Certification Racine
- 4 Autorités de Certification Intermédiaires.



Architecture de l'IGC-CPS2ter

Pour un certificat donné, sa chaîne de confiance est composée du certificat ACI de sa classe et du certificat ACR qui gère cette classe de certificats.

9 Annexe 2 - Liste des différents installeurs

Systèmes d'exploitation	Installeur	Version
Windows	CryptoLib-CPS2ter sous GALSS	V4.1.3
	CryptoLib-CPS2ter full PC/SC	V1.14
	Installeur Chaîne-2020	V1.0
MacOS	CryptoLib-CPS2ter sous GALSS	V4.0.3
	CryptoLib-CPS2ter full PC/SC	V1.02
	Installeur Chaîne-2020	V1.0
Linux (noyau 2.4 ou 2.6)	CryptoLib-CPS2ter sous GALSS	V3.07
	CryptoLib-CPS2ter full PC/SC	V1.02-1
	Installeur Chaîne-2020 (disponible sous forme de XPI = extension de Firefox)	V6.0

Notes :

1. La mise à jour de la CryptoLib-CPS2ter sur un poste PS n'est utile que pour les logiciels CPS qui exploitent directement le coffre-fort du système pour le stockage des chaînes de confiance des CPS (systèmes Windows ou MacOS).
2. Les installeurs référencés dans le tableau ci-dessus, suppriment l'ancienne chaîne de confiance (Chaîne-2014) et installent la nouvelle chaîne (Chaîne-2020) dans les navigateurs Internet Explorer (coffre-fort de Windows), Safari (coffre-fort de MacOS) et Firefox.