Guide de mise en œuvre d'une authentification forte avec une Carte de Professionnel de Santé (CPS) dans une application Web

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

v0.2.4 du 17/12/2013

AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

Guide de mise en œuvre d'une authentification forte avec une Carte de Professionnel de Santé (CPS) dans une application Web

« ASIP Santé »

Version 0.2.4 du 17/12/2013

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
T.+33 (0)1 58 45 32 50
esante.gouv.fr

Agir ensemble pour soigner mieux

Sommaire

1 Introduction

Ce guide de mise en œuvre technique est destiné plus spécifiquement aux chefs de projets de maitrises d'œuvre et aux architectes techniques et applicatifs.

Pour un système d'information ou une application devant mettre en œuvre l'authentification forte avec une carte CPS sur une application Web, la mise en œuvre les différents composants est complexe.

En effet, le comportement final de l'application vu de l'utilisateur est dépendant de l'interaction entre plusieurs composants logiciels situés sur le poste de travail et sur l'application côté serveur, qui peuvent être mis en œuvre dans plusieurs configurations.

Ce document a donc pour objectif :

- d'expliquer le fonctionnement de l'authentification par carte CPS dans une application Web,
- de proposer des solutions types permettant d'avoir un fonctionnement stable dans une application.

2 Glossaire

Abréviation	Signification
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
CCM	CPS Certificate Manager
CDSA	Common Data Security Architecture
CSP	Cryptographic Service Provider, API Microsoft d'accès aux algorithmes cryptographiques standards
CPA	Carte de Personnel Autorisé
CPE	Carte de Personnel d'Etablissement
CPS	Carte des Professionnels de Santé
DMP	Dossier Médical Personnel
FSE	Feuille de Soins Electronique
GALSS	Gestionnaire d'Accès au Lecteur Santé-Social
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure
IGC	Infrastructure de Gestion de Clés
MS	Microsoft
MSSanté	Messagerie Sécurisée de Santé
ODI	Outil de diagnostic et d'installation
OS	Operating System, Système d'exploitation
PKCS	Public Key Cryptographic Standards, ensemble de spécifications conçues par RSA
PSS	Protocole Santé Sociale
SI	Système d'Information
SSL	Secure Socket Layer
TLS	Transport Layer Security
TPE	Terminal de paiement électronique

Tableau 1 : Glossaire

3 Problématique de l'authentification par CPS dans une application Web

3.1 Définition des principaux composants

Les paragraphes suivant dressent la liste des principaux composants nécessaires au fonctionnement d'une application Web utilisant l'authentification par carte CPS.

3.1.1 Sur le poste de travail

3.1.1.1 Carte CPS

Les cartes à puce de la famille CPS (CPS, CPA, CPE[2]) sont attribuées à des personnes physiques. Elles permettent d'authentifier leurs utilisateurs de manière forte. La génération actuelle de carte est la CPS3, qui permet une utilisation en mode avec contact et en mode sans contact.

Les cartes en mode « contact » contiennent un certificat X509 d'authentification et un certificat X509 de signature dont l'accès est protégé par un code PIN. Ces certificats sont issus de l'IGC CPS, gérée par l'ASIP Santé.

Dans les cartes en mode « sans contact », les certificats X509 permettant l'authentification forte de l'utilisateur ou la signature ne sont pas accessibles. Cependant des scénarios techniques sont possibles qui peuvent associer une authentification forte en mode contact avec l'utilisation du mode sans contact. Il est possible en particulier de stocker après authentification forte un jeton d'authentification dans la carte en mode contact, et d'y accéder en lecture en mode sans contact.

Les informations détaillées sur la carte CPS et sur les certificats X509 issus de l'IGC CPS sont disponibles sur le site intégrateur de l'ASIP Santé :

http://integrateurs-cps.asipsante.fr/pages/La-carte-CPS3

3.1.1.2 Lecteur de carte

Les lecteurs de cartes utilisables pour une application Web peuvent être de deux types :

Lecteurs de type GIE SESAM Vitale:

Ces lecteurs (parfois appelés lecteurs PSS[3]) sont fabriqués et vendus par différents constructeurs qui doivent respecter le cahier des charges du GIE SESAM Vitale. Ce sont des lecteurs au minimum bi-fentes qui contiennent un logiciel permettant de prendre en charge la facturation FSE, et permettent la présence simultanée d'une carte CPS et d'une carte Vitale.

Ces lecteurs ne sont pas reconnus nativement par les systèmes d'exploitation. L'accès doit être géré par le composant GALSS (voir section suivante).

Ces lecteurs peuvent avoir une interface série RS232c ou une interface USB. Leurs performances sont très variables d'un modèle à l'autre.

[2] CPS: Carte de Professionnel de Santé; CPA: Carte de Personnel Autorisé; CPE : Carte de Personnel d'Etablissement

[3] PSS: Protocole Santé Social

Les lecteurs GIE SESAM Vitale sur USB fonctionnent en émulation de port série sur un port USB défini. Historiquement, il n'était pas possible de le changer de port physique sans avoir à faire une reconfiguration du poste de travail. **Le GIE SESAM Vitale travaille activement sur cette problématique et annonce en juin 2013 des améliorations conséquentes avec les lecteurs bi-fente en 3.30 sortis après 2008 avec le GALSS 3.36.01 sous Windows.**

Lecteurs de type PC/SC:

Les lecteurs de type PC/SC dits 'transparents' sont des lecteurs mono-fente, habituellement sans clavier ni afficheur.

Ces lecteurs sont reconnus nativement par Windows, MacOS X, Linux et certains Unix.

Ces lecteurs étant mono-fente, il faut prévoir deux lecteurs pour gérer simultanément la lecture de la carte CPS et de la carte Vitale.

Il existe des lecteurs PC/SC sans contact compatibles avec la CPS3.

3.1.1.3 Gestionnaires de lecteur

La présence d'un gestionnaire de ressource lecteur dans le système d'exploitation permet à celui-ci de gérer de façon centralisée l'accès aux cartes et aux lecteurs pour toutes les applications y accédant.

Les gestionnaires de ressources possibles sont :

Le Gestionnaire d'Accès au Lecteur Santé Social (GALSS):

Le GALSS est un composant permettant de gérer l'accès aux lecteurs SESAM Vitale et aux lecteurs de type PC/SC. Il est conçu par le GIE SESAM Vitale et l'ASIP Santé. Il est indispensable pour l'usage de la facturation FSE. Il nécessite une configuration manuelle (fichier GALSS.INI).

La configuration du GALSS n'étant pas automatique (gestion du fichier GALSS.INI), tout changement de configuration de lecteur (modèle, port de branchement, nombre de lecteurs) implique une modification de celle du GALSS.

Ce composant est disponible et supporté à ce jour pour les systèmes Windows, Linux et MacOS (détail en annexe 1).

L'information technique détaillée sur le GALSS est disponible sur le site du GIE SESAM Vitale:

http://www.sesam-vitale.fr/aides/atsam/1.20.11/ATSAM.html?GALSSInfosTech.html

Le Gestionnaire PC/SC:

C'est le gestionnaire de lecteurs PC/SC intégré nativement dans le système d'exploitation.

On peut le trouver sous Windows, MacOS X, Linux, et certains Unix.

3.1.1.4 Cryptolib CPS

Actuellement, le composant mis à disposition par l'ASIP Santé pour accéder à la CPS est la Cryptolib CPS.

Ce composant expose :

1. des API spécifiques CPS, historiques
2. des API conformes au standard PKCS#11
3. des API conformes au standard Windows CSP (Cryptographic Service Provider) pour les systèmes Windows
4. des API conformes au standard CDSA (Common Data Security Architecture) pour MacOS X

Il existe deux versions de la Cryptolib CPS

1. une version se basant sur le GALSS
2. une version « Full-PC/SC » se basant sur le gestionnaire PC/SC.

Sous Windows, l'ASIP fournit le CCM (CPS Certificate Manager), composant de surveillance des lecteurs et d'alimentation du magasin de certificats du système d'exploitation.

La Cryptolib CPS ainsi que toute la documentation associée est téléchargeable aux URL (Windows, Mac) ci-dessous:

http://esante.gouv.fr/services/espace-cps/telechargements-libres/cryptolib-cps-windows

http://esante.gouv.fr/services/espace-cps/telechargements-libres/cryptolib-cps-mac-os-x-0

Il faut noter que la Cryptolib CPS n'est pas indispensable pour les FSE (Feuilles de Soin Electronique). Un poste configuré pour la FSE aura un lecteur bi-fente et un GALSS installés mais n'aura pas nécessairement une Cryptolib CPS installée.

3.1.1.5 Navigateur Web

Le navigateur Web est l'outil permettant à l'utilisateur d'accéder aux applications Web. Les navigateurs du marché peuvent accéder au certificat d'authentification de la carte CPS si l'ensemble des composants requis sont installés (lecteur, gestionnaire de lecteur, Cryptolib CPS) et s'il est correctement configuré (magasin de certificats).

L'accès aux certificats se fait via un magasin de certificats. Dans les navigateurs du marché, on peut distinguer deux modes de fonctionnement :

1. Firefox possède son propre magasin de certificats qui s'appuie sur l'API PKCS#11, standard international très répandu et implémenté par la Cryptolib CPS, et permet notamment la prise en charge de l'arrachage de la carte.
2. Les autres principaux navigateurs du marché (Internet Explorer, Chrome, Safari) reposent sur le magasin de certificats du système d'exploitation et sur des architectures cryptographiques spécifiques propriétaires (CSP sous MS Windows, Tokend sous Mac).

Le navigateur n'offre aux développeurs qu'un **nombre restreint de fonctionnalités normalisées et interopérables** (comportements définis et garantis, support identique d'un navigateur à l'autre ou d'un OS à l'autre).

Aucune API permettant d'accéder aux ressources matérielles ou logicielles ne sont aujourd'hui normalisées pour ces navigateurs. En particulier, aucune API commune à tous les OS et tous les navigateurs ne permet de détecter les événements cartes, lecteurs de cartes ou de déclencher des opérations cryptographiques.

Lorsque de telles APIs existent, elles sont soit restreintes soit propriétaires, donc non interopérables, sujettes aux changements unilatéraux et peu supportées.

Le navigateur Web peut éventuellement prendre en charge un composant applicatif spécifique (applets, « add-ons » spécifiques) dédié à la gestion de la carte CPS. Ces mécanismes sont propriétaires et imposent des opérations de déploiement et des contextes de sécurité au moment de l'exécution qui doivent être anticipés (droits administrateur dans certains cas par exemple).

3.1.1.6 Synthèse

Les composants poste de travail et leurs interactions sont illustrés ci-dessous dans trois configurations possibles:

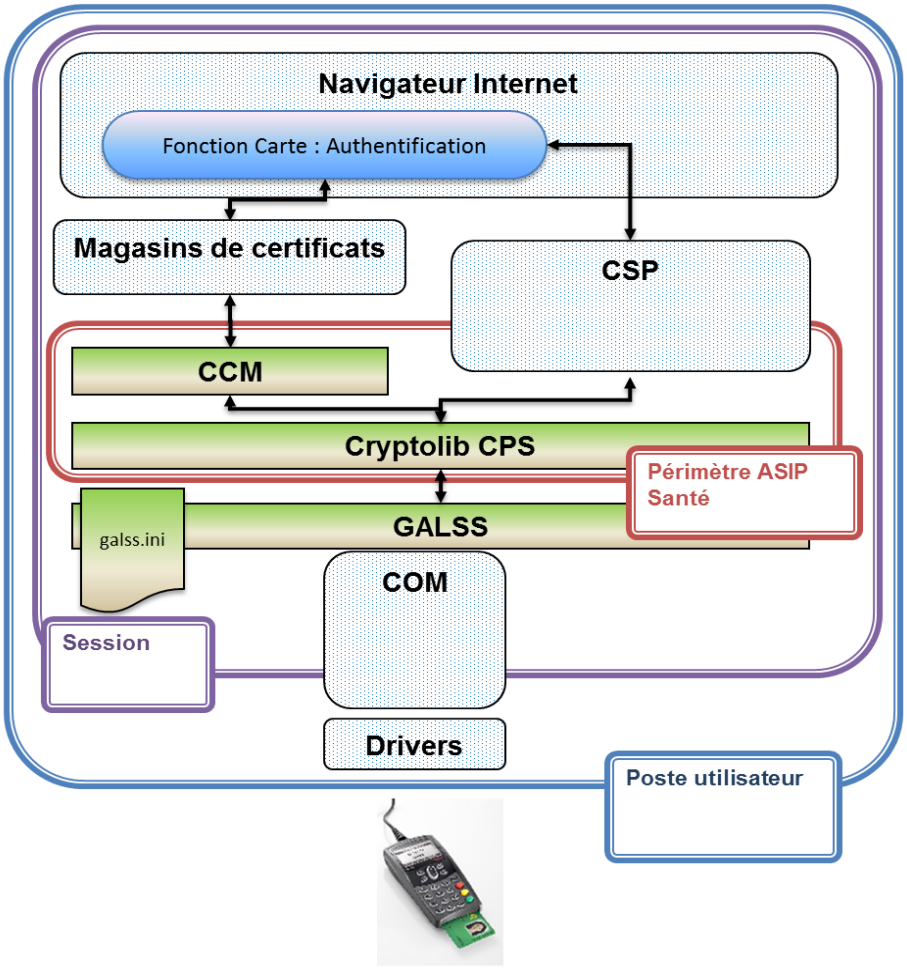

Figure 1 : Composants poste de travail avec GALSS et lecteur bi-fentes SESAM Vitale

NB : Cette première configuration est compatible FSE.

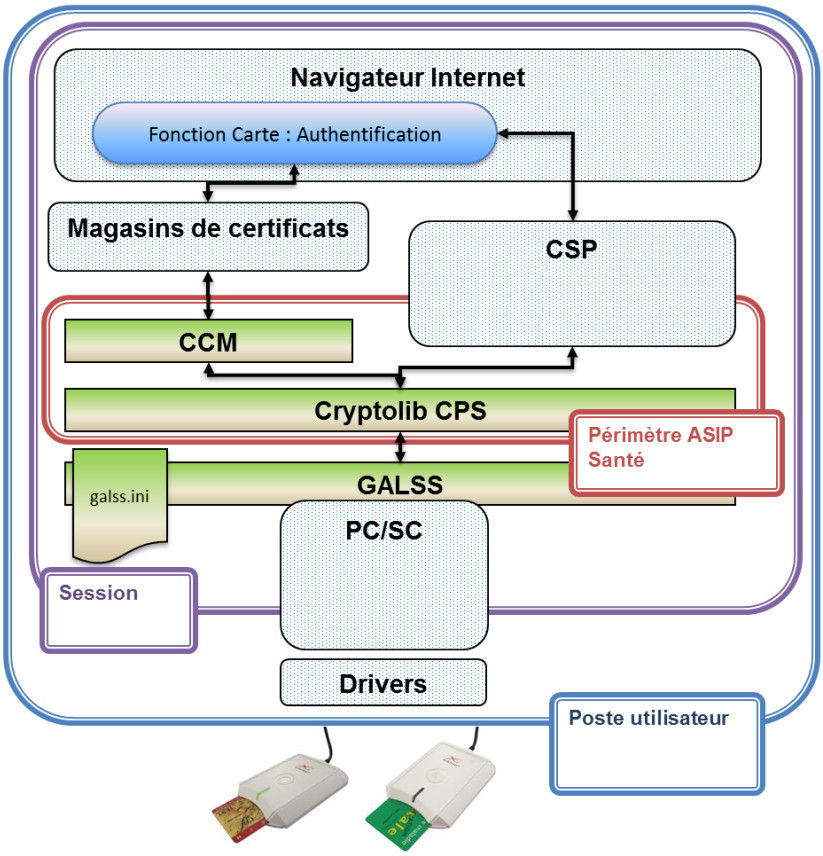

Figure 2: Composants poste de travail avec GALSS et lecteurs PC/SC

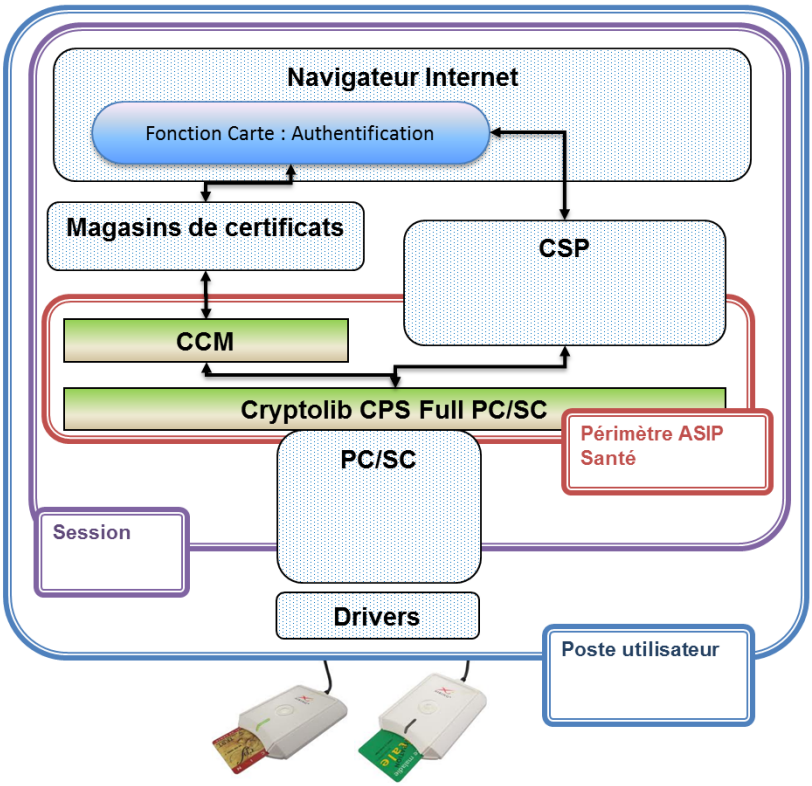

Figure 3: Composants poste de travail sans GALSS, avec lecteurs PC/SC et Cryptolib CPS full PC/SC

3.1.1.7 Outil de diagnostic et d'installation

L'ASIP Santé met à disposition un outil de diagnostic et d'installation en ligne « ODI PS », qui permet de vérifier les configurations techniques des postes de travail, et d'installer si nécessaire les composants manquants, pour Windows et MacOS X.

Cet outil permet de vérifier des prérequis tels que:

- L'installation du GALSS et la configuration des lecteurs,
- La présence et le bon fonctionnement de la Cryptolib CPS,
- La présence et la configuration d'une JVM,
- La version et la configuration du navigateur Web utilisé,
- La présence de l'API de lecture de la carte Vitale (si besoin).

Le diagnostic fait, l'ODI permet:

1. l'installation
2. la configuration des composants manquants
3. une restauration si la configuration des composants présents est corrompue

à condition que l'utilisateur ait les droits requis.

L'outil génère des rapports d'audit techniques détaillés qui peuvent être sauvegardés ou envoyés au support de l'application.

L'outil est configurable pour adapter son diagnostic et son visuel aux prérequis de différentes applications.

L'outil peut être lancé à partir de ces adresses, avec des configurations différentes correspondant aux applications concernées:

Nature du service	**URL**
portail des installateurs ASIP Santé	http://www.outil-diagnostic.asipsante.fr/
ODI pour le DMP	http://www.outil-diagnostic.dmp.gouv.fr/
ODI pour MSSanté	http://www.outil-diagnostic.mssante.fr/
ODI générique ASIP Santé	http://www.outil-diagnostic.asipsante.fr/ASIP/

Tableau 2: Liste des URL ODI

Il faut noter que l'application ODI est de type Java Web Start, et qu'elle nécessite par conséquent la présence d'une JVM.
La liste exhaustive des tests réalisés par l'ODI PS est donnée en annexe 2.

3.1.2 Sur le serveur

3.1.2.1 Reverse Proxy (Frontal HTTPS)

Sur une application Web, un composant est en général dédié spécifiquement à la gestion des connexions HTTP et HTTPS établies avec les navigateurs Web.

Les Reverse Proxy peuvent être des composants logiciels spécifiques installés sur des serveurs banalisés (Apache HTTPD, IIS, NGINX …), ou intégrés à des boitiers dédiés (Big IP F5, Alteon…).

Selon l'architecture du projet :

- La fonction Reverse Proxy peut éventuellement être rendue le même composant technique exécutant les composants applicatifs (Apache+Module PHP …).
- La fonction Reverse Proxy est parfois couplée dans le même composant à une fonction de répartiteur de charge pour les composants applicatifs sous-jacents.

Lorsqu'une authentification utilisateur est établie avec le certificat X509 d'authentification de la carte CPS sur HTTPS, c'est le composant Reverse Proxy (Frontal HTTPS) qui prend en charge la gestion de la connexion TLS:

L'authentification mutuelle n'a donc lieu effectivement qu'entre chaque client et le Reverse Proxy, elle ne donne lieu qu'à la mise en route d'un lien sécurisé **qui n'est garanti qu'entre** ces deux systèmes.

Le Reverse Proxy fonctionne en général sur des règles statiques basées sur les URL accédées, et ne gère pas les autorisations d'accès des utilisateurs. Il retransmet aux composants applicatifs sous-jacents les informations d'identité du certificat X509 de l'utilisateur.

La communication entre les Reverse Proxy et les autres composants applicatifs se fait dans une zone de confiance, possiblement « en clair ».

L'ASIP Santé met à disposition un guide de mise en œuvre de la prise en compte des certificats X509 issus de l'IGC CPS dans Apache et IIS disponible à l'adresse suivante :

http://integrateurs-cps.asipsante.fr/documents/ASIP_Guide-Int%C3%A9gration_CertificatSSL-Apache-IIS_V1.3_0.pdf

3.1.2.2 Composants applicatifs

Les composants applicatifs serveurs gèrent la cinématique de l'application Web. Par rapport à l'authentification par carte CPS, ils peuvent fonctionner de deux façons différentes :

- Soit l'authentification CPS est prise en charge par la connexion TLS établie avec le navigateur, et dans ce cas le composant applicatif récupère l'information d'identité transmise par le Reverse Proxy,
- Soit l'authentification CPS est gérée directement par les composants applicatifs, et dans ce cas le Reverse Proxy n'est pas sollicité, et c'est donc au composant applicatif de prendre en charge directement l'authentification en interaction avec le poste de travail.

Ces points sont détaillés plus loin dans le document (chapitre 4).

3.1.3 Exemples de mise en œuvre des composants

Dans ce premier exemple, les fonctions de répartiteur de charge, de Reverse Proxy et de serveur d'application sont prises en charge par des composants distincts (boitier F5, Apache, JBoss).

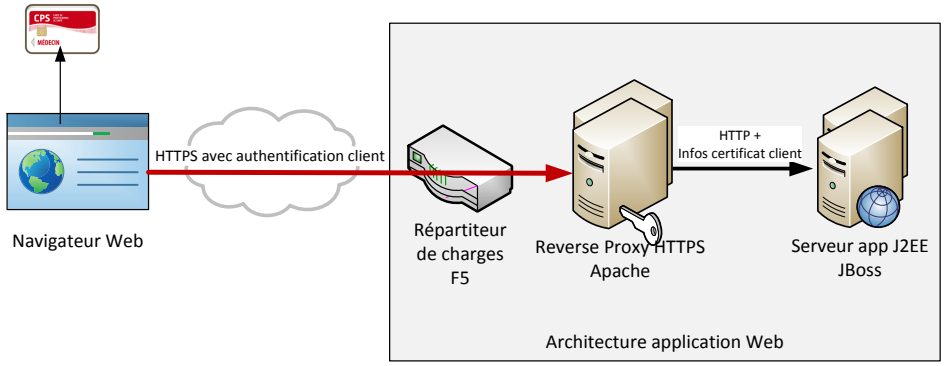

Figure 4 : répartiteur, reverse proxy et serveur d'application distincts

Dans ce second exemple, la fonction de Reverse Proxy est prise en charge par un boitier F5 qui fait office également de répartiteur de charge.

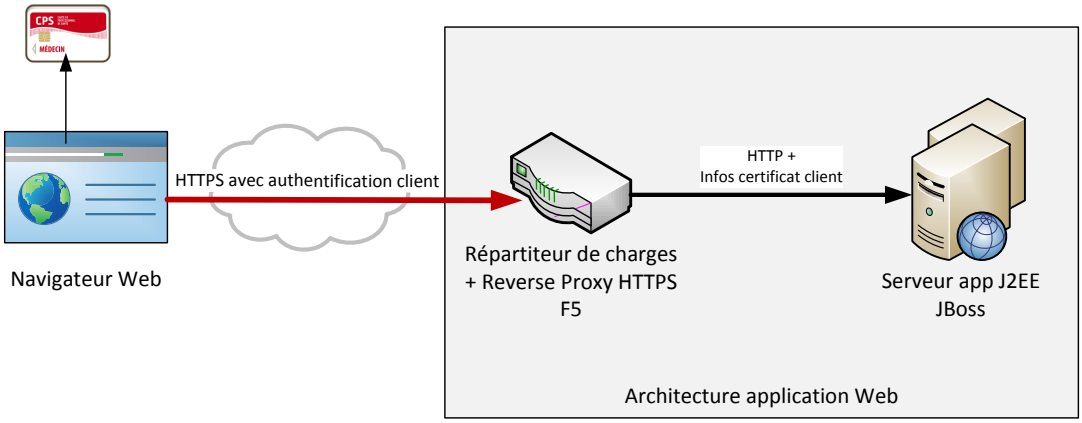

Figure 5 : répartiteur et reverse proxy dans le même équipement

Dans ce troisième exemple, le composant Reverse Proxy et le composant applicatif (PHP) sont hébergés sur le même composant (serveur Apache).

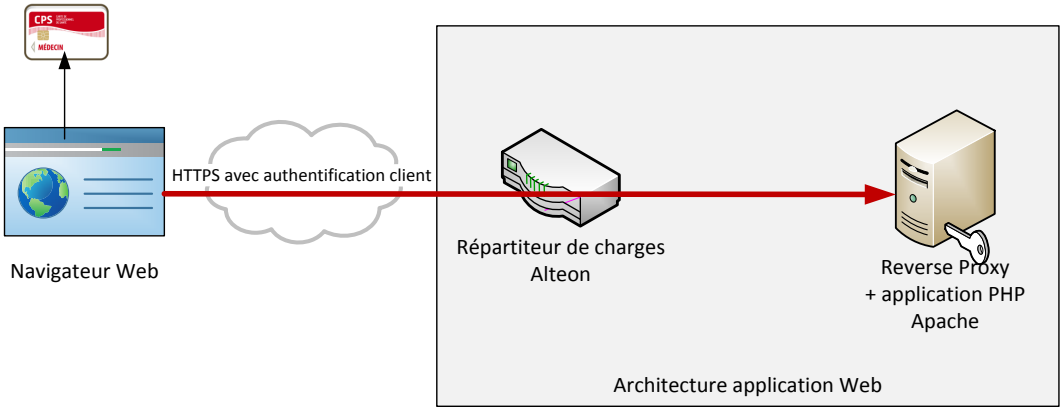

Figure 6 : reverse proxy et serveur d'application dans le même composant logiciel

3.2 Fonctionnement général et problèmes rencontrés

Pour mettre en œuvre l'authentification avec une carte CPS (ou avec un certificat logiciel) dans une application Web, il faut réaliser au même moment:

- l'authentification forte mutuelle entre le Reverse Proxy et le poste client afin d'établir le lien TLS à l'aide des certificats de l'utilisateur et du serveur
- la connexion de l'utilisateur dans les composants applicatifs (login applicatif).

Il est important de rappeler que, indépendamment de ces **deux actions simultanées,** la **sécurisation de la liaison (transport géré par le Reverse Proxy)** et le **login (application)**

- sont **deux choses différentes** en termes conceptuels et d'implémentation
    - cette différence d'implémentation est voulue par les bonnes pratiques logicielles (OSI) et largement répandue.
- ne sont **pas coordonnées** par défaut
    - elles doivent donc être coordonnées au niveau applicatif s'il s'agit du besoin fonctionnel à atteindre.

Le fonctionnement des composants de l'application Web et la configuration du Reverse Proxy HTTPS sont donc intimement liés.

L'authentification mutuelle avec login applicatif, qu'elle soit réalisée avec un certificat CPS ou un certificat logiciel, souffre historiquement :

- de limitations ergonomiques induites par des implémentations rudimentaires des éléments logiciels composants une PKI
    - boites de dialogue de demande de PIN archaïques
    - messages d'erreur incompréhensibles et répétitifs à l'origine d'acceptations utilisateurs systématiques…
- du manque de paramétrage des fonctionnalités liées:
    - à la recherche d'optimisations sur des phases cryptographiques réputées lentes
    - aux fonctionnalités propriétaires, liées aux vides normatifs
    - Exemple : paramétrage des caches pour éviter les renégociations

Le **nombre croissant** d'optimisations SSL, toutes propriétaires (« SSL resumption », « False start »…) et adressant des problématiques de masse (montées en charge), entraine des effets collatéraux face auxquels il est parfois nécessaire de trouver des solutions.

La mise en œuvre de l'authentification avec une carte CPS dans une application Web est toutefois **possible à implémenter**, en fonction des degrés d'exigences fonctionnelles de départ, dès lors que sont respectées un ensemble de règles :

- d'architecture
- de conception
- d'implémentation
- de tests
- de suivi de projet.

3.2.1 Accès carte et alimentation du magasin

Le CCM (CPS Certificate Manager) est un utilitaire installé avec la Cryptolib CPS qui permet de charger les certificats portés par la carte dans le magasin de certificats du système d'exploitation.

Instancié sur le poste de travail, le CCM offre deux modes de fonctionnement :

- Un mode de surveillance automatique, qui permet une mise à jour automatique du magasin de certificats sur les événements d'insertion et de retrait de la carte CPS
- Un mode manuel, offrant la possibilité à l'utilisateur de rafraichir manuellement le magasin de certificat.

Le mode automatique du CCM marche de façon très satisfaisante avec les lecteurs PC/SC. La fréquence de surveillance du certificat est de 2 secondes par défaut dans ce mode. Cette fréquence est configurable.

Le mode manuel est préconisé avec les lecteurs bi-fentes Sesam-Vitale fonctionnant sur GALSS, afin de ne pas perturber leurs opérations, ces lecteurs ne prévoyant pas dans leur conception de gérer plusieurs tâches en parallèle. Par exemple, certains de ces lecteurs font également office de Terminaux de Paiement Embarqué (TPE): dès lors qu'une application externe les sollicite de manière récurrente (cas du CCM en mode automatique), il n'est plus possible de saisir le montant d'une transaction et d'enclencher le processus de paiement.

Les Cryptolib CPS installent un CCM configuré en mode manuel par défaut du fait de la contrainte associée aux lecteurs Sesam-Vitale.

3.2.2 Opérations cryptographiques (communes tous tokens)

Sous Windows, l'opération d'alimentation du magasin de certificats s'accompagne d'une déclaration de mapping entre le token de sécurité (la carte dans ce cas), l'identifiant de la clef privée et le certificat associé.

Ce mapping permet aux applications, au moment de réaliser les opérations cryptographiques proprement dites (« au runtime »), de charger le bon CSP et d'effectuer les opérations avec les bons éléments.

Lors de l'exécution, du point de vue des applications, les utilisations de la carte ou de tout autre tokens (soft – p12, USB sécurisé....), **sont équivalentes** du point de vue cryptographique (intérêt de la couche d'abstraction CSP ou PKCS11) :

Les limitations constatées (retrait certificat mais session SSL ouverte…) avec les certificats carte se constatent de la même façon avec des certificats logiciels.

3.2.3 Niveau Transport : SSL vu du poste client

SSL permet de sécuriser un lien réseau à l'aide d'une authentification mutuelle des acteurs d'un réseau. Ce protocole est souvent utilisé pour sécuriser une liaison http, désignée alors sous le terme HTTPS.

Le handshake SSL suit la séquence suivante, visant une authentification mutuelle client / serveur et l'établissement d'un canal sécurisé protégé par une clef secrète :

(Source: Microsoft)

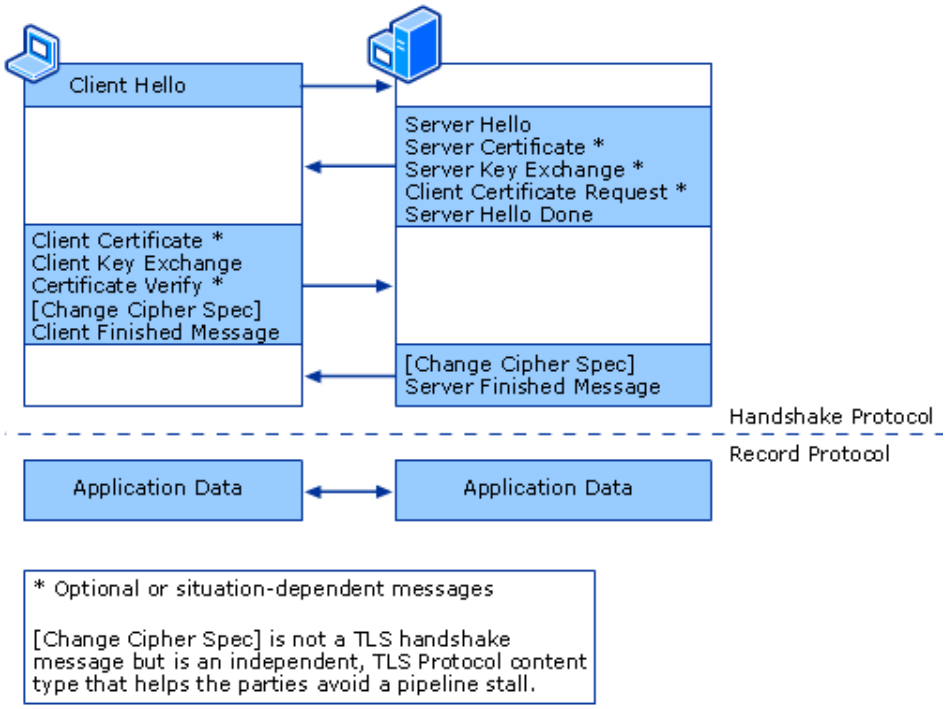

Figure 7 : Handshake SSL

Les champs optionnels permettent d'implémenter une authentification serveur simple, sans authentification client.

Comme il est possible de le constater sur le schéma, la spécification SSL ne prévoit aucune vérification de la présence des clés privées et des certificats ayant initiés le canal sécurisé, une fois ce canal de communication établi.

Ceci se traduit :

- **dans le diagramme de séquence SSL (illustrant les spécifications) : par l'absence de liens vers ou en provenance des tokens de sécurité ayant permis l'établissement du lien sécurisé**
- **dans les spécifications SSL : par l'absence d'exigence en lien avec ce type de fonctionnalités**

Le canal sécurisé peut dont être maintenu, même si clefs privées et certificats ont disparu du système (cas de la carte arrachée).

Tout élément tendant à illustrer le contraire est fortuit et **tient des particularités d'implémentations**:

- Un changement de <Location> Apache provoque une renégociation complète
- Un changement de processus IE provoque une renégociation complète
- NSS (Firefox) maintient sans doute une chaine de dérivation interne l'amenant à descendre le tunnel SSL en cas d'arrachage carte
- …

Certaines implémentations serveur permettent de forcer la renégociation TLS à des intervalles réguliers, ce qui peut éventuellement permettre de vérifier la présence du certificat de l'utilisateur mais ceci :

- Ne peut être fait avec une fréquence élevée sans avoir des impacts importants sur les performances de l'application (côté serveur et côté client),
- Ne permet pas d'avoir un comportement de l'application compréhensible par l'utilisateur ; pour l'utilisateur la détection de l'arrachage se traduit par une page d'erreur mais qui n'a aucun lien avec ses actions en cours (car non synchronisé avec l'arrachage de la carte qui a pu avoir lieu plusieurs minutes avant).

Le cas fonctionnel « insertion carte > authentification > retrait carte > persistance du transport » est donc le cas nominal.
Si cette présence doit être garantie, elle doit être implémentée spécifiquement, au plus près de la clef privée (agent additionnel du type applet ou plugin/add-on sur le poste).

3.2.3.1 Cas particulier du SSL sous Windows

Sur un OS Windows, l'ouverture et le maintien d'une communication SSL sur la base d'un certificat carte mettent en jeu :

- La carte et le **CCM** d'un côté pour l'alimentation du magasin de certificat **d'un coté**
- Le magasin de certificat, le **CSP** ASIP et la carte pour la réalisation des opérations cryptographiques **d'un autre côté**.

Le « **pont** » entre les deux est assuré par des composants de niveau applicatif.

Si l'application est un Navigateur Internet Explorer, l'intermédiaire est **schannel.dll** :

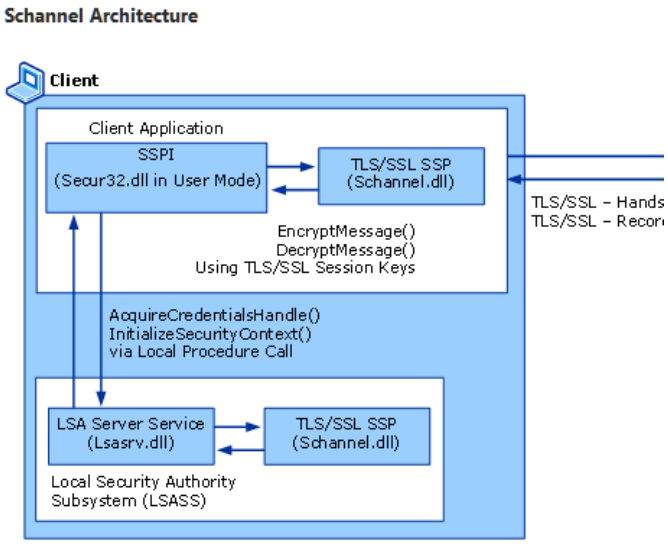

Figure 8 : Windows SChannel

Le lien entre **Schannel** et la stack TCP est assuré par **Wininet**:

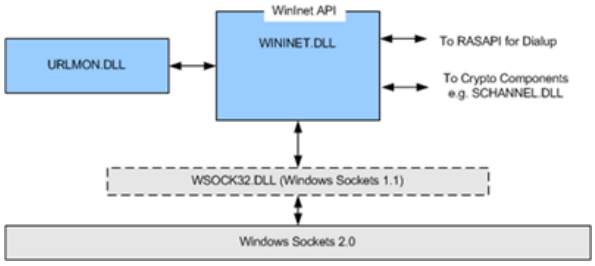

Figure 9 : Windows Wininet

Le lien entre **Schannel.dll** (SSL) et les opérations carte est assuré par le **CSP** (**fourni par l'ASIP Santé pour la carte CPS**).

Une étude est à prévoir sur MacOS X pour détailler le fonctionnement spécifique sur ce système.

3.2.4 Niveau Applicatif: authentification (Login)

Le caractère optionnel de certaines fonctionnalités de SSL est à l'origine de confusions préjudiciables entre sécurisation du lien client-serveur (opération de niveau transport, décrit ci-dessus) et login (opération de niveau applicatif).

3.2.4.1 Login avec transport en « authentification mutuelle »

Avec l'option « authentification mutuelle », le lien est sécurisé par SSL à l'aide du certificat client (utilisé une 1ere fois) et le **login** applicatif est **initié** par le (2nd) traitement du certificat client. Les deux traitements – maintien du transport et maintien de la session applicative – sont alors **indépendants**.

Cette indépendance est **importante**. Elle est **voulue** conceptuellement (OSI) et largement implémentée. Elle permet de construire des infrastructures réseau complexes, en particulier des infrastructures mettant en œuvre des frontaux web assurant l'offload SSL[4] couplés à des serveurs d'application en backend. Dans ce cas, le client et le frontal s'authentifient mutuellement et un composant de niveau applicatif supplémentaire doit :

- organiser l'authentification en « point à point » (partie cliente, partie serveur en passant par les éléments de réseau intermédiaires)
- reporter les informations de login de sorte que le **Subject** soit créé par le serveur d'application situé derrière le frontal
- **reporter les évènements de logout depuis le serveur d'application vers le frontal pour (à minima) libérer les ressources allouées pour la sécurisation du transport**

Ce **besoin de coordination** entre les différents acteurs de la partie serveur (synchronisation des états d'authentification, synchronisation des états de login, synchronisation des authentification/login) tend à montrer qu'une solution pérenne pour gérer ces aspects consiste à **utiliser un SSO** ou, à défaut, de s'inspirer des **concepts et bonnes pratiques** que les **solutions de SSO** couvrent.

[4] Offload SSL : le fait de déléguer à un composant logiciel spécifique la gestion des connexions SSL/TLS dans une application serveur

3.2.4.2 Login avec transport en « authentification serveur seule »

Ce cas de figure est le plus fréquent. Il couvre en particulier le cas où le lien client-serveur est un lien HTTPS sécurisant la transmission d'un couple login/mot de passe.

Dans ce scénario, la communication (couche transport) est sécurisée par SSL/TLS après une authentification simple du serveur et le login applicatif (couche application) peut être assuré :

- Soit par authentification client simple (1 seul facteur)
  - Par login/mot de passe
  - Cette implémentation est standard
  - Son implémentation est largement répandue
  - La carte n'est pas mise en œuvre
- Soit par authentification client forte
  - Le poste client est authentifié de manière forte
    - 2 facteurs
      - Via la carte
      - ou via OTP
  - Ce cas de figure est à évaluer du point de vue sécuritaire, les authentifications se passant
    - à des niveaux différents
      - L'authentification du serveur a lieu au niveau transport (SSL/TLS)
      - L'authentification du client a lieu au niveau applicatif
    - l'une après l'autre
      - authentification serveur puis authentification client
    - sans création et utilisation de secret commun
      - aucun clef symétrique n'est générée ni utilisée
      - les données échangées ne sont pas protégées suite à ces authentifications réciproques
  - Cette implémentation n'est pas standard et nécessite aussi bien un composant additionnel (de type applet) coté client que code côté serveur
  - **Exemple** : **RASS**

- Soit par authentification mutuelle « End-to-end »
  - Le poste client est authentifié de manière forte (2 facteurs via la carte)
  - Avec ou sans création de secret commun, ie avec ou sans protection des données en confidentialité ou en intégrité.
    - Le transport est sécurisé après une authentification simple du serveur.
    - L'authentification mutuelle est ré-implémentée au niveau applicatif coté client et coté serveur.
  - Cette implémentation n'est pas standard et nécessite aussi bien un composant additionnel (de type applet) coté client que code côté serveur
  - **Cette solution est la meilleure solution du point de vue conceptuel.**

Dans les deux derniers cas, selon les bonnes pratiques de sécurité, les implémentations doivent utiliser les enceintes sécurisées disponibles (hardware – HSM, ou software – LSA chez MS, NSS chez Firefox) pour mettre en œuvre les opérations cryptographiques (pas de clef en bytearray…). Ceci est à confronter toutefois à l'analyse de risque spécifique à chaque projet.

4 Les solutions types de gestion de l'authentification par carte CPS

4.1 Présentation de l'approche générale

Pour prendre en charge l'authentification par carte CPS, il n'existe pas de solution unique, réutilisable dans toutes les applications. La bonne solution dépend d'un ensemble de facteurs qui peuvent se combiner :

- Les besoins fonctionnels de l'application liés aux cartes, au-delà de la simple authentification par CPS : lecture Carte Vitale, signature électronique …
- Les exigences ergonomiques : les pages d'erreur par défaut du navigateur sont-elles acceptables ou exige-t-on des pages personnalisées ?
- Les exigences de sécurité de l'application : gestion plus ou moins fine de l'arrachage de carte, vérification en continu de la présence de la carte, besoins de traces applicatives de mise en œuvre de la carte …
- Les configurations de poste de travail visées : OS, navigateurs, prérequis techniques comme la compatibilité avec les configurations « FSE »,
- Les solutions logicielles serveur utilisées : sont-elles développées spécifiquement ou intègrent-elles des progiciels existants, qui imposent un certain fonctionnement ?

Ce chapitre présente donc différentes solutions de mise en œuvre de l'authentification dans des applications Web, qui répondent à la majorité des cas rencontrés.

4.2 Les modes d'authentification

Pour gérer l'authentification par carte dans une application Web, deux grandes approches sont possibles :

4.2.1 Authentification par TLS gérée par le navigateur

Dans ce cas, le navigateur gère directement l'authentification forte en se basant sur les composants standards du poste de travail.

Cette configuration nécessite:

- Un lecteur de carte CPS correctement* configuré,
- La Cryptolib CPS correctement * installée sur le poste de travail,
- Un navigateur Web correctement* configuré pour s'interfacer avec la CPS.

*Remarque : la vérification de tous ces prérequis sur le poste de travail et l'installation de la Cryptolib CPS sont gérés par l'outil « ODI PS » mis à disposition par l'ASIP Santé (CF chapitre 3.1.1.7).

Dans ce mode, lorsque l'application serveur exige la présentation d'un certificat client, c'est le navigateur qui prend en charge

- la sélection du certificat (en présentant éventuellement une boite de dialogue à l'utilisateur)
- la saisie du code PIN de la carte par l'utilisateur
- l'établissement de la session TLS avec l'application serveur.

Pour résumer les spécificités de ce mode d'authentification sont les suivantes :

Le comportement de tous les navigateurs ne sont pas les mêmes, en fonction de leur façon de gérer les magasins de certificats, en fonction de leur fonctionnent interne : l'application serveur doit donc prendre en compte ce paramètre lors de la conception de l'authentification pour que le comportement vis-à-vis de l'utilisateur final soit cohérent dans toutes les cas de figures. Ainsi le navigateur Firefox détecte lui-même l'arrachage de la carte, alors que ce n'est pas le cas pour les autres navigateurs Windows qui s'appuient sur le magasin de certificats du système d'exploitation (Chrome, IE, Safari).

En cas d'arrachage de carte ou d'insertion tardive de la carte, une page d'erreur spécifique au navigateur est présentée à l'utilisateur, qui ne peut pas être personnalisée pour une application spécifique. La mise en œuvre d'une page d'erreur 403 spécifique est éventuellement faisable mais reste à valider techniquement.

En revanche, la validation des configurations postes de travail est largement simplifiée par le fait que les seuls composants à déployer sur le poste sont ceux cités ci-dessus. Ces derniers existent depuis longtemps, ont un comportement connu qui peut donc être anticipé lors de la conception de l'application.

La gestion de l'authentification par les navigateurs est sous la responsabilité de l'éditeur du logiciel, et on peut donc estimer que celle-ci est mise en œuvre de façon fiable. Ce point doit cependant faire l'objet d'une vigilance particulière pour les navigateurs tels que Firefox et Chrome qui se mettent à jour automatiquement et très souvent, sans pouvoir anticiper facilement d'éventuels changements de fonctionnement ou d'éventuelles régressions.

4.2.2 Authentification applicative par add-on navigateur

Dans ce cas, le navigateur Web est l'interface utilisateur permettant d'accéder à l'application, mais celui-ci délègue à un autre composant présent sur le poste de l'utilisateur la gestion de l'authentification : on parle alors d'authentification applicative par add-on navigateur.

L'authentification applicative par add-on permet de gérer un certain nombre de fonctions liées à la carte de façon beaucoup plus fine que l'authentification navigateur, et adaptée spécifiquement aux besoins de l'application Web (sélection du certificat, saisie du code PIN, insertion de la carte, arrachage de la carte …), et ceci avec un comportement identique pour tous les navigateurs compatibles avec ce composant spécifique gérant la carte.

L'authentification en elle-même peut se faire de plusieurs manières, comme par exemple :

- Par des échanges applicatifs entre la carte et l'application serveur, au sein de la connexion TLS gérée par le navigateur, qui mettent en œuvre la signature électronique de la carte CPS,
- Par une connexion TLS utilisant le certificat d'authentification de la carte, gérée par le composant applicatif, par laquelle transitent les transactions du navigateur Web.

Le composant gérant l'authentification peut prendre plusieurs formes, comme par exemple :

- Une Applet Java chargée dans le navigateur (portable inter-navigateurs)
- Une extension navigateur (spécifique au navigateur)
- Un logiciel installé sur le poste client (indépendant du navigateur mais spécifique à l'OS).

La mise en œuvre de ce type de composant pose la problématique de la gestion à la fois de la compatibilité des configurations systèmes et de la gestion de la configuration des postes (maintien des configurations et des mises à jour des versions, vérification des prérequis techniques sur le poste). On peut toutefois distinguer deux types de composants :

- Les composants installés définitivement sur le poste de travail (ex : SrvSvCNAM de la CNAMTS),
- les composants téléchargés à l'usage depuis l'application Web (ex : applets Java) : la compatibilité avec les prérequis postes reste à gérer (JVM par exemple), mais le composant utilisé est assuré d'être toujours compatible avec l'application Web, étant donné qu'elle gère la cohérence entre ses propres composants.

En fonction de la façon dont est développé le composant gérant l'authentification applicative, les prérequis sur le poste ne sont pas les mêmes. Il faudra toujours *à minima* un pilote pour le lecteur de cartes, et un GALSS si un lecteur bi-fentes est utilisé, mais au-delà de ça, il n'est pas forcément nécessaire d'avoir d'autre prérequis, tels que la Cryptolib CPS, le composant pouvant intégrer lui-même l'accès aux fonctions cryptographiques de la carte.

4.2.3 Exemples de solutions mises en œuvre dans des projets de l'ASIP Santé

L'application MSSanté: complexité reportée sur le Reverse Proxy

L'application Web MSSanté utilise l'authentification CPS par TLS gérée par le navigateur Web. Les seuls composants nécessaires sur le poste de travail sont donc un lecteur de carte, la Cryptolib CPS et un navigateur.

L'authentification CPS sur TLS est donc prise en charge par le Reverse Proxy dont la configuration (ainsi que celle de l'application) est adaptée au comportement de tous les navigateurs Web.

Le mode de fonctionnement de ce Reverse Proxy doit donc évoluer dans le temps en fonction de l'évolution des systèmes d'exploitation et des navigateurs.

Le RASS: complexité reportée sur un produit

A contrario, l'authentification par CPS sur l'application Web du RASS repose uniquement sur une solution applicative du marché basée sur une applet Java gérant l'authentification en utilisant la signature électronique de la carte, et sur un serveur d'authentification spécifique qui prend en charge la vérification de cette signature et la propagation au niveau applicatif de cette authentification. Cette applet Java prend en charge également l'arrachage de la carte et la propagation au niveau applicatif de la déconnexion de l'utilisateur.

Le navigateur Web n'est donc aucunement sollicité pour la mise en œuvre de l'authentification dans cette application. Il est utilisé uniquement pour établir un canal HTTPS sans authentification client, pour assurer la confidentialité des échanges.

Ce produit gérant la CPS doit lui aussi évoluer en fonction des technologies OS/Navigateurs présentes sur le marché et des différentes versions de Java.

DMP: une solution mixte

L'application Web DMP utilise une applet Java. Mais il faut distinguer le fait d'utiliser une applet (pour des raisons applicatives) et la gestion de l'authentification par l'applet, même si, de fait, lorsqu'un composant spécifique est déployé sur le poste de travail, il est facile de lui déléguer un maximum de fonctions.

Ainsi, l'application Web DMP utilise bien une authentification TLS par navigateur, l'applet servant à d'autres usages, en particulier :

- La lecture des données de la CPS et la signature électronique des lots de soumission,
- La gestion fine de l'arrachage de la CPS par polling du lecteur (on est donc dans une gestion applicative uniquement pour la déconnexion CPS),
- La lecture de la carte Vitale.

4.3 Cinématiques d'authentification et bonnes pratiques

Plusieurs solutions sont envisageables pour mettre en œuvre l'authentification par CPS de façon aisée.

Le choix d'une solution peut se faire sur plusieurs critères tels que :

- Les exigences fonctionnelles et de sécurité de l'application,
- La mise en œuvre d'un ou plusieurs modes d'authentification (CPS uniquement, Login/password/OTP + CPS),
- La capacité de l'application à gérer tel ou tel type d'authentification, considérant que certains progiciels imposent une cinématique spécifique,
- Les prérequis poste de travail.

Ce chapitre présente 4 solutions utilisables en fonction de différents critères. Une grille de lecture possible de ces solutions peut être la suivante :

Mode d'authent. | *Scénarios*	**Navigateur seul**	**Navigateur + add-on**
Authent. CPS uniquement	Cas 1	Cas 2
Authent. CPS + OTP	Cas 3	Cas 4

Tableau 3 : Résumé des solutions envisageables pour l'authentification avec CPS

Les solutions préconisées doivent à terme couvrir au mieux la combinatoire (X modes d'authentification, Y clients possibles) et donc tendre vers des préconisations SSO.

4.3.1 Vérification en continu de la présence de la carte dans l'application

Dans ce mode, à cause d'exigences de sécurité ou parce que l'application fonctionne de cette manière, la présence de la carte dans le lecteur doit être assurée tout le long de l'usage de l'application.

4.3.1.1 Cas1 : authentification par le navigateur

L'application Web doit être découpée en deux domaines qui se retrouvent de façon identique au niveau applicatif et au niveau de la configuration du Reverse Proxy :

- Un domaine non authentifié ne requérant pas la carte CPS,
- Un domaine authentifié requérant la carte CPS.

L'utilisateur accède initialement à l'application Web par le domaine ne requérant pas la carte CPS.

Lorsque l'utilisateur veut accéder à la partie authentifiée de l'application, l'utilisateur doit avoir inséré préalablement la carte CPS dans le lecteur et rafraichi si besoin l'état du lecteur. Le lecteur doit être rafraichi par l'utilitaire CCM s'il n'était pas branché préalablement ou si la carte n'était pas insérée. L'utilisateur clique alors sur le lien qui l'envoie dans le domaine qui requiert la carte CPS (cet aspect est géré au niveau serveur par le Reverse Proxy gérant la connexion TLS avec le navigateur). Le navigateur présente alors le choix du certificat à utiliser et la saisie du code PIN (le code PIN n'est pas demandé si le navigateur l'a déjà fait préalablement).

Tant que l'utilisateur doit rester authentifié, L'application Web reste sur le même domaine « authentifié » requérant la carte CPS. Lors de chaque requête http envoyée par le navigateur, le certificat X509 de l'utilisateur est accessible depuis l'application Web.

La vérification de la présence de la carte CPS est gérée différemment selon le navigateur :

- Firefox gère lui-même l'arrachage de la carte, et dès que la carte est retirée du lecteur, le navigateur affiche une page d'erreur interne et l'utilisateur est déconnecté,
- IE ou Chrome (qui s'appuient sur le magasin de certificats de Windows) ne détectent pas directement l'arrachage de la carte : la vérification de la présence carte est donc faite lors de renégociations de la connexion TLS qui accède à la clé privée de la carte. Cette renégociation est paramétrée au niveau du Reverse Proxy pour se faire à des intervalles de temps réguliers de plusieurs minutes (configurable). Si, lors d'une renégociation, le certificat n'est plus accessible (la carte n'est plus dans le lecteur), alors le navigateur affiche une page d'erreur interne (non configurable) et l'utilisateur est déconnecté. Il peut donc s'écouler plusieurs minutes entre l'arrachage effectif de la carte et la déconnexion.

En cas de déconnexion dans l'application (après timeout applicatif ou action de l'utilisateur), l'utilisateur doit être redirigé vers le domaine ne requérant pas l'authentification CPS.

Le schéma ci-dessous synthétise le fonctionnement nominal décrit dans ce chapitre :

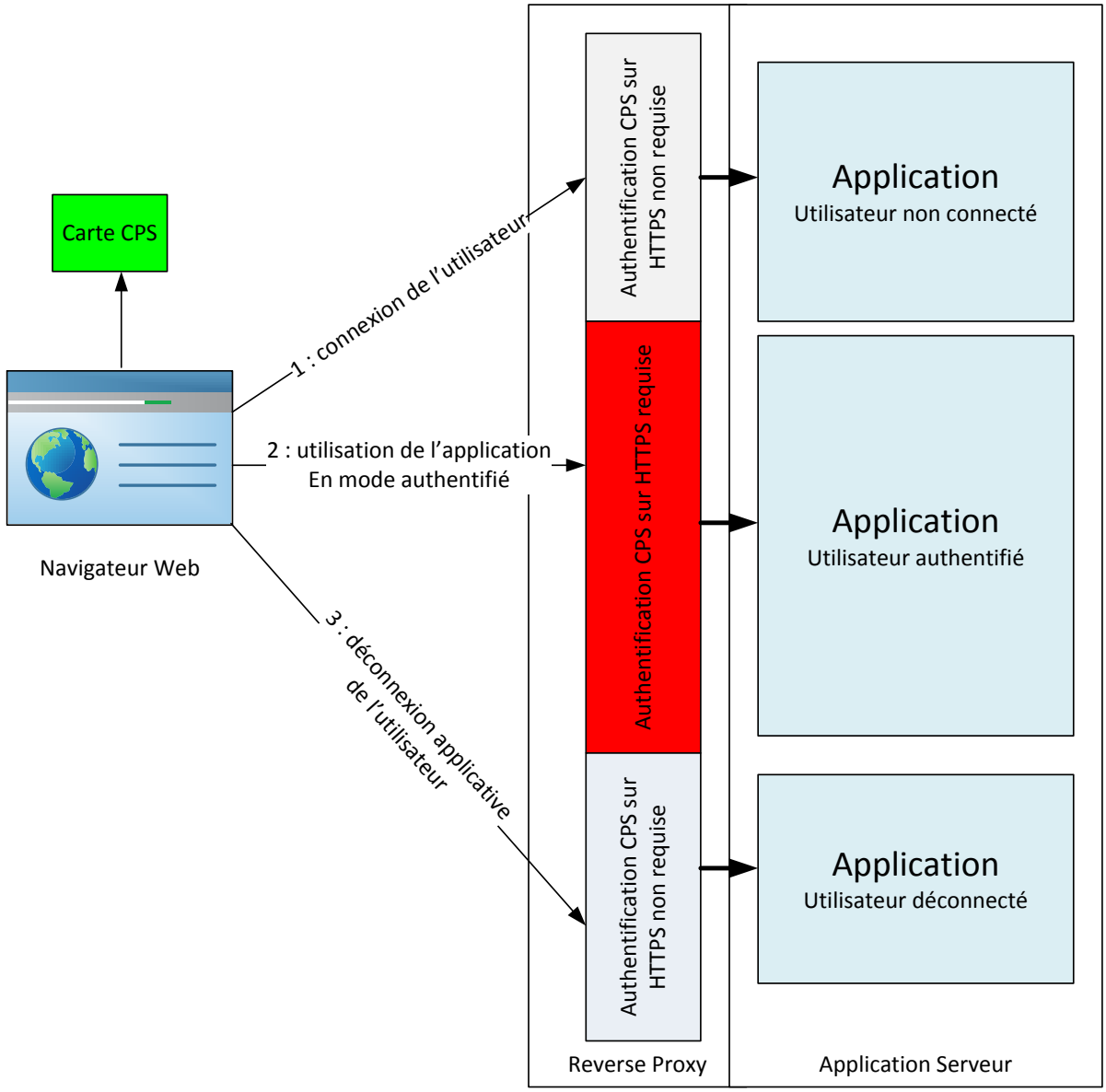

Figure 10 : Cas1 - authentification par le navigateur et vérification de la présence carte

4.3.1.2 Cas 2 : authentification applicative avec add-on

L'authentification applicative étant entièrement sous contrôle de l'application Web, il n'y a pas un mode de fonctionnement unique pour prendre en compte ce besoin. Ce chapitre présente donc un mode de fonctionnement *possible*, mettant en œuvre un composant de type applet ou ayant un fonctionnement similaire (ActiveX, plugin navigateur..).

L'utilisateur se connecte sur l'application Web en HTTPS sans authentification client sur TLS.

Lorsque l'utilisateur accède à la partie authentifiée, alors le composant spécifique sur le poste de travail gérant l'authentification est activé par l'application. Il demande le code PIN permettant de déverrouiller l'accès aux certificats de la carte, et échange applicativement (mise en œuvre de la signature CPS) au sein de la connexion HTTPS du navigateur avec l'application, qui s'assure ainsi de l'identité de l'utilisateur.

La session utilisateur est maintenue par l'application Web. Le composant gérant l'accès à la carte reste actif pendant l'usage de l'application et fait un polling régulier sur la carte. En cas d'arrachage de la carte, le composant le détecte, envoie une requête applicative au serveur, qui renvoie l'utilisateur sur une page Web lui indiquant sa déconnexion.

En cas de déconnexion dans l'application (après timeout applicatif ou action de l'utilisateur), le contexte applicatif de l'utilisateur est supprimé côté serveur et côté navigateur, et l'utilisateur est redirigé vers une page ne requérant pas d'authentification.

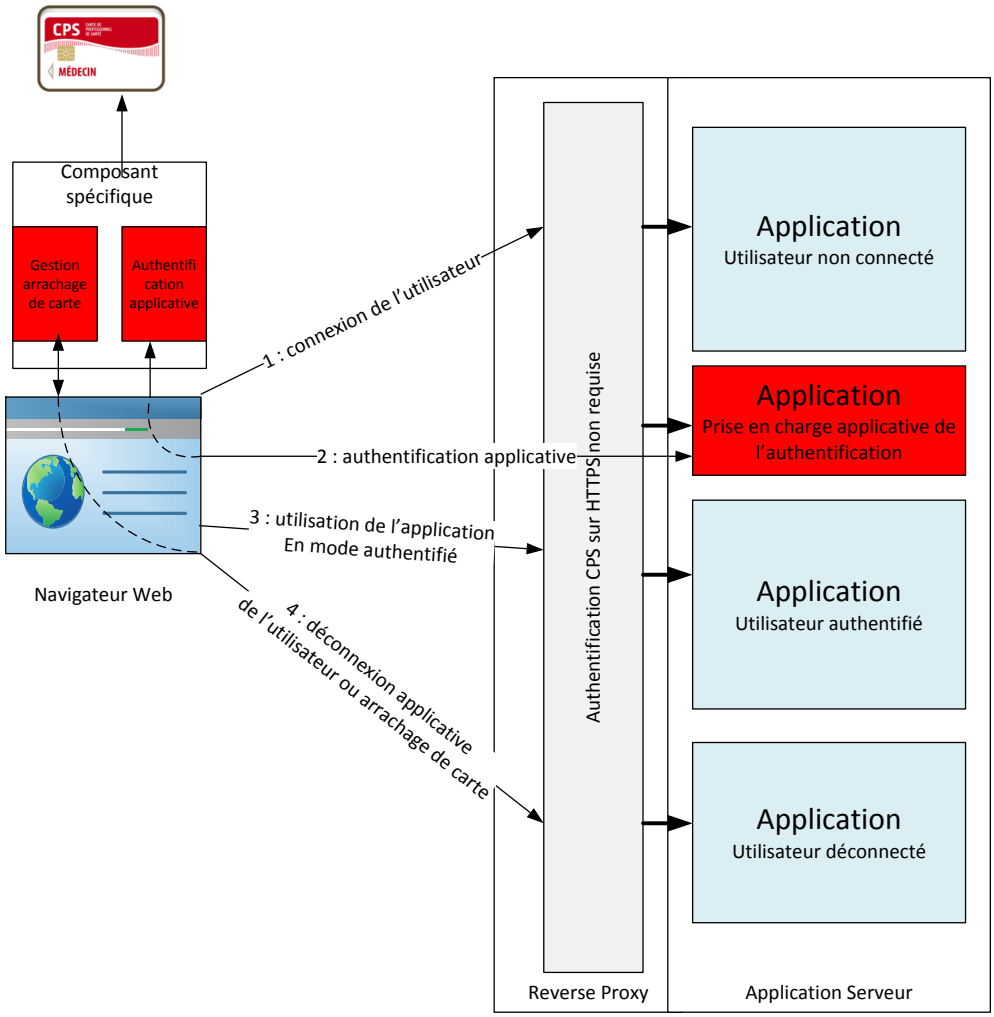

Figure 11 : Cas 2 - authentification applicative avec add-on et vérification de la présence carte

4.3.2 Authentification limitée à la présence initiale de la carte

Dans ce mode de fonctionnement, la carte CPS est nécessaire à l'initialisation de l'accès à l'application, et n'est plus requise pas la suite, l'authentification étant matérialisée par la présence d'un jeton. L'authentification est donc valide pour une certaine durée, que la carte soit ou non toujours présente dans le lecteur.

Cette cinématique de fonctionnement a l'avantage d'être la même qu'avec d'autres modes d'authentification (par exemple identifiant/mot de passe/OTP). C'est par exemple la cinématique qui est mise en œuvre par les Web Services de messagerie MSSanté.

Elle est également compatible :

- Avec le mode de fonctionnement de nombreux logiciels du marché utilisant des jetons d'authentification;
- Avec des composants du marché spécialisés dans la gestion de l'authentification, basés éventuellement sur la norme SAML V2 qui peut servir de base à la mise en place ultérieure d'un portail d'authentification inter-applicatif.

4.3.2.1 Cas 3 : authentification par le navigateur

L'application Web doit être découpée en trois domaines qui se retrouvent de façon identique au niveau applicatif et au niveau de la configuration du Reverse Proxy :

- Un domaine non authentifié ne requérant pas la carte CPS,
- Un domaine d'authentification qui requiert la carte CPS et qui génère un jeton d'authentification,
- Un domaine authentifié ne requérant pas directement la carte CPS (au niveau TLS), mais requérant un jeton d'authentification, sans lequel l'utilisateur ne peut pas accéder aux fonctions.

L'utilisateur accède initialement à l'application Web par le domaine ne requérant pas la carte CPS.

Lorsque l'utilisateur veut accéder à la partie authentifiée de l'application, l'utilisateur doit avoir inséré préalablement la carte CPS dans le lecteur et rafraichi si besoin l'état du lecteur. L'utilisateur clique alors sur le lien qui l'envoie dans le domaine d'authentification qui requiert la carte CPS (cet aspect est géré au niveau serveur par le Reverse Proxy gérant la connexion TLS avec le navigateur). Le navigateur présente alors le choix du certificat à utiliser et la saisie éventuelle du code PIN.

Une fois authentifié au niveau TLS, l'application côté serveur génère un jeton d'authentification qui est retourné à l'utilisateur, et ce dernier est renvoyé (redirection HTTP avec le status code 302) sur le domaine 'authentifié', dans lequel l'application serveur vérifie la présence et la validité du jeton d'authentification.

A partir de ce moment, si la carte CPS est retirée du lecteur, l'application continue à fonctionner puisque la carte n'est plus requise au niveau de la connexion HTTPS.

En cas de déconnexion dans l'application (suite à l'expiration de la validité du jeton d'authentification ou action de l'utilisateur), l'utilisateur doit être redirigé vers le domaine non authentifié ne requérant pas l'authentification CPS.

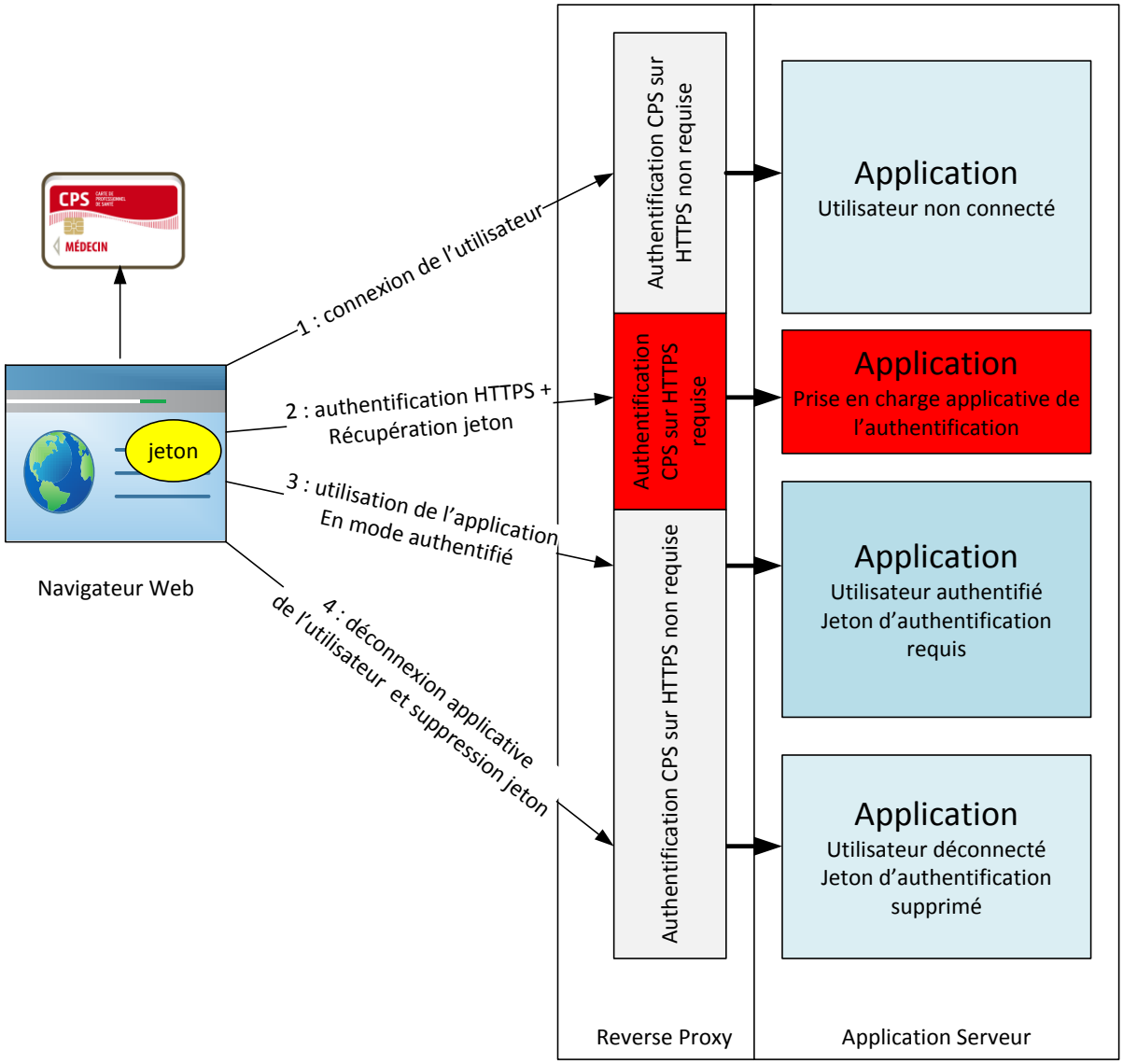

Figure 12 : Cas 3 - authentification par le navigateur sans vérification ultérieure de la présence carte

4.3.2.2 Cas 4 : authentification applicative avec add-on

La cinématique est comparable à celle du cas 3, avec un composant applicatif gérant l'accès à la CPS plutôt que reposer sur les mécanismes TLS du navigateur.

Cela permet de gérer plus finement l'insertion tardive de la carte, et une page d'erreur personnalisée en cas d'échec de l'authentification.

Cette solution peut être décrite par le schéma ci-dessous :

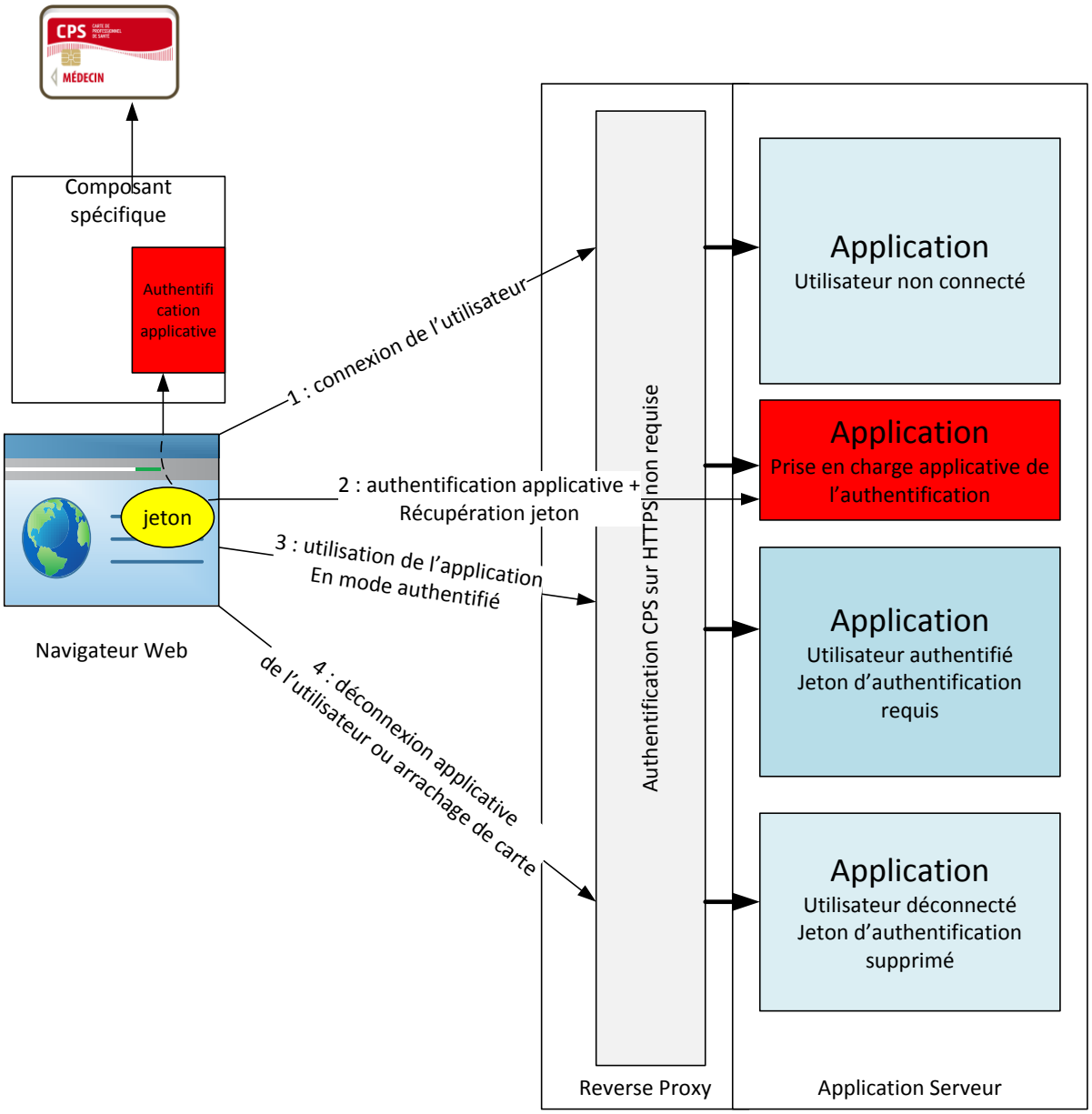

Figure 13 : Cas 4 - authentification par add-on sans vérification ultérieure de la présence carte

4.4 Synthèse des cas d'usage

Ce chapitre présente une synthèse comparative des solutions présentées, regroupées en deux « familles » :

- Les cas 1 et 3 : Authentification et login CPS en utilisant le navigateur Web seul (sans add-on navigateur spécifique),
- Les cas 2 et 4 : Authentification et login CPS en utilisant un add-on navigateur dédié à la prise en charge de l'authentification par CPS.

Ce tableau permet aux chefs de projets, experts ou architectes de :

- prendre connaissance et définir ce qu'il est possible de faire,
- définir les limites d'une situation donnée,
- organiser les documents, revues et intervention des experts.

Il a donc vocation à servir de « check list » au moment des initialisations de projets impliquant la CPS.

Son formalisme et son niveau de détail pourront être approfondis dans des versions ultérieures.

En l'état, par exemple :

- un chef de projet
    - souhaitant garantir que :
        - **l'arrachage de carte soit géré instantanément**
    - pourrait aller chercher la ligne « Gestion des évènements (...) / Cartes / Temps réel »
        - **filtre sur la colonne « Aspects de mise en œuvre »**
    - dans ce tableau et s'apercevoir qu'il se trouve du coup dans le scénario
        - « Authentification CPS et login avec add-on »
    - Et ainsi **réexaminer l'ensemble des éléments** concomitants à ce scénario précis

Il ressort de cette synthèse qu'un composant spécifique sur le poste de travail est nécessaire à partir du moment où une fonction demandée va au-delà de ce que peut faire nativement un navigateur Web.

Aspect de mise en œuvre dans l'application	**Détails**	**Cas 1 et 3: Authentification et login CPS navigateur (sans add-on)**	**Cas 2 et 4: Authentification CPS et login avec add-on**
Type de client requis		Léger	Léger + Add-on
Exigence de sécurité requise sur l'authentification		Forte	Très forte
Exigence requise pour l'ergonomie de l'application		Bonne	Très bonne
Log in (connexion de l'utilisateur à l'application)	Méthode	Client-cert	Client-cert
	Plusieurs méthodes Log in possibles (ex : CPS+OTP)	Oui	Oui
	Insertion tardive CPS	Oui	Oui
Configuration de l'utilitaire CCM recommandée	Mode de détection	Mode automatique activé	Indépendant de l'état de recherche du CCM
Protocole de transport		TLS (HTTPS)	TLS (HTTPS)
Gestion des CRL par l'application serveur		Oui	Oui
Offload SSL (gestion TLS par un composant dédié)		Oui	Oui
Pages d'erreur d'authentification à l'application		Oui (403 uniquement, à valider techniquement)	Oui pour toutes les cas d'erreurs (1)
Gestion applicative des événements sur le poste de travail	Evénements Lecteur (branchement, débranchement)	Non	Temps réel
	Evénements Carte (insertion, retrait)	Non	Temps réel
	Evénements magasin (montée/descente des certificats)	Non (2)	Temps réel
Vérification de la disponibilité de la clef privée de la carte		Non (3)	Oui
Configuration du poste de travail			Plus complexe car composant spécifique
Architecture serveur			Plus complexe car composant spécifique
Authentification	Authent. client	Forte (sans gestion de tous les évènements)	Forte (gestion possible de tous les évènements)
	Authent. serveur	Oui (TLS)	Oui, paramétrable
	Authent. Mutuelle	Oui (TLS)	Possible (End to end), dépend des composants
Log off (déconnexion)	Never	Oui	Oui
	On-demand	Oui	Oui
	Timeout	Oui	Oui
	Arrachage	Gestion difficile, dépend du navigateur (4)	Oui

Tableau 4 : Tableau de synthèse des mises en œuvre

(1), (2), (3), (4): Ces appréciations sont préciser par des travaux complémentaires.

5 La problématique des CRL

Les listes de révocation de certificats (CRL) sont produites par toutes les infrastructures de gestion de clés (IGC) gérant des certificats X509. Ce sont des listes qui regroupent tous les certificats qui ont été révoqués avant leur date d'expiration quelle que soit la raison (perte, vol, dysfonctionnement …).

Pour information, les CRL sont téléchargeables à partir de l'annuaire CPS (http://annuaire.gip-cps.fr/). Les tailles des principales CRL correspondant aux cartes produites par l'ASIP Santé sont les suivantes (juillet 2013):

Nom	Description	Taille
GIP-CPS CLASSE-0.crl	Cartes CPE non-nominatives	3 Mo
GIP-CPS CLASSE-1.crl	Cartes CPS et CPF	11 Mo
GIP-CPS CLASSE-2.crl	Cartes CDE et CPA responsables d'entités	417 Ko
GIP-CPS CLASSE-3.crl	Cartes CPE et CPA employés de structures	677 Ko

Tableau 5 : Tailles des CRL ASIP Santé

Les CRL produites actuellement par l'IGC CPS pour les cartes CPS ont deux caractéristiques à prendre en compte dès la conception :

- Les listes sont de grande taille (environs 600 000 lignes, 11 Mo),
- Les CRL sont signées par un certificat différent de celui qui signe les certificats utilisateurs : ceci est conforme à la norme, mais peu implémenté dans les produits du marché. De fait aucun Reverse Proxy du marché n'implémente nativement la gestion de cette CRL, et l'ASIP Santé développe et maintient un patch pour le Reverse Proxy Apache pour mettre à disposition une solution opérante[5].

La version actuellement utilisée d'Apache (2.2) gère mal les CRL de grande taille, ce qui peut provoquer des problèmes de performances.

Le patch spécifique à l'IGC CPS pour Apache, mis à disposition par l'ASIP Santé, est en cours de portage sur la version 2.4 du produit. Indépendamment du patch, la vérification de l'amélioration des performances d'Apache sur cette version pour la gestion des CRL de grande taille devra être faite.

Il faut noter que les CRL seront amenées à réduire progressivement en taille durant les mois et années à venir (fin de la généralisation de la CPS3).

Cette problématique des CRL disparaitra à terme avec la nouvelle IGC Santé (S2 2014), qui prévoit

- une gestion standard de la signature des CRL, et donc une compatibilité avec tous les produits du marché,
- un répondeur OCSP, qui permettra aux composants Reverse Proxy d'appeler un service centralisé de vérification de validité du certificat, sans avoir à gérer directement les CRL.

Les solutions actuellement possibles pour gérer les CRL sont donc les suivantes :

[5] Le patch Apache est disponible sur le site intégrateur de l'ASIP Santé (moyennant inscription) :

http://integrateurs-cps.asipsante.fr/informations_cps/Patch-mod_SSL-pour-Apache-2.2.17

1) Utiliser les CRL dans Apache et augmenter les ressources techniques dédiées

Il s'agit d'augmenter les ressources CPU et RAM des serveurs hébergeant les serveurs Apache, afin qu'ils soient en mesure d'absorber la charge.

Cela doit s'accompagner d'une configuration qui limite le plus possible la vérification de la CRL à l'authentification initiale de l'utilisateur, et donc en désactivant le contrôle CRL lors des renégociations TLS qui peuvent se dérouler ultérieurement.

2) Désactiver la gestion des CRL dans le Reverse Proxy et déléguer cette fonction à un composant applicatif

La gestion des CRL n'est pas nécessairement à faire au niveau du reverse proxy, qui peut la désactiver. Les composants applicatifs peuvent gérer eux-mêmes la non-révocation d'un certificat en dehors du Reverse Proxy, ce qui fait que ce dernier n'est pas nécessairement un serveur Apache « patché ASIP Santé ».

La gestion des CRL peut être faite par composant du marché ou par un composant développé spécifiquement.

A noter qu'une application Web de l'ASIP Santé a choisi une solution de ce type, à savoir :

- Une gestion de l'authentification carte dans des boitiers dédiés faisant office de Reverse Proxy, mais qui ne gèrent pas les CRL,
- Un composant logiciel développé spécifiquement intégré à l'application DMP pour gérer les CRL au format spécifique de l'IGC CPS.

6 Conclusion et perspectives

La mise en œuvre de de l'authentification par carte CPS dans une application Web repose sur des composants qui sont techniquement fiables, et qui, une fois maitrisés, ont un comportement prédictible. Elle peut être sécurisée dès l'instant où des choix cohérents sont faits entre les solutions techniques retenues (navigateur seul, applet …) et les besoins fonctionnels (arrachage de cartes, pages d'erreurs personnalisées…).

Les problèmes rencontrés sont principalement liés au manque de prise en compte en amont des caractéristiques du système CPS et au fonctionnement de ses composants. Ce constat existe pour tout système à base de cartes à puces.

Le tableau du chapitre 4.4 tend à démontrer que les solutions utilisant des navigateurs avec add-on sont les plus simples à mettre en œuvre pour bien gérer l'authentification par carte CPS, tout en permettant à l'application de s'affranchir des différences de comportement des navigateurs Web. Ces solutions, spécifiques, doivent toutefois être maintenues et déployées pour toutes les configurations des systèmes utilisateurs, et doivent évoluer dans le temps avec les versions d'OS, navigateurs et autres middlewares éventuels (JVM…).

Ce document est un instantané technique et fonctionnel qui fera l'objet de mises à jour régulières. Les recommandations de l'ASIP Santé pourront évoluer en conséquence.

Il devra évoluer pour prendre en compte l'évolution des technologies, notamment :

- Les nouvelles versions d'OS et Navigateurs,
- Les Reverse Proxy.

7 Annexes

7.1 Annexe 1: OS supportés par le GALSS

Les versions des systèmes supportés à ce jour (juillet 2013) par le GALSS sont les suivantes:

Système	Versions
Windows	Windows XP Service pack 3 (32 bits) Windows Vista Service pack 2 (32 et 64 bits) Windows 7 Service pack 1 (32 et 64 bits) Windows 8 (32 et 64 bits)
Linux	Linux noyau 2.4 ou 2.6 sous Red Hat Enterprise
MacOS X	A minima MacOS X 10.6.8 (Snow Leopard)

Tableau 6 : OS Supportés par le GALSS

7.2 Annexe 2: tests effectués par ODI-PS

Les tests pris en charge par la version actuelle de l'ODI PS sont les suivants.

Pour rappel: pour une configuration donnée de l'outil, chaque ligne est activable ou non ; par exemple les configurations pour le DMP et la MSSanté ne réalisent pas exactement les mêmes diagnostics.

#	Diagnostic	Catégorie		Condition si contrôle activé
	Windows			
1		**Système d'exploitation**		obligatoire
1.1			version de Windows	obligatoire
1.2			version du Service Pack	obligatoire
1.3			Contrôle du compte de l'utilisateur (UAC)	optionnelle
2		**Navigateur**		obligatoire
2.1			version d'Internet Explorer, Firefox, Chrome	obligatoire
2.2			JavaScript activé	obligatoire
2.3			Applets Java activées	obligatoire
2.4			TLS 1.0 activé	obligatoire
2.5			Chaîne de confiance des certificats IGC-A	optionnelle
2.6			Chaine de confiance des certificats CPS	optionnelle
2.7			Configuration du gestionnaire de sécurité PKCS11 CPS	optionnelle
3		**Lecture de document**		
3.1			plugin lecture PDF	obligatoire
3.2			lecture des fichiers RTF	obligatoire
3.3			lecture des fichiers TIF	obligatoire
4		**Environnement Java**		optionnelle
4.1			version JRE	obligatoire
4.2			Téléchargement d'applet	optionnelle
4.5			Exécution d'applet	obligatoire
5		**Environnement CPS**		obligatoire
5.1			Gestionnaire d'accès lecteur	obligatoire
5.2			Librairies Cryptographiques	obligatoire
5.3			Librairie Cryptographique Filière « GALSS »	obligatoire
5.4			Certificats d'autorités CPS	optionnelle
5.5			Test de lecture	optionnelle
5.6			Audit de la carte CPS	optionnelle
6		**Environnement Vitale**		optionnelle
6.1			Droits sur le disque dur	obligatoire

#	Diagnostic	Catégorie		Condition si contrôle activé
6.2			Lecteur de la carte Vitale	obligatoire
6.3			Installation de la librairie de lecture	obligatoire
6.4			Gestionnaire d'accès lecteur	obligatoire
6.5			Librairie de lecture	obligatoire
6.6			Test de lecture	optionnelle
	Mac OS X			
1		**Système d'exploitation**		obligatoire
1.1			version de mac os	obligatoire
2		**Navigateur**		obligatoire
2.1			version SAFARI / Firefox / Chrome	obligatoire
2.2			JavaScript activé	obligatoire
2.3			Applet java activée	obligatoire
2.4			TLS 1.0 activé	obligatoire
2.5			Chaîne de confiance des certificats IGC-A	optionnelle
2.6			Chaine de confiance des certificats CPS	optionnelle
2.7			Configuration du gestionnaire de sécurité PKCS11 CPS	obligatoire
3		**Lecture de document**		optionnelle
3.1			plugin lecture PDF	obligatoire
3.2			lecture des fichiers RTF	obligatoire
3.3			lecture des fichiers TIF	obligatoire
4		**Environnement Java**		obligatoire
4.1			version JRE	obligatoire
4.2			Téléchargement d'applet	optionnelle
4.3			Exécution d'applet	obligatoire
5		**Environnement CPS**		obligatoire
5.1			Gestionnaire d'accès lecteur	obligatoire
5.2			Librairies Cryptographiques	obligatoire
5.3			Librairie Cryptographique Filière « GALSS »	obligatoire
5.4			Certificats d'autorités CPS	optionnelle
5.5			Test de lecture	optionnelle
5.6			Audit de la carte CPS	optionnelle
6		**Environnement Vitale**		optionnelle
6.1			Droits sur le disque dur	obligatoire
6.2			Lecteur de la carte Vitale	obligatoire
6.3			Installation de la librairie de lecture	obligatoire
6.4			Gestionnaire d'accès lecteur	obligatoire

#	Diagnostic	Catégorie		Condition si contrôle activé
6.5			Librairie de lecture	obligatoire
6.6			Test de lecture	optionnelle

Tableau 7 : Matrice des tests ODI

8 Annexe – Liste des figures

9 Annexe – Liste des tableaux

10Notes

[fin du document]

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
Tel : 01 58 45 32 50
esante.gouv.fr