



Guide
de mise en œuvre
de la
Cryptolib CPS
en
environnement
TSE/Citrix



AGENCE DES SYSTÈMES
D'INFORMATION
PARTAGÉS DE SANTÉ

Systeme CPS

Guide de mise en œuvre de la Cryptolib CPS en environnement TSE/Citrix

« ASIP Santé / PTS / PSCE »

Version 1.0.12 du 24/09/2014

Documents de référence				
N°	Version	Date	Auteur	Document
[1]	1.4		ASIP Santé	Manuel-d'installation-de-la-Cryptolib-environnement-TSE-CITRIX-V1.4.pdf
[2]	1.0.2		ASIP Santé	ASIP_Manuel_Pack-DMP-Etab_v1.0.2.pdf
[3]	1.0.2		ASIP Santé	ASIP_Manuel_Pack-DMP-Etab_TSE_CITRIX_v1.0.2.pdf
[4]			Microsoft	Microsoft Windows 2008R2 Remote Desktop Services Resource Kit - Microsoft Press
[5]			ASIP Santé	Site intégrateurs
[6]			ASIP Santé	Spécifications des MSI GALSS, Cryptolib CPS, API Vitale, Composants DMP
[7]			Wikipedia	Introduction à RDP en anglais Remote Desktop Services
[8]			Wikipedia	Présentation de Citrix en français Citrix Systems
[9]			Citrix	XenApp Compatibility WP US.pdf
[10]			Microsoft	W2003 Program compatibility flags
[11]			Microsoft	Microsoft Application Compatibility Toolkit 5.6
[12]			Microsoft	Guide pas à pas de RemoteApp Terminal Services de Windows Server 2008
[13]			Microsoft	Remote Desktop Connection 7 for Windows 7, Windows XP & Windows Vista Matrices d'usages comparés de RDP selon les OS
[14]	1.0.1		ASIP Santé	Guide de mise en œuvre des profils itinérants
[15]	2.5.3		ASIP Santé	Guide de mise en œuvre d'un Smartcard logon avec une carte CPS

Tableau 1 : Documents de référence

1 Résumé

Ce document s'adresse aux architectes techniques ou aux chefs de projets souhaitant mettre en œuvre la carte CPx dans des environnements utilisant les technologies TSE ou Citrix.

Il décrit dans une première partie l'état de l'art sur ces sujets puis expose dans une seconde partie les différents livrables fournis par l'ASIP Santé, leur domaine d'application et les modalités de mise en œuvre pour aboutir à l'exploitation des fonctionnalités offertes par la carte CPx dans ces environnements.

2 Sommaire

1	Résumé.....	4
2	Sommaire	5
3	Introduction.....	6
4	Glossaire	7
5	Les architectures TSE/Citrix.....	9
5.1	Une architecture "Microsoft".....	10
5.1.1	Côté Serveur	10
5.1.2	Côté Client	13
5.2	Une architecture "client-serveur"	21
5.3	Une architecture "client léger"	23
5.4	Points forts	24
5.5	Points d'attention.....	25
5.6	Citrix	26
5.6.1	Serveur Citrix XenApp 6.0 sous W2008R2 SP1.....	26
5.6.2	Points forts de la surcouche Citrix.....	27
5.6.3	Points d'attention de la surcouche Citrix	27
5.7	Smartcard logon	28
5.8	Profils itinérants	29
5.9	Considérations techniques.....	30
5.9.1	Impacts sur la conception applicative	30
5.9.2	Fonctionnalités avancées	31
5.9.3	Sécurisation des liens RDP/ICA.....	33
6	Les projets ASIP Santé concernés par TSE/Citrix.....	34
6.1	Rappels d'architecture carte CPx / carte Vitale	34
6.1.1	Exemple : Architecture GALSS pour l'application AW PS DMP	34
6.1.2	Exemple : Architecture PC/SC pour l'application AW PS DMP.....	35
6.2	Liste des projets.....	36
7	Le pack établissement	37
7.1	Fiche de synthèse	37
7.2	Contenu du Pack Etablissement.....	38
8	Annexe – principales GPOs.....	41
8.1	Autoriser les ouvertures de sessions à distance	41
8.2	Activer le service Plug-and-Play de la carte à puce.....	42
9	Annexe – Citrix	43
9.1	Installation du client léger et connexion à l'aide du client léger	43
9.2	Remarques connexion « Bureau à distance »	49
9.3	Paramétrage des GPO Citrix	52
10	Annexe – Table des figures.....	53
11	Annexe – Liste des tableaux	55
12	Notes	56

3 Introduction

Une installation rigoureuse des composants techniques, liés à la carte CPx, sur le poste de travail de l'utilisateur est requise pour les fonctionnements en environnement TSE ou Citrix.

L'ASIP Santé porte une attention particulière à ces "enablers" en les distribuant sous forme de packages qui répondent à deux cas d'usage:

1. l'utilisation de services à base de carte CPx / carte Vitale dans les cabinets privés, dans des configurations compatibles avec la facturation FSE
2. l'utilisation de services à base de carte CPx / carte Vitale dans les établissements, dans des configurations compatibles avec l'usage du Smartcard logon de Windows, entre autres.

En établissement, les contraintes rencontrées lors des installations, utilisations et mises à jour des composants logiciels sont celles de parcs de postes dits "administrés".

Dans ce cas, l'administration des postes de travail fait l'objet d'une centralisation orchestrée par les administrateurs système et réseau du SI.

L'ASIP Santé met donc à disposition un "pack" à l'attention des administrateurs réseaux des établissements, appelé "Pack établissement".

Ce pack permet d'automatiser les installations des composants ASIP Santé dans des environnements multi-utilisateurs conçus autour:

- des technologies serveurs Microsoft RDP/TSE
- avec ou sans surcouche Citrix XenApp/MetaFrame

Il est donc destiné à un public d'informaticiens expérimentés sur ces environnements.

L'ASIP Santé, à travers la maintenance de ce pack :

- suit les évolutions du GALSS et de l'API de lecture Vitale
- suit les évolutions de la Cryptolib CPS
- documente et diffuse le pack et sa documentation à travers le portail intégrateur
- en assure le support auprès des utilisateurs

4 Glossaire

Abréviation	Signification
ACT	Microsoft Application Compatibility Toolkit
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
AW PS DMP	Accès Web des Professionnels de Santé au DMP
CCM	CPS Certificate Manager
CDSA	Common Data Security Architecture
CPS	Carte des Professionnels de Santé
DMP	Dossier Médical Personnel
GALSS	Gestionnaire d'Accès au Lecteur Santé-Social
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure
ICA	Independent Computing Architecture
LAN	Local Area Network
MS	Microsoft
MSSanté	Messagerie Sécurisée de Santé
ODI	Outil de diagnostic et d'installation
OS	Operating System, Système d'exploitation
OSM	Outils de messagerie
PKCS	Public Key Cryptographic Standards, ensemble de spécifications conçues par RSA
PSCE	Prestataire de Service de Certification Electronique
PSS	Protocole Santé Sociale
PTS	Pôle Technique et Sécurité

Abréviation	Signification
RDP	Remote Desktop Protocol
RemoteApp	Remote Application, ie. application distante
SI	Système d'Information
SSL	Secure Socket Layer
TBW	A compléter
TLS	Transport Layer Security
TSE	Terminal Server Edition
WAN	Wide Area Network

Tableau 2 : Glossaire

5 Les architectures TSE/Citrix

Les technologies serveurs Microsoft "Remote Desktop Services" (RDP, anciennement TS(E) pour Terminal Services (Edition), cf. [7]) sont basées sur une architecture :

- Client-serveur
- Avec clients légers

Les technologies Citrix XenApp (anciennement Citrix MetaFrame) s'installent sur des serveurs Microsoft Server (le terme de « surcouche » est souvent employé).

Ces technologies sont développées par Citrix Systems, entreprise qui propose une large palette de produits s'appuyant sur ceux de Microsoft (cf. [8]).

Ces installations (TSE ou Citrix) sont largement répandues en établissements, à l'image d'ailleurs de ce qui se fait en dehors du monde de la santé.

5.1 Une architecture "Microsoft"

Cette partie présente TSE de façon visuelle afin de fixer les idées du lecteur.

5.1.1 Côté Serveur

TSE se présente sous la forme d'un serveur Windows Server (ici 2008R2 SP1) avec le « rôle TSE » activé:

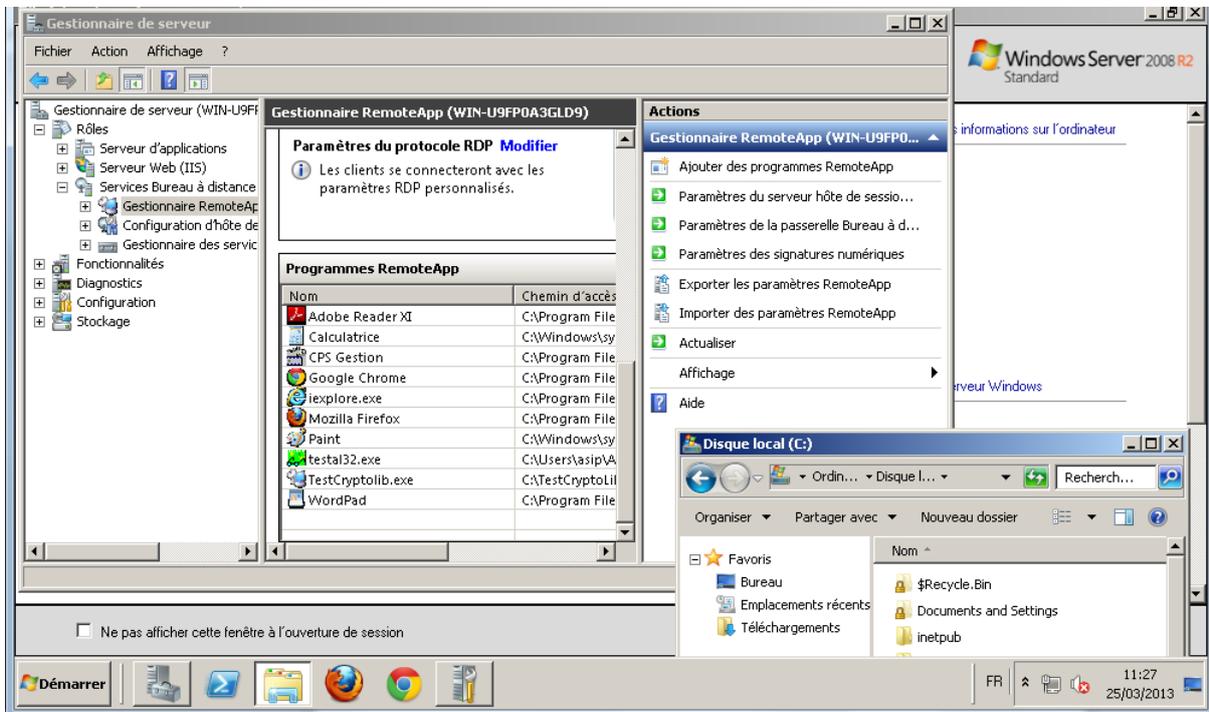


Figure 1: Console graphique d'un serveur Windows Server 2008

La fonction TSE est activée.

L'interface graphique est celle d'un OS Windows « normal ».

Le serveur TSE permet de « publier » des applications distantes (« RemoteApp ») :



Figure 2: Fonction d'installation d'une application distante sous TSE

Le serveur TSE permet de gérer les applications distantes [W2008]:

Programmes RemoteApp			
Nom	Chemin d'accès	Accès Burea...	Argur
Adobe Reader XI	C:\Program Files (x86)\Adobe...	Oui	Désac
Calculatrice	C:\Windows\system32\calc.exe	Oui	Désac
CPS Gestion	C:\Program Files (x86)\santes...	Oui	Désac
Google Chrome	C:\Program Files (x86)\Googl...	Oui	-no-s
iexplore.exe	C:\Program Files\Internet Ex...	Oui	Désac
Mozilla Firefox	C:\Program Files (x86)\Mozill...	Oui	Désac
Paint	C:\Windows\system32\mspai...	Oui	Désac
testal32.exe	C:\Users\asip\AppData\Local...	Oui	Désac
TestCryptolib.exe	C:\TestCryptoLib\TestCryptoli...	Oui	Désac
WordPad	C:\Program Files\Windows N...	Oui	Désac

Figure 3: Liste des applications publiées

Un administrateur peut :

- [1] Accorder des droits sur des applications distantes en utilisant le système de droits Microsoft (et donc Active directory, si il est déployé) [W2008R2]:



Figure 4: Saisie des droits sur application distante

- [2] Rendre une application disponible via l'accès Web TS ou non [W2008R2]:

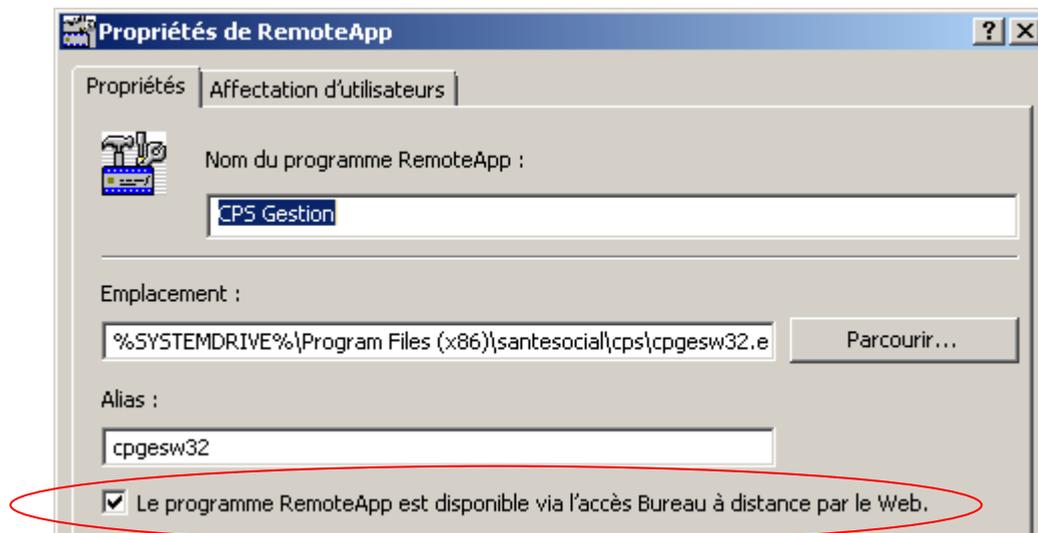


Figure 5: Rendre disponible une application distante via le Web

5.1.2 Côté Client

5.1.2.1 Client RDP [W2003+]

Depuis son poste client léger, qui peut être un Windows avec ou sans application installée, un Windows Embedded ou un Windows Thin PC, l'utilisateur initie une session (voir architecture client-serveur ci-après) en exécutant un client RDP (exécutable **mstsc.exe** dans le gestionnaire de tâches):

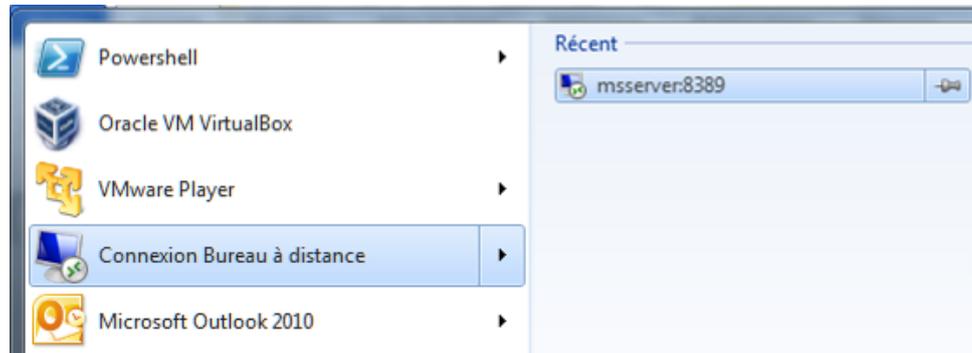


Figure 6: Lancement du client « remote desktop » sous Windows 7

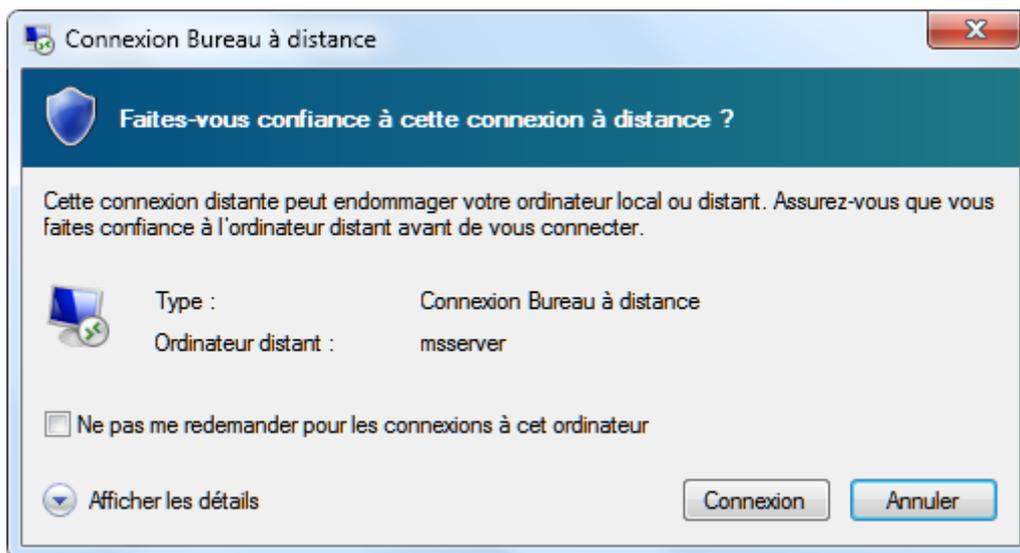


Figure 7: Lancement du client « Remote Desktop » sous Windows 7

Cette fenêtre permet de spécifier des options avancées en cliquant sur « Afficher les détails » :

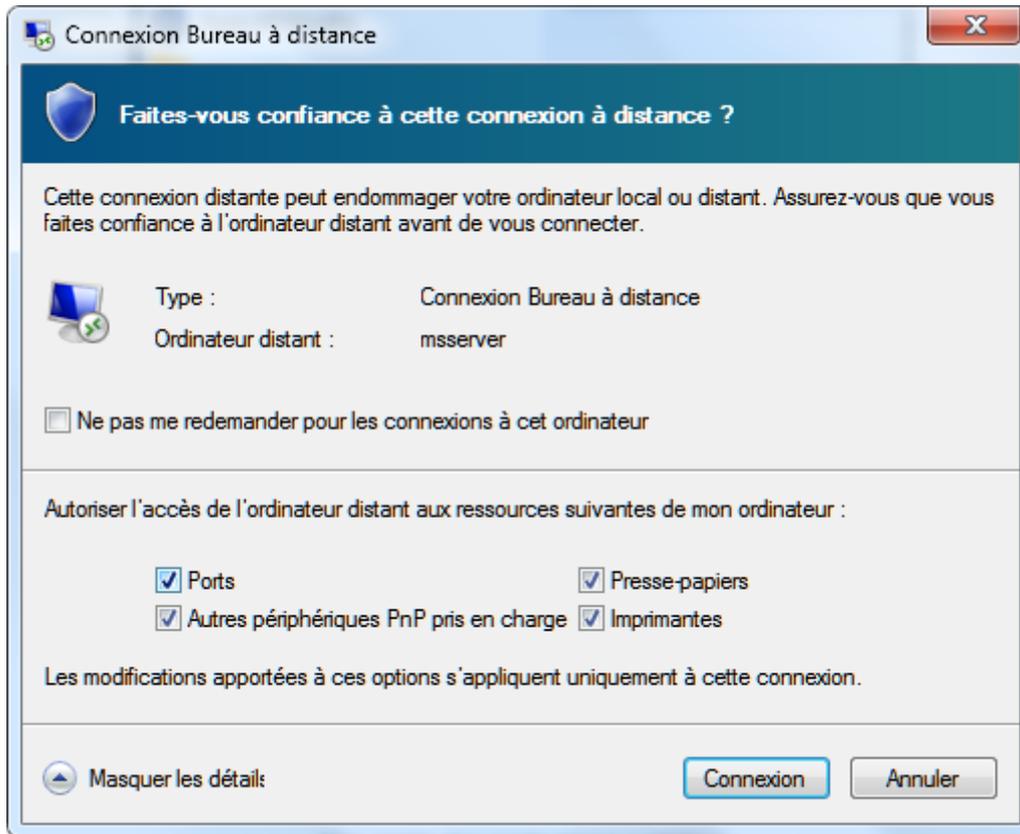


Figure 8: Partage des ressources locales du poste client

Cette fonctionnalité est importante puisqu'elle permet de partager, entre le poste client et le serveur, les lecteurs cartes connectés localement au poste de travail.

L'utilisateur a alors accès à un environnement Windows dont la composition lui est assignée par l'administrateur :

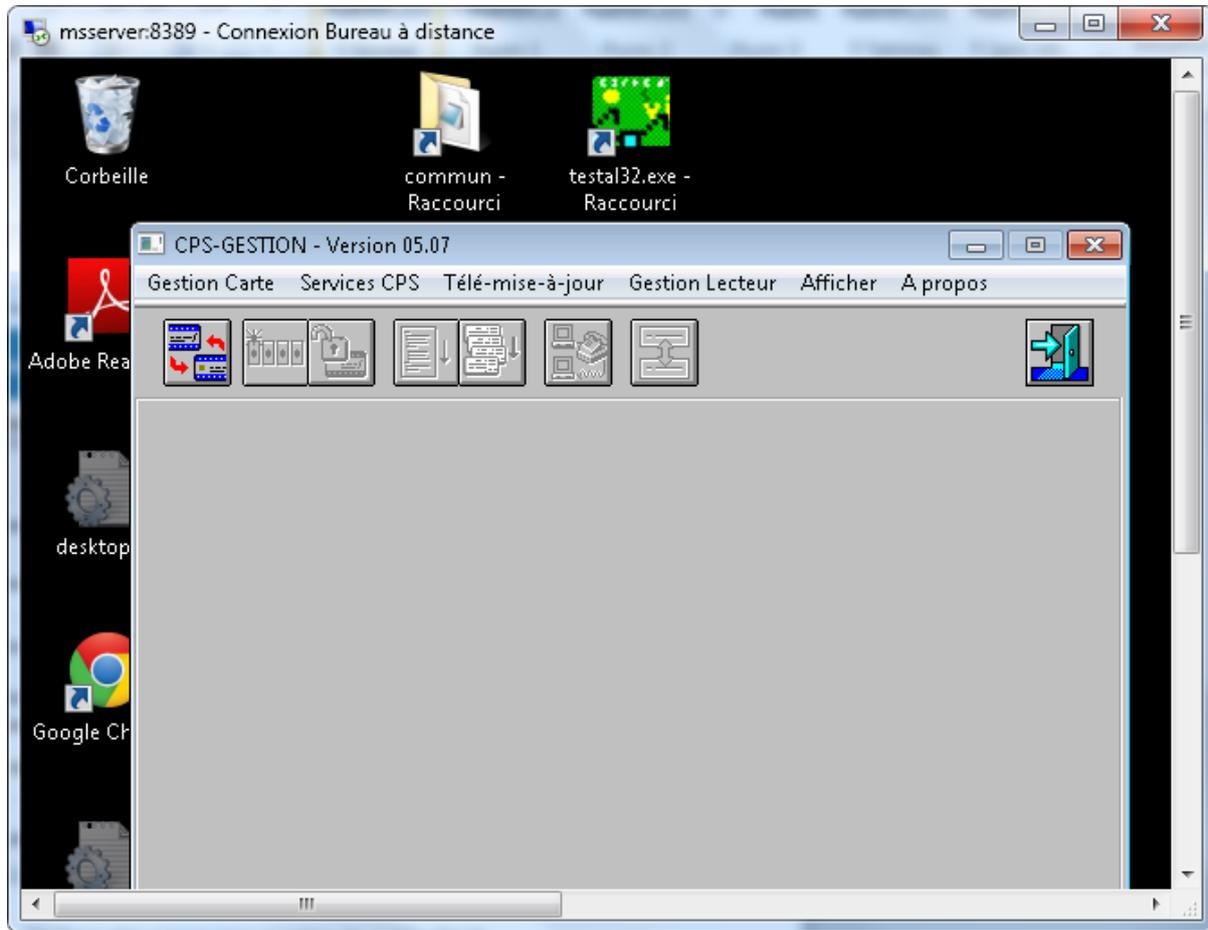


Figure 9: Vue du bureau distant

Le poste du client n'a qu'une fonction d'affichage : toutes les applications lancées par l'utilisateur sont exécutées par le serveur.

Plusieurs utilisateurs peuvent être connectés simultanément sur le serveur.

Dans la barre de tâches du poste client, la symbolique suivante est retenue pour signifier l'exécution d'une session distante :



Figure 10: Symbolique dans la barre de tâches

Une double flèche verte signale une exécution distante. Au centre, l'application Outlook est exécutée localement, à droite, une session distante est en cours d'exécution.

Il s'agit à priori du scénario d'utilisation le plus fréquent de TSE en établissement. Dans ce cas, les établissements utilisent un seul lecteur PC/SC.

5.1.2.2 Client Remote Desktop Applicatif [W2008+, RDP 6.1]

Ce mode permet à l'utilisateur de lancer une application sans passer par un bureau Windows distant avant.

L'utilisateur dispose par exemple sur son bureau de raccourcis vers l'application distante (positionnés par un administrateur système par exemple), qui se lance directement:



Figure 11: Exemples de liens directs vers des applications distantes

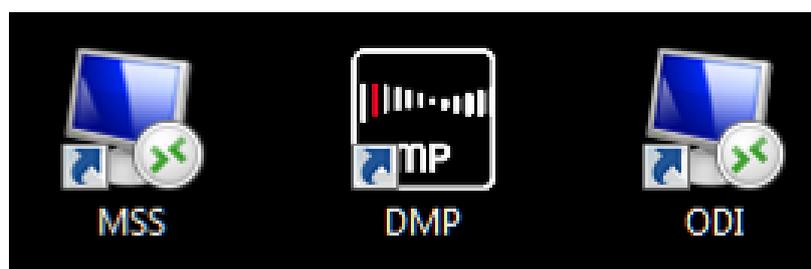


Figure 12: Exemples de liens directs personnalisés vers des applications distantes

Ce mode est particulièrement utile pour concevoir des postes de travail verrouillés et durcis, adressant un environnement sécuritaire contraint.

Dans le cas présent, le fait de cliquer sur « **DMP** » lance un navigateur sur le serveur sur la page du DMP. Le navigateur affiche après lectures CPS et Vitale:



Figure 13: Instance virtualisée de Internet Explorer 10 ouverte directement sur le DMP

Ce mode est présent depuis longtemps chez Citrix (.ica au lieu de .rdp).

Les .rdp peuvent être signés (cf. rdpsign), ce qui permet de sécuriser les déploiements (lutte contre le « spoofing » en particulier).

Du point de vue de l'utilisateur, aucune différence notable n'est perceptible entre une application exécutée localement et cette même application consommée à distance:



Figure 14: Similitude du rendu application locale / application distante

A gauche : Instance de Firefox virtualisée, à droite : instance locale de Firefox. Aucune différence notable.



Figure 15: Symbolique dans la barre de tâches

A gauche : Instance virtualisée, à droite : instance locale. Une double flèche verte signale une exécution distante.

5.1.2.3 Client Remote Desktop Accès Web TS [W2008+]

La liste des applications disponibles pour un utilisateur donné est accessible depuis un simple navigateur. L'utilisateur lance Internet Explorer sur le serveur TSE depuis son poste client léger et s'authentifie. Le serveur lui renvoie une liste d'applications disponibles.

La sélection d'une application ramène l'utilisateur dans le scénario décrit dans le paragraphe précédent (4.1.2.2- Client Remote Desktop Applicatif) :

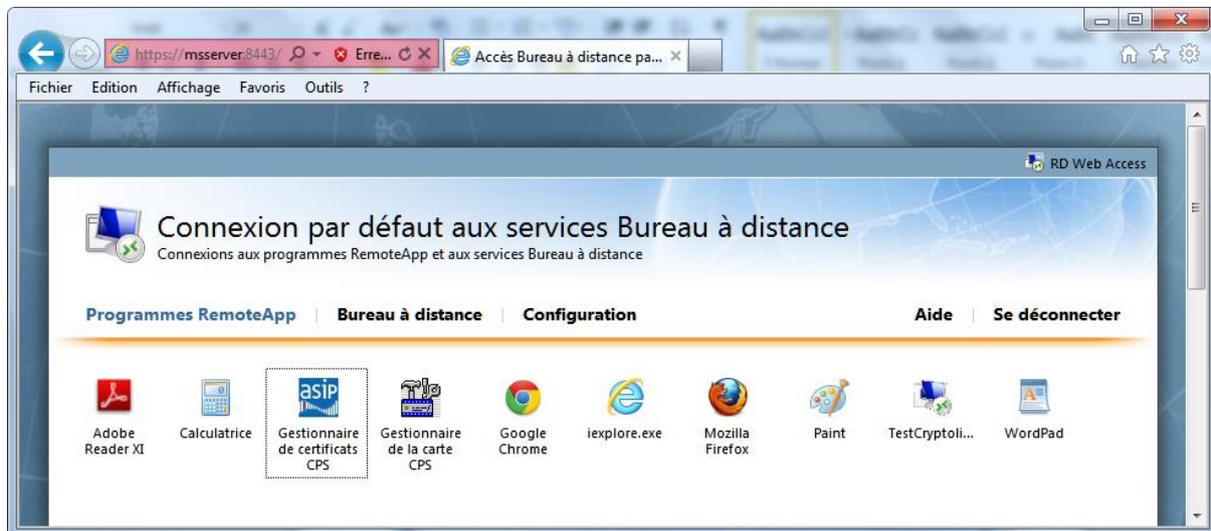


Figure 16: Interface RD Web Access du Pack établissement GALSS

La figure ci-dessus montre une vue, en pack établissement GALSS, de l'interface RD Web Access avec CCM.exe (« Gestionnaire de certificats CPS »), Gestionnaire de la cartes CPS (CPS Gestion), Internet Explorer, Firefox et Chrome déployés.

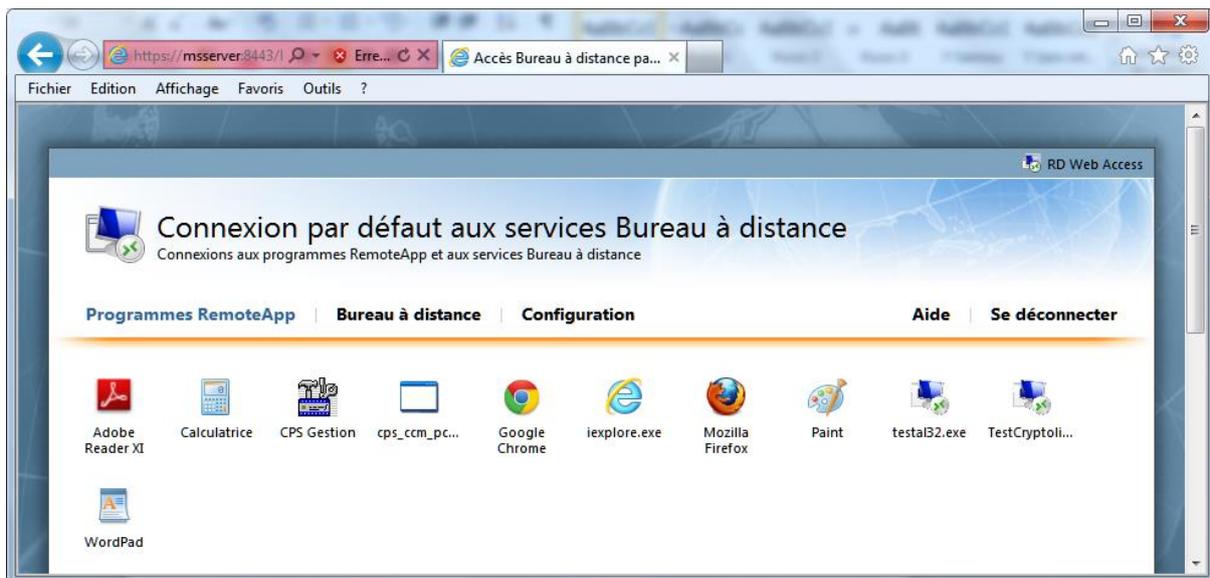


Figure 17 Interface RD Web Access du Pack établissement Full PC/SC (en test)

La figure ci-dessus montre une vue, en pack établissement Full PC/SC (en test), de l'interface RD Web Access avec cps_ccm_pcsc.exe, CPS Gestion, Internet Explorer, Firefox et Chrome déployés.

[12] est un bon point d'entrée pour les administrateurs Microsoft désireux de commencer avec RDP/TSE.

5.2 Une architecture "client-serveur"

Les notions de « client », « serveur » et de « sessions » ont déjà été évoqués dans la présentation précédente.

TSE s'appuie donc sur une architecture client/serveur illustrée ci-dessous :

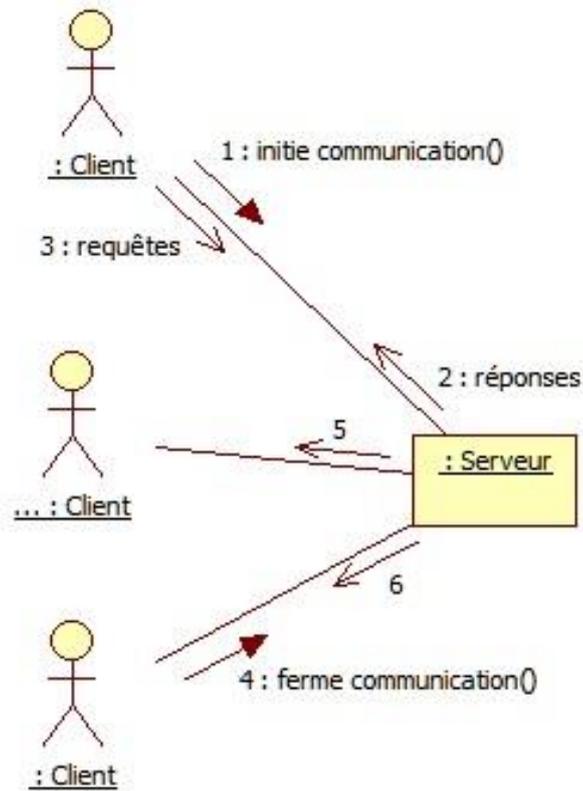


Figure 18: Diagramme réseau associé au mode client serveur

Id	Remarque	Explication
	Plusieurs clients pour un serveur	Plusieurs postes client peuvent s'adresser à un unique serveur, qui leur offre un service commun.
1	Une communication à l'initiative du client	Généralement, la communication est établie à l'initiative du client, qui se signale auprès du serveur. Le serveur réserve des ressources pour traiter cette nouvelle communication (session).
3	Les clients requêtent	Les clients adressent des requêtes au serveur en utilisant un protocole de communication préétabli. Dans le cas de TSE, le protocole mis en œuvre est RDP. Dans le cas de Citrix, il s'agit de ICA.
2, 5, 6	Le serveur répond	Le serveur examine la requête, compose une réponse et la retourne au client.
4	Fin de communication et libération des ressources	Le client signale au serveur qu'il a fini. Le serveur libère les ressources qu'il avait allouées pour répondre à ce client.
1, 3, 4	Des clients « concurrents »	Sur le schéma ci-dessus, un client ouvre une session pendant qu'un autre communique activement et qu'un troisième termine sa session. Les communications entre clients et serveur peuvent se faire en parallèle. Le serveur assure les isolations fonctionnelle et sécuritaire entre les sessions.

Tableau 3 : Diagramme de collaboration client-serveur

5.3 Une architecture "client léger"

Dans le cas de TSE/Citrix, le poste de travail client est dit « léger » :

- il ne contient aucune intelligence
- Il apporte des périphériques (typiquement un lecteur de cartes, une imprimante...)
- Il apporte des moyens d'interaction (clavier, souris)
- Il apporte une capacité d'affichage (écran)
- Il apporte une capacité protocolaire
 - Mise en œuvre d'un client RDP dans le cas de TSE
 - Mise en œuvre d'un client ICA dans le cas de Citrix
 - Afin de pouvoir échanger avec le serveur

L'ensemble des processus sont exécutés par le serveur.

Le stockage de données est généralement réalisé sur des disques distants gérés par le serveur et dont les accès et la redondance sont protégés par les administrateurs réseaux.

5.4 Points forts

Id	Remarque	Explication
CL_AV_01	centralisation des ressources	La gestion des données et des traitements est centralisée, ce qui simplifie les contrôles de sécurité, l'administration, la mise à jour des données et des logiciels. Les problèmes de redondance et de contradiction sont évités. Les ressources partagées, matérielles et logicielles, sont gérées en cohérence, laissant apparaître aux utilisateurs un ensemble homogène.
CL_AV_02	performance / mise à l'échelle	Les technologies employées sont généralement très performantes (taux de disponibilité, matériels haut de gamme...) et permettent une mise à l'échelle dite "verticale" (augmentation des tailles disques, RAM, du nombre de processeurs...). Des suppressions ou ajouts de poste clients voire de serveurs (mise à l'échelle dite " horizontale ") sont possibles sans impact majeur.
CL_AV_03	sécurité	Par rapport à un système complètement distribué, le nombre de points d'entrée permettant l'accès aux données est moins important. Les points d'attention, à protéger, sauvegarder, redonder, ... sont moins nombreux.
CL_AV_04	administration dédiée	les postes clients, transformés en terminaux simples, généralement très nombreux quelle que soit l'architecture, n'ont pas ou peu besoin d'être administrés. La maintenance matérielle sur ces postes est restreinte.

Tableau 4 : Client léger : Avantages

5.5 Points d'attention

Id	Remarque	Explication
CL_AT_01	coût	Les coûts de mise en place et de maintenance peuvent être élevés.
CL_AT_02	disponibilité / tolérance aux pannes	En cas d'indisponibilité du serveur, aucun client n'est fonctionnel. Des systèmes rendant le serveur tolérant aux pannes doivent être mis en place suivant la criticité déterminée des services hébergés (actif/actif, actif/passif, failover, loadbalancing..., voir "performance / mise à l'échelle")
CL_AT_03	dimensionnement	Des études de dimensionnements précises doivent être menées: <ul style="list-style-type: none">• Le surdimensionnement implique des surcoûts• Le sous-dimensionnement implique des pertes fonctionnelles

Tableau 5 : Client Léger : Points d'attention

5.6 Citrix

Cf. Aperçus d'écran en annexe.

5.6.1 Serveur Citrix XenApp 6.0 sous W2008R2 SP1

Les produits Citrix généralement utilisés en établissement pour sous-tendre les architectures d'applications virtualisées sont les applications « XenApp » (6.0 et 6.5, anciennement MetaFrame).

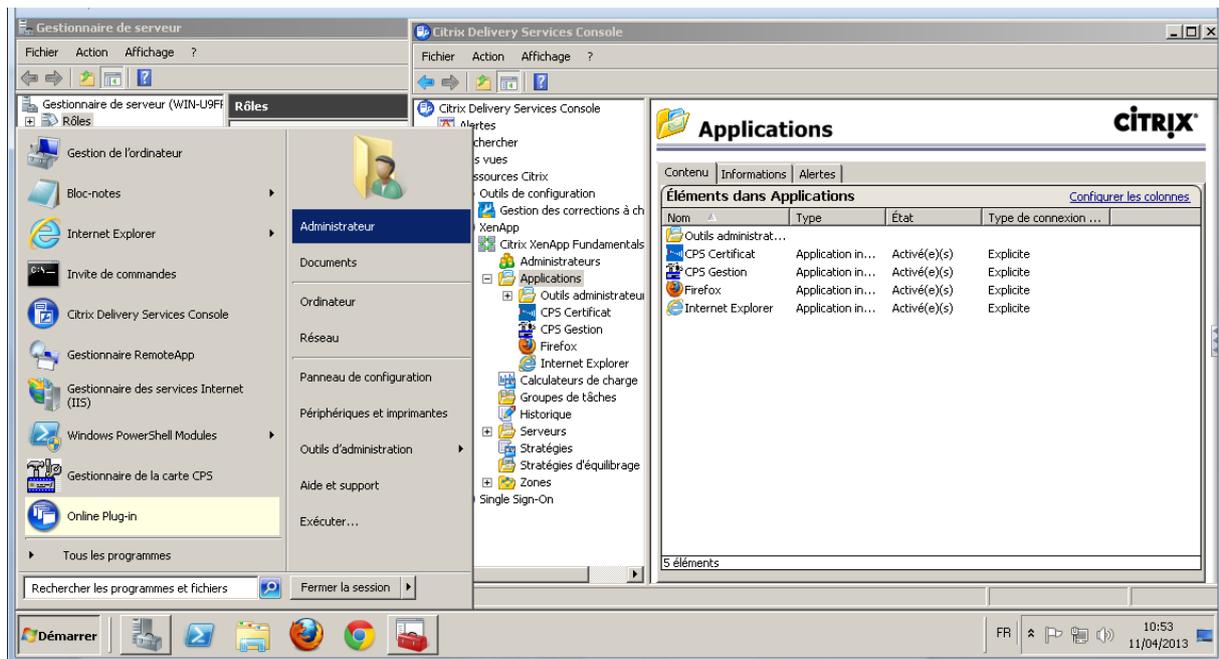


Figure 19: Aperçu de la console d'administration Citrix XenApp 6.0 sous Windows 2008R2 SP1

5.6.2 Points forts de la surcouche Citrix

L'utilisation des produits Citrix a un impact en termes de coûts (licence). Cette utilisation peut toutefois s'imposer.

Apports Citrix
Simplicité
Ergonomie et qualité des Outils d'administration
Gestion et équilibrage de la charge
Ecosystème
Protocole ICA performant en WAN
Optimisation de la gestion des profils itinérants (cf. [14])
« Receiver » disponible pour de nombreuses plateformes (a contrario, des clients RDP existent pour des plate-formes autres que Microsoft mais leurs implémentations sont de qualités diverses)

Tableau 6 : Citrix : points forts

5.6.3 Points d'attention de la surcouche Citrix

Points d'attention Citrix
<p>Doublons de fonctionnalités ? : certaines fonctionnalités des versions 6.0 et 6.5 de Citrix ont été reportées de fonctionnalités au sein même de Windows Server 2012.</p> <p>Synchronisation des versions avec les sorties des nouveaux produits Microsoft ? : Citrix XenApp n'est disponible pour Windows Server 2012 que depuis avril 2014 avec la version 7.5. La version XenApp 7.6 devrait sortir en octobre 2014.</p> <p>Il est nécessaire de prendre en compte la politique de support de Citrix sur ses produits, en sus du même travail sur les produits Microsoft.</p>

Tableau 7 : Citrix : points d'attention

5.7 Smartcard logon

Depuis Windows 2000, il est possible d'ouvrir une session Windows en utilisant une carte à puce.

La carte CPS et la Cryptolib CPS sont conçues pour supporter ce mécanisme qui permet une authentification dite « forte » du porteur (2 facteurs présentés : « ce que j'ai » i.e. la carte CPS, « ce que je sais » i.e. le code porte de la carte CPS).

La mise en œuvre du Smartcard logon permet d'implémenter un système d'accès particulièrement ergonomique (insertion de la carte dans le lecteur, introduction d'un code PIN, ouverture de la session. Ou au contraire, arrachage de la carte et fermeture de la session).

TSE/Citrix est compatible avec les mécanismes de Smartcard logon.

La mise en œuvre du Smartcard logon est décrite dans **[15] Guide de mise en œuvre d'un Smartcard logon avec une carte CPS.**

5.8 Profils itinérants

La gestion des profils utilisateur « itinérants » (« profils itinérant ») offerte par les systèmes Microsoft offrent une solution intéressante aux administrateurs système et réseaux désireux d'adresser les scénarios de mobilité basés sur le déplacement des personnels dans l'enceinte d'établissement.

Cette gestion est décrite dans **[14] Guide de mise en œuvre des profils itinérants.**

TSE/Citrix supporte ce mode, Citrix apportant quelques fonctionnalités supplémentaires potentiellement intéressantes (gestion plus fine des règles de synchronisation des fichiers des profils via un système de règles avancé).

5.9 Considérations techniques

5.9.1 Impacts sur la conception applicative

L'aspect concurrentiel lié à l'exécution en mode TSE/Citrix doit être impérativement pris en compte dès la conception de l'application.

Microsoft propose une boîte à outils de tests de compatibilité (Microsoft ACT) [11].

Afin de passer avec succès ce type de tests, **et avant de se reposer sur des fonctionnalités avancées et souvent payantes et chères des produits sur étagère**, il est nécessaire de mettre en place des règles de conception adaptées.

La littérature sur le sujet est pléthorique et souvent de sens commun.

Exemple : le fichier de configuration d'un programme doit être répliqué si cette configuration est propre à un utilisateur dans :

- %USERPROFILE%\AppData\Local\<Manufacturer>\<Product>\<Product Version>

[9] rappelle les règles essentielles aux développements pour Citrix. Ce document est « orienté » dans la mesure où il est adapté aux fonctionnalités avancées que propose Citrix pour pallier à un certain nombre de problèmes de conception.

A minima, les ressources du poste de travail ASIP Santé qui font l'objet de travaux pour adresser les problématiques d'accès concurrents sont :

Ressource Poste de travail ASIP Santé
%USERPROFILE%\WINDOWS\GALSS.ini
%USERPROFILE%\WINDOWS\cpgesw32.INI
%ALLUSERSPROFILE%\Application Data\santesocial\cps\coffre\cps_pkcs11_safe.ini
%ALLUSERSPROFILE%\Application Data\santesocial\cps\coffre\[NOM_MACHINE_CLIENTE]_lecteurs_pcsc.cfg
%ALLUSERSPROFILE%\Application Data\santesocial\cps\coffre\Ccert.bin
%USERPROFILE%\Application Data\santesocial\DMP1\api_lec.ini
%USERPROFILE%\Application Data\santesocial\DMP1\sedica.ini
mozilla.cfg
tablebin.lec
pdt-cdc-011.csv
asipsante.properties

Le choix de %ALLUSERPROFILE% pour ccert.bin en particulier était à revoir, ce qui a été fait avec la Cryptolib CPS v5.

5.9.2 Fonctionnalités avancées

5.9.2.1 Fonctions liées à la concurrence et l'isolation

[9] montre par exemple que les versions récentes de Citrix XenApp répondent à la problématique de la virtualisation des applications « single-users » :

- When an application was not developed based on **Terminal Services compatibility**, it was difficult to publish with XenApp. Now, if an application based on single-user access only has user registry settings stored in HKLM\Software or user-specific files stored in C:\Program Files or C:\Windows, application virtualization and streaming can address these issues by installing into an isolation environment, as shown below:

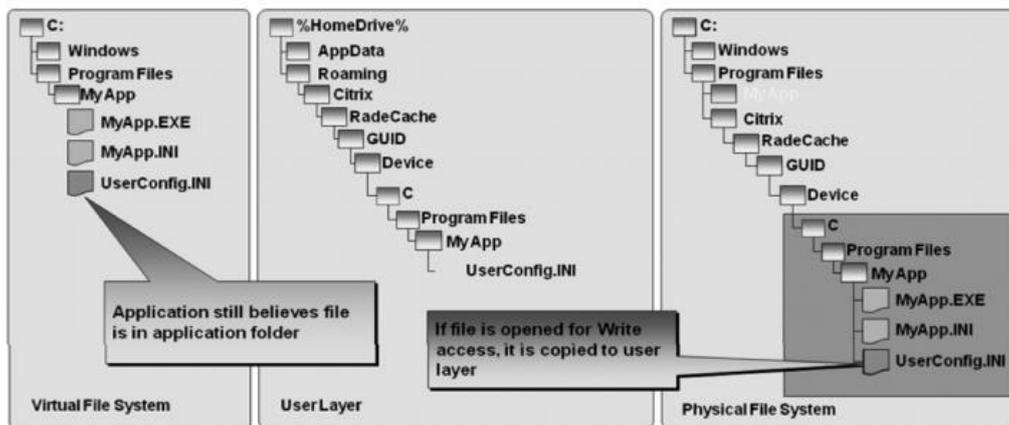


Figure 20: Virtualisation d'une application single-user sous Citrix XenApp

Voir aussi l'UAC / VirtualStore des noyaux Vista+ pour l'isolation à l'exécution :

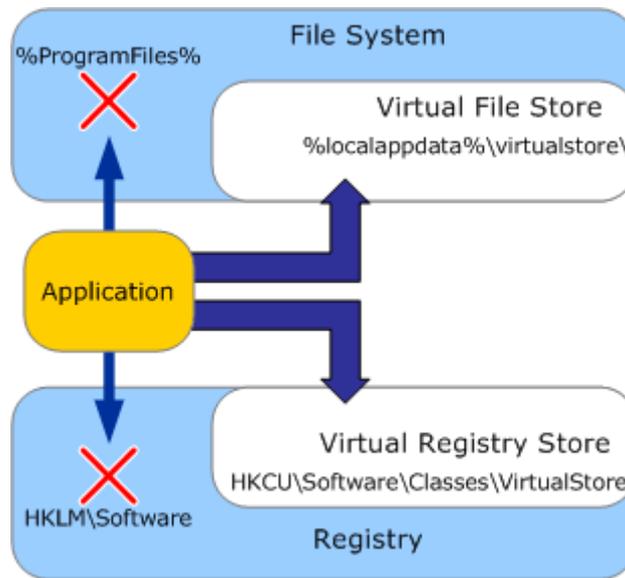


Figure 21: Virtualisation d'une application single-user avec les noyaux Windows Vista+

Autre exemple : [10] montre comment changer le comportement des APIs Windows pour une application virtualisée particulière (changement de comportement de GetWindowsDir – problème en GALSS 3.26, cf. corrections du GALSS 3.27 ou GetComputerName par exemple).

5.9.2.2 Caches et optimisations de bande passante

La phase de mise en production d'applications basées sur ce type d'architecture doit être précédée

- d'une phase de pré-dimensionnement
- d'une phase de mise au point de ce type de paramètres (« tuning »)
 - pour chacun des sous-composants : réseau, OS, surcouche, applications.

Un paramétrage pertinent doit être identifié :

- Besoin de profondeur d'images en 32bit ? 16bit est-il acceptable ?
- Besoin de partager les disques dur des postes clients ?
- Besoin de mapper la carte son ?
- ...

Exemple : afin d'optimiser le volume des flux d'images :

Paramètre	Valeur
Paramètre RDP	"bitmapcachesize:i:1500"
Paramètre ICA	PersistentCacheEnabled=on

Tableau 8 : Paramètres d'optimisation des flux d'images pour RD et ICA

La littérature est exhaustive sur le sujet. Se distinguent particulièrement :

ID	Référence
OPTIM_01	http://www.norskale.com/articles/article/windows-2008-r2-remote-desktop-and-xenapp-6-tuning-tips-update
OPTIM_02	http://support.citrix.com/servlet/KbServlet/download/2131-102-671534/wWAN_Optimization_WP_3.pdf
OPTIM_03	http://rdpdesk.com/documentation/parameters-for-ica/

Tableau 9 : Références de guides d'optimisation pour RDP / ICA

5.9.3 Sécurisation des liens RDP/ICA

Le lien RDP ou ICA sont sécurisables. Cette partie sera documentée par ailleurs.

6 Les projets ASIP Santé concernés par TSE/Citrix

6.1 Rappels d'architecture carte CPx / carte Vitale

6.1.1 Exemple : Architecture GALSS pour l'application AW PS DMP

Le schéma illustre le cas particulier de l'accès Web PS DMP qui utilise l'API de lecture Vitale (L'API de lecture n'est pas indispensable en général). Les composants logiciels qui doivent être installés en filière GALSS afin que les services soient accessibles sont :

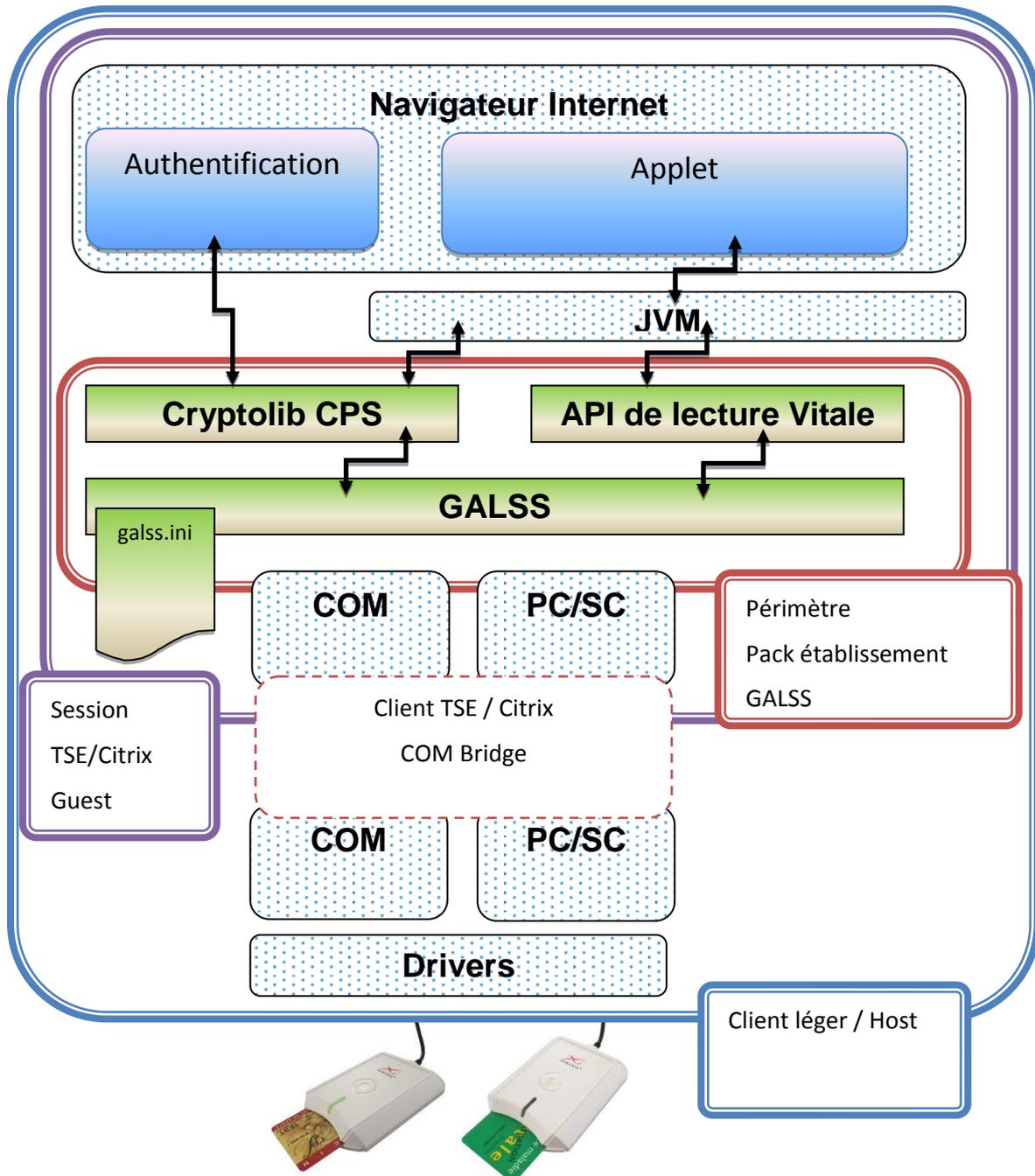


Figure 22: Installation d'un poste de travail en filière GALSS

6.1.2 Exemple : Architecture PC/SC pour l'application AW PS DMP

Le schéma illustre le cas particulier de l'accès Web PS DMP qui utilise l'API de lecture Vitale (L'API de lecture n'est pas indispensable en général). Les composants logiciels qui doivent être installés en filière Full PC/SC afin que les services soient accessibles sont:

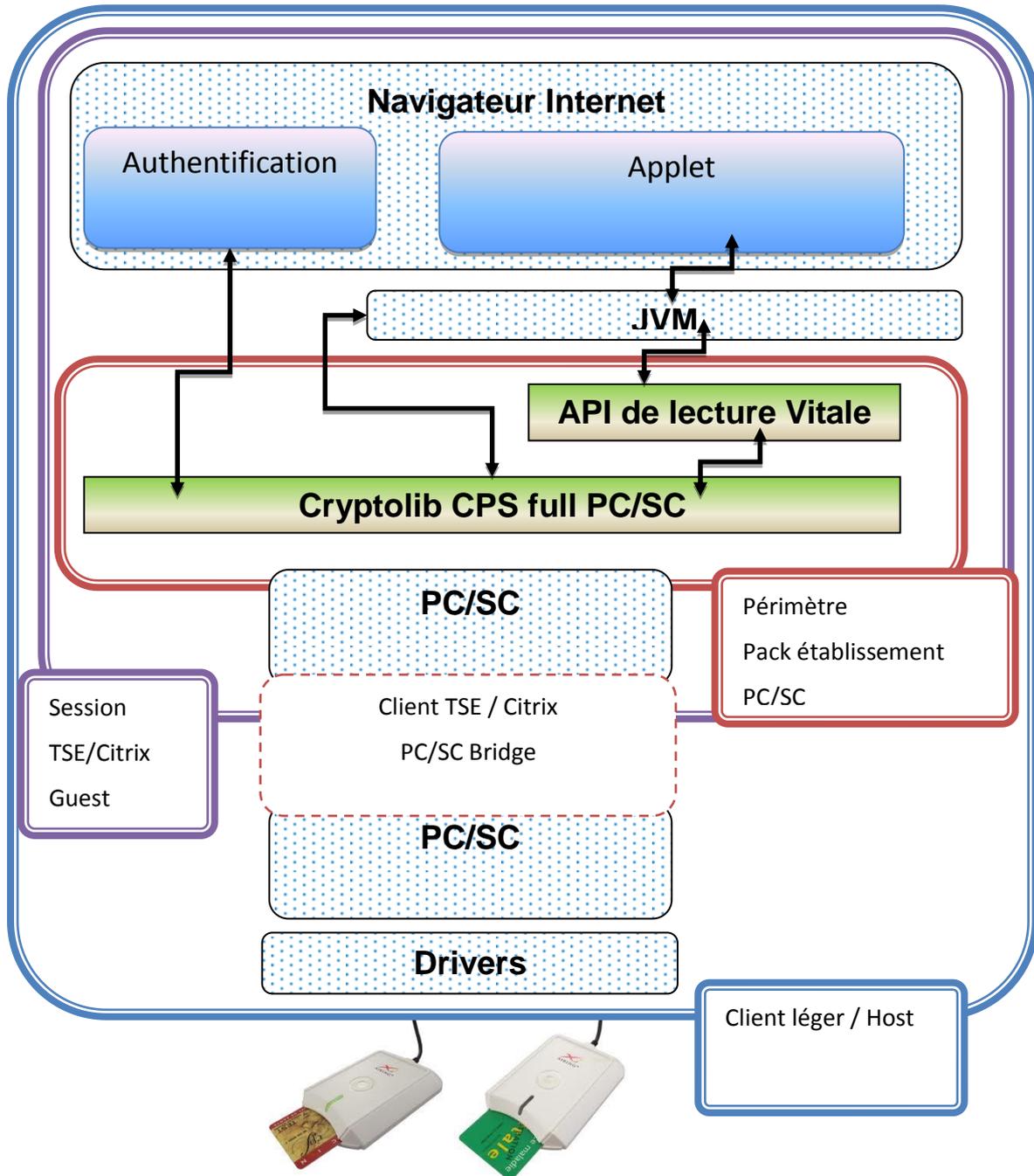


Figure 23: Installation d'un poste de travail en filière Full PC/SC

6.2 Liste des projets

Les projets suivants sont concernés par le Pack Etablissement :

Projet	Version	Volet TSE / Citrix
AW PS DMP	1.2.0	Oui
MSSanté	1.3	Oui
RASS	1.0	Oui
Smartcard logon CPS	2.5.3	Oui

Tableau 10 : Liste des projets ASIP Santé concernés par TSE/Citrix

7 Le pack établissement

7.1 Fiche de synthèse

La fiche de synthèse du pack établissement est la suivante:

Propriété	Valeur
Cible	Professionnels
Dernière version	1.4
Media de diffusion	http://integrateurs-cps.asipsante.fr/
Nombre de livrables	1
Politique de release	Cf. http://integrateurs-cps.asipsante.fr/
Roadmaps	Cf. http://integrateurs-cps.asipsante.fr/
Fréquence	1 par an (indicatif, Cf. http://integrateurs-cps.asipsante.fr/)

Tableau 11 : Pack Etablissement : Fiche de synthèse

7.2 Contenu du Pack Etablissement

Le pack établissement GALSS TSE permet l'installation de la Cryptolib CPS, le déploiement de postes client sous Windows et la virtualisation des applications accédant aux cartes CPx/Vitale suivantes:

- Internet Explorer
- Firefox
- Google Chrome
- Outils de tests du GIE SESAM-Vitale et de l'ASIP Santé

Une attention particulière est portée sur:

- L'accès à Testssl
- L'accès à l'AW PS DMP

Le pack établissement en filière GALSS contient les éléments suivants:

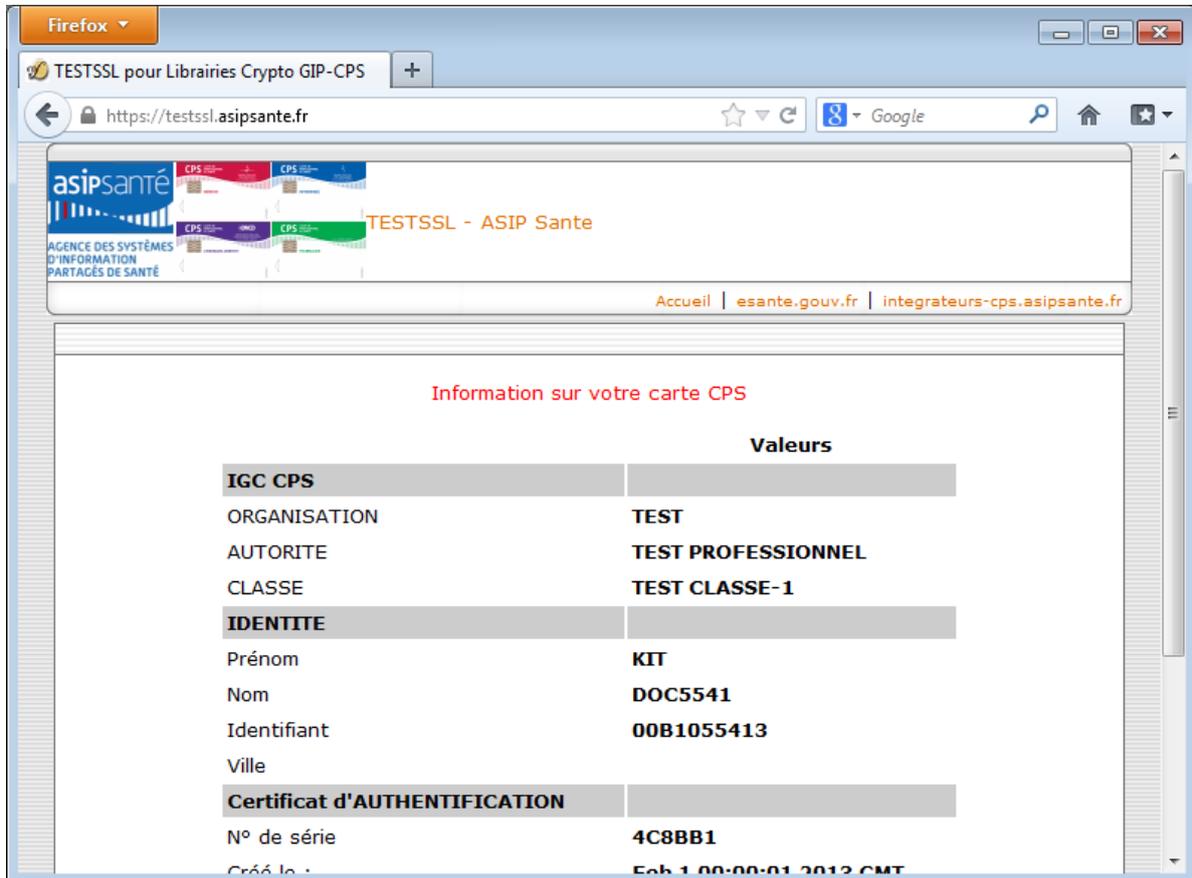
Composant	Version
Package établissement GALSS	1.4
GALSS	3.36.01
Cryptolib CPS GALSS	4.1.7
API de lecture Vitale	Non fourni depuis le pack 1.4, installée par l'applet AW PS DMP

Tableau 12 : Pack Etablissement Pack GALSS

7.2.1.1 Testssl

Une fois le pack établissement installé, le poste de travail doit pouvoir passer un test « Testssl » avec succès.

Cela garantit le bon accès à la carte CPS en environnement virtualisé (cf. annexe – Tests avec Testssl)



The screenshot shows a Firefox browser window with the address bar displaying <https://testssl.asipsante.fr>. The page content includes the ASIP Santé logo and navigation links. The main section is titled 'Information sur votre carte CPS' and contains a table with the following data:

	Valeurs
IGC CPS	
ORGANISATION	TEST
AUTORITE	TEST PROFESSIONNEL
CLASSE	TEST CLASSE-1
IDENTITE	
Prénom	KIT
Nom	DOC5541
Identifiant	00B1055413
Ville	
Certificat d'AUTHENTIFICATION	
N° de série	4C8BB1
Créé le :	Feb 1 00:00:01 2013 GMT

Figure 24: Page Testssl OK

7.2.1.2 ODI

Une fois le pack établissement installé, le poste de travail doit pouvoir passer un test « ODI » avec succès.

Cela garantit le bon accès à la carte CPS en environnement virtualisé ainsi que la présence de dépendances logicielles requises (Java, Adobe Acrobat Reader, UAC désactivé..., cf. annexe – Tests avec ODI).

7.2.1.3 AW PS DMP

Une fois le pack établissement installé, le poste de travail doit pouvoir se connecter au portail DMP Access Web et passer permettre une lecture de carte Vitale.



Figure 25: Page AW PS DMP OK

8 Annexe – principales GPOs

8.1 Autoriser les ouvertures de sessions à distance

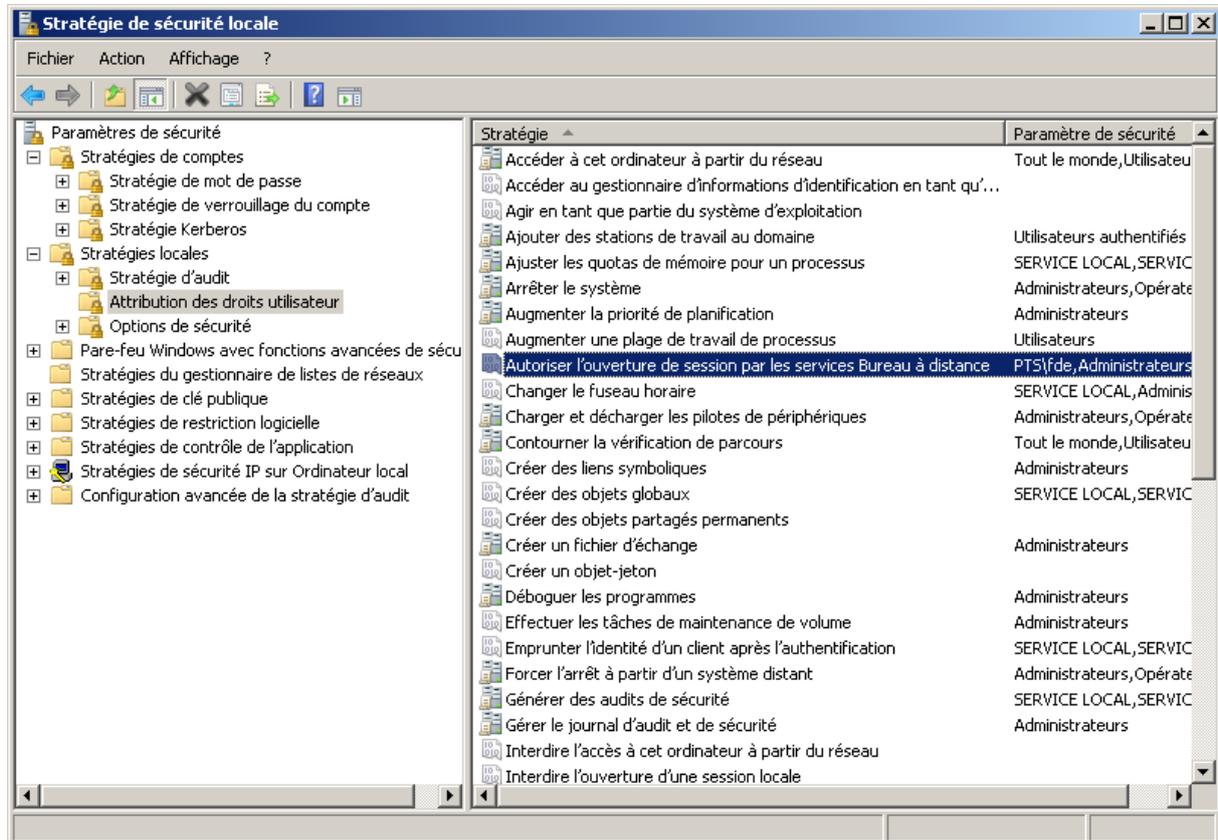


Figure 26 : Stratégie de sécurité locale : Autoriser l'ouverture de session par les services Bureau à distance

8.2 Activer le service Plug-and-Play de la carte à puce

Type	GPO	
Chemin	Computer Configuration / Administrative Templates / Windows Components / Smart Card	
Description	Turn on Smart Card Plug and Play service	
Description	Activer le service Plug-and-Play de la carte à puce	
Détails	<p>Ce paramètre de stratégie permet de contrôler le fonctionnement du service Plug-and-Play de la carte à puce.</p> <p>Si vous activez ou ne configurez pas ce paramètre de stratégie, le service Plug-and-Play de la carte à puce est activé et le système essaiera d'installer un pilote de périphérique pour la carte à puce la première fois qu'une carte sera insérée dans un lecteur de carte à puce.</p> <p>Si vous désactivez ce paramètre de stratégie, le service Plug-and-Play de la carte à puce est désactivé et aucun pilote de périphérique ne sera installé en cas d'insertion d'une carte dans un lecteur de carte à puce.</p> <p>Remarque : ce paramètre de stratégie s'applique uniquement aux cartes à puce conformes au test de qualité WHQL (Windows Hardware Quality Labs).</p>	
Valeurs	Paramètre par défaut	Activé
	Poste lourd	Paramètre par défaut
	Poste léger (VM/TSE/Citrix)	Désactivé
	Session distante TSE/Citrix	Paramètre par défaut
	VM	Paramètre par défaut
	Reboot	Oui

Tableau 13 : GPO : Activer le service Plug-and-Play de la carte à puce

9 Annexe – Citrix

9.1 Installation du client léger et connexion à l'aide du client léger

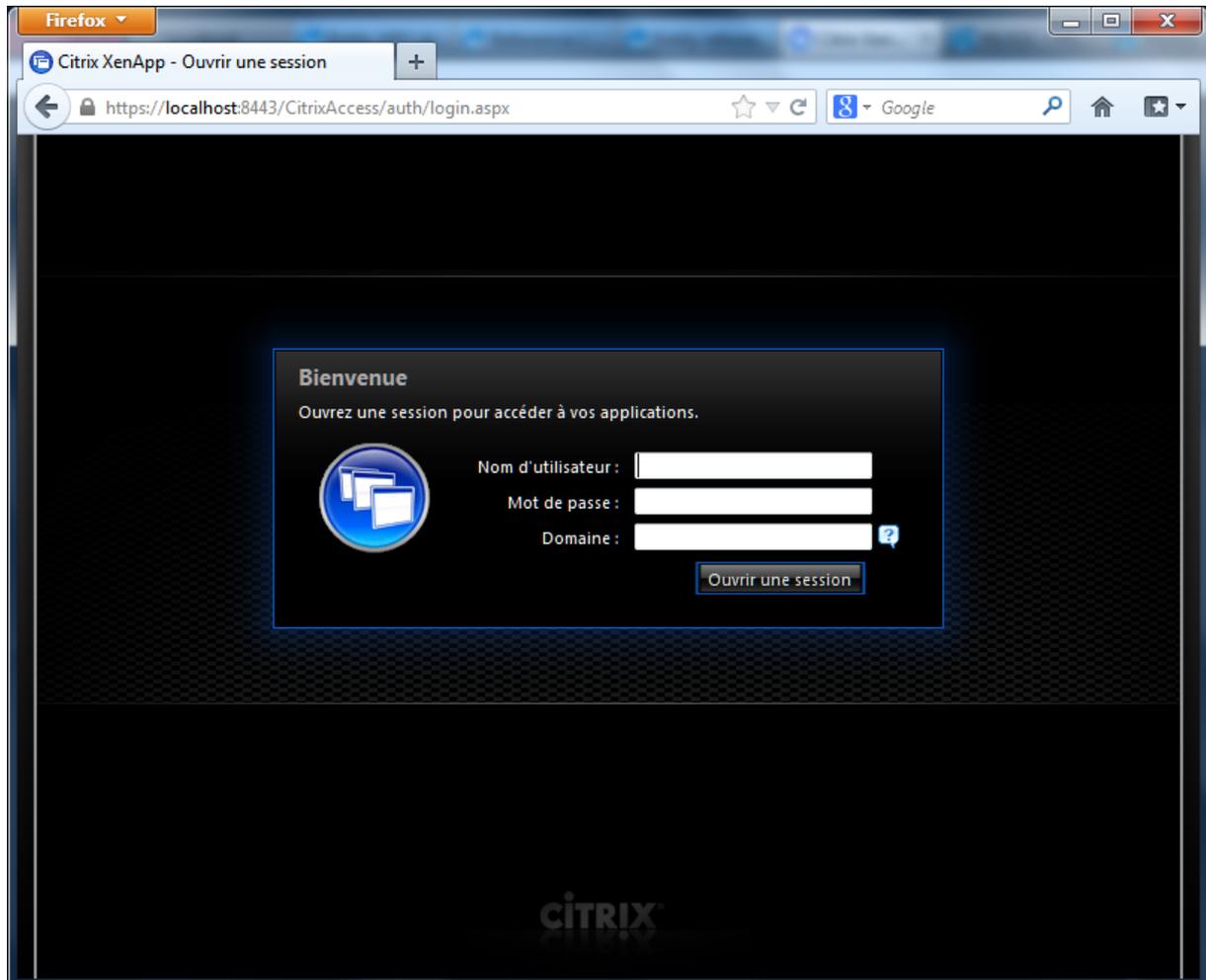


Figure 27: Console d'accès Web Citrix XenApp 6.0

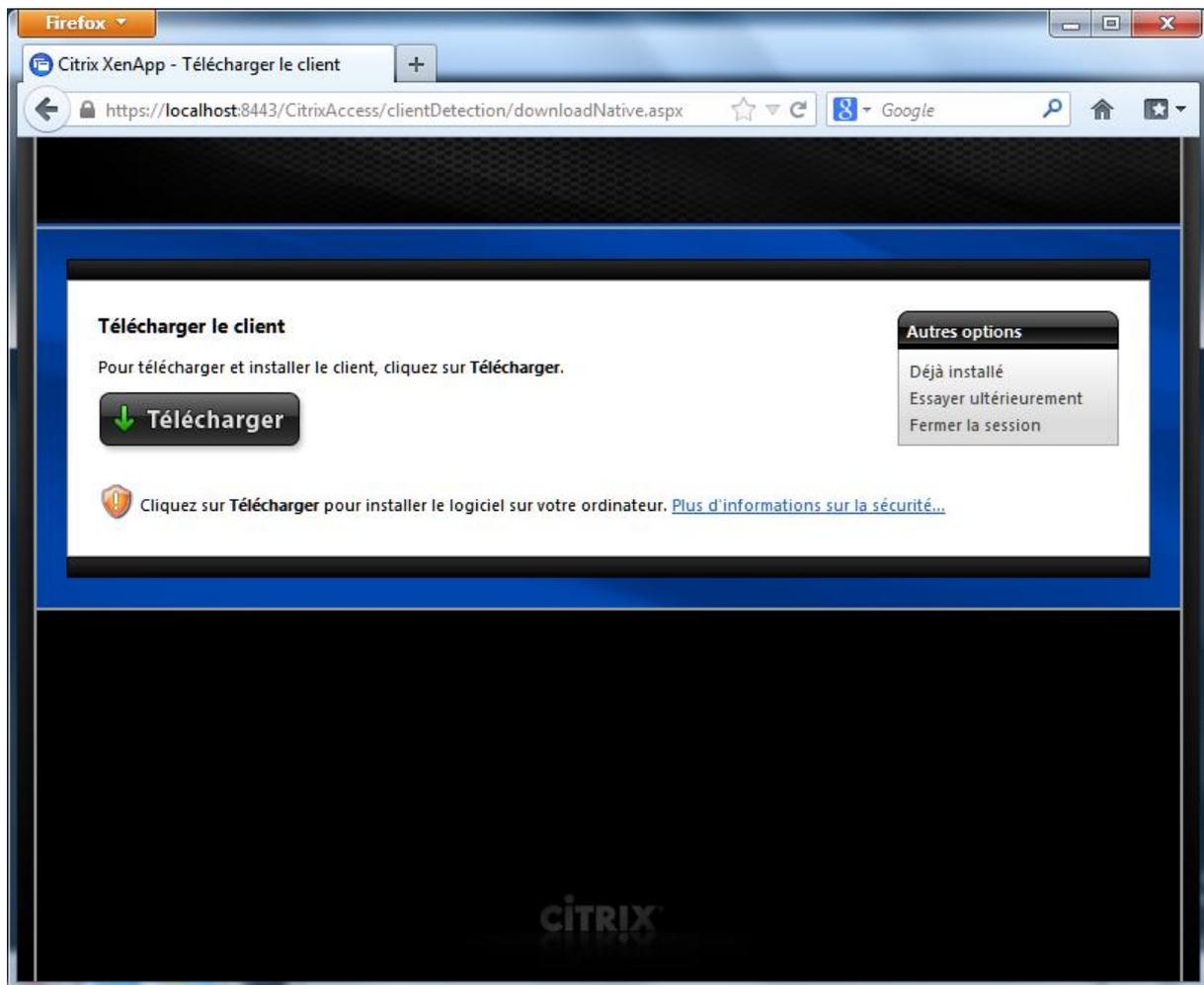


Figure 28: Installation du client Citrix XenApp 6.0

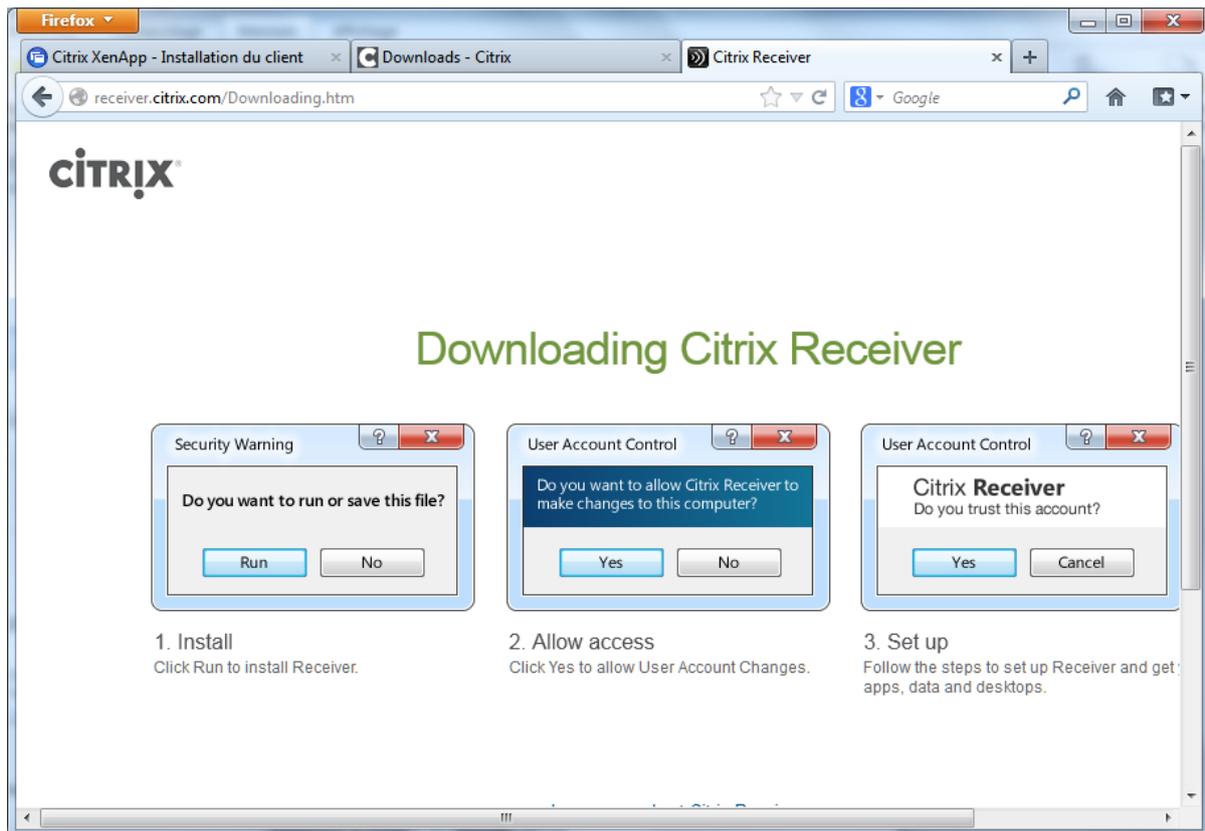


Figure 29: Installation du client Citrix XenApp 6.0

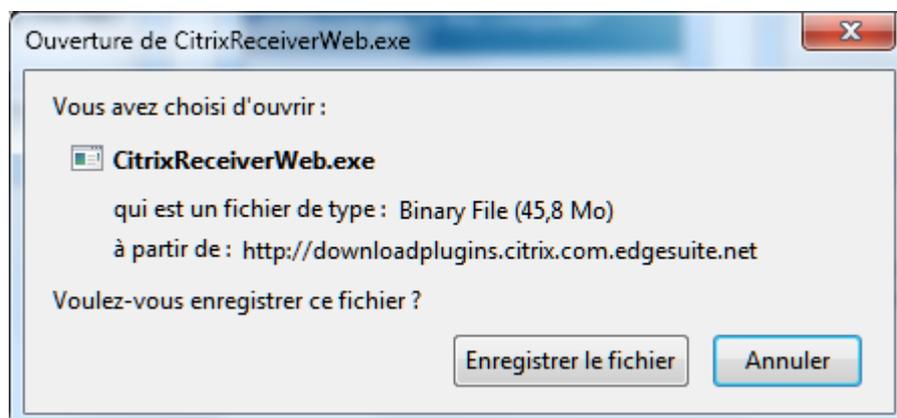


Figure 30: Installation du client Citrix XenApp 6.0

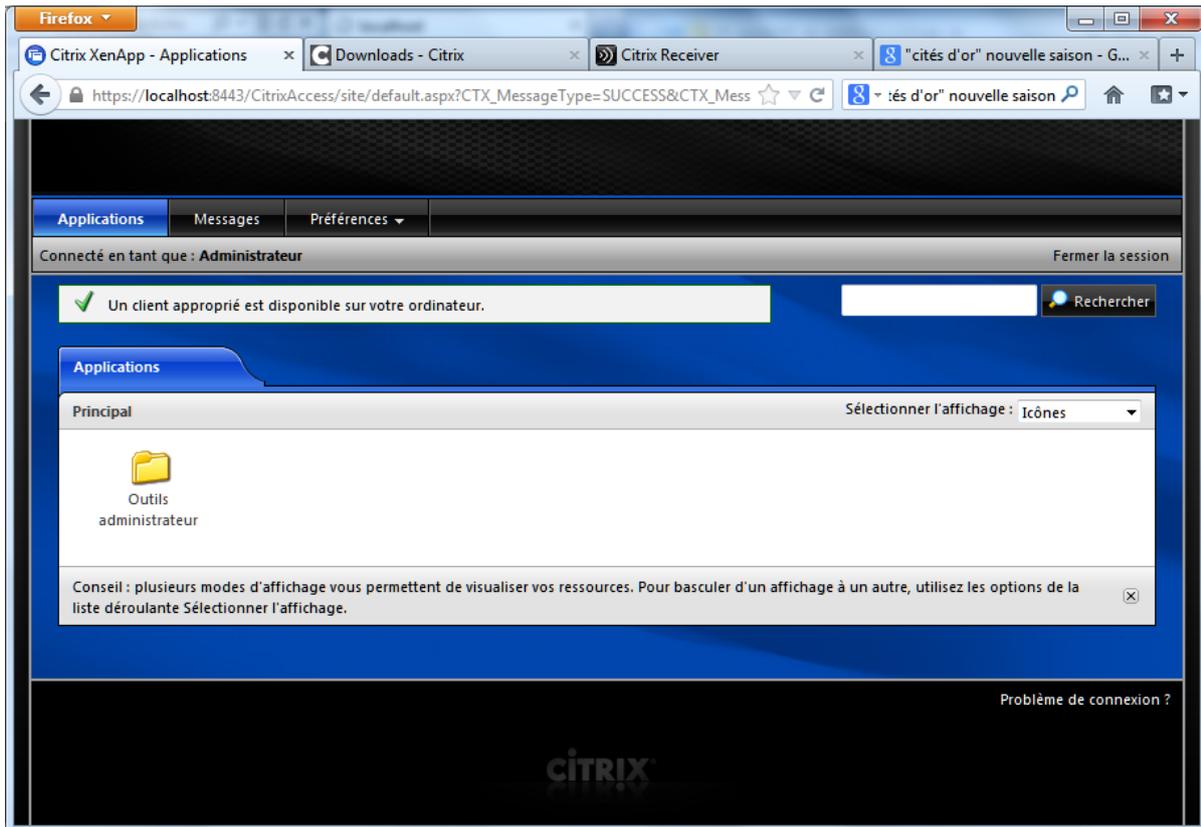


Figure 31: Console d'accès Web Citrix XenApp 6.0

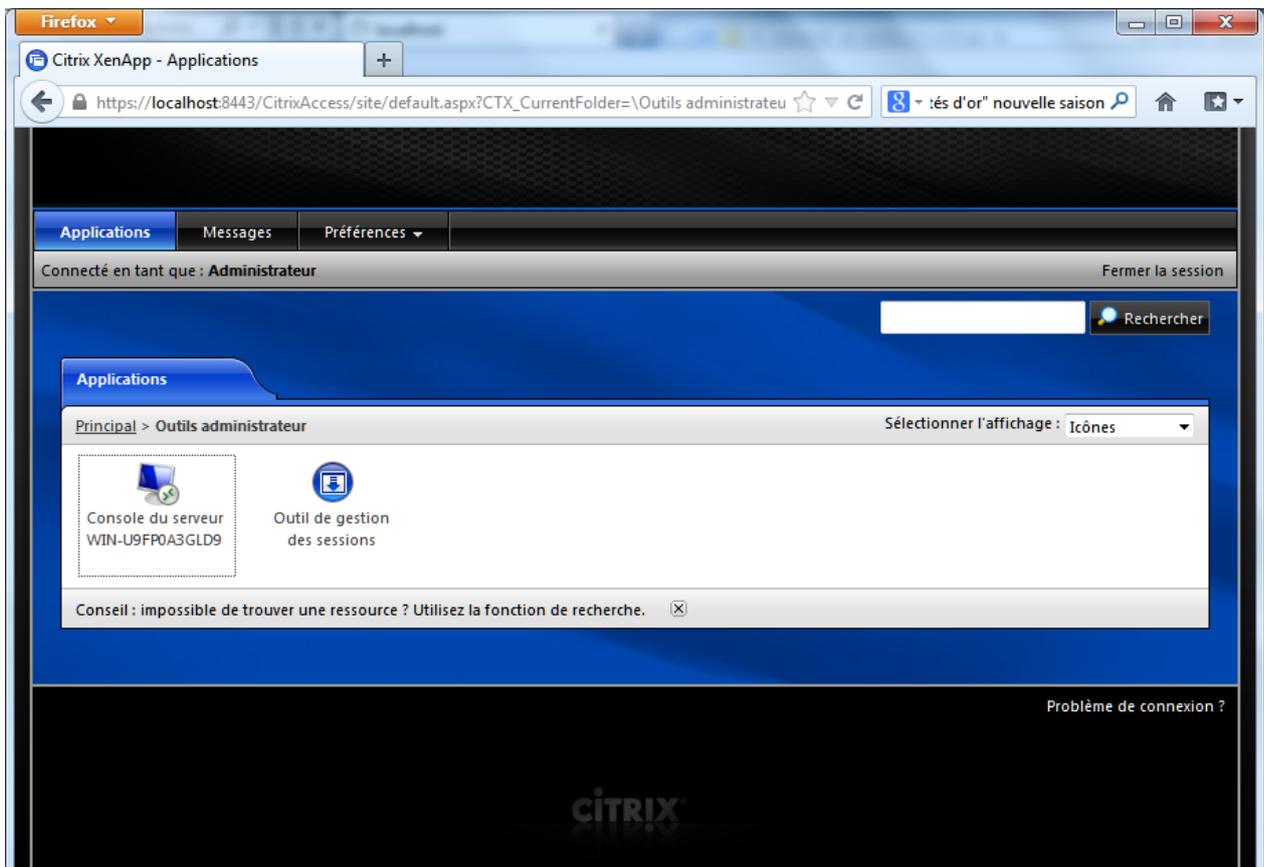


Figure 32: Applications d'administration disponibles par défaut à travers de la console d'accès Web Citrix XenApp 6.0

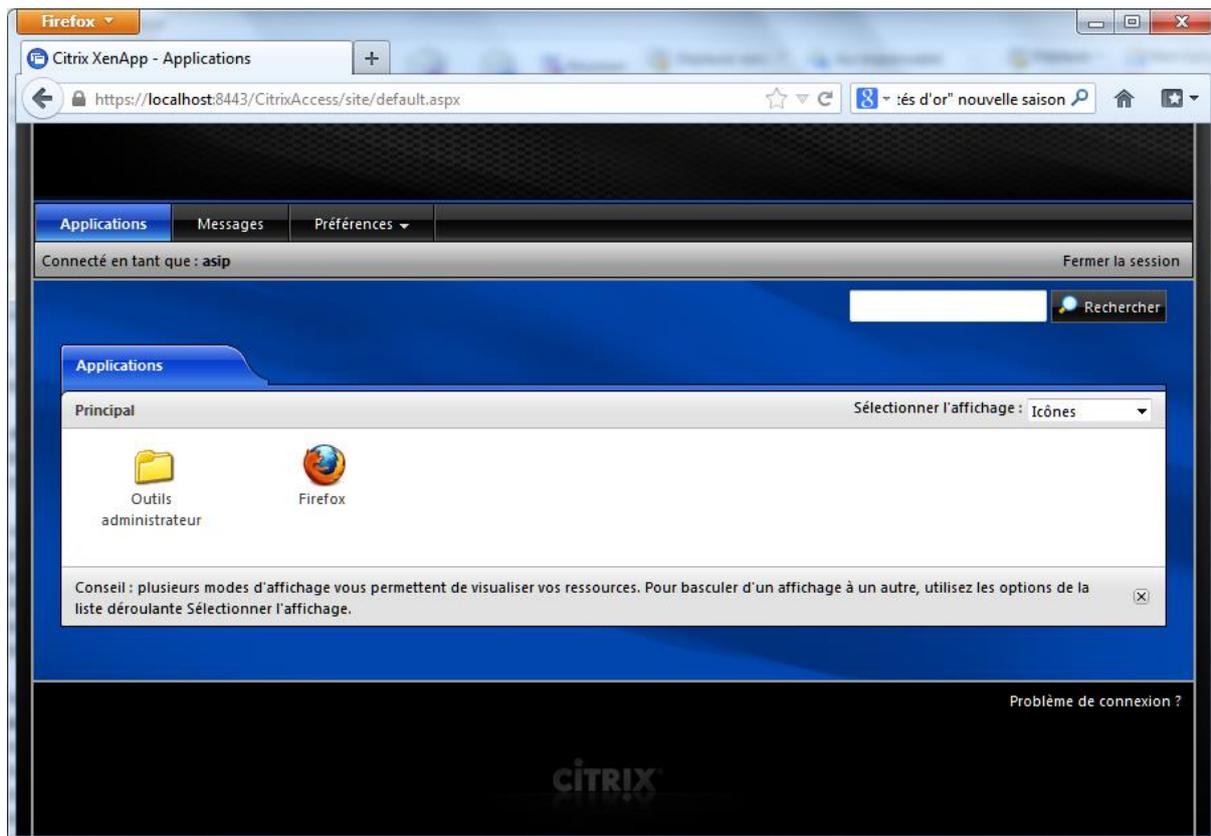


Figure 33: Publication de Firefox sous Citrix XenApp 6.0

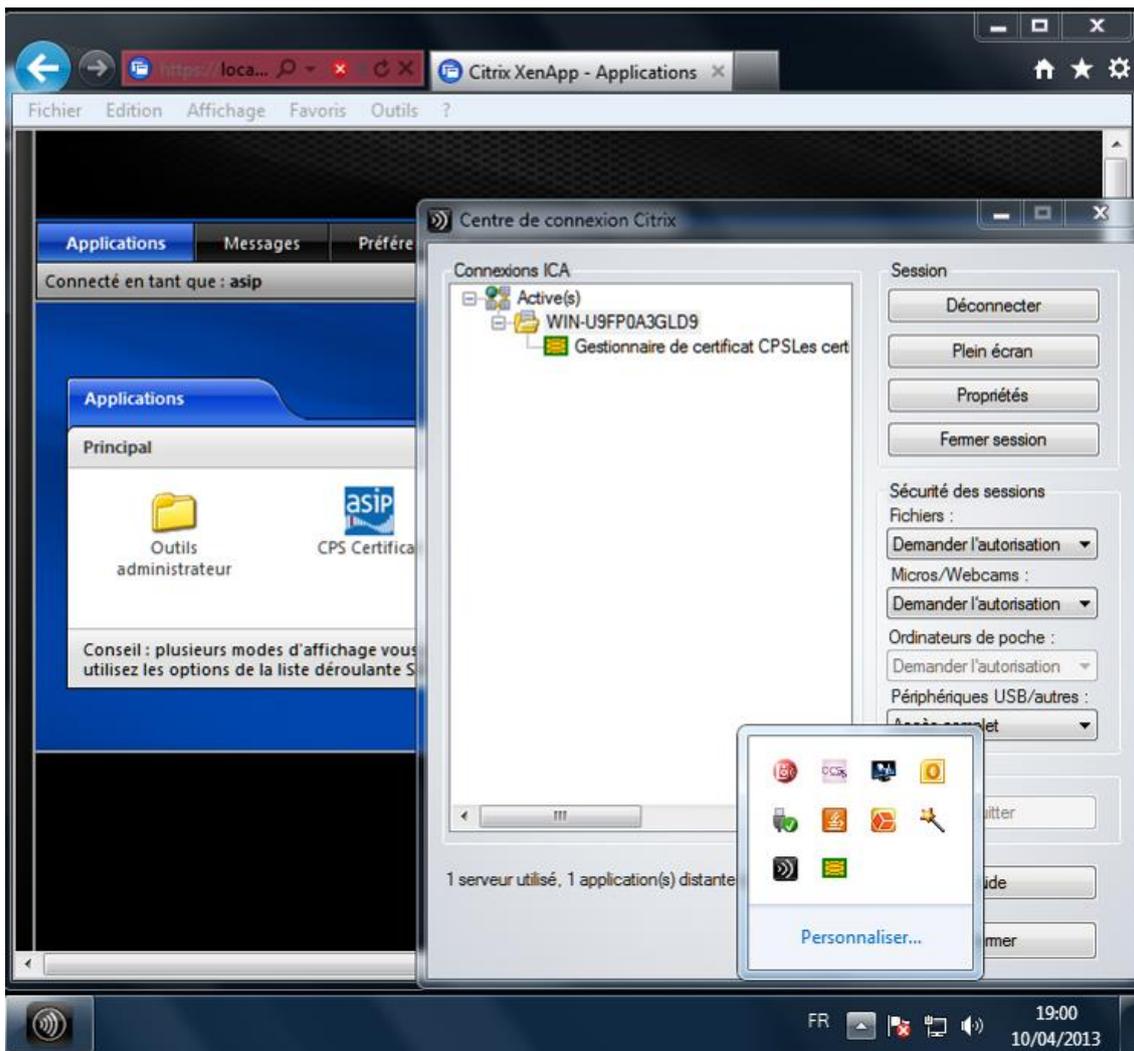


Figure 34: CCM Publiée sous Citrix XenApp 6.0 avec carte CPS détectée

9.2 Remarques connexion « Bureau à distance »

La connexion au Bureau à Distance sous Citrix est proposée par défaut aux utilisateurs du groupe administrateurs.

Elle est déployée sous forme d'un client RDP mstsc.exe virtualisé.

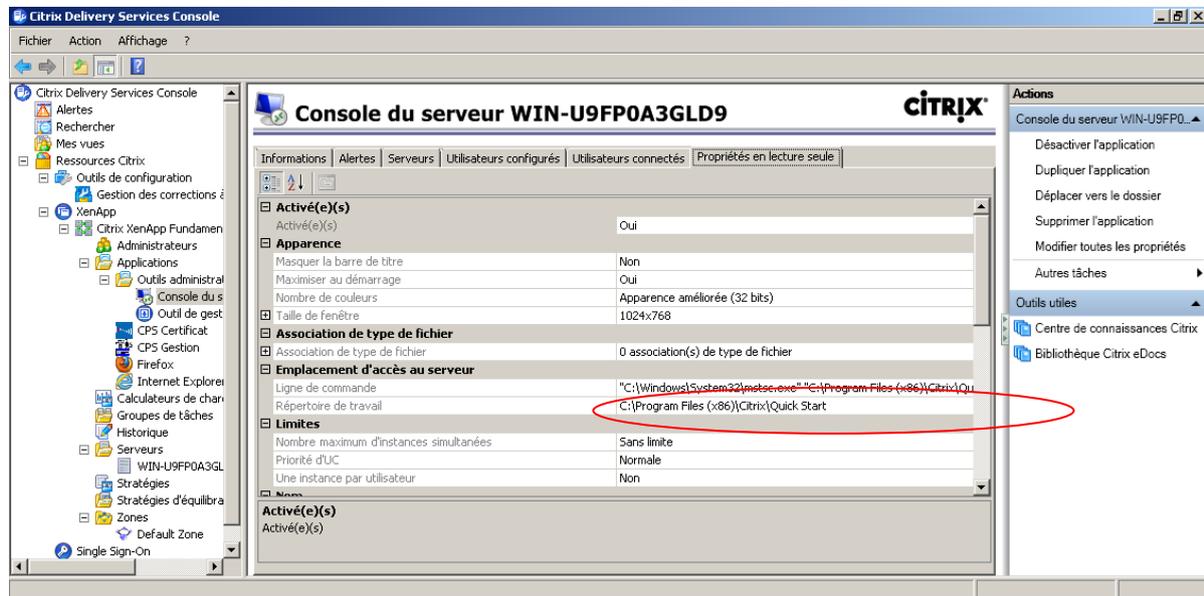


Figure 35: Publication du bureau à distance virtualisé sous Citrix XenApp

Par défaut, la configuration du client RDP virtualisé se fait donc dans **C:\Program Files (x86)\Citrix\Quick Start\Console_w2k8.rdp**

Il est nécessaire d'y activer la redirection de ports COM afin que le GALSS / CCM marche dans cette connexion :

```

Console_w2k8.rdp - Bloc-notes
Fichier Edition Format Affichage ?
screen mode id:i:2
desktopwidth:i:1280
desktopheight:i:1024
session bpp:i:24
winposstr:s:0,1,347,130,1147,730
full address:s:localhost /admin
compression:i:1
keyboardhook:i:2
audiomode:i:0
redirectdrives:i:0
redirectprinters:i:1
redirectcomports:i:1
redirectsmartcards:i:1
displayconnectionbar:i:1
autoreconnection enabled:i:1
  
```

Figure 36: Activation de la redirection de port COM dans la connexion bureau à distance sous Citrix

Il est par ailleurs vivement conseillé de changer cette configuration par défaut par soucis de sécurité :

- Renommage du fichier .rdp
- Vérification de l'adéquation de l'autorisation par défaut {groupe administrateurs <-> Connexion remote desktop}

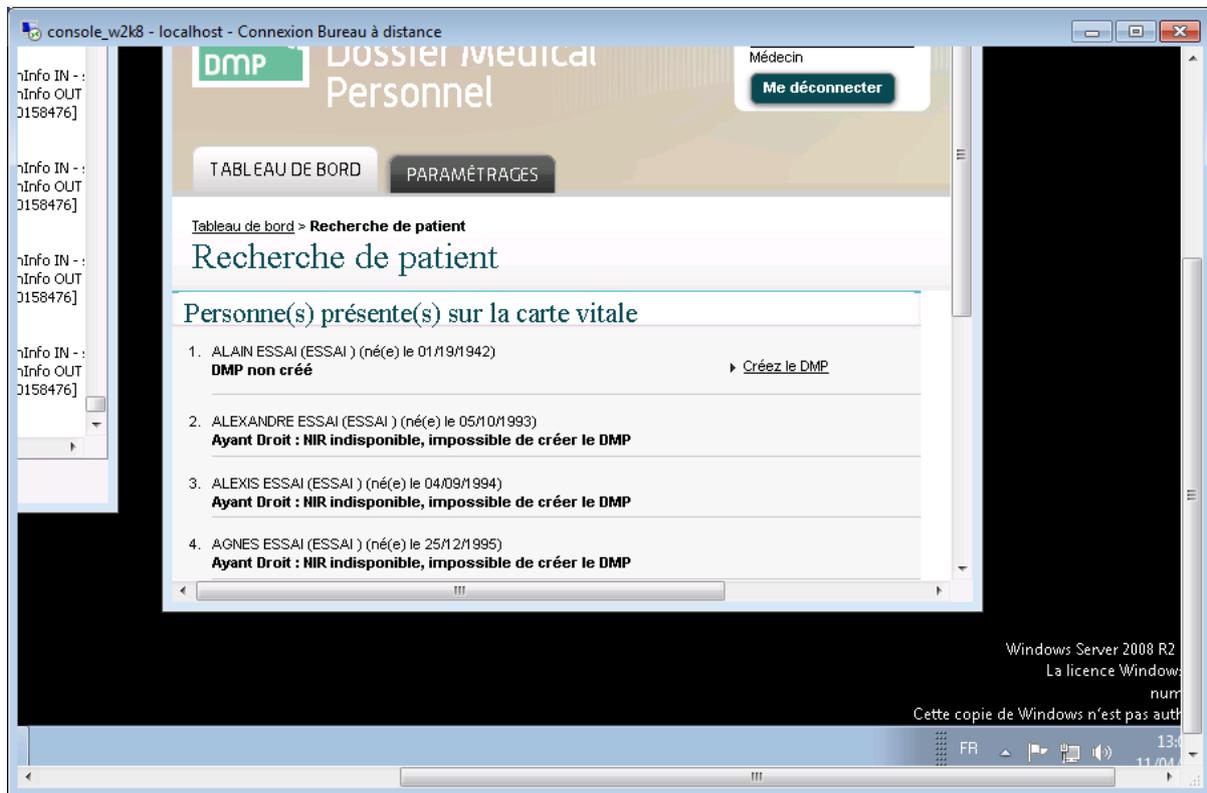


Figure 37: LectureVitale OK sous Firefox dans un bureau distant sous Citrix XenApp

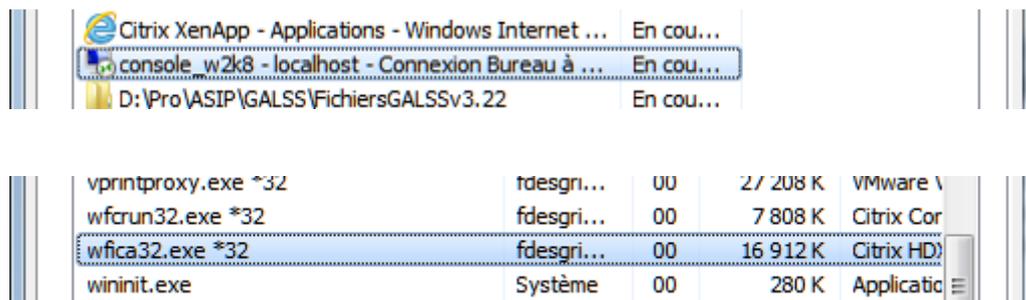


Figure 38: Taskmanager côté client pour la connexion à un bureau distant avec le client Citrix

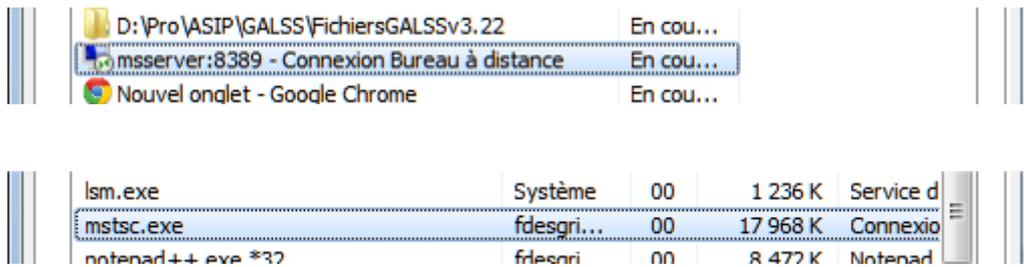


Figure 39: Taskmanager côté client pour la connexion un bureau distant avec le client RDP traditionnel

Côté serveur, sous Citrix, 2 connexions aux services distants apparaissent pour cette unique fonction de bureau : 1 connexion ICA depuis le client et 1 connexion RDP en loopback :

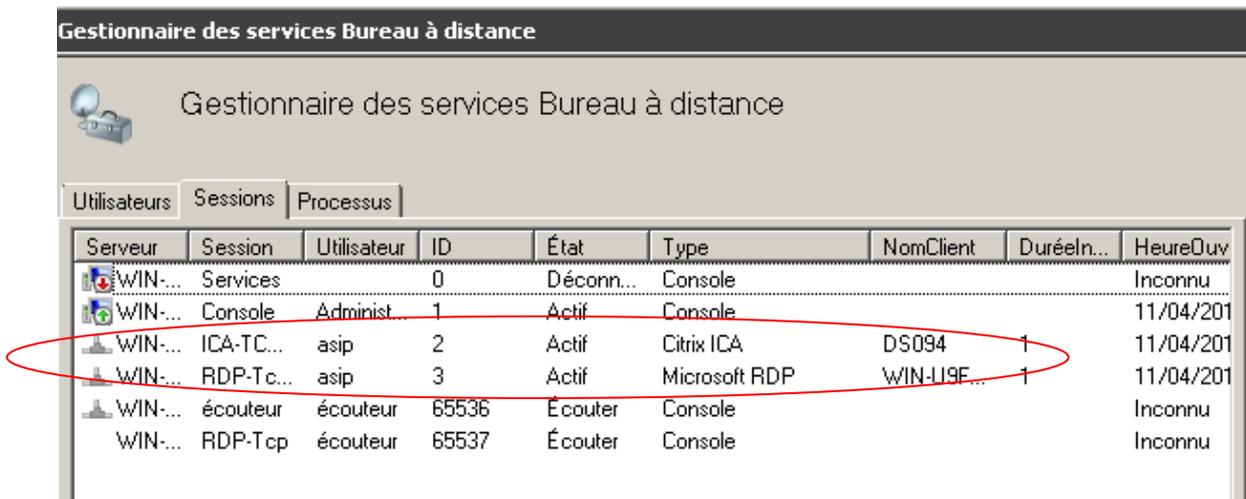


Figure 40: Taskmanager côté client pour la connexion un bureau distant avec le client RDP traditionnel

9.3 Paramétrage des GPO Citrix

Par défaut, les ports COM ou les périphériques USB du client ne sont pas redirigés dans la session Citrix. Cela peut se faire par GPO :

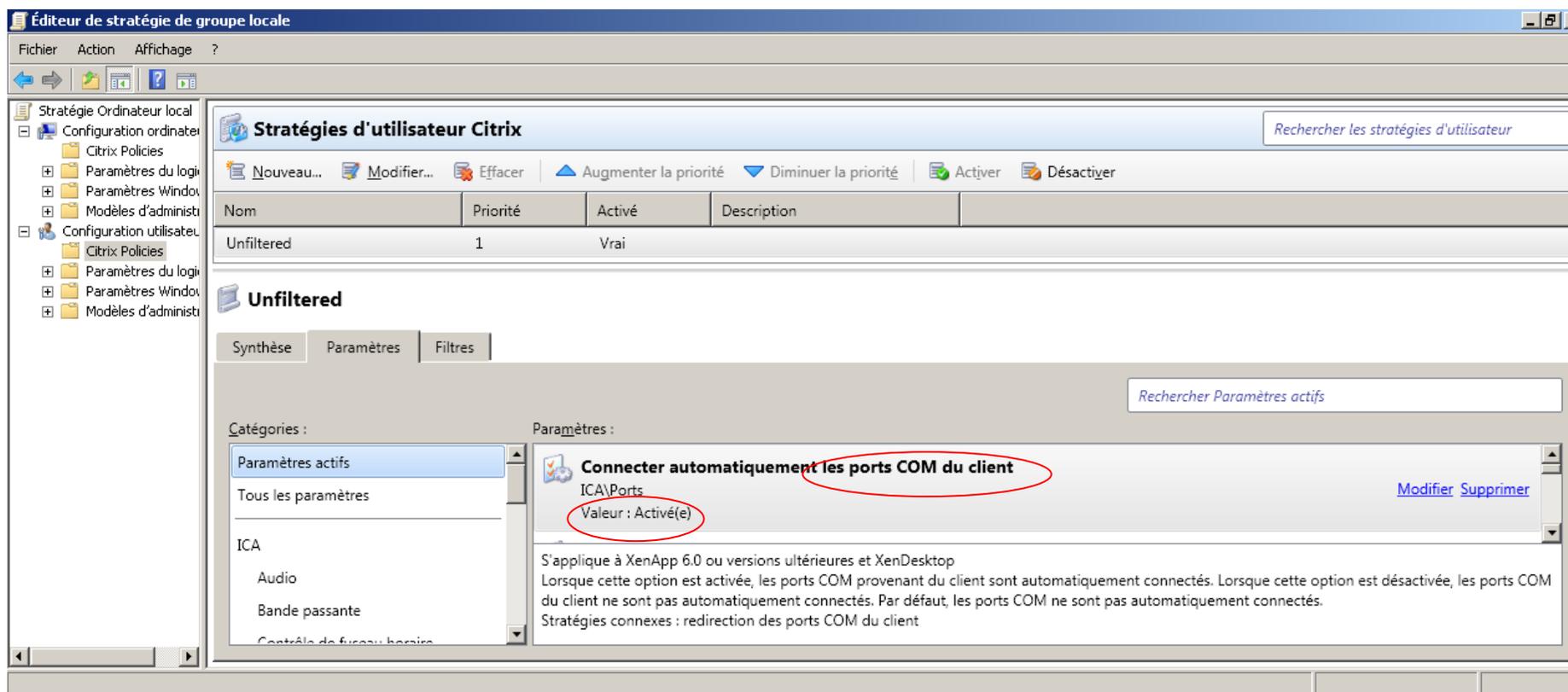


Figure 41: Configuration de la redirection de ports COM par GPO sous Citrix XenApp 6.0

10Annexe – Table des figures

Figure 1: Console graphique d'un serveur Windows Server 2008	10
Figure 2: Fonction d'installation d'une application distante sous TSE.....	11
Figure 3: Liste des applications publiées.....	11
Figure 4: Saisie des droits sur application distante.....	12
Figure 5: Rendre disponible une application distante via le Web.....	12
Figure 6: Lancement du client « remote desktop » sous Windows 7	13
Figure 7: Lancement du client « Remote Desktop » sous Windows 7	13
Figure 8: Partage des ressources locales du poste client.....	14
Figure 9: Vue du bureau distant.....	15
Figure 10: Symbolique dans la barre de tâches	16
Figure 11: Exemples de liens directs vers des applications distantes.....	16
Figure 12: Exemples de liens directs personnalisés vers des applications distantes.....	16
Figure 13: Instance virtualisée de Internet Explorer 10 ouverte directement sur le DMP	17
Figure 14: Similitude du rendu application locale / application distante	18
Figure 15: Symbolique dans la barre de tâches	18
Figure 16: Interface RD Web Access du Pack établissement GALSS	19
Figure 17 Interface RD Web Access du Pack établissement Full PC/SC (en test).....	20
Figure 18: Diagramme réseau associé au mode client serveur.....	21
Figure 19: Aperçu de la console d'administration Citrix XenApp 6.0 sous Windows 2008R2 SP1	26
Figure 20: Virtualisation d'une application single-user sous Citrix XenApp.....	31
Figure 21: Virtualisation d'une application single-user avec les noyaux Windows Vista+	32
Figure 22: Installation d'un poste de travail en filière GALSS	34
Figure 23: Installation d'un poste de travail en filière Full PC/SC.....	35
Figure 24: Page Testssl OK.....	39
Figure 25: Page AW PS DMP OK	40
Figure 26 : Stratégie de sécurité locale : Autoriser l'ouverture de session par les services Bureau à distance	41
Figure 27: Console d'accès Web Citrix XenApp 6.0.....	43
Figure 28: Installation du client Citrix XenApp 6.0	44
Figure 29: Installation du client Citrix XenApp 6.0.....	45
Figure 30: Installation du client Citrix XenApp 6.0.....	45
Figure 31: Console d'accès Web Citrix XenApp 6.0.....	46

Figure 32: Applications d'administration disponibles par défaut à travers de la console d'accès Web Citrix XenApp 6.0.....	46
Figure 33: Publication de Firefox sous Citrix XenApp 6.0.....	47
Figure 34: CCM Publiée sous Citrix XenApp 6.0 avec carte CPS détectée.....	48
Figure 35: Publication du bureau à distance virtualisé sous Citrix XenApp	49
Figure 36: Activation de la redirection de port COM dans la connexion bureau à distance sous Citrix	49
Figure 37: Lecture Vitale OK sous Firefox dans un bureau distant sous Citrix XenApp	50
Figure 38: Taskmanager côté client pour la connexion à un bureau distant avec le client Citrix.....	50
Figure 39: Taskmanager côté client pour la connexion un bureau distant avec le client RDP traditionnel.....	51
Figure 40: Taskmanager côté client pour la connexion un bureau distant avec le client RDP traditionnel.....	51
Figure 41: Configuration de la redirection de ports COM par GPO sous Citrix XenApp 6.0	52

11Annexe – Liste des tableaux

Tableau 1 : Documents de référence	3
Tableau 2 : Glossaire	8
Tableau 3 : Diagramme de collaboration client-serveur	22
Tableau 4 : Client léger : Avantages	24
Tableau 5 : Client Léger : Points d'attention	25
Tableau 6 : Citrix : points forts	27
Tableau 7 : Citrix : points d'attention.....	27
Tableau 8 : Paramètres d'optimisation des flux d'images pour RD et ICA.....	33
Tableau 9 : Références de guides d'optimisation pour RDP / ICA	33
Tableau 10 : Liste des projets ASIP Santé concernés par TSE/Citrix	36
Tableau 11 : Pack Etablissement : Fiche de synthèse	37
Tableau 12 : Pack Etablissement Pack GALSS.....	38
Tableau 13 : GPO : Activer le service Plug-and-Play de la carte à puce	42

12Notes

[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