Guide

de **mise en oeuvre** d'un Smartcard logon avec une carte CPS



Version 2.5.8 du 24/09/2014



Guide de mise en œuvre d'un Smartcard logon avec une Carte de Professionnel de Santé (CPS)

« ASIP Santé / PTS / PSCE »

Version 2.5.8 du 24/09/2014

| Historique du document | | | |
|------------------------|------------|--------|---|
| Version | Date | Auteur | Commentaires |
| 2.5.5 | 03/12/2013 | ASIP | + Suppression AT_0100 (Citrix) : retrofit dans doc installation/utilisation Cryptolib CPS + Nouvelle 1 ^{er} de couverture |
| 2.5.6 | | ASIP | + Paragraphe « Configuration Smartcard logon sur comptes AD existants » + Paragraphe « Projet » + Paragraphe « Smartcard logon linux » + Paragraphe « Smartcard logon Mac OS X » |
| 2.5.7 | | ASIP | + Certificats ASIP Santé PFCNG |
| 2.5.8 | 24/09/2014 | ASIP | + Références à WSUS et au KRA + Détails installation rôle RDP + Vérifications des statuts de certificats online et offline + Ajout d'illustrations ouverture de session avec « hint » + Précisions dans « Configuration Smartcard logon sur comptes AD existants » : cas 1-to-1 et n-to-m |

2 Références

| Documents de référence | | |
|------------------------|--|------------|
| ID | Titre | Auteur |
| [1] | The Smart Card Cryptographic Service Provider CookBook | Microsoft |
| [2] | Installation/configuration du provider de révocation de l'ASIP Santé | Microsoft |
| [3] | Guide de deploiement de louverture de session par carte CPSv3 v1.0.pdf | Microsoft |
| [4] | ASIP-PTS-PSCE Manuel-Installation-utilisation-Cryptolib- CPS 20140930 v5.0.9.pdf | ASIP Santé |
| [5] | ReleaseNote Public Cryptolib Win v5.0.13.pdf ReleaseNote Public Cryptolib Win v5.0.13 x64.pdf | ASIP Santé |
| [6] | Instructions pour l'activation de l'ouverture de session par carte à puce avec des autorités de certification tierces (KB281245) | Microsoft |
| [7] | Certificate Enumeration | Microsoft |
| [8] | Microsoft Lifecycle (politique de support Microsoft) | Microsoft |

3 Résumé

Ce guide présente la mise en œuvre du Smartcard logon Windows avec la carte CPS3 de l'ASIP Santé.

Le **Smartcard logon** permet d'ouvrir une session Windows en utilisant une carte à puce comme vecteur d'**authentification forte** de l'utilisateur.

La **carte à puce** se substitue alors au traditionnel couple login / mot de passe. Ceci permet d'adresser des cas d'usage liés aux milieux/contraintes professionnels (accès en mode « console », accès en mobilité, mise en sécurité du poste sur arrachage carte).

La carte **CPS3** diffusée par l'ASIP Santé est **compatible** avec ce mécanisme à condition qu'elle soit **insérée** dans un lecteur de cartes à puces de type **PC/SC**.

Ce guide documente un « **Kit de Smartcard Logon** » qui est désormais distribué par l'ASIP Santé en complément de ce guide. Ce kit contient les ressources nécessaires aux différentes actions de configuration (certificats et containers de certificats ASIP Santé en particulier).

La mise en œuvre du **Smartcard logon Windows** avec la **carte CPS3** s'appuie sur l'utilisation de la **Cryptolib CPS v5** diffusée par l'ASIP Santé.

Les **Cryptolib CPS v5** sont **indispensables** pour mettre en œuvre le **Smartcard logon Windows** avec la carte **CPS3**. Ce guide et le kit associé ont été conçus en utilisant cette version.

Les **Cryptolib CPS v5** sont des composants logiciels installés sur les postes de travail ainsi que sur les serveurs Microsoft permettant aux systèmes d'exploitation de tirer pleinement profit des fonctionnalités offertes par la carte CPS3 et notamment d'exploiter les fonctionnalités offertes par les volets IAS-ECC (signature, authentification) et sans contact de cette carte.

Cette version de la Cryptolib CPS gère aussi les anciennes cartes CPS2ter qui auront disparu du terrain d'ici mars 2014. Par contre, **seules les cartes CPS3 diffusées depuis mars 2011** permettent de faire du Smartcard logon, les certificats contenus dans les cartes CPS2ter ne présentant pas les caractéristiques requises pour activer cette fonctionnalité.

Les Cryptolib CPS v5 64bit sont nécessaires sur les systèmes 64bit, qui se démocratisent.

Ce guide et ce kit s'adresse :

- aux développeurs et architectes désireux de s'approprier ou d'évaluer la technologie du Smartcard logon
- aux architectes, chef de projets, DSI ou chef d'établissement ayant besoin d'évaluer les tâches et les charges liées à la mise en place de solutions s'appuyant sur le Smartcard logon
- aux éditeurs de logiciels, quelles que soient leurs tailles, qui souhaitent proposer des solutions intégrant ce type de fonctionnalité ou qui souhaitent pouvoir proposer cette solution en tant que projet d'intégration à leurs clients.

Ce document est une refondation de la version 1.4.0 du guide disponible sur le site intégrateurs de l'ASIP Santé et complète le guide rédigé par Microsoft en collaboration avec l'ASIP Santé (cf. **[3]**, avec des indications en anglais).

Le document s'organise en 5 parties :

- 1. <u>Présentation générale du Smartcard Logon</u>
- 2. <u>Prérequis et Configurations requises (aspects généraux)</u>
- 3. Mise en œuvre détaillée, en pas à pas, en français, sur une architecture simple (Annexe 6)
- 4. <u>Limitations connues et contournements</u>
- 5. <u>Descriptif du « Kit Smartcard logon ASIP Santé »</u>

4 Sommaire

| 2 | Références4 | | | |
|----|-------------|----------|--|----|
| 3 | Résumé | | | |
| 4 | Sommaire | | | |
| 5 | Glos | saire | | 9 |
| 6 | Listo | doc | antroprisos sitéos | 10 |
| 0 | Liste | ues | entreprises citees | 10 |
| 7 | Aver | tisse | ments | 11 |
| 8 | Intro | duct | ion | 12 |
| 8 | .1 | Obje | ctifs | 12 |
| 8 | .2 | Pres | entation generale du Smartcard logon | 12 |
| 8 | .3 | Inter | et du Smartcard logon | 14 |
| 9 | Arch | itect | ure et fonctionnement général | 16 |
| 9 | .1 | Sché | ma de principe | 16 |
| 9 | .2 | Fond | tionnement général | 19 |
| | 9.2.1 | _ | Protocole Kerberos | 19 |
| | 9.2.2 | <u>,</u> | | 21 |
| ~ | 9.2.3 | 5 C | Cinematique initiale | 21 |
| 9 | .3 | Sma | rtcard logon et services de terminal | 22 |
| 10 | Spéc | ificat | ions matérielles et prérequis | 23 |
| 1 | 0.1 | Arch | itecture « serveur » | 23 |
| | 10.1 | .1 | Composants | 23 |
| | 10.1 | .2 | PKI et Autorités de certification | 25 |
| 1 | 0.2 | Arch | itecture « client » | 27 |
| | 10.2 | .1 | Matériel | 27 |
| | 10.2 | .2 | Logiciel | 27 |
| | 10.2 | .3 | Cartes et certificats | 27 |
| 11 | Conf | igura | tion | 30 |
| 1 | 1.1 | Conf | iguration du poste client | 30 |
| 1 | 1.2 | Conf | iguration Serveur allégée | 33 |
| 1 | 1.3 | Conf | iguration d'un contrôleur de domaine | 33 |
| 1 | 1.4 | Conf | iguration du serveur de certificats (PKI Microsoft) | 36 |
| 1 | 1.5 | Conf | iguration des options de sécurité | 37 |
| | 11.5 | .1 | Forcer l'utilisation de la carte à puce | 37 |
| | 11.5 | .2 | Comportement du système au retrait de la carte à puce | 38 |
| | 11.5 | .3 | Forcer l'approbation du contrôleur de domaine à l'ouverture de session | 38 |
| | 11.5 | .4 | Désactivation de la vérification des CRLs | 39 |
| 1 | 1.6 | Exen | nple pratique d'une configuration de serveur | 40 |
| 1 | 1.7 | Exen | nples d'architecture réseau | 43 |
| 12 | Anne | exes. | | 44 |
| 1 | 2.1 | Mag | uette de Smartcard logon avec une carte CPx | 44 |
| | 12.1 | .1 . | « Brief Project » | 44 |
| | 12.1 | .2 | Ressources nécessaires | 45 |
| | 12.1 | .3 | Livrables | 46 |
| | 12.1 | .4 | Macro-Planning | 46 |
| | 12.1 | .5 | Remarques | 48 |
| 1 | 2.2 | Insta | Ilation du poste de travail client | 49 |

| 12.3 I | nstallation de Windows 2008 R2 SP1 | 58 |
|--|--|--|
| 12.4 I | nstallation d'un rôle Active Directory | 69 |
| 12.5 I | nstallation d'un rôle Certificate Server | 85 |
| 12.6 I | nstallation d'un rôle Terminal Server | |
| 12.6.1 | Installation des composants du rôle Terminal Server | |
| 12.6.2 | 2 Activation du serveur de licence RDP | 106 |
| 12.6.3 | 8 Configurations des comptes « Serveurs de licences des services Terminal Ser | veur » 108 |
| 12.6.4 | Installation des licences sur le serveur de licences | 108 |
| 12.6.5 | Configuration de l'hôte Terminal Server | 111 |
| 12.6.6 | Paramétrage du serveur RDP | 113 |
| 12.6.7 | Configuration du certificat du serveur RDP | 120 |
| 12.6.8 | 3 Autres GPOs | 132 |
| 12.7 I | nstallation d'un rôle IIS | 134 |
| 12.8 I | nstallation de la Cryptolib CPS sur le serveur | 138 |
| 12.8.1 | Désactivation du CCM au lancement | 138 |
| 12.8.2 | Activation du CCM à l'ouverture de session au cas par cas | 138 |
| 12.8.3 | Remarque sur le provisionning des magasins de certificats | 138 |
| 12.9 I | nstallation du Provider de révocation ASIP Santé – Microsoft sur le serveur | 139 |
| 12.9.1 | Installation du Provider de révocation ASIP Santé – Microsoft | 139 |
| 12.9.2 | Mise à jour des magasins de certificats Local Machine | 141 |
| 12.9.3 | Configuration du Provider de révocation ASIP Santé – Microsoft | |
| 12.9.4 | Cas des contrôleurs de domaine avec accès internet : vérification des | statuts de |
| certifi | cats « online » | |
| 12.9.5 | Cas des contrôleurs de domaine sans accès internet : vérification des | statuts de |
| certifi | cats « offline » via l'alimentation du magasin de CRL en ligne de commande | |
| 1296 | · Test du Drevider de révession ACID Centé - Misrosett en véritient le s | |
| 12.5.0 | 5 Test du Provider de revocation ASIP Sante – Microsoft en Vermant le s | statut d'un |
| certifi | cat 148 | |
| certifi 12.10 (| cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log | on 151 |
| certifi 12.10 (12.11 (| cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 |
| certifi 12.10 (12.11 (12.11 | cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 160 |
| certifi 12.10 (12.11 (12.11 12.11 | cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 160 166 |
| certifi 12.10 (12.11 (12.11 12.11 12.12 (12.12 | cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon 1 Magasins de certificats 2 Stratégie Active Directory Création des utilisateurs | on 151 160 160 166 168 |
| certifi 12.10 (12.11 (12.11 12.11 12.12 (12.12 12.12 | cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 166 168 168 |
| certifi 12.10 (12.11 (12.11 12.11 12.12 (12.12 12.12 12.12 | a Test du Provider de revocation ASIP sante – Microsoft en Vermant le s cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 168 168 168 170 |
| certifi 12.10 (12.11 (12.11 (12.12 (12.12 (12.12 12.12 12.12 | a Test du Provider de revocation ASIP sante – Microsoft en Vermant le s cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 168 168 168 170 171 |
| certifi 12.10 (12.11 (12.11 12.11 12.12 (12.12 12.12 12.12 12.13 F | a Test du Provider de revocation ASIP sante – Microsoft en Vermant le s cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 166 168 168 170 171 174 |
| certifi 12.10 (12.11 (12.11 (12.12 (12.12 12.12 12.12 12.12 12.13 F 12.13 | a Test du Provider de revocation ASIP Sante – Microsoft en Vermant le s cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 168 168 170 171 174 174 174 |
| certifi 12.10 (12.11 (12.11 (12.12 (12.12 12.12 12.12 12.12 12.13 F 12.13 12.14 F | cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 168 168 168 170 171 174 174 177 |
| certifi 12.10 (12.11 (12.11 12.12 (12.12 12.12 12.12 12.13 F 12.13 12.14 F 12.14 | a Test du Provider de revocation ASIP sante – Microsoft en Vermant le s cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 166 168 170 171 174 174 174 177 177 |
| certifi 12.10 (12.11 (12.11 (12.12 (12.12 12.12 12.12 12.12 12.13 F 12.13 F 12.14 F 12.14 12.14 [12.14 | a Test du Provider de revocation ASIP Sante – Microsoft en Vermant le s cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 168 168 170 171 174 174 177 177 ficats X509 |
| certifi 12.10 (12.11 (12.11 (12.12 (12.12 12.12 12.12 12.12 12.13 12.14 F 12.14 12.14 [Win2 12.14 | a fest du Provider de revocation ASIP sante – Microsoft en vermant le s cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 168 168 170 171 174 174 177 ficats X509 178 178 |
| certifi 12.10 (12.11 (12.11 (12.12 (12.12 12.12 12.12 12.13 F 12.13 F 12.14 F 12.14 [Win2 12.14 [Win2 12.14 | a fest du Provider de revocation ASIP sante – Microsoft en Vermant le s cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 168 168 170 171 174 174 177 177 177 178 182 182 |
| certifi 12.10 (12.11 (12.11 (12.12 (12.12 12.12 12.12 12.13 F 12.13 12.14 F 12.14 [Win2 12.14 [Win2 12.14 12.14 12.14 | a fest du Provider de revocation ASIP sante – Microsoft en verifiant le s cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 168 168 170 171 174 174 174 177 ficats X509 178 182 182 182 |
| certifi 12.10 (12.11 (12.11 (12.12 (12.12 12.12 12.12 12.12 12.13 12.14 F 12.13 12.14 F 12.14 [Win2 12.14 12.14 12.14 12.14 | a fest du Provider de revocation AsiP sante – Microsoft en Venhant le s cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 |
| certifi 12.10 (12.11 (12.11 (12.11 (12.12 (12.12 (12.12 (12.12 (12.12 (12.13 F 12.13 F 12.14 F 12.14 (12.14 | action ASIP Sante – Microsoft en Vermant le's cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 168 168 168 170 171 171 174 177 177 177 177 177 178 182 182 184 185 185 |
| certifi 12.10 (12.11 (12.11 (12.12 (12.12 12.12 12.12 12.13 F 12.13 12.14 F 12.14 [Win2 12.14 12.14 12.14 12.14 12.14 12.14 12.14 12.14 | a fest du Provider de revocation AsiP sante – Microsoft en Vermant le s cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 168 168 176 171 174 174 174 177 ficats X509 178 182 182 184 185 188 201 |
| certifi 12.10 (12.11 (12.11 (12.12 (12.12 (12.12 12.12 12.12 12.12 12.13 12.14 F 12.14 12.14 [Win2 12.14 12.14 12.14 12.14 12.14 12.14 12.14 12.14 12.15 (12.16 [12.17 [12.17 [12.17 [| Test du Provider de revocation AsiP sante – Microsoft en Vermant le s cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 168 168 168 170 171 174 174 174 177 ficats X509 178 182 182 184 185 188 201 201 201 |
| certifi 12.10 (12.11 (12.11 (12.11 (12.12 (12.12 (12.12 (12.12 (12.12 (12.13 F 12.13 F 12.14 F 12.14 (12.14 (12.17 (12.17))))))))))))))))))))))))))))))))))) | A rest du Provider de revocation ASIP Sante – Microsoft en Vermant le s cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 168 168 168 170 171 177 177 177 ficats X509 178 182 182 184 185 188 201 201 201 201 |
| certifi 12.10 (12.11 (12.11 (12.12 (12.12 12.12 12.12 12.13 F 12.14 F 12.14 12.14 [Win2 12.14 12.14 12.14 12.14 12.14 12.14 12.14 12.14 12.14 12.14 12.15 (12.16 [12.17 [12.17 [12.17] 12.18 [| rest du Provider de revocation ASIP Sante – Microsoft en Vermant le s cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 168 168 170 171 174 174 174 177 ficats X509 178 182 182 184 185 188 201 201 201 201 |
| certifi 12.10 (12.11 (12.11 (12.12 (12.12 (12.12 12.12 12.12 12.13 F 12.13 12.14 F 12.14 12.14 12.14 12.14 12.14 12.14 12.14 12.14 12.14 12.15 (12.17 [12.17 12.18 F 12 18 | cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 168 168 168 170 171 174 174 174 177 ficats X509 178 182 182 182 184 185 188 201 201 204 204 204 |
| certifi 12.10 (12.11 (12.11 (12.11 (12.12 (12.12 (12.12 (12.12 (12.12 (12.13 F 12.13 F 12.14 F 12.14 (12.14 (12.17 (12.17 (12.17 (12.17 (12.17 (12.17 (12.18 ()))))))))))))))))))))))))))))))))))) | Test du Provider de revocation ASIP Sante – Microsoft en Vernant le s cat 148 Configuration d'une console de composants enfichables dédiée au Smartcard log Configuration du Contrôleur de domaine pour la Smartcard logon | on 151 160 166 168 168 168 170 171 177 177 177 177 177 177 177 177 177 177 177 182 182 182 182 182 182 182 182 182 182 182 184 185 1201 201 201 204 204 204 |

| 13 | Cont | enu du « Kit Smartcard logon ASIP Santé » | 214 |
|----|-------|--|-----|
| 14 | Smar | tcard logon sous Linux | 217 |
| 1 | 4.1 | Installation de la Cryptolib CPS v5 pour Linux | 217 |
| 1 | 4.2 | Configuration du lancement automatique du daemon PCSCD | 217 |
| 1 | .4.3 | Installation et configuration du PAM OpenSC | 217 |
| | 14.3. | 1 Récupération et installation de libpam-pkcs11 | 217 |
| | 14.3. | 2 Initialisation du fichier pam_pkcs11.conf, des certificats et des CRLs | 218 |
| | 14.3. | 3 Edition de /etc/pam.d/sudo | 218 |
| | 14.3. | 4 Edition de /etc/pam.d/common-auth | 218 |
| | 14.3. | 5 Edition de /etc/pam_pkcs11/pam_pkcs11.conf | 219 |
| | 14.3. | 6 Configuration d'un compte pour le Smartcard logon | 219 |
| 15 | Smar | tcard logon sous Mac OS X | 220 |
| 1 | 5.1 | Pré-requis | 220 |
| 1 | 5.2 | Méthode | 220 |
| 1 | 5.3 | Autres commandes utiles | 220 |
| 1 | 5.4 | Remarques | 221 |
| 16 | Anne | xe – Liste des figures | 222 |
| 17 | Anne | xe – Liste des tables | 226 |
| 18 | Note | s | 228 |

5 Glossaire

| Sigle | Signification |
|---------------------|--|
| ΑΡΙ | Application Programming Interface |
| ATR | Answer to reset : Réponse d'une carte à puce à sa mise sous tension. |
| CPS | Carte de Professionnel de Santé |
| CSP | Cryptographic Service Provider : Bibliothèque logicielle de fonctions cryptographiques fournie par Microsoft ou un éditeur tiers (fournisseur de carte). |
| Kerberos | Protocole d'authentification réseau, basé sur l'utilisation de tickets. Utilisé par défaut à partir de Windows 2000. |
| KRA | Microsoft Key Recovery Agent |
| MSGINA / GINA | Microsoft GINA (Graphical Identification And Authentification): DLL standard Microsoft gérant l'interface graphique utilisateur, lors de l'ouverture de session. Elle se charge notamment de demander à l'utilisateur le code porteur de sa carte. |
| MSI | Microsoft Installer : Format de fichier d'installation de Microsoft, géré par le moteur d'installation Windows Installer. |
| NTAuth | Magasin de certificats d'un poste Windows client, alimenté exclusivement par le contrôleur de domaine par propagation. Contient les certificats d'autorités de confiance. Utilisé par Winlogon. |
| PC/SC | Personal Computer/Smart Card : Bibliothèque logicielle standard pour l'accès aux lecteurs et aux cartes à puce. |
| PDC | Primary Domain Controller : Contrôleur de domaine principal. |
| PKI (IGC) | Public Key Infrastructure (Infrastructure de Gestion des Clefs) |
| SI | Système d'information : Ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) |
| TSE | Terminal Server Edition : Service de Terminal de Microsoft. Composant permettant d'accéder à des applications et des données sur un ordinateur distant au travers de n'importe quel type de réseau. |
| RDP | Remote Desktop Protocol : Protocole de communication utilisé par TSE. |
| wsus | Windows Server Update Services |

Tableau 1 : Glossaire

6 Liste des entreprises citées

Le présent document cite les produits des entreprises ou organismes suivants:

| Nom | Site Web | Lien avec le Smartcard logon |
|-------------------|-----------------------|---|
| Apple | www.apple.com | Mac OS X |
| Citrix | www.citrix.com | Env. TSE/Citrix |
| Debian | www.debian.org | Linux, .deb |
| Microsoft | www.microsoft.com | Windows, CSP, TSE, AD DC, AD CS |
| PC/SC Workgroup | www.pcscworkgroup.com | Responsable du standard PC/SC visant l'intégration de la carte à puce et des lecteurs de cartes dans les systèmes informatiques |
| Redhat | www.redhat.com | Linux, .rpm |
| RSA Security Inc. | www.rsa.com | PKCS, RSA |

Tableau 2 : Entreprises citées

7 Avertissements

Sur le nécessaire strict respect des procédures décrites dans le manuel

L'attention de l'utilisateur est attirée sur l'importance de respecter strictement les procédures décrites dans le présent guide de mise en œuvre du Smartcard logon avec une carte CPS.

Toutes les procédures qui y sont décrites ont été préalablement testées par l'ASIP Santé. Elles doivent permettre à l'utilisateur de mettre en œuvre le Smartcard logon avec une carte CPS sur son poste de travail ou tout autre dispositif informatique. En cas de non-respect de ces procédures et des conditions normales d'utilisation des composants logiciels mentionnés dans ce guide, sa mise en œuvre est susceptible d'engendrer des dysfonctionnements dans l'environnement de travail de l'utilisateur.

En cas de dysfonctionnement, quel qu'il soit, l'ASIP Santé prêtera dans la mesure du possible assistance à l'utilisateur, qui ne pourra rechercher sa responsabilité en cas de non-respect des procédures décrites dans le présent manuel.

Sur les liens externes

Le présent guide contient des liens vers des sites Internet.

Ces liens ne visent qu'à informer l'utilisateur. Ces sites Web ne sont pas gérés par l'ASIP Santé et l'ASIP Santé n'exerce sur eux aucun contrôle : leur mention ne saurait engager l'ASIP Santé quant à leur contenu.

L'utilisation des sites tiers mentionnés relève de la seule responsabilité du lecteur ou de l'utilisateur des produits documentés.

Sur les copies d'écran et les lignes de commande

Les lignes de commandes données ci-après le sont à titre indicatif. Elles documentent des cas « passants » qui peuvent différer d'un système à l'autre.

Les copies d'écran présentées dans ce document sont données à titre illustratif.

Les pages ou écrans réellement affichés peuvent être différents, notamment en raison de montées de version ou de configurations d'environnements différentes.

Citations

L'ASIP Santé est contrainte de citer le nom de certaines entreprises recensées au tableau n°2 afin d'apporter toute l'aide nécessaire aux utilisateurs désireux de mettre en œuvre le Smartcard logon avec une carte CPS.

Les entreprises citées peuvent prendre contact avec l'ASIP Santé à l'adresse email

editeurs@asipsante.fr pour toute demande en lien avec la citation les concernant.

Les entreprises non citées dans ce manuel et ayant une activité en lien avec le Smartcard logon CPS peuvent également se faire connaître auprès de l'ASIP Santé en la contactant à la même adresse.

Contact

Toute question en rapport avec le contenu du présent guide doit être adressée à l'adresse suivante: <u>editeurs@asipsante.fr</u>

Tableau 3 : Avertissements

8 Introduction

8.1 Objectifs

L'objectif de ce document est d'accompagner le déploiement d'un mécanisme d'ouverture de session Microsoft Windows à partir d'une carte à puce de la famille CPS.

Ce document décrit les bonnes pratiques pour un déploiement d'un mécanisme de Smartcard logon sur un réseau Microsoft.

Il n'est pas exhaustif : toutes les architectures clientes existantes ou futures ne sont pas couvertes. Il adresse cependant les principales architectures « standards ».

Il vise la réussite de la mise en place d'une architecture simple de Smartcard logon.

Il est basé sur les expériences de l'ASIP Santé dans ce domaine. Il regroupe les différentes techniques de configuration standard au Smartcard logon, adaptées à l'utilisation de la carte CPS.

Il contient des tableaux récapitulatifs qu'il est utile d'imprimer afin d'appliquer au mieux le paramétrage requis.

8.2 Présentation générale du Smartcard logon

Il est possible depuis Microsoft Windows 2000 de remplacer la saisie du couple login / mot de passe par une authentification par carte à puce au moment de réaliser une ouverture de session Windows dite « interactive ».

Tout réseau utilisant Active Directory et un contrôleur de domaine Microsoft (Windows Server 2000, 2003 ou 2008) peut bénéficier de la technologie "Smartcard logon" en standard.

Ce mécanisme d'ouverture de sessions Windows par carte à puce est par ailleurs compatible avec les sessions Terminal Services TSE (voir chapitre « **Smartcard logon et les services de terminal** »).

Le principe de base de ce mécanisme est une authentification mutuelle entre la carte présente dans un lecteur du poste client et le serveur du domaine à partir de certificats électroniques X.509. Le lecteur de carte doit impérativement être de type PC/SC.



Figure 1 : Ecran d'accueil de Windows XP, configuré pour ouvrir une session avec une carte à puce.



Figure 2 : Ecran d'accueil de Windows 7, configuré pour ouvrir une session avec une carte à puce.

| Sécurité de Windo | ews |
|---|--|
| Entrer vos i Ces informatio msserver. | nformations d'identification ns d'identification seront utilisées pour vous connecter à |
| | Utiliser un autre compte |
| | 50000000018119/CPAT0 Identification pour la carte à puce 5.0000000018119.CPAT0001@cart |
| | Code confidentiel |
| Mémo | oriser ces informations |
| | OK Annuler |

Figure 3 : Ecran du client Terminal Server sous Windows 7 pour ouvrir une session avec une carte à puce.

8.3 Intérêt du Smartcard logon

Cette section analyse les raisons d'utiliser une carte à puce (de type CPS par exemple) plutôt qu'une authentification standard login/mot de passe pour l'ouverture de session utilisateur.

| Inconvénients login-mdp | Description |
|----------------------------|---|
| I_0010 | Mot de passe faible (choisi par l'utilisateur), facilement « crackable » (attaque par dictionnaire par exemple) |
| I_0020 | Algorithmes LM/NTLM/NTLMv2 faibles |
| I_0030 | Systèmes de sécurité logiciels cassables (récupération des mots de passe dans la SAM, « KeyLoggers »,) |
| I_0040 | Multiplication des mots de passe |

Tableau 4 : Inconvénients du couple login/mot de passe

| Avantages carte à puce | Description |
|---------------------------|---|
| I_0050 | La clé est générée par le système (pas de clé faible) |
| I_0060 | Les algorithmes sont robustes |
| I_0070 | La longueur de clé est importante |
| I_0080 | La clé privée est stockée dans la carte et ne peut pas être extraite |
| I_0090 | Le certificat de l'utilisateur devient son identité numérique |
| I_0100 | Cette identité est standard : elle suit des normes et des préconisations normalisées, reconnues et largement adoptées par ailleurs. |
| I_0110 | La phase de login fait intervenir 2 facteurs d'authentification différents : 1. « ce que j'ai » : la carte CPS 2. « ce que je saisi » : le code porteur de la carte CPS L'authentification est dite « forte ». |

Tableau 5 : Avantages de la carte à puce

| Inconvénients carte à puce / login-mdp | Description |
|--|--|
| I_0120 | Architecture parfois délicate à mettre en place (PKI serveur, accès externe à un annuaire, installation matérielle et logicielle du poste) |
| I_0130 | Ouverture de session un peu plus longue (de l'ordre de quelques secondes supplémentaires, en fonction de la vitesse d'accès et de calcul de la carte, et du poste client). Ces temps sont optimisés avec la Cryptolib CPS v5 via l'utilisation d'un cache de certificats. |
| I_0140 | Administration plus complexe de l'architecture (gestion des PKI, gestion des flux externes, expiration des certificats,) |

 Tableau 6 : Inconvénients de la carte à puce face au couple login/mot de passe

Les inconvénients d'ordre technique liés à la mise en œuvre de la carte à puce sont mineurs par rapport aux avantages (notamment en terme de sécurité) apportés par cette technologie et au regard des limitations et faiblesses avérées du login/mot de passe.

9 Architecture et fonctionnement général

9.1 Schéma de principe

Le mécanisme d'ouverture de session Windows est illustré ci-dessous.

Ce mécanisme est complexe par essence. Les considérations de sécurité y prévalent, conjointement aux considérations de performance qu'il faut introduire sans compromettre le système.



Figure 4 : Schéma fonctionnel global du Smartcard logon de Microsoft (Win 2000 et XP)

Microsoft a revu ce mécanisme lors de la sortie de Windows Vista.

Si la logique du mécanisme reste sensiblement la même, l'implémentation change avec la disparition de MS Gina et l'apparition du composante Base CSP / Minidriver.



Figure 5 : Schéma fonctionnel global du Smartcard logon de Microsoft (Win Vista+) [7]

| Composant | Description |
|--------------|--|
| MSGINA | [Windows XP] Microsoft GINA (Graphical Identification And Authentification) = Bibliothèque standard Microsoft gérant l'interface graphique utilisateur, lors de l'ouverture de session. Elle se charge notamment de demander à l'utilisateur le code porteur de sa carte. |
| LSA | Local Security Authority : il s'assure que l'utilisateur à la permission d'accéder au système. Il crée les jetons d'accès. C'est lui qui lance le processus d'authentification du module Kerberos. |
| Kerberos SSP | (Kerberos Security Support Provider) : DLL principale intervenant dans le processus d'ouverture de session entre un client et un serveur (le protocole standard actuel est appelé Kerberos V5, normalisé par l'IETF dans les RFC 1510). Elle intervient aussi bien dans une ouverture de session standard (avec logon/mot de passe), que dans une ouverture par carte à puce (PKINIT). |
| KDC | Key Distribution Center = Centre de distribution des clés. Module serveur implémenté par le protocole Kerberos (pour l'authentification et l'autorisation des utilisateurs distants). |
| РАС | Privilege attribute certificate : contient les informations à destination du client telles que : le SID (User security ID), les droits de l'utilisateur sur le domaine. |

 Tableau 7 : Smartcard logon: Principaux Composants Microsoft mis en œuvre

Mettre en œuvre le Smartcard logon revient à configurer chaque acteur impliqué dans ce mécanisme.

9.2 Fonctionnement général

9.2.1 Protocole Kerberos

L'ouverture de session Windows repose sur le protocole d'authentification réseau Kerberos qui gère aussi bien, via le protocole PKINIT, l'authentification par login/password que par carte à puce.

Voici, schématiquement le fonctionnement du protocole **Kerberos V5** lors de l'ouverture de session:

Un système Kerberos fait intervenir les trois sous protocoles suivants:

- 1. AS (Authentication Service)
- 2. TGS (Ticket-Granting Service)
- 3. CS (Client/Server)

Les échanges de données entre le client et le serveur se font par des messages de requêtes/réponses normalisés suivant le protocole Kerberos suivant :

| Etape | Code | Communication | Description |
|-------|-------------|------------------|--|
| 1 | KRB_AS_REQ | Client > Serveur | Requête de service d'authentification Kerberos. (Vérification de l'identité du client) Le certificat d'authentification (présent dans la carte) est sursigné par sa propre clé privée et envoyé, accompagné de données relatives au client, du poste client vers le serveur. |
| 2 | KRB_AS_REP | Serveur > Client | Réponse du serveur. Le serveur envoie au client, en cas d'authentification réussie, une clé de session (clé symétrique) et un TGT (Ticket d'accès au service de délivrement de ticket, limité dans le temps). Le tout chiffré avec la clé publique du client (envoyée dans le message de requête). |
| 3 | KRB_TGS_REQ | Client > Serveur | Requête de ticket de session au serveur de ticket (Chiffrée par la clé de session). Envoi du TGT dans la requête. |
| 4 | KRB_TGS_REP | Serveur > Client | Réponse du serveur. Envoi du ticket de session au client (Ticket d'accès au serveur) |
| 5 | KRB_AP_REQ | Client > Serveur | Requête applicative. Envoi du ticket de session. |
| 6 | KRB_AP_REP | Serveur > Client | Réponse du serveur. La session peut être ouverte. Les échanges peuvent se poursuivre entre le client et le serveur. |

Tableau 8 : Smartcard logon: Protocole Kerberos

9.2.2 Protocole PKINIT

Le scénario d'ouverture d'une session Windows à partir d'une carte à puce (Smartcard logon) suit une procédure stricte définie par Microsoft.

La procédure complète est décrite dans le document : **The Smart Card Cryptographic Service Provider CookBook [1]** disponible en accès libre sur le site de Microsoft.

Ce protocole est appelé PKINIT. PKINIT est une extension du protocole Kerberos qui rend possible l'utilisation de certificats numériques X509 pour la phase d'authentification. Cette extension permet en particulier de remplacer l'authentification login/mot de passe par une authentification par carte à puce.

Il définit précisément les échanges entre la carte (via le CSP et PC/SC) et Kerberos (via Winlogon).

9.2.3 Cinématique initiale

La cinématique réalisée lorsqu'une carte à puce est insérée dans un lecteur d'un poste configuré pour le Smartcard logon est la suivante :

| Etape | Description |
|--------|---|
| C_0010 | Une carte est insérée dans un lecteur PC/SC du poste client. |
| C_0020 | Le service ScardSvr du poste client (service Windows « Smartcard Server » : gestionnaire des lecteurs de carte sur le poste) détecte cette insertion via Winscard.dll (bibliothèque de gestion PC/SC de Microsoft « Smartcard API »). |
| C_0030 | Le processus Winlogon est réveillé par le service ScardSvr. |
| C_0040 | Winlogon envoie une commande de demande d'ATR à la carte (via le gestionnaire de cartes). |
| C_0050 | Winlogon reçoit l'ATR et recherche en base de registres, s'il existe une association avec un CSP dans la table de correspondance ATR<->CSP. |
| C_0060 | Si un CSP est trouvé, Winlogon va demander (via GINA sous Windows XP), le code porteur à l'utilisateur. |
| C_0070 | Il va ensuite demander à récupérer le certificat d'authentification de la carte (en passant à la carte le code porteur rentré par l'utilisateur, via le CSP associé). |
| C_0080 | Winlogon peut alors lancer le processus Kerberos (via LSA) qui va exécuter la procédure d'authentification/vérification du client par le serveur de domaine, par carte à puce (protocole PKINIT), et lui renvoyer le certificat d'authentification récupéré dans la carte. |
| C_0090 | Si toute la procédure s'est déroulée correctement (identification/authentification correcte de l'utilisateur par le contrôleur de domaine), l'utilisateur est alors autorisé à ouvrir une session sur le poste client. |

Tableau 9 : Smartcard logon: Cinématique de l'authentification par carte à puce

9.3 Smartcard logon et services de terminal

Le mécanisme d'ouverture Windows par carte à puce (Smartcard logon) est compatible avec les sessions Terminal Services TSE, bureau à distance (qui s'appuient sur le protocole RDP) et architecture CITRIX (protocole ICA).



Figure 6 : Smartcard logon et TSE : Redirection des APDU [1]

Il est donc possible d'ouvrir nativement une session client/serveur à distance par carte à puce (à partir d'un client dit « léger »).

La connexion à distance doit être configurée pour qu'elle utilise le(s) lecteur(s) de cartes à puce PC/SC présents sur le poste client (redirection carte à puce, PC/SC).

10Spécifications matérielles et prérequis

10.1 Architecture « serveur »

10.1.1 Composants

| Composant | Description | |
|-----------|---|--|
| COMP_01 | Un réseau informatique « Microsoft » : postes clients Windows (à partir de Windows 2000), intégrés à un domaine géré par un ou des contrôleur(s) de domaine Windows. | |
| COMP_02 | Au moins un serveur avec le rôle de contrôleur de domaine (Windows 2000 Server, 2003 Server ou supérieur) avec un Active Directory (gestion des utilisateurs). | |
| COMP_03 | Des contrôleurs de domaine secondaires peuvent être présents sur le domaine. Dans ce cas, la configuration spécifique au Smartcard logon devra être reproduite sur chaque contrôleur (pour que chaque contrôleur soit configuré de la même manière). | |
| COMP_04 | Composants d'une IGC (PKI) pour les certificats serveur et client : Un accès externe à l'annuaire de l'ASIP Santé (en http et/ou LDAP), pour permettre au module de vérification de révocation (« Provider de révocation ») d'accéder aux CRLs correspondantes aux certificats délivrés par l'ASIP Santé. Microsoft Certificate Server (pour une PKI serveur Microsoft) Provider de révocation ASIP Santé¹ développé par Microsoft pour la vérification des CRLs des certificats client de la carte sur chaque contrôleur de domaine. | |

Tableau 10 : Smartcard logon: Cinématique de l'authentification par carte à puce

¹ Dans l'IGC de l'ASIP Santé, l'autorité qui signe les certificats est différente de celle qui signe les CRL.



Figure 7 : Architecture: Exemple d'un réseau informatique configuré pour le Smartcard logon

10.1.2 PKI et Autorités de certification

Pour fonctionner, le mécanisme du Smartcard logon effectue une authentification mutuelle entre un poste client et le contrôleur de domaine, basé sur des certificats X509 : le client présente un certificat d'authentification contenu dans la carte, le serveur présente un certificat serveur authentifiant le contrôleur de domaine.

Pour vérifier l'authenticité du certificat client, le serveur vérifie notamment que la chaîne d'autorité de ce certificat est de confiance (Validité structurelle et temporelle du certificat, non révocation, autorités associées valides et non révoquées).

De même pour le client qui vérifie que la chaîne d'autorité du certificat serveur est de confiance.

Pour cela, il faut que chaque entité (client et serveur) possède un certificat associé à une PKI accessible à partir du/des contrôleur(s) de domaine et des postes client.

Lors de la procédure d'ouverture de session par carte à puce, et plus précisément lors de la vérification de la validité des certificats client et serveur (ainsi que leurs autorités), la vérification de la révocation doit être obligatoirement effectuée.

10.1.2.1 PKI cliente

Pour les cartes CPS, la PKI est gérée par l'ASIP Santé.

Les autorités de certification ainsi que les CDPs (point de distribution des CRLs) sont disponibles sur l'annuaire public de l'ASIP Santé.

Ces CRLs seront <u>obligatoirement</u> vérifiées par le composant « **provider de révocation ASIP Santé** » (**CPSRev**) installé sur chaque contrôleur de domaine. Ces vérifications ont lieu à chaque demande d'ouverture de session par un client. En cas d'échec du contrôle, l'utilisateur ne pourra pas ouvrir de session.

Il est possible - mais déconseillé - de désactiver la vérification des CRLs (voir section « **désactivation de la vérification des CRLs** » et annexe 6).

10.1.2.2 PKI serveur

En ce qui concerne la PKI du certificat serveur, plusieurs implémentations techniques sont possibles:

| Scénario | Description |
|----------|---|
| | PKI Microsoft |
| 1 | composant intégré à Windows 2000 Server, 2003 Server, 2008 Server, 2012 Server : Microsoft Certificate Server ou Active Directory Certificate Server (AD CS) (voir documentation spécifique pour l'installation et la configuration) |
| | PKI ASIP Santé |
| 2 | un certificat serveur généré (type DomainController) + sa chaîne de certification complète certifié par l'ASIP Santé (autorité Classe 4 par exemple (classe des certificats serveur)). Cette PKI est déjà utilisée pour les certificats client. |
| 3 | PKI externe |
| | un certificat serveur généré (type DomainController) + sa chaîne de certification complète de confiance (autre que ASIP Santé). |

Tableau 11 : Architecture: Scénarios d'implémentation de PKI serveur

Problématique:

- La chaîne de certification doit avoir des CDP (points de distribution de CRL) à tous les niveaux (certificat final + certificat AC intermédiaire).
 Ce n'est pas le cas de la chaîne du GIP-CPS classe 4.
 La vérification des CRLs étant obligatoire, l'utilisation d'une PKI externe basée sur les autorités de l'ASIP Santé (cas 2) semble impossible.
- Le **cas 3** reste possible mais est très fastidieux à mettre en place et à intégrer à l'infrastructure Microsoft. Cette option est donc déconseillée, sauf si une PKI existe déjà et est utilisée pour une autre fonction.
- La solution conseillée est donc le cas 1, c'est-à-dire d'utiliser la PKI de Microsoft (Microsoft Certificate Server ou AD CS), pour générer et administrer une PKI en local sur le réseau interne. Ce module s'intègre facilement et rapidement à l'infrastructure existante (serveurs Windows, Active Directory), et permet de configurer une PKI, et de générer un certificat serveur (contrôleur de domaine) en très peu de temps.

L'installation de Microsoft Certificate Server met en place et configure automatiquement toute une PKI par défaut, et donc notamment :

- La mise en place des CDPs par publication sur le réseau (accès par LDAP)
- la diffusion des autorités de certification sur toutes les machines du domaine.
- L'autorité d'enregistrement : génération très simple d'un certificat pour un contrôleur de domaine (un certificat serveur de type « Domain Controller » (DC))

10.1.2.3 Format d'un certificat « Domain Controller » (DC)

Ce certificat d'authentification installé sur un serveur de domaine permet l'authentification de ce serveur de domaine par un poste client.

Le certificat DC doit contenir les champs suivants:

- CDP (CRL Distribution Point).
- « Key usage » = Digital Signature, Key Encipherment
- « Application policies » =
 - -> Client Authentication (1.3.6.1.5.5.7.3.2)
 - -> Server Authentication (1.3.6.1.5.5.7.3.1)
- « Subject Alternative Name » =

-> GUID de l'objet contrôleur de domaine et nom DNS (= identifiant unique du serveur)

- CSP RSA Schannel pour générer la clé
- Gabarit de certificat = DomainController

Le sujet de l'objet doit être : CN =<dcname> (=le nom du contrôleur de domaine), pour pouvoir être publié dans l'Active Directory du contrôleur de domaine (pour retrouver le chemin de l'AD correspondant).

10.2 Architecture « client »

Une ouverture de session dite « interactive » (ouverture par carte à puce), n'est gérée en natif qu'à partir de Windows 2000. Les systèmes d'exploitation Windows XP, Vista, Seven et Windows 8 supportent ce mécanisme.

Peu de modifications sont donc nécessaires pour faire fonctionner le Smartcard logon.

Le présent paragraphe détaille les conditions requises pour utiliser une carte à puce CPS en ouverture d'une session Windows.

10.2.1 Matériel

- Au moins un lecteur de type PC/SC doit être installé (pilotes spécifiques installés) et présent sur le poste client, (le protocole PC/SC étant une architecture intégrée nativement dans l'OS et qui permet de prendre en compte l'insertion de la carte comme déclencheur de l'ouverture de session)
- Le poste client doit être connecté physiquement à un réseau privé et être déclaré sur un domaine de ce réseau.

L'authentification par carte à puce est une authentification forte établie obligatoirement entre un client et un serveur: une authentification locale sur le poste n'est pas possible.

<u>Remarque</u>: si ces deux prérequis ne sont pas respectés, l'écran d'accueil du poste client (GINA sous Windows XP) ne proposera pas l'insertion carte.

10.2.2 Logiciel

• La GINA (Graphical Identification and Authentication) d'origine.

Pour pouvoir ainsi gérer l'événement insertion carte. Toute autre GINA développée spécifiquement, désactivera la détection carte : par exemple une GINA de gestion biométrique d'empreinte digitale.

Ce pré requis est valable uniquement pour Windows 200 et XP.

A partir de Windows Vista, la GINA n'est plus modifiable, seuls des « credential provider » peuvent être ajoutés.

• Un CSP (Cryptographic Service Provider) d'interface standard et prévu pour dialoguer avec les cartes CPS doit être installé et correctement configuré, ainsi que les APIs correspondantes pour accéder à la carte via le lecteur. Ce CSP est fourni par l'ASIP Santé dans le setup MSI de la Cryptolib CPS à partir de la version 5 (ou en version PC/SC).

10.2.3 Cartes et certificats

Pour une utilisation en Smartcard logon, les certificats X509 d'authentification des cartes CPS doivent être de type « Smartcard logon » (SC), c'est-à-dire doivent posséder les champs suivants :

- « Extended Key Usage »
 (OIDs) = Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
- « Subject Alternative Name » = UPN = ID_user@carte-cps.fr (ID_user étant un identifiant unique du porteur)
- Un point de distribution de la liste de révocation (CDP) valide (adresse d'une CRL dans l'annuaire CPS pour une carte CPS)

Cet UPN sera l'identifiant unique du couple {porteur ; carte CPS} qui sera rattaché à un compte utilisateur du domaine Microsoft (voir Annexes pour la structure exacte des UPNs, ainsi que des exemples de script pour un déploiement dans l'Active Directory).

| Certificat | ? X Certificat ? X |
|--|---|
| Général Détails Chemin d'accès de certification | Général Détails Chemin d'accès de certification |
| Afficher : <a>Tout> | Afficher : <a>Tout> |
| Champ Valeur Identificateur de la clé du s f7 5f f2 64 ff f8 30 78 ed 21 0 Utilisation avancée de la clé Authentification du client (1.3 Contraintes de base [1]Stratégie du certificat : Ide Contraintes de base Type d'objet=Entité finale, Co Points de distribution de la li [1]Point de distribution de la lis Liste de révocation de certif [1]Liste de révocation de certi Autre nom de l'objet Autre nom :Nom principal=5.1 Autre nom de l'objet Authentification de client SSL (Authentification du client (1.3.6.1.5.5.7.3.2) Ouverture de session par carte à puce (1.3.6.1.4.1.311.20.2.2) | Champ Valeur Identificateur de clé de l'aut ID de la clé=49 02 5f 34 83 f2 Identificateur de la clé du s f7 5f f2 64 ff f8 30 78 ed 21 0 Utilisation avancée de la clé Authentification du client (1.3 Stratégies de certificat [1]Stratégie du certificat : Ide Contraintes de base Type d'objet=Entité finale, Co Points de distribution de la li [1]Point de distribution de la lis Liste de révocation de certif [1]Liste de révocation de certi Autre nom de l'objet Autre nom :Nom principal=5.1 Nom principal=5.18003000900039.WINLOGON01@carte-cps.fr |
| Modifi <u>e</u> r les propriétés <u>C</u> opier dans un fichier | Modifier les propriétés Copier dans un fichier |
| 40 | |
| Certificat | <u>? ×</u> |
| Général Details Chemin d'accès de certification | 1 |
| Afficher : <a>Tout> | |
| Champ Valeur Identificateur de clé de l'aut ID de la clé=49 02 5f 34 83 f2 Identificateur de la clé du s f7 5f f2 64 ff f8 30 78 ed 21 0 Utilisation avancée de la clé Authentification du client (1.3 Utilisation avancée de la clé Authentification du client (1.3 Stratégies de certificat [1]Stratégie du certificat : Ide Contraintes de base Type d'objet=Entité finale, Co Points de distribution de la li [1]Point de distribution de la lis Liste de révocation de certif [1]Liste de révocation de certi Autre nom de l'objet Autre nom :Nom principal=5.1 | |
| [1]Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : URL=http://annuaire.gip-cps.fr/crl/GIP-CPS CLASSE-3.crl [2]Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : URL=ldap://annuaire.gip-cps.fr/cn=gip-cps classe-3,ou=gip- cps structure,o=gip-cps,c=fr?certificaterevocationlist;binary | |
| ОК | |

Figure 8 : Exemple d'un certificat de type « Smartcard logon »

Pour qu'un certificat soit utilisable en « <u>ouverture de session par carte à puce</u> » (champ « utilisation avancée de la clé »), il faut qu'il « hérite » de ce rôle: son <u>autorité de certification doit posséder ce</u> <u>rôle</u> dans sa liste des utilisations avancées de la clé.

| Exemple d'un affichage correct des rôles d'ur son autorité de certification (ici GIP-CPS CLASS | n certifi SE-3) | cat « Smartca | rd logon ». Rôles qui sont autorisés par |
|--|-------------------------------------|---|---|
| Certificat Général Détails Chemin d'accès de certification Informations sur le certificat Ce certificat est conçu pour les rôles suivauts : • Garantit votre identité auprès d'un ordinateur distant • Ouverture de session par carte à puce Délivré à : 518003000900039/WINLOGON01 Délivré par : GIP-CP5 CLASSE-3 Valide à partir du 11/02/2009 jusqu'au 01/03/2012 | Certificat Général Certificat | ? × Détails Chemin of Informations certificat est consults utes les stratégies of | ? X f'accès de certification sur le certificat çu pour les rôles suivants : f'application |
| Installer le <u>c</u> ertificat | | Délivré à : Délivré par : Valide à partir d | 5IP-CPS CLASSE-3 5IP-CPS STRUCTURE Iu 01/12/2008 jusqu'au 01/01/2015 |
| | | | Déclaration de l'émetteur |
| Exemple des rôles de l'autorité de certification | n (ici GI | P-CPS CLASSE- | -3) d'un certificat « Smartcard logon » |

Figure 9 : Informations des certificats de type « Smartcard logon »

<u>Attention</u>: Cette autorité intermédiaire possédant toutes les stratégies d'application (ExtendedKeyUsage) doit être présente obligatoirement uniquement <u>coté serveur</u> (magasin des autorités intermédiaires et magasin NTAuth).

<u>Coté client</u>, aucune autorité n'est obligatoire (le Winlogon se base uniquement sur le magasin NTAuth alimenté par le serveur)

<u>Remarque</u>: les cartes CPS possédant des certificats compatibles « Smartcard logon » sont diffusées depuis mars 2011 (cartes « CPS3 »).

11Configuration

Cette partie donne les bases pour configurer les différents composants client et serveur décrits précédemment afin de mettre en place et d'administrer le Smartcard logon.

11.1 Configuration du poste client

Cf. Annexe pour des aperçus d'installation du poste de travail.

Les **composants logiciels nécessaires** sur le poste client sont:

- Les Cryptolib CPS v5 de l'ASIP Santé devront être installées
 - Le CSP de l'ASIP Santé, compatible avec le Smartcard logon, devra être installé.
 - Configuration en base de registres du mapping entre l'ATR d'une carte CPS et le CSP ASIP Santé permettant l'accès à la carte CPS.
 - (HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Cryptography/Calais/SmardCards)

La <u>Cryptolib CPS v5</u> apporte un nouveau CSP faisant abstraction des filières GALSS ou PC/SC : la Cryptolib CPS v5 adresse le lecteur PC/SC nécessaire pour le Smartcard logon directement en PC/SC même si le GALSS est présent.

Le Setup d'installation de cette version de la Cryptolib CPS installe l'ensemble des composants nécessaires au Smartcard logon: PKCS#11, CSP et configuration de la base de registres pour le Smartcard logon.

Il installe aussi l'ensemble des autorités de l'ASIP Santé (racine et intermédiaire) dans le magasin des certificats du poste client (non obligatoire pour l'ouverture de session par carte à puce).

Important : Sur les postes clients 64 bit, il est nécessaire d'installer les Cryptolib CPS x64

Une fois l'installation terminée, les erreurs carte à puces disparaissent. Il est alors utile de vérifier le magasin de certificat :

Démarrer > Rechercher Programmes et fichiers > inetcpl.cpl > entrer

En cliquant sur « **Contenu > Certificats** », les magasins apparaissent. Le Magasin « **Personnel** » contient les deux certificats carte d'authentification et de signature.

Il est utile d'identifier le certificat d'authentification et de noter l'UPN associé afin d'enrôler le certificat correctement coté serveur (voir document par ailleurs) :

| Certificates | | | | × | B Certificate |
|----------------------------|----------------------------|--------------------------|---------------------------------|------|---|
| ntended purpose: <a> | > | | | • | General Details Certification Path |
| Personal Other People | Intermediate Certification | Authorities Tru | sted Root Certificatior | | Certificate Information |
| Issued To | Issued By | Expiratio | Friendly Name | | |
| 00B1055421 | TEST CLASSE-1 | 29/02/2016 | <none></none> | _ | This certificate is intended for the following purpose(s): |
| 00B1055421 | TEST CLASSE-1 FDJ | 31/03/2016 08/05/2110 | <none> <none></none></none> | | Proves your identity to a remote computer Smart Card Logon |
| | | | | | Issued to: 0081055421 |
| Import Export. | . Remove | | Advar | iced | Issued by: TEST CLASSE-1 |
| Certificate intended purpo | ses | | | | Valid from 01/02/2013 to 29/02/2016 |
| Client Authentication, Sma | rt Card Logon | | | _ | $\ref{eq:product}$ You have a private key that corresponds to this certificate. |
| earn more about certificat | | | View | | Issuer Statement |
| | | | | | |
| | ок с | ancel A | | | ОК |

Figure 10 : Poste client: Vérifier le certificat d'authentification

| E Certificate | | | | |
|--|----------------------------------|--|--|--|
| General Details Certification Path | 1 | | | |
| et la | | | | |
| Suom: I <vii></vii> | | | | |
| Field | Value | | | |
| 🗊 Subject Key Identifier | 17 31 7c 1a 7b 2c 8e da 09 0a | | | |
| 🗊 Enhanced Key Usage | Client Authentication (1.3.6.1 | | | |
| Certificate Policies | [1]Certificate Policy:Policy Ide | | | |
| Basic Constraints | Subject Type=End Entity, Pat | | | |
| CRL Distribution Points | [1]CRL Distribution Point: Distr | | | |
| Freshest CRL | [1]Freshest CRL: Distribution | | | |
| Subject Alternative Name | Other Name:Principal Name=0 | | | |
| Netscape Cert Type | SSL Client Authentication (80) | | | |
| | | | | |
| Other Name: Principal Name=0.0B1055421@carte-cps.fr | | | | |
| Edit Properties Copy to File | | | | |
| | ОК | | | |

Figure 11 : Poste client: identifier l'UPN du certificat d'authentification

Dans cet exemple, l'UPN est 0.0B1055421@carte-cps.fr.

Cette vérification permet de vérifier les chaines de signatures : les certificats des chaines de certificats concernés par le parc de carte visé devront être correctement provisionnés coté serveur.

| 🚰 Certificate | × |
|---|---|
| General Details Certification Path Certification path TEST PROFESSIONNEL TEST CLASSE-1 00B1055421 | |
| View Certificate | |
| Certificate status: | |
| This certificate is OK. | |
| Learn more about <u>certification paths</u> | |
| ОК | |

Figure 12 : Poste client: identifier l'UPN du certificat d'authentification

Les certificats d'autorité client (racine et intermédiaire), ainsi que l'autorité racine du serveur, devront être présents dans **le magasin NTAuth** du poste client (propagé exclusivement par le contrôleur de domaine principal (PDC), lors de l'ajout du poste client au domaine, puis régulièrement).

11.2 Configuration Serveur allégée

Cf. Annexe pour des aperçus d'installation d'un serveur Windows 2008R2 Server.

Afin de s'approprier les tâches de paramétrage liées à la configuration de la fonction de Smartcard logon, il est utile d'installer un unique serveur offrant les fonctionnalités suivantes :

- Active Directory (sans DNS, si un DNS est déjà présent sur le réseau local!)
 <u>Cf. annexe d'installation d'un rôle Active Directory</u>
- Certificate Serveur
 - o <u>Cf. annexe d'installation d'un rôle Certificate Server (« AD CS »)</u>
- Remote desktop (facultatif mais utile)
 Cf. annexe d'installation d'un rôle Remote Desktop
- IIS (facultatif mais utile)
 - o Cf. annexe d'installation d'un rôle IIS

11.3 Configuration d'un contrôleur de domaine

Cf. Annexe pour des aperçus d'installation d'un serveur Windows 2008R2 Server.

Les postes clients devant être déclarés sur un domaine du réseau, au moins un contrôleur de domaine doit être présent sur le réseau interne.

Les systèmes d'exploitation possibles pour un contrôleur de domaine sont:

- Windows 2003R2 SP1 Server
- Windows 2008R2 SP1 Server
- Windows 2012

Les rôles installés sur le(s) serveur(s) de domaine sont:

- contrôleur de domaine basé sur Active Directory de Microsoft
 - Tout autre annuaire d'identification réseau peut être utilisé, mais la configuration du Smartcard logon sera beaucoup plus complexe

Cf. annexe d'installation d'un rôle Active Directory

Sur le contrôleur primaire (PDC – Primary Domain Controller):

→ Ajout des autorités racine (de confiance) client et serveur à la stratégie de groupe du domaine.

(par interface graphique : Outils d'administration -> Stratégie de sécurité du domaine -> Paramètres de sécurité -> Stratégie de clés publique -> Autorité de certification racines de confiance -> importer)

 → Ajout des autorités racine (de confiance) et intermédiaire au container NTAuth d'Active Directory, dans le but de diffuser ces autorités aux machines déclarées sur le domaine (pour permettre une vérification du certificat serveur par les postes client).
 En fonction de la version du serveur, cette opération se fera soit par fichiers de script

(Windows 2000 Server), soit par interface graphique (à partir de Windows 2003 Server)

Sur chaque contrôleur (primaire et secondaires, si présents):

- → Installation du provider de révocation de l'ASIP Santé (pour vérifier que les CRLs correspondant à la chaîne de certification du certificat client sont non révoquées) Ce provider peut être récupéré à l'adresse suivante : <u>http://www.microsoft.com/france/interop/ressources/gip-cps.aspx</u>
- → Ajout des autorités racine et intermédiaires dans les différents magasins correspondants (voir le document d'installation/configuration du provider de révocation de l'ASIP Santé), pour permettre au provider de révocation de vérifier la validité des CRLs.

Cf. annexe d'installation du provider de révocation ASIP Santé

Cf. annexe de configuration du Contrôleur de domaine (certificats)

Cf. tableau 11 et tableau 12, ci-après, récapitulatifs des étapes d'installation et de configuration dans un scénario d'implémentation de serveur « allégé »

Il est aussi nécessaire de rattacher les comptes utilisateur à leurs cartes CPS respectives.

Dans Active Directory, pour chaque compte utilisateur du domaine, on rajoutera l'**UPN de la carte CPS** associé à ce compte au champ **« nom d'ouverture de session de l'utilisateur »** (une seule carte possible par compte).

| Login du couple login/password standard du compte | | | |
|--|--|--|--|
| Suffixe de l'UPN de la carte à associer à ce compte | | | |
| Préfixe de l'UPN de la carte à associer à ce compte | | | |
| Propriétés de user1 | | | |
| Environnement Sessions Contrôle à distance Profil de services Termina Server 0 DM+ Général Adresse Compte P ofil Téléphones Organisation Membre de Appel entrant Nom d'ouverture de session de lutilisateur : 5.18003000900039.WINLOGON01 @carte-cps.fr Image: Compte de session de l'utilisateur (antérieur à <u>W</u> indows 2000) : Image: Compte de session de l'utilisateur (antérieur à <u>W</u> indows 2000) : GIP-CPS\ user1 Image: Compte de session Se connecter à | | | |
| Le compte est <u>v</u> errouillé Options de compte : | | | |
| | | | |
| Image: Complete complete Image: Complete< | | | |
| OK Annuler Appliquer | | | |
| Option sélectionnée pour une ouverture de session exclusivement par carte à puce | | | |

Figure 13 : Active Directory: Smartcard logon : Configuration d'un compte utilisateur

Cf. annexe de configuration du poste de travail (vérification des UPNs)

Cf. annexe de configuration du Contrôleur de domaine (certificats et utilisateur)

Si le suffixe de l'UPN n'apparait pas dans la liste des noms de domaines connus, une relation d'approbation avec le domaine existant devra préalablement être créée:

Outils d'administration -> Domaines et approbations Active Directory.

Pour ajouter une approbation au domaine existant :

| Somaines et approbations Active Directory | |
|--|--|
| Eichier Action Affichage 2 → ▲ ▲<!--</td--><td>Propriétés de Domaines et approbations Active Directory Image: Comparison of the second s</td> | Propriétés de Domaines et approbations Active Directory Image: Comparison of the second s |
| | |

Figure 14 : Active Directory: Approbation du suffixe UPN « carte-cps.fr »

<u>Remarque</u>: le nom de domaine DNS « **carte-cps.fr** » a été réservé par l'ASIP Santé.

11.4 Configuration du serveur de certificats (PKI Microsoft)

Ce chapitre explique comment installer/configurer une PKI Microsoft avec le composant Microsoft Certificate Server.

Certificate Server est un composant gratuit intégré aux versions Server de Windows. Comme expliqué précédemment, il pourra donc être installé sur une machine serveur présente sur le domaine. Il peut être installé directement sur le serveur faisant office de contrôleur de domaine (par exemple, dans le cas d'un petit réseau, qui ne peut pas dédier un serveur à cette tâche uniquement).

Il est cependant préférable pour des raisons :

- 1. de sécurité
- 2. de fiabilité du réseau

de l'installer sur une autre machine du domaine, qui sera dédiée à ce rôle.

L'installation de Certificate Server sur un serveur le « gèle »: il est ensuite impossible de modifier son nom ou son domaine tant que ce composant est installé.

<u>Procédure d'installation</u> : « Panneau de configuration -> Ajout/suppression de programmes -> Ajouter/Supprimer des composants -> Service de certificats (PKI Microsoft) »

L'installation se déroule automatiquement. Durant cette installation, il sera demandé de générer l'autorité racine de cette PKI :

- **Type d'autorité** : obligatoirement : autorité racine d'entreprise (pour permettre la propagation automatique de cette autorité sur toutes les machines du domaine)
- **Nom commun et période de validité de l'autorité** : à définir en fonction de la politique de sécurité du réseau informatique local.

Cf. annexe d'installation d'un rôle Certificate Server (« AD CS »)

Une fois l'autorité de certification générée et l'installation terminée, cette autorité est automatiquement déployée sur toutes les machines du domaine.

Il ne reste plus ensuite qu'au contrôleur de domaine à faire une demande de certificat serveur de type DC (Domain Controller), auprès de cette autorité.

(Au reboot du contrôleur de domaine : inscription automatique auprès de la PKI du domaine, et demande automatique d'un certificat serveur DC)

Ce serveur hébergeant la PKI devra être en permanence accessible via le réseau par protocole LDAP depuis toutes les autres machines qui veulent vérifier la non-révocation du certificat serveur et depuis son autorité.
11.5 Configuration des options de sécurité

Ce chapitre explique quelques réglages de base du Smartcard logon pour une meilleure sécurité du domaine géré.

11.5.1 Forcer l'utilisation de la carte à puce

Par défaut, un compte configuré pour ouvrir une session par carte à puce, pourra aussi ouvrir une session par login/mot de passe.

Pour augmenter la sécurité du réseau, il sera recommandé d'imposer l'ouverture de session uniquement par carte à puce.

Pour cela, 2 possibilités :

- Soit à partir d'un compte utilisateur : sélection de l'attribut « Carte à puce nécessaire pour ouvrir une session interactive ». Dans ce cas, le mot de passe du compte utilisateur sera modifié automatiquement à une valeur inconnue.
- Soit par stratégie de groupe (secpol.msc) : « Paramètres de sécurité locaux -> Stratégie locale -> Options de sécurité -> Interactive Login : Smart Card Required »
 - Valeur : activated

Requiert au minimum Windows XP SP2 pour les postes client. Ne modifie pas le mot de passe du/des compte(s) utilisateur impacté(s) par la stratégie.



Figure 15 : Forcer l'utilisation de la carte à puce par stratégie locale

Attention: l'utilisation de cette stratégie impacte tous les comptes, dont les comptes administrateurs, qui auront besoin d'une carte à puce pour se logger

11.5.2 Comportement du système au retrait de la carte à puce

Par défaut, à l'extraction de la carte à puce du lecteur pendant une session, aucune action n'est réalisée.

Mais pour plus de sécurité, il est possible de configurer le comportement de la session sur cet évènement d'arrachage de carte :

Par stratégie de groupe : « Paramètres de sécurité locaux -> Stratégie locale -> Options de sécurité - > Comportement lorsque la carte est retirée »

- Aucune action.
- Verrouille session (verrouillage de la session).
- Force Logout. (fermeture de la session).

11.5.3 Forcer l'approbation du contrôleur de domaine à l'ouverture de session

Par défaut, si le contrôleur de domaine est injoignable ou indisponible, une session cliente peut être ouverte même sans réponse du serveur, en utilisant les informations de session mises en cache.

Ceci est valable aussi bien en ouverture de session par login/password qu'en ouverture de session par carte à puce.

Les informations de la dernière session ouverte sont alors utilisées, ce pour un certain nombre d'ouvertures de session sans contrôleur de domaine, défini par stratégie de groupe.

Il est possible de modifier ce comportement en forçant l'approbation du serveur de domaine à chaque ouverture de session, par stratégie de groupe :

« Paramètres de sécurité du contrôleur de domaine -> options de sécurité -> ouverture de session interactive -> nécessite l'authentification par le contrôleur de domaine pour le déverrouillage... -> Activé »

Attention: dans ce cas, si le serveur est injoignable, la session ne pourra pas s'ouvrir.

11.5.4 Désactivation de la vérification des CRLs

A partir de Windows 2008 server, il est possible de désactiver la vérification des CRLs des certificats carte et serveur et donc de ne pas utiliser de provider de révocation.

Cette option est déconseillée car elle diminue le niveau de sécurité du SI (pas de vérification sur l'état de révocation des cartes utilisées) mais elle peut être utile, par exemple :

- 1. dans le but de faciliter les tests
- 2. pour valider des architectures réseau (qui n'ont pas forcement d'accès externes pour la récupération des CRLs)

Voici les clés à ajouter en base de registres, sur le(s) contrôleur(s) de domaine (contenant le KDC):

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters] Clé : "UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors" = (type:dword) valeur : 1

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kdc] clé : "UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors" = (type:dword) valeur : 1

Tableau 12 : CPSRev : désactivation de la vérification des CRLs

Il suffit de repasser les valeurs des clés à 0 pour réactiver la vérification des CRLs.

Aucun redémarrage du serveur concerné n'est nécessaire pour la prise en compte des modifications.

11.6 Exemple pratique d'une configuration de serveur

Cf. aperçus écran en annexe.

Conseils:

- ⇒ imprimer ces 2 tableaux
- ⇒ imprimer les aperçus en annexe
- ⇒ annoter les impressions papier au fur et à mesure de l'avancement
- ⇒ faire des impressions d'écrans
- ⇒ alimenter le dossier d'exploitation

Exemple de procédure de configuration minimale d'un contrôleur de domaine pour une utilisation Smartcard logon:

| Installation | Windows 2008 Server | | Windows 2003 Server |
|---|---|--|-----------------------------------|
| | Inst <u>Cf. a</u> <u>du p</u> | allation du provider de révocation annexe pour aperçus d'installation et documentation provider | |
| | 1 | Lancement de l'installeur CPSRevSetup.msi | |
| | 2 | configuration de la base de registres | |
| | 3 | configuration des magasins de certificats | Identique Windows 2008 |
| Providor do | 4 | En cas de contrôleurs de domaine multiple : installation sur chaque contrôleur | Remarque : le journal |
| révocation | 5 | Accès internet requis pour récupération des CRLs | CPSRev se trouve |
| | Véri | ification | directement dans l'observateur |
| | Journal « CPSRev » installé dans l'observateur 1 d'événements »-> « journaux des applications et des services » | | d'événements. |
| | 2 | commande certutil -verify cert.cer | |
| | 3 | commande certutil -pulse (cert.cer = certificat d'authentification d'une carte CPS) | |
| | Inst | allation de AD CS sur le contrôleur de domaine, ou sur | |
| | un a | autre serveur du domaine. | |
| | <u>Ct. a</u> | annexe pour aperçus d'installation | |
| Service de certificats (IGC Microsoft) | 1 | Gestionnaire de serveur-> Rôles -> Ajouter des rôles -> Service de certificats Active Directory (PKI Microsoft) | |
| | 2 | Génération du certificat racine (choisir « autorité racine d'entreprise ») | Identique Windows 2008 |
| | 3 | génération du certificat serveur DC. (généré automatiquement lors de l'installation de la PKI, sur tous les contrôleurs de domaine du domaine) | |
| | 4 | Reboot du serveur + contrôleur(s) de domaine. | |

Tableau 13 : Serveur: Installation du serveur

| Configuration | Windows 2008 Server | | Windows 2003 Server | |
|--|--|--|---|--|
| | Ajout des autori stratégie de gro | tés racines client et serveur à la upe du domaine | Ajout des autorités racines client et serveur : | |
| Configuration | Cf. annexe pour aperçus de configuration | | => Outils d'administration -> Stratégie de sécurité du domaine -> paramètres de sécurité -> Stratégie de clés publique -> Autorité de certification racine de confiance -> importer | |
| de la stratégie de groupe du domaine. | commande MMC -> Stratégie Default Domain Controllers policy -> Configuration ordinateur -> paramètres Windows -> Paramètres de sécurité -> Stratégie de clés publique -> Autorité de certification racines de confiance -> importer. | | | |
| | Ajout des certifi intermédiaire) + NTAuth. | cats d'autorités client (racine + · serveur (racine) dans le magasin | | |
| Configuration du | Cf. annexe pour | aperçus de configuration | Identique Windows 2008 installation préalable de Rktools pour Windows 2003, pour avoir le module PKIView (enterprise PKI) | |
| container NTAuth (Active Directory) | commande MM conteneurs Activ NTAuthCertifica | C -> PKI d'entreprise -> gérer les /e Directory -> Conteneur tes -> Ajouter | | |
| | Vérification | | | |
| | commande Certutil -viewstore -enterprise NTAuth | | | |
| | Configuration de serveur | es magasins de certificats du | | |
| | Cf. annexe pour | aperçus de configuration | | |
| | Commande MMC -> certificats -> ordinateur local | | | |
| | Magasin Personnel | certificats racine ASIP certificat du contrôleur de domaine émis par l'AD CS | | |
| Configuration des magasins de certificats du serveur. | Magasin Autorités de certification racine de confiance | certificats racine ASIP certificat du contrôleur de domaine émis par l'AD CS | Identique Windows 2008 | |
| | Magasin | certificats client racine (signeur de CRL) | | |
| | Autorités intermédiaires | certificats intermédiaires : client signeur de certificats et CRLs | | |
| | en cas de contrôleurs de domaine multiple : installer ces certificats sur chaque contrôleur | | | |

| Configuration | Windows 2008 Server | Windows 2003 Server | |
|---|--|---|--|
| Création | Ajouter dans la liste le suffixe de l'UPN de la carte CPS | Identique Windows 2008 | |
| d'une relation d'approbation pour le suffixe UPN | Outils d'administration -> Domaine et 1 approbations AD -> Clic Droit -> Propriétés -> Suffixes UPN | | |
| des cartes CPS. | Ajouter dans la liste le suffixe de l'UPN de la carte CPS. (« carte-cps.fr » pour les cartes CPS compatible Smartcard logon) | | |
| | Attacher l'identifiant de la carte CPS (l'UPN présent dans le certificat d'authentification de la carte CPS) à un compte utilisateur Active Directory | | |
| Configuration d'un | 1 Ouvrir les propriétés d'un compte utilisateur du domaine. | | |
| compte utilisateur sur Active Directory | 2 Onglet Compte : dans le champ « nom d'ouverture de session de l'utilisateur » : ajouter l'UPN de la carte à associer à ce compte. | Identique Windows 2008 | |
| | Vérification | | |
| | le suffixe de l'UPN, créé auparavant par relation d'approbation, apparaît dans la liste des suffixes | | |
| | Test de la configuration | | |
| | 1 Configuration poste client minimal : un lecteur PC/SC + son driver + Cryptolib CPS v5 | Identique Windows 2008 | |
| Test de la configuration | Exécuter sur le contrôleur de domaine : certutil -pulse pour propager les autorités et stratégies sur les postes clients. | au lieu de certutil -pulse installer Dsstore pour Windows | |
| | 3 Redémarrer une machine cliente, et tester l'ouverture de session par carte CPS. | | |

Tableau 14 : Serveur: Configuration

11.7 Exemples d'architecture réseau

Exemple d'une architecture réseau « évoluée » : un client sur un domaine A, se connecte à distance sur un domaine B via un canal VPN sur un serveur TSE (ou CITRIX), via une carte CPS.



Figure 16 : Architecture : Exemple d'architecture réseau évoluée

12Annexes

Ces annexes présentent la mise en œuvre simplifiée du Smartcard logon avec une carte CPx (maquette).

Cette maquette a pour principaux intérêts :

- 1. de démontrer la configuration de tous les éléments nécessaires au Smartcard logon avec une carte CPx
- 2. de le prendre en mains complètement
- 3. de déterminer s'il correspond ou non aux besoins effectifs de l'entreprise.

L'entreprise pourra à cette occasion en profiter pour faire un bilan

- 1. de son SI
- 2. de son référentiel documentaire
- 3. de ses compétences/connaissances internes relatives aux cartes de santé, à la sécurité et à la PKI

12.1 Maquette de Smartcard logon avec une carte CPx

12.1.1 « Brief Project »

| Clé | Valeur | | |
|-----------|---|---|--|
| Nom | Projet « maquette » de Smartcard logon avec une carte CPx | | |
| | 1 | Prendre en main le Smartcard logon | |
| | 2 | Mesurer la pertinence du cas d'usage dans le contexte particulier de l'entreprise | |
| | 3 | Affiner l'expression de besoin | |
| Objectifs | 4 | Tester les réactions utilisateurs | |
| | 5 | Tirer un bilan sur l'état du SI : états des DEX / DAT / PCA, adéquation des niveaux de sécurité requis vs. Implémentés, bilan des flux | |
| | 6 | Monter en compétence les équipes sur la PKI Microsoft et les composants matériels et logiciels ASIP Santé | |

Tableau 15 : « Brief Project » « maquette de Smartcard logon avec une carte CPx »

12.1.2 Ressources nécessaires

| Ressource | Rôle | Profil | Implication | |
|-----------------|---|--|------------------------|--|
| MANAGEMENT_1 | Donne son aval au projet | DSI / RSSI | 0,5 jours | |
| | Collecte les différents documents d'architecture existants | | 7,0 jours | |
| | Prend connaissance du guide | | | |
| | Ecrit l'expression de besoin | | | |
| | Ecrit le scénario de démonstration | | | |
| PROJET_1 | Veille aux jalons | Chef de projet | | |
| | Assure la cohérence des tests | | | |
| | Organise la démonstration | | | |
| | Met à jour les documents d'architecture existants | | | |
| | Ecrit et rapporte le « project learning » | | | |
| INTEG_CLIENT_1 | Installe et configure 1 ou 2 postes clients, reflet des postes de travail de l'entreprise | Technicien poste de travail Windows connaissant le poste de travail | 2,0 jours | |
| | Teste unitairement ses installations. | Santé&Social | | |
| INITED SEDVED 1 | Installe et configure la partie serveur. | Ingénieur Système pré | 6,0 jours 3,0 jours | |
| INTEG_SERVER_I | Teste unitairement ses installations. | sensibilisé à la PKI. | | |
| DEVEL SERVER 1 | En fonction de l'expression de besoin, automatise les tâches d'édition de l'annuaire de l'entreprise pour l'adapter au Smartcard logon. | Ingénieur développement idéalement | | |
| | A défaut : identifie et documente les développements nécessaires. | C#/PowerShell connaissant Active Directory et LDAP | | |
| | Teste unitairement ses développements. | , , | | |
| | Ecrit le plan de test fonctionnel | | 2,0 jours | |
| | Passe le plan de test | Testeur connaissant | | |
| QA_1 | Donne son aval pour la démonstration (qualité suffisante, adéquation avec l'expression de besoin). | les usages poste de travail Santé&Social | | |

Tableau 16 : Ressources « maquette de Smartcard logon avec une carte CPx »

12.1.3 Livrables

| # | Livrable | Responsable |
|---|---|----------------|
| 1 | Expression de besoins | PROJET_1 |
| 2 | Spécifications / Scénario de démo | PROJET_1 |
| 3 | Cahier de tests unitaires DEV | INTEG_SERVER_1 |
| 4 | Cahier de tests « Assurance Qualité » (« QA ») | QA_1 |
| 5 | Maquette | PROJET_1 |
| 6 | Dossier d'Architecture Technique (DAT) Maquette (config. Poste de travail utilisé, versions de composants serveurs et client, flux, IP,) | PROJET_1 |
| 7 | Spécifications des développements réalisés ou à réaliser | DEVEL_SERVER_1 |
| 8 | Analyse de gaps sur les documents suivants : Dossier d'Architecture Technique (DAT) Dossier d'exploitation (DEX) Plan de Continuité d'Activité (PCA) | PROJET_1 |
| 9 | Bilan projet (avec Pros&Cons, limitations identifiées documentées, besoins en développements identifiés et évalués) | PROJET_1 |

Tableau 17 : Livrables « maquette de Smartcard logon avec une carte CPx »

12.1.4 Macro-Planning

| Jalon | Description | Valeur |
|-------|---|------------------|
| т0 | Date de début | (ici 10/02/2014) |
| T1 | Début de l'intégration (Spécifications et cahiers de tests validés) | T0 + 7j |
| т2 | Début des tests « Assurance Qualité » (Q&A) | T0 + 15j |
| Т3 | Début Démo et project learning | T0 + 17j |
| Т4 | Date de fin | T0 + 20j |

Tableau 18 : Macro-planning « maquette de Smartcard logon avec une carte CPx »



asipsanté

Figure 17 : Macro-planning « maquette de Smartcard logon avec une carte CPx »



12.1.5 Remarques

Remarques Ces éléments sont donnés à titre indicatif. Ils correspondent aux retours d'expérience de l'ASIP Santé sur le sujet. Ils sont fournis pour aider à la décision et pour éviter les déconvenues. 1 Ils n'engagent en aucune manière l'ASIP Santé quant à la réussite du projet (techniquement, en coûts ou en délais). Chacun verra, au final, midi à sa porte afin de mener à bien ce projet. 1. Le temps passé en spécification 2. La charge de travail du chef de projet Sont proportionnellement plus importants que sur un projet d'intégration classique du fait de 2 la nature du projet et de ses objectifs : bilan de l'existant • organisation de la démo en elle-même et project learning o i.e. composition des pièces qui alimenteront le projet définitif La charge de travail de chacun peut augmenter ou diminuer en fonction des profils finalement 3 retenus. Les rôles peuvent être confondus (ex. PROJET_1 et INTEG_SERVER_1, ou INTEG_SERVER_1, DEVEL SERVER 1 et INTEG CLIENT 1). Il est cependant recommandé de garder un testeur 4 (QA 1) indépendant, afin de garantir la qualité du démonstrateur et l'intérêt pour le management d'assister à la démo (prise de décision possible). S'agissant d'une maquette, les durées indiquées incluent la recherche de machines physiques disponibles pour la maguette mais n'incluent pas les temps passés en recherche de licences ou 5 en passage de commandes par exemple. Aucun temps de VSR/VABF, aucune tâche de support, aucune re-livraison ne sont inclus. La suite du document détaille les étapes de configuration à effectuer 6

Tableau 19 : Remarques « maquette de Smartcard logon avec une carte CPx »

12.2 Installation du poste de travail client

Lorsque les Cryptolib CPS ne sont pas installées sur le poste client, les fenêtres de login signalent une erreur de carte à puce:

| Windows Securit | γ | × |
|------------------------------------|---|---|
| Enter your cre These credential | edentials Is will be used to connect to cosign. | _ |
| | florent.desgrippes | |
| | Use another account | |
| | Smart card error The card supplied requires drivers that | |
| 🗌 Remer | mber my credentials | |
| | OK Cancel | |

Figure 18 : Poste client : Erreur de carte à puce sur un login TSE si les Cryptolib CPS ne sont pas installées

<u>Important</u>: Seule la version <u>Full PC/SC</u> de la <u>Cryptolib CPS v4</u> permettait de gérer le Smartcard logon avec des cartes CPS. La <u>Cryptolib CPS v5</u> apporte un nouveau CSP faisant abstraction des filières GALSS ou PC/SC : la Cryptolib CPS v5 adresse le lecteur PC/SC nécessaire pour le Smartcard logon directement en PC/SC, sans passer par le GALSS. L'insertion de la carte CPS dans un lecteur de type PC/SC reste requis (pas de drivers PC/SC, requis, pour les lecteurs PSS).

Important : Sur les postes clients 64 bit, il est nécessaire d'installer les Cryptolib CPS x64

| 🚰 Composants Cryptographiques CPS | 5 v5.0.6 (x64) | | × |
|--|--------------------------------------|---------------|------------------|
| Bienvenue dans l'assistant d' Composants Cryptographique | installation des es CPS v5.0.6 (x | 64). | asipsanté |
| L'assistant d'installation va installer les C votre système. Pour continuer, diquez s | Composants Cryptogi sur Suivant. | raphiques CPS | v5.0.6 (x64) sur |
| | | | |
| | | | |
| | | | |
| InstallShield | < Précédent | Suivant > | Annuler |

Figure 19 : Poste client : Installation Cryptolib CPS x64

| 🙀 Composants Cryptographiques CPS | v5.0.6 (x64) | | × |
|---|--|-------------------------------------|--------------|
| Type d'installation | | • | asipsanté |
| Sélectionnez le type d'installation voulu. | | | |
| Veuillez sélectionner un type d'installatio | n. | | |
| Installation standard | | | |
| Permet d'installer toute maximum en espace dis | s les fonctions du que.) | programme. (Be | soins |
| Installation personnalisée | | | |
| Permet d'effectuer une l'emplacement cible des plus expérimentés. | installation sélecti fonctions choisies | ve et de définir . S'adresse aux | utilisateurs |
| InstallShield | | | |
| | < Précédent | Suivant > | Annuler |

Figure 20 : Poste client: Installation Cryptolib CPS x64 : installation perso avec la filière CPS2Ter Full PC/SC

| 🖶 Composants Cryptographiques CPS v5.0.6 (x64) | X |
|---|---|
| Sélectionnez les fonctions du programme que vous souhaitez | installer. |
| Pour modifier les paramètres d'installation d'une fonction, dique | Description de la fonction Installation des composants cryptographiques de la carte CPS2ter utilisant la couche PC/SC. Cette fonction nécessite 3949ko d'espace disque. |
| InstallShield | Suivant > Annuler |

Figure 21 : Poste client: Installation Cryptolib CPS x64 : installation perso avec la filière CPS2Ter Full PC/SC

| 🔂 Composants Cryptographiques CP5 v5.0.6 (x64) | × |
|---|-----------------------------|
| L'installation du programme peut commencer | asipsanté |
| Cliquez sur Installer pour commencer l'installation. Pour revenir au début de l'installation, diquez sur Précédent. Pour quitter installer le programme, diquez sur Annuler. Merci de quitter les applications utilisant les Composan Cryptographiques CPS (navigateurs, logiciels médicaux | ľassistant sans ts). |
| InstallShield < Précédent 💮 Installer | Annuler |

Figure 22 : Poste client : Installation Cryptolib CPS x64 : Installer

Si l'UAC est activée sur le poste, il faut accepter l'installation du MSI fourni par l'ASIP Santé :

| 5' | دی <mark>ہے۔</mark> الا (| mposani | ts Crypto n doc Co r Account | graphiques CPS v managemente Countro Control | /5.0.6 (x64) | | acipo | |
|-------|---------------------------------|---------|------------------------------------|--|--|-----------------------------|-----------------------|---------|
| n | | 2 | Do you v compute | want to allow the er? | following pro | gram to insta | ll software o | on this |
| | Ī | | | Program name: Verified publisher: | 47bf1b.msi AGENCE NAT INFORMATIO | IONALE DES S ON PARTAGES | YSTEMES D DE SANTE | |
| μ | | | | File origin: | Hard drive on t | his computer | | |
| ta | | • | Show deta | ils | | Yes | No | _ |
| 1 | | | | | <u>Chang</u> | e when these n | otifications | appear |
| | Install | Shield | | | | , | | |
| | | | | | < Précédent | Suivant > | Anr | nuler |

Figure 23 : Poste client: Installation Cryptolib CPS x64 : Fenêtre d'UAC

Certains antivirus peuvent nécessiter des acquittements :



Figure 24 : Poste client : Installation Cryptolib CPS x64 avec AVAST

Une fois l'installation terminée, les erreurs carte à puces disparaissent :

| Windows Securit | Vindows Security | | | | |
|-----------------------------------|--|--|--|--|--|
| Enter your cre These credentia | edentials Is will be used to connect to cosign. | | | | |
| | florent.desgrippes | | | | |
| | Use another account | | | | |
| | 00B1055421 Smart card credential 0.0B1055421@carte-cps.fr PIN | | | | |
| Reme | mber my credentials | | | | |
| | OK Cancel | | | | |

Figure 25 : Poste client : Driver carte à puce OK sur un login TSE (les Cryptolib CPS sont installées)

Vérifier le magasin de certificat :

« Démarrer > Rechercher Programmes et fichiers > inetcpl.cpl > entrer »

| Internet Properties | | | | | | |
|--|--|--|--|--|--|--|
| General Security Privacy Content Connections Programs Advanced | | | | | | |
| Family Safety | | | | | | |
| Control the Internet content that can Pamily Safety be viewed. | | | | | | |
| Certificates | | | | | | |
| Use certificates for encrypted connections and identification. | | | | | | |
| Clear SSL state Certificates Publishers | | | | | | |
| AutoComplete | | | | | | |
| AutoComplete stores previous entries Settings for you. | | | | | | |
| Feeds and Web Slices | | | | | | |
| Feeds and Web Slices provide updated Settings content from websites that can be read in Internet Explorer and other programs. | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| OK Cancel Apply | | | | | | |

Figure 26 : Poste client : Vérifier le magasin de certificats

Identifier le certificat d'authentification et noter l'UPN

« Contenu > Certificats > Magasin Personnel »

| 🖬 👍 🖼 🖳 🗸 🦊 🔛 I at 💷 📭 💙 I | ····································· | 100 % Y 🕑 斗 Kead 👳 | | | | |
|---|--|--|--|--|--|---------------------------------------|
| Certificates | | Certificate | | | | |
| Intended purpose: <a>All> | T | General Details Certification Path | | | | |
| Personal Other People Intermediate Certit | fication Authorities Trusted Root Certification | Certificate Information | | | | |
| Issued To Issued By | Expiratio Friendly Name | This certificate is intended for the following purpose(s): | | | | |
| GRUUDB 1055421 TEST CLASSE-1 GRUUDB 1055421 TEST CLASSE-1 GRUUDB TEST C | 31/03/2016 <none> 31/03/2016 <none> 08/05/2110 <none> A 05/01/2013 3fd5c5aa29b7c5</none></none></none> | Proves your identity to a remote computer Smart Card Logon | | | | |
| | | Issued to: 00B1055421 Issued by: TEST CLASSE-1 | | | | |
| Certificate intended purposes | Auvanceu | Valid from 01/ 02/ 2013 to 29/ 02/ 2016 | | | | |
| Client Authentication, Smart Card Logon View Learn more about certificates Close | | | | | | |
| | | | | | | OK Cancel Apply te stores previous en |

Figure 27 : Poste client : Vérifier le certificat d'authentification

| 🚼 Certificate | × | | | | |
|--|----------------------------------|--|--|--|--|
| General Details Certification Path | 1 | | | | |
| | | | | | |
| Show: <all></all> | | | | | |
| | | | | | |
| Field | Value | | | | |
| Subject Key Identifier | 17 31 7c 1a 7b 2c 8e da 09 0a | | | | |
| Enhanced Key Usage | Client Authentication (1.3.6.1 | | | | |
| Certificate Policies | [1]Certificate Policy:Policy Ide | | | | |
| Basic Constraints | Subject Type=End Entity, Pat | | | | |
| CRL Distribution Points | [1]CRL Distribution Point: Distr | | | | |
| Freshest CRL | [1]Freshest CRL: Distribution | | | | |
| Subject Alternative Name | Other Name:Principal Name=0 | | | | |
| i interscape Cert Type | SSL Client Authentication (80) | | | | |
| Other Name: Principal Name=0.0B1055421@carte-cps.fr | | | | | |
| Edit Properties Copy to File | | | | | |
| | ОК | | | | |

Figure 28 : Poste client : identifier l'UPN du certificat d'authentification

Dans cet exemple, l'UPN est <u>0.0B1055421@carte-cps.fr</u>.

Vérifier les chaines de signatures : les certificats des chaines de certificats concernés par le parc de carte visé devront être correctement provisionnés coté serveur.

| 🖥 Certificate | × |
|---|---|
| General Details Certification Path | _ |
| Certification path | |
| View Certificate | |
| Certificate status: | |
| This certificate is OK. | |
| Learn more about <u>certification paths</u> | |
| ОК | |

Figure 29 : Poste client : identifier l'UPN du certificat d'authentification

Conseil : pour les postes clients Win7 d'un parc, il est conseillé de

- 1. désactiver la rechercher automatique de drivers de cartes à puces
- 2. de maitriser la politique de mises à jour Windows Update des postes



Figure 30 : Poste client : Périphériques et imprimantes : Paramètres d'installation de périphériques et Windows Update

12.3 Installation de Windows 2008 R2 SP1



Figure 31 : Windows serveur: Installation: choix du type d'installation

Choisir Windows 2008R2 SP1 (64bit) Enterprise Full



Figure 32 : Windows serveur: Installation: copie de fichier



Figure 33 : Windows serveur: Installation: mot de passe administrateur



Figure 34 : Windows serveur: Installation: saisie mot de passe administrateur

Conseil : Attention au numlock

Conseil : noter le mot de passe dans le dossier d'exploitation



Figure 35 : Windows serveur: Installation: mot de passe administrateur changé

| 🔁 W2008 | R2-B | ase - VMware Player (Non-commer | cial use only) | | <u>- 🗆 ×</u> | |
|----------|--|---|---|--|------------------------|--|
| Player 👻 | | - 🗄 📜 🐻 | | | * | |
| Tâches | de c | onfiguration initiales | | | _ 8 × | |
| | Effectuez les tâches suivantes pour configurer ce serveur | | | | 1°2008 <mark>R2</mark> | |
| | | Indiquer un nom d'ordinateur et | Nom complet de | WIN-92TJH90G03S | _ | |
| | | | Groupe de travail : | WORKGROUP | | |
| C | 2 | Mettre à jour ce serveur | | Mise à jour du serveur Windows | | |
| | | Activer la mise à jour et l'envoi de rapports automatiques | Mises à jour : Rapports : | Non configuré Rapport d'erreurs Windows désactivé Ne pas participer au Programme d'amélioration du produit | | |
| | | Yélécharger et installer les mises à jour | Mises à jour recherchées : Mises à jour installées : | Jamais Jamais | | |
| | Personnaliser ce serveur | | | Personnalisation du serveur | | |
| | | Ajouter des rôles | Rôles : | Aucun | | |
| | ſ | Ajouter des fonctionnalités | Fonctionnalités : | Aucun | | |
| | | Activer le Bureau à distance | Bureau à distance : | Désactivé | | |
| | | Configurer le Pare-feu Windows | Pare-feu : | Public : Activé | - | |
| | Ne | pas afficher cette fenêtre à l'ouverture de | session | Fermer | | |
| 灯 Démarr | Image: Second | | | | | |

Figure 36 : Windows serveur: Installation: accueil

Conseil: « Démarrer > panneau de configuration > Petites icônes »

Conseil: « Démarrer > panneau de configuration > Options des dossiers > décocher les options « masquer... » » **Conseil**: Pour les tests / la configuration du serveur avant la production, désactiver la sécurité renforcée

« Démarrer > panneau de configuration > Programmes et fonctionnalités > Activer ou désactiver des fonctionnalités de Windows »



Figure 37 : Windows serveur: Installation: sécurité renforcée

« Paramétrer la Configuration de sécurité renforcée d'Internet Explorer > désactivé »

| 🛂 W2008R2-Base - VMware Player (Non-commercial use only) | | | | | | |
|---|---|--|--|--|--|--|
| Player 👻 📔 👻 📰 🔲 | Š | * | | | | |
| 📕 Gestionnaire de serveur | ÷ | | | | | |
| Fichier Action Affichage ? | | | | | | |
| Gestionnaire de serveur (WIN-92 Rôles Fonctionnalités Diagnostics | Configuration de sécurité renforcée d'Internet Explorer La Configuration de sécurité renforcée d'Internet Explorer (IE ESC) diminue l'exposition de votre serveur à des attaques potentielles provenant de contenus Web. | x thes de gestion de haut niveau, et | | | | |
| | par défaut pour les groupes Administrateurs et Utilisateurs. Administrateurs : | au pare-feu Windows | | | | |
| | C Désactivé | rer les mises à jour her de nouveaux rôles r l'Assistant Configuration curité | | | | |
| | Utilisateurs : Ø C Activé (recommandé) | rer la Configuration de renforcée d'Internet | | | | |
| | 😵 🕞 Désactivé | | | | | |
| | Pour en savoir plus sur la Configuration de sécurité renforcée OK Annuler | | | | | |
| Kesume des roles Alice sur Résumé des rôles Dernière actualisation : Aujourd'hui à 22:31 Configurer l'actualisation | | | | | | |
| Démarrer | | FR 22:31 29/06/2013 | | | | |

Figure 38 : Windows serveur: Installation: Paramétrage de la sécurité renforcée

Conseil: Pour la production, réactiver la sécurité renforcée

Conseil : Pour la production : **désactiver** les mises à jour Windows Update automatique et/ou **utiliser WSUS** (Windows Server Update Services).

Les environnements serveur doivent être des environnements <u>qualifiés</u>, dont la configuration est maitrisée et les changements de configuration décidés et validés.

Les mises à jour doivent être préalablement effectuées et validées sur des environnements de recette.

Une fois validées, elles peuvent être propagées sur les environnements de production suivant une procédure clairement définie qui permet d'anticiper les impacts pour les utilisateurs et sur les applications.

Ces bonnes pratiques concernent aussi bien Windows que les applications tierces.

Ceci concerne en particulier Java, dont les mises à jour automatiques doivent être impérativement désactivées sur les serveurs, **une veille des mises à jour Java doit être mise en place et les mises à jour doivent être préalablement recettées avant mise en production.**



Figure 39 : Windows serveur: Configuration: maitriser les mises à jour

« Modifier les paramètres »

| 🙀 W2008R2-Base - VMware Player (Non-commercial use only) | |
|---|------------------------|
| Player 👻 🛄 📼 🛄 📷 | * |
| 🖉 Panneau de configuration\Tous les Panneaux de configuration\Windows Update\Modifier les pi | _ 8 × |
| GO ✓ ✓ Windows Update × Modifier les paramètres ▼ Image: Compare the second | 2 |
| Choisissez comment Windows installe les mises à jour | |
| Lorsque votre ordinateur est en ligne, Windows peut rechercher automatiquement les mises à jour importantes et les installer en utilisant ces paramètres. Si des mises à jour sont disponibles, vous pouvez également les installer avant d'éteindre votre ordinateur. | |
| En quoi la mise à jour automatique m'aide-t-elle ? | |
| Mises à jour importantes | |
| Ne jamais rechercher des mises à jour (non recommandé) | |
| Installer les nouvelles mises à jour : Tous les jours 🖉 à 03:00 💌 | |
| Mises à jour recommandées | |
| Recevoir les mises à jour recommandées de la même façon que vous recevez les mises à jour importantes | |
| Qui peut installer les mises à jour | |
| Autoriser tous les utilisateurs à installer les mises à jour sur cet ordinateur | |
| Remarque : Windows Update peut se mettre à jour automatiquement avant de rechercher d'autres mises à jour. Consultez la <u>déclaration de confidentialité en ligne</u> . | |
| | |
| | |
| | |
| OK Annuler | |
| | |
| Model Image: Second seco | 22:35 29/06/2013 == |

Figure 40 : Windows serveur: Configuration: maitriser les mises à jour

Conseil : A ce stade : changer le nom de la machine : **Start**, click **Run..., cmd**, **control system**, **Paramètres système avancés, nom de l'ordinateur.**

| 1 W2008R2SP1 - | VMware Player (Non-commercial u | se only) | |
|-----------------|--|---|------------------------------------|
| Player 👻 📘 | - 🗄 📜 🎼 | | « |
| 🕎 Panneau de co | onfiguration\Tous les Panneaux d | e configuration système | _ 8 × ^ |
| GO ~ 🖻 | Tous les Panneaux de configuration | • Système 🔹 🐨 Recher | cher 🔎 |
| Fichier Edition | Affichage Outils ? | Modification du nom ou du domaine de l'ordinateur | xI |
| Page d'accue | ropriétés système | Le nom de cet ordinateur a été modifié. Vous devez redémarrer | |
| configuration | Paramètres système avancés Nom de l'ordinateur | cet ordinateur pour que la modification de nom prenne effet avant de pouvoir modifier son appartenance au domaine. | |
| Gestionnaire | | | |
| Paramètres (| ordinateur sur le réseau. | Nom de l'ordinateur : | |
| | Description de | New completion l'articitations | |
| | Par exempl "Serveur d | msserver | |
| | Nom complet de msserver l'ordinateur : | Autres | |
| | Groupe de travail : WORKGR | Membre d'un | E |
| | Pour renommer cet ordinateur ou cha | O Domanie: | 79 CH7 |
| | ou de groupe de travail, cilquez sur in | Groupe de travail : | 75 012 |
| | | WORKGROUP | |
| | | | tylet n'est pas disponible sur cet |
| | | OK. Annuler | J |
| | | changera en msserve rdinateur) | er après le Modifier les |
| Voir aussi | Les modifications prendront effe | t lorsque l'ordinateur aura redémarré. | |
| Centre de mi | Ear | mer Appriler Appliquer | |
| | | Summer Shandaren | T |
| 灯 Démarrer | 1. 🛛 🚞 👔 | | FR 🕿 🐂 🕼 11:07 |

Figure 41 : Windows serveur: Configuration: nom de l'ordinateur

12.4 Installation d'un rôle Active Directory

Le rôle Active Directory s'installe en ajoutant le rôle « Services de domaine Active Directory » :

| 핵 W2008R2-Base - VMware Player (Non-commercial use only) | | | | | | |
|--|--|---|--|--|--|--|
| Player 👻 🔛 📜 📷 🔍 « | | | | | | |
| Assistant Ajout de rôles | k | <u>×۲</u> | | | | |
| Sélectionnez des rôles de serveurs | | | | | | |
| Avant de commencer | Sélectionnez un ou plusieurs rôles à installer sur ce serveur. | L | | | | |
| Rôles de serveurs | Rôles : | Description : | | | | |
| Services de domaine Active Direc Confirmation État d'avancement Résultats | Hyper-V Serveur d'applications Serveur de télécopie Serveur DHCP Serveur DNS Serveur Web (IIS) Services AD LDS (Active Directory Lightweight Directory Services) Services AD RMS (Active Directory Rights Management Services) Services ADFS (Active Directory Rights Management Services) Services ADFS (Active Directory Federation Services) Services de certificats Active Directory Services de déploiement Windows Services de domaine Active Directory Services de fichiers Services de fichiers Services de stratégie et d'accès réseau Services WSUS (Windows Server Update Services) | Les <u>services Bureau à distance</u> , anciennement Services Terminal Server, intègrent des technologies qui permettent aux utilisateurs d'accéder aux programmes Windows installés sur un serveur Hôte de session Bureau à distance ou d'accéder à tout le Bureau Windows. Grâce aux services Bureau à distance, les utilisateurs peuvent accéder à un serveur Hôte de session Bureau à distance ou à un ordinateur virtuel à partir de votre réseau d'entreprise ou d'Internet. | | | | |
| - | En savoir plus sur les roles de serveur | | | | | |
| | < Précédent Suivant | > Installer Annuler | | | | |
| Image: Second | | | | | | |

Figure 42 : Active Directory: Installation du rôle



Figure 43 : Active Directory: Installation du rôle : résultat

Promouvoir le serveur en tant que contrôleur de domaine Active Directory en lancant l'assistant « **dcpromo.exe** » (le serveur devra rebooter à la fin de cette phase) :

| 🙀 W2008R2-Base - VMware Player (Non-con | nmercial use only) | |
|--|--|-------------------|
| Player 👻 🔛 💌 📑 | | * |
| 🖡 Gestionnaire de serveur | + | |
| Fichier Action Affichage ? | | |
| 🗢 🔿 [📶 🛛 🔽 | | |
| Gestionnaire de serveur (WIN-92TJH90G03S) | Services de domaine Active Directory | |
| Services de domaine Active Directory Services de domaine Active Directory Fonctionnalités Diagnostics Manual Configuration | Stocke les données d'annuaire et gère les communications entre les utilisateurs et les domaines, notamment les processus d'ouverture de session utilisateur, l'authentificat recherches dans l'annuaire. | on et les |
| 🕀 🔠 Stockage | | |
| | Ce serveur n'a pas encore le rôle de contrôleur de domaine. Exécutez l'Assistant Installation des services de domaine Active Directory (dcpromo.exe). Aucun Áucun Événements : erreur(s)/événement(s) pendant 24 heures Filtrer les événements Filtrer les événements Propriétés | |
| | Deroière actualisation : Autourd'hui à 23:11. Configurer l'actualisation | |
| | | |
| MDémarrer | FR 🕆 🕞 👘 🗘 29/0 | 3:11)6/2013 💻 |

Figure 44 : Active Directory: Configuration du rôle

| 🙀 W2008R2-Base - VMware Player (Non-cor | nmercial use only) | |
|---|--|-------------------|
| Player 👻 🔛 💌 📷 | | * |
| 📕 Gestionnaire de serveur | ÷ | |
| Fichier Action Affichage ? | | |
| 🗢 🔿 🖄 📧 🛛 👔 | | |
| Gestionnaire de serveur (WIN-92TJH90G03S) Rôles Services de domaine Active Directory Fonctionnalités Diagnostics Configuration | Services de domaine Active Directory Stocke les données d'annuaire et gère les communications entre les utilisateurs et les domaines, notamment les processus d'ouverture de session utilisateur, l'authentificati recherches dans l'annuaire. | on et les |
| 🗄 🔠 Stockage | 🔿 Résumé | |
| | Ce serveur n'a pas encore le rôle de contrôleur de domaine. Exécutez l'Assistant Installation des services de domaine Active Directory (dcpromo.exe). | |
| | Aucun Aucun Événements : erreur(s)/événement(s) pendant 24 heures Propriétés | |
| | ✓ ID de l'év Date et h | |
| <f< th=""><td>Dernière actualisation : Aujourd'hui à 23:11 Configurer l'actualisation</td><td>•</td></f<> | Dernière actualisation : Aujourd'hui à 23:11 Configurer l'actualisation | • |
| | | |
| MDémarrer | FR * P (22)0 | 3:11 6/2013 == |

Figure 45 : Active Directory: Configuration du rôle : Exécution de l'assistant


Figure 46 : Active Directory: Configuration du rôle : mode avancé

| 🙀 W2008R2-Base - VMware Player (Non-commercial use only) | |
|---|--|
| Player 👻 📙 🛥 🗐 🌀 | * |
| Gestionnaire de serveur | |
| Choisissez une configuration de déploiement Vous pouvez créer un contrôleur de domaine pour une forêt nouvelle ou existante. | |
| E C Forêt existante | mmunications entre les utilisateurs et les ture de session utilisateur, l'authentification et les |
| E E Ajouter un contrôleur de domaine à un domaine existant | A |
| C Créer un nouveau domaine dans une forêt existante Ce serveur va devenir le premier contrôleur de domaine du nouveau domaine. | le domaine. Exécutez l'Assistant ctory (dcpromo.exe). |
| Créer une nouvelle racine d'arborescence de domaine au lieu d'un nouveau domaine enfant Créer un domaine dans une nouvelle forêt | Accéder à l'Observateur d'événements Filtrer les événements |
| En savoir plus sur les <u>configurations de déploiement possibles</u> | Proprietes |
| <pre></pre> | er l'actualisation |
| Démarrer | FR FR 10 10 10 10 10 10 10 10 10 10 10 10 10 |

Figure 47 : Active Directory: Configuration du rôle : nouvelle forêt

| 🙀 W2008R2-Base - VMware Player (Non-commercial use only) | |
|--|--|
| Player 👻 🔛 💻 🥅 | * |
| Gestionnaire de serveur | |
| Assistant Installation des services de domaine Active Directory | × |
| Nommez le domaine racine de la forêt Le premier domaine de la forêt est le domaine racine de la forêt. Il porte également le nom de la forêt. | |
| E E E E E E E E E E Trez le nom de domaine complet du nouveau domaine racine de forêt. | mmunications entre les utilisateurs et les ture de session utilisateur, l'authentification et les |
| E Nom de domaine complet du domaine racine de forêt : | |
| eu.cosign | la domaina. Evécutar l'Assistant |
| Exemple : corp.contoso.com | ctory (dcpromo.exe). |
| | er l'actualisation |
| | |
| Mathematical Control C | FR 🗭 📪 🎲 23:13 💻 |

Figure 48 : Active Directory: Configuration du rôle : nom de domaine

| 🙀 W2008R2-Base - VMware Player (Non-commercial use only) | |
|---|--|
| Player 👻 📙 🛥 🚍 🕞 | * |
| Gestionnaire de serveur Assistant Installation des services de domaine Active Directory | |
| Nommez le domaine racine de la forêt Le premier domaine de la forêt est le domaine racine de la forêt. Il porte également le nom de la forêt. | |
| E E E Entrez le nom de domaine complet du nouveau domaine racine de forêt. | mmunications entre les utilisateurs et les ture de session utilisateur, l'authentification et les |
| Nom de domaine complet du domaine racine de forêt : | - |
| Exemple : corp.d Vérification de la disponibilité du nouveau nom de forêt | le domaine. Exécutez l'Assistant ctory (dcpromo.exe). |
| | Accéder à l'Observateur d'événements Filtrer les événements Propriétés |
| | |
| | _ |
| | er l'actualisation |
| | 23:13 |
| | FR 客 🕞 👘 🕼 29/06/2013 💻 |

Figure 49 : Active Directory: Configuration du rôle : vérification de la disponibilité du nom de la forêt

| 🙀 W2008R2-Base - VMware Player (Non-commercial use only) | | |
|--|--|--|
| Player 👻 📙 😴 🔚 🥫 | | * |
| E Gestionnaire de serveur | | |
| Assistant Installation des services de domaine Active Direc | tory X | |
| Nom de domaine NetBIOS Il s'agit du nom que les utilisateurs des versions antérieures de Wi | ndows utiliseront pour | |
| identifier le nouveau domaine. | | |
| | | mmunications entre les utilisateurs et les |
| L'Assistant génère un nom NetBIOS par défaut. Cette page de l'Au que si vous avez sélectionné le mode avancé ou si l'Assistant a de le nom par défaut. | sistant ne s'affiche itecté un conflit dans | |
| Acceptez le nom généré par l'Assistant ou tapez un nouveau nom Suivant. | puis cliquez sur | de domaine, Exécutez l'Assistant |
| Nom de domaine NetBIOS : COSIGN | | ctory (dcpromo.exe). |
| | | Accéder à l'Observateur |
| | | d'evenements |
| | | Propriétés |
| | | |
| | | |
| | | |
| | | |
| | | |
| < Précédent | Suivant > Annuler | er l'actualisation |
| | | |
| Moemarrer | | FR 🖈 🕞 📳 🕼 23:13 💻 |

Figure 50 : Active Directory: Configuration du rôle : NetBIOS

| 😼 W2008R2-Base - VMware Player (Non-commercial use only) | |
|---|--|
| Player 👻 📙 😴 🔚 🥫 | * |
| Gestionnaire de serveur Assistant Installation des services de domaine Active Directory | ×□ |
| Nom de domaine NetBIOS Il s'agit du nom que les utilisateurs des versions antérieures de Windows utiliseront pour identifier le nouveau domaine. | |
| E E L'Assistant génère un nom NetBIOS par défaut. Cette page de l'Assistant ne s'affiche que si vous avez sélectionné le mode avancé ou si l'Assistant a détecté un conflit dans | mmunications entre les utilisateurs et les ture de session utilisateur, l'authentification et les |
| le nom par défaut. Acceptez le nom <u>dédéré par l'Assistant ou tapez un pouveau pom puis cliqu</u> ez sur Suivant. Nom de domaine Vérification du nom NetBIOS | le domaine. Exécutez l'Assistant ctory (dcpromo.exe). |
| | Accéder à l'Observateur d'événements Filtrer les événements Propriétés |
| | |
| Précédent Suivant > Annuler | er l'actualisation |
| Démarrer | FR 🖈 🕞 👘 🕼 23:14 29/06/2013 ⋿ |

Figure 51 : Active Directory: Configuration du rôle : Vérif. NetBIOS

| Player Player | « |
|--|---|
| Gestionnaire de serveur Assistant Installation des services de domaine Active Directory | |
| | × |
| Définir le niveau fonctionnel de la forêt Sélectionnez le niveau fonctionnel de la forêt. | |
| mmunications entre les utilisateurs et les ture de session utilisateur, l'authentification et les Windows Server 2008 R2 | |
| Détails : Le niveau fonctionnel de forêt Windows Server 2008 R2 procure toutes les fonctionnalités disponibles dans le niveau fonctionnel de forêt Windows Server 2008, ainsi que les fonctionnalités supplémentaires suprimés dans leur intégralité pendant que les services de domaine Active Directory s'exécutent. Tout nouveau domaine créé dans cette forêt fonctionne par défaut au niveau qui exécutent Windows Server 2008 R2 ou ultérieur. Image: Construint de les services de domaine active de domaine créé dans cette forêt que des contrôleurs de domaine qui exécutent Windows Server 2008 R2 ou ultérieur. Image: Construint de les services de forêt et de domaine de domaine qui exécutent Windows Server 2008 R2 ou ultérieur. | |
| < | |

Figure 52 : Active Directory: Configuration du rôle : Niveau fonctionnel

L'étape suivante « Analyse de la configuration DNS » peut prendre du temps :

| 🙀 W2008R2-Base - VMware Player (Non-commercial use only) | |
|--|--|
| Player 👻 🔛 💻 🔚 | * |
| Gestionnaire de serveur Assistant Installation des services de domaine Active Directory | |
| Définir le niveau fonctionnel de la forêt Sélectionnez le niveau fonctionnel de la forêt. | |
| E Niveau fonctionnel de la forêt : | mmunications entre les utilisateurs et les ture de session utilisateur, l'authentification et les |
| Windows Server 2008 R2 | |
| Détails : Le niveau foncti fonctionnalités de la configuration DNS - Corbe supprimés dans I Directory s'exéc Tout nouveau d Vous qui executent Windows Server 2008 R2 ou ulteneur. En savoir plus sur les <u>niveaux fonctionnels de forêt et de domaine</u> | le domaine. Exécutez l'Assistant ctory (dcpromo.exe). |
| < Précédent Suivant > Annuler | er l'actualisation |
| Démarrer | FR R 10 123:14 29/06/2013 |

Figure 53 : Active Directory: Configuration du rôle : Configuration DNS

A priori, **décocher** l'option « **Serveur DNS** ». A défaut, bien maitriser cette option, sous peine de faire dysfonctionner le réseau sur lequel le serveur est installé.

| 🙀 W2008R2-Base - VMware Player (Non-commercial use only) | |
|--|--|
| Player 👻 🛄 😴 🔚 🥫 | * |
| Gestionnaire de serveur Gestionnaire de serveur Gestionnaire de serveur Options supplémentaires pour le contrôleur de domaine | |
| mmunications entre les utilisateur, l'a | ateurs et les authentification et les |
| Sélectionnez des options supplé Serveur DNS Serveur DNS Catalogue global Contrôleur de domaine en Informations supplémentaires : Vous avez choisi de ne pas installer de serveur DNS sur ce contrôleur de domaine, mais votre environnement ne prend pas en charge le serveur DNS pour ce nom de domaine. La prise en charge du serveur DNS est nécessaire pour permettre aux services de domaine Active Directory de fonctionner correctement. Informations supplémentaires : Le premier contrôleur de domaine domaine. Nous vous recommandons d'i contrôleur de domaine. Page du serveur DNS sur ce contrôleur de domaine domaine, installez le serveur DNS sur ce tordinateur et créez une délégation pour la nouvelle zone DNS eu cosign », à partir de la zone racine du DNS. Les contrôleur de domaine, installez le serveur DNS sur ce tordinateur et créez une délégation pour la nouvelle zone DNS eu cosign », à partir de la zone racine vers ce serveur DNS. Le serveur DNS principal testé était : a.root-servers.net (198.41.0.4) I est vivement recommandé d'installer les services serveur DNS sur ce contrôleur de domaine. | nt |
| En savoir plus sur les <u>options s</u> Oui Non | 23:20 |
| | 29/06/2013 💳 |

Figure 54 : Active Directory: Configuration du rôle : Décocher DNS

| 🔁 w | 2008R2-Base - VMware Player (Non-commercial use only) | | | 4 |
|--------------|---|---------|--|---|
| Playe | er 🗸 🚹 🗶 🚍 🥫 | | • | : |
| - <u>-</u> - | estionnaire de serveur | | | I |
| F | Assistant Installation des services de domaine Active Directory | × | | |
| | Mot de passe administrateur de restauration des services d'annuaire | | | |
| Ę. | | | | |
| | | | mmunications entre les utilisateurs et les | |
| 0 | Le compte d'administration de restauration des services d'annuaire est différent du compte d'administrateur de domaine. | | ture de session utilisateur, l'authentification et les | |
| e | Attribuez un mot de passe au compte d'administrateur qui sera utilisé lors du démarrage de ce contrôleur de domaine en mode Restauration des services d'annuaire. Nous vous recommandons de choisir un mot de passe fort. | | Je domaine. Exécutez l'Assistant | |
| | Mot de passe : | | ctory (dcpromo.exe). | |
| | Confirmer le mot de passe : | | Accéder à l'Observateur | |
| | En savoir plus sur le mot de passe de restauration des services d'annuaire | | d'événements | |
| | | | Propriétés | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | l |
| | < Précédent Suivant > | Annuler | er l'actualisation | 1 |
| | | | | Í |
| A De | émarrer | | FR FR 123:21 29/06/2013 | |

Figure 55 : Active Directory: Configuration du rôle : mot de passe LDAP

Conseil : Noter le mot de passe saisi dans le dossier d'exploitation

| 👼 Assistant Installation des services de domaine Active Directory | | × |
|--|----------------------------|-------|
| Emplacement de la base de données, des fichiers journaux et o Spécifiez les dossiers qui contiendront la base de données du contrôleu Active Directory, les fichiers journaux et SYSVOL. | le SYSVOL ur de domaine | |
| Pour de meilleures performances et une meilleure récupération, stockez données et les fichiers journaux sur des volumes séparés. Dossier de la base de données : | la base de | |
| C:\Windows\NTDS | Parcourir | |
| , Dossier des fichiers journaux : | | |
| C:\Windows\NTDS | Parcourir | |
| Dossier SYSVOL : | | |
| C:\Windows\SYSVOL | Parcourir | |
| En savoir plus sur le <u>placement des fichiers des services de domaine Ac</u> | <u>tive Directory</u> | |
| < Précédent Sui | vant > Ar | nuler |

Figure 56 : Active Directory: Configuration du rôle : configuration des bases de données

| ۳ | W2008R2-Base - VMware Play | yer (Non-commercial use only) | _0> | × |
|----------|--|---|--|---|
| Pla | yer 👻 📙 👻 📑 📜 | 0 | * | ĸ |
| | Gestionnaire de serveur Assistant Installation des | services de domaine Active Directory | _ 🗆 × | 1 |
| | Résumé | mmunications e | ηtre les utilisateurs et les | |
| 6 | Vérifiez vos sélections : | Assistant Installation des services de domaine Active Directory | utilisateur, l'authentification et les | |
| ē | Configurer ce serveur en d'une nouvelle forêt. Le nouveau nom de dom forêt. Le nom NetRIOS du dom | L'Assistant effectue la configuration des services de domaine Active Directory. Ce processus peut durer de quelques minutes à quelques heures, en fonction de votre environnement et des options que vous avez sélectionnées. | cutez l'Assistant .exe). | |
| | Niveau fonctionnel de la Niveau fonctionnel du do Site : Default-First-Site-Na | Installation de la Console de gestion des stratégies de groupe | l'Observateur ents événements | |
| | sur Suivant. Vous pouvez exporter ce: réponses pour les utiliser ; installation sans assistanc En savoir plus sur l' <u>utilisat</u> | Redémarrer à la fin de l'opération | | |
| | | < Précédent Suivant > Annuler er l'actualisation | | |
| Ë | | | | |
| . | Démarrer | FR FR | × 🕞 📜 🌜 23:21 29/06/2013 🗖 | |

Figure 57 : Active Directory: Configuration du rôle : Installation GPMC

12.5 Installation d'un rôle Certificate Server

Sous Windows 2008R2, le rôle Certificate Server s'installe en ajoutant le rôle « Services de certificats Active Directory ».

Conseil : bien revérifier les noms de la machine et du domaine car ils ne pourront plus être modifiés une fois le rôle Certificate Server installé.



Figure 58 : AD CS : Installation du rôle



Figure 59 : AD CS : service du rôle « Autorité de certification »

| 🙀 W2008R2-Base - VMware Player (N | lon-commercial use only) | | |
|---|--|-------|--|
| Player 👻 🔛 💌 👘 | | * | |
| Assistant Ajout de rôles | | ×1 | |
| Spécifier le type | d'installation | | |
| Avant de commencer Rôles de serveurs | Les autorités de certification peuvent utiliser les données d'Active Directory pour simplifier l'émission et la gestion de certificats. Indiquez si vous souhaitez établir une autorité de certification d'entreprise ou autor | nome. | |
| AD CS Services de rôle Type d'installation | Entreprise Sélectionnez cette option si cette autorité de certification est un membre de domaine et peut utiliser la service d'annuaire pour émettre et gérer des certificats. | e | |
| Type d'autorité de certification Clé privée Chiffrement Nom de l'autorité de certific Période de validité | C Autonome Sélectionnez cette option si cette autorité de certification n'utilise pas les données du service d'annua pour émettre ou gérer des certificats. Une autorité de certification autonome peut être membre d'un domaine. | ire | |
| Base de données de certificats Confirmation État d'avancement Résultats | | J | |
| 1 | En savoir plus sur les différences entre l'installation d'entreprise et autonome | | |
| | < Précédent Suivant > Installer Annuler | | |
| Image: Second | | | |

Figure 60 : AD CS : Type d'installation : Choisir « Entreprise »

Sélectionner obligatoirement « entreprise » (pour permettre la propagation automatique de cette autorité sur toutes les machines du domaine)

| 🙀 W2008R2-Base - VMware Player (N | on-commercial use only) | |
|--|---|------------------|
| Player 👻 🔛 💌 📑 🐻 | | * |
| Assistant Ajout de rôles | | × |
| Spécifier le type | d'autorité de certification | |
| Avant de commencer Rôles de serveurs AD CS Services de rôle Type d'installation Type d'autorité de certification Clé privée Chiffrement Nom de l'autorité de certific Période de validité Base de données de certificats Confirmation État d'avancement Résultats | Une combinaison d'autorités de certification racines et secondaires peut être configurée pour créer une infrastructure hiérarchique à dé publique (PKI). Une autorité de certification racine est une autorité qui ér son propre certificat auto-signé. Une autorité de certification secondaire reçoit son certificat d'une autre autorité de certification. Indiquez si vous souhaitez installer une autorité de certification racine ou second Autorité de certification racine Sélectionnez cette option si vous installez la première et unique autorité de certification dans une infrastructure à dé publique. Autorité de certification secondaire Sélectionnez cette option si votre autorité de certification obtient son certificat d'autorité de certification plus élevée dans une infrastructure à dé publique. | enet aire. |
| | En savoir plus sur l'infrastructure à dé publique (PKI) | ľ |
| | < Précédent Suivant > Installer Annuler | |
| M Démarrer | FR R 0 | 0:05 6/2013 💻 |

Figure 61 : AD CS : type d'autorité : Choisir « Autorité de certification racine »

| 🙀 W2008R2-Base - VMware Player (N | lon-commercial use only) | <u>_ X</u> |
|---|---|------------------|
| Player 👻 🔛 💌 📑 | | * |
| Assistant Ajout de rôles | | × |
| Configurer la clé | privée | |
| Avant de commencer Rôles de serveurs | Pour générer et émettre des certificats à des dients, une autorité de certification doit avoir une dé privée Indiquez si vous souhaitez créer une nouvelle dé privée ou utiliser une dé existante. | · |
| AD CS | Créer une nouvelle dé privée | |
| Services de rôle | Utilisez cette option si vous n'avez pas de dé privée ou si vous souhaitez créer une nouvelle dé privée améliorer la sécurité. Un message vous invitera à sélectionner un fournisseur de services de chiffreme | pour [|
| Type d'installation | à spécifier une longueur de clé pour la clé privée. Pour émettre de nouveaux certificats, vous devez | |
| Type d'autorité de certification | egalement selectionner un algorithme de nachage. | |
| Clé privée | Utiliser une dé privée existante Utiliser cette option pour garantir la continuité avec des certificats précédemment émis lors de la | |
| Chiffrement | réinstallation d'une autorité de certification. | |
| Nom de l'autorité de certific | Sélectionner un certificat et utiliser sa dé privée associée | |
| Période de validité | Sélectionnez cette option si vous avez un certificat existant sur cet ordinateur ou si vous souhaite | z |
| Base de données de certificats | Importer un ceruncat et udiiser sa de privee associee. | |
| Confirmation | Selectionnez de prive existance sur del ordinateur Sélectionnez cette option si vous avez conservé des dés privées d'une installation précédente ou | si |
| État d'avancement | vous souhaitez utiliser une dé privée d'une autre source. | |
| Résultats | | |
| | En savoir plus sur les dés publiques et privées | L |
| | < Précédent Suivant > Installer Annuler | Ī |
| Marrer 5 | FR 客 🕞 👘 🕼 30/0 | 0:05 6/2013 💻 |

Figure 62 : AD CS : Choisir « Créer une nouvelle clé privée »

| 🙀 W2008R2-Base - VMware Player (N | on-commercial use only) | |
|---|--|---------------------------|
| Player 👻 🔛 💌 📷 | | * |
| Assistant Ajout de rôles | | ×I |
| Configurer le chif | frement pour l'autorité de certification | |
| Avant de commencer Rôles de serveurs AD CS Services de rôle Type d'installation Type d'autorité de certification Clé privée Chiffrement Nom de l'autorité de certific | Pour créer une nouvelle clé privée, vous devez d'abord sélectionner un <u>fournisseur de services de</u> <u>chiffrement</u> , un <u>algorithme de hachage</u> et une longueur de clé adaptée à l'utilisation prévue des certif que vous émettez. La sélection d'une valeur élevée pour la longueur de clé donnera une sécurité renforcée, mais allongera les opérations de signature. Sélectionnez un fournisseur de services de chiffrement : RSA#Microsoft Software Key Storage Provider Sélectionnez l'algorithme de hachage pour la signature des certificats émis par cette autorité de certification SHA512 SHA1 MD5 V | = icats :s : n : |
| Période de validité Base de données de certificats Confirmation État d'avancement Résultats | Autoriser l'interaction de l'administrateur lorsque l'autorité de certification accède à la dé privée. | |
| | En savoir plus sur les options de chiffrement d'une autorité de certification | |
| Momerarer | <précédent suivant=""> Installer Annuler FR R P P 00 30/06</précédent> | 1:06 5/2013 = |

Figure 63 : AD CS : clé privée : Chiffrement

S'assurer que le choix effectué est en adéquation avec la politique de sécurité de l'environnement de production visé.

| 😼 W2008R2-Base - VMware Player (N | on-commercial use only) | |
|--|--|-----------------|
| Player 👻 🔛 💌 💼 📷 | | * |
| Assistant Ajout de rôles | | × |
| Configurer le nor | n de l'autorité de certification | |
| Avant de commencer Rôles de serveurs AD CS | Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificat émis par l'autorité de certification. Des valeurs de suffixe de nom uniques sont automatiquement générées mais ne peuvent pas être modifiées. | S |
| Services de rôle | Nom commun de cette autorité de certification : | — HI |
| Type d'installation | Jeu-cosign-ca | |
| Type d'autorité de certification | Suffixe du nom unique : | |
| Clé privée | DC=eu,DC=cosign | |
| Chiffrement | | |
| Nom de l'autorité de certific | Anna Anna an Anna Anna Anna Anna Anna A | |
| Période de validité | Aperça da nom anique : CN=eu-cosign-ca.DC=eu.DC=cosign | — III |
| Base de données de certificats | | |
| Confirmation | | |
| État d'avancement | | |
| Résultats | En savoir plus sur la configuration d'un nom d'autorité de certification | |
| | | 14 |
| | < Précédent Suivant > Installer Annuler | |
| Marrer bémarrer | FR 客 PP 🖫 🕼 30/06 | :06 5/2013 💻 |

Figure 64 : AD CS : clé privée : Préciser le nom de l'AC

| 🙀 W2008R2-Base - VMware Player (M | on-commercial use only) | |
|--|---|-----------------|
| Player 👻 🔛 💌 📷 | | * |
| Assistant Ajout de rôles | | × |
| Période de validi | té du certificat | |
| Avant de commencer Rôles de serveurs AD CS Services de rôle | Un certificat sera émis par cette autorité de certification pour sécuriser les communications avec d'autres autorités de certification et avec des dients demandant des certificats. La période de validité d'un certifica d'autorité de certification peut être basée sur un certain nombre de facteurs, notamment la fonction prévu l'autorité de certification et les mesures de sécurité que vous avez instaurées pour sécuriser l'autorité de certification. | t Je de |
| Type d'installation Type d'autorité de certification | Sélectionnez la période de validité du certificat généré par cette autorité de certification : 5 Années | |
| Clé privée | Date d'expiration de l'autorité de certification : 30/06/2018 00:04 | |
| Chiffrement | Notez qu'une autorité de certification n'émettra des certificats valides que jusqu'à sa date d'expiration. | |
| Nom de l'autorité de certific | | |
| Période de validité | | |
| Base de données de certificats | | |
| Confirmation | | |
| État d'avancement | | |
| Résultats | | |
| | En savoir plus sur la définition de la période de validité des certificats | 1 |
| | < Précédent Suivant > Installer Annuler | |
| Marrer | FR 客 🕞 📜 00 | :07 5/2013 💻 |

Figure 65 : AD CS : clé privée : Préciser la période de validité

| 🙀 W2008R2-Base - VMware Player (N | on-commercial use only) | <u>- 🗆 ×</u> |
|--|---|------------------|
| Player 👻 🔛 🕶 📑 🥫 | | * |
| Assistant Ajout de rôles | | ×I |
| Configurer la bas | e de données de certificats | |
| Avant de commencer Rôles de serveurs AD CS | La base de données de certificats enregistre toutes les demandes de certificats, les certificats émis, et les certificats révoqués ou expirés. Le journal de la base de données peut être utilisé pour analyser les activit de gestion d'une autorité de certification. | és |
| Services de rôle | Emplacement de la base de données de certificats : | L L |
| Type d'installation | C:\Windows\system32\CertLog Parcourir. | |
| Type d'autorité de certification | Utiliser la BdD de certificats d'une installation précédente à cet emplacement | |
| Clé privée | Emplacement du journal de la base de données de certificats : | |
| Chiffrement | C:\Windows\system32\CertLog Parcourir. | |
| Nom de l'autorité de certific | | _ |
| Période de validité | | |
| Base de données de certificats | | 4 |
| Confirmation | | |
| État d'avancement | | |
| Résultats | < Précédent Suivant > Installer Annuler | 1 |
| Marrer | FR 🖈 🔁 🕼 🕺 30/0 |):07 5/2013 🏧 |

Figure 66 : AD CS : clé privée : Base de données de certificats

| 😼 W2008R2-Base - VMware Player (N | lon-commercial use only) | | |
|--|--|---|--------------------|
| Player 👻 🔛 💌 📷 | | | * |
| Assistant Ajout de rôles | A | | ×I |
| Confirmer les sél | ections pour l'installation | | |
| Avant de commencer Rôles de serveurs AD CS Services de rôle | Pour installer les rôles, les services de r 1 message(s) d'avertissement, 1 I est possible que ce serveur do | ôle ou les fonctionnalités suivants, diquez sur Installer. message(s) d'information ci-dessous ive être redémarré à la fin de l'installation. | |
| Type d'installation | Services de certificats Active | Directory | |
| Type d'autorité de certification | Autorité de certification | | |
| Clé privée | Les paramètres de nom et de de l'autorité de certification installé | omaine de cet ordinateur ne peuvent pas être changés une fois | |
| Chiffrement | Type d'autorité de certification : | Racine d'entreprise | |
| Nom de l'autorité de certific | Fournisseur de services de | RSA#Microsoft Software Key Storage Provider | |
| Période de validité | Algorithme de hachage : | SHA1 | |
| Base de données de certificats | Longueur de la dé : | 2048 | |
| Confirmation | Autoriser l'interaction avec le fournisseur de services de chiffrement : | Désactivé | |
| D (a deta | Période de validité du certificat : | 30/06/2018 00:04 | |
| Resultats | Nom unique : | CN=eu-cosign-ca,DC=eu,DC=cosign | |
| | Emplacement de la base de données de certificats : | C:\Windows\system32\CertLog | |
| | Emplacement du journal de la base de données de certificats : | C: \Windows\system32\CertLog | - - |
| a | Imprimer, envoyer ou enregistrer cette | information | 1 |
| | | < Précédent Suivant > Installer Annule | r L |
| 🖉 Démarrer | | FR 🕆 🕞 📳 🕼 30/ | 00:07 06/2013 💻 |

Figure 67 : AD CS : clé privée : confirmation



Figure 68 : AD CS : clé privée : résultats

| Gestionnaire de serveur | | | | | |
|--|---|--|--|--|--------------------------------------|
| Fichier Action Affichage ? | Propriétés de : pts-WI | N-U9FPOA3GL | D9-C A | | ? × |
| | Agents d'inscription | Audit | Agents de | récupération | Sécurité |
| Gestionnaire de serveur (WIN-U9FP0A3GLD9) Rôles Gestionnaire de serveur (WIN-U9FP0A3GLD9) Rôles Gestionaire de serveur d'applications Gervices Bureau à distance Gervices de certificats Active Directory RNI d'entreprise Modèles de certificats (WIN-U9FP0 Certificats délivrés Certificats délivrés Certificats délivrés Certificats délivrés Certificats de certificats Modèles de c | Agents d'inscription Extensions Général Autorité de certificati Nom : Certificats d'autorité d Certificat n° 0 Paramètres de chiffre Fournisseur : Microsoft Software K Algorithme de hacha SHA1 | Audit Stockage Module de pts-WIN-U9Ff de certification : ement ey Storage Prov ge : | Agents de > 0 stratégie P0A3GLD9-CA | récupération àestionnaires de Module | Sécurité certificats de sortie |
| | | or 15 | | 6 F | |
| | | | Annuler | Appliquer | Aide |



| Certificat | × |
|--|----|
| Général Détails Chemin d'accès de certification | 1 |
| Informations sur le certificat | |
| Ce certificat est conçu pour les rôles suivants : | |
| Toutes les stratégies d'émissions Toutes les stratégies d'application | |
| | |
| | |
| | |
| Délivré à : pts-WIN-U9FP0A3GLD9-CA | |
| Délivré par : pts-WIN-U9FP0A3GLD9-CA | |
| Valide du 27/06/2013 au 27/06/2018 | |
| | |
| Déclaration de l'émette | ur |
| En savoir plus sur les <u>cercificats</u> | |
| o | ĸ |

Figure 70 : AD CS: Certificat AD CS

Conseil: exporter ce certificat dans un fichier %USERPROFILE%\Desktop**ad-cs-rootca.cer**

Rebooter le Domain Controller.

Une fois que le Domain Controller a rebooté, le certificat délivré par l'AD CS au Domain Controler apparaît dans le liste des certificats délivrés par l'AD CS :



Figure 71 : AD: Certificat AD deliver par AD CS

| Certificat X |
|--|
| Général Détails Chemin d'accès de certification |
| |
| Informations sur le certificat |
| Ce certificat est conçu pour les rôles suivants : |
| Garantit votre identité auprès d'un ordinateur distant Garantit l'identité d'un ordinateur distant |
| · Garantit Indentite u un ordinateur distant |
| |
| |
| |
| Délivré à : WIN-U9FP0A3GLD9.pts.psce.fde.fr |
| |
| Délivré par : pts-WIN-U9FP0A3GLD9-CA |
| Valide du 27/ 06/ 2013 au 27/ 06/ 2014 |
| |
| |
| Déclaration de l'émetteur |
| En cavoir plus cur les certificats |
| En savoir plas sur los <u>corançaes</u> |
| |
| |

Figure 72 : AD: Certificat AD DomainController délivré par AD CS

Conseil: exporter ce certificat dans un fichier %USERPROFILE%\Desktop\ad-dc-rootca.cer

Sur un SI en production, l'autorité racine (ACR) ne doit pas délivrée de certificats end-user directement : on préférera créer une autorité intermédiaire (ACI) qui le fera.

Le rôle AD CS est critique dans ce type de système. Se posent en particulier les questions de continuité de service en cas de défaillance de la machine hébergeant ce service ou d'expiration des certificats d'ACRR ou d'ACI.

En production, il faut donc prévoir une sauvegarde de ces environnements et éventuellement de mettre en œuvre le séquestre Microsoft (KRA – Key Recovery Agent).

12.6 Installation d'un rôle Terminal Server

12.6.1 Installation des composants du rôle Terminal Server

Terminal Server s'installe en ajoutant le rôle « **Service de bureau à distance** ». Le serveur doit rebooter à la fin de l'installation du rôle.



Figure 73 : Terminal Server : installation du rôle

| 🙀 W2008R2-Base - VMware Player (N | Ion-commercial use only) | |
|---|--|---|
| Player 👻 🔛 💌 💼 📷 | | * |
| Assistant Ajout de rôles | | × |
| Sélectionner les | services de rôle | |
| Avant de commencer | Sélectionner les services de rôle à installer pour Services Bureau à distance : | F |
| Rôles de serveurs | Services de rôle : Description : | |
| Services Bureau à distance Services de rôle Compatibilité des applications Méthode d'authentification Mode de licence Groupes d'utilisateurs Expérience dient Confirmation État d'avancement Résultats | ✓ Hôte de session Bureau à distance ☐ Hôte de virtualisation des services Bureau à distance ☐ Services de base ☐ RemoteFX ☐ Gestionnaire de licences des services Bureau à distance ☐ Service Broker pour les connexions Bureau à distance ☐ Passerelle des services Bureau à distance ☐ Accès Bureau à distance par le Web | tent aux à des les : reau à shiques |
| | En savoir plus sur les services de rôle | 1 |
| | < Précédent Suivant > Installer Annu | uler |
| Momerrer | 📑 🧾 FR 客 🕞 🧐 😘 💡 | 00:09 30/06/2013 💻 |

Figure 74 : Terminal Server : service de rôle : choisir « Hôte de session Bureau à distance »

| 🙀 W2008R2-Base - VMware Player (M | lon-commercial use only) | |
|---|--|--------|
| Player 👻 🔛 💌 📰 📑 | | * |
| Assistant Ajout de rôles | | × |
| Spécifier une mé | thode d'authentification pour le service Hôte de session Bureau à distance | e |
| Avant de commencer Rôles de serveurs Services Bureau à distance Services de rôle Compatibilité des applications <u>Méthode d'authentification</u> Mode de licence Groupes d'utilisateurs Expérience dient Confirmation État d'avancement Résultats | L'authentification au niveau du réseau est une nouvelle méthode d'authentification qui améliore la sécurité en fournissant une authentification d'utilisateur plus tôt dans le processus de connexion lorsqu'un dient se connecte à un serveur Hôte de session Bureau à distance. Avec l'authentification au niveau du réseau, l'authentification de l'utilisateur intervient avant l'établissement d'une connexion Bureau à distance au serveur Hôte de session Bureau à distance. Spécifiez si l'authentification au niveau du réseau est requise. © Exiger l'authentification au niveau du réseau Seuls les ordinateurs qui exécutent une version de Windows et une version du client Connexion Bureau à distance prenant en charge l'authentification au niveau du réseau peuvent se connecter à ce serveur Hôte de session Bureau à distance. Si vous êtes connecté à distance à ce serveur, vérifiez que votre ordinateur prend en charge l'authentification au niveau du réseau Les ordinateurs qui exécutent une des versions du client Connexion à ce serveur. © Ne nécessite pas l'authentification au niveau du réseau Les ordinateurs qui exécutent une des versions du client Connexion Bureau à distance peuvent se connecter à ce serveur Hôte de session Bureau à distance. W Cette option est moins sécurisée que l'authentification au niveau du réseau car l'authentification intervient plus tard dans le processus de connexion. | e r |
| 1 | | |
| | < Précédent Suivant > Installer Annuler | Ĩ |
| Marrer | FR R P P & 00:10 30/06/20 |)13 💻 |

Figure 75 : Terminal Server : mode d'authentification RDP : Choisir « Ne nécessite pas l'authentification au niveau réseau »

« L'authentification au niveau réseau » est une fonctionnalité récente des serveurs RDP Microsoft. Des tests sont en cours pour vérifier que les Cryptolib CPS supportent ce mode en Smartcard logon.

| 🛱 W2008R2-Base - VMware Player (Non-commercial use only) | | |
|---|--|--|
| Player 👻 🔛 💌 🙀 🏹 | | * |
| Assistant Ajout de rôles | | × |
| Spécifier le mode | e de licence | |
| Avant de commencer Rôles de serveurs Services Bureau à distance Services de rôle Compatibilité des applications Méthode d'authentification <u>Mode de licence</u> Groupes d'utilisateurs Expérience dient Confirmation État d'avancement Résultats | Le mode de licence des services Bureau à distance détermine le type de licence d'accès dient aux services Bureau à distance qu'un serveur de licences doit délivrer aux dients qui se connectent à ce serveur Hôte session Bureau à distance. Spécifiez le mode de licence des services Bureau à distance que ce serveur Hôte de session Bureau à dist doit utiliser. © Configurer ultérieurement Me rappeler d'utiliser l'outil de configuration d'hôte de session Bureau à distance ou la stratégie de gu pour configurer le mode de licence dans les 120 jours suivants. © Par périphérique Une licence d'accès client aux services Bureau à distance par périphérique doit être disponible pour ce périphérique qui se connecte à ce serveur Hôte de session Bureau à distance. © Par utilisateur Une licence d'accès client aux services Bureau à distance par utilisateur doit être disponible pour cha utilisateur qui se connecte à ce serveur Hôte de session Bureau à distance. () Le mode de licence que vous spécifiez doit correspondre aux licences d'accès client aux services Bureau distance disponibles auprès de votre serveur de licences des services Bureau à distance. | tance tance roupe thaque eau à |
| | En savoir plus sur le mode de licence des services Bureau à distance | |
| | < Précédent Suivant > Installer Annuler | r L |
| Marrer bémarrer | FR 🖈 🔁 🕼 30/ | 00:10 06/2013 💻 |

Figure 76 : Terminal Server : mode de licence : Choisir « Configurer ultérieurement »

L'activation et l'installation des licences RDP doit faire l'objet d'une attention particulière. Elle n'est pas « urgente ». Même si elle n'est pas effectuée, des tests sont possibles. Cf. ci-après.

| 🙀 W2008R2-Base - VMware Player (N | ion-commercial use only) | <u> </u> |
|---|---|----------|
| Player 👻 🔛 💌 📑 | | * |
| Assistant Ajout de rôles | | ×1 |
| Sélectionner les Bureau à distanc | groupes d'utilisateurs autorisés à accéder à ce serveur Hôte de sessior e | |
| Avant de commencer Rôles de serveurs Services Bureau à distance | Ajoutez les utilisateurs ou les groupes d'utilisateurs qui peuvent se connecter à ce serveur Hôte de sessior Bureau à distance. Ces utilisateurs et groupes d'utilisateurs seront ajoutés au groupe Utilisateurs du Burea distance. Le groupe Administrateurs est ajouté par défaut et ne peut pas être supprimé. | au à |
| Services de role | Consateurs ou groupes a dunsateurs : | _, H |
| Méthode d'authentification | Administrateurs | - ∥ |
| Mode de licence | Supprime | r |
| Groupes d'utilisateurs | | |
| Expérience client | | Γ |
| Confirmation | | |
| État d'avancement | | |
| Résultats | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | En savoir plus sur le groupe Utilisateurs du Bureau à distance | |
| | | |
| | < Précédent Suivant > Tostaller Annuler | |
| | |):11 _ |
| Démarrer | | 5/2013 = |

Figure 77 : Terminal Server : utilisateurs : garder « Administrateurs »

Il conviendra d'ajouter le groupe « Utilisateurs de bureau à distance » plus tard dans la configuration du serveur (cf. ci-après).

| 🔂 W2008R2-Base - VMware Player (Non-commercial use only) | | | | |
|---|---|------------------|--|--|
| Player 👻 🔛 💌 📷 | | * | | |
| Assistant Ajout de rôles | | ×I | | |
| Configurer l'expé | érience client | | | |
| Avant de commencer Rôles de serveurs Services Bureau à distance | Vous pouvez configurer le serveur Hôte de session Bureau à distance de façon que les utilisateurs se connectant à une session de Bureau à distance puissent utiliser une fonctionnalité similaire à celle fournie j Windows 7. | e Dar | | |
| Services de rôle Compatibilité des applications | La mise en œuvre de cette fonctionnalité nécessite des ressources système et de bande passan supplémentaires et peut affecter l'évolutivité du serveur Hôte de session Bureau à distance. | te . | | |
| Méthode d'authentification Mode de licence | Sélectionnez la fonctionnalité que vous souhaitez fournir. Une fonctionnalité supplémentaire peut être configurée en utilisant l'outil de configuration d'hôte de session Bureau à distance. | | | |
| Groupes d'utilisateurs Expérience dient Confirmation | La sélection de Lecture audio et vidéo ou de Composition du Bureau installe la <u>fonctionnalité</u> <u>Expérience utilisateur</u> sur le serveur Hôte de session Bureau à distance. | | | |
| État d'avancement Résultats | Lecture audio et vidéo <u>R</u> edirection de l'enregistrement audio <u>C</u> omposition du Bureau (fournit les éléments de l'interface utilisateur de Windows Aero) | | | |
| | Si une sélection est estompée, un paramètre de stratégie de groupe est actuellement appliq l'ordinateur et empêche la configuration de cette fonctionnalité. Pour plus d'informations, consultez la rubrique sur les <u>paramètres de stratégie de groupe et la configuration de</u> <u>l'expérience client</u> . En saveir plus eu la configuration de l'expérience client. | ué à | | |
| Memarrer | < <u>Précédent</u> <u>Suivant</u> > <u>Installer</u> <u>Annuler</u> FR R R R R R R R R R R |):13 6/2013 💻 | | |

Figure 78 : Terminal Server : expérience client

Un reboot est nécessaire.

| 🔁 W2008R2-Base - VMware Player (N | on-commercial use only) | |
|--|---|-----------------|
| Player 👻 🔛 💌 📑 | | * |
| Assistant Reprise de la configuratio | n 💦 | ×1 |
| Résultats de l'ins | tallation | |
| Reprise de la configuration État d'avancement | Les rôles, les services de rôle ou les fonctionnalités suivants ont été installés : | |
| Résultats | Services Bureau à distance Services Bureau à distance | — II |
| | Les services de rôle suivants ont été installés : Hôte de session Bureau à distance Activez les fonctionnalités Windows 7 sur ce serveur Hôte de session Bureau à distance à l'aide d la fonctionnalité Expérience Bureau. | e de |
| l. | Imprimer, envoyer ou enregistrer le rapport d'installation | |
| Ĭ | < Précédent Suivant > Fermer Annuler | |
| 灯 Démarrer | FR R 00 | :17 5/2013 💻 |

Figure 79 : Terminal Server : résultat de l'installation

12.6.2 Activation du serveur de licence RDP

Une fois le rôle installé, il faut activer le serveur de licences RDP via le **Gestionnaire des licences des services Bureau à distance.** Cette activation est gratuite. Elle se fait auprès de Microsoft. Elle peut se faire ultérieurement.



Figure 80 : Terminal Server : Lancer le Gestionnaire des licences des services Bureau à distance



Figure 81 : Terminal Server : Clic-droit > propriétés

Préciser les propriétés du serveur de licences :



Figure 82 : Terminal Server : Mode de connexion > Navigateur Web

Puis choisir « Activer le serveur » (griser en figure 81).

Le serveur peut être réactivé (clic-droit > avancé > Réactivé le serveur).

12.6.3 Configurations des comptes « Serveurs de licences des services Terminal Serveur »

Le compte sous lequel tourne le serveur de licences ainsi que le compte « SERVICE RESEAU » doivent faire partie du groupe « Serveurs de licences des services Terminal Serveur »

| ropriété | s de : Serveurs de lic | ences des services Terminal Server | ? × |
|-------------------|------------------------|---|--------|
| Général | Membres Membre de | Géré par Objet Sécurité Éditeur d'attr | ibuts |
| Membre | es : | | |
| Nom | | Dossier Services de domaine Active Dire | ectory |
| - <u>&</u> Ac | lministrateur | eu.cosign/Users | |
| SE 🔮 SE | RVICE RÉSEAU | AUTORITE NT | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| • | | | |
| Ajou | iter Supprimer | 1 | |
| | | 1 | |
| | | | |
| | | OK Annuler Appliquer | Aide |
| | | | |

Figure 83 : Terminal Server : Configurations des comptes « Serveurs de licences des services Terminal Serveur »

12.6.4 Installation des licences sur le serveur de licences

L'installation de licences est payante. Là aussi un délai d'évaluation est accordé, ce qui permet de faire quelques tests en attendant d'acheter les licences requises (ordres d'idées : 35€ la licence CAL, 150€ le pack de 5 licences CAL, cf. Microsoft ou revendeurs, hors prix des licences serveur). Elle peut se faire dans la foulée de l'activation du serveur de Bureau à distance ou ultérieurement par clic droit sur le serveur puis « Installer les licences ».


Figure 84 : Terminal Server : Fin de l'activation du serveur de licences Terminal Serveur

| Assistant Activation du serve | ur | × |
|--|--|---|
| Programme de licence Sélectionnez le programm | e de licence approprié. | |
| Chaque client se connect hôte de virtualisation des s licence d'accès client aux services Terminal Server o avec lequel vous avez ac | ant à un serveur hôte de session Bureau à distance ou un serveur services Bureau à distance (le cas échéant) doit posséder une services Bureau à distance, une licence d'accès client aux ou une licence VDI valide. Sélectionnez le programme de licence heté vos licences. | |
| P <u>r</u> ogramme de licence : | Pack de licence (vers. comm.) | |
| Description : | Cette licence a été achetée en quantité prédéfinie dans un magasin ou chez un distributeur. Le package peut s'appeler « Pack de licence client Microsoft Windows ». | |
| Format et emplacement : | Le code de licence contenu dans le Pack de licence sera demandé. Le code de licence est une suite de cinq jeux de cinq caractères alphanumériques. | |
| Exemple : | 1A2B3 1A2B3 1A2B3 1A2B3 1A2B3 | |
| Vérifiez que vos informatio | ns de licence sont similaires à l'exemple avant de continuer. | |
| Figure | 85 : Terminal Server : Installation d'un pack de licences | |

12.6.5 Configuration de l'hôte Terminal Server

| Gestionnaire de serveur (FR-ASIPSANTE-00) | Diagnostic des licen | ces (FR-ASIPSANTE-00) |
|--|--------------------------------|--|
| 🖻 💕 Roles | l'hôte de session Bureau à di | stance |
| Gestionnaire Fichier Action | Affichage ? | |
| Configuratio | | |
| | | |
| FR-ASIP | hôte de session Général | Actions |
| Fonctionnali 😥 Bureaux à distance | | 📔 Services Bureau à distance 🔹 🔸 |
| E Diagnostics | ession Bureau à distance | Analyseur de performances |
| E O Perform Gestionnaire de licences | des services Bureau à distance | 🚡 Assistant Configuration de la sécurité |
| Gestionnaire des services | s Bureau à distance | Configuration du système |
| Invite de co 🔄 Gestionnaire RemoteApp | | Diagnostic de mémoire Windows |
| Plac patra | | 🔄 Explorateur de stockage |
| - Dioc-hotes | | 🚼 Gestion de l'ordinateur |
| Gestionnaire de licences des | Administrateur | Gestion du partage et du stockage |
| aligi services Bureau à distance | | 🚡 Gestionnaire de serveur |
| Gestionnaire des services Bureau à | Documents | S Initiateur iSCSI |
| | Ordinateur | Boservateur d'événements |
| Configuration d'hôte de session Bureau à distance | | Pare-feu Windows avec fonctions avancees de securite |
| ~ | Réseau | Crunearde de Wiedene Carner |
| Services | - | Services de composants |
| | Panneau de configuration | Service |
| | Périphériques et imprimantes | Sources de données (ODBC) |
| | - enprienques et imprimarices | Stratégie de sécurité locale |
| | Outils d'administration | Windows PowerShell Modules |
| | and the second | |
| | Alde et support | |
| | Exécuter | |
| - | | |
| Tous les programmes | | |
| Rechercher les programmes et fichiers | Fermer la session | |

Figure 86 : Terminal Server : Configuration d'hôte de session Bureau à distance

| Général | | |
|--|---------------------------------|--|
| Supprimer les dossiers temporaires en quittant | Oui | |
| 🖆 Utiliser des dossiers temporaires par session | Oui | |
| 🚰 Restreindre chaque utilisateur à une seule ses | Oui | |
| 🖆 Mode d'ouverture de session de l'utilisateur | Autoriser toutes les connexions | |
| Gestionnaire de licences | | |
| 🚰 Mode de licence des services Bureau à dista | Parutilisateur | |
| 🖆 Serveurs de licences des services Bureau à d | Spécifié | |
| Service Broker pour les connexions Burea | u à distance | |
| Membre d'une batterie dans le service Broker | Non | |
| Virtualisation IP des services Bureau à dis | tance | |
| Virtualisation IP | Non activé | |

Figure 87 : Terminal Server : Configuration d'hôte de session Bureau à distance > mode de licence et serveurs de licences

| | Service Broker p | pour les connexions Bureau a distance |
|--|---|--|
| | Virtualisation | n IP des services Bureau à distance |
| | Général | Gestionnaire de licences |
| lode | de licence des service | es Bureau à distance |
| c | Non spécifié | |
| C | Par périphérique | |
| - | - | |
| Sen Le s licer | Par <u>u</u> tilisateur reurs de licences des s erveur hôte de session ice d'accès client aux s ices spécifiés selon l'or | services Bureau à distance 1 Bureau à distance enverra des demandes de services Bureau à distance aux serveurs de rdre dans lequel ils sont répertoriés. |
| Sen Le s licer licer | Par utilisateur reurs de licences des s erveur hôte de session ice d'accès client aux s ices spécifiés selon l'or eurs de licences spécif | services Bureau à distance n Bureau à distance enverra des demandes de services Bureau à distance aux serveurs de ırdre dans lequel ils sont répertoriés. fiés : |
| Sen Le s licer licer <u>S</u> erv | Par utilisateur reurs de licences des s erveur hôte de session ice d'accès client aux s ices spécifiés selon l'or eurs de licences spécif ipsante-00 | services Bureau à distance n Bureau à distance enverra des demandes de services Bureau à distance aux serveurs de ırdre dans lequel ils sont répertoriés. fiés : |
| Sen Le s licen licen <u>S</u> erv fr-as | Par utilisateur veurs de licences des s erveur hôte de session ice d'accès client aux s ices spécifiés selon l'or eurs de licences spécif ipsante-00 | services Bureau à distance n Bureau à distance enverra des demandes de services Bureau à distance aux serveurs de irdre dans lequel ils sont répertoriés. fiés : Monter |
| (• Sen Le s licer licer <u>S</u> erv | Par <u>u</u> tilisateur veurs de licences des s erveur hôte de session ice d'accès client aux s ices spécifiés selon l'or eurs de licences spécif ipsante-00 | services Bureau à distance n Bureau à distance enverra des demandes de services Bureau à distance aux serveurs de irdre dans lequel ils sont répertoriés. fiés : <u>Monter</u> |
| Serv Le s licer <u>S</u> erv fr-as | Par <u>u</u> tilisateur veurs de licences des s erveur hôte de session ice d'accès client aux s ices spécifiés selon l'or eurs de licences spécif apsante-00 | services Bureau à distance n Bureau à distance enverra des demandes de services Bureau à distance aux serveurs de irdre dans lequel ils sont répertoriés. fiés : <u>Monter</u> <u>Descendre</u> |
| Serv Le s licer <u>Serv</u> fr-as | Par <u>u</u> tilisateur veurs de licences des s erveur hôte de session ice d'accès client aux s ices spécifiés selon l'or eurs de licences spécif ipsante-00 | services Bureau à distance n Bureau à distance enverra des demandes de services Bureau à distance aux serveurs de indre dans lequel ils sont répertoriés. filés : <u>Monter</u> <u>Descendre</u> |
| Sen Le s licer licer | Par <u>u</u> tilisateur veurs de licences des s erveur hôte de session ice d'accès client aux s ices spécifiés selon l'or eurs de licences spécif ipsante-00 Aiouter | services Bureau à distance n Bureau à distance enverra des demandes de services Bureau à distance aux serveurs de irdre dans lequel ils sont répertoriés. fiés : |

Figure 88 : Terminal Server : Configuration d'hôte de session Bureau à distance > mode de licence et serveurs de licences

12.6.6 Paramétrage du serveur RDP

Une fois le rôle installé, le paramétrage du serveur RDP et des comptes se font de la façon suivante :



Figure 89 : Terminal Server : Configuration des paramètres serveur

| Paramètres de déploien | ent RemoteApp | X | | |
|--|--|--|--|--|
| Signature numérique P Serveur hôte de session Br | aramètres RDP communs ireau à distance Passerelle | Paramètres RDP personnalisés des services Bureau à distance | | |
| Les clients utiliseront ces session Bureau à distance | paramètres lorsqu'ils se conne e. | cteront à ce serveur hôte de | | |
| Nom du serveur : | cosign | | | |
| _ | Si le serveur hôte de session dans une batterie de serveurs | Bureau à distance se trouve s, entrez le nom DNS de | | |
| Port <u>R</u> DP : | 8389 | | | |
| Accès au Bureau à distance Afficher une connexion Bureau à distance sur ce serveur hôte de session Bureau à distance dans l'accès Bureau à distance par le Web Accéder aux programmes non listés Ne pas permettre aux utilisateurs de démarrer les programmes non répertoriés sur la connexion initiale (Becommandé) | | | | |
| O Permettre aux utilisateurs de démarrer les programmes répertoriés et non | | | | |
| | | | | |
| | 0 <u>K</u> | Annuler <u>Appliquer</u> | | |

Figure 90 : Terminal Server : config. nom du serveur et port externe

| Assistant RemoteApp | × |
|--|---|
| Choisir les programmes à ajouter à la liste des programmes RemoteApp Sélectionnez les programmes que vous souhaitez ajouter à la liste Programmes RemoteApp. Vous pouvez également configurer des propriétés RemoteApp distinctes, comme l'îcône à afficher. | |
| Nom Informations système Initiateur iSCSI Module Active Directory pour Windows PowerShell Moniteur de ressources Imitiateur is Se connecter à un projecteur Sources de données (ODBC) Vindows PowerShell Vindows PowerShell Vindows PowerShell Vindows PowerShell Vindows PowerShell (x86) Vindows Update Vindows Update VordPad | |
| | |

Figure 91 : Terminal Server : Déclaration d'une remote app de test

Démarrer, click Exécuter..., « cmd » puis entrer "control system", « Paramètres système avancés », « Utilisation à distance » :

| opriétés système | | | 2 |
|--|-----------------------|-----------------------|-------------------|
| Nom de l'ordinateur Paramètres système avancés | l l | Maté Jtilisation à | iriel distance |
| Assistance à distance | | | |
| Autoriser les connexions d'assistance | à distanc | e vers cet i | ordinateur |
| | | Options a | a <u>v</u> ancées |
| ⊢ Bureau à distance | | | |
| Cliquez sur une option puis spécifiez qui p | eut se co | nnecter. | |
| C Ne <u>p</u> as autoriser les connexions à cet | ordinateu | r | |
| Autoriser la connexion des ordinateurs version du Bureau à distance (moins s | exécutar ûr) | nt n'importe | quelle |
| C N'autoriser <u>q</u> ue la connexion des ordir distance avec authentification NLA (pl | iateurs ex us sûr) | écutant le | Bureau à |
| Comment choisir ? | <u>S</u> électio | nnez des u | tilisateurs |
| | | |] |
| ОК | - / | Annuler | Appliquer |

Figure 92 : Terminal Server : Compatibilité ascendante RDP

« Sélectionnez des utilisateurs... » fait apparaitre la fenêtre suivante :



Figure 93 : Terminal Server : Ajout d'utilisateur du bureau à distance



Figure 94 : Terminal Server : Groupe utilisateur du Bureau à distance

« Démarrer > Exécuter...> secpol.msc » :

| Stratégie de sécurité locale | | |
|--|---|----------------------------|
| Eichier Action Affichage ? | | |
| 🗢 🔿 🞽 🖬 💥 🖬 🗟 🖬 | | |
| 🚡 Paramètres de sécurité | Stratégie 🔺 | Paramètre de sécurité |
| 🗉 📴 Stratégies de comptes | 🖾 Augmenter une plage de travail de processus | Utilisateurs |
| 🖃 📴 Stratégies locales | 闕 Autoriser l'ouverture de session par les services Bureau à distance | Administrateurs |
| E Stratégie d'audit | 🗒 Changer le fuseau horaire | SERVICE LOCAL, Administr |
| Attribution des droits utilisateur | 🚰 Charger et décharger les pilotes de périphériques | Administrateurs, Opérateu |
| 🗄 📴 Options de securite | Contourner la vérification de parcours | Tout le monde,Utilisateurs |
| Pare-reu windows avec fonctions avance Stratégies du gestionpaire de listes de réu | 🔯 Créer des liens symboliques | Administrateurs |
| Stratégies de dé publique | 📓 Créer des objets globaux | SERVICE LOCAL, SERVICE |
| | 🗓 Créer des objets partagés permanents | |
| Stratégies de restriction logicielle Stratégies de contrôle de l'application | 🛗 Créer un fichier d'échange | Administrateurs |
| 🗉 🥷 Stratégies de sécurité IP sur Ordinateur k | 📓 Créer un objet-jeton | |
| 🗉 🎽 Configuration avancée de la stratégie d'a | 🚰 Déboguer les programmes | Administrateurs |
| | Effectuer les tâches de maintenance de volume | Administrateurs |
| | B Emprunter l'identité d'un client après l'authentification | SERVICE LOCAL, SERVICE |
| | Forcer l'arrêt à partir d'un système distant | Administrateurs,Opérateu |
| | Générer des audits de sécurité | SERVICE LOCAL, SERVICE |
| | 🚰 Gérer le journal d'audit et de sécurité | Administrateurs |
| | 📖 Interdire l'accès à cet ordinateur à partir du réseau | |
| | 📖 Interdire l'ouverture d'une session locale | |
| | 📖 Interdire l'ouverture de session en tant que service | |
| | 📖 Interdire l'ouverture de session en tant que tâche | _ |
| | 🔯 Interdire l'ouverture de session par les services Bureau à distance | |
| | 🚰 Modifier l'heure système | SERVICE LOCAL, Administr |
| | 🛗 Modifier les valeurs de l'environnement du microprogramme | Administrateurs |
| | 🔯 Modifier un nom d'objet | |
| | 🗒 Ouvrir une session en tant que service | NT SERVICE ALL SERVICE |
| | 🚰 Ouvrir une session en tant que tâche | Administrateurs,Opérateu |
| | 🗄 Derformance système du profil | Administrateurs NT SED//I |
| | | |

Figure 95 : Terminal Server : Droits d'ouverture de session à distance

| ropriétés | de : Autoriser l'ou | verture de se | ssion par les ser | vices B ? |
|--------------------|-----------------------------------|----------------|-----------------------|------------------|
| Paramètre | de sécurité locale E | xpli | de : Autoriser l'ouve | erture de sessi |
| | Autoriser l'ouverture distance | de session par | les services Bureau | à |
| Administ COSIGN | rateurs IVflorent.desgrippes | | | |
| | | | | |
| Ajoute | r un utilisateur ou un g | groupe | Supprimer |] |
| | | | | |
| | | OK | 1 Annular 1 | Appliquer |

Figure 96 : Terminal Server : Droits d'ouverture de session à distance pour un utilisateur précis

Il est possible d'ajouter à cet endroit le groupe « Utilisateur du Bureau à distance » :

| Propriétés de : Autoriser l'ouverture de session | nar les services B |
|--|--------------------|
| | |
| Parametre de securite locale Expliquer | 1 |
| Autoriser l'ouverture de session par les ser distance | rvices Bureau à |
| | |
| Administrateurs Utilisateurs du Bureau à distance | |
| | |
| | |
| | |
| Ajouter un utilisateur ou un groupe | Supprimer |
| | |
| | |
| | |
| | |
| ОК | Annuler Appliquer |

Figure 97 : Terminal Server : Droits d'ouverture de session à distance pour le groupe « Utilisateur du Bureau à distance »

12.6.7 Configuration du certificat du serveur RDP

Sur une infrastructure de production, le lien RDP doit être correctement paramétré.

En particulier, si le rôle AD CS est installé sur un serveur du SI, il est possible de faire signer le certificat serveur du lien RDP par l'autorité de certification racine de l'AD CS. De fait, ceci est même conseiller dans la mesure où le certificat racine de l'AD CS est provisionné via l'AD dans les magasins de certificats des postes clients.

http://blogs.msdn.com/b/rds/archive/2010/04/09/configuring-remote-desktop-certificates.aspx

(Malheureusement, documentation assez incomplète, un peu complétée ici) :



Figure 98 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS

| Propriétés de : RemoteDesktopComputer | <u>? ×</u> |
|--|------------|
| Conditions d'émission Modèles obsolètes Extensions Sécurité Servi Général Modèles Traitement de la demande Nom du sujet Nom du s | eur |
| RemoteDesktopComputer Autorités de certification minimales prises en Windows Server 2003 Enterprise charge : Nom du modèle : | |
| RemoteDesktopComputer Période de validité : Période de renouvellement : Image: Image | |
| Publier le certificat dans Active Directory Ne pas utiliser la réinscription automatique si un certificat dupliqué existe dans Active Directory | |
| Pour le renouvellement automatique des certificats de carte à puce, utiliser la clé existante si la création d'une clé est impossible | |
| OK Annuler Appliquer Aide | • |

Figure 99 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS

| 🛼 Gestionnaire de serveur | | |
|---|--|-----------------------------------|
| Fichier Action Affichage ? | | |
| 🗢 🔿 🗾 🖻 🗟 🔒 🛛 🗊 | | |
| Gestionnaire de serveur (WIN-U9FP0A3GLD9) | Propriétés du nouveau modèle | × |
| Serveur d' Console1 - [Racine de la console\Modèles c Service S Servi | Général Traitement de la demande Nom du sujet Serveur Conditions d'émission Modèles obsolètes Extensions Sécurité Pour modifier une extension, sélectionnez-la et cliquez su Ajouter une stratégie d'application (nor Windows 2000) définit la manié Sélectionnez la stratégie d'application (serveur Vindows 2000) définit la manié Sélectionnez la stratégies d'application (serveur stratégies d'application Stratégies d'application : Stratégies d'application | Incation |
| Image: Constraint of the second s | A. Utilisation de la clé Nouvelle stratégie d'application Entrez le nom de la nouvelle stratégie d'application, puis modifie Tridentification du client Authentification du client Authentification du serve Identificateur d'objet : I.3.6.1.4.1.311.54.1.2 | sz sz Annuler OK Annuler |
| Gestionne Configuration Stockane | OK Annuler Appliquer Aide | |

Figure 100 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS

| 🛜 Console1 - [Racine de la console\Modèles de certificats (WIN-U9FP0A3GLD9.pts.psce.fde.fr)] | | | | |
|--|---|----------------------------|---------|--------------------------|
| 🚡 Fichier Action Affichage Favoris Fenêtre ? | | | | |
| 🗢 🔿 🖄 📊 🗶 📄 🔒 👔 | | | | |
| 📔 Racine de la console | Nom complet du modèle 🔺 | Autorités de certification | Version | Rôles prévus 🔺 |
| 🚇 Modèles de certificats (WIN-U9FF | 🚇 IPSEC (requête hors connexion) | Windows 2000 | 7.1 | |
| | 🚇 Ordinateur | Windows 2000 | 5.1 | |
| | 🚇 Points de distribution de certificats croisés | Windows Server 2003 Ent | 105.0 | |
| | 🚇 Réplication de la messagerie de l'annuaire | Windows Server 2003 Ent | 115.0 | Réplication de messag |
| | Routeur (requête hors-connexion) | Windows 2000 | 4.1 | |
| | 🚇 Serveur RAS et IAS | Windows Server 2003 Ent | 101.0 | Authentification du clie |
| | 🚇 Serveur Web | Windows 2000 | 4.1 | |
| | 🖳 Session authentifiée | Windows 2000 | 3.1 | |
| | 🚇 Signature de l'utilisateur uniquement | Windows 2000 | 4.1 | |
| | 🚇 Signature de liste d'approbation | Windows 2000 | 3.1 | |
| | 🚇 Signature de réponse OCSP | Windows Server 2008 Ent | 101.0 | Signature OCSP |
| | 🚇 Signature du code | Windows 2000 | 3.1 | |
| | 🚇 Signature Exchange uniquement | Windows 2000 | 6.1 | |
| | 🚇 Utilisateur | Windows 2000 | 3.1 | |
| | 🚇 Utilisateur de carte à puce | Windows 2000 | 11.1 | |
| | 🚇 Utilisateur Exchange | Windows 2000 | 7.1 | |
| | | Windows Server 2003 Ent | 100.2 | Remote Desktop Comp |
| | • | | | Þ |
| | | | | |

Figure 101 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS

| 🧱 Console1 - [Racine de la console\Autorité de certification (Local)\pts-WIN-U9FP0A3GLD9-CA\Modèles de certificats] | | | | | |
|---|--|--|--|--|--|
| 🚟 Fichier Action Affichage Favor | 🚡 Fichier Action Affichage Favoris Fenêtre ? | | | | |
| 🗢 🔿 🙋 🖬 🤷 📾 | | | | | |
| 📔 Racine de la console | Nom | Rôle prévu | | | |
| Modèles de certificats (WIN-U9FF | RemoteDesktopComputer | 1.3.6.1.4.1.311.54.1.2 | | | |
| 🖃 🚋 Autorité de certification (Local) | 🚇 Réplication de la messagerie de l'annuaire | Réplication de messages du service d'annu | | | |
| 🖃 🚮 pts-WIN-U9FP0A3GLD9-CA | 🚇 Authentification du contrôleur de domaine | Authentification du client, Authentification | | | |
| Certificats révoqués | 🚇 Agent de récupération EFS | Récupération de fichiers | | | |
| Certificats délivrés | 🚇 EFS basique | Système de fichiers EFS (Encrypting File Sy | | | |
| Demandes en attente | 🚇 Contrôleur de domaine | Authentification du client, Authentification | | | |
| Demandes ayant echoue | 🚇 Serveur Web | Authentification du serveur | | | |
| | 🚇 Ordinateur | Authentification du client, Authentification | | | |
| | 🚇 Utilisateur | Système de fichiers EFS (Encrypting File Sy | | | |
| | 🚇 Autorité de certification secondaire | <tous></tous> | | | |
| | R Administrateur | Signature de liste d'approbation Microsoft, \ldots | | | |

Figure 102 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS

| Propriétés de : RemoteDesktopComputer | <u>? ×</u> |
|--|--|
| Général Traitement de la demande Conditions d'émission Modèles obsolètes Extensions | Nom du sujet Sécurité Serveur |
| Administrateur Administrateur Administrateur Administrateur Administrateur Administrateurs du domaine (PTS\Adminis du domaine) Administrateurs du domaine (PTS\Ordinateurs du domaine) Administrateurs de l'entreprise (PTS\Administrateurs de l'entre | eprise) |
| Autorisations pour Administrateur | ijouter Supprimer Autoriser Refuser |
| Contrôle total Lecture Écriture Inscrire Inscription automatique | |
| Pour les autorisations spéciales et les paramètres avancés, clique Avancé. Informations sur le contrôle d'accès et les autorisations | z sur <u>Avancé</u> |
| OK Annuler | Appliquer Aide |

Figure 103 : Terminal Server : Droits sur le modèle de certificat Remote Desktop

| Propriétés de : RemoteDesktopComputer | ?> |
|--|----------------------------------|
| Général Traitement de la demande Conditions d'émission Modèles obsolètes Extensions | Nom du sujet Sécurité Serveur |
| Noms de groupes ou d'utilisateurs : | reprise) |
| Autorisations pour WIN-U9FP0A3GLD9 | Ajouter Supprimer |
| Contrôle total Lecture Écriture Inscrire Inscription automatique | |
| Pour les autorisations spéciales et les paramètres avancés, clique Avancé. Informations sur le contrôle d'accès et les autorisations | ez sur Avancé |
| OK Annuler | Appliquer Aide |

Figure 104 : Terminal Server : Droits sur le modèle de certificat Remote Desktop

| 📕 Éditeur de gestion des stratégies de groupe | | | | | |
|---|--|--|---------------------------|--|----------------------|
| Fichier Action Affichage ? | | | | | |
| 🗢 🔿 🖄 📷 🗟 🖬 🛛 🐨 | | | | | |
| 🗈 🧰 Sauvegarde 🖉 | 🧧 Sécurité | | | | |
| Serveur pour NIS | | | | | |
| Service d'installation ActiveX | Modèle de certificat | Paramètre | | État | Commentaire |
| Service Digital Locker | d'authentification serveur | 📰 Modèle de certificat d'authentific | cation serveur | Activé | Non |
| Service Journal des evenements | 11 10 1 N TO 1 | • • • • • • • • • • • • • • • • • • • | de la accession altrait | Min | Man and and |
| Services ADFS (Active Directory Federation Serv | Modifier <u>le parametre</u> Modèle de c | ertificat d'authentification serveu | ur | | |
| E Client Connexion Pureau à distance | Configuration requise 📰 Madàla da | soutificant d'authomatification converue | | | |
| Gestionpaire de licences des services Bureau | Au minimum Windows | ceruncacu authenuncation serveur | Paramètre | précédent Paramé | ètre suivant |
| Hôte de la session Bureau à distance | Description (| | | | |
| Compatibilité des applications | Ce paramètre de stra' C Non config | uré Commentaire : | | | A |
| | permet de spécifier le | | | | |
| Délais d'expiration des sessions | de certificat qui déter (Activé | | | | |
| Dossiers temporaires | authentifier un server construction | | | | - |
| Environnement de session à distance | session Bureau à dista | | | | |
| Gestionnaire de licences | | Pris en charge sur : Au mir | inimum Windows Vista | | <u>^</u> |
| 🦰 Profils | Un certificat est néces | | | | - |
| Redirection de l'imprimante | session Bureau à dista | I | | | |
| Redirection de périphérique et de ressou | (TLS 1.0) est utilisé pc Options : | | Aide : | | |
| Sécurité | communications entre | | | | |
| Service Broker pour les connexions Bure- | distance pendant des | | | | |
| Stratégies de lecture automatique | (Remote Desktop Prot Nom du modè | le de certificat | ce parametre de strateg | jie vous permet de spec i détermine le certificet | célectionné |
| Synchronisation de mot de passe | RemoteDeskto | nComputer | automatiquement nour | authentifier un sen/eur | Hôte de la session |
| Système de couleurs Windows | Si ce parametre de sti | peoinpater | Bureau à distance. | addrenance arrocited | |
| H lablet PC | de modèle de certifica | | | | |
| Iransfert dievenements - | certificats créés à l'aic | | Un certificat est nécessa | aire pour authentifier ur | n serveur Hôte de la |
| Windows Derender | certificat spécifié sont | | session Bureau à distan | ce lorsque SSL (TLS 1.0) | est utilisé pour |
| Windows Installer | certificat pour authen | | sécuriser les communic | ations entre un client et | t un serveur Hôte |
| Windows Media Center | Hôte de la session Bui | | de la session Bureau à c | listance pendant des co | nnexions RDP |
| Windows Messenger | Un certificat est sélec | | (Remote Desktop Proto | coi). | |
| <u>▲ </u> | Étendu Standard | | Si ce paramètre de strat | égie est activé, yous de | vez spécifier un |
| 7 paramètre(s) | | | nom de modèle de cert | ificat. Seuls les certificat | ts créés à l'aide du |

Figure 105 : Terminal Server : Déploiement du modèle de certificat Remote Desktop sur les postes clients via l'AD

| 🚟 Console_smartcard_login - [Racine de la console\Certifica | ats (ordinateur local)\Personnel\Certifi | icats] | |
|---|--|----------------------|--------------------|
| 🚟 Fichier Action Affichage Favoris Fenêtre ? | | | _ _ 8 × |
| 🗇 🔿 🗾 📋 😟 💀 🔽 🖬 | | | , |
| 📔 Racine de la console | ▲ Délivré à ▲ | Délivré par | Actions |
| 🕀 🟥 PKI d'entreprise | GIP-CPS | GIP-CPS | Certificats |
| Stratégie Default Domain Controllers Policy [WIN-U9FP0A3GL Gertificate (ordinateur local) | GIP-CPS ANONYME | GIP-CPS ANONYME | Autres actions |
| | GIP-CPS PROFESSIONNEL | GIP-CPS PROFESSIONNE | |
| | GIP-CPS STRUCTURE | GIP-CPS STRUCTURE | |
| Aut Ioutes les taches Demar | nder un nouveau certificat | WINH INFORCED | |
| Cor Affichage | sce.fde.fr | pts-WIN-U9FP0A3GLD9- | |
| Aut Nouvelle fenêtre à partir d'ici Opéra Opéra | itions avancées 🔹 🕨 p9 | WMSvc-WIN-U9FP0A3GL | |
| | | | |
| E Aut Actualizar | | | |
| Per Exporter la liste | | | |
| | | | |
| | | | |
| Barines de confiance de carte à nuce | | | |
| | | | |
| 표 🧮 Périphériques approuvés | | | |
| 🗄 📃 Utilisateurs et ordinateurs Active Directory [WIN-U9FP0A3GL] | ┛Ĺ | | |
| | | Þ | |
| Demander un nouveau certificat à une autorité de certification de votre | domaine | | |

Figure 106 : Terminal Server : Demande de certificat Terminal Server

| 🙀 Inscription de certificats | | |
|---|--|------------------------------|
| 🙀 Inscription de certificats | | |
| Demander des certificats Vous pouvez demander les types de certificats suiv cliquez sur Inscription. | ants. Sélectionnez les certificats que | e vous voulez demander, puis |
| Stratégie d'inscription à Active Dire | ctory | |
| Authentification du contrôleur de domaine | 🔱 Statut : Disponible | Détails 🛞 |
| Contrôleur de domaine | 😲 Statut : Disponible | Détails 🛞 |
| | 😲 Statut : Disponible | Détails 🛞 |
| Réplication de la messagerie de l'annuaire | 🗘 Statut : Disponible | Détails 🛞 |
| Afficher tous les modèles En savoir plus sur les <u>certificats</u> | | |
| | | Inscription Annuler |

Figure 107 : Terminal Server : Demande de certificat Terminal Server : Sélection de « RemoteDesktopComputer »

| 🔙 Insc | ription de certificats | | |
|--------|--|------------------------------------|-----------|
| ᇘ Insc | cription de certificats | | |
| R | tésultats de l'installation des certific es certificats suivants ont été inscrits et in | ats stallés sur cet ordinateur. | |
| [| Stratégie d'inscription à Activ | e Directory | |
| | RemoteDesktopComputer | Statut : Opération réussie | Détails 🛞 |
| | | | Terminer |

Figure 108 : Terminal Server : Demande de certificat Terminal Server





| Console_smartcard_login - [Racine de la console\Certificats (ordinateur local)\Personnel\Certificats] | | | | | | |
|---|--|------------------------|-------------------|---|-----------------|--|
| 🚟 Fichier Action Affichage Favoris Fenêtre ? | Fichier Action Affichage Favoris Fenêtre ? | | | | | |
| 🗢 🔿 📶 🤞 🖕 🗙 🗉 🔒 🚺 🖬 | | | | | | |
| 🧮 Racine de la console 📃 | Délivré à 🔺 | Délivré par | Date d'expiration | Rôles prévus | Nom convivial | |
| 🖻 🏥 PKI d'entreprise | GIP-CPS | GIP-CP5 | 31/12/2020 | <tout></tout> | <aucun></aucun> | |
| pts-WIN-U9FP0A3GLD9-CA (V0.0) | GIP-CPS ANONYME | GIP-CP5 ANONYME | 31/12/2020 | <tout></tout> | <aucun></aucun> | |
| E I Stratégie Default Domain Controllers Policy [WIN-U9FP0A3GL | GIP-CPS PROFESSIONNEL | GIP-CP5 PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun></aucun> | |
| 🖃 🙀 Certificats (ordinateur local) | GIP-CPS STRUCTURE | GIP-CPS STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | |
| E Personnel | gpts-WIN-U9FP0A3GLD9-CA | pts-WIN-U9FP0A3GLD9-CA | 27/06/2018 | <tout></tout> | <aucun></aucun> | |
| Certificats | WIN-U9FP0A3GLD9 | WIN-U9FP0A3GLD9 | 10/09/2013 | Authentification du serveur | <aucun></aucun> | |
| Autorites de certification racines de confiance | WIN-U9FP0A3GLD9.pts.psce.fde.fr | pts-WIN-U9FP0A3GLD9-CA | 27/06/2014 | Authentification du client, Authentification du serveur | <aucun></aucun> | |
| Contrance de l'entreprise | WIN-U9FP0A3GLD9.pts.psce.fde.fr | pts-WIN-U9FP0A3GLD9-CA | 05/07/2014 | Remote Desktop Computer | <aucun></aucun> | |
| Autorites de cercificación internieulaires Éditeurs approuvés | WMSvc-WIN-U9FP0A3GLD9 | WM5vc-WIN-U9FP0A3GLD9 | 10/03/2023 | Authentification du serveur | <aucun></aucun> | |
| File Certificats non autorisés | | | | | | |
| 🗉 🧮 Autorités de certification racine tierce partie | 1 | | | | | |
| | 1 | | | | | |
| 🗆 🖴 Domete Dockton | 1 | | | | | |

Figure 110 : Terminal Server : Vérification du certificat Terminal Server émis sur le Terminal Serveur

Conseil : sauvegarder ce certificat sous le nom %USERPROFILE%\Desktop\rd-rootca.cer

Figure 111 : Terminal Server : Installation du certificat Terminal Server

- 1. mmc.exe (Microsoft Management Console)
- 2. ajouter le composant enfichable: certificates ("computer" -> "ordinateur local" / "local computer")
- 3. Répertoire "remote desktop" -> certificats
- 4. Effacer le certificate for the name of the server and close the mmc instance

| 🖀 Console_smartcard_login - [Racine de la console\Certificats (ordinateur local)\Remote Desktop\Certificats] 📃 🛛 🗶 | | | | |
|---|---------------------------------|----------------------|----------------------------------|----------|
| 🚟 Fichier Action Affichage Favoris Fenêtre ? | | | | × |
| 🗢 🔿 🙍 🔏 💺 💥 🖬 🛃 🖬 | | | | |
| 📔 Racine de la console 📃 | Délivré à 🔺 | Délivré par | Actions | |
| 🛨 🟥 PKI d'entreprise | WIN-U9FP0A3GLD9.pts.psce.fde.fr | WIN-U9FP0A3GLD9.pts. | Certificats | |
| 🗄 🧾 Stratégie Default Domain Controllers Policy [WIN-U9FP0A3GL | | | | |
| E Grificats (ordinateur local) | | | Autres actions | 1 |
| Personnel Autoritée de cartification regimes de configues | | | WIN-LIGEPOA3GLD9.pts.psce.fde.fr | |
| Adorices de Centincation racines de conmance | | | | |
| Connance de rencieprise Autorités de certification intermédiaires | | | Autres actions | <u>۲</u> |
| Image: Trades do contractor integration Image: Trades do contractor integration Image: Trades do contractor Image: Trades do contractor <t< td=""><td></td><td></td><td></td><td></td></t<> | | | | |
| Certificats non autorisés | | | | |
| 🕀 🛅 Autorités de certification racine tierce partie | | | | |
| 🛨 🚞 Personnes autorisées | | | | |
| 🖃 🚞 Remote Desktop | | | | |
| Certificats | | | | |
| 🗄 🚞 Demandes d'inscription de certificat | | | | |
| 🕀 🔛 Racines de confiance de carte à puce | | | | |
| | | | | |
| Périphériques approuvés | | | | |
| Utilisateurs et ordinateurs Active Directory [WIN-U9FP0A3GL] | | | | |
| Domaines et approbations Active Directory [w1N-D9PP0A3GL - | | | | |
| | | | | _ |
| Le magasin Remote Desktop contient 1 certificat. | | | | |

Figure 112 : Terminal Server : Configuration

- 5. Outils d'administration -> Services de bureau à distance -> Configuration d'hôte de session Bureau à distance
- 6. rdp -tcp -> clic droit -> propriétés

| 🖡 Gestionnaire de serveur | | |
|--|---|--|
| Fichier Action Affichage ? | | |
| 🗇 🔿 🗾 🔽 🗾 | | Propriétés de RDP-Tcp |
| Gestionnaire de serveur (WIN-U9FP0A3GLD9) Rôles Serveur d'applications Serveur Web (IIS) Services Bureau à distance Gestionnaire RemoteApp (WIN-U9FP0A3GLD Configuration dhôte de session Bureau à distance Gestionnaire des services Bureau à distance Gestionnaire des services Bureau à distance | Configuration d'hôte de session Bureau à distan Configuration du serveur hôte de WIN-U9FPOA3GLD9 Vous pouvez utiliser l'outil de configuration d'hôte de ses connexions, modifier ceux des connexions existantes et : connexion par connexion, ou pour le serveur hôte de ses | Contrôle à distance Paramètres du client Carte réseau Sécurité Général Paramètres d'ouverture de session Sessions Environnement Type : RDP-Tcp Transport : tcp Commentaire : |
| Gervices de certificats Active Directory Services de domaine Active Directory Services de domaine Active Directory Services de domaine Active Directory Solutionalités Diagnostics Sobservateur dévénements Sestionnaire de périphériques Gestionnaire de périphériques Configuration Stockage | Connexions Nom de la connexion Type de connexion Tran BDP-Tcp Microsoft RDP 7.1 tcp | Securité Négocier La couche la plus sécuritée prise en charge par le client sera utilisée. Si le protocole SSL (TLS 1.0) est pris en charge, il sera utilisé. Niveau de chiffrement : Compatible client Toutes les données envoyées entre le client et le serveur sont protégées par un chiffrement basé sur la puissance maximale prise en charge par le client. |
| | Modifier les paramètres Général E Supprimer les dossiers temporaires en quittant Utiliser des dossiers temporaires par session Utiliser des dossiers temporaires par session Mode d'ouverture de session de l'utilisateur Au Gestionnaire de licences Mode de licence des services Bureau à dista No Serveurs de licences des services Bureau à d | Autoriser les connexions uniquement à patir des ordinateurs exécutant le Bureau à distance avec une authentification au niveau du réseau Certificat : <u>Généré automatiquement</u> <u>Sélectionner</u> Par défaut <u>En savoir plus sur la configuration des paramètres de sécurité</u> <u>OK</u> Annuler <u>Appliquer</u> on spéché |

Figure 113 : Terminal Server : Installation du certificat Terminal Server

7. Sélectionner -> retrouver le certificat Remote Desktop :

| _ | Propriétés de RDP-Tcp | <u>x</u> | |
|----------------|---|--|------------|
| n | Contrôle à distance Paramètres du clier Général Paramètres d'ouverture de sessi | Sécurité de Windows | × |
| 5: | | Sélectionner un certificat | on |
| Bı im Bı | Type : HDP-I cp Transport : tcp Commentaire : Sécurité | WMSvc-WIN-U9FP0A3GL Émetteur : WMSvc-WIN-U9FP0A3GLD9 Valide à partir du : 12/03/2013 au 10/0 | |
| l | Couche de Sécurité : Ne La couche la plus sécurisée prise en char le protocole SSL (TLS 1.0) est pris en cha | pts-WIN-U9FP0A3GLD9-CA Émetteur : pts-WIN-U9FP0A3GLD9-CA Valide à partir du : 27/06/2013 au 27/0 | : ₽ |
| _ | Niveau de chiffrement : Co Toutes les données envoyées entre le cli par un chiffrement basé sur la puissance i client. | WIN-U9FP0A3GLD9.pts.ps Émetteur : pts-WIN-U9FP0A3GLD9-CA Valide à partir du : 05/07/2013 au 05/0 Cliquez ici pour afficher les propriétés | |
| | Autoriser les connexions uniquement à exécutant le Bureau à distance avec u du réseau Certificat : <u>Généré automatin</u> | WIN-U9FP0A3GLD9.pts.ps Émetteur : pts-WIN-U9FP0A3GLD9-CA Valide à partir du : 27/06/2013 au 27/0 | |
| эr | Sélectionner Par défaut En savoir plus sur la configuration des par | OK Annuler | |
| éc | OK . | Annuler Appliquer | |

Figure 114 : Terminal Server : Installation du certificat Terminal Server



Figure 115 : Terminal Server : Vérifier l'installation du certificat Terminal Server

12.6.8 Autres GPOs

| November 2015 - Connexion Bureau à distance | | | |
|--|---|---|---------------|
| 🗢 🄿 🖄 📷 📑 👔 🐨 | | | * |
| 🗐 Stratégie Default Domain Controllers Policy [FR-As | Connexions | | |
| E 🚰 Configuration ordinateur | N'autoriser qu'une session de | Paramètre | État |
| E Strategies | services Bureau à distance par | E Reconnexion automatique | Non configuré |
| Parametres du logiciel | utilisateur | Autoriser les utilisateurs à se connecter à distance à l'aide des se | Non configuré |
| Installation de logiciel | | Refuser la déconnexion d'un administrateur connecté à la session | Non configuré |
| Parametres windows | Modifier <u>le paramètre de stratégie</u> | Configurer l'intervalle de conservation des connexions | Non configuré |
| Strategie de resolution de noms | Configuration requise : | | Non configuré |
| Scripts (demarrage)arret) | Au minimum Windows Server 2003 | E Définir les règles pour le contrôle à distance des sessions utilisate | Non configuré |
| Parametres de securite | | Nautoricer qu'une cession de cervices Bureau à distance par utilis | Décactivé |
| Modèles d'administration : définitions s | Description : Ce paramètre de stratégie yous permet | Autoriser le démarrage distant de programmes pop répertoriés | Non configuré |
| E Composants Windows | de limiter les utilisateurs à une seule | E Décartiver la planification de répartition de charge équilibrée du t | Non configuré |
| Analyse de fiabilité Windows | session de services Bureau à distance. | E Desactiver la planificación de repartición de charge equilibree du C | Non coningere |
| Assistance en ligne | Commentioner en en en el transfere de | | |
| Biométrie | stratégie, les utilisateurs qui ouvrent une | | |
| Calendrier Windows | session à distance via les services Bureau | | |
| Carte à puce | à distance seront limités à une seule | | |
| Centre de mobilité Windows | session (active ou déconnectée) sur ce | | |
| Centre de sécurité | dans un état déconnecté, il se | | |
| 🕀 🧰 Chiffrement de lecteur BitLock | reconnecte automatiquement à cette | | |
| Compatibilité des applications | session lors de la prochaine ouverture de | | |
| Emplacement et capteurs | session. | | |
| 📔 Environnement distant Windov | Si vous désactivez ce paramètre de | | E |
| 📔 Explorateur de jeux | stratégie, les utilisateurs sont autorisés à | | |
| 🕀 🚞 Explorateur Windows | faire un nombre illimité de connexions | | |
| 📔 Flux RSS | simultanees a distance a l'aide des services Bureau à distance. | | |
| 🧮 Gadgets du Bureau | | | |
| | Si vous ne configurez pas ce paramètre | | |
| Gestion des droits numériques | de strategie, le parametre « Limiter les utilisateurs à une seule session » de l'outil | | |
| Gestionnaire de fenêtres du Bi | Configuration de l'hôte de la session | | |
| Gestionnaire de ressources sy | Bureau à distance détermine si les | | |
| Groupe residentiel | utilisateurs sont limités à une seule session de services Bureau à distance | | |
| | session de services bureau à distance. | | |
| Internet Explorer Internet Information Services | 1 | | |
| Lecteur Windows Media | | | |
| | | | |
| Mise à niveau express | | | |
| NetMeeting | 1 | | |
| Observateur d'événements | | | |
| Options d'arrêt | | | |
| Options d'ouverture de session | | | |
| Paramètres de présentation | | | |
| Parental Controls | | | |
| Planificateur de tâches | | | |
| Programme d'amélioration de l' | | | |
| Projecteur réseau | | | |
| Protection d'accès réseau | 1 | | |
| Rapport d'erreurs Windows | | | |
| E Sauvegarde | | | |
| Serveur pour NIS | I | | Ψ |
| • | III | | H. ▲ |

| 🗐 Éditeur de gestion des stratégies de groupe | | |
|--|---|--|
| Fichier Action Affichage ? | | |
| 🔶 🄿 🞽 💼 🗟 🖬 🛛 🍸 | | |
| Service Digital Locker 📃 | Connexions | |
| | N'autoriser qu'une session de services Bureau à distance par utilisateur | Paramètre Reconnexion automatique Autoriser les utilisateurs à se connecter à distance à l'aic |
| Redirection de périphé Gestionnaire de licences de Hôte de la session Bureau Compatibilité des appli | Modifier <u>le paramètre de stratéqie</u> Configuration requise : Au minimum Windows Server 2003 | El Refuser la déconnexion d'un administrateur connecté à l El Configurer l'intervalle de conservation des connexions El Limiter le nombre de connexions El Définir les règles pour le contrôle à distance des sessions |
| Connexions Connexions Délais d'expiration des Dossiers temporaires Environnement de ses Gestionnaire de licence | Description : Ce paramètre de stratégie vous permet de limiter les utilisateurs à une seule session de services Bureau à distance. | N'autoriser qu'une session de services Bureau à distance Autoriser le démarrage distant de programmes non répe Désactiver la planification de répartition de charge équilil |
| Profils Profils Redirection de l'imprim Sécurité Service Broker pour le: Stratégies de lecture automati Synchronisation de mot de pa: Système de couleurs Windows | Si vous activez ce paramètre de stratégie, les utilisateurs qui ouvrent une session à distance via les services Bureau à distance seront limités à une seule session (active ou déconnectée) sur ce serveur. Si l'utilisateur quitte la session dans un état déconnecté, il se reconnecte automatiquement à cette session lors de la prochaine ouverture de session. | |
| Transfert d'événements | Si vous désactivez ce paramètre de stratégie, les utilisateurs sont autorisés à faire un nombre illimité de connexions simultanées à distance à l'aide des services Bureau à distance. | |
| | Étendu / Standard / | |
| 9 paramètre(s) | | |

12.7 Installation d'un rôle IIS

| 🙀 W2008R2-Base - VMware Player (N | 🖥 W2008R2-Base - VMware Player (Non-commercial use only) | | | | | | | |
|-----------------------------------|---|---|--|--|--|--|--|--|
| Player 👻 🔛 💌 📷 | | « | | | | | | |
| Assistant Ajout de rôles | A | × | | | | | | |
| Sélectionnez des | rôles de serveurs | - | | | | | | |
| Avant de commencer | Sélectionnez un ou plucieurs rôles à installer sur ce serveur | - III - I | | | | | | |
| Rôles de serveurs | Rôles : | Description : | | | | | | |
| Serveur Web (IIS) | | Serveur Web (IIS) fournit une | | | | | | |
| Services de rôle | Serveur d'applications | infrastructure d'application Web fiable, | | | | | | |
| Confirmation | Serveur de télécopie | gerable et evolutive. | | | | | | |
| État d'annual | Serveur DHCP | | | | | | | |
| Etat d avancement | Serveur DNS | | | | | | | |
| Résultats | Services AD LDS (Active Directory Lightweight Directory Services) | | | | | | | |
| | Services AD RMS (Active Directory Rights Management Services) | | | | | | | |
| | Services ADFS (Active Directory Federation Services) | | | | | | | |
| | Services Bureau à distance (Installé) | | | | | | | |
| | Services de certificats Active Directory (Installe) | | | | | | | |
| | Services de decliments et d'impression | | | | | | | |
| | ✓ Services de docainer la ce a impression ✓ Services de domaine Active Directory (Installé) | P1 | | | | | | |
| | Services de fichiers | | | | | | | |
| | Services de stratégie et d'accès réseau | | | | | | | |
| | Services WSUS (Windows Server Update Services) | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | En savoir plus sur les rôles de serveur | 4 | | | | | | |
| - | | 4 | | | | | | |
| L . | | | | | | | | |
| <u>L</u> | < Précédent Suivant | > Installer Annuler | | | | | | |
| 🌌 Démarrer | | FR 🛠 📜 🏷 00:18 30/06/2013 💻 | | | | | | |

Figure 116 : IIS: Installation du rôle



Figure 117 : IIS: Installation du rôle : sélection des options de sécurité

| 🙀 W2008R2-Base - VMware Player (Non- | commercial use only) | <u> </u> |
|--------------------------------------|--|--------------------|
| Player 👻 🔛 💌 🔚 🏹 | | * |
| Assistant Ajout de rôles | | ۱۱ |
| Progression de l'ins | tallation | |
| Avant de commencer | Les rôles, les services de rôle ou les fonctionnalités suivants sont en cours d'installation : | Ē |
| Rôles de serveurs | Serveur Web (IIS) | - 11 |
| Serveur Web (IIS) | | |
| Services de rôle | | 4 |
| Confirmation | | |
| Etat d'avancement | | |
| Resultats | | |
| | | |
| | | 1 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | - |
| | Gamma Installation | |
| - | | ľ |
| Ĩ | < Précédent Suivant > Instalier Annuler | 1 |
| 🎝 Démarrer 🛛 🏭 🕢 🚞 | FR R 10 10 10 10 10 10 10 10 10 10 10 10 10 | 00:20 06/2013 💻 |

Figure 118 : IIS: Installation du rôle : état d'avancement



Figure 119 : IIS: Installation du rôle : Résultat

12.8 Installation de la Cryptolib CPS sur le serveur

Afin de pouvoir faire du Smartcard logon à base de CPS via TSE, il est nécessaire d'installer les Cryptolib CPS 64bit sur le serveur TSE en étant administrateur de la machine, en sus du rôle « Terminal Server ». cf. « Points d'attention » par ailleurs.

Conseil : ne pas laisser les fichiers .msi d'installation sur un serveur de production (sécurité), à défaut : vérifier que les droits accordés sur les .msi sont adéquates.

12.8.1 Désactivation du CCM au lancement

Dans ce cas, sur le serveur, il est conseillé de ne pas lancer le CCM automatiquement :

démarrer > **exécuter**...> « **msconfig** » > « **Démarrage** » > **décocher** « **CPS CCM** » (reboot requis mais une option « ultérieurement » permet d'attendre le prochain reboot).

12.8.2 Activation du CCM à l'ouverture de session au cas par cas

Eventuellement, lancer le CCM au démarrage des sessions utilisateurs (copie du raccourci « CCM.exe » dans le répertoire « Démarrage » du profil de l'utilisateur -%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup):



Figure 120 : CCM: lancement du CCM au démarrage des sessions utilisateurs sur un serveur Windows

12.8.3 Remarque sur le provisionning des magasins de certificats

Si l'installation de la Cryptolib CPS est réalisée côté serveur, les magasins de certificats (root et intermédiaire) sont provisionnés avec les certificats ASIP Santé de production. Si des cartes de test sont utilisées en maquette, il faut tout de même provisionner ces magasins avec

les chaines de tests (voir Configuration du Contrôleur de domaine pour la Smartcard logon).

12.9 Installation du Provider de révocation ASIP Santé – Microsoft sur le serveur

Le Provider de révocation ASIP Santé développé par Microsoft doit être installé sur chaque contrôleur de domaine pour la vérification des CRLs des certificats client de la carte.

12.9.1 Installation du Provider de révocation ASIP Santé – Microsoft

| 🙀 GIP-CPS Revocation Provider for | Windows | |
|--|---|---|
| Select Installation Folde | r | |
| The installer will install GIP-CPS Revocati To install in this folder, click "Next". To in Folder: | ion Provider for Windows to the fol stall to a different folder, enter it be | lowing folder. Ilow or click "Browse". |
| C:\Program Files\GIP-CPS\ | | Browse |
| | | Disk Cost |
| | | |
| | Cancel < Back | Next > |

Figure 121 : CPSRev: répertoire d'installation

| 🕌 C:\Program Files\GIP-CP | C:\Program Files\GIP-CPS | | | | | | |
|--|--|------------------|------------------------|--------|-------|---|--|
| 🕞 🖓 🚽 🗸 🗸 | · ▼ Disque local (C:) ▼ Programmes ▼ GIP-CPS | - 🚱 | Rechercher dans : GIP- | CPS | | 2 | |
| Organiser ▼ Indure dans la bibliothèque ▼ Partager avec ▼ Nouveau dossier | | | | | | | |
| 쑦 Favoris | Nom * | Modifié le | Туре | Taille | | | |
| 📃 Bureau | 🚳 CPSRev.dll | 18/10/2011 11:22 | Extension de l'applic | | 85 Ko | | |
| Emplacements récents | license.txt | 18/10/2011 11:23 | Document texte | | 22 Ko | | |
| Téléchargements | RegCPSRev.exe | 18/10/2011 11:23 | Application | | 55 Ko | | |
| Bibliothèques Documents Images Musique Vidéos Ordinateur Disque local (C:) | | | | | | | |
| 실 Lecteur de DVD (D:) G 에 Réseau I♥ MACHA I♥ vmware-host | | | | | | | |
| 3 élément(s) | | | | | | | |

Figure 122 : CPSRev: résultat d'installation

12.9.2 Mise à jour des magasins de certificats Local Machine

Il est ensuite nécessaire de mettre à jour les magasins de certificats Local machine.

Vérifier le magasin « Local machine \ racine » : Les certificats ASIP Santé <u>racine</u> doivent être présents.

| ፳ Console_cosign - [Racine de la console\Certificats (ordinateur local)\Autorités de certification racines de confiance\Certificats] | | | | | | | _ 8 × |
|--|--------------------------------------|---|-------------------|-------------------------------|------------------------|----------------|-------|
| 🚡 Eichier Action Affichage Fayoris Fegêtre 2 | | | | | | _ 8 × | |
| 🗢 🔿 🗾 📋 🖻 💀 🔽 🗊 | | | | | | | |
| 📔 Racine de la console | Délivré à 🔺 | Délivré par | Date d'expiration | Rôles prévus | Nom convivial | Actions | |
| Certificats - Utilisateur actuel | ASIP-SANTE TECHNIQUE | ASIP-SANTE TECHNIQUE | 31/12/2030 | <tout></tout> | <aucun></aucun> | Certificats | |
| E Personnel | Baltimore CyberTrust Root | Baltimore CyberTrust Root | 13/05/2025 | Authentification du s | Baltimore CyberTrust | Autros actions | • |
| Ceruncais Ceruncais Autoritón do contification racinos do configuro | Class 3 Public Primary Certification | Class 3 Public Primary Certification A | 02/08/2028 | Messagerie électroni | VeriSign Class 3 Publi | Add es acuoris | |
| Certificats | Class 3 Public Primary Certification | Class 3 Public Primary Certification A | 08/01/2004 | Messagerie électroni | VeriSign | | |
| E Confiance de l'entreprise | Copyright (c) 1997 Microsoft Corp. | Copyright (c) 1997 Microsoft Corp. | 31/12/1999 | Enregistrement des i | Microsoft Timestamp | | |
| Autorités de certification intermédiaires | Leu-cosign-ca | eu-cosign-ca | 30/06/2018 | <tout></tout> | <aucun></aucun> | | |
| Liste de révocation des certificats | Egleu-cosign-ca | eu-cosign-ca | 30/06/2018 | <tout></tout> | <aucun></aucun> | | |
| Certificats | Lalgip-CPS | GIP-CPS | 31/12/2020 | <iout></iout> | <aucun></aucun> | | |
| Objet utilisateur Active Directory | GIP-CPS ANONYME | GIP-CPS ANONYME | 31/12/2020 | <lout></lout> | <aucun></aucun> | | |
| Editeurs approuvés | GIP-CPS PROFESSIONNEL | GIP-CPS PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| E Certificats non autorisés | | GIP-CPS STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Autorités de certification racine tierce partie | CTE CuberTaust Clebal Deat | GIP-CPS-TEST | 14/02/2010 | <10Ut> Magazania électroni | <aucun></aucun> | | |
| Personnes autorisees | Signa of Authorities de (tra) Deet | Missaad Authoritized (br) Deet Au | 14/08/2018 | Messagerie electroni | GTE Cyber trust Glob | | |
| Cortificate (ordinate de carte a puce | Microsoft Root Authority | Microsoft Root Authority | 21/12/2020 | Touts | Microsoft Root Auth | | |
| | Microsoft Root Cortificate Authority | Microsoft Root Cartificate Authority | 10/05/2020 | Tout> | Microsoft Root Cartif | | |
| Certificats | | NO LIABILITY ACCEPTED (c)97 Veri | 08/01/2021 | Enregistrement des i | VeriSign Time Stampi | | |
| Autorités de certification racines de confiance | TEST ANONYME | TEST ANONYME | 31/12/2020 | <tout></tout> | <augun></augun> | | |
| Certificats | TEST PROFESSIONNEL | TEST PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| E Confiance de l'entreprise | TEST STRUCTURE | TEST STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Autorités de certification intermédiaires | TEST TECHNIQUE | TEST TECHNIQUE | 31/12/2030 | <tout></tout> | <aucun></aucun> | | |
| Liste de révocation des certificats | Thawte Timestamping CA | Thawte Timestamping CA | 01/01/2021 | Enregistrement des i | Thawte Timestampin | | |
| Certificats | VeriSign Class 3 Public Primary Cer | VeriSign Class 3 Public Primary Certifi | 17/07/2036 | Authentification du s | VeriSian | | |
| Editeurs approuvés | WMSvc-WIN-92TJH90G03S | WMSvc-WIN-92TJH90G03S | 28/06/2023 | Authentification du s | <aucun></aucun> | | |
| Certificats non autorises | | | | | | | |
| Autorites de certification racine tierce partie | | | | | | | |
| Personnes autonsees | | | | | | | |
| Centre Description de certificat | | | | | | | |
| Racines de confiance de carte à puce | | | | | | | |
| Périphériques approuvés | | | | | | | |
| 🗉 🎆 Configuration d'hôte de session Bureau à distance | | | | | | | |
| 🗄 式 Domaines et approbations Active Directory | | | | | | | |
| 🗉 🧾 Stratégie Default Domain Controllers Policy [WIN-9. | | | | | | | |
| 🗈 📷 Gestionnaire des services Bureau à distance | | | | | | | |
| 🖭 🏥 PKI d'entreprise | | | | | | | |
| Sites et services Active Directory [WIN-92TJH90G0 | | | | | | | |
| 🗄 🧮 Utilisateurs et ordinateurs Active Directory [WIN-9: | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | 1 | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | <u> </u> | | | | Þ | | |
| magasin Autorités de certification racines de confiance contient 24 certificats. | | | | | | | |

Figure 123 : CPSRev: vérification du magasin Root (Local machine)

A minima, les 5 certificats <u>racine</u> de production de l'ASIP Santé doivent être présents (se reporter au chapitre « Détails de certificat »):

Si des cartes de test sont utilisées (environnements de tests et d'homologation), les 5 certificats racine de test de l'ASIP Santé doivent être présents (se reporter au chapitre « Détails de certificat »).

Il peut donc y avoir jusqu'à **10** certificats « root » ASIP dans ce magasin.

L'import par fichier « P7B » est possible :

- cer\p7b\01-prod-root.p7b
 - o 5 certificats de production
- cer\p7b\03-test-root.p7b
 - 5 certificats de test
 - cer\p7b\05-all-root.p7b

•

• 10 certificats de production et de test

Conseil : les certificats de <u>test</u> ASIP Santé doivent être supprimés des environnements de production

Conseil : ne pas utiliser le mécanisme Microsoft de sélection automatique du magasin de certificats lors de l'opération d'import !

Vérifier le magasin « Local machine \ intermédiaire » : Les certificats ASIP Santé <u>intermédiaires</u> doivent être présents.

| 🚟 Console_cosign - [Racine de la console\Certifica | Console_cosign - [Racine de la console\Certificats (ordinateur local)\Autorités de certification intermédiaires\Certificats] | | | | | | |
|---|--|--|-------------------|-----------------------|-----------------|--|---|
| Eichier Action Affichage Favoris Fenêtre ? | 🔓 Bichier Action Affichage Fayoris Fenetre 2 | | | | | | |
| (= -) 2 📰 🗈 🕰 💀 👔 🖬 | | | | | | | |
| Racine de la console | Délivré à 🔺 | Délivré par | Date d'expiration | Rôles prévus | Nom convivial | Actions | |
| 🖃 🙀 Certificats - Utilisateur actuel | AC-CLASSE-4 | GIP-CPS | 30/12/2020 | Messagerie électroni | <aucun></aucun> | Certificats | |
| Personnel | AC-CLASSE-4-TEST | GIP-CPS-TEST | 30/12/2020 | Messagerie électroni | <aucun></aucun> | certaileates | |
| Certificats | AC-CLASSE-5 | GIP-CPS | 30/12/2020 | Messagerie électroni | <aucun></aucun> | Autres actions | • |
| Autorités de certification racines de confiance | AC-CLASSE-5-TEST | GIP-CPS-TEST | 30/12/2020 | Messagerie électroni | <aucun></aucun> | | |
| Certificats | AC-CLASSE-6 | GIP-CPS | 30/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Contiance de l'entreprise | AC-CLASSE-6-TEST | GIP-CPS-TEST | 30/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Autorites de certification intermediares | 🛱 eu-cosign-ca | eu-cosign-ca | 30/06/2018 | <tout></tout> | <aucun></aucun> | | |
| Certificate | 🔄 eu-cosign-ca | eu-cosign-ca | 30/06/2018 | <tout></tout> | <aucun></aucun> | | |
| Objet utilizateur: Active Directory | GIP-CPS | GIP-CPS | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Éditeurs approuvés | GIP-CPS ANONYME | GIP-CPS ANONYME | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Certificats non autorisés | GIP-CPS CLASSE-0 | GIP-CPS ANONYME | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Autorités de certification racine tierce partie | GIP-CPS CLASSE-0 | GIP-CPS ANONYME | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Personnes autorisées | GIP-CPS CLASSE-1 | GIP-CPS PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Racines de confiance de carte à puce | GIP-CPS CLASSE-1 | GIP-CPS PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| E G Certificats (ordinateur local) | GIP-CPS CLASSE-2 | GIP-CPS STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| 🗄 🔛 Personnel | GIP-CPS CLASSE-2 | GIP-CPS STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Certificats | GIP-CPS CLASSE-3 | GIP-CPS STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Autorités de certification racines de confiance | GIP-CPS CLASSE-3 | GIP-CPS STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Certificats | GIP-CPS PROFESSIONNEL | GIP-CPS PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| E Confiance de l'entreprise | GIP-CPS STRUCTURE | GIP-CPS STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Autorités de certification intermédiaires | GIP-CPS-TEST | GIP-CPS-TEST | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Liste de révocation des certificats | Microsoft Windows Hardware Compa | tibility soft Root Authority | 31/12/2002 | Signature du code, V | <aucun></aucun> | | |
| Certificats | Root Agency | Root Agency | 01/01/2040 | <tout></tout> | <aucun></aucun> | | |
| Editeurs approuvés | TEST ANONYME | TEST ANONYME | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Certificats non autorises | TEST CLASSE-0 | TEST ANONYME | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Autorites de cerdification racine derce parte | TEST CLASSE-0 | TEST ANONYME | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Personnes autorisees | TEST CLASSE-1 | TEST PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Centre Desktop Demander directintion de certificat | TEST CLASSE-1 | TEST PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Pariner de confiance de carte à nuce | TEST CLASSE-2 | TEST STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| E Périphériques approuvés | TEST CLASSE-2 | TEST STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| + Configuration d'hôte de session Bureau à distance | TEST CLASSE-3 | TEST STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Domaines et approbations Active Directory | TEST CLASSE-3 | TEST STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| 🗉 🧾 Stratégie Default Domain Controllers Policy [WIN-9 | TEST PROFESSIONNEL | TEST PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aurun></aurun> | | |
| 🗉 🚃 Gestionnaire des services Bureau à distance | TEST STRUCTURE | TEST STRUCTURE | 31/12/2020 | <tout></tout> | <aurun></aurun> | | |
| 🗉 🏥 PKI d'entreprise | www.verisian.com/CPS Incorp.by | Class 3 Public Primary Certification A | 25/10/2016 | Authentification du s | <aucun></aucun> | | |
| ⊞ Bites et services Active Directory [WIN-92TJH90G0 | | | | | | | |
| 🕑 📃 Utilisateurs et ordinateurs Active Directory [WIN-9: | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | <u>)</u> | I <u>. </u> | |
| Le magasin Autorites de certification intermédiaires contient | asin Autorites de certification intermediares contient 35 certificatis. | | | | | | |

Figure 124 : CPSRev: vérification du magasin Intermediate CA (Local machine)

A minima, les 15 certificats intermédiaires de production de l'ASIP Santé doivent être présents.

Si des cartes de test sont utilisées (environnements de tests et d'homologation), les 15 certificats intermédiaires de test de l'ASIP Santé doivent être présents.

Il peut donc y avoir jusqu'à **30** certificats « intermédiaires » ASIP dans ce magasin.

L'import par fichier « P7B » est possible (et conseillé!):

- cer\p7b\02-prod-inter.p7b
 - 15 certificats de production
 - cer\p7b\04-test-inter.p7b
 - \circ 15 certificats de test
- cer\p7b\06-all-inter.p7b

•

• 30 certificats de production et de test

Conseil : Se reporter au chapitre « Détails de certificat ») et imprimer ce tableau et matérialiser la vérification en cochant la case « Check »

Conseil : les certificats de <u>test</u> ASIP Santé doivent être supprimés des environnements de production

Conseil : ne pas utiliser le mécanisme Microsoft de sélection automatique du magasin de certificats lors de l'opération d'import !

Vérifier les magasins « Utilisateur actuel » :

Certificats racines :

Les certificats ASIP Santé <u>racine</u> doivent être présents, ils sont normalement provisionnés à partir du moment où le magasin « local machine » correspondant l'a correctement été (cf. étapes précédentes).

| 🐺 Console_cosign - [Racine de la console\Certificats - Utilisateur actuel\Autorités de certification racines de confiance\Certificats] | | | | | | _ 8 × | |
|--|--------------------------------------|---|-------------------|-----------------------|------------------------|----------------|----------|
| 🚡 Ejchier Action Affichage Fayoris Fenetre 2 | | | | | | | |
| 🗢 🔿 🙍 🛅 📋 💁 🛃 🗊 | | | | | | | |
| 📔 Racine de la console | Délivré à 🔶 | Délivré par | Date d'expiration | Rôles prévus | Nom convivial | Actions | |
| 🖃 🗊 Certificats - Utilisateur actuel | ASIP-SANTE TECHNIQUE | ASIP-SANTE TECHNIQUE | 31/12/2030 | <tout></tout> | <aucun></aucun> | Certificats | ^ |
| E Personnel | Baltimore CyberTrust Root | Baltimore CyberTrust Root | 13/05/2025 | Authentification du s | Baltimore CyberTrust | | |
| Certificats | Class 3 Public Primary Certification | Class 3 Public Primary Certification A | 02/08/2028 | Messagerie électroni | VeriSign Class 3 Publi | Autres actions | • |
| Autorites de certification racines de confiance | Class 3 Public Primary Certification | Class 3 Public Primary Certification A | 08/01/2004 | Messagerie électroni | VeriSign | | |
| Certincats | Copyright (c) 1997 Microsoft Corp. | Copyright (c) 1997 Microsoft Corp. | 31/12/1999 | Enregistrement des i | Microsoft Timestamp | | |
| Comance de rentreprise Autorités de certification intermédiaires | 📮 eu-cosign-ca | eu-cosign-ca | 30/06/2018 | <tout></tout> | <aucun></aucun> | | |
| Liste de révocation des certificats | 🖕 eu-cosign-ca | eu-cosign-ca | 30/06/2018 | <tout></tout> | <aucun></aucun> | | |
| Certificats | GIP-CPS | GIP-CPS | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Objet utilisateur Active Directory Objet util | GIP-CPS ANONYME | GIP-CPS ANONYME | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| | GIP-CPS PROFESSIONNEL | GIP-CPS PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| El Certificats non autorisés | GIP-CPS STRUCTURE | GIP-CPS STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Autorités de certification racine tierce partie | GIP-CPS-TEST | GIP-CPS-TEST | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Personnes autorisées | GTE CyberTrust Global Root | GTE CyberTrust Global Root | 14/08/2018 | Messagerie électroni | GTE CyberTrust Glob | | |
| Racines de confiance de carte à puce | Microsoft Authenticode(tm) Root | Microsoft Authenticode(tm) Root Au | 01/01/2000 | Messagerie électroni | Microsoft Authentico | | |
| Certificats (ordinateur local) | Microsoft Root Authority | Microsoft Root Authority | 31/12/2020 | <tout></tout> | Microsoft Root Auth | | |
| Personnel | Microsoft Root Certificate Authority | Microsoft Root Certificate Authority | 10/05/2021 | <tout></tout> | Microsoft Root Certif | | |
| Certification raciona do configence | NO LIABILITY ACCEPTED, (c)97 V | NO LIABILITY ACCEPTED, (c)97 Veri | 08/01/2004 | Enregistrement des i | VeriSign Time Stampi | | |
| Certificate | TEST ANONYME | TEST ANONYME | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Confiance de l'entreprise | TEST PROFESSIONNEL | TEST PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Autorités de certification intermédiaires | La TEST STRUCTURE | TEST STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Liste de révocation des certificats | LETTEST TECHNIQUE | TEST TECHNIQUE | 31/12/2030 | <tout></tout> | <aucun></aucun> | | |
| Certificats | Thawte Timestamping CA | Thawte Timestamping CA | 01/01/2021 | Enregistrement des i | Thawte Timestampin | | |
| Éditeurs approuvés Éditeurs approuvés | Verisign Class 3 Public Primary Cer | verisign Class 3 Public Primary Certifi | 1//0//2036 | Authentification du s | vensign | | |
| El Certificats non autorisés | En WMSVC-WIN-921 JH90G03S | WMSVC-WIN-921JH90G03S | 28/06/2023 | Authentification du s | <aucun></aucun> | | |
| Autorités de certification racine tierce partie | | | | | | | |
| Personnes autorisées | | | | | | | |
| Remote Desktop | | | | | | | |
| Demandes d'inscription de certificat | | | | | | | |
| Racines de confiance de carte à puce | | | | | | | |
| Peripheriques approuves | | | | | | | |
| Configuration dinote de session Bureau a distance | | | | | | | |
| Stratégie Default Domain Controllers Policy M/IN-0 | | | | | | | |
| Gestionnaire des services Rureau à distance | | | | | | | |
| Bertenrise | | | | | | | |
| Sites et services Active Directory [WIN-92TJH90G0] | | | | | | | |
| | | | | | | | |
| - | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | 4 | | | |
| | | | | | Þ |] | |
| s magasin Autorités de certification racines de confiance contient 24 certificatis. | | | | | | | |

Figure 125 : CPSRev: vérification du magasin Root CA (User)

Certificats intermédiaires :

Les certificats ASIP Santé <u>intermédiaires</u> doivent être présents, ils sont normalement provisionnés à partir du moment où le magasin « local machine » correspondant l'a correctement été (cf. étapes précédentes).

| 👼 Console_cosign - [Racine de la console\Certificats - Utilisateur actuel\Autorités de certification intermédiaires\Certificats] | | | | | | | × |
|--|-----------------------------------|--|-------------------|-----------------------|-----------------|----------------|---|
| 🚡 Echier Action Affichage Fagoris Fegètre 2 | | | | | | | × |
| 🗢 🔿 📶 📋 🔯 🗟 🖬 | | | | | | | |
| Racine de la console | Délivré à 🔺 | Délivré par | Date d'expiration | Rôles prévus | Nom convivial | Actions | _ |
| 🖃 🙀 Certificats - Utilisateur actuel | AC-CLASSE-4 | GIP-CPS | 30/12/2020 | Messagerie électroni | <aucun></aucun> | Contificate | |
| Personnel | AC-CLASSE-4-TEST | GIP-CPS-TEST | 30/12/2020 | Messagerie électroni | <aucun></aucun> | Certificatio | |
| Certificats | AC-CLASSE-5 | GIP-CPS | 30/12/2020 | Messagerie électroni | <aucun></aucun> | Autres actions | |
| Autorités de certification racines de confiance | AC-CLASSE-5-TEST | GIP-CPS-TEST | 30/12/2020 | Messagerie électroni | <aucun></aucun> | | |
| Certificats | GAC-CLASSE-6 | GIP-CPS | 30/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Confiance de l'entreprise | GAC-CLASSE-6-TEST | GIP-CPS-TEST | 30/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Autorités de certification intermédiaires | 🛱 eu-cosign-ca | eu-cosign-ca | 30/06/2018 | <tout></tout> | <aucun></aucun> | | |
| Liste de revocation des certificats | au-cosign-ca | eu-cosign-ca | 30/06/2018 | <tout></tout> | <aucun></aucun> | | |
| Certificates | GIP-CPS | GIP-CPS | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Gojet duisateur Acuve Directory | GIP-CPS ANONYME | GIP-CPS ANONYME | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Certificate non autorisée | GIP-CPS CLASSE-0 | GIP-CPS ANONYME | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Autorités de certification racine tierce partie | GIP-CPS CLASSE-0 | GIP-CPS ANONYME | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Personnes autorisées | GIP-CPS CLASSE-1 | GIP-CPS PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Racines de confiance de carte à puce | GIP-CPS CLASSE-1 | GIP-CPS PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Certificats (ordinateur local) | GIP-CPS CLASSE-2 | GIP-CPS STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Personnel | GIP-CPS CLASSE-2 | GIP-CPS STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Certificats | GIP-CPS CLASSE-3 | GIP-CPS STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Autorités de certification racines de confiance | GIP-CPS CLASSE-3 | GIP-CPS STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Certificats | GIP-CPS PROFESSIONNEL | GIP-CPS PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| E Confiance de l'entreprise | GIP-CPS STRUCTURE | GIP-CPS STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Autorités de certification intermédiaires | GIP-CPS-TEST | GIP-CPS-TEST | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Liste de révocation des certificats | Microsoft Windows Hardware Com | Microsoft Root Authority | 31/12/2002 | Signature du code, V | <aucun></aucun> | | |
| Certificats | Root Agency | Root Agency | 01/01/2040 | <tout></tout> | <aucun></aucun> | | |
| Editeurs approuvés | TEST ANONYME | TEST ANONYME | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Certificats non autorisés | TEST CLASSE-0 | TEST ANONYME | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Autorités de certification racine tierce partie | TEST CLASSE-0 | TEST ANONYME | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Personnes autorisees | TEST CLASSE-1 | TEST PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Remote Desktop | TEST CLASSE-1 | TEST PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| E Bacines de confiance de carte à purce | TEST CLASSE-2 | TEST STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Périphériques approuvés | TEST CLASSE-2 | TEST STRUCTURE | 31/12/2020 | <tout></tout> | <aucun></aucun> | | |
| Configuration d'hôte de sersion Bureau à distance | TEST CLASSE-3 | TEST STRUCTURE | 31/12/2020 | Tout | <augun></augun> | | |
| Comigardian anote de session barcad a distance | TEST CLASSE 3 | TEST STRUCTURE | 31/12/2020 | Tout> | <aucun></aucun> | | |
| Stratégie Default Domain Controllers Policy [WIN-9] | | TEST DROFESSIONNEL | 31/12/2020 | Tout> | <aucun></aucun> | | |
| 🗐 📻 Gestionnaire des services Bureau à distance | | TEST STDI ICTI IDE | 31/12/2020 | Tout> | <aucun></aucun> | | |
| 🖭 🏥 PKI d'entreprise | www.verisign.com/CPS Incorp.by | Class 3 Public Primary Certification A | 25/10/2016 | Authentification du c | <aucun></aucun> | | |
| F III Sites et services Active Directory [WIN-92TJH90G0 | Canwww.venaigh.com/er a theorp.by | class 5 Fubic Frinary Certification A | 23/10/2010 | Addicitation do a | CAUCUITZ | | |
| 🗉 📃 Utilisateurs et ordinateurs Active Directory [WIN-9] | | | | | | | |
| - | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | 1 | | | | | | |
| | 1 | | | | | | |
| | 1 | | | | | | |
| | 1 | | | | | | |
| | | | | | | | |
| | 1 | | | | • | | |
| Le magasin Autorités de certification intermédiaires contient | 35 certificats. | | | | | | |

Figure 126 : CPSRev: vérification du magasin Intermediate CA (User)

Conseil : les certificats de <u>test</u> ASIP Santé doivent être supprimés des environnements de production
12.9.3 Configuration du Provider de révocation ASIP Santé – Microsoft

Mettre à jour la base de registre avec les paramètres CPSRev (cf. documentation du provider de révocation ASIP Santé), en particulier si des cartes de tests sont utilisées (prise en compte des cartes non GIP-CPS, les cartes de tests n'en étant pas pour des raisons de sécurité) :

; Configuration de CPSRev pour prendre en compte les certificats de test ASIP Santé:

[HKEY_LOCAL_MACHINE\SOFTWARE\GIPCPS\CPSRev] "LogLevel"=dword:0000003 "WarnIfNotGIPCPSCert"=dword:00000001 "CheckAllCerts"=dword:0000001 "LogUndeterminatedAsError"=dword:00000001

Tableau 20 : CPSRev : Configuration de CPSRev pour prise en compte des certificats de test ASIP Santé

; Désactivation de la vérification des listes de révocation sous Win2008+

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters] "UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kdc] "UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=dword:00000001

 Tableau 21 : CPSRev : Désactivation de la vérification des listes de révocation sous Win2008+

; Activation de la vérification des listes de révocation sous Win2008+

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters] "UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=-

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kdc] "UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=-

Tableau 22 : CPSRev : (Ré-)Activation de la vérification des listes de révocation sous Win2008+

12.9.4 Cas des contrôleurs de domaine avec accès internet : vérification des statuts de certificats « online »

Vérifier les flux vers les serveurs ASIP <u>avec IE</u> :

| Flux HTTP | http://annuaire.gip-cps.fr/crl/test/TEST%20CLASSE-2.crl |
|-----------|---|
| Flux LDAP | ldap://annuaire.gip-cps.fr/cn=test classe-2,ou=test structure,o=test,c=fr?certificaterevocationlist;binary |

 Tableau 23 : CPSRev : Vérification des flux vers l'annuaire ASIP Santé

Vérifier l'état d'un certificat carte d'authentification (extrait avec CPS Gestion ou avec inetcpl.cpl) depuis le serveur avec certutil -verify -urlfetch.

12.9.5 Cas des contrôleurs de domaine sans accès internet : vérification des statuts de certificats « offline » via l'alimentation du magasin de CRL en ligne de commande

Dans le cas – répandu – où les contrôleurs de domaine n'ont pas d'accès internet, il est nécessaire

- 1. de télécharger les CRLs ASIP Santé sur une machine dédiée
- 2. de les copier sur les contrôleurs de domaine
- 3. de les importer dans le magasin de liste de révocation

Cette dernière opération s'automatise avec l'outil certmgr.exe de Microsoft fourni avec Visual Studio. La ligne de commande est la suivante :

"certmgr.exe" -add -v -crl "chemin_du_fichier.crl" -s -r localMachine CA

Tableau 24 : CPSRev : Ligne de commande certmgr.exe

La documentation de certmgr.exe est ici : <u>http://msdn.microsoft.com/en-</u>us/library/e78byta0(v=vs.110).aspx

Le magasin est consultable visuellement en utilisant la mmc (autorité de certification intermédiaire > Liste de révocation des certificats):

| 🧱 Console1 - [Racine de la console\Certificats (ordinateur local)\Autorités de certification intermédiaires | | | | | | |
|---|--|--------------|----------------|--|--|--|
| 🚠 Fichier Action Affichage Favoris Fenêtre ? | | | | | | |
| | | | | | | |
| 📔 Racine de la console | Délivré par 🔺 | Date d'effet | Prochaine mise | | | |
| 🖃 🔜 Certificats (ordinateur local) | 📧 AC-CLASSE-4, GIP-CPS, FR | 30/09/2014 | 07/10/2014 | | | |
| 🛨 🚞 Personnel | 🐮 AC-CLASSE-4, GIP-CPS, FR | 30/09/2014 | 07/10/2014 | | | |
| Autorités de certification ra | 🖲 AC-CLASSE-4-TEST, GIP-CPS-TES | 30/09/2014 | 07/10/2014 | | | |
| Confiance de l'entreprise | 🗵 AC-CLASSE-4-TEST, GIP-CPS-TES | 30/09/2014 | 07/10/2014 | | | |
| Autorités de certification inl | 🐮 AC-CLASSE-5, GIP-CPS, FR | 30/09/2014 | 07/10/2014 | | | |
| Liste de revocation des | 🐮 AC-CLASSE-5, GIP-CPS, FR | 30/09/2014 | 07/10/2014 | | | |
| Certificats | 🖲 AC-CLASSE-5-TEST, GIP-CPS-TES | 30/09/2014 | 07/10/2014 | | | |
| Euleurs approuves | 🗵 AC-CLASSE-5-TEST, GIP-CPS-TES | 30/09/2014 | 07/10/2014 | | | |
| Electronicals non-adionses Electronicals non-adionses | 🐮 AC-CLASSE-6, GIP-CPS, FR | 30/09/2014 | 07/10/2014 | | | |
| Acconces de cordinadorria Personnes autorisées | 📧 AC-CLASSE-6, GIP-CPS, FR | 30/09/2014 | 07/10/2014 | | | |
| F F Remote Desktop | 📧 AC-CLASSE-6-TEST, GIP-CPS, FR | 30/09/2014 | 07/10/2014 | | | |
| 🕀 🧮 Racines de confiance de ca | 🐮 AC-CLASSE-6-TEST, GIP-CPS, FR | 30/09/2014 | 07/10/2014 | | | |
| 🛨 🧮 SPC | 🐮 GIP-CPS ANONYME, GIP-CPS, FR | 30/09/2014 | 06/10/2014 | | | |
| 표 🚞 Périphériques approuvés | 📧 GIP-CPS ANONYME, GIP-CPS, FR | 30/09/2014 | 06/10/2014 | | | |
| | 📧 GIP-CPS CLASSE-0, GIP-CPS ANO | 30/09/2014 | 06/10/2014 | | | |
| | 🖲 GIP-CPS CLASSE-0, GIP-CPS ANO | 30/09/2014 | 06/10/2014 | | | |
| | 📧 GIP-CPS CLASSE-1, GIP-CPS PRO | 30/09/2014 | 06/10/2014 | | | |
| | 📧 GIP-CPS CLASSE-1, GIP-CPS PRO | 30/09/2014 | 06/10/2014 | | | |
| | 📧 GIP-CPS CLASSE-2, GIP-CPS STR | 30/09/2014 | 06/10/2014 | | | |
| | 📧 GIP-CPS CLASSE-2, GIP-CPS STR | 30/09/2014 | 06/10/2014 | | | |
| | 📧 GIP-CPS CLASSE-3, GIP-CPS STR | 30/09/2014 | 06/10/2014 | | | |
| | 🗵 GIP-CPS CLASSE-3, GIP-CPS STR | 30/09/2014 | 06/10/2014 | | | |
| | E GIP-CPS PROFESSIONNEL, GIP-C | 30/09/2014 | 06/10/2014 | | | |
| | E GIP-CPS PROFESSIONNEL, GIP-C | 30/09/2014 | 06/10/2014 | | | |
| | E GIP-CPS STRUCTURE, GIP-CPS, FR | 30/09/2014 | 06/10/2014 | | | |
| | E GIP-CPS STRUCTURE, GIP-CPS, FR | 30/09/2014 | 06/10/2014 | | | |
| | E GIP-CPS, FR | 30/09/2014 | 06/10/2014 | | | |
| | I GIP-CPS, FR | 05/08/2003 | 07/08/2003 | | | |
| | 😢 GIP-CPS, FR | 05/08/2003 | 07/08/2003 | | | |
| | GIP-CPS, FR | 30/09/2014 | 06/10/2014 | | | |
| | SIP-CPS-TEST, FR | 30/09/2014 | 06/10/2014 | | | |
| | 🐮 GIP-CPS-TEST, FR | 30/09/2014 | 06/10/2014 | | | |
| | EST ANONYME, TEST, FR | 30/09/2014 | 06/10/2014 | | | |
| | EST ANONYME, TEST, FR | 30/09/2014 | 06/10/2014 | | | |
| | EST CLASSE-U, TEST ANONYME, | 30/09/2014 | 06/10/2014 | | | |
| | TEST CLASSE-U, TEST ANONYME, | 30/09/2014 | 06/10/2014 | | | |
| | TEST CLASSE-1, TEST PROFESSI | 30/09/2014 | 06/10/2014 | | | |
| | KEST CLASSE-1, TEST PROFESSI KEST CLASSE 2, TEST STRUCTUR | 30/09/2014 | 06/10/2014 | | | |
| | ■ TEST CLASSE-2, TEST STRUCTUR | 30/09/2014 | 06/10/2014 | | | |
| | TEST CLASSE-2, TEST STRUCTUR | 30/09/2014 | 06/10/2014 | | | |
| | TEST CLASSES, TEST STRUCTUR | 30/09/2014 | 06/10/2014 | | | |
| | TEST DE DE STONNEL TEST EN | 30/09/2014 | 06/10/2014 | | | |
| | | 30/09/2014 | 06/10/2014 | | | |
| | EST FROFESSIONNEL, TEST, FR | 30/09/2014 | 06/10/2014 | | | |
| | EST STDUCTURE TEST ED | 30/09/2014 | 06/10/2014 | | | |
| | VeriSign Commercial Software Pub | 24/03/2001 | 00/10/2014 | | | |
| | | 2.70072001 | 30/01/2001 | | | |
| 1 | | | | | | |

Figure 127 ; CPSRev : vérification des statuts de certificats offline : consultation du magasin de CRL

12.9.6 Test du Provider de révocation ASIP Santé – Microsoft en vérifiant le statut d'un certificat

Ex. : certutil -verify -urlfetch 03-asipsante-cpsrev-test.cer

Les messages renvoyés par certutil diffèrent entre une vérification « online » et une vérification « offline ».

Dans les 2 cas, le message « Vérification de révocation du certificat feuille réussie » final doit s'afficher.

| Emetter:: CN-TEST CLASSE 2 OU-TEST STRUCTURE O-TEST C+FR Obje:: CN-50000000018119/CPAT0001 + SN-RESPONSABLE0000018110001 + G-CHARLES OU-30000000008119 L=Paris (73) O-TEST C-FR Numéro de série du certificat : 4:8ddd dwfiags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x2000000) dwfiags = CA_VERIFY_FLAGS_OUNDLE_TRACE (0x2000000) dwfiags = CA_VERIFY_FLAGS_OUNDLE_TRACE (0x2000000) dwfiags = CA_VERIFY_FLAGS_OUNDLE_TRACE (0x2000000) dwfiags = CA_VERIFY_FLAGS_OUNDLE_TRACE (0x2000000) ChainFags = CA_VERIFY_FLAGS_OUNDLE_TRACE (0x2000000) Herce_LOCAL_MACHINE CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) Herce_LOCAL_MACHINE CERT_CHAIN_ECONTEXT ChainContext.dwinfostatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwinfostatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x10) SimpleChain.dwinfostatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x10) SimpleChain.dwinfostatus = CERT_TRUST_HAS_REFERRED_ISSUER (0x10) SimpleChain.dwinfostatus = | |
|---|---|
| CM-FEST CASSE-2 OU-TEST STRUCTURE O-TEST C-FR Objet: CM-500000000018119/CPAT0001 + SN-RESPONSABLE0000018110001 + G-CHARLES OU-30000000018119 L=Paris (75) O-TEST C-FR Numéro de série du certificat : 4:8ddd dwFlags = CA_UERIFY_ELAGS_CONSOLE_TRACE (0x2000000) dwFlags = CA_UERIFY_ELAGS_CONSOLE_TRACE (0x2000000) ChainFlags = CA_UERIFY_ELAGS_CONSOLE_TRACE (0x2000000) ChainFlags = CA_UERIFY_ELAGS_CONSOLE_TRACE (0x2000000) ChainFlags = CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) HCCE_LOCAL_MACHINE CERT_CHAIN_POLICY_BASE | Emetteur: |
| OU-FTEST STRUCTURE O-FTEST C-FR Object: CM-50000000018119/CPAT0001 + SN-RESPONSABLE0000018110001 + G-CHARLES OU-3000000018119 L=Poris (75) O-FTEST C-FR Numéro de série du certificat : 4c8ddd dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x2000000) dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x2000000) ChainFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x20000000) ChainContext_dwinfoStatus = CERT_TRUST_HAS_PREFERED_ISSUER (0x100) SimpleChain.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds CertContext[0][0]: dwinfoStatus=102 dwErrorStatus=0 Issuer: CN-TEST CLASSE=2, OU-TEST STRUCTURE, O-TEST, C-FR NotkBefore: 01/02/2013 02:00 <td>CN=TEST CLASSE-2</td> | CN=TEST CLASSE-2 |
| O-TEST CxFR Objet: CM-5000000018113/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES OU=30000000018113 L=Paris (75) O-TEST CxFR Numéro de série du certificat : 4c8ddd dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x2000000) dwFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x4000000) ChainFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x4000000) ChainFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000) ChainFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000) ChainFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000) ChainFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000) ChainFlags = CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) ChainFlags = CERT_TRUST_MAS_PREFERED_ISSUER (0x100) ChainContext.dwaRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds SimpleChain.dwaRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds CertContext[0][0]: dwainfoStatus=102 dwErrorStatus=0 Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, 0=TEST, C=FR NoteBefore: 01/02/2013 02:00 | OU=TEST STRUCTURE |
| C-FR Objet: CN-50000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES OU-30000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES OU-30000000018119/CPAT0001 + SN=RESPONSABLE0000001 O=TEST C-FR Numéro de série du certificat : 4c8ddd dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x2000000) dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x2000000) dwFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000) ChainFlags = CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) HCCE_LOCAL_MACHINE CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) HCCE_LOCAL_MACHINE CERT_CHAIN_POLICY_BASE CHainContext.dwInf0Status = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) ChainContext.dwInf0Status = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds CertContext[0][0]: dwInf0Status=102 dwErrorStatus=0 ssuer: CN=TEST_CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBéfre: 01/02/2016 23:59 Subject: CM=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBéfre: 01/02/2016 23:59 Subject: M=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBéfre: 01/02/2016 23:59 Subject: M=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBéfre: 01/02/2016 23:59 Subject: M=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBéfre: 01/02/2016 23:59 Subject: M=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBéfre: 01/02/2016 23:59 Subject: M=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBéfre: 01/02/2016 23:59 Subject: M=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBéfre: 01/02/2016 23:59 Subject: M=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBéfre: 01/02/2016 23:59 Subject: M=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBéfre: 01/02/2016 23:59 Subject: M=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBéfre: 01/02/2016 23:59 Subject: M=TEST CLASSE-2, OU=TEST STRUCTURE, OSUBER (0x100) | O=TEST |
| Objet: CM-50000000015119/CPAT0001 + SN-RESPONSABLE0000018110001 + G-CHARLES OU-3000000018119 L=Paris (75) O-TEST C-FR Numéro de série du certificat : 4c8ddd dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x2000000) dwFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000) ChainFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000) ChainFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000) ChainFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000) ChainFlags = CAT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) ChainFlags = CAT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) ChainContext.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) ChainContext.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwinfoStatus = CERT_TRUST_HAS_PREFERERED_ISSUER (0x100) SimpleChain.dwinfoStatus = | C=FR |
| CN=50000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES OU=3000000018119 L=Porks (75) O=TEST C=FR Numéro de série du certificat : 4c8ddd dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x2000000) dwFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000) ChainFlags = CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) ChainFlags = CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) ChainContext.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) ChainContext.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwinfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) NotAffer: 20/02/2016 23:59 Subject: ChainSe-2, OU=TEST STRUCTURE, O=TEST, C=FR NotAffer: 20/02/2016 23:59 Subject: Cha | Objet: |
| OU=3000000018119 L=Paris (75) O=TEST C=FR Numéro de série du certificat : 4C8ddd dwFlags = CA_VERIPY_FLAGS_CONSOLE_TRACE (0x2000000) dwFlags = CA_VERIPY_FLAGS_DUMP_CHAIN (0x40000000) ChainFlags = CAT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) HCCE_LOCAL_MACHINE CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) HCCE_LOCAL_MACHINE CERT_CHAIN_FOLICY_BASE CERT_CHAIN_CONTEXT ChainContext.dwinfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) ChainContext.dwinfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwinfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwinfoStatus = 02 dwErrorStatus=0 Issuer: CN=TEST CLASSE-2, 0U=TEST STRUCTURE, 0=TEST, C=FR NatBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject: AltiNamere: Autre nom :Nom principal=5.00000000018119.CPAT0001 # G=CHARLES, OU=30000000018119, L=Paris (75), O=TEST, C=FR NatBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject: CN=500000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=300000000018119, L=Paris (75), O=TEST, C=FR NatAfter: 29/02/2016 23:59 Subject: AltiNamere | CN=50000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES |
| L=Paris (75) O=TEST C=FR Numéro de série du certificat : 4C8ddd dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x2000000) dwFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x4000000) ChainFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x4000000) HCCE_LOCA_MACHINE CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) HCCE_LOCA_MACHINE CERT_CHAIN_POLICY_BASE CERT_CHAIN_POLICY_BASE CERT_CHAIN_CONTEXT ChainContext.dwinfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) ChainContext.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds SimpleChain.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds CertContext[0](0]: dwInfoStatus=102 dwErrorStatus=0 Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, 0=TEST, C=FR NotBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject: CN=500000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=30000000018119, L=Paris (75), O=TEST, C=FR NotBefore: 1.02/2016 23:59 Subject: CN=500000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=30000000018119, L=Paris (75), O=TEST, C=FR NotBefore: 01/02/2016 23:59 Subject: CN=500000000018119/CPAT0001 + SN=RESPONSABLE0000018119.CPAT0001@carte-cps.fr cc 8c f 7 e3 0c 7 b 6f 27 f 66 75 5a 32 9 2 a ce 1 a 2 95 d7 65 Element.dwInfoStatus = CERT_TRUST_HAS_REFERRED_ISSUER (0x10) Element.dwInfoStatus = CERT_TRUST_HAS_REFERRED_ISSUER (0x20) Element.dwInfoStatus = CERT_TRUST_HAS_REFERRED_ISSUER (0x20) Element.dwInfoStatus = CERT_TRUST_HAS_REFERRED_ISSUER (0x20) Element.dwInfoStatus = CERT_TRUST_HAS_REFERRED_ISSUER (0x100) | OU=3000000018119 |
| O=TEST C-FR Numéro de série du certificat : 4.68ddd dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x2000000) dwFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000) Chainfags = CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) HCCE_LOCAL_MACHINE CERT_CHAIN_POLICY_BASE CERT_CHAIN_CONTEXT ChoinContext.dwinfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) ChoinContext.dwinfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwinfoStatus=0 CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwinfoStatus=0.2000 Issuer: CN=TEST CLASSE=2, OU=TEST STRUCTURE, 0=TEST, C=FR NotBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject: CN=S00000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=30000000018119, L=Paris (75), 0=TEST, C=FR Serial: 4.88ddd Subject: CN=S0000000018119/CPAT0001 + SN=RESPONSABLE000001811001 + G=CHARLES, OU=30000000018119, L=Paris (75), 0=TEST, C=FR Serial: 4.88ddd Subject: CN=S00000000018119/CPAT0001 + SN=RESPONSABLE0000018119(001 + G=CHARLES, OU=30000000018119, L=Paris (75), 0=TEST, C=FR Serial: 4.88ddd Subject: CN=S0000000018119/CPAT0001 + SN=RESPONSABLE0000018119(Darte-cps.fr cc 8C 7 7 80 67 96 67 5 53 23 29 ac el a2 95 d7 65 <t< td=""><td>L=Paris (75)</td></t<> | L=Paris (75) |
| C=FR Numéro de série du certificat : 4:88ddd dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x2000000) dwFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000) Chainfags = CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) HCCE_LOCAL_MACHINE CERT_CHAIN_POLICY_BASE CERT_CHAIN_OSTATUS = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) ChainContext.dwinfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) ChainContext.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds SimpleChain.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) NotBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject: CN=S00000000018119/CPAT0001 + SN=RESPONSABLE000001811001 + G=CHARLES, 0U=30000000018119, L=Paris (75), e=TEST, C=FR Seria: 4:88ddd SubjectAtINNORE: Autre nom :Nom principal=5.00000000018119, CPAT0000@carte-cps.fr cc: 86_7 26 10 c 7b 66 72 76 8 75 8 29 29 ac et a 2 | O=TEST |
| Numéro de série du certificat : 4:8ddd dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x2000000) dwFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x4000000) ChainFlags = CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) HCCE_LOCAL_MACHINE CERT_CHAIN_POLICY_BASE | C=FR |
| dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x2000000) dwFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000) ChainFlags = CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) HCCE_LOCAL_MACHINE CERT_CHAIN_POLICY_BASE CERT_CHAIN_CONTEXT ChainContext.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) ChainContext.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) ChainContext.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds SimpleChain.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwInfoStatus = 102 dwErrorStatus=0 Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject CN=S000000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=300000000018119, L=Paris (75), O=TEST, C=FR Serial: 4cBddd SubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.fr cc & (7 P 23 0c 7b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65 Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) | Numéro de série du certificat : 4c8ddd |
| dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x2000000) dwFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000) ChainFlags = CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) HCCE_LOCAL_MACHINE CERT_CHAIN_POLICY_BASE CERT_CHAIN_CONTEXT ChainContext.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) ChainContext.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds SimpleChain.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwInfoStatus = 0 deterrorStatus=0 Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, 0=TEST, C=FR NotBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject: CN=5000000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=300000000018119, L=Paris (75), 0=TEST, C=FR Serial: 4c8ddd SubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.fr cc & C f 7 e3 0c 7b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65 Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x100) | |
| dwFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x4000000) ChainFlags = CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x4000000) HCCE_LOCAL_MACHINE CERT_CHAIN_ROLICY_BASE CERT_CHAIN_CONTEXT ChainContext.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) ChainContext.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds SimpleChain.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwInfoStatus=102 dwErrorStatus=0 Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject: CN=50000000018119/CPAT0001 + SN=RESPONSABLE000018110001 + G=CHARLES, OU=30000000018119, L=Paris (75), O=TEST, C=FR Serial: 4c8ddd SubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.fr cc & C f7 e3 0c 7b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65 Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) Siture CARTEST CLASSE-2, TAUST_HAS_KEY_MATCH_ISSUER (0x100) Lement.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) Authe certificat | dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x20000000) |
| ChainFlags = CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x4000000) HCCE_LOCAL_MACHINE CERT_CHAIN_ROLICY_BASE | dwFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x4000000) |
| HCCE_LOCAL_MACHINE CERT_CHAIN_POLICY_BASE | ChainFlags = CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000) |
| CERT_CHAIN_POLICY_BASE CERT_CHAIN_CONTEXT ChainContext.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) ChainContext.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds SimpleChain.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds CertContext[0][0]: dwlnfoStatus=102 dwErrorStatus=0 Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject: CN=500000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=30000000018119, L=Paris (75), O=-TEST, C=FR Seriai: 4c8ddd SubjectAitName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.fr cc & c f7 e3 0 c7 b 6 f6 27 f 66 76 5a 32 92 ac e1 a2 95 d7 65 Element.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x2) Element.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x2) | HCCE_LOCAL_MACHINE |
| CERT_CHAIN_CONTEXT ChainContext.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) ChainContext.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds SimpleChain.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds CertContext[0][0]: dwlnfoStatus=102 dwErrorStatus=0 Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, 0=TEST, C=FR NotBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject: CN=500000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=30000000018119, L=Paris (75), O=TEST_CLASSE-2 Serial: 4c8ddd SubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.fr cc & c f7 e 3 0 c 7b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65 Element.dwlnfoStatus = CERT_TRUST_HAS_REFERRED_ISSUER (0x2) Element.dwlnfoStatus = CERT_TRUST_HAS_REFERRED_ISSUER (0x100) AlA de certificat | CERT_CHAIN_POLICY_BASE |
| ChainContext.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) ChainContext.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds SimpleChain.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds CertContext[0][0]: dwlnfoStatus=102 dwErrorStatus=0 Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject: CN=50000000018119/CPAT0001 + SN=RESPONSABLE000018110001 + G=CHARLES, OU=30000000018119, L=Paris (75), O=TEST, C=FR Serial: 4c8ddd SubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.fr cc & cf 7 e 3 0c 7b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65 Element.dwlnfoStatus = CERT_TRUST_HAS_REFERRED_ISSUER (0x2) Element.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) AIA de certificat | CERT_CHAIN_CONTEXT |
| ChainContext.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds SimpleChain.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds CertContext[0][0]: dwInfoStatus=102 dwErrorStatus=0 Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject: CN=50000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=30000000018119, L=Paris (75), O=TEST, C=FR Serial: 4c8ddd SubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.fr cc & f7 e 3 0 c7 b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65 Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwInfoStatus = CERT_TRUST_HAS_REFERRED_ISSUER (0x100) AlA de certificat | ChainContext.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) |
| SimpleChain.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds CertContext[0][0]: dwInfoStatus=102 dwErrorStatus=0 Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject: CN=50000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=30000000018119, L=Paris (75), O=TEST, C=FR Serial: 4c8ddd SubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.fr cc & cf 7 e3 0 c7 b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65 Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) AIA de certificat | ChainContext.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds |
| SimpleChain.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) SimpleChain.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds CertContext[0][0]: dwlnfoStatus=102 dwErrorStatus=0 Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject: CN=500000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=30000000018119, L=Paris (75), O=TEST, C=FR Serial: 4c8ddd SubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.fr cc & cf 7 e3 0c 7b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65 Element.dwlnfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) AIA de certificat | |
| SimpleChain.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds CertContext[0][0]: dwInfoStatus=102 dwErrorStatus=0 Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject: CN=50000000018119/CPAT0001 + SN=RESPONSABLE000018110001 + G=CHARLES, OU=3000000018119, L=Paris (75), O=TEST, C=FR Serial: 4c8ddd SubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.fr cc & f7 e3 0c 7b 6f 62 7f 66 76 sa 32 92 ac e1 a2 95 d7 65 Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwInfoStatus = CERT_TRUST_HAS_REFERRED_ISSUER (0x100) | SimpleChain.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) |
| CertContext[0][0]: dwlnfoStatus=102 dwErrorStatus=0 Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject: CN=50000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=30000000018119, L=Paris (75), O=TEST, C=FR Serial: 4c8ddd SubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.fr cc 8c f7 e3 0c 7b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65 Element.dwlnfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) | SimpleChain.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds |
| CertContext[0][0]: dwlnfoStatus=102 dwErrorStatus=0 Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR NotBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject: CN=50000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=30000000018119, L=Paris (75), O=TEST, C=FR Serial: 4c8ddd SubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.fr cc 8c f7 e3 0c 7b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65 Element.dwlnfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) AIA de certificat | |
| Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FRNotBefore: 01/02/2013 02:00NotAfter: 29/02/2016 23:59Subject: CN=500000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=30000000018119, L=Paris (75), O=TEST, C=FRSerial: 4c8dddSubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.frcc 8c f7 e3 0c 7b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2)Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) | CertContext[0][0]: dwInfoStatus=102 dwErrorStatus=0 |
| NotBefore: 01/02/2013 02:00 NotAfter: 29/02/2016 23:59 Subject: CN=50000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=30000000018119, L=Paris (75), O=TEST, C=FR Serial: 4c8ddd SubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.fr cc 8c f7 e3 0c 7b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65 Element.dwlnfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) | Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR |
| NotAfter: 29/02/2016 23:59Subject: CN=50000000018119/CPAT0001 + SN=RESPONSABLE000018110001 + G=CHARLES, OU=30000000018119, L=Paris (75), O=TEST, C=FRSerial: 4c8dddSubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.frcc 8c f7 e3 0c 7b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2)Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) | NotBefore: 01/02/2013 02:00 |
| Subject: CN=50000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=30000000018119, L=Paris (75), O=TEST, C=FR Serial: 4c8ddd SubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.fr cc 8c f7 e3 0c 7b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65 Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) AIA de certificat | NotAfter: 29/02/2016 23:59 |
| Serial: 4c8ddd SubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.fr cc 8c f7 e3 0c 7b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65 Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) AIA de certificat | Subject: CN=50000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=30000000018119, L=Paris (75), O=TEST, C=FR |
| SubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.fr cc 8c f7 e3 0c 7b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65 Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) AIA de certificat | Serial: 4c8ddd |
| cc 8c f7 e3 0c 7b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65 Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) AIA de certificat | SubjectAltName: Autre nom :Nom principal=5.0000000018119.CPAT0001@carte-cps.fr |
| Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) AIA de certificat | cc 8c f7 e3 0c 7b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65 |
| Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) AIA de certificat | Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) |
| AIA de certificat | Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) |
| | AIA de certificat |

| | Pas d'URL "Aucun" Heure : 0 |
|---|--|
| Émetteur incorrect "Liste de révocation des certificats de base (108)" Heure : 0 [1.0] Idap//annuaire.gip-qas.fr/ch/test/TEST CLASSE-2.cd/ Émetteur incorrect "Liste de révocation des certificats de base (108)" Heure : 0 [1.1] Idap//annuaire.gip-qas.fr/ch-etest classe-2.ou-test structure.o-test.cl-fr/certificaterevocationlist;binary | CDP de certificat |
| <pre>[0.0] http://onuaire.gip-cps.fr/cr/test/TEST CLASSE-2.cd Emetteur incorrect "Liste de révocation des certificats de base (108f)" Heure : 0 [1.0] blap://onuaire.gip-cps.fr/cr=test classe-2.ou=test structure.o=test.e=fr?certificaterevocationist.binary </pre> | Émetteur incorrect "Liste de révocation des certificats de base (108f)" Heure : 0 |
| Emetteur incorrect "Liste de révocation des certificats de base (108)" Heure : 0 [1.0] Idap://annuoire.ajip-cps.fr/cn=test classe - 2.ou=test structure, o=test, c=fr?certificaterevocationlist, binary | [0.0] http://annuaire.gip-cps.fr/crl/test/TEST CLASSE-2.crl |
| [1.0] Idap://onuoire.gip-cps.fr/cn=test close-2.ou-test structure.o=test.c-fr?certificaterevacationlist.binary | Émetteur incorrect "Liste de révocation des certificats de base (108f)" Heure : 0 |
| CDP de liste de révocation des certificats de base Pas d'URL "Aucun" Heure : 0 | [1.0] Idap://annuaire.gip-cps.fr/cn=test classe-2,ou=test structure,o=test,c=fr?certificaterevocationlist;binary |
| Pas d'URL "Aucun" Heure : 0 | CDP de liste de révocation des certificats de base |
| | Pas d'URL "Aucun" Heure : 0 |
| Pos d'URL "Aucun" Heure : 0 | Protocole OCSP du certificat |
| CRL 108f: Issuer: CN-TEST CLASSE-2, OU-TEST STRUCTURE, O=TEST, C=FR 91 77 do b2 82 bc 7d 55 68 b3 2c b1 a 0c 4f 92 0b d2 e9 0e Deta CRL 108f: issuer: CN-TEST CLASSE-2, OU-TEST STRUCTURE, O=TEST, C=FR d5 34 f9 02 93 o6 c5 e5 52 10 17 61 43 35 b0 17 4e b8 82 b Application[0] = 1.3.6.1.4.1.311.20.2.2 Ouverture de session par carte à puce CertContext[0][1]: dwinfoStatus=102 dwErorStatus=0 Issuer: OL-TEST STRUCTURE, O=TEST, C=FR NotBefore: 11/10/2004 02:00 NotAfter: 31/12/2020 23:59 Subject: CN-TEST CLASSE-2, OU-TEST STRUCTURE, O=TEST, C=FR Serial: 1212 54 df e 1a c4 cd 8d 5a cf 32 f7 ae 12 1e f2 6a 33 8f f1 3d Element.dwinfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwinfoStatus = CERT_TRUST_HAS_PPEFERRED_ISSUER (0x100) | Pas d'URL "Aucun" Heure : 0 |
| CRL 108f: Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR 91 77 d0 b2 82 bc 7d 55 36 8b 32 cb 1a 0c 4f 92 0b d2 e9 0e Deha CRL 108f: Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR d5 34 f9 02 93 a9 cs 66 56 21 01 76 14 33 5b 01 74 eb 88 2b Application[0] = 1.3.6.1.5.7.3.2 Authentification du client Application[1] = 1.3.6.1.4.1.311.20.2.2 Ouverture de session por carte à puce CertContext[0][1]: dwinfoStatus=102 dwErrorStatus=0 Issuer: OU=TEST STRUCTURE, 0=TEST, C=FR NotBefore: 11/10/2004 02:00 NotAfter: 31/12/2020 23:59 Subjecti: CN=TEST CLASSE-2, OU=TEST STRUCTURE, 0=TEST, C=FR Serial: 1212 54 df ee 1a c4 cd 8d 5a cf 32 f7 ae 12 1e f2 6a 33 8f f1 3d Element.dwinfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwinfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x100) | |
| Issuer: CN-TEST CLASSE-2, OU-TEST STRUCTURE, O-TEST, C-FR 91 77 d0 b2 82 bc 7d 55 36 8b 32 cb 10 0c 4f 92 0b d2 e9 0e Delta CRL 108f: Issuer: CN-TEST CLASSE-2, OU-TEST STRUCTURE, O-TEST, C=FR d5 34 f9 02 93 a9 C5 e6 56 21 01 76 14 33 5b 01 74 eb 88 2b Application[0] = 1.3.6.1.5.7.3.2 Authentification du client Application[1] = 1.3.6.1.4.1.311.20.2.2 Ouverture de session par carte à puce CertContext[0][1]: dwinfoStatus=102 dwErrorStatus=0 Issuer: OU-TEST STRUCTURE, 0-TEST, C=FR Notbefor: 11/10/2004 02:00 Notefier: 31/12/2020 23:59 Subject: CN-TEST CLASSE-2, OU-TEST STRUCTURE, 0-TEST, C=FR Serial: 1212 54 df ee 10 c4 cd 8d 50 cf 32 f7 oe 12 1e f2 6a 33 8f f1 3d Element.dwinfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwinfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x100) | CRL 108f: |
| 91 77 d0 b2 82 bc 7d 55 36 8b 32 cb 1a 0c 4f 92 0b d2 e9 0e Delta CRL 108f: Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR d5 34 f9 02 93 o9 c5 e6 56 21 01 76 14 33 5b 01 74 eb 88 2b Application[0] = 1.3.6.1.5.5.7.3.2 Authentification du clent Application[1] = 1.3.6.1.4.1.311.20.2.2 Ouverture de session par carte à puce CertContext[0][1]: dwinfoStatus=102 dwErrorStatus=0 Issuer: OU=TEST STRUCTURE, O=TEST, C=FR NotBéfore: 11/10/2004 02:00 NotAfter: 31/12/2020 23:59 Subject: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR Serial: 1212 54 df ee 1a c4 cd 8d 5a cf 32 f7 ae 12 1e f2 6a 33 8f f1 3d Element.dwinfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwinfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) | Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR |
| Delta CRL 108f: Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR d5 34 f9 02 93 a9 c5 e6 56 21 01 76 14 33 5b 01 74 eb 88 2b Application[0] = 1.3.6.1.5.5.7.3.2 Authentification du client Application[1] = 1.3.6.1.4.1.311.20.2.2 Ouverture de session par carte à puce CertContext[0][1]: dwlnfoStatus=102 dwErrorStatus=0 Issuer: OU=TEST STRUCTURE, 0=TEST, C=FR NotBépre: 11/10/2004 02:00 NotAfter: 31/12/2020 23:59 Subject: CN=TEST CLASSE-2, OU=TEST STRUCTURE, 0=TEST, C=FR Serial: 1212 54 df ec 1a c4 cd 8d 5a cf 32 f7 ac 12 1e f2 6a 33 8f f1 3d Element.dwlnfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwlnfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x100) | 91 77 d0 b2 82 bc 7d 55 36 8b 32 cb 1a 0c 4f 92 0b d2 e9 0e |
| Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR d5 34 f9 02 93 a9 c5 e6 56 21 01 76 14 33 5b 01 74 eb 88 2b Application[0] = 1.3.6.1.5.5.7.3.2 Authentification du client Application[1] = 1.3.6.1.4.1.311.20.2.2 Ouverture de session par carte à puce CertContext[0][1]: dwinfoStatus=102 dwErrorStatus=0 Issuer: OU=TEST STRUCTURE, 0=TEST, C=FR NotBefore: 11/10/2004 02:00 NotAfter: 31/12/2020 23:59 Subject: CN=TEST CLASSE-2, OU=TEST STRUCTURE, 0=TEST, C=FR Serial: 1212 54 df ea 1a c4 cd 8d 5a cf 32 f7 ae 12 1e f2 6a 33 8f f1 3d Element.dwinfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x20) | Delta CRL 108f: |
| d5 34 f9 02 93 09 c5 e6 56 21 01 76 14 33 5b 01 74 eb 88 2b Application[0] = 1.3.6.1.5.5.7.3.2 Authentification du client Application[1] = 1.3.6.1.4.1.311.20.2.2 Ouverture de session par carte à puce CertContext[0][1]: dwinfoStatus=102 dwErrorStatus=0 Issuer: OU=TEST STRUCTURE, 0=TEST, C=FR NotBefore: 11/10/2004 02:00 NotAfter: 31/12/2020 23:59 Subject: CN=TEST CLASSE-2, OU=TEST STRUCTURE, 0=TEST, C=FR Seriai: 1212 54 df ee 1a c4 cd 8d 5a cf 32 f7 ae 12 1e f2 6a 33 8f f1 3d Element.dwinfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwinfoStatus = Cert_TRUST_HAS_PREFERRED_ISSUER (0x100) | Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR |
| Application[0] = 1.3.6.1.5.5.7.3.2 Authentification du client Application[1] = 1.3.6.1.4.1.311.20.2.2 Ouverture de session par carte à puce CertContext[0][1]: dwinfoStatus=102 dwErrorStatus=0 Issuer: OU=TEST STRUCTURE, 0=TEST, C=FR NotBefore: 11/10/2004 02:00 NotAfter: 31/12/2020 23:59 Subject: CN=TEST CLASSE-2, OU=TEST STRUCTURE, 0=TEST, C=FR Serial: 1212 54 df ee 1a c4 cd 8d 5a cf 32 f7 ae 12 1e f2 6a 33 8f f1 3d Element.dwinfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwinfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) | d5 34 f9 02 93 a9 c5 e6 56 21 01 76 14 33 5b 01 74 eb 88 2b |
| Application[1] = 1.3.6.1.4.1.311.20.2.2 Ouverture de session par carte à puce CertContext[0][1]: dwinfoStatus=102 dwErrorStatus=0 Issuer: OU=TEST STRUCTURE, O=TEST, C=FR NotBéfore: 11/10/2004 02:00 NotAfter: 31/12/2020 23:59 Subject: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR Serial: 1212 54 df ee 1a c4 cd 8d 5a cf 32 f7 ae 12 1e f2 6a 33 8f f1 3d Element.dwinfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwinfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) | Application[0] = 1.3.6.1.5.5.7.3.2 Authentification du client |
| CertContext[0][1]: dwinfoStatus=102 dwErrorStatus=0 Issuer: OU=TEST STRUCTURE, O=TEST, C=FR NotBefore: 11/10/2004 02:00 NotAfter: 31/12/2020 23:59 Subject: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR Serial: 1212 54 df ee 1a c4 cd 8d 5a cf 32 f7 ae 12 1e f2 6a 33 8f f1 3d Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) | Application[1] = 1.3.6.1.4.1.311.20.2.2 Ouverture de session par carte à puce |
| Issuer: OU=TEST STRUCTURE, O=TEST, C=FR NotBefore: 11/10/2004 02:00 NotAfter: 31/12/2020 23:59 Subject: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR Serial: 1212 54 df ee 1a c4 cd 8d 5a cf 32 f7 ae 12 1e f2 6a 33 8f f1 3d Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwInfoStatus = CERT_TRUST_HAS_REFERRED_ISSUER (0x100) AIA de certificat Pas d'URL "Aucun" Heure : 0 Efmetteur incorrect "Liste de révocation des certificats de base (108f)" Heure : 0 [0.0] Idap://annuaire.gip-cps.fr/ou=test structure.o=test,c=fr?certificaterevocationlist;binary Pas d'URL "Aucun" Heure : 0 | CertContext[0][1]: dwInfoStatus=102 dwErrorStatus=0 |
| NotBefore: 11/10/2004 02:00 NotAfter: 31/12/2020 23:59 Subject: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR Serial: 1212 54 df ee 1a c4 cd 8d 5a cf 32 f7 ae 12 1e f2 6a 33 8f f1 3d Element.dwinfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwinfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) | Issuer: OU=TEST STRUCTURE, O=TEST, C=FR |
| NotAfter: 31/12/2020 23:59 Subject: CN=TEST CLASSE-2, OU=TEST STRUCTURE, 0=TEST, C=FR Serial: 1212 54 df ee 1a c4 cd 8d 5a cf 32 f7 ae 12 1e f2 6a 33 8f f1 3d Element.dwinfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwinfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) | NotBefore: 11/10/2004 02:00 |
| Subject: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR Serial: 1212 54 df ee 1a c4 cd 8d 5a cf 32 f7 ae 12 1e f2 6a 33 8f f1 3d Element.dwlnfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) | NotAfter: 31/12/2020 23:59 |
| Serial: 1212 54 df ee 1a c4 cd 8d 5a cf 32 f7 ae 12 1e f2 6a 33 8f f1 3d Element.dwlnfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) | Subject: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR |
| 54 df ee 1a c4 cd 8d 5a cf 32 f7 ae 12 1e f2 6a 33 8f f1 3d Element.dwlnfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) | Serial: 1212 |
| Element.dwlnfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) Element.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) | 54 df ee 1a c4 cd 8d 5a cf 32 f7 ae 12 1e f2 6a 33 8f f1 3d |
| Element.dwlnfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) | Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2) |
| AlA de certificat Pas d'URL "Aucun" Heure : 0 | Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100) |
| Pas d'URL "Aucun" Heure : 0 | AIA de certificat |
| CDP de certificat Émetteur incorrect "Liste de révocation des certificats de base (108f)" Heure : 0 [0.0] Idap://annuaire.gip-cps.fr/ou=test structure,o=test,c=fr?certificaterevocationlist;binary | Pas d'URL "Aucun" Heure : 0 |
| Émetteur incorrect "Liste de révocation des certificats de base (108f)" Heure : 0 [0.0] Idap://annuaire.gip-cps.fr/ou=test structure,o=test,c=fr?certificaterevocationlist;binary CDP de liste de révocation des certificats de base Pas d'URL "Aucun" Heure : 0 Protocole OCSP du certificat Pas d'URL "Aucun" Heure : 0 CRL 108f: Issuer: OU=TEST STRUCTURE, O=TEST, C=FR | CDP de certificat |
| [0.0] Idap://annuaire.gip-cps.fr/ou=test structure,o=test,c=fr?certificaterevocationlist;binary CDP de liste de révocation des certificats de base Pas d'URL "Aucun" Heure : 0 Protocole OCSP du certificat Pas d'URL "Aucun" Heure : 0 CRL 108f: Issuer: OU=TEST STRUCTURE, O=TEST, C=FR | Émetteur incorrect "Liste de révocation des certificats de base (108f)" Heure : 0 |
| CDP de liste de révocation des certificats de base Pas d'URL "Aucun" Heure : 0 Protocole OCSP du certificat Pas d'URL "Aucun" Heure : 0 CRL 108f: Issuer: OU=TEST STRUCTURE, O=TEST, C=FR | [0.0] Idap://annuaire.gip-cps.fr/ou=test structure,o=test,c=fr?certificaterevocationlist;binary |
| Pas d'URL "Aucun" Heure : 0 Protocole OCSP du certificat Pas d'URL "Aucun" Heure : 0 CRL 108f: Issuer: OU=TEST STRUCTURE, O=TEST, C=FR | CDP de liste de révocation des certificats de base |
| Protocole OCSP du certificat Pas d'URL "Aucun" Heure : 0 CRL 108f: Issuer: OU=TEST STRUCTURE, O=TEST, C=FR | Pas d'URL "Aucun" Heure : 0 |
| Pas d'URL "Aucun" Heure : 0 CRL 108f: Issuer: OU=TEST STRUCTURE, O=TEST, C=FR | Protocole OCSP du certificat |
| CRL 108f: Issuer: OU=TEST STRUCTURE, O=TEST, C=FR | Pas d'URL "Aucun" Heure : 0 |
| Issuer: OU=TEST STRUCTURE, O=TEST, C=FR | CRL 108f: |
| | Issuer: OU=TEST STRUCTURE, O=TEST, C=FR |

| 7f e1 a1 b9 19 0c 35 50 98 72 88 fa b6 6b ed 7c 81 33 de d1 |
|---|
| CertContext[0][2]: dw/nfoStatus=10c dwFrrorStatus=0 |
| |
| NotRefere: 11/10/2004 02:00 |
| NotAfter: 21/12/2020 22:50 |
| Subject: OU-TEST STRUCTURE O-TEST C-ER |
| Sarial: 1201 |
| Serial. 1201 00 da $2a \in d$ 0.2 1f a^2 78 dE Ec ap pa $2c = 7 k^2 2c = 7 c^2 75 \in k$ |
| So the second of the second s |
| $Element dwlnfoStatus = CERT_TRUST_IC_SELE_SIGNED (0x8)$ |
| Element dwinijostatus = CERT_TRUST_USS_ELF_SIGNED (0x8) |
| element.dwinijostatus = Ceki _ ikosi _mAs_preferked_issoek (0x100) |
| |
| Pas a URL Aucun Heure : U |
| |
| |
| |
| Pas a URL "Aucun" Heure : U |
| Issuance[0] = 1.2.250.1.71.3.7.9.2.0.0.1 |
| Exclude leaf cert |
| h8 7e ah 1e de 9h 6d 71 f8 60 5e a4 4h 36 5c 3h 16 01 cd 22 |
| |
| 8a 22 b7 a5 66 c5 f8 e0 7f 9b 48 8b aa e2 f2 88 75 18 7e c0 |
| Stratégies d'émissions vérifiées: Aucun |
| Stratégies d'application vérifiées: |
| 1 3 6 1 5 5 7 3 2 Authentification du client |
| 1 3 6 1 4 1 311 20 2 2 Ouverture de session par carte à nuce |
| Le certificat est un certificat d'entité de fin |
| Vérification de révocation du certificat feuille réussie |
| Certi Itil: -verific la commande s'est terminée correctement |
| |

Tableau 25 : CPSRev : Résultat de la vérification d'un certificat avec CPSRev

12.10 Configuration d'une console de composants enfichables dédiée au Smartcard logon

Il est particulièrement intéressant de « centraliser » les éléments à configurer dans une console unique.

Cette opération se fait de la façon suivante :

« Démarrer > Exécuter > MMC » :

| 🙀 W2008R2-Base - VMware Player (Non-commercial use only) | |
|--|--|
| Player 👻 📙 😴 🔚 📜 🏹 | * |
| 💂 Gestionnaire de serveur | |
| Fichier Action Affichage ? | |
| | |
| Gestionnaire de serveur (WIN-92TJH90G03S) | |
| Programmes (1) | |
| 🚟 mmc.exe | astructure d'application Web fiable, gérable et évolutive. |
| | |
| | |
| | un Cs)/événement(s) d'événements |
| | dant 24 heures |
| | ements : 0 📴 Propriétés |
| | |
| | ID de l'év Date et h |
| | |
| | |
| | |
| | |
| | 4 service(s) en cours |
| ho Voir plus de résultats | : d'exécution, 2 service(s) arrêté(s) |
| | ujourd'hui à 00:21 Configurer l'actualisation |
| | |
| Marrer | FR 🕞 🎦 👘 🕲 00:23 💻 30/06/2013 |

Figure 128 : Console Enfichable: MMC

Pour plus de rapidité, cliquer sur **« Fichier > Ouvrir... »** et choisir **bin/01-asipsante-console-smartcard-logon.msc** fourni dans le Pack.

Une fois cette console chargée, la quasi-totalité des éléments à configurer est disponible de façon centralisée.

Ce qui suit vous permet de composer des composants enfichables dans un fichier .msc « personnalisé ». Il n'est pas généralement pas nécessaire de suivre ce qui suit si **01-asipsante-console-smartcard-logon.msc** s'est correctement chargée.

« Fichier > Ajouter/Supprimer un composant enfichable... » :

| 🙀 W2008R2-Base - | VMv | ware Player (Non-commercial use only) | - 🗆 🗵 |
|-----------------------------|----------|---|--------------|
| Player 👻 📘 👻 | | | * |
| 📕 Gestionnaire de | serv | veur | |
| Fichier Action A | fficha | age ? | |
| 🗢 🔿 🚺 🖬 | ? | | |
| Gestionnaire de s | ervei | ur (WIN-92TJH90G03S) Serveur Web (IIS) | |
| 🖃 🔂 Rôles | | | |
| Serveur | <u>8</u> | Console1 - [Racine de la console] | |
| 🗄 🐏 Gesti | - | Fichier Action Affichage Favoris Fenêtre ? | |
| ⊕ | | Nouveau Ctrl+N | |
| E Services | | Cuvrir Ctri+O | _ 11 |
| 🕀 💥 Services | | Enregistrer sous aperçu. Racine de la c 🔺 | |
| Poncuonnait Diagnostics | | Ajouter/Supprimer un composant logiciel enfichable Ctrl+M Autres acti | |
| E Configuration | | Options | |
| + Stockage | | Fichier récent | |
| | LI | Quitter | |
| | 1.1 | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | Crée | er une nouvelle console. | - |
| | | Dernière actualisation : Aujourd'hui à 00:23 Configurer l'actualisation | |
| | | | |
| Ø Démarrer | | FR 客 🎦 😼 | 24 2013 💻 |

Figure 129 : Console Enfichable: Ajout de composants enfichables

« Certificats » :

| 1008R2 | Base - VMware Player (Non-commercial use | only) | | | |
|-------------------|---|-------------------------------------|--|-----------------------------------|----------------------|
| Player 👻 | | | | | * |
| E. Gestionn | aire de serveur | | | | - 101 × 1 |
| Eichier Act | ion Affichage 2 | | | | |
| | | | | | |
| | | | | | |
| Gestionn | Ajouter ou supprimer des composants logicie | els enfichable | 5 | | × |
| + ¥ - ♀ s | Vous pouvez sélectionner des composants logiciels e composants logiciels enfichables extensibles, vous p | enfichables parr ouvez spécifier | ni ceux disponibles sur votre ordinateur, • quelles extensions doivent être activée | et les configurer. Pour les s. | |
| Ē∮ | Composants logiciels enfichables disponibles : | 1 | Composants logiciels enfi. sélectionnés : | | |
| ± 5 | Composant logiciel enfi Fournisseur | | Racine de la console | Modifier les extensions | • |
| | Nalyseur de perfor Microsoft Cor | | | Supprimer | |
| ء 😭 🗉 | Autorité de certificat Microsoft Cor | | | | |
| Fonc | Certificats Microsoft Cor | | | Mashav | |
| E Conf | Configuration d'hôte Microsoft Cor | | | Monter | _ |
| E Stod | Configuration du die Microsoft Cor | I | | Descendre | |
| | Configuration et ana Microsoft Cor | Ajouter > | | | |
| | Contrôle ActiveX Microsoft Cor | | | | |
| | Contrôle WMI Microsoft Cor | | | | |
| | Domaines et approb Microsoft Cor | | | | |
| | Dossier Microsoft Cor | | | | |
| | Bossiers partagés Microsoft Cor | | | | |
| | Editeur d'objets de s Microsoft Cor | | | Avancé | |
| | Editeur d'oblets de s Microsoft Cor | | | | |
| | Description : | | | | |
| | Le composant logiciel enfichable Certificats vous pe | ermet de parcou | urir le contenu des magasins de certificat | s pour vous, un service ou | |
| | un ordinateur. | | | | |
| | | | | | |
| | | | Г | OK Appular | |
| | | | L | OK Annuer | |
| <u> </u> | | | J | J | |
| Ø Démarrer | 🛃 🛛 🚞 💊 | | | FR 🕆 🕩 🛍 🕼 30 | 00:24 D/06/2013 💻 |

Figure 130 : Console Enfichable: Certificats

| 🙀 W2008R2-Base - VMware Player (Non-commercial use only) | |
|--|--------------------------------|
| Player 👻 🔛 🖳 🥫 | « |
| Gestionnaire de serveur | _ _ _ _ _ |
| Fichier Action Affichage ? | |
| | |
| Gestionn Ajouter ou supprimer des composants logiciels enfichables | |
| | es configurer. Pour les |
| E composant logiciel enfichable gérera toujours les certificats pour : | |
| Mon compte d'utilisateur | Modifier les extensions |
| | Supprimer |
| | |
| | Monter |
| E Conf E Stod (| Descendre |
| | |
| | |
| | |
| | |
| | Avancé |
| | |
| < Précédent Teminer Annuler | ur vous, un service ou |
| | |
| | |
| | OK Annuler |
| | |
| MDémarrer | R * P 1 13 00:24 30/06/2013 |

Figure 131 : Console Enfichable: Certificats utilisateur

| 🙀 W2008R2-Base - VMware Player (Non-commercial use only) | |
|---|-------------------------|
| Player 👻 🔛 🖳 🥫 | * |
| E Gestionnaire de serveur | |
| Fichier Action Affichage ? | |
| | |
| Gestionn Ajouter ou supprimer des composants logiciels enfichables | L X |
| | es configurer. Pour les |
| Ce composant logiciel enfichable gérera toujours les certificats pour : | |
| ⊕ ↓ ∪ □ ↓ □ ↓ □ ↓ □ ↓ □ ↓ □ ↓ □ ↓ □ ↓ □ ↓ | Modifier les extensions |
| | |
| E S Un compte d'ordinateur | |
| on Fonc ' ⊡ ma Diagu | Monter |
| | Descendre |
| | |
| | |
| | |
| | |
| | - turnet |
| | Avance |
| C C C C C C C C C C C C C C C C C C C | |
| | pur vous, un service ou |
| | |
| | OK Annuler |
| | |
| | 3 a Dr 🕒 👍 00:25 📥 |
| | 30/06/2013 🔤 |

Figure 132 : Console Enfichable: Certificats Local Machine

| 🙀 W2008R2-Base - VMware Player (Non-commercial use only) | |
|---|---------------------|
| Player 👻 🔛 🚛 📺 | « |
| 🚆 Gestionnaire de serveur | |
| Fichier Action Affichage ? | |
| | |
| Gestion Ajouter ou supprimer des composants logiciels enfichables | × |
| Sélectionnez l'ordinateur devant être géré par ce composant logiciel enfichable | ifigurer. Pour les |
| | |
| Ordinateur local (l'ordinateur sur lequel cette console s'exécute) | r les extensions |
| C Un autre ordinateur : | Supprimer |
| Conception de l'ordinateur sélectionné lors de l'exécution à partir de la ligne | Monter |
| Cont de commande. Ceci ne s'applique que si vous enregistrez la console. | Descendre |
| | Avancé |
| D C C C C C C C C C C C C C C C C C C C | |
| | |
| | |
| OK | Annuler |
| Marrer | 00:25 10/06/2013 |

Figure 133 : Console Enfichable: Certificats Local Machine

| 🙀 W2008R2-Base - VMware Player (Non-commercia | l use only) | _ | |
|---|--|--------------------------|------|
| Player 👻 🛄 😴 🧱 | | | « |
| 🚆 Gestionnaire de serveur | ÷ | <u>_ </u> | IN |
| Fichier Action Affichage ? | | | |
| 🗢 🔿 🙍 🖬 🛛 | | | |
| Gestionn Ajouter ou supprimer des composants l | ogiciels enfichables | | |
| | groupe X | es configurer. Pour les | |
| □ □ □ Assistant Stratégie de groupe □ □ □ | | | |
| | | Modifier les extensions | |
| | | Supprimer | 1 |
| Fonc | Les objets de strategie de groupe peuvent etre stockes dans l'annuaire Active Directory ou sur un ordinateur local. | | |
| | Cliquez sur le bouton Parcourir pour sélectionner un objet | Monter | |
| E Stod | de stratègie de groupe. | Descendre | |
| | | | |
| | Default Domain Controllers Policy | | |
| | | | |
| | Parcounr | | |
| Ľ | | Avancé | |
| D | enfichable de stratégie de groupe lors de l'exécution à | | |
| | si vous enregistrez la console. | en liaison avec un site, | |
| | | | |
| | < Précédent Terminer Annuler | OK Appuler | |
| | | | |
| | | 00:26 | |
| | | 30/06/201 | 13 💻 |

Figure 134 : Console Enfichable: Stratégie de groupe du contrôleur de domaine

| 🙀 W2008R2-Base - VMware Player | (Non-commercial use only) | | <u>_ </u> |
|---|-------------------------------------|--------|--|
| Player 👻 🔛 💌 📷 | 1 | | * |
| 🚟 Console1 - [Racine de la cons 🛛 |] | | <u>_ 8 ×</u> |
| 🚡 Fichier Action Affichage Favo | oris Fenêtre ? | | _ 8 × |
| | | | |
| Racine de la console | Nom | | Actions |
| Gertificats - Utilisateur actuel Gertificats (ordinateur local) | Certificats - Utilisateur actuel | | Racine de la c 🔺 |
| Configuration d'hôte de session | Configuration d'hôte de session B | | Autres acti 🕨 |
| E Domaines et approbations Activ | Domaines et approbations Active | | |
| Strategie Default Domain Contre Gestionnaire des services Burea | 🗐 Stratégie Default Domain Controll | | |
| 🖭 👸 PKI d'entreprise | Gestionnaire des services Bureau | | |
| Sites et services Active Director | Sites et services Active Directory | | |
| | Utilisateurs et ordinateurs Active | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| • | | | |
| | | | |
| M Démarrer | iii | FR 🗭 🗎 | 00:28 30/06/2013 |

Figure 135 : Console Enfichable: Liste des composants utilisés pour le Smartcard logon

« Fichier > Enregistrer sous... » : choisir « console-smartcard-logon.msc » sur le bureau.

| Player 👻 🔡 💌 🛄 ң | * |
|--|----------------------|
| 👼 Con 🛌 le1 - [Racine de la console] | _ 8 × |
| Fichier Action Affichage Favoris Fenêtre ? | _ 8 × |
| Nouveau Ctrl+N | |
| Ouvrir Ctrl+O | |
| Enregistrer Ctrl+S el Racine | de la c |
| | tras acti |
| Ajouter/Supprimer un composant logiciel enfichable Ctrl+M sion B | tres act 🕨 |
| | |
| Fichier récent ureau | |
| Quitter | |
| Utilisateurs et ordinateurs Active | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | 00:28 0/06/2013 💻 |

Figure 136 : Console Enfichable: Sauvegarde

12.11 Configuration du Contrôleur de domaine pour la Smartcard logon

12.11.1 Magasins de certificats

Commande MMC -> certificats -> ordinateur local

- Magasin Personnel
 - o certificats racine
 - o certificats DC (DomainController) du serveur
- Magasin Autorités de certification racine de confiance
 - o certificats racine client
 - o serveur
- Magasin Autorités intermédiaires
 - o certificats client racine (signeur de CRL)
 - o certificats intermédiaires client signeur de certificats et CRLs

En cas de contrôleurs de domaine multiple : installer ces certificats sur chaque contrôleur

12.11.1.1 Magasin personnel

Après installation de la Cryptolib CPS ou du provider de révocation, les certificats racine ne sont pas présents dans le magasin personnel (normal):

| 🧱 Console_cosign - [Racine de la console\Certificats (ordinateur local)\Personnel\Certificats] | | | | |
|---|-----------------------------|--------------|----------------|-------|
| 🚡 Eichier Action Affichage Favoris Fenêtre ? | | | | _ 8 × |
| 🗢 🔿 🖄 🖬 📋 🖻 🔒 👔 🖬 | | | | |
| 📔 Racine de la console | Délivré à 🔺 | Délivré par | Actions | |
| 🗉 🙀 Certificats - Utilisateur actuel | 🛱 eu-cosign-ca | eu-cosign-ca | Certificats | |
| Certificats (ordinateur local) | 🛱 WIN-92TJH90G03S.eu.cosign | eu-cosign-ca | | |
| Personnel | WMSvc-WIN-92TJH90G03S | WMSvc-WIN-9: | Autres actions | • |
| Certificats | - | | | |
| Autorités de certification racines de confiance | | | | |
| Certificats | | | | |
| Confiance de l'entreprise | | | | |
| Autorités de certification intermédiaires | | | | |
| Liste de revocation des certificats | | | | |
| | | | | |
| Editeurs approuves | | | | |
| Certificats non autorises | | | | |
| Autorites de cer uncauori racine derce parde | | | | |
| | | | | |
| The management of the sector of the sec | | | | |
| Bacines de confiance de carte à nuce | | | | |
| Périphériques approuvés | | | | |
| Configuration d'hôte de session Bureau à distance | | | | |
| Domaines et approbations Active Directory | | | | |
| Stratégie Default Domain Controllers Policy [WIN-9] | | | | |
| 🕀 🚃 Gestionnaire des services Bureau à distance | | | | |
| 🗉 🚔 PKI d'entreprise | | | | |
| ⊞ | | | | |
| 🗉 📃 Utilisateurs et ordinateurs Active Directory [WIN-9: | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | ► I | | |
| Le magasin Personnel contient 3 certificats. | | | | |

Figure 137 : Active Directory: Configuration: Certificat Local Machine personnel

Il est possible de les copier/coller depuis le magasin Root vers le magasin Personnel de l'ordinateur local :

| 🚟 01-asipsante-smartcard-logon-conso | le - [Racine de la console\Certificats | (ordinateur local)\Autorités de cer | tification racines | de confiance\Certificat | s] 🔺 |
|--|--|---|--------------------|-------------------------|-------------------------|
| 🚠 Fichier Action Affichage Favoris I | Fenêtre ? | | | | |
| 🗢 🔿 🖄 📰 🖌 🖦 🛛 | | | | | |
| Racine de la console | Délivré à 🔺 | Délivré par | Date d'expiration | Rôles prévus | Nom cor |
| 🖃 🗊 Certificats (ordinateur local) | AC RACINE IGC-SANTE ELEMENT | AC RACINE IGC-SANTE ELEMENTAIRE | 25/06/2033 | <tout></tout> | <aucun< td=""></aucun<> |
| 🖻 🧮 Personnel | AC RACINE IGC-SANTE FORT | AC RACINE IGC-SANTE FORT | 25/06/2033 | <tout></tout> | <aucun< td=""></aucun<> |
| 🚞 Certificats | AC RACINE IGC-SANTE STANDARD | AC RACINE IGC-SANTE STANDARD | 25/06/2033 | <tout></tout> | <aucun< td=""></aucun<> |
| Autorités de certification racines de | AddTrust External CA Root | AddTrust External CA Root | 30/05/2020 | Authentification du s | USERTri |
| Certificats | ASIP-SANTE TECHNIQUE | ASIP-SANTE TECHNIQUE | 31/12/2030 | <tout></tout> | <aucun< td=""></aucun<> |
| | Baltimore CyberTrust Root | Baltimore CyberTrust Root | 13/05/2025 | Authentification du s | Baltimor |
| Autorités de certification intermédi | Glass 3 Public Primary Certification | Class 3 Public Primary Certification A | 02/08/2028 | Messagerie électroni | VeriSign |
| Editeurs approuves | Class 3 Public Primary Certification | Class 3 Public Primary Certification A | 08/01/2004 | Messagerie électroni | VeriSign |
| Certificats non autorises | Copyright (c) 1997 Microsoft Corp. | Copyright (c) 1997 Microsoft Corp. | 31/12/1999 | Enregistrement des i | Microsol |
| Autorites de certification racine del Personnes autorisées | DigiCert Assured ID Root CA | DigiCert Assured ID Root CA | 10/11/2031 | Authentification du s | DigiCert |
| Personnes autorisees Remote Desktop | GigiCert Global Root CA | DigiCert Global Root CA | 10/11/2031 | Authentification du s | DigiCert = |
| Remote Desktop Demandes d'inscription de certifical | DigiCert High Assurance EV Root CA | DigiCert High Assurance EV Root CA | 10/11/2031 | Authentification du s | DigiCert |
| E Contantació d'inscripción de certaned E Carte à pui | Equifax Secure Certificate Authority | Equifax Secure Certificate Authority | 22/08/2018 | Messagerie électroni | GeoTrus |
| F F SPC | www.FR-ASIPSANTE-00-CA | eu-FR-ASIPSANTE-00-CA | 30/09/2019 | <tout></tout> | <aucun< td=""></aucun<> |
| ⊕ ☐ Périphériques approuvés ☐ | Contraction Contractica Contra | eu-FR-ASIPSANTE-00-CA | 30/09/2019 | <tout></tout> | <aucun< td=""></aucun<> |
| 표 🔜 Certificats - Utilisateur actuel | GeoTrust Global CA | GeoTrust Global CA | 21/05/2022 | Authentification du s | GeoTrus |
| 🗉 🚰 Configuration d'hôte de session Bureau | GIP-CPS | GIP-CPS | 31/12/2020 | <tout></tout> | <aucun< td=""></aucun<> |
| 🗉 📆 Domaines et approbations Active Direc | GIP-CPS ANONYME | GIP-CPS ANONYME | 31/12/2020 | <tout></tout> | <aucun< td=""></aucun<> |
| 🕀 🧾 Stratégie Default Domain Controllers P | GIP-CPS PROFESSIONNEL | GIP-CPS PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun< td=""></aucun<> |
| 🛨 📷 Gestionnaire des services Bureau à disl | GIP-CPS STRUCTURE | GIP-CPS STRUCTURE | 31/12/2020 | <tout></tout> | <aucun< td=""></aucun<> |
| 🛨 🎒 PKI d'entreprise | GIP-CPS-TEST | GIP-CPS-TEST | 31/12/2020 | <tout></tout> | <aucun< td=""></aucun<> |
| Sites et services Active Directory | GlobalSign Root CA | GlobalSign Root CA | 28/01/2028 | Authentification du s | GlobalSi |
| 🕀 📔 Utilisateurs et ordinateurs Active Direct | GTE CyberTrust Global Root | GTE CyberTrust Global Root | 14/08/2018 | Messagerie électroni | GTE Cył |
| | IGC/A | IGC/A | 17/10/2020 | Authentification du s | Secréta |
| | Microsoft Authenticode(tm) Root | Microsoft Authenticode(tm) Root Au | 01/01/2000 | Messagerie électroni | Microsol |
| | Microsoft Root Authority | Microsoft Root Authority | 31/12/2020 | <tout></tout> | Microsol |
| | Microsoft Root Certificate Authority | Microsoft Root Certificate Authority | 10/05/2021 | <tout></tout> | Microsol |
| | NO LIABILITY ACCEPTED, (c)97 V | NO LIABILITY ACCEPTED, (c)97 Veri | 08/01/2004 | Enregistrement des i | VeriSian |
| | TEST ANONYME | TEST ANONYME | 31/12/2020 | <tout></tout> | <aucun< td=""></aucun<> |
| | TEST PROFESSIONNEL | TEST PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun< td=""></aucun<> |
| | | TEST STRUCTURE | 31/12/2020 | <tout></tout> | <aucun< td=""></aucun<> |
| | | TEST TECHNIQUE | 31/12/2030 | <tout></tout> | <aucun< td=""></aucun<> |
| | Thawte Premium Server CA | Thawte Premium Server CA | 02/01/2021 | Authentification du s | Thawte |
| | Thawte Premium Server CA | Thawte Premium Server CA | 01/01/2021 | Authentification du s | thawte |
| | thawte Primary Root CA | thawte Primary Root CA | 17/07/2036 | Authentification du s | thawte |
| | Thawte Timestamping CA | Thawte Timestamping CA | 01/01/2021 | Enregistrement des i | Thawte |
| | UTN - DATACorp SGC | UTN - DATACorp SGC | 24/06/2019 | Authentification du s | USERTri |
| | VeriSign Class 3 Public Primary Cer | VeriSign Class 3 Public Primary Certifi | 17/07/2036 | Authentification du s | VeriSign 🖕 |
| • | | | | | ► |

Figure 138 : Active Directory: Configuration: Copie de certificats Racine

| 長 192.168.7.14 - Connexion Bureau à distar | nce | | | | • × |
|--|------------------------------|---------------------------------|-------------------|------------------------|-----------------------------|
| 👼 01-asipsante-smartcard-logon-console - [Racine de la console\Certificats (ordinateur local)\Personnel\Certificats] 🔷 🔺 | | | | | |
| Fichier Action Affichage Favoris Fenêtre ? | | | | | |
| 🗢 🔿 🖄 💼 🔏 🖦 🔽 | | | | | |
| 📔 Racine de la console | Délivré à 🔺 | Délivré par | Date d'expiration | Rôles prévus | Nom cor |
| 🖃 🗊 Certificats (ordinateur local) | au-FR-ASIPSANTE-00-CA | eu-FR-ASIPSANTE-00-CA | 30/09/2019 | <tout></tout> | <aucun< td=""></aucun<> |
| | 🙀 fr-asipsante-00.eu.cosign | eu-FR-ASIPSANTE-00-CA | 30/09/2015 | Authentification du cl | <aucun< td=""></aucun<> |
| Certificats | AC RACINE IGC-SANTE ELEMENT | AC RACINE IGC-SANTE ELEMENTAIRE | 25/06/2033 | <tout></tout> | <aucun< td=""></aucun<> |
| Autorites de certification racines de Cortificate | AC RACINE IGC-SANTE FORT | AC RACINE IGC-SANTE FORT | 25/06/2033 | <tout></tout> | <aucun< td=""></aucun<> |
| Certificats | AC RACINE IGC-SANTE STANDARD | AC RACINE IGC-SANTE STANDARD | 25/06/2033 | <tout></tout> | <aucun< td=""></aucun<> |
| El connance de rendreprise El Connance de rendreprise El Connance de rendreprise | | ASIP-SANTE TECHNIQUE | 31/12/2030 | <tout></tout> | <aucun< td=""></aucun<> |
| E fditeurs approuvés | 🖳 GIP-CPS | GIP-CPS | 31/12/2020 | <tout></tout> | <aucun< td=""></aucun<> |
| | GIP-CPS ANONYME | GIP-CPS ANONYME | 31/12/2020 | <tout></tout> | <aucun< td=""></aucun<> |
| 🕀 🚞 Autorités de certification racine tier | GIP-CPS PROFESSIONNEL | GIP-CPS PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun< td=""></aucun<> |
| 🛨 🚞 Personnes autorisées | GIP-CPS STRUCTURE | GIP-CPS STRUCTURE | 31/12/2020 | <tout></tout> | <aucun< td=""></aucun<> |
| 표 🚞 Remote Desktop | GIP-CPS-TEST | GIP-CPS-TEST | 31/12/2020 | <tout></tout> | <aucun td="" 😑<=""></aucun> |
| 🕀 📔 Demandes d'inscription de certifical | | TEST ANONYME | 31/12/2020 | <tout></tout> | <aucun< td=""></aucun<> |
| 🕀 🚞 Racines de confiance de carte à pu | | TEST PROFESSIONNEL | 31/12/2020 | <tout></tout> | <aucun< td=""></aucun<> |
| I SPC | | TEST STRUCTURE | 31/12/2020 | <tout></tout> | <aucun< td=""></aucun<> |
| Périphériques approuvés | | TEST TECHNIQUE | 31/12/2030 | <tout></tout> | <aucun< td=""></aucun<> |
| Certificats - Utilisateur actuel Certificats - Utilisateur actuel | | | | | _ |
| Configuration d'hote de session Bureau | | | | | _ |
| Domaines et approbations Active Direc | | | | | |
| 🐨 🧾 Scrategie Deradic Domain Concrollers Pr | | | | | |
| E 🏥 PKI d'entrenrise | | | | | |
| Sites et services Active Directory | | | | | |
| F Utilisateurs et ordinateurs Active Direct | | | | | |
| | | | | | |
| | | | | | |
| | | | | | _ |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | - |
| • | | | | | ۰. |
| | | | | | |

Figure 139 : Active Directory: Configuration: Collage de certificats Racine dans le magasin personnel

Le certificat racine « ASIP-SANTE TECHNIQUE » doit aussi être présent.

A minima, les 5 certificats root de production de l'ASIP Santé doivent être présents (les 5 root de l'IGC de santé de production actuelle).

Si des cartes de test sont utilisées (environnements de tests et d'homologation), les 5 certificats root de test de l'ASIP Santé doivent être présents.

Les **3** certificats root de production de la future IGC de santé peuvent être déployés.

Il peut donc y avoir jusqu'à **13** certificats « root » ASIP dans ce magasin.

L'import par fichier « P7B » est aussi possible :

- cer\p7b\01-prod-root.p7b
 - 8 certificats de production
 - cer\p7b\03-test-root.p7b
 - o 5 certificats de test
- cer\p7b\05-all-root.p7b
 - o 13 certificats de production et de test

Conseil : Se reporter au chapitre « Détails de certificat » et imprimer le tableau et matérialiser la vérification en cochant la case « Check »

Conseil : les certificats de <u>test</u> ASIP Santé doivent être supprimés des environnements de production

12.11.1.2 Magasins Certificats Racine et intermédiaires

Cf. CPSRev.

S'assurer que le certificat racine de l'AD CS est provisionné dans la magasin racine (fait par défaut sur l'AD CS est sur le contrôleur de domaine).

12.11.1.3 Magasin NTAuth

Ajout des certificats d'autorités **client (racine + intermédiaire) + serveur** (racine) dans le magasin **NTAuth**.:

« MMC -> PKI d'entreprise -> Clic droit -> gérer les conteneurs Active Directory -> Conteneur NTAuthCertificates -> Ajouter »

| Gérer les conteneurs Active Directory | × |
|---|---|
| Conteneur des autorités de certification Conteneur des Conteneur NTAuthCertificates Conteneur AIA Conteneur | s services d'inscription CDP Conteneur KRA |
| Nom | Statut OK |
| | |
| | |
| | |
| Ajouter | |
| | OK Annuler |

Figure 140 : Active Directory: Configuration: Magasin NTAUTH avant import

| Conteneur des autorités de certification Uniteneur d Conteneur NTAuthCertificates Conteneur AIA Conteneur | es services « CDD Ì c | : d'inscription Contonour K D A |
|--|--------------------------|------------------------------------|
| | | |
| Nom | Statut | |
| AC IGC-SANTE ELEMENTAIRE ORGANISATIONS | OK | |
| 🙀 AC IGC-SANTE ELEMENTAIRE PERSONNES | OK | |
| 🙀 AC IGC-SANTE FORT ORGANISATIONS | OK | |
| 🙀 AC IGC-SANTE FORT PERSONNES | OK | |
| 🙀 AC IGC-SANTE STANDARD ORGANISATIONS | OK | |
| 🙀 AC IGC-SANTE STANDARD PERSONNES | OK | |
| 🙀 AC RACINE IGC-SANTE ELEMENTAIRE | OK | |
| 🙀 AC RACINE IGC-SANTE FORT | OK | |
| 🙀 AC RACINE IGC-SANTE STANDARD | OK | |
| 🙀 AC-CLASSE-4 | OK | |
| 🙀 AC-CLASSE-4-TEST | OK | |
| 🙀 AC-CLASSE-5 | OK | |
| 🙀 AC-CLASSE-5-TEST | OK | |
| 🙀 AC-CLASSE-6 | OK | |
| 🙀 AC-CLASSE-6-TEST | OK | |
| ↓ | | |
| Aiguter Supprimer Afficher | | |
| | | |

Figure 141 : Active Directory: Configuration: Magasin NTAUTH après import

- ⇒ 49 certificats au format .cer à importer 1 à 1
 - 40 certificats ASIP Santé
 - 20 de test
 - 5 root, 15 intermédiaires
 - 20 de production
 - 5 root, 15 intermédiaires
 - 9 certificats correspondants à la future IGC de santé
 - 9 de production
 - 3 root, 6 intermédiaires
 - fournis dans le répertoire cer\cer\,
- ⇒ 1 certificat Autorité de certification AD CS

A minima:

- 1. les 5 certificats racine de l'IGC de production actuelle de l'ASIP Santé
- 2. les 15 certificats intermédiaires de l'IGC de production de actuelle l'ASIP Santé
- 3. les 9 certificats (3 roots + 6 intermédiaires) de la future IGC de production l'ASIP Santé
- 4. le certificat du l'autorité de certification de l'AD CS

doivent être présents.

Si des cartes de test sont utilisées (environnements de tests et d'homologation), les 5 certificats racines et les 15 certificats intermédiaires de test de l'ASIP Santé doivent être présents.

Il peut donc y avoir jusqu'à 49 certificats ASIP dans ce magasin et 1 certificat AD CS.

L'import par fichier « P7B » n'est pas possible, 2 choix s'offrent à nous:

- import un à un des certificats au format .cer
 - source d'erreur!
- import par fichier batch
 - o vivement conseillé !
 - o cf. script bin\00-asipsante-smartcard-logon-ntauth-manage.cmd fourni

La commande qui permet d'automatiser cet import est:

certutil -dspublish -f "fichier_certificat_a_importer.cer" NTAuthCA

Tableau 26 : Active Directory: Configuration: Commande certutil d'import des certificats dans le magasin NTAUTH

Conseil : Se reporter au chapitre « Détails des certificats ASIP Santé », imprimer ce tableau et matérialiser la vérification en cochant la case « Check »

Conseil : les certificats de <u>test</u> ASIP Santé doivent être supprimés des environnements de production

12.11.2 Stratégie Active Directory

12.11.2.1 Ajout des autorités racines client et serveur

« MMC -> Default Domain Controllers policy -> Configuration ordinateur -> Stratégies -> Paramètres Windows -> Paramètres de sécurité -> Stratégie de clé publique -> Autorité de certification racines de confiance -> importer »





| 🧱 01-asipsante-smartcard-logon-console - [Racine de la console\Stratégie D | efau | ult Domain Controllers Policy [fr-asip | osante-00.eu.cosign] | \Configuration ordinateur\] 📃 🗖 🗙 |
|--|------|--|--|--|
| 🚰 Eichier Action Affichage Fayoris Fenêtre ? | | | | X |
| 🗢 🔿 🗾 📋 🖻 😹 🛛 🖬 | | | | · · · · · · · · · · · · · · · · · · · |
| Etchier Action Affichage Fayoris Fengêtre 2 Final Control Facine de la console Final Control Final Control Final Control Final Control Final Control Final Control Final Control Final Control Final Control Final Control Final Control Final Control Final Control Final Control Final Contiguration ordinateur Final Control Final Control Final Control Final Contiguration ordinateur Final Control Final Control Final Control Final Contiguration ordinateur Final Control Final Control Final Control Final Contiguration ordinateur Final Control Final Control Final Control Final Contiguration ordinateur Final Control Final Control Final Control Final Contiguration ordinateur Final Control Final Control Final Control Final Control Paramètres de Socurté Final Control Final Control Final Control Final Control Final Control Final Control Final Control Final Control Final Control Final Control Final | | Délivré à A AC RACINE IGC-SANTE ELEMENT AC RACINE IGC-SANTE TANDARD ASIP-SANTE TECHNIQUE GU-R-ASIPSANTE-00-CA GIP-CPS GIP-CPS GIP-CPS TEST RUCTURE GIP-CPS-TEST TEST PROFESSIONNEL TEST PROFESSIONNEL TEST TECHNIQUE TEST TECHNIQUE | Délivré par AC RACINE IGC-SAN AC RACINE IGC-SAN AC RACINE IGC-SAN ASIP-SANTE TECHNIK eu-RFA-SIPSANTE-OC GIP-CPS PROFESSION GIP-CPS STRUCTURE GIP-CPS STRUCTURE TEST ANONYME TEST STRUCTURE TEST STRUCTURE TEST STRUCTURE | Actions Autorités de certification racines d Autres actions |
| Autorités de centritication racines de certificat Autorités de certification racines de confiance Confiance de l'entreprise Autorités de certification intermédiaires Autorités non autorités | | | | |
| x | ľ | • | Þ | |
| Le magasin Autorités de certification racines de confiance contient 14 certificats. | | | | |

Figure 143 : Active Directory: Configuration: Stratégie de clé publique après import

A minima:

- 1. les 5 certificats racine de l'IGC de production actuelle de l'ASIP Santé
- 2. les 3 certificats racine de la future IGC de production de l'ASIP Santé
- 3. le certificat du l'autorité de certification de l'AD CS

Doivent être présents.

Si des cartes de test sont utilisées (environnements de tests et d'homologation), les 5 certificats racines de l'ASIP Santé doivent être présents.

Il peut donc y avoir jusqu'à 13 certificats ASIP dans ce magasin et <u>1 certificat AD CS</u>.

L'import par fichier « P7B » est possible :

- cer\p7b\01-prod-root.p7b
 - 8 certificats de production
- cer\p7b\03-test-root.p7b
 - 5 certificats de test
- cer\p7b\05-all-root.p7b
 - \circ 13 certificats de production et de test

Conseil : Se reporter au chapitre « Détails de certificat », imprimer le tableau et matérialiser la vérification en cochant la case « Check »

Conseil : les certificats de <u>test</u> ASIP Santé doivent être supprimés des environnements de production

12.11.2.2 Ajout des autorités intermédiaires client et serveur

[3] page 17 point 13 stipule de compléter l'action précédente par :

« MMC -> Default Domain Controllers policy -> Configuration ordinateur -> Stratégies -> Paramètres Windows -> Paramètres de sécurité -> Stratégie de clé publique -> Autorité de certification intermédiaire -> importer »

Dans une configuration « de base », cette opération n'est apparemment pas nécessaire. Elle peut l'être sur une infrastructure complexe.

12.12 Création des utilisateurs

12.12.1 Construction de l'identifiant UPN

L'UPN (Universal Principal Name) est un identifiant unique présent dans le certificat d'authentification de la carte CPS (depuis Mars 2011) qui sert à faire le lien avec un compte utilisateur dans un annuaire Active Directory sur un contrôleur de domaine.

Cet UPN est construit de la manière suivante: préfixeUPN@suffixeUPN

Le **préfixeUPN** est la partie identifiant de manière unique la carte CPS.

- Il est construit de la manière suivante :
- Format : <Type d'identifiant>.<Id registre national>.<Id registre structure>
- Données correspondants au champ « CN » (= identifiant professionnel et personnel de santé) du champ « Objet » présent dans les certificats de la carte CPS.
- Cet identifiant PS est aussi inscrit physiquement sur le recto de la carte CPS, sur la première ligne imprimée sous la puce électronique.
- Un point est rajouté en deuxième position, pour séparer le premier chiffre (code du type d'identifiant PS sur un caractère), du reste de l'identifiant PS.
- Un point remplace chaque caractère spécial de cet identifiant PS.
- L'identifiant sur le registre de la structure est optionnel (en fonction du type d'identifiant).

Le suffixeUPN correspond à un nom de domaine générique géré par l'ASIP Santé

- il est fixe
- il a pour valeur : carte-cps.fr

Exemples d'UPN:

| identifiant PS | CN | UPN |
|---|---------------------------|--|
| numéro de SIRET (code '5') + numéro de registre (numéro interne à la structure) | 51871275100020/0000000137 | 5.18751275100020.0000000137@ carte-cps.fr |
| numéro FINESS (code '3') + numéro de registre structure | 30B0018289/CPET0003 | 3.0B0018289.CPET0003@carte- cps.fr |
| numéro ADELI (code '0') | 00B6010140 | 0.0B6010140@carte-cps.fr |
| numéro RPPS (code '8') | 899700011143 | 8.99700011143@carte-cps.fr |

Tableau 27 : Déploiement UPN : Construction de l'UPN

12.12.3 Déclaration du suffixe carte-cps.fr dans l'AD

Si le suffixe de l'UPN n'apparait pas dans la liste des noms de domaines connus, une relation d'approbation avec le domaine existant devra préalablement être créée:

Outils d'administration -> Domaines et approbations Active Directory.

Pour ajouter une approbation au domaine existant, cliquer droit sur « **Domaines et approbations Active Directory »** puis choisir **« Propriétés »** et ajouter « **carte-cps.fr** »:

| 🔒 Domaines et approbations Active D | irectory | Propriétés de : Domaines et approbations Active Directory [m 🕐 🗙 |
|-------------------------------------|----------|---|
| Fichier Action Affichage ? | Nom | Suffixes UPN Les noms du domaine actif et du domaine racine sont les suffixes UPN (nom utilisateur principal) par défaut. L'ajout d'autres noms de domaines augmente la sécurité des sessions et simplifie les noms d'ouverture de session des utilisateurs. Si vous voulez que d'autres suffixes UPN apparaissent lors de la création d'utilisateurs, ajoutez-les à la liste suivante. Autres suffixes UPN : Carte-cps.fr Supprimer |
| | | OK Annuler Appliquer Aide |

 $\textbf{Figure 144:} Active \ Directory: \ Configuration: \ Approbation \ du \ suffixe \ UPN \ « \ carte-cps.fr \ »$

12.12.4 Déclaration d'un utilisateur

Un nouvel utilisateur se déclare de la façon suivante dans l'AD :

| ouvel objet - Utilisat | eur | | | × |
|------------------------|---------------------|-----------------|-----------------|---------|
| Créer dans : | eu.cosign/Us | ers | | |
| Prénom : | Carte1 | | Initiales : | |
| Nom : | | | | |
| Nom complet : | Carte1 | | | |
| Nom d'ouverture de s | ession de l'utilisa | ateur : | | |
| 0.0B1055421 | | @carte-cps: | fr | • |
| Nom d'ouverture de s | ession de l'utilisa | ateur (antérieu | rà Windows 2000 | D) : |
| cosign\ | | Carte 1 | | |
| | | | | |
| | - | < Précédent | Suivant > | Annuler |

Figure 145 : Active Directory: Configuration: Définition d'un compte avec Smartcard logon activé

| Nouvel objet - Utilisateur | × |
|---|---|
| Créer dans : eu.cosign/Users | |
| Mot de passe : | |
| Confirmer le mot de passe : | |
| L'utilisateur doit changer le mot de passe à la proc <u>h</u> aine ouverture de session | |
| L'utilisateur <u>n</u> e peut pas changer de mot de passe | |
| Le mot de passe n'expire jamais | |
| Le compte est désactivé | |
| | |
| | |
| < <u>P</u> récédent <u>S</u> uivant > Annule | r |

Figure 146 : Active Directory: Configuration: Définition d'un compte avec Smartcard logon activé

Prêter attention à bien spécifier le domaine carte-cps.fr.

- ⇒ Voir annexe sur l'UPN
- ⇒ Voir figure « Active Directory: Approbation du suffixe UPN « carte-cps.fr » »

Si ce compte fait du Smartcard logon en TSE, se reporter à la section Terminal Serveur pour l'autorisation d'ouverture de session TSE associée.

➡ Voir annexe sur le service de bureau à distance si le bureau à distance est utilisé (groupe et stratégie AD)

| Windows Securi | ty | × |
|-----------------------------------|---|---|
| Enter your cro These credentia | edentials als will be used to connect to cosign. | _ |
| | florent.desgrippes | |
| | Use another account | |
| | 00B1055421 Smart card credential 0.0B1055421@carte-cps.fr •••• | |
| 🗌 Reme | mber my credentials | |
| | OK Cancel | |

Figure 147 : Active Directory: Configuration: Smartcard logon en TSE



Figure 148 : Active Directory: Configuration: Bureau à distance et CPS Gestion après Smartcard logon

12.13 Paramétrage du Smartcard logon sur des nouveaux comptes AD

Le paramétrage démontré précédemment permet de configurer des comptes nouvellement créés pour le cas d'usage spécifique du Smartcard logon.

Le cas d'utilisation le plus fréquent concerne cependant l'ajout de la possibilité de faire du Smartcard logon à des comptes AD préexistants.

Cette section décrit le paramétrage et les développements nécessaires pour implémenter ce cas d'usage.

12.13.1 Script de déploiement des UPNs dans un active directory

La manière la plus simple de relier une carte CPS à un utilisateur stocké dans un annuaire Active Directory est d'éditer directement cet utilisateur dans l'Active Directory en lui attribuant l'UPN de la carte CPS correspondante, dans ses propriétés.

Néanmoins, dans les grosses structures contenant des centaines, voire des milliers d'utilisateurs déjà existants, il sera fastidieux de modifier manuellement chaque utilisateur.

On utilise alors, pour faciliter le déploiement, des scripts de modification de l'Active Directory, automatisés.

Les langages de scripts les plus courants sont :

- VBS (Visual Basic Scripting)
 - vivement déconseillé, sauf à disposer de compétences déjà bien établies sur cette technologie
- Windows PowerShell
 - Vivement conseillé

Ce sont des outils puissants de création de scripts d'administration.

Deux exemples de scripts VBS sont fournis ci-dessous.

Ils permettent l'ajout ou la modification de comptes utilisateurs dans un Active Directory.

La modification des utilisateurs se base sur une liste d'utilisateurs existants, reformatée dans un fichier texte dont la grammaire est fournie.

Ces scripts sont à adapter en fonction de l'architecture existante :

- utilisateurs stockés dans des OUs particuliers
- connexion à l'AD différente
- modification d'autres caractéristiques des utilisateurs
- etc...

Le script qui suit est un exemple de script VBS permettant la modification de l'UPN d'utilisateurs existants dans un annuaire Active Directory, à partir d'une liste d'utilisateurs/UPNs stockée dans un fichier texte (ici « c:\users.txt ») :

| set Root = GetObject("LDAP://RootDSE") |
|--|
| DomainPath = Root.Get("DefaultNamingContext") |
| Set Domain = GetObject("LDAP://" & DomainPath) |
| wscript.echo DomainPath 'nom de domaine récupéré |
| ' modification utilisateurs en masse |
| Const ForReading = 1 |
| numError = 0 |
| set fso = CreateObject("Scripting.FileSystemObject") |
| set usersTextFile = fso.OpenTextFile(" C:\users.txt ", ForReading, False) 'ouverture du fichier texte des utilisateurs |
| On error Resume next |
| While Not usersTextFile.atEndOfStream 'boucle sur le fichier texte |
| strRecord = usersTextFile.ReadLine ' Lecture d une ligne entiere |
| arrRecord = Split(strRecord, ";") ' decoupage avec caractere de separation ; |
| wscript.echo "utilisateur : " & arrRecord(0) & " - UPN: " & arrRecord(1) |
| Set objUser = GetObject("LDAP://localhost:389/CN=" & arrRecord(0) & ",CN=Users,"& DomainPath) ' |
| connexion a l'objet USER |
| if (Err.Number <> 0) then |
| Err.Number = 0 |
| wscript.echo "erreur : utilisateur introuvable: " & arrRecord(0) |
| numError = numError + 1 |
| end if |
| objUser.Put "UserPrincipalName", arrRecord(1) ' modification de l UPN |
| objUser.SetInfo 'validation de la modification |
| Wend |
| usersTextFile.close 'fermeture du fichier texte |
| wscript.echo "FIN script modification utilisateur OK : nombre d'erreurs : " & numError |

 Tableau 28 : Déploiement UPN : Exemple de script VBS permettant la modification de l'UPN d'utilisateurs existants dans un annuaire Active Directory

Le fichier **c:\users.txt** correspondant contiendrait des données organisées de cette manière:

user1;8.99700011141@carte-cps.fr user2;8.99700011142@carte-cps.fr user3;8.99700011143@carte-cps.fr user4;8.99700011144@carte-cps.fr user5;8.99700011145@carte-cps.fr user6;8.99700011146@carte-cps.fr user7;8.99700011147@carte-cps.fr user8;8.99700011148@carte-cps.fr

Tableau 29: Déploiement UPN : Exemple de Fichier « users.txt »

Ci-après, un exemple de script VBS permettant la création d'utilisateurs en masse (ici 10), dans un annuaire Active Directory :

set Root = GetObject("LDAP://RootDSE") DomainPath = Root.Get("DefaultNamingContext") Set Domain = GetObject("LDAP://" & DomainPath) wscript.echo DomainPath 'nom de domaine récupéré Set objOU = GetObject("LDAP://localhost:389/CN=Users," & DomainPath) for i =1 to 10 ' Ajout ici de 10 utilisateurs automatiquement Set objUSER = objOU.Create("User", "cn=testUSERnum" & i) objUser.Put "givenName", "test_givenName" &i objUser.Put "sn", "test_surName"&i objUser.Put "displayName", "test_DisplayName"&i objUser.Put "SAMAccountName", "USER test" & i objUser.Put "UserPrincipalName", "UPNtest" & i & "@carte-cps.fr" objUser.Put "mail", "test_mail@asipsante.fr" objUser.Put "initials", "asip" & i objUser.SetInfo objUser.AccountDisabled = FALSE ' activation du compte objUser.SetInfo Next wscript.echo "FIN script ajout utilisateur OK."

 Tableau 30 : Déploiement UPN: Exemple de script VBS permettant la création d'utilisateurs dans un annuaire Active

 Directory

12.14 Paramétrage du Smartcard logon sur des comptes AD préexistants

12.14.1 Cas "1-to-1" : {un compte existant ; une carte}

Dans le cas bijectif {un compte existant ; une carte}, l'idée est de ramener à la déclaration de compte de :

| Propriétés de : Carte6 Carte6. Carte6 🛛 🔋 🗙 |
|---|
| Environnement Sessions Contrôle à distance Profil des services Bureau à distance Bureau virtuel personnel COM+ |
| Général Adresse Compte Profil Téléphones Organisation Membre de Appel entrant Nom d'ouverture de session de l'utilisateur : @eu.cosign Image: Cartebook Image: Carteboo |
| Horaires d'accès Se connecter à |
| L'utilisateur devra changer le mot de passe L'utilisateur ne peut pas changer de mot de passe V Le mot de passe n'expire jamais Enregistrer le mot de passe en utilisant un chiffrement réversible |
| Date d'expiration du compte Image: Good State Image: Good State Image: State |
| OK Annuler Appliquer Aide |

à:

| ropriétés de : Carte6 Carte6. Carte6 🛛 🧍 🗙 |
|--|
| Environnement Sessions Contrôle à distance |
| Profil des services Bureau à distance Bureau virtuel personnel COM+ |
| General Adresse Compre Proni Telephones Urganisation Membre de Appel entrant |
| Nom d'o <u>u</u> verture de session de l'utilisateur : |
| 0.0B1055413 |
| Nom d'ouverture de session de l'utilisateur (antérieur à <u>W</u> indows 2000) : |
| cosign\ Carte6 |
| Horaires d'accès <u>S</u> e connecter à |
| Déverrouiller le compte |
| Options de compte : |
| 🗖 L´utilisateur devra changer le mot de passe |
| L'utilisateur ne peut pas changer de mot de passe |
| I ← Le mot de passe n'expire jamais |
| |
| Date d'expiration du compte |
| 🖸 Jamais |
| O <u>F</u> in de : samedi 15 novembre 2014 |
| |
| |
| OK Annuler Aide Aide |

Figure 149 : Paramétrage du Smartcard logon sur des comptes AD préexistants : cas {un compte existant ; une carte}

Dans ce cas, l'utilisateur peut se logger en Smartcard logon avec sa carte CPx (UPN <u>0.0B1055413@carte-cps.fr</u> ici).

Il peut aussi se logger en login / mot de passe en utilisant dans ce cas:

- Login : COSIGN\Carte6 (à adapter)
- Mot de passe : son_mot_de_passe

Cette opération peut être automatisée.

12.14.2 Cas "n-to-m": mappages de comptes existants sur des attributs de certificats X509 [Win2008R2]

Il est possible d'associer plusieurs cartes un utilisateur ou même 1 carte à plusieurs utilisateurs (ce dernier cas étant par ailleurs déconseillé).

Ce cas permet aussi de retrouver le cas particulier "1-to-1", sans éditer le nom d'ouverture de session utilisateur mais en perdant en ergonomie (voir ci-après).

Lancer la gestion d'utilisateur dans une MMS en choisissant les « Fonctionnalités avancées »



Figure 150 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants

Clic-droit sur le « user » :

| 01-asipsante-smartcard-logon-co Fichier Action Affichage Favor Fichier Action Affichage Favor | onsole - [Racine de is Fenêtre ? | e la console\Utilisi | ateurs et ordinateurs A |
|--|--|---|--|
| 🚞 Racine de la console | Nom | Туре | Description |
| PKI d'entreprise Certificats (ordinateur local) Utilisateurs et ordinateurs Active Requêtes enregistrées E eu.cosign Builtin Computers Domain Controllers ForeignSecurityPrincipals LostAndFound Managed Service Account | Administrateur Administrate Administrate Administrate Admins du do Contrôleurs Contrôleurs CPS3 CL Éditeurs de c Florent Desg | Utilisateur Groupe de sécu Groupe de sécu Groupe de sécu Groupe de sécu Groupe de sécu Utilisateur Groupe de sécu Utilisateur | Compte d'utilisateur d'ad Administrateurs désignés Administrateurs désignés Administrateurs désignés Tous les contrôleurs de d Les membres de ce group Les membres de ce group |
| | Florest FDF Copier Gro Gro Ajouter Invi Désactiv Réinitiali Déplacer | Utilizatione à un groupe es des noms er le compte ser le mot de passe | nots de passe des m nots de passe des m pte d'utilisateur invit les invités du domai pte de service du ce |

Figure 151 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants

Choisir « Mappages des noms » :

| ertificats X.509 Noms Kert | peros | |
|---|----------------|--|
| Compte d'utilisateur mappé | : | |
| eu.cosign/Users/Florent Fl Certificats X-509 : | DE. Desgrippes | |
| Certificats pour | Délivré par | |
| | | |
| | | |
| | | |
| Ajouter Modifie | r Supprimer | |
| | | |

Figure 152 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants

Ajouter le certificat carte :

| Mappage des identités de sécurité | ?× |
|---|------|
| Certificats X.509 Noms Kerberos | |
| Compte d'utilisateur mappé : | |
| eu.cosign/Users/Florent FDE. Desgrippes | |
| Certificats X-509 : | |
| Certificats pour | |
| CN=518/512/5100020/0000000311 SN=DESGRIPPES G=FLC | ORE |
| | |
| | |
| | ъ |
| Ajouter Modifier Supprimer | |
| OK Annuler Applic | quer |

Figure 153 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants

Cela correspond en fait à une alimentation des attributs de l'utilisateur dans l'AD :

| ofil des services Bureau atributs : | à distance Bureau virtuel person | Éditeur de chaînes à valeurs multiples Attribut : altSecurityIdentities | |
|--|--|---|----------|
| Attribut | Valeur | Voley z zin der i | |
| accountExpires accountNameHistory | (jamais) <non défini=""></non> | Valeure : | Ajouter |
| adminCount adminDescription adminDisplayName | <non défini=""> <non défini=""> <non défini=""></non></non></non> | X509: <i>C=FR,O=GIP-CPS,OU=GIP-CPS STRUCT</i> | Supprime |
| alt Security Identities assistant attribute Certificate Attri audio | X509: <i>C=FR,O=GIP-CPS,OU=G <non défini=""> . <non défini=""> <non défini=""></non></non></non></i> | | |
| badPasswordTime badPwdCount businessCategory | (jamais) 0 <non défini=""></non> | | |
| c ∢[` | <non défini=""></non> | | |
| Madfar | | ОК | Annuler |

Figure 154 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants
Cet enrôlement est automatisable sans qu'il soit nécessaire d'extraire tous les certificats d'authentification de tous les porteurs.

Le format choisi par défaut par Windows pour la chaine de caractère d'identification est :

X509:<I>issuer dn(dn de l'émetteur du certificat carte)<S>subject dn (dn du certificat de la carte)

L'ensemble des possibilités de mapping user / certificat étant :

| Méthode | altSecurityIdentities |
|----------------------|---|
| UPN | |
| Subject | X509: <i>issuer dn(dn de l'émetteur du certificat carte)<s>subject dn (dn du certificat de la carte)</s></i> |
| and Issuer fields | X509: <i>C=FR,O=TEST,OU=TEST PROFESSIONNEL,CN=TEST CLASSE-1<s> C=FR,O=TEST,OU=Médecin,CN=00B1051552+SN=MAXIMAXIMAXIMAXIMAXIMAX5155+G=MUMU MUMUMUMUMUMUMUMUMUMUM</s></i> |
| | X509: <s>subject dn (dn du certificat de la carte)</s> |
| Subject DN | X509: <s> C=FR,O=TEST,OU=Médecin,CN=00B1051552+SN=MAXIMAXIMAXIMAXIMAXIMAX5155+G=MUMU MUMUMUMUMUMUMUMUMUMUM</s> |
| Subject | X509: <ski>subject key identifier (Identificateur de la clé du sujet)</ski> |
| Key Identifier | X509: <ski>b8b585887bd28b0276a58ee878d9f8bfda85fa89</ski> |
| Issuer, and | X509: <i>issuer dn(dn de l'émetteur du certificat carte)<sr><mark>reverse</mark>(numéro de série (serial number))</sr></i> |
| Serial Number | Serial number=4c 70 7d => 7d704c X509: <i>C=FR,O=TEST,OU=TEST PROFESSIONNEL,CN=TEST CLASSE-1<sr>7d704c</sr></i> |
| | X509: <sha1-pukey>thumbprint (empreinte numérique)</sha1-pukey> |
| SHA1 Hash | X509: <sha1-pukey>2bbafed16923267e1a0d205557749691d7829103</sha1-pukey> |
| DECODO | X509: <rfc822>adresse email précisée dans le SAN du certificat</rfc822> |
| name | Méthode non disponible avec les certificats de l'IGC de Santé CPS2Ter actuellement en production (pas de champ email dans le SAN). |

Tableau 31 : Liste des possibilités de mapping user / certificat pour l'authentification par certificat

12.14.3 Cas "n-to-m" : Désactivation de l'utilisation du subjectAltName (SAN)

Par contre, dans le cas du Smartcard logon (authentification par certificat venant d'une carte à puce), l'utilisateur va soumettre son certificat par l'intermédiaire des « couches carte à puce » de Windows qui va chercher, par défaut, à exploiter le subjectAltName (SAN) du certificat pour authentifier l'utilisateur : il faut donc désactiver l'usage du subjectAltName (SAN):

L'usage du subjectAltName (SAN) se désactive en appliquant les paramètres de base de registre suivants :

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kdc] "UseSubjectAltName"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters] "UseSubjectAltName"=dword:0000000

Tableau 32 : Désactivation de l'utilisation du SubjectAltName (SAN)

Cette désactivation doit être effectuée sur tous les KDC.

12.14.4 Cas "n-to-m" : Activation du « hint »

Il faut aussi modifier la GPO Default Domain Policy pour activer la politique :

« MMC -> Default Domain Policy -> Computer Configuration -> Administrative Templates -> Windows Components -> Smart Card -> Allow user name hint »

« MMC -> Default Domain Policy -> Configuration ordinateur -> Stratégies -> Modèles d'administration -> Carte à puce -> Autoriser l'indication du nom d'utilisateur »

Tableau 33 : Activation du « hint »

Afin que de permettre au KDC de retrouver le compte AD:

| 🗐 Éditeur de gestion des stratégies de g | oupe | 1 - | |
|---|--|---|---|
| Fichier Action Affichage ? | | | |
| 🗢 🔿 🙋 📅 🛃 🖬 🝸 | | | |
| Image: Stratégie Default Domain Policy [FR-ASI Image: Stratégies Image: Strate Strategies Image: Strategies Ima | Selectionnez un élément pour obtenir une description. Paramètre Autoriser les certificats sans a Autoriser les certificats sans a Autoriser les certificats dont le Autoriser la propagation de certific E Autoriser l'utilisation de certific E Filtrer les certificats d'ouvertur E Forcer la lecture de tous les ce Artiver la propaga les douerd E Inverser le nom du sujet stock Autoriser l'utilisateur en cas d'ins E Autoriser l'Indication du nom de | État thribut d'utilisation avancée de la clé Activé n de déblocage intégré lors de l'ouvert Non configuré valide pour l'ouverture de session Non configuré é délai de validité a expiré Non configuré ificat à partir d'une carte à puce Non configuré rificat racine Non configuré odes confidentiels en texte brut par l Non configuré codes confidentiels en texte brut par l Non configuré codes confidentiels en texte brut par l Non configuré cidat session e Non configuré e carte à puce Non configuré e carte à puce exbloquée Non configuré é dans un certificat lors de son affich Non configuré stallation réussie du pilote de la carte Non configuré tallation réussie du pilote de la carte Non configuré | |
| Gestionnaire de res: Groupe résidentiel | | | |
| 🕀 🧰 Internet Explorer | • | | Þ |
| | Étendu / Standard / | | |
| 16 paramètre(s) | | | |

Figure 155 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants : GPO « Allow user hint »

Les références pour ce cas d'usage sont :

| # | Références |
|---|--|
| 1 | UseSubjectAltName and smartcard logon |
| | http://blogs.technet.com/b/instan/archive/2010/06/16/usesubjectaltname-and-smartcard- logon.aspx |
| | Disable UPN mapping for SmartCard logon |
| 2 | http://blogs.msdn.com/b/spatdsg/archive/2010/06/14/howto_3a00disable-upn-mapping- for-smartcard-logon.aspx |
| 3 | Map a user to a certificate via all the methods available in the altSecurityIdentities attribute |
| | http://blogs.msdn.com/b/spatdsg/archive/2010/06/18/howto-map-a-user-to-a-certificate-via- all-the-methods-available-in-the-altsecurityidentities-attribute.aspx |

Tableau 34 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants : Références

12.14.5 Cas "n-to-m" : Interface de logon et ergonomie

Les écrans de Winlogon sont alors les suivants :

| | 00B1055413 Ouverture de session par carte à puce 00B1055413@carte-cps.fr Code confidentiel Aide-mémoire du nom d'utilisateur |
|---|--|
| | Changer d'utilisateur |
| C | See Windows: 7 Professionnel N |

Figure 156 : Comptes existants : Ecran de Smartcard logon après lecture d'une carte

L'utilisateur saisit son code porteur et son compte dans le champ « hint » :

| 00B1055413 Ouverture de session par carte à puce 0.0B1055413@carte-cps.fr |
|---|
| •••• COSIGN\Cartel |

Figure 157 : Comptes existants : Saisie du code porteur et du « hint »

La session s'ouvre :



L'ergonomie de ce scénario n'est pas aussi satisfaisante que celle associée à un compte pour lequel l'UPN du SAN est utilisé. Il est nécessaire de bien peser cet élément au moment de la définition du projet.

 Tableau 35 : Comptes existants : Considération d'ergonomie en Smartcard logon sur compte préexistant

12.15 Configuration de la stratégie de détection d'arrachage de la carte

- Démarrer > Exécuter...> services.msc
- Localiser « Stratégie de retrait de la carte à puce » :

| Services | bage 2 | | | | | J× |
|------------------|--|--|--------------|------|-------------------|---------|
| |) 🗟 🔽 📰 🕨 🔳 🛙 🕪 | | | | | |
| Services (local) | Ö Services (local) | | | | | |
| | - Services (weekly | | | | | |
| | Stratégie de retrait de la carte à | Nom 🔺 | Description | État | Type de démarrage | |
| | puce | 🧠 Service Panneau de saisie Tablet PC | Active les f | | Manuel | |
| | Real and the second sec | Service SSTP (Secure Socket Tunnel | Prend en c | | Manuel | |
| | Demarrer le service | 🔍 Services Bureau à distance | Autorise le | Déma | Manuel | |
| | | 🤹 Services de base de module de plat | Active l'acc | | Manuel | |
| | Description : | 🤹 Services de certificats Active Directory | Crée, gère | Déma | Automatique | |
| | Autorise le système à être configuré pour | 🔍 Services de chiffrement | Fournit qu | Déma | Automatique | |
| | moment du retrait de la carte à puce. | 🤹 Services de domaine Active Directory | Service de | Déma | Automatique | |
| | | Services Web Active Directory | Ce service | Déma | Automatique | |
| | | 🔍 Spouleur d'impression | Charge les | Déma | Automatique | |
| | | 🤹 Station de travail | Crée et ma… | Déma | Automatique | |
| | | Stratégie de retrait de la carte à puce | Autorise le | | Manuel | |
| | | Système d'événement COM+ | Prend en c | Déma | Automatique | |
| | | 🤹 Système de couleurs Windows | Le service | | Manuel | |
| | | 🔍 Système de fichiers EFS (Encrypting | Fournit la t | | Manuel | |
| | | 🔍 Téléphonie | Prend en c | | Manuel | |
| | | 🕵 Temps Windows | Conserve I | Déma | Automatique | |
| | | 🔅 Thèmes | Fournit un | Déma | Automatique | |
| | | TP AutoConnect Service | ThinPrint | Déma | Manuel | |
| | | 🔍 TP VC Gateway Service | ThinPrint c | | Manuel | |
| | | 🔍 VMware Snapshot Provider | VMware Sn | | Manuel | |
| | | 🔍 VMware Tools | Fournit un | Déma | Automatique | |
| | | 🔍 WebClient | Permet à u | | Manuel | |
| | | 🔍 Windows CardSpace | Active en t | | Manuel | |
| | | 🐝 Windows Defender | Protection | Déma | Automatique (débu | · 💽 |
| | | <u>اً</u> | | | | ۲Ē |
| | Étendu 🖌 Standard 🖊 | | | | | _ |
| | | | | | | |

Figure 159 : Configuration de la Stratégie de retrait de la carte à puce (manuel)

| Propriétés de Stra | tégie de retrait de la carte à puce (Ordinateur I 🗴 |
|-------------------------------------|--|
| Général Connexio | on Récupérati Propriétés de Stratégie de retrait de la carte à |
| Nom du service : | SCPolicySvc |
| Nom complet : | Stratégie de retrait de la carte à puce |
| Description : | Autorise le système à être configuré pour verrouiller 🔺 le Bureau de l'utilisateur au moment du retrait de la 🚽 |
| Chemin d'accès d C:\Windows\syst | les fichiers exécutables : em32\svchost.exe -k netsvcs |
| Type de démarrag | ge : Automatique |
| <u>Obtenir de l'aide p</u> | oour configurer les options de démarrage des services. |
| État du service : | Arrêté |
| Démarrer | Arrêter Suspendre Reprendre |
| Vous pouvez spé service. | cifier les paramètres qui s'appliquent au démarrage du |
| Paramètres de dé | marrage : |
| | |
| | |
| | |
| | OK Annuler Appliquer |

Figure 160 : Configuration de la Stratégie de retrait de la carte à puce (passage en automatique)

| Q Services | | | | | |
|----------------------|---|--|--------------|------|---------------------|
| Fichier Action Affic | hage ? | | | | |
| 🧇 🔿 📅 📮 🧔 | à 🗟 🛛 🖬 🕨 🔲 II ID | | | | |
| 🤹 Services (local) | 🔕 Services (local) | | | | |
| | Stratégie de retrait de la carte à | Nom 🔺 | Description | État | Type de démarrage 🔺 |
| | puce | 🥋 Service Panneau de saisie Tablet PC | Active les f | | Manuel |
| | Démorror la convice | Service SSTP (Secure Socket Tunnel | Prend en c | | Manuel |
| | Demarren le service | 🥵 Services Bureau à distance | Autorise le | Déma | Manuel |
| | | Services de base de module de plat | Active l'acc | | Manuel |
| | Description : | Services de certificats Active Directory | Crée, gère | Déma | Automatique |
| | verrouiller le Bureau de l'utilisateur au | Services de chiffrement | Fournit qu | Déma | Automatique |
| | moment du retrait de la carte à puce. | Services de domaine Active Directory | Service de | Déma | Automatique |
| | | Services Web Active Directory | Ce service | Déma | Automatique |
| | | 🤤 Spouleur d'impression | Charge les | Déma | Automatique |
| | | Station de travail | Crée et ma… | Déma | Automatique |
| | | Stratégie de retrait de la carte à puce | Autorise le | | Automatique |
| | | Système d'événement COM+ | Prend en c | Déma | Automatique |
| | | Système de couleurs Windows | Le service | | Manuel |
| | | Système de fichiers EFS (Encrypting | Fournit la t | | Manuel |
| | | 🤐 Téléphonie | Prend en c | | Manuel |
| | | 😪 Temps Windows | Conserve I | Déma | Automatique |
| | | 🤐 Thèmes | Fournit un | Déma | Automatique |
| | | 😘 TP AutoConnect Service | ThinPrint | Déma | Manuel |
| | | 😘 TP VC Gateway Service | ThinPrint c | | Manuel |
| | | 🤐 VMware Snapshot Provider | VMware Sn | | Manuel |
| | | 🔍 VMware Tools | Fournit un | Déma | Automatique |
| | | 🔍 WebClient | Permet à u | | Manuel |
| | | 🧠 Windows CardSpace | Active en t | | Manuel 📃 |
| | | 🤐 Windows Defender | Protection | Déma | Automatique (débu 🖵 |
| | | <u> ا</u> | | | Þ |
| | Étendu / Standard / | | | | |
| | | | | | |

Figure 161 : Configuration de la Stratégie de retrait de la carte à puce (automatique)

12.16 Détails des certificats ASIP Santé

| Abréviation | Local Machine | Rôle dans l'infrastructure | Fonction | Détails |
|-------------|---------------|----------------------------|---------------------------|---------------|
| LM Perso. | Local Machine | Domain Controller | Magasin de certificats | Personnel |
| LM Inter. | Local Machine | Domain Controller | Magasin de certificats | Intermédiaire |
| LM Root | Local Machine | Domain Controller | Magasin de certificats | Racine |
| NTAuth | Local Machine | Domain Controller | Active Directory | NTAuth |
| Strat. Ro. | Local Machine | Domain Controller | Stratégie de clé publique | Racine |
| Strat. Int. | Local Machine | Domain Controller | Stratégie de clé publique | Intermédiaire |

| Env. | Туре | DN | IssuerDN | Fichier (rép. cer\cer\) | Thumbprint (SHA-1) | SubjectKeyldentifie r | AuthorityKeyldent ifier | LM Perso. | LM inter. | LM root | NTAuth | Strat. Ro. | Start. Int. | Check |
|------|------|--|---|--|--|--|----------------------------|-----------|-----------|---------|--------|------------|-------------|-------|
| Prod | Root | O=GIP-CPS, C=FR | O=GIP-CPS, C=FR | 01-root- GIP-CPS.cer | 8E4471D30842B54B C7E2582770009469 ABD02CC7 | E7A8FD8D3D09169 6AEFC7563279023 795E5BD9B4 | | x | | х | x | х | | |
| Prod | Root | OU=ASIP-SANTE TECHNIQUE, O=ASIP-SANTE, C=FR | OU=ASIP- SANTE TECHNIQUE, O=ASIP- SANTE, C=FR | 02-root- ASIPSANTE TECHNIQU E.cer | 4AAA2092B960A4D9 A8E6E917A6791A14 A5E61F39 | 951EE95DC79A8E0 5E0AE7DE13D8F5D 804D4C7861 | | x | | x | x | x | | |
| Prod | Root | OU=GIP-CPS ANONYME, O=GIP-CPS, C=FR | OU=GIP-CPS ANONYME, O=GIP-CPS, C=FR | 03-root- GIP-CPS ANONYME. cer | 552C001B751B326A CCCDFE9A6F1148AD CC687816 | F1CFCF34D25A2F4 B2B77D4B01F082D BF03C1FF77 | | x | | x | x | x | | |

| Env. | Туре | DN | IssuerDN | Fichier (rép. cer\cer\) | Thumbprint (SHA-1) | SubjectKeyldentifie r | AuthorityKeyldent ifier | LM Perso. | LM inter. | LM root | NTAuth | Strat. Ro. | Start. Int. | Check |
|------|-------|--|--|---|--|--|--|-----------|-----------|---------|--------|------------|-------------|-------|
| Prod | Root | OU=GIP-CPS PROFESSIONNEL , O=GIP-CPS, C=FR | OU=GIP-CPS PROFESSION NEL, O=GIP- CPS, C=FR | 04-root- GIP-CPS PROFESION NEL.cer | 9956634AD724F00A 18C479E56463C6FB1 C7A073D | CA2386BD652FBF5 07EB5B63A5D0C33 56297597F3 | | x | | x | x | x | | |
| Prod | Root | OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR | OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR | 05-root- GIP-CPS STRUCTUR E.cer | 514F46F3E278FBF6D 8268286E19ADEE0C C443642 | E7D8047AC370F8D C02E4A00B2CB275 A59228FCBB | | x | | x | x | x | | |
| Prod | Inter | CN=GIP-CPS CLASSE-0, OU=GIP-CPS ANONYME, O=GIP-CPS, C=FR | OU=GIP-CPS ANONYME, O=GIP-CPS, C=FR | 06-inter- gip-cps- class0.cer | 148D663D3F75DED9 2B5CB2608EEA182C CFB1862E | AA6638EFC10C44E 1BA288B1AB0D4C2 72E7B49730 | F1CFCF34D25A2F 4B2B77D4B01F08 2DBF03C1FF77 | | x | | x | | x | |
| Prod | Inter | CN=GIP-CPS CLASSE-0, OU=GIP-CPS ANONYME, O=GIP-CPS, C=FR | OU=GIP-CPS ANONYME, O=GIP-CPS, C=FR | 07-inter- gip-cps- class0.cer | 052A8A966D4BF1E9 832D717D98AD35C1 4EC9119C | FC3D7599995F2A1 DDE244F7DF7AF30 FCDE3C8CE3 | F1CFCF34D25A2F 4B2B77D4B01F08 2DBF03C1FF77 | | x | | x | | x | |
| Prod | Inter | CN=GIP-CPS CLASSE-1, OU=GIP-CPS PROFESSIONNEL , O=GIP-CPS, C=FR | OU=GIP-CPS PROFESSION NEL, O=GIP- CPS, C=FR | 08-inter- gip-cps- class1.cer | 48630CFA410034E00 4A9BDB75D0CCB9DF 8EBA4AC | 3CBA21D0CD3D5E 3EE335080A193EC BA9CBB24EBC | CA2386BD652FBF 507EB5B63A5D0C 3356297597F3 | | x | | x | | x | |

| Env. | Туре | DN | IssuerDN | Fichier (rép. cer\cer\) | Thumbprint (SHA-1) | SubjectKeyldentifie r | AuthorityKeyldent ifier | LM Perso. | LM inter. | LM root | NTAuth | Strat. Ro. | Start. Int. | Check |
|------|-------|--|--|-------------------------------------|--|--|--|-----------|-----------|---------|--------|------------|-------------|-------|
| Prod | Inter | CN=GIP-CPS CLASSE-1, OU=GIP-CPS PROFESSIONNEL , O=GIP-CPS, C=FR | OU=GIP-CPS PROFESSION NEL, O=GIP- CPS, C=FR | 09-inter- gip-cps- class1.cer | 46934C7CDAD63C04 B3FE76F5FFBF7512E 55B8F7E | 726C14AEAD8384A D2B174AC0239593 31DF256735 | CA2386BD652FBF 507EB5B63A5D0C 3356297597F3 | | x | | x | | x | |
| Prod | Inter | CN=GIP-CPS CLASSE-2, OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR | OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR | 10-inter- gip-cps- class2.cer | 8A94BBBB12BD5567 318FCF191B349B8FF D8A992D | F34F6B7F90A2A51 F1F46A687AD8615 B1010A62D6 | E7D8047AC370F8 DC02E4A00B2CB2 75A59228FCBB | | x | | x | | x | |
| Prod | Inter | CN=GIP-CPS CLASSE-2, OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR | OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR | 11-inter- gip-cps- class2.cer | 3E85E5F32C4C2E6F2 D82884228C515AE7 3A5C8D7 | 935920931D30024 DD1BB2D2DD105B F1373A94D00 | E7D8047AC370F8 DC02E4A00B2CB2 75A59228FCBB | | x | | x | | x | |
| Prod | Inter | CN=GIP-CPS CLASSE-3, OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR | OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR | 12-inter- gip-cps- class3.cer | BA33690A8AC857D5 E5514AC5FD817EE8 CA1F7819 | 49025F3483F2E965 5353FFCFBD8E638 615008AA0 | E7D8047AC370F8 DC02E4A00B2CB2 75A59228FCBB | | x | | x | | x | |

| Env. | Туре | DN | IssuerDN | Fichier (rép. cer\cer\) | Thumbprint (SHA-1) | SubjectKeyldentifie r | AuthorityKeyldent ifier | LM Perso. | LM inter. | LM root | NTAuth | Strat. Ro. | Start. Int. | Check |
|------|-------|---|--|---|--|--|--|-----------|-----------|---------|--------|------------|-------------|-------|
| Prod | Inter | CN=GIP-CPS CLASSE-3, OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR | OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR | 13-inter- gip-cps- class3.cer | 9F92B6CBF7FC61EBE A76F63ADD8D54C1A C2DDFB8 | 16E5E9F2E7246988 DA3B7F2AF6690FC 49BEFBE85 | E7D8047AC370F8 DC02E4A00B2CB2 75A59228FCBB | | x | | x | | x | |
| Prod | Inter | O=GIP-CPS, C=FR | O=GIP-CPS, C=FR | 14-inter- gip-cps.cer | 4AC2FC4B4AD07766 9A9A6C4ACF8FA718 10717407 | ED5A0A4E712B0E5 C4FA1E48B916254 9675C73B18 | E7A8FD8D3D0916 96AEFC75632790 23795E5BD9B4 | | x | | x | | x | |
| Prod | Inter | OU=AC-CLASSE- 4, O=GIP-CPS, C=FR | O=GIP-CPS, C=FR | 15-inter-ac- class4.cer | 3182462F180AE880B 6F43FA040CEC025D C2F2042 | 25AF15AFC24AAE4 8D1CF241B14B8FC 7D0F041FEB | E7A8FD8D3D0916 96AEFC75632790 23795E5BD9B4 | | x | | x | | x | |
| Prod | Inter | OU=AC-CLASSE- 5, O=GIP-CPS, C=FR | O=GIP-CPS, C=FR | 16-inter-ac- class5.cer | 5F3C2C90B974FE9FA 8F9D2BDE11338C4D 2681E37 | A2CB0165BA5C408 5F3FB071C3014C8 5EEF3C2A26 | E7A8FD8D3D0916 96AEFC75632790 23795E5BD9B4 | | x | | x | | x | |
| Prod | Inter | OU=AC-CLASSE- 6, O=GIP-CPS, C=FR | O=GIP-CPS, C=FR | 17-inter-ac- class6.cer | 08C053B382E9D794 FD7A9C44679B95E5 C6B21B84 | 9691F5B5F398DF1 4B370E777A31B2F 7E26B6FFB9 | E7A8FD8D3D0916 96AEFC75632790 23795E5BD9B4 | | x | | x | | x | |
| Prod | Inter | OU=GIP-CPS ANONYME, O=GIP-CPS, C=FR | OU=GIP-CPS ANONYME, O=GIP-CPS, C=FR | 18-inter- gip-cps- anonyme.c er | BED257C7AC336AA2 AC6DDE832B2EA3D2 E10FD6EB | 19ADD26C1AC9C7F C1AD8C4308563E5 7702F0D7E2 | F1CFCF34D25A2F 4B2B77D4B01F08 2DBF03C1FF77 | | x | | x | | x | |
| Prod | Inter | OU=GIP-CPS PROFESSIONNEL , O=GIP-CPS, C=FR | OU=GIP-CPS PROFESSION NEL, O=GIP- CPS, C=FR | 19-inter- gip-cps- professione l.cer | 307E5E5CB30966F05 DF1670927A6154E9 1719EF3 | C3692C6AC8592E8 638779AEB1F055B E2F112EA92 | CA2386BD652FBF 507EB5B63A5D0C 3356297597F3 | | x | | х | | x | |

| Env. | Туре | DN | IssuerDN | Fichier (rép. cer\cer\) | Thumbprint (SHA-1) | SubjectKeyldentifie r | AuthorityKeyldent ifier | LM Perso. | LM inter. | LM root | NTAuth | Strat. Ro. | Start. Int. | Check |
|------|-------|---|--|--|--|--|--|-----------|-----------|---------|--------|------------|-------------|-------|
| Prod | Inter | OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR | OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR | 20-inter- gip-cps- structure.c er | D031C6132A5345BC BC52C499B89B87E4 0A077BFE | ACE6F2C855B2CE3 50304710C119F50 70545D4F06 | E7D8047AC370F8 DC02E4A00B2CB2 75A59228FCBB | | x | | x | | x | |
| Test | Root | O=GIP-CPS- TEST, C=FR | O=GIP-CPS- TEST, C=FR | 21-root- GIP-CPS TEST.cer | 717E472799B45FF75 5A97A0F2F2B30245 C7FE379 | AF3B167480F5D95 47A21C738E625FA 24FE34D504 | | х | | x | x | x | | |
| Test | Root | OU=TEST ANONYME, O=TEST, C=FR | OU=TEST ANONYME, O=TEST, C=FR | 22-root- TEST ANONYME. cer | B8B9576489E0D294 145C2016F61469E71 CBF323F | 97BF4F0C6226425 292B9FA26738570 14B55B243D | | x | | x | x | x | | |
| Test | Root | OU=TEST PROFESSIONNEL , O=TEST, C=FR | OU=TEST PROFESSION NEL, O=TEST, C=FR | 23-root- TEST PROFESSIO NEL.cer | 71E9AC03FCE331770 7C7F5D5D429EA209 ECA2305 | 75C14776C4AD282 F67AA568B032200 0C7AC38584 | | x | | x | x | x | | |
| Test | Root | OU=TEST STRUCTURE, O=TEST, C=FR | OU=TEST STRUCTURE, O=TEST, C=FR | 24-root- TEST STRUCTUR E.cer | 90DA3E6D021FA378 D55CEEEA3CE7B82C A7C8756B | 54B7A98F06847DB 7B79C35FB8FAE69 5D73D59375 | | x | | x | x | x | | |
| Test | Root | OU=TEST TECHNIQUE, O=TEST, C=FR | OU=TEST TECHNIQUE, O=TEST, C=FR | 25-root- TEST TECHNIQU E.cer | 42111D850BB4E3B4 D30A920ACCB6D64B D9CA3F98 | 26ECC1EBBD3B9CC EAFF32FED04200D 698593223D | | x | | x | x | x | | |
| Test | Inter | CN=TEST CLASSE-0, OU=TEST ANONYME, O=TEST, C=FR | OU=TEST ANONYME, O=TEST, C=FR | 26-inter- test- class0.cer | D367C327413DAEA6 82681C388C1C8DE3 560BD841 | 4DB168E2C11E74F 9FE368173340687E 6D940F5B0 | 97BF4F0C6226425 292B9FA2673857 014B55B243D | | x | | x | | x | |

| Env. | Туре | DN | IssuerDN | Fichier (rép. cer\cer\) | Thumbprint (SHA-1) | SubjectKeyldentifie r | AuthorityKeyldent ifier | LM Perso. | LM inter. | LM root | NTAuth | Strat. Ro. | Start. Int. | Check |
|------|-------|--|---|----------------------------------|--|--|--|-----------|-----------|---------|--------|------------|-------------|-------|
| Test | Inter | CN=TEST CLASSE-0, OU=TEST ANONYME, O=TEST, C=FR | OU=TEST ANONYME, O=TEST, C=FR | 27-inter- test- class0.cer | 4443FC0599A80C3A 61C416A9CD174BB9 D42C61BF | 898C2D753B73969 C3BA1B1599868ED C1999E92EE | 97BF4F0C6226425 292B9FA2673857 014B55B243D | | x | | x | | x | |
| Test | Inter | CN=TEST CLASSE-1, OU=TEST PROFESSIONNEL , O=TEST, C=FR | OU=TEST PROFESSION NEL, O=TEST, C=FR | 28-inter- test- class1.cer | 933D2D2BD62FFFD0 CCE7FA092C0D34C3 B64E69E7 | 0A26371072F587F CA7A0C4713D77F0 BB235FEE4A | 75C14776C4AD28 2F67AA568B0322 000C7AC38584 | | x | | x | | x | |
| Test | Inter | CN=TEST CLASSE-1, OU=TEST PROFESSIONNEL , O=TEST, C=FR | OU=TEST PROFESSION NEL, O=TEST, C=FR | 29-inter- test- class1.cer | 2438CFC8F2756CBB2 6850273F7A0E47C57 B2233E | 76103543B48B7F8 C6E00B792A69082 B3C14BD2EA | 75C14776C4AD28 2F67AA568B0322 000C7AC38584 | | x | | x | | × | |
| Test | Inter | CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR | OU=TEST STRUCTURE, O=TEST, C=FR | 30-inter- test- class2.cer | B027E02F33F0DC128 47CDE8B0BC0AC5B7 67E0473 | DB39068C884F434 D60505B3996737C D3A2DE5694 | 54B7A98F06847D B7B79C35FB8FAE 695D73D59375 | | x | | x | | x | |
| Test | Inter | CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR | OU=TEST STRUCTURE, O=TEST, C=FR | 31-inter- test- class2.cer | 54DFEE1AC4CD8D5A CF32F7AE121EF26A3 38FF13D | 44721289C272779 BDB0A3B8F4A32AE 4E2CAF5876 | 54B7A98F06847D B7B79C35FB8FAE 695D73D59375 | | x | | x | | x | |

| Env. | Туре | DN | IssuerDN | Fichier (rép. cer\cer\) | Thumbprint (SHA-1) | SubjectKeyldentifie r | AuthorityKeyldent ifier | LM Perso. | LM inter. | LM root | NTAuth | Strat. Ro. | Start. Int. | Check |
|------|-------|---|--|---------------------------------------|--|--|--|-----------|-----------|---------|--------|------------|-------------|-------|
| Test | Inter | CN=TEST CLASSE-3, OU=TEST STRUCTURE, O=TEST, C=FR | OU=TEST STRUCTURE, O=TEST, C=FR | 32-inter- test- class3.cer | 874F4F184DA9F896F ADE58AADE1185467 E63834A | 6E721567491689E 5F0DDD211D4701F EC6B55DB6A | 54B7A98F06847D B7B79C35FB8FAE 695D73D59375 | | x | | x | | x | |
| Test | Inter | CN=TEST CLASSE-3, OU=TEST STRUCTURE, O=TEST, C=FR | OU=TEST STRUCTURE, O=TEST, C=FR | 33-inter- test- class3.cer | 2BEB8461F6F2FEC5E E95872FCC52B9E736 125CB1 | 06EEE31E10446ED 72CD4A312D4427F 289A5B94EF | 54B7A98F06847D B7B79C35FB8FAE 695D73D59375 | | x | | x | | x | |
| Test | Inter | O=GIP-CPS- TEST, C=FR | O=GIP-CPS- TEST, C=FR | 34-inter- gip-cps- test.cer | 5ED0889BCEAE671A 4A368AB405E2B254 31AC20D2 | E1FA17F81423C5D E9F7B4956A2E542 986CE44A2F | AF3B167480F5D9 547A21C738E625 FA24FE34D504 | | x | | x | | x | |
| Test | Inter | OU=AC-CLASSE- 4-TEST, O=GIP- CPS-TEST, C=FR | O=GIP-CPS- TEST, C=FR | 35-inter-ac- class4- test.cer | 01ED444C889EF19F3 75EEB6D87137A84C F83BEB9 | C256EFEF20F25917 BC406C59B3CCF89 B93BB681A | AF3B167480F5D9 547A21C738E625 FA24FE34D504 | | x | | x | | х | |
| Test | Inter | OU=AC-CLASSE- 5-TEST, O=GIP- CPS-TEST, C=FR | O=GIP-CPS- TEST, C=FR | 36-inter-ac- class5- test.cer | D202CB693A9668A5 0E28C967947AE7B8 4FE1C3EB | 90DA136A53A6487 AD32680936E708B 93D2DEEC94 | AF3B167480F5D9 547A21C738E625 FA24FE34D504 | | x | | x | | х | |
| Test | Inter | OU=AC-CLASSE- 6-TEST, O=GIP- CPS, C=FR | O=GIP-CPS- TEST, C=FR | 37-inter-ac- class6- test.cer | 1235CB411691D502 93DCA42AFA7297B9 34E10EB6 | 9805991A5C4935A ABF7733FEEAB542 C9B7A9D647 | AF3B167480F5D9 547A21C738E625 FA24FE34D504 | | x | | x | | x | |
| Test | Inter | OU=TEST ANONYME, O=TEST, C=FR | OU=TEST ANONYME, O=TEST, C=FR | 38-inter- test- anonyme.c er | EA2953E1AFCD8D71 74508D211DD784AC B3F8CCDE | 5B0EC162BE14E88 F8727F96BBD84AC 08F5FC7952 | 97BF4F0C6226425 292B9FA2673857 014B55B243D | | x | | x | | x | |

| Env. | Туре | DN | IssuerDN | Fichier (rép. cer\cer\) | Thumbprint (SHA-1) | SubjectKeyldentifie r | AuthorityKeyldent ifier | LM Perso. | LM inter. | LM root | NTAuth | Strat. Ro. | Start. Int. | Check |
|------|----------------------|--|---|--|--|--|--|-----------|-----------|---------|--------|------------|-------------|-------|
| Test | Inter | OU=TEST PROFESSIONNEL , O=TEST, C=FR | OU=TEST PROFESSION NEL, O=TEST, C=FR | 39-inter- test- professionn el.cer | D7E070C9C5D64595 8317E023C855DC48 FDB49F0C | 254BDD0F8A5D08B 05BBA312076A002 55C08A0183 | 75C14776C4AD28 2F67AA568B0322 000C7AC38584 | | x | | x | | x | |
| Test | Inter | OU=TEST STRUCTURE, O=TEST, C=FR | OU=TEST STRUCTURE, O=TEST, C=FR | 40-inter- test- structure.c er | BD5976486680623C 98B15F64C2884E265 4E54446 | 9DAA04AFF9307FE 3719DE1FFA62F0C 8A242C05B8 | 54B7A98F06847D B7B79C35FB8FAE 695D73D59375 | | x | | x | | x | |
| Prod | PKI Micr osoft | | | %USERPRO FILE%\Desk top\ ad-cs- rootca.cer | | | | x | x | x | x | x | | |
| Prod | PKI Micr osoft | | | %USERPRO FILE%\Desk top\ ad-dc- rootca.cer | | | | x | | | | | | |
| Prod | PKI Micr osoft | | | %USERPRO FILE%\Desk top\ rd- rootca.cer | | | | x | | | | | | |

| Env. | Туре | DN | lssuerDN | Fichier (rép. cer\cer\) | Thumbprint (SHA-1) | SubjectKeyldentifie r | AuthorityKeyldent ifier | LM Perso. | LM inter. | LM root | NTAuth | Strat. Ro. | Start. Int. | Check |
|-----------|------|---|--|-------------------------------|--|--|--|-----------|-----------|---------|--------|------------|-------------|-------|
| PFC NG | Root | CN=AC RACINE IGC-SANTE FORT, OU=IGC- SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR | CN=AC RACINE IGC- SANTE FORT, OU=IGC- SANTE, OU=0002 187512751, O=ASIP- SANTE, C=FR | | BBE751C8B107ACD2 9F7D12E0FCDD717E 00138764 | 38430511002EE75 2C3E8974674F8A4 FB9CDCE5EE | 38430511002EE75 2C3E8974674F8A 4FB9CDCE5EE | x | | x | x | x | | |
| PFC NG | Root | CN=AC RACINE IGC-SANTE STANDARD, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR | CN=AC RACINE IGC- SANTE STANDARD, OU=IGC- SANTE, OU=0002 187512751, O=ASIP- SANTE, C=FR | | B6BA1D6D5224BCED A95A67F6F37B8689 6EDD0006 | C0AC89F12470D52 BE2D5D4B48405C0 810572539B | C0AC89F12470D5 2BE2D5D4B48405 C0810572539B | x | | x | x | x | | |

ASIP Santé

24/09/2014

| Env. | Туре | DN | lssuerDN | Fichier (rép. cer\cer\) | Thumbprint (SHA-1) | SubjectKeyldentifie r | AuthorityKeyldent ifier | LM Perso. | LM inter. | LM root | NTAuth | Strat. Ro. | Start. Int. | Check |
|-----------|-------|--|--|-------------------------------|--|--|--|-----------|-----------|---------|--------|------------|-------------|-------|
| PFC NG | Root | CN=AC RACINE IGC-SANTE ELEMENTAIRE, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR | CN=AC RACINE IGC- SANTE ELEMENTAIR E, OU=IGC- SANTE, OU=0002 187512751, O=ASIP- SANTE, C=FR | | 4B23D44DC5CBDA23 0FC052DFF52407ED AF373C69 | 8C6FEAD58B82FAF 9BE87DC730E2715 0747C49E2F | 8C6FEAD58B82FA F9BE87DC730E27 150747C49E2F | x | | x | x | x | | |
| PFC NG | Inter | CN=AC IGC- SANTE FORT ORGANISATION S, OU=IGC- SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR | CN=AC RACINE IGC- SANTE FORT, OU=IGC- SANTE, OU=0002 187512751, O=ASIP- SANTE, C=FR | | 7C3AF35B76FE34699 FBC72C6A340BC7F1 AC4D854 | EDE618D2E0FE734 5CBF8242F566BA6 06E20F7331 | 38430511002EE75 2C3E8974674F8A 4FB9CDCE5EE | | x | | x | | х | |

| Env. | Туре | DN | lssuerDN | Fichier (rép. cer\cer\) | Thumbprint (SHA-1) | SubjectKeyldentifie r | AuthorityKeyldent ifier | LM Perso. | LM inter. | LM root | NTAuth | Strat. Ro. | Start. Int. | Check |
|-----------|-------|---|--|-------------------------------|--|--|--|-----------|-----------|---------|--------|------------|-------------|-------|
| PFC NG | Inter | CN=AC IGC- SANTE FORT PERSONNES, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR | CN=AC RACINE IGC- SANTE FORT, OU=IGC- SANTE, OU=0002 187512751, O=ASIP- SANTE, C=FR | | AA6131E760B95622 C0F4C2AA9D985002 C21F3A0C | 800F918821797D5 555C65D6DD5938 D6ADE5C2AA6 | 38430511002EE75 2C3E8974674F8A 4FB9CDCE5EE | | x | | x | | x | |
| PFC NG | Inter | CN=AC IGC- SANTE STANDARD ORGANISATION S, OU=IGC- SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR | CN=AC RACINE IGC- SANTE STANDARD, OU=IGC- SANTE, OU=0002 187512751, O=ASIP- SANTE, C=FR | | EA8752036E115EE8A A1653672289074A2 4B23994 | 66B62D3DB8FC1E1 A13496882845873 24C4ACE5A0 | C0AC89F12470D5 2BE2D5D4B48405 C0810572539B | | x | | x | | x | |

| Env. | Туре | DN | IssuerDN | Fichier (rép. cer\cer\) | Thumbprint (SHA-1) | SubjectKeyldentifie r | AuthorityKeyldent ifier | LM Perso. | LM inter. | LM root | NTAuth | Strat. Ro. | Start. Int. | Check |
|-----------|-------|--|--|-------------------------------|--|--|--|-----------|-----------|---------|--------|------------|-------------|-------|
| PFC NG | Inter | CN=AC IGC- SANTE STANDARD PERSONNES, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR | CN=AC RACINE IGC- SANTE STANDARD, OU=IGC- SANTE, OU=0002 187512751, O=ASIP- SANTE, C=FR | | E0D6E1D8481FED62 C65C53ED9DFCDA94 9C3D1D81 | 19F276D58D7A17C A829BE97B5AEF3F 05A690D4F3 | C0AC89F12470D5 2BE2D5D4B48405 C0810572539B | | x | | x | | x | |
| PFC NG | Inter | CN=AC IGC- SANTE ELEMENTAIRE ORGANISATION S, OU=IGC- SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR | CN=AC RACINE IGC- SANTE ELEMENTAIR E, OU=IGC- SANTE, OU=0002 187512751, O=ASIP- SANTE, C=FR | | 2CBFA991750AF778 348B3156C21609A1 AB45A848 | D7FBFADCD5027FE 7C153864D4BE8A4 4A1E0BBB63 | 8C6FEAD58B82FA F9BE87DC730E27 150747C49E2F | | x | | x | | x | |

| Env. | Туре | DN | IssuerDN | Fichier (rép. cer\cer\) | Thumbprint (SHA-1) | SubjectKeyldentifie r | AuthorityKeyldent ifier | LM Perso. | LM inter. | LM root | NTAuth | Strat. Ro. | Start. Int. | Check |
|-----------|-------|---|--|-------------------------------|--|--|--|-----------|-----------|---------|--------|------------|-------------|-------|
| PFC NG | Inter | CN=AC IGC- SANTE ELEMENTAIRE PERSONNES, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR | CN=AC RACINE IGC- SANTE ELEMENTAIR E, OU=IGC- SANTE, OU=0002 187512751, O=ASIP- SANTE, C=FR | | 86A0DE3D866E2DB5 095F6785A57FD5CC 53B2F049 | CEAF9B1C194A6B5 3A7A8C9D81FDB61 14CD07F22E | 8C6FEAD58B82FA F9BE87DC730E27 150747C49E2F | | x | | x | | x | |

Tableau 36 : Liste de certificats



12.17 Debugging

12.17.1 Traces Cryptolib CPS

| Gestion des traces Cryptolib CPS | | | | | | | | |
|---|---|--|--|--|--|--|--|--|
| Activation en fusionnant le fichier | %ProgramFiles%\santesocial\CPS\activation_traces.reg | | | | | | | |
| Traces générées dans le répertoire | %ALLUSERSPROFILE%\santesocial\CPS\log\ | | | | | | | |
| Désactivation en fusionnant le fichier | %ProgramFiles%\santesocial\CPS\desactivation_traces.reg | | | | | | | |

Tableau 37 : Activation des traces Kerberos via la base de registre

12.17.2 Traces Kerberos

2 méthodes sont disponibles :

12.17.2.1 Via la base de registre

12.17.2.1.1Activation

Les traces Kerberos s'activent en fusionnant les paramètres suivants en base de registre:

| Activation d | es traces Kerberos via la base de registre |
|---|--|
| En modifiant les clés suivantes : | [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0] "NtLmInfoLevel"=dword:c0015003 [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos] "LogToFile"=dword:0000001 [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters] "LogToFile"=dword:0000001 [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters] "KerbDebugLevel"=dword:c000043 [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Kdc] "KdcDebugLevel"=dword:c0000803 |
| En fusionnant le fichier suivant : | log\kerberos-reg\debug-smartcard-logon-kerberos-activate.reg |

Tableau 38 : Activation des traces Kerberos via la base de registre

12.17.2.1.2Génération

| Emplacement des traces Kerberos via la base de registre | | | | | | |
|---|--|--|--|--|--|--|
| Répertoires suivants: | %systemroot%\system32\lsass.log %systemroot%\tracing\msv1_0 %systemroot%\tracing\kerberos %systemroot%\tracing\kdcsvc | | | | | |

Tableau 39 : Emplacement des traces Kerberos après activation via la base de registre

12.17.2.1.3 Désactivation

Les traces Kerberos se désactivent en fusionnant les paramètres suivants en base de registre:

| Désactivation des traces Kerberos via la base de registre | | | | | | | | |
|---|---|--|--|--|--|--|--|--|
| En modifiant les clés suivantes : | <pre>[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0] "NtLmInfoLevel"=- [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos] "LogLevel"=- [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos] "LogToFile"=- [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters] "KerbDebugLevel"=- [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters] "LogLevel"=- [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters] "LogToFile"=- [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters] "LogToFile"=- [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters] "KerbDebugLevel"=-</pre> | | | | | | | |
| En fusionnant le fichier suivant : | log\kerberos-reg\debug-smartcard-logon-kerberos-deactivate.reg | | | | | | | |

Tableau 40 : Désactivation des traces Kerberos activées via la base de registre

12.17.2.2 Via Tracelog

Tracelog.exe est un outil Microsoft fourni avec Visual Studio ou avec le WDK (fourni dans le répertoire **bin** du Kit ASIP Santé Smartcard logon).

12.17.2.2.1 Activation

| Activation des traces Kerberos via Tracelog | | | | | |
|---|---|--|--|--|--|
| En utilisant les appels: | tracelog.exe -kd -rt -start ntlm -guid #5BBB6C18-AA45-49b1-A15F- 085F7ED0AA90 -f .\ntlm.etl -flags 0x15003 -ft 1 tracelog.exe -kd -rt -start kerb -guid #6B510852-3583-4e2d-AFFE-A67F9F223438 -f .\kerb.etl -flags 0x43 -ft 1 tracelog.exe -kd -rt -start kdc -guid #1BBA8B19-7F31-43c0-9643-6E911F79A06B - f .\kdc.etl -flags 0x803 -ft 1 | | | | |
| En fusionnant le fichier de commande: | log\kerberos-tracelog\02-asipsante-smartcard-logon-kerberos-tracelog.cmd start | | | | |

Tableau 41 : Activation des traces Kerberos via Tracelog

12.17.2.2.2Génération

| Emplacement des traces Kerberos via Tracelog | | | | | | | |
|--|---------------------------------------|--|--|--|--|--|--|
| Fichiers suivants: | .\ntlm.etl .\kerb.etl .\kdc.etl | | | | | | |

Tableau 42 : Emplacement des traces Kerberos après activation via Tracelog

12.17.2.2.3 Désactivation

| Activation des traces Kerberos via Tracelog | | | | | | |
|---|--|--|--|--|--|--|
| En utilisant les appels: | tracelog.exe -stop ntlm tracelog.exe -stop kerb tracelog.exe -stop kdc | | | | | |
| En fusionnant le fichier de commande: | log\kerberos-tracelog\02-asipsante-smartcard-logon-kerberos-tracelog.cmd stop | | | | | |

Tableau 43 : Désactivation des traces Kerberos activées via Tracelog

Attention :

- supprimer ou protéger les fichiers d'activation/désactivation de traces des machines de productions
- désactiver les traces avant de (re)passer en production (pénalisant pour les performances)

12.18 Points d'attention et contournements

12.18.1 Limitations

En date de juillet 2013 :

asipsar

[]]Dessut[]

AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

| ID | Ticket(s) | OS | Archi | Limitation | Alternative | Statut Problème | Statut Alternative |
|---------|-----------|----|-------|--|---|--------------------|-----------------------|
| AT_0010 | | | | Env. TSE : Les clients RDP installés avec les Cryptolib CPS « GALSS » 5.0.4 ou 5.0.6 ne fonctionnent pas en Smartcard Logon. | Installer les Cryptolib CPS v5.0.8 sur le poste client (cf. Annexe 6, installation du poste client), <u>x64 sur</u> <u>les OS x64</u> , x32 sur les OS x32 | Confirmé | Confirmé |
| AT_0020 | 0001075 | | | Env. TSE : Les serveurs RDP installés avec Cryptolib CPS v5.0.6 ne permettent pas de rouvrir une session après qu'une première session ait été ouverte préalablement. | Installer les Cryptolib CPS v5.0.8 côté serveur. | Confirmé | Confirmé |

| ID | Ticket(s) | OS | Archi | Limitation | Alternative | Statut Problème | Statut Alternative |
|---------|--------------------|----|-------|--|--|--------------------|-----------------------|
| AT_0030 | 0001074 | | | Env. TSE : Sur une session verrouillée, l'introduction d'un mauvais code porteur déverrouille la session. | Installer les Cryptolib CPS v5.0.8 côté client et serveur. | Confirmé | Confirmé |
| AT_0040 | 0001071 0001073 | | | Env. TSE : Lors d'une ouverture de session, le login reste bloqué sur « lecture de la carte à puce » si on retire la carte juste après son insertion. | Vérifier le comportement lorsque la GPO de propagation du certificat est désactivée. | Non reproduit | |

| ID | Ticket(s) | OS | Archi | Limitation | Alternative | Statut Problème | Statut Alternative |
|---------|--------------------|----|-------|--|---|--------------------|-----------------------|
| AT_0050 | 0001071 0001073 | | | Env. TSE : Le service de propagation de certificat se bloque sur on retire la carte lors d'une lecture avec les Cryptolib CPS. | Vérifier le comportement lorsque la GPO de propagation du certificat est désactivée : le CCM assure la propagation des certificats. Contrairement au Service de propagation MS, il assure le retrait des certificats du magasin lors du retrait carte. | Non reproduit | |
| AT_0060 | 0001071 0001073 | | | Env. TSE : L'ouverture de session reste bloquée sur « Bienvenue » lors d'authentification simultanées. | | Non reproduit | |

| ID | Ticket(s) | OS | Archi | Limitation | Alternative | Statut Problème | Statut Alternative |
|---------|-----------|----|-------|--|--|--------------------|-----------------------|
| AT_0070 | 0001075 | | | Env. TSE : L'ouverture de session signale des erreurs. | Installer les Cryptolib CPS v5.0.8 sur le poste client (cf. Annexe 6, installation du poste client). | Confirmé | Confirmé |

| ID | Ticket(s) | OS | Archi | Limitation | Alternative | Statut Problème | Statut Alternative |
|---------|-----------|----|-------|---|-------------|--|-----------------------|
| | | | | | | Non reproduit | |
| AT_0080 | | | | Env. TSE : Il n'est pas possible d'ouvrir une session lorsque l'option SSL du service NLA (Network Level Authentication) SSL est activée. | | 20130731 : Cette fonctionnalit é est nouvelle dans W2008R2 (noyaux Vista+ et RDP | |
| | | | | Cf. 6.5 « Installation d'un rôle Terminal Server » | | 6.0), n'a pas encore été testée et n'est pas encore supportée. | |

| ID | Ticket(s) | OS | Archi | Limitation | Alternative | Statut Problème | Statut Alternative |
|---------|-----------|----|-------|--|---|--------------------|-----------------------|
| AT_0090 | 0001075 | | | Env. TSE : Une fenêtre d'erreur Microsoft Visual C++ apparait aléatoirement | Installer les Cryptolib CPS v5.0.8 côté client et serveur. | Confirmé | Confirmé |

| ID | Ticket(s) | OS | Archi | Limitation | Alternative | Statut Problème | Statut Alternative |
|---------|-----------|----|-------|--|---|--------------------|-----------------------|
| AT_0100 | 0001047 | | | Env. Citrix : http://support.citrix.com/article/CTX136248 http://support.citrix.com/article/CTX136922 cf. [4] ASIP-PTS-PSCE_Manuel-Installation- utilisation-Cryptolib- CPS_20140224_v5.0.2.pdf | | Clos | |
| AT_0110 | | | | Env. TSE :Les utilisateurs ne peuvent pas utiliser une carte à puce pour se connecter à une session de Services Terminal Server sur un ordinateur qui exécute Windows Server 2008 | Installer W2008R2 SP1 ou le KB958596 http://support.microsoft.com/kb/95 8596/en | Clos | |
| AT_0120 | | | | Available Updates for Remote Desktop Services (Terminal Services) on Windows Server 2008 R2 SP1 | http://support.microsoft.com/?id=2 601888 http://support.microsoft.com/kb/25 21923 | Clos | |
| AT_0130 | 0001097 | | | La sélection automatique des certificats carte en Smartcard logon ne marche pas lorsque 2 cartes sont présentes sur le poste client. Il n'est pas possible d'ouvrir 2 sessions TSE automatiquement en parallèle avec 2 cartes depuis un même poste client. Les 2 sessions s'ouvrent sir la sélection est explicitée par l'utilisateur. | http://blogs.technet.com/b/instan/a rchive/2011/01/27/automatic-logon- to-rds-using-smartcards-with- multiple-certificates-with-or- without-ts-gateway.aspx | Clos | Clos |

Tableau 44 : Points d'attention

12.18.2 Contournements

12.18.2.1AT_0030 - Désactivation du verrouillage de session

Le minimum consiste à positionner cette valeur en base de registre:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

"DisableLockWorkstation"=dword:0000001



Figure 162 : Workaround : Désactivation verrouillage de session

Il est possible d'affiner le paramétrage de sorte qu'aucune manière de locker la session ne soit accessible ou que plus généralement le cycle de vie de la session utilisateur soit parfaitement maitrisé par l'administrateur système (ce qui est d'ailleurs important dans le cas du Smartcard logon): Cf. http://msdn.microsoft.com/en-us/library/ms815238.aspx

Cf. http://technet.microsoft.com/fr-fr/library/ee617162%28v=ws.10%29.aspx



Figure 163 : Workaround : Désactivation verrouillage de session sur Ctrl+Alt+Suppr



Figure 164 : Workaround : Désactivation changement d'utilisateur

Ne pas oublier la commande « gpupdate » pour propager les nouvelles policies.

13Contenu du « Kit Smartcard logon ASIP Santé »

| ID | Répertoire | Description Répertoire | Fichier | Description Fichier |
|---------------|---------------|---|--|---|
| Pack_SCL_0001 | bin | Fichiers binaires ou exécutables | 00-asipsante-smartcard-logon-ntauth-manage.cmd | Script de peuplement du magasin NTAuth |
| Pack_SCL_0002 | bin | | 01-asipsante-smartcard-logon-console.msc | Console MMC centralisant les principaux snap-in nécessaires à la configuration des serveurs MS requis pour le Smartcard logon |
| Pack_SCL_0003 | bin | | tracelog.exe | Outils de prise de traces MS |
| Pack_SCL_0004 | bin\msi-5.x.y | Installation Cryptolib CPS | Cryptolib-CPS.txt | Lien vers les installeurs MSI de la Cryptolib CPS v5 32b et 64b |
| Pack_SCL_0005 | cer\cer | 40 certificats ASIP Santé au format .cer | хх-уу.cer | 40 certificats ASIP Santé au format .cer pour peuplement des magasins de certificats |
| Pack_SCL_0006 | cer\p7b | certificats ASIP Santé au format P7B | 01-prod-root.p7b | Certificats root de production |
| Pack_SCL_0007 | cer\p7b | | 02-prod-inter.p7b | Certificats inter. de production |
| Pack_SCL_0008 | cer\p7b | | 03-test-root.p7b | Certificats root de test |
| Pack_SCL_0009 | cer\p7b | | 04-test-inter.p7b | Certificats inter. de test |

| ID | Répertoire | Description Répertoire | Fichier | Description Fichier |
|---------------|---------------|---|---|--|
| Pack_SCL_0010 | cer\p7b | | 05-all-root.p7b | Certificats root de test et de production |
| Pack_SCL_0011 | cer\p7b | | 06-all-inter.p7b | Certificats inter. de test et de production |
| Pack_SCL_0012 | cer\pem | 40 certificats ASIP Santé au format .pem | xx-yy.pem | Fournis par commodité. Peuvent servir aux configurations de profiles Firefox par exemple. |
| Pack_SCL_0013 | cfg | Fichiers de configuration | cps_pkcs11_pcsc.ini | Exemple de fichier de config Cryptolib |
| Pack_SCL_0014 | doc | Documentation et ReleaseNotes | ASIP-PTS-PSCE_Guide-de-mise-en-oeuvre-d-un- smartcard-logon-avec-une-carte- CPS_yyyyMMdd_vX.Y.Z.pdf | Le présent document |
| Pack_SCL_0015 | doc | | Guide_de_deploiement_de_louverture_de_session _par_carte_CPSv3_v1.0.pdf | Guide écrit et diffusé par MS |
| Pack_SCL_0016 | leg | Mentions légales | COPYRIGHT.txt | |
| Pack_SCL_0017 | leg | | DISCLAIMER.txt | |
| Pack_SCL_0018 | leg | | LICENSE.txt | |
| Pack_SCL_0019 | leg | | README.txt | |
| Pack_SCL_0020 | log\cryptolib | Pack de prise de traces | debug-cryptolib-activate.reg | Activation des traces de la Cryptolib CPS |

| ID | Répertoire | Description Répertoire | Fichier | Description Fichier |
|---------------|-----------------------|------------------------|--|---|
| | | | debug-cryptolib-deactivate.reg | Désactivation des traces de la Cryptolib CPS |
| Pack_SCL_0021 | log\kerberos-reg | | debug-smartcard-logon-kerberos-activate.reg | Activation des traces Kerberos |
| Pack_SCL_0022 | log\kerberos-reg | | debug-smartcard-logon-kerberos-deactivate.reg | Désactivation des traces Kerberos via la BdR |
| Pack_SCL_0023 | log\kerberos-tracelog | | 02-asipsante-smartcard-logon-kerberos- tracelog.cmd | Activation / désactivation des traces Kerberos via tracelog |
| Pack_SCL_0024 | [RACINE] | | README.txt | |

Tableau 45 : Contenu du « Kit Smartcard logon CPS ASIP Santé»


14 Smartcard logon sous Linux

Il est possible de configurer le PAM Linux pour faire du Smartcard logon.

Ce chapitre décrit les principales étapes à réaliser afin d'effectuer un Smartcard logon local (testé OK sous LUbuntu 12.04 x32 avec la Cryptolib CPS v5 x32 – pas de Cryptolib CPS v5 x64 pour Linux!).

14.1 Installation de la Cryptolib CPS v5 pour Linux

Cf. Manuel d'installation et d'utilisation de la Cryptolib CPS v5.

14.2 Configuration du lancement automatique du daemon PCSCD

| # Se référer à : | |
|---------------------------------|--|
| Source0 | http://ludovicrousseau.blogspot.fr/2010/12/configuring-your-system-for-pcscd- auto.html |
| # En particulier: | |
| sudo addgroupsystem pcscd | |
| sudo mkdir /var/run/pcscd | |
| sudo chgrp pcscd /var/run/pcscd | |
| sudo chmod g+w /var/run/pcscd | |

14.3 Installation et configuration du PAM OpenSC

| Source1 | https://www.opensc-project.org/opensc/wiki/ApplicationSupport |
|---------|---|
| Source2 | http://blog.fkraiem.org/2013/03/13/linux-smart-card-authentication-pam/ |

14.3.1 Récupération et installation de libpam-pkcs11

| sudo apt-get install libpam-pkcs11 |
|------------------------------------|
| # Début de la configuration |
| sudo mkdir /etc/pam_pkcs11 |
| sudo mkdir /etc/pam_pkcs11/cacerts |
| sudo mkdir /etc/pam_pkcs11/crls |

14.3.2 Initialisation du fichier pam_pkcs11.conf, des certificats et des CRLs

| zcat /usr/share/doc/libpam-pkcs11/examples/pam_pkcs11.conf.example.gz sudo tee /etc/pam_pkcs11/pam_pkcs11.conf |
|---|
| sudo vi /etc/pam_pkcs11/pam_pkcs11.conf |
| # edit the use_mappers line to list only pwent |
| # copy the certificate of the CA who signed your own certificate (if your certificate is self-signed, |
| that's the certificate itself) into /etc/pam_pkcs11/cacerts and rehash the list of CA certificates with: |
| sudo cp /etc/opt/santesocial/CPS/Coffre/*.cer /etc/pam_pkcs11/cacerts/ |
| cd /etc/pam_pkcs11/cacerts |
| sudo pkcs11 make hash link |

sudo pkcs11_make_hash_link

14.3.3 Edition de /etc/pam.d/sudo

| sudo vi /etc/pam.d/sudo | | |
|---|--|--|
| # contenu normal: | | |
| #%PAM-1.0 | | |
| | | |
| auth required pam_env.so readenv=1 user_readenv=0 | | |
| auth required pam_env.so readenv=1 envfile=/etc/default/locale user_readenv=0 | | |
| @include common-auth | | |
| @include common-account | | |
| @include common-session-noninteractive | | |
| | | |
| # Edition du contenu: | | |
| auth required pam_env.so readenv=1 user_readenv=0 | | |
| auth required pam_env.so readenv=1 envfile=/etc/default/locale user_readenv=0 | | |
| auth sufficient pam_pkcs11.so | | |
| @include common-auth | | |
| @include common-account | | |
| @include common-session-noninteractive | | |
| # test with | | |
| sudo -i | | |
| # revert to initial /etc/pam.d/sudo content | | |
| | | |

14.3.4 Edition de /etc/pam.d/common-auth

| sudo vi /etc/pa | am.d/common-auth | | |
|-------------------|---------------------|---------------|--|
| # Verifier la lig | ne: | | |
| auth [succes | s=3 default=ignore] | pam_pkcs11.so | |

14.3.5 Edition de /etc/pam_pkcs11/pam_pkcs11.conf

| # Source3: http://opensc.github.io/pam_pkcs11/doc/pam_pkcs11.html#idp5105696 |
|--|
| sudo vi /etc/pam_pkcs11/pam_pkcs11.conf |
| use_pkcs11_module = cps; |
| [] |
| pkcs11_module cps { |
| module = /opt/santesocial/CPS/lib/libcps3_pkcs11_lux.so |
| description = "CPS3"; |
| <pre>slot_description = "none";</pre> |
| support_threads = false; |
| ca_dir = /etc/pam_pkcs11/cacerts; |
| crl_dir = /etc/pam_pkcs11/crls; |
| cert_policy = none; |
| crl_policy = none; |
| } |
| [] |
| <pre>#use_mappers = digest, cn, pwent, uid, mail, subject, null;</pre> |
| use_mappers = subject |

14.3.6 Configuration d'un compte pour le Smartcard logon

14.3.6.1 Création d'un utilisateur de test

| # Définition d'un compte « scl », par exemple : |
|---|
| sudo adduser <mark>scl</mark> |
| password: scl |
| sudo adduser scl root |
| |

14.3.6.2 Définition du mapping DN / Compte : /etc/pam_pkcs11/subject_mapping

| # Lancer la commande : |
|--|
| pklogin_finder |
| # si la carte est bien lue, une ligne du type suivant apparait: |
| /C=FR/O=GIP-CPS/L=Paris |
| (75)/OU=318751275100020/CN=518751275100020/0000000311/SN=NOM/GN=PRENOM |
| |

éditer /etc/pam_pkcs11/subject_mapping:

sudo vi /etc/pam_pkcs11/subject_mapping

ajouter une ligne du type :

/C=FR/O=GIP-CPS/L=Paris (75)/OU=318751275100020/CN=518751275100020/0000000311/SN= NOM/GN=PRENOM -> scl

(chaine DN -> nom du compte)

tester le mapping avec:

pklogin_finder

15Smartcard logon sous Mac OS X

| Source0 | http://support.apple.com/kb/ta24244 |
|---------|--|
| Source1 | http://www.charismathics.com/fileadmin/files/pdf/manuals/Mac_Logon.pdf |

La fonctionnalité de Smartcard logon est a priori offerte par Mac OS X.

Elle était bien supportée et documentée sur Mac OS X 10.4 Tiger.

Ce n'est plus forcément le cas sur les Mac OS X récents.

La procédure décrite ci-après a été testée sous Mac OS X 10.9 Mavericks.

15.1 Pré-requis

| # | Pré-requis au Smartcard logon sous Mac OS X |
|---|---|
| 1 | Certificats AC racine dans trousseau « AC Racines » |
| 2 | Certificats AC intermédiaires dans trousseau « Système » (ce que l'installeur de la Cryptolib CPS ne fait pas) |
| 3 | Lecteur et carte fonctionnent |

Tableau 46 : Pré-requis au Smartcard logon sous Mac OS X

15.2 Méthode

Récupérer les hash de clé

\$ sc_auth hash

retour : <cert_auth_hash> : AABB8F7E3E94D924E46550A1A5EEB8DD6F14XXYY par exemple

Ajouter un hash pour l'authentification (voir « man » pour la suppression d'un hash)

\$ sudo sc_auth accept -u <nom_du_compte> -h <cert_auth_hash>

Autoriser l'authentification par carte à puce (disable pour désactiver)

\$ sudo security authorizationdb smartcard enable

 Tableau 47 : Methode pour appliquer le Smartcard logon sous Mac OS X

15.3 Autres commandes utiles

\$ sudo sc_auth remove -u <nom_du_compte> \$ sudo sc_auth list -u <nom_du_compte>

Tableau 48 : Commandes utiles au Smartcard logon sous Mac OS X

15.4 Remarques

- La configuration avec des comptes réseau est différente
 Of. internet pour ces configurations plus spécifiques
- L'authentification par mot de passe n'est pas désactivée
 - Apparemment, il n'est pas possible de le faire
- Ne pas faire les tests trop vite
 - 2 ou 3 secondes peuvent être nécessaires pour que la fenêtre change en « code porteur » à l'insertion de la carte
- Ce cas d'usage semble être peu sponsorisé par Apple

16Annexe – Liste des figures

| Figure 1 : Ecran d'accueil de Windows XP, configuré pour ouvrir une session avec une carte à puce. | 13 |
|---|------|
| Figure 2 : Ecran d'accueil de Windows 7, configuré pour ouvrir une session avec une carte à puce | 13 |
| Figure 3 : Ecran du client Terminal Server sous Windows 7 pour ouvrir une session avec une carte | e à |
| puce | 13 |
| Figure 4 : Schéma fonctionnel global du Smartcard logon de Microsoft (Win 2000 et XP) | 16 |
| Figure 5 : Schéma fonctionnel global du Smartcard logon de Microsoft (Win Vista+) [7] | 17 |
| Figure 6 : Smartcard logon et TSE : Redirection des APDU [1] | 22 |
| Figure 7 : Architecture: Exemple d'un réseau informatique configuré pour le Smartcard logon | 24 |
| Figure 8 : Exemple d'un certificat de type « Smartcard logon » | 28 |
| Figure 9 : Informations des certificats de type « Smartcard logon » | 29 |
| Figure 10 : Poste client: Vérifier le certificat d'authentification | 31 |
| Figure 11 : Poste client: identifier I'UPN du certificat d'authentification | 31 |
| Figure 12 : Poste client: identifier I'UPN du certificat d'authentification | 32 |
| Figure 13 : Active Directory: Smartcard logon : Configuration d'un compte utilisateur | 34 |
| Figure 14 : Active Directory: Approbation du suffixe UPN « carte-cps.fr » | 35 |
| Figure 15 : Forcer l'utilisation de la carte à puce par stratégie locale | 37 |
| Figure 16 : Architecture : Exemple d'architecture réseau évoluée | 43 |
| Figure 17 : Macro-planning « maquette de Smartcard logon avec une carte CPx » | 47 |
| Figure 18 : Poste client : Erreur de carte à puce sur un login TSE si les Cryptolib CPS ne sont p | bas |
| installées | 49 |
| Figure 19 : Poste client : Installation Cryptolib CPS x64 | 50 |
| Figure 20 : Poste client: Installation Cryptolib CPS x64 : installation perso avec la filière CPS2Ter F | iull |
| PC/SC | 50 |
| Figure 21 · Poste client· Installation Cryntolib CPS x64 · installation perso avec la filière CPS2Ter F | -ull |
| PC/SC | 51 |
| Figure 22 : Poste client : Installation Cryptolib CPS x64 : Installer | 51 |
| Figure 23 · Poste client: Installation Cryptolic CPS x64 · Fenêtre d'IIAC | 52 |
| Figure 24 : Poste client : Installation Cryptolib CPS $x64$ avec $\Delta V/\Delta ST$ | 52 |
| Figure 25 : Poste client : Installation of yptons of 9 xo4 avec 707 81 | 52 |
| Figure 26 : Poste client : Vérifier le magasin de certificats | 53 |
| Figure 27 : Poste client : Vérifier le certificat d'authentification | 57 |
| Figure 28 : Poste client : identifier l'HDN du certificat d'authentification | 55 |
| Figure 20 : Poste client : identifier l'UPN du certificat d'authentification | 56 |
| Figure 20 : Poste client : Dériphériques et imprimantes : Daramètres d'installation de périphériques | 50 |
| Pigure 50. Poste client . Periphenques et imprimantes . Parametres u installation de periphenques | . el |
| Villuows Opuale | |
| Figure 31 : Windows serveur: Installation: choix du type d'Installation | 50 |
| Figure 32 : Windows serveur: Installation: copie de lichier | 59 |
| Figure 33 : Windows serveur: Installation: mot de passe administrateur | 60 |
| Figure 34 : Windows serveur: Installation: saisle mot de passe administrateur | 61 |
| Figure 35 : Windows serveur: Installation: mot de passe administrateur change | 62 |
| Figure 36 : Windows serveur: Installation: accueil | 63 |
| Figure 37 : Windows serveur: Installation: sécurité renforcée | 64 |
| Figure 38 : Windows serveur: Installation: Paramétrage de la sécurité renforcée | 65 |
| Figure 39 : Windows serveur: Configuration: maitriser les mises à jour | 66 |
| Figure 40 : Windows serveur: Configuration: maitriser les mises à jour | 67 |
| Figure 41 : Windows serveur: Configuration: nom de l'ordinateur | 68 |
| Figure 42 : Active Directory: Installation du rôle | 69 |
| Figure 43 : Active Directory: Installation du rôle : résultat | 70 |
| | |

| Figure 45 : Active Directory: Configuration du rôle : Exécution de l'assistant | . 72 |
|--|------|
| Figure 46 : Active Directory: Configuration du rôle : mode avancé | . 73 |
| Figure 47 : Active Directory: Configuration du rôle : nouvelle forêt | . 74 |
| Figure 48 : Active Directory: Configuration du rôle : nom de domaine | . 75 |
| Figure 49 : Active Directory: Configuration du rôle : vérification de la disponibilité du nom de la fo | orêt |
| | . 76 |
| Figure 50 : Active Directory: Configuration du rôle : NetBIOS | . 77 |
| Figure 51 : Active Directory: Configuration du rôle : Vérif. NetBIOS | . 78 |
| Figure 52 : Active Directory: Configuration du rôle : Niveau fonctionnel | . 79 |
| Figure 53 : Active Directory: Configuration du rôle : Configuration DNS | . 80 |
| Figure 54 : Active Directory: Configuration du rôle : Décocher DNS | . 81 |
| Figure 55 : Active Directory: Configuration du rôle : mot de passe LDAP | . 82 |
| Figure 56 : Active Directory: Configuration du rôle : configuration des bases de données | . 83 |
| Figure 57 : Active Directory: Configuration du rôle : Installation GPMC | . 84 |
| Figure 58 : AD CS : Installation du rôle | . 85 |
| Figure 59 : AD CS : service du rôle « Autorité de certification » | 86 |
| Figure 60 : AD CS : Type d'installation : Choisir « Entreprise » | 87 |
| Figure 61 : AD CS : type d'autorité : Choisir « Autorité de certification racine » | 88 |
| Figure 62 : AD CS : Choisir « Créer une nouvelle clé privée » | 89 |
| Figure 63 : AD CS : clé privée : Chiffrement | 90 |
| Figure 64 : AD CS : clé privée : Préciser le nom de l'AC | 91 |
| Figure 65 : AD CS : clé privée : Préciser la période de validité | 92 |
| Figure 66 : AD CS : clé privée : Base de données de certificats | . 93 |
| Figure 67 : AD CS : clé privée : confirmation | . 94 |
| Figure 68 : AD CS : clé privée : résultats | 95 |
| Figure 69 : AD CS: Certificat AD CS | . 96 |
| Figure 70 : AD CS: Certificat AD CS | 97 |
| Figure 71 : AD: Certificat AD deliver nar AD CS | 98 |
| Figure 72 : AD: Certificat AD DomainController délivré par AD CS | 98 |
| Figure 72 : Terminal Server : installation du rôle | 99 |
| Figure 74 : Terminal Server : service de rôle : choisir « Hôte de session Bureau à distance » | 100 |
| Figure 75 · Terminal Server · mode d'authentification RDP · Choisir « Ne nécessite | nas |
| l'authentification au niveau réseau » | 101 |
| Figure 76 : Terminal Server : mode de licence : Choisir « Configurer ultérieurement » | 102 |
| Figure 77 : Terminal Server : utilisateurs : garder « Administrateurs » | 102 |
| Figure 78 : Terminal Server : expérience client | 103 |
| Figure 70 : Terminal Server : résultat de l'installation | 104 |
| Figure 80 : Terminal Server : Lancer le Gestionnaire des licences des services Bureau à distance | 105 |
| Figure 80. Terminal Server : Clic droit > propriótóc | 100 |
| Figure 81 : Terminal Server : Mode de connexion > Navigatour Web | 100 |
| Figure 82 : Terminal Server : Configurations des comptes « Serveurs de licenses des convices Term | 107 |
| Figure 65 : Terminal Server : Comigurations des comptes « Serveurs de licences des services Termi | 100 |
| Serveur » | 100 |
| Figure 84 : Terminal Server : Fin de l'activation du serveur de licences Terminal Serveur | 109 |
| Figure 85 : Terminal Server : Installation d un pack de licences | 110 |
| Figure 86 : Terminal Server : Configuration d'hote de session Bureau a distance | 111 |
| Figure 87 : Terminal Server : Configuration d'hote de session Bureau à distance > mode de licenc | e et |
| serveurs de licences | 112 |
| Figure 88 : Terminal Server : Configuration d'hôte de session Bureau à distance > mode de licenc | e et |
| serveurs de licences | 112 |
| Figure 89 : Terminal Server : Configuration des paramètres serveur | 113 |
| Figure 90 : Terminal Server : config. nom du serveur et port externe | 114 |
| Figure 91 : Terminal Server : Déclaration d'une remote app de test | 115 |

| Figure 92 : Terminal Server : Compatibilité ascendante RDP | . 116 |
|--|-------|
| Figure 93 : Terminal Server : Ajout d'utilisateur du bureau à distance | . 117 |
| Figure 94 : Terminal Server : Groupe utilisateur du Bureau à distance | . 117 |
| Figure 95 : Terminal Server : Droits d'ouverture de session à distance | . 118 |
| Figure 96 : Terminal Server : Droits d'ouverture de session à distance pour un utilisateur précis | . 118 |
| Figure 97 : Terminal Server : Droits d'ouverture de session à distance pour le groupe « Utilisate | ur du |
| Bureau à distance » | . 119 |
| Figure 98 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS | . 120 |
| Figure 99 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS | . 121 |
| Figure 100 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS | . 122 |
| Figure 101 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS | . 122 |
| Figure 102 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS | . 123 |
| Figure 103 : Terminal Server : Droits sur le modèle de certificat Remote Desktop | . 123 |
| Figure 104 : Terminal Server : Droits sur le modèle de certificat Remote Desktop | . 124 |
| Figure 105 : Terminal Server : Déploiement du modèle de certificat Remote Desktop sur les po | ostes |
| clients via l'AD | . 124 |
| Figure 106 : Terminal Server : Demande de certificat Terminal Server | . 125 |
| Figure 107 : Terminal Server : Demande de certificat Terminal Server : Sélection | ı de |
| « RemoteDesktopComputer » | . 125 |
| Figure 108 : Terminal Server : Demande de certificat Terminal Server | . 126 |
| Figure 109 : Terminal Server : Vérification du certificat Terminal Server émis sur l'AD CS | . 127 |
| Figure 110 : Terminal Server : Vérification du certificat Terminal Server émis sur le Terminal Ser | rveur |
| | . 127 |
| Figure 111 : Terminal Server : Installation du certificat Terminal Server | . 128 |
| Figure 112 : Terminal Server : Configuration | . 129 |
| Figure 113 : Terminal Server : Installation du certificat Terminal Server | . 129 |
| Figure 114 : Terminal Server : Installation du certificat Terminal Server | . 130 |
| Figure 115 : Terminal Server : Vérifier l'installation du certificat Terminal Server | . 131 |
| Figure 116 : IIS: Installation du rôle | . 134 |
| Figure 117 : IIS: Installation du rôle : sélection des options de sécurité | . 135 |
| Figure 118 : IIS: Installation du rôle : état d'avancement | . 136 |
| Figure 119 : IIS: Installation du rôle : Résultat | . 137 |
| Figure 120 : CCM: lancement du CCM au démarrage des sessions utilisateurs sur un serveur Wind | dows |
| | . 138 |
| Figure 121 : CPSRev: répertoire d'installation | . 139 |
| Figure 122 : CPSRev: résultat d'installation | . 140 |
| Figure 123 : CPSRev: vérification du magasin Root (Local machine) | . 141 |
| Figure 124 : CPSRev: vérification du magasin Intermediate CA (Local machine) | . 142 |
| Figure 125 : CPSRev: vérification du magasin Root CA (User) | . 143 |
| Figure 126 : CPSRev: vérification du magasin Intermediate CA (User) | . 144 |
| Figure 127 ; CPSRev : vérification des statuts de certificats offline : consultation du magasin de | e CRL |
| | . 147 |
| Figure 128 : Console Enfichable: MMC | . 151 |
| Figure 129 : Console Enfichable: Ajout de composants enfichables | . 152 |
| Figure 130 : Console Enfichable: Certificats | . 153 |
| Figure 131 : Console Enfichable: Certificats utilisateur | . 154 |
| Figure 132 : Console Enfichable: Certificats Local Machine | . 155 |
| Figure 133 : Console Enfichable: Certificats Local Machine | . 156 |
| Figure 134 : Console Enfichable: Stratégie de groupe du contrôleur de domaine | . 157 |
| Figure 135 : Console Enfichable: Liste des composants utilisés pour le Smartcard logon | . 158 |
| Figure 136 : Console Enfichable: Sauvegarde | . 159 |
| Figure 137 : Active Directory: Configuration: Certificat Local Machine personnel | . 160 |

| Figure 138 : Active Directory: Configuration: Copie de certificats Racine | 161 |
|---|-------|
| Figure 139 : Active Directory: Configuration: Collage de certificats Racine dans le magasin pers | onnel |
| | 162 |
| Figure 140 : Active Directory: Configuration: Magasin NTAUTH avant import | 163 |
| Figure 141 : Active Directory: Configuration: Magasin NTAUTH après import | 164 |
| Figure 142 : Active Directory: Configuration: Stratégie de clé publique avant import | 166 |
| Figure 143 : Active Directory: Configuration: Stratégie de clé publique après import | 167 |
| Figure 144 : Active Directory: Configuration: Approbation du suffixe UPN « carte-cps.fr » | 170 |
| Figure 145 : Active Directory: Configuration: Définition d'un compte avec Smartcard logon activé | é.171 |
| Figure 146 : Active Directory: Configuration: Définition d'un compte avec Smartcard logon active | é.171 |
| Figure 147 : Active Directory: Configuration: Smartcard logon en TSE | 172 |
| Figure 148 : Active Directory: Configuration: Bureau à distance et CPS Gestion après Smartcard | logon |
| | 173 |
| Figure 149 : Paramétrage du Smartcard logon sur des comptes AD préexistants : cas {un co | ompte |
| existant ; une carte} | 177 |
| Figure 150 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants | 178 |
| Figure 151 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants | 179 |
| Figure 152 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants | 179 |
| Figure 153 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants | 180 |
| Figure 154 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants | 180 |
| Figure 155 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants | : GPO |
| « Allow user hint » | 183 |
| Figure 156 : Comptes existants : Ecran de Smartcard logon après lecture d'une carte | 184 |
| Figure 157 : Comptes existants : Saisie du code porteur et du « hint » | 184 |
| Figure 158 : Comptes existants : Ouverture de session Windows | 184 |
| Figure 159 : Configuration de la Stratégie de retrait de la carte à puce (manuel) | 185 |
| Figure 160 : Configuration de la Stratégie de retrait de la carte à puce (passage en automatique) | 186 |
| Figure 161 : Configuration de la Stratégie de retrait de la carte à puce (automatique) | 187 |
| Figure 162 : Workaround : Désactivation verrouillage de session | 211 |
| Figure 163 : Workaround : Désactivation verrouillage de session sur Ctrl+Alt+Suppr | 212 |
| Figure 164 : Workaround : Désactivation changement d'utilisateur | 213 |

17Annexe – Liste des tables

| Tableau 1 : Glossaire | 9 |
|--|--------|
| Tableau 2 : Entreprises citées | 10 |
| Tableau 3 : Avertissements | 11 |
| Tableau 4 : Inconvénients du couple login/mot de passe | 14 |
| Tableau 5 : Avantages de la carte à puce | 14 |
| Tableau 6 : Inconvénients de la carte à puce face au couple login/mot de passe | 15 |
| Tableau 7 : Smartcard logon: Principaux Composants Microsoft mis en œuvre | 18 |
| Tableau 8 : Smartcard logon: Protocole Kerberos | 20 |
| Tableau 9 : Smartcard logon: Cinématique de l'authentification par carte à puce | 21 |
| Tableau 10 : Smartcard logon: Cinématique de l'authentification par carte à puce | 23 |
| Tableau 11 : Architecture: Scénarios d'implémentation de PKI serveur | 25 |
| Tableau 12 : CPSRev : désactivation de la vérification des CRLs | 39 |
| Tableau 13 : Serveur: Installation du serveur | 40 |
| Tableau 14 : Serveur: Configuration | 42 |
| Tableau 15 : « Brief Project » « maquette de Smartcard logon avec une carte CPx » | 44 |
| Tableau 16 : Ressources « maquette de Smartcard logon avec une carte CPx » | 45 |
| Tableau 17 : Livrables « maquette de Smartcard logon avec une carte CPx » | 46 |
| Tableau 18 : Macro-planning « maquette de Smartcard logon avec une carte CPx » | 46 |
| Tableau 19 : Remarques « maquette de Smartcard logon avec une carte CPx » | 48 |
| Tableau 20 : CPSRev : Configuration de CPSRev pour prise en compte des certificats de test | : ASIP |
| Santé | 145 |
| Tableau 21 : CPSRev : Désactivation de la vérification des listes de révocation sous Win2008+ | 145 |
| Tableau 22 : CPSRev : (Ré-)Activation de la vérification des listes de révocation sous Win2008+ | 145 |
| Tableau 23 : CPSRev : Vérification des flux vers l'annuaire ASIP Santé | 146 |
| Tableau 24 : CPSRev : Ligne de commande certmgr.exe | 146 |
| Tableau 25 : CPSRev : Résultat de la vérification d'un certificat avec CPSRev | 150 |
| Tableau 26 : Active Directory: Configuration: Commande certutil d'import des certificats da | ans le |
| magasin NTAUTH | 165 |
| Tableau 27 : Déploiement UPN : Construction de l'UPN | 169 |
| Tableau 28 : Déploiement UPN : Exemple de script VBS permettant la modification de | ľUPN |
| d'utilisateurs existants dans un annuaire Active Directory | 175 |
| Tableau 29: Déploiement UPN : Exemple de Fichier « users.txt » | 175 |
| Tableau 30 : Déploiement UPN: Exemple de script VBS permettant la création d'utilisateurs da | ns un |
| annuaire Active Directory | 176 |
| Tableau 31 : Liste des possibilités de mapping user / certificat pour l'authentification par certifica | at181 |
| Tableau 32 : Désactivation de l'utilisation du SubjectAltName (SAN) | 182 |
| Tableau 33 : Activation du « hint » | 182 |
| Tableau 34 : Active Directory: Configuration du Smartcard logon pour utilisateurs exist | ants : |
| Références | 183 |
| Tableau 35 : Comptes existants : Considération d'ergonomie en Smartcard logon sur co | ompte |
| préexistant | 184 |
| Tableau 36 : Liste de certificats | 200 |
| Tableau 37 : Activation des traces Kerberos via la base de registre | 201 |
| Tableau 38 : Activation des traces Kerberos via la base de registre | 201 |
| Tableau 39 : Emplacement des traces Kerberos après activation via la base de registre | 202 |
| Tableau 40 : Désactivation des traces Kerberos activées via la base de registre | 202 |
| Tableau 41 : Activation des traces Kerberos via Tracelog | 203 |
| Tableau 42 : Emplacement des traces Kerberos après activation via Tracelog | 203 |
| I ableau 43 : Désactivation des traces Kerberos activées via Tracelog | 203 |

| Tableau 44 : Points d'attention | 210 |
|--|-----|
| Tableau 45 : Contenu du « Kit Smartcard logon CPS ASIP Santé» | 216 |
| Tableau 46 : Pré-requis au Smartcard logon sous Mac OS X | 220 |
| Tableau 47 : Methode pour appliquer le Smartcard logon sous Mac OS X | 220 |
| Tableau 48 : Commandes utiles au Smartcard logon sous Mac OS X | 220 |

18Notes

[fin du document]



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