Table des matières

[1. Prérequis poste partenaire 2](#_Toc7162214)

[2. Authentification forte 3](#_Toc7162215)

[2.1 Lecteur de cartes 3](#_Toc7162216)

[2.2 Installation des drivers de badge GEMALTO 4](#_Toc7162217)

[3. Installations 5](#_Toc7162219)

[3.1 Installation du client Netscaler 5](#_Toc7162220)

[3.2 Installation du client Citrix Receiver 6](#_Toc7162221)

[3.3 Installation Certificat DigiCert 7](#_Toc7162222)

[3.4 Installation Certificats Bouygues Telecom 8](#_Toc7162223)

[4. Portails PAX 10](#_Toc7162224)

[4.1 Portails interne (LL ou VPN Lan to Lan) 10](#_Toc7162225)

[4.2 Portails internet 10](#_Toc7162226)

[4.3 Mode d’accès au portail 11](#_Toc7162227)

**Document destiné au service informatique du partenaire**

# Prérequis poste partenaire

Le poste utilisateur ne doit pas être un poste avec un master Bouygues Telecom.

Il doit être masterisé par le partenaire avec l’un des systèmes d’exploitation ci-dessous.

Le poste utilisateur doit disposer d’un poste informatique équipé d’un :

* Système d’exploitation Windows Seven 32/64 bits, Seven SP1, Windows 8.1 ou **Windows 10 (jusqu’à build 1803)**
* Firewall activé. Le firewall peut être celui natif de l'OS Microsoft mais également un firewall d’un fournisseur tiers. Il est nécessaire que ce firewall soit actif sur le réseau où se trouve le poste du partenaire.
* Navigateur Internet Explorer version 11 **UNIQUEMENT**
* Client Netscaler Gateway (fourni par Bouygues Telecom – cf chapitre suivant)
* Client Xendesktop (fourni par Bouygues Telecom – cf chapitre suivant)
* Certificats digiCert (fourni par Bouygues Telecom – cf chapitre suivant)
* Certificats Bouygues Telecom (fourni par Bouygues Telecom – cf chapitre suivant)
* Accès internet
* Anti-virus installé avec signatures à jour et protection en temps réelle activée – antivirus doit être détecté par le centre de sécurité Windows **(signatures datant de moins de 3 jours)**
* Lecteur de carte à puce compatible Gemalto pour l’authentification forte
* Le poste doit disposer des correctifs de sécurité fournis par Microsoft au travers du service Windows Update. Nous autorisons les postes à jour avec un délai de 2 mois de retard par rapport aux derniers correctifs de sécurité fournis par Microsoft. Ainsi, après la sortie des correctifs de juin, nous autorisons les postes disposant des correctifs de juin mais également ceux qui ne disposent que des correctifs de mai ou d'avril. Les versions d'OS Microsoft traités sont celles supportées par Microsoft.

**IMPORTANT : s’assurer que le poste dispose bien des dernières mises à jour des fix de sécurités critiques et importantes (Windows Update)**

**Le centre de maintenance du Panneau de configuration, partie Sécurité, doit être activé pour que l’antivirus soit reconnu**

**Recommandation Microsoft : internet explorer doit être installé avec une distribution de la même langue que le noyau du système d’exploitation.**

# Authentification forte

Chaque prestataire doit disposer d’un badge «L» initialisé auprès du responsable Bouygues Telecom.

## Lecteur de cartes

Les badges utilisés sont des badges GEMALTO (.Net v2 et MD830).

Les sites partenaires doivent équiper leurs postes de travail de lecteur de cartes compatibles avec les normes suivantes :

> ISO 7810 : standard size format ID-1

> ISO 7811 - 1 to 5: supports embossing and magnetic strip.

> ISO 7816 – 1 to 3

> ISO 7816 – 4 limited to transmission protocol T=0.

Selon les poste du partenaire, deux cas de figure se présentent :

* Lecteur carte inclus dans le poste : Vigilance malgré tout auprès du master mis en place avec généralement la dernière version de driver du périphérique lecteur carte sous le gestionnaire du périphérique ( voir aupres du support bureautique du partenaire).
* Lecteur de carte externe : Il s’agit de s’en procurer, les recommandations côté Bouygues Telecom est d’utiliser les lecteurs IDbridge CT30 ou CT40

Voici les références des 2 lecteurs de cartes externes :

IDbridge CT30

* Présentation produit : <http://www.nis-infor.com/fr/produit/lecteur-de-carte-a-puce-idbridge-ct30-pc-usb-tr/12>
* Drivers : <http://support.gemalto.com/?id=pc_usb_tr_and_pc_twin#.Wuxa7bpuLIU>
* Achat : par ex sous Amazon <https://www.amazon.fr/Nouveau-iDBridge-cT30-double-lecteur/dp/B00HEMJPYY/ref=sr_1_fkmr0_1?ie=UTF8&qid=1525439373&sr=8-1-fkmr0&keywords=IdBridge+CT-30>

IDbridge CT40

* Présentation produit : <http://www.nis-infor.com/fr/produit/lecteur-de-carte-a-puce-idbridge-ct40-pc-usb-sl/31>
* Drivers : <http://support.gemalto.com/?id=pc_usb_sl#.WuxbVrpuLIU>
* Achat : par ex sous Amazon <http://www.accord-distribution.com/contents/fr/p2143_GEMALTO-IDBRIDGE-CT40-HWP108841E-001.html>

« Attention » :  les opérations de renouvellement des certificats des badges L doivent s’effectuer depuis un lecteur de carte externe compatible (comme indiqué ci-dessus)

Les claviers avec lecteurs intégrés ne sont pas supportés et ne doivent pas être utilisés pour réaliser l’opération de renouvellement. (Ils peuvent cependant fonctionner lors de la lecture du badge)

## Installation des drivers de badge GEMALTO



Il est recommandé de mettre à jour le système d’exploitation Windows avec la dernière version des drivers GEMALTO qui apportent de meilleures performances et des fonctionnalités étendues pour l’utilisation des cartes à puces GEMALTO .NET V2 +  et IDPrime MD830.

**La dernière version des drivers est disponible dans le dossier « badge » du kit PAX. Il est nécessaire d’installer les drivers fournis dans les répertoires IDGo800-Minidriver et IDGo800-PKCS11.**

**IMPORTANT** : le mot de passe du code PIN doit comporter uniquement des chiffres

# Installations

Pour se connecter aux portails PAX, il est indispensable d’installer des logiciels et certificats.

***IMPORTANT :***

* *Avoir les droits administrateurs sur le poste utilisateur pour installer ces logiciels* ***(installer avec un compte administrateur local du poste)***

## Installation du client Netscaler

**Pour un OS Win 7/Win 10 32 bits : exécuter nsepa\_setup32.exe**

**Pour un OS Win 7/Win 10 64 bits : exécuter nsepa\_setup64.exe**

|  |  |
| --- | --- |
|  | * Cliquer sur « Installer » |

|  |  |
| --- | --- |
|  | * Installation en cours |

|  |  |
| --- | --- |
|  | * Cliquer sur « Terminer » |

## Installation du client Citrix Receiver

**Ligne de commande à exécuter dans le répertoire où se trouve l’exécutable** :

CitrixReceiver.exe /noreboot /Silent /IncludeSSON=NO /AllowAddStore=N /EnableCEIP=false /AutoUpdateCheck=disabled

Aller dans le panneau de configuration, pour vérification de la version :

|  |
| --- |
| cid:image001.png@01D35719.D5174FB0 |

**Désactiver la mise à jour automatique (auto update) du client Receiver**

## Installation Certificat DigiCert

Chaque poste prestataire devra installer les certificats Digicert (Verisign & Symantec) pour se connecter aux portails Bouygues Telecom.

Ces certificats sont émis par la société DigiCert: certificat Verisign class 3 secure server CA – G3, Symantec Class 3 Secure Server CA - G4 délivré par Verisign class 3 public primary certifications Authority – G5 et DigiCert SHA2 Secure Server CA.cer délivré par DigiCert Global Root CA.cer.

**IMPORTANT :**

Avoir les droits administrateurs sur le poste utilisateur pour installer ces certificats **(installer avec un compte administrateur local du poste)**

**Ouvrir une fenêtre DOS en tant qu’administrateur**

Procédure d’installation ou renommer le fichier « lignes de commandes certificats » en.bat et l’exécuter depuis le répertoire où se trouvent les certificats :

* Recopier les fichiers « Verisign Class 3 Public Primary Certification Authority - G5 », « Verisign Class 3 Secure Server CA - G3 », « Symantec Class 3 Secure Server CA - G4 », "DigiCert Global Root CA.cer" et "DigiCert SHA2 Secure Server CA.cer" dans un répertoire du poste utilisateur
* Lancer une fenêtre DOS sous windows et aller dans le répertoire où sont copiés les 5 fichiers ci-dessus et exécuter les lignes de commandes suivantes **(ne pas double-cliquer sur ces fichiers car cela n’aura pas les mêmes effets):**
* certutil -addstore -enterprise Root "Verisign Class 3 Public Primary Certification Authority - G5.cer"
* certutil -addstore -enterprise CA "Verisign Class 3 Secure Server CA - G3.cer"
* certutil -addstore -enterprise CA "Symantec Class 3 Secure Server CA - G4.cer"
* certutil -addstore -enterprise Root "DigiCert Global Root CA.cer" (nouveau certificat)
* certutil -addstore -enterprise CA "DigiCert SHA2 Secure Server CA.cer" (nouveau certificat)

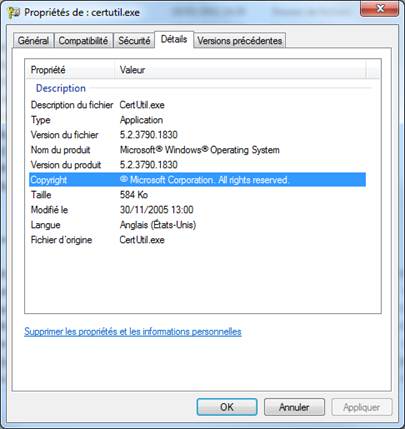
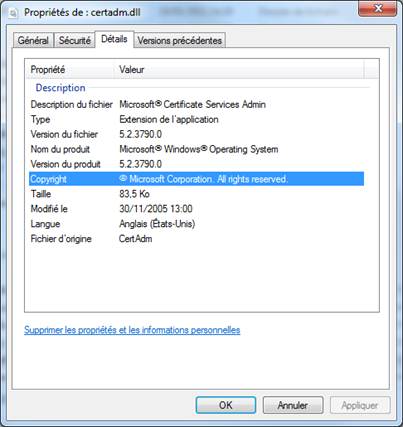
Les programmes certutil et certadm sont nécessaires pour exécuter ces commandes

Les mises à jour seront effectuées avec Windows Update (mise à jour des certificats racine)

**Pour Windows, les programmes certutil et certadm sont natifs à ce système d’exploitation. Il ne faut absolument pas recopier les 2 programmes fournis par Bouygues Telecom sur le poste mais utiliser ceux déjà présent.**

Attention également à la langue des fichiers. Par défaut, les fichiers fournis sont en version US (supportés par les versions US et US avec MUI).

Dans le cas d’utilisation d’une autre langue sur Windows, il est nécessaire de récupérer les fichiers associés à cette langue.

**VERIFICATION EMPLACEMENT DES CERTIFICATS:**

* Verisign Class 3 Public Primary Certification Authority - G5.cer
  + Certificat devant être dans l’onglet « autorités de certification racines de confiance »
* Verisign Class 3 Secure Server CA - G3.cer
  + Certificat devant être dans l’onglet « autorités intermédiaires »
* Symantec Class 3 Secure Server CA - G4.cer
  + Certificat devant être dans l’onglet « autorités intermédiaires »
* DigiCert Global Root CA.cer
  + Certificat devant être dans l’onglet « autorités de certification racines de confiance »
* DigiCert SHA2 Secure Server CA.cer
  + Certificat devant être dans l’onglet « autorités intermédiaires »

## Installation Certificats Bouygues Telecom

Chaque poste prestataire devra installer les certificats Bouygues Telecom pour se connecter au portail Bouygues Telecom (certificat d’authentification utilisateur).

**IMPORTANT :**

Avoir les droits administrateurs sur le poste utilisateur pour installer ces certificats **(installer avec un compte administrateur local du poste)**

Procédure d’installation ou renommer le fichier « lignes de commandes certificats » en.bat et l’exécuter depuis le répertoire où se trouvent les certificats) :

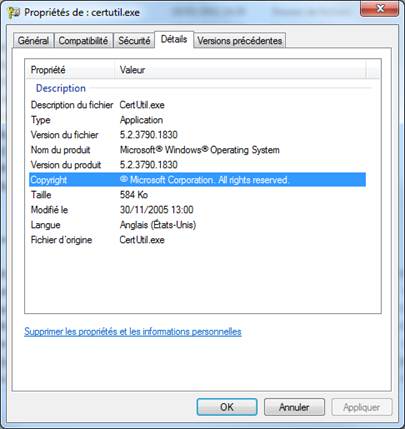
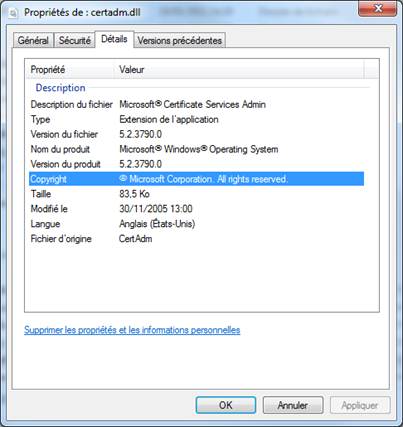
* Recopier les fichiers « acexterne», « acproduction », «acracinebytel » et «acracinegroupe »   dans un répertoire du poste utilisateur
* **Ouvrir une fenêtre DOS sen tant qu’administrateur** et aller dans le répertoire où sont copiés les 4 fichiers ci-dessus et exécuter les lignes de commandes suivantes **(ne pas double-cliquer sur ces fichiers car cela n’aura pas les mêmes effets):**
* certutil -addstore -enterprise Root "acracinegroupe.cer"
* certutil -addstore -enterprise CA "acracinebytel.cer"
* certutil -addstore -enterprise CA "acexterne.cer"
* certutil -addstore -enterprise CA "acproduction.cer"

Les programmes certutil et certadm sont nécessaires pour exécuter ces commandes

**Pour Windows, les programmes certutil et certadm sont natifs à ce système d’exploitation. Il ne faut absolument pas recopier les 2 programmes fournis par Bouygues Telecom sur le poste mais utiliser ceux déjà présent.**

Attention également à la langue des fichiers. Par défaut, les fichiers fournis sont en version US (supportés par les versions US et US avec MUI).

Dans le cas d’utilisation d’une autre langue sur Windows, il est nécessaire de récupérer les fichiers associés à cette langue.

**VERIFICATION EMPLACEMENT DES CERTIFICATS:**

* acracinegroupe.cer
  + Certificat devant être dans l’onglet « autorités de certification racines de confiance»
* acracinebytel.cer , acexterne.cer et acproduction.cer
  + Certificats devant être dans l’onglet « autorités intermédiaires »

# Portails PAX

## Portails interne (LL ou VPN Lan to Lan)

**BOUYGUES TELECOM préconise d’utiliser ce mode de connexion.**

**Il est donc nécessaire de mettre en place une interconnexion entre le site du partenaire et BOUYGUES TELECOM.**

Les noms des portails PAXS1 et PAXS3 doivent être résolus soit par le fichier hosts du poste client ou par le DNS interne du prestataire afin d’envoyer les requêtes vers la LL ou VPN Lan to Lan et non internet.

paxs1.bouyguestelecom.fr  172.21.55.5 #Url d’accès au portail PAX Bouygues Telecom (https - port 443)

paxs3.bouyguestelecom.fr  172.24.224.39 #Url d’accès au portail PAX Bouygues Telecom (https - port 443)

<https://paxs1.bouyguestelecom.fr>

<https://paxs3.bouyguestelecom.fr>

## Portails internet

**Ce mode de connexion est à utiliser uniquement en cas d’indisponibilité des portails internes.**

**Un filtrage IP est en place pour l’accès à ces portails de backup. Fournir au responsable BYTEL la liste des IP publiques du partenaire pour en obtenir l’accès. L’accès aux portails PAX n’est possible que depuis la sortie internet du partenaire.**

Le prestataire doit résoudre les adresses des portails internet Bouygues Telecom home5 et home7 en envoyant les requêtes vers internet (déclaration à effectuer dans le proxy du prestataire)

<https://home5.bouyguestelecom.fr> (62.201.133.36)

<https://home7.bouyguestelecom.fr> (212.195.100.204)

## Mode d’accès au portail

2 modes de connexions sont possibles aux portails PAX

|  |  |
| --- | --- |
| **Mode d’accès** | **Prérequis poste prestataire** |
| LS/LL ou VPN Lan to Lan | Ouverture FWL entre le site du prestataire et Bouygues Telecom : https (443) et http (80) pour la mise à jour des certificats  Postes à jour suivant les exigences de sécurité Bouygues Telecom (cf chapitre 1)  Liste autorité de certification  DigiCert sur le poste du prestataire (mise à jour sur le site internet DigiCert)  Authentification par certificat Bouygues Telecom  Résolution du nom du portail Bouygues Telecom chez le prestataire (fichier hosts)  Accès aux CRL DigiCert (url publique internet) |
| Internet | Ouverture FWL entre le site du prestataire et internet : https (443) et http (80) pour la mise à jour des certificats  Postes à jour suivant les exigences de sécurité Bouygues Telecom (cf chapitre 1)  Liste autorité de certification  DigiCert sur le poste du prestataire (mise à jour sur le site internet DigiCert)  Authentification par certificat Bouygues Telecom  Résolution du nom publique du portail Bytel chez le prestataire (DNS public internet)  Accès aux CRL DigiCert (url publique internet) |

Chaque poste prestataire doit disposer d’un accès internet (en mode anonyme) même limité mais devant accéder aux sites CRL de DigiCert ainsi qu’aux sites CRL de Bouygues Telecom et Bouygues pour le contrôle de révocation des certificats

La vérification des certificats fournis par Bouygues Telecom pour identifier les utilisateurs se fait sur les CRL de Bouygues Telecom et Bouygues :

<http://edc-ext.bouyguestelecom.fr/acdbouyguestelecompersonnes.crl>

<http://edc-ext.bouyguestelecom.fr/acbouyguestelecomracine.crl>

<http://edcg-ext.bouygues.com/ar-edcg.crl>

<http://edcg-int.bouygues.com/ar-edcg.crl>

<http://edc-ext.bouyguestelecom.fr/AC_Bouygues_Telecom_Racine_SHA256.crl>

La vérification du certificat protégeant le portail d’accès se fait sur les CRL de DigiCert, ces sites pouvant être modifiés par DigiCert lors d’une évolution :

<http://SVRSecure-G3-crl.verisign.com/SVRSecureG3.crl>

<http://crl.verisign.com/pca3-g5.crl>

<http://sd.symcb.com/sd.crl>

<http://s1.symcb.com/pca3-g5.crl>

<http://ss.symcb.com/ss.crl>

<http://s2.symcb.com>

<http://crl3.digicert.com/ssca-sha2-g6.crl>

<http://crl4.digicert.com/ssca-sha2-g6.crl>

Les ports et protocoles utilisés sont :

* HTTPS (TCP 443) pour le tunnel entre le poste client et le portail d’accès. C’est le seul protocole qui circule sur le réseau et qui doive être autorisé en entrée/sortie réseau
  + HTTP (TCP 80) localement sur le poste en dialogue dans le tunnel HTTPS
  + HTTPS (TCP 443) localement sur le poste en dialogue dans le tunnel HTTPS
  + RDP (TCP 3389) localement sur le poste en dialogue dans le tunnel HTTPS