Client VPN Windows Enterprise 7

Note technique : Authentification et format des certificats

Dernière mise à jour : 22 janvier 2024
Référence du document : 20240122_TNC_VPE_7_FR_1.2

www.thegreenbow.com

Table des matières

Tableau des révisions

Version	Date	Sections/pages affectées	Description de la modification	Auteur
1.0	2022-08-30	Toutes	Version initiale	ALE, JLB, BB
1.1	2023-01-11	4	Correction du renvoi vers le chapitre du Guide de l'administrateur	FG, BB
1.2	2024-01-22	2.3, 3.1 & 4	Mise à jour des informations pour tenir compte des évolutions liées à la v7.5	FG, BB

1 Introduction

En raison des exigences de sécurité renforcées, de la dépréciation de certains algorithmes et d'une utilisation plus rigoureuse des certificats, la version 7 du Client VPN Windows Enterprise comprend des restrictions sur les certificats.

Certains de nos clients nous ont fait part d'incompréhensions et de difficultés rencontrées lors du déploiement de la version 7 du Client VPN Windows Enterprise avec des tokens et des cartes à puces. C'est pourquoi, il nous a semblé utile et important d'apporter quelques éclairages sur des notions élémentaires liées à l'authentification et au format des certificats.

Algorithmes SHA, RSA et ECDSA

Les signatures numériques font généralement intervenir deux algorithmes différents :

- un algorithme de hachage (SHA ou *secure hash algorithm*) et
- un algorithme de signature (RSA : initiales des trois inventeurs ou ECDSA : *elliptic curve digital signature algorithm*).

La force du chiffrement RSA dépend de la taille de la clé utilisée. Dès lors que la taille est doublée, l'opération de déchiffrage va demander une puissance de traitement six à sept fois supérieure.

Selon l'ANSSI et le NIST, la taille de clé minimale recommandée est de 2048 bits.

Les algorithmes de hachage peuvent subir deux types d'attaques :

- la collision et
- la pré-image.

Une collision a lieu lorsque deux fichiers différents produisent le même condensat et qu'il est donc possible de substituer l'un pour l'autre.

La pré-image consiste à déterminer la valeur d'un fichier à partir de son condensat. Une pré-image secondaire consiste à produire à partir du condensat une valeur différente que celle à l'origine du hachage.

Selon l'ANSSI, la famille de fonctions de hachage SHA-1 n'est plus conforme à son référentiel général de sécurité et il convient par conséquent d'utiliser la famille SHA-2. Le NIST encourage de la même manière les agences fédérales étatsuniennes d'abandonner le SHA-1 au profit du SHA-2.

Les règles appliquées par le Client VPN Windows Enterprise suivent les recommandations de l'ANSSI et du NIST. Toutefois, si la PKI implémentée ne répond pas à ces exigences, il est possible de débrider le logiciel à l'aide de paramètres dynamiques.

2 Accès aux certificats

2.1 CSP, CNG et PKCS#11 : quelles différences ?

La gestion des certificats sous Windows fait intervenir différents logiciels et normes pour leur stockage, que ce soit dans un magasin de certificats, sur un token ou sur une carte à puce.

Les certificats stockés sur des cartes à puce ou tokens sont généralement copiés dans le magasin de certificats de l'utilisateur actuel, lorsque la carte est insérée dans le lecteur ou que le token est connecté à l'ordinateur.

CSP, CNG et PKCS#11 sont des notions connexes qui font toutes appel à des interfaces de programmation d'application (API) pour la gestion des certificats, mais la technologie mise en œuvre est différente dans chaque cas.

2.1.1 CSP et KSP

Sous Windows, la gestion des certificats fait traditionnellement appel à des modules logiciels indépendants appelés fournisseurs de services cryptographiques ou *Cryptographic Service Providers* (CSP) en anglais. Les CSP servent notamment à exécuter des algorithmes pour l'authentification, l'encodage et le chiffrement.

Il existe désormais une nouvelle génération de ces modules logiciels indépendants appelés fournisseurs de stockage de clés ou *Key Storage Providers* (KSP) en anglais. Un KSP sert à créer, gérer, stocker et récupérer des clés privées.

2.1.2 CAPI et CNG

L'évolution des normes de sécurité a conduit Microsoft à rendre obsolète l'API associée aux CSP, appelée Cryptography API (CryptoAPI ou CAPI). Celle-ci a été remplacée par Cryptography API: Next Generation (CNG), dans laquelle les fournisseurs de services cryptographiques sont dissociés des fournisseurs de stockage de clés.

C'est pourquoi le Client VPN Windows Enterprise prend en charge les CSP jusqu'aux versions 6.8x et que seule l'API CNG est prise en charge par les versions 7.x. Pour ces dernières, il est donc nécessaire de s'assurer que le certificat est importé dans le magasin de certificats Windows avec la bonne bibliothèque (cf. section 2.2 Déterminer le type de conteneur d'un certificat ci-dessous).

2.1.3 Magasin machine et magasin utilisateur

Par ailleurs, il convient de savoir qu'il existe deux magasins de certificats sous Windows :

- le magasin machine, disponible pour tous les utilisateurs d'une machine, et
- le magasin utilisateur, uniquement disponible pour l'utilisateur actuel d'une machine.

Dans les lignes de commande, l'option `-user` de la commande `certutil` sert à spécifier le magasin utilisateur. Lorsqu'elle est omise, le magasin machine est utilisé par défaut.

2.1.4 PKCS#11

Enfin, en cryptographie, il existe des normes de cryptographie à clé publique ou *Public Key Cryptography Standards* (PKCS) en anglais. Il s'agit d'un ensemble de spécifications conçues par la société RSA Security.

La norme PKCS#11 fournit des applications avec une méthode d'accès aux périphériques matériels (cartes à puce ou tokens), indépendamment du type d'appareil. Elle comporte donc une API servant d'interface générique à un pilote de périphérique prenant en charge la norme PKCS#11. Cette API est prise en charge par les deux versions 6.8x et 7.x du Client VPN Windows Enterprise dès lors qu'un middleware correspondant est installé.

2.1.5 Synthèse

En résumé, il existe donc plusieurs types de middleware d'accès aux certificats stockés sur token, sur carte à puce et dans un magasin de certificats (`certmgr.msc`) :

- **CSP** pour **C**ryptographic **S**ervice **P**rovider (déprécié au profit de CNG) : pris en charge jusqu'à la version 6.8x.
- **CNG** pour **C**ryptography API: **N**ext **G**eneration : seule API prise en charge dans les versions 7.x. Dans le cas présent, il est nécessaire d'importer le certificat dans le magasin Windows avec la bonne bibliothèque.
- **PKCS#11** pour **P**ublic-**K**ey **C**ryptography **S**tandards : pris en charge par les deux versions 6.8x et 7.x.

2.2 Déterminer le type de conteneur d'un certificat

CSP et CNG sont des middlewares Microsoft. Sous Windows, les certificats sont stockés dans des conteneurs de type CNG ou de type CSP.

Pour connaître le conteneur des certificats dans le magasin de certificats, le token ou la carte à puce, vous pouvez lister les certificats contenus dans le magasin (utilisateur ou machine). Les informations retournées indiquent le type de fournisseur à partir duquel vous pouvez déduire le type de conteneur (CSP ou CNG). Ce dernier vous permet ensuite de déterminer la compatibilité du certificat avec votre version du Client VPN Windows Enterprise.

- Pour lister les certificats contenus dans le magasin utilisateur, exécutez la commande suivante :

```
certutil -verifystore -user My
```

- Pour lister les certificats contenus dans le magasin machine, exécutez la commande suivante :

```
certutil -verifystore My
```

À partir des informations retournées, vous pouvez déterminer le type de conteneur de la manière suivante. Si le fournisseur est :

- Microsoft Smart Card Key Storage Provider, le conteneur est de type CNG (compatible avec les versions 7.x) ;
- Microsoft Base Smart Card Crypto Provider, le conteneur est de type CSP (compatible avec les versions 6.8x).

Pour les certificats faisant appel au middleware PKCS#11, le type de conteneur est indifférent étant donné qu'il est compatible avec les deux versions du Client VPN Windows Enterprise.

2.3 Importer un certificat en fonction du type de magasin

Lors de l'importation de certificats utilisant le middleware CNG, il convient de spécifier le type de magasin utilisé (utilisateur ou machine) dans la ligne de commande. Ci-dessous, vous trouverez des exemples de ligne de commande avec les options à préciser.

- Magasin utilisateur :

```
certutil -csp KSP -user -importpfx CertFileName.p12
```

- Magasin machine :

```
certutil -csp KSP -importpfx CertFileName.p12
```

Dans les lignes de commande, l'option `-user` de la commande `certutil` sert à spécifier le magasin utilisateur. Lorsqu'elle est omise, le magasin machine est utilisé par défaut.

Depuis la version 7.4 du Client VPN Windows Enterprise, une option permet de sélectionner automatiquement le certificat utilisateur depuis un token /une carte à puce, le magasin de certificats Windows ou les deux (voir la section « Sélection automatique » au chapitre 18 du « Guide de l'administrateur ».

En vue d'offrir une granularité plus fine dans la configuration du choix de magasin de certificats à utiliser, depuis la version 7.5 du Client VPN Windows Enterprise, ce choix n'est plus opéré au niveau du poste, mais à celui du tunnel.

3 Format des certificats

À partir de la version 7 du Client VPN Windows Enterprise, le format des certificats doit respecter une taille de clé et un algorithme de hachage précis.

Obligatoire

- Longueur de clé (en bits) : dans le cas des certificats RSA, la taille doit être de 2048 ou plus
- Algorithme de prise d'empreinte (ou *digest algorithm*) : doit être SHA-256, SHA-384 ou SHA-512

Optionnel

La vérification de la CRL du certificat utilisateur.

3.1 Certificat passerelle

Partie Key Usage extension

- doit être présente,
- doit être marquée comme critique et
- ne doit contenir que les valeurs `digitalSignature` et/ou `nonRepudiation`.

☞ Si ce n'est pas le cas, référez-vous au paramètre dynamique `allow_server_extra_keyusage` décrit à la section « Contraintes relatives à l'extension Key Usage » au chapitre 18 du « Guide de l'administrateur ».

Conformément aux exigences de sécurité, la valeur `keyEncipherment` de l'extension Key Usage a été rendue obsolète et remplacée par la valeur `nonRepudiation`, qui est désormais acceptée par défaut. Cependant, la version 7.5 du Client VPN Windows Enterprise continue d'accepter la valeur `keyEncipherment` sans l'utilisation du paramètre dynamique `allow_extra_keyusage`.

Il est recommandé de préférer la valeur `nonRepudiation` de l'extension Key Usage à la valeur `keyEncipherment`.

Partie Extended Key Usage extension

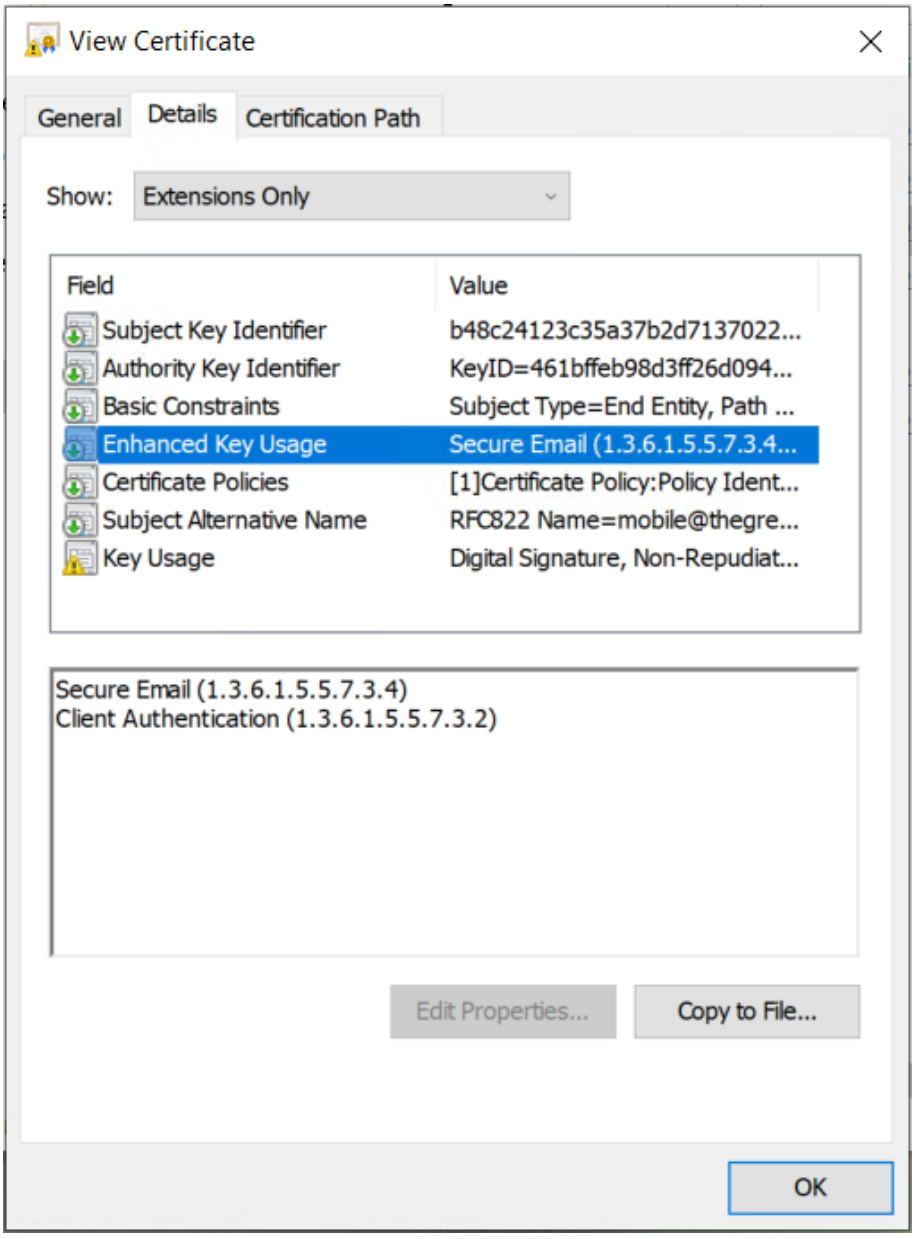
- peut être absente ou présente,
- si elle est présente, elle doit :
  - doit être marquée comme non-critique et
  - uniquement contenir les valeurs suivantes :
    - `id-kp-serverAuth` ou
    - `id-kp-serverAuth` + `id-kp-ipsecIKE`.

☞ Si ce n'est pas le cas, référez-vous au paramètre dynamique `allow_server_and_client_auth` décrit à la section « Contraintes relatives à l'extension Extended Key Usage » au chapitre 18 du « Guide de l'administrateur ».

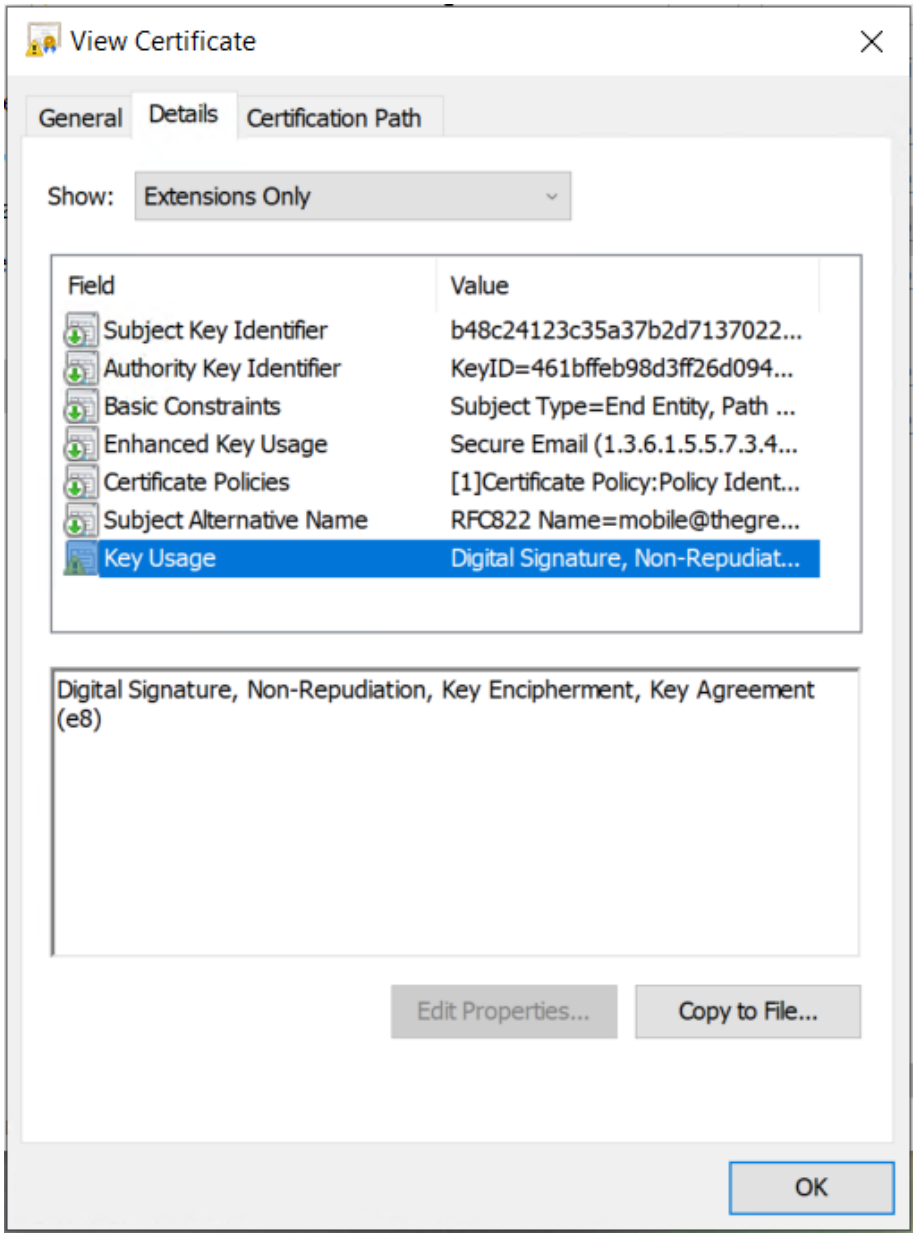
3.2 Exemple de certificat sous Windows

Dans une PKI Windows, voici la relation entre un certificat et les extensions :

- Extended Key Usage :



- Key Usage :


View Certificate
General
Details
Certification Path
Show:
Extensions Only
Field
Value
Subject Key Identifier
b48c24123c35a37b2d7137022...
Authority Key Identifier
KeyID=461bffeb98d3ff26d094...
Basic Constraints
Subject Type=End Entity, Path ...
Enhanced Key Usage
Secure Email (1.3.6.1.5.5.7.3.4...
Certificate Policies
[1]Certificate Policy:Policy Ident...
Subject Alternative Name
RFC822 Name=mobile@thegre...
Key Usage
Digital Signature, Non-Repudiat...
Digital Signature, Non-Repudiation, Key Encipherment, Key Agreement (e8)
Edit Properties...
Copy to File...
OK

3.3 Exemple de log d'un certificat

Les extensions sont présentes dans un log de certificat (fichier `tgbikeng.log`) :

```
20220826 17:20:23:953    Local0.Info          [11204]
X509v3 extensions
20220826 17:20:23:956    Local0.Info          [11204]
Basic constraints :
20220826 17:20:23:960    Local0.Info          [11204]
CA:FALSE
20220826 17:20:23:965    Local0.Info          [11204]
Netscape Certificate comment :
20220826 17:20:23:968    Local0.Info          [11204]
TheGreenBow PKI generated server certificate
20220826 17:20:23:971    Local0.Info          [11204]
Subject key identifier :
20220826 17:20:23:974    Local0.Info          [11204]
FB:D6:5A:EF:FE:1B:DC:68:90:66:B9:D7:47:45:EA:B5:86:97:4
A:B3
20220826 17:20:23:978    Local0.Info          [11204]
Authority key identifier :
20220826 17:20:23:981    Local0.Info          [11204]
keyIdentifier:
6F:6D:B8:A5:0B:EA:64:82:2E:B4:5F:0A:35:53:8B:80:05:4C:7
B:0E
20220826 17:20:23:984    Local0.Info          [11204]
authorityCertIssuer: C = FR, ST = Ile-de-France, L =
Paris, O = TheGreenBow, OU = QA40, CN = Root CA
20220826 17:20:23:988    Local0.Info          [11204]
authorityCertSerialNumber: 10:00
20220826 17:20:23:990    Local0.Info          [11204]
Key usage : critical
20220826 17:20:23:995    Local0.Info          [11204]
Digital signature
20220826 17:20:24:000    Local0.Info          [11204]
Extended key usage :
20220826 17:20:24:003    Local0.Info          [11204]
Server authentication
```

3.4 Certificat utilisateur

Dans le cas d'un certificat utilisateur, il peut il y avoir des avertissements, mais il n'est pas nécessaire de débrider le Client VPN. Les messages sont affichés dans la Console.

4 Méthode d'authentification

La version 7.5 du Client VPN Windows Enterprise prend en charge les méthodes d'authentification de certificat suivantes :

- Méthode 1 : signature numérique RSA avec SHA-2 [RFC 7296]
- Méthode 9 : ECDSA « secp256r1 » avec SHA-2 (256 bits) sur la courbe P-256 [RFC 4754]
- Méthode 10 : ECDSA « secp384r1 » avec SHA-2 (384 bits) sur la courbe P-384 [RFC 4754]
- Méthode 11 : ECDSA « secp521r1 » avec SHA-2 (512 bits) sur la courbe P-521 [RFC 4754]
- Méthode 14 : signature numérique RSASSA-PSS et RSASSA-PKCS1-v1_5 avec SHA-2 (256/384/512 bits) [RFC 7427]
- Méthode 214 : ECDSA « BrainpoolP256r1 » avec SHA-2 (256 bits) sur la courbe BrainpoolP256r1 (uniquement disponible avec des passerelles prenant en charge cette méthode)
- Fin de prise en charge de la Méthode 1 : RSA Digital Signature avec SHA-1 [RFC 7296]
- Refus des certificats RSA de taille inférieure à 2048 bits
- Vérification des Key Usage et Extended Key Usage des certificats
- La vérification de la CRL du certificat utilisateur est devenue optionnelle

Selon la version du Client VPN utilisé, les méthodes d'authentification par défaut sont différentes :

- Sur la version 6.87 : Méthode 1 (RSA Digital Signature)
- Sur la version 7.5 : Méthode 14 (RSA-PSS Digital Signature)

☞ Si ce n'est pas le cas, référez-vous au paramètre dynamique `Method14_RSASSA_PKCS1` décrit à la section « Méthodes d'authentification des certificats » au chapitre 29 du « Guide de l'administrateur » pour utiliser notamment du `RSASSA_PKCS1.5`.

5 Contact

5.1 Information

Toutes les informations sur les produits TheGreenBow sont disponibles sur le site : https://thegreenbow.com/.

5.2 Commercial

Contact téléphonique : +33.1.43.12.39.30

Contact mail : sales@thegreenbow.com

5.3 Support

Le site TheGreenBow propose plusieurs pages concernant le support technique des logiciels :

Aide en ligne

https://thegreenbow.com/fr/support/assistance/

FAQ

https://thegreenbow.com/fr/faq/

Formulaire de contact

Le support technique est accessible via un formulaire disponible sur le site TheGreenBow à l'adresse : https://thegreenbow.com/fr/support/assistance/support-technique/.

Vos connexions protégées
en toutes circonstances

28, rue Caumartin
75009 Paris — France

sales@thegreenbow.com

www.thegreenbow.com