Windows Enterprise VPN Client 7

Technical Note: Authentication and Certificate Format

Latest update: 22 January 2024
Document reference number: 20240122_TNC_VPE_7_EN_1.2

www.thegreenbow.com

Table of contents

Document revision history

Version	Date	Sections/pages concerned	Description of change	Author
1.0	2022-08-30	All	Initial draft	ALE, JLB, BB
1.1	2023-01-11	4	Updated reference to chapter in Administrator's Guide	FG, BB
1.2	2024-01-22	2.3, 3.1 & 4	Updated information to account for changes in v7.5	FG, BB

1 Introduction

Due to increased security requirements, deprecation of certain algorithms, and stricter rules for using certificates, version 7 of the Windows Enterprise VPN Client comes with certain restrictions on certificates.

Some of our customers have shared with us misunderstandings and difficulties they encountered when deploying version 7 of the Windows Enterprise VPN Client in combination with tokens and smart cards. For this reason, we thought it both useful and important to shed some light on some basic concepts pertaining to authentication and certificate format.

SHA, RSA, and ECDSA algorithms

Digital signatures generally involve two different types of algorithms:

- A hash algorithm (SHA: Secure Hash Algorithm)
- A signature algorithm (RSA: initials of the three inventors or ECDSA: Elliptic Curve Digital Signature Algorithm)

The strength of RSA encryption depends on the size of the key used. With every doubling of the key length, decryption is six to seven times slower.

According to the NIST and the ANSSI, the recommended minimum key size is 2048 bits.

Hash algorithms can be attacked in either of the following two ways:

- Hash collision
- Preimage

A collision occurs when two distinct files produce the same hash value, and it thus becomes possible to substitute one for the other.

Preimage consists in determining the value of a file from its hash value. A second preimage consists in starting out from the hash value to produce a value that is different from the one originally used with the hash function.

According to the ANSSI, the family of SHA-1 hash functions no longer complies with its general security reference system (RGS) and the SHA-2 family should therefore be used. The NIST similarly encourages US federal agencies to switch from SHA-1 to SHA-2.

The rules applied by the Windows Enterprise VPN Client follow NIST and ANSSI recommendations. However, if the implemented PKI does not meet these requirements, some of these restrictions can be removed from the software using dynamic parameters.

2 Accessing certificates

2.1 CSP, CNG, and PKCS#11: what are the differences?

Certificate management in Windows involves a variety of software and standards regardless of whether certificates are stored in a certificate store, on a token, or on a smart card.

Certificates stored on smart cards or tokens are usually copied to the current user's certificate store when the card is inserted into the reader or when the token is connected to the computer.

CSP, CNG, and PKCS#11 are related concepts that all use application programming interfaces (APIs) for certificate management, but the technology implemented is different in each case.

2.1.1 CSP and KSP

In Windows, certificate management traditionally uses independent software modules called Cryptographic Service Providers (CSPs). CSPs actually perform algorithms for authentication, encoding, and encryption.

Today, there is a new generation of independent software modules called Key Storage Providers (KSPs). A KSP is used to create, manage, store, and retrieve private keys.

2.1.2 CAPI and CNG

Changing security standards have led Microsoft to deprecate the API associated with CSPs, called Cryptography API (CryptoAPI or CAPI). It has now been replaced with Cryptography API: Next Generation (CNG), which separates cryptographic service providers from key storage providers.

For this reason, the Windows Enterprise VPN Client supports CSPs up to versions 6.8x and only supports the CNG API starting with versions 7.x. For the latter, you therefore need to ensure that the certificate is imported into the Windows Certificate Store with the correct library (see section 2.2 Determining a certificate's container type below).

2.1.3 Machine store and user store

It should also be noted that there are two certificate stores in Windows:

- The machine store that is available to all users of a machine
- The user store that is only available to the current user of a machine

In command lines, the `-user` option of the `certutil` command is used to specify the user store. When it is omitted, the machine store will be used by default.

2.1.4 PKCS#11

In cryptography, PKCS stands for Public Key Cryptography Standards. They are a set of specifications developed by RSA Security.

The PKCS#11 standard provides applications with a method of accessing hardware peripherals (smart cards or tokens), regardless of the type of device. It therefore includes an API serving as a generic interface for a device driver that supports the PKCS#11 standard. This API is supported both by versions 6.8x and 7.x of the Windows Enterprise VPN Client if a corresponding middleware is installed.

2.1.5 Summary

In summary, there are several types of middleware used to access certificates stored on tokens, on smart cards, and in certificate stores (`certmgr.msc`):

- **CSP** stands for **C**ryptographic **S**ervice **P**rovider (deprecated and replaced with CNG): supported up to versions 6.8x
- **CNG** stands for **C**ryptography API: **N**ext **G**eneration: only API supported in versions 7.x. In this case, you must import the certificate into the Windows store using the right library.
- **PKCS#11** stands for **P**ublic-**K**ey **C**ryptography **S**tandards: supported by both versions 6.8x and 7.x

2.2 Determining a certificate's container type

CSP and CNG are Microsoft middleware. In Windows, certificates are stored in containers of CNG or CSP type.

To find out the container used for certificates stored in the certificate store, on a token, or on a smart card, you can list the certificates contained in the (user or machine) store. The information returned specifies the type of supplier based on which you can infer the container type (CSP or CNG). The

latter will then allow you to determine whether the certificate is compatible with your version of the Windows Enterprise VPN Client.

- To list the certificates contained in the user store, run the following command:

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

- To list the certificates contained in the machine store, run the following command:

```
certutil -verifystore My
```

Based on the information returned, you can determine the container type as follows. If the supplier is:

- Microsoft Smart Card Key Storage Provider, the container is of CNG type (compatible with versions 7.x)
- Microsoft Base Smart Card Crypto Provider, the container is of CSP type (compatible with versions 6.8x)

For certificates using the PKCS#11 middleware, the container type is irrelevant since it is compatible with both versions of the Windows Enterprise VPN Client.

2.3 Importing a certificate depending on the store used

When importing certificates using the CNG middleware, the store used (user or machine store) must be specified in the command line. Below you will find examples of command lines with the options you need to specify.

- User store:

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

- Machine store:

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

In command lines, the `-user` option of the `certutil` command is used to specify the user store. When it iso mitted, the machine store will be used by default.

As of version 7.4 of the Windows Enterprise VPN Client, an option can be used to automatically select the user certificate from a token/smart card, the Windows certificate store, or both (see the section entitled “Automatic selection” in chapter 18 of the “Administrator’s Guide”.

To offer finer granularity in how the choice of certificate store to use is configured, as of version 7.5 of the Windows Enterprise VPN Client, this choice is no longer made at the workstation level, but at the tunnel level.

3 Certificate format

As of version 7 of the Windows Enterprise VPN Client, certificates must be in a format that conforms to a specific key size and hash algorithm.

Mandatory

- Key length: must be at least 2048 bits for RSA certificates
- Digest algorithm: must be SHA-256, SHA-384, or SHA-512

Optional

CRL checking for user certificates

3.1 Gateway certificate

Key Usage extension part

- Must be present
- Must be marked as critical, and
- Must only contain the values `digitalSignature` and/or `nonRepudiation`

☞ If this is not the case, refer to the dynamic parameter `allow_server_extra_keyusage` described in the section “Constraints on the Key Usage extension” in chapter 18 of the “Administrator's Guide”.

In accordance with security requirements, the `keyEncipherment` value of the Key Usage extension has been deprecated and replaced with the `nonRepudiation` value, which is now accepted by default. However, version 7.5 of the Windows Enterprise VPN Client continues to accept the `keyEncipherment` value without needing to use dynamic parameter `allow extra keyusage`.

We recommend that you give preference to the `nonRepudiation` value over the `keyEncipherment` value of the Key Usage extension.

Extended Key Usage extension part

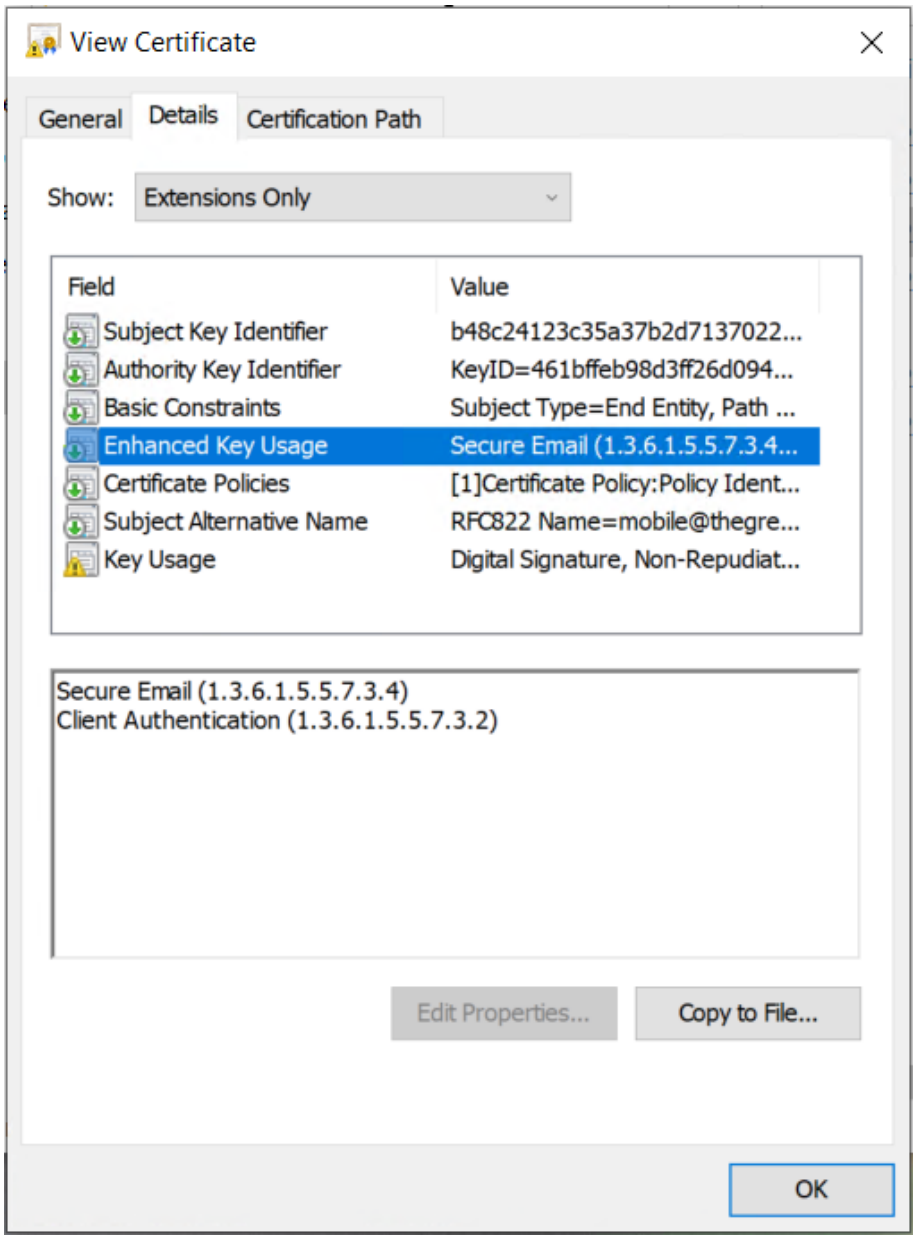
- Can be present or not
- If it is present, it must:
  - Be marked as non-critical, and
  - Only contain either of the following values
    - `id-kp-serverAuth` or
    - `id-kp-serverAuth` and `id-kp-ipsecIKE`

☞ If this is not the case, refer to the dynamic parameter `allow_server_and_client_auth` described in the section “Constraints on the Extended Key Usage extension” in chapter 18 of the “Administrator's Guide”.

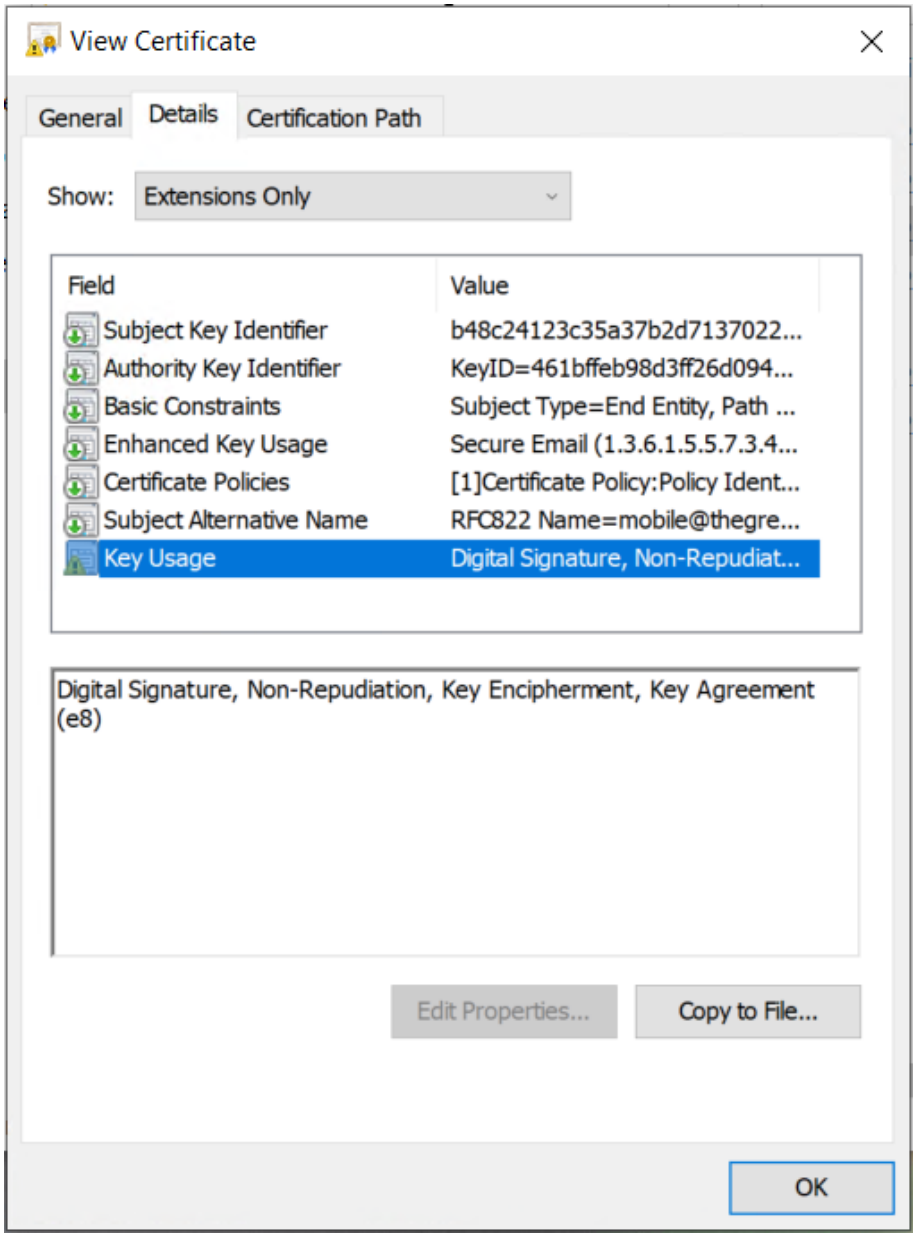
3.2 Example of a certificate in Windows

In a Windows PKI, the following is the relationship between a certificate and its 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 Example of a certificate log

The extensions are included in a certificate log (file named `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 User certificate

Warning messages may be displayed in the Console for a user certificate, but you do not need to remove any restrictions from the VPN Client.

4 Authentication method

Version 7.5 of the Windows Enterprise VPN Client supports the following certificate authentication methods:

- Method 1: RSA Digital Signature with SHA-2 [RFC 7296]
- Method 9: ECDSA “secp256r1” with SHA-2 (256 bits) on the P-256 curve [RFC 4754]
- Method 10: ECDSA “secp384r1” with SHA-2 (384 bits) on the P-384 curve [RFC 4754]
- Method 11: ECDSA “secp521r1” with SHA-2 (512 bits) on the P-521 curve [RFC 4754]
- Method 14: Digital Signature RSASSA-PSS, RSASSA-PKCS1-v1_5, and Brainpool with SHA-2 (256/384/512 bits) [RFC 7427]
- Method 214: ECDSA “BrainpoolP256r1” with SHA-2 (256 bits) on the BrainpoolP256r1 curve (only available with gateways that support this method)
- End of support for Method 1: RSA Digital Signature with SHA-1 [RFC 7296]
- RSA certificates with less than 2048-bit key length are rejected
- Key Usage and Extended Key Usage of certificates is verified
- Verification of the user certificate CRL has become optional

The default authentication methods are different depending on the version of the VPN Client used:

- Version 6.87: Method 1 (RSA Digital Signature)
- Version 7.5: Method 14 (RSA-PSS Digital Signature)

☞ If this is not the case, refer to the dynamic parameter `Method14_RSASSA_PKCS1` described in the section “Certificate authentication methods” in chapter 29 of the “Administrator's Guide,” among others to use `RSASSA_PKCS1.5`.

5 Contact

5.1 Information

All the information on TheGreenBow products is available on our website: https://thegreenbow.com/.

5.2 Sales

Phone: +33.1.43.12.39.30

E-mail: sales@thegreenbow.com

5.3 Support

There are several pages related to the software's technical support on our website:

Online help

https://www.thegreenbow.com/en/support/online-support/

FAQ

https://www.thegreenbow.com/en/frequently-asked-questions/

Contact form

Technical support can be reached using the form on our website at the following address: https://www.thegreenbow.com/en/support/online-support/technical-support/.

Protect your connections
in any situation

28, rue Caumartin
75009 Paris – France

sales@thegreenbow.com

www.thegreenbow.com