NETASQ IPSEC VPN CLIENT

DEPLOYMENT GUIDE

PKI OPTIONS

Site Web : http://www.netasq.com
Contact : support@netasq.com

Référence : naengde_vpn_client-version-5.5_pki
Décembre 2012 (Mise à jour)

Table of Content

1. Introduction

This document describes how to take advantage of new settings introduced in TheGreenBow IPSec VPN Client. These settings allow configuring how to select Certificates from token and smart card readers, and how Certificates are used by the software.

This document is intended to administrator software. It describes the parameters "Options PKI", how to use them, and how to implement them.

These settings are grouped under the term "PKI Options" and are configurable:

- In an initialization file used by the software installation: VpnSetup.ini
- In an initialization file used by the software once installed: VpnConf.ini
- Via the software installation command line options.

These parameters "PKI Options" are also fully configurable via the Configuration Panel of the VPN Client software, as described in "Managing Certificates (PKI Options)" from the " NETASQ VPN Client User's Guide".

This document is an extension of the ‘Deployment Guide’ (i.e. ‘naengde_vpn_client-version-5.5_deployment.pdf’) available on http://vpn.netasq.com.

2. PKI Options Parameters

The PKI Options parameters allow the user to define several rules that need to be considered by NETASQ VPN Client software:

- Rules to select a token or smart card: see "*SmartCardRoaming*" and "*PKC11Only*"
- Rules to select a Certificate from tokens or smart cards: see "*SmartCardRoaming*" et "*KeyUsage*"
- Rules to use Root Certificates: see "*NoCACertReq*"
- Rules to check Certificates from the VPN Gateway: see "*PkiCheck*"

2.1. SmartCardRoaming

The parameter SmartCardRoaming enables to set the rules that need to be considered by NETASQ VPN Client software to select a Certificate from tokens or smart cards. It is used to automate deployment of software in environment with a mix of heterogeneous tokens and smart cards.

Here are the possibilities for "*SmartCardRoaming*":

Card Reader to be selected	Certificat to be selected	SmartCardRoaming
Card reader set into the VPN Configuration	Certificate with subject as set into the VPN Configuration	not set
	Any Certificate	"01"
Card reader set into the section [ROAMING] of vpnconf.ini	Certificate with subject as set into the VPN Configuration	"02"
	Any Certificate	"03"
First card reader plugged in, found, containing a smartcard	Certificate with subject as set into the VPN Configuration	"04"
	Any Certificate	"05"

2.2. KeyUsage

The parameter KeyUsage parameter forces NETASQ VPN Client to select only 'Authentication' certificate types, meaning the certificates whose 'Key Usage' contains 'Digital Signature'.

Here are the possibilities for "*KeyUsage*":

Certificate to be selected	KeyUsage
Type of Certificate not checked.	not set
Limit access only to 'Authentication' certificates from the Token or SmartCard.	"01"

2.3. NoCACertReq

When a VPN client and a VPN gateway use certificates from different Certificate Authorities (i.e. derived from different intermediate CAs but under the same root certification authority), it is necessary to adapt IKE protocol.

In this case, the parameter "*NoCACertReq*" must be set as follow:

Condition	NoCACertReq
Allow a Certificate from the VPN Gateway with different Certificate Authority.	"01"

2.4. PkiCheck

The parameter PkiCheck parameter forces the VPN Client to check the Certificate Root Authority when receiving a Certificate from the VPN gateway. This requires to import the Root Certificate and all Certificates in the certification chain into the Windows Certificate store.

The VPN Client will use the CRL (Certificate Revocation List) of the various certification authorities. If these CRL are absent from the certificate store or if these CRL are not downloadable while opening the VPN tunnel, the VPN Client won't be able to validate the certificate of the gateway.

Checking each element of the chain means:

- Expiration date of the certificate
- Checking the signatures of all certificates of the certificate chain (including root certificate, intermediate certificates and the server certificate)
- Updating CRL of all certificate issuers in the chain of certification by doing the following:
  - Recovery of all CRL Distribution Points (i.e. CDP) from the certificate to be checked and other certificates,
  - Downloading the CRL on different Distribution Points available,
  - Checking the expiration date of the CRL,
  - Checking the signature of the CRL with the public key of issuer certificate,
  - Importing the CRL into the certificate store,
- Checking of the absence of certificate revocation in the corresponding CRLs.

Here are the possibilities for "*PkiCheck* ":

Condition	PkiCheck
Certificate from the VPN gateway not checked.	not set
Force to check the Certificate Root Authority when receiving a Certificate from VPN gateway.	"01"

2.5. PKCS11Only

By default, NETASQ VPN Client uses the CSP type of middleware to access to tokens or smart cards. The parameter PKCS11Only forces NETASQ VPN Client to use the PKCS#11 type of middleware.

NOTE :
When accessing the Windows Certificate Store, TheGreenBow IPsec VPN Client always uses the CSP type of middleware.

Here are the possibilities for "*PKCS11Only*":

Middleware type to be used	PKCS11Only
CSP type of middleware. Default.	not set
Force using only 'PKCS#11' type of middleware to access Token or SmartCard.	"01"

3. VpnSetup.ini File

3.1. Purpose

The VpnSetup.ini file allows you to configure NETASQ VPN Client software installation.
It must be located in the same directory as the executable installation: Vpnclient_setup.exe.

NOTE :
The file VpnSetup.ini is an editable text file with notepad for example.

3.2. Syntax

This file consists of several sections, tags and values:

- [PKIOptions] section set how to select Certificates from token and smart card readers, and how Certificates are used by the software.

3.2.1. PKIOptions Section

It allows you to set the rules that need to be considered by NETASQ VPN Client software to select a Certificate from tokens or smart cards.

This section must be unique and is optional.

KeyUsage	01 to limit access only to 'Authentication' certificates from the Token or SmartCard.
SmartCardRoaming	xx being the rule used to fetch a Certificate from the Token or SmartCard.
PKCS11Only	01 to force using only to 'PKCS#11' middleware to access Token or SmartCard. Default = CSP type.
NoCaCertReq	01 to allow a Certificate with different Certificate Authority the VPN Gateway is using.
PkiCheck	01 to force the VPN Client to check the Certificate Root Authority when receiving a Certificate from the VPN gateway.

NOTE:
PkiCheck, NoCACertReq, KeyUsage and PKCS11Only must be set to "01" or not provided.

NOTE:
SmartCardRoaming must be set to "01", "02", "03", "04", "05" or not provided.

Example:

```
[PKIOptions]

PkiCheck=01

SmartCardRoaming=01

NoCACertReq=01

KeyUsage=01

PKCS11Only=01
```

4. vpnConf.ini File

4.1. Purpose

The VpnConf.ini file is taken into account when TheGreenBow IPSec VPN Client software starts. It must be located in the installation directory of the software (eg: "C:\Program Files\Netasq\VPN Client").

The vpnConf.ini file allows to setup few parameters related to the software installation or specific hardware environment e.g. smartcard reader middleware.

NETASQ VPN Client recognizes the smartcards or USB tokens of the leading manufacturers (Gemalto, Oberthur, Schlumberger, Aladdin, SafeNet, Feitian, etc ...). The cards are automatically recognized based on their 'ATR' and NETASQ VPN Client will use the associated CSP middleware or the pre-registered PKCS#11 middleware.

However, administrators have the ability to specify their own cards and the paths to custom middleware by adding a vpnconf.ini file.

NOTE:
The file VpnSetup.ini is an editable text file with notepad for example.

4.2. Syntax

This file consists of several sections, tags and values:

- [ROAMING] section specifies the card reader or Token that shall be used.
- [ATR] section defines Tokens that are not yet known by NETASQ VPN Client.

Here is an example:

```
[ROAMING]

SmartCardReader="Reader Name"

SmartCardMiddleware="middleware.dll"

SmartCardMiddlewareType="PKCS#11"

SmartCardMiddlewareRegistry="KEY_LOCAL_MACHINE:SOFTWARE\\Compa
nyName\\ProductName\\CK:PKCS#11DLL"
```

```
SmartCardMiddelwarePath=”c:\path\to\middleware\mdlw.dll”


// New Token description#1

[3B:0F:52:4E:42:4F:24:00:23:00:00:00:00:00:00:01]

mask="FF:FF:FF:FF:FF:FF:FF:00:FF:00:00:FF:FF:00:00:00:FF"

scname="Card Name"

manufacturer="Company Name"

pkcs11DllName="mdlw.dll"

registry="KEY_LOCAL_MACHINE:SOFTWARE\\CompanyName\\ProductName
\\CK:PKCS#11DLL"
```

4.2.1. ROAMING Section

It allows you to specify the smartcard reader or USB Token that shall be used to open the tunnel.

This section must be unique and is optional.

SmartCardReader:	Name of card reader to use to access the Token.
SmartCardMiddleware:	DLL file used to communicate with the Token.
SmartCardMiddlewareType:	PKCS#11
SmartCardMiddelwarePath:	Path to the middleware including the name of the middleware.
SmartCardMiddlewareRegistry:	Name of the key in the registry containing the path to the middleware.

NOTE :

- The information from the section ROAMING overrides the information from the VPN Configuration.
- This section will be taken into account only if the parameter SmartCardRoaming is "02" or "03", and PKCS11Only is set in vpnSetup.ini file.
- Either SmartCardMiddlewareRegistry or SmartCardMiddelwarePath must be provided.
- Registry parameters structure: PRIMARY_KEY:path\\toward\\the\\key\\specific:value
- PKCS#11 type is the only supported value for SmartCardMiddlewareType.

Example:

```
[ROAMING]

SmartCardReader="Axalto reader"

SmartCardMiddleware="middleware.dll"

SmartCardMiddlewareType="PKCS#11"

SmartCardMiddelwarePath="c:\path\to\middleware\mdlw.dll"

SmartCardMiddlewareRegistry="HKEY_LOCAL_MACHINE:SOFTWARE\\Axal
to\\Access\\CK:PKCS#11DLL"
```

4.2.2. ATR Section

It allows you to specify the Token attributes.
This section must be multiple and is optional.

[**ATR#**]:	token id
mask:	mask for this ATR
scname:	name of the token.
manufacturer:	manufacturer's name.
pkcs11DllName:	pkcs11 dll name.
registry:	name of the key in registry indicating the path to the middleware (optional)
DllPath:	path to the PKCS # 11 DLL

NOTE :

- Either 'registry' or 'DllPath' must be provided.
- Registry parameters structure:
  PRIMARY_KEY:path\\toward\\the\\key\\specific:value

Example:

```
[3B:0F:52:4E:42:4F:24:00:23:00:00:00:00:00:00:01]

mask="FF:FF:FF:FF:FF:FF:FF:00:FF:00:00:FF:FF:00:00:00:FF"

scname="Access"

manufacturer="Axalto"

pkcs11DllName="mdlw.dll"

registry="KEY_LOCAL_MACHINE:SOFTWARE\\Axalto\\Access\\CK:PKCS#11DLL"
```

5. PKI Options Setup Command Lines

Some of the PKI Options parameters can be configured via VPN Client setup command lines:

- Pkicheck (equivalent to the PkiCheck parameter in the VpnSetup.ini file)
- smartcardroaming (equivalent to the SmartCardRoaming parameter in the VpnSetup.ini file)

NOTE :

- Command-line options that require a parameter must be specified with no space between the option and its parameter. Quotation marks around an option's parameter are required only if the parameter contains spaces.
- The parameters specified in the file VpnSetup.ini overrides the parameters passed via the command line.

5.1.1. --pkicheck

Syntax: `--pkicheck=1`

Usage: Force the VPN Client to check the Certificate Root Authority when receiving a Certification from the VPN gateway. This parameter is either set to 1 or not set at all.

Example: `Vpnclient_setup.exe /S --pkicheck=1`

5.1.2. -- smartcardroaming

Syntax: `-- smartcardroaming=1`

Usage: Enable to set the rules that need to be considered by NETASQ VPN Client software to select a Certificate from tokens or smart cards. It is used to automate deployment of software in environment with a mix of heterogeneous tokens and smart cards. This parameter is either set to 1, 2, 3, 4, 5 or not set at all.

Example: `Vpnclient_setup.exe /S -- smartcardroaming=1`

6. Support

Information and update are available at: vpn.netasq.com

Technical support via email at: support@netasq.com

Sales via email at: sales@thegreenbow.com