TheGreenBow VPN Client

Token Configuration Guide
HID ActivKey SIM

Written by: **TheGreenBow Engineering Team**
Company: **www.thegreenbow.com**

Website: **www.thegreenbow.com**
Contact: **support@thegreenbow.com**

Table of Contents

1 Introduction

TheGreenBow VPN Client can take into account automatically a wide range of tokens or smartcards.
The list of qualified and supported token with TheGreenBow VPN Client is available at:
http://www.thegreenbow.com/vpn/vpn_token.html

TheGreenBow VPN Client also allows the use of token which are not automatically recognized by the software.
These new tokens just have to be configured in a configuration file called "vpnconf.ini".
The "vpnconf.ini" configuration file must be located in the software installation directory.

For further information about the way the token can be configured with TheGreenBow VPN Client, see also
our Token Configuration Guide available at **http://www.thegreenbow.com/vpn/vpn_token.html**

This document describes how to configure TheGreenBow VPN Client to use a **HID ActivKey SIM** token.

2 General terminology (CSP, PKCS11, ATR)

Two modes of access to tokens are defined: CSP and PKCS11.

CSP is the "Cryptographic Service Provider" provided by Microsoft Windows. This mode doesn't require
additional configuration steps in the VPN Client. However not all the tokens support that mode.

PKCS11 is standardized API to access token. This mode requires a PKCS11 DLL provided by the manufacturer
and this DLL has to be configured in the VPN Client. Usually all tokens are supposed to be PKCS11 compatible
and the manufacturer provides the DLL through a middleware package to be installed on the computer.

ATR means "Answer To Reset" but is actually a specific identifier returned by any token or smartcard. When
the ATR is known by the VPN client, the PKCS11 DLL doesn't have to be configured. When the ATR is not
known by the VPN client, a vpnconf.ini file is required to use the token or smartcard.
If the ATR is known and a VpnConf.ini file is present anyway, the VpnConf.ini file information is used (this is
useful to have the VPN Client using a specific PKCS11 dll).

3 CSP Compatibility

This token can work in CSP mode beginning with VPN 6.5x releases for Windows 7 & 10. For previous releases,
a vpnconf.ini file must be created.
For Windows 10, the CSP software is installed automatically by Windows when the hardware is inserted, and
there is nothing else to configure to use the token.
For Windows 7, it may be required to install the software from the manufacturer (usually "ActivIdentity Device
Installer x64 x.y.msi" and "ActivClient x64 x.y.z.msi").

4 PKCS11 Compatibility

This token can work in PKCS11 mode beginning with VPN Client 6.5x. Therefore it is compatible with Windows
XP,7 & 10 in that mode. It is required to install the PKCS11 middleware provided by the manufacturer (usually
"ActivIdentity Device Installer x64 x.y.msi" and "ActivClient x64 x.y.z.msi").
For previous releases, a vpnconf.ini file must be created.

5   "vpnconf.ini" file configuration

In case you need to specify a vpnconf.ini here is a template for that token:

```
[3B:DF:96:FF:81:31:FE:45:5A:01:80:48:49:44:43:31:31:58:58:73:00:01:1B:09]
mask="FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF"
scname="ActivKey SIM"
manufacturer="HID Global"
pkcs11DllName="acpkcs211.dll"
dllpath="C:\Program Files (x86)\ActivIdentity\ActivClient\acpkcs211.dll"
```

For CSP mode, you don't have to specify pkcs11DllName nor dllpath. This is only for Pkcs11 mode.

If it doesn't work in Pkcs11 mode, please check the DLL file exists in the specified location. If it doesn't exist, it means the PKCS#11 middleware from the manufacturer is not installed, or it is installed but the DLL filename has changed. Then the manufacturer has to be contacted to get the new pkcs11 DLL to be used with that smartcard.

If the DLL exists and the token is not recognized, then you need to check the ATR string reported by the token (it could have changed if it is a brand-new one). To do that, enable the logs in VPNConf (with CTRL-ALT-T), quit/restart VpnConf, and open the certificate tab for the tunnel. Then open "C:\ProgramData\TheGreenBow\TheGreenBow VPN\LogFiles\VpnDbg.log" and look for "ATR found:" in the log file.
Beginning with 6.5x release, the console window also contains information when an ATR is not known.

6   Contacts

News and updates on TheGreenBow web site: **www.thegreenbow.com**

Technical support by email at: **support@thegreenbow.com**

Sales contacts by email at: **sales@thegreenbow.com**

Secure, Strong, Simple
TheGreenBow Security Software