BerryRemote 1.00 Installation Instructions

For external employees

Doc.Version 1.00

29.07.2014

FIIN1 dept.

Contents

1. Introduction

Target group of the application are external users. This document describes the installation and setup of the standard parameters for Remote access client “BerryRemote” to connect to the Network of Boge Elastmetall GmbH and if necessary also to the ZF Network via “ZF Net Remote” with additional links.

Operation, expanded configuration, and troubleshooting are explained in the current operating instructions.

1.1. Comment

Attention: The software must be installed "as administrator"!
Other VPN-Clients must be de-installed prior to the installation.
Previous program versions must be de-installed prior to the installation.
The computer must be restarted after the installation.

1.2. Possible installation versions

The software clients are compatible with Windows 7 32/64 (SP1).

Windows 7 32/64 bit (SP1)

Junos Pulse 32 / 64bit

RSA 32 / 64bit

1.3. Installation file

The software is the same for all domains.
The respective current version of the software is provided with the packet request. Please copy the file below and unzip to e.g. c:\Ablage

>>> BerryRemote_V1.01_Externs.zip

Comment:
These instructions and its screenshots were created using a 64bit WIN7 system.

1.3.1. Softwareversion

- Junos Pulse 5.0.4.1.44471
- RSA SecureID Token 4.1.1.836

1.4. Hardware requirements for 32 + 64 bit operating systems

- Minimum 1 GB with Windows XP; 2GB with Windows 7
- Minimum 1 GHz CPU
- Minimum 4 GB available hard drive space

2. Junos Pulse Client

SSL VPN client for dialing into the Telekom ZF-Juniper-SSL system

<u>Software and setup files</u>

32 bit Systeme:	j-pulse-win-5.0r4.1-b47117-32bitinstaller.msi
64 bit Systeme:	j-pulse-win-5.0r4.1-b47117-64bitinstaller.msi
32+64 bit systems:	ZFNR_Berry.jnprpreconfig

A ready-to-install Junos Pulse client must be installed via CMD command lines for embedding the prepared configuration file[1)] and parameterization[2)], see following information.
Prior to this, the required files: Junos Pulse, MS-Installer (respective operating system), and Junos configuration should have been placed in the corresponding directory (here, for example, c:\Ablage).

2.1. Installation using command lines

Open a command line via the Start → Run menu. Then enter the CMD command. In the open command line, enter one of the following commands, depending on the operating system.

<u>WIN 7 64</u>[3]

```
msiexec /i C:\Ablage\j-pulse-win-5.0r4.1-b47117-64bitinstaller.msi
CONFIGFILE=C:\Ablage\ZFNR_Berry.jnprpreconfig ADDLOCAL=PulseSA /qb
```

<u>WIN 7 32</u>[3]

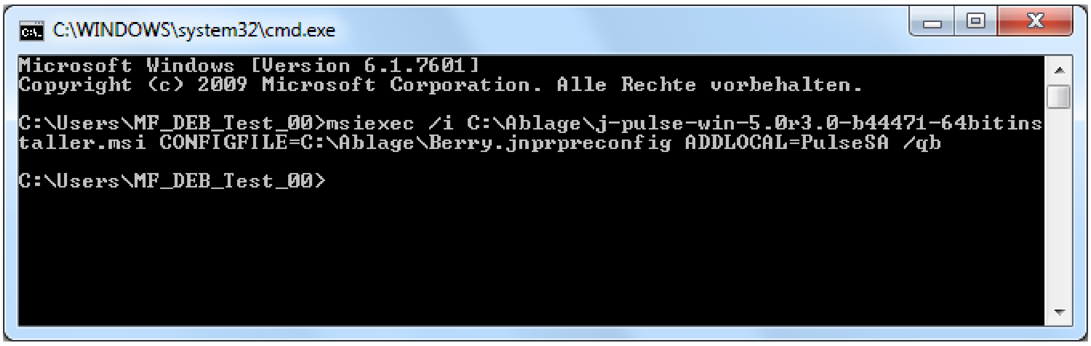
```
msiexec /i C:\Ablage\j-pulse-win-5.0r4.1-b47117-32bitinstaller.msi
CONFIGFILE=C:\Ablage\ZFNR_Berry.jnprpreconfig ADDLOCAL=PulseSA /qb
```

[1)] ZFNR_Berry.jnprpreconfig EMEA/AMERICA/APA dialing profiles

[2)] ADDLOCAL=PulseSA /qb Connection window view reduced to dialing profiles

[3)] To avoid typos an additional bat-file “Berry_Externs.bat” is included in the zip file to install the Junos Pulse. Please start this file instead of the above CMD- line entry.

2.2. Installation with ADDLOCAL – install. parameter



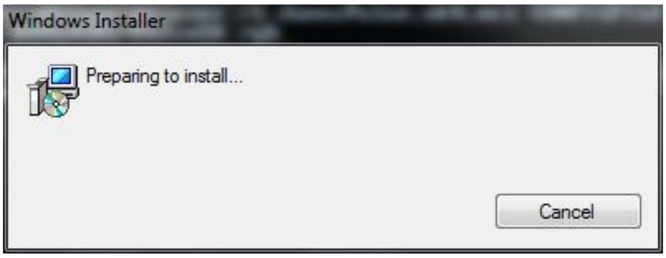
C:\WINDOWS\system32\cmd.exe

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\MF_DEB_Test_00>msiexec /i C:\Ablage\j-pulse-win-5.0r3.0-b44471-64bitins
taller.msi CONFIGFILE=C:\Ablage\Berry.jnprpreconfig ADDLOCAL=PulseSA /qb

C:\Users\MF_DEB_Test_00>
```

2.3. Start of the Junos Pulse installation

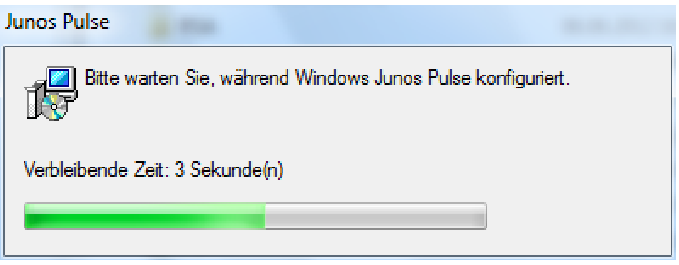


Windows Installer

Preparing to install...

2.4. User Account Control

Installation begins after switch to admin context



Junos Pulse

Bitte warten Sie, während Windows Junos Pulse konfiguriert.

Verbleibende Zeit: 3 Sekunde(n)

NOTE:
During the installation, the Ethernet connection is temporarily disrupted due to the installation and the incorporation of a virtual network adapter, in order to integrate the virtual network adapter!!!

2.5. Junos Pulse: Deactivate program start

Reason for deactivation: The Junos Pulse client exists in the current version and an auto-update is not required. Later updates are effected by means of manual subsequent installations.

Remove following entry in the auto-run registration of the Windows registration:

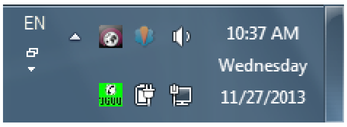
For 64 bit systems:
[Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run] Junos Pulse = C:\Program Files (x86)\Common Files\Juniper Networks\JamUI\Pulse.exe -tray

For 32 bit systems:
[Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] JunosPulse=C:\Program Files\Common Files\Juniper Networks\JamUI\Pulse.exe -tray

Background: The Junos Pulse would occupy the SysTray already at Windows start, which is not desired and impedes operation.

2.6. Deactivation and restart of Junos Pulse

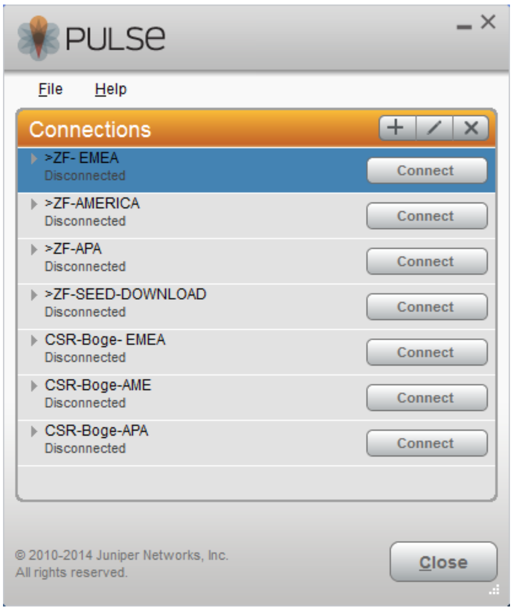
After the installation the Junos Pulse client is active in the tray bar. After Windows reboot the Junos Pulse client does not start automatically and cannot launched from tray bar in this state.



The Junos Pulse client can now be opened for initializing the first VPN-client connection by using the corresponding program icon under start → programs → Junos Pulse.

2.7. Junos connection window view with the dialing profiles

- Three BerryRemote (CSR-Boge) and
- Four ZF Net Remote dialing profiles



PULSE

File Help

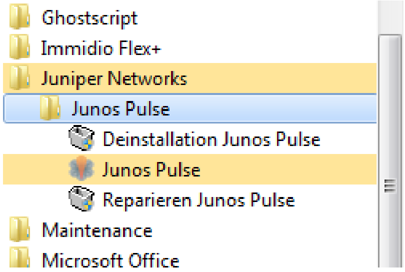
Connections

>ZF- EMEA Disconnected	Connect
>ZF-AMERICA Disconnected	Connect
>ZF-APA Disconnected	Connect
>ZF-SEED-DOWNLOAD Disconnected	Connect
CSR-Boge- EMEA Disconnected	Connect
CSR-Boge-AME Disconnected	Connect
CSR-Boge-APA Disconnected	Connect

© 2010-2014 Juniper Networks, Inc.
All rights reserved.

Close

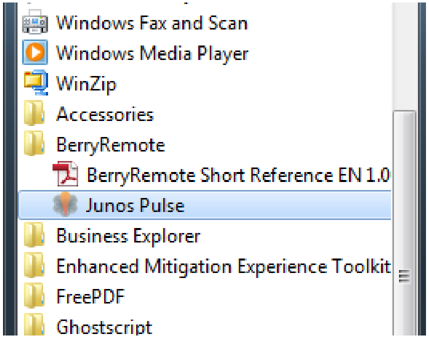
2.8. Program list after installation and reorganisation



- Ghostscript
- Immidio Flex+
- Juniper Networks
  - Junos Pulse
    - Deinstallation Junos Pulse
    - Junos Pulse
    - Reparieren Junos Pulse
- Maintenance
- Microsoft Office

- Create a folder named “BerryRemote” in All Programs
- Copy the Link “Junos Pulse” to the folder
- Copy the “ZF Net Remote Berry Short Reference EN 1.00.pdf” from c:\Ablage to the folder
- Delete folder “Junos Pulse” with all files

Similar view with different pdf name:



- Windows Fax and Scan
- Windows Media Player
- WinZip
- Accessories
- BerryRemote
  - BerryRemote Short Reference EN 1.0
  - Junos Pulse
- Business Explorer
- Enhanced Mitigation Experience Toolkit
- FreePDF
- Ghostscript

2.9. Completion of the installation

The computer must be rebooted once after completion of the installation.

2.10. Important configuration settings

The following registry keys are added by installing the .Reg files in the Windows registry. To install Admin rights are required. In general, a double-click on the file is sufficient to enter the registration key.

Operating System	.reg file
WIN 7 64	-

2.11. Junos Pulse Client uninstallation

To uninstall administrator rights are required. The uninstallation via the Control Panel is necessary even when a software update or a reinstall is necessary.

The computer must be rebooted once after completion of the uninstallation.

3. RSA – Client (SecurID token software)

The RSA Client software is need if you need access to ZF Friedrichshafen AG (ZF).

The "SecurID Token" program saves and manages the soft token. The soft token is required for 2-factor SSL VPN authentication to access to the ZF Network. In order to initialize the token, a seed file is needed, which is securely saved in the RSA client and personalizes this application by tying it to the user.
The automation version of the "SecurID Token" software is installed, i.e. the currently generated token can be prompted and accepted during login by the "Junos Pulse SSL VPN client" via a corresponding application interface.

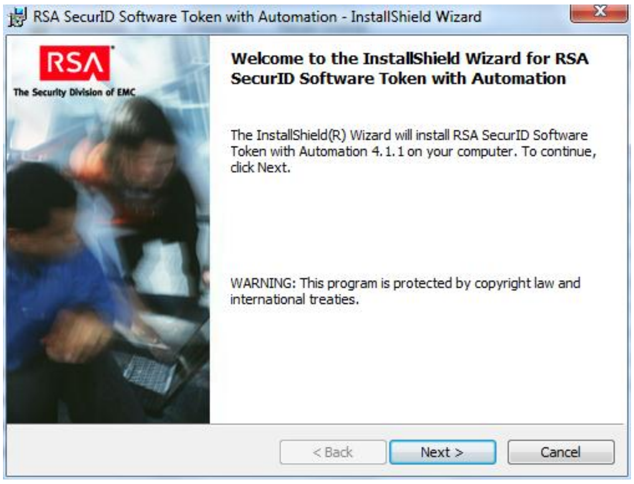
Software and setup files

32+64 bit systems:	RSASecurIDTokenAuto411.msi

3.1. "RSA SecurID" – installation

NOTE: Installation of the RSA SecurID client is executed in admin context!
Before installation please uninstall old software versions (Refer chapter 3.9).

Installation start of the automation version.

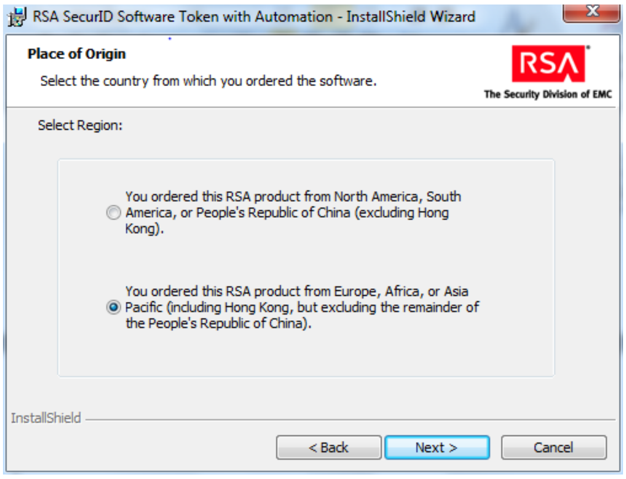

RSA SecurID Software Token with Automation - InstallShield Wizard

Welcome to the InstallShield Wizard for RSA SecurID Software Token with Automation

The InstallShield(R) Wizard will install RSA SecurID Software Token with Automation 4.1.1 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

3.2. Selection of order region



RSA SecurID Software Token with Automation - InstallShield Wizard
RSA
The Security Division of EMC
InstallShield
< Back
Next >
Cancel

Place of Origin

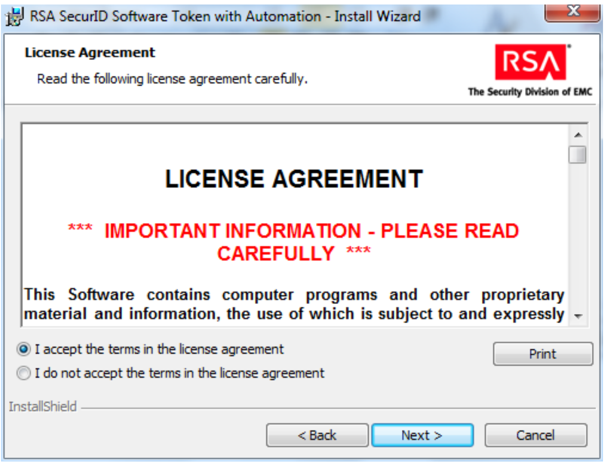
Select the country from which you ordered the software.

Select Region:

○ You ordered this RSA product from North America, South America, or People's Republic of China (excluding Hong Kong).

● You ordered this RSA product from Europe, Africa, or Asia Pacific (including Hong Kong, but excluding the remainder of the People's Republic of China).

3.3. Confirmation of license agreement



RSA SecurID Software Token with Automation - Install Wizard
RSA
The Security Division of EMC
Print
InstallShield
< Back
Next >
Cancel

License Agreement

Read the following license agreement carefully.

LICENSE AGREEMENT

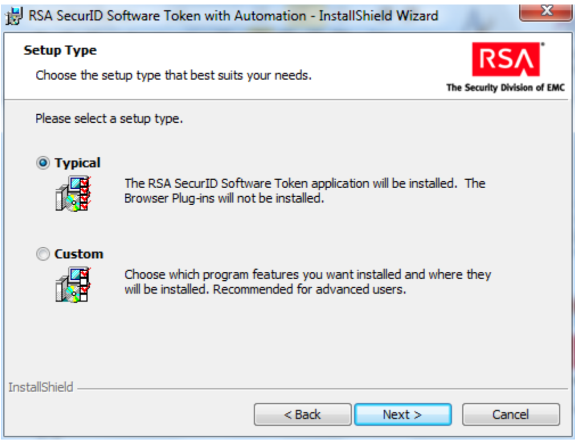
*** IMPORTANT INFORMATION - PLEASE READ CAREFULLY ***

This Software contains computer programs and other proprietary material and information, the use of which is subject to and expressly

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

3.4. Confirmation of the standard installation



RSA SecurID Software Token with Automation - InstallShield Wizard
RSA
The Security Division of EMC
InstallShield
< Back
Next >
Cancel

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● **Typical**

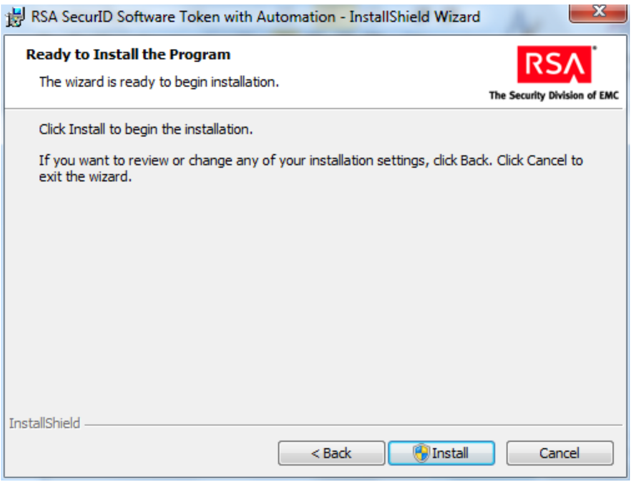
The RSA SecurID Software Token application will be installed. The Browser Plug-ins will not be installed.

○ **Custom**

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

3.5. User Account Control

Switching to admin context



RSA SecurID Software Token with Automation - InstallShield Wizard

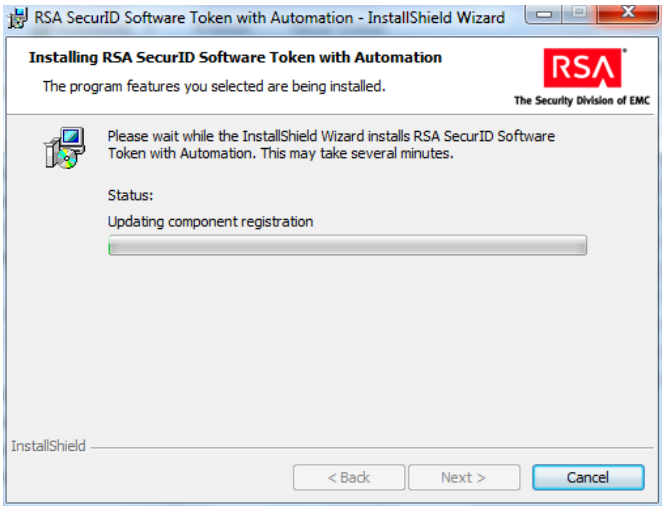
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

3.6. Installation started



RSA SecurID Software Token with Automation - InstallShield Wizard

Installing RSA SecurID Software Token with Automation

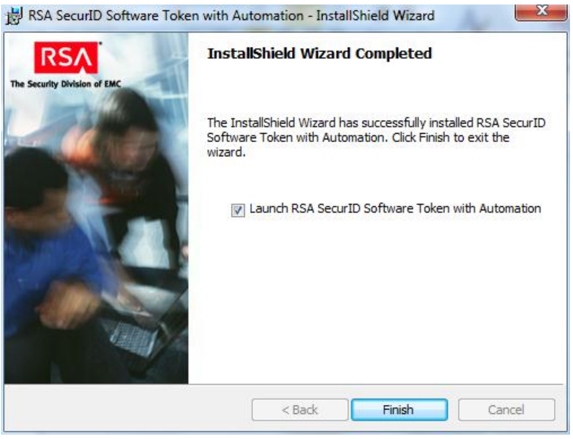
The program features you selected are being installed.

Please wait while the InstallShield Wizard installs RSA SecurID Software Token with Automation. This may take several minutes.

Status:

Updating component registration

3.7. Start RSA – soft token – program



RSA SecurID Software Token with Automation - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed RSA SecurID Software Token with Automation. Click Finish to exit the wizard.

☑ Launch RSA SecurID Software Token with Automation

3.8. Completion of the installation

The installation can be aborted at the prompting of the token. The soft token seed is uploaded to the computer by the user at a later step of the process.
The software has been completely installed, also after the abort.

3.9. Important configuration settings

The following registry keys are added by installing the .Reg files in the Windows registry. To install Admin rights are required. In general, a double-click on the file is sufficient to enter the registration key.

Operating System	.reg file
WIN 7 32	ZFNRKey32_Ext_1.xx.reg
WIN 7 64	ZFNRKey64_Ext_1.xx.reg

The settings will cause:

- The software "RSA SecureID token" is called up on the foreground.
- In the software "RSA SecureID token" the URL for the seed is permanently - Download entered.

3.10. Completion of the Program list

Move the link “RSA SecurID Token” to folder BerryRemote in the start menue.

3.11. "RSA SecurID" uninstallation

To uninstall administrator rights are required. The uninstallation via the Control Panel is necessary even when a software update or a reinstall is necessary. A reboot after installation is not required.

4. WINDOWS 7 – MTU setting

Installation NOT mandatory: The settings are need in some cases if network recources cannot reach **(local admin rights required)**

The most secure method is the establishment of a smaller MTU directly at the connection partners. With Windows 7, this can be achieved with the help of the **NETSH.EXE** command line instruction. For this, a prompt as administrator is started. In the [Start] menu, CMD.EXE is entered into the text field and started by pressing the CTRL+SHIFT and Enter keys. Thereafter it is determined which network adapters exist and which index they possess.

4.1. Determining adapter settings

```
>> netsh.exe interface ipv4 show interfaces
```

One receives a list of the network adapters existing in the system

```
Idx   Met      MTU       State            Name
---  ----------  ----------  ------------  ---------------------------
 1       50      1400  connected     Loopback Pseudo-Interface 1
11        5      1400  disconnected  Wireless Network Connection
12       20      1500  connected     Local Area Connection
```

4.2. Modify MTU

Then set the required MTU size for the network adapter handling the connection, e.g. for Idx 1:

```
>> netsh interface ipv4 set subinterface interface=1 mtu=1280 store=persistent
```

If the MTU must be modified for all connections:

```
netsh interface ipv4 set subinterface interface=1 mtu=1280 store=persistent
netsh interface ipv4 set subinterface interface=11 mtu=1280 store=persistent
netsh interface ipv4 set subinterface interface=12 mtu=1280 store=persistent
```

The option store=persistent ensures that the setting is preserved, also after a restart. The change is effective immediately.

```
Idx   Met      MTU       State            Name
---  ----------  ----------  ------------  ---------------------------
 1       50      1280  connected     Loopback Pseudo-Interface 1
11        5      1280  disconnected  Wireless Network Connection
12       20      1280  connected     Local Area Connection
```

I believe that only Idx 11+12 must be modified for ZF. The **Idx** index is potentially different.
Source of the basic settings: Internet

5. WINDOWS 7 – Installation Certificates

Installation NOT mandatory: The settings are need in some cases if the gateway ask for certificates.
For Activation and SSL.VPN-Connection ZFNR-Client needs following Certificates at Windows Client System, have to install additive according to certain Certificate error messages.

Check of Certificates can be done with IE-Browser menu under [Tools – Internet options – Content – Certificates in Certificates-Store : „Trusted Root Certification Authorities“ and “Intermediate Certification Authorities”].

- **DigiCert High Assurance EV Root CA**
- **DigiCert SHA2 High Assurance Server CA**
- **RSA Authentication Manager Root CA**

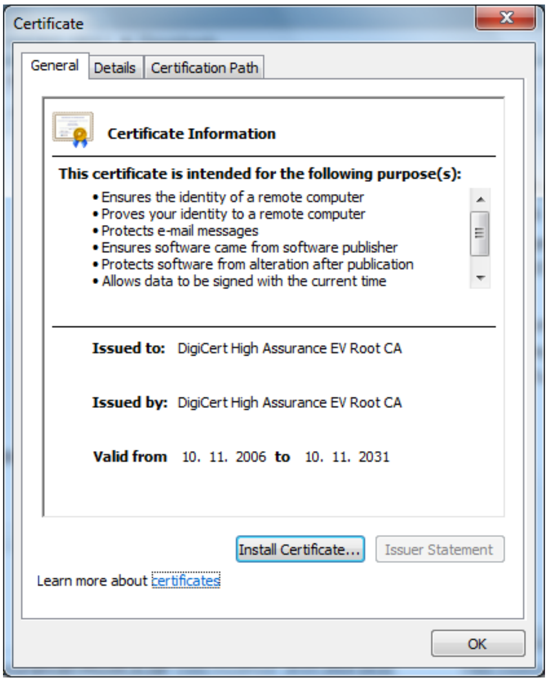
Certificates can be found under “C:\Ablage” (s. section 1.3) and can be installed as follows, if required.

a. Certificate Files:

- DigiCertHighAssuranceEVRootCA.cer
- DigiCertSHA2HighAssuranceServerCA.cer
- RSAAuthenticationManagerRootCA.cer

b. Install both Certificates each with double click to

- DigiCertHighAssuranceEVRootCA.cer



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

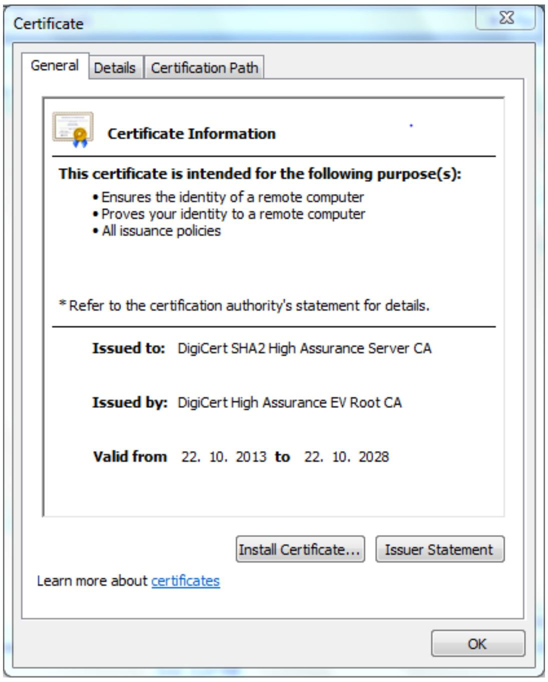
- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication
- Allows data to be signed with the current time

Issued to: DigiCert High Assurance EV Root CA

Issued by: DigiCert High Assurance EV Root CA

Valid from 10. 11. 2006 **to** 10. 11. 2031

- DigiCertSHA2HighAssuranceServerCA.cer



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- All issuance policies

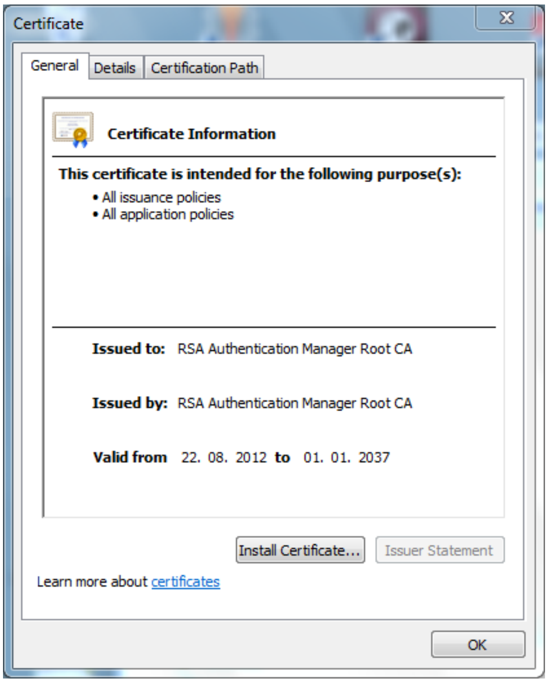
* Refer to the certification authority's statement for details.

Issued to: DigiCert SHA2 High Assurance Server CA

Issued by: DigiCert High Assurance EV Root CA

Valid from 22. 10. 2013 **to** 22. 10. 2028

- RSA Authentication Manager Root CA.cer



Certificate Information

This certificate is intended for the following purpose(s):

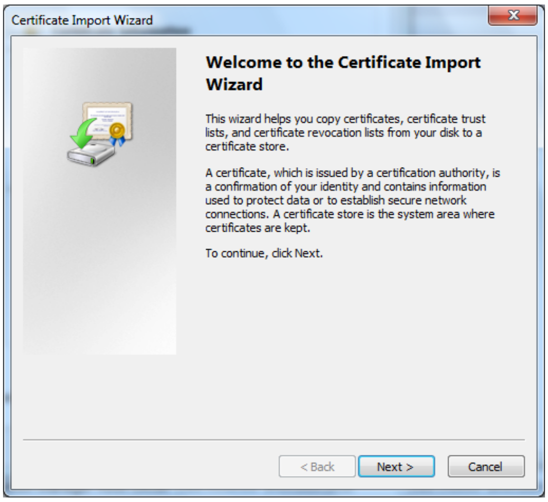
- All issuance policies
- All application policies

Issued to: RSA Authentication Manager Root CA

Issued by: RSA Authentication Manager Root CA

Valid from 22. 08. 2012 **to** 01. 01. 2037

Install process after particular Click to [Install Certificate…]-Button:



Certificate Import Wizard

Welcome to the Certificate Import Wizard

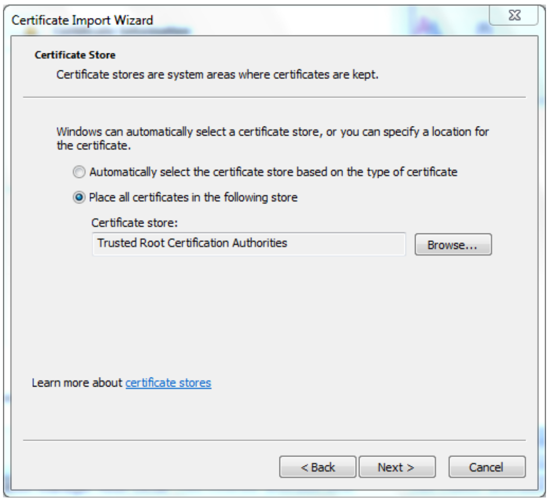
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Attention ! Following both Certificates have to assign into Certificates-Store: „Trusted Root Certification Authorities“

- **DigiCert High Assurance EV Root CA**
- **RSA Authentication Manager Root CA**



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

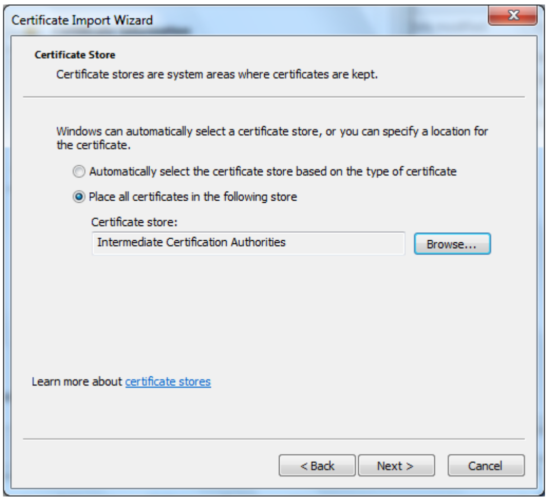
● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Learn more about certificate stores

Attention ! Following Certificate has to assign into Certificates-Store:
„Intermediate Certification Authorities“

- **DigiCert SHA2 High Assurance Server CA**



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

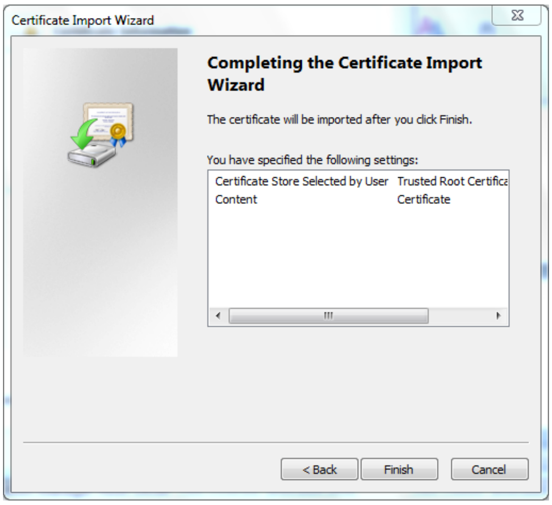
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Intermediate Certification Authorities

Learn more about certificate stores



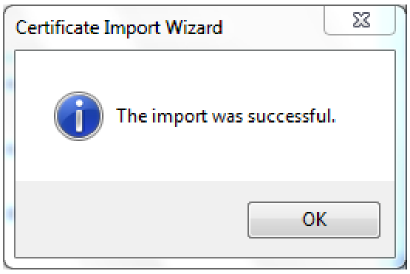
Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certifica
Content	Certificate



Certificate Import Wizard

The import was successful.