SIEMENS

Trusting of Self-Signed Certificates in Browsers

V1.00

Application Note

NOTE

For your own safety, please observe the warnings and safety instructions contained in this manual.

Document version: V1.00

Release status: 04.2017

Version of the product described: V1.00

Preface

Purpose of the Manual

This manual contains information about:

- The way of securely trusting self-signed certificates in general
- Adding self-signed certificates to the certificate trust store of Internet Explorer, Chrome, and Firefox

Target Audience

Security system engineers and persons entrusted with the setting, testing and maintenance of automation, selective protection and control equipment, and operational crew in electrical installations and power plants.

Scope

This manual applies to all EM DG PRO products having a secure web-based engineering interface over HTTPS.

Further Documentation

Indication of Conformity

This product complies with the directive of the Council of the European Communities on harmonization of the laws of the Member States relating to electromagnetic compatibility (EMC Council Directive 2004/108/EC) and concerning electrical equipment for use within specified voltage limits (Low Voltage Directive 2006/95/EC).

This conformity has been proved by tests performed according to the Council Directive in accordance with the generic standards EN 61000-6-2 and EN 61000-6-4 (for EMC directive) and with the standard EN 60255-27 (for Low Voltage Directive) by Siemens AG.

The device is designed and manufactured for application in an industrial environment.

The product conforms with the international standards of IEC 60255 and the German standard VDE 0435.

Other Standards

IEEE Std C 37.90

The technical data of the product is approved in accordance with UL.

File E194016

Additional Support

For questions about the system, please contact your Siemens sales partner.

Support

Our Customer Support Center provides a 24-hour service.

Tel.: +49 (1805) 24-7000

Phone: +49 (1805) 24-2471

E-mail: support.ic@siemens.com

Training Courses

Inquiries regarding individual training courses should be addressed to our Training Center:

Siemens AG

Siemens Power Academy

Humboldtstrasse 59

90459 Nuremberg

Tel.: +49 (911) 433-7415

Phone: +49 (911) 433-5482

E-mail: td.power-academy.energy@siemens.com

Internet http://www.siemens.com/energy/power-academy

Safety Information

This manual is not a complete index of all safety measures required for operation of the equipment (module, device). However, it comprises important information that must be noted for purposes of personal safety, as well as in order to avoid material damage. Information is highlighted and illustrated as follows according to the degree of danger.

DANGER

DANGER means that death or severe injury **will** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid death or severe injuries.

WARNING

WARNING means that death or severe injury **may** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid death or severe injuries.

CAUTION

CAUTION means that medium-severe or slight injuries **can** occur if the specified measures are not taken.

✧ Comply with all instructions, in order to avoid medium-severe or slight injuries.

NOTICE

NOTICE means that material damage **can** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid material damage.

NOTE

Important information about the product, product handling, or a certain section of the documentation, which must be given particular attention.

Qualified Electrical Engineering Personnel

Only qualified electrical engineering personnel may commission and operate the equipment (module, device) described in this document. Qualified electrical engineering personnel in the sense of this manual are people who can demonstrate technical qualifications as electrical technicians. These persons may commission, isolate, ground and label devices, systems and circuits according to the standards of safety engineering.

Use as Prescribed

The equipment (device, module) may only be used for such applications as set out in the catalogs and the technical description, and only in combination with third-party equipment recommended and approved by Siemens.

Problem-free and safe operation of the product depends on the following:

- Proper transport
- Proper storage, setup, and installation
- Proper operation and maintenance

When electrical equipment is operated, hazardous voltages are inevitably present in certain parts. If proper action is not taken, death, severe injury, or material damage can result.

- The equipment must be grounded at the grounding terminal before any connections are made.
- All circuit components connected to the power supply may be subject to dangerous voltage.
- Hazardous voltages may be present in equipment even after the supply voltage has been disconnected (capacitors can still be charged).
- Equipment with exposed current transformer circuits must not be operated.
- The limit values stated in the document may not be exceeded. This must also be considered during testing and commissioning.

Table of Contents

1 Goal/Purpose

1.1 Motivation

Besides using an engineering tool like DIGSI 5 or SICAM TOOLBOX II to configure and maintain, several products offer a Web front-end to be used with a regular browser. Formerly, most of these front-ends have, if at all, a flawed security concept caused by the lack of methods to enforce integrity and confidentiality of the communication between browser and device. Adding TLS to the communication-stack and switch from HTTP:// to HTTPS:// circumvents the most obvious attacks (for example, replay, pw-sniffing, MITM).

Due to the authentication-scheme used by browsers, Siemens cannot provide certificates (for example, during assembly) to be used for HTTPS with browsers.
This is because either the DNS name or the IP address of the device has to be part of the signed certificate, both of which are ultimately determined after installation at the customer's site. That's why the products generate a self-signed certificate after the IP address has been set.

This self-signed certificate has to be trusted in a secure way on all clients used to access this device.

2 Trusting of Self-Signed Certificates in Browsers

2.1 The Secure Way of Trusting Self-Signed Certificates

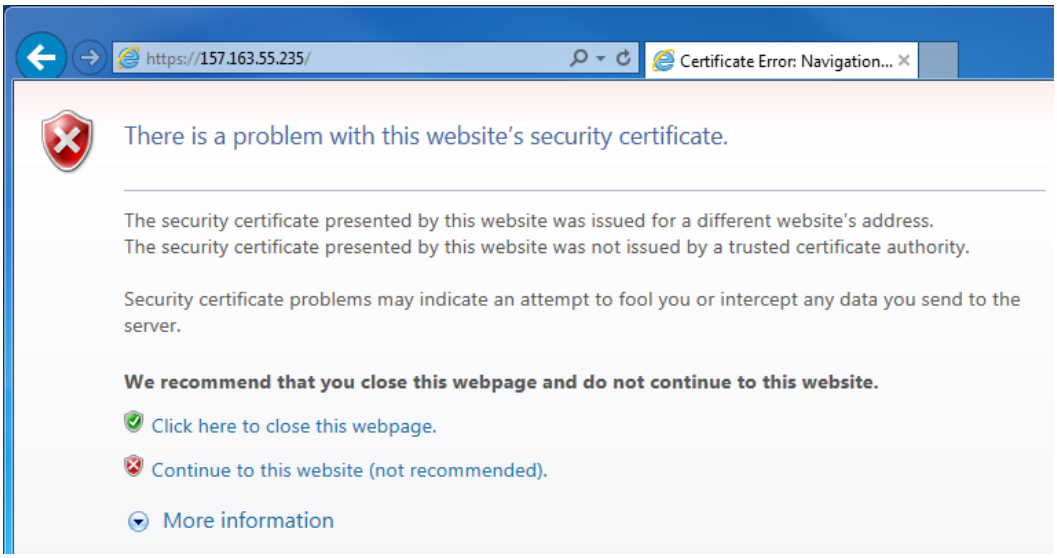
As with the usage of self-signed certificates there is no hierarchy of trust (certificate authority) which can be imported in browsers trust store, the way of trusting self-signed certificates must be done in a secure way to circumvent potential man-in-the-middle attacks.

Downloading the certificate via browser over an unsecure network includes the risk of downloading the certificate from the attacker. This would in fact lead to unsecure communication. To prevent this attack, the certificate of a device has to be downloaded by physically connecting directly to the devices LAN interface. After collecting the certificates of all devices, these certificates have to be deployed in a secure manner to the client systems (for example, by using Active Directory Domain Services and a Group Policy object).

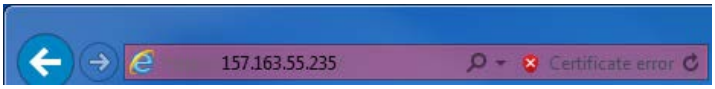
2.2 Downloading Self-Signed Certificates via Browser

Internet Explorer

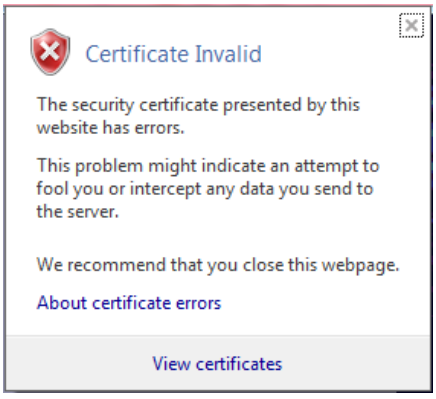
1. Navigate to the Internet site of your device by entering the target IP address in the address bar of the browser. A certificate error site is shown.



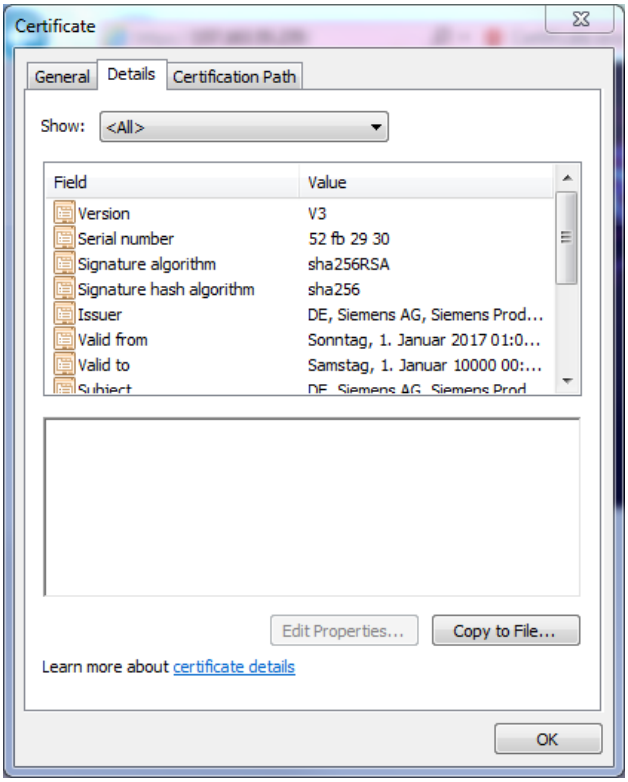
2. Click **Continue to this website (not recommended)**. The Internet site is shown and the address bar of the browser shows a **Certificate error**.



3. Click **Certificate error** to open the details.

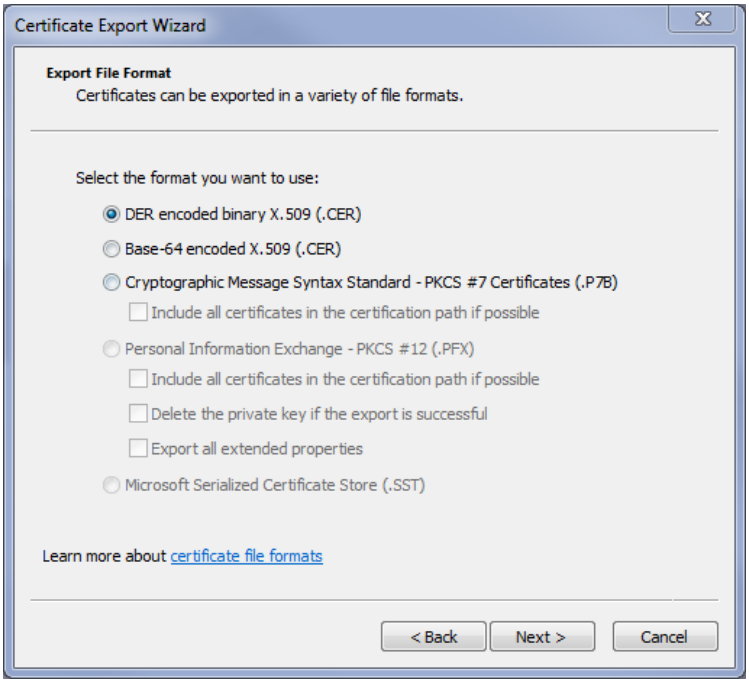


4. Click **View certificates**. The Certificate window is shown.

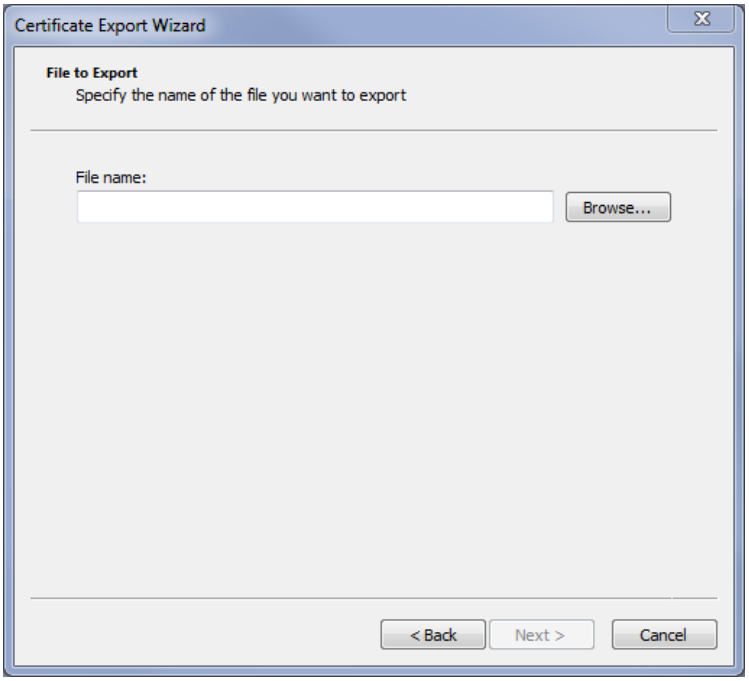


5. Navigate to the **Details** tab and click **Copy to File...**. The **Welcome to the Certificate Export Wizard** dialog appears.

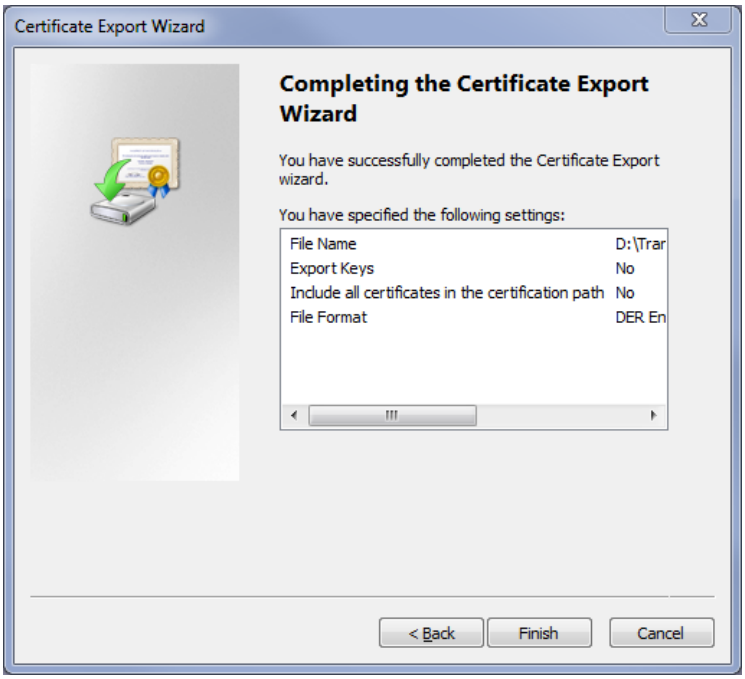
6. Click **Next >**. The **Export File Format** dialog appears.



7. Click **Next >**.



8. Click **Browse...**.
9. Select a name and a location where to store the certificate and click **Save**.
10. Click **Next >**. The **Completing the Certificate Export Wizard** dialog appears.



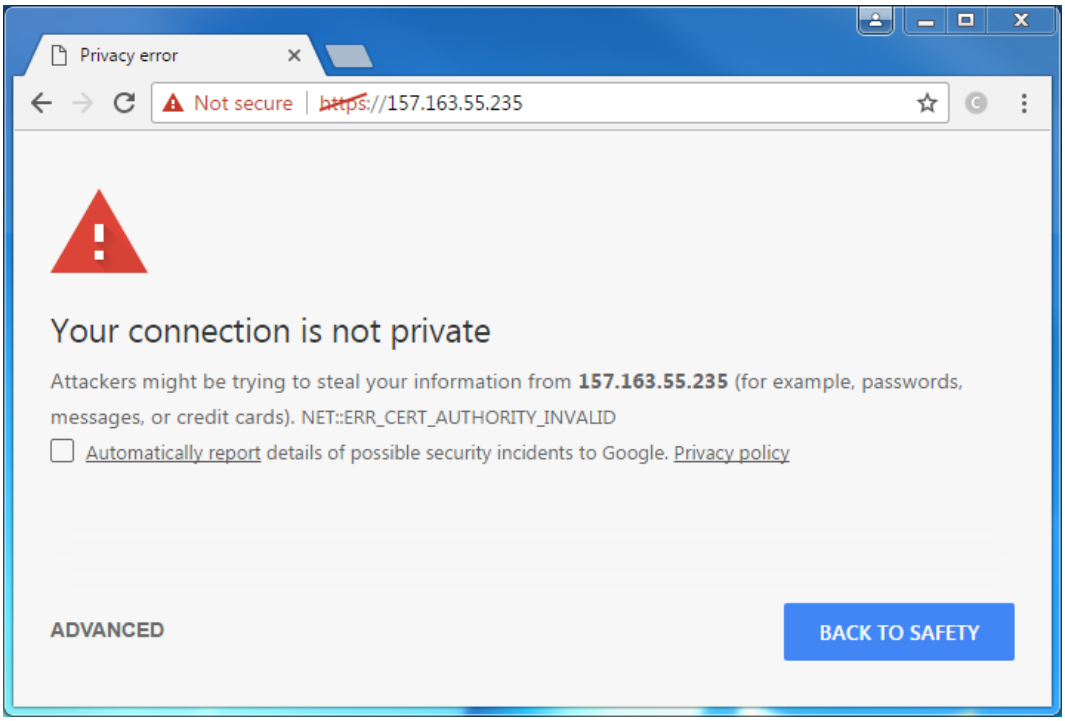
11. Click **Finish**. The **Export was successful** dialog appears.
12. Click **OK** to finish the export of certificate.

EDGE

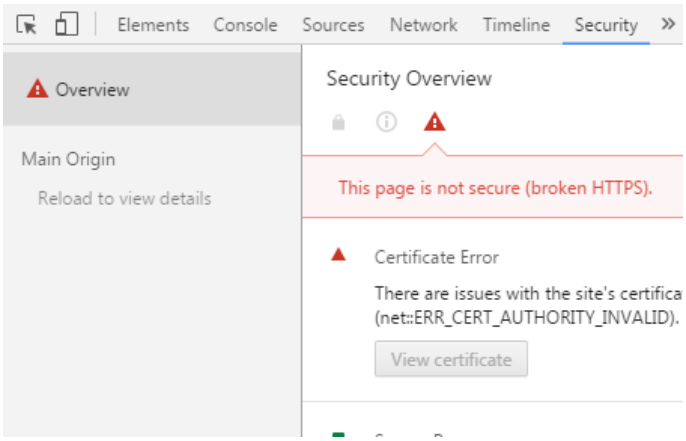
There is no way to download the certificate with EDGE. Use one of the other browsers.

Google Chrome

1. Navigate to the Internet site of your device by entering the target IP address in the address bar of the browser. A privacy error site is shown.



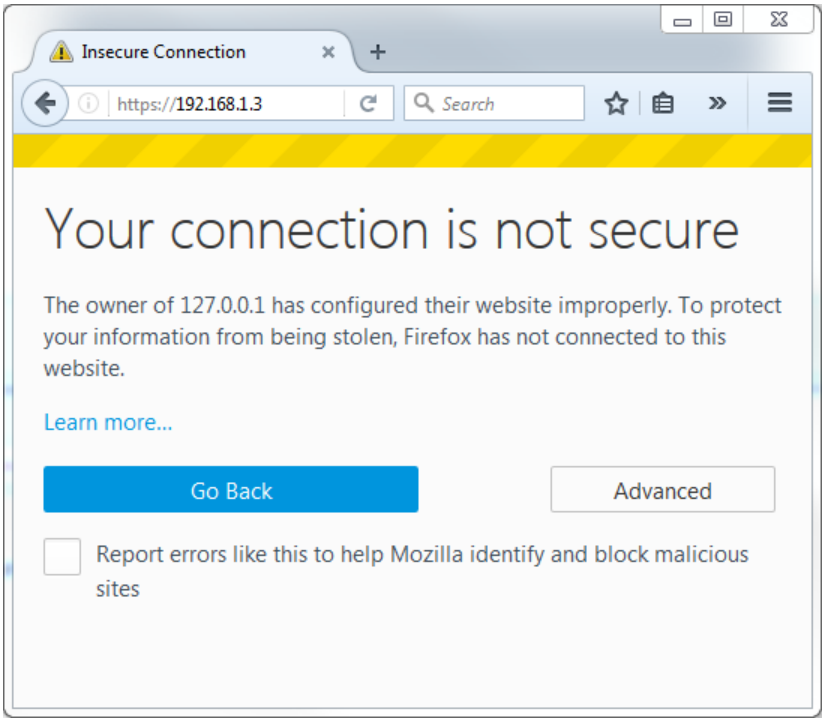
2. Press the F12 button on your keyboard and click **Security**.



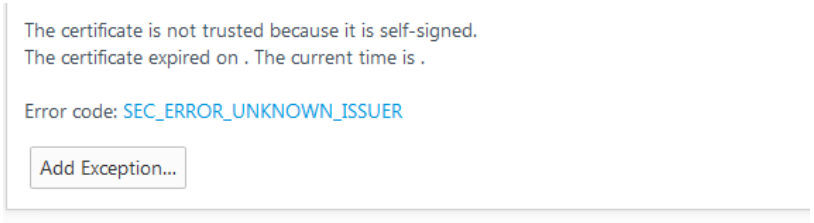
3. Click **View certificate**.
4. Proceed with step 5 in the chapter **Internet Explorer**.

Mozilla Firefox

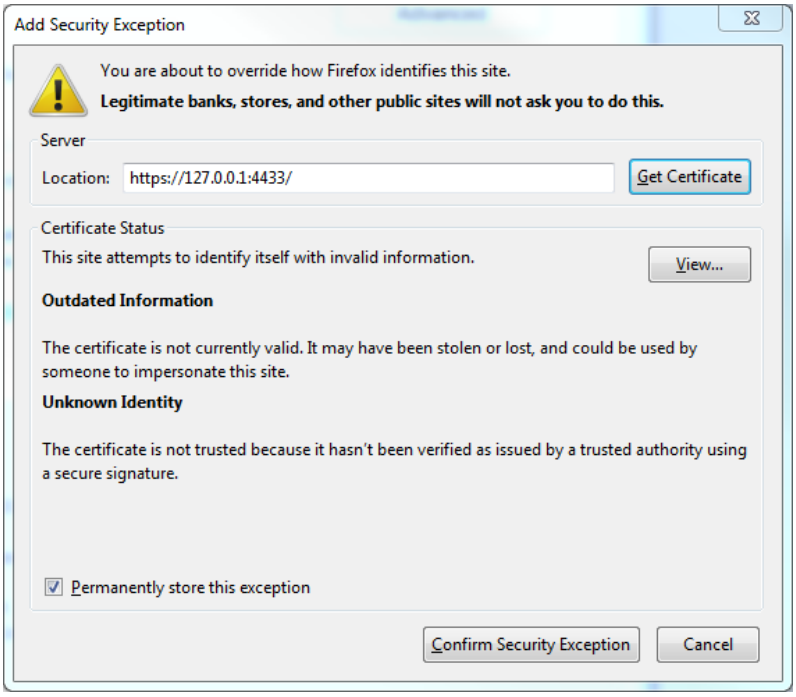
1. Navigate to the Internet site of your device by entering the target IP address in the address bar of the browser. An **Insecure Connection** site is shown.



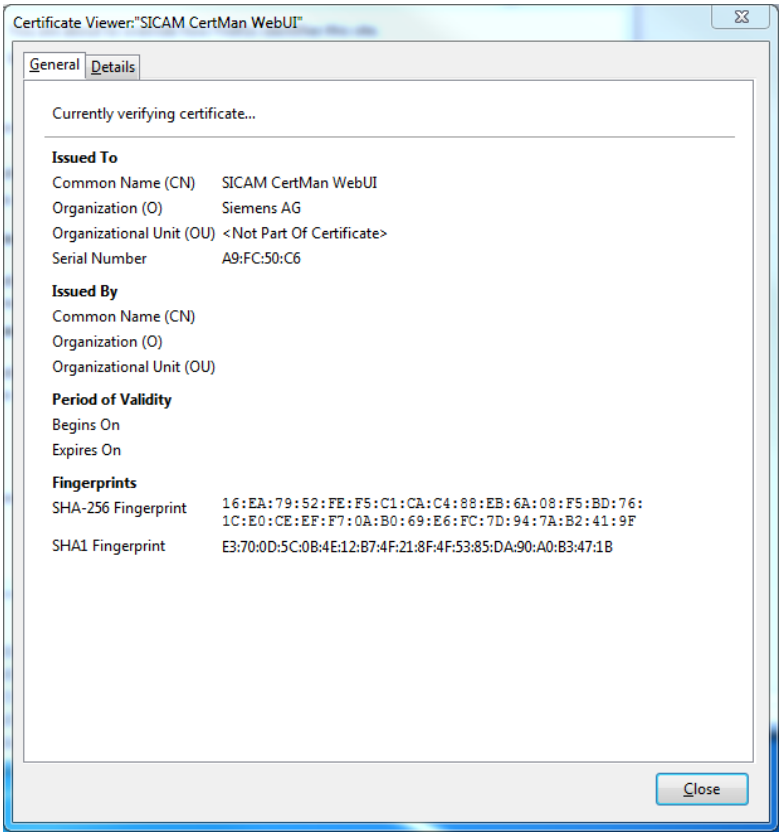
2. Click **Advanced**.



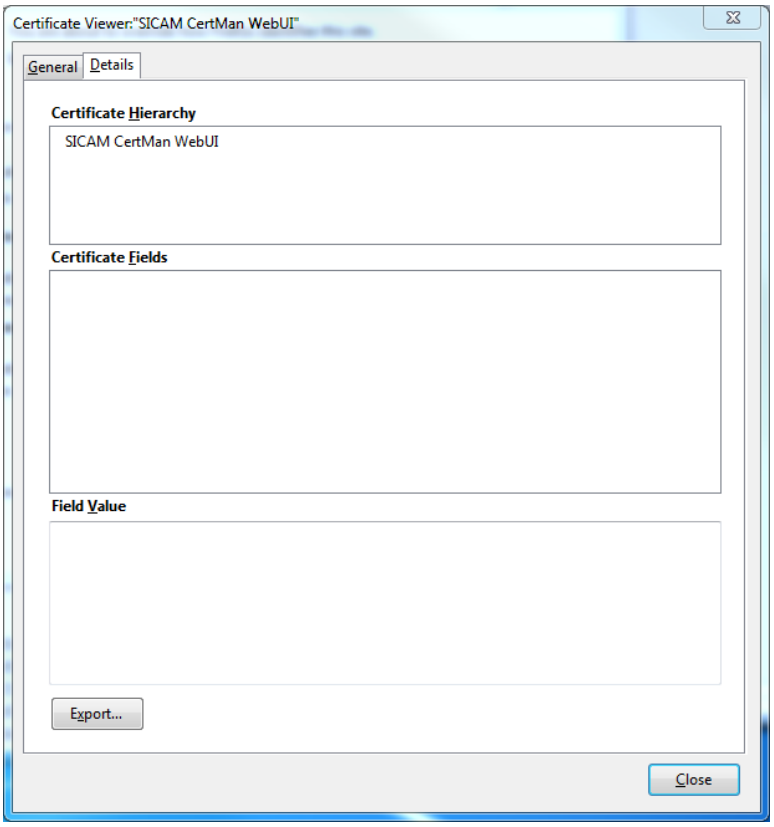
3. Click **Add Exception**. The **Add Security Exception** dialog is shown.



4. Click **View...**. The **Certificate Viewer** dialog is shown.



5. Click the **Details** tab.



6. Click **Export...**. The **Save Certificate To File** dialog is shown.
7. Select a name and a location where to store the certificate and click **Save**.
8. Click **Close** in the **Certificate Viewer** dialog.
9. Click **Cancel** in the **Add Security Exception** dialog.

2.3 Adding Self-Signed Certificates to the Microsoft Certificate Store

To execute the following steps, your user account must at least be a member of the user groups **Users** or **local administrators**:

1. On the **Start** menu, click **Run**, and then type **mmc**. Click **Enter** and confirm the **UAC window** with **Yes**. The Microsoft Management Console (MMC) is shown.
2. In the console, click the **File** menu and then click **Add/Remove Snap-in**.
3. On the Snap-in list, select **Certificates** and click **Add**.
4. In the **Certificates Snap-in** window, select **Computer account**, and then click **Next >**.
5. In the **Select Computer** window, select **Local computer** and then click **Finish**. This adds the Certificates snap-in to the list.
6. In the **Add/Remove snap-in** window, click **OK**. This adds the Certificates snap-in to the **mmc** console.
7. Double-click **Certificates (Local Computer)** in the left panel.
8. Right-click **Trusted Root Certification Authorities** and select **All tasks – Import…** in the context menu.
9. In the **Welcome to the Certificate Import Wizard** window, click **Next >**.
10. Click **Browse**, select the self-signed certificate in the file system, and confirm the dialog with **Open**.
11. Confirm the dialog with **Next >.**
12. Select **Place all certificates in the following store** and click **Next >.**
13. Confirm the **Completing the Certificate Import Wizard** dialog with **Finish.**
14. A dialog with the message **The import was successful** appears. Click **OK** to close it.

The self-signed certificate is now imported in Microsoft Certificate Store.

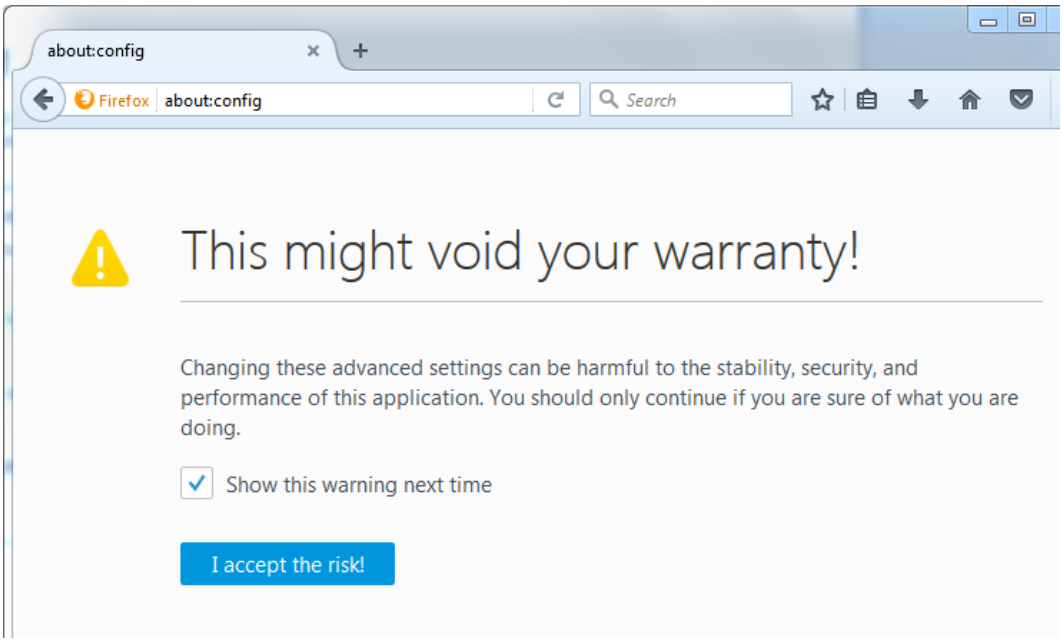
2.4 Usage in a Browser

Microsoft Internet Explorer, Microsoft Edge, and Google Chrome are using the Microsoft Certificate Store of the operating system (for example, Windows 7) for certificate trusting.

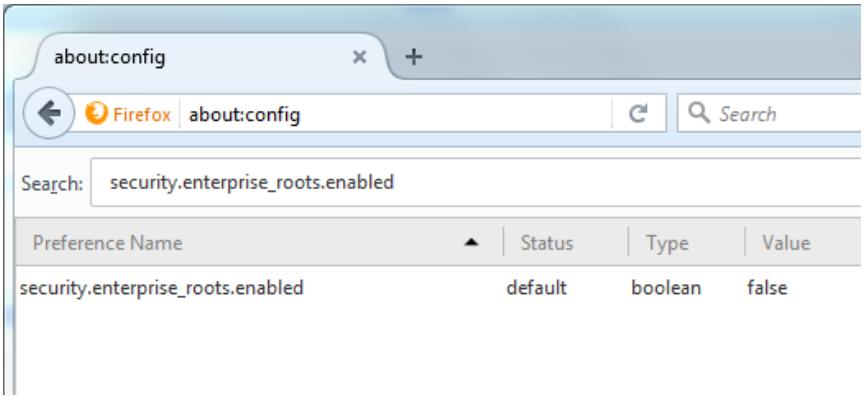
Mozilla Firefox is using its own certificate store per default for certificate trusting, but it has also the possibility to additionally use the Microsoft Certificate Store. Because with the latest release of Firefox, it is not possible to import self-signed certificates, Siemens recommends configuring the browser for usage of the Microsoft Certificate Store.

To configure Firefox for usage of the Microsoft Certificate Store, execute the following steps:

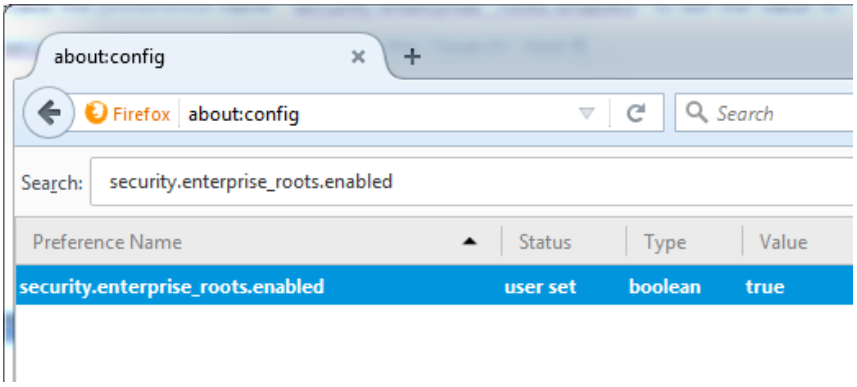
1. Type **about:config** in the address bar of Firefox.



2. Confirm the button **I accept the risk!**.
3. Type **security.enterprise_roots.enabled** in the **Search** field.



4. Double-click the preference name **security.enterprise_roots.enabled** to set the value to **true**.



5. Restart the browser.

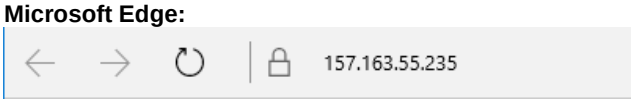
   Firefox is now ready to use the Microsoft Certificate Store

The following screenshots show how a trusted connection is displayed in the address bar of browsers.

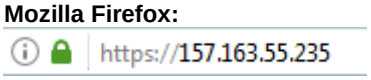
- **Microsoft Internet Explorer:**

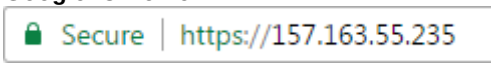
- **Microsoft Edge:**

- **Mozilla Firefox:**

- **Google. Chrome:**

3 Appendix

3.1 Browser Versions

This Application Note is based on the following browser versions.

Microsoft Internet Explorer: 11.0.9600.18537 Update: 11.0.38

Microsoft Edge: 38.14393.0.0

Mozilla Firefox: 52.0 b4

Google. Chrome: 56.0.2924.76