SIEMENS

Table of Contents

Motivation 1

Trusting Self-Signed Certificates in Browsers Appendix A

Index

Digital Grid Automation Products

Trusting Self-Signed Certificates in Browsers

V01.20

Supplementary Note



NOTE

For your own safety, observe the warnings and safety instructions contained in this document, if available.

Disclaimer of Liability

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

Document version: E50417-X0040-C154-A2.02

Edition: 06.2019

Version of the product described: V01.20

Copyright

Copyright © Siemens 2019. All rights reserved.

The disclosure, duplication, distribution and editing of this document, or utilization and communication of the content are not permitted, unless authorized in writing. All rights, including rights created by patent grant or registration of a utility model or a design, are reserved.

Trademarks

SIPROTEC[™], DIGSI[™], SIGUARD[™], SIMEAS[™], and SICAM[™] are trademarks of Siemens AG. Any unauthorized use is prohibited. All other designations in this document may represent trademarks whose use by third parties for their own purposes may violate the proprietary rights of the owner.

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

This manual is mainly intended for security system engineers and persons entrusted with the setting, testing, and maintenance of automation, selective protection, and control equipment, as well as for operational crews in electrical installations and power plants.

Scope

This manual applies to all **Digital Grid Automation Products** having a secure web-based engineering interface via HTTPS.

Additional Support

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

Support

Our Customer Support Center provides a 24-hour service.

E-Mail: support.energy@siemens.com

Training Courses

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

Siemens AG

Siemens Power Academy TD

Humboldtstraße 59

90459 Nürnberg

Germany

Phone: +49 (911) 433-7415 Fax: +49 (911) 433-7929

E-Mail: poweracademy@siemens.com

Internet: www.siemens.com/poweracademy

Table of Contents

| | Preface | e | 3 |
|---|---------|--|----|
| 1 | Motiva | tion | 7 |
| 2 | Trustin | g Self-Signed Certificates in Browsers | 9 |
| | 2.1 | Secure Way of Trusting Self-Signed Certificates | 10 |
| | 2.2 | Downloading Self-Signed Certificates via Browser | 11 |
| | 2.2.1 | Microsoft Internet Explorer | 11 |
| | 2.2.2 | Microsoft Edge | 17 |
| | 2.2.3 | Google Chrome | 19 |
| | 2.2.4 | Mozilla Firefox | 20 |
| | 2.3 | Adding Self-Signed Certificates to the Microsoft Certificate Store | 23 |
| | 2.4 | Using the Microsoft Certificate Store in a Browser | 24 |
| Α | Append | dix | 25 |
| | A.1 | Browser Versions | 26 |
| | A.2 | Mismatched Address Error in Microsoft Internet Explorer and Microsoft Edge | 27 |
| | Index | | 29 |

1 Motivation

Besides using an engineering tool like DIGSI 5 or SICAM TOOLBOX II for configuration and maintenance, several products offer a Web front-end to be used with a regular browser. Formerly, most of these front-ends had, 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, password sniffing, MITM).

Due to the authentication scheme used by browsers, Siemens cannot provide certificates to be used for HTTPS with browsers (for example, during assembly).

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. Therefore, 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 Self-Signed Certificates in Browsers |
|---|---|
| | |

2.1 Secure Way of Trusting Self-Signed Certificates

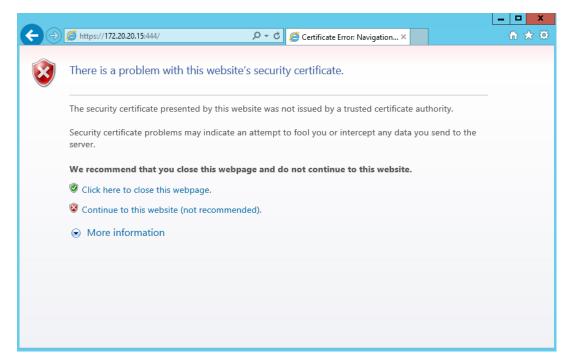
As with the usage of self-signed certificates there is no hierarchy of trust (certificate authority) which can be imported in the browser's trust store, the way of trusting self-signed certificates must be done in a secure way to circumvent potential man-in-the-middle attacks.

Downloading the certificate via browser over an insecure network includes the risk of downloading the certificate from the attacker. This would in fact lead to insecure 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).

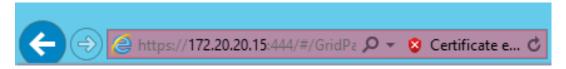
2.2 Downloading Self-Signed Certificates via Browser

2.2.1 Microsoft Internet Explorer

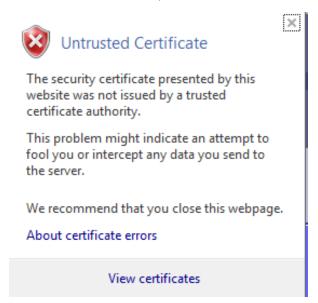
♦ Navigate to the website of your device by entering the target IP address in the address bar of the browser. A certificate error site is shown.



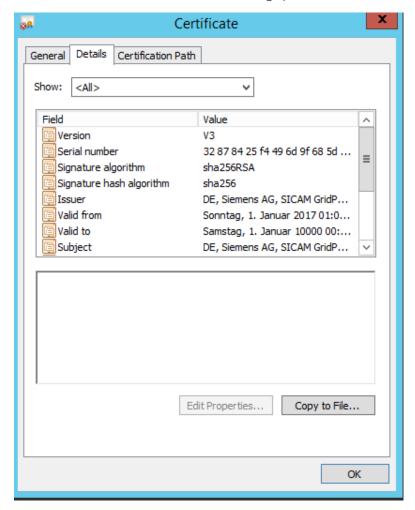
♦ Click Continue to this website (not recommended). The website is opened and the address bar of the browser shows a Certificate error.



♦ Click Certificate error to open the details.



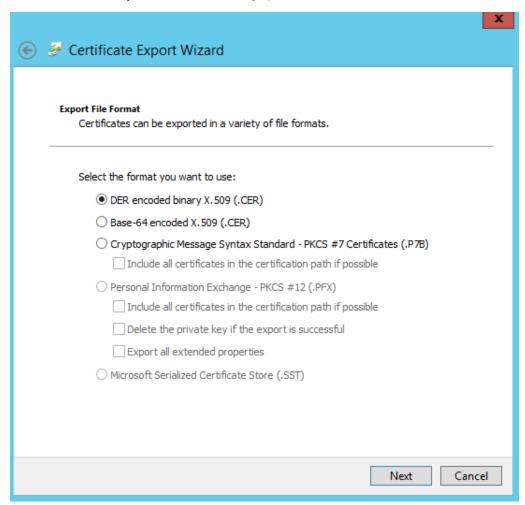
♦ Click View certificates. The Certificate dialog opens.



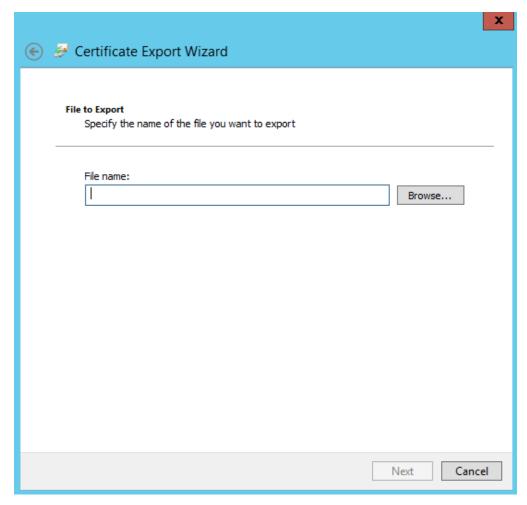
♦ Navigate to the **Details** tab and click **Copy to File...**. The **Welcome to the Certificate Export Wizard** dialog opens.



♦ Click Next >. The Export File Format dialog opens.



♦ Click Next >.



- ♦ Click Browse....
- ♦ Select a name and a location where to store the certificate, then click **Save**.

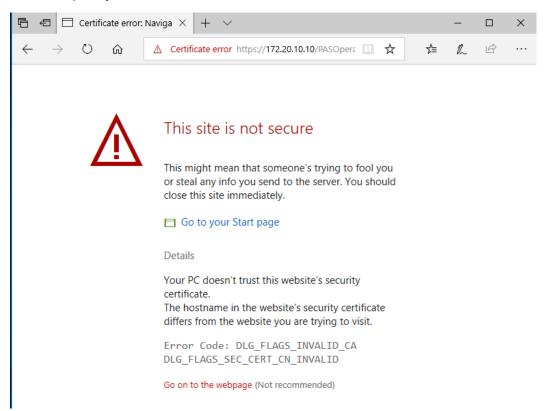
♦ Click Next >. The Completing the Certificate Export Wizard dialog opens.



- ♦ Click Finish. The Export was successful dialog opens.
- ♦ Click **OK** to finish the export of certificate.

2.2.2 Microsoft Edge

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



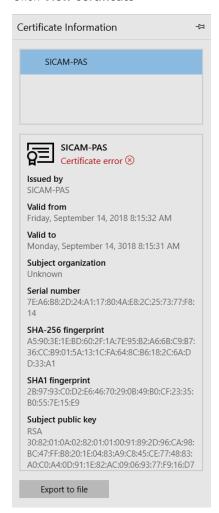
♦ Click Certificate error

Website problem

There's a problem with this website's security certificate. This might mean that someone's trying to fool you or steal any info you send to the server.

View certificate

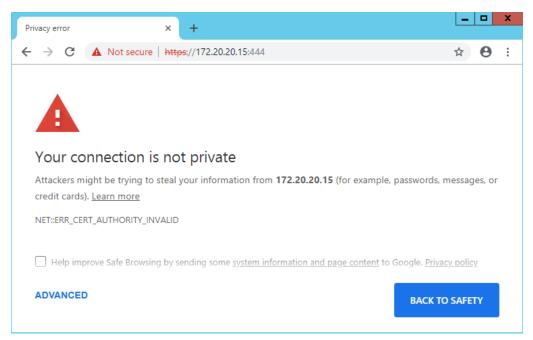
♦ Click View certificate



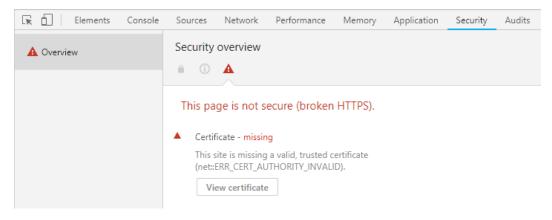
- ♦ Click Export to file
- ♦ Save the Certificate to a X.509 Certificate file
- Proceed from here with the Adding Self-Signed Certificates to the Microsoft Certificate Store as described in 2.3

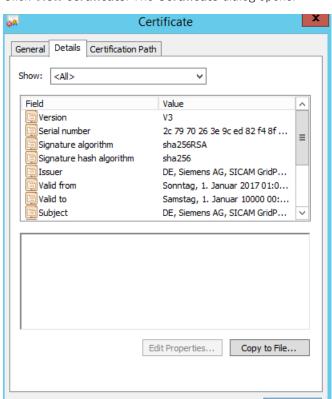
2.2.3 Google Chrome

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



♦ Press <F12> and click Security.





♦ Click View certificate. The Certificate dialog opens.

♦ Proceed from here with the Certificate Export Wizard as described in 2.2.1 Microsoft Internet Explorer

OK

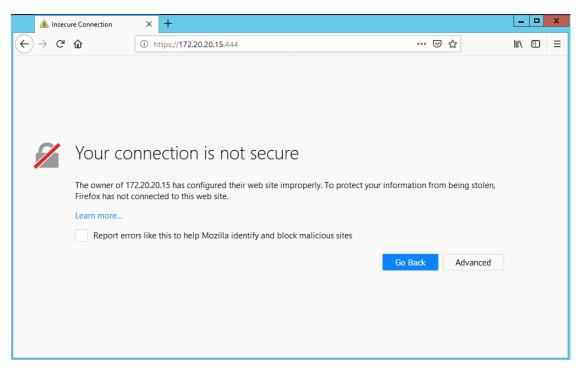
2.2.4 Mozilla Firefox

As of Version 59, Mozilla Firefox doesn 't support self-signed certificates anymore.

As workaround add the web site as an exception.

♦ Navigate to the website of your device by entering the target IP address in the address bar of the browser.

An Insecure Connection site is shown.



♦ Click Advanced.

172.20.20.15:444 uses an invalid security certificate.

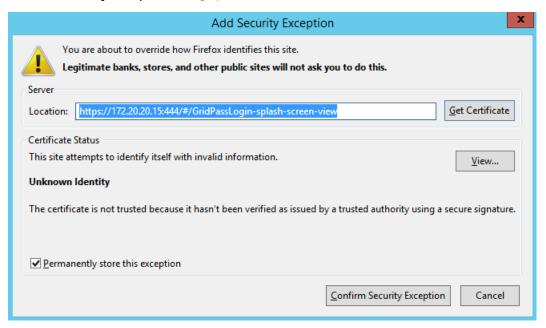
The certificate is not trusted because it is self-signed.

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

Add Exception...

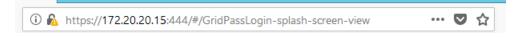
♦ Click Add Exception.

The **Add Security Exception** dialog opens.



♦ Click Confirm Security Exception...

The web site is shown.



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**:

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

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

2.4 Using the Microsoft Certificate Store in a Browser

Trusted Connection

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

Microsoft Internet Explorer
 https://157.163.55.235/
 Microsoft Edge
 ← → ○ | △ 157.163.55.235
 Google Chrome
 Secure | https://157.163.55.235

Microsoft Internet Explorer, Microsoft Edge, Google Chrome

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

A Appendix

A.1 Browser Versions

A.1 Browser Versions

This document is based on the following browser versions:

• Microsoft Internet Explorer: 11.0.125

• Microsoft Edge: 42.17134.0 and 44.17763

Mozilla Firefox: 67.0.1

• Google Chrome: 75.0.3770.80

A.2 Mismatched Address Error in Microsoft Internet Explorer and Microsoft Edge

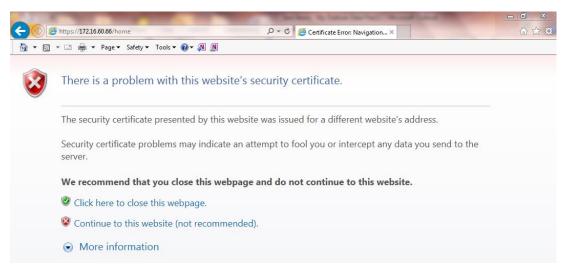
This error occurs when using old versions of Microsoft Internet Explorer and Microsoft Edge.

Use Internet Explorer 11.545.10586.0 or higher, or Edge 25.10586.0.0 or higher on Microsoft Windows 10 to avoid this issue. Alternatively, use Google Chrome or Mozilla Firefox to avoid this issue.

Error Example

The following example shows what the error looks like in the Microsoft Internet Explorer:

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



Click Continue to this website (not recommended). The website is opened and the address bar of the browser shows a Certificate error.



♦ Click Certificate error to open the details.



Mismatched Address

The security certificate presented by this website was issued for a different website's address.

×

This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

About certificate errors

View certificates

Index

```
Α
Adding self-signed certificates 9, 22
    Microsoft Certificate Store 9, 22
D
Downloading self-signed certificates 11, 15, 17
    Google Chrome 15
    Microsoft Edge 15
    Microsoft IE 11, 17
    Mozilla Firefox 17
Ε
Error 27, 29
    Mismatched Address in IE 27, 29
G
Goal 1, 7
M
Microsoft Certificate Store 9, 22, 23
    Adding self-signed certificates 9, 22
    Using in browser 9, 23
Motivation 1, 7
S
Secure way of trusting 9, 10
```