

Installation Instructions for Website Certificate

Version 1.0 (valid from Cubis MCA Firmware 09-03-05.xx.xx)

Document history

Version	Date	Changed sections	Description of the changes
1.0	2020-11-18		New Document

Author	Hendrik Woidt	2020-11-09
Review	Jan von Steuben	2020-11-18
Release	Jan von Steuben	2020-11-18

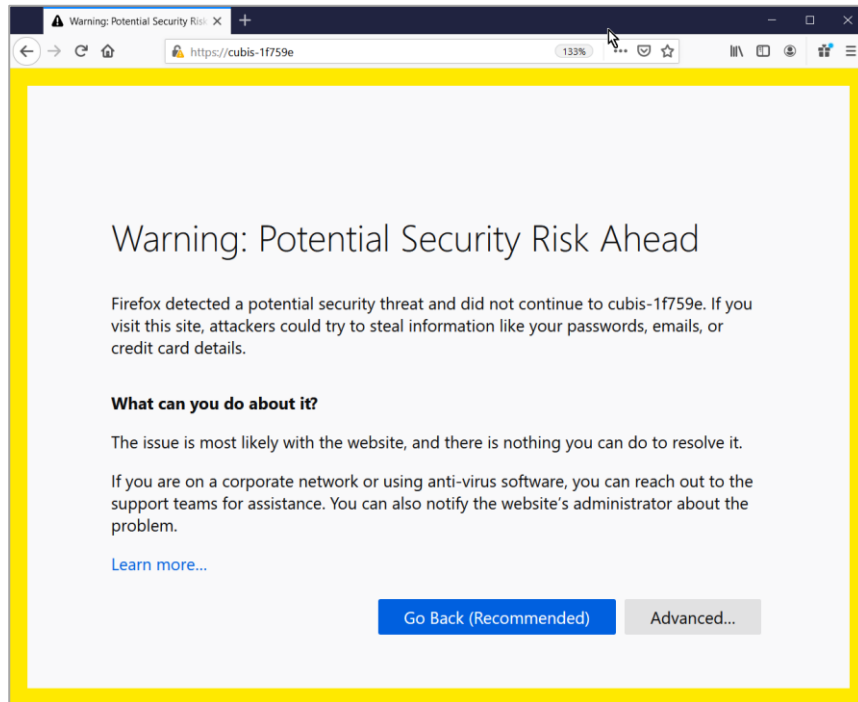
Passing on, duplication, distribution and / or editing of this document as well as exploitation of its contents and communication to third parties are not permitted without express permission.

Table of contents

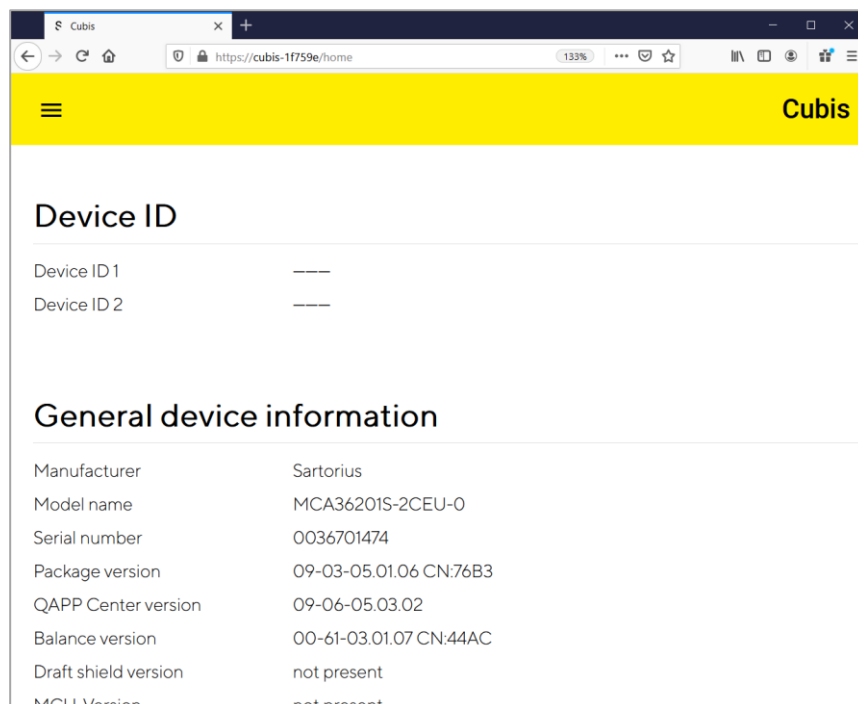
1. Purpose and Background.....	3
2. Preparation for all browsers.....	4
3. Installation for Firefox (Windows/Linux)	5
4. Installation for Chrome/Edge (Windows)	7
5. Installation for Chrome (Android)	10
6. Installation for iOS / iPadOS (all browser)	11

1. Purpose and Background

Cubis balances only provide a secure connection for communication with the device website. If the browser does not recognize the certificates of the website, a warning message will appear when the website is accessed.



In order for this warning message to disappear and the device to be recognized as a trusted device, it is necessary to install a certificate on the device in use. Only after the installation of the certificate the web page appears.



This guide describes the easiest way to install the necessary certificate to establish a trusted connection to the device website for different browsers and operating systems. A trusted root certificate from Sartorius is installed. Make sure that the certificate comes directly from Sartorius. A manipulated certificate could be used by attackers to pretend the trustworthiness of other websites visited with the browser. For maximum security, it is recommended that you install your own certificates on the device.

2. Preparation for all browsers

Download the file "CubisND Product Authority.crt" to the device on which you want to install the certificate.

The certificate is included in the "Cubis II MCA firmware" package in the folder "Website SSL Certificate".

The latest Cubis II MCA firmware package is available on the Sartorius website.

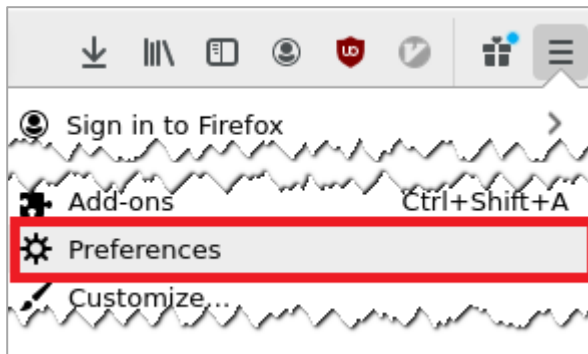
<https://www.sartorius.com/en/products/weighing/laboratory-balances/premium-level-balances/cubis-ii>

The fingerprints to verify the authenticity of the certificate for release 09-03-05.xx.xx are

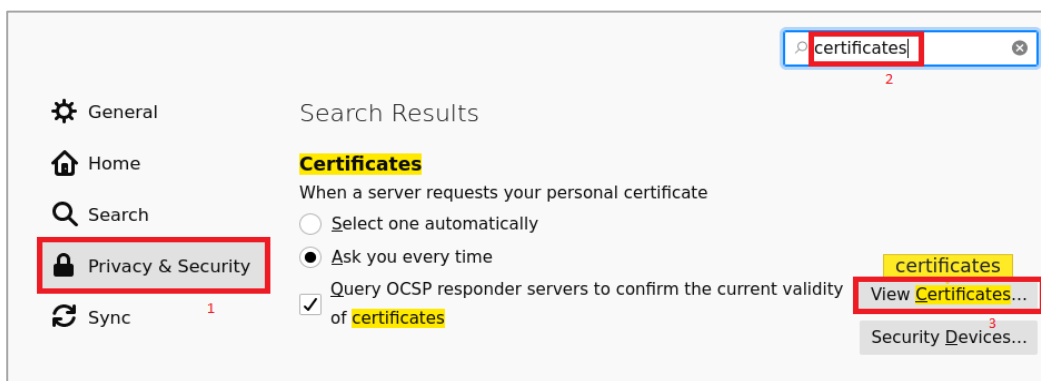
- SHA-256: 4F:3C:E4:97:8B:4C:15:6C:6A:66:37:38:81:22:C5:A0:
D5:4B:45:7D:83:6D:1A:62:B4:53:4B:0A:90:B9:39:48
- SHA-1: 62604fbdbf32f1bbbed35d3bd13ca3e6b0bae9930

3. Installation for Firefox (Windows/Linux)

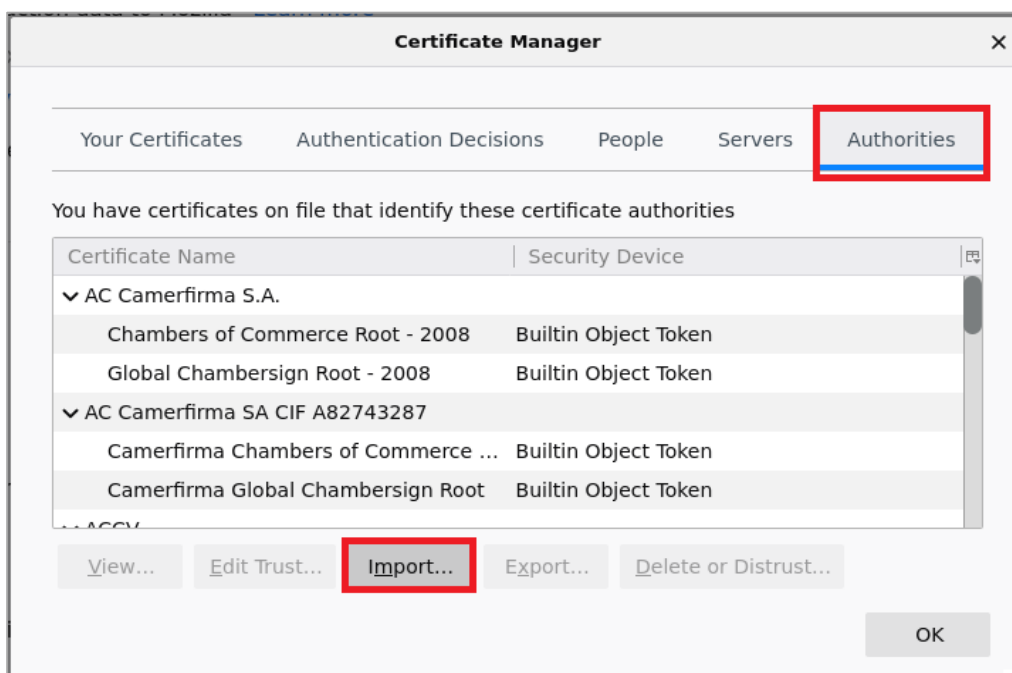
1. Open the Menu
2. Select "Preferences"



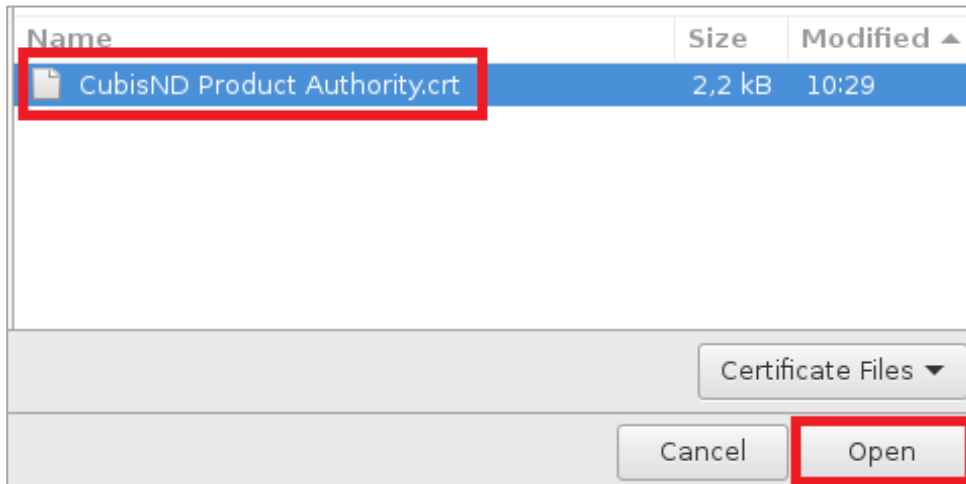
3. Go to section "Privacy & Security"
4. Scroll down to the bottom and select "View Certificates" in the "Security" section



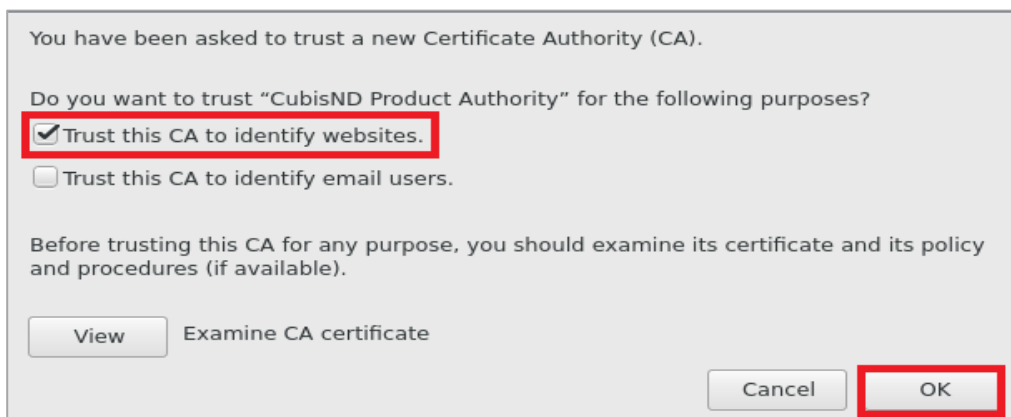
5. Select the "Authorities" tab



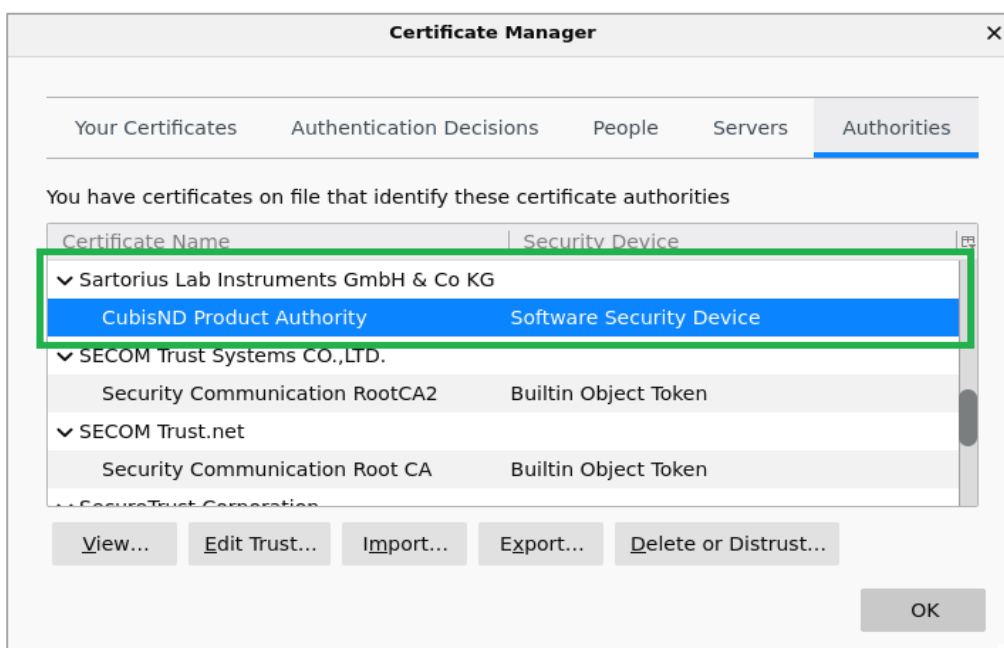
- Click "Import..."
- Select the file "CubisND Product Authority.crt" you downloaded earlier



- Select the checkbox "Trust this CA to identify websites"

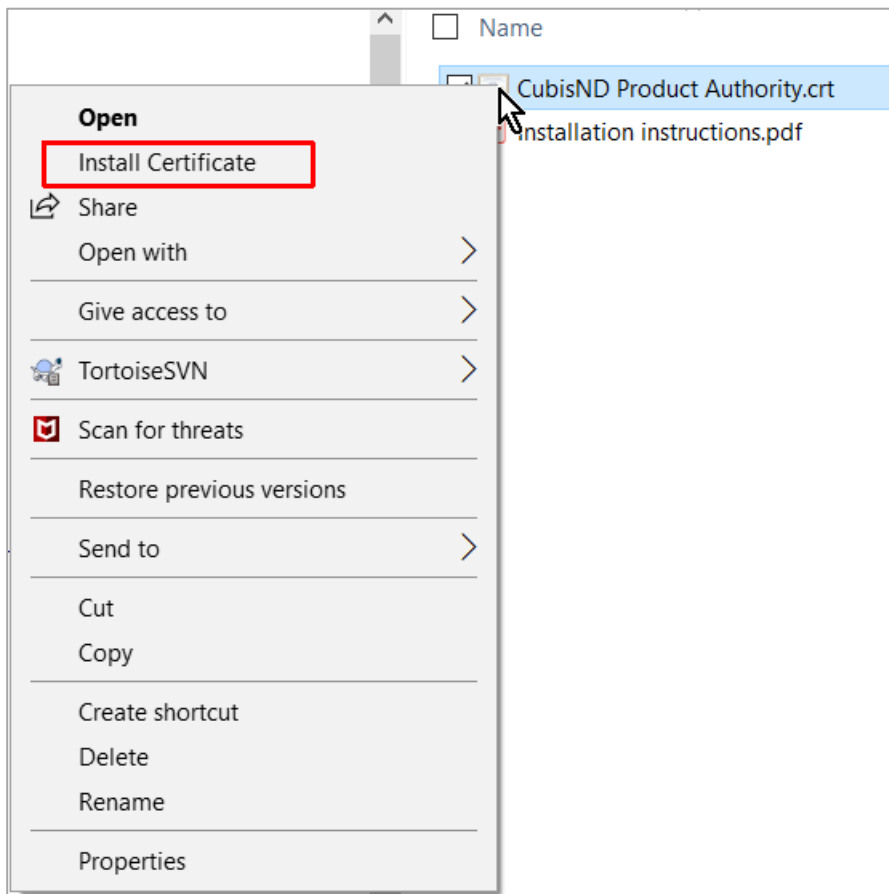


- Confirm the dialog to import and trust the certificate

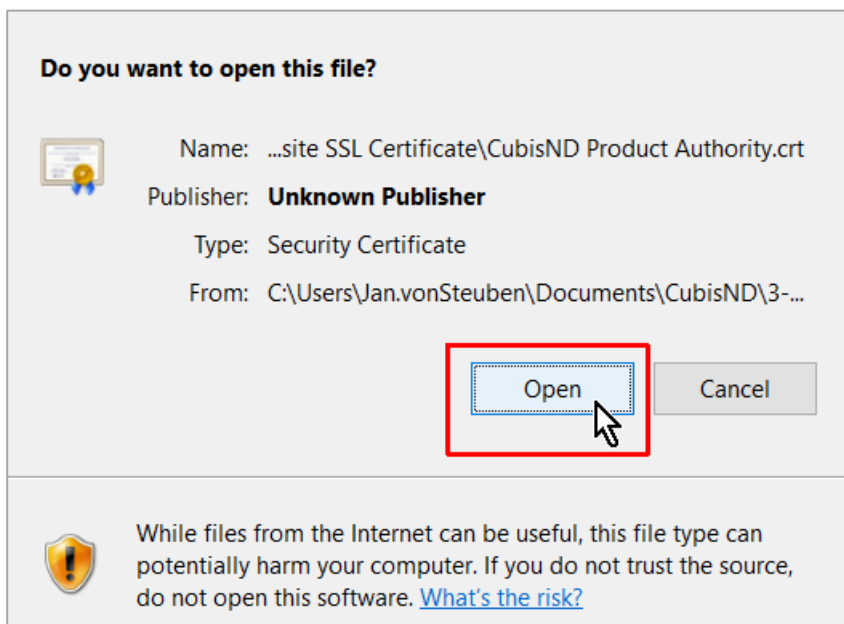


4. Installation for Chrome/Edge (Windows)

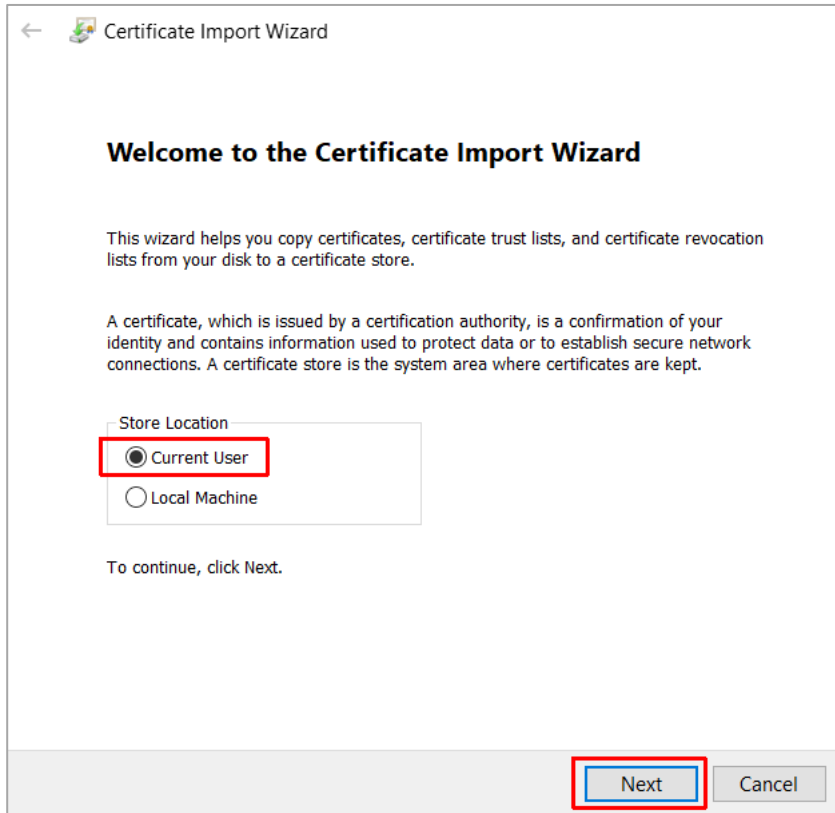
1. Right click on the file "Trusted Certificate Authorities".



2. Confirm to "Open" the file.



3. Select Store Location "Current User" and click on "Next".



← 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.

Store Location

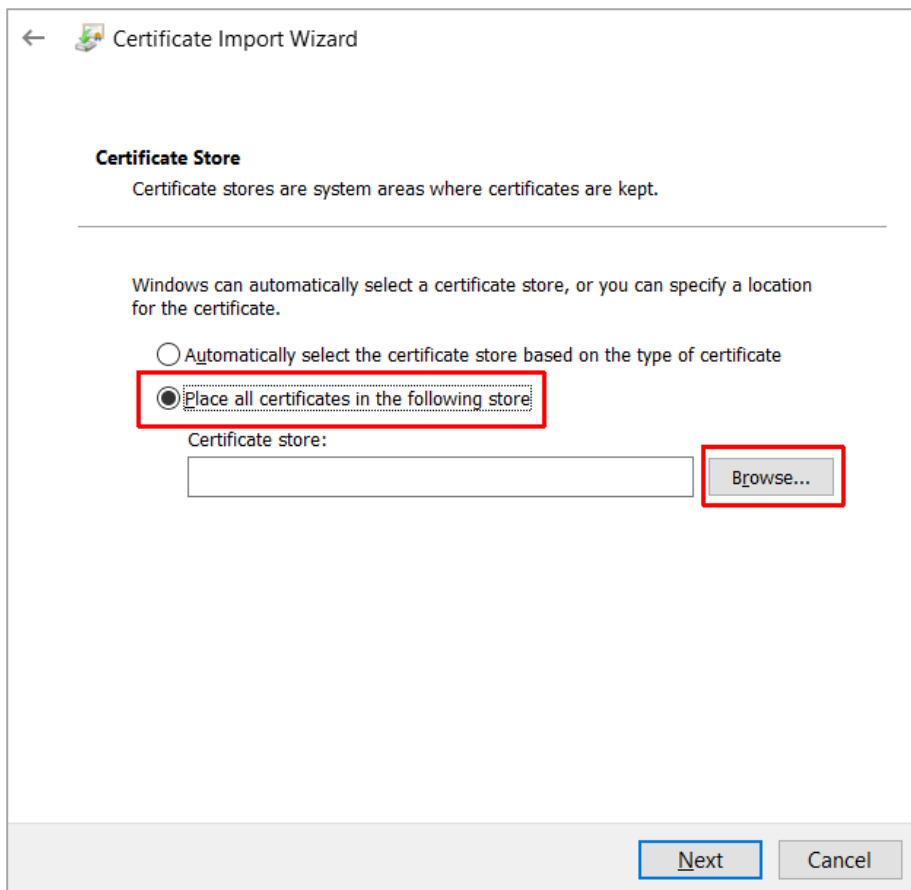
☒ Current User

☐ Local Machine

To continue, click Next.

Next Cancel

4. Select "Place all certificates in the following store" and then click on "Browse ..."



← 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

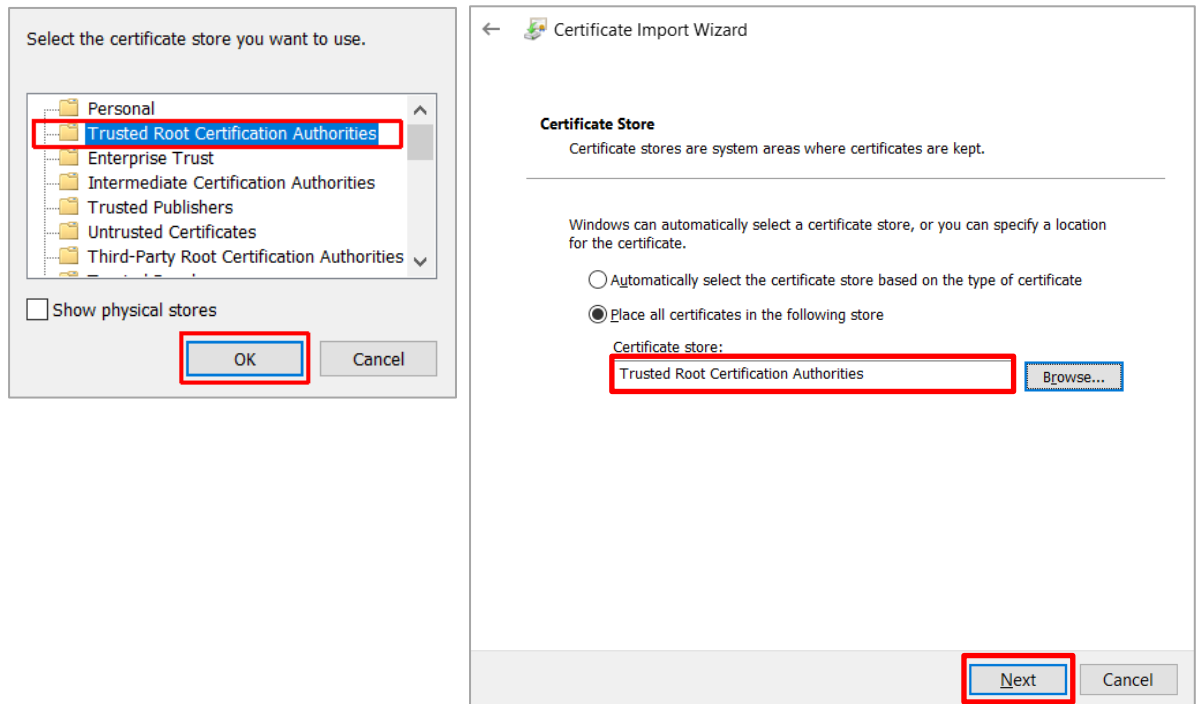
☒ Place all certificates in the following store

Certificate store:

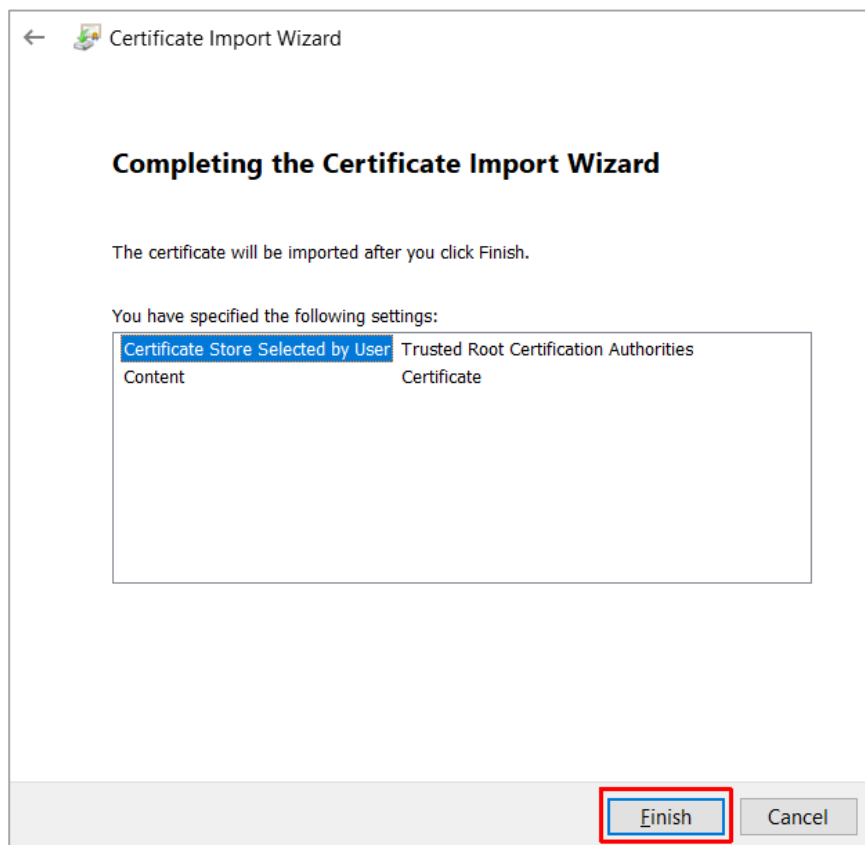
Browse...

Next Cancel

5. Select the certificate store “Trusted Root Certification Authorities” and confirm with “OK”. Then click “Next” on the Import Wizard.

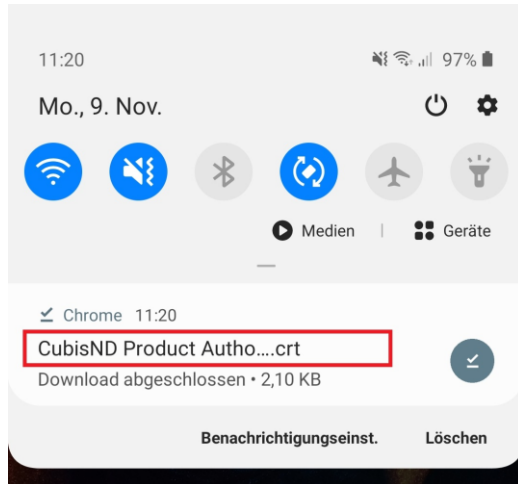


6. Complete the Import with a click on “Finish”.

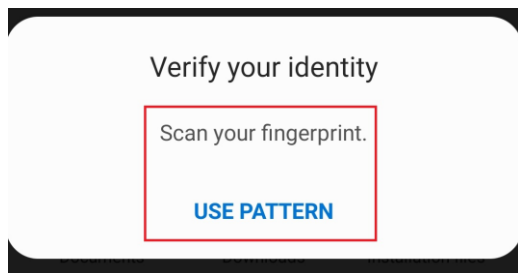


5. Installation for Chrome (Android)

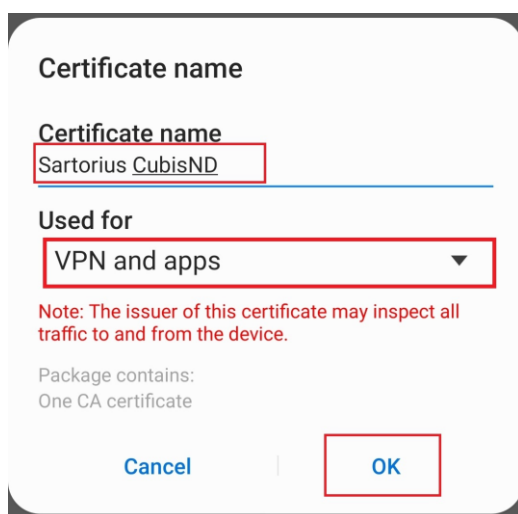
1. Download the certificate file "CubisND Product Authority.crt" to the device.
2. Open the file from the download folder



3. Authenticate yourself when asked (e.g. enter your pin / biometric authentication / ..)

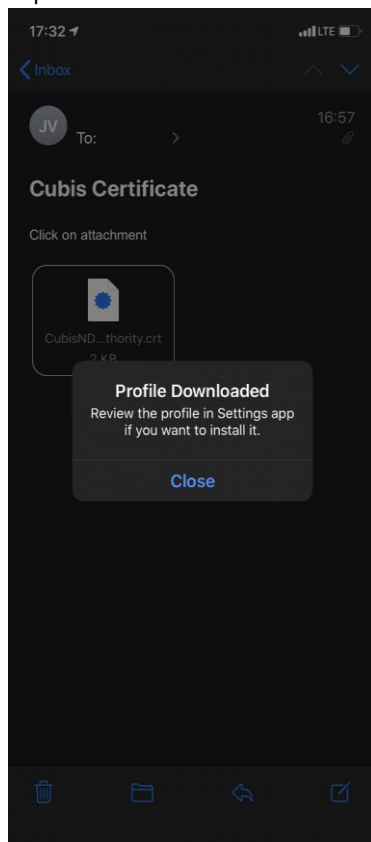


4. Enter a name for the certificate e.g. "Sartorius CubisND"
5. Select "For VPN/Apps" as the certificate category

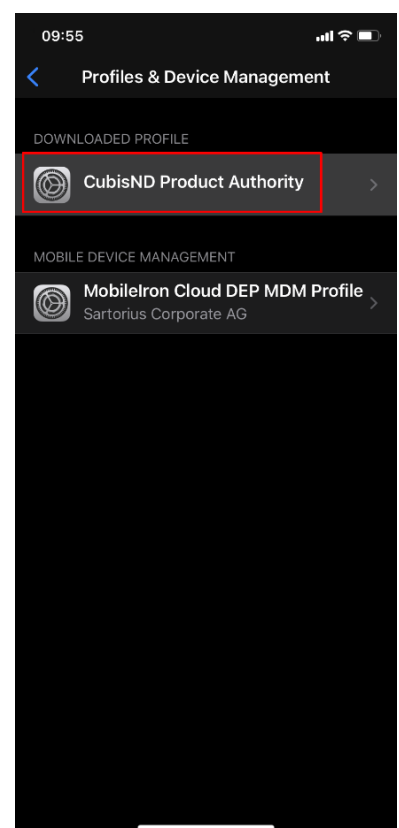
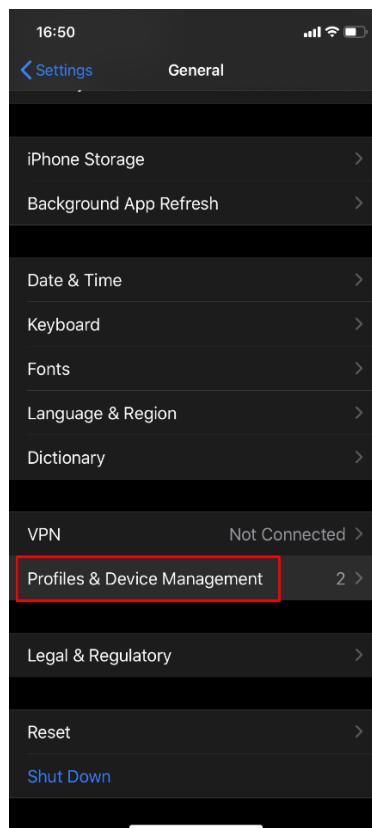
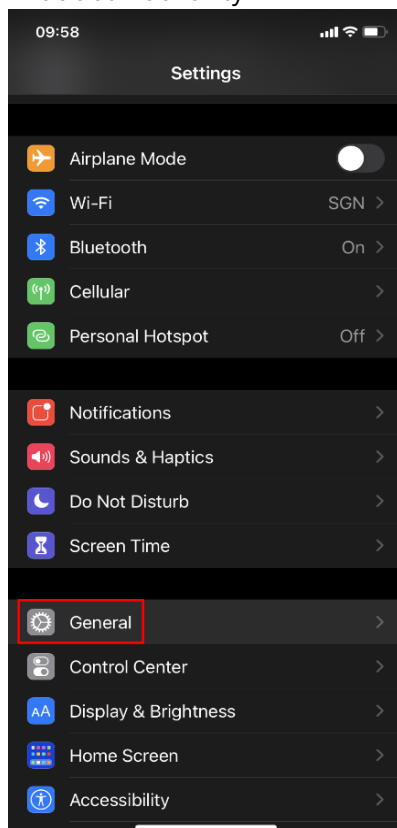


6. Installation for iOS / iPadOS (all browser)

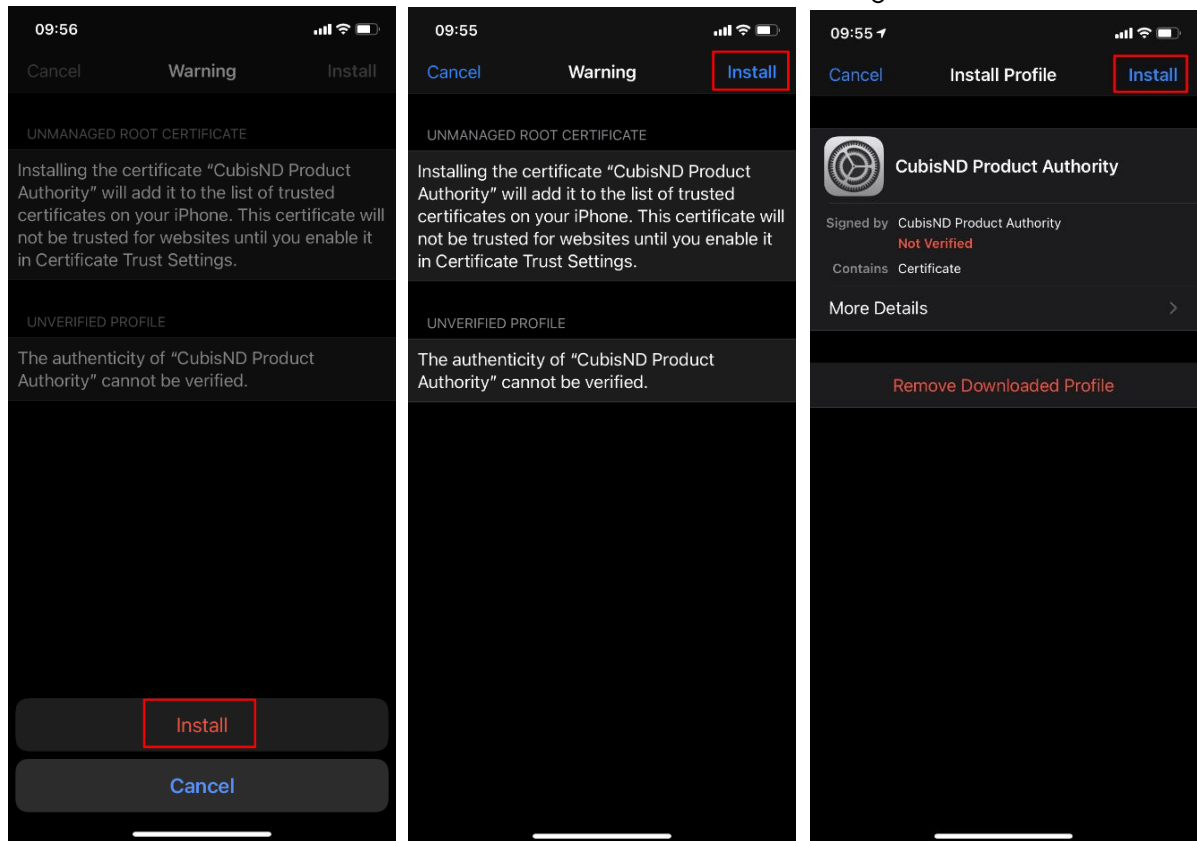
1. Open the downloaded file in the native iOS "Mail" app or in the native "Files" app.



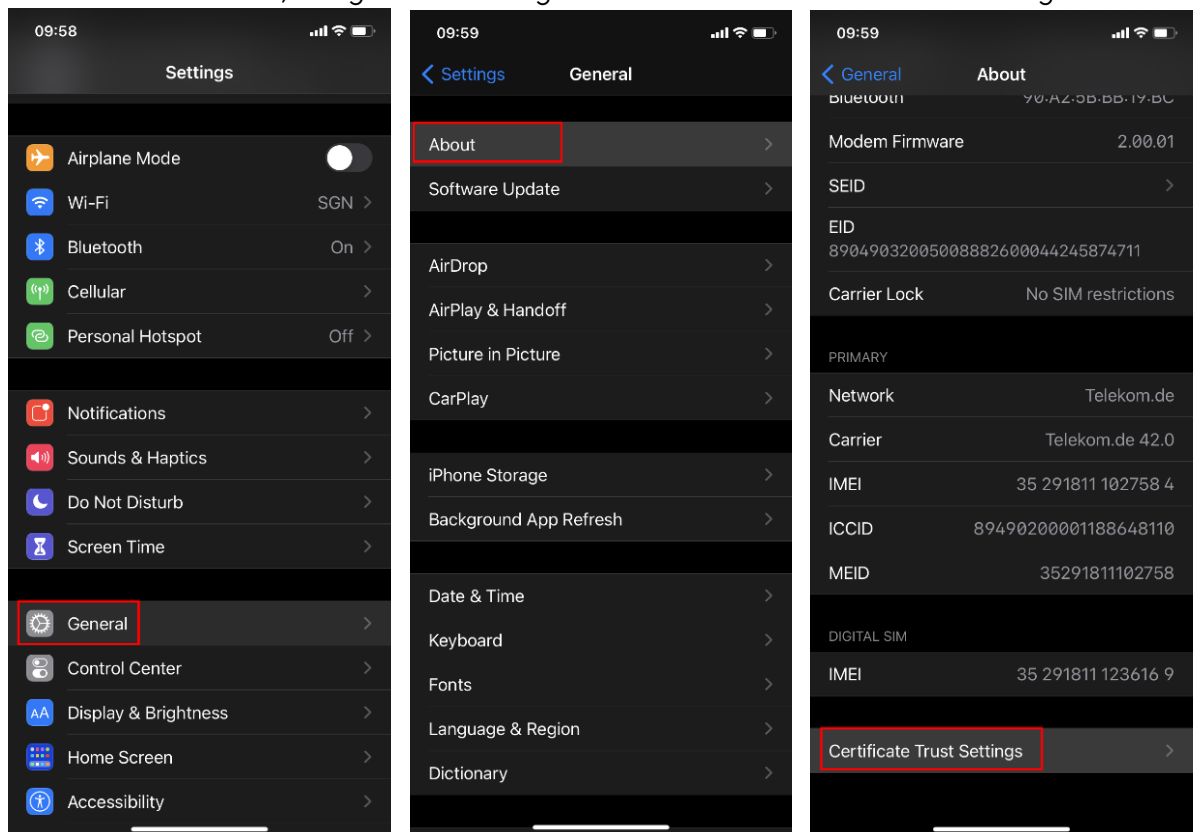
2. Navigate to "Settings" > "General" > "Profiles & Device Management" > "CubisND Product Authority"



- Press "install" three times to confirm the various confirmation dialogs.



- From the main menu, navigate to "Settings" > "About" > "Certificate Trust Settings"



5. Enable the slide switch for "CubisND Product Authority" and confirm with "continue"

