E-Smart Systems d.o.o. | Adress: Kneza Višeslava 70a, 11030 Belgrade, Serbia | Sertification authority (ESS QCA) | Tel: 011 3050280| E-mail: qca@e-smartsys.com | MB: 17247565 , Reg.No: 01117247565 , Bussiness code: 6201, VAT: 101833141

U-QCA-354

Document code

Instructions for Installation of Prerequisites Required to Use a Qualified Certificate for Electronic Signature and Seal – Linux

Content

1. Downloading the ESS QCA Linux Installation Package

The installation package containing all required components can be downloaded from the ESS QCA website at https://essqca.esmartsys.com on the "Download Software" page, click "ESS QCA Linux Installation Package" to start downloading the package.

Before use, extract the ZIP archive by double-clicking it. Locate the downloaded file in the downloads folder and double-click it to begin the extraction process.

After extraction, you can proceed with the installation of the software components required to use an ESS QCA qualified certificate for electronic signature and seal.

Note: The software for certificates is currently only supported on Ubuntu and CentOS distributions and the installations are performed by running commands in the Terminal.

2. Installing the ESS QCA „chain of trust"

ESS QCA „chain of trust" consists of the Root CA i Issuer CA certiicates, which are located in the „Certificates" folder of the Linux installation package. Depending on the date of issue and type of qualified certificate, the appropriate set of specified certificates must be installed.

- For qualified certificates for electronic signature issued before 04/08/2024, the following CA certificates must be installed:
  - **"ESS RQCA.cer"**
  - **"ESS IQCA1(3).cer"**
- For qualified certificates for electronic signature issued after 04/08/2024, the following CA certificates must be installed:
  - **"ESS RQCA V3.cer"**
  - **"ESS IQCA1 V3.cer"**
- For qualified certificates for electronic seal, the following CA certificates must be installed:
  - **"ESS RQCA V3.cer"**
  - **"ESS IQCA2 V3.cer"**

These certificates must be imported into the local Linux system in the following two locations:

a) **/usr/local/share/ca-certificates/,**
b) **/etc/ssl/certs/**

First of all, it is necessary to open the Terminal in the location where the CA certificates are stored, as shown in Figure 1.

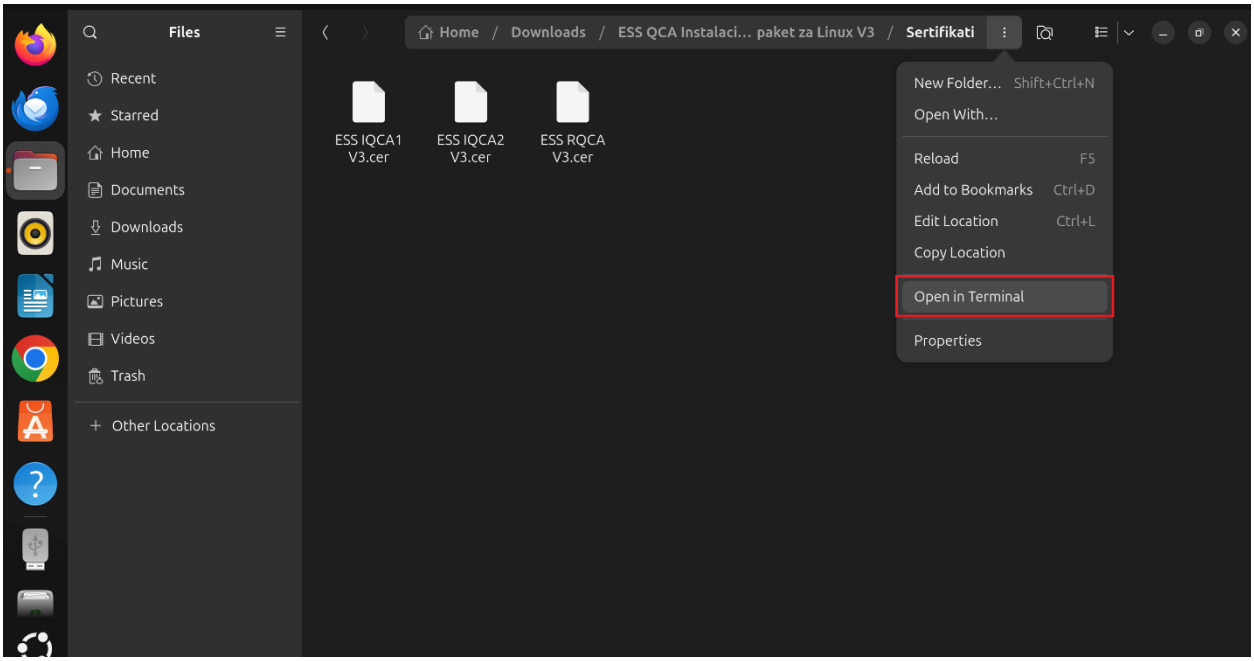

Figure 1.

After that, the certificate installation is executed by running the following commands:

a) ***sudo cp "ESS RQCA V3.cer" /usr/local/share/ca-certificates/***
b) ***sudo cp "/usr/local/share/ca-certificates/ESS RQCA V3.cer" /etc/ssl/certs/***
c) ***sudo update-ca-certificates***

Napomena:

- Command **a)** must be executed for each CA certificate in the chain of trust being imported. For example, for the V3 Root CA and Issuer CA, the following commands are executed:
    - sudo cp "ESS RQCA V3.cer" /usr/local/share/ca-certificates/
    - sudo cp "ESS IQCA1 V3.cer" /usr/local/share/ca-certificates/
- Command **b)** must be executed for each CA certificate previously imported via command a), in order to transfer those certificates from /usr/local/share/ca-certificates/ to /etc/ssl/certs/. If you encounter an issue executing command b) and are unable to transfer the certificates, it means the current user lacks the necessary permissions to transfer files to /etc/ssl/certs/. In this case, you need to grant the appropriate permissions for the certificates by running the command **sudo chmod 644 "/usr/local/share/ca-certificates/ESS RQCA V3.cer"**. After executing this command, you must rerun command **b)** for each problematic CA certificate.
- Command **c)** needs to be executed only once at the very end, after successfully executing commands **a)** and **b)**.

3. Installation of ESS QCA SafeNet Authentication Client Middleware

In order for the Linux system to recognize the smart card chip containing the qualified certificate for electronic signature or seal, it is necessary to install the SafeNet Authentication Client middleware. The "SafeNet Authentication Client Linux" folder contains subfolders for selecting the Linux operating system distribution: "Ubuntu" or "CentOS". Each of these two folders contains an "Installation" directory, which includes options for selecting the installation type: "Standard" and "withoutUI" (without the SAC Tool). It is recommended to always install the "Standard" version. If you are using an Ubuntu machine, open the "Ubuntu" folder, which contains the file with the .deb extension. The selected file must be executed from the Terminal. As shown in Figure 2, open the Terminal using the shortcut:

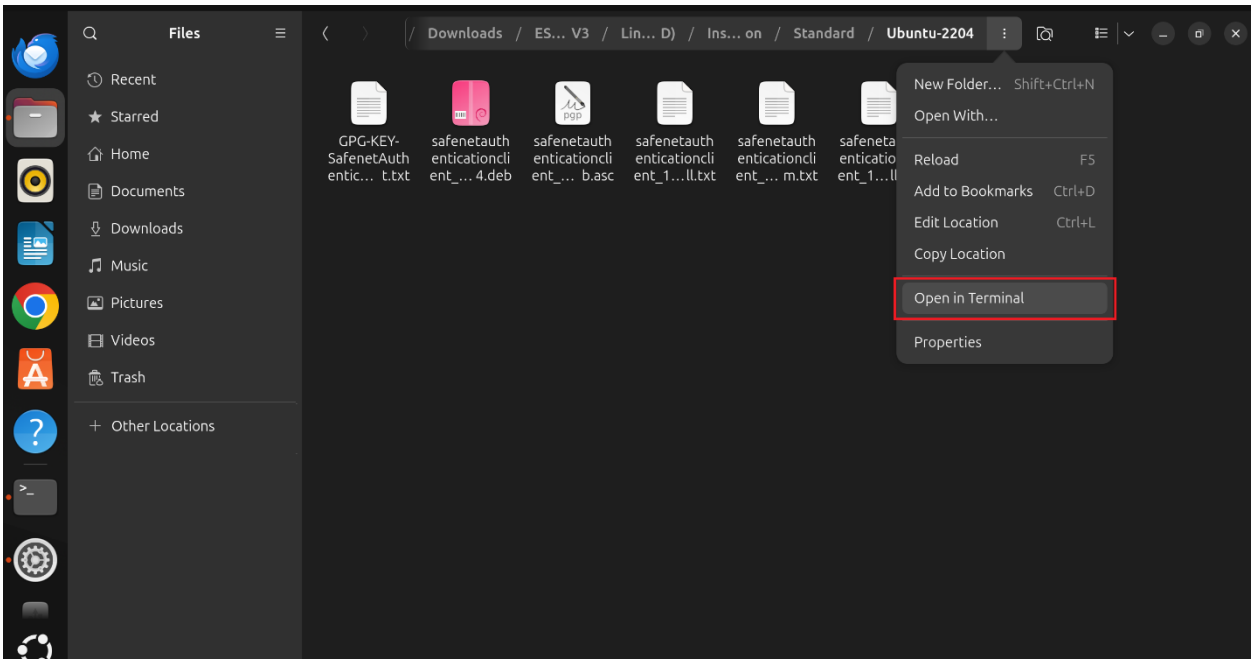

Figure 2.

Run the installation command**: sudo apt install ./safenetauthenticationclient_10.9.6885_amd64.deb**

If the installation fails and you receive an error such as: **couldn't be accessed by user "_apt" pkgAcquire::run (13: Permission denied)**, run the following command to fix the permissions: **sudo chmod 644 ./safenetauthenticationclient_10.9.6885_amd64.deb**

Then, retry the installation command. It is highly likely that the system will prompt you for your user password; if so, enter it and proceed with the installation.If you have accidentally installed the wrong package version, open the Terminal and run the following command to completely remove it: **sudo apt remove --purge safenetauthenticationclient**.

After that, restart your machine and attempt to install the correct package again.

Once the SafeNet Authentication Client middleware is successfully installed, you can verify it in the App Manager. The application should appear as shown in Figure 3.

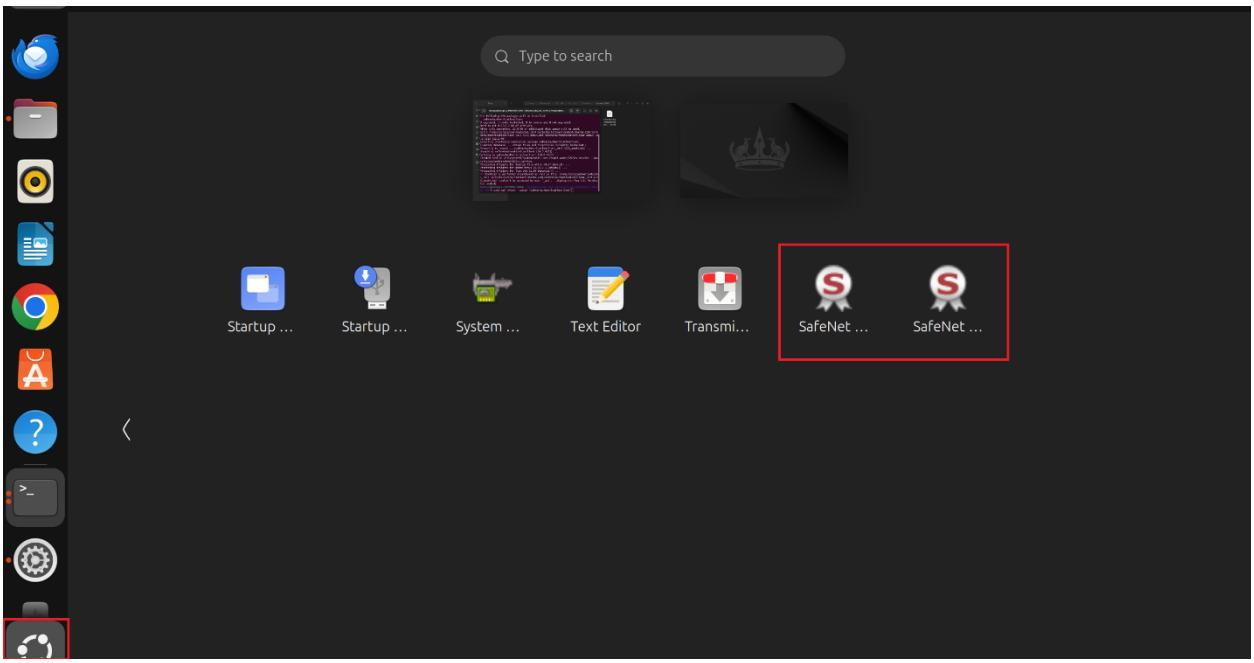

Figure 3.

4. Additional Configuration for Using the Qualified Certificates in Web Browsers

In order for web browsers to detect the qualified certificate, it is necessary to run the following three commands:

a) **sudo apt update,**

b) **sudo apt install libnss3-tools,**

c) **modutil -dbdir sql:$HOME/.pki/nssdb -add "SafeNet PKCS11" -libfile /opt/SafeNetAuthenticationClient/lib/libeToken.so**

Note: These steps are mandatory because browsers do not natively recognize tokens or smart cards; instead, they rely on PKCS#11 modules for access. This configuration is required so that the user can use the certificate for authentication in both Firefox and Chrome browsers..

5. Installing Drivers for ACS Smart Card Readers

Before proceeding with this step, please go to step 6 to determine whether it is actually necessary to install the drivers for ACS smart card readers. If the smart card reader is not recognized (i.e., the certificate does not work because the system cannot detect the reader itself), you should proceed with the ACS driver installation.

The ACS driver package is located in the folder **Smart Card Reader Drivers Linux / ACS Driver linux**. Similar to the SafeNet middleware installation, you need to locate the folder corresponding to your Linux distribution and version. Open that folder, and if you see a file with a .deb extension, open the Terminal using the shortcut shown in Figure 4.

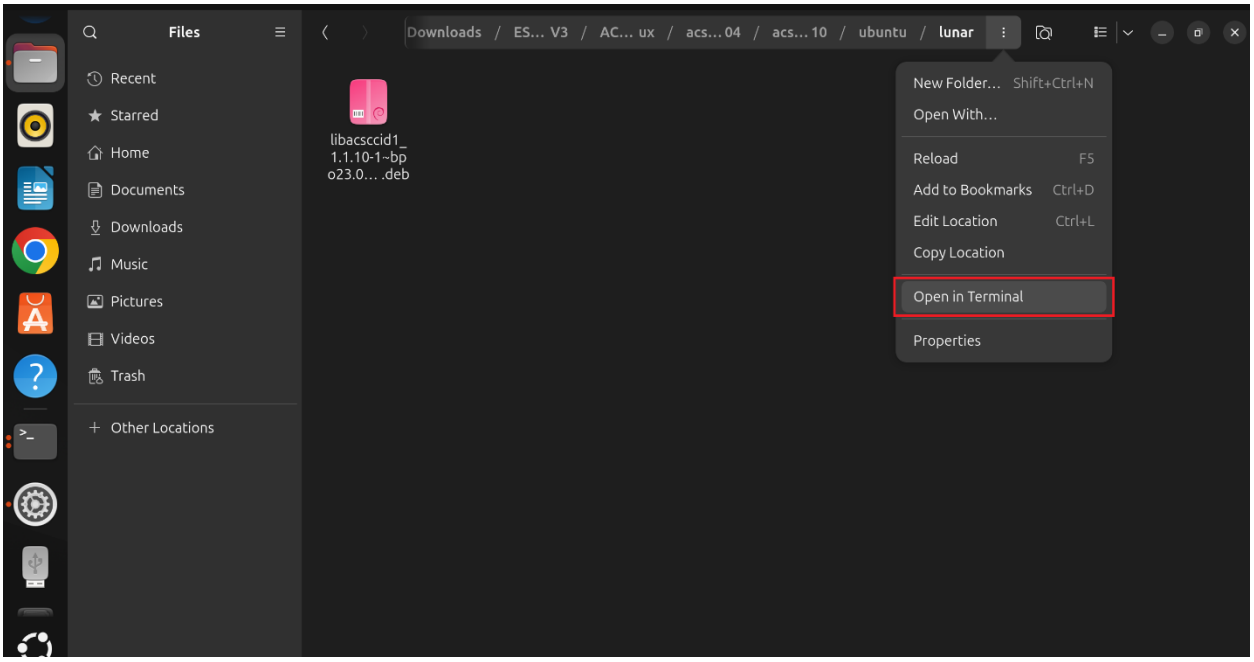

Figure 4.

Run the command: **sudo apt install ./[package-name (*driver-ver,linux-ver*)].deb**, then restart your computer and proceed to step 7.

6. Installing Drivers for Thales-Gemalto Smart Card Readers

Before proceeding with this step, please go to step 7 to determine whether it is actually necessary to install the drivers for Thales-Gemalto smart card readers. If the smart card reader is not recognized (i.e., the certificate does not work because the system cannot detect the reader itself), you should proceed with the Thales-Gemalto driver installation.

The Thales-Gemalto driver package is located in the folder **Smart Card Reader Drivers Linux / Thales - Gemalto Driver linux**. Similar to the SafeNet middleware installation, you need to locate the folder corresponding to your Linux distribution and version. Open that folder, and if you see a file with a .deb extension, open the Terminal using the shortcut shown in Figure 5.

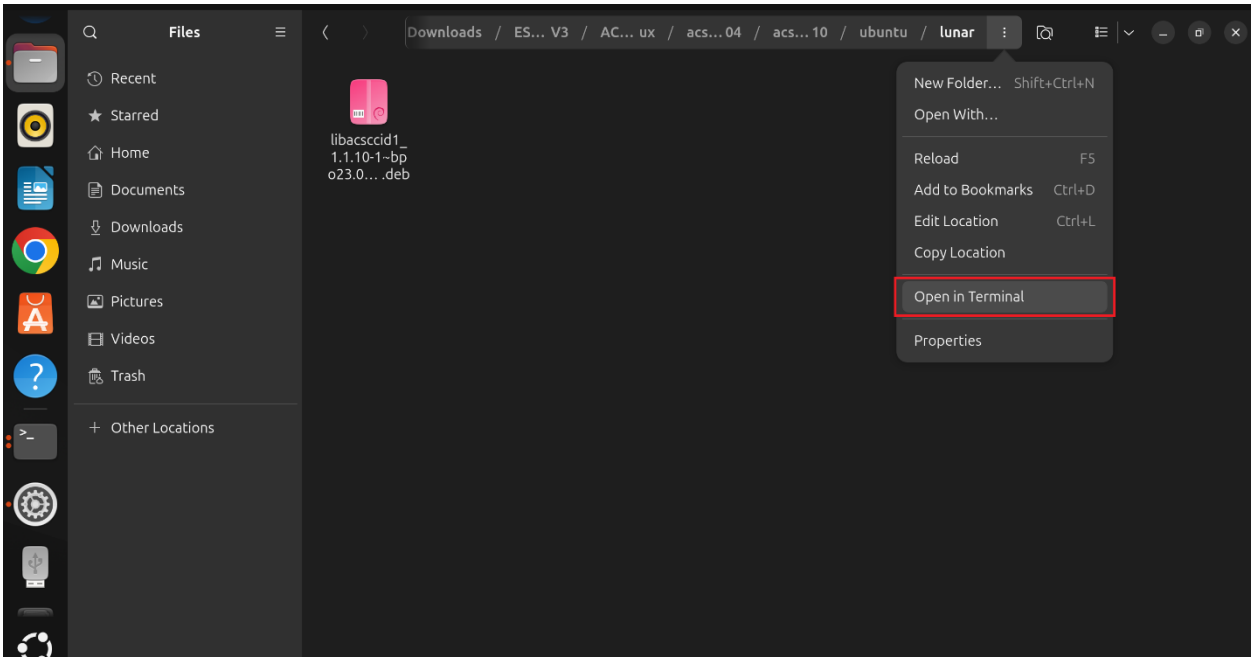

Figure 5.

Run the command: **sudo apt install ./[package-name (driver-ver,linux-ver)].deb**, then restart your computer and proceed to step 7.

7. Verifying the Installation of Prerequisites for Qualified Certificates on Linux

As confirmation of a successful installation of all necessary prerequisites on the Linux system, the SafeNet Authentication Client icon will appear in the top bar (header), as shown in Figure 6..

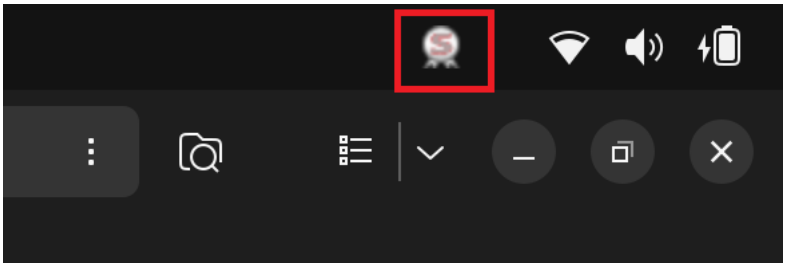

Figure 6.

(Note: If you do not see this icon, you need to find the SafeNet Authentication Client in the App Manager and launch it).

Once you insert your qualified certificate into the computer, the SafeNet icon in the top bar will light up, as shown in Figure 7. This indicates that the computer is ready to use the qualified certificate. If the reader is faulty or the qualified certificate is not properly inserted, the icon will remain gray (as shown in Figure 6), and you should verify that the qualified certificate is placed correctly inside the smart card reader.

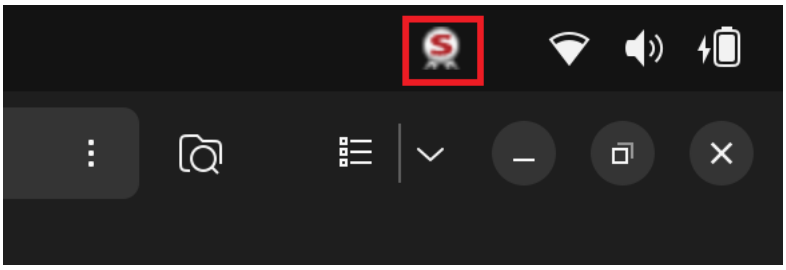

Figure 7.

In case of any issues, please submit a ticket via our web form or send an email to qca@esshitsupport.zohodesk.eu, and we will contact you as soon as possible.