Client Certification

13/01/2022

Presented By: Louis Hamers

Purpose: This webinar is solely for providers who have not installed their certificate (to access the CTS++ platform) yet. No other topics will be discussed.

Note: This webinar is being recorded. Questions can be asked in the TEAMS chat.

Agenda

1. Why Client Certification
2. Timeline
3. Step by Step Guide
4. Q&A

part of eex group

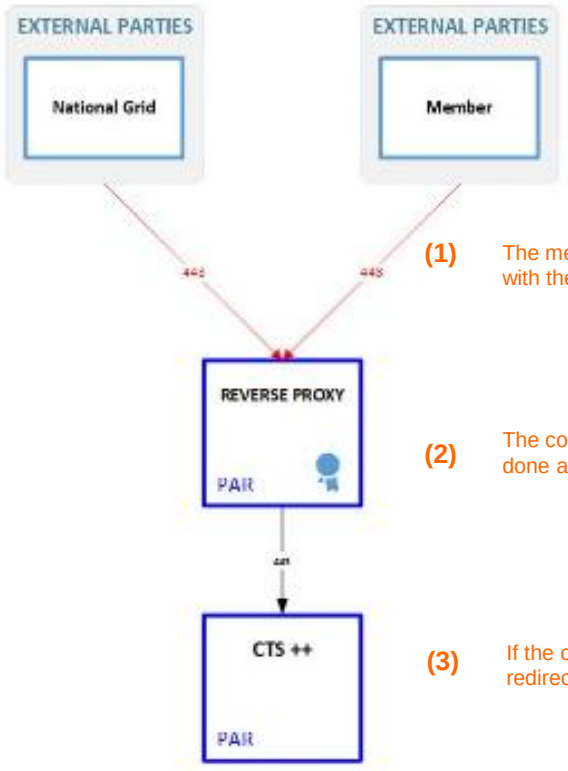
Why Client Certification?

A digital certificate that is used by the end-user system to make authenticated request to a remote server.

The certification is installed on the device and the Web Browser of the end-user, otherwise the end-user cannot connect.

End-users will install it on their device from where they want to access CTS++ platform. Benefits of Client Certification are:

- **Secure Multi Factor Authentication**
- **User-friendly** - once installed no further interaction required until certification expires
- Renewal **once a year**
- **Reduction** of operational **cost** and **risk**
- Certificates are **centrally managed**



(1) The members goes to the CTS++ website with the certificate installed on his browser

(2) The control of the certificate is done at the reverse proxy level

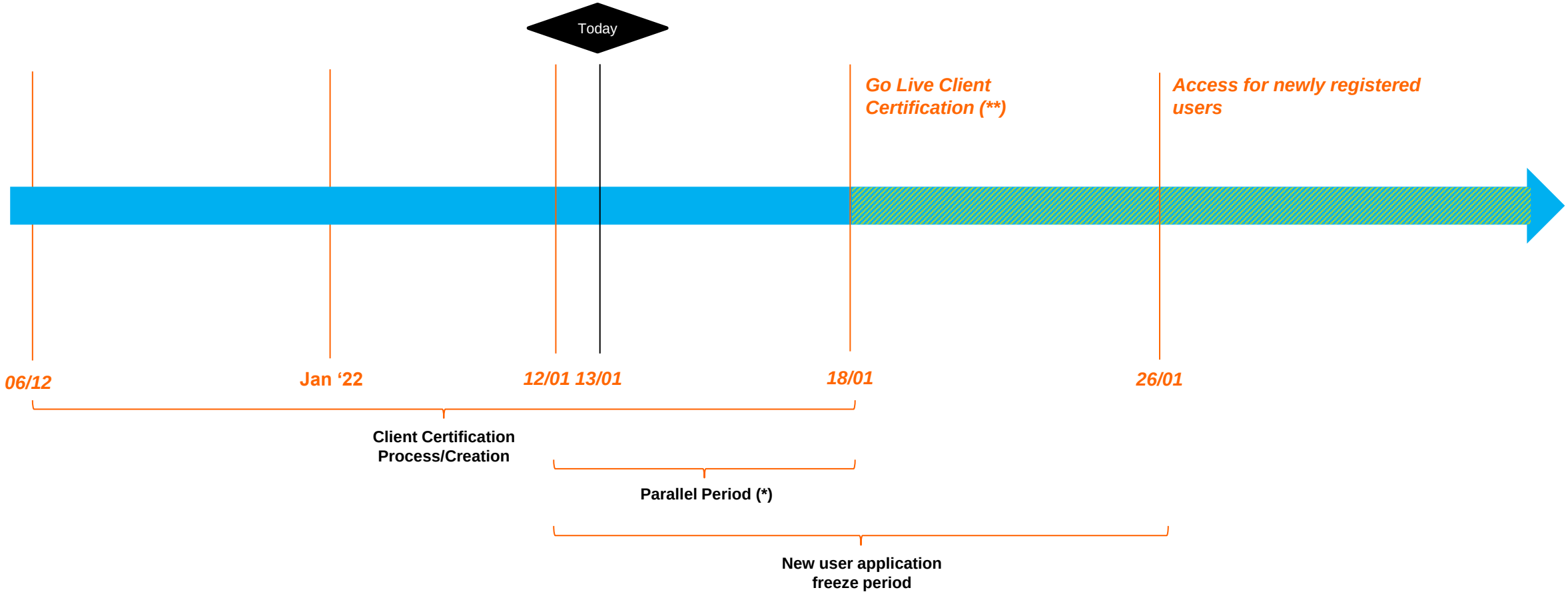
(3) If the certificate is validated, the member is redirected to the CTS++ authentification page

Agenda

1. Why Client Certification
2. Timeline
3. Step by Step Guide
4. Q&A

part of eex group

Timeline of Client Certification Process



(*) Registered users can access the CTS++ platform either with their user credentials OR user credentials and Client Certificate

(**) Starting from 5PM CET on Tuesday 18/01, registered users who have not installed their certificate will not be able to access the CTS++ platform anymore

Agenda

1. Why Client Certification
2. Timeline
3. Step by Step Guide
4. Q&A

epexspot

part of eex group

Step by Step Guide

Three main tasks required from CTS++ Users

1. Download OpenSSL
2. Create CSR file and provide the file to EPEX team
3. Receive the .PEM file from EPEX team and install + follow instructions

All steps and information on the Client Certification process are detailed in the installation guide in Section 3

CTS++ - Certificates Installation Guide_v0.5.pdf

Agenda

1. Why Client Certification
2. Timeline
3. Step by Step Guide
4. Q&A

part of eex group

Q&A - **Updated**

- Can we have the same certificate for multiple machines in case we are using a generic email account to access CTS++?

  A same certificate can be installed on multiple machines/units

- How can we check if the certificate has been installed?

  See next slide 10

- What if I have Apple OS and no Windows OS?

  A seperate guide can be provided

- I cannot install the OpenSSL software?

  Use the alternative online tool → https://decoder.link/csr_generator

- How long is the certificate valid for?

  One year

- How do I know when my certificate will expire? Will I be informed about this?

  You will be informed through email one month in advance by EPEX Market Operator Team

- Can we generate the CSR from ISS instead of OpenSSL and export the PFX that way?

  Yes, this is possible.

How to check if you Certificate has been installed?

1. Go to ‘’Browser Settings’’

2. Search for ‘’Certificates’’, usually found in ‘’Privacy and Security’’

3. Click on ‘Manage Certificates’

4. Verify if the Certificate is in place