Public

Report

Creation of self-signed Certificates for ECP-CD Tests

|  |  |
| --- | --- |
| Version | V0.1 of 23rd July 2019 |
| Author | Uwe Schröder Technology |

Distribution list

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Company** | **Note** | **Date** |
|  |  |  |  |
|  |  |  |  |

Revision

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **V0.1 of** | **Author / Department** | **Section** |
|  |  |  |  |
|  |  |  |  |

Content

[1 Motivation 3](#_Toc14942356)

[2 Background 4](#_Toc14942357)

[3 Procedure 5](#_Toc14942358)

# Motivation

This document describes the creation of the certificate store to setup ECP-CD for testing purposes.

# Background

The Certificate Authorities, like other certificates, have an expiration time and may be compromised. Although these events will occur scarcely, a process allows replacing the old or compromised certificate authorities with new ones. The GUI only supports part of the procedures, but some steps have to be performed outside of the ECP software.

The process requires the cooperation of the ECP Root Certificate Authority Administrator (ECP CA Administrator), the Component Directory Administrators (CD Administrators) and ECP Components Administrators.

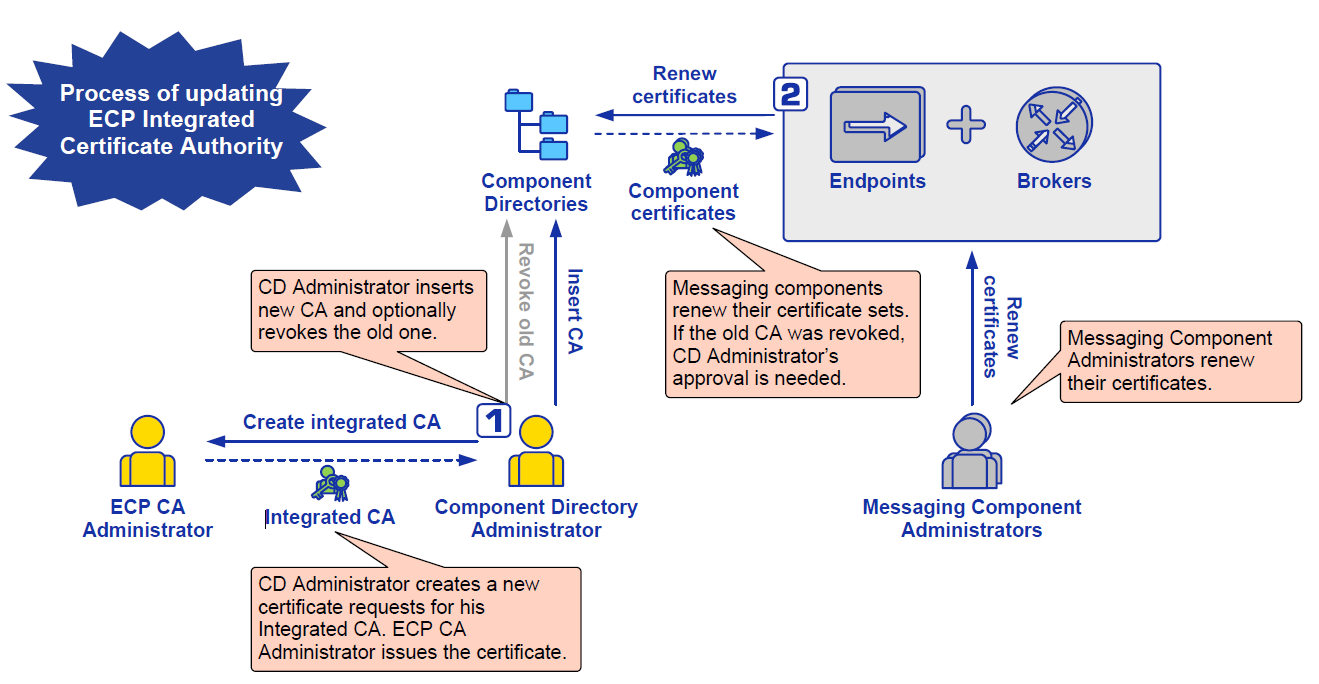


Figure 1: Build Own Registration Certificate

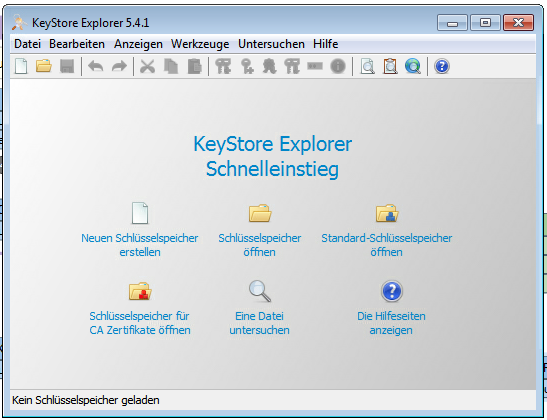
# Procedure

In an ECP network it is sufficient to have 1 ECP CD. In case 2 ECP Endpoints which should communicate together are registered in different ECP CDs, then ECP CD synchronization has to be configured for both of them. Since ECP version 4.4 it is possible to synchronize ECP CD with different root CAs.

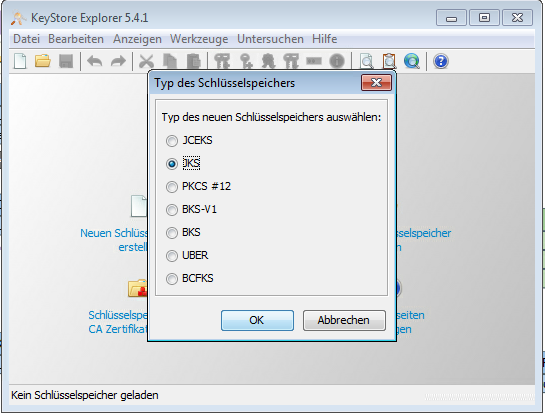
Below versions of ECP can synchronize only ECP CDs with the same root CA.

Root and integrated certificate generation process for Windows and KeyStore Explorer:

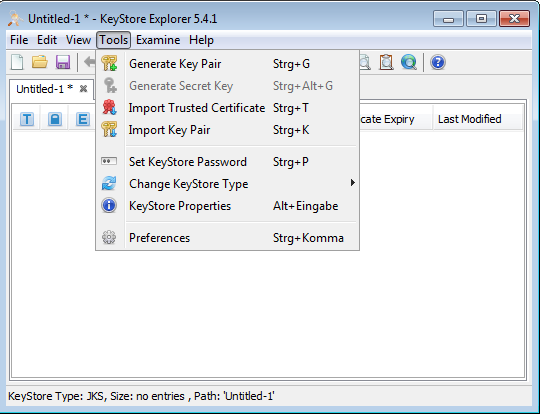
1. Start KeyStore Explorer application



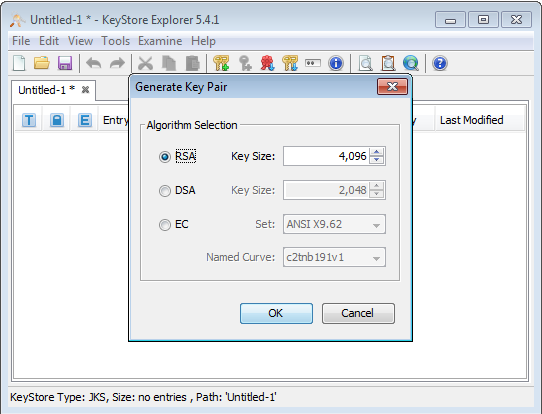
1. Select "Create a new KeyStore" and type "JKS"[[1]](#footnote-1)

**Summary:** Use BCFKS or Hardware Security Modules (HSM) or at least PKCS#12 key store, and specify manual Password Protection arguments when storing keys with PKCS#12. Avoid the proprietary key stores, like JKS or JCEKS

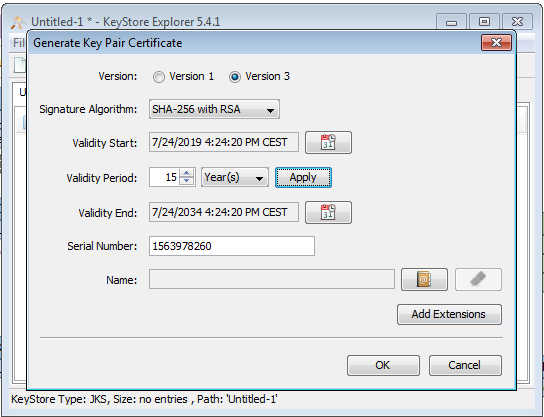
1. Creation of root (global) certificate  
   * Click on Tools -> Generate Keypair



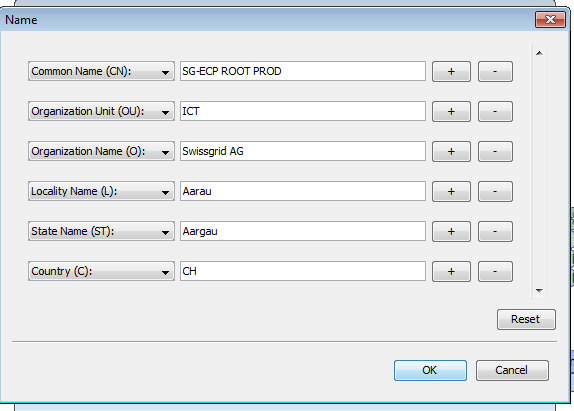
* + Generate Key Pair screen
    - Select RSA Algorithm with key size 4096, then click OK



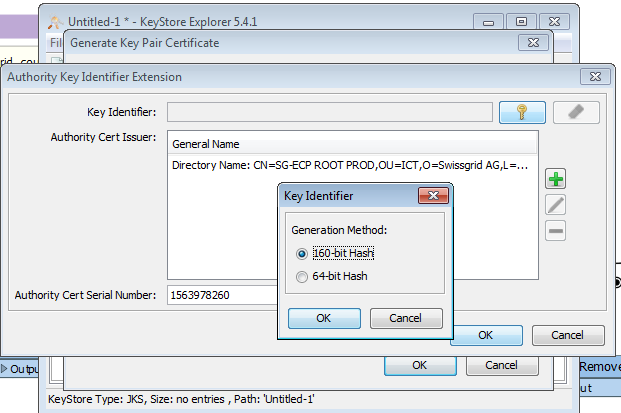
* + Generate Key Pair Certificate screen
    1. Select Version 3, SHA-256 with RSA, validity period e.g. 15 years and click Apply



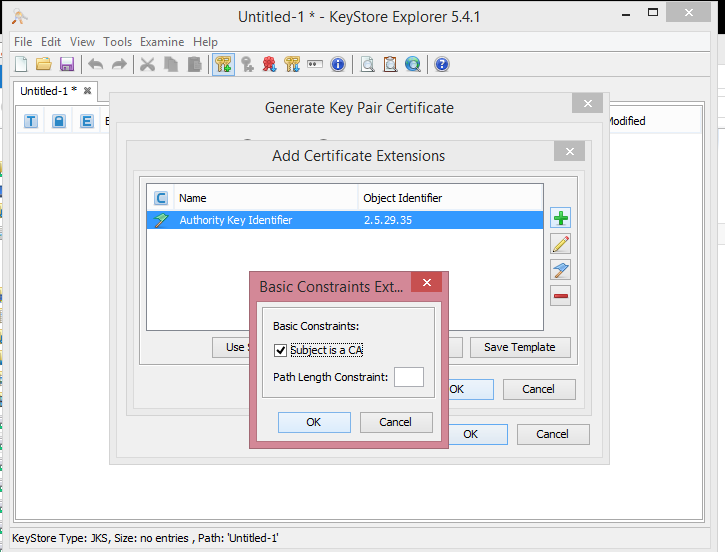
* + 1. Fill the name fields - email, common name, organization, locality name and country



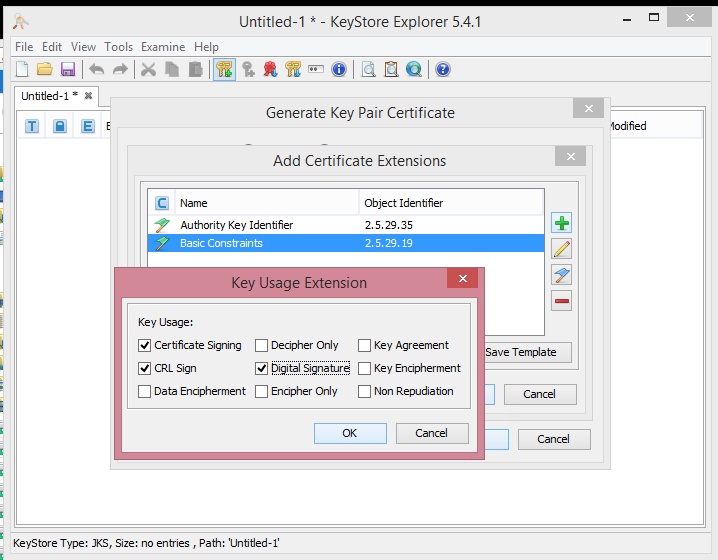
* + 1. Add Extensions
       - Authority Key Identifier - Key Identifier 160-bit hash



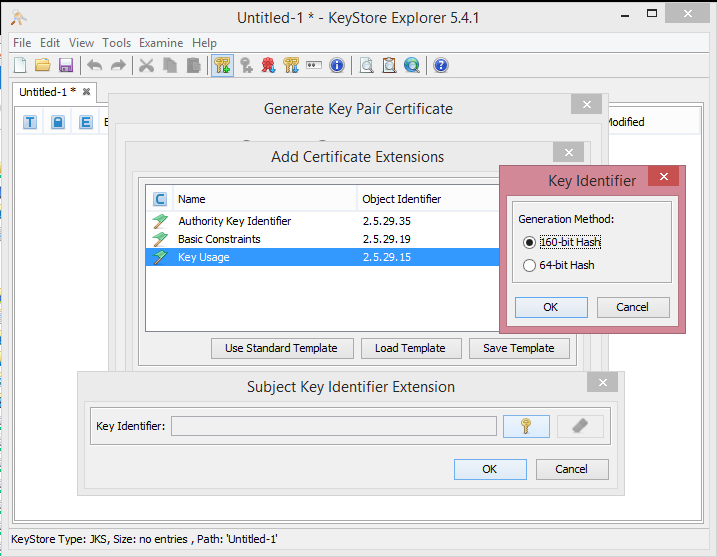
* + - * Basic Constraints with Critical flag - Mark "Subject is a CA"



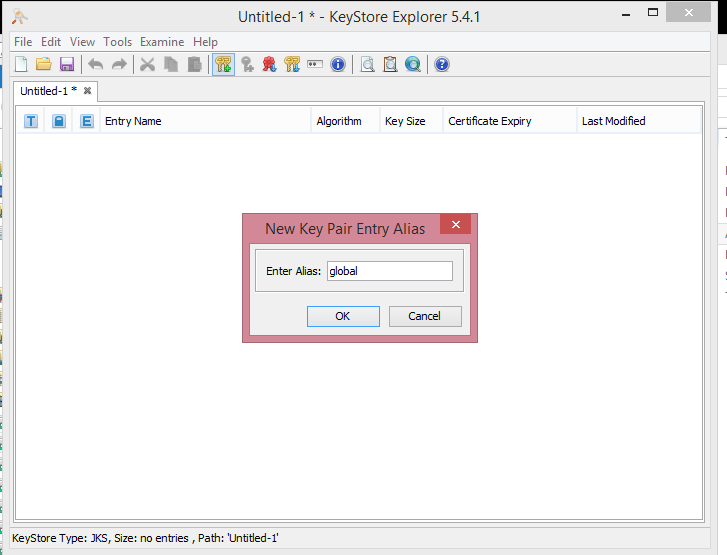
* + - * Key Usage - Select "Digital Certificate", "Certificate Signing", "CRL Signing"



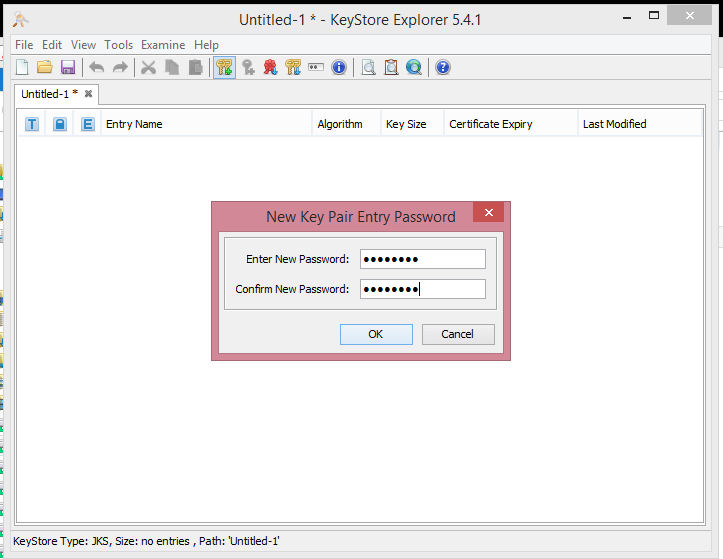
* + - * Subject Key Identifier - Key Identifier 160-bit hash

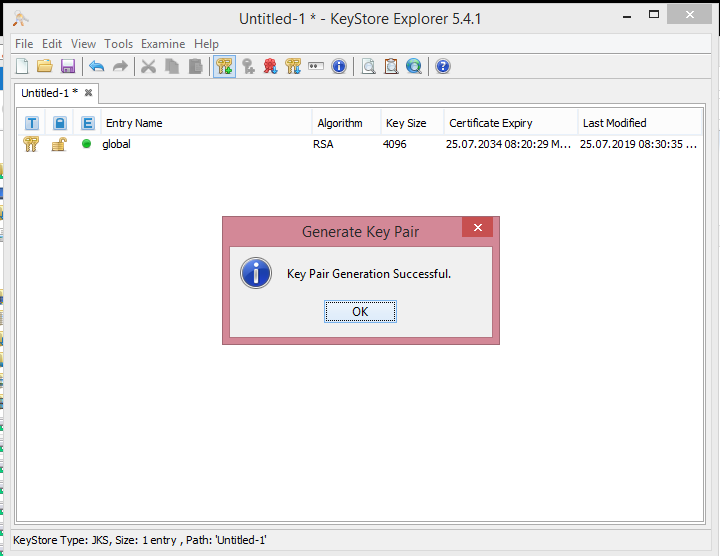


* + - * Click OK
    1. Click OK
  + Click OK
  + Enter Alias "global"

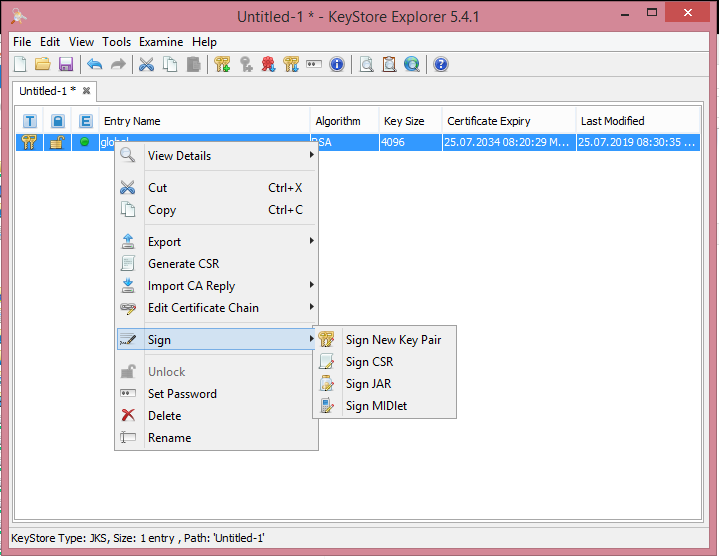


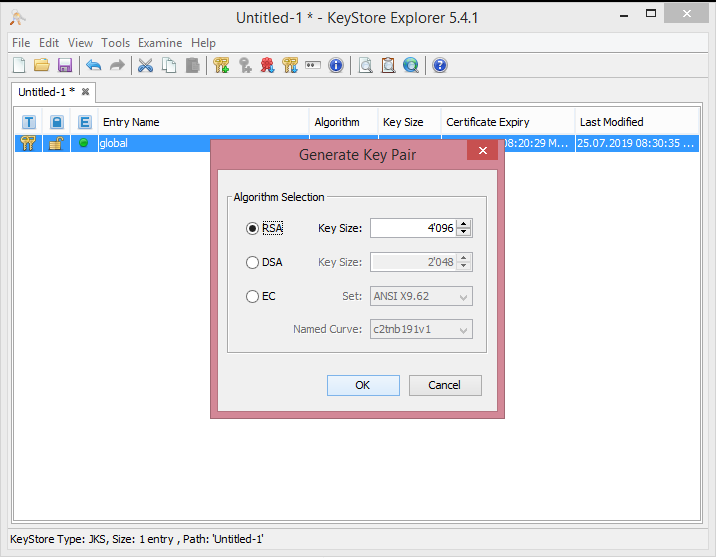
* + Enter new password "password"

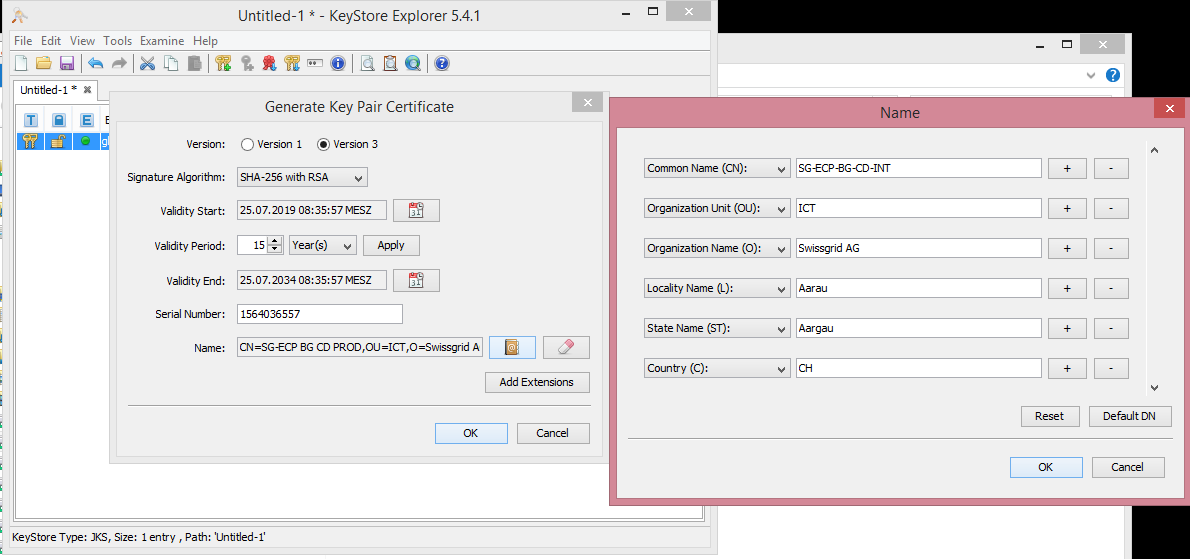




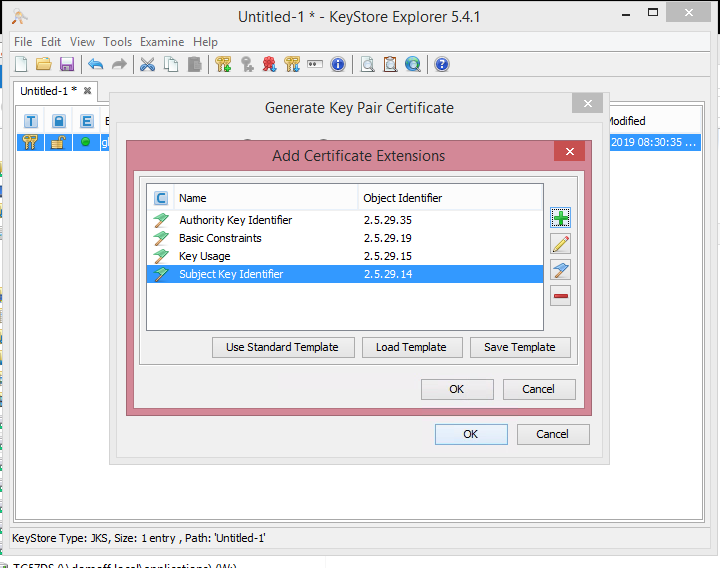
1. Creation of integrated certificate (for ECP CD)
   1. Right click on global certificate and select Sign -> Sign New Key Pair

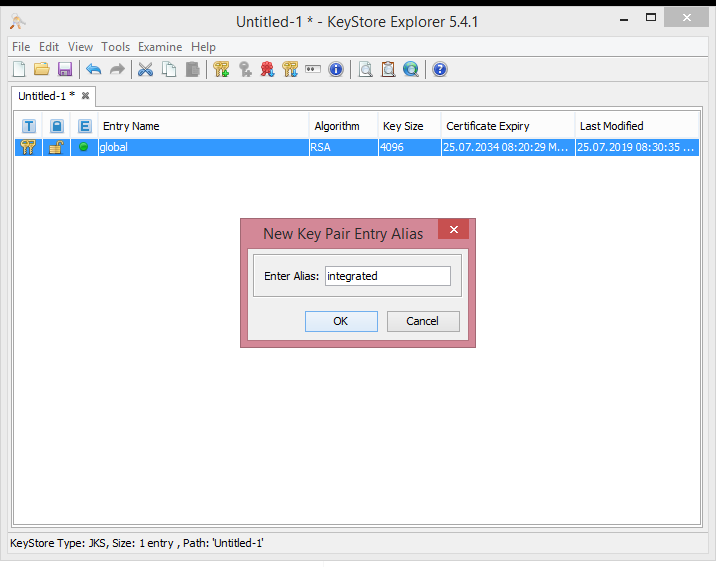


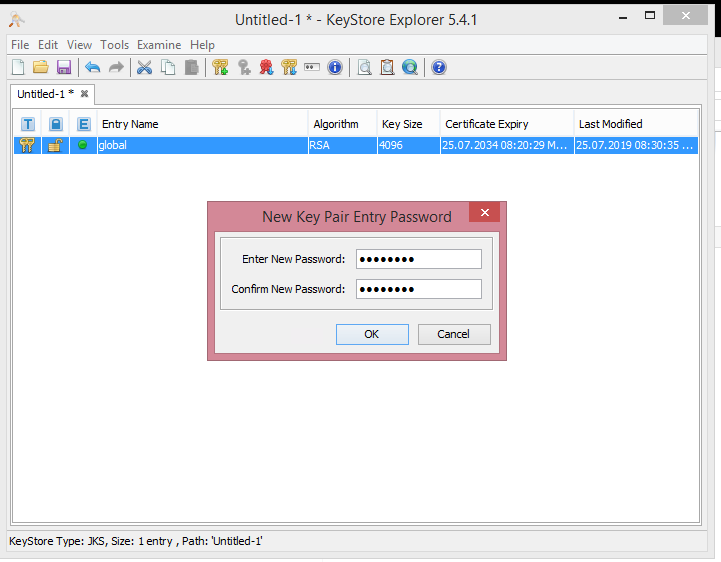
* 1. Generate Key Pair screen
     + Select RSA Algorithm with key size 4096, then click OK
  + 
  1. Generate Key Pair Certificate screen
     + Select Version 3, SHA-256 with RSA, validity period e.g. 15 years and click Apply
     + Fill the name fields - email, common name, organization, locality name and country



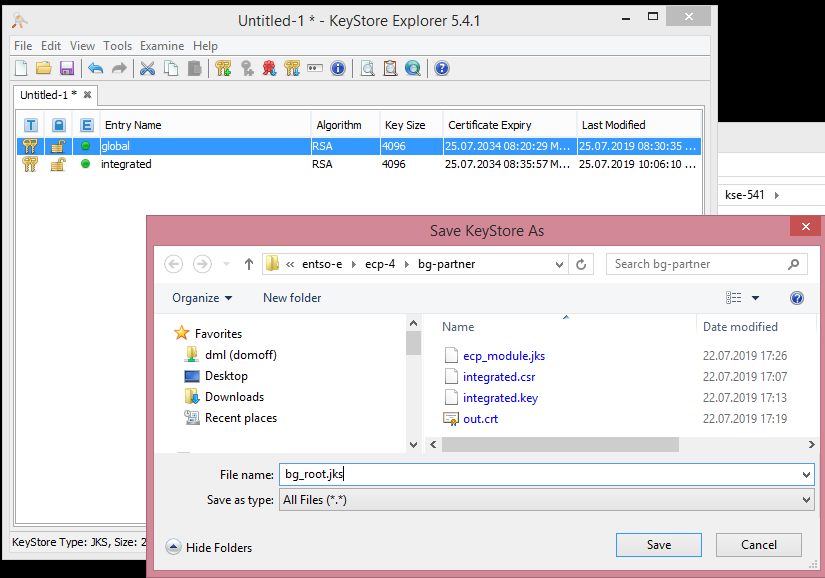
* + - 🡪 Common name has to be vCode of the ECP CD
  1. Add Extensions
     + - Authority Key Identifier - Key Identifier 160-bit hash
       - Basic Constraints with Critical flag - Mark "Subject is a CA"
       - Key Usage - Select "Digital Certificate", "Certificate Signing", "CRL Signing"
       - Subject Key Identifier - Key Identifier 160-bit hash
       - Click OK



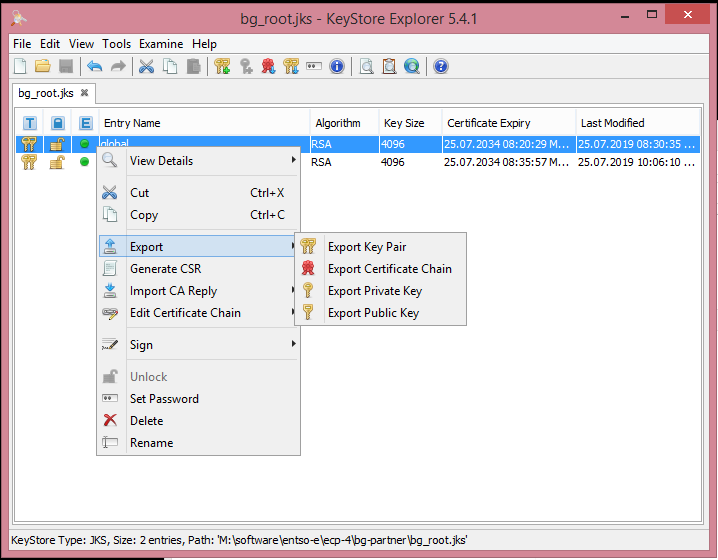
* 1. Click OK
  + Click OK
  + Enter Alias "integrated"
  + 
  + Enter new password "password"

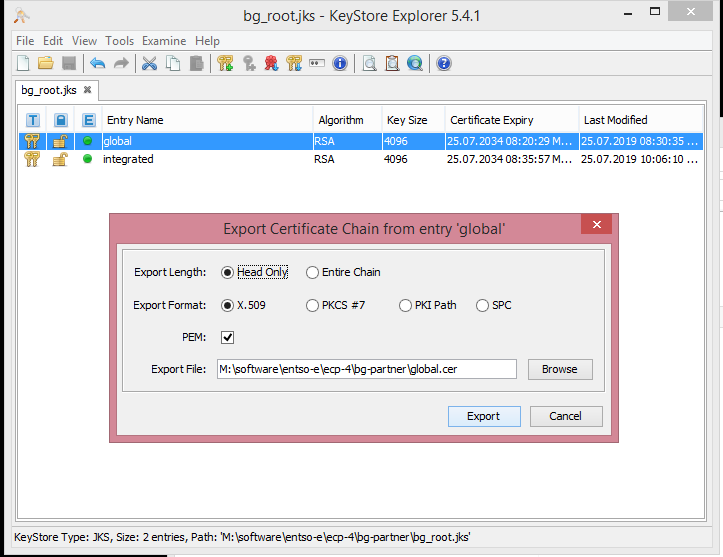


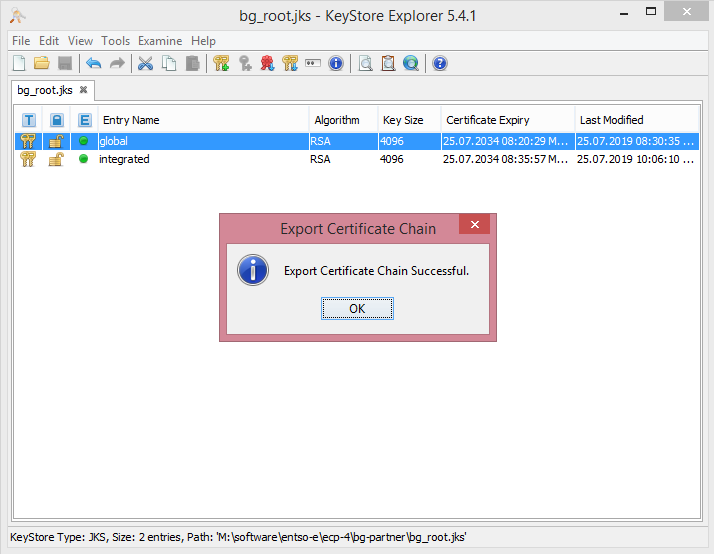
* + Save the created keystore and place it on safe place - this is the keystore which can be used for generating certificates for another ECP CDs



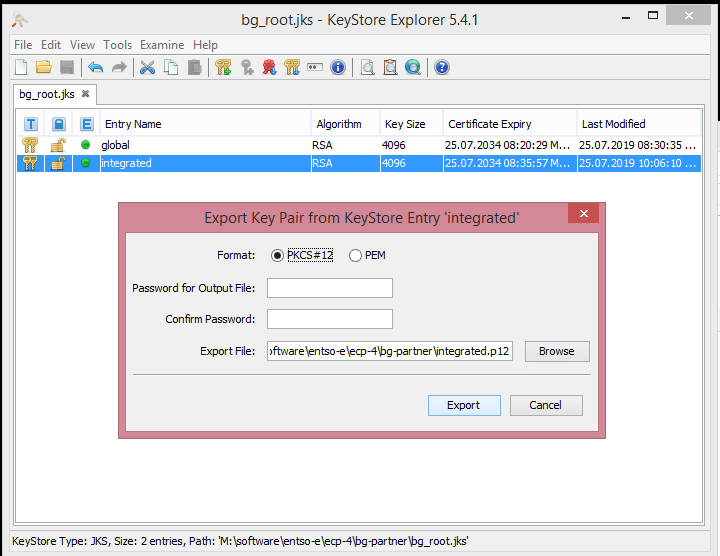
* + Right click on global certificate and select Export -> Export Certificate Chain
    - * Head Only, X.509, PEM
      * Save it as global.cer

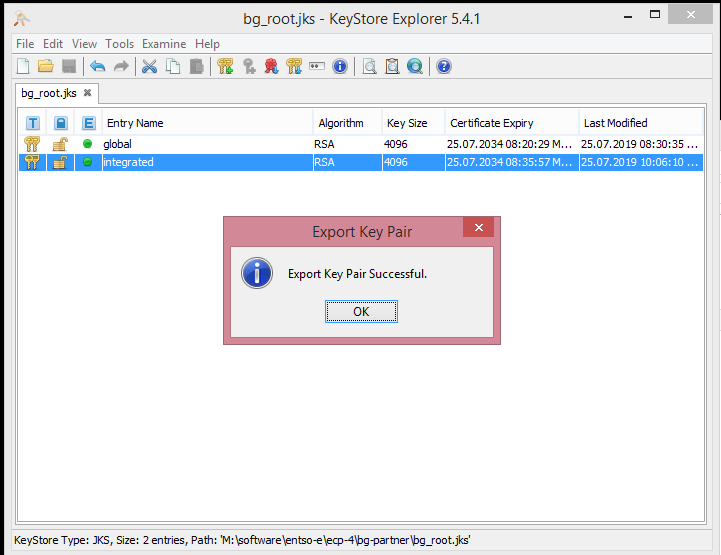




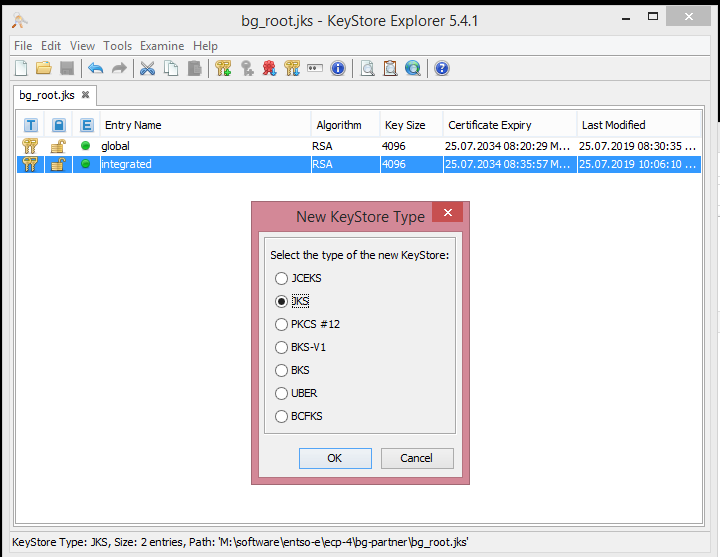


* + Right click on integrated certificate and select Export -> Export Key Pair
    - * Save it as integrated.p12

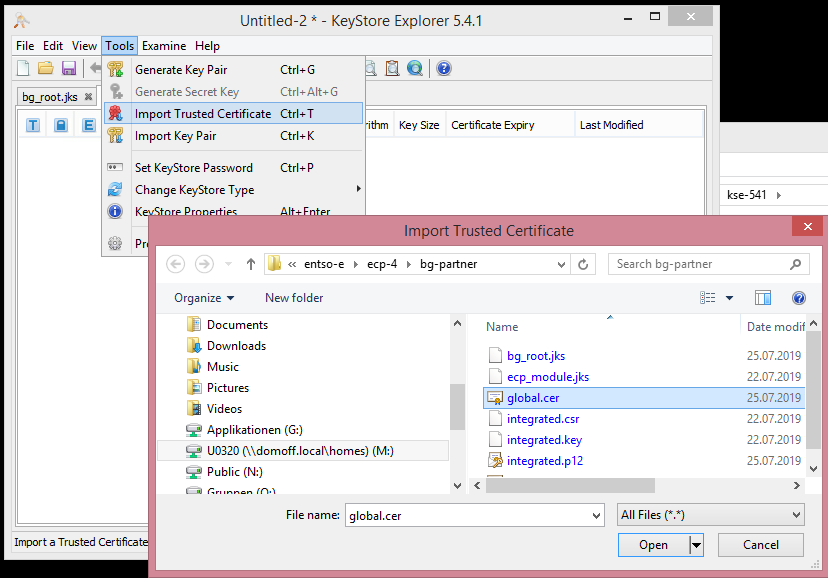




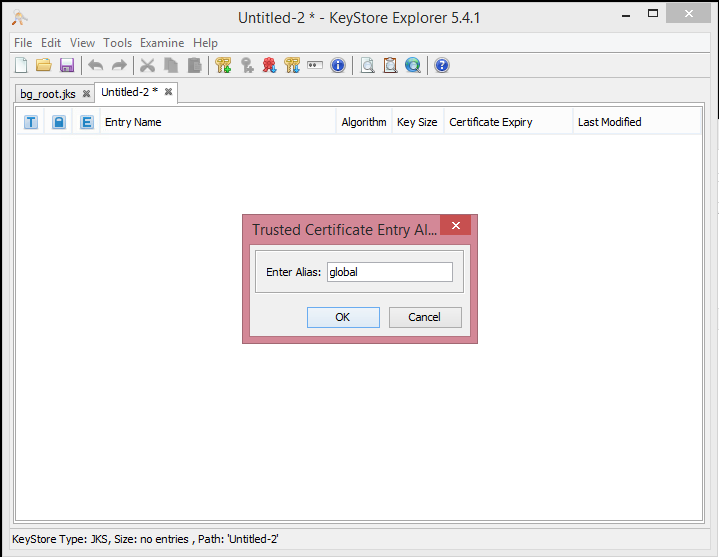
* + Compilation of keystore for ECP CD
  + Click on File -> New and select JKS

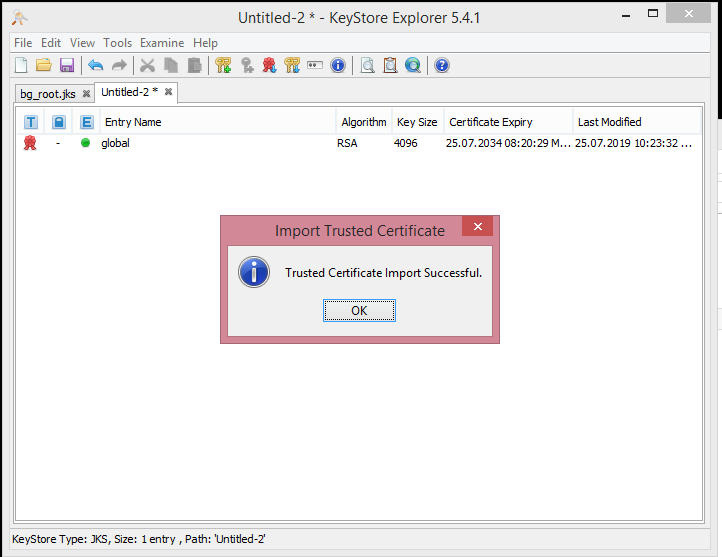


* + Click on Tools -> Import Trusted Certificate and select file global.cer

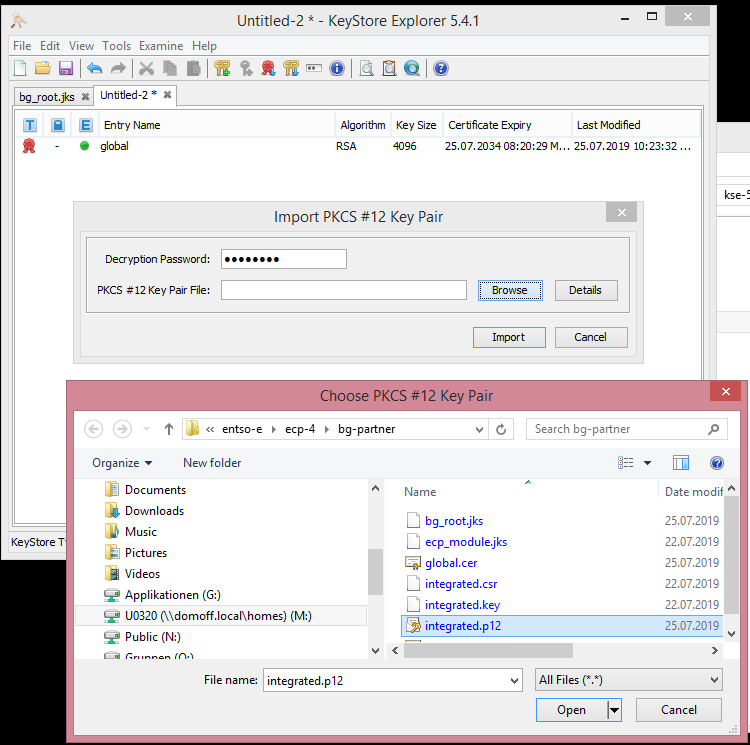


* + - Fill Alias "global"

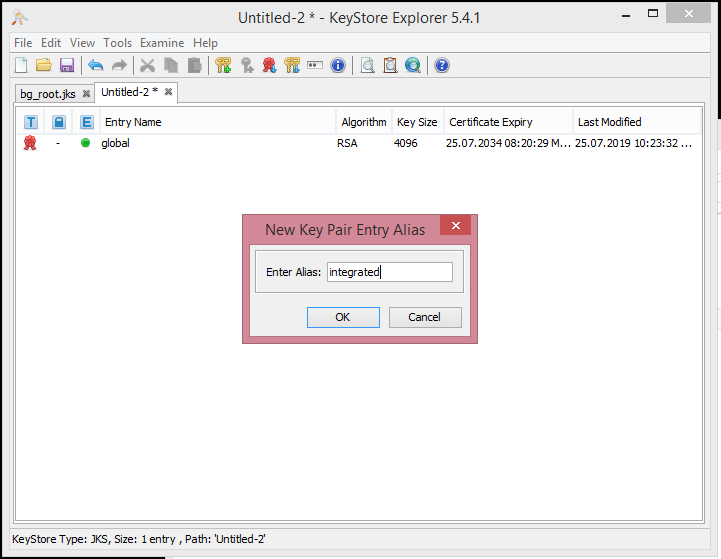


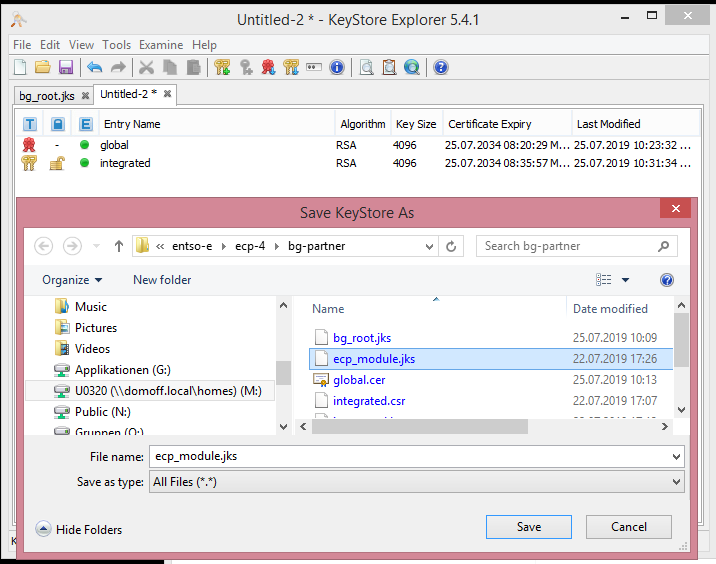


* + Click on Tools -> Import Key Pair, select PKCS #12 and select file integrated.p12

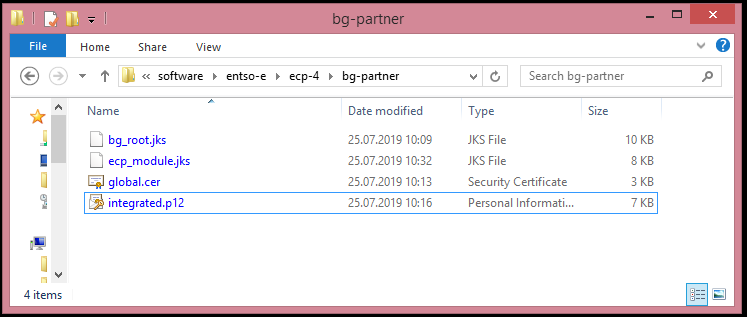


* + - Fill Alias "integrated" and password "password"

1. 
   * + Save the created keystore as ecp\_module\_cd.jks



1. After installation of ECP CD, use ecp\_module\_cd.jks for registration of ECP CD



1. Please first read carefully the gory details of JKS before use https://neilmadden.blog/2017/11/17/java-keystores-the-gory-details/ and https://cryptosense.com/blog/cracking-java-keystores-with-hashcat/Find details about Bouncy Castle Keystore Security (BCFKS) under https://cryptosense.com/blog/bouncycastle-keystore-security/ [↑](#footnote-ref-1)