Creating Relying Party Certificates

Version 4.0.2

2020-11-18

Table of Contents

1 Introduction

This document describes how to use the BankID Keygen tool to create Relying Party Certificates (RP Certificates), certificate requests and PFX-files. RP certificates are required for service providers to use the BankID service. RP certificates are used to identify relying parties and to show which service a user is logging in to or signing information at.

1.1 Versions

Date	Version	Description	Author
2020-11-18	4.0.2	Minor corrections	BankID
2020-03-23	4.0	New version for rewrite of BankID Keygen. No GUI version in version 4.	BankID

2 RP Certificate for Test Purposes

For test environments, you should not order a certificate. Instructions for obtaining an RP certificate for testing are available for download at https://www.bankid.com/utvecklare/rp-info, and in the document "**BankID Relying Party Guidelines**" you will find detailed instructions.

3 System Requirements for BankID Keygen

In order to run the BankID Keygen software you need to start a command prompt or terminal application for your operating system (Windows, Mac OS or Linux respectively). You don't need to install anything to run this application.

3.1 Download BankID Keygen

You will get the application from your bank and you can also download the most recent version here:

https://www.bankid.com/bankid-keygen

3.2 Unpack BankId Keygen

Unpack the file "BankID_Keygen.ZIP" in your preferred folder. BankID Keygen requires no installation and can be run from e.g. a USB flash drive.

4 Create RP Certificate Request

Windows:

From command prompt navigate to where you saved the BankID Keygen (keygen.exe) and then run the command ***keygen.exe***

macOS and Linux:

Depending on your local environment and permissions you might have to change permissions to run the application. To change permission, write ***% chmod x keygen***

Start a terminal and navigate to where you saved the BankID Keygen and then type ***./keygen***

This will start the Welcome screen of BankID Keygen.

To generate a CSR, select 1 on the Welcome screen and press Enter. The following information is required in the CSR process:

- **Official name of your organisation:**
  This should be your organisation's registered company name (max 64 characters)
- **Corporate identity number of your organisation:**
  Enter your company's corporate registrations number according to Bolagsverket or equivalent without hyphens or spaces (10 digits)
- **Choose a password to protect your Private Key:**
  This is your own password to protect your private key that will be generated. It must be at least 12 characters long and contain 4 letters and 1 digit. You will have to use this password later in the process when creating your PKCS#12.
  Note - Its very important that you remember this password. If you lose it, there is no way to restore the password.
- **Display Name that will be shown to the end users:**
  This is what will be shown to the user when they authenticate or sign to your services. Enter the name to be displayed (max 40 characters) according to the instructions from your bank.

Before the certificate request is created you will have the options of verifying the information.

If all looks good then press Y and enter to create the certificate request.

- **Private Key file:**
  The application will suggest a filename for Private Key file that if you accept will be save in the working directory. If you want to save in another place you can manually type the path and file name. Make sure the file extension is still .key.
- **Certificate request file:**
  The application will suggest a filename for CSR file that if you accept will be save in the working directory. If you want to save in another place you can manually type the path and file name. Make sure the file extension is still .p10. This is the file that you later should send to the bank for the issuing of your certificate.

  This will end the CSR generation and you will see that the certificate request is created and saved to disk.

5 Order and receive RP certificate

You should now provide the certificate request file you just created (example CSR_Ericsson_20200323.p10) to the bank that you have signed the BankID agreement with. This shall be done according to the instructions from the bank. You should receive the recipient and delivery information where you received this instruction.

Note – It's only the P10 file you should send and never the private key file.

When you receive the certificate from the bank, start with instructions in the next section.

6 Create the PKCS#12 / PFX file

Once you have received the issued certificate from the bank you should now create the bundle containing the private key and the certificate to be used from your application in communication with the BankID service. The bundle is often referred to as a PKCS#12, P12 or PFX file.

Windows:

From a command prompt, navigate to where you saved the BankID Keygen (keygen.exe) and then run the command ***keygen.exe***

macOS and Linux:

Depending on your local environment and permissions you might have to change permissions to run the application. To change permission, write ***% chmod x keygen***

Start a terminal and navigate to where you saved the BankID Keygen and then type ***./keygen***

This will start the Welcome screen of BankID Keygen.

1. In the Welcome screen, select **3. Generate PKCS#12 / PFX**
2. BankID Keygen will show a numbered list with all the files with .key extension found in the working directory. Select the number in the list of the private key you want to use and press **Enter**. Note 1 – This has to be the key corresponding to the CSR you previously sent to the bank. Note 2 – If there's only one key in the directory the number will be **1**.
3. You will now be asked to **enter the password for the private key.** This is the password you chose when creating CSR in section 4.2. Type the password and press **Enter**.
4. Next you will be asked for the certificate you received from the bank. If you have saved the file in the working directory (where keygen is saved) it will be shown in a numbered list. If you have saved in somewhere else you need to manually enter the path to the file.
5. **PKCS#12 output file** is the final step where you enter the path where you want to save the PKCS#12 file. Press Enter to save in working directory with default file name or manually enter new file name and path to save the file.