
Installing Certificates to S60 3rd Edition Devices

Version 1.1
May 10, 2007

S60 platform

Legal notice

Copyright © 2007 Nokia Corporation. All rights reserved.

Nokia and Nokia Connecting People are registered trademarks of Nokia Corporation. Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

Disclaimer

The information in this document is provided “as is,” with no warranties whatsoever, including any warranty of merchantability, fitness for any particular purpose, or any warranty otherwise arising out of any proposal, specification, or sample. Furthermore, information provided in this document is preliminary, and may be changed substantially prior to final release. This document is provided for informational purposes only.

Nokia Corporation disclaims all liability, including liability for infringement of any proprietary rights, relating to implementation of information presented in this document. Nokia Corporation does not warrant or represent that such use will not infringe such rights.

Nokia Corporation retains the right to make changes to this specification at any time, without notice.

License

A license is hereby granted to download and print a copy of this specification for personal use only. No other license to any other intellectual property rights is granted herein.

Contents

1.	Introduction	5
2.	Root certificates for application signing.....	5
3.	Installing SSL certificates.....	5
4.	Using client certificates to authenticate a user.....	5
5.	Using certificate to authenticate a Web server	8
5.1	Importing a non-CA certificate	8
5.2	Importing a CA certificate.....	9
6.	Evaluate this resource	11

Change history

February 22, 2007	Version 1.0	Initial document release
May 10, 2007	Version 1.1	Chapters 3 and 4 updated.

1. Introduction

The purpose of this document is to discuss how additional root certificates can be placed to S60 3rd Edition devices.

2. Root certificates for application signing

Generally speaking, all certificates intended for Java™ application signing or signing Symbian installation packages (SIS files) need to be included during manufacturing of the device. For developers to be able to get their applications signed, it is recommended that they use Java Verified or Symbian Signed process. After passing the process the application is signed against the root certificate used by the program that is available in S60 3rd Edition devices.

3. Installing SSL certificates

A Secure Sockets Layer (SSL) certificate can be used for different purposes:

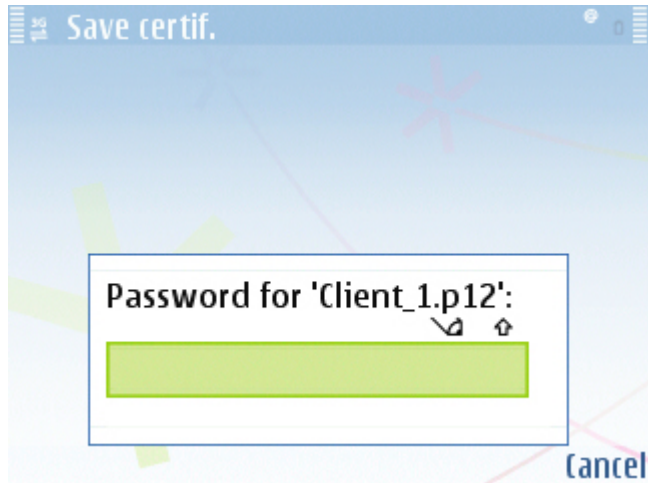
- Authenticating a client to a server (for example, SSL/TLS client authentication)
- Authenticating a server during SSL/TLS handshake

The installation of these different certificates to S60 3rd Edition devices is discussed in detail in the sections that follow. Please note that the two solutions presented in Chapters 4 and 5 are separate and not linked to each other.

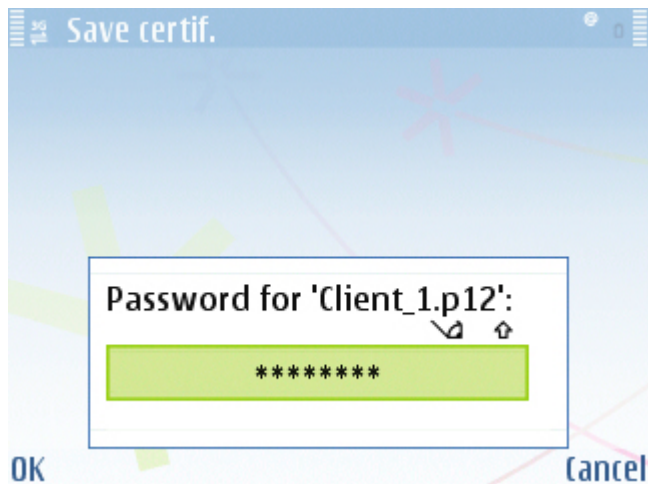
4. Using client certificates to authenticate a user

S60 only allows importing personal certificates and associated keys from .p12 files. The certificate must be a general X.509 certificate that is DER encoded. A private key and a certificate file are to be packaged into a PKCS 12 package (.p12 format). Please note that it is not possible to export a private key previously imported to device from a PKCS 12 package. The file can then be imported to the device, for example by using file transfer. When the file is opened, the system will ask if the certificate should be saved to the device.

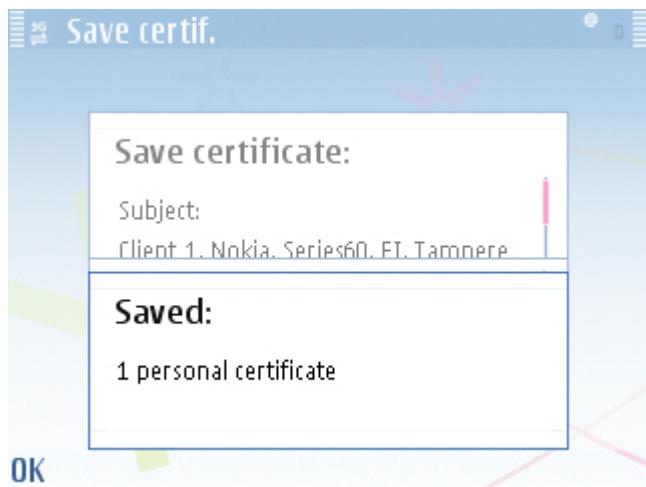
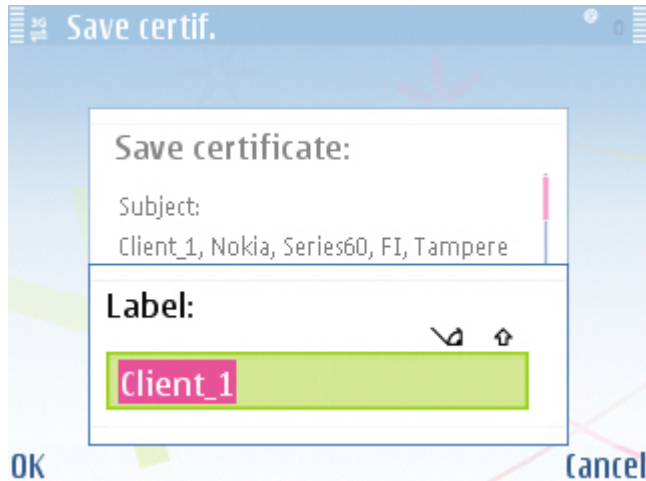
At the import of the certificate, the password of the package must be provided.



The Save process will then provide information about the contents of the package and the details of the certificates.



The user must provide the Label of the certificate, and then the Save process is complete.



5. Using a certificate to authenticate a Web server

The certificate must be a general X.509 certificate that is DER encoded. In order to import the certificate, it must be recognized as a CA certificate to make it work.

If the certificate is not recognized as a CA certificate (meaning that key usage is not CertSigning and BasicConstraints doesn't indicate that it is a CA certificate), follow the steps described below.

5.1 Importing a non-CA certificate

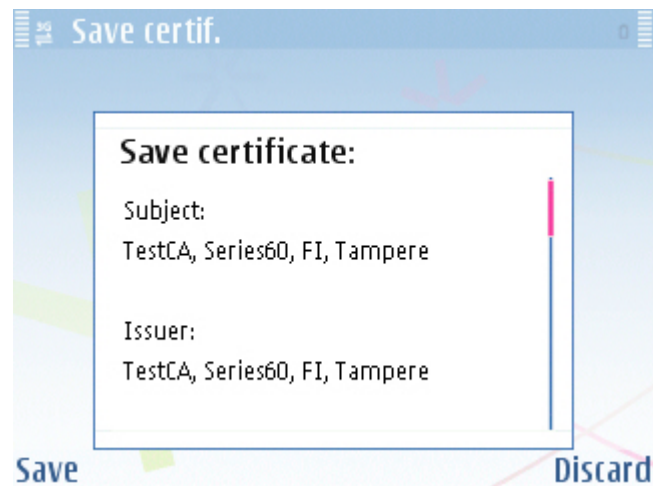
Using a Web server:

1. Copy the certificate file to the Web server.
2. Set the MIME type for the directory where the certificate is located as: application/x-x509-ca-cert.
3. Use the Web browser in the S60 device to browse the certificate.
4. Import the certificate.

5.2 Importing a CA certificate

Using file transfer:

1. Transfer the file to the device.
2. Open the file; the device automatically suggests importing the file.





Please note that if the device is formatted or data is deleted from the device, this certificate needs to be reinstalled to the device.

6. Evaluate this resource

Please spare a moment to help us improve documentation quality and recognize the resources you find most valuable, by [rating this resource](#).