Certificate Guide

Version 1.1

Revision History

Version	Date	Description
1.0	2015-01-27	Initial Version
1.1	2015-02-04	Edited the document

Table of Contents

1. OVERVIEW

Code signing is used in combination with device information. This ensures that signed applications runs only on test devices which the developer specifies. Code signing ensures that the application cannot be distributed easily in public.

The developer has to take the certification steps not only for testing the application on the actual device but also for uploading the application to Samsung GALAXY Application Seller site. If the developer does not have any actual device but want to upload the applications to Samsung GALAXY Apps Seller site, the virtual Device Unique ID can be used by following the steps indicated below. Details regarding certificates can be found in the Help Contents of the IDE (Help Contents > Certificates).

2. How to generate developer certificate

To run the Gear application on Tizen devices, the developer must generate a certificate containing the DUID (Device Unique Identifier) of the Gear. Two types of certificate are needed in developer certificate process: the author certificate and the device profile. These certificates are used for signing and verifying the developer's applications.

2.1. Generating a Certificate Signing Request

The developer must first generate a certificate signing request file (author.csr).

To generate a certificate signing request file:

I. On the Tizen IDE toolbar, click the button.

   The Request and Register a Certificate dialog opens.

II. Click Generate a certificate signing request (CSR file).

There are 3 ways to generate a certificate request:

- Request a certificate from scratch
- Use an existing certificate
- Use the Android keystore

2.1.1. Generating the certificate from scratch

Below are the steps to make a certificate request from scratch:

I. Select Generate a new certificate signing request and click Next.

   The Generate a new certificate signing request page will open.

II. Enter the following information:
   - Mandatory information
     - Name
     - Private key password
     - Password confirm
   - Optional information
     - Country
     - State
     - City
     - Organization
     - Department

III. Click Finish.

The developer will obtain an author certificate if the request is successful. The author.csr file and related resources will be generated in the keystore folder inside Tizen SDK data folder (for example, ~/tizen-sdk-data/keystore/author.csr).

2.1.2. Generate from an Existing Certificate

Below are the steps in using an existing certificate:

I. Select Import the certificate signing request from an existing certificate and click Next.

The Import the certificate signing request from an existing certificate page will open.

II. Enter the existing certificate file path.
III. Enter the password.
IV. Click Finish.

If the request is successful, the developer will obtain an author certificate. The author.csr file and related resources will be generated in the keystore folder inside Tizen SDK data folder (for example, ~/tizen-sdk-data/keystore/author.csr).

2.1.3. Using an Existing Android Keystore

Below are the steps to make a certificate request using an existing Android keystore:

I. Select Import the certificate signing request from an android keystore and click Next.

The Import the certificate signing request from an android keystore page will open.

II. Click Import.
III. In the Import dialog, enter the existing Android keystore file path and keystore password, and then click Finish.
IV. Enter the following information:
  - Mandatory information
    - Alias
    - Password of alias
    - Name
  - Optional information
    - Country
    - State
    - City
    - Organization
    - Department

V. Click Finish.

If the request is successful, the developer will obtain an author certificate. The author.csr file and related resources will be generated in the keystore folder inside Tizen SDK data folder (for example, ~/tizen-sdk-data/keystore/android/author.csr).

2.2. Requesting Certificates

The developer must have a CSR file at least once. The developer can request the author certificate and the device profile certificate from the Tizen IDE through the Samsung Developer Center.

To request an author certificate:

I. On the Tizen IDE toolbar, click the button.

   The **Request and Register a Certificate** dialog will open.

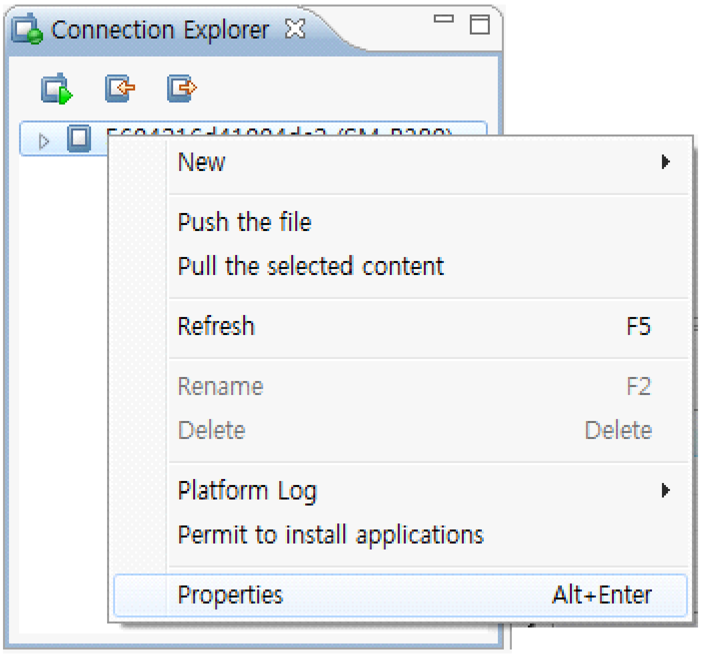
II. Click **Request the certificate** in the **Author** group.

   A browser opens for requesting the author certificate.

III. Follow the instructions in the browser to upload the author.crt file
IV. The author.crt file will be sent to you in an email in a few minutes.
V. Copy the file to a known location. (This file will be imported into the Request and Register a Certification dialog with your certificate password).

To request a device profile certificate:

I. Check the DUID (Device Unique Identifier) of your devices.
   A. In the **Connection Explorer** view, select a device and then right click.
   B. To view the DUID, select **Properties**.



II. Click **Request a certificate** in the **Device Profile** group.

   A browser will open for creating a device profile certificate request.

III. Generally select Public for Privilege Level, and Individual for Developer Type.

Paste the DUID to the Device ID field and click OK.

IV. A device-profile.xml will be generated and returned to you as an email attachment along with a device certificate password.
V. Copy the file to a known location like in the author certificate (This file will be imported into Device Certificate section of the Request and Register a Certificate panel.)

2.3. Registering Certificates

Register the author and device profile certificates using the author.crt and the device-profile.xml files received from the Samsung Developer Center.

To register the certificates, see the steps below:

I. On the Tizen IDE toolbar, click the button.

The **Request and Register a Certificate** dialog opens.

II. Enter the author.crt file path.
III. Enter the author password.

This is the password the developer created when the author certificate was generated.

IV. Enter the device-profile.xml file path.
V. Enter the distributor password.

This is the password received from Samsung with your device-profile.xml.

VI. Click **OK**.

The author and distributor certificate files are generated in the keystore folder inside Tizen SDK data folder (tizen-sdk-data). A default security profile is also created.

If the author certificate is created from the Android keystore, click **Certificate file from android keystore** to explicitly enable it.

If the developer has a legacy certificate of Gear 2 which was received from the Samsung Developer Center, the developer can register it using the certificate-registration.xml file, as indicated in the steps below:

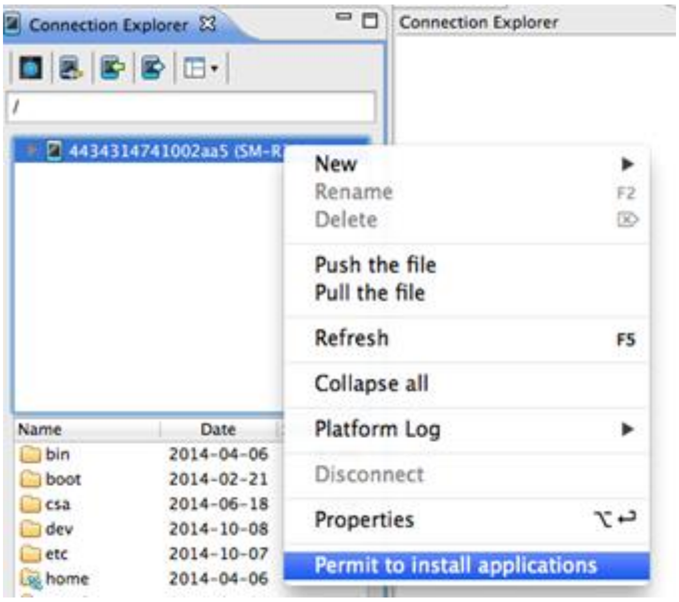
I. On the Tizen IDE toolbar, click the button.

The **Request and Register a Certificate** dialog opens.

II. Click **Use the legacy certificate**.
III. Enter the certificate-registration.xml file path.
IV. Enter the password.
V. Click **OK**.

2.3.1. Permitting Application Installations

The developer must permit a device to install applications by uploading a certificate file on the device. To give the permission, right-click on a device displayed in the **Connection Explorer** view and select **Permit to install applications**.



This will copy the device-profile.xml file to '/home/developer' folder in the device.

If the developer uses a legacy DUIDs (Device Unique Identifiers) for the old Gear in the xml, device-profile.xml will be replaced to certificate-registration.xml.

The developer can now install apps to the Gear.

2.4. Adding Certificates to Security Profiles

After registering, the author and distributor certificates are automatically added to the Security Profile in Tizen SDK. So in normal cases, the developer doesn't need to configure this step all by himself/herself.

To manually change the certificate settings:

I. In the Tizen IDE, go to **Window > Preferences > Tizen SDK > Security Profiles**.
II. To add a signed profile, click **Add** in the **Profiles** panel.
III. To edit the certificates:

- In the **Author Certificate** panel, click **Edit** to set the author certificate path and password.

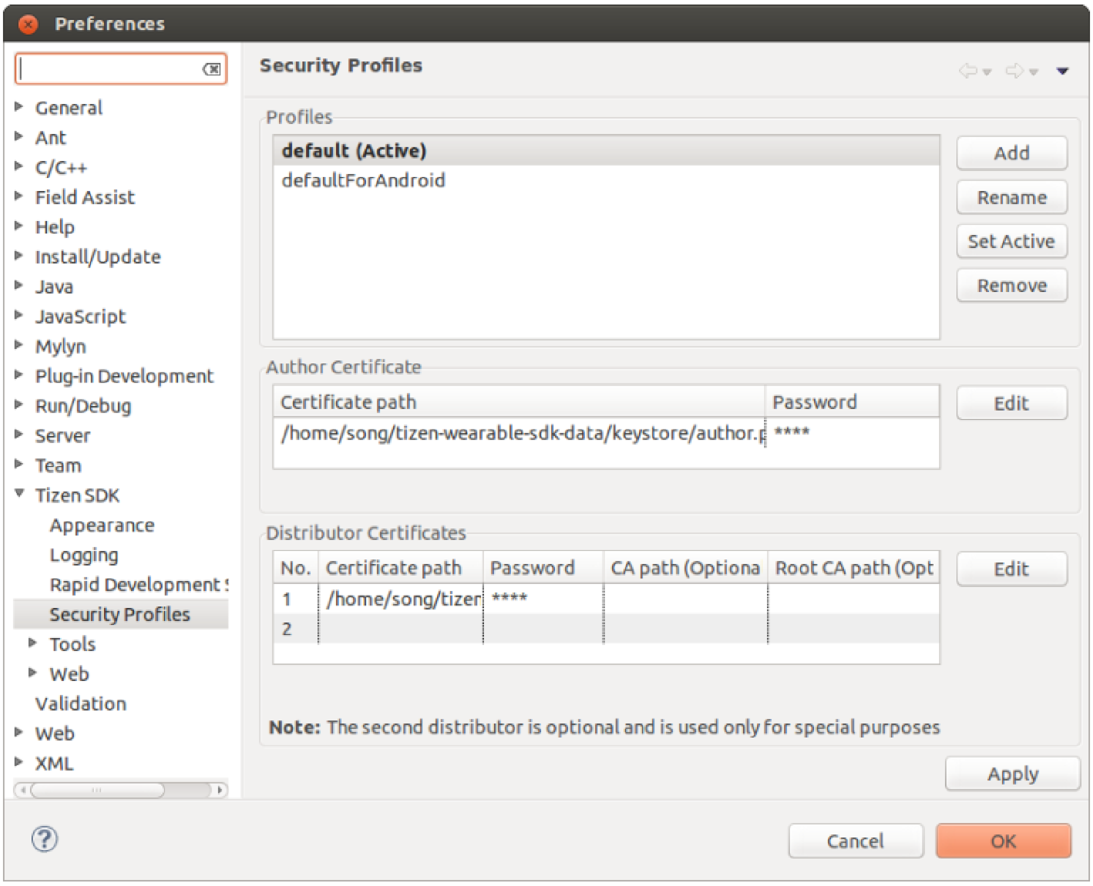
  Author certificate is located at tizen-sdk-data/keystore/author.p12.

  Password is the one the developer created.

- In the **Distributor Certificates** panel, select a certificate in the table and click **Edit** to modify the distributor certificate path and password.

Distributor certificate is located at tizen-sdk-data/keystore/distributor.p12.

Use the password the developer received from Samsung with your device-profile.xml.



Security Profiles

Profiles

- **default (Active)**
- defaultForAndroid

Author Certificate

Certificate path	Password
/home/song/tizen-wearable-sdk-data/keystore/author.p	****

Distributor Certificates

No.	Certificate path	Password	CA path (Optiona	Root CA path (Opt
1	/home/song/tizer	****		
2				

Note: The second distributor is optional and is used only for special purposes

Copyright

Though every care has been taken to ensure the accuracy of this document, Samsung Electronics Co., Ltd. cannot accept responsibility for any errors or omissions or for any loss occurred to any person, whether legal or natural, from acting, or refraining from action, as a result of the information contained herein. Information in this document is subject to change at any time without obligation to notify any person of such changes.

Samsung Electronics Co. Ltd. may have patents or patent pending applications, trademarks copyrights or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give the recipient or reader any license to these patents, trademarks copyrights or other intellectual property rights.

The document is subject to revision without further notice.

For more information, please visit http://developer.samsung.com/