Domain name with spaces in certificate path results in MIDlet installation failure on S60 (Known Issue)

Description

On S60 devices, the installation of Thawte and VeriSign-signed Java applications can fail with **Certificate Error** (S60 3rd Edition, Feature Pack 2 and subsequent Editions) or **Unable to install** (S60 3rd Edition, Feature Pack 1 and prior Editions) authentication failure notifications.

Both are due to the same issue:

On certain occasions, Thawte and VeriSign code signing certificates have been issued by a Certificate Authority with an additional data field called Subject Alternative Name (SAN) together with a domain name set as the value for that field. While the defined data field should not exist as part of the code signing in the first place, the actual root cause which results in the defined error notifications is the value, i.e. the domain name and especially space characters included in the name.

For domain names, S60 platform complies to the Application Techniques for Checking and Transformation of Names specification which states that domain names must not contain blank spaces. This compliance by S60 platform means that when the installation of an application which has been signed with a code signing certificate which includes a SAN and a domain name with space characters is initiated, and the certificate checking is made as part of the installation process, the installation gets cancelled by the S60 platform because of the faulty domain name format defined in the application signature.

How to reproduce

To verify whether a code signing certificate is a faulty one:

1. Open the JAD file which containts the code signature. Copy the full certificate path line after the `MIDlet-Certificate-1-1` attribute (For example, `MIDlet-Certificate-1-1: MIIE2TCCA8GgAwI...`).
2. Paste the copied line into a text file and save that file with the suffix **.der** so that the text file is converted into a security certificate file for further examination. The naming of the file can be anything as long as the final format of the file is as follows: **somefilename.der**
3. Double-click the created **.der** file to open it. From the top of the file dialog, click the **Details** tab.
4. From the **Details** tab, ensure that the **Show:** drop-down dialog has got **<All>** selected.
5. From the **Field** and **Value** list, check if it contains the following field and value pair:

Subject Alternative Name, DNS Name=Some name with SPACE characters If the described SAN + DNS Name pair is there, then it is very likely the root cause of the installation failure.

Solution

The application developer who has signed the application needs to contact the Certificate Authority (Thawte or VeriSign) which has issued the code signing certificate, and ask for a replacement certificate.

(C) Copyright Nokia 2014. All rights reserved.

(c) Copyright Nokia 2014. All rights reserved.