

| | | | |
|-----------------|-----------------|----------------------|------------------|
| ID | TSS000454 | Creation date | October 19, 2006 |
| Platform | S60 3rd Edition | Devices | |
| Category | Symbian C++ | Subcategory | |

Keywords (APIs, classes, methods, functions):

Overview

DLL capability model in a secure platform

Description

With platform security, every DLL must have at least the same set of capabilities as the loading process, or otherwise the process is not allowed to load the DLL. For this reason most general-purpose DLLs would need (or close to) ALL -TCB as they cannot know in beforehand all the processes that can/will load them at some point in the future. Even if your DLL is set to have ALL -TCB capabilities, it does not mean that it is using all of them. A DLL (that has a higher capability set than the loading process) cannot leak capabilities to the process, but a process can leak capabilities to the DLL because the DLL is "granted" the same capabilities as the process.

A DLL capability does not grant the DLL access to any capability-restricted resources (not even if the DLL has ALL -TCB). For that access you will need a process with ALL -TCB capabilities. DLL capabilities only reflect the level of trust, so that the loading process can be sure that the DLL it is capable of loading has been tested to be trusted with the set of capabilities that the process has.

To get your DLL signed with these heavy capabilities:

For example, all MTM, FEP, and browser plug-ins require ALL -TCB. If you are developing such a component and require ALL -TCB capabilities, you need to fill in the Capability request form on the Symbian Signed Web site <https://www.symbiansigned.com/app/page/requirements> and send the form to nokia.testing@nokia.com.

In the form you have to explain why each capability is requested and also give some company background information, for example, if you already have some co-operation with Nokia. This should be done before requesting the developer certificate.

When Nokia gets the capability request form, the case is evaluated with S60 platform. Manufacturer-approved capabilities are granted so that those DLLs that require sensitive capabilities are packaged to an embedded SIS file which is certified first, and the developer should use it in the delivery.

For more information about the process, see the Testing and Signing with Symbian Platform Security document at www.forum.nokia.com/testing.