

There are three main modules in the Symbian Security Model:

1. Trusted computing base.
2. Data caging.
3. Capabilities.

Contents

- 1 Trusted computing base
- 2 Data caging
 - ◆ 2.1 \resource
 - ◆ 2.2 \sys
 - ◆ 2.3 \private
 - ◆ 2.4 \all the rest
- 3 Capabilities
 - ◆ 3.1 Open to all
 - ◆ 3.2 Granted by the user at installation time
 - ◆ 3.3 Granted through Symbian Signed
 - ◆ 3.4 Granted by the manufacturer
- 4 Internal Links

Trusted computing base

The trusted computing base is a collection of software that enforces capabilities and data caging. It contains the kernel, the file system, and the software installer. This is the controlling part of the operating system for the platform security model.

Data caging

Data caging means that the applications and the users have access only to certain areas of the file system. In practice the applications can access their own private directories and directories that are marked as open. It means, for example, that one application cannot access another application's private directory and data.

The access is restricted as follows:

\resource

Location for application icons, bitmaps, etc. Writing allowed only at application installation. Everyone can read the folder.

\sys

Location for binaries, including application installation registry and root certificates. Writing allowed only at application installation. Reading allowed to backup the application.

\private

This is a private playground for each application. Reading and writing is only allowed to the application's own directory. Backup software has read and write access to this directory.

\all the rest

Access to all the other folders is free for all, for example, user's own photos, music, and documents.

Capabilities

A capability grants access to a set of APIs and can be obtained through certification, for example Symbian Signed. The capabilities can be divided into four:

Open to all

- APIs in this category enable development of all the basic applications, for example, most of the single-player games.
- Generally speaking, about 60 percent of the APIs are freely available without any capability requirement.

Granted by the user at installation time

- Some capabilities can be granted by the user at the application installation phase.
- The application will have the capability until the application is removed from the device.
- This option may not be active in some devices by default. Thus the user has to activate the installation time capability granting separately.

Granted through Symbian Signed

- Some capabilities are available after passing Symbian Signed testing.
- More sensitive capabilities require declarative justification why the application needs access to such a capability. Passing the testing is required as well.
- The most sensitive capabilities require the developer to fill in the Capability Request Form and acceptance from the platform manufacturer. Passing the testing is required as well.

Granted by the manufacturer

- Submit your request via the Symbian Signed site, as above, but select Nokia as the device manufacturer. Manufacturer approval is needed if your request contains AllFiles, DRM, or TCB - or if you list more than 1000 IMEIs in your request.

Internal Links

- [Symbian Signed for Nokia](#)
 - [Developer certificate](#)
 - [How to pass Symbian Signed for Nokia tests](#)
 - [Application Signing](#)
 - [Freeware signing](#)
 - [Signing](#)
 - [Data Caging](#)
-