

Contents

- [1 Overview](#)
- [2 Rationale](#)
- [3 Programming](#)
- [4 Trusted computing base](#)
- [5 See also](#)
- [6 Discussion](#)

Overview

Symbian OS platform security was introduced in S60 3rd Edition with the implementation of Symbian OS V9 as the S60 platform's underlying operating system. Platform security enhances the existing security features of Symbian OS to deliver a more secure platform for mobile devices. This secure platform offers device users greater assurance about the security of their devices and the data they hold.

Platform security offers developers a larger, more confident base of mobile consumers, who are more willing to install applications. This page provides links to key resources that will help developers to embrace this new technology and answers to the most frequently asked questions about platform security. Security in general can be considered as one of the key aspects in quality application. For more information about the importance of security aspects in the application development and quality assurance process, see www.forum.nokia.com/quality.

Rationale

Platform security was designed to make the security impact of architectural decisions visible. Architecturally, software components can be divided to groups where the components trust each other to behave well. Boundaries between these groups are termed security boundaries.

In practice, this means that if a software component wants to run code from a shared library, it effectively brings that code within its own security boundary, and must therefore trust that code. In addition, when supplying services to a component outside its own security boundary, the component must do certain checks to see whether the other component is entitled to such services.

Both of these actions (making a trust decision for shared code, and checking permissions of a calling component) are facilitated through the use of **capabilities**.

The need for capabilities can be used as an architectural tool: the amount of capabilities required from a component reflects the trust that is placed on it. If the amount of capabilities seems excessive, this can be construed as a hint that security boundaries may be too large.

Programming

- [Capabilities](#)

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.

See also

[Platform Security in Forum Nokia](#)

[Symbian OS - Platform Security from Symbian](#)

[Platform Security - A Technical Overview from Symbian \(PDF\)](#)

Discussion

[Forum Nokia discussion board](#)