

Symbian Platform Security: Granting Sensitive Capabilities

(AllFiles, CommDD, DiskAdmin, MultimediaDD, NetworkControl,
DRM & TCB)



Get Connected

Background

- In Symbian Platform Security, access to certain functions is restricted by capabilities
- Developers can access most of the capabilities through Symbian Signed
 - Refer to the backup material (slide 8-) for further clarification
- Some of the capabilities are considered as sensitive and are split in this presentation as follows:
 - The five (AllFiles, CommDD, DiskAdmin, MultimediaDD & NetworkControl)
 - DRM & TCB
- Applications can receive sensitive capabilities through Symbian Signed for Nokia
- If the developer is a Symbian Self Certifier, Nokia can also recommend Symbian to give the developer access to the mentioned capabilities
- The developer can use Symbian Developer Certificates to test the application on a live device
 - For the sensitive capabilities these are granted only if the developer can also receive the final acceptance for the application



Need for sensitive capabilities

Capabilities are used to access certain APIs to create certain functionality:

- TCB: Antivirus, File encryption
- DiskAdmin: ES TARM (device management)
- CommDD: VPN/IPsec and firewalls
- AllFiles: only a few isolated and rare cases
 - A general purpose “file manager” functionality cannot be accepted (due to copy protection / DRM-related issues)
- MultimediaDD / NetworkControl: VoIP applications + more in-depth access to multimedia and network

A process cannot load a DLL with a smaller set of capabilities than itself:

- All-TCB (All except TCB): MTM, FEP & Browser Plug-ins
- The capabilities are not “actively used” – used only for DLL loading purposes



Granting the Five

1. Developer fills in the Symbian Signed Capability Request Form (download it from <http://www.symbiansigned.com/app/page/overview/testcriteria>).
2. Developer sends the form to nokia.testing@nokia.com
 - This is provided by the developer at the latest when requesting the Developer Certificate
 - This is needed to provide enough technical information of the capability need
3. Technical justification is checked
3. Each case is evaluated and handled in a board which convenes biweekly
4. The developer is guided to Symbian Signed for Nokia for final certification
 - Legal framework is handled at the time of registration
 - The sensitive part of the application is packaged into an embedded SIS, if architecturally feasible
 - Developer pays for the testing and signing
 - Application is tested against Symbian Signed and Nokia criteria (see www.forum.nokia.com/testing for the excluded test cases)



Granting TCB & DRM

- Both TCB and DRM capabilities enable an application to access sensitive DRM-related material
- Nokia has licensed the DRM material under CM-LA and WMDRM agreements and is liable for maintaining the integrity of the DRM solutions
 - If any developer application breaks the integrity, Nokia will have to pay according to the liability clauses



Granting TCB & DRM or Self Certification Rights

1. The developer fills in the Symbian Signed Capability Request Form and sends it to nokia.testing@nokia.com
 - This is provided by the developer at the latest when requesting the Developer Certificate
 - This is needed to provide enough technical information of the capability need
 - This also applies to any Symbian Self Certifier requesting access to any of the seven sensitive capabilities
2. Technical justification is checked
3. Due to high liability, each case requires a business relationship and legal agreement between Nokia and the developer



Granting TCB & DRM or Self Certification Rights

4. When the case is accepted:

- Legal framework is created by the Nokia business owner
- The developer is guided to Symbian Signed for Nokia for final certification
- If the developer is a Symbian Self Certifier, Symbian is notified about the decision and they will grant the access to the capabilities
- This acceptance is per application
- The developer pays for the testing and signing
- Application is tested against Symbian Signed and Nokia criteria



Backup material



Get Connected

Java Verified and Symbian Signed

-Industry-wide application testing programs-

Application
running on
Symbian OS

www.symbiansigned.com
Symbian OS devices

Common test criteria

Symbian, Nokia, SonyEricsson,
Sendo, Siemens, Orange,
T-Mobile, Handango



Digitally
signed
applications



Channels
operators,
aggregators.

Utilizing the
programs does
not cost
anything



www.javaverified.com
MIDP 1.0 & 2.0

Common test criteria

Sun, Motorola, Nokia, Siemens,
SonyEricsson, Vodafone, Samsung,
Orange, T-Mobile, LG, Handango

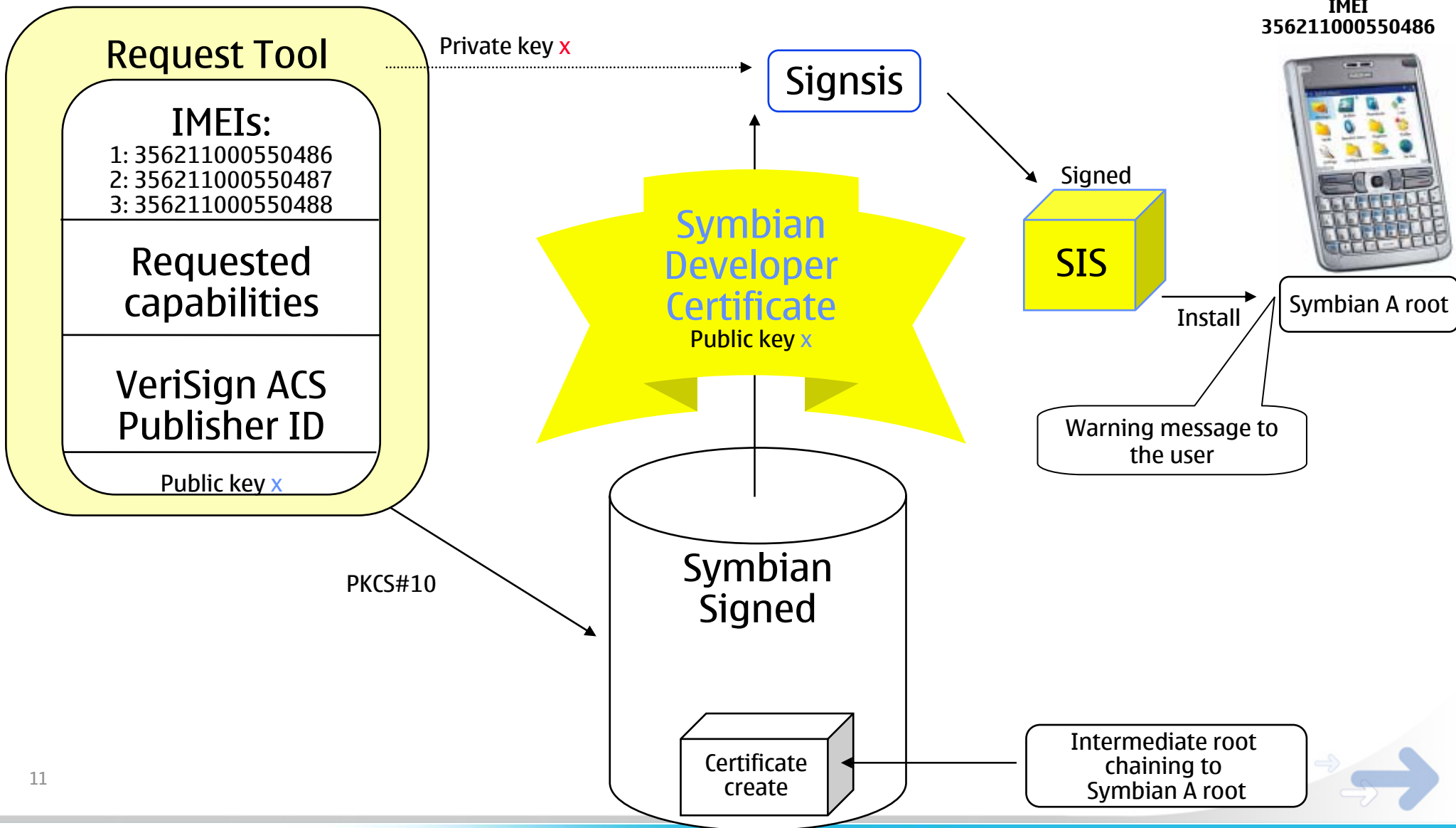
Java™ ME
application

Symbian Signed – services

- UID (Unique Identifier)
 - “Social security number” for the application
- Developer certificate
- Application testing and signing
 - Getting your application Symbian Signed
 - Use a “for Symbian OS logo”
 - Get the application listed on a Symbian Signed application catalogue
- Freeware certification



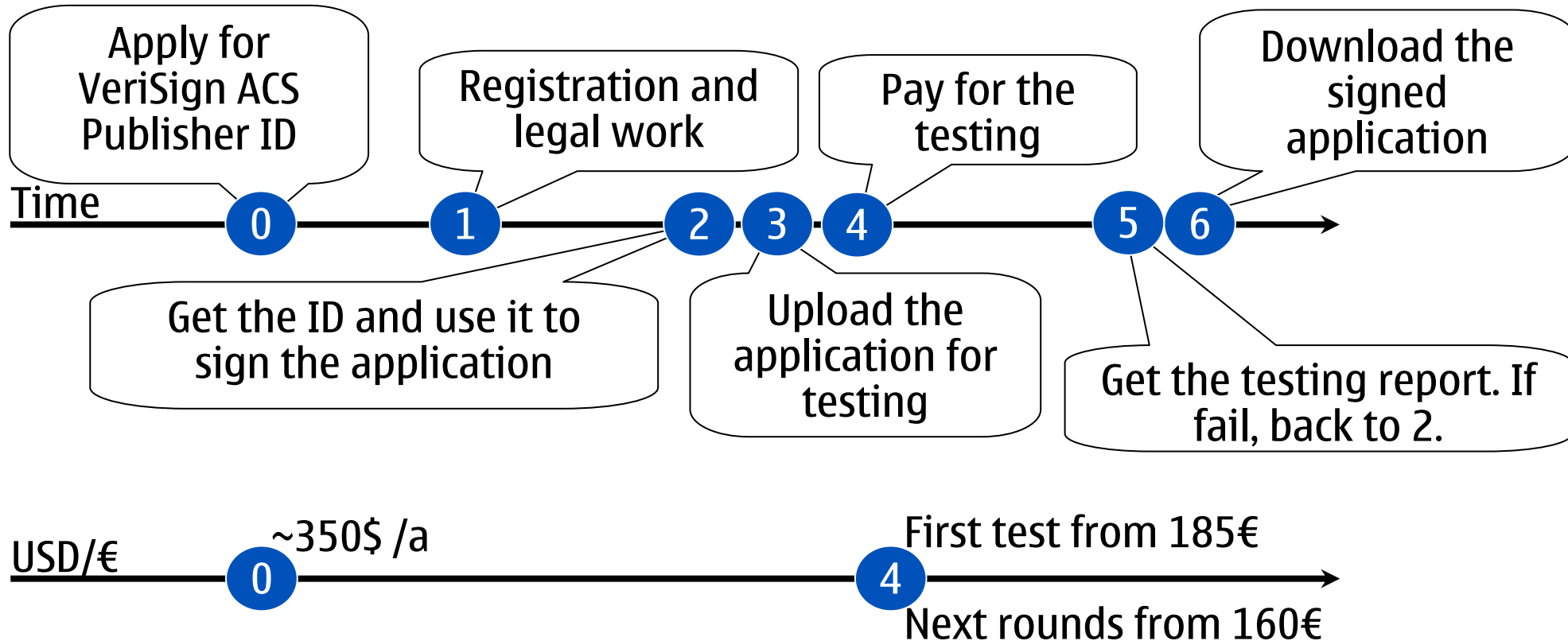
Symbian Developer Certificate – details



Symbian Developer Certificates

Number of IMEIs	Authentication	Capabilities
1	Symbian Signed account	LocalServices, UserEnvironment, NetworkServices, Location, ReadUserData, WriteUserData, SWEvent, SurroundingsDD, ProtSrv, PowerMgmt
20	VeriSign ACS Publisher ID and Symbian Signed account	As above + ReadDeviceData, WriteDeviceData, TrustedUI
> 20	VeriSign ACS Publisher ID, Symbian Signed account and licensee support	As above + DRM, NetworkControl, MultimediaDD, TCB, AllFiles, CommDD, DiskAdmin

Symbian Signed process



Access to capabilities

Unrestricted

(60% of APIs)

User-Grantable (at installation time)

ReadUserData
WriteUserData
NetworkServices
LocalServices
UserEnvironment

Symbian Signed

The user-grantable
capabilities
+
Location
ReadDeviceData
WriteDeviceData
PowerMgmt
SurroundingsDD
ProtServ
TrustedUI
SwEvent

Licensee/Platform Approval

Symbian Signed
capabilities
+

DRM
TCB

Manufacturer

DiskAdmin
AllFiles
CommDD
MultiMediaDD
NetworkControl

S60

Implementations
may vary!

