



# Symbian code signing

or - how to implement a mobile code signing scheme

# Overview - theory

- History of OS
- The Symbian Foundation
- Future outlook

# Overview - coding

- Development options
- Native applications in C++
- Selling an application
- Where to go for help

# Overview – security I

- Why handset-based security
- Stakeholders in mobile security
- Architectural goals of the Platform Security Model
- Pillars of the Platform Security Model

# Overview – security II

- The Native Software Installer
- Signing games

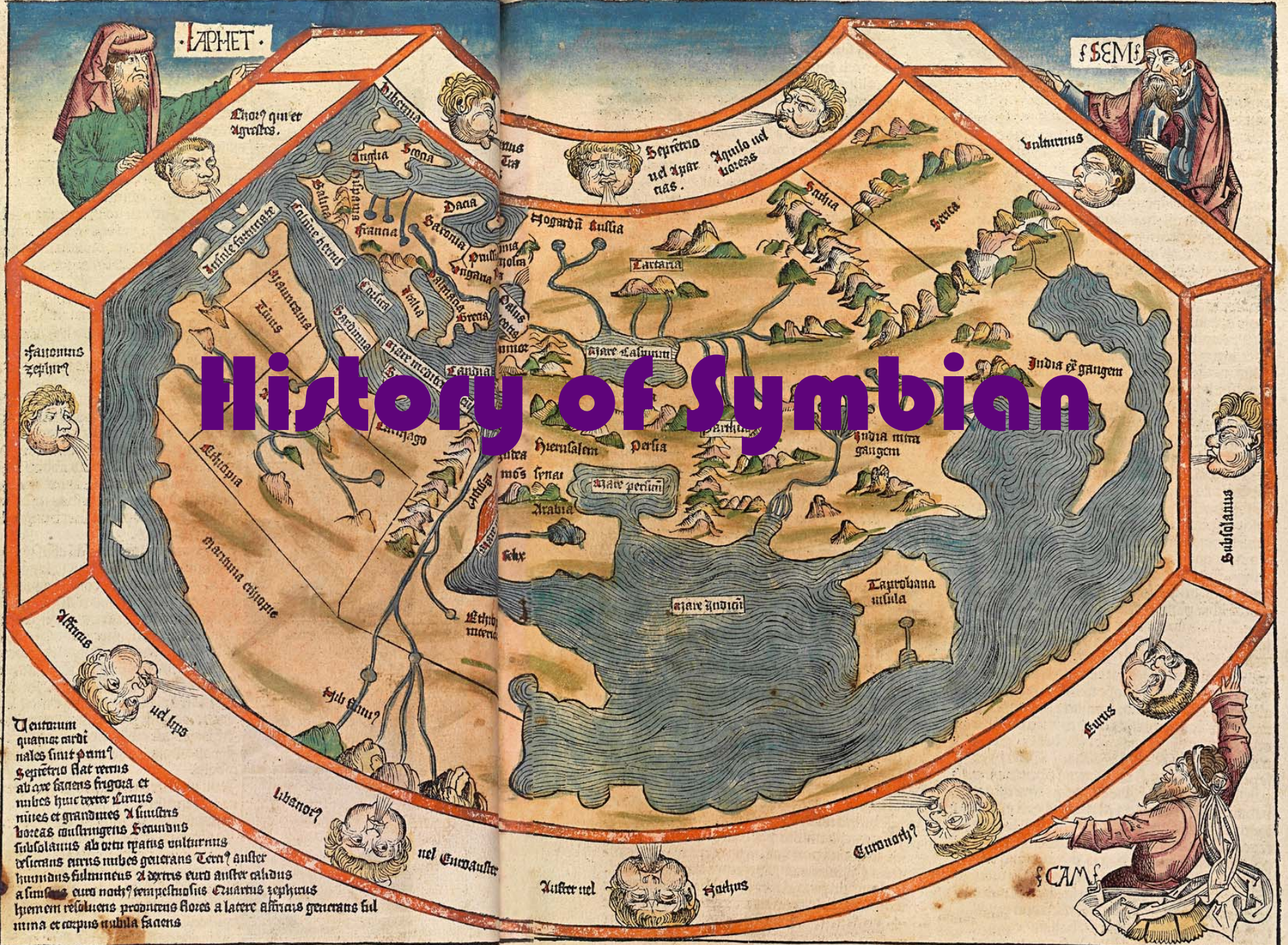
# About /me



- Tam HANNA
  - CEO, Tamoggemon Ltd.
  - Runs web sites about mobile computing

LAPMET

SEMS



# History of Symbionn

Chor? qui et  
Agrates.

Sepretio  
vel Apar  
nas.

Aquila vel  
luceras

Unlucurus

fanonius  
zeplur?

Ethiopia

tractura ethiopiae

Affinis

vel lypis

Ubanor?

vel Eucrauster

Auster vel

Hathus

Euronath?

Eurus

Subsolarius

CAM

Teitarum  
 quanae ardi  
 nales sunt dam?  
 Sepretio flat ventis  
 ab axe fixans frigora et  
 nubes hinc venter Lunus  
 nives et grandines A linciens  
 boreas multirigenis Secundus  
 subsolarius ab ortu spatius unlucurus  
 tralicans parvis nubes generans Teen? auster  
 humidus fulmineus A dextera euro auster calidus  
 a sinistra euro north? tempestuosus Quarnus zephyrus  
 hincem resoluens produens flores a latere sinistra generans sul  
 mina et corpus nubila faciens

# EPOC

- Developed by Psion
  - Series5
  - Revo
  
- “Thrown out” to Symbian



# Series60



- First versions
  - Introduced on 7650
- S60v2 still common
  - Nokia N70

# S60v3

- Renamed due to virus problems
- Introduces mandatory signing
  - Binary break
- Three feature packs
  - Downward compatible



# S60v5



- S60v3 + touch
  - Lives along v3
- Very basic GUI
- Partially downward compatible
  - Apps run, but cant be controlled due to lack of buttons

# **The Symbian foundation**

# Who owns it

- Non-profit organization
  - Governed by boards
  - Members picked on "amount of merit"
- Founded by various cell phone companies
- Every organization can become a member
  - "Smallish" software houses can also join

# licensing

- Code is currently being moved to EPL
  - Expected done in mid-2010
  - Parts out earlier
- Currently, members can access all code
  - Symbian Public License

FUTURE

**future outlook**



# The Symbian Foundation Platform Plan

Open for contribution

2009

2010

2011

*\* Proposal under review*

S^2

## Symbian^2

- Personal: Customisable home screen supporting embedded widgets and other personal content
- Dynamic: Ability for apps to take action in response to the user's changing location

S^4

## Symbian^4

- Direct UI\*: Fresh new user experience
- Qt integrated as primary runtime environment\*
- Majority of SHAI in place

Symbian^2

Symbian^3

Symbian^4

Symbian^5

S^3

## Symbian^3

- Looking good: Graphics support for advanced layering and effects
- Sounding clear: High performance networking architecture enabling fixed internet performance, ideal for streaming high def video and high quality VoIP calls

### Also available:

- SDK based on Forum Nokia SDK 5th Edition, compatible with Symbian OS v9.x and S60 5th Edition

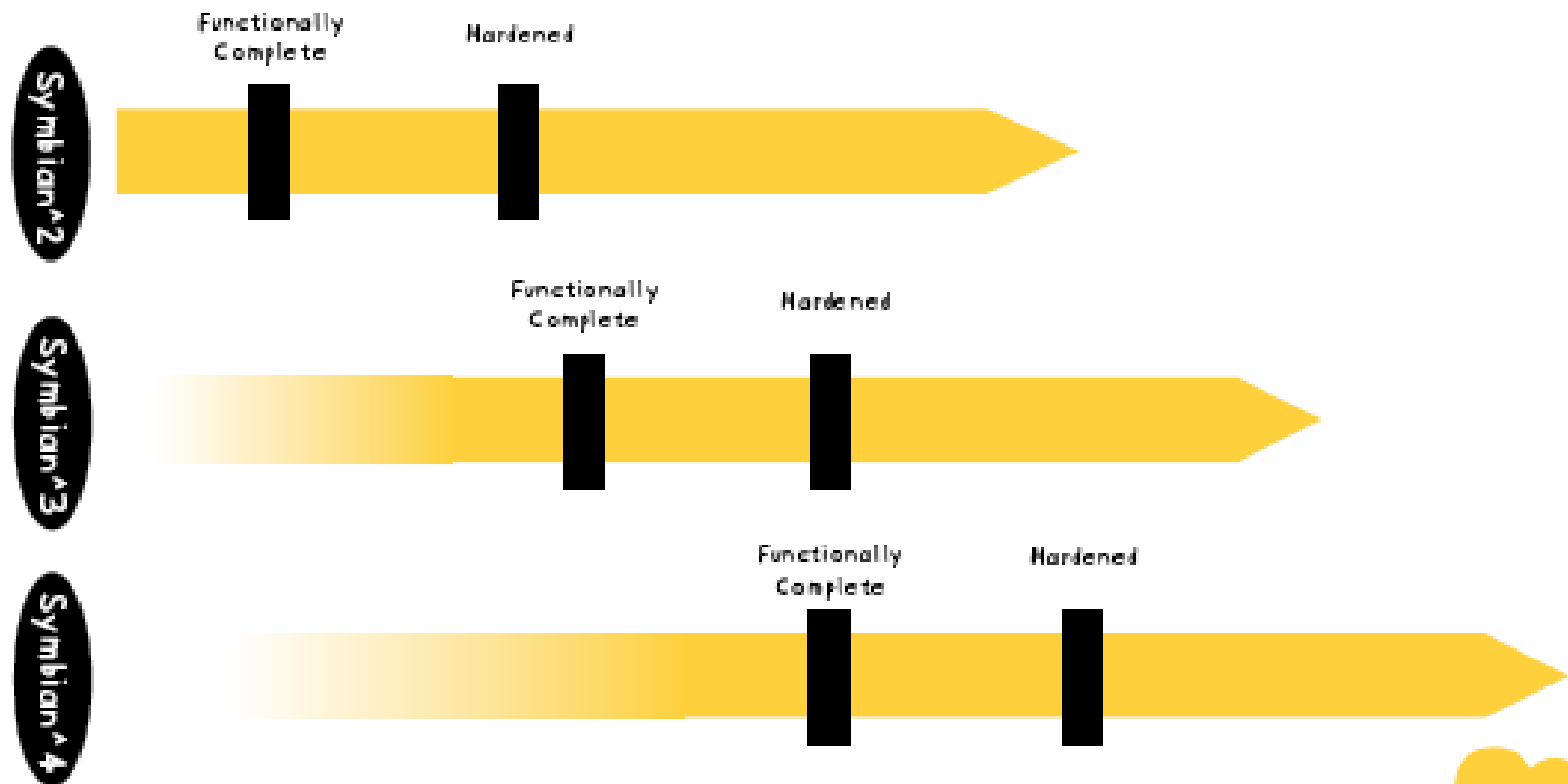


# Symbian Foundation Platform Plan

Open for contribution



*Missed milestones to be confirmed by Release Council*



# What to expect

- Will switch to QT
  - Known to open-source heads
  - Native development will remain possible
- Symbian^4 – new UI stack
  - LARGE binary break

A Theory of Mobile Processes

CAMBRIDGE

Guzdial  
Rose



*Squeak*

Open Personal Computing  
and Multimedia

DYBVIK | THE SCHEME PROGRAMMING LANGUAGE ANSI SCHEME

SECOND  
EDITION



Nelson

Systems Programming with **Modula-3**

Learning Python

Lutz & Ascher

Programming Perl

Wall,  
Christiansen  
& O'Reart

THIRD EDITION

Miranda™

The Craft of  
Functional  
Programming

Thompson

ULLMAN

ELEMENTS OF FUNCTIONAL PROGRAMMING

ML97 EDITION

The Little MLer

Felleisen and Friedman

The Java™ Programming Language  
Second Edition

Arnold  
Gosling



The Dylan  
Reference Manual

Shalit

Addison  
Wesley

THE C++ PROGRAMMING LANGUAGE

THIRD  
EDITION

THE C PROGRAMMING LANGUAGE

SECOND EDITION

Development Options

# C++

- Symbian “fucked” C++
  - “C with objects”
- Somewhat difficult to learn and understand
- But:
  - Apps somewhat easy to sell
  - Full device access

# .NET CF

- Net60
  - from third party
- Must be purchased
- Great communality with PPC et al

# J2ME

- Oldest run time environment
- Developing for it is somewhat easy
- But:
  - Bad user experience (prompts)
  - Might be dropped from future boxen

# WRT / flash / etc

- Various Web 2.0-Technologies available
- Easy to develop for
- But:
  - Selling results is difficult at times
  - Extremely limited functionality

# Native applications in C++



# Carbide.c++

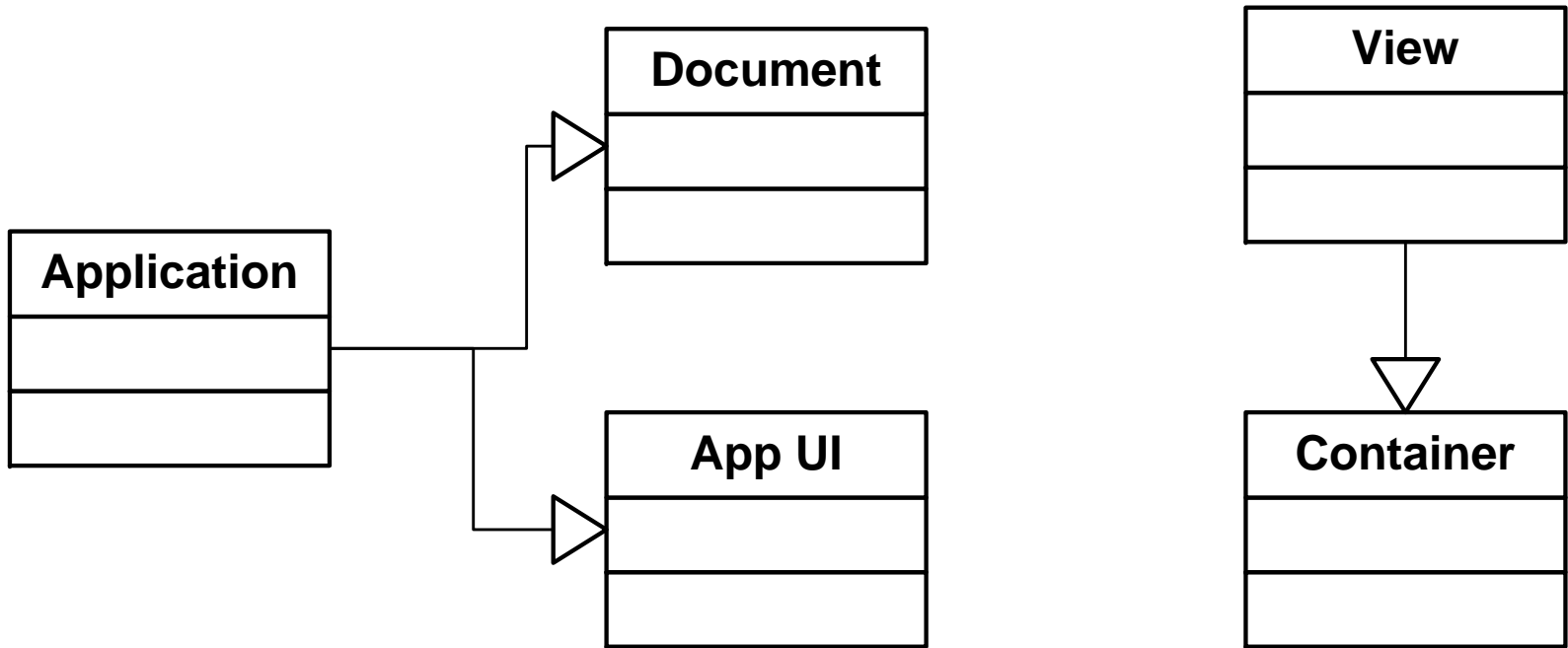
- Free, Eclipse-based IDE



- Contains dangerously buggy UI editor
  - COMMIT CODE TO CVS FREQUENTLY!!!

# Basic app structure

- Five classes:



- Auto-generated

# Application / Document

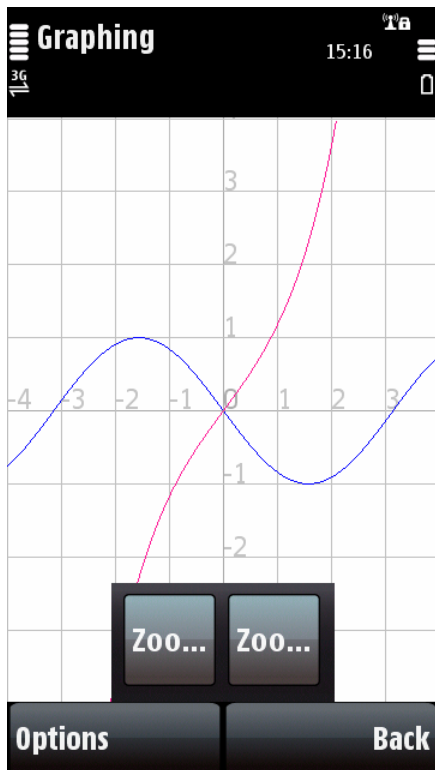
- Do not touch
- Let Carbide generate them, and ignore
- Development mantra: if it works, its ok
  - F00K the rules

# AppUi

- Use as "static repository"
  - Stores global data
- Can be accessed easily from forms
- `CLocaNoteAppUi* temp =  
(static_cast<CLocaNoteAppUi*>((CCoeEnv::Static())  
->AppUi()))`

# View / Container

- Contain logic for "forms"
- One view, one container per form



# Two-phase initialization

- Handsets always low on memory
- “Clean up stack” catches object references
  - Stack unwinding, clean-up
- Can generally be ignored

```
/**  
 * First phase of Symbian two-phase construction. Should not contain any  
 * code that could leave.  
 */
```

```
CTouchCalcContainerView::CTouchCalcContainerView()
```

```
{  
 // [[[ begin generated region: do not modify [Generated Contents]  
 iTouchCalcContainer = NULL;  
 // ]]] end generated region [Generated Contents]  
  
}
```

```
/**  
 * The view's destructor removes the container from the control  
 * stack and destroys it.  
 */
```

```
CTouchCalcContainerView::~~CTouchCalcContainerView()
```

```
{  
 // [[[ begin generated region: do not modify [Generated Contents]  
 delete iTouchCalcContainer;  
 iTouchCalcContainer = NULL;  
 // ]]] end generated region [Generated Contents]
```

```
▪ }
```

```
/**  
 * Symbian two-phase constructor.  
 * This creates an instance then calls the second-phase constructor  
 * without leaving the instance on the cleanup stack.  
 * @return new instance of CTouchCalcContainerView  
 */
```

```
CTouchCalcContainerView* CTouchCalcContainerView::NewL()  
{  
CTouchCalcContainerView* self = CTouchCalcContainerView::NewL();  
CleanupStack::Pop( self );  
return self;  
}
```

```
/**  
 * Symbian two-phase constructor.  
 * This creates an instance, pushes it on the cleanup stack,  
 * then calls the second-phase constructor.  
 * @return new instance of CTouchCalcContainerView  
 */  
CTouchCalcContainerView* CTouchCalcContainerView::NewLC()  
{  
CTouchCalcContainerView* self = new ( ELeave ) CTouchCalcContainerView();  
CleanupStack::PushL( self );  
self->ConstructL();  
return self;  
}
```

```
/**
 * Second-phase constructor for view.
 * Initialize contents from resource.
 */
void CTouchCalcContainerView::ConstructL()
{
// [[[ begin generated region: do not modify [Generated Code]
BaseConstructL( R_TOUCH_CALC_CONTAINER_TOUCH_CALC_CONTAINER_VIEW );

// ]]] end generated region [Generated Code]

// add your own initialization code here

}
```

# Active objects

- Primitive form of multi-tasking
- An AO runs “in the background”
- Needed for some API calls

```

void CSaveImageAO::SaveAsL(CFbsBitmap* aBitmap, TFileName& aFileName, TUid almageType,
    TUid almageSubType)
{
    ilmageEncoder->Convert( &iStatus, *aBitmap);
    SetActive();
}
}

void CSaveImageAO::DoCancel()
{
    ilmageEncoder->Cancel();
}

void CSaveImageAO::RunL()
{
    iObserver->ImageSaved(iStatus.Int());

}

TInt CSaveImageAO::RunError(TInt aError)
{
    iObserver->ImageSaved(aError);
    return KErrNone;
}

```

■

# Testing

- Simulator
  - Very slow
  - With HookLogger => mem leak buster
- Real device (might need DevCert)
  - Faster
  - Works via USB
  - Install Nokia PC Suite, TRK



**Selling applications**

# Signing

- Express signed – 20\$
  - Doesn't permit all capabilities
  - Usually no checks done
- Certified signed – 200\$
  - Permits most capabilities
  - Thorough checks (!!!)

# Signing - II

- Certificate needed
  - Obtained from TrustCenter Germany
- Requires registered company
  - Recommendation: UK Limited
  - [www.go-ahead.de](http://www.go-ahead.de)

# Ovi Store

- Nokia's sale channel
- 70% of gross
- Somewhat slow ATM

# Traditional channels

- Various traditional ESD's
  - Handango
  - MobiHand
  
- Diminishing importance

**Where to go for help**



# forum nokia

Forum.Nokia.com  
Driving mobile innovation

[Register](#) | [Login](#)

[Home](#) | [I Want To](#) | [Devices](#) | [Technology Topics](#) | [Ovi](#) | [Tools, Docs & Code](#) | [Community](#) | [Learning & Events](#) | [Premium Services](#)

[Blogs](#) | [Discussion Boards](#) | [Wiki](#) | [Champions](#) | [Forum Nokia for Universities](#)

You Are Here: [Home](#) > [Community](#) > [Discussion Boards](#)

[Regional Sites](#) ▼

## Community: [Developer Discussion Boards](#)

### Search Forums

[Today's Posts](#)  
[FAQ](#)  
[Mark Forums Read](#)

[Go To Market](#)

[Getting Started with Mobile Development](#)  
[Device Specifications](#)  
[Tools and SDKs](#)  
[Documentation](#)  
[Knowledge Base](#)  
[Training](#)  
[Developer Programs](#)



## Welcome

If this is your first visit, be sure to check out the [FAQ](#) by clicking the link above. You may have to [register](#) before you can post: click the register link above to proceed. To start viewing messages, select the forum that you want to visit from the selection below.

### Developer Discussions

[Feedback to Forum Nokia, Open Discussion, Jobs and News](#)

	Forum	Last Post	Threads	Posts
	<b>Forum Nokia Services Feedback</b> Feedback on Forum Nokia Services; Series 40 and S60 Platforms; Tools and SDKs; Developer Resources	<b>E55 problem</b> by xtrcom Today 12:11 >>	1,335	4,934
	<b>Open Discussions</b> General Discussions; News, Announcements and Job Listings	<b>how to convert mod to...</b> by Pearlerous Today 11:37 >>	8,991	24,429

### Development Platforms

# forum Nokia - II

- Free to register and use
  - But: bad search engine
- Most questions get answered quickly
  - Nokia employees around
- <http://discussion.forum.nokia.com/forum/>

# Nokia Wiki

- Nokia-operated Wiki
- Contains valuable tutorials

# Symbian foundation

- Has developer help services of its own
- Less developed than Nokia's
- => Stick to Nokia until told otherwise

# **Why handset-based security**

# Different user perceptions

- Mobile phones are always on the user
  - More personal
- User feels that unit "is safe"
  - No large-scale outbreaks so far
  - User is unwilling to accept implications of AV software

# Carriers can't do it alone

- GSM / CDMA
  - Can be protected
- Bluetooth
  - Can't really be protected by the carrier
- WiFi
  - Don't even ask

# **Users are stupid**

- Cabir displayed THREE warning alerts
  - Perimeter security is not enough
- Users choose dancing pigs over security
  - Ed Felton



# Stakeholders

# Carriers

- Don't want to invest \$\$\$
  - Don't burden us with investments / infrastructure
- Don't want to deal with unhappy users
  - Keep them happy
- Gain revenue if users buy more apps
  - Feeling safe == more app sales

# Developers

- Want easy access to full OS features
  - Will move to other platform if not given
- Want simple development process
- Gain revenue if users buy more apps
  - Feeling safe == more app sales
- Less risk if bugs occur
  - Can't access dangerous stuff

# OS vendor

- Doesn't want large virus outbreaks
  - Bad PR
- Doesn't want to piss off developers
- Doesn't want to piss off users
  
- Doesn't care much about power users

# User

- Doesn't want to be bugged
  - J2ME, anyone?
- Doesn't want battery drain, etc
  - Caused by AV activity
- Wants cheap apps
- Wants data to be safe

# User (power user)

- Wants full access to the system
- Wants powerful apps
- (Gets f##ed most of the time)

# **Architectural goals of PSM**

# Ensure Understandability

- Users are the weakest point of secure systems
- Users don't understand technology
- DON'T offload decisions to them
  - No IE-like prompts

# Support open phones

- Successful app market == Successful OS
- Minimize impact on legitimate developers
  - But keep jerks out

# Protect the network

- Carriers want their networks to be safe
- Software may NEVER damage the network
  - More carriers will use the OS
  - Larger market

# Be light-weight

- Preserve CPU cycles
- Don't do unnecessary checks
  - Less than 40% of API is "managed"
  - Access rights are computed at start-up of the app

# Provide a basis for trust

- Make users trust their phones
  - More app sales
  - More OS sales
- Everybody benefits



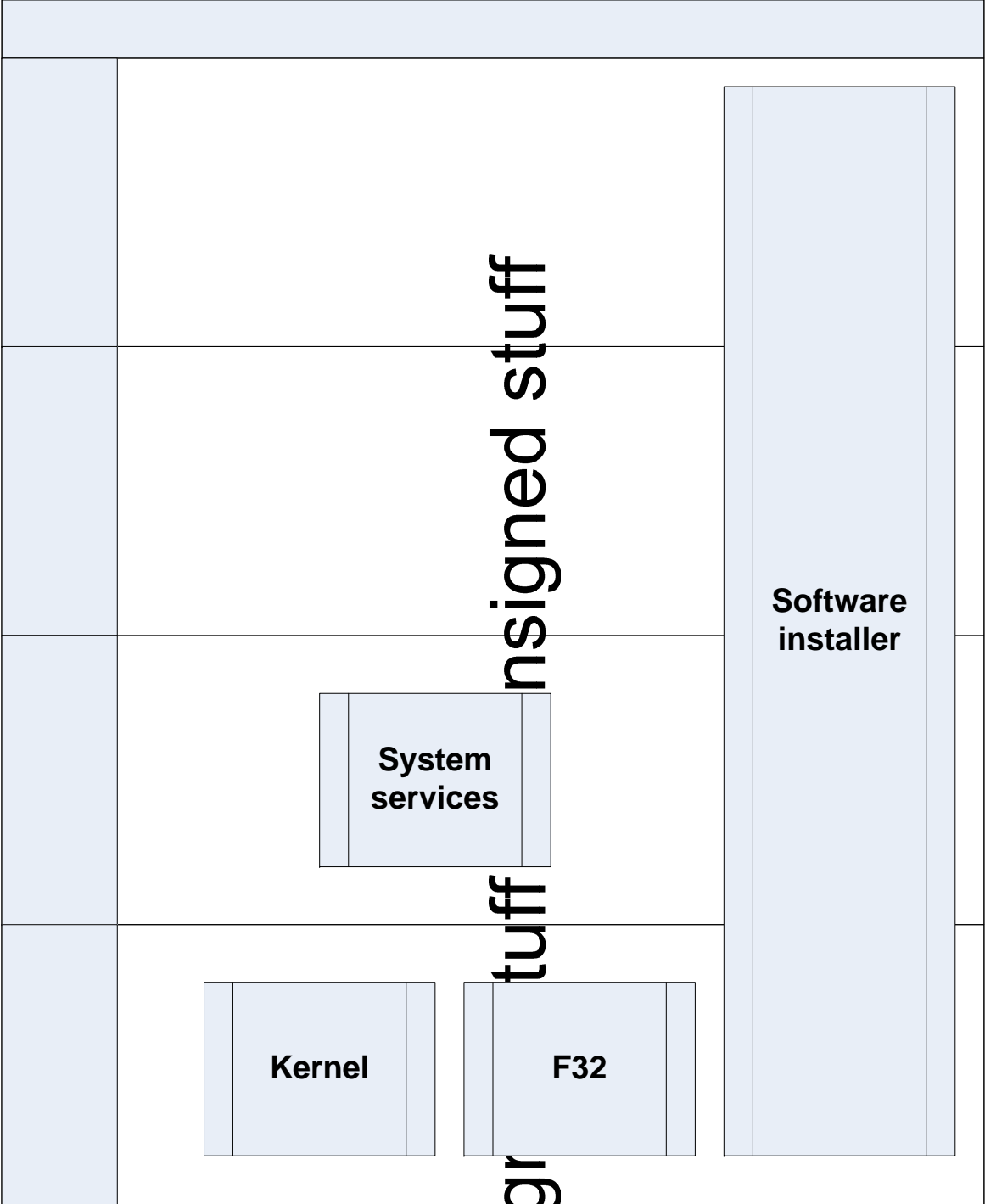
# The pillars of PSM

# The Process - I

- Mobile phone users are usually "authorized"
  - No multi-user phones
  - PIN Authentication
- User-based rights management doesn't make sense

# The Process - II

- Processes are the smallest sensible unit
- **The Process is the Unit of Trust**
- 1 process = 1 app
- Processes are divided into tiers



# The capability

- **A capability is a token which must be presented to gain access to a privileged service**
- Come in three classes
  - TCB
  - System
  - User

# The capability - II

- TCB Capabilities: TCB
- Granted to TCB processes only
- Lets them do things nobody else can

# The capability - III

- System Capabilities
  - Not meaningful to user
  - Granted by a signing house
  
- User Capabilities
  - "Not really dangerous"
  - Granted by user (like J2ME)

# Data caging

- Access to some folders is restricted
- Provides "secure storage"
- But: MMC/SD readers

# Data caging - II

Path	Read	Write
/sys	AllFiles	TCB
/resource	-	TCB
/private/mySID	-	-
/private/notMe	AllFiles	AllFiles
/other	-	-

# Capabilities

An overview

# Capability eekers

- 1 capability? 2000 capabilities?
- Granularity must be set up reasonable
- Symbian has 20 capabilities

# TCB

- Write to executables
- Write to read-only rsrc files
- Not usually given out – MANUFACTURER

# Allfiles

- Read access to the entire FS
- Not usually given out - MANUFACTURER
  - Caused the death of third-party file managers

# DRM

- Access to DRM-protected content
- Not usually given out – MANUFACTURER

# CommDD

- Direct access to Wifi, etc hardware / drivers

# DiskAdmin

- Mount, unmount file systems

# MultimediaDD

- Direct access to camera, etc drivers
- "Priority multimedia access"

# NetworkControl

- Control network protocols
- E.G. Close all TCP/IP links
- Set network defaults

# PowerMgmt

- Kill processes
- Turn off box
- Disable peripherals

# ProtServ

- Register protected server
  - Name with ! At the beginning

# ReadDeviceData

- Read data like:
  - PIN
  - List of installed apps

# SurroundingsDD

- GPS / biometrics driver access

# SwEvent

- Handle and dispatch key, pointer events GLOBALLY

# TrustedUI

- Display trusted dialogs

# WriteDeviceData

- Change things like:
  - Time zone
  - Device lock
  - System Time

# LocalServices

- Access to BT, IR, ...
  - May NOT cost user \$\$\$
- USER-granted

# location

- Access to GPS coordinates
- USER-granted

# NetworkServices

- Access to GSM/EVDO
  - Might cost user \$\$\$
- USER-granted

# ReadUserData

- Contacts
- Messages
- Appointments
  
- USER-granted

# UserEnvironment

- Access to recording, etc at API level
- USER-granted

# WriteUserData

- Write access to "user data"
- Depends on device
- USER-granted



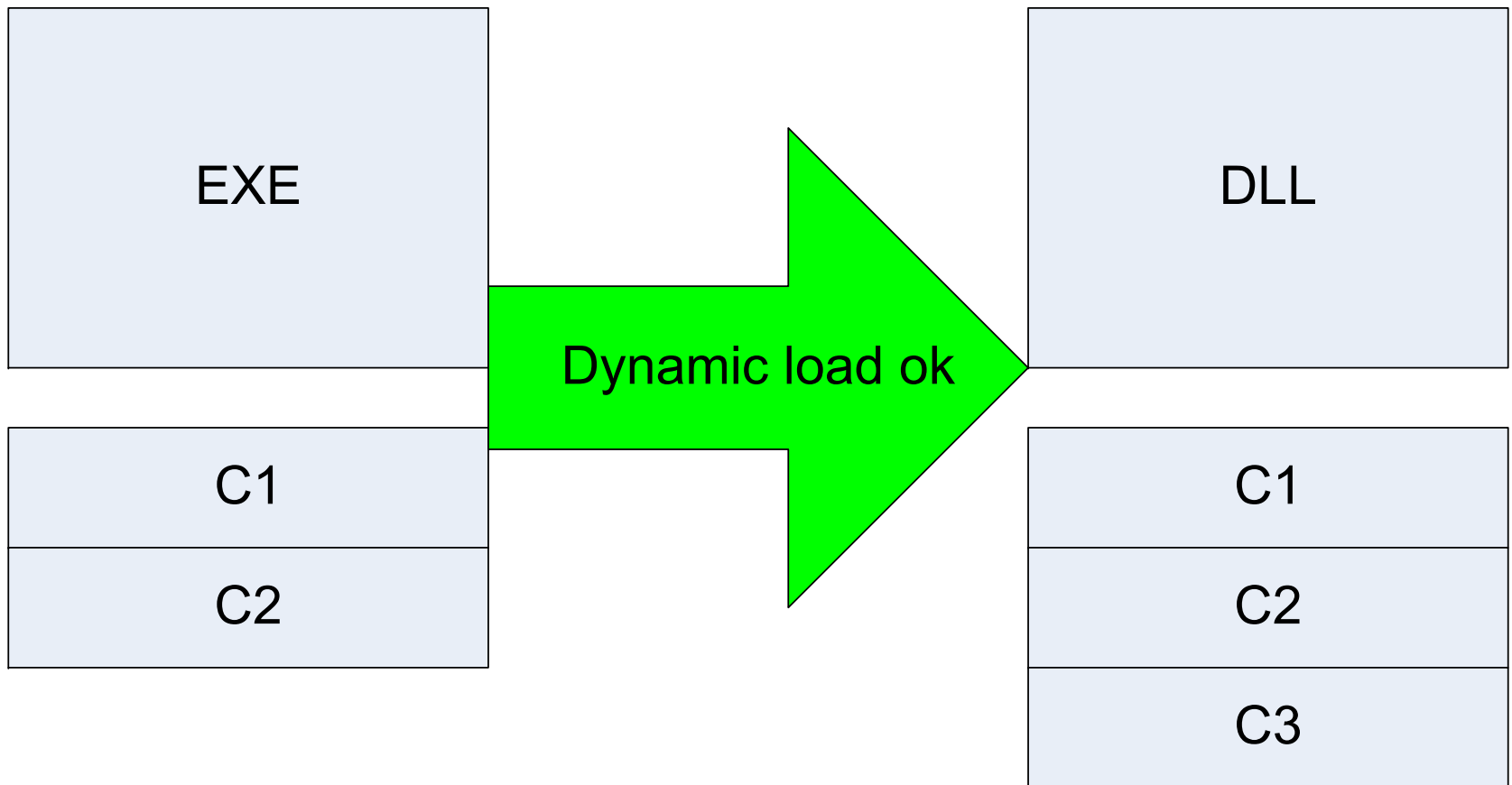
**Capability inheritance**

# Who cares / Why care?

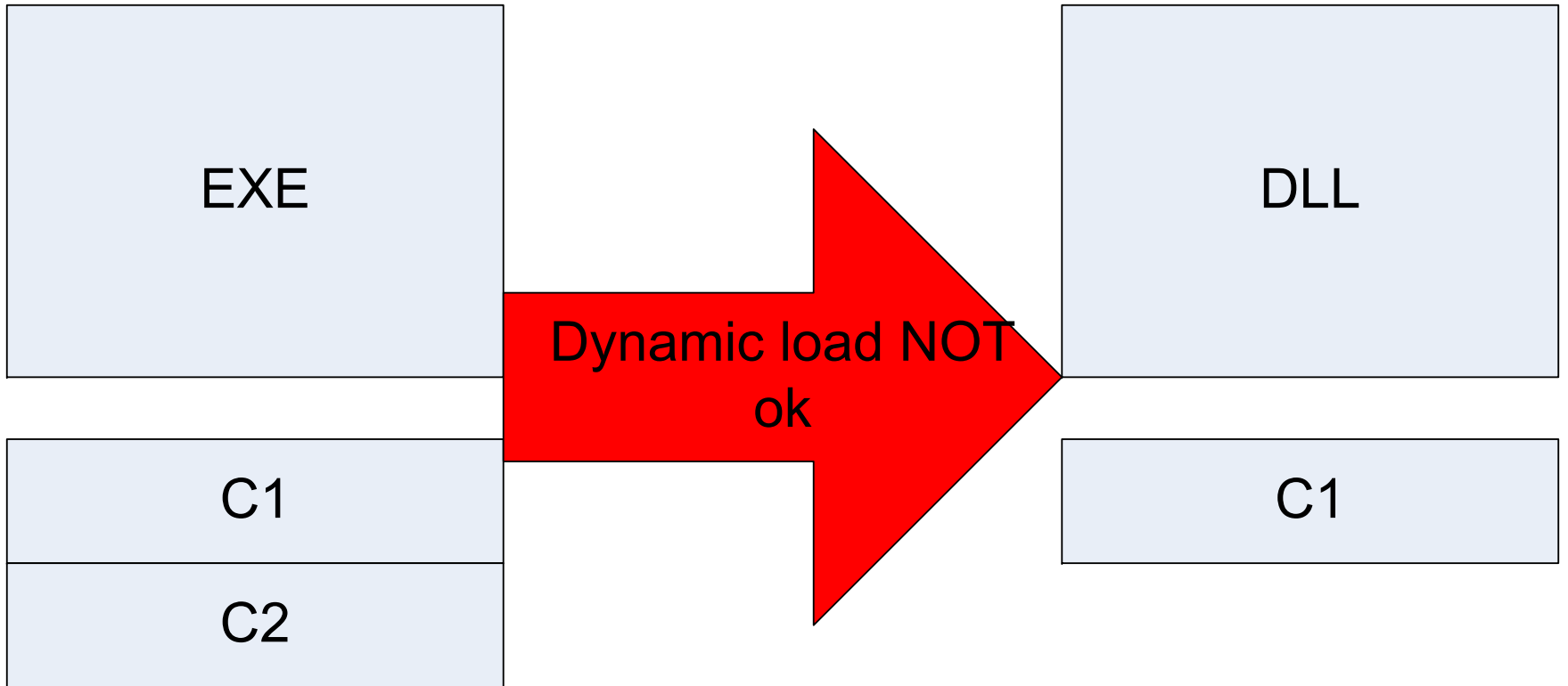
- My capabilities are limited?
- I can spawn a process from another DLL
- It has more privileges than I do
- Uh-Oh!

# Direct loading of DLL

- Don't allow DLLs to import malicious code



# Dynamic loading - II

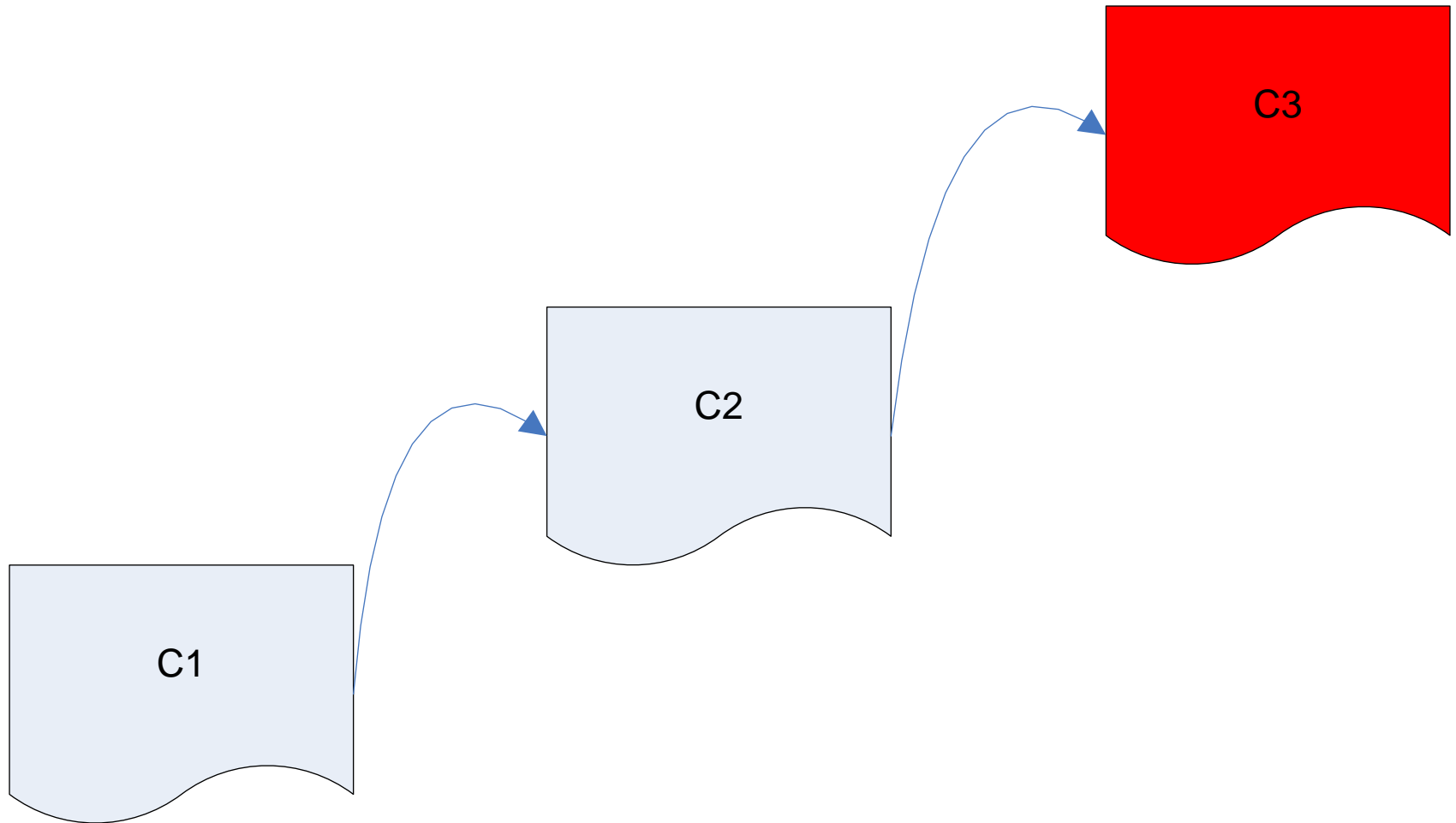


# **The native software installer**

# What does he do?

- Acts as gatekeeper between apps and system
- Performs signature check
- Performs capability check
- Handles file moving

# The signature chain



# **But: who manages the trust?**

- Somebody has access to the "root" certs
- This somebody: signing house



**Signing games**

# Open Signed Online

Symbian Signed - Mozilla Firefox 3.6 Beta 2

File Edit View History Bookmarks Tools Help

symbiansigned.com https://www.symbiansigned.com/app/page/public/openSignedOnline.do

Symbian Signed

Symbian Signed Overview My Symbian Signed Account Settings

Test houses

Symbian.org

developer.symbian.org

OPERATED BY  
**IXONOS**

PROTECTED BY  
**F-SECURE**

## Open Signed Online

### Open Signed Online (BETA) Service Information

- Open Signed Online beta service has now moved to 24hour availability
- If we discover issues that impact the performance and/or functionality of the service. Such problems may result in the service being taken off-line at short notice for extended periods.
- Open Signed Online currently does not allow you to sign a SIS that is allocated to someone else and hasn't been enabled for Open Signing; i.e. if the email address you use for Open Signed Online MUST match the email address of the account which created a UID.
- Alternatively the service will allow signing of SIS files with UIDs in the Test Range; i.e. 0xE0000000...0xEEFFFFFF.
- If you attempt to sign the same SIS file in rapid succession, the service you receive will proportionally slow down. This is to prevent abuse of the service.
- Installation of the signed SIS file will be restricted to the IMEI (i.e. mobile phone) you entered and valid for 36 months.
- SIS files that have been Open Signed will present a notification upon installation that the SIS file is intended for development purposes only.
- The service will work for SIS files intended for all Symbian-based UIs, i.e. S60 and UIQ.
- SIS files can be signed for all Platform Security Capabilities except CommDD, MultimediaDD, NetworkControl, DiskAdmin, DRM, AllFiles, TCB.

### Application information

**IMEI number\***

**Email\***

**Application\***

### Symbian Developer Network

The Symbian Developer Network is the primary source for all developer requirements for Symbian OS. Click [here](#) for downloads, technical papers, system documentation and newsgroups...

### Forum Nokia

Forum Nokia provides a wealth of information to help you develop applications for S60 phones on Symbian OS.

▶ [Click here to find out more](#)

### Sony Ericsson Developer World

Sony Ericsson Developer World helps professional developers get on the fast track from mind to market.

▶ [Click here for more information](#)

# The publisher ID

- Binds ID to company
  - Given out by Trust Center
- Elementary "trust token"
- Needed for successive signings

# Developer certificate

- Limited by IMEI
- Allows self-signing for testing purposes

# Express signed

- Gives "full signing"
  - But not all capabilities
- Not every app is checked
- Lower cost (approx 20\$)

# **Certified signed**

- Thorough checks
- Gives almost every capability
- High cost (at least 200\$)

# The end

Questions?

Answers at [tamhan@tamoggemon.com](mailto:tamhan@tamoggemon.com)

images by Julius Kusuma, Cimexus of Canberra, adactio, 3dh3m, Snowmanradio, zephyris, Paul Goyette, Agnostic Preachers Kid