

Symbian 平台安全性的测试 与认证

Version 1.4

2006.9.15

法律声明

Nokia 公司版权所有©2005-2006

Nokia 与 Nokia 论坛是 Nokia 公司的注册商标。本文的其他产品与公司名称可能为交易商各自拥有的名字。

非承诺声明

本文中的信息仅供参考，并不对其的可靠性与商业应用的可靠性，特殊情形下的适用性，除此之外的其他任何情况下的目的，样例或规范做出保证。再者，本文所提供的信息是有时效性的，在最终版本发布时可能会有改变，本文目的仅为提供信息。

Nokia 公司不承诺所有责任，包括关系本文列举信息所关联的对所有私人权利保护的责任。Nokia 公司不保证或声明这类信息的使用不会侵害相关权益。

Nokia 公司重申该规范可能在任何时间不经通告而发生变化。

证书

此处的证书被授权用于私人目的及对本规范拷贝的下载。此处并无其他关于知识产权的相关证书。

内 容

1. 绪论	4
2. Symbian 安全模型	4
2.1 对Symbian平台安全模型的论证	4
2.2 Symbian 平台安全模型实践	4
2.2.1 基于可信计算	4
2.2.3 功能	4
2.3 应用程序认证	5
2.4 分配功能	5
2.5 平台需求或制造商架构	7
3. 入侵检测系统	7
3.1 唯一标示符	7
3.2 产品序列号	7
3.3 制造商序列号	7
3.4 制造商序列号和产品序列号使用	8
4. 嵌入SIS文件	8
5. 应用开发时的Symbian安全模型	8
5.1 定义应用程序	8
5.2 应用程序测试	8
5.2.1 Symbian 开发商证书	8
5.3 Symbian注册	9
5.4 授予TCB/DRM	10
5.5 Symbian 自主验证	10
6. 术语与缩写	11
7. 资源评估	11

变更历史

2005.9.5	1.0 版	初始文档发布
2005.10.17	1.1 版	关于开发者资质证书价格的更新
2006.3.1	1.2 版	功能信息的更新 添加了入侵检测系统章
2006.3.20	1.3 版	添加了嵌入式 SIS 文件章 对身份标示章的小更新
2006.9.15	1.4 版	对授予增加段功能的澄清 2.5 节增加了那些包含需求特定功能的案例描述

1、绪论

本文档描述了 Symbian 平台安全的一些基本概念，并对开发商如何获取相关功能进行了延伸探讨。

2、Symbian 安全模型

2.1 对 Symbian 平台安全模型的论证

移动设备所具有的能力日益增长，因此，用户在使用移动设备处理大量的重要信息时，移动资源所拥有的资源的重要性亦不断增长。然而，对于移动设备来说，虽然他们和普通的计算机并不一样，但令用户发现他们的电话易用、可靠、安全和值得信任仍是我们的目标。从这个目标出发，我们向大家介绍 Symbian 平台安全模型。这个模型的目的不是令用户关掉他们的手机，而是想让用户和以前一样，将其作为一个简便的，值得信任的工具来使用。将这个设想应用在广大用户群所拥有的只能设备上，是完全可能的。同时，这个目标亦会为应用程序带来大批的用户。

2.2 Symbian 平台安全模型实践

Symbian 安全模型主要使用以下三种模型：

1. 基于可信计算。
2. 数据牢笼
3. 功能

2.2.1 基于可信计算

基于可信计算是一种关于强制使用功能和数据囚笼模式软件的集成方式。其包括核心，文件系统和软件安装程序。对于平台安全模型来说，这是操作系统的控制部分。

2.2.2 数据牢笼

数据牢笼意味着用户只能访问文件系统的部分区域。在实际应用中，用户可以访问他们自己的目录与标记设定为开放的目录。这意味着，举个例子，一个应用程序不能访问其它应用程序的私有目录与数据。其获取限定方法如下：

\资源

应用程序图标的位置，位图等等。仅在应用程序安装时允许写操作。所有人都可以对文件夹执行读操作。

\系统

二进制的位置，包括应用程序安装注册与登陆证书。用户仅在应用程序安装时拥有写权限。当备份应用程序时有读权限。

\私有

这是每个应用程序的私有空间。用户仅在应用程序所在的目录有读权限与写权限。当备份软件时，允许对该目录进行读写。

\其它

可以对其它所有的文件夹不受限制的访问，例如，用户的照片，音乐和文档。

2.2.3 功能

可以通过证明为一类应用程序接口授予功能访问权限。例如 Symbian 认证。功能可被分为 4 个部分。

1. 对所有开放
 - 在目录下的应用程序接口拥有所有的基本属性，例如，大部分的单主角游戏。
 - 一般来说，约 60% 的应用程序接口可以自由使用而不需要定义特别的容量需求。
2. 在安装时授予用户
 - 一些功能可以在用户进行安装时进行授权。
 - 应用程序设定为默认获得，直到应用程序从设备上移除。
 - 在某些缺省设备上选项将不被激活。因此用户不得不单独激活那些安装阶段授权的功能。

Symbian 平台安全性的测试与认证

3. 通过 Symbian 认证授权

- 当通过 Symbian 认证授权后，一些功能将可用。
- 某些敏感功能需要在使用时进行验证。也可能需要通过测试。
- 大多数敏感功能要求开发商填写功能需求表与平台制造商同意表，还需要通过一些包括额外平台开发商所定义规范的测试。关于 S60 的规范可以在 www.forum.nokia.com/testing 的 Nokia Test Criteria for Symbian C++ Applications 文档中找到。

4. 通过制造商进行授权

- 功能需求表包括 TCB 与 DRM 功能。其由设备制造商提供并由一个法律协议规范。
- 由于强烈的商业原因，通常需要获得这些功能

2.3 应用程序认证

S60 第三版介绍了应用程序托管认证。这意味着如果没有使用认证，应用程序将无法安装。一般来说有以下两种认证：

1. 使用任意私有标签(私钥)获得唯一认证并且确保 SIS 文件的完整性。使用 makekeys 程序可获得私钥，而利用运行 signsis 程序则可完成应用程序认证过程。以上两种应用程序均可由 SDK 获得。
2. 使用特殊私有密钥注册从而获得证书——认证应用程序从而使设备上的可信根证书认证应用程序。

在部署过程期间，为了将应用程序安装到设备上，开发商应该使用第一种 认证。后一种认证方法可以通过 Symbian 注册来获得相关功能。

2.4 分配功能

应用程序所需要的功能可以在程序设计阶段定义下来。应用程序定义文件包括一个 MMP 文件，其包含了应用程序所拥有功能的相关信息。然而，车载用户可以通过车载设备用户界面在一个特殊区域获得功能信息。

在应用程序安装阶段，设备将检测应用程序是否注册或认证。随后其将检测根证书用于确定设备是否被授予应用程序所需求的相应功能。如果没有遇到问题，安装过程将继续直至完成。

表 1 显示了功能是如何划分的。

非受限	安装时用户授权	Symbian 认证	制造商核准
60% 的 API	读用户信息 写用户信息 网络服务 本地服务 用户环境 注意：实施可能在两台设备间完成	用户授予权限+定位 声明： 读设备数据 写设备数据 准许在系统中中断任何进程或者转换机器状态（关掉设备） 准许访问提供外围设备输入信息的逻辑设备驱动 准许服务器应用可以用一个受保护的名字进行注册 区分” normal” 应用和” trusted” 应用的 UI 准许生成或者捕获键盘以及笔输入事件	Symbian 认证功能+ 功能需求表与功能商鉴定： ● DRM ● TCB
		功能需求格式及核准平台	

		准许进行硬盘管理操作，例如 格式化驱动器 所有文件操作 准许访问通信设备驱动 准许对所有多媒体设备驱动 （声音、摄像头等）的访问 准许修改或者访问网络协议控 制	
--	--	---	--

表 1 功能对比

表 2 为实践环节的更多功能提供了信息

	功能	说明
1	准许修改或者访问网络协议控制 (NetworkServices)	例如拨号或发文本信息的功能
2	本地服务 (LocalServices)	通过 USB,红外或点对点蓝牙规范通信的能力
3	读用户数据(ReadUserData)	授予用户读信息的权限。当授予该级规范与用户数据时，系统服务器与应用程序引擎是非限的
4	写用户数据 (WriteUserData)	授予用户数据写权限。同时，当授予该级规范与用户数据时，系统服务器与应用程序引擎是非限的
5	准许访问手机的位置信息 (Location)	授予可获得电话位置的权限
6	准许访问用户及其附近环境的实时保密信息(UserEnvironment)	授予访问涉及他/她紧密环境的生活秘密信息的能力。
7	准许在系统中中断任何进程或者 转换机器状态（关掉设备） (PowerMgmt)	准许在系统中中断任何进程或者转换机器状态（关掉设备）
8	准许对所有多媒体设备驱动（声 音、摄像头等）的访问 (MultimediaDD)	控制访问所有多媒体设备驱动的能力（声音，照相等等）
9	读设备信息(ReadDeviceData)	授予读敏感设备数据信息的能力
10	写设备信息 (WriteDeviceData)	授予写敏感设备数据信息的能力
11	准许访问 DRM 保护的內容 (DRM)	准许访问 DRM 保护的內容的能力
12	区分” normal” 应用和” trusted” 应用的 UI (TrustedUI)	该功能区分” normal” 应用和” trusted” 应用的 UI。当一个” trusted” 应用在屏幕上显示内容时，一个” normal” 的应用不能伪造它。
13	准许服务器应用可以用一个受保 护的名字进行注册(ProtServ)	授予服务器以受保护名进行注册的权限。受保护名以“!”开头，其核心是阻止无该权限的服务器使用这类名称，并且这种方式将保护服务器信息的私有化
14	准许修改或者访问网络协议控制 (NetworkControl)	授予可以修改或获得网络协议控制能力的权限。
15	准许生成或者捕获键盘以及笔输 入事件(SwEvent)	授予生成与捕获软件关键词与画笔事件的权限。

16	准许访问提供外围设备输入信息的逻辑设备驱动(SurroundingsDD)	授予通过电话等周边设备向本地设备提供输入信息的权限。
17	准许在终端中访问 /sys 以及 /resource 目录(TCB)	授予访问电话/sys 或/resource 的权限
18	准许访问通信设备驱动(CommDD)	准许访问通信设备驱动
19	准许进行硬盘管理操作, 例如格式化驱动器(DiskAdmin)	准许进行硬盘管理操作, 例如格式化驱动器
20	准许系统中的所有文件可见, 而且还可对在/private 下的文件进行写操作(AllFiles)	准许系统中的所有文件可见, 而且还可对在/private 下的文件进行写操作

表 2: 功能描述

2.5 平台需求或制造商架构

在一些情况下, 某种功能是需要, 而在其它情况下, 对这类需求并没有直接的应用。例如:

1. 在 S60 第三版中, 使用除了可信计算基外其它所有功能的应用程序为:

- 消息类型模块
- 前后进程
- 浏览器插件

2. 使用文件服务进程的设备加密应用程序需要以下功能: 可信计算基, ProtServ, DiskAdmin, AllFiles, PowerMgmt, 和 CommDD。

3. 反病毒应用程序至少需要可信计算基。

一些特定情况下, 应用文档描述所需要的特定功能, 但深层检查可以得知其是否需要使用特定功能。在诺基亚论坛, 需要使用特殊功能的情况在关于平台安全页的问题回答段有相关描述

www.forum.nokia.com/platformsecurity。

3、入侵检测系统

Symbian 操作系统使用一些不同的入侵检测系统。因此, 了解一些入侵检测系统的详细信息是非常必要的。

3.1 唯一标识符

一个唯一标识符用来唯一标识应用程序。唯一标识符可以从Symbian的网站www.symbiansigned.com获得。当使用唯一标识符时, 推荐使用公司数字签名ACS出版序列号所描述的精确名称。

唯一标识符可以分成两个域:

受保护唯一标识符域: 0X00000000...0X7FFFFFFF

非保护唯一标识符域: 0X80000000...0XFFFFFFFF

保护域面向从受鉴应用程序——非保护域则面向认证应用程序。如果认证应用程序获得鉴定, 则唯一标识符需要被更换。

3.2 产品序列号

一个产品序列号用来表示产品即应用程序是否可以运行。如果你使用一个特殊设备产品序列号, 则应用程序需要安装在特殊设备上, 如果你使用一个特定版本平台的产品序列号, 则应用程序将在特定版本平台上安装所有的产品。如果产品序列号非法, 则用户会接到一个报警信息, 但安装仍然将继续执行。

3.3 制造商序列号

如果你在一个 if else 段使用一个制造商序列号，例如，一个平台序列号，应用程序将仅安装平台上特定制造商的设备。

3.4 制造商序列号和产品序列号使用

下列文件是部分 PKG 文件。

```
;Supports S60 3rd  
fOx101F7961], 0, 0  
Edition  
0, { " Series603rdEditionProductID"  
IF manufacturer=2;(2 is Nokia)  
;This part will then contain the installation information about the  
;files of the application  
ELSE  
}}badmanufacturer.txt" —"  
ENDIF  
FILETEXT  
TEXTEXIT
```

在这个例子中，应用程序可以在来自 Nokia 的所有 S60 第三版设备上被安装。

4、嵌入 SIS 文件

当授予敏感功能时，对敏感功能进行限定是非常必要的。可以通过将一个 SIS 文件绑定主体分布式 SIS 应用文件来完成。在这种方式下，嵌入式 SIS 文件将仅包括需求某些敏感功能的嵌入式 SIS 文件。CommDD, MultimediaDD, NetworkControl, DiskAdmin, AllFiles, DRM 和 TCB 被确认为是敏感功能。

一个 SIS 文件的 SA 类型可以被轻易的嵌入一个 SA 类型的 SIS 文件。嵌入的过程可以通过为主 SIS 文件添加下行语句完成。

@ " The Embedded SIS name. sis" (The- Embedded-SIS UID)

使用 SA 型 SIS 文件的好处是其使用起来非常容易。在应用程序管理器上，下载端嵌入式 SIS 文件是可见的。因此，用户可能偶然的移除该文件。

5、应用开发时的 Symbian 安全模型

想更好的理解安全模型描述，了解和掌握应用程序所需要的功能是非常重要的。

5.1 定义应用程序

当应用程序在设计阶段时，用于定义和规划，有两个主要的议题需要被讨论。

1. 对于 Symbian 上的应用程序，到底需要什么认证标准？
2. 如果需要的话，应用程序需要那些功能？

5.2 应用程序测试

应用程序可以用一个 SDK 模拟器进行测试。建议在真实网络环境中使用实际设备进行测试——很少有模拟器能收到拨号。如果应用程序所使用的功能需要数字信号，为了测试应用程序在设备上所期望的功能，则必须首先使用模拟器进行测试，其次使用 Symbian 认证的开发商证书。

5.2.1 Symbian 开发商证书

Symbian 开发商证书可以被开发商用于认证他们的应用程序，从而使设备测试获得所需求的功能规范。证书是针对特定国际移动设备验证码的约束，并且不能被更换。对于获取 Symbian 开发商证书由一些限制如表 3 所示：

国际移动身份验证码数量	证明	功能
1	Symbian 认证帐号	本地服务, 用户环境, 网络服务, 位置, 读用户数据, 写用户数据, SWEvent,SurroundingsDD,ProtSrv,Power Mgmt
超过 20	VeriSign 内容认证服务与 Symbian 注册帐号	上栏所有+读设备数据与写设备数据, 可信 UI
常规	VeriSign 内容认证服务, Symbian 注册帐号与制造商支持	上栏所有+DRM,网络控制, MultimediaDD, TCB,所有文件, CommDD,Disk Admin

表 3: Symbian 开发商证书需求

总的来说, 过程需要完成如下需求:

1. 开发商进入 Symbian 注册端口及注册
2. 开发商使用需求工具给开发商证书发送请求
 - 可以从 Symbian 注册网站下载的工具
 - 可能在这个阶段需要 VeriSign 内容认证服务出版序列号。

注意 VeriSign 内容认证出版序列号在一年内有效。

3. 证书生成与返还开发商
 - 自开发商证书获取日期证书有效期为 6 个月
 - Symbian 开发商注册证书更换免费; 然而, 开发商可能需要 VeriSign 内容认证出版序列号, 该序列号的获取需要付费。

使用不同的链接, 通过获取通用开发商证书, 可以使用同样的端口来完成流程。然而, 制造商需要在开发商获取开发商证书前验证其需求。若应用程序可以获取一个开发商证书, 申请可以通过一个基本申请表来完成, 这个流程同样将获得一个最终证书。

5.3 Symbian 注册

为了获取最终证书, 应用程序必须通过 Symbian 注册。本节将展示该流程的几个要点, 从而帮助理解流程的重点。

当提交 Symbian 注册时, 需要 VeriSign 内容认证出版序列号。这是进行 Symbian 注册的先决条件。同样地, VeriSign 内容认证出版序列号可以在申请开发商证书时使用。

如先前提示的那样, 确定功能可以通过标准 Symbian 认证与对确定 Symbian 认证的声明来完成。在这种情况下, 应用程序需要以下功能:

- CommDD
- MulitmediaDD
- NetworkControl
- DiskAdmin
- AllFiles

当提交应用程序时, 开发商必须提交功能请求表, 功能请求表将被发送至平台制造商用于验证。

下列需求适用于以上五个功能:

- 应用程序必须通过Symbian注册测试与默认的附加标准。Nokia关于S60 应用程序的测试标准可以在Nokia关于SymbianC++应用程序的测试标准中获知, 详情可见: www.forum.nokia.com/testing。
- 如果应用程序架构可行, 则敏感功能的扩散应当使用第 4 章“嵌入式 SIS 文件”所描述的嵌入式 SIS 文件进行限制。
- 部分需要使用上述功能的应用程序应当打包进入分离的 SIS 文件。
 - SIS 文件将有需求的功能。

- 开发商可使用如在主应用程序 SIS 文件中使用的嵌入式 SIS 完成应用程序的发布。

5.4 授予 TCB/DRM

当使用 TCB 或者 DRM 功能时，流程有一些不同。如要获得这些功能，开发商必须填写功能请求表。当开发商接触更多细节时，需要评估下述细节。

需求的应答请求如下：

- 与 Nokia 达成的一个关于使用该功能所需义务的协议。
- 应用程序必须通过 Symbian 注册测试与默认的附加标准。Nokia 关于 S60 应用程序的测试标准可以在 Nokia 关于 Symbian C++ 应用程序的测试标准中获知，详情可见：www.forum.nokia.com/testing。
- 应用程序可以被定义安装在来自 Nokia 的同型平台上。详情可见 3.4 节，“制造商序列号与产品序列号的使用。”
- 应用程序的相关部分需求将上述提及的功能需求加入到独立的 SIS 包中去。

SIS 文件需要包含所需求的功能。

在应用程序发布时，开发商可以将 SIS 文件嵌入主应用程序的 SIS 文件。

5.5 Symbian 自主验证

创建大量应用程序的开发商通常可以成为一个 Symbian 自主验证者。这类开发商必须有一个坚实的质量保证流程，并且拥有良好的声誉。他们必须拥有至少一个 Symbian 优先注册程序。他们必须与 Symbian 达成法律协议。这类架构将要求开发商向 Symbian 支付通告费用。

这类开发商可以确定他们的应用程序拥有通过 Symbian 注册的，不考虑平台或设备制造商设备支持的相关功能。如果开发商创建的应用程序依赖平台或设备制造商认证，则 Symbian 自主验证有以下两个选项：

1. 利用平台或者设备制造商获取一份协议，从而开发商可以使用必须的功能。这类协议需要有坚实的商业原因以说明为什么开发商不得不采用自主验证的方式来获得平台或设备制造商提供的功能。
2. 将应用程序需求平台或设备制造商提供的功能打包到独立的 SIS 文件中，从而进行分离验证，开发商将 SIS 文件捆绑进入主应用程序支付过程，同时使用自主验证架构来验证应用程序。

6、术语与缩写

术语与缩写	含义
API	应用程序接口
CA	信用验证
PKI	公钥基础设施
SIS	Symbian 系统格式化文件
UI	用户接口
PU type SIS file	SIS 文件分部升级类型
VerSign ACS Publisher ID	VerSign 的产品，一个统一的证书，“授权内容注册出版商序列号”

7、资源评估

通过使用资源占有率，将占用您的一小段时间用于帮助我们提升文档质量并且标示你发现的最优价值资源。