

Symbian Platform 安全测试及认证

版本 1.3
2006 年 4 月 28 日

S
Y
M
B
I
A
N
O
S

法律声明：

版权©诺基亚公司 2006。版权所有。

Nokia 和 Nokia Connecting People 是诺基亚公司的注册商标。Java 以及基于 Java 的商标是 Sun Microsystems 公司的注册商标。本文中提到的其它产品和公司名称可能是其相应公司的商标或商号。

否认声明：

本文内容按“现状” (as is) 提供，即没有任何形式的保证，包括对产品可销售、适合特定目的以及其它由本文任何建议、规范和范例衍生出来的任何保证。另外，本文提供的信息是初级的，因此在最终版本确定之前其可能有很大改动。本文目的仅是提供信息参考。

诺基亚公司不承诺承担任何责任，包括对任何所有权的侵害责任，尽管这些所有权与实施本文给出的内容有关。诺基亚公司不保证或声称使用本文内容不会侵害上述所有权。

诺基亚保留对本文，在未经事先通知的情况下，随时进行变更的权力。

许可声明：

允许对本文进行仅用于个人使用目的的下载和打印。在此没有许可任何其它知识产权。

目录

1.	引言	5
2.	Symbian 安全模型	6
2.1	Symbian Platform 安全模型的论证	6
2.2	实际使用的 Symbian Platform 安全模型	6
2.2.1	可信计算基	6
2.2.2	数据锁定	6
2.2.3	能力	7
2.3	应用签名认证	7
2.4	能力分配	7
3.	IDs	10
3.1	UID	10
3.2	产品 ID	10
3.3	制造商 ID	10
3.4	制造商 ID 和产品 ID 使用范例	10
4.	嵌入式 SIS 文件	11
5.	应用开发的 Symbian 安全模型	12
5.1	定义应用	12
5.2	测试应用	12
5.2.1	Symbian 开发者证书	12
5.3	Symbian 签名	13
5.4	赋予 TCB/DRM	13
6.	术语及缩写	15
7.	资源评估	16

修订记录

2005 年 9 月 5 日	版本 1.0	初始文档版本
2005 年 10 月 17 日	版本 1.1	更改开发者证书定价信息
2006 年 3 月 1 日	版本 1.2	更改能力信息 增加关于 ID 的章节
2006 年 4 月 28 日	版本 1.3	增加关于嵌入式 SIS 文件的章节 对 ID 章节进行少量更改

1. 引言

本文首先描述了 Symbian Platform 安全基础，然后对这些基础展开了讨论并且介绍了开发者如何获取能力。

2. Symbian 安全模型

2.1 Symbian Platform 安全模型的论证

移动设备的功能越来越多，因此它们具有的大量重要信息对其用户而言也更有价值了。但是，由于移动设备和计算机不同，而且其理念是确保用户仍认为他们的手机简单好用、可靠、安全、并且可以信赖。基于这个目的，我们提出了 Symbian Platform 安全模型。此模型的目的不是要关闭手机，而是确保用户能像以前一样，继续便捷而且信赖地使用他们的手机。

2.2 实际使用的 Symbian Platform 安全模型

Symbian Platform 安全模型有三个主要模块：

1. 可信计算基
2. 数据锁定
3. 能力

2.2.1 可信计算基

可信计算基是一个保证和实施能力和数据锁定的软件的集合。它包含内核、文件系统、以及软件安装三个部分。这是平台安全模型操作系统的控制部分。

2.2.2 数据锁定

数据锁定意味着应用程序和用户只能访问文件系统的某些区域。在实际应用中，应用程序能访问它们自己的私有目录和标明为公开的目录。这就意味着，例如一个应用程序将无法访问另一个应用程序的私有目录和数据。

访问限制如下：

\资源

这是一个存放应用程序图标、位图等的位置。只允许在应用程序安装时写入。每个应用都可以读取此文件夹。

\系统

这是一个存放包含应用程序安装注册和根证书(roo certificate)的二进制码的位置。只允许在应用程序安装时写入。允许读取以便备份应用程序。

\私有

这是每个应用程序的私有场所。只能读写应用程序自己的目录。备份软件可以读写此目录。

\其它

任何一个应用都能访问所有其它的文件夹，例如，用户的图片、音乐以及文档。

2.2.3 能力

能力允许访问一组 API,它可以通过认证获得,例如 Symbian 签名 (Symbian signed)。能力可以分为下四种类型:

1. 对所有人开放
 - 这些 API 支持所有基本应用软件的开发,例如大多数的单人游戏。
 - 一般来说,大约 60%的 API 可以免费得到,并且无需任何能力要求。
2. 在安装时由用户授权
 - 有一些能力可以由用户在应用软件安装阶段授权。
 - 此应用软件将具有此能力直到应用软件从设备上被卸载。
 - 这一选择项在有些设备上缺省未被激活。因此,用户必须单独激活安装时间能力授权。
3. 通过 Symbian 签名授权
 - 有一些能力在经过 Symbian 签名测试后才可用。
 - 有些更加敏感的能力要求给出应用软件需要访问这种能力的明确理由。因此必须通过相应的测试。
 - 最敏感的能力要求开发者填写能力请求表格而且还要得到平台制造商的允许。而且必须通过相应的测试。
4. 由制造商授权
 - 诺基亚论坛给出了一种 *制造商核准能力要求表格 (Manufacturer Approvable Capability Request Form)*, 此表格可以在 www.forum.nokia.com/testing 下载。

2.3 应用签名认证

S60 第三版本提出强制性的应用软件签名认证。这意味着如果还没有签名,那么应用软件就不能安装。一般而言有两种签名方式:

1. 用任一私钥进行签名以达到唯一性,并确保 SIS 文件的完整性。“Makkeys”应用生成应用软件可以用来生成需要的密钥,而“signsis”可以用来签名应用软件。这两个应用软件都可以在相应的 SDK 安装文件中找到。
2. 用一种特殊的私钥进行签名以获取认证—签名应用软件,这样设备上的可信的根证书将会信任此应用软件。

为了能在设备上安装应用软件,开发者需要在开发过程中完成第一种签名方式。第二种签名方式能够通过 Symbian 签名来完成,并通过 Symbian 签名来赋予能力。

2.4 能力分配

应用软件需要的能力应该在应用软件设计阶段定义。应用软件二进制码包括一个 MMP 文件,此文件含有应用软件所用能力的信息。

在安装阶段，设备中的安装应用软件会检测应用软件是否已被认证或签名。然后检查 MMP 文件中的能力列表。如果此应用软件已被认证，那么再进一步检查根证书是否可以授权所要求的能力。如未遇问题则安装继续。

表 1 说明了能力是如何分类的。

无限制的	用户授权（在安装阶段）	Symbian 签名	制造商授权
API 的 60%	ReadUserData	用户赋予能力+	Symbian 签名能力+
	WriteUserData	公布的： <ul style="list-style-type: none"> • Location • ReadDeviceData • WriteDeviceData • PowerMgmt • SurroundingsDD • ProtServ • TrustedUI • SwEvent 	DRM TCB
	NetworkServices LocalServices UserEnvironment		
注：不同设备的实现方式可能不同	能力请求表格和平台授权： <ul style="list-style-type: none"> • DiskAdmin • AllFiles • CommDD • MultiMediaDD • NetworkControl 		

表 1：能力比较

表 2 提供了实际应用中关于各种能力的更多信息。

	能力	描述
1	NetworkServices	此能力可以用来拨打一个号码或者发送一个文本消息。
2	LocalServices	此能力可以通过 USB、IR 以及端到端的蓝牙外设发送或者接收信息。
3	ReadUserData	赋予读用户数据的功能。系统服务器和应用软件引擎能对其数据赋予这种限制级别。

	能力	描述
4	WriteUserData	赋予写用户数据的功能。同样，系统服务器和应用软件引擎能对其数据赋予这种限制级别。
5	Location	赋予查询电话位置的功能。
6	UserEnvironment	赋予查询用户实时机密信息及其当前环境的功能
7	PowerMgmt	赋予中止系统中任一进程或者改变机器状态（关机）的功能。
8	MultimediaDD	控制访问所有多媒体设备的驱动（声音、照相等）
9	ReadDeviceData	赋予读敏感系统数据的功能。
10	WriteDeviceData	赋予写敏感系统数据的功能。
11	DRM	赋予访问受保护内容的功能。
12	TrustedUI	这一能力将“常规的”应用软件和“可信的”应用软件区分开来。如果一个可信的应用软件在屏幕上显示内容，那么一个常规的应用软件不能仿造这些内容。
13	ProtServ	授权服务器用一个受保护的名字登记。受保护的名字以一个“!”开头（惊叹号）。Kernel 禁止没有 ProtServ 功能的服务器使用这样的名字，这样就预防了受保护的服务器被模仿。
14	NetworkControl	赋予修改或访问网络协议控制的功能。
15	SwEvent	赋予产生和捕捉软件键事件以及笔(pen)事件的功能。
16	SurroundingsDD	赋予访问提供关于电话环境输入信息的逻辑设备驱动的功能。
17	TBC	赋予访问电话中/sys 和/recourse 路径的功能。
18	CommDD	赋予访问通信设备驱动的功能。
19	DiskAdmin	赋予磁盘管理功能，例如格式化驱动器。
20	AllFiles	赋予对系统中所有文件可见的功能，以及对/private 目录下的文件进行写操作的功能。

表 2：能力描述

如前所述，有些能力是由设备制造商赋予的。制造商在赋予这些能力之前将行使其判断力。通常通过充分的商业推理就足以确定是否赋予这些能力。

对于需要为其应用软件申请制造商能力的开发者来说，必须与相关的制造商联系以便获取更为详细的信息。

3. IDs

在 Symbian 操作系统中使用了很多不同类型的 ID。更详细地了解一下其中一些 ID 是很重要的。

3.1 UID

唯一标识符 (UID) 是用来唯一地标识应用程序的。UID 可以从 Symbian 获得, 其网址为 www.symbiansigned.com。当申请一个 UID 时, 建议使用公司的 VeriSign ACS Publisher ID 中定义的相同的公司名称。

UID 分为两个范围:

- 受保护的 UID 的范围: 0x00000000 ... 0x7FFFFFFF
- 不受保护的 UID 的范围: 0x80000000 ... 0xFFFFFFFF

受保护的 UID 用于需要认证的应用软件——而不受保护的 UID 用于签名的应用软件。如果已经签名的应用软件需要认证, 则必须改变其 UID。

3.2 产品 ID

产品 ID 用来标识应用程序应该在什么产品上运行。如果你使用特定设备的产品 ID, 则应用程序只能在此特定设备上安装。如果你使用特定平台版本的产品 ID, 则应用程序能够在使用此特定平台版本的所有产品上安装。如果产品 ID 不正确, 那么用户将收到一个警告信息, 但可以继续安装。

3.3 制造商 ID

如果你在一个具有平台 ID 的 IF ELSE 语句中使用制造商 ID, 则应用程序只能在此平台的特定制造商设备上安装。

3.4 制造商 ID 和产品 ID 使用范例

下面范例是一个 PKG 文件的一部分:

```
;Supports S60 3rd Edition
[0x101F7961], 0, 0, 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"-", FILETEXT, TEXTEXIT
ENDIF
```

在此例中, 应用程序可以在诺基亚所有的 S60 第三版设备上安装。

4. 嵌入式 SIS 文件

在赋予敏感能力时，将敏感能力开发限制到最小值是很重要的。通过将 SIS 文件嵌入到主要应用软件发布 SIS 文件中可以实现这一目的。这样，嵌入的 SIS 文件将仅包含应用软件中要求更多敏感能力的部分。CommDD、MultimediaDD、NetworkControl、DiskAdmin、AllFiles、DRM 和 TCB 被认为是敏感能力。

SIS 文件的 SA 类型可以很容易地嵌入到 SA-类型的 SIS 文件中，通过将下行加入到主 SIS 文件的 PKG 文件中就能完成。

```
@ " The_Embedded_SIS_name.sis", (The_Embedded_SIS_UID)
```

使用 SA-类型的 SIS 文件的好处是实现起来相对容易。但其不利方面是嵌入式 SIS 文件在应用软件管理器中是可见的。因此，用户可能会不小心删除此文件。

5. 应用开发的 Symbian 安全模型

根据以上安全模型描述，应用软件需要哪些能力以及怎样获得这些能力都很重要。

5.1 定义应用

当应用软件开发处于开始阶段，也就是处于计划和定义阶段，有两个主要问题需要考虑：

1. Symbian 签名标准对应用软件有什么要求？
2. 如果需要的话，应用软件需要哪些能力？

5.2 测试应用

应用软件可以用 SDK 的模拟器进行测试。建议在现网中对真实设备的应用软件也进行测试—模拟器很难收到任何呼入呼叫。如果应用软件需要获得数字签名的能力，那么就首先用模拟器进行测试，其次通过 Symbian 签名得到开发者证书，以便获得用于测试设备的应用软件所需的能力。

5.2.1 Symbian 开发者证书

开发者可以利用 Symbian 开发者证书来签名他们的应用软件以获得受限的能力进行设备测试。此证书仅适用于某个给定的 IMEI 组，而且这个组不可更改。针对如何获得 Symbian 开发者证书有一些要求，表 3 中列出了这些要求。

IMEI 的数量	认证	能力
1	Symbian 签名帐户	Local Services, User Environment, Network Services, Location, Read User Data, Write User Data, SWEvent, SurroundingsDD, ProtSrv, Power Mgmt
不大于 20	VeriSign ACS Publisher ID 以及 Symbian 签名帐户	如上能力+ ReadDeviceData & Write Device Data, Trusted UI
定制	VeriSign ACS Publisher ID, Symbian 签名帐户以及制造商支持	如上能力+ DRM, Network Control, MultimediaDD, TCB, All Files, CommDD, Disk Admin

表 3: Symbian 开发者证书要求

总体上，过程如下所述：

1. 开发者登录 Symbian 签名网站并注册。
2. 开发者用一个请求工具来递交开发者证书请求。
 - 此工具可以从 Symbian 签名网址下载。

- 此阶段需要 VeriSign ACS Publisher ID。注意，VeriSign ACS Publisher ID 需要缴纳年费。
3. 生成证书并发送给开发者。
- 证书的有效期为从开发者收到证书之日起的六个月。
 - Symbian 开发者证书是免费的。但开发者可能需要 VeriSign ACS Publisher ID，而此 ID 需要缴费。

获取定制开发者证书的过程也在相同的网站进行，但使用另一个不同的链接。然而，在开发者得到开发者证书之前，其要求需要获得制造商批准。这一批准是基于这样的基本假设：如果应用软件能够获得开发者证书，那么它将同样能够获得最终认证。

5.3 Symbian 签名

为了获得最终的认证，应用软件必须通过 Symbian 签名。这一节将列出此过程中需要了解的一些要点。

对于任意一个提交给 Symbian 签名的应用软件均需要 VeriSign ACS Publisher ID。这是进行 Symbian 签名的先决条件。Symbian 签名使用的 VeriSign ACS Publisher ID 与申请开发者证书所用的 VeriSign ACS Publisher ID 是相同的。

如前所述，有些能力可以通过标准 Symbian 签名的方式得到，方法是通过相应的测试并且声明使用这些能力的原因。如果应用软件需要下面这些能力

- CommDD
- MultimediaDD
- NetworkControl
- DiskAdmin
- AllFiles

开发者在提交应用软件时必须填写能力请求表格。能力请求表格将发送至平台制造商以获得批准。

下面的要求适用于上面提到的五种能力：

- 需要上面提到的五种能力的应用软件部分必须打包至一个单独的 SIS 文件。
 - 此 SIS 文件将具有请求的能力。
 - 在应用软件发行时，开发者可以使用嵌入主应用软件 SIS 文件的此 SIS 文件。

5.4 赋予 TCB/DRM

对于TCB和DRM能力，它们的过程是不同的。为了获得这些能力，开发者必须登录 www.forum.nokia.com/testing，并要填写 *制造商核准能力请求表格*。在开发者的请求被评估之后，制造商将会就细节与开发者联系。

接受条件如下：

- 与诺基亚就可能的责任以及能力的使用达成一份法律协议。
- 对应用软件进行定义，这样此应用软件可以在诺基亚相同平台版本的所有设备上安装。参见章节 3.4——“制造商 ID 和产品 ID 的使用范例”
- 需要上面提到的能力的应用软件部分必须打包至一个单独的 SIS 文件。
 - 此 SIS 文件将具有请求的能力。
 - 在应用软件发行时，开发者可以使用嵌入主应用软件 SIS 文件的此 SIS 文件。

6. 术语及缩写

术语或缩写	含义
API	应用软件编程接口
CA	认证授权
PKI	公钥基础设施
SIS	Symbian 操作系统所用的安装文件格式
VeriSign ACS Publisher ID	VeriSign 的产品，一种身份证书。“内容认证签名 Publisher ID”。

7. 资源评估

请您花几分钟时间，通过[评估本资源](#)的方式来帮助我们提高文档质量，并且选出您觉得最具价值的资源。