

诺基亚论坛

安全入门

版本 1.0; 2005 年 10 月 28 日

NOKIA

版权©诺基亚公司 20055。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	背景	5
2	应用签名基础知识.....	5
2.1	应用签名示例.....	5
2.2	获取信任	6
2.3	应用来源	6
2.4	SIS 文件内容.....	6
2.5	Java 域.....	6
3	实际测试和签名	7
3.1	应用测试和签名	7
4	文档评价	9

修订记录

2005 年 10 月 28 日	版本 1.0	初始文档版本

1 背景

本文旨在介绍支持诺基亚设备中应用安装所使用的安全模型的理论。

2 应用签名基础知识

数字签名基于标准的公共密钥基础设施（PKI）模型。一种不涉及技术细节的 PKI 模型的定义是，它是双方之间的一种信任。

2.1 应用签名示例

例如，一把门锁可能有多个钥匙，这些钥匙可用于打开此锁。锁与打开锁的钥匙之间存在一种信任。如果使用错误的钥匙或者不用力，门将不会被打开。也可以使用一个铁撬打开锁。然而，此时使用了外力，它不是一种受信的开锁方式。在某些地方，采用这种方式开门可能会触发警报。总之，锁与正确的钥匙之间存在信任，但锁与铁撬之间不存在信任。

现在问题是，信任从何而来？在上述锁的示例中，从得到授权的锁匠那里购买一把锁是最安全的方式。在获得钥匙后，可以确保不会有复制的钥匙。您可以从当地五金商店购买一个铁撬，其他人也一样可以。因此，试图使用铁撬开门的用户无法获得信任。

数字签名的实现方式与上述相同。需要有一个信任组件（锁的钥匙），将该组件用于所需目标（锁）以获得所需结果（打开门）。如果您使用其他方法（铁撬）达到目的，则会显示警告（触发报警）。

当通过 Symbian OS 设备和支持 MIDP 2.0 的设备将此模型应用到应用安装程序时，该内容则通过安装程序（门）安装到设备上。该内容在（需要通过门的）SIS 文件（例如，本机的 Symbian 应用）或 JAD/JAR 文件对（Java™应用）中提供。然后在安装程序和应用程序包文件之间对信任进行测量。为了达到此目的，设备拥有一个被称为根证书（锁）的实体，文件中用于提供应用的信任实体是数字签名（钥匙或铁撬）。

例如，当安装程序引入 SIS 文件时，安装程序检查 SIS 文件是否已经获得数字签名（采用什么方式打开锁）。如果 SIS 文件没有签名，则使用铁撬方式。

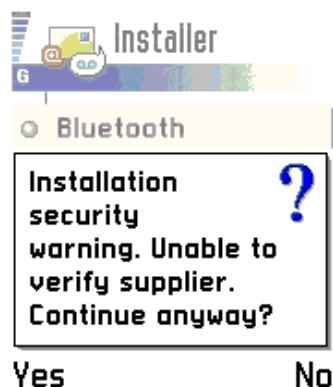


图 1：诺基亚 6600 设备向用户显示的警告消息

如果 SIS 文件已经获得数字签名，则安装程序会检查它拥有什么类型的签名。在检查签名后，它将签名与设备中应用安装所使用的所有证书相比较。如果所有证书都不信任该签名，安装程序将得到与选择铁撬方式相同的结果。对于 Symbian SIS 文件，应用能够安装，但同时会向用户显示警告信

息。然而，此时用户可以看到 SIS 文件拥有哪个签名；换言之，谁对它进行了签名。对于 Java 应用（JAD/JAR），安装程序将指示安全检查失败，无法安装应用。因此，对门来讲，铁撬还不够强大。

如果应用拥有一个受到应用安装程序所使用的其中一个证书信任的签名，则不会显示警告消息，并且能够安装应用。此时，用户可以看到对应用进行了签名的机构。

2.2 获取信任

为了使用户信任应用安装中的签名和证书，对应用进行签名的过程必须非常安全。这意味着只有某些受信机构可以对应用进行签名。发放证书和签名的机构被称为证书授权机构（CA）。

在对应用安装文件进行签名之前，需要执行一些检查。这自然取决于签名的属性，但当前模型中存在两种检查方式：

- 应用来源
- 基于某种测试标准的应用质量

2.3 应用来源

可以通过发放身份证书验证应用源。这意味着应用的提供者需要为 CA 提供某种程度的存在证明。在提供证明后，CA 可以为应用提供者发放身份证书。接着，应用提供者可以使用该身份证书对应用安装文件进行签名，以验证：

- 应用源
- 应用安装文件的完整性

签名能够保护已签署文件的完整性。如果已签署文件被更改，签名则被破坏，文件的完整性也被损坏。使用身份证书对文件进行签名无法向应用安装程序提供任何信任，因为身份证书仅用于验证提供者的身份。要想获得信任，应用需要通过测试和签名程序。

2.4 SIS 文件内容

SIS 文件可用于为 Symbian OS 设备提供不同内容。这意味着开发者可以为设备创建各种素材，并以同一种文件格式（例如 SIS 文件）向用户提供内容。这些内容可以是：

- 应用
- 主题
- 应用所使用的内容（新字典数据库、新地图、新游戏级别，等等）

这样，恶意软件开发者有机会在 SIS 文件中加入任何内容—主题也可能导致多余的功能。因此，对 SIS 文件中所有内容进行测试并检查以确保不包含任何恶意内容非常重要；它们必须通过适当的测试和签名程序。

2.5 Java 域

在 MIDP 2.0 中，存在一个专用安全模型，该模型为应用定义了四个“域”。因此如果根证书被定义到设备的“A”域中，所有为信任该证书而签名的应用都将获得该“A”域的益处。以下是 MIDP 2.0 规范的最优方法所描述的四个域：

- 非受信第三方域

应用没有获得签名，它们将在安装时给出一条警告消息，并始终在通信之前询问是否允许。

- 受信第三方域

应用在安装时不会给出警告消息，它们始终在通信前询问是否允许。所有商用应用将在此处签名。例如，可以使用公认的测试和签名程序对该域的应用进行签名。

- 运营商城

应用在安装时不会给出警告消息，它们不会在通信前询问是否允许。对使用通信选项的运营商特定的应用最理想，并且用户知道通信费用。运营商将对该域的应用进行签名。

- 制造商域

应用在安装时不会给出警告消息，它们不会在通信前询问是否允许，它们可能拥有访问特殊 API 的权限。对使用设备的一些特定功能的运营商特定的应用最理想，使用这些功能的应用数量必须有限。制造商将负责这些应用，并对该域的应用进行签名。

3 实际测试和签名

对于 Symbian 应用，已经存在一个业内公认的应用测试和签名计划。它签名的应用在业内受到信任，因此用户能够以最小风险安装应用。该计划被称为 **Symbian Signed**，并且它于 2004 年 5 月起对应用开放。如果希望支持该计划，设备需要拥有 **Symbian Signed** 所使用的根证书。由 Symbian OS 设备的制造商将根证书置于其设备中。

对于 Java 应用，业内在 2003 年夏季启动了统一测试项目 (UTI)。UTI 的目标是为 Java 应用建立一个共同的、全行业范围内的应用测试计划。它于 2004 年 2 月对应用开放。该计划被称作 **Java Verified**。如果希望支持该计划，设备需要拥有 UTI 根证书。由设备制造商将证书加入到设备中。UTI 继续支持、开发和管理 **Java Verified** 计划。

支持该计划的制造商正在引导开发者使用 **Java Verified** 和 **Symbian Signed** 对应用进行签名。因此，它们正在确保被测试应用的质量并通过保证应用源提高安全性。有关这两个计划的更多信息可以从 www.javaverified.com 和 www.symbiansigned.com 上以及下一节中找到。

3.1 应用测试和签名

诺基亚支持两种应用签名程序：

- Java Verified
- Symbian Signed

从开发者的角度来看，**Java Verified** 与 **Symbian Signed** 的引入是为了解决测试领域中的分裂。在这些计划发布之前，开发者必须使应用通过多个不同的应用测试和签名计划。这些计划彼此之间没有协作或支持。因此，应用在一个计划中测试完之后，开发者必须在另一个计划中采用几乎相同的标准对其进行全程测试。**Java Verified** 于 2004 年 2 月启用，而 **Symbian Signed** 于 2004 年 5 月面世。

Java Verified 与 **Symbian Signed** 是在许多电信行业的公司支持下建立的，分别由 Sun 和 Symbian 运作。诺基亚积极投身于 **Java Verified** 与 **Symbian Signed** 计划的创建，并且是其有力支持者。例如，用于 Preminet (www.nokia.com/preminet) 和 Nokia Software Market (www.softwaremarket.nokia.com) 的所有应用在进入渠道之前都需要通过这些计划的测试。并非只有诺基亚支持这些计划；一些运营商和制造商也对 **Java Verified** 和 **Symbian Signed** 计划提供了类似的支持。

如上所述，两个计划都将验证内容源。在编写此文档时，**Java Verified** 还不能为开发者提供此功能。此功能在 2005 年下半年将会实现。**Symbian Signed** 目前使用 VeriSign 的 ACS Publisher ID 实现此功能。

Java Verified 与 Symbian Signed 均为应用定义了测试标准。应用在被接受之前需要通过这些标准。因为应用执行环境的属性不同，所以这两个计划中的标准不同。在应用通过测试后，这两个计划都能够对这些应用进行数字签名。

可以从下列网站获得有关 Java Verified 与 Symbian Signed 的更多信息：

- www.forum.nokia.com/testing
- www.javaverified.com
- www.symbiansigned.com

4 文档评价

请您花几分钟时间，通过[评估本文档](#)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文档。