代码签名的简介

GlobalSign

目录.

章节 1.

什么是代码签名

什么是代码签名

代码签名是虚拟等效压缩包装CD为基础的软件分发。

从零售商店购买软件的客户会收到一个压缩包装的包裹，并且可以清楚地确定是谁发布了软件，以及包裹是否被篡改或打开。因此，客户可以很容易地做出是否信任软件的决定。从互联网下载软件的客户也需要类似的保证。代码签名机制提供了这种保证，并在通过internet分发软件时充当“虚拟收缩包装”的作用。

代码签名是对分布在Internet上的软件/应用程序进行数字签名的过程。签名代码为客户提供了与商店购买的压缩包装软件相同的安全性，因为一旦代码被签名，它就包含了发布者的名称，并防止恶意软件注入和其他破坏。

代码签名证明“签名”软件是:

- 合法的
- 来自一个已知的软件供应商
- 代码自发布以来没有被篡改过

代码签名防止:

- 用户放弃安装应用程序
- 恶意更改合法代码
- 供应商或代码作者的身份盗窃

章节 2.

代码签名证书 101

什么是代码签名证书?

代码签名证书的定义

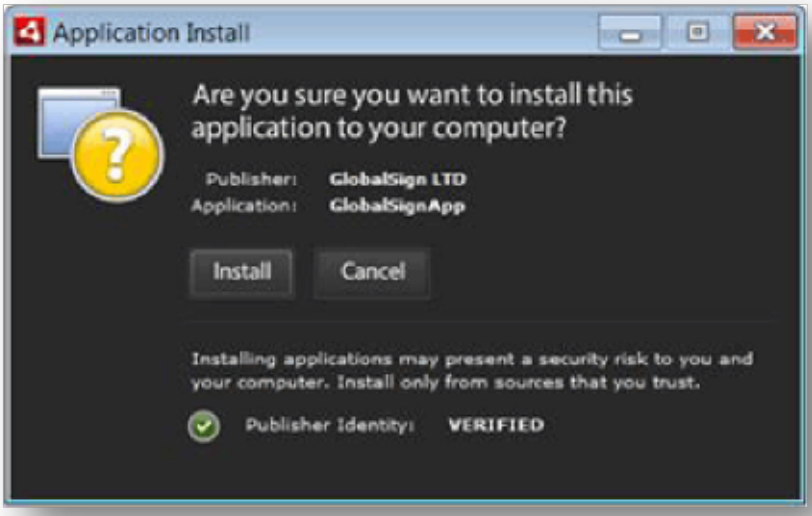
代码签名证书是一种数字证书，包含完全识别实体的信息，由证书颁发机构(如GlobalSign)颁发。

代码签名证书允许开发人员通过使用数字签名来包含关于自己和代码的信息。为了创建数字签名(代码签名的行为)，开发人员使用数字证书。

数字证书将一个组织的身份绑定到一个公钥上，该公钥在数学上与对应的私钥对相关。私钥用于对通过散列算法运行的代码的缩短版本应用数字签名，而公钥用于验证签名。对代码的哈希值进行签名提供了一个方法，用于验证代码自签名以来是否以任何方式发生了更改。即使改变一行代码中的一个字符，也会改变哈希值，从而被检测到可疑。

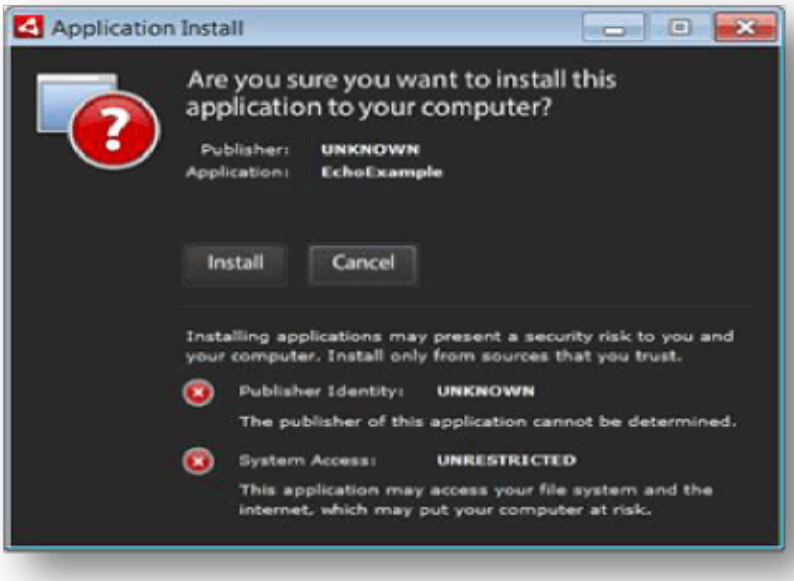
实际签发证书的代码

使用代码签名证书签署的应用程序



数字签名应用程序在安装界面上突出显示发行商的名称，确认应用是可验证的，并且来源可信。

未使用代码签名证书签名的应用程序



未签名的应用程序会向最终用户显示令人担忧的安全警报，警告他们应用程序的发布者未知，并建议他们只从他们信任的源安装应用程序。

代码签名有助于证明:

内容来源

代码签名标识软件或应用程序来自特定的来源(开发人员或签名者)。当从互联网下载软件时，浏览器将显示一个警告消息，说明下载数据可能存在的危险，或显示一个“未知的发布者”警告。代码签名将删除“未知发布者”安全警告并标识发布者的名称(即。组织名称)。

内容完整性

代码签名确保一段代码没有被修改，并确定代码用于特定目的是否可信。如果数字签名后的应用程序/软件代码被篡改或篡改，则签名将显得无效和不可信。

签名代码有利于用户下载应用程序，也有利于开发人员。用户可以确定他们从谁那里下载软件，并可以决定是否信任来源。开发人员可以标记他们的“品牌”，并保护他们的软件免受不必要的更改。

章节 3.

为什么以及何时对代码进行数字签名

为什么以及何时应该对代码进行数字签名

运行无符号代码可能很危险!

不像商店购买的软件，篡改明显的包装不存在的在线软件;交易背后没有可信的可见供应商，也没有明显的方法来确定软件的来源。

未签名的软件可能会被篡改，例如插入间谍软件或恶意软件，因此建议最终用户不要运行未签名的代码。因此，下载或运行未签名的应用程序将产生令人担忧的“未知发布者”安全警告。

软件分发使开发人员能够在桌面上交付品牌丰富的互联网应用程序，从而与客户建立更紧密的联系。这提高了web应用程序的生产力和功能，从而扩大了web服务器的覆盖范围，并增强了客户体验。

平台提供商鼓励代码签名

各种平台都支持代码签名，允许对不同类型的代码进行签名。

Microsoft Authenticode

签署 .exe, .cab, .dll, .ocx, .msi, xpi, .xap,控件和内核软件

Adobe Air

签署 .air 和 .airi 文件

Apple

为Mac OS桌面签署软件、应用程序、插件和内容

Mozilla & Netscape

为Firefox的Mozilla XPI包和Netscape对象的文件签名

Macros and Visual Basic Applications

在Microsoft Office中对VBA对象、脚本和宏进行签名

Java

为.jar文件和Java应用程序签名

章节 4.

自签名VS.公开可信签名

自签名VS.公开可信签名

有两种基本类型的代码签名证书可用于为应用程序签名:

- *自签名代码签名证书*
- *公开可信代码签名证书*

自签名代码签名证书

自签名代码签名证书本质上是不可信的凭据，依赖方无法立即验证发布者的真实性

使用自签名证书的注意事项:

- 代码的接收者没有明显的方法知道身份是否真实
- 签名将显示一个信任警告，指示发布者未经过验证，并显示“未知发布者”
- 自签名证书是不能被吊销的，所以如果证书被泄露，就会对你的软件的用户造成伤害

自签名代码签名证书通常最适合为测试代码签名。

.

自签名VS.公开可信签名

公开可信代码签名证书

公开可信代码签名证书是由公开可信证书颁发机构(public trusted Certificate Authority, CA)颁发的证书。

公开的根代码签名证书，比如GlobalSign的根代码签名证书，不仅提供了一种保证软件内容完整性的机制，而且还提供了一种立即验证软件来源的方法。作为一个网络可信的认证机构，GlobalSign对出版商和出版商组织都进行了“审查”。

使用公开可信的代码签名证书的好处:

使用由公共可信CA颁发的代码签名证书对代码进行数字签名有很多好处，包括:

- 当收件人下载已签名的应用程序时，显示发布者名称
- 如果证书有问题，证书可以被吊销
- 代码使用时间戳进行数字签名

时间戳

理解时间戳的好处很重要，因为它扩展了代码的信任。当应用数字签名时，也会记录一个时间戳。这个时间戳特性的作用是确保签名代码即使在数字证书过期后仍然有效。除非你向应用程序中添加了额外的代码，否则即使最初为代码签名的证书过期了，也不需要应用新的签名。

章节 5.

买家注意事项

买家注意事项

如果你决定从公开可信的证书颁发机构购买代码签名证书，那么你可能有多个CA可供选择。在选择代码签名提供程序时，你应该考虑以下方面:

普遍性

为了让应用程序的接收者信任应用于代码的签名，CA需要有一个全局的根嵌入程序，以确保所有应用程序都得到支持。

时间戳服务

为了确保签名在数字证书过期后不会失效，可以考虑选择提供免费时间戳服务的认证机构。

价格和价值

与价格相比，你获得的体验、支持和功能是否物有所值

技术支持

是否与核心业务涉及数字证书的供应商合作

签名量限制

使用数码身份证申请签署的次数是否有限制

可信度

什么类型的第三方独立审计，如WebTrust，验证证书机构的操作完全符合他们发布的证书实践声明

易用性

申请证书是否容易;安装有多容易

建立信任，并向用户展示您的代码来自可信的开发人员

GlobalSign代码签名证书是多用途的，这意味着你可以使用一个证书对多个平台进行数字签名。一张证书可以用于数字签名:

- Microsoft Authenticode文件(32位和64位)，包括内核软件
- Adobe Air应用程序
- Apple桌面应用程序
- Java应用程序Macros
- Microsoft Office 和 Visual Basic
- Firefox的Mozilla XPI包

其他独特的GlobalSign代码签名功能f:

- 对无限数量的应用程序进行数字签名
- 时间戳服务使数字签名不会过期
- 免费的代码签名工具可简化签名过程

“与其他证书提供商的显著区别在于，我们可以使用相同的证书对用户代码和内核空间代码进行签名。

GlobalSign提供的代码签名工具让事情变得非常简单，但每当需要帮助时，我们都会发现GlobalSign的人就在我们身边，每一步都非常直接和个人的沟通。”

Nikos Mouratidis, Qualtek.

今天就购买代码签名证书!

www.globalsign.cn/code-signing

GlobalSign