

代码签名证书 最佳实践



腾讯云

【 版权声明 】

© 2013–2023 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分內容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

最佳实践

数字签名工具使用指南

最佳实践

数字签名工具使用指南

最近更新时间：2023-09-18 16:38:02

操作场景

本文档将指导您在申请并购买代码数字签名证书成功之后，如何使用腾讯云提供的 **数字签名工具** 为您的应用进行签名。

前提条件

已拥有代码数字签名证书。

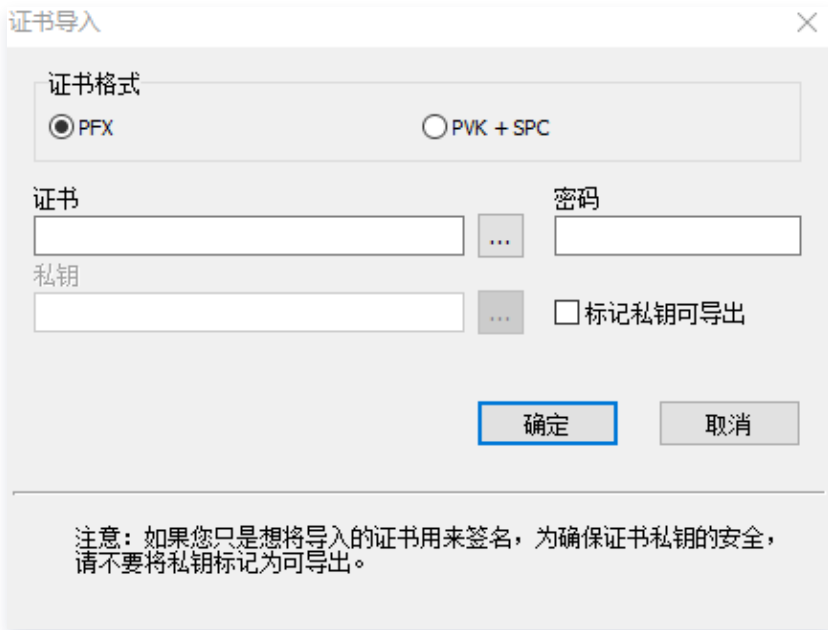
操作指南

步骤1：导入证书

1. 请 [单击此处](#) 下载并安装数字签名工具。
2. 打开数字签名工具专业版，并单击**证书管理 > 导入**。如下图所示：



3. 在弹出的**证书导入**窗口中，选择您的证书文件。如下图所示：



The image shows a 'Certificate Import' dialog box with the following elements:

- 证书格式 (Certificate Format):** Two radio buttons: PFX and PVK + SPC.
- 证书 (Certificate):** A text input field with a browse button (...).
- 密码 (Password):** A text input field.
- 私钥 (Private Key):** A text input field with a browse button (...).
- 标记私钥可导出 (Mark private key as exportable):** A checkbox.
- Buttons:** '确定' (OK) and '取消' (Cancel).
- Note:** A note at the bottom states: '注意：如果您只是想将导入的证书用来签名，为确保证书私钥的安全，请不要将私钥标记为可导出。' (Note: If you only want to use the imported certificate for signing, to ensure the security of the certificate private key, please do not mark the private key as exportable.)

- **证书格式：**选择导入的数字证书格式，若您是在腾讯云申请的代码数字签名证书，可选择 PFX。
- **证书：**选择导入该证书的路径。
- **私钥：**选择导入该证书私钥文件路径。

① 说明

证书格式为 PFX 时，私钥选项不可用。

- **密码：**该证书的有效密码。
- **标记私钥可导出：**可勾选。

⚠ 注意

若您导入的证书不需要再导出备份，请勿勾选标记私钥可导出。

4. 导入成功后，即可在证书管理列表中查看和管理导入的证书。如下图所示：



步骤2：添加签名规则

1. 单击**签名规则 > 添加**，添加签名规则。如下图所示：



2. 在弹出的添加规则窗口中，填写相关规则信息。如下图所示：



○ 签名选项

- 规则名：请填写规则名，用来区分不同规则。
- 证书：请选择数字签名证书。如若没有安装证书，请先 [导入证书](#)。

- **SHA2 证书**: 请选择 `Tencent Test Code Sign`。
- **文件扩展名**: 默认即可。
- **包含子目录**: 请勾选, 批量签名时允许遍历子目录。
- **跳过有效签名文件**: 请勾选, 签名时跳过已经包含有效签名的文件, 避免了其他有效签名被覆盖。
- **签名信息 (可选)**
 - **内容描述**: 主要用于 ActiveX 签名。
 - **信息 URL**: 主要用于 ActiveX 签名。
 - **时间戳服务**: 确保证书过期后, 签名不过期。TrustAsia 为 VeriSign 在国内的代理服务器, 速度可能会快一些。

3. 单击**确定**, 进入“步骤3 模式选择”操作。

步骤3: 模式选择

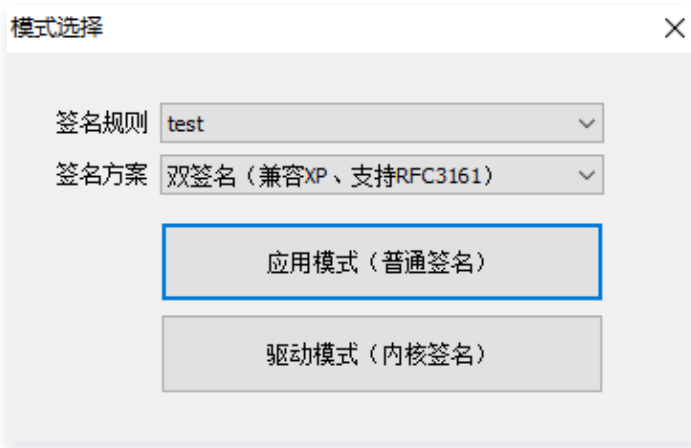
⚠ 注意

- 请确保已添加**签名规则**, 添加后才可进行**数字签名**、**签名验证**等操作。
- 若已存在签名规则, 默认情况下会自动选中第一条规则, 以方便进行数字签名操作。

1. 单击**数字签名 > 数字签名**。如下图所示:



2. 在弹出的**模式选择**窗口中, 选择相关内容。如下图所示:



- **签名规则**：选择您已有的签名规则。
- **签名方案**：为了兼容新旧系统，推荐使用“双签名”方案。
 - **双签名**：使用 SHA1 与 MS Authenticode 时间戳和 SHA256 与 RFC3161 时间戳同时进行签名，前者兼容 XP 等老系统，后者支持新系统并消除安全警告。
 - **SHA256 追加签名**：不覆盖第一个签名并进行追加签名，使用 SHA256 + RFC3161 时间戳。
 - **SHA1/SH256 单签名**：会覆盖第一个签名。
 - **时间戳**：单独进行时间戳补签，支持给双签名分别采用不同的时间戳进行补签，解决漏签时间戳的情况。
- **模式选择**：请根据文件类型选择相应模式。
 - **应用模式**：一般用于应用程序、ActiveX 控件等非驱动程序的签名和验证。
 - **驱动模式**：用于对驱动的签名和验证，会自动加入微软的交叉证书。

3. 模式选择后可进入“步骤4 数字签名”操作，

步骤4：数字签名

1. 单击数字签名 > 添加文件，选择需要添加签名的文件或直接拖入文件至列表。
2. 选择相应签名方案和模式，单击签名验证，即可开始签名。如下图所示：

