芯语创作客户端 3.0 • 签名与发布

代码签名证书
申请与替换指南

从自签名开发证书，到正式 CA 签名与 SmartScreen 信誉

当前状态	目标状态	适用	更新
自签名开发证书 已附加签名	CA 签发 OV/EV 带时间戳	Windows x64 .exe 安装包与主程序	2026-10 · v1.0

先说结论：受 Windows 公共信任的代码签名证书不能由开发者自行生成。自签名证书只能在本机或自管设备上通过手动信任来使用，不能替代 CA 证书。正式对外分发必须向受信任的证书颁发机构（CA）申请，并完成组织身份审核。

一、当前安装包的签名状态

项目	当前值
签名类型	自签名开发证书（Authenticode）
证书主题	`CN=Xinyu Studio Dev Code Signing, O=Xinyu Studio, C=CN`
证书指纹	`731F5A8E9F4720022E9A34888F37CA50CE445C60`
有效期	至 2028-10-28
时间戳	未添加。证书到期后，签名有效性会受影响。
公共信任	否。其他电脑默认不信任该证书；本机可通过信任脚本导入。
适用场景	本机演示、校内试讲、功能验收，不可作为正式对外发行版本。

二、正式代码签名证书有哪几种

类型	审核强度	适用场景	注意事项
OV Code Signing	验证企业/组织真实存在、申请人身份与联系方式	常规桌面软件、校内/企业分发、官网下载	价格相对低；SmartScreen 信誉需逐步积累。
EV Code Signing	更严格的组织与申请人核验，通常要求硬件令牌或云签名	面向公众的商业软件、需要更快建立信任	价格更高；仍需时间戳；并不等于立即没有 SmartScreen 提示。

类型	审核强度	适用场景	注意事项
云签名 / HSM 服务	CA 或云平台托管私钥，按签名次数/订阅计费	团队协作、无法保管 USB Token、CI 自动构建	需要接入 CA 的签名工具或 API；适合持续发布。
自签名证书	无第三方审核	本机开发、内网测试、教学演示	不能替代 CA 证书；只能在受控设备手动信任。

本产品是 Windows 桌面 .exe，应选择支持 Microsoft Authenticode 的代码签名证书；不要购买“SSL 证书”或“邮件签名证书”代替。

三、从哪里申请

可选择国内或国际 CA，以下仅列出常见机构，不构成推荐或背书；价格、审核周期与产品形态以 CA 当期报价为准。

地区	常见机构	常见交付形式
国内	天威诚信、沃通（WoSign）、上海 CA、数安时代（GDCA）等	USB Token、云签名、部分场景提供 PFX（以 CA 政策为准）
国际	DigiCert、Sectigo、GlobalSign、SSL.com 等	USB Token、HSM、云签名（KeyLocker / eSigner 等）

> **行业变化：**自 2023 年起，CA/Browser Forum 对代码签名私钥保护提出更高要求，许多 CA 不再直接交付可导出的 PFX，而是发放 USB Token 或云签名服务。申请前务必确认“私钥如何交付、是否支持 signtool、是否支持时间戳”。

四、申请流程（以组织证书为例）

1. **确定主体：**用学校、公司或工作室的合法主体申请。个人开发者证书审核范围有限，正式教育产品建议用组织主体。
2. **选择类型：**常规分发选 OV；面向公众、需要更强信任选 EV；团队/CI 发布选云签名。
3. **提交资料：**营业执照或事业单位法人证书、组织机构信息、申请人身份证明、联系电话、邮箱、办公地址；部分 CA 会电话回访或要求域名/邮箱验证。
4. **签订合同与付款：**确认证书年限、签名次数、是否含时间戳、是否支持 Windows Authenticode、发票类型。
5. **完成审核：**CA 进行组织与申请人核验；周期通常为数个工作日，EV 可能更长。
6. **接收私钥载体：**USB Token 需要安装驱动；云签名需要开通账号与签名权限；若 CA 提供 PFX，必须用强密码保护并限制存放位置。
7. **签名与时间戳：**使用 signtool 或 CA 工具签名，并添加 RFC 3161 时间戳，保证证书到期后已发布版本仍可验证。
8. **验证与归档：**在干净 Windows 机器上验证签名链；归档证书、合同、签名记录与安装包哈希。

五、替换当前开发证书的三种方式

方式 A：CA 提供 PFX 文件

这是最直接的替换方式。把 PFX 放到受控目录（不要放在桌面交付包），通过环境变量提供密码，重新构建：

```
$env:CSC_LINK = 'D:\secure\your-code-signing.pfx'
$env:CSC_KEY_PASSWORD = '<从密码管理器读取，不要写进脚本>'
cd D:\芯语教育IDE_产品级演示\desktop
npm run dist
```

electron-builder 会自动签名主程序、安装包、便携版与卸载器。构建完成后用下面的“验证命令”检查。不要在聊天、邮件或 Git 中发送 PFX 与密码。

> **本机已提供自动化脚本：** `D:\芯语教育IDE_产品级演示\desktop\sign-ca.ps1`。在该目录运行后，按提示输入 PFX 路径与密码，脚本会重新构建并输出签名验证结果；密码只保存在当前进程环境变量中，脚本结束即清除。

方式 B：USB Token（硬件令牌）

1. 安装 CA 提供的令牌驱动与中间证书。
2. 插入令牌，在“证书管理器 → 个人”中确认证书存在且有私钥。
3. 用 signtool 指定指纹签名；或为 electron-builder 配置自定义签名钩子，在打包每个 .exe 时调用 signtool。
4. 签名时必须输入令牌 PIN；建议使用支持时间戳的签名命令。

```
signtool sign /sha1 <证书指纹> /fd SHA256 /tr http://timestamp.digicert.com /td SHA256 "芯语创作客户端.exe"
```

方式 C：云签名 / HSM

使用 CA 提供的云签名客户端或 API（如 KeyLocker、eSigner、Azure Trusted Signing 等）。云签名通常不导出私钥，适合团队和 CI。需要把 electron-builder 的签名步骤替换为 CA 工具或自定义签名钩子，并在构建日志中保留签名请求 ID。

六、签名验证命令

```
# 查看签名主体、指纹与状态
Get-AuthenticodeSignature "D:\...\Xinyu-Client-Setup-3.0.0-x64.exe" |
  Select-Object Status, StatusMessage, @{n='Subject';e={$_.SignerCertificate.Subject}}

# 严格验证签名链（需要 Windows SDK 的 signtool）
signtool verify /pa /v "D:\...\Xinyu-Client-Setup-3.0.0-x64.exe"
```

正式证书签名后，状态应为 `Valid`，签名者应显示学校/公司名称；若仍显示 `UnknownError`，检查根证书、中间证书、时间戳和系统时间。

七、SmartScreen 与信誉

- 代码签名只解决“文件是否被篡改、发布者是谁”，不自动等于“SmartScreen 不再提示”。
- 新证书需要积累下载与使用信誉；EV 证书通常有助于更快建立信任，但不是即时消除提示的保证。
- 正式发布应使用同一主体、稳定文件名与版本号，避免频繁更换证书或安装包哈希。
- 向用户提供 SHA256 校验值与官方下载渠道，减少“未知来源”风险。

八、教育场景的采购与合规建议

事项	建议
采购主体	以学校、教育机构或公司名义申请；保留合同、发票与付款记录。
软件著作权	正式发行前建议办理软件著作权登记，便于学校采购、竞赛提交与维权。
教育应用备案	若面向中小学或公众提供教育服务，按当地要求完成教育移动应用备案、安全评估与内容审核；代码签名不能替代备案。
数据与隐私	保持“最小化采集、本机保存、密钥加密、AI 输出可审核”的设计；不要把学生个人信息写入提示词。
合同与 SLA	与 CA 确认签名次数、重签政策、证书吊销、时间戳服务与技术支持。

九、替换后的交付清单

1. 用正式证书重新构建，主程序、安装包、便携版、卸载器均已签名。
2. 签名已添加 RFC 3161 时间戳；在干净 Windows 机器验证通过。
3. 替换桌面交付包中的安装包，删除开发证书与信任脚本。
4. 重新生成并核对 SHA256.txt，更新版本号与发行说明。
5. 确认未泄露 PFX、Token PIN、云签名凭据；必要时吊销旧证书。

十、安全底线

- 不要把 PFX、Token PIN、云签名密码发到聊天、邮件、Git 或截图里。
- 不要在多台不受控电脑上复制私钥；优先使用 USB Token 或云签名。
- 为签名私钥设置独立保管人；离职或交接时立即吊销并重发。
- 保留每个发布版本的签名记录、哈希与验证截图，便于审计与回溯。

> **本指南不构成法律或采购意见。**证书类型、价格、审核材料与教育备案要求以 CA、学校和主管部门的最新规定为准。