QIANLUE　仟略技术

# 安全私钥授权终端

产品规格书

**型号：QL-EIA100**

气隙隔离　|　私钥永不出机　|　所见即所签

江苏仟略信息技术有限公司

网址：www.qianlue.cn

文档版本：V1.0

# 1 产品概述

QL-EIA100 安全私钥授权终端是仟略技术面向高安全等级业务场景推出的一款便携式、气隙隔离型硬件签名授权设备。设备以独立安全芯片为信任根，在终端内部完成私钥生成、存储与签名运算，私钥永不出机；与业务系统之间通过二维码扫码方式完成待签数据的接收与签名结果回传，不建立任何有线或无线网络连接，从物理链路层面杜绝私钥通道泄露与重放攻击风险。

产品定位为"所见即所签"的离线授权介质，适用于运维登录、配置变更、高危操作双签、现场离线维护以及审计留痕等对身份可信、操作可追溯有严格要求的场景，为每一次授权提供设备级可信根支撑。

# 2 功能特性

## 2.1 硬件身份载体

设备内置独立安全芯片，首次上电后在芯片内部生成专属非对称私钥，私钥生成过程不出芯片硬件边界；对应的公钥以二维码形式在设备本地展示，业务系统或应用通过扫码完成设备公钥的绑定与注册，建立端到端的设备级信任根。

## 2.2 私钥本地签名

所有签名运算均在安全芯片内部完成，私钥不以任何明文、密文或导出口径形式离开设备；业务系统与设备之间不存在任何数据通道，从架构上杜绝因通信链路被窃听、中间人攻击或主机被攻破而导致的私钥泄露风险。

## 2.3 离线扫码授权

设备无 USB 数据口、无网络口、无蓝牙/NFC 等无线通信能力，授权交互完全通过二维码完成：业务应用在界面上出示待签二维码，用户在 QL-EIA100 终端屏幕上核对待签内容后，通过设备物理按键人工确认；设备签名完成后在屏幕上生成签名结果二维码，业务应用扫码回传验签，形成完整的"所见即所签"人工确认闭环。

### 2.4 卡片便携设计

整机采用铝合金竖卡形态，尺寸约 65 × 92 × 8 mm，重量约 60 g；可桌面立式摆放、手持操作或配合挂绳随身携带。设备仅配备 USB-C 充电口，该接口仅用于充电，不承载任何数据通信，从接口层面进一步保证气隙隔离边界。

## 3 核心优势

| 优势项 | 说明 |
| --- | --- |
| **设备级可信根** | 安全芯片内生成并托管私钥，作为设备身份的硬件信任锚。 |
| **私钥不出机** | 私钥生成、存储、签名全流程封闭在芯片内，不导出、不传输。 |
| **双向身份认证** | 业务侧通过扫码绑定公钥识别设备，设备侧通过屏幕展示待签内容确认业务。 |
| **操作授权确认** | 每一次签名均需用户在设备上肉眼核对、物理按键确认，杜绝远程代签。 |
| **审计追溯支撑** | 签名过程可与业务侧审计日志关联，形成不可抵赖的授权留痕。 |
| **易集成易部署** | 业务侧仅需嵌入二维码扫描与生成组件，无需驱动、无需专线。 |
| **气隙隔离交互** | 无任何数据通信接口，物理隔离主机与网络攻击面。 |
| **国密算法防重放** | 支持国密密码算法体系，内置挑战-响应机制抵御重放攻击。 |

表 1 QL-EIA100 核心优势一览

## 4 技术规格

下表给出 QL-EIA100 的主要技术参数。标注"以出厂版本为准"的项目，最终规格以实际发货批次的出厂检验报告为准。

### 4.1 硬件与物理规格

| 项目 | 规格参数 |
| --- | --- |
| **产品型号** | QL-EIA100 |
| **产品形态** | 铝合金竖卡式手持终端 |

| | |
|---|---|
| **外形尺寸** | 约 65 × 92 × 8 mm（宽 × 高 × 厚） |
| **整机重量** | 约 60 g |
| **壳体材质** | 铝合金 |
| **显示屏幕** | 彩色显示屏，用于展示待签内容与签名结果二维码 |
| **按键** | 物理确认按键（人工授权确认） |
| **充电接口** | USB-C（仅充电，无数据通信能力） |
| **安装方式** | 桌面立式 / 手持 / 挂绳携带 |

表 2　硬件与物理规格

## 4.2　安全与密码规格

| 项目 | 规格参数 |
|---|---|
| **安全芯片** | 内置独立安全芯片，私钥不出芯片硬件边界 |
| **私钥生成** | 芯片内部首次上电生成专属非对称私钥 |
| **私钥存储** | 安全芯片内加密存储，不可导出、不可备份导出 |
| **签名运算** | 全部在安全芯片内部完成 |
| **密码算法** | 支持国密算法体系（具体算法套件以出厂版本为准） |
| **抗重放机制** | 挑战-响应 / 时间因子机制，防止签名内容被重放 |
| **通信隔离** | 无 USB 数据口、无网络口、无蓝牙/NFC 等无线数据通道 |
| **业务交互** | 二维码扫码：待签内容二维码录入 + 签名结果二维码回传 |

表 3　安全与密码规格

## 4.3　电气与环境规格

| 项目 | 规格参数 |
|---|---|
| **供电方式** | 内置可充电电池，USB-C 充电 |
| **数据接口** | 无（气隙隔离，仅保留充电口） |
| **工作温度** | 以出厂规格书为准 |
| **存储温度** | 以出厂规格书为准 |
| **相对湿度** | 以出厂规格书为准 |
| **防护等级** | 以出厂规格书为准 |

表 4　电气与环境规格

# 5　典型授权流程

QL-EIA100 与业务系统之间的一次完整离线授权流程如下：

（1）设备绑定：业务系统通过扫描设备公钥二维码，完成设备公钥登记与绑定。

（2）待签出示：业务应用在需要授权的界面上出示待签数据二维码。

（3）内容核对：用户使用 QL-EIA100 扫描该二维码，设备屏幕展示待签业务摘要。

（4）人工确认：用户核对屏幕上的待签内容无误后，按下设备物理确认键。

（5）本地签名：安全芯片在机内完成签名运算，私钥不出机。

（6）结果回传：设备屏幕生成签名结果二维码，业务应用扫码获取签名值并验签。

（7）审计留痕：授权记录与业务操作日志关联归档，形成可追溯的审计证据。

# 6 典型应用场景

| 应用场景 | 用途说明 |
| --- | --- |
| **应用登录认证** | 作为高权限账号的第二硬件因子，替代软 Token 与短信验证码。 |
| **网管 / 运维登录** | 网络设备、网管平台与运维跳板机的强身份认证介质。 |
| **配置变更签名** | 关键网络与安全设备配置下发前，由责任人在设备上签名确认。 |
| **高危操作双签** | 删除、关停、批量下发等高危操作的双人或多人授权签名。 |
| **现场离线维护** | 无网络条件下的现场设备维护，通过二维码完成授权凭据交互。 |
| **审计归档留痕** | 所有授权行为与业务日志关联归档，满足等保与行业审计要求。 |

表 5 典型应用场景

# 7　产品外观




图 1　QL-EIA100 安全私钥授权终端产品外观

# 8　订货信息与联系方式

| 项目 | 内容 |
| --- | --- |
| **产品名称** | 安全私钥授权终端 |
| **产品型号** | QL-EIA100 |
| **标配附件** | 主机 ×1、USB-C 充电线 ×1（具体以装箱清单为准） |
| **厂商** | 南京仟略技术有限公司 |
| **官方网站** | www.qianlue.cn |

表 6　订货与联系信息

**安全连接，每一次授权都可信。**