创芯工坊 Safety License Shield

(PowerLink 用户自定义授权安全盾)

(开发规范/用户手册)

版本: V1.0

创芯工坊硬件平台技术部

目录

一:注意事项

1:文档使用约定

此文本为公开文档,powerlink 用户可以根据此文档编写自定义离线授权工具.配合 powerlink 完成烧录的离线授权.

创芯工坊平台一直重视产品安全性和用户的知识产权,作为一个平台服务提供商,旗下的 web 云以及相关硬件产品.生产解决方案.均不会收集用户项目的敏感数据.我们一直在努力提供完整的.安全的行业解决方案.

2:唯一性

为了开发和管理烧录器,配套的软硬件产品都应该遵守此协议.(包括第三方用户,自定义开发加密算法).以确保烧录器产品的正常工作.以及维护.

3:约定

3.1：数据传输格式均采用小端模式

3.2: 本文档的默认左侧为低地址.LSB.右侧为高地址 MSB

例如:0x01,0x02,0x03,0x04,0x05 表示:0x01 是低地址.0x05 是高地址

二：更新历史

版本	修订日期	修订人	修订内容
V1.0	2019-11-22	csh@icworkshop.com	初版定义

三:基本描述

1:通讯协议

基于 TTL/UART 协议,默认协议参数如下:
波特率:115200
校验位:无
数据位: 8bit
停止位: 1bit

2:协议格式

帧头(6)	Rand-factor(2)	命令(2)	数据长度(4)	有效长度(4)	Payload(x)	CRC32(4)	帧尾(6)

2.1 帧头:

6 个字节: 固定为 “SLSTA:” (无 ‘\0’)

2.2 Rand-factor:

2 个字节: 通讯中由命令发送方产生的随机数,同一个数据加密会有不同的结果

1: 协议采用对称加密,强度足够,采用穷举法枚举密钥的可能性几乎不可能
2: 证书生成可用非对称算法签名,用户自行调整证书生成流程,或者自定义签名算法,确保授权工具和产品中一致即可,如果对称密码(16byte 密码 + 16byte IV = 256bit 被暴力破解),而真正的 License 由用户自主设计,可采用 ECC 等非对称算法,SHA256/BASE64 加密,一机一密,无法复制,无法伪造(无法确定签名算法流程))

2.3 命令:

2 个字节: 请参考命令列表

2.4 数据长度：

4 个字节: Payload 的数据长度

2.5 有效长度：

4 个字节: PayLoad 的有效数据长度

(PayLoad 对其到 16 字节,协议用 AES128(CBC 模式,包括 IV 密码长度累积 256bit) 加密< 帧头帧尾不加密,用于协议同步>)

2.6 Payload(x)

可变长度: 不同协议有不同的数据格式.请参考命令 Payload 说明

(PayLoad 对其到 16 字节)

2.7 CRC32：

4 个字节: 包含以下区段的 CRC32(加密前的 CRC32)

Rand-factor(2)	命令(2)	数据长度(4)	有效长度(4)	Payload(x)

2.8 帧尾：

6 个字节: 固定为 ":SLEND" (无 '\0')

四:通讯数据的加密

4.1 AES128 (CBC 模式)

采用 AES128 (CBC)模式,Key + IV 累计 256bit 长度,AES128 只用于协议加密.
授权算法由用户自主设计,所有权掌握在用户手上侧.

4.2 加密的部分

除帧头帧尾之后全部加密.PayLoad 部分需要对其到 16 字节,不足的部分补齐 16 字节.填充数据无特殊要求

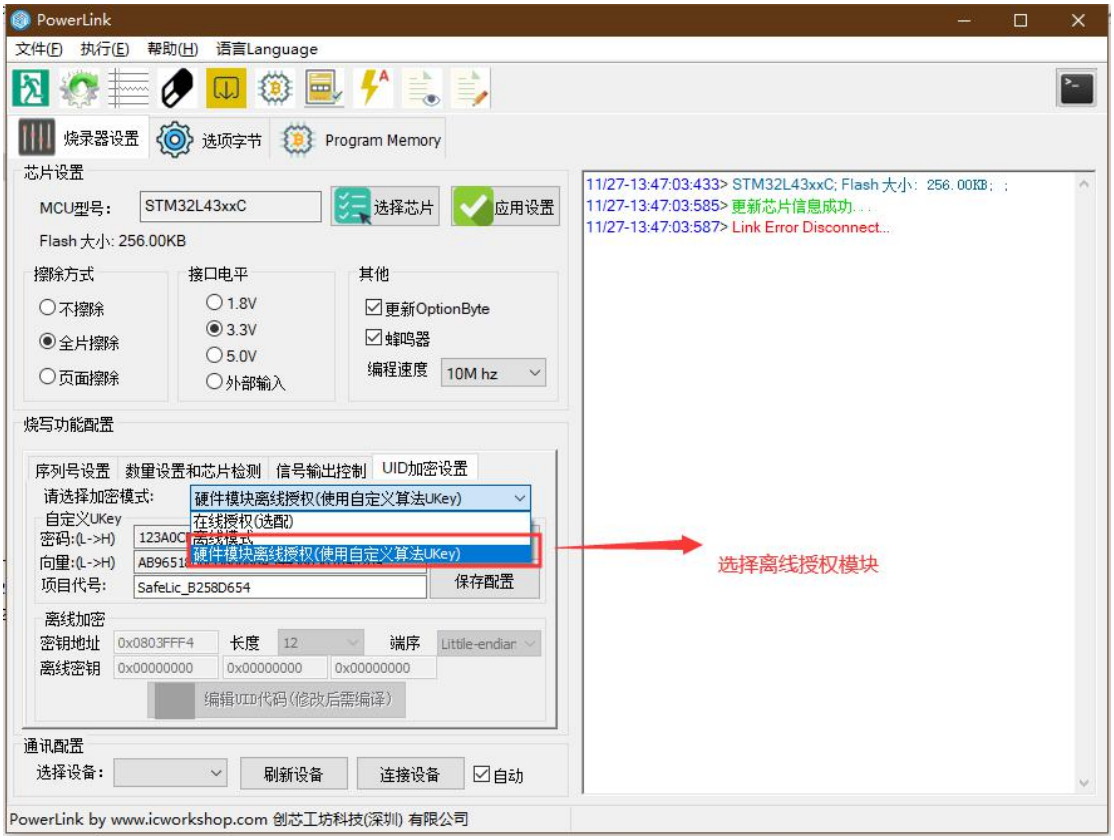
注意:
1: Safety License Shided 的默认通讯密码为 “0123456789ABCDEF”,IV:”FEDCBA9876543210”),使用之前请用配置配套的配置工具对授权工具进行配置.否则授权工具的授权功能是禁用的.返回 cmdErrorDefaultPassword 错误 (其他查询功能根据是否开启可以使用)

2: 授权工具使用了内部计时模块 (内部 RTC 时钟), 如果连续连续遇到 3 次以上通讯密码错误.(Package 解包错误),则下一次通讯时间会延长 5 分钟. 内部自动存储 Delay 标记.如果此过程被断电.再次上电会查询此标记是否存在.如果存在会继续等待 5 分钟才能使用.

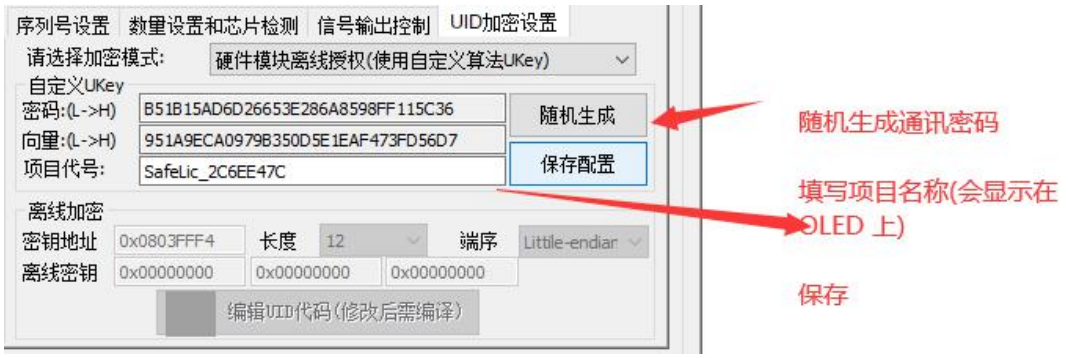
此举措的目的是防止暴力破解加密协议.等待的过程中会返回发送请求会返回 cmdErrorBusy

4.2 PowerLink 和 Safety License Shided 使用流程

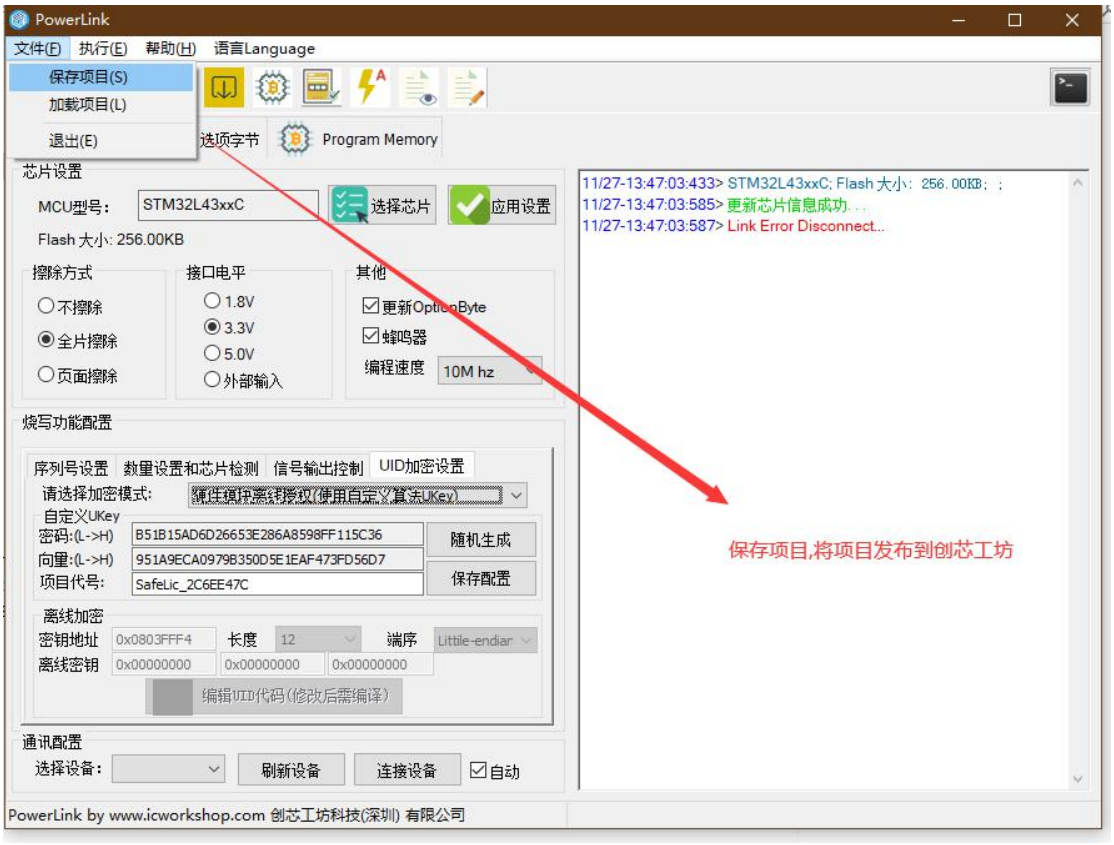
1: 选择 UKey 自定义授权



2: 随机生成通讯协议的 加密密码(AES128 CBC)和 IV, 填写项目代号



3：设置完成之后,包括其他设置,然后保存项目并加载到 PowerLink 烧录器



4：将授权模块 连接到 PowerLink 和 电源上.
生产时,PowerLink 会自动从 UKey 上获取授权信息.
连接图如下：

五：命令概览

5.1 命令概览

PL: 如无特别说明,PowerLink 简称为 PL
PC：如无特殊说明,PC 代表 PC 端 Safe License Shied 配置软件
Device: 如无特别说明,Safe License Shied 称为 Device

Chip: 代指目标芯片

命令	命令代号	取值	方向	触发条件
查找授权工具	cmdDeviceFind	0x0001	PL(C)->Device	首次查找时返回
返回 Device 信息	cmdDeviceInfo	0x0002	Device-> PL(C)	cmdDeviceFind 返回
配对到 Device	cmdDevicePair	0x0003	PL(C)->Device	如果设备在线.PL 会请求配对
配对到 Device 响应	cmdDevicePairResp	0x0004	Device-> PL(C)	配对成功返回
取消配对 Device	cmdDeviceUnPair	0x0005	PL(C)->Device	取消配对
配置 Device 信息(厂家)	cmdDeviceConfig	0x0006	PC->Device	厂家对授权工具重新配置(慎用)
升级 Device 固件(厂家)	cmdDeviceFwStart	0x0007	PC->Device	厂家对授权工具升级固件(慎用)
发送 Device 固件包(厂家)	cmdDeviceFwPkgSend	0x0008	PC->Device	厂家对授权工具发送固件(慎用)
完成 Device 升级(厂家)	cmdDeviceFwPkgEnd	0x0009	PC->Device	厂家对授权工具完成升级(慎用)
写入 Device 附加数据 (厂家)	cmdDeviceExtDatSet	0x000A	PC->Device	厂家对授权工具 写入附加数据
读取 Device 附加数据 (厂家)	cmdDeviceExtDatReq	0x000B	PC->Device	厂家读取授权工具数据(慎用)
返回 Device 附加数据 (厂家)	cmdDeviceExtDatResp	0x000C	Device->PC	厂家读取授权工具数据(慎用)
读取 Device 授权日志(厂家)	cmdDeviceLicLogReq	0x000D	PC->Device	厂家读取授权工具授权日志
返回 Device 授权日志(厂家)	cmdDeviceLicLogResp	0x000E	Device->PC	厂家读取授权工具授权日志
请求 Device 授权	cmdChipLicenseReq	0x000D	PL->Device	请求 Device 对目标芯片授权
返回 Device 授权	cmdChipLicenseResp	0x000E	Device->PL	根据 UID 返回设备授权数据
确认 Device 授权	cmdChipLicenseConfirm	0x000F	PL->Device	Device 保存授权记录.可读取
(保留)	(保留)	(保留)	(保留)	(保留)
OK 命令	cmdOK	0xFFFE	双向	无需返回数据响应
Error 命令	cmdError	0xFFFF	双向	遇到错误时返回给对方

5.2 cmdOK 命令 Payload

(注: 配对前的所有命令,无需 handler 参数.配对完成后需要 handler 参数.)

名称	格式	默认值	附加信息
handler	uint32_t	无	通讯句柄(配对前为空)
project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称

5.3 cmdError 命令 Payload

名称	格式	默认值	附加信息

handler	uint32_t	无	通讯句柄(配对前为空)
project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称
errCode	uint16_t	cmdErrorUnKnow	错误代码

5.4 cmdError 错误代码汇总

错误代码内容	命令代号	取值	触发命令
未知错误(未定义错误)	cmdErrorUnKnow	0x0000	ALL
CRC 校验错误	cmdErrorCRC32	0x0001	ALL
Project 不匹配	cmdErrorProject	0x0002	ALL
Device Busy	cmdErrorBusy	0x0003	请求过于频繁
Device Paired	cmdErrrorPaired	0x0004	已经在配对使用中
Hander 错误	cmdErrorHander	0x0005	Handler 不匹配
写入配置信息失败	cmdErrorConfigUpdate	0x0006	写入配置失败
更新固件失败	cmdErrorFWUpdate	0x0007	更新固件失败
UID 错误	cmdErrorUIDInfo	0x0008	UID 错误
License Disabled	CmdErrorLicDisabled	0x0009	授权已经被禁用
License 已用完	cmdErrorLicNoLeft	0x000A	授权数据已经用完
Device 没有配对	cmdErrorUnPaired	0x000B	没有请求配对
内部异常	cmdErrorInterError	0x000C	内部错误(异常)
内存不足	cmdErrorMemory	0x000D	内存不足
超时	cmdErrorTimeOut	0x000E	请求超时
Size 错误	cmdErrorSize	0x000F	Size Error
无法识别的指令	cmdErrorCmd	0x0010	无法识别的指令
参数错误	cmdErrorParams	0x0011	参数错误
权限错误	cmdErrorPermissions	0x0012	没有操作权限
功能没有开启	cmdErrorDisable	0x0013	此功能没有启用
使用了默认的通讯密码	cmdErrorDefaultPassword	0x0014	使用了默认的通讯密码

5.5 其他命令 Payload

5.5.1 查找授权工具(cmdDeviceFind)

名称	格式	默认值	附加信息
handler	uint32_t	无	通讯句柄(配对前为空)
project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称

(由 PowerLink 发给授权工具,如果授权工具收到命令,则响应 cmdDeviceInfo)

5.5.2 返回 Device 信息(cmdDeviceInfo)

handler	uint32_t	无	通讯句柄(配对前为空)
project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称
sn	uint8_t[17]	Device 内置.用于厂家查询	厂家给授权工具配置的序号
hwVer	uint8_t[6]	由创芯工坊定义.尽量不要修改	模块硬件版本
fwVer	uint8_t[6]	授权工具固件版本	固件版本
licEnable	uint8_t	是否使能授权工具	是否使能
uidlimitEnable	uint8_t	默认不限制	是否限制 Uid 授权范围
fwUpdateEn	uint8_t	默认开启	是否开启固件升级功能
extDatWriteEn	uint8_t	默认开启	是否容许写入附加数据
extDatReadEn	uint8_t	默认开启	是否允许回读附加数据
logEnable	uint8_t	默认开启	是否开启日志记录
licTotal	uint32_t	0	总授权次数
licLeft	uint32_t	0	剩余授权次数
uidLimitLwr	uint8_t[12]	无	UID 最小值(含)
uidLimitUpr	uint8_t[12]	无	UID 最大值(含)

(查找设备时返回,返回当前授权工具的配置信息)

5.5.3 配对到 Device (cmdDevicePair)

名称	格式	默认值	附加信息
handler	uint32_t	无	通讯句柄(配对前为空)
project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称
flag	uint8_t	0:默认配对 1:强制配对	强制配对会断开旧实例

(由 PowerLink 发给授权工具,如果授权工具返回 Pair 信息.如果已经配对过.则返回已经在使用中.可以拒绝配对)

5.5.4 配对到 Device 响应(cmdDevicePairResp)

名称	格式	默认值	附加信息
handler	uint32_t	此时生成句柄配对中使用	此时生成句柄
project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称

(hander 为配对成功之后,所有的请求都需要附带此参数.PowerLink 和 Device 都需要对其进行检查.直到下一次再次配对.分配新的句柄,才会更新此值,如果错误.上报错误码)

5.5.5 取消配对 Device(cmdDeviceUnPair)

名称	格式	默认值	附加信息
handler	uint32_t	Device 生成	有效句柄
project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称
flag	uint8_t	0:默认取消 1:强制取消	强制取消会断开当前实例

(PowerLink 会发送断开连接的消息给 Device 请求断开,Device 响应 OK.或者拒绝断开.并上报错误码)

5.5.6 配置 Device 信息(厂家慎用)(cmdDeviceConfig)

(注:我们尽可能的提供更多的功能给您,节省您宝贵的开发时间,但是我们仍然建议您.慎用 Device 的升级功能.可能会造成一些意外的风险.而降低授权工具的安全性,以下蓝色命令同理)

如果作为一次性的授权工具.可以在授权工具内部禁用这些命令.(或者容许出厂配置一次,以后不容许再次配置.在 ConfigTimeLeft 设置), 然后配置在内部固定设置

配置完成后,请重新连接 Device.

名称	格式	默认值	附加信息
handler	uint32_t	无	由 Device 随机生成,附带句柄
oldproject	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称
newProject	uint8_t[17]	新 Project 代码	更新项目代码(需要 powerlink)重新打包
newSn	uint8_t[17]	配置软件序列号	配置序列号用于追踪
newKey	uint8_t[16]	新密码	更新通讯密码
newIv	uint8_t[16]	新 IV	更新通讯 IV
licEnable	uint8_t	是否使能授权工具	是否使能
uidlimitEnable	uint8_t	默认不限制	是否限制 Uid 授权范围
fwUpdateEn	uint8_t	默认开启	是否开启固件升级功能
extDatWriteEn	uint8_t	默认开启	是否容许写入附加数据
extDatReadEn	uint8_t	默认开启	是否允许回读附加数据
logEnable	uint8_t	默认开启	是否开启日志记录
licTotal	Uint32	配置授权数量	配置授权数量
uidLimitLwr	uint8_t[12]	无	UID 最小值(含)
uidLimitUpr	uint8_t[12]	无	UID 最大值(含)
ConfigTimeLeft	uint16_t	默认只能配置一次	是否允许多次配置(此值第一次修改有效,第二次以后会被忽略,防止无限配置,也就是有最大值.最大配置 65535 次失效)

5.5.7 升级 Device 固件(厂家慎用)(cmdDeviceFwStart)

(固件更新地址请参考 Bootloader 和 APP 的资源分配.在代码中设置)

名称	格式	默认值	附加信息
handler	uint32_t	无	由 Device 随机生成,附带句柄
project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称
size	Uint32	新固件大小	更新固件大小
crc32	Uint32	新固件的 Crc32	Crc32

5.5.8 发送 Device 固件包(厂家慎用)(cmdDeviceFwPkgSend)

名称	格式	默认值	附加信息
handler	uint32_t	无	由 Device 随机生成,附带句柄
project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称
size	Uint32	当前包的有效大小	当前包的有效大小
data[256]	Uint32	包缓冲区	包缓冲区

5.5.9 完成 Device 升级(厂家慎用)(cmdDeviceFwPkgEnd)

(确认升级完成后,重新连接.)

名称	格式	默认值	附加信息
handler	uint32_t	无	由 Device 随机生成,附带句柄
project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称

5.5.10 写入附加数据(厂家慎用)(cmdDeviceExtDatSet)

(附加数据一般用于水印,可参数授权证书的生成,这样可以确保不同的项目用同一个证书.而改变签名水印实现)

名称	格式	默认值	附加信息
handler	uint32_t	无	由 Device 随机生成,附带句柄

project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称
Size	uint32_t	默认为 256 字节,最大 2K	不宜过大.一般 256/512/1K/2K
data	uint8_t *	附加数据块	填充的附加数据

5.5.11 读取附加数据(厂家慎用)(cmdDeviceExtDatReq)

(此功能可以禁用.)

名称	格式	默认值	附加信息
handler	uint32_t	无	由 Device 随机生成,附带句柄
project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称

5.5.11 返回附加数据(厂家慎用)(cmdDeviceExtDatResp)

(此功能可以禁用.)

名称	格式	默认值	附加信息
handler	uint32_t	无	由 Device 随机生成,附带句柄
project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称
Size	uint32_t	默认为 256 字节	实际的长度
data	uint8_t *	附加数据块	填充的附加数据

5.5.11 读取授权日志 (cmdDeviceLicLogReq)

名称	格式	默认值	附加信息
handler	uint32_t	无	由 Device 随机生成,附带句柄
project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称

5.5.12 返回授权日志 (cmdDeviceLicLogResp)

(只记录授权数量,不详细记录每颗芯片的 ID.授权证书.如果需要.需要外挂 SPI flash 并加密存储,用户拿到 SDK 可以调整此功能)

名称	格式	默认值	附加信息
handler	uint32_t	无	由 Device 随机生成,附带句柄
project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称
LicensedCnt	uint32_t	0	已下发的数量（发给烧录器的数量）
LicenseOKCnt	uint32_	0	已经成功写入的数量(烧录校验 OK)
LicenseErrCnt	uint32_t	0	烧录失败的数量(烧录校验 Error)
LicenseUnknow	uint32_t	0	已下发但是没有反馈(noResp)

5.5.10 请求 Chip 授权(cmdChipLicenseReq)

名称	格式	默认值	附加信息
handler	uint32_t	无	由 Device 随机生成,附带句柄
project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称
uidSize	uint16_t	ID 的长度	UID 的长度(一般为 12 字节)
uidData	uint8_t[12]	ID 缓冲区	UID 的数据.

5.5.11 返回 Chip 授权(cmdChipLicenseResp)

名称	格式	默认值	附加信息
handler	uint32_t	无	由 Device 随机生成,附带句柄
project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称
licSize	uint16_t	证书的长度	证书长度
licData	uint8_t *	证书的数据缓冲区	根据 UID 生成的证书

5.5.12 确认 Chip 授权(cmdChipLicenseConfirm)

名称	格式	默认值	附加信息
handler	uint32_t	无	由 Device 随机生成,附带句柄
project	uint8_t[17]	Device 内置.PowerLink 打包配置	通讯过程中附带项目名称
status	uint8_t	0:成功 1:失败	烧录器会上传成功或者失败.其余状态均为未知

五：附加

感谢阁下认可并使用创芯工坊的软硬件产品和服务,如果您在使用过程中遇到任何问题,或者建议和意见,定制化产品需求,请及时和我们取得联系,我们竭诚为您服务

创芯工坊硬件平台技术部