NEODUN通讯协议

版本号V1.2

版本变更

|  |  |
| --- | --- |
| 版本号 | 变更内容 |
| V1.0 | 新增据传输；  新增查询地址、添加地址、删除地址、导出安全信息  新增签名、拒绝签名 |
| V1.1 | 取消导出安全地址，新增安全通道；  新增固件升级、安装、卸载插件；  新增地址命名；  区分了BootLoader协议和APP协议； |
| V1.2 | 对各种失败回复协议增加了错误码。错误码均在4-5字节。  删减了安装固件、安装插件、卸载插件、增加地址、删除地址、更改地址名称的回复协议中的具体内容。  地址长度改为25字节。移动地址名称在协议中的位置 |

全局规则

上位机驱动 driver简称D，单片机签名机 signer简称S

D2S 表示上位机发往单片机的报文，S2D 表示单片机发往上位机的报文

报文长度 64字节，后文说第几字节，一律从零开始计数

* + 第0 1字节 用作报文识别信息，byte1 byte2
  + 第2 3字节 用作响应识别串号， 是一个小头在前的 uint16
  + 第 4~61 共58个字节用作报文数据区，由每条报文独自约定
  + 第 62 63 字节 用作报文验证位，是对报文0~62字节做crc32运算之后的整数，以小头在前存储，去前两个字节。

关于丢包，上位机向单片机发送，丢包是异常，可以捕获。

第一字节为分类字节

第二字节小于a0的是普通报文，msgid 是随机数

第二字节大于等于a0的是回复类报文，回复类报文是针对某条报文的回复，msgid 和该报文一致

第二字节大于等于e0的是错误类报文，用来报告错误，错误报文都是回复类报文

回复类报文没有对应的回复类报文

报文表达方式

D2S[tag1,tag2]，tag用十六进制byte

BootLoader通讯协议

**数据传输.**

D2S[01,01]发送数据包信息

|  |  |  |  |
| --- | --- | --- | --- |
| 2-3 | 4-7 | 8-39 | 62-63 |
| 串号，随机数 | 数据包大小 | 数据包哈希 | 验证位 |

D2S[01,a2]发送数据

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2-3 | 4-5 | 6-7 | 8-57 | 62-63 |
| 所响应的[01,10]请求数据的串号 | 本次发送数据的片号 | 分包序号 | 数据 | 验证位 |

D2S[01,a3]发送完毕

|  |  |  |
| --- | --- | --- |
| 2-3 | 4-5 | 62-63 |
| 所响应的[01,10]请求数据的串号 | 分包序号 | 验证位 |

S2D[01,e0]数据过大

|  |  |
| --- | --- |
| 2-3 | 62-63 |
| 报错所对应[01,01]的串号 | 验证位 |

S2D[01,10]请求数据

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2-3 | 4-5 | 6-7 | 8-39 | 62-63 |
| 随机数 | 请求数据的开始片数 | 请求数据的结束片数 | 请求内容哈希 | 验证位 |

S2D[01,11]接收完毕哈希正确

|  |  |  |  |
| --- | --- | --- | --- |
| 2-3 | 4-7 | 8-39 | 62-63 |
| 对应[01,01]串号 | 给该数据包分配的ID | 接收到的数据特征码 | 验证位 |

S2D[01,12]接收完毕哈希不正确

|  |  |  |  |
| --- | --- | --- | --- |
| 2-3 | 4-7 | 8-39 | 62-63 |
| 对应[01,01]串号 | 给该数据包分配的ID | 接收到的数据特征码 | 验证位 |

S2D[00,e0]报文出错

|  |  |
| --- | --- |
| 2-3 | 62-63 |
| 报错所对应的命令串号 | 验证位 |

**文件传输**

D2S[03,01] 安装更新APP现[02,0b]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2-3 | 4-5 | 6-7 | 8-39 | 40-41 | 42-61 | 62-63 |
| 随机数串号 | 安装类型 | 安装内容 | 文件哈希 | 版本号 | 数据包ID 1-5 | 验证位 |

安装类型有两种：固件安装（0000）与插件安装（0001）。

安装内容为安装的插件币种，与导入地址的类型一致，比如neo的地址类型。固件安装的安装内容为0000

数据包ID为分包传输的数据包ID，4字节一个ID，数量不足5个时未用到的ID为0

S2D[03,11] 等待更新

|  |  |
| --- | --- |
| 2-3 | 62-63 |
| 随机数串号 | 验证位 |

S2D[03,a1] 安装成功 现[02,c3]

|  |  |
| --- | --- |
| 2-3 | 62-63 |
| 对应[03,01]安装命令串号 | 验证位 |

S2D[03,e1] 安装失败 现[02,c4]

|  |  |  |
| --- | --- | --- |
| 2-3 | 4-5 | 62-63 |
| 对应[03,01]安装命令串号 | 错误码 | 验证位 |

错误码：0100文件哈希不正确

APP通讯协议

**数据传输.**

D2S[01,01]发送数据包信息

|  |  |  |  |
| --- | --- | --- | --- |
| 2-3 | 4-7 | 8-39 | 62-63 |
| 串号，随机数 | 数据包大小 | 数据包哈希 | 验证位 |

D2S[01,a2]发送数据

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2-3 | 4-5 | 6-7 | 8-57 | 62-63 |
| 所响应的[01,10]请求数据的串号 | 本次发送数据的片号 | 分包序号 | 数据 | 验证位 |

D2S[01,a3]发送完毕

|  |  |  |
| --- | --- | --- |
| 2-3 | 4-5 | 62-63 |
| 所响应的[01,10]请求数据的串号 | 分包序号 | 验证位 |

S2D[01,e0]数据过大

|  |  |
| --- | --- |
| 2-3 | 62-63 |
| 报错所对应[01,01]的串号 | 验证位 |

S2D[01,10]请求数据

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2-3 | 4-5 | 6-7 | 8-39 | 62-63 |
| 随机数 | 请求数据的开始片数 | 请求数据的结束片数 | 请求内容特征码 | 验证位 |

S2D[01,11]接收完毕哈希正确

|  |  |  |  |
| --- | --- | --- | --- |
| 2-3 | 4-7 | 8-39 | 62-63 |
| 对应[01,01]串号 | 给该数据包分配的ID | 接收到的数据特征码 | 验证位 |

S2D[01,12]接收完毕哈希不正确

|  |  |  |  |
| --- | --- | --- | --- |
| 2-3 | 4-7 | 8-39 | 62-63 |
| 对应[01,01]串号 | 给该数据包分配的ID | 接收到的数据特征码 | 验证位 |

S2D[00,e0]报文出错

|  |  |
| --- | --- |
| 2-3 | 62-63 |
| 报错所对应的命令串号 | 验证位 |

**文件传输**

D2S[03,01] 安装插件APP现[02,0b]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2-3 | 4-5 | 6-7 | 8-39 | 40-41 | 42-61 | 62-63 |
| 随机数串号 | 安装类型 | 安装内容 | 文件哈希 | 版本号 | 数据包ID 1-5 | 验证位 |

安装类型有两种：固件安装（00）与插件安装（01）。

安装内容为安装的插件币种，与导入地址的类型一致，比如neo的地址类型。固件安装的安装内容为0

S2D[03,a1] 安装成功现[02,c3]

|  |  |
| --- | --- |
| 2-3 | 62-63 |
| 对应[03,01安装]命令串号 | 验证位 |

S2D[03,e1] 安装失败现[02,c4]

|  |  |  |
| --- | --- | --- |
| 2-3 | 4-5 | 62-63 |
| 对应[03,01安装]命令串号 | 错误码 | 验证位 |

错误码：

0100：文件哈希不匹配

0101：安装空间不足

D2S[03,02]发送更新固件请求

|  |  |
| --- | --- |
| 2-3 | 62-63 |
| 随机数串号 | 验证位 |

S2D[03,a2]同意更新固件

|  |  |
| --- | --- |
| 2-3 | 62-63 |
| 对应[03,02]更新请求串号 | 验证位 |

S2D[03,e2]拒绝更新固件

|  |  |
| --- | --- |
| 2-3 | 62-63 |
| 对应[03,02]更新请求串号 | 验证位 |

D2S[03,03]卸载插件

|  |  |  |
| --- | --- | --- |
| 2-3 | 4-5 | 62-63 |
| 随机数串号 | 插件类型 | 验证位 |

插件类型为安装协议中的“安装内容”，和地址类型一致，比如neo、比特币等

S2D[03,a3]卸载成功

|  |  |
| --- | --- |
| 2-3 | 62-63 |
| 对应[03,03]卸载命令串号 | 验证位 |

S2D[03,e3]卸载失败

|  |  |  |
| --- | --- | --- |
| 2-3 | 4-5 | 62-63 |
| 对应[03,03]卸载命令串号 | 错误码 | 验证位 |

当钱包内保存有对应插件类型的地址时，返回卸载失败

错误码：0102：该APP正在使用中

D2S[03,04]查询固件插件版本

|  |  |
| --- | --- |
| 2-3 | 62-63 |
| 随机数串号 | 验证位 |

S2D[03,a4]回复固件版本

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2-3 | 4-5 | 6-7 | 8-9 | 10-11 | 12-13 | …… | 58-59 | 60-61 | 62-63 |
| 对应 [03,04]查询串号 | 固件版本号 | 插件1类型 | 插件1版本号 | 插件2类型 | 插件2版本号 | …… | 插件14类型 | 插件14版本号 | 验证位 |

特殊操作

D2S[04,01]请求安全通道公钥

|  |  |
| --- | --- |
| 2-3 | 62-63 |
| 随机数串号 | 验证位 |

S2D[04,a1]回复安全通道公钥

|  |  |  |
| --- | --- | --- |
| 2-3 | 4-35 | 62-63 |
| 对应[04,01]请求串号 | 安全通道公钥 | 验证位 |

地址签名相关

D2S[02,01]查询地址

|  |  |
| --- | --- |
| 2-3 | 62-63 |
| 随机串号 | 验证位 |

S2D[02,a0]返回一条地址

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2-3 | 4-5 | 6-7 | 8-9 | 10-35 | 36-41 | 62-63 |
| 对应[02,01]查询命令串号 | 当前地址索引 | 全部地址数 | 地址类型 | 地址数据 | 地址名称 | 验证位 |

地址类型增加隐藏类型。例如neo是0101,隐藏neo设置为0001。

隐藏地址类型只发送真实地址的前8位和后8位，中间全部为0。

S2D[02,a1]返回地址结束

|  |  |  |
| --- | --- | --- |
| 2-3 | 4-5 | 62-63 |
| 对应[02,01]查询命令串号 | 全部地址数量 | 验证位 |

D2S[02,02]设置地址名称

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2-3 | 4-29 | 30-31 | 32-37 | 62-63 |
| 随机串号 | 地址数据 | 地址名称长度 | 地址名称 | 验证位 |

S2D[02,a2]名称设置成功

|  |  |
| --- | --- |
| 2-3 | 62-63 |
| 对应 [02,02]设置地址名称串号 | 验证位 |

S2D[02,e2]名称设置失败

|  |  |  |
| --- | --- | --- |
| 2-3 | 4-5 | 62-63 |
| 对应 [02,02]设置地址名称串号 | 错误码 | 验证位 |

错误码：

0203地址名称重复

0206不存在该地址

D2S[02,03]删除一条地址

|  |  |  |  |
| --- | --- | --- | --- |
| 2-3 | 4-5 | 6-31 | 62-63 |
| 随机串号 | 地址类型 | 地址数据 | 验证位 |

S2D[02,a3]删除地址成功现为[02,c1]

|  |  |
| --- | --- |
| 2-3 | 62-63 |
| 对应 [02,03]删除地址命令串号 | 验证位 |

S2D[02,e3]删除地址失败现为[02,c2]

|  |  |  |
| --- | --- | --- |
| 2-3 | 4-5 | 62-63 |
| 对应 [02,03]删除地址命令串号 | 错误码 | 验证位 |

错误码：0401用户拒绝

D2S[02,04]增加一条地址

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2-3 | 4-5 | 6-31 | 46-49 | 50-53 | 54-57 | 58-61 | 62-63 |
| 随机数串号 | 地址类型 | 地址数据 | 参数0数据包ID | 参数1数据包ID | 参数2数据包ID | 参数3数据包ID | 验证位 |

增加地址的参数数据经过非对称加密，需要用安全通道的私钥进行解密后再储存。

S2D[02,a4]增加地址成功现为[02,b1]

|  |  |
| --- | --- |
| 2-3 | 62-63 |
| 对应[02,04]增加地址命令串号 | 验证位 |

S2D[02,e4]增加地址失败现为[02,b2]

|  |  |  |
| --- | --- | --- |
| 2-3 | 4-5 | 62-63 |
| 对应[02,04]增加地址命令串号 | 错误码 | 验证位 |

错误码：

0201私钥数量达到上限

0202该私钥已导入

0204未导入该币种插件

0205私钥格式错误

D2S[02,05]进行签名现为[02,0a]

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2-3 | 4-5 | 6-31 | 46-49 | 50-53 | 54-57 | 58-61 | 62-63 |
| 随机数串号 | 签名方法 | 地址 | 0号数据包ID | 1号数据包ID | 2号数据包ID | 3号数据包ID | 验证位 |

S2D[02,a5]签名成功现为[02,a8]

|  |  |  |  |
| --- | --- | --- | --- |
| 2-3 | 4-7 | 8-39 | 62-63 |
| 对应[02,05]签名命令串号 | 数据大小 | 数据哈希 | 验证位 |

S2D[02,e5]签名失败现为[02,e0]

|  |  |  |
| --- | --- | --- |
| 2-3 | 4-5 | 62-63 |
| 对应[02,05]签名命令串号 | 错误码 | 验证位 |

错误码

0301未导入所需私钥

0302不支持多签

0401用户拒绝