YK01 蓝牙通信协议

目录

1. 蓝牙连接规则

通用唯一识别码(Universally Unique Identifier)

采用如下UUID：0x0000xxxx-0000-1000-8000-00805F9B34FB

公司ID(VendorID)

VendorID = 0A01 // Reserved ID

服务ID(Service UUID)/特征ID

Service UUID = FEE7

Characteristic UUIDs 如下表定义：

特征值	36F1	36F2
属性	Write	Read Notify

2. 广播规则

蓝牙名称与广播内容定义

蓝牙广播名称:YK01-xxxxx

Manufacturer Data为6字节(byte)蓝牙Mac地址，采用大端模式排列

3. 广播间隔

默认广播间隔为：2000ms

设备根据自身逻辑设计，可变更该广播间隔.

4. 连接属性

默认参数如下:

最大连接间隔:50ms

最小连接间隔:16ms

从机延迟:0ms

连接超时:4000ms

该参数可通过协议指令配置

5. 编解码说明

编解码流程

1. 通过标识符识别出完整的消息，称为A
2. 对A进行转译，得到结果B
3. 从B获取校验码，check_code
4. 从B获取application_layer的长度，
5. 对application_layer进行异或校验，获得异或校验结果，check_code_result
6. 计算application_layer的长度，获得实际长度，application_layer_length_result
7. 对比check_code与check_code_result是否相等,对application_layer_length与application_layer_length_result是否相等
8. 对application_layer进行解密操作

加解密算法

采用AES-128加密算法。

补零方式:

不足16个字节，补0到16个字节； 正好16个字节的不补

转译算法

转译规则遵循如下表格

转译前	转译后
0x7e	0x7d 0x02
0x7d	0x7d 0x01

应用举例:

转译前:

0x30 0x7e 0x08 0x7d 0x55

转译后:

0x30 0x7d 0x02 0x08 0x7d 0x01 0x55

异或校验算法

异或校验算法

```
uint8 FW_Xor(uint8 *pData,int nLength)
{
    uint8 value = 0;

    for(int i = 0; i < nLength; i++)
    {
    value ^= *(pData+i);
    }
```

```
    return value;
}
```

外层封装(msg)定义

消息(msg)

名称	中文	类型	描述	单位	枚举
identifier	标识符	uint8	定值:0x7e	(无单位)	-
application_layer_length	应用层长度	uint8	用于说明应用层字节长度	bytes(字节)	-
application_layer	应用层	struct	用于表示消息具体内容 详见应用层(application_layer)参数说明	(无单位)	-
check_code	校验码	uint8	采用异或校验 校验从标识符(不含)到校验码之前的全部内容	(无单位)	-
identifier	标识符	uint8	定值:0x7e	(无单位)	-

应用层(application_layer)参数说明

名称	中文	类型	描述	单位	枚举

msg_head	消息头	struct	用于索引消息体采用何种数据结构进行解析 详见消息头(msg_head)参数说明	(无单位)	-
msg_body	消息体	bytes	用于承载具体的数据业务	(无单位)	-

消息头(msg_head)参数说明

名称	中文	类型	描述	单位	枚举
command_id	命令码	uint8	用于区分不同命 令	(无单位)	0x01:鉴权指令(auth) 0x81:鉴权指令响应(auth_response) 0x02:进入拷贝模式(enter_copy_mode) 0x82:进入拷贝模式响应(enter_copy_mode_response)

						0x03:查询拷贝进度(query_copy_progress) 0x83:查询拷贝进度响应(query_copy_progress_response) 0x04:退出拷贝模式(exit_copy_mode) 0x84:退出拷贝模式响应(exit_copy_mode_response) 0x05:查询拷贝信息(get_copy_info) 0x85:查询拷贝信息响应(get_copy_info_response)

					0x06:清除拷贝信息(clear_copy_info) 0x86:清除拷贝信息响应(clear_copy_info_response) 0x07:模式切换(mode_switch) 0x87:模式切换响应(mode_switch_response) 0x08:遥控命令(remote_control) 0x88:遥控命令响应(remote_control_response)

					0x10:请求升级命令(request_upgrade) 0x90:请求升级命令响应(request_upgrade_response) 0x11:写入固件文件(write_firm) 0x91:写入固件文件响应(write_firm_response)
msg_length	消息长度	uint8	-	(无单位)	-
msg_master_token	主机消息令 牌	uint8	由主机随机生成	(无单位)	-
msg_slave_token	从机消息令 牌	uint8	由从机随机生成	(无单位)	-

接口目录

序 号	名称	描述	类型
1	鉴权方法	1. 连接建立， 主机生成1字节随机值， 放入消息头的msg_master_token中， 同时获取主机MAC地址， 作为鉴权内容发送鉴权指令给从机 2. 从机收到鉴权指令后， 生成1字节随机值， 放入消息头msg_slave_token中， 将内容中的mac地址与连接 设备的mac进行对比， 如果一致，则鉴权成功， 发送结果给主机， 同时记录本次连接的主机的随机值； 如 果不一致， 鉴权失败， 发送鉴权结果，并断开连接。 3. 主机收到返回值后， 记录消息头中msg_slave_token	

		4. 之后双方通讯在解密后都要在比对各自的token是否一致，不一致就断开连接， 一致才正常执行指令 5. 设备断开连接后， 主机和从机缓存的token要清除，下次连接重新生成	
2	进入拷贝模式	进入拷贝模式	
3	查询拷贝进度		
4	退出拷贝模式	手机控制设备退出拷贝模式	
5	查询拷贝信息	手机查询拷贝信息	
6	清除拷贝信息	手机清除拷贝信息	
7	模式切换	手机控制模式切换	
8	遥控命令	手机控制相关遥控命令	
9	请求升级命令	手机控制设备开始升级	
10	写入固件文件	手机控制设备写入固件	

6. 接口列表

6.1 鉴权方法

英文:auth

类型:action(方法)

说明

1. 连接建立， 主机生成1字节随机值， 放入消息头的msg_master_token中， 同时获取主机MAC地址， 作为鉴权内容发送鉴权指令给从机
2. 从机收到鉴权指令后， 生成1字节随机值， 放入消息头msg_slave_token中， 将内容中的mac地址与连接设备的mac进行对比， 如果一致， 则鉴权成功， 发送结果给主机， 同时记录本次连接的主机的随机值； 如果不一致， 鉴权失败， 发送鉴权结果， 并断开连接。
3. 主机收到返回值后， 记录消息头中msg_slave_token
4. 之后双方通讯在解密后都要在比对各自的token是否一致，不一致就断开连接， 一致才正常执行指令
5. 设备断开连接后， 主机和从机缓存的token要清除，下次连接重新生成

发送

鉴权指令(auth) command_id = 0x01

名称	中文	类型	描述	单位	枚举
master_ble_mac	主机蓝牙MAC地址	uint8	需要说明大小端模式 长度为6bytes(字节)	(无单位)	-

返回

鉴权指令响应(auth_response) command_id = 0x81

名称	中文	类型	描述	单位	枚举
auth_result	鉴权结果	uint8	需要特别说明的： 针对鉴权失败的设备不进行响应并主动断开连接	(无单位)	1:鉴权成功(success)

6.2 进入拷贝模式

英文:enter_copy_mode

类型:action(方法)

说明

中控通过该方法， 进入拷贝模式

设备扫描不同的433频段，找到对应的钥匙数据

发送

进入拷贝模式(enter_copy_mode) command_id = 0x02

名称	中文	类型	描述	单位	枚举
scan_frequency	扫描频点	uint32	-	khz	433000 - 433M
scan_timeout	扫描超时时间	uint16	-	ms	超时时间

key_value	键值	uint8			0 - 开锁 1 - 设防 2 -

返回

进入拷贝模式响应(enter_copy_mode_response) command_id = 0x82

名称	中文	类型	描述	单位	枚举
enter_copy_result_status	扫描结果状态	uint8	-	(无单位)	0 - 拷贝到有效 1 - 进入拷贝模式失败 2 - 进入拷贝模式成功
enter_copy_result_code	拷贝码	uint16	-	(无单位)	
enter_copy_log	日志	l-v(8-8)	l-v 表示长度+有效数据 l-表示长度，1个字节表示，0表示无数据		

6.3 查询拷贝进度

说明

中控通过该方法， 查询拷贝进度

设备返回当关扫描的频段以及数据完成度

发送

查询拷贝进度(query_copy_progress) command_id = 0x03

返回

查询拷贝进度响应(query_copy_progress_response) command_id = 0x83

名称	中文	类型	描述	单位	枚举
enter_copy_result_status	扫描结果状态	uint8	-	(无单位)	0 - 拷贝已结束 1 - 拷贝进行中
enter_copy_result_code	当前扫描的频点	uint32	-	khz	
enter_copy_data_completeness	数据完整度	uint32	-		
enter_copy_log	日志	l-v(8-8)	l-v 表示长度+有效数据 l-表示长度，1个字节表示，0表示无数据		

6.4 退出拷贝模式

说明

中控通过该方法， 退出拷贝模式

app退出时，结束拷贝模式

发送

进入拷贝模式(exit_copy_mode) command_id = 0x04

返回

进入拷贝模式响应(exit_copy_mode_response) command_id = 0x84

名称	中文	类型	描述	单位	枚举
exit_copy_result_status	扫描结果状态	uint8	-	(无单位)	0 - 拷贝到有效 1 - 进入拷贝模式失败 2 - 进入拷贝模式成功
exit_copy_result_code	拷贝码	uint16	-	(无单位)	
exit_copy_log	日志	l-v(8-8)	l-v 表示长度+有效数据 l-表示长度，1个字节表示，0表示无数据		

6.5 查询拷贝信息

说明

中控通过该方法， 查询拷贝信息

查询已拷贝成功的数据

发送

进入拷贝模式(get_copy_info) command_id = 0x05

返回

进入拷贝模式响应(get_copy_info_response) command_id = 0x85

名称	中文	类型	描述	单位	枚举
get_copy_info_count	拷贝信息个数	uint8	-	(无单位)	0 - 拷贝到有效 1 - 进入拷贝模式失败 2 - 进入拷贝模式成功
copy_info_code	拷贝信息	uint16		(无单位)	

eget_copy_info_log	日志	l-v(8-8)	l-v 表示长度+有效数据 l-表示长度，1个字节表示，0表示无数据		

6.6 清除拷贝信息

说明

中控通过该方法， 清除拷贝信息

发送

进入拷贝模式(clear_copy_info) command_id = 0x06

名称	中文	类型	描述	单位	枚举
clear_copy_code	要清除的拷贝码	uint16	-	无	0 - 全部清除 其它 - 清除指定拷贝码

返回

进入拷贝模式响应(clear_copy_info_response) command_id = 0x86

名称	中文	类型	描述	单位	枚举

clear_copy_result_status	执行结果	uint8	-	(无单位)	0 - 清除成功 1 - 无此拷贝码
clear_copy_info_log	日志	l-v(8-8)	l-v 表示长度+有效数据 l-表示长度，1个字节表示，0表示无数据		

6.7 模式切换

说明

中控通过该方法， 进行设备的模式切换，包括正常模式，运输模式，测试模式

发送

进入拷贝模式(mode_switch) command_id = 0x07

名称	中文	类型	描述	单位	枚举
mode	模式选择	uint8	-	无	0 - 正常模式 1 - 运输模式 2 - 测试模式

返回

进入拷贝模式响应(mode_switch_response) command_id = 0x87

名称	中文	类型	描述	单位	枚举
mode_switch_result_status	执行结果	uint8	-	(无单位)	0 - 切换成功 1 - 切换失败
mode_switch_log	日志	l-v(8-8)	l-v 表示长度+有效数据 l-表示长度，1个字节表示，0表示无数据		

6.8 遥控命令

说明

中控通过该方法， 控制设备发送数据，发送不同的拷贝码

发送

进入拷贝模式(remote_control) command_id = 0x08

名称	中文	类型	描述	单位	枚举
remote_control_copy_code	执行的拷贝码	uint16	-	无	

返回

进入拷贝模式响应(remote_control_response) command_id = 0x88

名称	中文	类型	描述	单位	枚举
remote_control_result_status	执行结果	uint8	-	(无单位)	0 - 执行成功 1 - 无此拷贝码
remote_control_log	日志	l-v(8-8)	l-v 表示长度+有效数据 l-表示长度，1个字节表示，0表示无数据		

6.9 请求升级命令

说明

中控通过该方法， 控制设备开始升级

发送

进入拷贝模式(request_upgrade) command_id = 0x10

名称	中文	类型	描述	单位	枚举
firmware_size	升级文件大小	uint32	-	butes(字节)	

firmware_MD5	固件MD5校验值	uint8	16字节		

返回

进入拷贝模式响应(request_upgrade_response) command_id = 0x90

名称	中文	类型	描述	单位	枚举
update_action_result	执行结果	uint8	-	(无单位)	0:开始下载固件(StartUpdate) 1:下载指令失败-目标设备不存在(NoExistDevice) 2:下载指令失败-设备不支持更新(NotSupportUpdate) 3:下载指令失败-已为最新版本(AlreadyNew)

					4:下载指令失败-空间不足(SpaceNotEnough) 5:下载指令失败-无足够电量进行升级 (NoPowerToUpdate)
already_write_firm_DataL_length	已写入固件长度	uint32			
remote_control_log	日志	l-v(8-8)	l-v 表示长度+有效数据 l-表示长度，1个字节表示，0表示无数据		

6.10 写入固件数据

说明

主机通过该方法,向从机写入固件数据

主机分帧向从机写入数据

当从机侦测到写入完成后,进行MD5校验

校验成功后,设备自动进行重启

发送

进入拷贝模式(request_upgrade) command_id = 0x11

名称	中文	类型	描述	单位	枚举
firmware _data_length	固件数据包长度	uint8	-	butes(字节)	
firmware _data	固件数据包	uint8			

返回

进入拷贝模式响应(request_upgrade_response) command_id = 0x91

名称	中文	类型	描述	单位	枚举

update_action_result	执行结果	uint8	-	(无单位)	0:开始下载固件(StartUpdate) 1:下载指令失败-目标设备不存在(NoExistDevice) 2:下载指令失败-设备不支持更新(NotSupportUpdate) 3:下载指令失败-已为最新版本(AlreadyNew) 4:下载指令失败-空间不足(SpaceNotEnough) 5:下载指令失败-无足够电量进行升级(NoPowerToUpdate)

already_write_firm_DataL_length	已写入固件长度	uint32			
remote_control_log	日志	l-v(8-8)	l-v 表示长度+有效数据 l-表示长度，1个字节表示，0表示无数据		