**T-BOX与iBTM数据传输策略**

**修改历史**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本** | **编辑** | **日期** | **修改记录** | **审核** |
| V0.1 | 黄榆彬 | 2020-09-09 | 初版发布 |  |
| V0.2 | 黄榆彬 | 2020-09-14 | 1. 更改数据传输请求报文格式，CRC改为CRC16,CRC放在byte6，7； 2. 更改数据传输响应报文格式，CRC改为CRC16,CRC放在byte6，7； 3. 判断接收完所有数据DTF报文超时时间由10ms改为50ms； 4. TDTFS\_Time=20ms时间参数改为TDTFS\_Time=1000ms； 5. TDTFS\_Wait\_Time=50ms时间参数改为TDTFS\_Wait\_Time=950ms 6. 增加CRC验证错误重传要求； |  |
| V0.3 | 黄榆彬 |  | 1. 增加CRC16算法； |  |
| V0.4 | 邓利华 | 2020-09-22 | 增加信号定义和传输示例，第6、7章节 |  |
| V0.5 | 邓利华 | 2020-09-23 | 1、修改5.2.5 SCMD值  2、修改6.3.1内容 |  |
| V0.6 | 邓利华 | 2020-10-8 | 1、6.4.3离线激活通知增加激活时间字段 |  |
| V0.7 | 邓利华 | 2020-10-13 | 1. 增加6.2传输数据传输格式 2. 修改6.3章节子标题描述 3. 修改6.3中数据长度 |  |
| V0.8 | 邓利华 | 2020-10-14 | 1、修改第5和7章中信号定义不一致的地方 |  |
| V0.9 | 邓利华 | 2020-10-27 | 1. 增加数据反馈接收超时和CRC错误处理机制 2. 4.1中增加反馈传输数据响应报文类型 3. 7.2中增加反馈传输数据响应报文 |  |
| V0.10 | 邓利华 | 2020-11-11 | 1. 修改查询结果查询成功为钥匙有效 2. 数据解析失败改为解密后校验失败 3. 传输数据加密时数据区增加CMAC 4. 增加数据解析失败传输响应报文CMD定义 5. 修改IBTM端接收TBOX传输响应超时时间为10s 6. 反馈结果中钥匙已注销和被删除统一为钥匙失效 |  |
| V1.0 | 胡冬红 | 2020-11-24 | 1. 数据传输请求报文增加加密类型字段区分加密 2. 增加终端秘钥下发和用户证书下发功能 |  |
| V1.1 | 邓利华 | 2020-12-30 | 1、7.2参考示例修改，反馈传输数据报文加密类型为1  2、6.3.10修改IBTM用户证书下发数据格式  3、5.9增加终端密钥结果反馈状态 |  |
| V1.2 | 邓利华 | 2021-01-08 | 1、1.1传输请求报文增加信息安全功能类型字段  2、4.2增加传输请求超时 请求响应结果 |  |

**目录**

[1. 数据报文格式 4](#_Toc7433)

[1.1. 数据传输请求报文 4](#_Toc1320)

[1.2. 数据传输请求响应报文 4](#_Toc5963)

[1.3. 数据传输报文 5](#_Toc31121)

[1.4. 数据传输响应报文 5](#_Toc24608)

[2. 数据传输流程 6](#_Toc15869)

[2.1. 反馈结果未带数据密文传输流程 6](#_Toc702)

[2.2. 反馈结果带数据密文传输流程 7](#_Toc8353)

[3. CRC校验算法 10](#_Toc11506)

[4. 信号定义集合 10](#_Toc5829)

[4.1. T-BOX→IBTM 报文列表 10](#_Toc10983)

[4.2. IBTM→T-BOX发送报文列表 11](#_Toc16350)

[5. 反馈结果 12](#_Toc31317)

[5.1. 注册结果反馈 12](#_Toc22161)

[5.2. 查询所有钥匙结果 12](#_Toc30696)

[5.3. 查询特定钥匙结果 13](#_Toc9968)

[5.4. 删除特定钥匙结果反馈 13](#_Toc289)

[5.5. 删除所有钥匙结果反馈 13](#_Toc7013)

[5.6. 修改期限结果反馈 14](#_Toc30209)

[5.7. 修改权限结果反馈 14](#_Toc15911)

[5.8. 更新钥匙结果 14](#_Toc8503)

[6. 传输数据内容 15](#_Toc15153)

[6.1. 数据格式 15](#_Toc691)

[6.1.1. 传输数据格式 15](#_Toc3855)

[6.1.2. 反馈传输数据格式 15](#_Toc6082)

[6.1.3. 数据类型 16](#_Toc12546)

[6.1.4. 分帧传输帧数 16](#_Toc21797)

[6.2. 业务命令SCMD 16](#_Toc15173)

[6.2.1. T-BOX→IBTM 16](#_Toc27325)

[6.2.2. IBTM→T-BOX 17](#_Toc27258)

[6.3. T-BOX 发送SCMD数据内容 17](#_Toc26054)

[6.3.1. 注册 17](#_Toc21898)

[6.3.2. 查询所有钥匙 17](#_Toc11702)

[6.3.3. 查询特定钥匙 18](#_Toc2430)

[6.3.4. 删除特定钥匙 18](#_Toc31028)

[6.3.5. 删除所有钥匙 18](#_Toc20758)

[6.3.6. 修改有效期 18](#_Toc977)

[6.3.7. 修改权限 18](#_Toc28206)

[6.3.8. 更新认证信息 19](#_Toc21085)

[6.4. IBTM 发送SCMD数据内容 19](#_Toc31534)

[6.4.1. 车辆蓝牙信息上传 19](#_Toc783)

[6.4.2. 本地注销通知 19](#_Toc7450)

[6.4.3. 离线激活通知 20](#_Toc20452)

[6.4.4. 离线删除通知 20](#_Toc13049)

[6.5. 查询结果返回 20](#_Toc23760)

[6.5.1. 查询特定钥匙 20](#_Toc21938)

[6.5.2. 查询所有钥匙 20](#_Toc30918)

[7. 数据传输举例 21](#_Toc21392)

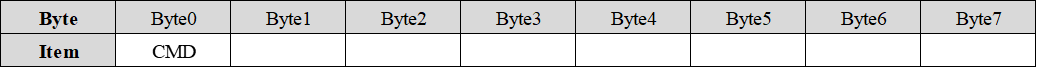
[7.1. 注册 21](#_Toc28567)

[7.2. 查询所有钥匙 21](#_Toc27903)

# 数据报文格式

数据报文包含：数据传输请求报文、数据传输请求响应报文、数据传输报文和数据传输响应报文，其格式如下表1所示；

1. 数据报文格式



其中：

CMD值为0x00时，此报文表示数据传输请求报文（DTRF）；

CMD值为0xF0～0xFF时，此报文表示数据传输请求响应报文(DTRFS)；

CMD值为0x01～0x7F时，此报文表示数据传输报文(DTF)；

CMD值为0x80～0xEF时，此报文表示数据传输响应报文(DTFS)。

## 数据传输请求报文

数据传输请求报文，其格式如下表2所示；

1. 数据传输请求报文格式

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Byte | Byte0 | Byte1 | Byte2 | Byte3（bit4:bit7） | Byte3（bit0:bit3） | Byte4 | Byte5 | Byte6 | Byte7 |
| Item | CMD | Data len | | S-task Type | Encrypt Type | Reserved | | CRC | |

其中：

CMD值为0x00；

Data Len表示数据传输报文中所需要传输的数据长度（明文传输则是明文长度，若传输数据加密，则是密文长度）；

S-task Type:表示信息安全功能数据传输任务类型，0表示非安全功能传输请求，1表示传输用户证书，2表示传输终端密钥，其他预留；

Encrypt Type 表示加密的类型 0x00：不加密 0x01：AES128 ；

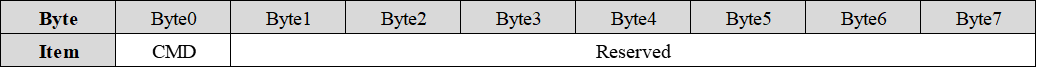
CRC表示所采用CRC16校验算法对所有传输数据（若传输的是加密后的数据则是对密文数据的校验）的校验；

Reserved预留字节，默认填充0x00。

## 数据传输请求响应报文

数据传输请求响应报文，其格式如下表3所示；

1. 数据传输请求响应报文格式



其中：

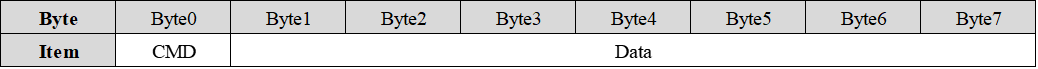
CMD值为0xF0～0xFF，表示数据传输请求响应结果，默认填充0xFF，表示允许传输，其余状态预留。

Reserved预留字节，默认填充0x00。

## 数据传输报文

数据传输报文，其格式如下表4所示；

1. 数据传输报文格式



其中：

CMD值为0x01～0x7F，表示数据分片传输的序号，超过0x7F时，应重新变为0x01；

Data表示密文数据。

## 数据传输响应报文

数据传输响应报文，其格式如下表5所示；

1. 数据传输响应报文格式

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Byte | Byte0 | Byte1 | Byte2 | Byte3 | Byte4（bit0:bit3） | Byte5 | Byte6 | Byte7 |
| Item | CMD | Response | Data len | | Encrypt Type | Reserved | CRC | |

其中：

CMD值为0x80～0xF0，表示控制命令子ID；

Response表示数据接收后，接收节点所反馈的结果；

Data Len表示数据传输报文中所需要传输的数据长度（明文传输则是明文长度，若传输数据加密，则是密文长度），如果Data Len为0，则表示反馈结果无数据传输，不需要解析CRC；如果Data Len不为0，则表示反馈结果带有数据密文，并解析CRC；

Encrypt Type 表示加密的类型 0x00：不加密 0x01：AES128 ；

CRC表示所采用CRC16校验算法对所有反馈传输数据（若传输的是加密后的数据则是对密文数据的校验）的校验；

Reserved预留字节，默认填充0x00。

# 数据传输流程

## 反馈结果未带数据密文传输流程

如图1所示，Sender需要往Receiver发送若干个字节长度的密文数据，Receiver在接收到Sender传输的数据后，将结果反馈给Sender，流程如下：

1. Sender给Receiver发送一个数据传输请求报文（DTRF）；
2. Receiver收到Sender数据传输请求报文（DTRF）之后，应在TDTRFS\_Time **=**40ms内发送一个数据传输请求响应报文(DTRFS)；
3. 如果Sender在TDTRFS\_Wait\_Time=50ms都未收到Receiver反馈的数据传输请求响应报文(DTRFS)，Sender应重新发送数据传输请求报文（DTRF）；
4. Sender重复请求5次后如果都未收到Receiver反馈的数据传输请求响应报文(DTRFS)，则Sender应停止自动重新向此Receiver发送数据传输请求报文（DTRF），并记录相应的故障；
5. Sender收到Receiver发送的数据传输请求响应报文(DTRFS)之后，应按照TDTF\_Cyclic=5ms周期发送数据传输报文(DTF)；
6. 如果Receiver在TDTF\_Wait\_Time=50ms内未收到数据传输的第一帧数据传输报文(DTF)，则认为此次数据传输失败；
7. Receiver收到的密文数据长度与数据传输请求报文（DTRF）中定义的一致，或超过50ms都没有再收到数据传输报文(DTF)，Receiver则认为Sender发送的数据传输报文(DTF)发送完成；
8. Receiver接收完所有的数据传输报文(DTF)之后，Receiver为IBTM时应在**TDTFS\_Time=950ms（**Receiver为TBOX时应在**TTFS\_Time=9500ms）**内发送数据传输响应报文(DTFS)，将结果反馈给Sender。
9. Sender在发送完数据传输报文(DTF)之后，sender为T-BOX时**TDTFS\_Wait\_Time=1000ms（**sender为IBTM时**TDTFS\_Wait\_Time=10000ms）**内未收到Receiver发送的数据传输响应报文(DTFS)，则认为数据传输失败，Sender应再次尝试重新传输请求，如累计尝试传输3次（从第1步开始），如果都未收到Receiver发送的数据传输响应报文(DTFS)，则Sender应停止自动重新向此Receiver传输数据，并记录相应的故障；
10. Sender接收反馈的结果为CRC错误时，应从第1步开始重新发送请求，如果Sender累计重复请求3次后，收到的反馈结果仍然为CRC错误，Sender应停止重新发送请求，并记录相应的故障。
11. Sender接收反馈的结果为接收超时，应从第1步开始重新发送请求，如果Sender累计重复请求3次后，收到的反馈结果仍然为接收超时，Sender应停止重新发送请求，并记录相应的故障；



1. 控制数据传输流程

## 反馈结果带数据密文传输流程

如图2所示，Sender需要往Receiver发送若干个字节长度的密文数据，Receiver在接收到Sender传输的数据后，将结果和结果相关的数据密文反馈给Sender，流程如下：

1. Sender给Receiver发送一个数据传输请求报文（DTRF）；
2. Receiver收到Sender数据传输请求报文（DTRF）之后，应在TDTRFS\_Time **=**40ms内发送一个数据传输请求响应报文(DTRFS)；
3. 如果Sender在TDTRFS\_Wait\_Time=50ms都未收到Receiver反馈的数据传输请求响应报文(DTRFS)，Sender应重新发送数据传输请求报文（DTRF）；
4. Sender重复请求5次后如果都未收到Receiver反馈的数据传输请求响应报文(DTRFS)，则Sender应停止自动重新向此Receiver发送数据传输请求报文（DTRF），并记录相应的故障；
5. Sender收到Receiver发送的数据传输请求响应报文(DTRFS)之后，应按照TDTF\_Cyclic=5ms周期发送数据传输报文(DTF)；
6. 如果Receiver在TDTF\_Wait\_Time=50ms内未收到数据传输的第一帧数据传输报文(DTF)，则认为此次数据传输失败；
7. Receiver收到的密文数据长度与数据传输请求报文（DTRF）中定义的一致，或超过50ms都没有再收到数据传输报文(DTF)，则认为Sender发送给Receiver的数据传输报文(DTF)发送完成；
8. Receiver接收完所有的数据传输报文(DTF)之后，Receiver为IBTM时应在**TDTFS\_Time=950ms（**Receiver为TBOX时应在**TTFS\_Time=9500ms）**内发送数据传输响应报文(DTFS)，将结果反馈给Sender；
9. Sender在发送完数据传输报文(DTF)之后，sender为T-BOX时**TDTFS\_Wait\_Time=1000ms（**sender为IBTM时**TDTFS\_Wait\_Time=10000ms）**内未收到Receiver发送的数据传输响应报文(DTFS)，则认为数据传输失败，Sender应再次尝试传输，如累计尝试传输3次（从第1步开始），如果都未收到Receiver发送的数据传输响应报文(DTFS)，则Sender应停止自动重新向此Receiver传输数据，并记录相应的故障；
10. Sender接收反馈的结果为CRC错误时，应从第1步开始重新发送请求，如果Sender累计重复请求3次后，收到的反馈结果仍然为CRC错误，Sender应停止重新发送请求，并记录相应的故障。
11. Sender接收反馈的结果为接收超时，应从第1步开始重新发送请求，如果Sender累计重复请求3次后，收到的反馈结果仍然为接收超时，Sender应停止重新发送请求，并记录相应的故障；
12. Sender收到Receiver的数据传输响应报文(DTFS)之后，应在TDTRFS\_Time **=**50ms内发送第一个数据传输请求响应报文(DTRFS)；
13. 如果Receiver在TDTRFS\_Wait\_Time=50ms都未收到Sender反馈的数据传输请求响应报文(DTRFS)，Receiver应重新发送数据传输响应报文(DTFS)；
14. Receiver重复发送发送数据传输响应报文(DTFS)5次后，如果都未收到Sender反馈的数据传输请求响应报文(DTRFS)，则Receiver应停止自动重新发送数据传输响应报文(DTFS)，并记录相应的故障；
15. Receiver收到Sender发送的数据传输请求响应报文(DTRFS)之后，应按照TDTF\_Cyclic=5ms周期发送数据传输报文(DTF)；
16. Sender收到的密文数据长度与数据传输请求报文（DTRF）中定义的一致，或超过50ms都没有再收到数据传输报文(DTF)，则认为Receiver发送给Sender的数据传输报文(DTF)发送完成；
17. Sender接收完所有的数据传输报文(DTF)之后，Sender为IBTM时应在**TDTFS\_Time=950ms（**Sender为T-BOX时应在**TTFS\_Time=9500ms）**内发送数据传输响应报文(DTFS)，将结果反馈给Receiver；
18. Receiver在发送完数据传输报文(DTF)之后，Receiver为T-BOX时**TDTFS\_Wait\_Time=1000ms（**Receiver为IBMT时**TDTFS\_Wait\_Time=10000ms）**内未收到Sender发送的数据传输响应报文(DTFS)，则认为数据传输失败，Receiver应再次尝试传输（从8步开始），如累计尝试传输3次，均都未收到Sender发送的数据传输响应报文(DTFS)，则Receiver应停止自动重新向此Sender传输数据，并记录相应的故障。
19. Sender接收反馈的结果为CRC错误时，应从第8步开始重新发送请求，如果Sender累计重复请求3次后，收到的反馈结果仍然为CRC错误，Sender应停止重新发送请求，并记录相应的故障。
20. Sender接收反馈的结果为接收超时，应从第8步开始重新发送请求，如果Sender累计重复请求3次后，收到的反馈结果仍然为接收超时，Sender应停止重新发送请求，并记录相应的故障；



1. 带密文反馈数据传输流程

# CRC校验算法

校验算法采用CRC-16/CCITT算法，初始值和异或值均为0x0000，多项式 POLY为0x1021，多项式为：X16 + X12 + X5 + 1,采用顺序异或计算多项式值。

**验证算法的参数：**

Byte1=0x1F,Byte2=0x50,Byte3=0x33,Byte4=0x35,Byte5=0x2C,Byte6=0x9C,Byte7=0x29;

CRC16\_value=0xAD42;

# 信号定义集合

## T-BOX→IBTM 报文列表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | CMD | 信号类型 | 信号定义 |
| 1 | 0x00 | 传输请求报文 | 0x00:请求传输数据 |
| 2 | 0xF0~0xFF | 传输请求响应报文 | 0xFF:允许传输报文（仅0xFF允许） |
| 0xFE:未联网 |
| 0xFD:任务处理中（本文其他传输数据处理中） |
| 0xFC:请求报文数据格式错误 |
| 0xF0~0xFB:预留 |
| 3 | 0x01-0x7F | 数据传输报文 | 0x01:第一帧数据  0x02:第二帧数据  0x03:第三帧数据  ... |
| 4 | 0x80~0x9F | 数据传输响应报文  命令ID  （携带Response ） | 0x80:车辆蓝牙信息上传 |
| 0x81:本地注销通知 |
| 0x82:离线删除通知 |
| 0x83:离线激活钥匙通知 |
| 0x84:IBTM用户证书申请请求 |
| 0x85:IBTM用户证书同步请求 |
| 0x86~0x9F:预留 |
| 5 | 0xA2~0xA3 | 反馈传输数据响应报文命令ID  （携带Response ） | 0xA2:查询所有钥匙 |
| 0xA3:查询特定钥匙  0xA4~0xEE:预留 |
| 6 | 0xEF | 未知业务传输数据异常响应命令  （携带Response ） | 0xEF：未知业务传输数据异常响应命令 |

|  |  |  |  |
| --- | --- | --- | --- |
| **TBOX发送** | **值** | **定义** | **备注** |
| Response | 0x00 | 无效 | CMD:0x80~0x85,0xA2、0xA3,0xEF通用 |
| 0x01 | 成功（TSP反馈成功） |
| 0x02 | 请求响应超时（预留） |
| 0x03 | 传输数据接收超时 |
| 0x04 | CRC错误 |
| 0x05 | 数据解析失败（解密后校验失败） |
| 0x06 | 信号异常（未定义信号） |
| 0x07 | 发送TSP失败 |
| 0x08 | TSP反馈超时 |
| 0x09 | TSP反馈失败 |

## IBTM→T-BOX发送报文列表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | CMD | 数据类型 | 信号定义 |
| 1 | 0x00 | 传输请求报文 | 0x00:请求传输数据 |
| 2 | 0xF0~0xFF | 传输请求响应报文 | 0xFF:允许传输报文（仅0xFF允许） |
| 0xFE:没有传输密钥（终端密钥） |
| 0xFD:任务处理中（本文其他传输数据处理中） |
| 0xFC:没有证书 |
| 0xFB:传输请求超时（适用于异步流程） |
| 0xF0~0xFA:其他 |
| 3 | 0x01-0x7F | 数据传输报文 | 0x01:第一帧数据  0x02:第二帧数据  0x03:第三帧数据  ... |
| 4 | 0x80~0xEE | 数据传输响应报文  响应命令ID  （携带response ） | 0xA1:注册 |
| 0xA2:查询所有钥匙【携带响应内容，见6.4.1】 |
| 0xA3:查询特定钥匙【携带响应内容，见6.4.2】 |
| 0xA4:删除某把钥匙 |
| 0xA5:删除所有钥匙 |
| 0xA6:修改有效期 |
| 0xA7:修改权限 |
| 0xA8:更新认证信息 |
| 0xA9:终端秘钥下发 |
| 0xAA：IBTM用户证书下发 |
| 0xAB~0xEE:预留 |
| 6 | 0xEF | 未知业务传输数据异常响应命令  （携带Response ） | 0xEF：未知业务传输数据异常响应命令 |

|  |  |  |  |
| --- | --- | --- | --- |
| **IBTM发送** | **值** | **含 义** | **备注** |
| Response | 0x00 | 无效 | CMD:  0xA1~0xAA,0xEF 通用 |
| 0x01 | 成功 |
| 0x02 | 请求响应超时（预留，本地记录故障） |
| 0x03 | 传输数据接收超时 |
| 0x04 | CRC错误 |
| 0x05 | 数据解析失败（解密后校验失败） |
| 0x06 | 信号异常（未定义信号） |
| 0x07 | 操作无效（时间戳异常，不在误差内） |
|  |  |
| 0x10~ |  | 适合CMD:  0xA1~0xA8，具体业务定义5.1~5.7 |

# IBTM反馈结果

## 注册结果反馈

|  |  |  |  |
| --- | --- | --- | --- |
| **CMD** | **Response** | **含 义** | **备 注** |
| 0xA1 | 0x00 | 无效 |  |
| 0x01 | 注册成功 |  |
| 0x02 | 请求响应超时（预留，本地记录故障） |  |
| 0x03 | 传输数据接收超时 |  |
| 0x04 | CRC错误 |  |
| 0x05 | 数据解析失败（解密后校验失败） |  |
| 0x06 | 信号异常（未定义信号） |  |
| 0x07 | 操作无效（时间戳异常，不在误差内） |  |
| 0x10 | 数据存储失败 |  |
| 0x11 | 数量已满（已注册10把钥匙） |  |
| 0x12 | 钥匙已存在 |  |

## 查询所有钥匙结果

|  |  |  |  |
| --- | --- | --- | --- |
| **CMD** | **Respond** | **含 义** | **备 注** |
| 0xA2 | 0x00 | 无效 |  |
| 0x01 | 有有效钥匙（为1时携带数据内容） |  |
| 0x02 | 请求响应超时（预留，本地记录故障） |  |
| 0x03 | 传输数据接收超时 |  |
| 0x04 | CRC错误 |  |
| 0x05 | 数据解析失败（解密后校验失败） |  |
| 0x06 | 信号异常（未定义信号） |  |
| 0x07 | 操作无效（时间戳异常，不在误差内） |  |
| 0x10 | 不存在（无有效钥匙） |  |

## 查询特定钥匙结果

|  |  |  |  |
| --- | --- | --- | --- |
| **CMD** | **Response** | **含 义** | **备 注** |
| 0xA3 | 0x00 | 无效 |  |
| 0x01 | 钥匙有效（为1时携带数据内容） |  |
| 0x02 | 请求响应超时（预留，本地记录故障） |  |
| 0x03 | 传输数据接收超时 |  |
| 0x04 | CRC错误 |  |
| 0x05 | 数据解析失败（解密后校验失败） |  |
| 0x06 | 信号异常（未定义信号） |  |
| 0x07 | 操作无效（时间戳异常，不在误差内） |  |
| 0x10 | 钥匙不存在 |  |
| 0x11 | 钥匙已失效 |  |

## 删除特定钥匙结果反馈

|  |  |  |  |
| --- | --- | --- | --- |
| **CMD** | **Response** | **含 义** | **备 注** |
| 0xA4 | 0x00 | 无效 |  |
| 0x01 | 删除成功 |  |
| 0x02 | 请求响应超时（预留，本地记录故障） |  |
| 0x03 | 传输数据接收超时 |  |
| 0x04 | CRC错误 |  |
| 0x05 | 数据解析失败（解密后校验失败） |  |
| 0x06 | 信号异常（未定义信号） |  |
| 0x07 | 操作无效（时间戳异常，不在误差内） |  |
| 0x10 | 钥匙不存在 |  |
| 0x11 | 钥匙已失效 |  |
| 0x12 | 钥匙删除失败 |  |
| 0x13 | 不满足删除条件（钥匙使用中） |  |

## 删除所有钥匙结果反馈

|  |  |  |  |
| --- | --- | --- | --- |
| **CMD** | **Response** | **含 义** | **备 注** |
| 0xA5 | 0x00 | 无效 |  |
| 0x01 | 删除成功 |  |
| 0x02 | 请求响应超时（预留，本地记录故障） |  |
| 0x03 | 传输数据接收超时 |  |
| 0x04 | CRC错误 |  |
| 0x05 | 数据解析失败（解密后校验失败） |  |
| 0x06 | 信号异常（未定义信号） |  |
| 0x07 | 操作无效（时间戳异常，不在误差内） |  |
| 0x10 | 没有有效钥匙 |  |
| 0x11 | 钥匙删除失败 |  |

## 修改期限结果反馈

|  |  |  |  |
| --- | --- | --- | --- |
| **CMD** | **Response** | **含 义** | **备 注** |
| 0xA6 | 0x00 | 无效 |  |
| 0x01 | 修改成功 |  |
| 0x02 | 请求响应超时（预留，本地记录故障） |  |
| 0x03 | 传输数据接收超时 |  |
| 0x04 | CRC错误 |  |
| 0x05 | 数据解析失败（解密后校验失败） |  |
| 0x06 | 信号异常（未定义信号） |  |
| 0x07 | 操作无效（时间戳异常，不在误差内） |  |
| 0x10 | 钥匙不存在 |  |
| 0x11 | 钥匙已失效 |  |
| 0x12 | 期限异常（到期时间<当前时间） |  |

## 修改权限结果反馈

|  |  |  |  |
| --- | --- | --- | --- |
| **CMD** | **Response** | **含 义** | **备 注** |
| 0xA7 | 0x00 | 无效 |  |
| 0x01 | 修改成功 |  |
| 0x02 | 请求响应超时（预留，本地记录故障） |  |
| 0x03 | 传输数据接收超时 |  |
| 0x04 | CRC错误 |  |
| 0x05 | 数据解析失败（解密后校验失败） |  |
| 0x06 | 信号异常（未定义信号） |  |
| 0x07 | 操作无效（时间戳异常，不在误差内） |  |
| 0x10 | 钥匙不存在 |  |
| 0x11 | 钥匙已失效 |  |

## 更新钥匙结果反馈

|  |  |  |  |
| --- | --- | --- | --- |
| **CMD** | **Response** | **含 义** | **备 注** |
| 0xA8 | 0x00 | 无效 |  |
| 0x01 | 更新成功 |  |
| 0x02 | 请求响应超时（预留，本地记录故障） |  |
| 0x03 | 传输数据接收超时 |  |
| 0x04 | CRC错误 |  |
| 0x05 | 数据解析失败（解密后校验失败） |  |
| 0x06 | 信号异常（未定义信号） |  |
| 0x07 | 操作无效（时间戳异常，不在误差内） |  |
| 0x10 | 钥匙不存在 |  |
| 0x11 | 钥匙已失效 |  |

## 终端秘钥下发结果反馈

|  |  |  |  |
| --- | --- | --- | --- |
| **CMD** | **Response** | **含 义** | **备 注** |
| 0xA9 | 0x00 | 无效 |  |
| 0x01 | 下发成功 |  |
| 0x02 | 请求响应超时（预留，本地记录故障） |  |
| 0x03 | 传输数据接收超时 |  |
| 0x04 | CRC错误 |  |
| 0x05 | 数据解析失败（预留） |  |
| 0x06 | 信号异常（未定义信号） |  |
| 0x07 | 操作无效（时间戳异常，不在误差内） |  |
| 0x10 | 存储失败 |  |
| 0x11 | 验签失败 |  |
| 0x12 | 公钥证书验证失败 |  |
| 0x13 | 解密失败 |  |

## IBTM用户证书下发结果反馈

|  |  |  |  |
| --- | --- | --- | --- |
| **CMD** | **Response** | **含 义** | **备 注** |
| 0xAA | 0x00 | 无效 |  |
| 0x01 | 下发成功 |  |
| 0x02 | 请求响应超时（预留，本地记录故障） |  |
| 0x03 | 传输数据接收超时 |  |
| 0x04 | CRC错误 |  |
| 0x05 | 数据解析失败（预留） |  |
| 0x06 | 信号异常（未定义信号） |  |
| 0x07 | 操作无效（时间戳异常，不在误差内） |  |
| 0x10 | 存储失败 |  |
| 0x11 | 证书不合法（与私钥不匹配） |  |
| 0x12 | 预置的CA证书异常（没有or不可用） |  |

# 传输数据内容

## 数据格式

### 传输数据格式

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Item** | 传输数据内容 | | | | |
| **SCMD** | **Length** | Time | Data | CMAC |
| Length(B) | 1 | 2 | 4 |  | 4 |
| Description | 见4.1.5描述 | Time+Data长度 | 发送指令时间 | 业务数据内容 | 消息认证码(可选) |

SCMD指蓝牙钥匙相关业务命令，详见6.3中定义；

Length指Time+Data 区域数据长度；

Time 指发送这条报文的时间；

Data指具体业务携带的附加内容，详见6.4、6.5中定义；

CAMC：当传输数据需要加密传输时，需携带该校验码，对传输数据明文“SCMD+Length+Time+Data ”生成4byte的消息认证码。

注：AES128-CMAC截取前4个字节

### 反馈传输数据格式

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | 反馈传输数据内容 | | | |
| **Length** | Time | Data | CMAC |
| Length(B) | 2 | 4 |  | 4 |
| Description | Time+Data长度 | 发送指令时间 | 业务数据内容 | 消息认证码（可选） |

Length指Time+Data 区域数据长度；

Time 指发送这条报文的时间；

Data指具体业务携带的附加内容，详见6.6中定义；

CAMC：当反馈传输数据需要加密传输时，需携带该校验码，对反馈传输数据明文“Length+Time+Data ”生成4byte的消息认证码。

注：AES128-CMAC截取前4个字节

### 数据类型

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Item** | **SCMD** | **Length** | **time** | **UID** | **BTID** | **Type** | **KeyInfo** | **Startime** | **Endtime** | **Functionlist** |
| Data type | Unsigned char | Unsigned short | Unsigned int | Unsigned long | Unsigned long | Unsigned char | Unsigned char[16] | Unsigned int | Unsigned int | Unsigned long |
| Length(B) | 1 | 2 | 4 | 8 | 8 | 1 | 16 | 4 | 4 | 8 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Item** | **Authcode** | **MAC** | **HardConfig** | **PartNumber** | **SerialNumber** | **[Software Version](http://www.baidu.com/link?url=9Sx2T3oFD96uOTznzbW-Cr9BiK2KeuuEoQO4Wu9ubOzyKGADodEEGQOTPANEv5bgl7VkBlj2PeDZ172_Nj_fAbh8Yj1DGxfhjS8wLHaz86y1OhZZz2vyhGFdA6RyOFXe" \t "https://www.baidu.com/_blank)** |
| Data type | Unsigned int | Unsigned char[6] | Unsigned char | Unsigned char[13] | Unsigned char[10] | Unsigned char[6] |
| Length(B) | 4 | 6 | 1 | 13 | 10 | 6 |

|  |  |  |
| --- | --- | --- |
| **Item** | **CMAC** | **VIN** |
| Data type | Unsigned int | Unsigned char[17] |
| Length(B) | 4 | 17 |

### 分帧传输帧数

1. 需加密传输时，传输数据长度为M（传输数据M=length+3，反馈传输数据M=length+2），不分帧帧数为N，若M为7的整数倍，N=M/7，否则N=M/7+1；
2. 需加密传输时，传输数据长度为M（传输数据M=length+7，反馈传输数据M=length+6），加密密文长度M’ =(M/16+1)\*16，分帧帧数为N，若M’ 为7的整数倍，N=M’ /7，否则N=M’/7+1。

## 业务命令SCMD

### T-BOX→IBTM

* SCMD+DATA 数据AES128加密后传输；
* TBOX->IBTM业务命令**SCMD**定义与IBTM反馈的CMD相同：
* SCMD data type:unsigned char

|  |  |  |
| --- | --- | --- |
| **SCMD** | **含义** | **数据内容** |
| 0xA1 | 注册 | 见6.3.1 |
| 0xA2 | 查询所有钥匙 | 见6.3.2 |
| 0xA3 | 查询特定钥匙 | 见6.3.3 |
| 0xA4 | 删除特定钥匙 | 见6.3.4 |
| 0xA5 | 删除所有钥匙 | 见6.3.5 |
| 0xA6 | 修改有效期 | 见6.3.6 |
| 0xA7 | 修改权限 | 见6.3.7 |
| 0xA8 | 更新认证信息 | 见6.3.8 |
| 0xA9 | 终端秘钥下发 | 见6.3.9 |
| 0xAA | IBTM用户证书下发 | 见6.3.10 |

### IBTM→T-BOX

* SCMD+DATA 数据可以直接传输；
* IBTM->T-BOX业务命令**SCMD**定义与T-BOX反馈的CMD相同：

|  |  |  |
| --- | --- | --- |
| **SCMD** | **含义** | **数据内容** |
| 0x80 | 车辆蓝牙信息上传 | 见6.4.1 |
| 0x81 | 本地注销通知 | 见6.4.2 |
| 0x82 | 离线激活通知 | 见6.4.3 |
| 0x83 | 离线删除通知 | 见6.4.4 |
| 0x84 | IBTM用户证书申请请求 | 见6.4.5 |
| 0x85 | IBTM用户证书同步请求 | 见6.4.6 |

注：6.3、6.4 、6.5章节为业务传输内容汇总，具体参考需求规格书文档中的描述。

若定义传输数据加密，还需求携带CMAC。

## T-BOX 发送SCMD数据内容

### 注册（加密）

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Item** | **SCMD** | **Length** | **time** | **UID** | **BTID** | **Type** | **KeyInfo** | **Startime** | **Endtime** | **Functionlist** |
| Length(B) | 1 | 2 | 4 | 8 | 8 | 1 | 16 | 4 | 4 | 8 |
| Description | 0xA1 | 0x35 | 发送命令时间 | 标识账户的唯一ID | 钥匙唯一编号 | 表示不同属性的钥匙 | 钥匙机密信息 | 该钥匙生效时间 | 该钥匙失效时间 | 该钥匙可以控车的功能权限列表 |

### 查询所有钥匙 （加密）

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **SCMD** | **Length** | **time** |
| Length(B) | 1 | 2 | 4 |
| Description | 0xA2 | 0x04 | 发送命令时间 |

### 查询特定钥匙 （加密）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **SCMD** | **Length** | **time** | **BTID** |
| Length(B) | 1 | 2 | 4 | 8 |
| Description | 0xA3 | 0x0C | 发送命令时间 | 钥匙唯一编号 |

### 删除特定钥匙（加密）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **SCMD** | **Length** | **time** | **BTID** |
| Length(B) | 1 | 2 | 4 | 8 |
| Description | 0xA4 | 0x0C | 发送命令时间 | 钥匙唯一编号 |

### 删除所有钥匙（加密）

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **SCMD** | **Length** | **time** |
| Length(B) | 1 | 2 | 4 |
| Description | 0xA5 | 0x04 | 发送命令时间 |

### 修改有效期 （加密）

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Item** | **SCMD** | **Length** | **time** | **BTID** | **Startime** | **Endtime** |
| Length(B) | 1 | 2 | 4 | 8 | 4 | 4 |
| Description | 0xA6 | 0x14 | 发送命令时间 | 钥匙唯一编号 |  |  |

### 修改权限（加密）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Item** | **SCMD** | **Length** | **time** | **BTID** | **Functionlist** |
| Length(B) | 1 | 2 | 4 | 8 | 8 |
| Description | 0xA7 | 0x14 | 发送命令时间 | 钥匙唯一编号 |  |

### 更新认证信息（加密）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Item** | **SCMD** | **Length** | **time** | **BTID** | **KeyInfo** |
| Length(B) | 1 | 2 | 4 | 8 | 16 |
| Description | 0xA8 | 0x1C | 发送命令时间 | 钥匙唯一编号 |  |

### 终端秘钥下发（不加密）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Item** | **SCMD** | **Length** | **time** | **终端秘钥** | **数字签名** |
| Length(B) | 1 | 2 | 4 | 256 | 不固定（1K~2K） |
| Description | 0xA9 | xx | 发送命令时间 | 终端密钥密文 | 携带公钥证书 |

### IBTM用户证书下发（不加密）

注：申请和同步请求返回的证书文件都不加密

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **SCMD** | **Length** | **time** | **IBTM用户证书** |
| Length(B) | 1 | 2 | 4 | 不固定（1K~2K） |
| Description | 0xAA | xx | 发送命令时间 |  |

## IBTM 发送SCMD数据内容

### 车辆蓝牙信息上传（加密）

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Item** | **SCMD** | **Length** | **time** | **MAC** | **HardConfig** | **PartNumber** | **SerialNumber** | **[Software Version](http://www.baidu.com/link?url=9Sx2T3oFD96uOTznzbW-Cr9BiK2KeuuEoQO4Wu9ubOzyKGADodEEGQOTPANEv5bgl7VkBlj2PeDZ172_Nj_fAbh8Yj1DGxfhjS8wLHaz86y1OhZZz2vyhGFdA6RyOFXe" \t "https://www.baidu.com/_blank)** |
| Length(B) | 1 | 2 | 4 | 6 | 1 | 13 | 10 | 13 |
| Description | 0x80 | 0x28 |  | 蓝牙地址 | 0：无效 1：没有蓝牙钥匙 2：蓝牙天线（1） 3：蓝牙天线（1+3） 4：蓝牙天线（1+5） 5：蓝牙天线（1+6） |  |  | 软件版本 |

### 本地注销通知 （加密）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Item** | **SCMD** | **Length** | **time** | **BTID** | **ExpiredTime** |
| Length(B) | 1 | 2 | 4 | 8 | 4 |
| Description | 0x81 | 0x10 | 发送命令时间 | 钥匙唯一编号 | 注销时间 |

### 离线激活通知（加密）

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Item** | **SCMD** | **Length** | **time** | **Authcode** | **UID** | **BTID** | **Type** | **ActTime** |
| Length(B) | 1 | 2 | 4 | 4 | 8 | 8 | 1 | 4 |
| Description | 0x82 | 0x1D | 发送命令时间 | 授权码 |  | 钥匙唯一编号 |  | 激活时间 |

### 离线删除通知（加密）

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Item** | **SCMD** | **Length** | **time** | **UID** | **BTID** | **DeletedTime** |
| Length(B) | 1 | 2 | 4 | 8 | 8 | 4 |
| Description | 0x83 | 0x18 | 发送命令时间 |  | 钥匙唯一编号 |  |

### IBTM用户证书申请请求（不加密）

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Item** | **SCMD** | **Length** | **time** | **VIN** | **PartNumber** | **SerialNumber** | CSR |
| Length(B) | 1 | 2 | 4 | 17 | 13 | 10 | 不固定（0.8k-1k） |
| Description | 0x84 | xx | 命令发送时间 | 车架号 | 组合成设备ID | | 证书请求文件 |

### IBTM用户证书同步请求（加密）

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **SCMD** | **Length** | **time** |
| Length(B) | 1 | 2 | 4 |
| Description | 0x85 | 0x04 | 命令发送时间 |

## 查询结果返回

注：此章节为反馈传输数据内容

### 6.5.1查询特定钥匙（加密）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Length** | **time** | **BTID** | **Type** |
| Length(B) | 2 | 4 | 8 | 1 |
| Description | 0x0D |  |  |  |

### 6.5.2查询所有钥匙（加密）

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Item** | **Length** | **time** | **Num** | **BTID1** | **Type** | **BTIDn** | **Type** |
| Length(B) | 2 | 4 | 1 | 8 | 1 | 8 | 1 |
| Description | 5+9\*N |  | N |  |  |  |  |

# 数据传输举例

## 注册

**1.传输请求（ TBOX->IBTM ）**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| BYTE | BYTE0 | BYTE1 | BYTE2 | BYTE3 | BYTE4 | BYTE5 | BYTE6 | BYTE7 |
| Item | **0** | 64(传输密文长度) | | 0 | 0 | 0 | CRC16 | |

**2.传输请求响应报文（ IBTM->TBOX ）**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| BYTE | BYTE0 | BYTE1 | BYTE2 | BYTE3 | BYTE4 | BYTE5 | BYTE6 | BYTE7 |
| Item | **0xFF**:允许传输 | 0 |  | 0 | 0 | 0 | 0 | 0 |

**3.数据传输（ TBOX->IBTM ）**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| BYTE | BYTE0 | BYTE1 | BYTE2 | BYTE3 | BYTE4 | BYTE5 | BYTE6 | BYTE7 |
| Item | 1(第一帧) | Data1(明文中 SCMD：0xA2) | Data2 | Data3 | Data4 | Data5 | Data6 | Data7 |
| ... | ... | ... | ... | ... | ... | ... | ... |
| 9(第九帧) | Data57 | Data58 | Data59 | Data60 | Data61 | Data62 | Data63 |
| 10(第十帧) | Data64 | 0 | 0 | 0 | 0 | 0 | 0 |

**4.数据传输响应报文（ IBTM->TBOX ）**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| BYTE | BYTE0 | BYTE1 | BYTE2 | BYTE3 | BYTE4 | BYTE5 | BYTE6 | BYTE7 |
| Item | 0xA1:注册结果反馈 | Response | 0 | | 0 | 0 | 0 | |

## 查询所有钥匙

**1.传输请求（ TBOX->IBTM ）**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| BYTE | BYTE0 | BYTE1 | BYTE2 | BYTE3 | BYTE4 | BYTE5 | BYTE6 | BYTE7 |
| Item | 0 | 16 | | 0 | 0 | 0 | CRC16 | |

**2.传输请求响应报文（ IBTM->TBOX ）**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| BYTE | BYTE0 | BYTE1 | BYTE2 | BYTE3 | BYTE4 | BYTE5 | BYTE6 | BYTE7 |
| Item | 0xFF:允许传输 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**3.数据传输（ TBOX->IBTM ）**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| BYTE | BYTE0 | BYTE1 | BYTE2 | BYTE3 | BYTE4 | BYTE5 | BYTE6 | BYTE7 |
| Item | 1 | Data1 | Data2 | Data3 | Data4 | Data5 | Data6 | Data7 |
| 2 | Data8 | Data9 | Data10 | Data11 | Data12 | Data13 | Data14 |
| 3 | Data15 | Data16 | 0 | 0 | 0 | 0 | 0 |

**4.数据传输响应报文（携带反馈传输请求（ IBTM->TBOX ）**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| BYTE | BYTE0 | BYTE1 | BYTE2 | BYTE3 | BYTE4 | BYTE5 | BYTE6 | BYTE7 |
| Item | 0xA2:查询所有钥匙 | 1：成功（为1时才有后面的内容） | M=5+ 9\*N | | 1 | 0 | CRC16 | |

**5.传输请求响应报文（ TBOX->IBTM ）**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| BYTE | BYTE0 | BYTE1 | BYTE2 | BYTE3 | BYTE4 | BYTE5 | BYTE6 | BYTE7 |
| Item | 0xFF:允许传输 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**6.数据传输（ IBTM->TBOX ）**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| BYTE | BYTE0 | BYTE1 | BYTE2 | BYTE3 | BYTE4 | BYTE5 | BYTE6 | BYTE7 |
| Item | 1 | Data1 | Data2 | Data3 | Data4 | Data5 | Data6 | Data7 |
| 2 | ... |  |  |  |  |  |  |
| 3 | DataM |  |  |  |  |  |  |

**7.反馈数据传输响应报文（ TBOX->IBTM ）**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| BYTE | BYTE0 | BYTE1 | BYTE2 | BYTE3 | BYTE4 | BYTE5 | BYTE6 | | BYTE7 |
| Item | 0xA2:查询所有钥匙 | Response | 0 | 0 | 0 | 0 | 0 | 0 | |