ICS 43.040.10
CCS T 35

团 体 标 准

T/CTS 11—2023

汽车记录仪数据安全芯片技术要求

Technical requirements of data security chip for data recorder of vehicle

2023-3-1 发布　　2023-3-1 实施

中国道路交通安全协会　发布

目　　次

前　言

本文件按照《团体标准结构和编写指南》T/CAS 1.1—2017要求并参照《标准的结构和编写》GB/T 1.1-2020给出的规则起草。

本文件可能涉及专利，本文件的发布机构不承担识别专利的责任。

本文件由中国道路交通安全协会提出并归口管理。

本文件起草单位：北京中软政通信息技术有限公司、中国安全技术防范认证中心、江苏都万电子科技有限公司、杭州中导元生科技开发有限公司、北京工业大学、湖北民族大学、浙江省北斗卫星应用产业协会、杭州海康汽车技术有限公司、深圳市锐明技术股份有限公司。

本文件主要起草人：王东、朱峻涛、陈烨、尚洋、刘剑锋、林万才、李明伟、周煊华、张鑫、安宁、叶文宇、陈艳艳、郑明辉、孙方华、霍孟浩、孙继业。

本文件为首次发布。

引　言

汽车记录仪的数据安全是记录数据可用、可靠、可信的技术保证，汽车记录仪要实现记录数据防删除、防伪造、防篡改的安全性能要求，就必须对原始记录数据进行加密存储或进行具备时间标签特性的加密数字签名进行验证，同时对存储记录数据的存储器进行必要的防删除保护。这就要求汽车记录仪本身要具备实现这些数据安全功能的安全边界，而采用特定功能的安全芯片是建立高等级安全边界并实现数据安全功能性价比最优的技术手段和通行做法。同时数据安全芯片也可以为汽车记录仪本身的联网安全、系统安全和软件安全提供高等级安全边界的技术手段。

汽车记录仪数据安全芯片的安全功能采用自主可控的国家商用密码算法（SM1、SM2、SM3、SM4等）序列来实现，同时兼容国际通用的安全算法。对推广我们国家商用密码算法的普遍应用、普及和落实《中华人民共和国密码法》具有重要的意义。

汽车记录仪数据安全芯片技术要求

1 范围

本文件规定了适用汽车记录仪的数据安全芯片的一般要求、功能要求、性能要求、试验方法和包装。

本文件适用于安装在车辆上的各类汽车记录仪的数据安全芯片的设计、制造和使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 18030 信息技术 中文编码字符集

GB/T 12750 半导体器件 集成电路 第11部分：半导体集成电路分规范（不包括混合电路）

GB/T 19056 汽车行驶记录仪

GB/T 32918 信息安全技术 SM2椭圆曲线公钥密码算法（所有部分）

GM/T 0008 安全芯片密码检测准则

T/CTS 12 汽车行驶记录仪联网通信技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

汽车记录仪 data recorder of vehicle

装载在各种车辆上用于记录车辆行驶过程数据的电子装置，包括汽车行驶记录仪、汽车事件记录仪、车载视频记录系统等。

3.2

数据安全芯片 data security chip

含有密码算法、安全功能，可实现密钥管理机制、算法执行、数据安全存储及通信功能的集成电路芯片。

3.3

上行传输 upload

由汽车记录仪发出的，通过无线公共通信网络发送到远程网络设备或计算机的数据传输方式。

3.4

下行传输 download

由远程网络设备或计算机发出的，通过无线公共通信网络发送到汽车记录仪的数据传输方式。

3.5

生命周期 life cycle

汽车记录仪设备从生产、出厂、预装、安装、运行、维修、报废使用的可追溯全过程。

3.6

SM1 算法 SM1 algorithm

商用密码算法中的一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

3.7

SM2 算法 SM2 algorithm

商用密码算法中的一种椭圆曲线公钥密码算法，其私钥长度为 256 比特。

3.8

SM3 算法 SM3 algorithm

商用密码算法中的一种密码杂凑算法，其输出为 256 比特。

3.9

SM4 算法 SM4 algorithm

商用密码算法中的一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

4 缩略语

下列缩略语适用于本文件。

AES：高级加密标准（Advanced Encryption Standard）
SHA：安全哈希算法（secure hash algorithm）
RSA：一种非对称密码算法（由Rivest、Shamir和Adleman开发，取名来自三者的名字）
BCD：二进码十进数（Binary-Coded Decimal）
UART：通用异步收发传输器（Universal Asynchronous Receiver/Transmitter）
I2C：二线制同步串行主从通信总线（Inter Integrated Circuit）
CRC：循环冗余校验（cyclic redundancy check）
CBC：密文分组链接方式（cipher block chaining）
IV：初始化向量（initialization vector）
PKCS：公钥密码学标准 (Public Key Cryptography Standards)
ID：标识（Identity）
ASC：美国信息交换标准代码（American Standard Code for Information Interchange）
BIN：二进制（Binary）
RTC：实时时钟（Real Time Clock）
PPS：秒脉冲（Pulse Per Second）
GNSS：全球导航卫星系统（Global Navigation Satellite System）
CAN：控制器局域网络（Controller Area Network）

5 一般要求

5.1 外观要求

数据安全芯片（以下简称“芯片”）的封装可以采用常见封装，也可以订制封装形式，外形不大于 10 mm × 10 mm × 2 mm，芯片表面应至少标识型号、生产日期标识、产品流水号。

5.2 通信接口要求

对外通信接口应使用常用通信接口，应至少支持UART、I2C和ISO7816（智能卡（芯片）通信接口）接口的一种或几种。

6 功能要求

6.1 加密与解密

6.1.1 数据安全芯片的加密与解密应支持以下算法

a) 对称加密与解密算法 SM1、SM4 和 AES；
b) 非对称加密与解密算法 SM2、RSA。

6.1.2 数据安全芯片的加密与解密功能应支持以下方式

a) 对称加密与解密过程采用 CBC 模式，CBC 的初始化向量 IV 为 00H（所有数据字节为 00H）；
b) 对称加密的源数据需要填充时，无特定要求的采用 PKCS7；
c) 非对称加密的源数据需要填充时，无特定要求的采用 PKCS1；
d) 按数字证书的密钥和算法加密或解密源数据；
e) 按给定密钥和算法要求加密或解密源数据。

6.2 数字签名及验签

6.2.1 数据安全芯片的数字签名和验签应支持以下算法

a) 数据摘要算法 SM3、SHA；
b) 签名和验签算法 SM2、RSA。

6.2.2 数据安全芯片的签名和验签功能应符合以下要求

a) 按数字证书的密钥和算法对源数据进行签名；
b) 按给定的密钥和算法对源数据进行签名；
c) 按数字证书的密钥和算法对源数据及其签名数据进行验签；
d) 按给定的密钥和算法对源数据及其签名数据进行验签；
e) 数字签名格式应符合附录 A 表 A.8 的要求；
f) SM2 签名算法的可辨别标识 ID 为“T/CTS”；
g) 以汽车记录仪的记录仪编号、芯片时间、数字证书为参数生成设备实时验证码（6 位数字）。

6.2.3 应用于汽车行驶记录仪的数据安全芯片的数据记录块验证功能应符合以下要求

a) 用于生成验证记录块的 Salt 值应存储在数据安全芯片内部；
b) Salt 值经设置后不可修改；
c) 按给定的数据和 SM3 算法对源数据附加 Salt 值后生成验证数据。

6.3 数字证书

数据安全芯片的数字证书功能应符合以下要求：

a) 数据安全芯片支持的数字证书分类和更新、删除权限见附录 A 表 A.6；
b) 数据安全芯片支持的数字证书格式见附录 A 表 A.7。

6.4 实时时钟

数据安全芯片的实时时钟应满足以下要求：

a) 应内置实时时钟，除电源外，实时时钟的运行不依赖外部元器件；
b) 应记录实时时钟的末段时间点（精确到分钟），当数据安全芯片外部所有电源失效后重新上电运行时，实时时钟应从末段时间点开始，时间的年、月、日、时、分数值不应发生改变；
c) 数据安全芯片应能检测外部所有电源失效引起的时钟停振，并记录时钟停振次数；
d) 数据安全芯片应具备通过卫星导航系统的时间数据进行自动对时及通过通信接口进行外部对时的时间校准的功能；
e) 进行任何方式的时间校准，向后对时（时间倒退）的时间跨度应不大于 60 秒，且在连续的 24 小时内只能进行一次。

6.5 存储器保护

6.5.1 数据安全芯片的存储器保护功能应符合以下要求

a) 数据安全芯片应保存存储器初始化时给出的存储器写保护解锁密钥；
b) 数据安全芯片生成的单次写保护解锁数据应至少包含解锁轮次、解锁时间、随机数据，并支持包含设备给出的存储器型号。

6.5.2　存储器保护初始化流程见图 1

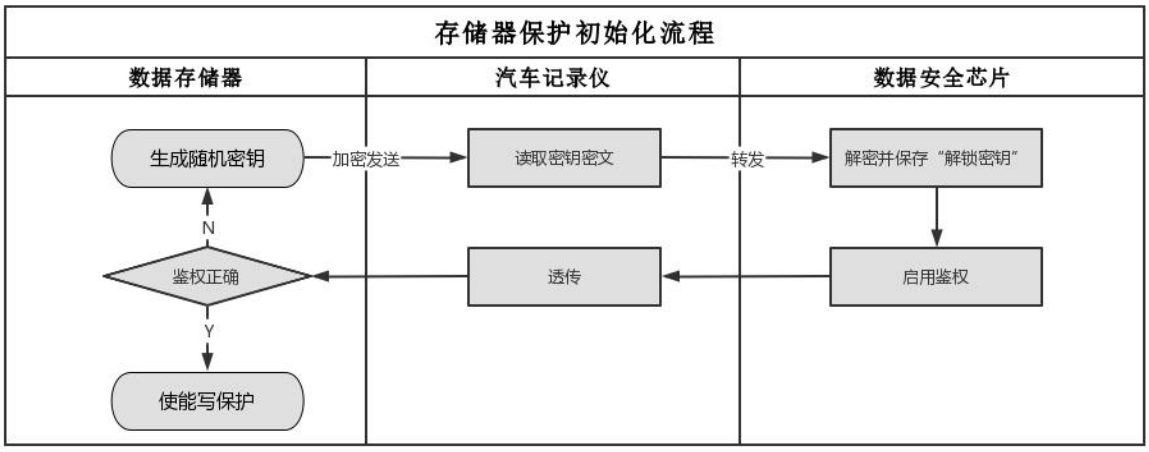

图 1　存储器保护初始化流程示意图

6.5.3　存储器保护单次解锁流程见图 2

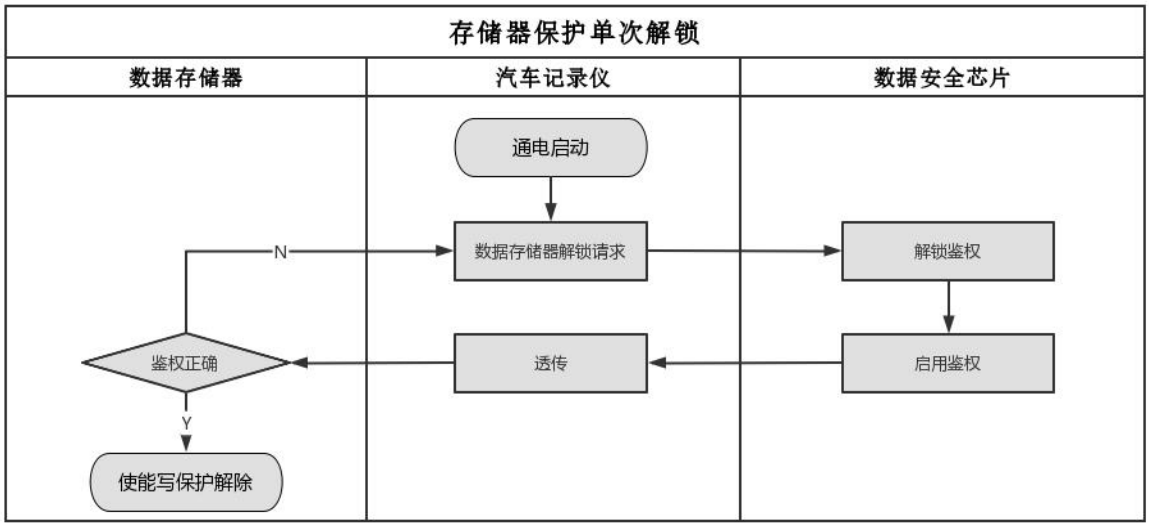

图 2　存储器保护单次解锁流程示意图

6.6　联网双向鉴权

6.6.1　数据安全芯片支持汽车记录仪的联网鉴权功能应符合以下要求

a)　数据安全芯片发起的联网鉴权数据应至少包含鉴权轮次、鉴权时间、随机数据；
b)　数据安全芯片发起的联网鉴权数据应支持包含汽车记录仪给出的特定数据；
c)　数据安全芯片应保存数字证书对应的鉴权轮次。

6.6.2　联网双向鉴权流程见图 3

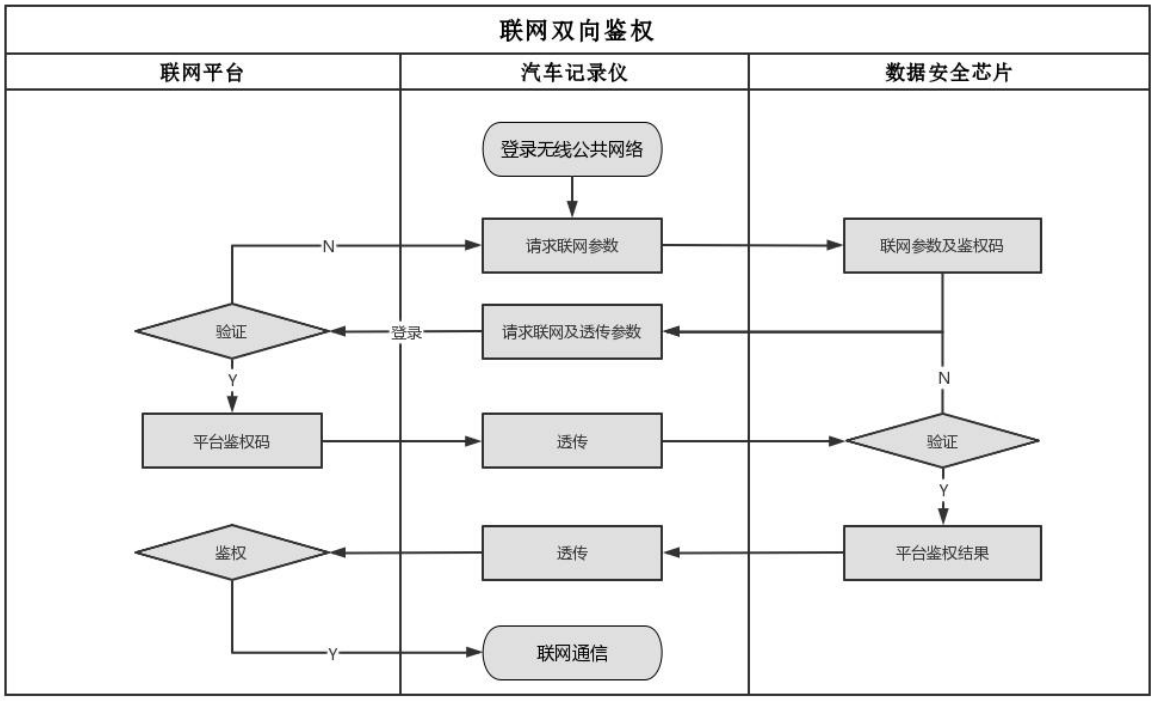

图 3　联网双向鉴权流程示意图

6.7　运行安全保护

数据安全芯片应支持汽车记录仪的软件功能安全、软件升级安全、车载总线安全，宜支持汽车记录仪的软件代码安全和车辆控制安全。

6.7.1　数据安全芯片应支持设备的运行安全保护的能力，并符合以下要求

a）　应至少具备 1 路用于汽车记录仪软件功能安全的功能模块使能信号输出，该输出在数据安全芯片上电后应处于使能无效状态，输出应具备有效输出极性定义和控制方式定义的功能；

b）　应至少具备 1 路用于汽车记录仪软件升级安全的软件代码芯片写保护信号输出，该输出在数据安全芯片上电后应处于保护使能状态，输出应具备有效输出极性定义和控制方式定义的功能；

c）　应至少具备 1 路用于支持车载总线安全的总线发送使能信号输出，该输出在数据安全芯片上电后应处于发送禁止状态，输出应具备有效输出极性定义和控制方式定义的功能；

d）　宜具备用于支持远程控制安全的控制执行模块使能信号输出，该输出在数据安全芯片上电后应处于控制无效状态，输出应具备有效输出极性定义和控制方式定义的功能；

e）　宜具备用于汽车记录仪软件代码安全（软件代码不被非法途径读取）的软件代码芯片片选使能信号输出，该输出信号在数据安全芯片上电后应处于使能有效且经过指定时间后变为使能无效，输出信号应具备有效输出极性定义和控制方式定义的功能。

6.7.2 汽车记录仪运行安全支持的连接见图 4

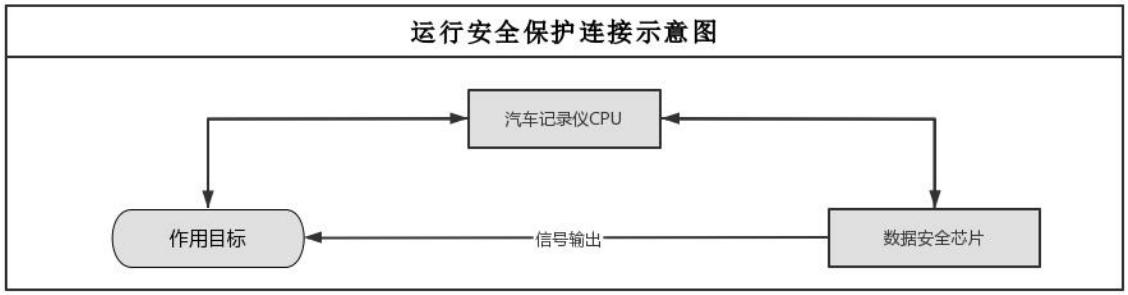

图 4 运行安全保护连接示意图

6.8 汽车行驶记录仪安装自检

应用在汽车行驶记录仪的数据安全芯片应具备安装自检功能，且符合以下要求：

a) 数据安全芯片应至少具备 6 路的开关量输入信号，输入信号应包括点火开关、制动踏板、车速脉冲、安全带、左转向、右转向信号；
b) 任意未被设置为检测屏蔽（见表 A.26）的输入信号在汽车行驶记录仪连续运行的 24 小时内未发生信号变化，开关量信号故障状态信息（见表 A.25）对应的标识位应被标识为故障；
c) 数据安全芯片应能接收和解析卫星定位数据，连续运行的 24 小时内卫星定位持续无效，记录仪（芯片）状态字（见表 A.12）对应的标识位应被标识为故障。

6.9 汽车行驶记录仪管理

6.9.1 应用在汽车行驶记录仪的数据安全芯片应具备管理功能

a) 数据安全芯片应存储汽车行驶记录仪的唯一性编号和数据摘要 Salt 值等关键参数，并符合 GB/T 19056 数据安全性的要求；
b) 数据安全芯片应保存汽车行驶记录仪的设备生命周期状态，状态包括：生产检验、出厂待装、车辆预装、安装准备、安装自检、正式运行、返厂维修、设备报废等状态；
c) 数据安全芯片应具备将产品生命周期状态信息、产品故障信息通过外部处理器及与之相连的联网通信模块发送到联网平台的功能；
d) 数据安全芯片在“生产检验”状态下可以设置生产检验用 VIN 号和车牌号码，VIN 号宜设为“TESTXXXXXXXXXXXXX”格式，车牌号码宜设为“检 X-XXXXX”，机动车电子标识序列号宜设为“99XXXXXXXXX-X”；
e) 数据安全芯片在转为“出厂待装（3H）”状态时，应删除生产检验用 VIN 号、车牌号码、机动车电子标识序列号，转为未设置状态；
f) 数据安全芯片在“车辆预装（4H）”状态下可以设置车辆 VIN 号；
g) 数据安全芯片未设置 VIN、车牌号码、电子标识序列号信息的，在“安装准备（5H）”状态下可设置对应信息；
h) 数据安全芯片未设置 VIN 号的，“安装自检（6H）”完成（无故障）状态下可以设置 VIN 号，VIN 号一经设置，仅允许修改一次，且修改的字符数量不大于 4 个；
i) 数据安全芯片未设置车牌号码的，在“安装自检（6H）”完成（无故障）状态下可以设置，车牌号码一经设置，仅允许修改一次，且修改的字符数量不大于 2 个，汉字按一个字符计算；
j) 数据安全芯片未设置机动车电子标识序列号的，在“安装自检（6H）”完成（无故障）状态下可以设置，机动车电子标识序列号一经设置，仅允许修改一次，且修改的字符数量不大于 4 个；
k) 数据安全芯片未设置机动脉冲系数的在“安装自检（6H）”完成（无故障）状态下可以设置
l) 在“安装自检（6H）”完成（无故障）状态下，且已经完成 VIN 号、车牌号码设置，才能进入“正式运行”状态，安装机动车电子标识的，应设置机动车电子标识序列号；
m) 在“正式运行”状态下，已设置的 VIN 号、车牌号码和机动车电子标识序列号不能更改，需要修改车牌号码和机动车电子标识序列号的，应通过联网平台进行；

n) 数据安全芯片应在一个通电周期里完成“安装自检”到“正式运行”的状态转换，“安装自检”状态下设备断电后重新通电运行应重新开始安装自检。

6.9.2 应用在汽车行驶记录仪的数据安全芯片生命周期状态转换见图 5

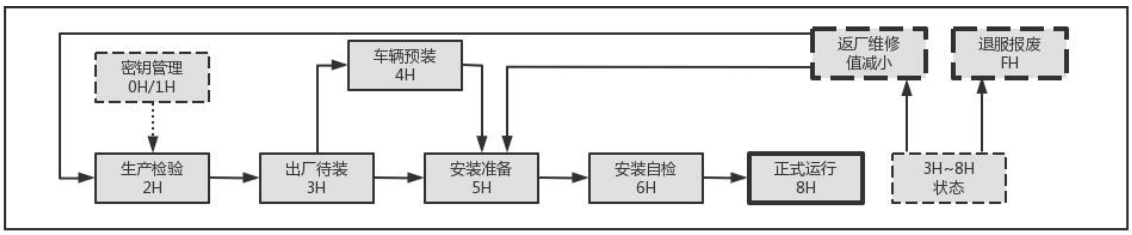

图 5 汽车行驶记录仪设备生命周期状态转换示意图

6.9.3 应用在汽车行驶记录仪的数据安全芯片生命周期状态转换应符合以下要求

a) 数据安全芯片进入“退服报废”状态后不能再次改变其状态；
b) 除“退服报废”状态外，其他任何状态可进入“返厂维修”状态；
c) 生命周期状态值（见 A.6.2.3：状态字位 04～01）减小视为“返厂维修”。

6.10 通信协议

数据安全芯片的通信协议见附录A和附录B。

7 性能要求

7.1 安全能力

数据安全芯片的安全能力应符合GM/T 0008 安全等级2的要求。

7.2 加密与解密

数据安全芯片使用对称算法加密和解密不大于256字节的源数据，所需时间应不大于10ms。
数据安全芯片使用非对称算法加密和解密不大于256字节的源数据，所需时间应不大于200ms。

7.3 数字证书管理

数据安全芯片对数字证书的更新和删除，所需时间应不大于100ms。
数据安全芯片存储和管理的数字证书数量应不少于32。

7.4 数字签名及验签

数据安全芯片使用本文件中规定应支持的算法进行数字签名或验签，所需时间应不大于200ms。

7.5 软件安全验证

数据安全芯片应至少保存4个主控制器软件版本对应的软件完整性摘要数据或软件签名数据。

7.6 实时时钟

数据安全芯片的实时时钟在未进行外部校准的条件下，运行误差在连续30天内应小于15秒。
数据安全芯片的实时时钟在主电源关闭条件下，使用后备电池供电时，消耗电流应小于5μA。

8 可靠性测试要求

数据安全芯片的检验要求、筛选顺序、抽样要求、试验和测试程序应符合GB/T 12750的要求。

9 安全性试验方法

数据安全芯片的数据安全性试验方法应符合GM/T 0008（试验方法、合格标准）要求。

10 包装

10.1 外包装

产品的外包装应包括如下内容：

a) 产品中文名称、规格型号、结构尺寸等；
b) 制造商名称、详细地址、邮编、电话、产品商标、制造日期、制造地；
c) 产品执行标准 T/CTS 11《汽车记录仪数据安全芯片技术要求》。

10.2 产品合格证

每批次出厂的数据安全芯片应有产品检验合格证，检验合格证应有如下内容：

a) 出厂检验结论、检验日期；
b) 检验员信息。

10.3 包装箱

包装箱应符合防潮、防尘、防震、运输的要求。

单个包装箱内应有产品合格证或检验标志及附件清单。

附 录 A
（规范性）
基本通信协议

A.1 通用约定

A.1.1 数据类型定义

表 A.1 数据类型定义表

数据类型	定义	数据类型	定义
BIN	若干字节二进制数据	U32	四字节无符号整型数据
U08	单字节无符号整型数据	S32	四字节有符号整型数据
S08	单字节有符号整型数据	BCD	若干字节的压缩 BCD 码
U16	双字节无符号整型数据	ASC[a]	仅包含英文字母和数字字符的字符串
S16	双字节有符号整型数据	STR[a]	GB 18030 字符串（含英文字符）
[a] ASC 和 STR 字符串未约定长度的以 00H 结尾，指定长度的不足部分以 00H 填充。			

A.1.2 数据表达、存储、传输约定

a) 如未特别说明，本文件所有附录数据的存储、传输顺序采用大端模式（Big-Endian）：高字节在前（低位地址）、低字节在后（高位地址）；
b) 十六进制数据以后缀‘H’表示：xxH，‘x’为字符‘0’～‘9’和‘A’～‘F’；十进制数据无后缀：xx，‘x’为字符‘0’～‘9’；二进制数据以后缀‘B’表示：xxB，‘x’为字符‘0’或‘1’；
c) 本文件所有附录的表格中的字节序号和字节数未能立即确定数值（因上一项数据长度为不确定的变动长度）的以省略号“...”表示；
d) 所有数据帧的长度应不大于 16K 字节；
e) 本协议中如未特别说明，数据摘要算法均采用 SM3，对称加解密均采用 SM1，非对称加解密及签名验签算法均采用 SM2；
f) 本文件附录中如未特别说明，“记录仪”特指汽车记录仪中与数据安全芯片通信的处理器，“芯片”特指数据安全芯片，“证书”特指数字证书，“签名”特指数字签名；
g) 记录仪与芯片间的通信由记录仪发起，记录仪发往芯片的数据帧简称为下行安全帧；芯片发往记录仪数据帧简称为上行安全帧，主动发起的数据帧称为请求帧，回应请求的称为应答帧；
h) 本附录中数据集合大小及包含关系按以下排列：数据帧 > 数据段 > 数据组 > 数据项，数据项为一个具备实际意义的数值或位集合。

A.2 数据帧格式

A.2.1 数据帧组成

通信的最小有效单元为数据帧，一个通信数据帧包含起始段、数据段、校验段三个部分，数据帧长度为这三个部分的总字节数，校验段仅含校验项，数据帧格式见表A.2：

表 A.2 数据帧格式表

项目序号	字节序号	字节数	段名称	项目名称	名称缩写	数据内容	说明
1	1	1	定义段	起始字节 1	SynB1	53H/35H	数据帧起始字节
2	2	1		起始字节 2	SynB2	78H	

项目序号	字节序号	字节数	段名称	项目名称	名称缩写	数据内容	说明
3	3	2	定义段	命令字	Cmd	U16	—
4	5	2		数据帧长度	Size	U16	项目 1～7 的总字节数
5	7	2		传输序列号	TImei	U16	—
6	9	...	内容段	数据帧内容	Data	BIN	与命令字相关的数据
7	...	2	校验段	校验字	Chk	U16	项目 1～6 的 CRC16 值

A.2.2 起始字节

记录仪发出的下行安全帧起始字节为53H，78H；芯片发出的上行安全帧起始字节为35H，78H。

A.2.3 命令字

A.2.3.1 命令字格式

表 A.3 命令字位定义表

位序号	内容	定义	备注
16	请求/应答帧标识	0：请求帧　　1：应答帧	—
15～05	请求/应答命令字	记录仪请求命令字：000H～5FFH 芯片请求命令字　：600H～7FFH	—
04～01	辅助命令	位 16=0（请求帧）： 0H～FH ：辅助命令	—
	应答结果	位 16=1（应答帧）： 0H ：执行成功 1H～FH ：错误代码，见表 A.4	

A.2.3.2 应答结果格式

a) 当请求被成功执行时，应答结果为 0H；
b) 当请求无法执行或执行错误时，应答结果为 1H～FH，表示错误代码，同时帧内容段为错误描述的 STR 字符串。

A.2.3.3 错误返回代码信息

表 A.4 错误返回代码信息表

返回值	错误内容	备注
1H	指定的证书 ID 错误或证书不存在	—
2H	证书中无指定的算法密钥，或密钥为空	—
3H	证书过期	—
4H	签名验证不通过	—
5H～BH	保留	—
CH～FH	未分类的错误，参照数据帧内容段错误信息描述	—

A.2.4 传输序列号

传输序列号是用来计数传输数据帧，记录仪在发起通信初始化请求时复位为0001H，芯片在应答通信初始化时复位为0001H,连接成功后发送的每个请求帧各自依次加1,数据帧发生传输错误需要重传时，传输序列号不变，传输序列号大于FF00H时，记录仪应重新进行通信初始化。记录仪和芯片在进行应答时，应答帧的传输序列号应和请求帧传输序列号一致。

A.2.5 校验段

校验段的校验字为项目1～6所有字节的CRC16计算值，CRC16值计算算法采用CRC16-CCITT方法，生成多项式为：x^16 + x^15 + x^2 + 1。

A.3 算法 ID

A.3.1 算法ID表

本协议中涉及的安全算法，算法类别及对应代码见表A.5：

表 A.5 算法 ID 表

项目序号	算法ID	说明	密钥长度	密钥分类	备注
1	11H	SM1 对称加解密算法	128	—	加解密/签名验签
2	13H	SM3 数据摘要加密	128	—	附加 Salt 值
3	14H	SM4 分组密码加解密算法	128	—	加解密/签名验签
4	31H	AES 对称加解密算法	128	—	加解密/签名验签
5	32H	AES 对称加解密算法	256	—	加解密/签名验签
6	52H	SM2 非对称加密与封装算法	512	公钥	加密
7		SM2 非对称解密与解封算法	256	私钥	解密
8	54H	SM2 非对称验签算法	512	公钥	验签
9		SM2 非对称签名算法	256	私钥	签名
10	72H	RSA 非对称加密算法（RSA2）	2048	公钥	加密
11		RSA 非对称解密算法（RSA2）	2048	私钥	解密
12	74H	RSA 非对称验签算法（RSA2）	2048	公钥	验签
13		RSA 非对称签名算法（RSA2）	2048	私钥	签名

A.4 数字证书

A.4.1 数字证书分类表

芯片支持的数字证书列表见表A.6：

表 A.6 数字证书分类表

项目序号	证书 ID	说明	非对称算法支持	对称算法支持	更新/删除权限 ID	备注
1	00H	出厂初始化证书	SM2	—	—	固件
2	01H	总根证书	SM2	SM1/SM4	01H	自身更新
3	04H	GA 记录签名证书	SM2	SM1/SM4	01H	数字签名、Salt 值
4	05H	GX 记录签名证书	SM2	SM1/SM4/AES	01H	数字签名
5	08H	DM 软件安全证书	SM2/RSA	—	—	启动及软件安全
6	10H	GA 通信根证书	SM2	SM1/SM4	01H	GA 平台通信加密
7	11H	GA 通信加密证书	SM2	SM1/SM4	01H/10H	—
8	20H	JT 通信根证书	SM2/RSA	SM1/SM4/AES	01H	—
9	21H	JT 通信加密证书	SM2/RSA	SM1/SM4/AES	01H/20H	—
10	22H	GX 通信根证书	SM2/RSA	SM1/SM4/AES	01H	—
11	23H	GX 通信加密证书	SM2/RSA	SM1/SM4/AES	01H/22H	—
12	24H	HB 通信根证书	SM2/RSA	SM1/SM4/AES	01H	—
13	25H	HB 通信加密证书	SM2/RSA	SM1/SM4/AES	01H/24H	—
14	26H	G1 通信根证书	SM2/RSA	SM1/SM4	01H	GOV 备用 1
15	27H	G1 通信加密证书	SM2/RSA	SM1/SM4	01H/26H	—
16	28H	G2 通信根证书	SM2/RSA	SM1/SM4/AES	01H	GOV 备用 2
17	29H	G2 通信加密证书	SM2/RSA	SM1/SM4/AES	01H/28H	—
18	30H	ZL 通信根证书	SM2/RSA	SM1/SM4/AES	01H	—
19	31H	ZL 通信加密证书	SM2/RSA	SM1/SM4/AES	01H/30H	—
20	40H	VM1 通信根证书	SM2/RSA	SM1/SM4/AES	01H	车辆制造商
21	41H	VM1 通信加密证书	SM2/RSA	SM1/SM4/AES	01H/40H	—
22	50H	VS1 通信根证书	SM2/RSA	SM1/SM4/AES	01H	经销商/运营商
23	51H	VS1 通信加密证书	SM2/RSA	SM1/SM4/AES	01H/50H	—
24	60H	VU1 通信根证书	SM2/RSA	SM1/SM4/AES	01H	车辆使用者
25	61H	VU1 通信加密证书	SM2/RSA	SM1/SM4/AES	01H/60H	—
26	62H	VU2 通信根证书	SM2/RSA	SM1/SM4/AES	01H	车辆使用者备用
27	63H	VU2 通信加密证书	SM2/RSA	SM1/SM4/AES	01H/62H	—
28	F0H	通用测试证书	SM2/RSA	SM1/SM4/AES	任意	测试用

A.4.2 数字证书格式

A.4.2.1 数字证书格式见表 A.7：

表 A.7 数字证书格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	4	特征字符		ASC	固定为：“#GA#”
2	5	1	证书 ID		BCD	如表 A.6 第 2 列
3	6	2	证书编号		BCD	从 0001 开始
4	8	5	支持的算法 ID 列表		BIN	不足填充 00H
5	13	6	证书有效期的开始时间		BCD	立即有效可设为： 01 01 01 00 00 00
6	19	6	证书有效期的结束时间		BCD	长期有效可设为： 99 12 31 00 00 00
7	25	4	具备更新、删除权限的证书 ID 列表		BCD	00H 为无效数据
8	29	32	发证机构名称		STR	—
9	61	40	未定义		BIN	证书备用数据
10	101	2	密钥数量		U16	—
11	103	2	密钥数据总长度		U16	项目 12～24 的总字节数
12	105	1	对称密钥（可选）	特征字符	ASC	字符‘@’
13	106	1		对称算法 ID	U08	如表 A.5
14	107	2		密钥字节数长度	U16	下一项的总字节数
15	109	...		密钥数据	BIN	—
16	...	1	非对称公钥（可选）	特征字符	ASC	字符‘#’
17	...	1		非对称算法 ID	U16	如表 A.5
18	...	2		密钥字节数长度	U16	下一项的总字节数
19	...	...		密钥数据	BIN	如表 A.7.1 和表 A.7.3
20	...	1	非对称私钥（可选）	特征字符	ASC	字符‘%’
21	...	1		非对称算法 ID	U08	如表 A.5
22	...	2		密钥字节数长度	U16	下一项的总字节数
23	...	...		密钥数据	BIN	如表 A.7.2，如表 A.7.4
24	...	...	其他密钥	密钥定义数据	BIN	如本表项目 12～15 部分
25	...	...	证书数字签名（如表 A.8）		U08	签名范围为项目 1～24
26	...	2	校验项		U16	项目 1～25 的 CRC16 值
注：一种算法 ID 在一张证书里只能保存一个对应密钥，同一种非对称加解密（签名验签）算法的公钥和私钥（算法 ID 不同）不一定是一对密钥的公钥和私钥。						

A.4.2.2 SM2 密钥公钥定义见表 A.7.1：

表 A.7.1 SM2 密钥公钥定义表

项目序号	字节序号	字节数	名称	数据类型	说明
1	1	2	特征字符	ASC	固定为：“*X”
2	3	2	公钥 X 长度	U16	—
3	5	...	公钥 X 数据	BIN	—
4	...	2	特征字符	ASC	固定为：“*Y”
5	...	2	公钥 Y 长度	U16	—
6	...	...	公钥 Y 数据	BIN	—

A.4.2.3 SM2 密钥私钥定义见表 A.7.2：

表 A.7.2 SM2 密钥私钥定义表

项目序号	字节序号	字节数	名称	数据类型	说明
1	1	2	特征字符	ASC	固定为：“*D”
2	3	2	私钥 D 长度	U16	—
3	5	...	私钥 D 数据	BIN	—

A.4.2.4 RSA 密钥公钥定义见表 A.7.3：

表 A.7.3 RSA 密钥公钥定义表

项目序号	字节序号	字节数	名称	数据类型	说明
1	1	2	特征字符	ASC	固定为：“*N”
2	3	2	公钥模 N 长度	U16	—
3	5	...	公钥模 N 数据	BIN	—
4	...	2	特征字符	ASC	固定为：“*E”
5	...	2	公钥指数 E 长度	U16	—
6	...	...	公钥指数 E 数据	BIN	—

A.4.2.5 RSA密钥私钥定义见表A.7.4：

表A.7.4 RSA密钥私钥定义表

项目序号	字节序号	字节数	名称	数据类型	说明
1	1	2	特征字符	ASC	固定为：“*P”
2	3	2	私钥P长度	U16	—
3	5	...	私钥P数据	BIN	—
4	...	2	特征字符	ASC	固定为：“*Q”
5	...	2	私钥Q长度	U16	—
6	...	...	私钥Q数据	BIN	—
7	...	2	特征字符	ASC	固定为：“*p”
8	...	2	私钥dP长度	U16	—
9	...	...	私钥dP数据	BIN	—
10	...	2	特征字符	ASC	固定为：“*q”
11	...	2	私钥dQ长度	U16	—
12	...	...	私钥dQ数据	BIN	—
13	...	2	特征字符	ASC	固定为：“*I”
14	...	2	私钥Qinv长度	U16	—
15	...	...	私钥Qinv数据	BIN	—

A.5 数字签名

A.5.1 数字签名格式

A.5.1.1 数字签名格式见表 A.8：

表 A.8 数字签名格式表

项目序号	字节序号	字节数	名称				数据类型	说明
1	1	4	签名标识（明文）	特征字符			ASC	固定为：“*GA*”
2	5	8		芯片 ID			BIN	如 3.表 A.11
3	13	1		签名数字证书 ID			BCD	—
4	14	2		签名数字证书编号			BCD	—
5	16	1		签名算法 ID			U08	如表 A.5
6	17	6		签名时间			BCD	—
7	23	2		签名时间毫秒值			BCD	000～999
8	25	6		源数据信息	源数据生成时间		BCD	—
9	31	4			源数据长度		U32	总字节数
10	35	32			源数据的摘要数据		BIN	SM3 算法
11	67	1			附加属性信息	属性标识 1	U08	如本表注 2
12	68	10				源数据设备唯一性 ID	BIN	行驶记录数据认证签名时为记录仪编号
13	78	1				属性标识 2	U08	如本表注 2
14	79	14				源数据设备绑定 ID	STR	行驶记录数据认证签名时为车牌号码
15	93	2	签名密文数据长度				U16	本表项目 16 的总字节数
16	95	...	项目 1～14 的数据摘要密文或签名数据 （对称密钥：数据摘要加密） （摘要密钥：附加 Salt 后二次摘要） （SM2 签名：符合 GB/T 32918.2 要求）				BIN	采用对称算法加密签名长度为 32 字节，其他的由签名算法确定长度
17	...	2	校验项				U16	项目 1～16 的 CRC16 值

注1：一个数字签名的总字节数最少为128字节，未满128字节的在检验段前填充00H。
数字签名的验证方式：采用非对称算法私钥签名的，可以使用公钥由所有人公开验证；采用对称算法或Salt摘要加密签名的，由证书发行机构或保存数字证书的数据安全芯片验证。

注2：属性标识字节的“位8～位5”表示属性类别（0H=保留，1H=唯一性ID，2H=绑定ID）；
属性标识字节的“位4～位1”表示属性数据的长度。

注3：源数据信息（项目8～14）的总字节数最少为68字节，不足部分填充00H；
源数据设备唯一性ID指生成签名的设备的固有且不可更改的编号，比如记录仪设备的记录仪编号，源数据设备绑定ID指设备的别名或与另一设备绑定时的另一设备标识，比如车牌号码。

A.6 基础信息

A.6.1 命令字分类

A.6.1.1 芯片基础信息通信命令字见表 A.9：

表 A.9 基础信息通信命令字列表

项目序号	Cmd	方向	请求/应答 说明	内容段数据	备注
1	0000H	下行	请求通信初始化	芯片型号（ASC）	如“AS5621”
2	8000H	上行	应答通信初始化	芯片基本信息	—
3	0010H	下行	请求读取芯片基本信息	行驶状态信息	心跳信息
4	8010H	上行	应答读取芯片基本信息	芯片基本信息	或为主动数据
5	0020H	下行	请求读取芯片详细信息	记录仪编号	—
6	8020H	上行	应答读取芯片详细信息	芯片详细信息	—

A.6.2 通信初始化

A.6.2.1 通信初始化由记录仪发起，芯片应答，记录仪发出的通信初始化下行安全请求帧，帧序列号应为 0001H，请求通信初始化帧格式定义见表 A.10：

表 A.10 请求通信初始化帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0000H
2	9	8	内容段	芯片型号	ASC	“AS5621M”
3	17	2	校验段		U16	—

A.6.2.2 应答通信初始化帧格式定义见表 A.11：

表 A.11 应答通信初始化帧格式表

项目序号	字节序号	字节数	名称			数据类型	说明
1	1	8	起始段			BIN	Cmd = 8000H
2	9	8	内容段	芯片型号		ASC	如“AS5621M”
3	17	1		芯片 ID	厂商代码	BCD	2 位数字，如“31”
4	18	3			型号代码	BCD	如“562101”
5	21	4			芯片序列号	BCD	如“32530001”
6	25	2		记录仪编号	制造商简称	ASC	符合 GB/T 19056-2021 附录 A 要求
7	27	3			产品型号简称	ASC	
8	30	4			产品流水号	BCD	
9	34	1			未定义	BIN	填充 00H

项目序号	字节序号	字节数	名称		数据类型	说明
10	35	6	内容段	芯片时间	BCD	如“191001101234”
11	41	2		记录仪（芯片）状态字	U16	见表 A.12
12	43	2	校验段		U16	—

A.6.2.3 记录仪（芯片）状态字位定义见表 A.12：

表 A.12 记录仪（芯片）状态字位定义表

位序号	内容	定义	备注
16	开关量故障信息	1：开关量有故障　　0：正常	—
15	GNSS 信息	1：卫星定位模块故障　0：正常	—
14	速度信号	1：车辆速度信号异常　0：正常	—
13～09	保留	未定义	—
08～05	维修计次	0H：出厂状态，设备未经历维修	—
		1H～FH：设备返修次数	—
04～01	记录仪（芯片）生命周期状态	00H：芯片未进行密钥注入和信息初始化 01H：芯片出厂状态，已配置记录仪编号 02H：记录仪生产（维修）检验阶段 03H：记录仪生产（维修）后出厂待装 04H：预安装状态，可设置 VIN 05H：安装准备，可设置 VIN、车牌号 06H：安装自检 08H：正式运行状态 0FH：报废/退服状态	位 04～01 值：0H ～ FH

A.6.3 数据安全芯片基本信息

A.6.3.1 芯片基本信息包含记录仪编号、RTC 时间、芯片状态等内容，记录仪应定期读取基本信息进行行驶记录信息的发送和通信维持，当记录仪和安全芯片工作在主从应答模式时，以每秒 1 次的间隔发送通信心跳（0010H）数据帧，心跳数据帧的帧序列号应为 0000H；当安全芯片空闲时，以芯片基本信息帧（8010H）应答，当安全芯片需要主动发送数据时，可以不应答芯片基本信息帧（8010H），直接发起信息请求。

A.6.3.2 请求芯片基本信息帧格式定义见表 A.13：

表 A.13 请求芯片基本信息帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0010H
2	9	6	内容段	时间	BCD	—
3	15	4		位置经度	S32	—
4	19	4		位置纬度	S32	—
5	23	2		位置高度	S16	—

项目序号	字节序号	字节数	名称		数据类型	说明
6	25	1	内容段	行驶方向	U08	—
7	26	1		行驶速度	U08	—
8	27	2		开关量信号	BIN	见表 A.14
9	29	1		行驶速度参考	U08	—
10	30	1		数据状态	BIN	见表 A.15
11	31	1		燃料消耗或电池输出功率	U08	—
12	32	1		发动机转速或电池充电功率	U08	—
13	33	1		油门踏板百分比	U08	—
14	34	1		车辆导向轮转向角	S08	顺时针（右转）为正
15	35	2	校验段		U16	—

A.6.3.3　开关量信号信息位定义见表 A.14：

表 A.14 开关量信息位定义

位号	内容	=1 定义	=0 定义	说明
16	点火开关	ON	OFF	—
15	制动	制动踏板踩下	未踩下	—
14	左转向	开	关	—
13	右转向	开	关	—
12	远光	开	关	—
11	近光	开	关	—
10	后雾灯	开	关	—
09	倒车	开	关	—
08	车门	打开	关闭	—
07	驾驶人座椅安全带	系上	未系上	—
06～01	自定义			

A.6.3.4　数据状态字位定义见表 A.15：

表 A.15 数据状态字位定义

位号	内容	=1 定义	=0 定义	说明
08	定位状态	未定位	定位	—
07	定位质量	2D 定位 （高度无效）	3D 定位 （高度有效）	—
06	PPS 脉冲状态	PPS 脉冲无效	PPS 脉冲有效	时间精度：0.1 ms

位号	内容	=1 定义	=0 定义	说明
05	定位模块故障状态	模块固件故障	模块工作正常	含天线开路、短路
04	除北斗外 的其他卫星定位系统	未使用其他 卫星定位系统	使用其他 卫星定位系统	GLONASS、GALILEO、GPS 等任意组合
03	内部 RTC 状态	RTC 功能异常	RTC 功能正常	RTC 故障或后备电池电压低
02	行驶速度来源	CAN 信号	车速传感器	—
01	制动以外的开关量 信号来源	CAN 信号	开关量传感器	—

A.6.3.5 应答芯片基本信息帧格式定义见表 A.16：

表 A.16 应答芯片基本信息帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8010H
2	9	8	内容段	芯片 ID	BCD	见表 A.11
3	17	10		记录仪编号	BIN	见表 A.11
4	27	6		芯片时间	BCD	—
5	33	2		记录仪（芯片）状态字	U16	见表 A.12
6	35	2	校验段		U16	—

A.6.4 芯片详细信息

A.6.4.1 芯片详细信息除芯片基本信息外还应包含制造商、生产日期、处理器型号等内容，详细信息文本（表 A.18 第 6 项）示例：

生产日期：2019-10-01
处理器：SC000
内存大小：128KB
代码空间：1024KB
固件版本：V31.20.1
固件日期：2021-12-31

A.6.4.2 请求芯片详细信息帧格式定义见表 A.17：

表 A.17 请求芯片详细信息帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0020H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	2	校验段		U16	—

A.6.4.3　应答芯片详细信息帧格式定义见表 A.18：

表 A.18 应答芯片详细信息帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8020H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		芯片时间	BCD	—
4	25	2		记录仪（芯片）状态字	U16	见表 A.12
5	27	2		详细信息长度	U16	—
6	29	...		详细信息文本	STR	—
7	...	2	校验段		U16	—

A.7　记录仪参数

A.7.1　命令字分类

A.7.1.1　记录仪参数是与记录仪运行相关的参数，分为预置参数、运行关键参数、运行一般参数，预置参数在芯片出厂前已经预置在芯片内部，出厂后不可更改。运行参数由记录仪在运行过程中设置的参数，运行关键参数一经设置不可更改（或授权后更改），一般参数可以由记录仪随时更改。

A.7.1.2　记录仪参数命令字见表 A.19：

表 A.19 记录仪参数命令字列表

项目序号	Cmd	方向	命令/应答 说明	内容段数据	备注
1	0110H	下行	请求读取记录仪预置参数	记录仪编号	—
2	8110H	上行	应答读取记录仪预置参数	预置参数	联网平台参数
3	0120H	下行	请求读取记录仪一般参数	读取位置及长度	—
4	8120H	上行	应答读取记录仪一般参数	一般参数	长度不超出 1kB
5	0130H	下行	请求写入记录仪一般参数	写入位置及长度	—
6	8130H	上行	应答写入记录仪一般参数	一般参数	长度不超出 1kB
7	0140H	下行	请求读取记录仪关键参数	记录仪编号	—
8	8140H	上行	应答读取记录仪关键参数	关键参数	—
9	0150H	下行	请求设置记录仪关键参数	记录仪编号	—
10	8150H	上行	应答设置记录仪关键参数	关键参数	—
11	0160H	下行	请求进入安装自检	记录仪编号	—
12	8160H	上行	应答进入安装自检	—	—
13	0170H	下行	请求进入正式运行	记录仪编号	—
14	8170H	上行	应答进入正式运行	—	—

项目序号	Cmd	方向	命令/应答 说明	内容段数据	备注
15	0180H	下行	请求变更记录仪生命周期状态	记录仪编号	—
16	8180H	上行	应答变更记录仪生命周期状态	—	—
17	0190H	下行	请求记录仪实时验证码	记录仪编号	—
18	8190H	上行	应答记录仪实时验证码	—	—
19	01A0H	下行	请求读取记录仪产品可追溯参数	记录仪编号	—
20	81A0H	上行	应答读取记录仪产品可追溯参数	可追溯参数	—
21	01B0H	下行	请求写入记录仪产品可追溯参数	记录仪编号	—
22	81B0H	上行	应答写入记录仪产品可追溯参数	可追溯参数	—

A.7.2 预置参数读取

A.7.2.1 预置参数为记录仪联网的网络连接参数，含主服务器域名和备服务器域名等信息，请求读取预置参数数据帧格式见表 A.20：

表 A.20 请求读取预置参数帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0110H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		记录仪时间	BCD	—
4	25	2	校验段		U16	—

A.7.2.2 应答读取预置参数数据帧格式见表 A.21：

表 A.21 应答读取预置参数帧格式表

项目序号	字节序号	字节数	名称			数据类型	说明
1	1	8	起始段			BIN	Cmd = 8110H
2	9	10	内容段	记录仪编号		BIN	见表 A.11
3	19	6		芯片时间		BCD	—
4	25	2		参数数量		U16	—
5	27	3		平台参数 1	参数类别	ASC	“MIP”
6	30	1			参数数据长度	U08	—
7	31	32			平台主服务器地址	ASC	—
8	63	3		平台参数 2	参数类别	ASC	“BIP”
9	66	1			参数数据长度	U08	—
10	67	32			平台备服务器地址	ASC	—

项目序号	字节序号	字节数	名称			数据类型	说明
11	99	3	内容段	传输参数 1	传输通信协议	ASC	‘GBT’
12	102	1			参数数据长度	U08	—
13	103	1			数据上传间隔	U08	单位：秒
14	104	1			19056 协议方式	ASC	‘T’：TCP ‘U’：UDP
15	105	2			19056 协议端口	U16	—
16	107	3		传输参数 2	传输通信协议	ASC	‘JTT’
17	110	1			参数数据长度	U08	—
18	111	1			数据上传间隔	U08	单位：秒
19	112	1			JT/T 808 协议方式	ASC	‘T’：TCP ‘U’：UDP
20	113	2			JT/T 808 协议端口	U16	—
21	115	2	校验段			U16	—

A.7.3 一般参数存取

A.7.3.1 一般参数由记录仪自行定义，芯片提供不小于 1kB 的存储空间，由记录仪写入或读出。

A.7.3.2 请求读取/写入一般参数帧格式见表 A.22：

表 A.22 请求读取/写入一般参数帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0120H （读取） Cmd = 0130H （写入）
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		记录仪时间	BCD	—
4	25	2		读取/写入开始位置	U16	—
5	27	2		读取/写入字节长度	U16	—
6	29	2		读取/写入 数据内容	BIN	请求读取时为空
7	31	2	校验段		U16	—

A.7.3.3 应答读取/写入一般参数帧格式见表 A.23：

表 A.23 应答读取/写入一般参数帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8120H （读取） Cmd = 8130H （写入）
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		芯片时间	BCD	—
4	25	2		读取/写入开始位置	U16	—

项目序号	字节序号	字节数	名称		数据类型	说明
5	27	2	内容段	读取/写入字节长度	U16	—
6	29	2		读取/写入 数据内容	BIN	—
7	31	2	校验段		U16	—
注：当读取/写入错误时，内容段为错误描述的 STR 字符串。						

A.7.4 关键参数读取

A.7.4.1 关键参数为记录仪运行过程不可更改信息，如车辆的 VIN 码（VDR_VIN），车辆的车牌号码（VDR_VCP），车辆的机动车电子标识序列号（VDR_VID）等信息。

A.7.4.2 请求读取关键参数数据帧格式见表 A.24：

表 A.24 请求读取关键参数帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0140H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		记录仪时间	BCD	—
4	25	2	校验段		U16	—

A.7.4.3 应答读取关键参数数据帧格式见表 A.25：

表 A.25 应答读取关键参数帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8140H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		芯片时间	BCD	—
4	25	2		记录仪（芯片）状态字	U16	见表 A.12
5	27	2		开关量信号故障状态信息	U16	见表 A.26
6	29	2		开关量检测屏蔽字	U16	见表 A.26
7	31	2		开关量信号状态信息	U16	见表 A.14
8	33	17		车辆 VIN	ASC	—
9	50	14		车辆车牌号码	STR	—
10	64	13		车辆机动车电子标识序列号	ASC	—
11	77	32		附加 Salt 值的数据摘要	BIN	本表 2～10 项并附加 Salt 值，Salt 值为 A.7.5 设置的值
12	109	2	校验段		U16	—

A.7.4.4　记录仪（芯片）的故障状态信息/检测屏蔽/反相位定义见表 A.26：

表 A.26 故障状态信息/检测屏蔽/反相位定义表

位序号	内容	=1 定义	=0 定义	备注
16	点火开关	故障状态信息： 信号 24 小时内无变化（通电运行时间） 检测屏蔽： 信号未输入或检测屏蔽 反相位： 信号输入为低电平时值为 1，反之为 0	故障状态信息： 信号 24 小时内有变化（通电运行时间） 检测屏蔽： 信号需要输入并进行检测 反相位： 信号输入为高电平时值为 1，反之为 0	屏蔽字初始化为 0
15	制动开关			屏蔽字初始化为 0
14	左转向			屏蔽字初始化为 0
13	右转向			屏蔽字初始化为 0
12	远光			屏蔽字初始化为 1
11	近光			屏蔽字初始化为 1
10	雾灯			屏蔽字初始化为 1
09	倒车			屏蔽字初始化为 1
08	车门			屏蔽字初始化为 1
07	安全带（驾驶员座椅）			屏蔽字初始化为 0
06～01	自定义			屏蔽字初始化为 1

A.7.4.5　开关量故障检测依据如下：

a)　当数据状态字（如表 A.15）位 01 为 1H（制动以外的开关量来源为 CAN 信号）时，开关量故障检测依据为芯片基本信息（如表 A.12）中的开关量信号值（序号 8）；

b)　当数据状态字（如表 A.15）位 01 为 0H（制动以外的开关量来源为传感器）时，开关量故障检测依据为芯片开关量输入引脚。

A.7.5　关键参数设置

A.7.5.1　关键参数可以写入或读出，汽车行驶记录仪的关键参数通过本指令设置，关键参数包含

a)　VIN：车辆 VIN 编码，ASC 类型，17 字节；

b)　VCP：车辆车牌号码，STR 类型，14 字节；

c)　VID：车辆的机动车电子标识序列号，ASC 类型，13 字节；

d)　SLT：数据摘要 Salt 值，BIN 类型，16 字节。

A.7.5.2　设置关键参数数据帧格式见表 A.27：

表 A.27 请求设置关键参数帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd =0150H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		记录仪时间	BCD	—
4	25	3		设置类别	ASC	VIN/VCP/VID/SLT
5	28	1		参数字节长度	U08	—
6	29	...		参数数据内容	BIN	—
7	...	2	校验段		U16	—

A.7.5.3　应答关键参数时数据帧格式见表 A.28：

表 A.28 应答设置关键参数帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8150H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		芯片时间	BCD	—
4	25	3		设置类别	ASC	VIN/VCP/VID/SLT
5	28	1		参数字节长度	U08	—
6	29	...		参数数据内容	BIN	—
7	...	2	校验段		U16	—

A.7.6　产品可追溯参数存取

A.7.6.1　产品可追溯参数由记录仪自行定义，芯片提供 256 块，每块 256 字节的存储空间，由记录仪写入或读出，每块空间仅能被写入一次，数据写入后不可更改或删除。

A.7.6.2　请求读取/写入产品可追溯参数帧格式见表 A.29：

表 A.29 请求读取/写入产品可追溯参数帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 01A0H （读取） Cmd = 01B0H （写入）
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		记录仪时间	BCD	—
4	25	1		读取/写入的块编号	BIN	—
5	26	1		参数块状态图应答标识	BIN	20H：应答状态图 00H：不应答状态图
6	27	2		读取/写入开始位置	U16	—
7	29	2		读取/写入字节长度	U16	—
8	31	...		读取/写入数据内容	BIN	请求读取时为空
9	...	2	校验段		U16	—

A.7.6.3　应答读取/写入产品可追溯参数帧格式见表 A.30：

表 A.30 应答读取/写入一般参数帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 81A0H[a] （读取） Cmd = 81B0H[b] （写入）
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		芯片时间	BCD	—

项目序号	字节序号	字节数	名称		数据类型	说明
4	25	1	内容段	读取/写入的块编号	BIN	—
5	26	1		参数块状态图应答标识	BIN	20H：应答　00H：不应答
6	27	[32]		参数块状态图[c]	BIN	项目 12 为 00H 时 本项目为空
7	...	2		读取/写入开始位置	U16	—
8	...	2		读取/写入字节长度	U16	—
9	...	...		读取/写入数据内容	BIN	—
10	...	2	校验段		U16	—
[a]、[b] 当读取/写入错误时，内容段为错误描述的 STR 字符串。 [c] 每 Bit 表示该参数块是否已写入数据，0B 为已写入，第 1 字节第 1Bit 表示第 1 参数块状态						

A.7.7　安装自检

A.7.7.1　安装自检是芯片转入正式运行状态前的必要步骤，芯片将设置所有故障状态为故障状态，必须变化所有未屏蔽开关量、卫星定位有效、速度正常后方可进入正式运行状态，请求进行入安装自检数据帧格式见表 A.31：

表 A.31 请求进入安装自检帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0160H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		记录仪时间	BCD	—
4	25	2	校验段		U16	—

A.7.7.2　应答进行入安装自检数据帧格式见表 A.32：

表 A.32 应答进入安装自检帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8160H
2	9	10	内容段	记录仪编号	ASC	
3	19	6		芯片时间	BCD	—
4	25	2		记录仪（芯片）状态字	U16	进入安装自检 见 A.6.2.3
5	27	2		开关量信号故障状态信息		见 A.7.4.4
6	29	2		开关量检测屏蔽字		见 A.7.4.4
7	31	17		车辆 VIN		—
8	48	14		车辆车牌号码		—
9	62	2	校验段		U16	—

A.7.8 正式运行

A.7.8.1 请求进行入正式运行数据帧格式见表 A.33：

表 A.33 请求进入正式运行帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0170H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		记录仪时间	BCD	—
4	25	2	校验段		U16	—

A.7.8.2 应答进行入正式运行数据帧格式见表 A.34：

表 A.34 应答进入正式运行帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8170H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		芯片时间	BCD	—
4	25	2		记录仪（芯片）状态字	U16	自检无故障 则进入正式运行
5	27	2		开关量信号故障状态信息		见 A.7.4.4
6	29	2		开关量检测屏蔽字		见 A.7.4.4
7	31	17		车辆 VIN		—
8	48	14		车辆车牌号码		—
9	62	2	校验段		U16	—

注1：应答使用的扩展错误代码0CH，表示安装自检未完成，故障信息未消除。

A.7.9 生命周期状态变更

A.7.9.1 生命周期变更是记录仪生命周期管理的必要步骤，请求生命周期变更数据帧格式见表 A.35：

表 A.35 请求记录仪生命周期变更帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0180H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		记录仪时间	BCD	—
4	25	2		开关量状态反相字	U16	信号输入低电平为有效时，对应位为 1，见表 A.14
5	27	4		未定义	BIN	—

项目序号	字节序号	字节数	名称		数据类型	说明
6	31	1	内容段	原生命周期状态	U08	A.6.2.3 的位 04～01
7	32	1		新生命周期状态	U08	A.6.2.3 的位 04～01
8	33	2	校验段		U16	—

A.7.9.2 芯片状态转换见图 5，并符合以下要求：

a) 由其他状态进入“返厂维修”状态时，A.6.2.3 的位 08～05 自动加 1，不能再增加时（为 FH 时），自动进入“退服报废”状态。

b) 本节指令（0180H）不支持进入“安装自检”状态，其专有指令见 A.7.6。

c) 本节指令（0180H）不支持进入“正式运行”状态，其专有指令见 A.7.8。

A.7.9.3 应答记录仪生命周期变更数据帧格式见表 A.36：

表 A.36 应答记录仪生命周期更新帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8180H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		芯片时间	BCD	—
4	25	1		原生命周期状态	U08	A.6.2.3 的位 08～01
5	26	1		新生命周期状态	U08	A.6.2.3 的位 08～01
6	27	32		设置结果描述	STR	成功/失败原因
7	59	2	校验段		U16	—

A.7.10 实时验证码

A.7.10.1 实时验证码是记录仪显示在屏幕上的用于人工交互或拍照识别证明记录仪合法身份的动态 6 位数字验证码，由安全芯片依据记录仪编号（见表 A.11 项目 6～9，共 10 字节）、安全芯片时间（BCD 码，6 字节）和 Salt 值（16 字节）生成，为这三部分数据（共 32 字节）数据摘要（SM3 算法）的最后 4 字节组成的 U32 十进制值最低 6 位数字，请求记录仪实时验证码数据帧格式见表 A.37：

表 A.37 请求记录仪实时验证码帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0190H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		记录仪时间	BCD	—
4	25	2	校验段		U16	—

A.7.10.2　应答记录仪实时验证码数据帧格式见表 A.38：

表 A.38 应答记录仪实时验证码帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8190H
2	9	10	内容段	记录仪编号	ASC	—
3	19	6		芯片时间	BCD	—
4	25	6		实时验证码	ASC	6 位数字
5	31	2	校验段		U16	—

例：最后4字节为：8AH 32H F6H 56H，十进制数值为：2318595670，实时验证码为：595670。

A.8　联网双向鉴权

A.8.1　命令字分类

记录仪的联网双向鉴权的过程命令请参照表A.39：

表 A.39 记录仪双向鉴权命令字列表

项目序号	Cmd	方向	命令/应答 说明	内容段数据	备注
1	0200H	下行	请求记录仪鉴权数据	鉴权方式	—
2	8200H	上行	应答记录仪鉴权数据包	设备鉴权数据包	—
3	0210H	下行	验证平台鉴权数据	平台鉴权数据包	—
4	8210H	上行	应答平台鉴权结果	鉴权结果	—

A.8.2　记录仪接入鉴权

A.8.2.1　请求记录仪接入平台鉴权数据帧格式见表 A.40：

表 A.40 请求记录仪接入平台鉴权数据帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0200H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	1		数字证书 ID	U08	见表 A.6， 例：GA 平台为 10H
4	20	1		鉴权算法 ID	U08	见表 A.5， 例：SM1 算法为 11H
5	21	1		记录仪附加数据长度	U08	无附加数据时为 00H
6	22	...		记录仪附加数据	BIN	平台分配的记录仪鉴权信息或其他数据
7	...	2	校验段		U16	—

A.8.2.2　应答记录仪接入平台鉴权数据帧格式见表 A.41：

表 A.41 应答记录仪接入平台鉴权数据帧格式表

项目序号	字节序号	字节数	名称			数据类型	说明
1	1	8	起始段			BIN	Cmd = 8200H
2	9	4	内容段	特征字节		ASC	@GA@
3	13	10		记录仪编号		BIN	见表 A.11
4	23	6		芯片时间		BCD	—
5	29	4		鉴权轮次		U32	加 1 后发出并保存
6	33	1		鉴权数字证书 ID		BCD	例：GA 平台为 10H
7	34	2		鉴权数字证书编号		BCD	—
8	36	1		鉴权算法 ID		U08	例：SM1 算法为 11H
9	37	2		设备状态字		U16	见表 A.12
10	39	1		记录仪附加数据长度		U08	见表 A.40
11	40	...		记录仪附加数据		BIN	见表 A.40
12	...	2		鉴权数据包长度		U16	项目 13、14 总字节数
13	...	32		加密的鉴权数据包	摘要数据加密	BIN	项目 2～11 的摘要
14	...	...			安全芯片数据	BIN	—
15	...	2	校验段			U16	—

A.8.3　平台反向鉴权

A.8.3.1　记录仪收到应答帧后，将内容段作为鉴权数据包发送给平台，平台通过记录仪鉴权后回复平台鉴权数据包，记录仪应将平台鉴权数据包发送给芯片，请求验证平台反向鉴权数据帧格式见表 A.42：

表 A.42 请求验证平台反向鉴权数据帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0210H
2	9	4	内容段	特征字节	ASC	@GA@
3	13	10		记录仪编号	BIN	见表 A.11
4	23	6		平台服务器时间	BCD	—
5	29	4		平台反向鉴权轮次	U32	加 1 后发出，并保存
6	33	1		鉴权数字证书 ID	BCD	例：GA 平台为 10H
7	34	2		鉴权数字证书编号	BCD	—
8	36	1		鉴权算法 ID	U08	例：SM1 算法为 11H
9	37	2		设备状态字	U16	—

项目序号	字节序号	字节数	名称			数据类型	说明
10	39	1	内容段	记录仪附加数据长度		U08	见表 A.40
11	...	...		记录仪附加数据		BIN	见表 A.40
12	...	2		鉴权数据包长度		U16	项目 13、14 总字节数
13	...	32		加密的鉴权数据包	摘要数据加密	BIN	项目 2～11 的摘要
14	...	...			联网通信参数	BIN	—
15	...	2	校验段			U16	—

A.8.3.2　芯片收到平台鉴权数据帧后，将内容段签名验签或数据解密后比对，并将结果反馈给记录仪，应答验证平台反向鉴权数据帧格式见表 A.43：

表 A.43 应答验证平台反向鉴权数据帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8210H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		芯片时间	BCD	—
4	25	...		联网通信参数 或鉴权不通过原因描述	BIN	SM4 动态密钥等 由表 A.42 项目 14 解密
5	...	2	校验段		U16	—

A.8.3.3　Cmd 为 8210H 时，表示反向鉴权通过，否则为不通过，不通过时表 A.43 项目 4 为原因描述。

A.8.3.4　平台和记录仪的鉴权轮次在发出前加 1 并存储，收到目标发来的有效鉴权轮次（大于本地存储的鉴权轮次值）时存储该鉴权轮次数据，平台和记录仪仅需保存一个鉴权轮次值，但平台需保存每一台入网记录仪各自对应的鉴权轮次值。

A.8.3.5　反向鉴权通过时，记录仪保存由平台分配的记录仪鉴权信息（见表 A.42 项目 11）。

表 A.44 联网通信参数格式

项目序号	字节序号	字节数	名称	数据类型	说明
1	1	4	参数 ID	U32	—
2	5	1	参数长度	U16	—
3	6	...	参数值	BIN	—

表 A.45 联网通信参数 ID 定义

项目序号	参数 ID	名称	数据类型	参数长度	说明
1	0000H～DFFFH	参数 ID	U16	2	符合 JT/T 808 要求
2	E000H	平台继续通信要求	U16	2	0000H：后续无通信要求 0001H：按参数要求通信
3	E001H	连续行驶状态传输间隔	U16	2	单位：秒

项目序号	参数 ID	名称	数据类型	参数长度	说明
4	E002H	网络心跳帧传输间隔	U16	2	单位：秒
5	E010H	当前路段限速值	U16	2	单位：km/h
6	E100H	SM4 动态密钥	BIN	16	—
7	E200H	鉴权标识[a]	ASC	16	—
[a]：鉴权标识由平台下发，记录仪初始化该数据全部为 30H					

A.9 联网数据加解密

A.9.1 命令字分类

记录仪的联网数据加密命令见表A.46：

表 A.46 记录仪联网数据加解密命令字列表

项目序号	Cmd	方向	命令/应答 说明	内容段数据	备注
1	0240H	下行	请求加密通信数据包	需加密数据及要求	—
2	8240H	上行	应答加密通信数据包	加密后数据及要求	—
3	0250H	下行	请求解密通信数据包	需解密数据及要求	—
4	8250H	上行	应答解密通信数据包	解密后数据及要求	—

A.9.2 联网上行数据加密

A.9.2.1 请求加密通信数据的数据帧格式见表 A.47：

表 A.47 请求加密通信数据帧格式表

项目序号	字节项目	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0240H
2	9	1	内容段	数字证书 ID	U08	见表 A.6
3	10	1		算法 ID	U08	见表 A.5
4	11	2		数据包长度	U16	本表项目 5 总字节数
5	13	...		需加密的数据包	BIN	—
6	...	2	校验段		U16	—

A.9.2.2　应答加密通信数据的数据帧格式见表 A.48：

表 A.48 应答加密通信数据帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8240H
2	9	1	内容段	数字证书 ID	U08	见表 A.6
3	10	1		算法 ID	U08	见表 A.5
4	11	2		数据包长度	U16	本表项目 5 总字节数
5	13	...		加密后数据包	BIN	—
6	...	2	校验段		U16	—

A.9.3　联网下行数据解密

A.9.3.1　请求解密通信数据的数据帧格式见表 A.49：

表 A.49 请求解密通信帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0250H
2	9	1	内容段	数字证书 ID	U08	见表 A.6
3	10	1		算法 ID	U08	见表 A.5
4	11	2		数据包长度	U16	本表项目 5 总字节数
5	13	...		需解密的数据包	BIN	—
6	...	2	校验段		U16	—

A.9.3.2　应答解密通信数据的数据帧格式见表 A.50：

表 A.50 应答解密通信帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8250H
2	9	1	内容段	数字证书 ID	U08	见表 A.6
3	10	1		算法 ID	U08	见表 A.5
4	11	2		数据包长度	U16	本表项目 5 总字节数
5	13	...		解密后数据包	BIN	—
6	...	2	校验段		U16	—

A.10 数据摘要及签名

A.10.1 命令字分类

A.10.1.1 记录仪的行驶数据记录认证命令见表 A.51：

表 A.51 记录数据认证签名及验证命令字列表

项目序号	Cmd	方向	命令/应答 说明	内容段数据	备注
1	0280H	下行	请求加密或签名摘要数据	摘要数据	—
2	8280H	上行	应答加密或签名摘要数据	加密或签名数据	—
3	0290H	下行	请求解密签名数据包	加密数据	—
4	8290H	上行	应答解密签名数据包	解密后数据	—
5	02A0H	下行	请求验签	加密数据	—
6	82A0H	上行	应答验签	解密后数据	—
7	02C0H	下行	请求生成单次摘要数据	源数据包	—
8	82C0H	上行	应答生成单次摘要数据	摘要数据	—
9	02D0H 02E0H 02F0H	下行	请求生成连续摘要数据 （02D0H：首帧 02E0H：过程） （02F0H：末帧）	源数据包	—
10	82D0H 82E0H 82F0H	上行	应答生成连续摘要数据	摘要数据	仅结束时摘要数据有效，其他为过程数据

A.10.2 摘要生成数字签名

A.10.2.1 请求数据摘要生成数字签名的数据帧格式见表 A.52：

表 A.52 请求摘要生成数字签名帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0280H
2	9	4	内容段	特征字符	ASC	固定为：“*GA*”
3	13	1		数字证书 ID	BCD	—
4	14	1		签名算法 ID	U08	见表 A.5 00H 为不加密
5	15	6		源数据生成时间	BCD	—
6	21	4		源数据长度	U32	总字节数
7	25	32		源数据的摘要数据	BIN	SM3 算法
8	57	2	校验段		U16	—

A.10.2.2　应答数据摘要生成数字签名的数据帧格式见表 A.53：

表 A.53 应答摘要生成数字签名帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8280H
2	9	...	内容段	数字签名	BIN	见表 A.8
3	...	2	校验段		U16	—

A.10.3　数据生成数字签名

A.10.3.1　请求特定数据的数字签名的数据帧格式见表 A.54：

表 A.54 请求数据生成数字签名帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0290H
2	9	4	内容段	特征字符	ASC	固定为：“*GA*”
3	13	1		数字证书 ID	BCD	—
4	14	1		签名算法 ID	U08	见表 A.5 00H 为不加密
5	15	6		源数据生成时间	BCD	—
6	21	4		源数据长度	U32	总字节数
7	25	...		源数据	BIN	—
8	...	2	校验段		U16	—

A.10.3.2　应答特定数据的数字签名的数据帧格式见表 A.55：

表 A.55 应答数据生成数字签名帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8290H
2	9	...	内容段	数字签名	BIN	见表 A.8
3	...	2	校验段		U16	—

A.10.4　数字签名验签

A.10.4.1　请求验证数字签名的数据帧格式见表 A.56：

表 A.56 请求数字签名验签帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 02A0H
2	9	...	内容段	数字签名	BIN	见表 A.8
3	...	2	校验段		U16	—

A.10.4.2　请打验证数字签名的数据帧格式见表 A.57：

表 A.57 应答数字签名验签帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 82A0H
2	9	2	内容段	验签结果	U16	0000H=验签通过
3	11	2	校验段		U16	—

A.10.5　单次数据生成摘要

A.10.5.1　请求单次数据生成数据摘要的数据帧格式见表 A.58：

表 A.58 请求单次数据生成摘要帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 02C0H
2	9	1	内容段	加 Salt 方式	U08	00H：不加 Salt 01H：附加 Salt 值
3	10	1		未定义	U08	—
4	11	4		源数据长度	U32	字节数
5	15	...		源数据	BIN	—
6	...	2	校验段		U16	—

A.10.5.2　记录仪在正式运行状态（芯片状态字为 X8H，见 A.6.2.3）时，Salt 值为数字证书 04H（证书 ID 为 04H）的 SM3（算法 ID=13H）密钥；其他状态下 Salt 值为设置值，未设置的全为 00H 字节。

A.10.5.3　应答单次数据生成数据摘要的数据帧格式见表 A.59：

表 A.59 应答单次数据生成摘要帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 82C0H
2	9	1	内容段	加 Salt 方式	U08	见表 A.58 项目 2
3	10	1		未定义	U08	—
4	11	32		数据摘要	BIN	—
5	43	2	校验段		U16	—

A.10.6 连续数据生成摘要

A.10.6.1 请求连续数据生成数据摘要的数据帧格式见表 A.60：

表 A.60 请求连续数据生成摘要帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 02D0H：首帧 02E0H：中间帧 02F0H：末帧
2	9	1	内容段	加 Salt 方式	U08	见表 A.58 项目 2
3	10	1		缓冲区编号	U08	00H～03H
4	11	4		源数据长度	U32	字节数
5	15	...		源数据	BIN	—
6	...	2	校验段		U16	—

A.10.6.2 记录仪在正式运行状态（芯片状态字为 X8H，见 A.6.2.3）时，Salt 值为数字证书 04H（证书 ID 为 04H）的 SM3（算法 ID=13H）密钥，其他状态下，Salt 值为 00H（16 个 00H 字节）。

A.10.6.3 应答连续数据生成数据摘要的数据帧格式见表 A.61：

表 A.61 应答连续数据生成摘要帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 82D0H：首帧 82E0H：中间帧 82F0H：末帧
2	9	1	内容段	加 Salt 方式	U08	见表 A.58 项目 2
3	10	1		缓冲区编号	U08	00H～03H
4	11	32		数据摘要值或过程值	BIN	—
5	43	2	校验段		U16	—

A.11 存储器保护

A.11.1 命令字分类

A.11.1.1 记录仪的防护存储器写保护初始化及解锁过程命令见表 A.62：

表 A.62 记录仪存储器保护命令字列表

项目序号	Cmd	方向	命令/应答 说明	内容段数据	备注
1	0300H	下行	请求初始化写保护密钥	保护解锁密钥	—
2	8300H	上行	应答初始化写保护密钥	解锁鉴权密钥	—
3	0310H	下行	请求存储器写保护解锁数据		—
4	8310H	上行	应答存储器写保护解锁数据	解锁鉴权密钥	—

A.11.2 存储器保护初始化

A.11.2.1 请求存储器保护密钥初始化的数据帧格式见表 A.63：

表 A.63 请求存储器保护密钥初始化数据帧格式表

项目序号	字节序号	字节数	名称			数据类型	说明
1	1	8	起始段			BIN	Cmd = 0300H
2	9	2	内容段	存储器类型识别符		ASC	如：“LS”
3	11	6		记录仪时间		BCD	—
4	17	1		算法 ID		U08	项目 6～10 加密算法
5	18	1		密文数据长度		U08	项目 6～10 总字节数
6	19	4		加密的初始化信息（密钥为预置安全密钥）	特征字符串	ASC	“!GA!”
7	23	4			存储器信息	ASC	如厂商、容量：“LS8G”
8	27	16			写保护密钥	BIN	存储器生成的密钥
9	43	16			随机数据	BIN	—
10	59	...			填充数据	BIN	可选，PKCS7 填充
11	...	2	校验段			U16	—

A.11.2.2 芯片收到写保护初始化数据包后，通过存储器类型识别字符（如“LS”）提取对应的解密密钥对加密的初始化信息进行解密，若前 4 字节为“!GA!”则为合法数据，保存写保护密钥并归零写保护密钥轮次。

A.11.2.3 应答存储器保护密钥初始化的数据帧格式见表 A.64：

表 A.64 应答存储器保护密钥初始化数据帧格式表

项目序号	字节序号	字节数	名称			数据类型	说明
1	1	8	起始段			BIN	Cmd = 8300H
2	9	2	内容段	存储器类型识别符		ASC	如：“LS”
3	11	6		芯片时间		BCD	
4	17	1		算法 ID		U08	项目 6～10 加密算法
5	18	1		密文数据长度		U08	项目 6～10 总字节数
6	19	4		加密数据（密钥见表 A.63 项目 8 的写保护密钥）加密数据（密钥见表 A.63 项目 8 的写保护密钥）	特征字符	ASC	“!GA!”
7	23	4			解锁轮次	U32	初始化为 0 本数据为小端模式
8	27	6			时间	BCD	—
9	33	18			随机字节	BIN	—
10	51	32			摘要数据	BIN	项目 6～9 并附加上写保护密钥（共 48 字节）的数据摘要
11	83	2	校验段			U16	—

A.11.2.4　芯片收到正确写保护初始化数据包后，应答写保护解锁数据包，解锁数据包（共 64 字节）使用写保护密钥加密后发出，同时解锁数据包中的摘要数据由写保护密钥参与运算，摘要数据的数据源由：“特征字符+密钥轮次+时间+随机字节+写保护密钥”组成。

A.11.3　存储器单次解锁

A.11.3.1　请求存储器单次解锁的数据帧格式见表 A.65：

表 A.65 请求存储器单次解锁数据帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0310H
2	9	2	内容段	存储器类型识别字符	ASC	如：“LS”
3	11	6		记录仪时间	BCD	—
4	17	2	校验段		U16	—

A.11.3.2　应答存储器单次解锁的数据帧格式见表 A.66：

表 A.66 应答存储器保护单次解锁数据帧格式表

项目序号	字节序号	字节数	名称			数据类型	说明
1	1	8	起始段			BIN	Cmd = 8310H
2	9	2	内容段	存储器类型识别字符		ASC	如：“LS”
3	11	6		芯片时间		BCD	
4	17	1		算法 ID		U08	项目 6～10 加密算法
5	18	1		密文数据长度		U08	项目 6～10 总字节数
6	19	4		加密数据（密钥见表 A.63 项目 8 的写保护密钥）	特征字符	ASC	“!GA!”
7	23	4			解锁轮次	U32	加 1 后发出并保存 本数据为小端模式
8	27	6			时间	BCD	—
9	33	18			随机字节	BIN	—
10	51	32			摘要数据	BIN	项目 6～9 并附加上写保护密钥（共 48 字节）的数据摘要
11	83	2	校验段			U16	—

A.12 CRC 校验矩阵及算法参考

A.12.1 CRC16 校验矩阵

```
const unsigned char    suCRC16[]=
{0x00,0xc1,0x81,0x40,0x01,0xc0,0x80,0x41,0x01,0xc0,0x80,0x41,0x00,0xc1,0x81,0x40, //0x0000 - 0x000f
 0x01,0xc0,0x80,0x41,0x00,0xc1,0x81,0x40,0x00,0xc1,0x81,0x40,0x01,0xc0,0x80,0x41, //0x0010 - 0x001f
 0x01,0xc0,0x80,0x41,0x00,0xc1,0x81,0x40,0x00,0xc1,0x81,0x40,0x01,0xc0,0x80,0x41, //0x0020 - 0x002f
 0x00,0xc1,0x81,0x40,0x01,0xc0,0x80,0x41,0x01,0xc0,0x80,0x41,0x00,0xc1,0x81,0x40, //0x0030 - 0x003f
 0x01,0xc0,0x80,0x41,0x00,0xc1,0x81,0x40,0x00,0xc1,0x81,0x40,0x01,0xc0,0x80,0x41, //0x0040 - 0x004f
 0x00,0xc1,0x81,0x40,0x01,0xc0,0x80,0x41,0x01,0xc0,0x80,0x41,0x00,0xc1,0x81,0x40, //0x0050 - 0x005f
 0x00,0xc1,0x81,0x40,0x01,0xc0,0x80,0x41,0x01,0xc0,0x80,0x41,0x00,0xc1,0x81,0x40, //0x0060 - 0x006f
 0x01,0xc0,0x80,0x41,0x00,0xc1,0x81,0x40,0x00,0xc1,0x81,0x40,0x01,0xc0,0x80,0x41, //0x0070 - 0x007f
 0x01,0xc0,0x80,0x41,0x00,0xc1,0x81,0x40,0x00,0xc1,0x81,0x40,0x01,0xc0,0x80,0x41, //0x0080 - 0x008f
 0x00,0xc1,0x81,0x40,0x01,0xc0,0x80,0x41,0x01,0xc0,0x80,0x41,0x00,0xc1,0x81,0x40, //0x0090 - 0x009f
 0x00,0xc1,0x81,0x40,0x01,0xc0,0x80,0x41,0x01,0xc0,0x80,0x41,0x00,0xc1,0x81,0x40, //0x00a0 - 0x00af
 0x01,0xc0,0x80,0x41,0x00,0xc1,0x81,0x40,0x00,0xc1,0x81,0x40,0x01,0xc0,0x80,0x41, //0x00b0 - 0x00bf
 0x00,0xc1,0x81,0x40,0x01,0xc0,0x80,0x41,0x01,0xc0,0x80,0x41,0x00,0xc1,0x81,0x40, //0x00c0 - 0x00cf
 0x01,0xc0,0x80,0x41,0x00,0xc1,0x81,0x40,0x00,0xc1,0x81,0x40,0x01,0xc0,0x80,0x41, //0x00d0 - 0x00df
 0x01,0xc0,0x80,0x41,0x00,0xc1,0x81,0x40,0x00,0xc1,0x81,0x40,0x01,0xc0,0x80,0x41, //0x00e0 - 0x00ef
 0x00,0xc1,0x81,0x40,0x01,0xc0,0x80,0x41,0x01,0xc0,0x80,0x41,0x00,0xc1,0x81,0x40, //0x00f0 - 0x00ff
 0x00,0xc0,0xc1,0x01,0xc3,0x03,0x02,0xc2,0xc6,0x06,0x07,0xc7,0x05,0xc5,0xc4,0x04, //0x0100 - 0x010f
 0xcc,0x0c,0x0d,0xcd,0x0f,0xcf,0xce,0x0e,0x0a,0xca,0xcb,0x0b,0xc9,0x09,0x08,0xc8, //0x0110 - 0x011f
 0xd8,0x18,0x19,0xd9,0x1b,0xdb,0xda,0x1a,0x1e,0xde,0xdf,0x1f,0xdd,0x1d,0x1c,0xdc, //0x0120 - 0x012f
 0x14,0xd4,0xd5,0x15,0xd7,0x17,0x16,0xd6,0xd2,0x12,0x13,0xd3,0x11,0xd1,0xd0,0x10, //0x0130 - 0x013f
 0xf0,0x30,0x31,0xf1,0x33,0xf3,0xf2,0x32,0x36,0xf6,0xf7,0x37,0xf5,0x35,0x34,0xf4, //0x0140 - 0x014f
 0x3c,0xfc,0xfd,0x3d,0xff,0x3f,0x3e,0xfe,0xfa,0x3a,0x3b,0xfb,0x39,0xf9,0xf8,0x38, //0x0150 - 0x015f
 0x28,0xe8,0xe9,0x29,0xeb,0x2b,0x2a,0xea,0xee,0x2e,0x2f,0xef,0x2d,0xed,0xec,0x2c, //0x0160 - 0x016f
 0xe4,0x24,0x25,0xe5,0x27,0xe7,0xe6,0x26,0x22,0xe2,0xe3,0x23,0xe1,0x21,0x20,0xe0, //0x0170 - 0x017f
 0xa0,0x60,0x61,0xa1,0x63,0xa3,0xa2,0x62,0x66,0xa6,0xa7,0x67,0xa5,0x65,0x64,0xa4, //0x0180 - 0x018f
 0x6c,0xac,0xad,0x6d,0xaf,0x6f,0x6e,0xae,0xaa,0x6a,0x6b,0xab,0x69,0xa9,0xa8,0x68, //0x0190 - 0x019f
 0x78,0xb8,0xb9,0x79,0xbb,0x7b,0x7a,0xba,0xbe,0x7e,0x7f,0xbf,0x7d,0xbd,0xbc,0x7c, //0x01a0 - 0x01af
 0xb4,0x74,0x75,0xb5,0x77,0xb7,0xb6,0x76,0x72,0xb2,0xb3,0x73,0xb1,0x71,0x70,0xb0, //0x01b0 - 0x01bf
 0x50,0x90,0x91,0x51,0x93,0x53,0x52,0x92,0x96,0x56,0x57,0x97,0x55,0x95,0x94,0x54, //0x01c0 - 0x01cf
 0x9c,0x5c,0x5d,0x9d,0x5f,0x9f,0x9e,0x5e,0x5a,0x9a,0x9b,0x5b,0x99,0x59,0x58,0x98, //0x01d0 - 0x01df
 0x88,0x48,0x49,0x89,0x4b,0x8b,0x8a,0x4a,0x4e,0x8e,0x8f,0x4f,0x8d,0x4d,0x4c,0x8c, //0x01e0 - 0x01ef
 0x44,0x84,0x85,0x45,0x87,0x47,0x46,0x86,0x82,0x42,0x43,0x83,0x41,0x81,0x80,0x40};//0x01f0 - 0x01ff
```

A.12.2 CRC16 校验算法参考

```
bool Check_CRC16(unsigned char * pBuf, int Length,unsigned char Mode)
{
 extern unsigned char  suCRC16[];
 STATIC unsigned char  cHi,cLo,ic;
 STATIC unsigned int   i;
 STATIC unsigned short Jcrc,Rcrc;

 cHi=0xff;
 cLo=0xff;
 for(i=0;i<Length;i++)
    {ic=cHi^pBuf[i];
     cHi=cLo^suCRC16[ic];
     cLo=suCRC16[ic+0x100];
    }
 Jcrc=(cHi<<8)|cLo;
 Rcrc=pBuf[Length]<<8|pBuf[Length+1];
 if (Mode==1)                                    //生成校验码 回写至数据区
    {pBuf[Length]  =cHi;
     pBuf[Length+1]=cLo;
     }
 return (Jcrc==Rcrc);                            //比较效验码并返回
}
```

附 录 B
（规范性）
扩展通信协议

B.1 芯片性能测试

B.1.1 命令字分类

芯片性能测试命令请见表B.1：

表 B.1 芯片性能测试命令字列表

项目序号	Cmd	方向	请求/应答 说明	内容段数据	备注
1	0080H	下行	请求芯片加密性能测试	测试算法及数据	—
2	8080H	上行	应答芯片加密性能测试	—	—
3	0090H	下行	请求芯片签名性能测试	测试算法及数据	—
4	8090H	上行	应答芯片签名性能测试	—	—
5	00A0H	下行	请求芯片验签性能测试	测试算法及数据	—
6	80A0H	上行	应答芯片验签性能测试	—	—

B.1.2 加密及签名性能测试

B.1.2.1 请求芯片加密及签名性能测试的数据帧格式见表 B.2：

表 B.2 请求芯片加密及签名性能测试帧格式表

项目序号	字节项目	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0080H/0090H
2	9	2	内容段	循环次数	U16	—
3	11	1		测试证书 ID	U08	见表 A.6
4	12	1		测试算法 ID	U08	见表 A.5
5	13	2		测试源数据长度	U16	—
6	15	...		测试源数据	BIN	—
7	...	2	校验段		U16	—

B.1.2.2 芯片接收完整的一帧数据后，进行加密或签名计算前，必须按照指定的偏移量将增量值与目标数据相加，如此循环直至完成指定的测试次数。

B.1.2.3 芯片每完成一次加密或签名计算，应立即将计算结果的最后四个有效字节以应答，应答芯片加密及签名性能测试的数据帧见表 B.3：

表 B.3 应答芯片加密及签名性能测试帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8080H/8090H
2	9	2	内容段	循环次数	U16	—
3	11	1		测试证书 ID	U08	见表 A.6
4	12	1		测试算法 ID	U08	见表 A.5
5	13	4		密文或签名最后 4 字节数据	BIN	—
6	17	2	校验段		U16	—

B.1.3 芯片验签性能测试

B.1.3.1 请求芯片验签性能测试的数据帧格式见表 B.4：

表 B.4 请求芯片验签性能测试帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 00A0H
2	9	2	内容段	测试次数	U16	一般为 4 次
3	11	1		测试证书 ID	U08	见表 A.6
4	12	1		测试算法 ID	U08	见表 A.5
5	13	2		测试 1 源数据长度	U16	—
6	15	...		测试 1 源数据	BIN	头部 4 字节暂为 00H
7	...	2		测试 1 签名数据长度	U16	—
8	...	...		测试 1 签名数据	BIN	—
9	...	...		...	BIN	—
10	...	2		测试 N 源数据长度	U16	—
11	...	...		测试 N 源数据	BIN	头部 4 字节暂为 00H
12	...	2		测试 N 签名数据长度	U16	—
13	...	...		测试 N 签名数据	BIN	—
14	...	4		测试 1 源数据头部 4 字节	BIN	—
15	...	4		...	BIN	—
16	...	4		测试 N 源数据头部 4 字节	BIN	—
17	...	2	校验段		U16	—

B.1.3.2　应答芯片验签性能测试的数据帧格式见表 B.5：

表 B.5 应答芯片验签性能测试帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 80A0H
2	9	2	内容段	测试次数	U16	—
3	11	1		测试证书 ID	U08	见表 A.6
4	12	1		测试算法 ID	U08	见表 A.5
5	13	...		验签结果	BIN	00H 为验签通过 其他为验签不通过
6	...	2	校验段		U16	—

B.2　软件安全及软件升级安全

B.2.1　命令字分类

记录仪的软件安全及OTA命令请见表B.6：

表 B.6 记录仪软件安全及软件升级安全命令字列表

项目序号	Cmd	方向	命令/应答 说明	内容段数据	备注
1	0340H	下行	请求初始化记录仪软件信息	版本信息及代码摘要	—
2	8340H	上行	应答初始化记录仪软件信息	初始化结果	—
3	0350H	下行	请求验证记录仪软件信息	版本信息及摘要加密	—
4	8350H	上行	应答验证记录仪软件信息	验证结果	—
5	0360H	下行	请求升级记录仪软件信息	版本信息及摘要加密	—
6	8360H	上行	应答升级记录仪软件信息	验证结果	—

B.2.2　初始化软件信息

B.2.2.1　请求初始化记录仪软件信息的数据帧格式见表 B.7：

表 B.7 请求初始化记录仪软件信息帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0340H
2	9	10	内容段（DM 证书的公钥加密）	记录仪编号	BIN	见表 A.11
3	19	6		记录仪时间	BCD	—
4	25	8		记录仪硬件信息	ASC	—
5	33	8		记录仪软件版本号	ASC	—
6	41	6		软件生成时间	BCD	—

项目序号	字节序号	字节数	名称		数据类型	说明
7	47	1	内容段（DM 证书的公钥加密）	软件代码安全策略（芯片片选）	U08	01H：延时后为高电平 02H：延时后为低电平
8	48	1		软件代码安全延时	U08	单位：秒，00H 为无效
9	49	1		软件功能安全策略（联网模块使能）	U08	01H：通过后为高电平 02H：通过后为低电平
10	50	1		软件功能安全延时	U08	时间：秒，00H 为无效
11	51	1		软件升级安全策略（芯片写保护）	U08	01H：延时后为高电平 02H：延时后为低电平
12	52	1		软件升级安全延时	U08	时间：秒，00H 无延时
13	53	32		软件代码摘要数据	BIN	
14	85	...		随机数据	BIN	可选，PKCS1 填充
15	...	2	校验段		U16	—

B.2.2.2　应答初始化记录仪软件信息的数据帧格式见表 B.8：

表 B.8 应答初始化记录仪软件信息帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8340H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		芯片时间	BCD	—
4	25	8		记录仪硬件信息	ASC	—
5	33	8		记录仪软件版本号	ASC	—
6	41	6		软件生成时间	BCD	—
7	47	1		软件代码安全策略	U08	见表 B.7 项目 7
8	48	1		软件代码安全延时	U08	见表 B.7 项目 8
9	49	1		软件功能安全策略	U08	见表 B.7 项目 9
10	50	1		软件功能安全延时	U08	见表 B.7 项目 10
11	51	1		软件升级安全策略	U08	见表 B.7 项目 11
12	52	1		软件升级安全延时	U08	见表 B.7 项目 12
13	53	2	校验段		U16	—

B.2.2.3　应答帧扩展的错误代码为 0CH，表示软件信息已经初始化。

B.2.3 验证软件信息

B.2.3.1 记录仪软件系统启动后计算所有代码的数据摘要并使用公钥加密方式提交数据由安全芯片验证，验证通过后，安全芯片将改变功能使能控制信号的输出电平，该信号可以启动或使能记录仪的关键模块（如联网模块），使记录仪具备全部可用功能，请求验证记录仪软件信息的数据帧见表 B.9：

表 B.9 请求验证记录仪软件信息帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0350H
2	9	10	内容段（DM 证书的公钥加密）	记录仪编号	BIN	见表 A.11
3	19	6		记录仪时间	BCD	—
4	25	8		记录仪硬件信息	ASC	—
5	33	8		记录仪软件版本号	ASC	—
6	41	8		随机数据	BIN	—
7	49	32		软件代码摘要数据	BIN	—
8	81	...		随机数据	BIN	—
9	...	2	校验段		U16	—

B.2.3.2 应答验证记录仪软件信息的数据帧见表 B.10：

表 B.10 应答验证记录仪软件信息帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8350H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		芯片时间	BCD	—
4	25	8		记录仪硬件信息	ASC	—
5	33	8		记录仪软件版本号	ASC	—
6	41	2	校验段		U16	—

B.2.3.3 应答帧扩展的错误代码如下：

a) 0CH：软件信息未初始化；
b) 0DH：时间戳重复或回溯。

B.2.4 软件升级安全

B.2.4.1 记录仪软件系统升级改写软件代码存储芯片的软件代码前应通过安全芯片验证原版本和新版本的软件信息，验证通过后，安全芯片将改变软件代码存储芯片片选信号和写保护信号的输出电平，该信号可以使能软件代码芯片和解除软件代码芯片的写保护，使记录仪的软件代码芯片可以更新升级。

B.2.4.2　请求记录仪软件升级信息的数据帧见表 B.11：

表 B.11 请求记录仪软件升级信息帧格式表

项目序号	字节序号	字节数	名称			数据类型	说明
1	1	8	起始段			BIN	Cmd = 0360H
2	9	10	内容段（公钥加密）	记录仪编号		BIN	见表 A.11
3	19	6		记录仪时间			—
4	25	8		原版本验证信息	记录仪硬件信息	ASC	—
5	33	8			记录仪软件版本号	ASC	—
6	41	6			软件生成时间	BCD	—
7	47	1			软件代码安全策略	U08	见表 B.7 项目 7
8	48	1			软件代码安全延时	U08	见表 B.7 项目 8
9	49	1			软件功能安全策略	U08	见表 B.7 项目 9
10	50	1			软件功能安全延时	U08	见表 B.7 项目 10
11	51	1			软件升级安全策略	U08	见表 B.7 项目 11
12	52	1			软件升级安全延时	U08	见表 B.7 项目 12
13	53	4			未定义	BIN	—
14	57	32			软件代码摘要数据	BIN	—
15	89	8		新版本验证信息	记录仪硬件信息	ASC	—
16	97	8			记录仪软件版本号	ASC	—
17	105	6			软件生成时间	BCD	—
18	111	1			软件代码安全策略	BIN	见表 B.7 项目 7
19	112	1			软件代码安全延时	ASC	见表 B.7 项目 8
20	113	1			软件功能安全策略	ASC	见表 B.7 项目 9
21	114	1			软件功能安全延时	BCD	见表 B.7 项目 10
22	115	1			软件升级安全策略	U08	见表 B.7 项目 11
23	116	1			软件升级安全延时	U08	见表 B.7 项目 12
24	117	4			未定义	BIN	—
25	121	32			软件代码摘要数据	BCD	—
26	153	...		随机数据		BIN	—
27	...	2	校验段			U16	—

B.2.4.3　应答记录仪软件升级信息的数据帧见表 B.12：

表 B.12 应答记录仪软件升级信息帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8360H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		芯片时间	BCD	—
4	25	8		记录仪硬件信息	ASC	—
5	33	8		记录仪软件版本号	ASC	新版本信息
6	41	6		软件生成时间	BCD	新版本信息
7	47	1		软件芯片片选策略	U08	见表 B.7 项目 7
8	48	1		软件芯片片选延时	U08	见表 B.7 项目 8
9	49	1		功能使能控制策略	U08	见表 B.7 项目 9
10	50	1		功能使能控制延时	U08	见表 B.7 项目 10
11	51	1		软件芯片写保护策略	U08	见表 B.7 项目 11
12	52	1		软件芯片写保护延时	U08	见表 B.7 项目 12
13	53	4		未定义	BIN	—
14	57	2	校验段		U16	—

B.2.4.4　应答帧扩展的错误代码如下：

a)　0CH：软件信息未初始化；

b)　0DH：原版本软件信息错误。

B.3　总线及控制安全

B.3.1　命令字分类

记录仪的联网总线及控制安全程命令请见表B.13。

表 B.13 记录仪总线及控制安全命令字列表

项目序号	Cmd	方向	命令/应答 说明	内容段数据	备注
1	0380H	下行	请求总线发送数据	总线数据及签名	—
2	8380H	上行	应答总线发送数据	—	—
3	0390H	下行	请求控制使能	总线数据及签名	—
4	8390H	上行	应答控制时能	—	—

B.3.2 总线数据发送使能

B.3.2.1 请求总线数据发送的数据帧见表 B.14：

表 B.14 请求总线数据发送帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0380H
2	9	8	内容段	记录仪硬件信息	ASC	—
3	17	8		记录仪软件信息	ASC	—
4	25	6		记录仪时间	BCD	—
5	31	2		总线开启时间长度	U16	秒
6	33	2		总线数据包长度	U16	—
7	...	...		总线数据包	BIN	—
8	...	...		总线数据包数字签名	BIN	—
9	...	2	校验段		U16	—

B.3.2.2 应答总线数据发送的数据帧见表 B.15：

表 B.15 应答总线数据发送帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8380H
2	9	8	内容段	记录仪硬件信息	ASC	—
3	17	8		记录仪软件信息	ASC	—
4	25	6		芯片时间	BCD	—
5	31	2		总线开启时间长度	U16	秒
6	...	2	校验段		U16	—

B.3.3 远程控制使能

B.3.3.1 请求远程控制使能的数据帧见表 B.16：

表 B.16 请求远程控制使能帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0390H
2	9	8	内容段	记录仪硬件信息	ASC	—
3	17	8		记录仪软件信息	ASC	—
4	25	6		记录仪时间	BCD	—
5	31	2		远程控制开启时间长度	U16	秒

项目序号	字节序号	字节数	名称		数据类型	说明
6	33	2	内容段	远程控制数据包长度	U16	—
7	...	...		远程控制数据包	BIN	—
8	...	...		远程控制数字签名	BIN	—
9	...	2	校验段		U16	—

B.3.3.2　应答远程控制使能的数据帧见表 B.17：

表 B.17 应答远程控制使能帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8390H
2	9	8	内容段	记录仪硬件信息	ASC	—
3	17	8		记录仪软件信息	ASC	—
4	25	6		芯片时间	BCD	—
5	31	2		远程控制使能时间长度	U16	秒
6	33	2	校验段		U16	—

B.4　数字证书管理

B.4.1　命令字分类

B.4.1.1　记录仪的数字证书命令见表 B.18。

表 B.18 记录仪数字证书管理命令字列表

项目序号	Cmd	方向	命令/应答 说明	内容段数据	备注
1	0400H	下行	请求删除数字证书	记录仪编号 证书 ID	—
2	8400H	上行	应答删除数字证书	—	—
3	0410H	下行	请求更新数字证书	记录仪编号 证书 ID	—
4	8410H	上行	应答更新数字证书	—	—

B.4.2　数字证书删除

B.4.2.1　请求数字证书删除的数据帧见表 B.19：

表 B.19 请求数字证书删除帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0400H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		记录仪时间	BCD	—

项目序号	字节序号	字节数	名称		数据类型	说明
4	25	1	内容段	数字证书 ID	U08	—
5	26	1		重复数字证书 ID	U08	—
6	27	...		数字签名	BIN	项目 2～5 数字签名
7	...	2	校验段		U16	—

B.4.2.2　应答数字证书删除的数据帧见表 B.20：

表 B.20 应答数字证书删除帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8400H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		芯片时间	BCD	—
4	25	1		数字证书 ID	U08	—
5	26	1		重复数字证书 ID	U08	—
6	27	2	校验段		U16	—

B.4.3　数字证书更新

B.4.3.1　请求数字证书更新的数据帧见表 B.21：

表 B.21 请求数字证书更新帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0410H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		记录仪时间	BCD	—
4	25	1		数字证书 ID	U08	—
5	26	1		重复数字证书 ID	U08	—
6	27	1		加密用数字证书 ID	BCD	—
7	28	2		加密用数字证书编号	BCD	—
8	30	1		加密算法	U08	—
9	31	2		数字证书长度	U16	—
10	33	...		加密的数字证书	BIN	项目 4～8 定义的算法
11	...	...		数字签名	BIN	项目 2～10 的数字签名
12	...	2	校验段		U16	—

B.4.3.2　应答数字证书更新的数据帧见表 B.22：

表 B.22 应答数字证书更新帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8410H
2	9	10	内容段	记录仪编号	BIN	见表 A.11
3	19	6		芯片时间	BCD	—
4	25	1		数字证书 ID	U08	—
5	26	1		重复数字证书 ID	U08	—
6	27	2	校验段		U16	—

B.5　联网数据透传

B.5.1　命令字分类

记录仪的联网数据透传过程命令见表B.23：

表 B.23 记录仪联网数据透传命令字列表

项目序号	Cmd	方向	命令/应答 说明	内容段数据	备注
1	6800H	上行	请求记录仪上传数据包	上传数据包	—
2	E800H	下行	应答记录仪上传数据包	—	—
3	0800H	下行	请求平台下发数据包	下发数据包	—
4	8800H	上行	应答平台下发数据包	—	—
5	6810H	上行	请求断开平台连接	平台编号	—
6	E810H	下行	应答断开平台连接	—	—

B.5.2　数据透明上传

B.5.2.1　请求数据透明上传的数据帧见表 B.24：

表 B.24 请求数据透明上传帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 6800H
2	9	1	内容段	平台编号	U08	—
3	10	20		平台域名或 IP 地址	STR	—
4	30	2		平台接入端口号	U16	—
5	32	1		接入方式	U08	—
6	33	2		透传数据包长度	U16	—
7	35	...		透传数据包	BIN	—
8	...	2	校验段		U16	—

B.5.2.2　应答数据透明上传的数据帧见表 B.25：

表 B.25 应答数据透明上传帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = E800H
2	9	1	内容段	平台编号	U08	—
3	10	2		上传的数据包长度	U16	—
4	12	...		执行结果描述	STR	—
5	...	2	校验段		U16	—

B.5.3　数据透明下发

B.5.3.1　请求数据透明下发的数据帧见表 B.26：

表 B.26 请求数据透明下发帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 0800H
2	9	1	内容段	平台编号	U08	—
3	10	2		透传数据包长度	U16	—
4	12	...		透传数据包	BIN	—
5	...	2	校验段		U16	—

B.5.3.2　应答数据透明下发的数据帧见表 B.27：

表 B.27 应答数据透明下发帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 8800H
2	9	1	内容段	平台编号	U08	—
3	10	2		透传数据包长度	U16	—
4	12	2	校验段		U16	—

B.5.4　断开平台连接

B.5.4.1　请求断开平台连接的数据帧见表 B.28：

表 B.28 请求断开平台连接帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = 6810H
2	9	1	内容段	平台编号	U08	—
3	10	2	校验段		U16	—

B.5.4.2　应答断开平台连接的数据帧见表 B.29：

表 B.29 应答断开平台连接帧格式表

项目序号	字节序号	字节数	名称		数据类型	说明
1	1	8	起始段		BIN	Cmd = E810H
2	9	1	内容段	平台编号	U08	—
3	10	...		执行结果描述	STR	—
4	...	2	校验段		U16	—

参 考 文 献

[1] GB/T 19392-2013 车载卫星导航设备通用规范
[2] GB/T 35787-2017 机动车电子标识读写设备安全技术要求
[3] GA/T 1201 道路交通安全违法行为卫星定位技术取证规范
[4] GB 7258-2017 机动车运行安全技术条件
[5] GA 16.4 道路交通管理信息代码 第4部分：机动车车辆类型代码
[6] GA 16.7 道路交通管理信息代码 第7部分：机动车号牌种类代码
[7] JT/T 1021-2016 交通运输信息系统基于XML的数据通用规则
[8] 国家智能交通工程技术研究中心 《中国智能交通体系框架》
[9] 中国人民公安大学出版社 《智能交通管理系统理论与实践》