ICS 43.040.10
CCS T 35

团 体 标 准

T/CTS XX—XXXX

汽车记录仪数据安全芯片技术要求

Technical requirements of data security chip

for vehicle recorder

（征求意见稿）

20XX-XX-XX 发布 20XX-XX-XX 实施

中 国 道 路 交 通 安 全 协 会 发 布

目　次

前　言---------- II
引　言---------- III
1 范围---------- 1
2 规范性引用文件---------- 1
3 术语和定义---------- 1
4 缩略语---------- 2
5 一般功能---------- 3
6 性能要求---------- 8
附录 A（规范性）通信协议---------- 10
附录 B（规范性）扩展通信协议---------- 43

前　言

本标准参照GB/T 1.1-2020给出的规则起草。

本标准由中国道路交通安全协会提出并归口管理。

本标准起草单位：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、公安部交通管理科学研究所、内蒙古自治区公安厅交通管理局、江苏都万电子科技有限公司、华为技术有限公司、杭州中导科技开发有限公司、成都三零嘉微电子科技有限公司、凌科芯安科技（北京）有限公司、北京工业大学、大连理工大学、湖北民族大学、浙江省北斗卫星应用产业协会、杭州海康威视系统技术有限公司、深圳国脉科技有限公司、杭州鸿泉物联网技术股份有限公司、深圳锐明技术股份有限公司、航天科技控股集团股份有限公司、铭创（福建）电子科技有限公司、深圳市华宝电子科技有限公司、厦门雅迅网络股份有限公司、深圳市特思威尔科技有限公司。

本标准主要起草人：

本标准为首次发布。

引　言

各类汽车记录仪（如行驶记录仪、事件记录仪、视频记录仪）在车辆上的广泛应用，为分析道路交通事故原因和真相、界定道路交通事故性质和厘清事故责任提供基础数据（如重庆公交坠江事件的车内视频和行驶记录数据），进而为提升驾乘人员道路交通安全意识并减少交通事故、加强公共交通乘客参与交通安全的主动意识等提供第一手资料。

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验证，同时对存储记录数据的存储器进行必要的删除保护。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，而通过特定功能的安全芯片来是建立高等级安全边界并实现数据安全功能的性价比最优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必要的高等级安全边界技术实现手段。

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》有重要的意义。

汽车记录仪数据安全芯片技术要求

1 范围

本标准规定了适用汽车记录仪的数据安全芯片的安全功能需求分类、安全算法技术要求、安全算法性能指标，记录数据可信验证的加密数字签名格式和数据安全的数字证书格式，以及支持和实现车联网网络安全功能的通信协议格式和通信过程技术要求。

本标准适用于安装在车辆上的汽车记录仪的数据安全芯片的技术规范要求。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 2312　　信息交换用汉字编码字符集 基本集
GB 16735　　道路车辆　车辆识别代号（VIN）
GB/T 19056　汽车行驶记录仪
GB/T 32905　信息安全技术 SM3 密码杂凑算法
GB/T 32907　信息安全技术 SM4 分组密码算法
GB/T 32918　信息安全技术 SM2 椭圆曲线公钥密码算法
GA 36　　中华人民共和国机动车号牌
GMT 0008　　安全芯片密码检测准则
T/CTS XX　　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

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。

3.2

安全密钥 security key

控制密码变换操作的关键信息或参数。

3.3

数字签名 digital signature

由且只由信息发送者生成的附在数据后面的数字串，或对数据通过密码变换方式进行操作。数据的接收者可以通过验证数字签名来鉴别数据的来源和完整性，数字签名还可以保护数据不被篡改、 伪造，保证数据的不可否认性。

3.4

数字证书 digital certificate

网络通信中用于标识设备身份、存放密钥、并具备有效性数字签名验证的一组数据集合。

3.5

证书管理 certificate management

根据安全策略，对数字证书的产生、认证、注销、分发、安装、更新、删除和销毁等操作制定并实施一组确定的规则。

3.6

双向鉴权 mutual authentication

通信的发起方和接受方均具备证明自身和验证对方合法性的能力，并在通信的开始进行证明和验证的过程。

3.7

上行传输 upload

由记录仪发出的，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。

3.8

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记录仪的数据传输方式。

3.9

生命周期 life cycle

记录仪设备从生产、出厂、预装、安装、运行、维修、报废使用的全过程。

3.10

记录仪编号 recorder ID

记录仪的唯一性编号标识，由生产厂商名称缩写（2个大写字符）、产品型号简称（3个大写字符或数字）、以及产品生产流水号（8位数字）组成。

4 缩略语

下列缩略语适用于本文件。

SM1： 国家商用密码算法定义的一种算法不公开的对称密钥加密及解密算法；

SM2： 国家商用密码算法定义的一种椭圆曲线公钥密码算法；
SM3： 国家商用密码算法定义的一种密码杂凑算法；
AES128： 密钥长度为128位的AES（advanced encryption standard）加密及解密算法；
AES256： 密钥长度为256位的AES（advanced encryption standard）加密及解密算法；
SHA256： 摘要信息长度为256位的SHA-1（secure hash algorithm 1）数据摘要算法；
SHA512： 摘要信息长度为512位的SHA-1（secure hash algorithm 1）数据摘要算法；
RSA2048：密钥长度为2048位的非对称RSA加密及解密算法；
CRC16： 结果为16比特的循环冗余校验（cyclic redundancy check）
CBC： 密文分组链接方式（cipher block chaining）
IV： 初始化向量（initialization vector）
PKCS1： 长度数据填充模式1（PKCS1 padding）
PKCS7： 长度数据填充模式7（PKCS7 padding）

5 一般功能

5.1 加密与解密

5.1.1 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、AES128和AES256；
b) 非对称加密与解密算法SM2、RSA2048。

5.1.2 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；

5.2 数字签名及验签

5.2.1 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、SHA256、SHA512；
b) 签名和验签算法SM2、RSA2048。

5.2.2 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.7的要求；
f) SM2签名算法的可辨别标识ID为“GB/T 19056-2021”；
g) 以记录仪编号、芯片时间、数字证书为参数生成设备实时验证码（6位数字）。

5.3 数字证书

5.3.1 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据证书数量应符合附录A表A.5的要求；
b) 数据安全芯片支持的数据证书格式应符合附录A表A.6的要求；
c) 数字证书的更新和删除权限应符合附录A表A.5的权限关系要求。

5.4 实时时钟

5.4.1 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定位的时间数据进行自动对时，和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。

5.5 联网双向鉴权

5.5.1 数据安全芯片支持记录仪的联网鉴权功能应符合以下要求：

a) 数据安全芯片的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) 数据安全芯片的发起的联网鉴权数据应支持包含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。

5.5.2 联网双向鉴权流程如图 1

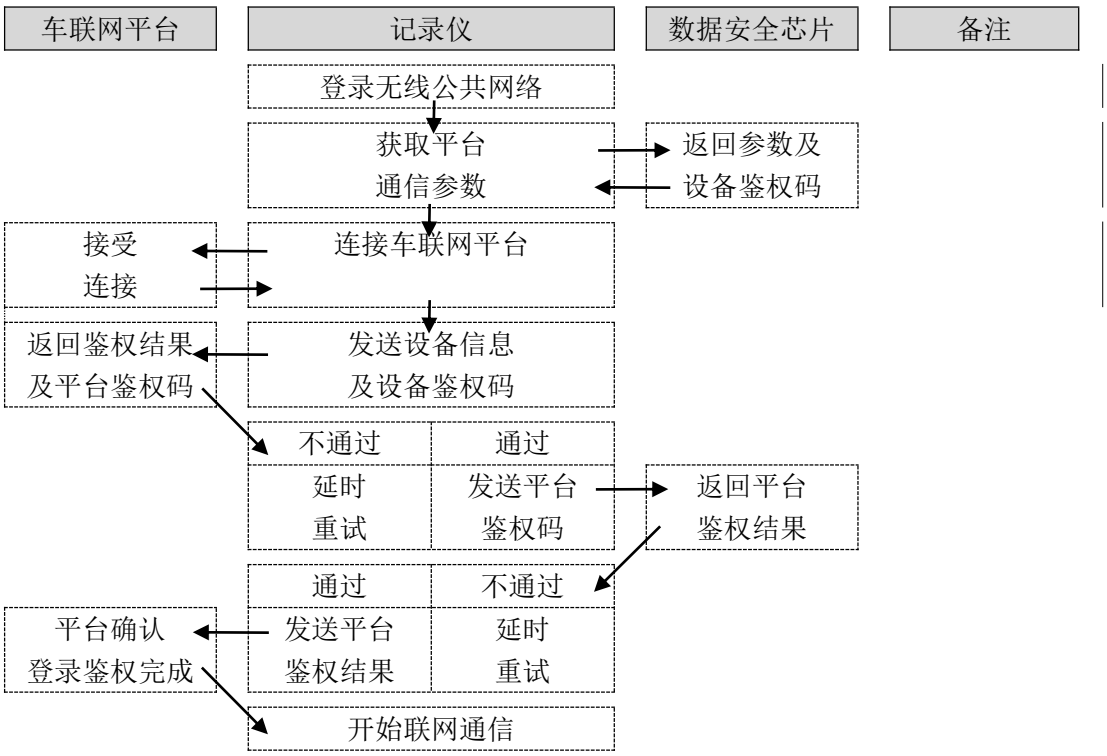

图 1 联网双向鉴权流程示意图

5.6 存储器保护

5.6.1 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。

5.6.2 存储器保护初始化流程如图 2：

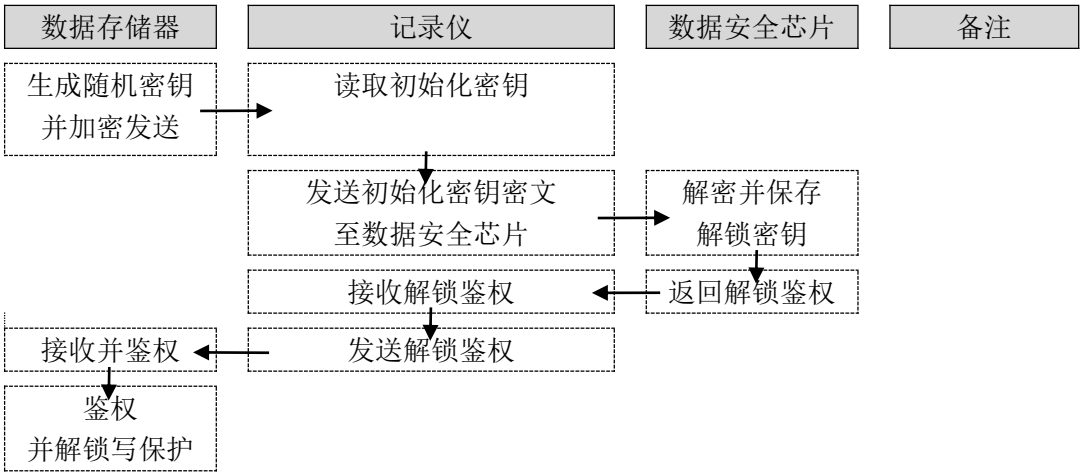

图 2 存储器保护初始化流程示意图

5.6.3 存储器保护单次解锁流程如图 3：

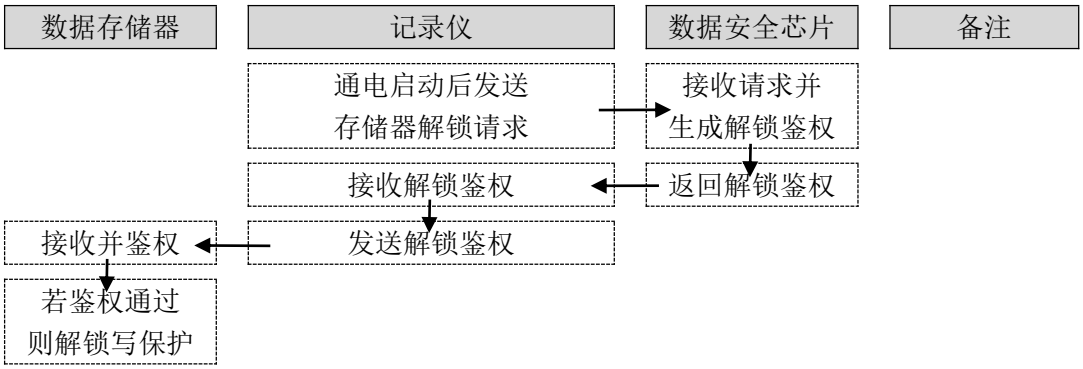

图 3 存储器保护单次解锁流程示意图

5.7 记录仪启动安全

5.7.1 数据安全芯片应支持记录仪软件安全的能力，并符合以下要求：

a) 数据安全芯片应至少具备1路的功能模块控制信号输出，用于记录仪的软件功能安全；
b) 数据安全芯片应至少具备1路的软件芯片片选信号输出，用于记录仪的软件代码安全；

c） 数据安全芯片的信号输出应具备有效性输出极性定义和控制方式定义；
d） 数据安全芯片的功能模块控制信号的输出在芯片上电后应处于控制无效；
e） 数据安全芯片的软件芯片片选信号的输出在芯片上电后使能有效，经过指定时间后应处于使能无效。

5.7.2 设备软件安全连接如图 4：

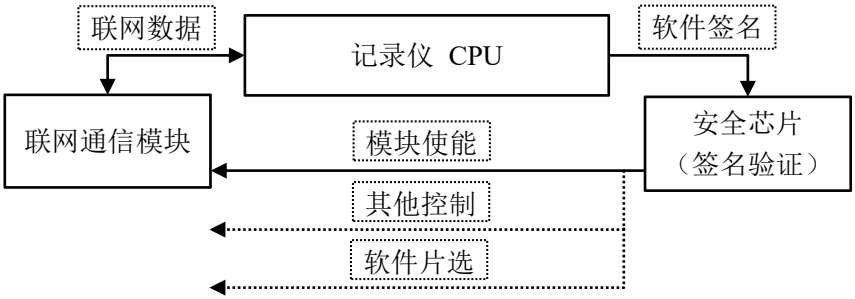

图 4 设备软件安全连接示意图

5.8 设备软件升级安全

5.8.1 数据安全芯片应具备支持记录仪软件升级安全的能力，并符合以下要求：

a） 数据安全芯片应至少具备1路的软件芯片写保护信号输出，用于记录仪的软件升级安全；
b） 数据安全芯片的软件芯片写保护信号的输出在芯片上电后应处于保护使能；
c） 记录仪进行软件升级时，数据安全芯片在验证原版本签名信息和记录新版本摘要数据和签名信息后解锁软件芯片写保护特定的时间。
d） 记录仪进行软件升级时，数据安全芯片在验证新版本信息时应同时比对硬件版本号。

5.8.2 设备软件升级安全连接如图 5：

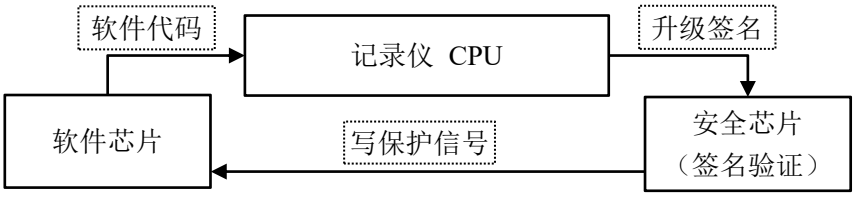

图 5 设备软件升级安全连接示意图

5.9 车载总线安全

5.9.1 数据安全芯片应具备支持记录仪总线安全的能力，并符合以下要求：

a） 数据安全芯片应至少具备1路的总线发送使能信号输出，用于记录仪的总线安全；
b） 数据安全芯片的总线发送使能信号应具备使能输出极性定义和使能控制方式定义；
c） 数据安全芯片的总线发送使能信号的输出在芯片上电后应处于无效状态；
d） 数据安全芯片在验证总线数据的签名有效后使能总线发送特定的时间。

5.9.2　设备总线安全连接如图 6：

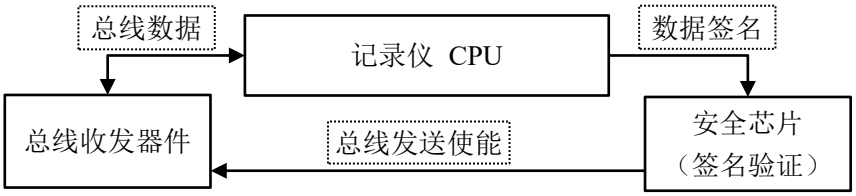

图 6 设备总线安全连接示意图

5.10　行驶记录仪安装自检

5.10.1　安装在汽车行驶记录仪的数据安全芯片应具备行驶记录仪安装自检功能，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) 任意未被屏蔽的输入信号在连续运行的48小时内未发生信号变化，对应故障位应被标识为故障。
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48小时内卫星定位持续无效，对应故障位应被标识为故障。

5.11　行驶记录仪管理

5.11.1　安装在汽车行驶记录仪的数据安全芯片应具备行驶记录仪管理功能，且符合以下要求：

a) 数据安全芯片保存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、安装自检、正式运行、返厂维修、设备报废等状态；
b) 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行驶记录仪管理平台的功能；
c) 记录仪在“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”，汽车电子标识序列号宜设为“99XXXXXXXXXX-X”；
d) 记录仪在转为“出厂待装”状态时，应删除生产检验用VIN号、车牌号码、汽车电子标识序列号，转为未设置状态；
e) 记录仪在“车辆预装”状态下可以设置车辆VIN号；
f) 记录仪未设置VIN号的，“安装自检”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。
g) 记录仪未设置车牌号码的，在“安全自检”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。
h) 记录仪未设置汽车电子标识序列号的，在“安全自检”完成（无故障）状态下可以设置，汽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。
i) 在“安全自检”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，安装汽车电子标识的，应设置汽车电子标识序列号；
j) 在“正式运行”状态下，已设置的VIN号、车牌号码和汽车电子标识序列号不能更改，需要修改车牌号码和汽车电子标识序列号的，应通过数据管理平台进行；

k） 记录仪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。

5.11.2 行驶记录仪设备生命周期状态转换如图 7：

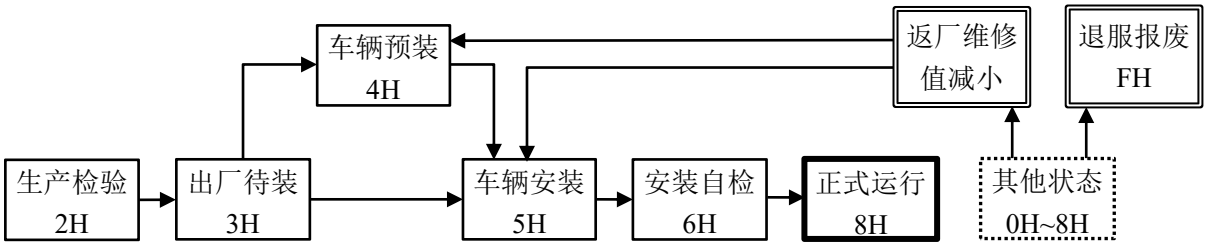

图 7 行驶记录仪设备生命周期状态转换示意图

5.11.3 行驶记录仪设备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（如表A.11：状态字位04～01）减小视为“返厂维修”

5.12 通信协议

数据安全芯片应支持附录A要求的通信协议。

6 性能要求

6.1 安全能力

6.1.1 数据安全芯片的安全能力应符合 GM/T 0008-2012 安全等级 2 或安全等级 3 的要求。

6.2 加密与解密

6.2.1 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；

6.2.2 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。

6.3 数字证书管理

6.3.1 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；

6.3.2 数据安全芯片存储和管理的数字证书数量应不少于 32。

6.4 数字签名及验签

6.4.1 数据安全芯片使用任意算法进行数字签名或验签，所需时间应不大于 200ms。

6.5 软件安全验证

6.5.1 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。

6.6 实时时钟

6.6.1　未进行校准的条件下，实时时钟的运行误差在连续的 30 天内应不大于 15 秒；

6.6.2　芯片主电源关闭条件下，使用后备电池供电时，消耗电流应不大于 2uA。

6.7　环境温度适应性

6.7.1　数据安全芯片应具备在于-40℃～85℃环境温度条件下工作的能力。

附　录　A
（规范性）
通信协议

A.1　通用约定

数据安全芯片的通信应遵循以下传输约定：

a） 本标准所有通信协议中的数据采用十六进制编码、8421BCD 码、ASCⅡ字符集及 GB 2312 字符集（采用 EUC-CN 表示方法）；涉及的数据类型缩写和数值范围约定：

--- Bit：比特位　　（0或1）
--- BIN：若干字节十六进制数据
--- U08：单字节无符号数　　（0 ～ 255）
--- S08：单字节有符号数　　（-128 ～ 127）
--- U16：双字节无符号数　　（0 ～ 65535）
--- S16：双字节有符号数　　（-32768 ～ 32767）
--- U32：四字节无符号数　　（0 ～ 4294967295）
--- S32：四字节有符号数　　（-2147483648 ～ 2147483647）
--- BCD：若干字节的压缩BCD码　　（0～99）（单字节表示范围）
--- ASC：仅包含英文字符和数字的ASCII字符串
--- STR：GB 2312字符串（含英文和数字字符）

b） 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；

c） 如未特别说明，本标准所有附录数据的存储、传输顺序采用大端模式（Big-Endian）模式：高字节在前（低位地址）、低字节在后（高位地址）；

d） 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’；

e） 本标准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；

f） 所有数据帧的长度应不大于 16K 字节；

g） 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；

h） 本附录中如未特别说明，“记录仪”特指记录仪设备或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；

i） 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；

j） 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　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，数据帧格式如表A.1：

表 A.1　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	
3.	3	2		命令字	Cmd	U16	
4.	5	2		数据帧长度	Size	U16	本表项目 1～7 部分的总字节数
5.	7	2		传输序列号	TImei	U16	
6.	9	xx	内容段	数据帧内容	Data	BIN	与命令字相关的数据
7.	...	2	校验段	校验项	Chk	U16	CRC16 计算值

A.2.2　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　命令字格式如表A.2：

表 A.2　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/应答码	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，如 b)表 A.3	

A.2.3.1　应答结果格式，含义如下：

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.2.3.2　错误代码信息如表A.3：

表 A.3　错误返回代码表

返回值	错误内容	备注
1H	指定的证书 ID 错误或证书不存在	

返回值	错误内容	备注
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　校验项为j）表A.1项目1～6所有字节的CRC16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　本协议中涉及安全算法，算法类别及对应代码如表A.4：

表 A.4　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	AES128 对称加解密算法	128		加解密/签名验签
5.	32H	AES256 对称加解密算法	256		加解密/签名验签
6.	52H	SM2 非对称加密算法	512	公钥	加密
7.		SM2 非对称解密算法	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	RSA2048 非对称加密算法（RSA2）	2048	公钥	加密
11.		RSA2048 非对称解密算法（RSA2）	2048	私钥	解密
12.	74H	RSA2048 非对称验签算法（RSA2）	2048	公钥	验签
13.		RSA2048 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

数据安全芯片涉及的数字证书列表如表A.5：

表 A.5 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			由固件固化
2.	01H	总根证书	SM2	SM1/SM4	01H	自身更新
3.	04H	GA 记录签名证书 1	SM2	SM1/SM4	01H	数字签名、Salt 值
4.	05H	GX 记录签名证书 2	SM2	SM1/SM4/AES	01H	数字签名、Salt 值
5.	08H	DM 软件安全证书	SM2/RSA			
6.	10H	GA 通信根证书	SM2	SM1/SM4	01H	
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	G3 通信根证书	SM2/RSA	SM1/SM4/AES	01H	GOV 备用 3
19.	31H	G3 通信加密证书	SM2/RSA	SM1/SM4/AES	01H/2AH	
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.	42H	VM2 通信根证书	SM2/RSA	SM1/SM4/AES	01H	车辆制造商备用
23.	43H	VM2 通信加密证书	SM2/RSA	SM1/SM4/AES	01H/42H	
24.	50H	VS1 通信根证书	SM2/RSA	SM1/SM4/AES	01H	经销商/运营商
25.	51H	VS1 通信加密证书	SM2/RSA	SM1/SM4/AES	01H/50H	

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
26.	52H	VS2 通信根证书	SM2/RSA	SM1/SM4/AES	01H	经销商/运营商备用
27.	53H	VS2 通信加密证书	SM2/RSA	SM1/SM4/AES	01H/52H	
28.	60H	VU1 通信根证书	SM2/RSA	SM1/SM4/AES	01H/40H	车辆使用者
29.	61H	VU1 通信加密证书	SM2/RSA	SM1/SM4/AES	01H/60H	
30.	62H	VU2 通信根证书	SM2/RSA	SM1/SM4/AES	01H/40H	车辆使用者备用
31.	63H	VU2 通信加密证书	SM2/RSA	SM1/SM4/AES	01H/62H	
32.	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 数字证书格式如表A.6：

表 A.6 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.5 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.4
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	

项目序号	字节序号	字节数	名称		数据类型	说明
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.4
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.6.1 如表 A.6.3
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.4
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.6.2 如表 A.6.4
24.	...	...	其他密钥	密钥定义数据	BIN	同本表 12～15 部分
25.	...	...	证书数字签名（如表 A.7）		U08	签名范围为项目 1～24
26.	...	2	证书校验字		U16	CRC16

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密钥公钥定义如32.表A.6.1

表 A.6.1 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密钥私钥定义如32.表A.6.2

表 A.6.2 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	

项目序号	字节序号	字节数	名称	数据类型	说明
3.	5	...	私钥 D 数据	BIN	

A.4.2.4 RSA密钥公钥定义如32.表A.6.3

表 A.6.3 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密钥私钥定义如32.表A.6.4

表 A.6.4 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”

项目序号	字节序号	字节数	名称	数据类型	说明
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 数字签名格式如表A.7：

表 A.7 数字签名格式表

<table>
<tr><th>项目序号</th><th>字节序号</th><th>字节数</th><th colspan="2">名称</th><th>数据类型</th><th>说明</th></tr>
<tr><td>1.</td><td>1</td><td>4</td><td rowspan="14">签名标识（明文）</td><td colspan="2">特征字符</td><td>ASC</td><td>固定为：“*GA*”</td></tr>
<tr><td>2.</td><td>5</td><td>8</td><td colspan="2">芯片 ID</td><td>BIN</td><td>如表 A.13</td></tr>
<tr><td>3.</td><td>13</td><td>1</td><td colspan="2">签名数字证书 ID</td><td>BCD</td><td></td></tr>
<tr><td>4.</td><td>14</td><td>2</td><td colspan="2">签名数字证书编号</td><td>BCD</td><td></td></tr>
<tr><td>5.</td><td>16</td><td>1</td><td colspan="2">签名算法 ID</td><td>U08</td><td>如表 A.4</td></tr>
<tr><td>6.</td><td>17</td><td>6</td><td colspan="2">签名日期时间</td><td>BCD</td><td></td></tr>
<tr><td>7.</td><td>23</td><td>2</td><td colspan="2">签名时间毫秒值</td><td>BCD</td><td>000～999</td></tr>
<tr><td>8.</td><td>25</td><td>6</td><td rowspan="7">源数据信息</td><td>源数据生成时间</td><td>BCD</td><td></td></tr>
<tr><td>9.</td><td>31</td><td>4</td><td>源数据长度</td><td>U32</td><td>总字节数</td></tr>
<tr><td>10.</td><td>35</td><td>32</td><td>源数据的摘要数据</td><td>BIN</td><td>SM3 算法</td></tr>
<tr><td>11.</td><td>67</td><td>1</td><td>数据属性 1</td><td>U08</td><td></td></tr>
<tr><td>12.</td><td>68</td><td>10</td><td>源数据设备唯一性 ID</td><td>BIN</td><td>行驶记录数据认证签名时为记录仪生产编号</td></tr>
<tr><td>13.</td><td>78</td><td>1</td><td>数据属性 2</td><td>U08</td><td></td></tr>
<tr><td>14.</td><td>79</td><td>14</td><td>源数据设备绑定 ID</td><td>STR</td><td>行驶记录数据认证签名时为车牌号码</td></tr>
<tr><td>15.</td><td>93</td><td>2</td><td colspan="3">签名密文数据长度</td><td>U16</td><td>本表 14 部分的总字节数</td></tr>
<tr><td>16.</td><td>95</td><td>...</td><td colspan="3">项目 1～13 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：按 GB/T 32918.2 要求）</td><td>BIN</td><td>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</td></tr>
</table>

项目序号	字节序号	字节数	名称	数据类型	说明
17.	...	2	校验段	U16	CRC16

注：

一个数字签名的长度最少为128字节。

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。

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生产编号，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

芯片的基础信息通信命令字如表A.8

表 A.8 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）	“AS5621M”
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	记录仪编号	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0000H，请求通信初始化帧格式定义如表A.9：

表 A.9 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如表A.10：

表 A.10　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 = 0000H
2.	9	8	内容段	芯片型号	ASC	如“AS5621M”
3.	17	8		芯片 ID	BIN	如表A.13
4.	25	10		记录仪编号	BIN	如表A.13
5.	35	6		芯片日期时间	BCD	如“191001101234”
6.	41	2		记录仪（芯片）状态字	U16	如表A.11
7.	43	2	校验段		U16	

表 A.11　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：卫星定位位置无效　0：正常	
14	速度信号	1：车辆速度信号异常　0：正常	
13～08	未定义		
08～05	维修计次	00H：芯片未初始化 01H：芯片出厂状态，已配置记录仪编号 02H：记录仪生产检验阶段 03H：记录仪出厂待装 04H：预安装状态，可设置 VIN 05H：安装状态，可设置 VIN、车牌号 06H：安装自检状态 08H：正式运行状态 0FH：报废/退服状态 1XH，2XH...FXH：返修后状态 （X 参照 02H ～ 0FH）	
04～01	记录仪（芯片）生命周期状态		

A.6.3　芯片基本信息

A.6.3.1　芯片基本信息包含记录仪编号、RTC日期时间、芯片状态等内容。

A.6.3.2　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，以秒1次的间隔发送通信心跳（0010H）数据帧；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.6.3.3　请求芯片基本信息帧格式定义如表A.12：

表 A.12　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	
6.	25	1		行驶方向	U08	
7.	26	1		行驶速度	U08	
8.	27	2		开关量信号	BIN	
9.	29	1		行驶速度参考	U08	
10.	30	1		数据状态	BIN	
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.6.3.4　应答芯片基本信息帧格式定义如表A.13：

表 A.13　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	1	内容段	芯片 ID	厂商代码	BCD	2位数字，如“31”
3.	10	3			型号代码	BCD	如“562101”
4.	13	4			芯片序列号	BCD	如“32530001”
5.	17	2		记录仪编号	制造商简称	ASC	如“DN”
6.	19	3			产品型号简称	ASC	如“VDR”

项目序号	字节序号	字节数	名称			数据类型	说明
7.	22	4			产品流水号	BCD	如“07290002”
8.	26	1			未定义	BIN	00H
9.	27	6		芯片日期时间		BCD	
10.	33	2		记录仪（芯片）状态字		U16	如表A.11
11.	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.15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：2020-03-20

A.6.4.2 请求芯片详细信息帧格式定义如表A.14：

表 A.14 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 = 0030H
2.	9	10	内容段	记录仪编号	ASC	
3.	19	2	校验段		U16	

A.6.4.3 应答芯片详细信息帧格式定义如表A.15

表 A.15 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 = 8030H
2.	9	10	内容段	记录仪编号	ASC	
3.	19	6		芯片日期时间	BCD	
4.	25	2		记录仪（芯片）状态字	U16	如表A.11
5.	27	2		详细信息长度	U16	

6.	29	6		详细信息文本	STR	
7.	35	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 记录仪参数命令字如表A.16

表 A.16 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（ASC）	
2.	8110H	上行	应答读取记录仪预置参数	预置参数（ASC）	管理平台参数
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（BIN）	长度不超出 1kB
5.	0130H	下行	请求写入记录仪一般参数	读取位置及长度	
6.	8130H	上行	应答写入记录仪一般参数	一般参数（BIN）	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（ASC）	
8.	8140H	上行	应答读取记录仪关键参数	关键参数（ASC）	
9.	0150H	下行	请求设置记录仪关键参数	记录仪编号（ASC）	
10.	8150H	上行	应答设置记录仪关键参数	关键参数（ASC）	
11.	0160H	下行	请求进入安装自检	记录仪编号（ASC）	
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（ASC）	
14.	8170H	上行	应答进入正式运行		
15.	0180H	下行	请求变更记录仪生命周期状态	记录仪编号（ASC）	
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（ASC）	
18.	8190H	上行	应答记录仪实时验证码		

A.7.2 预置参数读取

A.7.2.1 预置参数为记录仪管理平台网络连接参数，含主服务器域名和备服务器域名等信息：

A.7.2.2 请求读取预置参数数据帧格式如表A.17：

表 A.17　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	ASC	
3.	19	2	校验段		U16	

A.7.2.3　应答读取预置参数数据帧格式如表A.18：

表 A.18　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		ASC	
3.	19	6		芯片日期时间		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	20H
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	
11.	99	3		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			GB/T19056 协议方式	ASC	‘T’:TCP　‘U’:UDP
15.	105	2			GB/T19056 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/T808 协议方式	ASC	‘T’:TCP　‘U’:UDP
20.	113	2			JT/T808 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如表A.19：

表 A.19 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	ASC	
3.	19	6		日期时间	BCD	应答时为芯片时间
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如表A.20：

表 A.20 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
8.	1	8	起始段		BIN	Cmd = 8120H （读取） Cmd = 8130H （写入）
9.	9	10	内容段	记录仪编号	ASC	
10.	19	6		日期时间	BCD	应答时为芯片时间
11.	25	2		读取/写入开始位置	U16	
12.	27	2		读取/写入字节长度	U16	
13.	29	2		读取/写入 数据内容	BIN	请求读取时为空
14.	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，有产品状态标识（VDR_SAT），车辆的VIN码（VDR_VIN），车辆的车牌号码（VDR_VCP），车辆的汽车电子标识序列号（VDR_VID）。

示例：

VDR_SAT:03

VDR_VIN:VCAB9ACC3DA123456

VDR_VCP:苏BC123456

VDR_SWT:0000000000000000

A.7.4.2 请求读取关键参数数据帧格式如表A.21：

表 A.21 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	ASC	
3.	19	2	校验段		U16	

表 A.22 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	ASC	
3.	19	6		芯片日期时间	BCD	
4.	25	2		记录仪（芯片）状态字	U16	如表A.11
5.	27	2		开关量信号故障状态信息	U16	如0
6.	29	2		开关量检测屏蔽字	U16	如0
7.	31	17		车辆 VIN	ASC	
8.	48	14		车辆车牌号码	STR	
9.	62	13		车辆汽车电子标识序列号	ASC	
10.	75	32		附加 Salt 值数据摘要		本表 2～9 项并附加 Salt 值，Salt 值为 A.7.5 设置的值
11.	107	2	校验段		U16	

表 A.23　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： 24 小时内无变化 （通电运行时间） 检测屏蔽： 该信号检测屏蔽	故障状态信息： 24 小时内有变化 （通电运行时间） 检测屏蔽： 该信号需要检测	
15	制动开关			
14	左转向			
13	右转向			
12	远光			
11	近光			
10	雾灯			
09	倒车			
08	车门			
07	安全带（驾驶员座椅）			
06	雨刮器			
05～01	自定义			

A.7.5　关键参数设置

A.7.5.1　关键参数可以写入或读出，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：车辆的汽车电子标识序列号，ASC 类型，13 字节；

d）　SLT：数据摘要 Salt 值，BIN 类型，16 字节。

A.7.5.2　读取/写入关键参数时数据帧内容段数据格式如表A.24：

表 A.24　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 = 0130H / 0140H Cmd = 8130H / 8140H
2.	9	10	内容段	记录仪编号	ASC	
3.	19	6		日期时间	BCD	应答时为芯片时间
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	

表 A.25　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 = 0130H / 0140H Cmd = 8130H / 8140H
2.	9	10	内容段	记录仪编号	ASC	
3.	19	6		日期时间	BCD	应答时为芯片时间
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　安装自检

A.7.6.1　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：

表 A.26　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	ASC	
3.	19	6		日期时间	BCD	
4.	25	2	校验段		U16	

表 A.27　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		芯片日期时间	BCD	
4.	25	2		记录仪（芯片）状态字	U16	进入安装自检 如表A.11
5.	27	2		开关量信号故障状态信息		如表A.23

项目序号	字节序号	字节数	名称		数据类型	说明
6.	29	2		开关量检测屏蔽字		如表A.23
7.	31	17		车辆VIN		
8.	48	14		车辆车牌号码		
9.	62	2	校验段		U16	

A.7.7　正式运行

表 A.28　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	ASC	
3.	19	6		日期时间	BCD	
4.	25	2	校验段		U16	

表 A.29　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	ASC	
3.	19	6		芯片日期时间	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		如表A.23
6.	29	2		开关量检测屏蔽字		如表A.23
7.	31	17		车辆VIN		
8.	48	14		车辆车牌号码		
9.	62	2	校验段		U16	

扩展的错误代码：0CH：安装自检未完成，故障信息未消除

A.7.8　生命周期状态变更

A.7.8.1　生命周期变更是记录仪生命周期管理的必要步骤，如表A.30：

表 A.30　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
5.	1	8	起始段		BIN	Cmd = 0180H
6.	9	10	内容段	记录仪编号	ASC	
7.	19	6		日期时间	BCD	
8.	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 如表 A.23
9.	27	4		未定义	BIN	
10.	31	1		原生命周期状态	U08	表 A.11 的位 04～01
11.	32	1		新生命周期状态	U08	表 A.11 的位 04～01
12.	33	2	校验段		U16	

芯片状态转换图如5.11部分；

由其他状态进入“返厂维修”状态时，表A.11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。

本节指令（0180H）不支持进入“安装自检”状态，其专有指令如A.7.6。

本节指令（0180H）不支持进入“正式运行”状态，其专有指令如A.7.7。

表 A.31　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
10.	1	8	起始段		BIN	Cmd = 8180H/818XH
11.	9	10	内容段	记录仪编号	ASC	
12.	19	6		芯片日期时间	BCD	
13.	25	1		原生命周期状态	U08	表 A.11 的位 08～01
14.	26	1		新生命周期状态	U08	表 A.11 的位 08～01
15.	27	32		设置结果描述	STR	成功/失败原因
16.	59	2	校验段		U16	

A.7.9　实时验证码

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，有安全芯片依据记录仪编号、安全芯片时间和Salt值生成，为这三部分数据（共31字节）数据摘要的最后4字节组成的U32十进制值最低6位数字，如表A.32：

表 A.32　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
13.	1	8	起始段		BIN	Cmd = 0190H
14.	9	10	内容段	记录仪编号	ASC	
15.	19	6		日期时间	BCD	
16.	25	2	校验段		U16	

表 A.33　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
17.	1	8	起始段		BIN	Cmd = 8180H/818XH
18.	9	10	内容段	记录仪编号	ASC	
19.	19	6		芯片日期时间	BCD	
20.	25	6		实时验证码	ASC	6 位数字
21.	31	2	校验段		U16	

A.8　车联网双向鉴权

A.8.1　命令字分类

记录仪的车联网双向鉴权的登过程命令请参照如表A.34：

表 A.34　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	鉴权数据包	
3.	0210H	下行	验证平台鉴权数据	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

表 A.35 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	ASC	
3.	19	1		数字证书 ID	U08	如表 A.5
4.	20	1		鉴权算法 ID	U08	如表 A.4
5.	21	1		特定数据长度	U08	
6.	22	...		特定数据	BIN	记录仪鉴权信息 由平台分配
7.	...	2	校验段		U16	

表 A.36 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		ASC	
4.	23	6		芯片日期时间		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	
7.	34	2		鉴权数字证书编号		BCD	
8.	36	1		鉴权算法 ID		U08	如表 A.4
9.	37	2		设备状态字		U16	如表A.11
10.	39	1		附加数据长度		U08	可为 0
11.	40	...		附加数据		BIN	可为空
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 部分摘要
14.	...	...			安全芯片数据	BIN	预留扩展
15.	...	2	校验段			U16	

A.8.3 平台反向鉴权

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，格式如表A.37：

表 A.37 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		ASC	
4.	23	6		平台日期时间		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	
7.	34	2		鉴权数字证书编号		BCD	
8.	36	1		鉴权算法 ID		U08	如表 A.4
9.	37	2		设备状态字		U16	
10.	39	1		附加数据长度		U08	可为 0
11.	...	...		附加数据		BIN	记录仪鉴权信息（明文）
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 部分摘要
14.	...	...			联网通信参数	BIN	
15.	...	2	校验段			U16	

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，数据帧格式如下：

表 A.38 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 = 821XH
2.	9	10	内容段	记录仪编号	ASC	
3.	19	6		芯片日期时间	BCD	
4.	25	...		联网通信参数	BIN	SM4 动态密钥等

项目序号	字节序号	字节数	名称		数据类型	说明
				或鉴权不通过原因描述		由表 A.37 项目 14 解密
5.	41	2	校验段		U16	

Cmd为8210H时，表示反向鉴权通过，否则为不通过，不通过时表A.38项目4为原因描述。

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。

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（表A.37项目11）。

表 A.39　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.40　联网通信 ID 定义

项目序号	参数 ID	名称	数据类型	参数长度	说明
1.	＜E000H	如 JT/T 808			
2.	E001H	连续行驶状态传输间隔	U16	2	单位：秒
3.	E002H	网络心跳帧传输间隔	U16	2	单位：秒
4.	E010H	当前路段限速值	U16	2	单位：km/h
5.	E100H	SM4 动态密钥	BIN	16	

A.9　联网数据加解密

A.9.1　命令字分类

记录仪的车联网数据加密命令请参照如表A.41：

表 A.41　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	

项目序号	Cmd	方向	命令/应答 说明	内容段数据	备注
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

表 A.42 请求加密通信帧格式表

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	如表 A.5
3.	10	1		算法 ID	U08	如表 A.4
4.	11	2		数据包长度	U16	本表序号 5 总字节数
5.	13	...		需加密的数据包	BIN	
6.	...	2	校验段		U16	

表 A.43 应答加密通信帧格式表

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 = 8240H
2.	9	1	内容段	数字证书 ID	U08	如表 A.4
3.	10	1		算法 ID	U08	如表 A.4
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

表 A.44 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	如表 A.5
3.	10	1		算法 ID	U08	如表 A.4
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	

表 A.45　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	如表 A.5
3.	10	1		算法 ID	U08	如表 A.4
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

记录仪的行驶数据记录认证程命令请参照如表A.46：

表 A.46　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	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

项目序号	Cmd	方向	命令/应答 说明	内容段数据	备注
	82E0H 82F0H				效，其他为过程数据

A.10.2 摘要生成数字签名

表 A.47 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	如表 A.4 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	

表 A.48 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	如表 A.7
9.	...	2	校验段		U16	

A.10.3 数据生成数字签名

表 A.49 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		特征字符	ASC	固定为：“*GA*”

项目序号	字节序号	字节数	名称		数据类型	说明
3.	13	1	内容段	数字证书 ID	BCD	
4.	14	1		签名算法 ID	U08	如表 A.4 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	

表 A.50　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	4	内容段	数字签名	BIN	如表 A.7
3.	...	2	校验段		U16	

A.10.4　数字签名验签

表 A.51　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	4	内容段	数字签名	BIN	如表 A.7
3.	...	2	校验段		U16	

表 A.52　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

表 A.53 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	

记录仪在正式运行状态（芯片状态字为X8H，如表A.11）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）。

表 A.54 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	如表 A.53 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

表 A.55 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	如表 A.53 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	

记录仪在正式运行状态（芯片状态字为X8H，如表A.11）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）。

表 A.56　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	如表 A.53 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

记录仪的防护存储器写保护初始化及解锁过程命令请参照如表A.57：

表 A.57　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	
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	

A.11.2　存储器保护初始化

表 A.58　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

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	1		算法 ID		U08	项目 5～9 加密算法
4.	12	1		密文数据长度		U08	项目 5～9 总字节数
5.	13	4		加密数据（初始化信息）	特征字符串	ASC	“!GA!”
6.	17	4			存储器信息	ASC	如厂商、容量：“LS8G”
7.	21	16			写保护密钥	BIN	存储器生成的密钥
8.	37	16			随机数	BIN	
9.	53	...			填充数	BIN	可选，PKCS7 填充
10.	45	2	校验段			U16	

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后续的32字节进行解密，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。

表 A.59　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	1		算法 ID		U08	项目 5～9 加密算法
4.	12	1		密文数据长度		U08	项目 5～9 总字节数
5.	13	4		加密数据（密钥为写保护密钥）	特征字符	ASC	“!GA!”
6.	17	4			解锁轮次	U32	初始化为 0
7.	21	6			日期时间	BCD	
8.	27	18			随机字节	BIN	
9.	45	32			摘要数据	BIN	项目 5～8 以及写保护密钥（共 48 字节）的数据摘要
10.	77	2	校验段			U16	

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，摘要数据源由：“特征字符+密钥轮次+日期时间+随机字节+写保护密钥”组成。

A.11.3 存储器单次解锁

表 A.60 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	

表 A.61 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	1		算法 ID		U08	项目 5～9 加密算法
4.	12	1		密文数据长度		U08	项目 5～9 总字节数
5.	13	4		加密数据（密钥如表 A.58 项目 7）	特征字符	ASC	“!GA!”
6.	17	4			解锁轮次	U32	加 1 后发出并保存
7.	21	6			日期时间	BCD	
8.	27	18			随机字节	BIN	
9.	45	32			摘要数据	BIN	项目 5～8 以及写保护密钥（共 48 字节）的数据摘要
10.	77	2	校验段			U16	

附　录　B
（规范性）
扩展通信协议

B.1　芯片性能测试

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.1.1　加密及签名性能测试

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。

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帧（如表B.3）的方式发送。

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	如表 A.5
4.	12	1		测试算法 ID	U08	如表 A.4
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	

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	如表 A.5
4.	12	1		测试算法 ID	U08	如表 A.4
5.	13	4		密文或签名最后 4 字节数据	BIN	
6.	17	2	校验段		U16	

B.1.2 芯片验签性能测试

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	如表 A.5
4.	12	1		测试算法 ID	U08	如表 A.4
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	

表 B.5　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 = 80A0H
2.	9	2	内容段	测试次数	U16	
3.	11	1		测试证书 ID	U08	如表 A.5
4.	12	1		测试算法 ID	U08	如表 A.4
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

记录仪的软件安全及OTA命令请参照如表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.2.1　初始化软件信息

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（公钥加密）	记录仪编号	ASC	
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	

项目序号	字节序号	字节数	名称		数据类型	说明
6.	41	6		软件生成日期时间	BCD	
7.	47	1		软件芯片控制策略	U08	01H：延时后为高电平 02H：延时后为低电平
8.	48	1		软件芯片控制延时	U08	时间：秒，00H 为无效
9.	49	1		功能使能控制策略 （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		功能使能控制延时	U08	时间：秒，00H 为无效
11.	51	32		软件代码摘要数据	BIN	
12.	83	...		随机数据	BIN	可选，PKCS1 填充
13.	...	2	校验段		U16	

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	ASC	
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		软件生成日期时间	BCD	
7.	47	1		软件芯片控制策略	U08	如表 B.7 项目 7
8.	48	1		软件芯片控制延时	U08	如表 B.7 项目 8
9.	49	1		功能使能控制策略	U08	如表 B.7 项目 9
10.	50	1		功能使能控制延时	U08	如表 B.7 项目 10
11.	51	2	校验段		U16	

扩展的错误代码如下：

0CH：软件信息已经初始化

B.2.2 验证软件信息

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（公钥加密）	记录仪编号	ASC	
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	

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	ASC	
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	

扩展的错误代码如下：

0CH：软件信息未初始化

0DH：时间戳重复或回溯

B.2.3 软件升级安全

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		记录仪编号	ASC	

项目序号	字节序号	字节数	名称			数据类型	说明
3.	19	6	内容段（公钥加密）	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			软件生成日期时间	BCD	
7.	47	1			软件芯片控制策略	U08	如表 B.7 项目 7
8.	48	1			软件芯片控制延时	U08	如表 B.7 项目 8
9.	49	1			功能使能控制策略	U08	如表 B.7 项目 9
10.	50	1			功能使能控制延时	U08	如表 B.7 项目 10
11.	51	32			软件代码摘要数据	BIN	
12.	83	8		新版本验证信息	记录仪硬件信息	ASC	
13.	91	8			记录仪软件版本号	ASC	
14.	99	6			软件生成日期时间	BCD	
15.	105	1			软件芯片控制策略	BIN	如表 B.7 项目 7
16.	106	1			软件芯片控制延时	ASC	如表 B.7 项目 8
17.	107	1			功能使能控制策略	ASC	如表 B.7 项目 9
18.	108	1			功能使能控制延时	BCD	如表 B.7 项目 10
19.	109	32			软件代码摘要数据	BCD	
20.	141	...		随机数据		BIN	
21.	...	2	校验段			U16	

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	ASC	
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		软件生成日期时间	BCD	新版本信息
7.	47	1		软件芯片控制策略	U08	如表 B.7 项目 7

项目序号	字节序号	字节数	名称		数据类型	说明
8.	48	1		软件芯片控制延时	U08	如表 B.7 项目 8
9.	49	1		功能使能控制策略	U08	如表 B.7 项目 9
10.	50	1		功能使能控制延时	U08	如表 B.7 项目 10
11.	51	2	校验段		U16	

扩展的错误代码如下：

0CH：软件信息未初始化

0DH：原版本软件信息错误

B.3 总线及控制安全

记录仪的联网总线及控制安全程命令请参照如表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.3.1 总线数据发送使能

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		
7.	...	...		总线数据包		
8.	...	128		总线数据包数字签名		
9.	...	2	校验段		U16	

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.3.2　远程控制使能

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
6.	33	2		远程控制数据包长度		
7.	...	...		远程控制数据包		
8.	...	128		远程控制数字签名		
9.	...	2	校验段		U16	

表 B.17　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	

项目序号	字节序号	字节数	名称		数据类型	说明
4.	25	6		芯片时间	BCD	
5.	31	2		远程控制使能时间长度	U16	秒
6.	...	2	校验段		U16	

B.4 数字证书管理

记录仪的安全证书表B.18命令如：

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	上行	请求删除数字证书	记录仪编号 证书 ID	
2.	8400H	下行	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.4.1 数字证书删除

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	ASC	
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.	...	128		数字签名	BIN	项目 2～5 数字签名
7.	...	2	校验段		U16	

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		记录仪编号	ASC	

项目序号	字节序号	字节数	名称		数据类型	说明
3.	19	6	内容段	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.	...	2	校验段		U16	

B.4.2 数字证书更新

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	ASC	
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		加密用算法	U08	
9.	31	2		数字证书长度	U16	
10.	33	...		加密的数字证书	BIN	用 6-8 定义的加密算法
11.	...	128		数字签名	BIN	表 2-10 部分数字签名
12.	...	2	校验段		U16	

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	ASC	
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.	...	2	校验段		U16	

B.5 联网数据透传

记录仪的联网数据透传过程命令如表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.5.1 数据透明上传

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		需透传的数据包长度	U16	
7.	35	...		需透传的数据包	BIN	
8.	...	2	校验段		U16	

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	

项目序号	字节序号	字节数	名称		数据类型	说明
4.	12	...		执行结果描述	STR	
5.	...	2	校验段		U16	

B.5.2 数据透明下发

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		收到的数据包长度	U16	
4.	12	...		收到的数据包	BIN	
5.	...	2	校验段		U16	

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		收到的数据包长度	U16	
4.	12	2	校验段		U16	

B.5.3 断开平台连接

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	

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