ICS 35.240.01
L67

团　体　标　准

T/ZSPH ***-2022

智慧桥梁物联监测安全技术要求

Security Technology Requirements for Monitoring System of Smart Bridges in Internet of Things

2022–**–**发布　　2022–**–** 实施

中关村乐家智慧居住区产业技术联盟 发布

目　　次

前　　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国标准化研究院、中外建设信息有限责任公司等提出。

本文件由中关村乐家智慧居住区产业技术联盟归口。

本文件起草单位：

本文件主要起草人：

智慧桥梁物联监测安全技术要求

1 范围

本文件规定了智慧桥梁物联监测系统的总体安全要求以及安全加密要求等。

本文件适用于智慧桥梁物联监测系统和相关安全产品的设计、建设、运营和使用等相关方。

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/T 22186-2016 信息安全技术 具有中央处理器的IC卡芯片安全技术要求
GB/T 22239-2019 信息安全技术 信息系统安全等级保护基本要求
GB/T 25058-2019 信息安全技术 网络安全等级保护实施指南
GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求
GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求
GB/T 28449-2018 信息安全技术 网络安全等级保护评测过程指南
GB/T 28827.1-2012 信息技术服务 运行维护 第1部分：通用要求
GB/T 28827.2-2012 信息技术服务 运行维护 第2部分:交付规范
GB/T 28827.3-2012 信息技术服务 运行维护 第3部分:应急响应规范
GB/T 33474-2016 物联网 参考体系架构
GB/T 33745-2017 物联网 术语
GB/T 37044-2018 信息安全技术 物联网安全参考模型及通用要求
GB/T 37092-2018 信息安全技术 密码模块安全要求
GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求
GM/Z 0001-2013 密码术语
GM/T 0002-2012 SM4分组密码算法
GM/T 0003-2012 SM2椭圆曲线公钥密码算法
GM/T 0004-2012 SM3密码杂凑算法
GM/T 0006-2012 密码应用标识规范
GM/T 0017-2012 智能密码钥匙密码应用接口数据格式规范
JTG B01-2014 公路工程技术标准

3 术语和定义

下列术语和定义适用于本文件。

3.1

身份认证 identity authentication

通过一定的手段，完成对用户、设备、平台等的身份确认。

3.2

加密 encryption

以某种特殊的算法改变原有的信息数据，使得未授权的用户即使获得了已加密的信息，但因不知解密的方法，仍然无法了解信息的内容。

3.3

安全模块 security module

含有密码算法、安全功能，可实现密钥管理机制的相对独立的软件、硬件、固件或其组合。
[来源：GM/Z 0001-2013，2.1]

3.4

密钥 key

控制密码算法运算的关键信息或参数。
[来源：GM/Z 0001-2013，2.63]

3.5

解密 decryption

将“密文”变为“明文”的过程。

3.6

算法 algorithm

通过准确而完整的指令，实现解决问题的策略机制。

4 总体要求

4.1 参考模型

智慧桥梁物联监测系统应按照GB/T 33473的要求划分为用户域、目标对象域、感知控制域、服务提供域、运维管控域和资源交换域六个功能域，并按照GB/T 37044的要求划分为感控安全区、网络安全区、应用安全区和运维安全区五个安全区，物联网参考模型见图1，并符合下列要求：

a）感知控制域中应包含标签识别系统和安全加密系统；

b）服务提供域中基础服务系统应包含安全加密系统平台；

c）资源交换域中应配备安全加密系统设备或设备集群；

d）运维管控域中应包含安全加密模块，由第三方单位进行运维服务的，运维单位应配备安全加密设备或设备集群；

e）用户域中用户系统应配备安全加密模块、设备或设备集群。

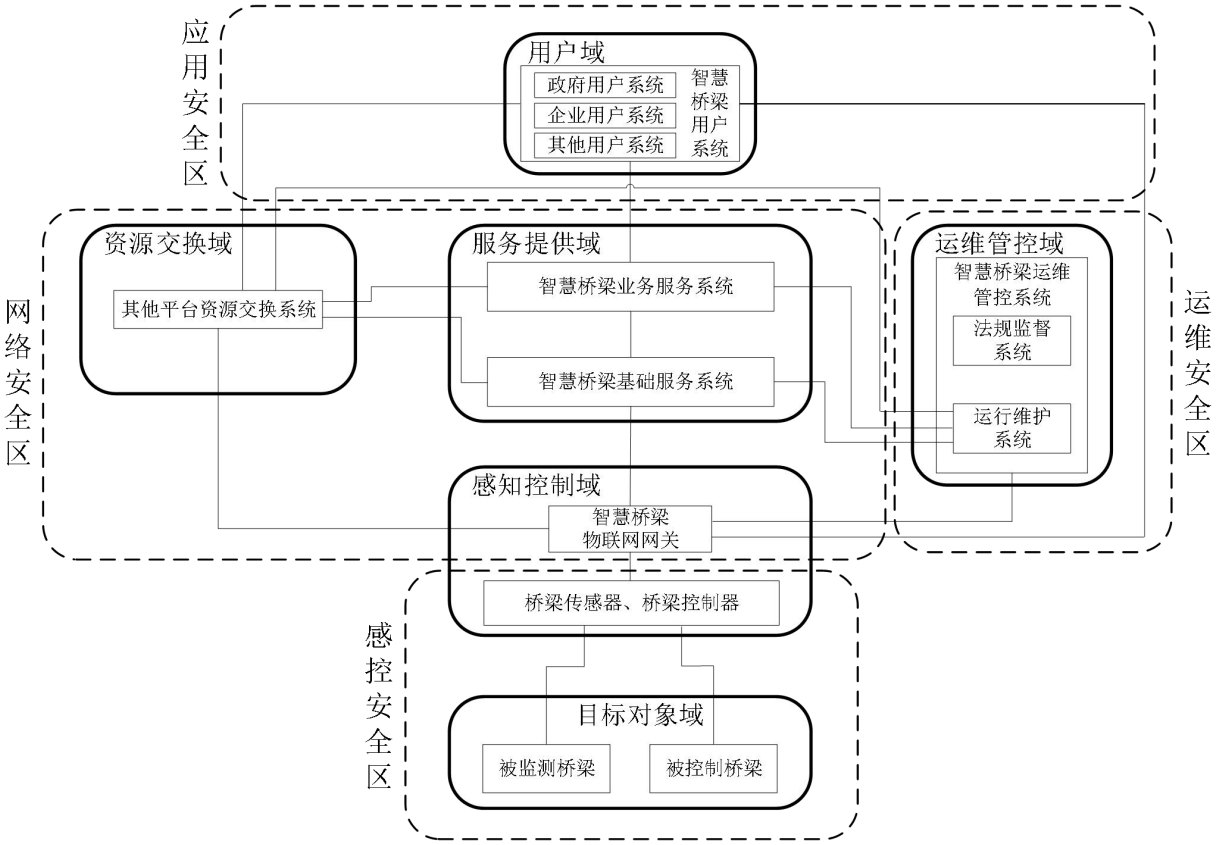

图 1 智慧桥梁物联监测系统参考模型

4.2 等级划分及要求

4.2.1 等级划分依据

根据JTG B01《公路工程技术标准》中关于桥涵的要求将桥梁划分为表1给出的四个等级：特大桥、大桥、中桥和小桥。根据桥梁等级的不同，智慧桥梁物联监测系统应满足不同的安全等级要求。

表1 桥涵分类

桥涵分类	多孔跨径总长 L（m）	单孔跨径 Lk（m）
特大桥	L＞1000	Lk＞150
大桥	100≤L≤1000	40≤Lk≤150
中桥	30＜L＜100	20≤Lk＜40
小桥	8≤L≤30	5≤Lk＜20

4.2.2 等级要求

根据桥梁等级不同，智慧桥梁物联监测系统应满足的安全要求见表2。

表 2 等级要求

序号	等级	安全区域	要求
1	小桥级智慧桥梁物联监测系统	感控安全区	应至少满足等保二级及以上要求； 满足其他法律法规及相关标准的要求。
		网络安全区	应至少满足等保二级及以上要求；

			满足其他法律法规及相关标准的要求。
		应用安全区	应至少满足等保二级及以上要求； 满足其他法律法规及相关标准的要求。
		运维安全区	应至少满足等保二级及以上要求； 满足其他法律法规及相关标准的要求。
2	中桥级智慧桥梁物联监测系统	感控安全区	应至少满足等保二级及以上要求； 满足其他法律法规及相关标准的要求。
		网络安全区	应至少满足等保三级及以上要求； 满足其他法律法规及相关标准的要求。
		应用安全区	应至少满足等保三级及以上要求； 满足其他法律法规及相关标准的要求。
		运维安全区	应至少满足等保二级及以上要求； 满足其他法律法规及相关标准的要求。
3	大桥级智慧桥梁物联监测系统	感控安全区	应至少满足等保二级及以上要求； 满足其他法律法规及相关标准的要求。
		网络安全区	应至少满足等保三级及以上要求； 满足其他法律法规及相关标准的要求。
		应用安全区	应至少满足等保三级及以上要求； 满足其他法律法规及相关标准的要求。
		运维安全区	应至少满足等保三级及以上要求； 满足其他法律法规及相关标准的要求。
4	特大桥级智慧桥梁物联监测系统	感控安全区	应至少满足等保三级及以上要求； 满足其他法律法规及相关标准的要求。
		网络安全区	应至少满足等保三级及以上要求； 满足其他法律法规及相关标准的要求。
		应用安全区	应至少满足等保三级及以上要求； 满足其他法律法规及相关标准的要求。
		运维安全区	应至少满足等保三级及以上要求； 满足其他法律法规及相关标准的要求。

5 安全要求

5.1 安全加密管控要求

5.1.1 安全加密管控架构

智慧桥梁物联监测系统安全加密管控应包含行业密码平台、数字身份安全服务平台（DISP），以及安全模块等。智慧桥梁物联监测系统安全加密管控架构见图2所示。

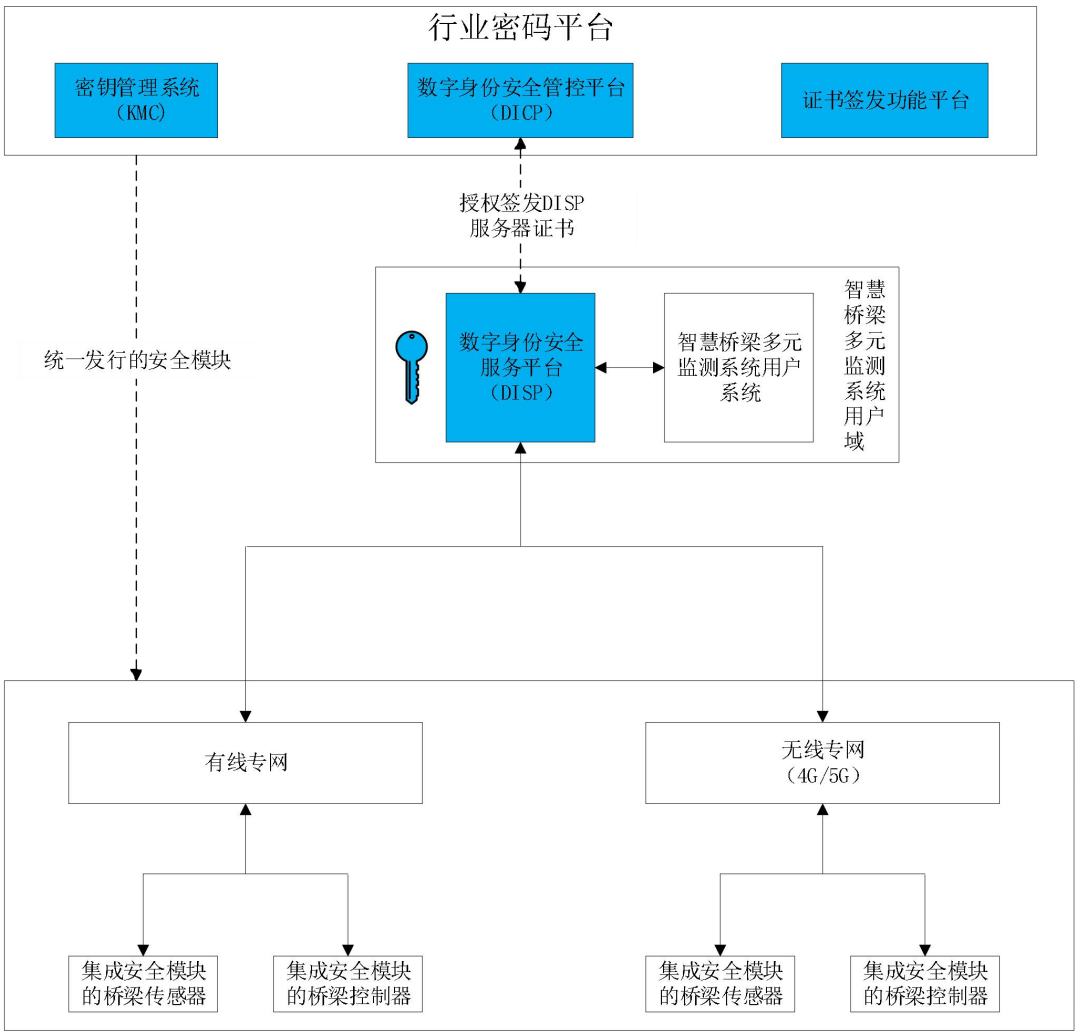

图 2 智慧桥梁物联监测系统安全加密管控架构图

5.1.2 行业密码平台要求

基础服务系统中安全加密系统平台应包括行业密码平台。行业密码平台具备以下功能：

a) 向数字身份安全服务平台（DISP）签发服务器证书，用于端到端的数字身份认证和密钥协商；服务器证书基于 SM2 签名验签算法，服务器数字证书格式采用标准 x509 格式；

b) 实现安全模块的发行管控，包括离线发行、在线发行。发行管理类密钥基于国密 SM4 算法，便于安全模块的逐级发行管控，且容易实现安全模块二次发行过程的安全管控，确保安全模块的可信、可管和可控性；

c) 给安全模块签发终端数字证书，用于端到端的数字身份认证和密钥协商。数字证书格式采用标准 x509 格式。

5.1.3 DISP 与智慧桥梁物联监测用户系统

基础服务系统的安全加密系统平台应包括数字身份安全服务平台（DISP），DISP 应部署在用户系统的本地机房，智慧桥梁物联监测系统通过调用 DISP 的安全服务接口 API，实现以下功能：

a) 认证桥梁传感器或桥梁控制器等设备的合法性；

b) 与桥梁监测传感器或桥梁监测控制器等设备建立安全的通信链路，确保用户系统所下发数据的机密性、完整性和不可抵赖性。

5.1.4 安全模块

5.1.4.1 一般规定

安全模块应包括安全芯片（SE）、软算法SDK、外置安全模块（安全盒子）等。应在智慧桥梁物联监测系统的桥梁传感器或控制器等设备中集成安全模块，安全模块应装载行业密码平台签发的终端数字证书，为桥梁传感器或桥梁控制器设备提供双向认证和安全加解密能力。安全模块应符合GB/T 37092-2018的相关要求。不同的应用场景可采用不同形态的安全模块，具体可按照以下要求执行：

a) 新增终端设备具有硬件改造条件，建议集成硬件安全芯片（SE）；
b) 存量终端设备不易集成安全芯片（硬件 SE），但终端软件操作系统支持升级，可通过软件升级集成软算法 SDK；
c) 存量终端不易硬件改造，且不易通过软件升级支持软算法 SDK 时，可通过终端设备的扩展网口配置外置安全模块（安全盒子）。

5.1.4.2 安全芯片（SE）

通过硬件改版集成SE后，为终端设备提供双向认证、业务数据加解密服务。并应符合下列要求：

a) 安全芯片作为独立的安全模块，为终端设备提供双向认证、业务数据加解密服务；
b) 安全芯片需加载住建行业密码平台签发的 SE 证书，证书格式为标准 x509 格式，在双向认证过程中，SE 和 DISP 通过交换证书以及计算签名值实现数字身份认证；
c) SE 的发行管理密钥体系、应用文件、指令集等由 SE 提供商自定义，不做具体要求，附录 A 仅给出参考示例。

5.1.4.3 软算法模块（SDK）

软算法模块（SDK）主要通过提供软算法库的方式，为终端设备提供双向认证、业务数据加解密服务。并应符合下列要求：

a) 软算法模块的优点在于终端设备不需要进行硬件改版，只需要通过集成软算法 SDK 的方式即可提升终端设备的安全能力；缺点是软算法 SDK 的安全级别相对较低，存在密钥泄露风险；
b) 对于非高安全级别的应用场景，可通过升级终端设备固件，集成软算法模块 SDK 方式提升终端安全；
c) SDK 具有终端设备证书写入功能。

5.1.4.4 外置安全模块（安全盒子）

外置安全模块（安全盒子）通过在终端可控环境下，通过配置一个外置的物理硬件安全盒子，为终端设备提供双向认证、业务数据加解密服务。应用技术架构见图3。并具有以下特点：

a) 终端侧软硬件基本不需改造，桥梁监测传感器或桥梁监测控制器设备通过自身的网口或串口与外置安全模块集成，即可实现与平台端的双向认证和业务数据加解密，确保通信链路的机密性、完整性和不可抵赖性；
b) 由主控芯片、安全芯片及其外围电路构成，提供两个以太网接口（一个用以连接上行通道，一个用以连接受保护设备）、Uart 串口，采用 12V DC 供电。

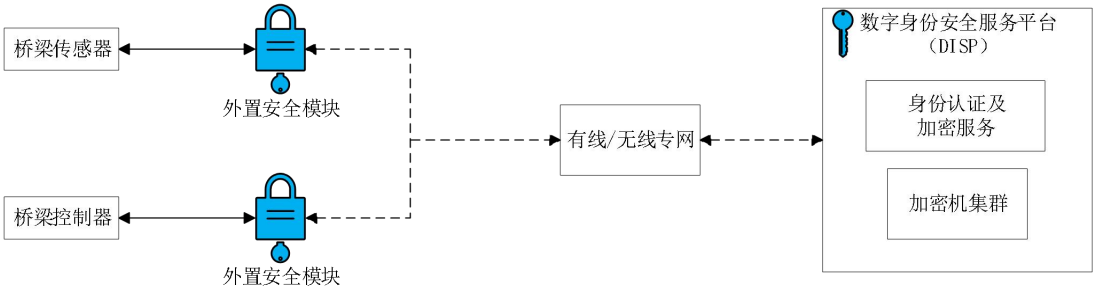

图 3 外置安全模块（安全盒子）应用技术架构

5.2 安全加密功能要求

5.2.1 一般规定

5.2.1.1 应用安全区安全加密要求

智慧桥梁物联监测系统应用安全区应符合下列要求：

a) 应用安全区内各用户系统均应符合 GB/T 22239-2019 的相关要求；
b) 应用安全区内各用户系统均应配置加密服务器或安全模块对控制命令和参数设置指令进行签名操作，用户系统和其他安全区的设备之间通过公网或专网通信时应采用双向认证机制，实现两者之间的身份鉴别，确保与设备层报文的机密性和完成性；
c) 应用安全区内各用户系统与其他安全区设备通过公网或专网进行通信时应进行用户身份鉴别，并符合 GM/T 0003-2012 的相关要求，实现签名/验证以及密钥交换；
d) 应用安全区内各用户系统与其他安全区设备通过公网或专网进行通信时应按照 GM/T 0004-2012 的相关要求，将待签名消息的进行摘要运算防止会话被篡改；
e) 应用安全区内各用户系统与其他安全区设备通过公网或专网进行通信时应按照 GM/T 0002-2012 的相关要求，实现数据加解密及消息认证，保证报文的机密性和完整性。

5.2.1.2 感控安全区要求

智慧桥梁物联监测系统感控安全区应符合下列要求：

a) 桥梁传感器和桥梁控制器应配置具有双向认证、防篡改、加解密功能的安全模块；
b) 安全模块应符合 GB/T 22186-2016 的相关要求要求，同时应支持随机数发生，随机数应符合 GM/T 0006-2012 及 NIST 随机数检测标准；
c) 安全模块应支持非对称密码 GM/T 0003-2012 SM2 椭圆曲线公钥密码算实现签名/验证以及密钥交换；
d) 安全模块应支持杂凑密码，符合 GM/T 0004-2012 SM3 密码杂凑算法的要求实现待签名消息的摘要运算；
e) 安全模块应支持对称密码，符合 GM/T 0002-2012 SM4 分组密码算法的要求，实现数据加解密及消息认证。

5.2.2 密钥协商流程

桥梁传感器和桥梁控制器集成安全模块，通过SM2、SM3、SM4等国密安全算法实现端到端的双向认证和密钥协商。密钥协商流程如下：

a) 桥梁传感器或桥梁控制器接入平台时上传数字证书链和签名数据,用户系统调用数字身份安全服务平台（DISP）的双向认证服务接口认证桥梁传感器或桥梁控制器设备的合法性；
b) DISP 认证终端设备合法性后，进行密钥协商，动态生成 SM4 会话密钥，之后生成服务器的签名数据，并返回到桥梁传感器或桥梁控制器的安全模块；
c) 桥梁传感器或桥梁控制器的安全模块校验服务器的合法性，并动态协商 SM4 会话密钥，进行密钥确认。

5.2.3 通信链路要求

桥梁传感器或桥梁控制器通过光纤或运营商无线网络接入到用户系统，通信链路应符合下列要求：

d) 通过有线专网或运营商 APN 专网方式接入主站；
e) 通过端到端的双向认证动态协商会话密钥，协商流程见图 4。使用会话密钥对通信链路业务数据加解密保护，保证主站所下发的业务数据的机密性、完整性和不可抵赖性。

5.3 交互流程

5.3.1 双向认证

桥梁传感器和桥梁控制器中的安全模块应与用户系统之间建立端到端的双向认证，并应符合下列要求：

a） 双向认证过程中的关键数据元应参与签名运算，并具有防篡改能力；
b） 双向认证中设置随机数和时间戳等信息，并具有防重放能力；
c） 会话密钥应采用动态协商的方式确保密钥安全性；
d） 终端设备可根据业务需求配置不同的认证策略，如开机认证、每次传输敏感数据前做认证等。

5.3.2 认证流程

双向认证流程应采用 GM/T 0017-2012 中 SM2 签名验签算法进行双向认证，基于 SM2 密钥离散算法进行会话密钥协商，生成 SM4 对称密钥。认证原理及流程见图 4，并符合下列要求：

a） 桥梁传感器和桥梁控制器集成安全模块（以 SE 为例），用于存储敏感数据并进行安全运算；
b） 桥梁传感器和桥梁控制器从 SE 中获取认证数据 M1，包括终端类型、SE 基本信息、认证计数器、时间戳、SE 随机数、临时公钥等，并使用 SE 私钥对 M1 进行 SM2 签名运算，用于数字身份安全服务平台（DISP）校验桥梁传感器或桥梁控制器身份的合法性。同时认证数据具备防重放安全控制字段；
c） 数字身份安全服务平台（DISP）认证桥梁传感器和桥梁控制器身份合法性，同时检查是否存在异常认证行为。如果桥梁传感器或桥梁控制器合法，则数字身份安全服务平台（DISP）生成共享数据，并生成 SM4 会话密钥，同时计算用户系统的认证数据 M2，并使用用户系统的私钥对 M2 进行 SM2 签名运算，用于桥梁传感器或桥梁控制器校验用户系统的身份合法性；
d） 桥梁传感器或桥梁控制器收到平台认证数据后，校验用户系统的身份合法性，然后进行密钥协商、密钥确认。如果 SM4 密钥一致，则双向认证完成。

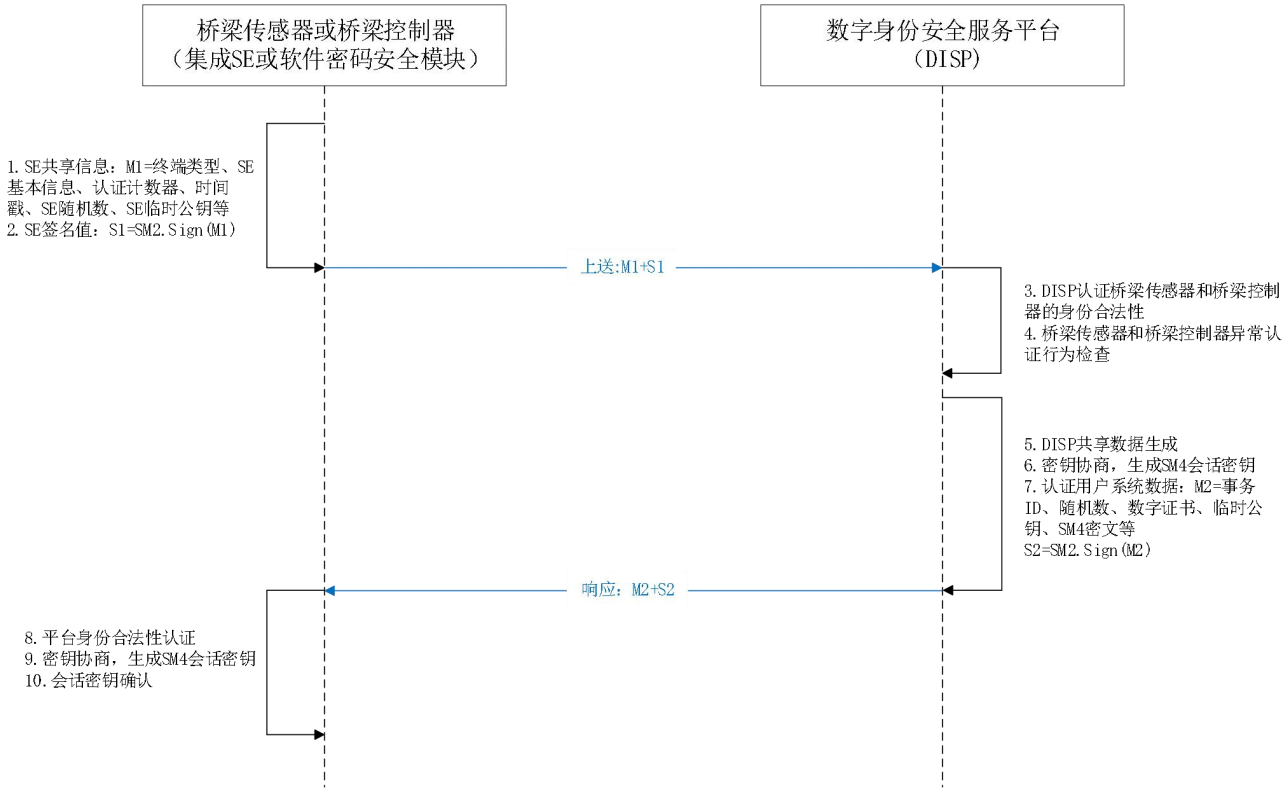

图 4 双向认证流程图

5.3.3 认证参数及算法

5.3.3.1 上行数据

上行数据元见表 2。

表 2 上行数据元

数据元	字段	数据类型	描述及要求
M1	DeviceID	BCD[10]	桥梁传感器或桥梁控制器编号，通常使用 IMEI 标识，BCD 编码格式，不足前补“0”
	DeviceType	BYTE[1]	0x01：通用物联网；0x02：智慧水务；0x03：智慧小区；0xFF：其它
	SEInfo	BYTE[N]	SE 基础信息，LV 结构，L 长度为 2 字节
	认证计数器	BYTE[2]	由 SE 生成，用于数字身份安全服务平台（DISP）做安全引擎规则，不用于流程控制
	时间戳	BYTE[6]	时间戳采用 16 进制编码格式，转换示例： 时间：2021-12-03 14:41:25.999 十进制：1638513685999 十六进制：17D7F06B5EF 时间戳具有一定的时效性，不能使用历史数据进行重试，桥梁传感器和桥梁控制器应具备与用户系统对时能力。
	SE 随机数	BYTE[8]	由 SE 生成
	SE 密钥协商临时公钥	BYTE[64]	由 SE 生成
S1	SE 签名值	BYTE[64]	对参与签名运算的数据元（DeviceID - SE 密钥协商临时公钥）进行 SM2 签名运算

SE信息定义见表3。

表 3 SEInfo 信息定义

字节	名称	长度	说明
SEInfo	行业应用标识	1	0x01：通用物联网；0x02：智慧水务；0x03：智慧小区；0xFF：其它
	RFU	10	芯片厂商注册标识
	标准版本号	1	标识技术规范版本号，范围 1.0 ~ 9.9
	COS 版本号	1	主版本号+次版本号，范围 1.0 ~ 9.9
	生产年份	4	比如：20200608
	SEID	16	编码格式参考 SE 技术规范
	RFU	5	初始值为 0xFFFFFFFFFF
	SE 证书	N	LV 格式，L 长度为 2 个字节，证书长度约 500 字节，采用标准 x509 格式

5.3.3.2 下行数据

下行数据元见表 4。

表 4 下行数据元

数据元	字段	数据类型	描述及要求
M2	会话密钥 ID	BYTE[1]	用于标识省域代码，编码格式参考 SE 技术规范

	会话密钥有效期	BYTE[6]	时间戳采用 16 进制编码格式，转换示例： 时间：2021-12-03 14:41:25.999 十进制：1638513685999 十六进制：17D7F06B5EF 时间戳具有一定的时效性,不能使用历史数据进行重试，终端应具备与平台对时能力。
	随机数	BYTE[8]	数字身份安全服务平台（DISP）生成
	公钥证书	BYTE[N]	采用 LV 结构，L 长度为 2 字节，证书长度约 500 字节，采用标准 x509 格式
	密钥协商临时公钥	BYTE[64]	数字身份安全服务平台（DISP）生成
	随机密文	BYTE[16]	SM4.ENC(SE 随机数+平台随机数)，CBC 模式
	MAC	BYTE[4]	SM4.MAC(随机密文)，CBC 模式
S2	平台签名值	BYTE[64]	对参与签名运算的数据元（会话密钥 ID－MAC）进行 SM2 签名运算

5.3.3.3 认证策略

桥梁传感器和桥梁控制器与用户系统的认证策略应符合下列要求：

a) 用户系统记录终端初始状态为未认证状态；

b) 当桥梁传感器或桥梁控制器上电后，则应主动向用户系统发起认证，并符合下列要求：

1) 当认证成功时，则用户系统记录终端处于认证成功状态，允许处理后续终端上传的业务指令；

2) 当认证失败时，则用户系统应主动同终端断开连接，用户系统记录终端处于未认证状态。

c) 桥梁传感器和桥梁控制器的运行过程，应符合下列要求：

1) 当在认证有效期内，能正常执行业务数据上传；

2) 应实施会话密钥有效期策略，桥梁传感器或桥梁控制器在话密钥即将过期时，应再次主动发起双向认证；

3) 当认证有效期过期时，用户系统应主动同终端断开连接，并设置终端处于未认证状态。

d) 用户系统应建立异常认证行为检测机制，并符合下列要求：

1) 用户系统应认证桥梁传感器和桥梁控制器上报的 IMEI，SEID 等信息的合法性；

2) 用户系统应建立异常预警机制，提供稽查能力。

5.3.4 控制命令安全下发流程

用户系统下发控制指令时，应调用 DISP 的加密服务接口，使用双向认证阶段动态生成的 SM4 会话密钥对控制指令进行加密并计算 MAC，再下发给集中控制器或单灯设备。加解密算法为 SM4，CBC 模式。控制命令安全下发流程见图 5。

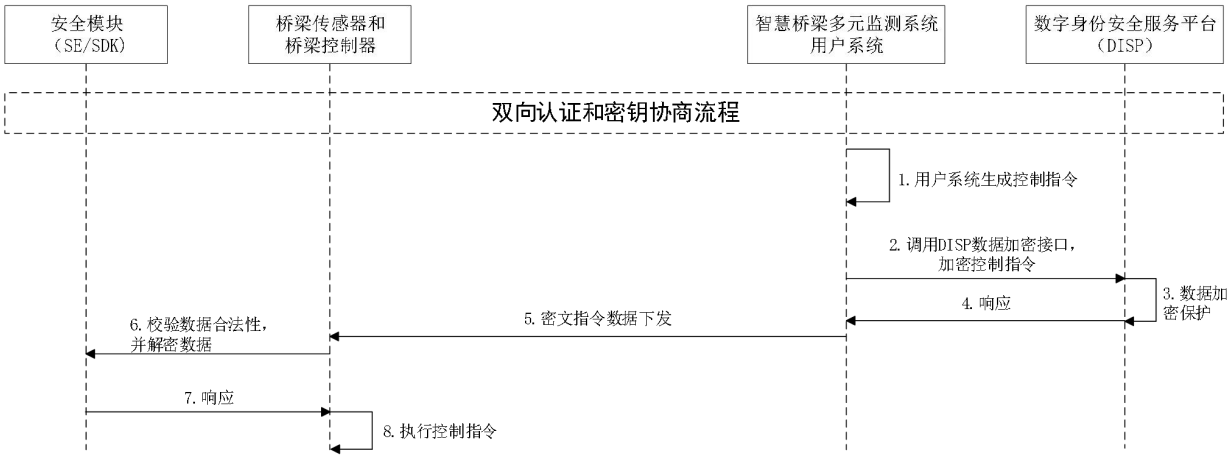

图5 控制命令安全下发流程

5.3.5 桥梁传感器和桥梁控制器业务数据加密上传流程

桥梁传感器或桥梁控制器设备有业务数据需要加解密上传时，需要调用SE/SDK的算法接口并计算MAC，确保数据在通信链路传输时的机密性和完整性。加解密时SE使用双向认证阶段生成的SM4会话密钥，算法为SM4算法，算法模式为CBC模式。业务数据加密上传流程见图6。如果方案集成外置安全模块（安全盒子）方案，则桥梁传感器和桥梁控制器设备不需要安全加解密操作，由安全盒子的主控芯片和SE实现对业务数据的加解密保护。

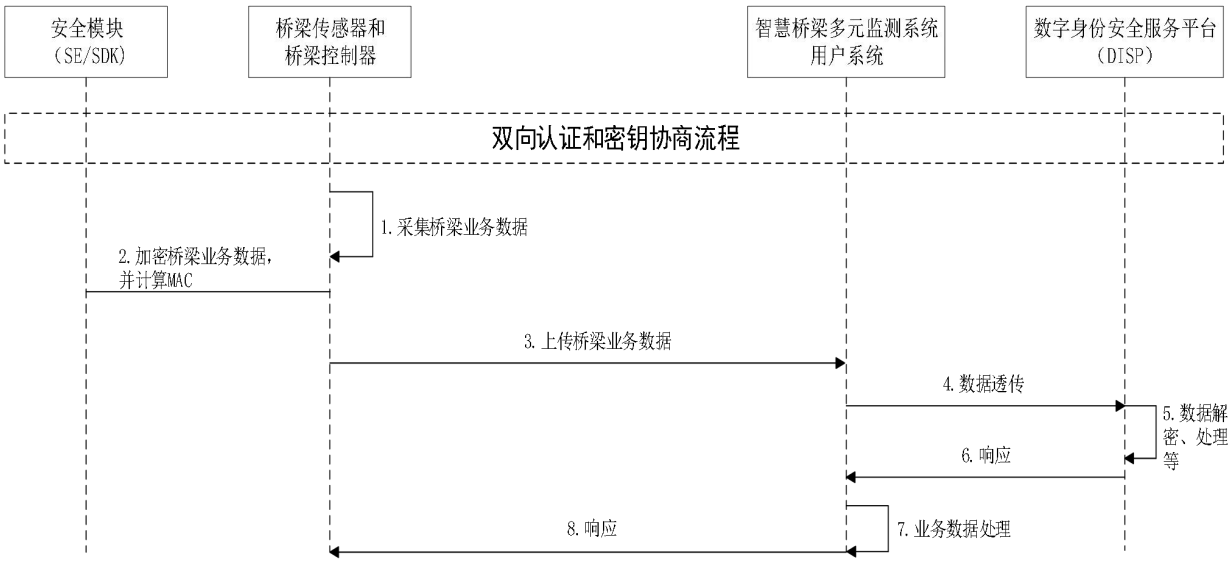

图6 业务数据加密上传流程

5.4 安全加密系统平台运维要求

5.4.1 一般规定

物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全以及管理制度、人员管理、建设运行、应急处置等密码应用管理要求应符合GB/T 39786-2021的要求。

5.4.2 设备要求

密码设备应使用符合国家管理规定的技术和产品。

5.4.3 安全运维要求

安全加密系统平台安全运维应符合下列要求：

a) 安全加密系统平台运行维护的基本要求应符合 GB/T 28827.1-2012 的要求；
b) 安全加密系统平台运行维护的交付应符合 GB/T 28827.2—2012 的要求；
c) 安全加密系统平台运行维护的应急响应符合 GB/T 28827.3—2012 的要求；
d) 通过安全信道进行平台管理，具备身份鉴别和认证等功能；
e) 建立内部流量汇聚点，监控网络动态和流量；
f) 对物理机、主机进行实时的中央处理器、带宽、磁盘监控，发现异常情况应立即告警。

附 录 A
（资料性）
安全芯片基本信息

A.1 文件结构要求

A.1.1 文件结构图

安全芯片文件结构图，见图A.1。

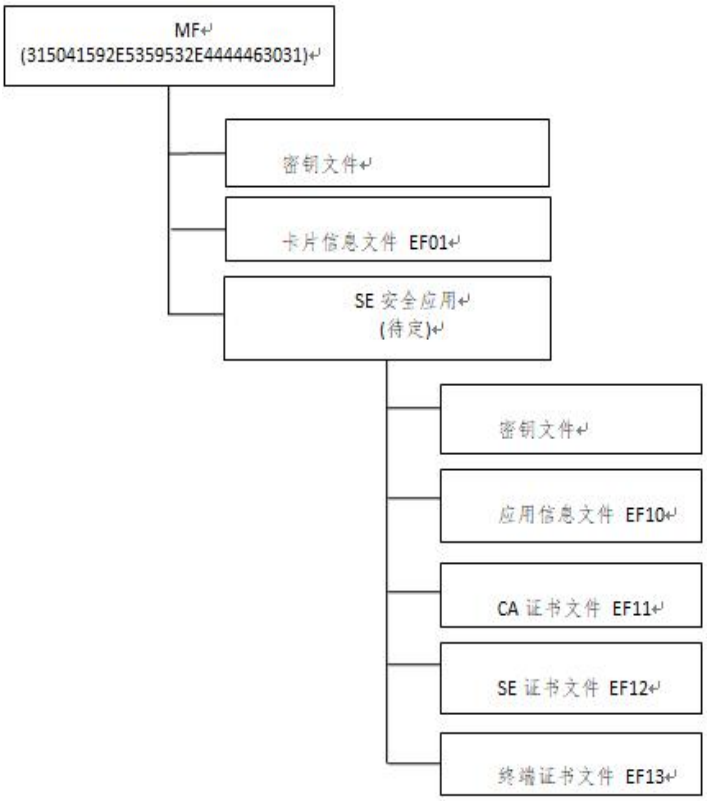

图 A.1 密码生成及分发流程

A.1.2 文件结构表

文件结构见表A.1。

表 A.1 文件结构表

文件名称	文件类型	文件标识符	读权	写权	备注
MF	主文件	--	--	--	出厂时创建
密钥文件	密钥文件	--	03	02	通过 MF 主控密钥 MK_MF 采用密文+MAC 方式写入密钥
卡片信息文件	二进制文件	EF01	00	01	明文读，写时使用 MK_MF 进行线路保护（明文+MAC）

续表 A.1 文件结构表

安全应用目录	目录文件	--	--	--	出厂时创建
密钥文件	密钥文件	--	03	02	通过通用安全应用主控密钥 MK_DF 采用密文+MAC 方式写入
应用信息文件	二进制文件	EF10	00	01	明文读，写时使用 DAMK_DF 进行线路保护（明文+MAC）
CA 公钥证书文件（CA_PUBKEY）	证书文件	EF11	03	01	禁止导出，导入使用 DAMK_DF 进行线路保护（明文+MAC）
SE 公钥证书文件（SE_PUBKEY）	证书文件	EF12	00	00	明文导出，明文导入，导入时使用 CA_PUBKEY 进行验证保护
签名公钥证书文件（TE_PUBKEY）	证书文件	EF13	00	00	明文导出，明文导入，导入时使用 CA_PUBKEY 进行验证保护

A.1.3 详细文件结构说明

A.1.3.1 安全芯片信息文件

安全芯片信息文件详细说明见表A.2。

表 A.2 安全芯片信息文件说明

文件标识（FID）		EF01
文件大小		96 字节
读取：明文		写入：DAMK_MF 保护（明文 + MAC）
字节	长度	内容
1-8	8	发行方标识
9	1	协议类型
10	1	合同版本
11 - 18	8	合同序列号
19 - 22	4	合同签署日期格式：YYYYMMDD
23 - 26	4	合同过期日期格式：YYYYMMDD
27	1	激活状态 高 4 位： 0000：未启用 1111：已启用 其它：预留 低 4 位： 0000：预留
28 - 96	69	预留

A.1.3.2 应用信息文件

应用信息文件详细说明见表A.3。

表 A.3 应用信息文件说明

文件标识（FID）		EF10
文件类型		二进制文件
文件大小		64 字节
读取：明文		写入：DAMK_DF 保护（明文 + MAC）
字节	长度	内容
1	1	应用规范版本号
2 - 5	4	启用时间格式：YYYYMMDD
6	1	支持算法类型 0：SM2 算法
7 - 64	58	预留

A.1.3.3 通用安全应用下CA公钥证书文件

通用安全应用下CA公钥证书文件详细说明见表A.4。

表 A.4 CA 公钥证书文件说明

文件标识（FID）		EF11
文件类型		证书文件
文件大小		1024
导出：明文		导入：DAMK_DF 保护（明文 + MAC）
字节	长度	内容
1 - 2	2	CA 公钥证书长度
3 -1024	1022	CA 公钥证书数据

A.1.3.4 通用安全应用下SE公钥证书文件

通用安全应用下SE公钥证书文件详细说明见表A.5。

表 A.5 SE 公钥证书文件说明

文件标识（FID）		EF12
文件类型		证书文件
文件大小		1024
导出：明文		导入：CA 证书公钥验证保护
字节	长度	内容
1 - 2	2	SE 公钥证书长度
3 -1024	1022	SE 公钥证书数据

A.1.3.5 通用安全应用下签名公钥证书文件

通用安全应用下签名公钥证书文件详细说明见表A.6。

表 A.6　签名公钥证书文件说明

文件标识（FID）		EF13
文件类型		证书文件
文件大小		1024
导出：明文		导入：CA 证书公钥验证保护
字节	长度	内容
1 - 2	2	终端公钥证书长度
3 - 1024	1022	终端公钥证书数据

A.1.4　密钥结构

密钥结构见表A.7。

表 A.7　密钥结构

密钥	密钥类型	密钥数量	密钥标识	算法标识	最大重试次数	密钥长度
MF（315041592E5359532E4444463031）						
主控密钥 MK_MF	00H	01H	00H	04H	03H	10H
维护密钥 DAMK_MF	01H	01H	00H	04H	FFH	10H
外部认证密钥 UK_MF	02H	01H	00H	04H	03H	10H
通用安全应用目录（待定）						
主控密钥 MK_DF	00H	01H	00H	04H	03H	10H
维护密钥 DAMK_DF	01H	01H	00H	04H	FFH	10H
外部认证密钥 UK_DF	02H	01H	00H	04H	05H	10H
会话密钥	03H	FFH	XXH	04H	FFH	10H
SE 公钥	--	01H	--	02H	--	40H
SE 私钥	--	01H	--	02H	--	20H
注1：最大重试次数为0xFF时，代表该密钥重试次数无限制； **注2**：会话密钥为临时密钥，复位后失效，同一个会话有效期内最大支持10支。						

A.2　命令集

安全芯片命令集见表A.8。

表 A.8　安全芯片命令集

编号	命令名称	CLA	INS	功能描述
1	SELECT	00	A4	选择应用
2	GET CHALLENGE	00	84	获取随机数
3	EXTERNAL AUTHENTICATE	80	82	外部认证
4	READ BINARY	00	B0	读二进制文件
5	READ RECORD	00	B2	读记录文件
6	UPDATE BINARY	00	D6	写二进制文件
7	UPDATE RECORD	00	DC	写记录文件
8	IMPORT CERTIFICATE	80	4C	导入证书
9	EXPORT CERTIFICATE	80	4E	导出证书
10	SM2 PRIVATE KEY SIGN	80	74	SM2 私钥签名
11	SM2 PUBLIC KEY VERIFY	80	76	SM2 公钥验签
12	SM2 PUBLIC KEY ENCRYPT	80	7A	SM2 公钥加密
13	SM2 PRIVATE KEY DECRYPT	80	7C	SM2 私钥解密
14	GENERATE SM2 KEY PAIR	80	78	生成 SM2 密钥对
15	IMPORT SM2 KEY PAIR	80	70	导入 SM2 密钥对
16	EXPORT SM2 PUBLIC KEY	80	72	导出 SM2 公钥
17	SM4 ENCRYPT	80	A6	SM4 加密
18	SM4 DECRYPT	80	AE	SM4 解密
19	SM4 CALCULATE MAC	80	BE	SM4 计算 MAC
20	SM3 HASH	80	B6	SM3 杂凑计算
21	GET AUTHENTICATION DATA	80	CA	获取 SE 认证数据
22	MUTUAL AUTHENTICATION	80	CC	双向认证
23	GENERATE P10 REQ DATA	80	CD	生成 P10 请求数据
24	GET RESPONSE DATA	80	CE	获取剩余响应数据
25	BIND DEVICE ID	80	DB	绑定设备 ID
26	ACTIVE DEVICE ID	04	DD	激活设备 ID
27	CREATE FILE	-	-	创建文件（自定义）
28	WRITE KEY	-	-	更新密钥（自定义）