KSSJ/CJ18-2023

智能化矿山数据融合共享
通信接口与协议规范
第 8 部分：安全

Intelligent mine data fusion and sharing

Specifications for communication interface and protocol

Part 8: Safety

国家矿山安全监察局

2023 年 6 月

目　次

前　言

本文件参照 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。

《智能化矿山数据融合共享 通信接口与协议规范》分为以下9个部分：

——第 1 部分：基本要求；

——第 2 部分：接口；

——第 3 部分：服务；

——第 4 部分：发现；

——第 5 部分：连接；

——第 6 部分：报文；

——第 7 部分：配置；

——第 8 部分：安全；

——第 9 部分：管理。

本文件是《智能化矿山数据融合共享 通信接口与协议规范》的第8部分。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件起草单位：国家能源投资集团有限责任公司、国能数智科技开发（北京）有限公司、国家能源集团乌海能源有限责任公司、中国华电集团有限公司、山东能源集团有限公司、陕西煤业化工集团有限责任公司、晋能控股集团有限公司、矿冶科技集团有限公司、应急管理部信息研究院、中国中煤能源集团有限公司、中煤科工集团常州研究院有限公司、浪潮通用软件有限公司、郑州恒达智控科技股份有限公司、山东黄金集团有限公司、华电煤业集团有限公司、煤炭科学研究总院有限公司矿山大数据研究院、中国矿业大学（北京）、山西阳光三极科技股份有限公司、南京北路智控科技股份有限公司、华夏天信物联科技有限公司、和利时卡优倍科技有限公司、精英数智科技股份有限公司、中煤信息技术（北京）有限公司、云鼎科技股份有限公司、华电煤业集团数智技术有限公司、陕煤集团神木张家峁矿业有限公司、重庆梅安森科技股份有限公司、深圳市翌日科技有限公司、中国煤炭地质总局安全与应急研究院、中兴通讯股份有限公司、西安科技大学、西安电子科技大学杭州研究院、中国工业互

联网研究院、新华三技术有限公司、上海山源电子科技股份有限公司、华为技术有限公司、航天智控（北京）监测技术有限公司、北京龙软科技股份有限公司、北京北矿智能科技有限公司、北京天玛智控科技股份有限公司、天津华宁电子有限公司、北京圆之翰工程技术有限公司、青岛慧拓智能机器有限公司、华洋通信科技股份有限公司、北京大地高科地质勘查有限公司、太重煤机有限公司。

本文件技术指导：杨荣明、徐会军、田臣、马世志、王海春、王致兵、王鹏、蔡峰、王秀林、杨林、赵宇波、宋文兵、谢旭阳、王瑞、樊九林、冯志华、郭军、贺耀宜、金卫朵、曹现刚、孙建国、马文静、扈天保、李晓方、吕杭榕、祝青、郭彪、赵威、姚松平、艾云峰。

本文件主要起草人：丁震、邓文革、钱海军、潘涛、张帆、鲍震、郑耀涛、王波、高静、高秋秋、柳建华、乔少利、李系民、曹正远、杨永生、聂志勇、王亚军、刘宁、崔磊、韩培强、卢欣奇、胡而已、张冬阳、胡文涛、逯宪彬、李国威、吉晓清、赵黄健、熊伟、刘庆富、杨振宇、王陈书略、赵文豪、徐金陵、黄金、陈帅领、呼少平、刘航、徐跃福、朱奎龙、陈阳、李秀文、高伟、李坤龙、张鹏鹏、周亚清、冯银辉、申军军、刘雷霆、陈龙、张永福、张彪、宋栋帅。

引　言

《智能化矿山数据融合共享 通信接口与协议规范》规定了智能化矿山数据采集、传输、协同共享过程中的接口方式和通信协议基本要求，明确了不同通信接口协议之间的转换规则。通过建立统一的矿山数据采集、传输、融合、共享规范体系，解决智能化矿山建设过程中面临的传输协议不开放、数据孤岛林立等突出问题，保障数据高效、有序、精准传输，实现矿山安全、生产、经营、管理等环节的数据融合和共享应用。

智能化矿山数据融合共享 通信接口与协议规范
第 8 部分：安全

1 范围

本文件规定了智能矿山通信接口与协议系统的信息安全要求、安全模型等。

本文件适用于矿山企业设备通信、交互的安全和认证。

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 15843.2-2017 信息技术—安全技术—实体鉴别 第2部分：采用对称加密算法的机制

GB/T 15843.3-2017 信息技术—安全技术—实体鉴别 第3部分：采用数字签名技术的机制

GB/T 15843.4-2017 信息技术—安全技术—实体鉴别 第4部分：采用密码校验函数的机制

GB 17859-1999 计算机信息系统 安全保护登记划分准则

GB/T 20518-2018 信息安全技术 公钥基础设施 数字证书格式

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 28181-2022 公共安全视频监控联网系统 信息传输、交换、控制技术要求

GB/T 29246-2017 信息技术 安全技术 信息安全管理体系 概述和词汇

GB/T 29765-2021 信息安全技术 数据备份与恢复产品技术要求与测试评价方法

GB/T 30976.1-2014 工业控制系统信息安全 第1部分：评估规范

GB/T 30976.2-2014 工业控制系统信息安全 第2部分：验收规范

GB/T 31168-2014 信息技术安全 云计算服务安全能力要求

GB/T 33863.2-2017 OPC统一架构 第2部分：安全模型

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 36643-2018 信息安全技术 网络安全威胁信息格式规范

GB/T 37025-2018 信息安全技术 物联网数据传输安全技术要求

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 38667-2020 信息技术 大数据 数据分类指南

YD/T 2399-2012 M2M应用通信协议技术要求

TC260-PG-21212A 网络安全标准实践指南——网络数据分类分级指引

RFC 1994 PPP挑战握手认证协议（PPP Challenge Handshake Authentication Protocol (CHAP)）

RFC 2246 传输层安全协议版本1.0（The TLS Protocol Version 1.0）

RFC 4279 用于传输层安全的预共享秘钥密码套件(Are-Shared Key Cipher suites for Transport Layer Security (TLS))

RFC 5019 轻量级在线证书状态协议配置文件(The Lightweight Online Certificate Status Protocol (OCSP) Profile)

RFC 5246 传输层安全协议版本1.2(The Transport Layer Security (TLS) Protocol Version 1.2)

RFC 5280 互联网X.509 公钥基础设施证书和证书吊销列表配置文件 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

RFC 5869 基于HMAC的密钥提取和扩展导出函数(Freebased Extract-and-Expand Key Derivation Function (HKDF))

RFC 7914 基于crypt密码的密钥派生函数(The crypt Password-Based Key Derivation Function(PBKDF))

3 术语和定义

下列术语和定义适用于本文件。

3.1 安全保护 secure protection

对会话数据的签名、加密，确保传输过程中会话数据的机密性和完整性。

3.2 访问控制 access control

用户身份及其所归属的某项定义组来限制用户对某些信息项的访问，或限制对某些功能的使用。

3.3 **会话/安全会话** session/secure session

会话指两个或多个通信设备之间，或计算机与用户之间临时的、交互式的信息交换的过程。

安全会话指会话数据经过安全保护、并由安全传输通道承载传输的会话。

3.4 **认证** authentication

验证人、设备或应用程序等身份的认证过程。

3.5 **安全传输通道** secure transmission channel

协议栈客户端、协议栈服务端之间建立的用于安全传输交互数据的逻辑概念上的网络通道。

3.6 **安全审计** security audit

对系统中与安全有关的活动的相关信息进行识别、记录、存储和分析。信息安全审计的记录用于检查验证与网络安全有关的活动。

4 缩略语

下列缩略语适用于本文件。

TCB:计算机内保护装置的总体，包括硬件、固件、软件和负责执行安全策略的组合体（Trusted Computing Base）

PKI:公共密钥基础设施（Public Key Infrastructure）

STRIDE:用于威胁建模的方法和工具

M2M:机器与机器或人之间的通信（Machine to Machine/man）

HSM:硬件安全模块，一种用于保护和管理强认证系统所使用的密钥和敏感数据，并同时提供相关密码学操作的计算机设备（Hardware Security Module）

5 总体要求

5.1 一般要求

5.1.1 安全性

进行通信、交互的设备应采用设备级的连接认证，通过加密、签名等方式保证数据的完整性、机密性、可靠性。

5.1.2　安全管理

安全管理应与矿山企业已有安全体系、安全基础设施结合，如安全运营、风险管理、身份认证、证书管理/PKI、权限管理等。（本文件中的安全要求仅面向设备间交互过程提供安全保证以及必要的安全管理支撑能力，但不涉及其它安全管理和基础安全设施等相关安全要求。）

5.1.3　配置灵活性

设备供应商、业务应用开发者以及设备使用者可根据具体环境、业务需求，为设备应用灵活配置安全策略。

5.1.4　网络安全保护

应根据系统数据安全要求设置不同的网络安全保护等级，并建立符合需求的安全保护措施，如边界防护、入侵检测等。网络安全保护应符合GB/T 22239-2019的要求。

5.1.5　数据接入安全

应明确数据的发送方、发送途径、发送方式及发送数据的类型。严禁未知身份的发送源访问本系统的数据接口。新增需要接入的数据源应报备和登记，并与现有接收方式保持一致。严格检验评估数据发起端和接收端的物理安全和网络安全。

5.1.6　数据生产安全

应使用消息校验码(MAC)或数字签名等技术手段对生产数据进行完整性验证，使用对称加密、动态口令、数字签名等进行真实性验证。针对敏感、涉密数据应保证数据机密性，使用密码加密功能，保障信息系统重要数据在传输、存储过程中的保密性以及身份鉴别信息、密钥数据的机密性。

5.1.7　OPC UA通讯安全

应从鉴别、授权、机密性、完整性、可审核性、可用性6个方面识别OPC UA通讯的威胁、弱点使系统保持较高稳定性，OPC UA通讯安全应符合GB/T 33863.2-2017的要求。

5.1.8　感知层设备安全

感知层设备应选用支持标准通用协议的设备（如：RS485、CAN、Modbus等），宜选用国产自主研发的智能传感器设备、控制器和控制系统，减少控制器自身系统漏洞被利用的风险，支持制定和执行访问控制策略的设备。

5.1.9　流媒体安全

流媒体数据安全加密方式宜采用对称密码体制，安全要求应符合GB/T 28181-2016第8部分。

5.2　安全模型

安全模型应包含身份识别和鉴别、访问控制和安全审计等方面安全要求，宜通过安全服务集和安全配置相互配合实现。安全模型应符合GB 17859-1999的要求。

5.3　威胁信息模型

应建立威胁信息分析系统和威胁信息模型，降低系统安全威胁的防护成本，提升网络整体安全防护效率，威胁信息模型应符合GB/T 36643-2018的要求。

5.4　安全验证模型

应建立数据安全验证模型，根据数据的特殊性可从数据采集、数据传输、数据存储、数据处理、数据交换和数据销毁6个阶段或其中几个阶段建立模型，安全验证模型应符合GB/T 37988-2019中第6节、第7节要求。

5.5　安全框架

安全框架应与矿山企业其它网络安全基础设施对接，形成矿山完整网络安全解决方案。安全框架应符合GB 17859-1999的要求，典型框架如图1所示。

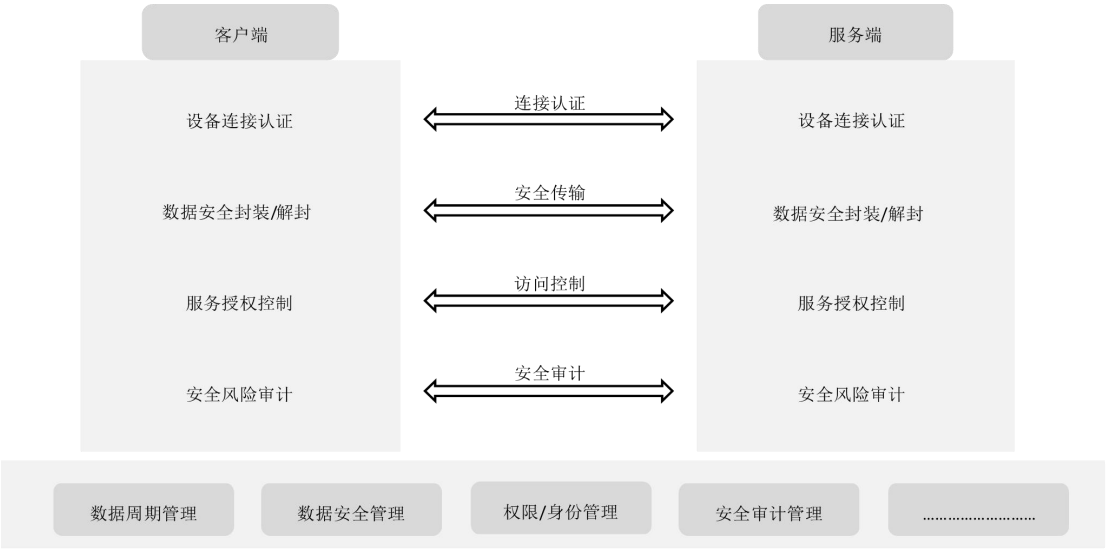

图 1　安全框架体系架构与功能要求

6　设备连接认证

6.1　认证场景

设备应根据具体业务场景，支持一种或多种连接认证方式。典型的设备间连接认证场景如图2所示。

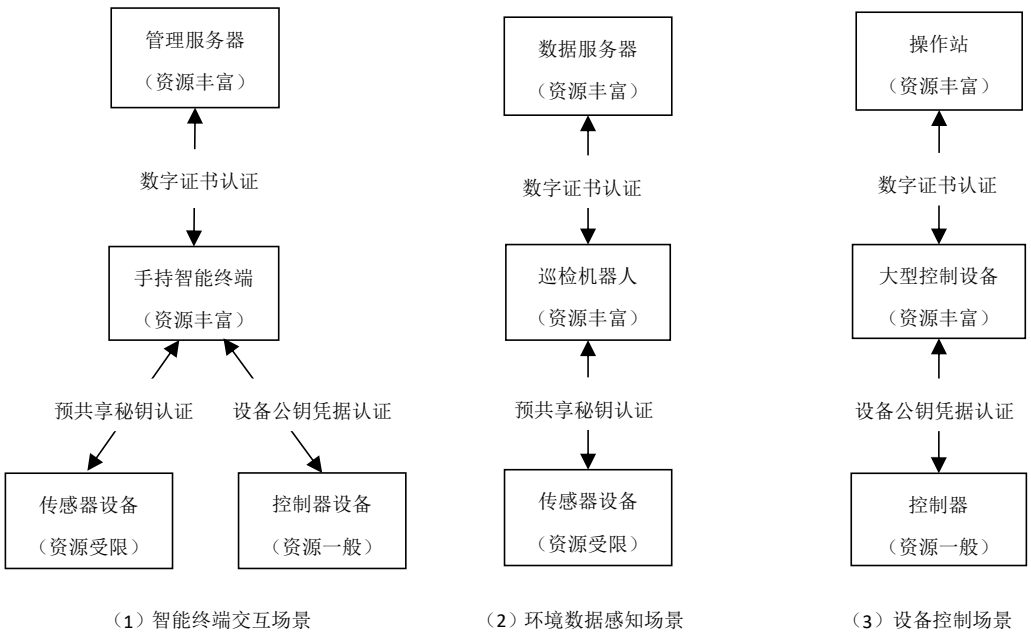

图 2　矿山智能化网络中典型的设备间连接认证场景示意图

6.2　认证过程

设备认证过程根据认证方式不同，在请求和响应中间还包括多个交互过程，即可能通过多个交互过程完成认证，不同的认证方式对应的具体流程和请求、响应参数存在差异。认证流程应符合YD/T 2399-2012的要求。

6.3 设备预置数字证书

6.3.1 证书内容

认证设备预置数字证书应遵循RFC5280定义的X.509 v3证书，证书内容和格式应符合GB/T 20518-2018的要求。

6.3.2 证书预置

设备数字证书应在设备进入生产作业之前预置到设备中，证书预置方式由设备制造商在生产线预置和用户（设备使用者、拥有者）在设备初始化配置过程中进行证书预置两种典型方式。

6.3.3 证书有效性校验

在使用设备数字证书实现身份认证的过程中，应对交互的另一端的设备证书进行有效性校验。

6.3.4 数字证书认证

数字证书的认证宜基于公钥认证进行双向认证和密钥协商。基于公钥认证的方法可参考ISO/IEC 9798-3中双向认证方式中“Tree pass authentication”。双方密钥协商的密钥算法根据r_A、r_B和r_{PMK}派生会话密钥集。典型交互过程如图3示。

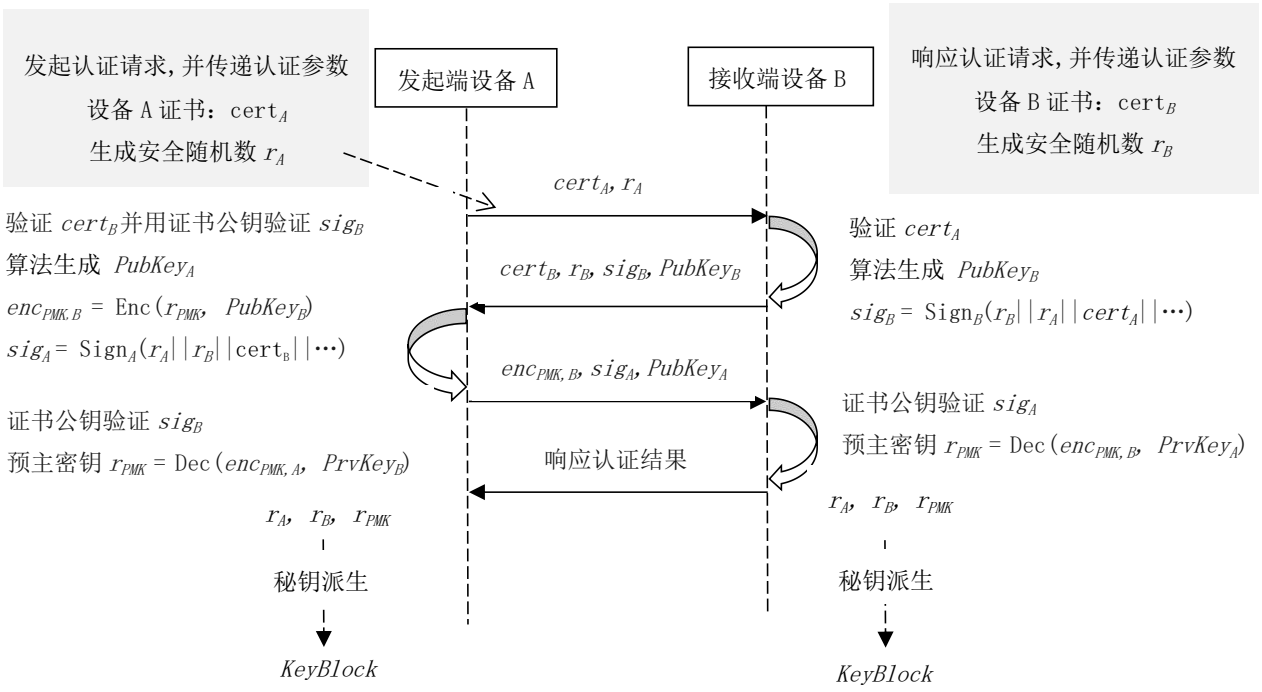

图 3　设备证书的连接认证的交互过程

6.4　设备预共享密钥

设备预共享密钥的认证方式为对称式认证，仅可用于硬件规格受限、计算能力较低的设备，应在设备作业之前将密钥预置于设备。

设备预共享密钥生成方式由厂商自行确定。但共享密钥长度应不少于256bit。设备供应商或用户可以预置多组共享密钥，每组共享密钥有唯一的标识符。

7　安全传输

7.1　一般要求

安全传输应提供互联互通互操作的安全传输通道，确保即使在非可信的传输通道上仍可安全地进行通信。安全传输应符合GB/T 37025-2018的要求。

7.2　安全传输场景

安全传输支持“请求—响应”、“订阅—发布”两类会话模型，提供数据传输过程中会话数据安全保证，根据会话模式的不同，安全传输提供对应的安全传输方案。两类会话模式如图4、图5所示。

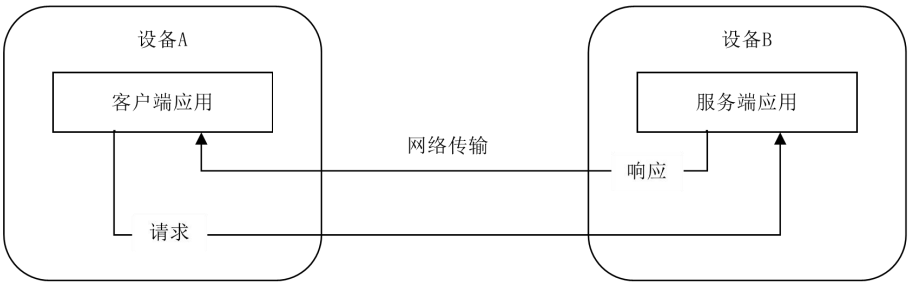

图 4　“请求—响应”会话模式示意

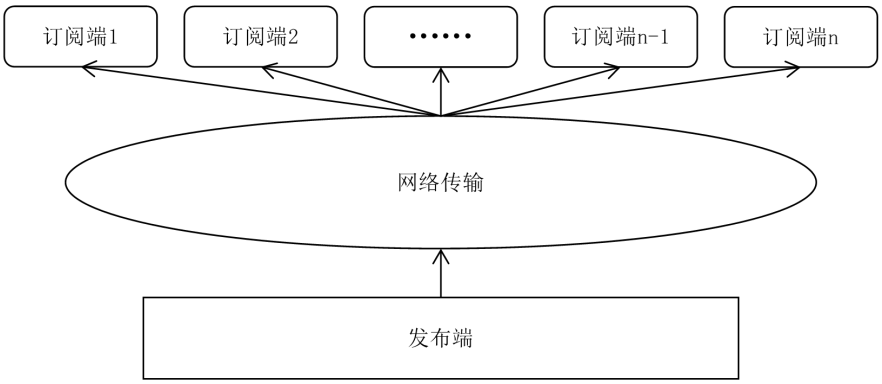

图 5　“订阅—发布”会话模式示意

7.3　安全传输模型

7.3.1　“请求—响应”式会话模式

应在设备间网络传输能力的基础上构建设备级的逻辑安全传输通道，通过该安全传输通道来承载应用间的“请求—响应”会话，保证会话数据安全。如图6所示。

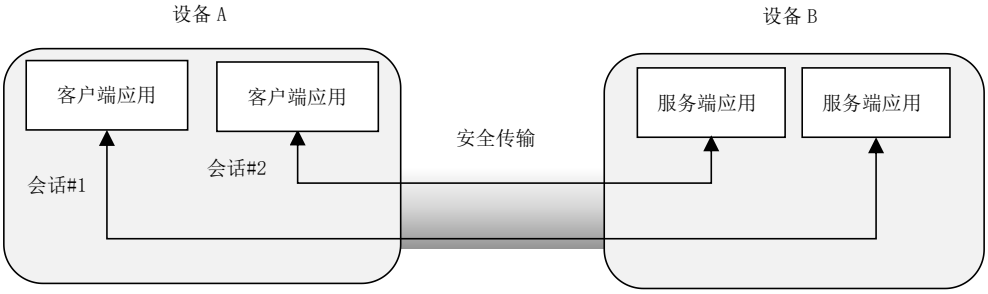

图 6　“请求—响应”模式的安全传输模型

7.3.2　“发布—订阅”式会话模式

安全传输采用合法参与者之间“共享密钥的组播加密方案”（Trivial Broadcast Encryption）的方式进行会话数据安全保护。

7.3.3 关闭安全会话

安全会话流程结束或异常终止时，应发送关闭安全会话请求，关闭指定的安全会话。

7.4 数据安全封装/解封要求

7.4.1 安全封装/解封模型

数据安全封装/解封的过程是基于服务的安全传输模式设置，应对服务的会话数据进行签名、加密、解密、验签。典型流程如图7所示。

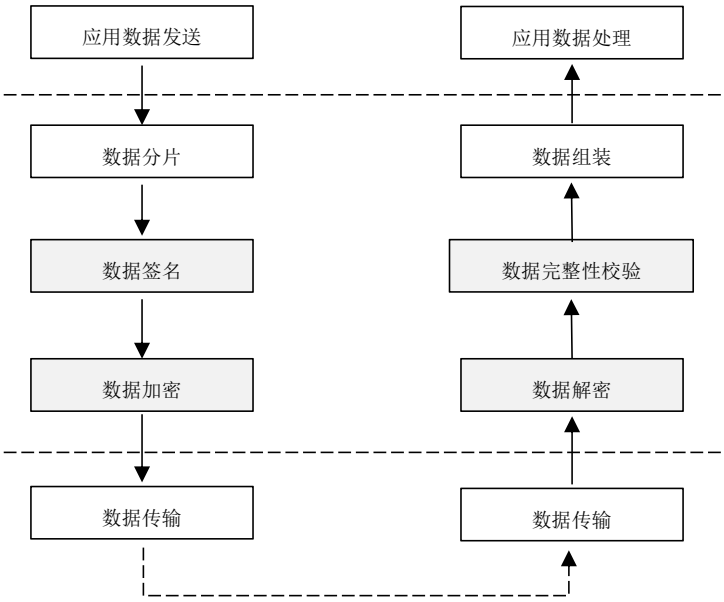

图 7 数据安全封装/接解封流程

7.4.2 端内数据处理

协议栈收到应用消息后，应进行安全保护，获取用于传送的安全数据，以及对应的解密过程。

7.4.3 数据安全封装格式

数据安全封装只对消息主体和签名部分进行加解密，安全封装后的消息应包括消息头、安全头、消息主体和签名4部分，交互双方可确定安全封装的密码算法策略以及对应的密钥信息等。

8 访问控制

8.1 概述

访问控制是指在鉴别用户的合法身份后，通过技术途径准许或限制用户对数据信息的访问能力及范围，阻止未经授权的资源访问，包括阻止以未经授权的方式使用资源。访问控制应符合GB/T 21168-2014第7部分要求。

8.2 访问控制流程

访问控制应提供“创建安全会话”服务以实现客户端身份凭据信息的传递、认证，以及初始化当前客户端在当前会话中的权限信息，在请求目标服务时由服务端进行请求鉴权。典型流程如图8所示。

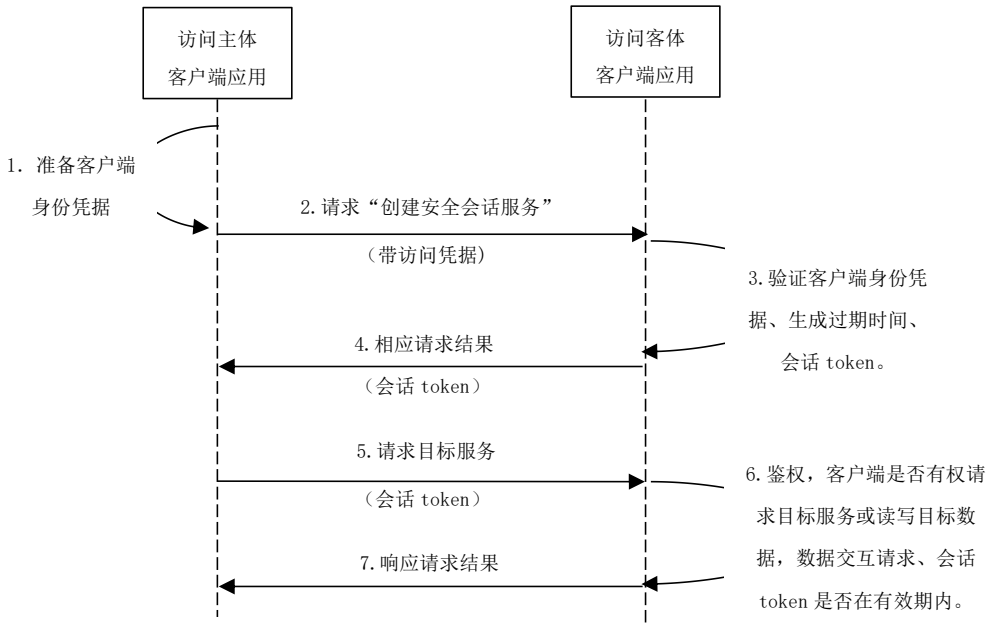

图 8 访问控制授权访问流程

8.3 应用场景

访问控制场景包括两类：一类是无工作人员/用户参与交互的M2M的设备间访问；另一类是有用户参与交互的U2M的跨设备访问控制场景。两类访问控制的典型场景如图9、图10所示。

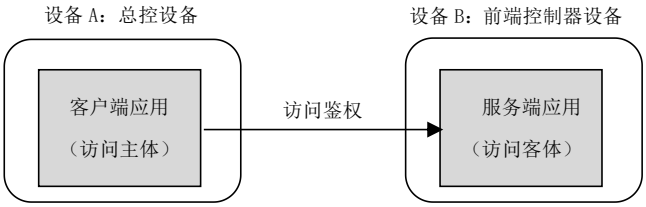

图 9　无用户参与的 M2M 访问控制场景

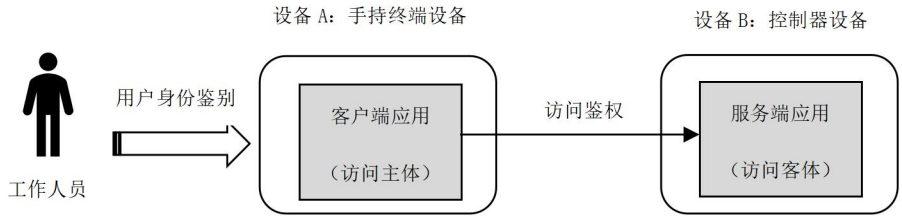

图 10　用户参与的 U2M 的跨设备访问控制场景

a）无用户参与的 M2M 的设备间服务访问控制场景，服务端应用将不验证用户身份凭据，仅基于客户端设备和客户端应用进行访问控制；

b）有用户参与的 U2M 跨设备访问控制场景：

1）支持用户直接交互、操作的设备，在其设备或设备内客户端应用实现对用户的认证和鉴权，由发起端设备完成用户授权（User Authorization）；

2）由客户端应用发起对服务端应用的请求，访问控制过程和 M2M 的设备间访问控制场景类似，仅授权用户、授权设备、授权客户端访问目标服务。

8.4　访问控制策略

设备服务、设备模型属性宜通过定义对应的访问控制策略，实现请求过程中的访问控制。访问控制策略应按照最小特权原则、最小泄露原则、多级安全策略进行设置。

9　安全审计

安全审计功能是系统的一项基本能力，提供一种跟踪、追溯系统操作、活动的方法。安全审计功能应符合GB/T 37962-2019第8部分。

10 存储安全

数据存储应采用数据备份、安全灾备、数据脱敏等技术对系统数据进行安全存储。数据存储安全应符合GB/T 29765-2021。

参 考 文 献

[1] GB/T 10113—2003 分类与编码通用术语

[2] GB/T 15259—2008 煤矿安全术语

[3] GB/T 18725-2008 制造业信息化 技术术语

[4] GB/T 32400-2015 信息技术 云计算 概览与词汇

[5] GB/T 37700-2019 信息技术 工业云 参考模型