ICS 73.100.99
CCS D 09

MT

中华人民共和国煤炭行业标准

MT/T 1202.4—2023

煤矿数据采集与传输技术要求
第4部分:信息安全

Specifications of data acquisition and transmission for coal mine
Part 4:Information security

2023-04-10 发布　　2023-07-01 实施

国家矿山安全监察局　发布

目　　次

前　言

本标准按照 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》进行编写。

MT/T 1202—2023《煤矿数据采集与传输技术要求》包括如下部分:

——第 1 部分:总体要求

——第 2 部分:服务集

——第 3 部分:设备发现与连接

——第 4 部分:信息安全

——第 5 部分:报文规范

——第 6 部分:配置要求

本标准是 MT/T 1202—2023《煤矿数据采集与传输技术要求》的第 4 部分。

请注意本标准的某些内容可能涉及专利。本标准的发布机构不承担识别专利的责任。

本标准由国家矿山安全监察局政策法规和科技装备司提出。

本标准由煤炭行业煤矿专用设备标准化技术委员会归口。

本标准起草单位:中国矿业大学(北京)、华为技术有限公司、神东煤炭集团公司、煤炭科学技术研究院有限公司、应急管理部信息研究院、应急管理部大数据中心、国家矿山安全监察局内蒙古局、国家矿山安全监察局陕西局、山东能源集团有限公司。

本标准主要起草人:孙继平、贺海涛、郭振兴、张立亚、亓玉浩、刘坤、林薇、高伟、郑文文、姚松平、张乐乐、吴正、郭浩平、刘勇、李哲、梁玉、王鹏、申志远。

本标准为首次发布。

煤矿数据采集与传输技术要求
第4部分:信息安全

1 范围

本标准规定了煤矿数据采集与传输中有关信息安全的术语和定义、缩略语、总体要求、连接认证、安全传输安全审计、实施要求。

本标准适用于煤矿数据采集与传输。

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标准必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本标准;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本标准。

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/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

MT/T 1202.1—2023 煤矿数据采集与传输技术要求 第1部分:总体要求

MT/T 1202.2—2023 煤矿数据采集与传输技术要求 第2部分:服务集

MT/T 1202.3—2023 煤矿数据采集与传输技术要求 第3部分:设备发现与连接

MT/T 1202.5—2023 煤矿数据采集与传输技术要求 第5部分:报文规范

MT/T 1202.6—2023 煤矿数据采集与传输技术要求 第6部分:配置要求

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 Transport Layer Security (TLS) Protocol Version 1.0)

RFC 4279 用于传输层安全的预共享密钥密码套件(Pre-Shared Key Ciphersuites 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 for High-Volume Environments)

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(HMAC-based Extract-and-Expand Key Derivation Function (HKDF))

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

RFC 9068 OAuth 2.0访问令牌的JSON Web令牌配置文件(JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens)

3 术语和定义

下列术语和定义适用于本标准。

3.1

安全保护 secure protection

对会话数据的签名、加密，用于确保传输过程中会话数据机密性和完整性。

3.2

安全传输通道 secure transmission channel

客户端、服务端之间建立的用于安全传输交互数据的逻辑通道。通道两端须进行连接认证，确认对端身份可信。

3.3

安全会话 secure session

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、设备或应用程序等实体身份的过程。身份认证技术包括检查用户凭据是否与授权用户数据库或数据身份验证服务器中的凭据匹配，或使用数字证书判断实体身份是否合法。基于身份认证技术可为系统提供合法的访问控制，确保企业信息安全。

4 缩略语

下列缩略语适用于本标准。

AES：高级加密标准（Advanced Encryption Standard）

DHE：临时迪菲-赫尔曼密钥交换（Diffie-Hellman Ephemeral）

ECDHE：临时椭圆曲线迪菲-赫尔曼密钥交换（Elliptic Curve Diffie-Hellman Ephemeral）

GCM：伽罗华计数器模式（Galois/Counter Mode）

HMAC：基于哈希的消息认证码（Hash-based Message Authentication Code）

HSM：硬件安全模组（Hardware Security Modules）

IdP：企业身份管理服务（Identity Provider）

IV：初始向量（Initialization Vector）

KDF：密钥派生函数（Key Derivation Function）

M2M：设备间交互（Machine to Machine）

MAC：消息认证码（Message Authentication Code）

MITM：中间人攻击（Man-in-the-Middle Attack）

PBKDF2：基于密码的密钥派生算法（Password-Based Key Derivation Function）

PEM：存储、传输密码学的密钥、公开密钥证书和其他数据的文件格式的业界标准（Privacy Enhanced Mail）

PKI：公钥基础设施（Public Key Infrastructure）

PRF：伪随机函数（Pseudorandom Function）

RSA：一种非对称加密算法（Rivest Shamir Adleman）

PSK：预共享密钥（Pre-Shared Key）

SHA：安全散列算法（Secure Hash Algorithm）

SSL：安全套接层（Secure Sockets Layer）

STRIDE：一种识别信息系统安全威胁的威胁建模方法（Spoofing，Tampering，Repudiation，Information Disclosure，Denial of Service，Elevation of Privilege）

TLS：传输层安全（Transport Layer Security）

U2M：用户—设备交互（User to Machine）

5 总体要求

5.1 威胁模型

5.1.1 应基于如下安全环境建立威胁模型：

a） 生产网络处于企业的半开放式环境，环境中可能存在欺骗设备和已失信的恶意设备；

b） 生产环境中可能存在不诚实的、恶意的现场工作人员，可能对设备发送恶意指令和进行恶意操作；

c） 企业 IT 设施中的 PKI、身份与权限管理等安全基础设施是安全可信的，即安全管理过程中不会引入安全威胁。

5.1.2 应采用 STRIDE 方法进行威胁分析和威胁建模，并构建安全框架：

a） 针对煤矿数据采集与传输的网络环境中存在的欺骗威胁，安全框架应提供包括设备连接认证、授权访问、会话管理等风险消减措施；

b） 针对煤矿数据采集与传输的网络环境中存在的篡改威胁，安全框架应提供安全传输能力，以建立设备间通信的安全通道，对会话数据通过消息签名方式实施完整性校验；

c） 针对煤矿数据采集与传输的网络环境中存在的抵赖威胁，安全框架应提供安全审计和日志能力，以及消息数据的签名等能力来消减抵赖风险；

d） 针对煤矿数据采集与传输的网络环境中存在的信息泄露风险，安全框架应提供安全传输、授权访问能力以实现会话数据的传输加密等，消减信息泄露风险；

e） 针对煤矿数据采集与传输的网络环境中存在的拒绝服务威胁，安全框架应提供包括设备连接认证、授权访问、会话管理安全过程，通过分层的模式逐级过滤未授权、无效的消息，以消减拒绝服务风险。

5.2 基本要求

5.2.1 安全性

安全性要求如下：

a） 进行通信、交互的设备应进行设备级的连接认证，保证参与交互的各设备的身份可信；

b） 应对跨设备交互过程中的数据进行安全保护，宜通过加密、签名等方式保证数据的完整性、机密性，并识别和拒绝恶意的或非法的交互数据，保证系统可用性；

5.2.2 可配置性

设备厂商、业务应用开发者以及设备使用者可根据具体环境、业务目标，为设备、应用灵活配置安全策略。

5.2.3 可管理性

安全过程应与企业安全管理设施兼容，能够对接 PKI、提供身份与权限管理等，让企业能够对基于本文件构建的设备进行安全管理、运营。

5.3 安全框架

5.3.1 一般要求

整体安全框架如图1所示。安全框架宜与企业其他信息化安全基础设施对接，形成完整的煤矿数据采集与传输安全解决方案。

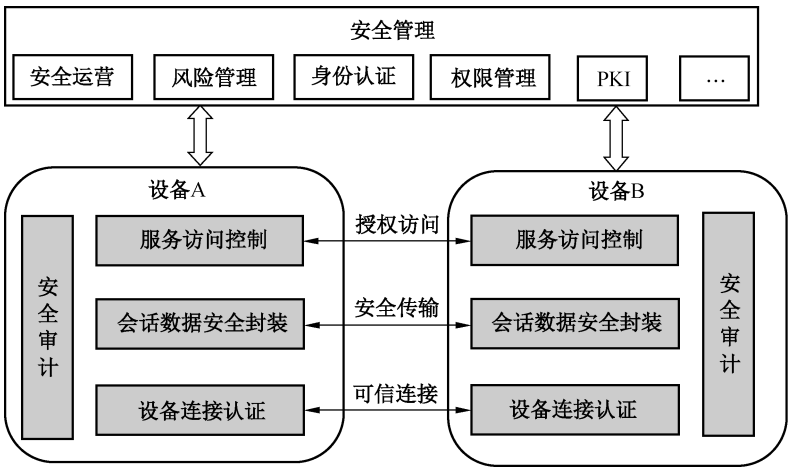

图 1 整体安全框架

5.3.2 可信连接

设备间建立连接后应进行设备连接认证，确保交互各方设备是可信的、合法的，确保仅通过设备身份认证、建立信任关系的设备才能进行交互。

5.3.3 安全传输

基于传输层、面向上层应用提供的端端应用之间的安全传输能力。通过对会话数据进行安全封装，确保即使在传输层不可信的情况下仍可保证上层应用数据传输时的完整性和机密性。

5.3.4 安全审计

对设备认证等安全相关活动进行审计，如认证失败、安全传输通道建立失败等。基于安全审计日志，可进一步进行威胁分析、风险识别，提供威胁发现抗抵赖、可追溯能力。

5.4 安全模型

5.4.1 安全模型包含设备连接认证、安全传输安全要求。这2项安全要求应通过安全服务集和安全配置相互配合实现。安全模型包括设备连接认证和安全传输能力，实现对业务场景下的网络安全威胁的消减和应对。

5.4.2 设备连接认证：定义多种设备间认证方式，提供设备间认证所需的证书、密钥或凭据等材料，具备设备间认证的能力，具体定义应符合“6 连接认证”要求。

5.4.3 安全传输：为业务交互创建安全传输通道、确定安全传输策略和安全传输模式，具备根据安全传输策略进行会话密钥协商的能力，具备数据安全封装/解封的安全传输功能。该安全传输通道是设备间端到端的逻辑通道，具体定义应符合“7 安全传输”要求。

5.5 安全设置与安全配置集

5.5.1 安全设置

安全能力应支持设备连接认证、安全传输的安全能力配置，设备和服务宜根据安全级别需求、运行环境以及设备规格等进行灵活配置。安全设置包括设备安全策略、安全传输模式等。

5.5.2 设备安全策略

提供设备级的协议安全设置，包括设备支持的安全连接认证方式、密码相关安全策略，要求如下：

a） 设备安全策略宜通过设备配置“开启设备认证”标志，决定在设备认证和安全传输过程中当前设备是否需要对对端设备进行身份认证。

b） 设备认证模式可配置多种设备认证方式，在设备认证时对端设备应选择合适的认证方式对本端设备进行认证。

c） 设备安全策略包含当前设备支持的密码相关安全策略，在密码策略中详细描述具体的密码算法、哈希算法、密钥长度等。密码策略主要用于安全传输场景，包括密钥协商、会话加密、签名等。

d） 设备安全策略针对“请求—响应”式消息提供安全设置项，使得会话数据可设置“密钥过期时间”来触发密钥重新协商。详细描述见“6.2 设备安全策略”。

5.5.3 密钥安全策略

用于安全认证、安全传输的密码策略应提供密钥协商、会话加密和签名等内容。各煤矿企业应根据自身实际情况选择一种适宜的密钥安全策略。密钥应由煤矿企业统一进行管理。策略编码及其语义说明见表1。在协商过程中，通过传递密码策略编码进行协商，编码长度为2字节。

表1 密码策略列表

ID	策略编码	名称	语义
1	0x0101	RSA_AES128	RSA方式进行密钥协商； AES_128_GCM方式进行消息加解密； MAC签名等过程中的哈希算法采用SHA256； AES密钥长度128位，IV长度96位，MAC密钥长度256位
2	0x0201	DHE_AES128	DHE方式进行密钥协商； AES_128_GCM方式进行消息加解密； MAC签名等过程中的哈希算法采用SHA256； AES密钥长度128位，IV长度96位，MAC密钥长度256位
3	0x0202	DHE_AES256	DHE方式进行密钥协商； AES_256_GCM方式进行消息加解密； MAC签名等过程中的哈希算法采用SHA384； AES密钥长度256位，IV长度96位，MAC密钥长度384位
4	0x0301	ECDHE_AES128	ECDHE方式进行密钥协商； AES_128_GCM方式进行消息加解密； MAC签名等过程中的哈希算法采用SHA256； AES密钥长度128位，IV长度96位，MAC密钥长度256位
5	0x0302	ECDHE_AES256	ECDHE方式进行密钥协商； AES_256_GCM方式进行消息加解密； MAC签名等过程中的哈希算法采用SHA384； AES密钥长度256位，IV长度96位，MAC密钥长度384位

表 1（续）

ID	策略编码	名称	语义
6	0x0401	PSK_AES128	PSK 方式进行密钥协商； AES_128_GCM 方式进行消息加解密； MAC 签名等过程中的哈希算法采用 SHA256； AES 密钥长度 128 位，IV 长度 96 位，MAC 密钥长度 256 位
7	0x0402	PSK_AES256	PSK 方式进行密钥协商； AES_256_GCM 方式进行消息加解密； MAC 签名等过程中的哈希算法采用 SHA384； AES 密钥长度 256 位，IV 长度 96 位，MAC 密钥长度 384 位

5.5.4 安全传输模式

安全传输应支持为服务设置会话数据的“安全传输模式”，确定服务会话数据的安全保护方式。安全保护方式有不加密不签名、签名并加密 2 种方式，煤矿数据采集与传输宜采用“签名并加密”的安全保护方式。安全传输应支持在设备安全策略中设置使用的密码算法套件。

6 连接认证

6.1 一般要求

6.1.1 设备间的连接认证应满足下列要求：

a） 应假设所有设备在初始连接阶段不可信，设备应通过设备连接认证、建立可信连接，才能作为网络中的有效设备节点进行业务交互。连接认证应对网络中拟进行交互的设备、终端进行身份认证、合法性判断，避免与不可信设备进行业务交互的风险。

b） 连接认证应为通过身份认证的设备创建后续设备间安全交互所需的密钥材料等。经过连接认证后的设备、终端，将有能力进行与网络中的其他设备节点进行安全的数据传输、业务交互。

c） 在设备规格、硬件性能满足的情况下，应优先使用设备数字证书，仅硬件受限条件下使用预共享密钥认证方式。

6.1.2 设备连接认证场景：设备应根据具体业务环境情况，支持一种或多种连接认证方式。

6.1.3 设备连接认证的基本流程如图 2 所示。

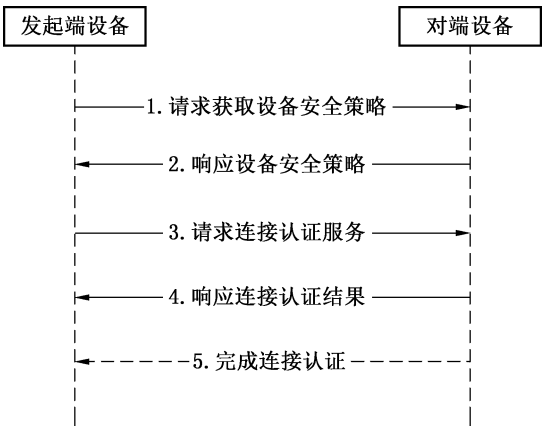

图 2 设备间连接认证的基本过程

a） 步骤1：请求获取对端设备安全策略。

b） 步骤2：对端设备响应自身设备安全策略。

c） 步骤3：基于设备安全策略中的设备认证方式列表，确定一种双方支持的设备认证方式，并配置认证参数，发起连接认证服务请求。

d） 步骤4：对端设备响应设备认证请求。根据选定的认证方式和对应的认证协议、密钥交换协商协议与发起端设备进行交互，完成连接认证并响应认证结果。

e） 步骤5：发起端设备处理响应结果，完成设备间的连接认证。若认证成功，则继续业务交互；若认证失败，则断开连接。

注1：设备认证过程根据认证方式不同，可能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。

注2：不同认证方式对应的具体流程以及请求和响应参数存在的差异，在对应认证方式中分别描述。

6.2 设备安全策略

设备安全策略的各个属性约束见表2。

表2 设备安全策略的属性说明

属性ID	属性名称	数据类型	属性描述
1	设备认证方式	byte	设备支持的认证方式列表，用一个byte表示，每一位代表一种认证方式，该位为1表示支持该认证方式，该位为0表示不支持该认证： bit 0：设备证书认证 bit 1：预置公钥凭据 bit 2：预共享密钥 bit 3～7：保留
2	开启设备认证	bool	是否验证对端： true：响应方要求验证对端身份 false：响应方不要求验证对端身份
3	安全能力标识	uint32	预留标识安全配置选项
4	支持的密码策略	uint16 array	支持的密码策略列表（密钥协商、加密解密、签名算法等）
5	预共享密钥信息	PSKInfo	预共享密钥标识的列表[identity-id]。设备内可能预制了多个设备认证的共享密钥，通过共享密钥标识进行区分，见表3
6	预置公钥凭据算法	byte	设备公钥凭据算法标识。不同值标识一组对应的密钥生成算法、凭据签名/验签算法信息 0：不支持设备凭据 1：ECDSA

表3 预共享密钥信息

属性ID	属性名称	数据类型	属性描述
1	预共享密钥标识个数	uint16	预共享密钥标识列表中密钥对个数
2	预共享密钥标识（PSK）	string	设备认证的共享密钥标识1

表 3（续）

属性 ID	属性名称	数据类型	属性描述
…	…	…	…
n+1	预共享密钥标识	string	设备认证的共享密钥标识 n

6.3 设备连接认证相关服务和过程

6.3.1 获取设备安全策略

6.3.1.1 获取指定设备的设备安全策略的请求见表 4。

表 4 获取设备安全策略的请求参数说明

ID	参数名	数据类型	参数说明
1	消息体头	uint16	消息类型为 0，服务集标识为 2，服务编码为 1
2	目标设备 ID	byte array	目标设备的设备标识
3	本端设备 ID	byte array	本端设备的设备标识

6.3.1.2 响应参数见表 5。

表 5 获取设备安全策略的响应参数说明

ID	参数名	数据类型	参数说明
1	消息体头	uint16	消息类型为 1，服务集标识为 2，服务编码为 1
2	结果状态	uint16	结果状态，取值定义要求参照 MT/T 1202.5—2023
3	设备安全策略	DeviceSecurityPolicy	响应的设备安全策略，仅结果状态取值为成功时携带。具体字段应符合“6.2 设备安全策略”的要求

6.3.1.3 处理过程要求：服务端收到请求后，将设备安全策略信息响应给客户端，客户端收到设备安全策略后进行解析，按需使用。如果服务端因异常无法响应设备安全策略，则应将结果状态置为失败，不携带设备安全策略，将失败响应发送给客户端。

6.3.2 设备连接认证服务

设备连接认证服务应支持不同设备连接认证方式的交互。设备连接认证服务宜根据设备情况、业务环境选择性支持一种或多种的完整设备连接认证过程。设备连接认证服务对应的请求和响应的消息报文格式是确定的，中间认证过程由请求参数中的认证方式决定，认证结果由响应参数决定。设备连接认证服务支持的认证方式包括设备证书认证、预共享密钥认证。

6.3.2.1 双向证书认证

6.3.2.1.1 基于 RSA 的双向证书认证

数字证书的认证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”。双方采用协商的密钥算法根据 r_A、r_B 和 r_{PMK} 派

生会话密钥集。在接下来的数据传输中，发起端设备和对端设备将会使用协商的密钥进行对称签名和加密，保证通信过程中的数据完整性、机密性。

基于 RAS 的双向证书认证应实现如下要求：

a） 双向认证流程如图 3 所示。

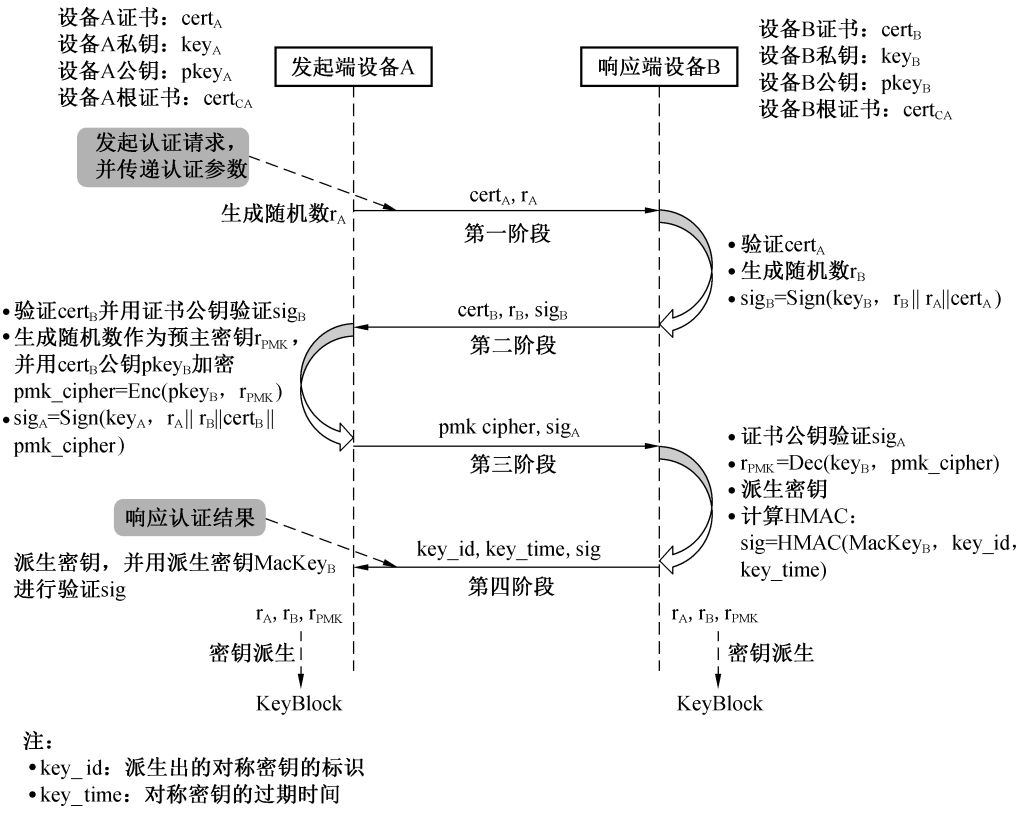

图 3 基于 RSA 的双向证书认证

b） 认证过程报文说明见表 6、表 7、表 8 和表 9。如果响应端设备在任意阶段过程中出现失败，则应直接回复第四阶段报文。

表 6 双向连接认证第一阶段报文

ID	参数名	数据类型	参数说明
1	消息体头	uint16	消息类型为 0，服务集标识为 2，服务编码为 2
2	认证阶段	byte	标识认证过程的阶段，值为 1
3	认证方式	byte	选定的设备认证类型，值为 1，设备证书认证
4	发起端身份凭据	byte array	发起端的 x509 v3 证书
5	发起端随机数	byte array	符合设备认证策略的随机数
6	有效期	uint32	使用安全通道时，标识安全通道的有效期。过期前，客户端将发起重认证以更新通道生命周期。不支持更新，则为 0。单位为秒
7	密码算法策略	uint16	设备认证过程中的密码算法策略标识。包括密钥派生函数、签名、加密等算法
8	请求认证对端	bool	标识是否认证对端。值为 true，需要认证对端

表 7　双向连接认证第二阶段报文

ID	参数名	数据类型	参数说明
1	消息体头	uint16	消息类型为 1,服务集标识为 2,服务编码为 2
2	认证阶段	byte	标识认证过程的阶段,值为 2
3	响应端证书	byte array	响应端的 x509 v3 证书
4	响应端随机数	byte array	符合设备认证策略的随机数
5	签名	byte array	对发送的数据进行签名,用于对端验证本端身份

表 8　双向连接认证第三阶段报文

ID	参数名	数据类型	参数说明
1	消息体头	uint16	消息类型为 0,服务集标识为 2,服务编码为 2
2	认证阶段	byte	标识认证过程的阶段,值为 3
3	加密的预主密钥	byte array	加密后符合设备认证策略的预主密钥
4	签名	byte array	对发送的数据进行签名,用于对端验证本端身份

表 9　双向连接认证第四阶段报文

ID	参数名	数据类型	参数说明
1	消息体头	uint16	消息类型为 1,服务集标识为 2,服务编码为 2
2	认证阶段	byte	标识认证过程的阶段,值为 4
3	结果状态	uint16	结果状态,取值定义要求参照 MT/T 1202.5—2023
4	密钥标识	byte	一组密钥的唯一标识,仅结果状态取值为成功时携带
5	安全通道过期时间	uint64	安全通道过期时间,不过期填 0,仅结果状态取值为成功时携带
6	签名	byte array	对发送的数据进行签名,用于对端验证本端身份,仅结果状态取值为成功时携带

6.3.2.1.2　基于 ECDHE/DHE 密钥协商的双向证书认证

ECDHE/DHE 双向证书认证流程(图 4)应实现如下要求:

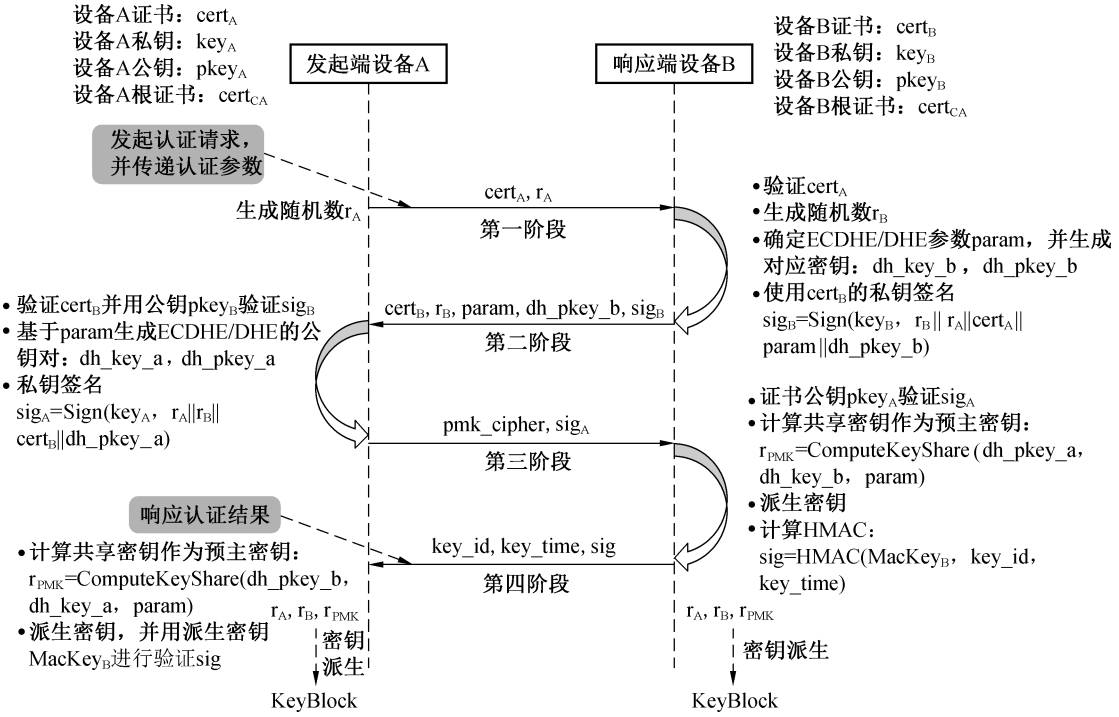

图 4　基于 ECDHE/DHE 密钥协商的双向证书认证流程图

认证过程报文说明见表 10、表 11、表 12 和表 13。如果响应端设备在任意阶段处理过程中出现失败，则应直接回复第四阶段报文。

表 10　双向连接认证第一阶段报文

ID	参数名	数据类型	参数说明
1	消息体头	uint16	消息类型为 0，服务集标识为 2，服务编码为 2
2	认证阶段	byte	标识认证过程的阶段，初始的认证请求中该字段为 1
3	认证方式	byte	选定的设备认证类型，值为 1，设备证书认证选定的设备认证类型。 1：设备证书认证
4	发起端身份凭据	byte array	发起端的 x509.v3 证书
5	发起端随机数	byte array	符合设备认证策略的随机数
6	有效期	uint32	使用安全通道时，标识安全通道的有效期。过期前，客户端将发起重认证以更新通道生命周期。不支持更新，则为 0。单位为秒
7	密码算法策略	uint16	设备认证过程中的密码算法策略标识。包括密钥派生函数、签名、加密等算法
8	请求认证对端	bool	标识是否认证对端。值为 true，需要认证对端

表 11　双向连接认证第二阶段报文

ID	参数名	数据类型	参数说明
1	消息体头	uint16	消息类型为 1,服务集标识为 2,服务编码为 2
2	认证阶段	byte	标识认证过程的阶段,值为 2
3	响应端身份凭据	byte array	响应端的 x509 v3 证书
4	响应端随机数	byte array	符合设备认证策略的随机数
5	ECDHE/DHE 参数	uint32	ECDHE/DHE 用于选择加密的参数
6	ECDHE/DHE 公钥	byte array	私钥对应的公钥
7	签名	byte array	对发送的数据进行签名,用于对端验证本端身份

表 12　双向连接认证第三阶段报文

ID	参数名	数据类型	参数说明
1	消息体头	uint16	消息类型为 0,服务集标识为 2,服务编码为 2
2	认证阶段	byte	标识认证过程的阶段,值为 3
3	ECDHE/DHE 公钥	byte array	私钥对应的公钥
4	签名	byte array	对发送的数据进行签名,用于对端验证本端身份

表 13　双向连接认证第四阶段报文

ID	参数名	数据类型	参数说明
1	消息体头	uint16	消息类型为 1,服务集标识为 2,服务编码为 2
2	认证阶段	byte	标识认证过程的阶段,值为 4
3	结果状态	uint16	结果状态,取值定义要求参照 MT/T 1202.5—2023
4	密钥标识	byte	一组密钥的唯一标识,仅结果状态取值为成功时携带
5	安全通道过期时间	uint64	安全通道过期时间,不过期填 0,仅结果状态取值为成功时携带
6	签名	byte array	对发送的数据进行签名,用于对端验证本端身份,仅结果状态取值为成功时携带

6.4　数字证书认证的密钥派生

基于数字证书的认证方式下,根据认证过程协商的 r_A、r_B 和 r_{PMK},应采用 RFC 5246 TLS v1.2 中 PRF 密钥派生函数进行密钥派生。

6.5　设备预共享密钥

6.5.1　适用范围

设备预共享密钥的认证方式为对称式密钥认证,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。

6.5.2 设备预共享密钥发放

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 32 字节。厂家可以预置多组共享密钥，每组共享密钥有唯一的标识符。

6.5.3 预共享密钥认证

预共享密钥认证交互流程如图 5 所示。

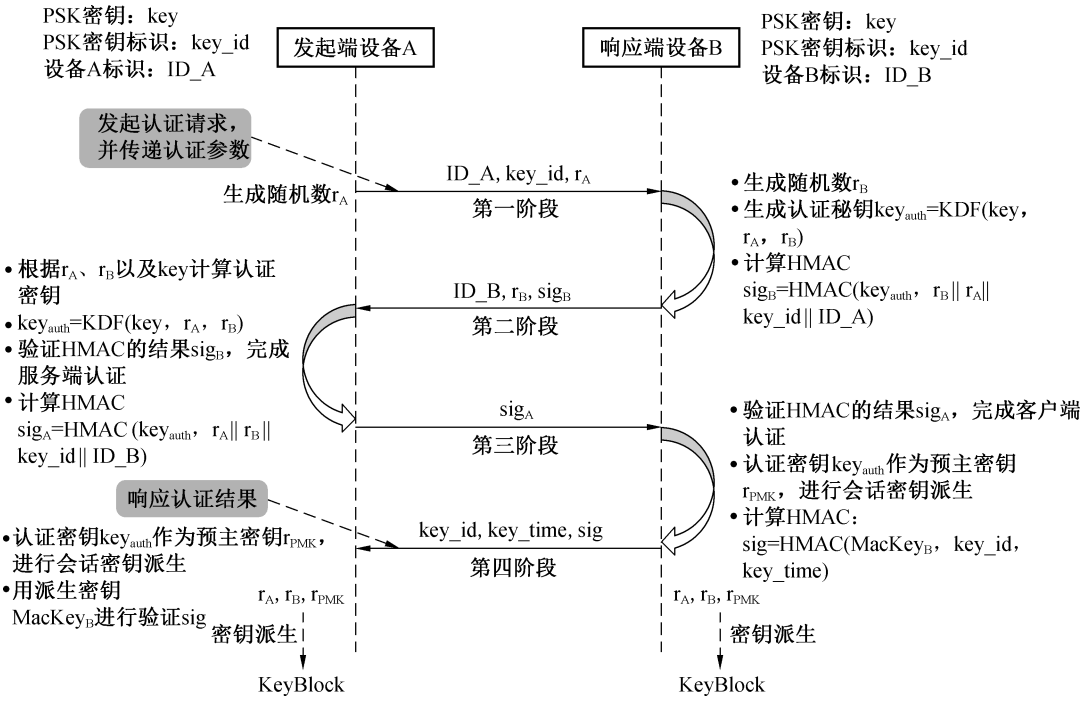

图 5 预共享密钥认证交互流程

6.5.3.1 通过 PSK 完成设备间双向认证的各阶段报文说明见表 14、表 15、表 16 和表 17。如果响应端设备在任意阶段处理过程中出现失败，则应直接回复第四阶段报文。

表 14 预共享密钥认证第一阶段报文

ID	参数名	数据类型	参数说明
1	消息体头	uint16	消息类型为 0，服务集标识为 2，服务编码为 2
2	认证阶段	byte	标识认证过程的阶段，值为 1
3	认证方式	byte	选定的设备认证类型。值为 4，预共享密钥
4	发起端的标识	uint16	发起端的标识，值为 0x0001
5	发起端密钥凭据	byte array	协商的 PSK 的标识
6	发起端随机数	byte array	符合设备认证策略的随机数
7	有效期	uint32	使用安全通道时，标识安全通道的有效期。过期前，客户端将发起重认证以更新通道生命周期。不支持更新，则为 0。单位为秒
8	密码算法策略	unit16	设备认证过程中的密码算法策略标识。包括密钥派生函数、签名、加密等算法

表 15　预共享密钥认证第二阶段报文

ID	参数名	数据类型	参数说明
1	消息体头	uint16	消息类型为 1,服务集标识为 2,服务编码为 2
2	认证阶段	byte	标识认证过程的阶段,值为 2
3	响应端的标识	uint16	响应端的标识,值为 0x0010
4	响应端随机数	byte array	符合设备认证策略的随机数
5	签名	byte array	对发送的数据进行签名,用于对端验证本端身份

表 16　预共享密钥认证第三阶段报文

ID	参数名	数据类型	参数说明
1	消息体头	uint16	消息类型为 0,服务集标识为 2,服务编码为 2
2	认证阶段	byte	标识认证过程的阶段,值为 3
3	签名	byte array	对发送的数据进行签名,用于对端验证本端身份

表 17　预共享密钥认证第四阶段报文

ID	参数名	数据类型	参数说明
1	消息体头	uint16	消息类型为 1,服务集标识为 2,服务编码为 2
2	认证阶段	byte	标识认证过程的阶段,值为 4
3	结果状态	uint16	结果状态
4	密钥标识	byte	一组密钥的唯一标识,仅结果状态取值为成功时携带
5	安全通道过期时间	uint64	安全通道过期时间,不过期填 0,仅结果状态取值为成功时携带
6	签名	byte array	对发送的数据进行签名,用于对端验证本端身份,仅结果状态取值为成功时携带

6.5.3.2　使用基于“预共享密钥—密码校验函数—采用随机数作为时变参数”的双向认证方案,即 ISO/IEC 9798-4 标准中的认证模型 4,宜通过预共享密钥和双方认证时产生的随机数派生后续传输使用的加密密钥和消息完整性保护的密钥及双方通信的 IV。其中密钥派生函数可以为 PBKDF2、PRF 等。

7　安全传输

7.1　一般要求

7.1.1　安全传输内容

安全传输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。安全传输为上层业务应用数据提供传输层透明、安全可靠的传输通道,有效保证应用数据的机密性、完整性。安全传输的保护对象是与业务交互的会话数据。安全传输包括设备间安全传输通道的建立、会话数据安全传输确定等。

7.1.2 安全传输场景

安全传输支持为“请求—响应”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。

7.1.3 安全传输要求

7.1.3.1 点对点的“请求—响应”式会话的安全保护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。

7.1.3.2 基于安全传输通道提供的安全能力应实现如下安全属性：

a） 安全传输通道的两端通过网络传输通道（裸通道）完成双向设备连接认证，建立互信关系。

b） 对安全通道承载的会话数据加密、签名后进行安全传输，保证数据的机密性、完整性。

c） 会话数据安全传输时使用的密钥信息（加密、签名的密钥信息）通过密钥协商方式确定；会话密钥集可通过安全通道进行更新。

7.1.3.3 客户端设备和服务端设备之间可建立一个或多个安全传输通道；不同的会话可复用同一个安全传输通道。安全传输通道的数量以及通道复用由业务和下层的连接管理决定。

7.1.3.4 安全传输通道能力的提供通过设备安全策略、服务声明的安全传输模式和安全传输服务实现。安全传输通道的能力通过初始化安全通道、会话建立、会话断开实现。

a） 初始化安全通道包括建立一个设备间的传输通道，并完成设备间连接认证，完成可信的安全传输通道的初始化。

b） 会话建立包括在已初始化的安全传输通道上基于服务的安全传输策略确定会话数据安全传输模式，并完成会话的客户端身份等信息传递。

c） 会话断开包括清除会话的客户端身份、权限等信息。

7.2 数据安全封装/解封的约定

7.2.1 一般要求

数据安全封装/解封的过程基于服务的安全传输模式设置，对服务的会话数据进行签名、加密、解密、验签。数据安全封装和解封适用于“请求—响应”会话模式，需会话两端已完成密钥协商、持有有效会话密钥。

7.2.2 端内数据处理过程

端内数据处理过程包含不签名不加密模式和签名并加密模式。

7.2.2.1 不签名不加密模式

不签名不加密模式下，不提供数据的完整性和机密性保护。

7.2.2.2 签名并加密模式

在签名加密模式下，提供数据的机密性和完整性保护。使用 AES-GCM 模式进行加密，报文头和安全头部分用来做校验。

7.2.2.2.1 客户端发送数据应实现如下处理要求：

a） 客户端根据消息体创建报文头，根据安全策略生成安全头。

b） 使用的加密算法对报文头、安全头和消息体，生成带 TAG 的密文部分。报文头、安全头会作为加密算法的 ADDITIONAL_DATA 传入，IV 后四位需要与报文头中的序列号做异或运

算，形成新的 IV 用于加密。

c） 将报文头、安全头和密文部分拼接，形成最终传输的安全数据。

7.2.2.2.2 服务端接收数据应实现如下处理要求：

a） 服务端接收安全数据后，拆封为报文头、安全头和密文数据。

b） 服务端对密文数据进行解密校验，解密校验填入对应的 ADDITIONAL_DATA 和 IV，如果解密校验通过，则将消息体交给接收方进行处理；如果失败，丢弃该数据。

7.2.3 数据的安全封装格式

7.2.3.1 安全封装格式

消息数据的安全封装格式如图 6 所示。

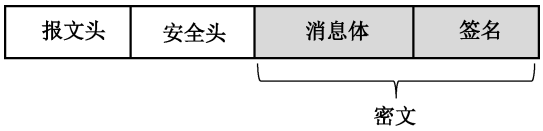

图 6 消息数据的安全封装格式

7.2.3.2 安全头

消息中的安全头字段说明见表 18。

表 18 消息中的安全头字段说明

字段 ID	字段名	数据类型	参数说明
1	安全传输模式	byte	标识消息体的安全处理方式。0x00：不签名不加密；0x01：仅签名不加密；0x02：签名并加密
2	密钥标识	byte	连接认证协商出的密钥标识

8 安全审计

8.1 一般要求

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。安全审计则是从安全的角度对系统中安全相关的操作、活动的审计，这既包括正常操作，也包括未预期的异常行为。基于这些审计记录，可进行持续性的安全分析、风险评估，以及事后的回溯、取证。安全审计包括设备间互联互通互操作过程中的安全相关活动，例如设备认证是否成功、安全选项协商结果、请求服务拒绝访问、配置策略变等的审计记录。

8.2 审计内容

安全审计日志在生成阶段应满足的要求包括对关键事件/活动进行记录、日志内容要准确完备，每一条审计日志中至少应包括事件主体、事件发生的时间日期、事件描述和结果。若采用远程登录方式对产品进行管理还应记录管理主机的地址。本标准中的审计内容应包括用户身份认证、设备连接认证、安全传输等过程和相关事件。安全审计日志的保存时间应不低于 6 个月。

8.3 安全审计的实施建议

安全审计宜使用如下一种或两种方法完成：

a） 生成审计事件的应用程序宜将审计条目记录到日志文件或其他存储位置中。

b） 生成审计事件的服务器宜使用事件机制发布审计事件。允许外部客户端订阅审计条目并将其记录到日志文件或其他存储位置。

8.4 审计记录的管理建议

审计功能是追踪入侵、追溯系统操作活动，以及恢复系统的直接证据，应保证审计记录自身的安全。审计系统的安全包括两个方面的内容，一个是审计事件的访问安全，一个是审计事件的存储安全。审计事件的访问应该受到严格限制，避免日志信息被未经授权的恶意篡改、删除等。审计记录中可能包含敏感信息，应对订阅审计事件的能力进行访问控制，以使其访问范围限定在特定的用户和应用程序。

9 实施要求

9.1 密钥等敏感数据存储和管理

密钥等敏感数据存储和管理应按照下列要求实施：

a） 设备上的设备证书及私钥、用于对称加密/签名的密钥等敏感数据在本地存储时应有安全保护机制，防止其以明文的形式保存在系统或代码中。

b） 密钥应采用分层管理结构。上层密钥的机密性保护需要用下层密钥加密来保证，用下层密钥来加密上层密钥，防止其以明文的形式保存在系统或代码中，如使用对称算法 AES 算法等对密钥进行加密保护。

c） 对于支持预共享密钥认证的设备，建议支持通过工具手动更新预共享密钥或自动更新密钥的机制，预共享密钥泄露后可在无需全部重置设备的情况下更新密钥。

d） 在系统环境允许的情况下，本规范相关的证书、密钥等可利用系统的密钥管理功能进行托管，并利用系统能力进行数据签名和验签等。

9.2 异常消息处理

协议实现中应在消息处理过程中进行严格的格式检查，对于异常格式消息进行丢弃处理；在会话过程中设置超时处理机制，会话超时将自动关闭安全会话、清除密钥信息等。