GB/T XXXXX—XXXX

ICS 35.240.99
L 78

团　　体　　标　　准

团体标准编号

建筑及居住区数字化户用计量仪表安全技术

XX 年 XX 月 XX 日发布　　XX 年 XX 月 XX 日实施

中国工程建设标准化协会 发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国工程建设标准化协会厨卫专业委会归口。

本标准起草单位：

本导则主要起草人：

建筑及居住区数字化 户用计量仪表安全技术

1 范围

本标准规定了建筑及居住区中户用计量仪表的一般规定、电气安全、物理安全、信息安全。

本标准适用于建筑及居住区中户用计量仪表系统的设计、建设及运营等。

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/T 778 饮用冷水水表和热水水表 第1部分：计量要求和技术要求

GB/T 4208 外壳防护等级(IP代码)

GB 4706 家用和类似用途电器的安全第1部分-通用要求

GB/T 6968 膜式燃气表

GB/T 25480 仪器仪表运输、贮存基本环境条件及试验方法

CJ 128 热量表

CJJ 34 城市热力网设计规范

CJ/T 166 建设事业集成电路（IC）卡应用技术条件

CJ/T 188 户用计量仪表数据技术条件

CJ/T 503 无线远传膜式燃气表

CJ/T 535 智能水表

JG/T 162 住宅远传抄表系统

JJG 162 冷水水表

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

安全模块 security module

具有密码算法、安全功能的媒体。

3.3

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。

3.4

解密 decryption
将“密文”变为“明文”的过程被称为解密。

3.5

算法 algorithm
指解题方案的准确而完整的描述，是一系列解决问题的清晰指令，算法代表着用系统的方法描述解决问题的策略机制。

3.6

密钥 key
控制加密转换操作的符号序列。

3.7

CPU卡 central processing unit card
一种具有微处理器芯片的IC卡。

3.8

SM4算法 SM4 algorithm
由GB/T 32907定义的一种分组密码算法。

4 缩略语

下列缩略语适用于本文件。
CPU 中央处理单元（Central Processing Unit）
IC 集成电路（integrated circuit）
MCU 微控制单元（Micro Controller Unit）
PIN 个人识别码(Personal Identification Number)
PKI 公钥基础设施(Public Key Infrastructure)

5 一般规定

5.1 概述

户用计量仪表原指专门用来测量水、气、电、油的压力、流量、温度的精密设备。本标准主要规范户用智能水表、智能燃气表、智能热量表技术要求。

5.2 智能水表

5.2.1 智能水表所使用的静压力应符合 JJG 162-2019 的规定。

5.2.2 智能水表的准确度等级分为 1 级和 2 级，不同准确度等级的水表在不同工作温度下的最大允许误差应符合表 2 的规定。（Q_1：最小流量；Q_2：分界流量；Q_4：过载流量）

表格 1 水表最大允许误差

流量		低区	高区	
		$Q_1 \leq Q \leq Q_2$	$Q_2 \leq Q \leq Q_4$	
工作温度		0.1≤Tw≤50	0.1≤Tw≤30	30<Tw≤50
最大允许误差	1级	±3%	±1%	±2%
	2级	±5%	±2%	±3%

5.3 智能燃气表

5.3.1 智能燃气表使用的基表应符合 GB/T 6968—2011 的规定。

5.3.2 智能燃气表流量范围应符合表 1 的规定。

表格 2 燃气表流量范围

单位为立方米每小时

公称流量	最大流量值	最小流量上限值	最大始动流量
1.6	2.5	0.016	0.003
2.5	4	0.025	0.005
4	6	0.040	0.005
6	10	0.060	0.008

5.4 智能热量表

5.4.1 智能热量表所使用的水质应符合 CJJ 34 的规定。

5.4.2 智能热量表的使用分为 4 各环境类别，其环境条件应符合表 3 的规定。

表格 3 热量表环境条件

环境条件	环境类别			
	A	B	C	D
温度/℃	5～55	-25～55	5～55	-25～55
相对湿度/%	<93	<93	<93	≥93
安装地点	建筑内	建筑外	工业环境	可能被水浸泡的环境
磁场范围	普通磁场	普通磁场	磁场强度较高	普通磁场

6 电气安全

6.1 智能水表

6.1.1 电磁环境

在静电放电、电磁敏感性、静磁场的电磁环境条件下，智能水表应符合 GB/T 778.1中的相关规定。

6.1.2 电源

6.1.2.1 智能水表的供电，应符合 GB/T 778.1 中的相关规定。

6.1.2.2 不可更换电池的智能水表，电池的额定寿命应符合表 4 的规定。

表格 4 电池额定寿命

公称口径/mm	电池寿命/年
≤25	6+1
32、40、50	4+1
>50	2+1
制造厂应确保点吃的额定寿命能保证水表的正常工作年限至少比水表的使用寿命长一年。	

6.1.2.3 可更换电池的智能水表，制造厂应对电池的更换做出明确规定。

6.1.2.4 智能水表电源连接端应有保护措施以防颤动。

6.1.3 电池电源中断

智能水表在电池电源电压短时中断条件下应符合GB/T 778.1中的相关规定。

6.1.4 电子装置可靠性

在规定的使用条件下，智能水表电子装置平均无故障工作时间（MTBF)不应小于$2.63 \times 10^4 h$。

6.2 智能燃气表

6.2.1 静态工作电流

燃气表静态工作电流应不大于$10\mu A$.

6.2.2 最大工作电流

基于微功率无线方式的燃气表阀门不动作时最大工作电流应不大于200mA,阀门动作时最大工作电流应不大于400 mA;基于无线公共网络方式的燃气表最大工体电流应不大于2A.

6.2.3 机电转换误差

机电转换误差应符合下列要求：

a)脉冲式燃气表机电转换误差应不超过±1个机电转换信号当量；

b)直读式燃气表机电转换误差应不超过士1个最小转换分度值。

6.2.4 断电数据存储

当燃气表断电后，重新上电后数据应恢复与断电前一致。

6.2.5 断电关阀

燃气表采用可更换电池供电方式时，应具有断电关阀功能。

6.2.6 电源欠压保护

当燃气表工作电压降至设计欠压值时，应有提示，当电源电压继续下降到设计最低工作电压时，应能关闭阀门，且表内数据不丢失、不错乱。

6.2.7 抗干扰性

6.2.7.1 静电放电抗扰度

智能燃气表受到干扰时，应自动关闭阀门，或应正常工作并符合6.2.1～6.2.6的规定。

6.2.7.2 辐射电磁场抗扰度

智能燃气表受到干扰时，应自动关闭阀门，或应正常工作并符合6.2.1～6.2.6的规定。

6.2.7.3 抗磁干扰

智能燃气表受到干扰时，应自动关闭阀门，或应正常工作并符合6.2.1～6.2.6的规定。

6.3 智能热量表

6.3.1 电源

6.3.1.1 一般规定

智能热量表可采用内置电池或外部电源。公称直径小于或等于DN40的热量表，应采用内置电池。

6.3.1.2 内置电池使用寿命

内置电池使用寿命的使用寿命应大于5+1年。

6.3.1.3 外部电源

外接交流电源电压应为$V_n =$ （220^{+22}_{-33}）V，频率$\int n =$ （50 ± 1）Hz。
外接直流电源电压可为（5±0.25）V、（12±0.6）V或（24±1.2）V。

6.3.1.4 电池欠压提示

电池的电压降低到设置的欠压值时，热量表应能显示欠压信息。

6.3.1.5 断电保护

当电源停止供电时，热量表必须能保存断电前记录的热量、累计流量和相对应的时间数据及历史数据，恢复供电后应能自动恢复正常计量功能。

6.3.1.6 抗磁场干扰

当受到强度不大于100kA/m的磁场干扰时，不应影响其计量特性。
有磁铁接近时，不能影响计量精度。

6.3.2 电器绝缘性

智能热量表的电器绝缘性能应符合 GB 4706.1的规定。

7 物理安全

7.1 智能水表

7.1.1 外观要求

智能水表的外观要求如下：

a)应有良好的表面处理，不应有毛刺、划痕、凹陷、裂纹、锈蚀、霉斑和涂层剥落等现象；

b)显示的数字应醒目、整齐，表示功能的文字符号和标志应完整、清晰、端正；

c)读数装置上的防护玻璃应有良好的透明度，不应有使读数畸变等妨碍读数的缺陷。

7.1.2 电子封印

智能水表电子封印应符合GB/T 778.1中的相关规定。

7.1.3 外壳防护

智能水表的电子装置连同引出线和引出线密封装置应达到GB/T 4208中规定的IP65防护等级。对于要求能浸没在水中工作的特殊应用，应达到IP68的防护等级。

7.1.4 抗运输冲击性能

智能水表在运输包装条件下，经GB/T 25480规定的模拟运输连续冲击和GB/T 2423.8规定的自由跌落试验后，均不应损坏和丢失信息，并能正常工作。

7.1.5 耐久性

智能水表耐久性应符合GB/T 778.1中的相关规定。

7.1.6 压力损失

智能水表的压力损失应符合 GB/T 778.1中的相关规定。

7.1.7 最高允许工作压力

智能水表的最高允许工作压力应符合GB/T 778.1 中的相关规定。

7.1.8 气候环境

在高温（无冷凝）、低温、交变湿热（冷凝）的气候环境条件下，智能水表应符合GB/T 778.1中的相关规定。

7.2 智能燃气表

7.2.1 外观要求

智能燃气表外观应符合下列规定：

a)燃气表外壳涂层应均匀，无气泡、脱落、划痕等缺陷；

b)金属部件应无锈蚀、无伤痕、涂覆颜色应一致；

c)计数器和铭牌应清晰可辨；

d)燃气表应有不经破坏就不能拆卸的防护封印。

7.2.2 电子封印

智能燃气表应具备经外力破坏方能拆卸的防护封印或其他措施。

7.2.3 外壳防护

智能燃气表控制器外壳防护等级应符合GB 4208中IP53等级的要求。

7.2.4 温度范围

7.2.4.1 智能燃气表的最小贮存温度范围应为-20℃～60℃，恢复到实验室环境温度后，智能燃气表性能应符合 6.2.1～6.2.6 的规定。

7.2.4.2 智能燃气表的最小工作环境温度范围应为-10℃～40℃，智能燃气表性能应符合 6.2.1～6.2.6 的规定。

7.2.5 恒温湿热

相对湿度93%,温度40℃,燃气表性能应符合6.2.1～6.2.6的规定，且外观应无锈蚀。

7.2.6 耐盐雾

燃气表应有抗盐雾性能，其性能应符合6.2.1～6.2.6的规定，且外观应无锈蚀。

7.2.7 耐振动

燃气表应承受正常运输搬运过程中的振动，其性能应符合6.2.1～6.2.6的规定。

7.2.8 阀门密封性

阀门在关闭状态下，在阀门人口处输入15kPa压力的气体，泄漏量应不大于0.3 L/h.

7.2.9 阀门耐用性

控制阀门开、关动作各5000次后，阀门密封性应符合7.3.7的规定。

7.2.10 整机密封性

燃气表输入15kPa压力的气体时，燃气表不应泄漏。

7.2.11 开阀保护

开阀动作应由现场人工干预完成。

7.3 智能热量表

7.3.1 外观要求

热量表无裂纹、毛刺等表面缺陷，壳体应能防水、防尘浸入，并用箭头标出水流动方向。

7.3.2 电子封印

智能热量表所有影响计量的可动部件有完好的封印保护。

7.3.3 外壳防护

智能热量表外壳防护等级的分类按GB 4208的规定执行。

a) 智能热量表环境A类应符合IP52的要求；
b) 环境B类的应合IP54的要求；
c) 环境C类的应合IP65的要求；
d) 冷热量表应合IP65的要求；

7.3.4 允许压力损失

智能热量表在常用流量下运行时，允许压力损失不应大于0.025MPa。

7.3.5 重复性

热量表的重复性误差不得大于最大允许误差限。

7.3.6 耐久性

热量表的有效使用周期应大于5年，有效使用周期采用耐久性试验考核。

8 信息安全

8.1 总体架构

根据物联网总体架构，分为四层，即应用层、平台层、传输层与设备层。结合智能水表、智能天然气表及智能热量表的实际应用，当设备层产生的大量数据经过传输层传送到应用层时，如果不经过有效地整合、分析和利用，户用计量仪表数字化就不可能发挥应有的作用。平台层提供数据存储、检索、分析、利用服务功能的同时，还要提供信息安全、隐私保护与网络管理功能，在管理之中体现出服务的目的。

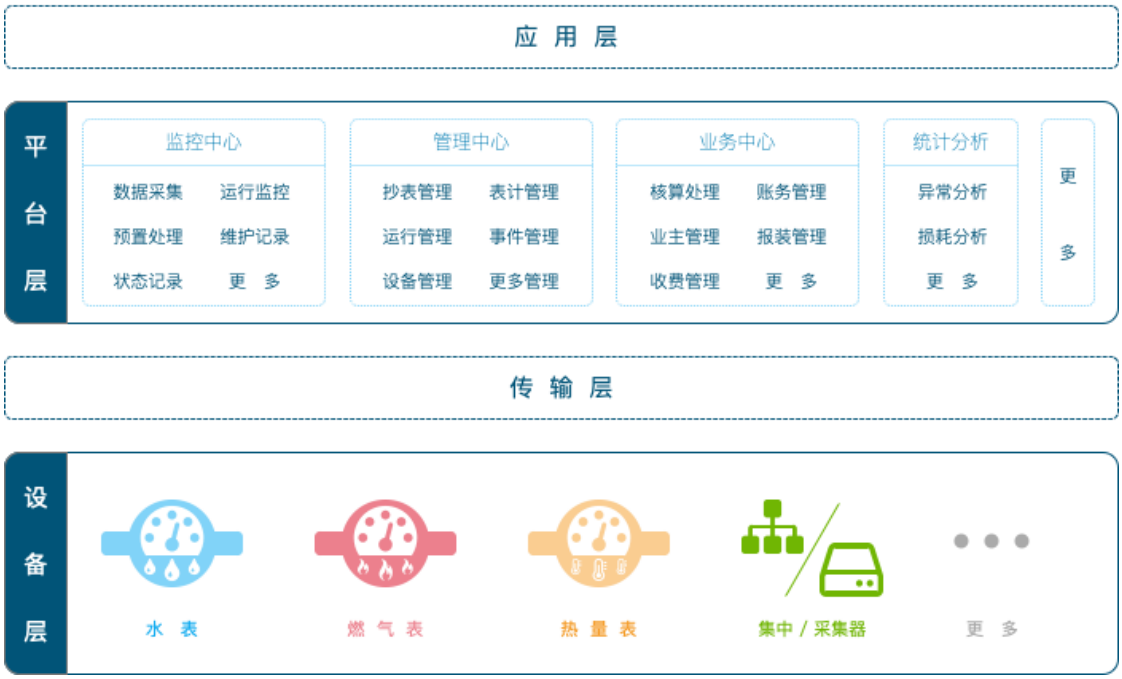

图 1 总体架构

信息安全，涉及平台层与设备层之间的接入与交互，业务平台通过安全服务（含密钥服务），保证平台层与设备层具备相互身份认证的能力，并在完成双向身份认证后，建立加密传输通道，实现信息安全的一般基本要求。这里所指平台应为与设备对接的平台，在不同的业务应用中，可能为设备接入平台或业务平台中的设备接入模块。

8.2 一般要求

户用计量仪表的信息安全，应使用国家密码管理局批准的商用密码算法，至少支持 SM4，密码算法，涉及设备、平台之间的身份认证与加密传输。

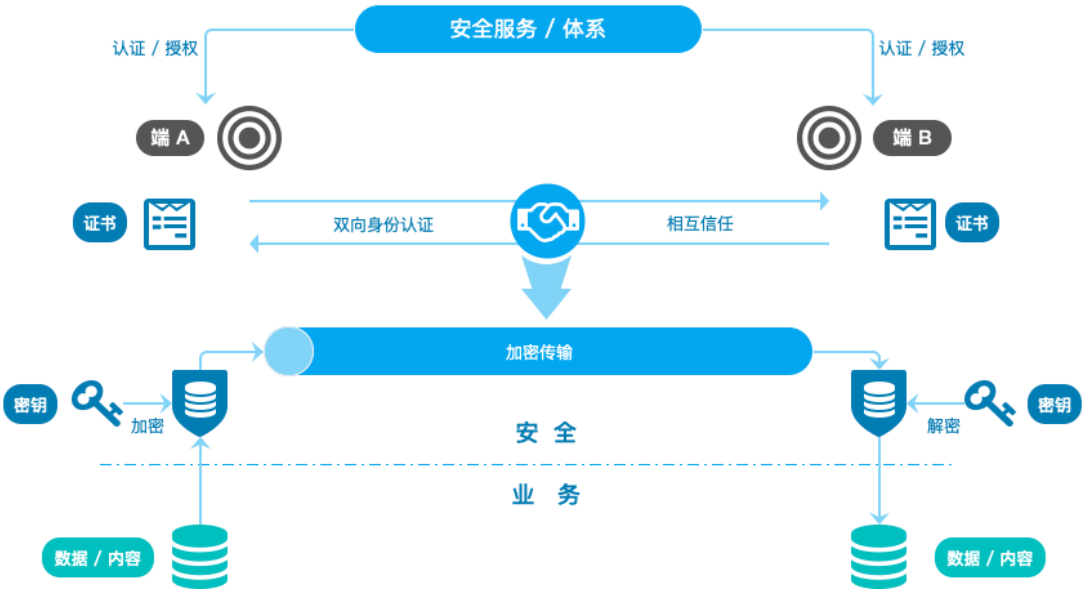

图 2 身份认证与加密传输

通过安全服务对两端进行认证/授权，两端通过认证获取的证书完成双向身份认证，进而建立加密传输通道，通过密钥对业务数据/内容，完成加密传输，满足户用计量仪表的信息安全。

8.3 设备层

8.3.1 一般规定

设备层的一般规定如下：

a) 设备层是指进行数据采集、储存能够与平台进行数据交换的远传水表、远传燃气表、远传热量表以及为实现数据交换而必备的附加设备如：采集器、集中器等。

b) 设备层中远传水表、远传燃气表、远传热量表应符合 CJ/T 188 《户用计量仪表数据传输条件》 4.5 仪表要求、5 物理层以及 6 数据链路层的要求，以下简称设备。

c) 设备电路应具备数据加解密功能，可采用集成了 SM2 或 SM4 加密算法的安全芯片对数据进行加解密，在 MCU 空间具备的情况下也可采用软件实现 SM2 或 SM4 进行数据的加解密。

d) 设备可具有放拆卸功能，设备拆卸报警电路，非正常拆卸时可将报警信息上传到平台。

8.3.2 设备认证

设备认证主要内容如下：

a) 设备第一次与平台联网时，应与平台进行双向身份认证。

b) 设备获取平台下发的平台凭证，通过内置于安全模块的设备凭证进行验证，完成对平台的认证。

c) 设备发送设备凭证至平台完成设备认证，并获取平台下发的会话密钥，作为数据传输时数据加解密使用。

8.3.3 设备存储数据安全要求

设备存储数据安全要求如下：

a) 设备密钥应以密文的方式存储。

b) 设备相关的参数信息包括但不限于服务器地址、通讯端口应以密文方式存储。
c) 设备记录信息包括但不限于累计用量、设备状态、采集时间可以密文的方式存储。

8.4 平台层

8.4.1 一般规定

平台层的一般规定如下：
a) 平台层是连接感知层和应用层的桥梁，提供安全可靠的设备连接通信能力，支持设备数据采集上云，规则引擎流转数据和云端数据下发设备端。
b) 平台层提供方便快捷的设备管理能力，支持物模型定义，数据结构化存储，和远程调试、监控、运维。

8.4.2 平台认证

平台认证的主要内容如下：
a) 平台应在设备注册前，通过安全服务完成平台的认证，认证信息应包括但不限于平台应用领域、业务类型等。
b) 平台第一次接入安全服务后，应完成相关认证（证书、密钥等）凭证的获取，并通过安全服务 SDK 内置于平台的系统中，保证每次调用安全服务的身份认证。

8.4.3 平台存储数据安全要求

平台存储数据安全要求如下：
a) 平台密钥应以密文的方式存储。
b) 平台相关的参数信息包括但不限于服务器地址、通讯端口应以密文方式存储。
c) 平台记录信息包括但不限于累计用量、设备状态、采集时间可以密文的方式存储。

8.5 安全要求

8.5.1 身份认证

8.5.1.1 证书的获取

证书分为平台证书与设备证书，具体如下：
a) 平台证书，由业务平台对接安全服务获取，通过集成适应环境的安全服务 SDK 完成证书的安全应用。
b) 设备证书，罐装于安全模块，设备通过生产、改造的方式，集成安全模块。

8.5.1.2 认证机制

认证机制包含设备对平台及平台对设备的认证，即双向认证为完整的身份认证，具体涂下：
a) 设备获取平台下发的平台证书，并通过设备证书的公钥进行验证，完成设备对平台的认证。
b) 平台获取设备上传的设备证书，并通过平台证书的公钥进行验证，完成平台对设备的认证。

8.5.2 加密传输

8.5.2.1 密钥的获取

用于加密传输的密钥为国产密码算法的对称密钥，通过该密钥（如表格5）将设备、平台信息进行分散、加密，形成用于传输的会话密钥。

表格 5 加密传输密钥

密钥	意义
名称	应用传输加密认证密钥（DF01 应用）
别名	DIAK
层级	4

传输密钥分为平台传输与设备传输，具体如下：

a) 平台传输密钥，由业务平台对接安全服务获取，通过集成适应环境的安全服务 SDK 完成密钥的安全应用。

b) 设备传输密钥，罐装于安全模块，设备通过生产、改造的方式，集成安全模块。

8.5.2.2 传输机制

传输机制，应用于业务平台与设备之间的传输，具体如下：

a) 业务平台通过应用传输加密认证密钥对设备与安全模块的信息进行分散、加密，形成用于传输的会话密钥，实现与设备间的数据加解密传输。

b) 设备通过应用传输加密认证密钥对设备与安全模块的信息进行分散、加密，形成用于传输的会话密钥，实现与设备间的数据加解密传输。

8.5.3 密钥管理

密钥的生成、分发等生命周期管理由安全服务支持，具体如下：

a) 在密钥信息及业务信息的传输过程中，均采用 PKI 体系做加密保护，采用国产密码算法对实际业务采用对称密钥加密；

b) 平台能够监控核心索引位置的密钥使用频率，从而对项目开展情况，有直观了解；

c) 项目级密钥管理通过安全服务支撑，需要在联网情况下使用，考虑到密钥管理服务的相对封闭性，因此每次交互操作（如密钥的获取与维护），都须验证平台的身份。

8.5.4 安全模块

能够提供必要的安全机制，以防止外接对终端所存储或处理的安全数据进行非法攻击的硬件加密模块，即芯片，用于智能计量仪表的安全模块均应满足以下基本安全要求：

a) 应使用国家密码管理局批准的商用密码算法，至少支持 SM4，密码算法由硬件实现；

b) 应通过国家密码管理局安全芯片等级一级或以上认证；

c) 应实现智能计量仪表业务安全所需加解密服务、数据鉴权、安全认证、子密钥生成等安全服务功能，并提供应用接口；

d) 应对智能计量仪表业务安全所需用户 PIN 码、用户身份鉴权数据等用户敏感信息进行安全存储，并提供应用接口；

e) 应提供根密钥安全存储接口，根密钥在发行时由运营方以安全方式写入设备，应保证写入后无法通过任意接口读取和修改根密钥；

f) 应支持一表一密、内外部认证等密钥管理机制，确保身份认证安全性，支持与设备绑定使用，在非绑定设备上应不能正常工作；

g) 应符合 CJ/T 166-2014 中关于安全存取模块和安全设备的相关要求。

8.5.5 数据安全

8.5.5.1 一般要求

系统加解密和密钥管理应符合国家密码管理的有关规定，具体要求如下：

a) 密码算法应符合 CJ/T 188-2018 7.2
b) 数据填充应符合 CJ/T 188-2018 7.4
c) 数据加密应符合 CJ/T 188-2018 7.5
d) 数据解密应符合 CJ/T 188-2018 7.6

8.5.5.2 密码算法

数据加解密采用 SM4 分组密码算法，分组长度 16 个字节。分组密码算法的工作模式为密码分组链接（Cipher Block Chaining，CBC)模式。

8.5.5.3 加解密要求

填充后的数据按照 SM4 密码算法进行加密。加密完成后，替换帧的数据域内容，并修改数据长度域和校验码为正确的数值。仪表应根据产品安全性要求决定报文指令是仅支持明文传输、仅支持密文传输还是同时支持两种方式。对于含有敏感数据的报文，例如写购入金额，可仅支持加密传输

数据解密是加密的逆过程，在接收数据后，按照 SM4 密码算法进行解密运算。数据解密完成，通过合法性验证后，去掉填充内容，恢复原始数据进行数据处理。