ICS 33.050
CCS M 30

团　体　标　准

T/TAF 194—2023

集成独立安全芯片的行业物联网模组安全技术要求

Security technical requirements for industrial IoT modules integrated independent security chips function

2023-11-24 发布　　2023-11-24 实施

电信终端产业协会　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。

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专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：郑州信大捷安信息技术股份有限公司、中国信息通信研究院、博鼎实华（北京）技术有限公司、联想（北京）有限公司、深圳信息通信研究院、高通无线通信技术(中国)有限公司、蚂蚁科技集团股份有限公司、国民认证科技（北京）有限公司、四川长虹电子控股集团有限公司、阿里巴巴(中国)有限公司、上海移柯通信技术股份有限公司。

本文件主要起草人：刘献伦、王平、袁琦、刘为华、李鑫、康亮、董雾、徐晓娜、王韬、李汝鑫、冯志芳、王江胜、林冠辰、王宇晓、李俊、张宏星、张一驰、黄天宁、王佳、黄德俊、刘俊、沈峰、杨超。

引　言

随着《中华人民共和国网络安全法》、《中华人民共和国密码法》、《中华人民共和国数据安全法》等相关法律的颁布实施，国内对信息安全问题越来越重视。

同时，随着 5G 的发展，国内物联网终端设备数量爆发式增长（截至 2021 年 8 月份，中国三大基础电信运营商发展蜂窝物联网终端用户已达 13 亿）。在垂直行业领域，物联网技术的推广和应用提高了行业生产的效率，然而信息安全问题成为是行业客户重点关注的问题，尤为关注的是物联网通信过程中数据被篡改、信息被泄露和身份被冒用等问题。

物联网模组是物联网终端设备传输数据的重要实现方式。虽然在目前各类蜂窝通信协议中已采用了多种密码技术来保证通信网络层安全，但在金融、电信、交通、能源、水利等关键信息基础设施行业应用中，网络层采用的信息安全保护措施还不足以满足行业客户对数据安全的要求。针对行业客户对信息安全合规性和对数据安全增强安保护的需求，需要在应用层采用更安全的密码技术对数据在存储、传输等环节进行机密性、真实性和完整性保护。

物联网设备自身要集成密码安全芯片、具备一定安全能力，需要对物联网设备进行硬件改造，对相应增加研发周期和成本。在不改变目前通信网络及物联网模组的使用方式下，如何给行业客户提供更多可选的数据安全保护能力、减少产品碎片化，优化行业物联网系统使用密码产品的周期和成本就显得尤为重要。为加快物联网设备集成安全芯片能力，降低改造难度，将安全芯片集成到物联网模组中，通过物联网模组为物联网设备提供安全服务成为较优的方式。所以，集成安全芯片功能的物联网模组方案被提出并推广使用。本文件就此类方案进行统一规范，便于更好的推动行业应用。

集成独立安全芯片的行业物联网模组安全技术要求

1 范围

本文件规定了集成独立安全芯片的行业物联网模组安全技术要求，主要包含集成独立安全芯片的物联网模组安全架构、物联网模组基本功能要求、物联网模组传输层安全协议技术要求、物联网模组安全技术要求、物联网模组安全AT指令技术要求和物联网模组可靠性要求等。

本文件适用于集成独立安全芯片的面向行业的物联网模组（如SE和物联网卡形态等）。个别条款不适用于特殊行业、专业应用，其他类似模组也可参考使用。

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 25069—2022 信息安全技术 术语

GB/T 35291—2017 智能密码钥匙应用接口规范

GM/T 0008—2012 安全芯片密码检测准则

ISO/IEC 15408 信息技术安全评估准则（Common Criteria for Information Technology Security Evaluation）

GSMA FS.48 基于GBA的证书配置指南（Guidelines for GBA Based Certificate Provisioning）

3GPP TS 27.007 终端设备AT指令集 AT command set for user equipment(UE)

3GPP TS 33.220 通用认证架构(GAA)；通用引导架构(GBA)（Generic Authentication Architecture (GAA)；Generic Bootstrapping Architecture (GBA)）

3GPP TS 33.535 5G系统基于3GPP凭据的应用层认证和密钥管理（Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)）

3 术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

物联网模组 IOT modules

集成了基带芯片、存储器、功放器件，并提供标准的接口功能，能使各种物联网设备实现蜂窝通信的通信模组。

3.2

集成独立安全芯片的物联网模组 IoT modules integrated security chips function

集成独立安全芯片，且具备一定安全能力并可对使用模组的物联网设备提供安全服务的物联网安全模组。

3.3

独立安全芯片 security chip

含有密码算法、真随机数生成等安全功能，能独立实现密钥管理机制的集成电路。
[来源：GB/T 25069-2022 有修订]

3.4

物联网安全平台 IOT security platform

具有对物联网设备身份认证、数据加解密、安全通信等安全能力的物联网服务平台。

3.5

安全服务组件 security service components

运行在物联网模组系统内，实现一定安全功能并提供安全相关的服务接口供其他程序调用的软件程序。

4 缩略语

下列缩略语适用于本文件。
5G：第五代移动通信技术（5th Generation Mobile Communication Technology）
AKMA：应用层认证和密钥管理（Authentication and Key Management for Applications）
AP：应用处理器（Application Processor）
API：应用编程接口（Application Programming Interface）
APN：接入点（Access Point Name）
AT：连接与通信指令（ATtention command）
CoAP：受限应用协议（Constrained Application Protocol）
COS：片内操作系统（Chip Operating System）
CPU：中央处理器（Central Processing Unit）
DTLS：数据包传输层安全性协议（Datagram Transport Layer Security）
GBA：通用引导架构（Generic Bootstrapping Architecture）
HTTP：超文本传输安全协议（Hyper Text Transfer Protocol）
I2C：集成电路总线（Inter-Integrated Circuit）
IP：网际协议（Internet Protocol）
LWM2M：轻量级机器对机器（lightweight Machine to Machine）
MCU：微控制器（Microcontroller Unit）
MQTT：消息队列遥测传输（Message Queuing Telemetry Transport）
NB-IoT：窄带蜂窝物联网（Narrow Band-Internet of Things）
PIN：个人标识码（Personal identification number）
QoS：服务质量（Quality of Service）
SE：安全芯片（Security Chip）

SIP：系统级封装（System In a Package）
SoC：系统级芯片（System on Chip）
SPI：串行外设接口（Serial Peripheral Interface）
TCP：传输控制协议（Transmission Control Protocol）
TEE：可信执行环境（Trusted Execution Environment）
TLCP：传输层密码协议（Transport Layer Cryptography Protocol）
TLS：传输层安全协议（Transport Layer Security）
UART：通用异步收发传输器（Universal Asynchronous Receiver/Transmitter）
UDP：用户数据报协议（User Datagram Protocol）
USB：通用串行总线（Universal Serial Bus）

5 概述

5.1 独立安全芯片

独立安全芯片是含有密码算法、真随机数生成等安全功能，能实现密钥管理机制的集成电路。独立安全芯片如图1所示。

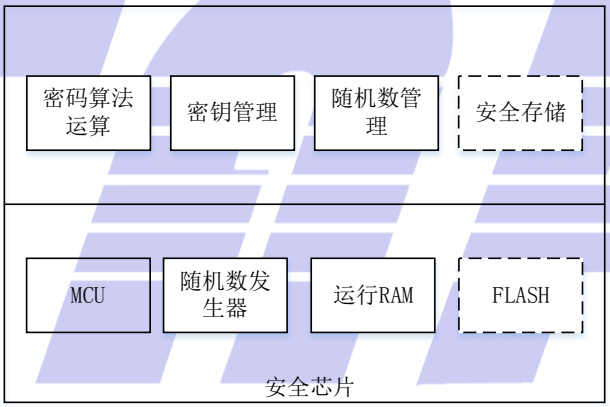

图1 独立安全芯片框图

安全芯片提供的功能主要包括：

a) 随机数生成：要具有物理噪声源生成真随机数的功能；
b) 密码算法运算：包括分组密码算法、公钥密码算法、杂凑密码算法和序列密码算法中的一种或多种；
c) 密钥管理：对密钥的生成、存储、使用、更新、导入、导出、销毁等环节有安全管理机制；
d) 敏感信息保护：对需要存储的敏感信息要有保密存储、访问控制等保护机制；
e) 安全访问接口：包括访问芯片的物理和逻辑接口，并且物理和逻辑接口要有相应的安全技术措施。

根据安全芯片要达到安全等级不同，安全芯片自身还会有自检、审计、密钥及敏感信息自毁、计时攻击防护、能量分析攻击防护、电磁分析攻击防护等功能。

注：独立安全芯片COS的最小功能集不限定Native Card或Java Card。

5.2 集成独立安全芯片的物联网模组安全架构

安全架构图主要有下列两种，集成独立安全芯片的物联网模组安全架构一般有下面两类常见方式：

a) 集成独立安全芯片功能的物联网模组是在物联网模组上集成独立安全芯片，独立安全芯片通过通用的硬件通信接口与物联网模组的主芯片连接，安全架构如图2所示。

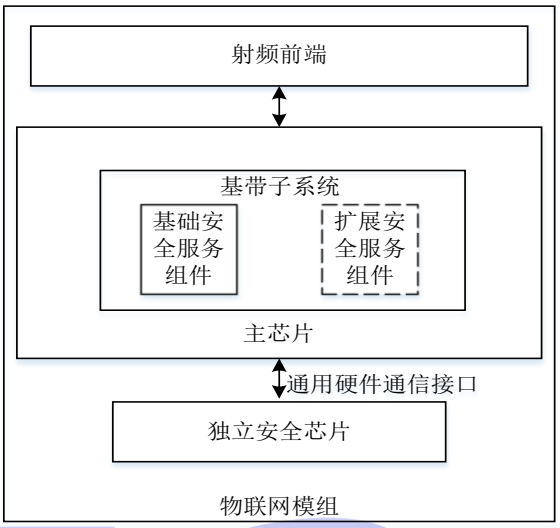

图2　集成独立安全芯片的物联网模组安全架构图

b) 在主芯片内有TEE的情况下，独立安全芯片的安全功能可通过TEE子系统提供。服务组件可通过TEE子系统调用独立安全芯片的能力，安全架构如图3所示。

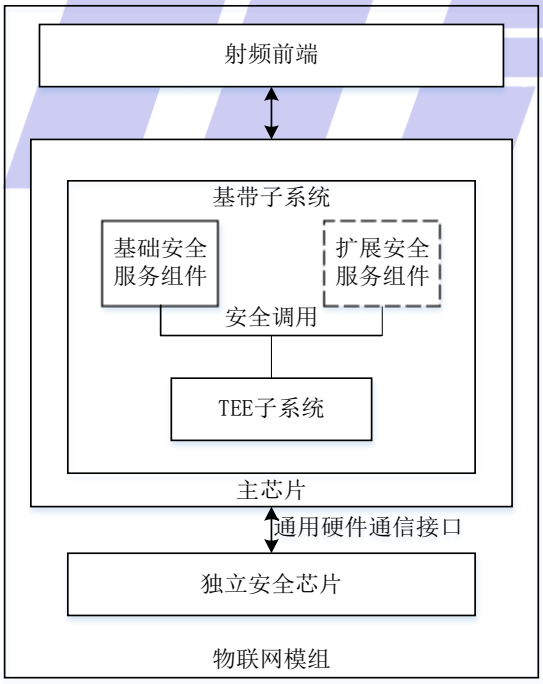

图3　通过TEE调用独立安全芯片安全的物联网模组安全架构图

5.3　集成独立安全芯片的物联网模组安全服务组件

物联网模组的MCU/AP运行操作系统，需在操作系统内以软件方式集成安全服务组件。一般安全服务组件包括基础安全服务组件和扩展安全服务组件两类。

a) 基础安全服务组件主要包括：
   1） 安全芯片硬件接口驱动程序，如 USB/SPI/I2C/ISO7816 等接口的驱动程序；
   2） 安全服务接口，该接口宜符合 GB/T 35291-2017 要求。
b) 扩展安全服务组件，是实现安全协议的程序，扩展安全服务组件通过调用基础服务组件的接口与安全芯片交互以实现安全功能。可根据不同的物联网模组选择集成不同的扩展安全服务组件，如 TLS/TCLP/CoAP/MQTT/DTLS/LWM2M 等协议组件。

基础安全服务组件一般是必须被集成的使用；扩展安全服务组件自主选择，一般为了便于使用安全功能，推荐被集成使用。

5.4 集成独立安全芯片的物联网模组架构图

集成独立安全芯片的物联网模组主要包含模组基本安全功能、模组安全协议、模组安全AT指令、模组安全和可靠性等要求，如图4所示。

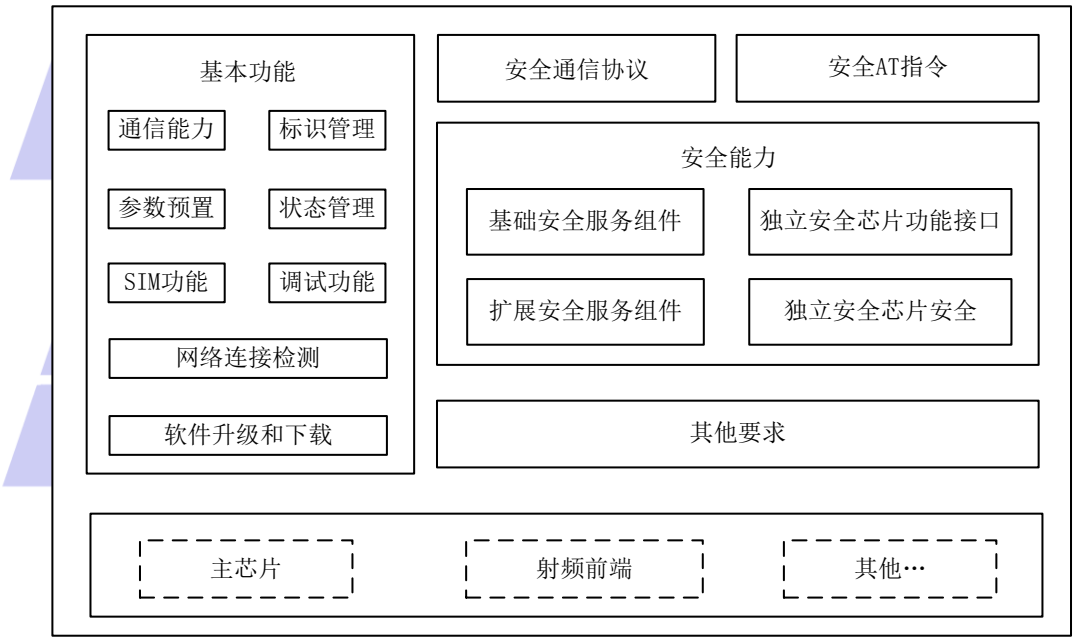

图4 集成独立安全芯片的物联网模组架构图

6 物联网模组基本功能要求

6.1 通信能力要求

根据业务需求，物联网模组应具有一种或多种蜂窝网络模式下接入和网络能力。相应制式应满足国内相关国家标准、行业标准的要求。

6.2 模组标识管理

物联网模组应具备模组标识，以便平台对模组和终端设备进行管理。

6.3 模组状态管理

物联网模组应具备模组状态管理功能，即具备模组状态信息的检测和上报能力。

6.4 模组参数预置管理

物联网模组应预置蜂窝网络承载接入参数，如APN、端口号等。

6.5 SIM卡功能要求

物联网模组应至少支持SIM、USIM、e-SIM三种卡中的一种。

6.6 调试功能要求

物联网模组应支持开发调试功能。

6.7 网络连接检测能力要求

物联网模组可支持模拟发包、心跳报文发送、QoS指标检测及上报的网络连接检测功能。

6.8 软件下载与升级管理

物联网模组应为集成该模组的终端提供软件下载和升级的通信通道，应支持通过本地升级或远程升级的方式进行自身软件下载与升级。

7 物联网模组传输层安全协议技术要求

7.1 物联网模组传输层安全协议概述

集成独立安全芯片的物联网模组，可选择不同的传输层安全协议连接物联网安全平台，以实现端到云的安全通信。如图5所示。

图5 物联网设备到物联网安全平台通信

7.2 物联网模组传输层安全协议要求

物联网模组传输层安全协议安全要求具体包括：

a) 传输层安全协议应调用安全芯片提供的安全能力，如在身份认证、协议握手、数据传输等过程调用安全芯片提供的安全能力；

b) 对支持传输层 TCP 协议的物联网模组，宜实现 TLS/TLCP 等安全协议（TLS 协议应使用 1.2 及以上版本，TLCP 协议应使用 1.1 及以上版本）。基于 TCP 协议的应用层协议（如 HTTP，MQTT 等）应使用支持的安全协议；

c） 对支持传输层 UDP 协议的物联网模组，宜实现 DTLS 安全协议（DTLS 协议应使用 1.2 及以上版本）。基于 UDP 协议的应用层协议（如 CoAP、LwM2M 等）应使用支持的安全协议。

8 物联网模组安全技术要求

8.1 独立安全芯片安全要求

安全芯片需符合下列要求：

a） 安全芯片硬件接口应支持 UART、SPI、USB、I2C、ISO7816 等中的一种或多种；

b） 安全芯片应使用安全的密码算法，应支持符合国家或行业标准要求的密码算法，具体包括：

1） 应支持常用的对称密码算法的一种或多种，如 SM4、AES 等密码算法；

2） 应支持常用的非对称密码算法一种或多种，如 SM2、RSA-2048、SM9 等密码算法；

3） 应支持常用的摘要密码算法一种或多种，如 SM3、SHA-256 等密码算法；

4） 应支持多种密码算法运算模式一种或多种，如 CBC、OFB、CBC-MAC、CTR、GCM 等运算模式。

c） 安全芯片应支持密码运算所需密钥的安全管理，包括密钥的导入、生成、存储或更新功能；应支持多组存储容器，每组可存储一对签名公私钥对、加密公私钥对和会话密钥等；

d） 安全芯片应支持证书安全管理，包括证书文件的导入、存储或更新功能；

e） 独立安全芯片应至少符合 GM/T 0008-2012 安全等级二级、GB/T 22186 的 EAL4+要求或 ISO/IEC 15408 的 EAL4+要求。

8.2 安全芯片功能通信接口安全技术要求

集成独立安全芯片的物联网模组为物联网设备提供安全芯片能力的通信接口一般有三类。如图6所示。

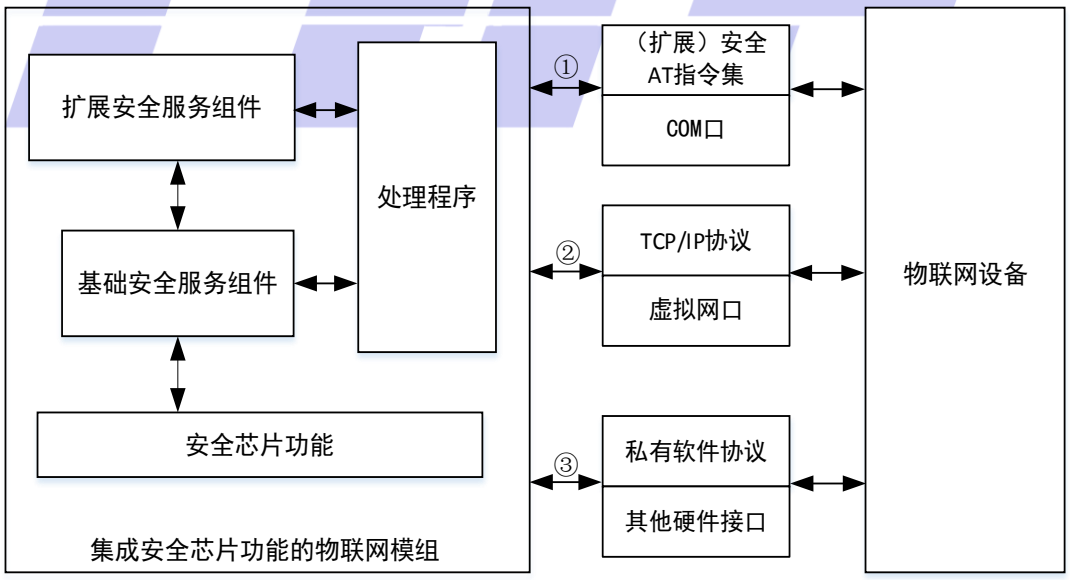

图 6 物联网模组和设备的通信方式示意图

针对三类通信方式，需符合下列要求：

a） 物联网模组应至少支持安全 AT 指令集通信方式，即第①类方式，扩展的安全 AT 指令集参考附录 A；

注 1：第①类通信方式通过 COM 口通信，该 COM 口支持 AT 指令。该方式下，根据 AT 指令规范，物联网模组扩展出和安全芯片能力相关的安全 AT 指令集。扩展安全 AT 指令集一般包含两部分，一部分是配置 AT 指令集，另一部分是安全能力 AT 指令集。参考附录 A。

b) 物联网模组可根据自身配置能力，宜支持虚拟网口通信方式，即第②类方式。

注 2：第②类通信方式通过虚拟网口通信，该网口支持物联网设备直接建立 TCP/IP 连接。该方式下，安全功能可选择由物联网模组内的扩展服务组件来实现。

c) 物联网模组可根据自身配置能力，可支持其他通用硬件接口通信方式，即第③类方式：

注 3：第③类通信方式通过其他的硬件接口通信，如 USB 接口等。该方式下，由物联网模组实现私有软件协议，物联网设备通过物联网模组提供的软件 API 接口的方式调用安全芯片功能。

注4：使用第②类或第③通信方式时，需要物联网模组至少实现扩展安全AT指令集中的配置指令。在使用时，需先调用配置指令进行相关配置。

8.3 基础安全服务组件安全要求

基础安全服务组件通过驱动程序和安全芯片通信，应支持不同的芯片形态和不同的硬件接口，同时提供可供扩展服务组件调用的API，API的定义宜支持GB/T 35291-2017要求。

基础安全服务组件应至少适用于Windows、Linux、Android等多种操作系统的一种。

8.4 扩展安全服务组件安全要求

扩展安全服务组件需符合下列要求。

a) 扩展安全服务组件宜符合 GB/T 35291-2017 要求；

b) 针对支持 TCP/IP 协议的物联网模组，如 LTE/5G 物联网模组，应符合 7.2 b 项要求；

c) 针对仅支持 UDP 协议的物联网模组，如窄带物联网（NB-IoT）模组，应符合 7.2 c 项要求；

d) 应至少适用于 Windows、Linux、Android 等协议栈完整的操作系统中的一种。

9 物联网模组安全 AT 指令技术要求

9.1 物联网模组安全 AT 指令概述

安全AT指令是物联网模组供物联网设备调用安全功能的方式之一，主要包含平台登录认证方式设置指令、TLS相关指令、PIN码相关指令和密码算法相关指令、证书相关指令和随机数相关指令等。这些AT指令可根据需要进行扩展。

9.2 物联网模组安全 AT 指令要求

物联网模组AT指令应符合3GPP TS 27.007，调用方式可参见8.2章节。

物联网模组安全AT指令参考附录A所示。

10 其他要求

10.1 温度要求

物联网模组应满足以下环境温度范围内正常工作及存储要求：

a) 各型模组应能在-40° C～85° C 的范围内存储；

b) 用于消费类应用的模组应能在-20° C～60° C 范围内正常工作；

c) 用于工业类应用的模组应能在-40° C～85° C 范围内正常工作；

d) 用于车规类应用的模组应能在-40°C～85°C范围内正常工作，可在85°C～125°C范围工作。

10.2 其他可靠性要求

物联网通用模组应符合集成该模组的终端所在行业的国家标准规定的可靠性要求。

附 录 A
（资料性）
物联网模组安全AT指令

A.1 平台登录认证方式设置 AT 指令

A.1.1 平台登录认证方式设置AT指令列表

平台登录认证方式设置AT指令见表A.1。

表A.1 平台登录认证方式设置AT指令

指令名称	指令格式	功能说明
平台登录认证方式设置	AT+SETAUTH	用于配置设备接入物联网平台采用的身份认证方式

A.1.2 AT+SETAUTH

平台登录认证方式设置指令AT+SETAUTH具体见表A.2。

表A.2 AT+SETAUTH指令

名称	描述	返回值
设置指令	AT+SETAUTH=<Auth type>	成功：OK 失败：+CME ERROR：<err>
查询指令	AT+SETAUTH?	成功： + SETAUTH:<x>（当前设置值） OK
测试指令	AT+SETAUTH=?	成功： + SETAUTH: (0,1,2) OK
功能说明	用于配置设备接入物联网平台采用的身份认证方式	
参数说明	<Auth type> 整形（备注：可扩展） 0 - NON （默认无设置） 1 - ID 认证 2 - 数字证书 认证	
设置指令举例	AT+SETAUTH=1	成功： OK

A.2 TLS 相关 AT 指令

A.2.1 TLS相关AT指令列表

TLS相关AT指令具体见表A.3。

表A.3　TLS相关AT指令

指令名称	指令格式	功能说明
TLS 相关 AT 指令	AT+TLSCFG	用于配置在物联网平台分配的设备 ID
	AT+TLSOPEN	用于建立与物联网平台安全接入网关的安全连接
	AT+TLSSTAT	用于查询与物联网平台安全接入网关的安全连接状态
	AT+TLSCLOSE	用于断开与物联网平台安全接入网关的安全连接
	AT+TLSVERSION	用于获取 TLS 组件版本信息

A.2.2　AT+TLSCFG

TLS配置ID指令AT+TLSCFG 见表A.4。

表A.4 AT+TLSCFG指令

名称	描述	返回值
设置指令	AT+ TLSCFG =<dev id>	成功：OK 失败：+CME ERROR：<err>
查询指令	AT+ TLSCFG?	成功： + TLSCFG：xxxxxxxx（当前设备ID值） OK
测试指令	AT+ TLSCFG =?	成功： + TLSCFG:(List of <dev id>) OK
功能说明	用于配置在物联网平台分配的设备 ID	—
参数说明	<dev id> 字符串 不大于32字节 物联网平台注册成功后分配的设备唯一 ID 号	—
设置指令举例	AT+TLSCFG=100439710013111111	成功： OK

A.2.3　AT+TLSOPEN

建立TLS安全连接指令AT+TLSOPEN见表A.5。

表A.5　AT+TLSOPEN指令

名称	描述	返回值
查询指令	AT+TLSOPEN?	成功： + TLSOPEN: 1（连接）或0（断开） OK
测试指令	AT+TLSOPEN=?	成功： + TLSOPEN: OK

表A.5　AT+TLSOPEN指令（续）

名称	描述	返回值
功能说明	用于建立与物联网平台安全接入网关的安全连接	—
查询指令	AT+TLSOPEN?	成功： + TLSOPEN: 1（连接）或0（断开） OK
测试指令	AT+TLSOPEN=?	成功： + TLSOPEN: OK
功能说明	用于建立与物联网平台安全接入网关的安全连接	—
参数说明	无	—
设置指令举例	AT+TLSOPEN	成功： OK

A.2.4　AT+TLSCLOSE

断开TLS安全连接指令AT+TLSCLOSE见表A.6。

表A.6　AT+TLSCLOSE指令

名称	描述	返回值
设置指令	AT+TLSCLOSE	成功：OK 失败：+CME ERROR：<err>
查询指令	AT+TLSCLOSE?	成功： + TLSCLOSE:1（断开）或0（连接） OK
测试指令	AT+TLSCLOSE=?	成功： + TLSCLOSE: OK
功能说明	用于断开与物联网平台安全接入网关的安全连接	—
参数说明	无	—
设置指令举例	AT+TLSCLOSE	成功： OK

A.2.5　AT+TLSSTAT

获取TLS连接状态指令AT+TLSSTAT见表A.7。

表A.7　AT+TLSSTAT指令

名称	描述	返回值
获取状态指令	AT+TLSSTAT	成功：OK 失败：+CME ERROR：<err>

表A.7　AT+TLSSTAT指令（续）

名称	描述	返回值
查询指令	AT+TLSSTAT?	成功： + TLSSTAT: 1（连接）或0（断开） OK
测试指令	AT+TLSSTAT=?	成功： + TLSSTAT: OK
功能说明	用于查询与物联网平台安全接入网关的安全连接状态	—
参数说明	无	—
获取状态指令举例	AT+TLSSTAT	成功： OK

A.2.6　AT+TLSVERSION

获取TLS组件版本指令AT+TLSVERSION见表A.8。

表A.8　AT+TLSVERSION指令

名称	描述	返回值
查询指令	AT+TLSVERSION	成功： + TLSVERSION: <version info> OK 失败：+CME ERROR：<err>
测试指令	AT+TLSVERSION=?	成功： + TLSVERSION:<TLS版本号> OK
功能说明	用于获取 TLS 组件版本信息	—
参数说明	<version info> 字符串，不大于64字节 描述 TLS 组件的版本信息	—
查询指令举例	AT+TLSVERSION	成功： + TLSVERSION: v1.0 OK

A.3　PIN 码相关 AT 指令

A.3.1　PIN码相关AT指令列表

PIN码相关AT指令具体见表A.9。

表A.9 PIN码相关AT指令

指令名称	指令格式	功能说明
PIN 码相关 AT 指令	AT+ChangePIN	用来修改管理员 PIN 码和用户 PIN 码，如果 PIN 码错误，会返回 PIN 码重试次数，当次数为 0 时表示 PIN 码已锁死
	AT+VerifyPIN	用来校验 PIN 码。校验成功后，会获取相应的权限，如果 PIN 码错误，会返回 PIN 码重试次数，当次数为 0 时表示 PIN 码已锁死

A.3.2 AT+ChangePIN

PIN码修改AT指令AT+ChangePIN见表A.10。

表A.10 AT+ChangePIN指令

名称	描述	返回值
设置指令	AT+ChangePIN=<ulPINType>,<szOldPIN>, <szNewPIN>	成功：OK 失败：+CME ERROR：RetryCount < RetryCount >
测试指令	AT+ ChangePIN =?	成功： + ChangePIN: (0,1), (List of <szOldPIN>), (List of <szNewPIN>) OK
功能说明	用来修改管理员 PIN 码和用户 PIN 码，如果 PIN 码错误，会返回 PIN 码重试次数，当次数为 0 时表示 PIN 码已锁死	—
参数说明	<ulPINType> 无符号整形 0 - 管理员PIN 1 - 用户PIN <szOldPIN> 字符串，6个字节 输入原 PIN 码值 <szNewPIN> 字符串，6个字节 输入新 PIN 码值	—
设置指令举例	AT+ChangePIN=1,111111,123456	成功： OK

A.3.3 AT+VerifyPIN

PIN码验证AT指令AT+VerifyPIN见表A.11。

表A.11　AT+VerifyPIN指令

名称	描述	返回值
验证指令	AT+ VerifyPIN=<ulPINType>,<szPIN>	成功：OK 失败：+CME ERROR：RetryCount < RetryCount >
测试指令	AT+ VerifyPIN=?	成功： + VerifyPIN: (0,1),(List of PIN) OK
功能说明	用来校验 PIN 码。校验成功后，会获取相应的权限，如果 PIN 码错误，会返回 PIN 码重试次数，当次数为 0 时表示 PIN 码已锁死	—
参数说明	<ulPINType> 无符号整形 0 - 管理员PIN 1 - 用户PIN <szPIN> 字符串，6个字节 输入的 PIN 码值	—
验证指令举例	AT+ VerifyPIN=1,123456	成功： OK

A.4　非对称加解密算法相关 AT 指令

A.4.1　非对称加解密算法相关AT指令列表

非对称加解密算法相关AT指令列表具体见表A.12。

表A.12　非对称加解密相关AT指令

指令名称	指令格式	功能说明
非对称加解密算法相关 AT 指令	AT+GenECCKeyPair	生成 ECC 签名密钥对并输出公钥
	AT+ImportECCKeyPairEx	导入 ECC 密钥对
	AT+ECCSignData	ECC 签名
	AT+ECCVerify	ECC 验签
	AT+ECCEncrypt	ECC 公钥加密
	AT+ECCDecrypt	ECC 私钥解密

A.4.2　AT+GenECCKeyPair

AT指令AT+GenECCKeyPair见表A.13。

表A.13 AT+GenECCKeyPair指令

名称	描述	返回值
设置指令	AT+GenECCKeyPair=<ulAlgId>	成功： OK 失败：+CME ERROR：<err>
测试指令	AT+GenECCKeyPair=?	成功： + GenECCKeyPair： Xxxxxx(生成的公钥), OK
功能说明	生成 ECC 签名密钥对并输出公钥	—
参数说明	ulAlgId 无符号整形　　算法标识，只支持SGD_SM2_1算法，取值为0x00020200(十六进制)	—
设置指令举例	AT+GenECCKeyPair=0x00020200	成功： OK

A.4.3 AT+ImportECCKeyPairEx

AT指令AT+ImportECCKeyPairEx见表A.14。

表A.14 AT+ImportECCKeyPairEx指令

名称	描述	返回值
设置指令	AT+ImportECCKeyPairEx=<bSignFlag>,<ulPubLen>,<pbPubKey><ulPriLen>,<pbPriKey>	成功： OK 失败：+CME ERROR：<err>
测试指令	AT+ ImportECCKeyPairEx =?	成功： + ImportECCKeyPair： (0,1), (<ulPubLen>), (<pbPubKey >), (<ulPriLen>), (<pbPriKey >) OK
功能说明	导入 ECC 密钥对	—
参数说明	<bSignFlag> 布尔类型 0 - 表示加密证书 1 - 表示签名证书 <ulPubLen> 无符号整形 输入公钥长度 <pbPubKey> 二进制字节流 输入公钥数据 <ulPriLen> 无符号整形 输入私钥长度 <pbPriKey> 二进制字节流 输入私钥数据	—
设置指令举例	AT+ ImportECCKeyPairEx =加密密钥对的数据	成功： OK

A.4.4 AT+ECCSignData

AT指令AT+ECCSignData见表A.15。

表A.15 AT+ECCSignData指令

名称	描述	返回值
设置指令	AT+ECCSignData=<ulDataLen>,<pbData>	成功： +ECCSignData: <SignLen> <SignValue> OK 失败：+CME ERROR：<err>
测试指令	AT+ECCSignData=?	成功： + ECCSignData： (<ulDataLen>), (< pbData >) OK
功能说明	ECC 签名	—
参数说明	<ulDataLen> 无符号整形 待签名的数据长度，必须小于密钥模长 <pbData> 二进制字节流 待签名的数据 <SignLen> 无符号整形 返回签名数据长度 <SignValue> 二进制字节流 返回签名数据	—
设置指令举例	AT+ECCSignData=长度值，二进制字节流	成功： 返回签名数据长度， 返回签名数据 OK

A.4.5 AT+ECCVerify

AT指令AT+ECCVerify见表A.16。

表A.16 AT+ECCVerify指令

名称	描述	返回值
设置指令	AT+ECCVerify=<pECCPubKeyBlob>,<ulDataLen>,<pbData>,<ulSignLen>,<pSignature>	成功：OK 失败：+CME ERROR：<err>
测试指令	AT+ECCVerify=?	成功： + ECCVerify： (<pECCPubKeyBlob>), (<ulDataLen>), (<pbData>), (<ulSignLen>), (<pSignature>) OK

表A.16 AT+ECCVerify指令（续）

名称	描述	返回值
功能说明	ECC 验签	—
参数说明	<pECCPubKeyBlob> 二进制字节流 结构化公钥数据 <ulDataLen> 无符号整形 待验证签名数据长度 <pbData> 二进制字节流 待验证签名的数据 <ulSignLen> 无符号整形 待验证签名值长度 <pSignature> 二进制字节流 待验证签名值	—
设置指令举例	AT+ECCVerify=结构化公钥数据，待验证签名数据长度，待验证签名的数据，待验证签名值长度，待验证签名值	成功： OK

A.4.6 AT+ECCEncrypt

AT指令AT+ECCEncrypt见表A.17。

表A.17 AT+ECCEncrypt指令

名称	描述	返回值
设置指令	AT+ECCEncrypt=<bSignFlag>,<ulPlainTextLen>,<pbPlainText>	成功： + ECCEncrypt: <EncDataLen> <EncData> OK 失败： +CME ERROR：<err>
测试指令	AT+ECCEncrypt=?	成功： +ECCEncrypt: (0,1) ,(< ulPlainTextLen>) ,(<pbPlainText>) OK
功能说明	ECC 公钥加密	—
参数说明	<bSignFlag> 布尔类型 0 －表示加密证书公钥加密 1 －表示使用签名证书公钥加密 <ulPlainTextLen> 无符号整形 明文数据长度 <pbPlainText> 二进制字节流 明文数据 <EncDataLen>无符号整形 返回密文数据长度 <EncData> 二进制字节流 返回密文数据，类型为ECCCIPHERBLOB	—

表A.17 AT+ECCEncrypt指令（续）

名称	描述	返回值
设置指令举例	AT+ECCEncrypt=公钥类型,明文数据长度,明文数据	成功： + ECCEncrypt: 密文数据长度， 类型为ECCCIPHERBLOB的二进制字节流 OK

A.4.7 AT+ECCDecrypt

AT指令AT+ECCDecrypt见表A.18。

表A.18 AT+ECCDecrypt指令

名称	描述	返回值
设置指令	AT+ECCDecrypt=<bSignFlag>,<pCipherTextLen>,<pCipherText>	成功： + ECCDecrypt: <DecDataLen> <DecData> OK 失败：+CME ERROR：<err>
测试指令	AT+ECCDecrypt=?	成功： + ECCDecrypt: (0,1), (<pCipherTextLen>) , (<pCipherText>) OK
功能说明	ECC 私钥解密	—
参数说明	<bSignFlag> 布尔类型 0 －表示加密证书公钥加密 1 －表示使用签名证书公钥加密 <pCipherTextLen> 无符号整形 密文数据长度 <pCipherText> 二进制字节流 密文数据，类型为ECCCIPHERBLOB <DecDataLen> 无符号整形 返回明文数据长度 <DecData> 二进制字节流 返回明文数据	—
设置指令举例	AT+ECCDecrypt=公钥类型,密文数据长度,密文数据	成功： + ECCDecrypt: 明文数据长度 明文数据 OK

A.5 对称加解密算法相关 AT 指令

A.5.1 对称加解密算法相关AT指令列表

对称加解密算法相关AT指令具体见表A.19。

表A.19 对称加解密算法相关AT指令

指令名称	指令格式	功能说明
对称加解密算法相关 AT 指令	AT+EncryptInit	加密初始化，设置数据加密的算法相关参数
	AT+Encrypt	单组数据加密。在使用 AT+ Encrypt 之前必须先使用 AT+ EncryptInit 初始化
	AT+DecryptInit	解密初始化，设置数据解密的算法相关参数
	AT+Decrypt	单组数据解密操作。在调用 AT+ Decrypt 之前必须先执行 AT+ DecryptInit

A.5.2 AT+ EncryptInit

AT指令AT+ EncryptInit见表A.20。

表A.20 AT+ EncryptInit指令

名称	描述	返回值
设置指令	AT+ EncryptInit=<EncryptParamLen>,<EncryptParam>	成功： + EncryptInit: OK 失败：+CME ERROR：<err>
测试指令	AT+ EncryptInit=?	成功： + EncryptInit: (<EncryptParamLen>), (<EncryptParam>) OK
功能说明	加密初始化，设置数据加密的算法相关参数	—
参数说明	分组密码算法相关参数: <EncryptParamLen> 无符号整形 对称加密参数长度 <EncryptParam> 二进制字节流 对称加密参数数据，类型为BLOCKCIPHERPARAM	—
设置指令举例	AT+ EncryptInit=参数长度，参数数据	成功： + EncryptInit: OK

A.5.3 AT+ Encrypt

AT指令AT+ Encrypt见表A.21。

表A.21 AT+ Encrypt指令

名称	描述	返回值
设置指令	AT+ Encrypt=<ulDataLen>,<pbData>	成功： + Encrypt： <pulEncryptedLen> <pbEncryptedData> OK 失败：+CME ERROR：<err>
测试指令	AT+ Encrypt=?	成功： + Encrypt： (<ulDataLen>), (<pbData>) OK
功能说明	单组数据加密。在使用 AT+ Encrypt 之前必须先使用 AT+ EncryptInit 初始化	—
参数说明	<ulDataLen> 无符号整形 待加密的明文数据长度 <pbData> 二进制字节流 待加密的明文数据 <pulEncryptedLen> 无符号整形 返回加密的数据长度 <pbEncryptedData> 二进制字节流 返回加密的数据	—
设置指令举例	AT+ Encrypt=待加密的明文数据长度,待加密的明文数据	成功： + Encrypt： 返回加密的数据长度 返回加密的数据 OK

A.5.4 AT+ DecryptInit

AT指令AT+ DecryptInit见表A.22。

表A.22 AT+ DecryptInit指令

名称	描述	返回值
设置指令	AT+ DecryptInit=<DecryptParamLen>,<DecryptParam>	成功： + DecryptInit： OK 失败：+CME ERROR：<err>

表A.22 AT+ DecryptInit指令（续）

名称	描述	返回值
测试指令	AT+ DecryptInit=?	成功： + DecryptInit： (<DecryptParamLen>), (<DecryptParam>) OK
功能说明	解密初始化，设置数据解密的算法相关参数	—
参数说明	< DecryptParamLen > 无符号整形 参数数据长度 <DecryptParam> 二进制字节流 参数数据，类型为BLOCKCIPHERPARAM	—
设置指令举例	AT+DecryptInit=参数长度，参数数据	成功： + DecryptInit： OK

A.5.5 AT+Decrypt

AT指令AT+Decrypt见表A.23。

表A.23 AT+Decrypt指令

名称	描述	返回值
设置指令	AT+Decrypt=<ulEncryptedLen>,<pbEncryptedData>	成功： + Decrypt： <pulDataLen> <pbData> OK 失败：+CME ERROR：<err>
测试指令	AT+ Decrypt=?	成功： + Decrypt： (<ulEncryptedLen>), (<pbEncryptedData>) OK
功能说明	单组数据解密操作。在调用AT+ Decrypt之前必须先执行AT+ DecryptInit	—
参数说明	<ulEncryptedLen> 无符号整形 待解密数据长度 <pbEncryptedData> 二进制字节流 待解密数据 <pulDataLen> 无符号整形 返回明文数据长度 <pbData> 二进制字节流 返回明文数据	—
设置指令举例	AT+ Decrypt=待解密数据长度,待解密数据	成功： + Decrypt： 明文数据长度 明文数据 OK

A.6 杂凑算法相关 AT 指令

A.6.1 杂凑算法相关AT指令列表

杂凑算法相关AT指令具体见表A.24。

表A.24 杂凑算法相关AT指令

指令名称	指令格式	功能说明
杂凑算法相关 AT 指令	AT+DigestInit	密码杂凑初始化
	AT+ Digest	单组数据密码杂凑计算。调用 AT+ Digest 之前必须执行 AT+ DigestInit 初始化

A.6.2 AT+DigestInit

AT指令AT+DigestInit见表A.25。

表A.25 AT+DigestInit指令

名称	描述	返回值
设置指令	AT+DigestInit=<ulAlgID>,<pPubKeyLen>,<pPubKey>, <ulIDLen>,<pucID>	成功： + DigestInit: OK 失败：+CME ERROR：<err>
测试指令	AT+ DigestInit=?	成功： + DigestInit: (<ulAlgID>), (<pPubKeyLen>), (<pPubKey>), (<ulIDLen>), (<pucID>) OK
功能说明	密码杂凑初始化	—
参数说明	<ulAlgID> 无符号整形 密码杂凑算法标识 <pPubKeyLen> 无符号整形 签名者公钥数据长度 <pPubKey> 结构化数据 签名者公钥数据，类型为ECCPUBLICKEYBLOB，当ulAlgID为SGD_SM3时有效 <ulIDLen> 无符号整形 签名者ID的长度，当ulAlgID为SGD_SM3时有效 <pucID> 二进制字节流 签名者 ID	—
设置指令举例	AT+ DigestInit=密码杂凑算法标识,签名者公钥长度,签名者公钥,签名者ID的长度,签名者ID	成功： + DigestInit: OK

A.6.3 AT+ Digest

AT指令AT+ Digest见表A.26。

表A.26 AT+ Digest指令

名称	描述	返回值
设置指令	AT+ Digest=<ulDataLen>,<pbData>	成功： + Digest: <pulHashLen> <pbHashData> OK 失败：+CME ERROR：<err>
测试指令	AT+ Digest=?	成功： + Digest: (<ulDataLen>), (<pbData>) OK
功能说明	单组数据密码杂凑计算。调用AT+ Digest之前必须执行AT+ DigestInit初始化。	—
参数说明	<ulDataLen> 无符号整形 消息数据长度 <pbData> 二进制字节流 消息数据 <pulHashLen> 无符号整形 返回消息摘要数据长度 <pbHashData> 二进制字节流 返回消息摘要数据	—
设置指令举例	AT+ Digest=消息数据长度,消息数据	成功： + Digest: 消息摘要数据长度 消息摘要数据 OK

A.7 数字证书相关 AT 指令

A.7.1 数字证书相关AT指令列表

数字证书相关AT指令具体见表A.27。

表A.27 数字证书相关AT指令

指令名称	指令格式	功能说明
数字证书相关 AT 指令	AT+ImportCert	导入数字证书
	AT+ExportCert	导出数字证书

A.7.2 AT+ImportCert

AT指令AT+ImportCert见表A.28。

表A.28 AT+ImportCert指令

名称	描述	返回值
设置指令	AT+ImportCert=<bSignFlag>,<ulCertLen>,<pbCert>	成功： OK 失败：+CME ERROR：<err>
测试指令	AT+ImportCert=?	成功： + ImportCert： (0,1), (<ulCertLen>), (<pbCert>) OK
功能说明	导入数字证书	—
参数说明	<bSignFlag> 布尔类型 0 - 表示加密证书 1 - 表示签名证书 <ulCertLen> 无符号整形 证书长度 <pbCert> 二进制字节流 证书数据	—
设置指令举例	AT+ImportCert=1, 证书长度, 证书数据	成功： + ImportCert： OK

A.7.3 AT+ExportCert

AT指令AT+ExportCert见表A.29。

表A.29 AT+ExportCert指令

名称	描述	返回值
设置指令	AT+ExportCert=<bSignFlag>	成功： +ExportCert: <CertLen>, <CertStream> OK 失败：+CME ERROR：<err>
测试指令	AT+ExportCert=?	成功： + ExportCert： (0,1), OK
功能说明	导出数字证书	—

表A.29 AT+ExportCert指令（续）

名称	描述	返回值
参数说明	<bSignFlag> 布尔类型 0 - 表示加密证书 1 - 表示签名证书 <CertLen> 无符号整形 返回证书长度 <CertStream> 二进制字节流 返回证书数据	—
设置指令举例	AT+ExportCert=1	成功： +ExportCert： 证书长度 证书数据 OK

A.8 随机数相关 AT 指令

A.8.1 随机数相关AT指令列表

随机数相关AT指令概要见表A.30。

表A.30 随机数相关AT指令

指令名称	指令格式	功能说明
随机数相关 AT 指令	AT+ GenRandom	生成指定长度随机数

A.8.2 AT+ GenRandom

随机数相关AT指令AT+ GenRandom见表A.31。

表A.31 AT+ GenRandom指令

名称	描述	返回值
设置指令	AT+ GenRandom=<ulRandomLen>	成功： + GenRandom： <Random> OK 失败：+CME ERROR：<err>
测试指令	AT+ GenRandom=?	成功： + GenRandom：(0-512) OK
功能说明	生成指定长度随机数	—
参数说明	<ulRandomLen>无符号整形 产生多少字节随机数 <Random>二进制字节流 返回随机数	—

表A.31　AT+ GenRandom指令（续）

名称	描述	返回值
设置指令举例	AT+ GenRandom=16	成功： + GenRandom： 4567895212356894 OK

参 考 文 献

[1] GB/T 25069-2022 信息安全技术 术语
[2] YD/T 3988-2021 5G通用模组技术要求（第一阶段）
[3] YD/T 4110-2022 面向行业终端的5G通用模组可靠性技术要求及测试方法
[4] TTAF 005-2017 面向窄带物联网（NB-IoT）的终端模组总体规范－第一阶段
[5] TTAF 006-2017 面向窄带物联网（NB-IoT）的终端模组规范_B5分册_第一阶段
[6] TTAF 018-2018 面向低功耗广域物联网（LPWAN）的终端模组AT命令规范
[7] 《物联网安全标准白皮书》-全国信息安全标准化技术委员会
[8] 《面向5G的通用模组研究》-中国通信标准化协会

电信终端产业协会团体标准

集成独立安全芯片的行业物联网模组安全技术要求

T/TAF 194—2023

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn