Q/TX

腾　讯　集　团　企　业　标　准

Q/TX 001. 1—2019

腾讯物联网安全技术规范

第 1 部分：基本要求

Security technical specifications for Tencent IoT

Part 1:Basic requirements

2019-12-20 发布　　2019-12-20 实施

腾讯科技（深圳）有限公司　发布

目　录

前　言

本标准是基于物联网的总体安全技术规范，从物联网终端安全、物联网通信安全、物联网云平台安全等方面制定安全技术要求，帮助物联网厂商建立完善的物联网安全体系，提升物联网设备与生态的安全性，并为普通用户提供智能设备安全性指标参考。

本标准分拟分成部分出版，包括基本要求和具体物联网智能设备类型的安全技术要求。目前计划发布如下部分：

——第 1 部分：基本要求；

——第 2 部分：智能门锁安全技术要求；

——第 3 部分：智能摄像头安全技术要求；

——……。

本部分为 Q/TX 001-2019 的第 1 部分。

本标准遵循 GB/T 1.1—2009 制定。

本标准由腾讯科技（深圳）有限公司提出。

本标准由腾讯科技（深圳）有限公司组织制定，最终解释归口。

本标准为首次发布。

腾讯物联网安全技术规范 第1部分：基本要求

1 范围

本部分规定了腾讯物联网安全技术规范，对物联网终端、物联网通信、物联网云平台提出了基本安全要求。

本部分适用于腾讯物联网合作厂商落实物联网安全技术措施，也适用于为其它物联网厂商提供安全技术建议和参考。

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，仅所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 25069—2010 信息安全技术 术语

GB 4943.1—2011 信息技术设备 安全 第1部分：通用要求

GB/T 22080-2016 信息技术 安全技术 信息安全管理体系 要求

GB/T 30146-2013 公共安全 业务连续性管理体系要求

GB 17859-1999 计算机信息系统安全保护等级划分准则

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 37093-2018 信息安全技术 物联网感知层接入通信网的安全要求

GB/T 36951-2018 信息安全技术 物联网感知终端应用安全技术要求

GB/T 37024-2018 信息安全技术 物联网感知层网关安全技术要求

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 37033.1-2018 信息安全技术 射频识别系统密码应用技术要求 第1部分：密码安全保护框架及安全级别

GB/T 37033.3-2018 信息安全技术 射频识别系统密码应用技术要求 第3部分：密钥管理技术要求

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

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 35317-2017 公安物联网系统信息安全等级保护要求

GB/T 35592-2017 公安物联网感知终端接入安全技术要求

BS EN 60950-1-2001 Information technology equipment - Safety - General requirements

GSM协会（GSMA）《物联网安全指南》

3 术语、定义和缩略词

GB/T 25069—2010中界定的以及下列术语和定义适用于本文件。

3.1 术语和定义

3.1.1

物联网 internet of things，IoT

通过感知设备，按照约定协议，连接物、人、系统和信息资源，实现对物理和虚拟世界的信息进

行处理并作出反应的智能服务系统。

注：物即物理实体

3.1.2

传感器 transducer / sensor

能感受被测量并按照一定的规律转换成可用输出信号的器件或装置，通常由敏感元件和转换元件组成。

3.1.3

安全单元 security element

提供安全存储、身份验证、电子签名、加密解密等功能的硬件载体。

3.1.4

密钥 key

控制加密转换操作的符号序列。

3.1.5

安全服务 Security service

根据安全策略，为用户提供的某种安全功能及相关的保障。

3.1.6

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注 1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨 迹、住宿信息、健康生理信息、交易信息等。

注 2： 关于个人信息的范围和类型可参见《信息安全技术 个人信息安全规范》附录 A。

3.1.7

个人敏感信息 personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注 1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、 14 岁以下（含）儿童的个人信息等。

注 2：关于个人敏感信息的范围和类型可参见《信息安全技术 个人信息安全规范》附录 B。

3.1.8

固件 firmware

在设备内部与设备安全性相关的所有可执行程序代码。

3.1.9

通信接口 communication interface

智能门锁与其他电子设备交换数据的连接端口。

3.2 缩略词

下列缩略词适用于本文件。

ABP 个性化激活（Activation By Personalization）

ACL 访问控制列表（Access Control List）

APP 应用（application）

BGA　球状阵列排列（Ball Grid Array）
BLE　　低功耗蓝牙　（Bluetooth Low Energy）
COAP　受限应用协议（The Constrained Application Protocol）
COS　芯片操作系统（Chip Operating System）
CPU　　中央处理器（Central Processing Unit）
DDos　分布式拒绝服务（Distributed Denial of service）
DTLS　数据包传输层安全协议（Datagram Transport Layer Security）
EPPROM　带电可擦可编程只读存储器（Electrically Erasable Programmable read only memory）
Flash　闪存（Flash memory）
GATT　通用属性（低功耗蓝牙设备之间通信协议）（Generic Attributes）
HTTPS　超文本传输安全协议（Hyper Text Transfer Protocol Secure）
IoT　　物联网（Internet of Things）
IPSEC　互联网安全协议（Internet Protocol Security）
JTAG　联合测试工作组（Joint Test Action Group）
LoRaWAN　远距离广域网（Long Range Wide Area Netword）
MCU　　微控制单元（Micro Controller Unit）
MQTT　消息队列遥测传输协议（Message Queuing Telemetry Transport）
NB-IoT　窄带物联网（Narrow Band Internet of Things）
NFC　近场通信（NearField Communication）
OOB　带外传输（Out of Band）
OTAA　空中激活（Over-The-Air-Activation）
PCB　印制电路板（Printed Circuit Board）
PIN　　个人识别码(Personal Identification Number)
URL　统一资源定位符（Uniform Resource Locator）
RAM　　随机存取存储器（Random Access Memory）
RCC　　限域通信（Range Controlled Communication）
RFID　　射频识别（Radio Frequency Identification）
ROM　　只读存储器（Read-Only Memory）
SE　　安全单元（Secure Element）
SHA　哈希算法/安全散列算法（Secure Hash Algorithm）
SPI　串行外设接口（Serial Peripheral Interface）
SWD　串行线调试（Serial Wire Debug）
RSRP　　参考信号接受功率　（Reference Signal Receiving Power）
RSSI　　接收信号强度（Received Signal Strength Indication）
SINR　　信号与干扰加噪声比　（Signal to Interference plus Noise Ratio）
TCP/IP　传输控制协议/因特网互联协议(Transmission Control Protocol/Internet Protocol)
TEE　可信执行环境（Trusted Execution Environment）
UART　通用异步收发传输器（Universal Asynchronous Receiver/Transmitter）
UID　唯一标识符（Unique Identifier）
UPnP　通用即插即用（Universal Plug and Play）
WEP　有线等效保密（Wired Equivalent Privacy）
WIPS　无线入侵防御系统（Wireless Intrusion Prevention）
WPS　无线局域网安全防护设置（Wi-Fi Protected Setup）
Wi-Fi　基于 IEEE 802.11b 的无线局域网（Wireless Fidelity）

WPA 无线局域网安全接入（Wi-Fi Protected Access）

4 系统架构

本规范所述基于云（云平台）、管（通信）、端（终端）的物联网安全模型如下图 1。

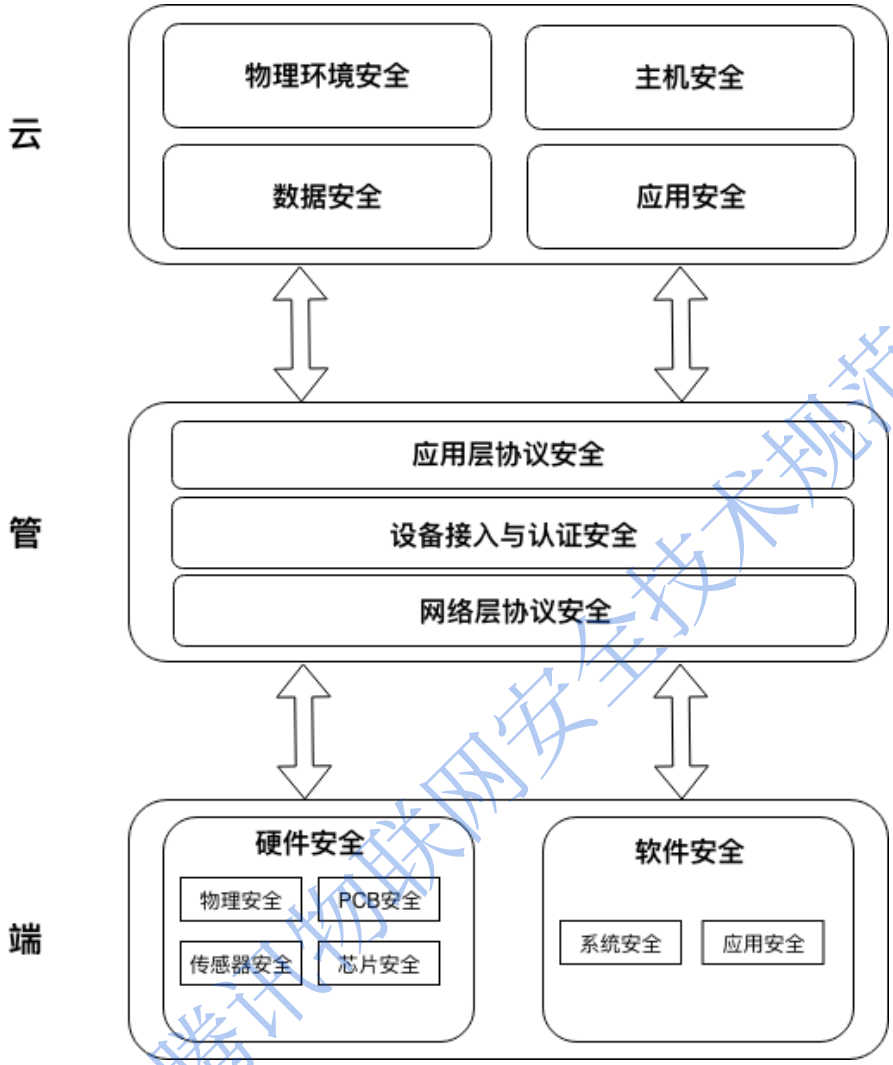

图 1 云、管、端物联网安全模型

此模型主要从云、管、端的攻击面出发， 分析可能受到攻击的物联网生态入口，进一步 细分了 9 个部分。由于不同物联网产品业务架构区别较大，考虑移动 App 安全规范与生态已经较为独立与成熟，此安全模型暂未将移动 App 列入独立模块。同时由于许多物联网设备使用的系统为 Android 系统，本规范在软件安全与应用层协议安全的部分内容，也可作为厂商移动 App 产品安全要求的参考与补充。

5 总体安全要求

5.1 物联网终端安全

物联网终端安全包含了物理安全、硬件电路安全、传感器安全、芯片安全、系统安全、软件安全、移动 APP 控制端安全。

5.1.1 物理安全

1）物理防护

——物联网终端设备外壳应该具备简单的防破坏措施，能够避免设备在无工具情况下被快速拆解，建议使用螺钉等方式对外壳进行封闭；

——电气安全要求应符合GB 4943.1-2011的有关规定，应防止和减少部件发生火灾、电冲击和人身伤害的可能性；

2）通信接口

——设备外壳应该尽量避免对外暴露存在风险的通信接口，如正常情况下闲置或非必要的USB接口，调试串口等；

3）人机交互

——对于公共服务类等特殊设备，如提供了触摸屏，键盘，鼠标等交互方式，应该为除正常功能外的操作（如后台管理，开启调试模式等）添加密码验证等安全防护，防止设备正常业务逻辑被绕过；

——对于公共服务类等特殊设备，应避免对外暴露重置功能，系统重启功能等特殊权限按键；

5.1.2 硬件电路安全

设备在外壳被拆解后，其硬件电路将会暴露于安全风险中，故应该满足以下安全要求：

1）PCB 信息

——设备电路板应去除敏感接口丝印信息，如调试与烧录接口焊点印刷标识；

2）PCB接口

——设备电路板中应避免留存非必要的调试与烧录接口或焊点，如JTAG、SWD、UART、SPI等接口， 如需要留存返修维护接口，应该使用具备密码保护功能的调试或烧录工具，提升设备固件提取与读写难度；

5.1.3 传感器安全

智能终端设备可能带有大量传感器进行各种数据收集，这些传感器同样需要按以下安全要求进行防护。

1）麦克风

——对于支持语音识别及声纹识别的设备，麦克风传感器应该选择仅支持人耳可识别范围内声音（频率响应：20hz - 20Khz）的型号，防止类似海豚音（超声波）攻击；

2）摄像头

——高安全需求设备的摄像头传感器应该选择支持3D人脸识别与活体检测的型号，防止照片，视频，人脸模具等伪造人脸攻击；

3）指纹识别

高安全需求设备应采用支持活体检测的指纹识别传感器，防止指纹膜等伪造指纹攻击；

4）GPS定位

设备应该采用GPS定位+WiFi 辅助定位方案，避免使用仅依靠GPS定位系统进行定位与授时，防止受到GPS信号欺骗攻击；

5.1.4 芯片安全

部分计算能力较强的终端设备内部有大量芯片，这些芯片同样是可能受到攻击需要进行防护。此外，正确的使用 SE 芯片能够帮助高安全需求设备迅速有效提升安全能力。

1）Flash 芯片

——使用独立 Flash 芯片的设备应该尽量采用 BGA 封装的型号；

2）MCU与SE芯片

——对于支持熔丝功能的MCU或安全芯片，应该在量产时对熔丝位进行熔断处理，防止芯片内部数据被读取；

——如设备MCU自身支持硬件级加密与校验功能，应通过此功能关闭芯片的调试，读写，Boot方式选择功能或添加密码保护，同时启用系统固件的加密与校验功能；

5.1.5 系统安全

对于使用了基于嵌入式 Linux，Android 等系统的设备，正确配置系统安全策略与安全更新机制可以提升设备系统安全性。

1）可信启动

——使用 Android 系统的设备，应该开启系统的 Verfield Boot(Android7.0 以上或 dm-verity(Android 4.4 以上)功能；

2）安全加固

——设备在系统支持的情况下，应该根据性能与安全需求正确启用进程沙盒隔离，系统安全机制，提升漏洞攻击难度；

3）安全更新

——设备系统应该具备远程在线升级功能，用于更新系统固件与软件应用；

——设备系统更新功能应该支持推送系统安全补丁，厂商发现系统与软件存在安全漏洞后，应及时开发并推送修复补丁；

——设备更新包应进行加密，提升固件逆向门槛；

——设备应对更新包完整性进行校验，建议使用非对称算法进行签名校验；

5.1.6 软件安全

1）开发安全

——设备厂商应该使用代码安全扫描工具进行代码审计，提升代码质量，同时在编绎 C/C++代码时使用安全编绎选项，提升内存类型漏洞攻击成本；

2）第三方库安全

——尽量避免使用历史漏洞较多或停止维护的高风险第三方库；

3）网络安全

——尽量避免对外开放网络端口以及明文传输敏感数据；

4）密码安全

——避免在本地明文存储敏感数据，加密时不要在代码中硬编码对称密钥或使用弱密钥；

5.1.7 移动 APP 控制端安全

1）访问控制

——应对登录用户进行身份鉴别，如登录口令，并对用户的鉴别信息进行复杂度检查；

2）数据安全

——应加密存储敏感数据，敏感数据存储路径应设置严格的访问控制机制，避免数据泄露；

——用于加密的密钥应妥善保存，避免被直接获取；

——应禁止日志数据包含与用户数据相关的数据；

——客户端向服务端发送数据时，应采用密钥技术对数据进行完整性签名。

3）反编译保护

——客户端应采用包括代码混淆或加壳等代码加固方式部署；

——客户端应具备动态防调试能力；

4）防篡改保护

——客户端应具有对自身签名进行校验的能力，防止应用重打包；

——客户端启动和更新时，宜进行真实性和完整性校验，防范客户端被篡改。

5）客户端管理安全

——客户端应有规范的上线发布流程，并应提供安全可靠的客户端下载、发布、升级渠道；

——客户端软件在卸载时，应清除所有缓存文件、日志文件等不必要的信息。

5.2 通信安全

物联网终端网关与物联网云平台，终端与终端，终端与网关间使用了多种通信技术与认证方式，厂商应根据实际情况选择较为安全的通信方案，并需要符合以下安全要求。

5.2.1 网络层通信安全

网络层通信包含了各种近场无线通信与远距离无线通信技术，常见的安全风险包含了数据包重放，中间人嗅探，破解与劫持等。

1）WiFi

——WiFi 网关必须启用密码认证，建议不要使用 WEP/WPA 等加密标准，WiFi 密码避免使用弱密码；

2）蓝牙通信

——BLE设备开放GATT协议服务时，应对敏感属性或数据的读写进行权限限制；

3）射频通信

——设备射频通信协议应具备防重放攻击能力，如使用加密认证，序列号验证等机制；

4）ZigBee

——设备ZigBee通信密钥禁止使用ZigBee联盟通用密钥、芯片厂商默认密钥或弱密钥 ，禁止在设备固件或系统中明文存储密钥；

5）LoRaWAN

——设备可以使用ABP或OTAA方式入网，如使用ABP方式入网必须保证设备预置密钥随机性与保密性；

6）移动网络

——设备应避免选用2G、3G等不安全的移动通信方式；

5.2.2 设备接入与认证

物联网终端设备在接入云端网络时，必须分配一个独一无二的身份编号，这个编号（通常称为设备 ID）应具备无法伪造与防硬件篡改的属性，可用于对设备进行认证。设备 ID 是保障物联网系统正常运转的重要基础。

1）ID 分发安全

——设备 ID 通常需要在出厂前预置于设备中或在入网认证协商成功后从云端下发，对自建 IoT 认证体系与平台的厂商，应该保证设备 ID 在分发过程中的保密性；

——对于使用腾讯云 IoT 平台的厂商，应该按平台提供的文档规范进行设备接入开发；

2）设备认证安全

——对于自建IoT认证体系与平台的厂商，设备在连接云端认证平台时，应该使用TLS加密协议或相同安全强度的协议保证通信过程的安全性，同时认证机制应该选择具备单向认证或双向认证能力；

——对于使用腾讯云IoT平台的厂商，应该按平台提供的文档规范进行设备认证开发；

5.2.3 应用层通信安全

1）MQTT

——在资源开销可满足的情况下，使用 TLS（如 TLS v1.1、TLS v1.2）加密协议保护整个 MQTT 的通讯安全；

2）COAP

——在资源开销可满足的情况下，使用DTLS（如DTLS v1.2或对称加密协议保护整个COAP的通信安全。

3）HTTPS

——证书签名使用的哈希算法为 SHA 256；

——检查证书有效期，防止证书过期；

——HTTP跳转到HTTPS ，使用30X 跳转（301,302,307等）；

5.2.4 通信安全管理要求

1）网络速度及时延

——网络速度应大于 10kbps、时延应小于 200ms；

——通过网络方式的开锁操作，从业务发起到锁体开启时间应不超过 10s，通过本地方式的开锁操作，从业务发起到锁体开启时间应不超过 3s；

2）稳定性

——丢包率小于 10%，应有重传机制，若采用长连接通信应有心跳机制，保证在网率。

5.3 物联网云平台安全

5.3.1 物理环境安全

1）私有独立的物理机房

——使用私有独立的机房环境，可以有效的控制安全风险，厂商也能够完全的管理业务与服务器。有能力的厂商可以自建机房。

2）共用的物理机房

——共用环境下，自机房中其他厂商的安全问题可能会影响到自身服务的安全，存在不可控的安全风险。厂家可以通过网络隔离方式保护自身的业务环境不受影响。

3）腾讯云服务

——共用情况下的风险隔离，建议使用腾讯云的VPC服务可以很好的解决，能保障各家业务环境分离，互不影响；

5.3.2 主机安全

1）访问控制

——应遵循权限最小化原则，对服务器和网络访问范围进行严格管理，防止被非法 IP 访问。如通过防火墙、路由器、ACL、IPSEC、iptables、腾讯云安全组等方式进行控制；

2）身份认证

——登录服务器，访问各类服务时，必须对访问者的身份进行合法性认证，保留各用户的访问登录记录；

3）账号管理

——服务器、设备等不能使用废旧账号、弱口令账号。严格按照最小化权限原则分配账号；

4）端口安全

——对于服务器、设备上不使用的服务端口，需要全部清理关闭或者删除。

5.3.3 应用安全

1）网络攻击防御

——公网上的服务容易受到 DDos 攻击、Web 漏洞攻击，会导致服务不可用、数据被窃取等严重后果。智能门锁厂家必须具备抗 DDos 攻击的防护能力、Web 漏洞检测和拦截能力、以及服务器被入侵检测能力。

部署在腾讯云上的智能终端厂家，建议使用腾讯云上的 DDos 防御服务、Web 漏洞扫描服务、web 应用防火墙、主机安全服务等配套安全服务保障服务安全。

2）管理后台安全

——管理后台需放在内网中访问，如果必须放到外网访问，需要通过严格的访问控制与身份认证，确保管理后台被合法授权访问。

3）第三方组件安全

——服务器上安装的第三方开源组件（如nginx、apache等），必须使用官方站点上的最新无安全漏洞版本。

5.3.4 数据安全

1）数据存储安全

——服务生成的个人信息、个人敏感信息、业务数据等敏感或者重要的数据，不能明文存储，必须通过适当加密后存储在数据库中；

——数据库不得开放在外网访问，只能在内网中访问，需要做好严格的访问控制；

——对数据库的访问，必须遵守访问控制、身份认证、账号管理的要求；

——所有对数据的访问操作，需要有详细的记录信息，并进行异常审计。

2）数据传输安全

——通过网络传输的敏感数据必须加密处理，并通过安全可靠的加密通信协议传输，保障数据完整性。

3）数据使用安全

——必须对数据访问者的身份进行认证和授权检查，并使用最小化授权原则，严格限制允许访问的范围，禁止并记录非法访问；

——对展示的敏感数据进行脱敏处理；

——对外接口需对URL参数、用户操作进行合法性验证；

——保存一段时期内的web访问日志，用户操作记录；

5.3.5 云端安全

——SaaS 平台软件应支持对代码进行安全测试并进行缺陷修复的能力。

——SaaS 平台软件应支持安全加固能力。

加固策略应遵守业界最佳实践，如：遵循最小化安装、关闭不需要的服务、安装最新补丁、修改默认口令、最小权限运行账号等。

——SaaS 平台软件应支持对入侵行为进行监测和告警的能力。

检测到入侵行为时，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间。

——SaaS 平台软件应支持对恶意代码进行检测，对检测出来的后门进行访问控制和隔离的能力。

——SaaS 平台软件应支持监视远程管理连接，发现未授权管理连接时中断连接的能力。

——SaaS 平台软件应支持对远程执行 SaaS 平台软件特权管理命令进行限制的能力。

——SaaS 平台软件应支持安全启动能力。

安全启动指启动时的版本和预期是一致的，完整性没有受到破坏。

——SaaS 平台软件应支持对重要配置文件完整性检测的能力。

——SaaS 平台软件应支持最小化安装，仅安装必要的组件和应用程序的能力。

——SaaS 系统应支持资源集中监控能力。

附录 A

（规范性附录）

标准修订历史

修订时间	版本号	修订内容
2019年12月20日	V1.0	正式发布