ICS 01.040.33
M04

YDB

中 国 通 信 标 准 化 协 会 标 准

YDB XXX –201X

物联网安全需求

Security requirements of internet of things

201X –XX –XX 印发

中国通信标准化协会

目 次

前　　言

为适应信息通信业发展对通信标准文件的需要，由中国通信标准化协会组织制定“中国通信标准化协会标准”，推荐有关方面参考采用。有关对本标准的建议和意见，向中国通信标准化协会反映。

本标准由中国通信标准化协会提出并归口。

本标准起草单位： 中国移动通信集团公司、工业和信息化部电信研究院、武汉邮电科学研究院、中国联合网络通信集团有限公司、大唐电信科技产业集团、华为技术有限公司、中兴通讯股份有限公司、上海贝尔股份有限公司。

本标准主要起草人： 朱红儒、齐旻鹏、刘斐、袁琦、陈淞、桑梓勤、张尼、徐晖、魏瑛、许怡娴、陈书义、胡志远。

物联网安全需求

1 范围

本标准分析了物联网存在的安全威胁，并以此为基础提出了物联网终端、物联网端节点、物联网接入网关、感知延伸网络、核心、接入网络和应用层及物联网层间等方面的系统安全需求。

本标准适用于物联网系统安全技术领域。

2 术语和定义

YDB XXX-201X《物联网的需求》界定的术语和定义适用于本文件。

3 缩略语

下列缩略语适用于本文件。

DoS	拒绝服务	Denial of Service
IoT	物联网	Internet of Things
MITM	中间人	Man In The Middle
PKI	公钥基础设施	Public Key Infrastructure
RFID	无线射频识别	Radio Frequency IDentification
SIM	客户识别模块	Subscriber Identity Module
UICC	通用集成电路卡	Universal Integrated Circuit Card
VPN	虚拟专用网络	Virtual Private Network

4 概述

物联网是指通过部署具有一定感知、计算、执行和通信等能力的各种设备，获得物理世界的信息，通过网络实现信息的传输、协同和处理，从而实现人与物通信、物与物通信的互联的网络。在物联网中，涉及到诸多安全需求亟待解决，如在支付系统的物联网应用中，需要保证用户的支付数据等敏感信息的机密性完整性；在车载应用中，需要保证用户位置等隐私信息的机密性和完整性等。

本标准按照物联网总体架构的网络层次划分方式，以感知延伸层、网络层、应用层为出发点，制定物联网所面临的安全威胁和制定物联网安全标准需求，主要包括：从物联网的物联网终端、物联网端节点和物联网接入网关、感知延伸网络、接入、核心网络、应用层、控制管理以及物联网层间方面等不同的角度分析物联网面临的安全威胁和存在的安全隐患；并在此基础上，提出物联网感知延伸层、网络层、应用层以及相关业务应用的安全需求。

5 总体安全框架

物联网安全应能够对物联网络的访问加以控制，确定用户（如抽象的有权限的账户、人、物联网终端、物联网端节点或物联网接入网关）身份真实有效以及私密性，保证用户行为不可抵赖，保证传输和存储数据的机密性、完整性，保证物联网的可用性，防止网络、业务遇到偶然的、被动的和主动的威胁以及蠕虫病毒的扩散，对影响网络、业务的意外事故具有应急措施。

根据物联网通用分层模型，物联网在逻辑功能上划分为三层，即：感知延伸层、网络/业务层和应用层。

基于通用分层模型,物联网安全需求主要划分为：感知延伸层的末端节点的安全需求、感知层安全需求；网络/业务层的网络层安全需求、业务层安全需求；应用层的安全需求、支撑物联网系统运行的运维管理安全需求以及物联网不同层次间的安全需求，分别包括：

a） 末端节点的安全需求包括物理安全防护、访问控制、认证、不可抵赖性、机密性、完整性、可用性、私密性等；

b） 感知层安全需求包括机密性、数据源认证、设备认证、完整性、可用性、时效性等；

c） 网络层安全需求包括总体安全需求、机密性、完整性、隐私性、认证的一般需求、组认证、密钥的一般需求、可用性等；

c） 业务层安全需求包括：身份认证、业务认证、组认证、隐私保护、完整性、机密性、密钥安全性、防抵赖、抗重放、可用性等；

d） 应用层安全需求与具体物联网应用关联紧密，应根据具体的物联网应用进行分析和定义，本标准不涉及。

e） 运维管理安全需求包括：远程配置安全、软件授权下载、管理员身份鉴别、制定统一安全平台等；

f） 物联网不同层次间的安全需求包括：层间传输敏感信息的完整性与机密性、跨层认证与授权、敏感信息隔离等。

根据上述物联网的特征分析和安全需求的要求，物联网安全设计的基本原则主要有：

a） 由于物联网终端和物联网端节点可能处于无人值守的环境中，所以物联网终端的本地安全相较于现有通讯网络终端安全问题更大巨大，因此需要更加重视物联网终端和物联网端节点的安全性；

b） 物联网具有节点数量巨大、物联网端节点组群化、低移动性等特点，而且，针对一般的物联网终端，其携带能量有限，因此需要针对物联网的这些特点定制更加符合物联网特性的，低能耗的安全要求；

c） 物联网中轻量级的，特定的安全要求将会使得物联网安全机制与现有网络安全机制略有不同，但安全物联网尽可能的复用现有网络，因此物联网安全保护强度不能低于现有网络安全强度，避免在现有网络中制造安全薄弱环节。

6 物联网的安全问题

6.1 末端节点本身的安全问题

物联网的末端节点包括：物联网终端、物联网端节点和物联网接入网关。

物联网末端节点的安全威胁见表1，包括：

a） 非授权读取节点信息：由于末端节点被物理俘获或逻辑攻破，攻击者可利用简单的工具分析出末端节点所存储的敏感信息，以及与人身份关联的隐私信息；

b） 节点不可用：由于末端节点被物理俘获或逻辑攻破，攻击者可使末端节点不工作；

c） 假冒节点：攻击者通过假冒物联网终端、物联网端节点和物联网接入网关，向感知延伸网络注入信息，从而发动多种攻击，如监听感知延伸网络中传输的信息，向感知延伸网络中发布假的路由信息或传送假的数据信息、进行拒绝服务攻击等；

d） 自私性威胁：末端节点之间本应协同工作，但部分末端节点不愿消耗自己的能量或是有效的网络带宽为其它末端节点提供转发数据包的服务，影响网络的效率或使网络失效；

e） 恶意代码攻击：木马、病毒和垃圾信息等攻击，这是由于终端操作系统或应用软件的漏洞所引起的安全威胁。

表1 末端节点的安全威胁和脆弱性分析

安全威胁及脆弱性	物联网终端	物联网端节点	物联网接入网关
非授权读取节点信息	√	√	√
拒绝工作	√	√	√
假冒节点对传感网络进行攻击		√	√
自私性威胁		√	√
恶意代码攻击	√	√	√

6.2 感知延伸网络的安全问题

由于感知延伸网络具有资源受限、拓扑动态变化、网络环境复杂、以数据为中心以及与应用密切相关等特点，与传统的无线网络相比，更容易受到威胁和攻击。

感知网络除了可能遭受同现有网络相同的安全威胁外，还可能受到一些特有的威胁：

a） 传输威胁：任何有机密信息交换的通信都必须防止被窃听。传输信息主要面临的威胁有以下几种：

1)中断：路由协议分组，特别是路由发现和路由更新消息，会被恶意末端节点中断和阻塞。攻击者可以有选择地过滤控制消息和路由更新消息，并中断路由协议的正常工作。

2)拦截：路由协议传输的信息，如“保持有效”等命令和“是否在线”等查询，会被攻击者中途拦截，并重定向到其他末端节点，从而扰乱网络的正常通信。

3)篡改：攻击者通过篡改路由协议分组，破坏分组中信息的完整性，并建立错误的路由，造成合法末端节点被排斥在网络之外。

4)伪造：无线传感网络内部的恶意物联网端节点可能伪造虚假的路由信息，并把这些信息插入到正常的协议分组中，对网络造成的破坏。

b） 拒绝服务：拒绝服务主要是破坏网络的可用性，减少、降低执行网络或系统执行某一期望功能能力的任何事件。如试图中断、颠覆或毁坏感知网络，包括恶意干扰网络中协议的传送、物理损害物联网端节点以及消耗物联网端节点能量，另外还包括硬件失败、软件缺陷、资源耗尽、环境条件等；

c） 路由攻击：恶意物联网端节点拒绝转发特定的消息并将其丢弃，以使得这些数据包不再进行任何传播。另一种表现形式是攻击者修改特定物联网端节点传送来的数据包，并将其可靠地转发给其它物联网端节点，从而降低被怀疑的程度。当恶意节点在数据流传输路径上时选择转发攻击最有威胁。

6.3 通信网络安全问题

a） 隐私的泄露问题：由于一些物联网设备很可能是处在物理不安全的位置，就给了攻击者可趁之机，从物理不安全的设备中获得用户身份等隐私信息，并以此设备对通信网络进行一些攻击；

b） 传输的安全问题：

1)通信网络存在的一般性的安全问题，会对信令的机密性产生威胁；

2)通信网络存在的一般性的安全问题，会对信令的完整性产生威胁；

c） 大量物联网设备接入带来的问题：

1)DoS攻击： 物联网设备数量巨大，如果通过现有的认证方法对设备进行认证，那么信令流量对网络侧来说是不可忽略的。大量设备在很短时间内接入网络很可能会带来网络拥塞，而网络拥塞会给攻击者带来可趁之机，从而对服务器产生拒绝服务攻击；

2)密钥：传统的通信网络认证是对终端逐个进行认证，并生成相应的加密和完整性保护密钥。这样带来的问题是当网络中存在比传统手机终端多得多的物联网设备时，如果也按照逐一认证产生密钥的方式，会给网络带来大量的资源消耗。

d） 感知延伸层和通信网络安全机制之间的融合会带来如下问题：

1)中间人攻击：攻击者可以发动MITM攻击，使得物联网设备与通信网络失去联系，或者诱使物联网设备向通信网络发送假冒的请求或响应，从而使得通信网络做出错误的判断而影响网络安全；

2)伪造网络消息：攻击者可以利用感知网络的安全性等特点，伪造通信网络的信令指示，从而使得物联网设备断开连接或者做出错误的操作或响应。

6.4 业务的安全问题

物联网业务层主要面临以下安全问题：

a） 隐私威胁：隐私信息可能被攻击者获取，给个人用户带来安全隐患。物联网的隐私威胁主要包括隐私泄漏和恶意跟踪：

1)隐私泄漏：隐私泄露是指个人用户的隐私信息暴露给攻击者，例如用户的病历信息、个人身份信息、兴趣爱好、商业机密等信息。

2)恶意跟踪：隐私信息的获取者可以对个人用户进行恶意跟踪。例如隐私侵犯者可以通过标签的位置信息获取标签用户的行踪，抢劫犯能够利用标识信息来确定并跟踪贵重物品的数量及位置信息等。

b） 业务滥用：物联网中可能存在业务滥用攻击，例如非法用户使用未授权的业务或者合法用户使用未定制的业务等；

c） 身份冒充：物联网中存在无人值守设备，这些设备可能被劫持，然后用于伪装成客户端或者应用服务器发送数据信息、执行操作。例如智能家居场景中，针对自动门禁远程控制系统，通过伪装成基于网络的后端服务器，可以解除告警、打开门禁进入房间；

d） 业务信息窃听/篡改：由于物联网通信需要通过异构、多域网络，这些网络情况多样，安全机制相互独立，因此应用层数据很可能被窃听、注入和篡改；

e） 抵赖：通信的所有参与者可能否认曾经完成的操作和承诺；

f） 重放威胁：攻击者向目标（末端节点或物联网应用服务器）发送已接收过的消息，来达到欺骗系统的目的；

g） 拒绝服务攻击：目前的认证方式是应用终端与应用服务器之间的1对1认证。而在物联网中，物联网端节点和物联网终端设备数量巨大，当短期内这些数量巨大的终端同时使用业务，会与应用服务器之间产生大规模的认证请求消息。这些消息将会导致应用服务器过载，使得网络中信令通道拥塞，引起拒绝服务攻击。

6.5 运维管理方面的安全问题

a） 远程配置、更新末端节点上的软件应用问题

由于物联网中的末端节点数量巨大,部署位置广泛,人工更新末端节点上的软件应用变得更加困难，远程配置、更新末端节点上的应用则更加重要，因此需要提供对远程配置、更新时的安全保护能力；此外，病毒、蠕虫等恶意攻击软件可以通过远程通信方式置入末端节点，从而导致末端节点被破坏，甚至进而对通信网络造成破坏。

b） 配置管理末端节点的特征时的安全问题

攻击者可以伪装成合法用户，向网络控制管理设备发出虚假的更新请求，使得网络为末端配置错误的参数和应用，从而导致末端终端不可用，破坏物联网的正常使用。

c） 安全管理问题

在传统网络中，由于需要管理的设备较少，对于各种业务的日志审计等安全信息由各自业务平台负责，而在物联网环境中，由于物联网末端节点无人值守，并且规模庞大，节点加入退出没有安全运维机制，因此如何对这些末端节点的日志、密钥等安全信息进行管理成为了新的问题。

6.6 物联网层间安全问题

a） 敏感信息在层间边界泄露

层间的敏感信息可能在边界处无法受到保护。

b） 伪造身份

应用层实体的身份合法性在网络层无法得到验证。

c） 敏感信息在层间扩散引起的泄露

层内敏感信息可能扩散至其他层中导致信息泄露。

7 物联网的安全需求

7.1 末端节点的安全需求

末端节点的安全需求主要体现在对末端节点特性的分析，不同特性的末端节点的脆弱性与安全威胁、安全防护要求及可能采取的安全措施将各不相同。这些特性包括：末端节点的存储、通信及处理能

力等物理特性；末端节点所提供服务的差异；末端节点所服务的环境及使用用户要求的差异等。表2列出了末端节点的脆弱性与安全威胁所对应的安全需求。

a） 物理安全防护

需要采取措施保护末端节点避免失窃，或被攻击者物理上获得或复制。

针对有卡的设备，需要采取措施防止将UICC或者SIM卡非法操作。

针对无卡的设备，需要采取措施防止信任状非法操作。

当末端节点和卡的物理安全防护被破坏后，应无法正常使用。

b） 访问控制

需要采取访问控制的方式，防止末端节点被逻辑攻破，或向其它末端节点或网络设备泄露用户或末端节点信息。

c） 认证

物联网终端、物联网端节点与物联网接入网关需要支持物联网网络/业务层的认证功能。

物联网终端是可以直接与物联网网络/业务层相关功能实体进行交互的终端，典型的代表有移动终端、RFID读写器等。为确保采集数据来源的合法性及有效性需对物联网终端进行认证。

物联网端节点通过物联网接入网关连接至物联网网络/业务层。物联网端节点通常在功能、处理能力、通信能力、供电上具有一定的局限性，典型代表是无线传感器节点。对物联网端节点做适度的认证，可对物联网端节点的真实性进行鉴别，确保信息源的可靠。

物联网接入网关中继物联网端节点到物联网网络/业务层之间的信息。某些物联网感知延伸层节点可能只具有近距离通信功能，为了连接到广域网络，此时需要通过感知延伸网和物联网接入网关实现到广域网的接入；另外一种典型需求是利用物联网接入网关来实现网络连接的汇聚和信息的汇聚，简化网络连接和相应的管理等。根据应用场景，物联网接入网关有多种类型，如车载网关、企业网关、家庭网关等。对物联网接入网关的身份认证是网络边界防护的重要手段，能控制合法物联网接入网关的接入，阻断非法物联网接入网关的连接。

d） 不可抵赖性

末端节点在读写数据时要提供记录，以便识别用户或其它设备访问或使用了网络或业务。

e） 机密性

末端节点所存储的数据或所传送的数据要加密。

f） 数据完整性

需要采取措施防止末端节点的数据被篡改。

g） 可用性

需要采取措施保护末端节点，例如采用防病毒软件，防火墙等措施，使之不会被逻辑攻破或被病毒攻击导致不工作，也需要采取措施使多个末端节点不仅仅是消耗网络资源而且能贡献自身资源，从而正常协同工作。

h） 私密性

需要保护末端节点所存储的用户隐私，并防止与用户身份有关的信息泄露。

表 2 末端节点的脆弱性、安全威胁与对应的安全需求

	非授权读取末端节点信息	使末端节点失效	假冒末端节点	末端节点的自私性	木马、病毒、垃圾信息攻击	信息泄露
物理安全防护	√	√	√			
防病毒、防火墙措施					√	
访问控制	√	√	√			√
认证	√	√	√			√
不可抵赖性	√	√	√			√

机密性	√	√	√			√
数据完整性			√			
可用性		√		√	√	
私密性	√					√

7.2 感知延伸网络的安全需求

感知延伸网络的安全需求应该建立在感知网络自身的特点、服务的末端节点特征及使用用户的要求基础上。一般的感知网络具有低功耗、分布松散、信令简练、协议简单、广播特性、少量交互甚至无交互的特点，因此安全应建立在利用尽可能少的能量及带宽资源之上、设计出既精简又安全的算法、密钥体系及安全协议，解决相应的安全问题。如：对终端接入鉴权，防止非法接入或非授权使用；对传输信息的保护，防止泄露、篡改、假冒或重放。

a） 机密性

避免非法用户读取机密数据。一个感知网络不应泄漏机密数据到相邻网络。

b） 数据源认证

避免物联网端节点被恶意注入虚假信息，确保信息来源于正确的物联网端节点。

c） 设备认证

避免非法设备接入网络，确保设备是其所声称的设备。

d） 完整性

通过校验来检测数据是否被修改,确保消息被非法（未经认证的）改变后能够被识别。

e） 可用性

确保感知网络的信息和服务在任何时间都可以提供给合法用户，可通过数据备份等实现。

f） 时效性

保证接收到数据的时效性，确保没有恶意末端节点重放过时的消息。

7.3 通信网络的安全需求

通信网络主要包括有线、无线通信网络及卫星信道等，通信网络的安全需求主要包括接入鉴权；话音、数据及多媒体业务信息的传输保护；在公共网络设施上构建虚拟专网（VPN）的应用需求，用户个人信息或集团信息的隐蔽；各种网络病毒、网络攻击、DoS攻击等。针对不同的网络特征及用户需求，采取一般的安全防护或增强的安全防护措施能基本解决物联网通信网络的大部分安全问题。

因此，通信网络应具有以下安全能力：

a） 总体安全需求：

物联网的通信网络的总体安全需求不得低于一般通信网络的安全需求；

b） 机密性：

需要保证物联网通信网络的信令的机密性；可以保证物联网通信网络的数据的机密性。

c） 完整性：

需要保证物联网通信网络的信令的完整性；

d） 隐私性：

需要保证物联网通信网络用户身份、物联网终端位置等的隐私性；

e） 认证的一般需求：

物联网的物联网终端和网络的相互认证可以采用多种认证方式；

f） 组认证

物联网的物联网终端可以基于组的形式进行认证,来避免大规模终端认证造成的网络信令拥塞并防止可能的DoS攻击；

群组设备的认证可以通过认证代理来完成，如物联网接入网关或主设备；

g） 密钥的一般需求：

物联网终端/物联网接入网关和网络侧实体可以根据组认证来共享某些密钥；

物联网终端/物联网接入网关和网络侧可以根据不同的协议层共享相应协议层的密钥；

用多种鉴权权物联网终端/物联网接入网关可以生成全部协议层的密钥，也可以只生成部分协议层的密钥。

h） 可用性

确保物联网通信网络的信息和服务在任何时间都可以提供给合法用户，可通过数据备份等实现。

7.4 业务的安全需求

业务的安全问题研究范畴是基于物联网实现广域或大范围的人与物、物与物之间信息交换的各行业应用或服务于广大群众的物联网应用的基础上进行的。安全问题及安全需求研究需结合各个应用层次分别开展研究，如针对智能城市、智能交通、智能物流、智能环境监控、智能社区及家居、智能医疗等应用，其安全问题及安全需求存在共性及差异。共性的安全需求包括对操作用户的身份认证、访问控制，对行业敏感信息的信源加密及完整性保护、证书及PKI应用实现身份鉴别、数字签名及抗抵赖；安全审计等，见表3。应用层个性化的安全需求还需针对各类智能应用的特点、使用场景、服务对象及用户特殊要求进行有针对性的分析研究。

针对业务存在的共性安全问题，主要有以下安全需求：

a） 身份认证：物联网服务器或者末端节点的真实身份的认证，防止身份伪造和末端节点克隆等攻击。

b） 业务认证：物联网应用服务器对末端节点之间需要进行业务认证，为防止假冒用户使用未授权的业务或者合法用户使用未定制的业务，用户请求使用业务前必须经过严格的业务认证。

c） 组认证：物联网应用通常对应大量的末端节点，这些末端节点可能构成一个组，物联网应用服务器需要提供对这些末端节点进行组认证的能力。

d） 隐私保护：保护行为或者通信信息不泄密，这些信息包括通信内容、用户地理位置和用户身份等。

e） 完整性：考虑到物联网络中恶意末端节点可能注入、篡改应用层消息。因此，物联网应用层需要避免未授权的删除、插入和复制操作。由于物联网需要通过多种异构网络进行通信，这些网络间的安全机制相互独立且并不一致，因此需要为应用通信提供端到端的完整性保护。

f） 机密性：在物联网络中各种数据和消息只能让授权用户查看。机密性保护可以避免非授权访问和应用层数据内容非授权阅读。由于物联网需要通过多种异构网络进行通信，这些网络间的安全机制相互独立且并不一致，因此需要为应用通信提供端到端的机密性保护。

g） 密钥的安全性：采用动态下载密钥参数与动态更新登录密码的方式来实现。

h） 防抵赖：提供不可抵赖性机制，保证通信各方对自己行为及对行为发生的时间的不可抵赖性。例如通过进行身份认证和数字签名，数字时间戳等机制避免对行为发生的抵赖。

i） 抗重放：提供抵御重放攻击的机制。

j）可用性：确保物联网应用层的信息和服务在任何时间都可以提供给合法用户，可通过数据备份等实现。

表3应用层的脆弱性、安全威胁与对应的安全需求

	窃听	篡改	业务滥用	隐私泄露	重放攻击	拒绝服务攻击	抵赖攻击
完整性		√					
机密性	√			√			
认证			√			√	
隐私保护				√			
抗重放					√		
不可抵赖性							√

7.5 运维管理方面的安全需求

基于物联网所构建的信息系统或控制系统主要面临的安全问题包括对海量末端节点的有效管理及跟踪控制，包括：对信息系统数据库信息的保护，防泄露、篡改或非授权使用；通过安全可靠通信确保

对末端节点的有效跟踪及控制;确保信息系统或控制系统采集的末端节点信息及下达的决策控制信息的真实性，防篡改、假冒或重放；对信息系统及控制系统的安全审计等。

因此，物联网络中控制管理方面的安全需求包括：

a） 远程配置更新末端节点上软件应用时应当提供安全保护；

b） 只有经过授权的软件应用才能被下载到末端节点上；

c） 只有合法用户可以通过外部接口提交关于末端节点的信息更改请求；

d） 提供统一的安全管理平台，保证平台上敏感信息的完整性。

7.6 物联网层间安全需求

物联网层间主要面临的安全问题是：层间的敏感信息可能在边界处无法受到保护，并且应用层实体的身份合法性在网络层无法得到验证，以及层内敏感信息可能扩散至其他层中导致信息泄露。因此，物联网层间安全需求包括：

a） 保证物联网各层之间传输的敏感信息的完整性和机密性；

b） 物联网应用层访问网络层时需要进行身份认证和授权；

c） 保证物联网各层内部敏感信息不扩散至其他层。

附录A
（资料性附录）
物联网安全需求总结

基于物联网不同层次上的安全问题及安全需求如表A.1。

表A.1 物联网安全问题与安全需求

类别	分类或特点	安全威胁和问题	安全需求
末端节点	物联网终端、物联网端节点、物联网接入网关等	a) 非授权读取或篡改末端节点信息 b) 物理俘获或逻辑攻破，使不工作 c) 假冒末端节点 d) 末端节点的自私性威胁 e) 木马、病毒、垃圾信息的攻击 f) 与用户身份有关的信息泄露：如个人信息、使用习惯、用户位置等	a) 物理安全防护 b) 针对有卡的设备，需要采取措施防止将UICC或者SIM卡非法拔出或者替换 c) 防病毒、防火墙措施需求 d) 访问控制 e) 认证需求 f) 不可抵赖性 g) 机密性需求 h) 数据完整性需求 i) 可用性需求 j) 私密性需求
感知延伸层	低功耗、分布松散、信令简练、协议简单、广播特性、少量交互甚至无交互	a) 传输威胁：中断、拦截、篡改、伪造、重放 b) 拒绝服务 c) 路由攻击	a) 机密性 b) 数据源点认证 c) 设备认证 d) 完整性 e) 可用性 f) 时效性
通信网络	有线、无线及卫星信道等	a) 隐私的泄露：从物理不安全的设备中获得用户身份等的隐私信息，并以此设备对通信网络进行一些攻击 b) 传输的安全问题：机密性威胁、完整性威胁 c) 大量物联网设备接入带来的问题： – 网络拥塞和Dos攻击 – 密钥问题：在物联网比传统手机终端多得多的条件下，逐一认证产生密钥的方式会给网络带来大量的资源消耗 d) 感知网络和通信网络安全机制之间的融合会带来的问题 e) 中间人攻击、伪造网络消息	a) 总体安全需求：在网络的通信网络的总体安全需求不得低于一般通信网络的安全需求 b) 机密性 c) 完整性 d) 隐私性 e) 组认证：群组设备的认证可以通过认证代理或物联网接入网关或主设备来完成 f) 认证的一般需求：设备和网络的互认证可以采用多种认证方式 g) 密钥的一般需求：共享密钥等
应用层	人与物、物与物之间信息交换的各行业应用； 服务于广大群众的物联网应用等；如： 智能城市、智能交通、智能物流、	a) 隐私威胁：如隐私泄露或恶意跟踪 b) 业务滥用：非法用户使用未授权业务或合法用户使用未定制的业务 c) 身份冒充：假冒人、假冒设备、伪造客户端或应用服务器发送数据、执行操作等	a) 身份认证及访问控制 b) 业务认证 c) 组认证 d) 隐私保护：保护行为或者通信信息不泄露 e) 机密性 f) 完整性 g) 密钥的安全性

	智能环境监控、智能社区及家居、智能医疗等	d) 应用层信息窃听/篡改 e) 抵赖和否认：抵赖和否认曾经完成的操作或承诺 f) 重放威胁 g) 拒绝服务攻击	h) 防抵赖 i) 防重放
运维管理方面	海量末端节点信息管理及控制	a) 远程配置、更新末端节点上的软件应用问题：提供对远程配置、更新时的安全保护能力，并防止病毒、蠕虫等恶意攻击软件 b) 配置末端节点特征时的安全问题；伪造用户，虚假更新请求，导致终端不可用。 c) 安全管理问题： 在物联网环境中，由于物联网终端无人值守，且规模庞大，对这些末端终端的日志等安全信息进行管理是个新问题	a) 远程配置更新末端节点上软件应用时应当提供安全保护 b) 只有经过授权的软件应用才能被下载到末端节点上 c) 只有合法用户可以通过外部接口提交关于末端节点的信息更改请求。 d) 提供统一的安全管理平台
物联网层间安全需求	物联网在逻辑功能上划分成感知延伸层、网络层及应用层。	a) 层间的敏感信息可能在边界处无法受到保护 b) 应用层实体的身份合法性在网络层无法得到验证， c) 层内敏感信息可能扩散至其他层中导致信息泄露	a) 保证物联网各层之间传输的敏感信息的完整性和机密性； b) 物联网应用层访问网络层时需要进行身份认证和授权； c) 保证物联网各层内部敏感信息不扩散至其他层。

YDB XXX –201X

中国通信标准化协会标准

物联网安全需求

YDB XXX –201X

*