国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X.1365

(03/2020)

X系列：数据网、开放系统通信和安全性

安全应用和服务(2) – 物联网（IoT）安全

在电信网络上使用基于身份的密码来支持物联网服务的安全方法

ITU-T X.1365 建议书

国际电信联盟

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	**X.1360–X.1369**
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
分布式账簿技术安全	X.1430–X.1449
安全协议（2）	X.1450–X.1459
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1365 建议书

在电信网络上使用基于身份的密码来支持物联网（IoT）服务的安全方法

摘要

ITU-T X.1365建议书为支持包括身份管理、密钥管理架构、密钥管理操作和鉴权机制在内的电信网上的物联网服务的IBC公钥技术的使用提供了一种安全方式。

传统的基于证书的安全方法涉及包括证书分发、查询和撤销在内的重量级密钥管理操作。此类系统在跟上日益增加的接入物联网（IoT）设备的步伐的同时维持良好性能方面面临巨大的困难。

基于身份的密码（IBC）技术是使用实体身份作为公钥的另一种安全方法。物联网的一个关键特征是所有物品都拥有一个唯一标识符（ID）。采用这些标识符作为公钥无需使用证书。因此，IBC安全解决方案采用更简便的密钥管理，使分散的管理机构能够控制自身设备并大量扩展至庞大数量的端点和各类设备。

沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1365	2020-03-26	17	11.1002/1000/14089

关键词

物联网（IoT）、基于身份的密码（IBC）、安全方法、用户数据安全。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1365 建议书

在电信网络上使用基于身份的密码来支持物联网（IoT）服务的安全方法

1 范围

本建议书为使用支持电信网络上物联网（IoT）服务的基于身份的密码（IBC）技术规定了安全方法。该安全方法包括设备识别、私钥发放、公共参数查询和鉴权协议机制。

注：本方法不仅限于物联网服务，其他服务亦可使用。

2 参考文献

下列ITU-T建议书及含有本建议书引用条款的其它参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其它参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其它参考文献的可能性。ITUT-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

[IETF RFC 4764] IETF RFC 4764 (2007), *The EAP-PSK protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method*.

[IETF RFC 5091] IETF RFC 5091 (2007), *Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems*.

[IETF RFC 5216] IETF RFC 5216 (2008), *The EAP-TLS Authentication Protocol*.

[IETF RFC 5280] IETF RFC 5280 (2008), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[IETF RFC 5408] IETF RFC 5408 (2009), *Identity-Based Encryption Architecture and Supporting Data Structures*.

[IETF RFC 5480] IETF RFC 5480 (2009), *Elliptic Curve Cryptography Subject Public Key Information*.

[IETF RFC 5958] IETF RFC 5958(2010), *Asymmetric Key Packages*.

[IETF RFC 6507] IETF RFC 6507 (2012), *Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)*.

[IETF RFC 6508] IETF RFC 6508 (2012), *Sakai–Kasahara Key Encryption (SAKKE)*.

[IETF RFC 6960] IETF RFC 6960 (2013), *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*.

[IETF RFC 7250] IETF RFC 7250 (2014), *Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*.

[IETF RFC 8446] IETF RFC 8446 (2018), *The Transport Layer Security (TLS) Protocol Version 1.3*.

[ISO/IEC 11770-3] ISO/IEC 11770-3:2015, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques*.

[ISO/IEC 14888-3] ISO/IEC 14888-3:2018, *IT Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms*.

[ISO/IEC 18033-5] ISO/IEC 18033-5:2015, *Information technology – Security techniques – Encryption algorithms – Part 5: Identity-based ciphers*.

3 定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语：

3.1.1 身份提供商（identity provider）[b-ITU-T Y.2720]：创建、维护和管理其他实体（如，用户/订阅用户、组织和设备）的可信身份信息的实体，它基于信任、服务和其他类型的关系提供基于身份的服务。

3.1.2 标识符（identifier）（ID）[b-ITU-T E.101]：用来标识某个订阅用户、用户、网络元素、功能、网络实体、业务或应用的数位、字符和符号系列。标识符可用于注册或授权。标识符中有所有网络的公众标识符或特定网络的专用标识符（专用ID通常不披露给第三方）。

3.1.3 主公钥（master public key）（MPK）[ISO/IEC 18033-5]：由对应主密钥唯一决定的公共值。

3.1.4 主密钥（master secret key）（MSK）[ISO/IEC 18033-5]：私钥生成器使用的用于为基于身份的密码（IBE）算法计算私钥的秘密值。

3.1.5 私钥生成器（private key generator）（PKG）[ISO/IEC 18033-5]：生成一套私钥的实体或功能。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 身份域（identity domain）：共享同一套公共参数和身份命名规则的实体的集合。

3.2.2 公共参数（public parameter）：用于加密计算的参数之一，包括从一系列特定加密方案或函数中，或从一系列数学空间和主公钥 中精选出的一个特定的加密方案或函数。

3.2.3 公共参数服务器（public parameter server）：根据要求提供公共参数的实体。

3.2.4 安全模块（security module）（SecM）：安全地执行加密机制并提供安全业务的软件或硬件, 或软件和硬件的组合。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

4G 第四代

5G 第五代

AuC 鉴权中心

AGW 集总网关

AK 鉴权密钥

AKA 鉴权的密钥协议

AN 接入节点

AS	接入系统
ASN.1	抽象句法记法一
AU	鉴权单元
BN	Barreto-Naehrig
BLS-12	Barreto-Lynn-Scott嵌入次数12
BLS-24	Barreto-Lynn-Scott嵌入次数24
CRL	证书撤销列表
DER	唯一编码规则
EAP	可扩展鉴权协议
ECCSI	用于基于身份加密的椭圆曲线无证书签名
EID	eUICC-ID
EIS	eUICC信息集
eUICC	嵌入式通用集成电路卡
EUM	eUICC制造商
GW	网关
HSM	硬件安全模块
HTTP	超文本传输协议
IBAKA	基于身份的鉴权密钥协议
IBC	基于身份的密码
IBE	基于身份的加密
IBS	基于身份的签名
ID	标识符
IdP	身份提供商
IMSI	国际移动订阅身份
IoT	物联网
ISP	物联网服务平台
IRL	身份撤销列表
ISD	发布者安全域
KDF	密钥推导函数
KDK	密钥推导密钥
KEK	密钥加密密钥
KEM	密钥封装机制
KMIP	密钥管理互操作性协议
KMS	密钥管理业务
KPAK	KMS公共鉴权密钥
KSS-16	Kachisa-Schaefer-Scott嵌入次数16
KSS-18	Kachisa-Schaefer-Scott 嵌入次数18

LTE	长期演进
LTE-M	长期演进，类别M1
MAC	媒体接入控制
MNO	移动网络运营商
MSK	主密钥
NB-IoT	窄带物联网
OCSP	在线证书状态协议
OID	对象标识符
OISP	在线身份状态协议
PKG	私钥生成器
PKI	公钥基础设施
PPS	公钥参数服务器
PVT	公钥验证令牌
RSF	撤销服务器函数
SecM	安全模块
SK	Sakai-Kasahara
SM-DP	订阅管理器数据准备
SM-SR	订阅管理器安全路由
SOK	Sakai-Ohgishi-Kasahara
SSK	秘密签名密钥
TLS	传输层安全性
TLV	标签、长度和矢量
TVP	时变参数
UE	用户设备
UICC	通用集成电路卡

5 惯例

无。

6 概述

根据[b-ITU-T Y.4000]第6.1款，物联网（IoT）“可以视为信息社会的全球基础设施，可在现有的和不断出现的互操作信息通信技术（ICT）基础上，通过物物连接（物理的和虚拟的）实现先进的业务。”由于设备无处不在的特性加上用户数据日益增加的敏感度，物联网的安全成为最重要的关切。[b-ITU-T Y.4100]描述了物联网的高级别共同安全要求，包括通信安全、数据管理安全、业务提供安全，以及相互鉴权和授权。[b-ITU-T X.1361]进一步分析了物联网环境中的威胁和挑战，并描述了能够应对和减轻这些威胁和挑战的能力。[b-ITU-T X.1361]定义的必要的安全能力包括：

– 支持安全、可信和隐私保护的通信的安全通信能力；
– 支持安全通信的安全密钥管理能力；
– 提供安全、可信和隐私保护的数据管理的安全数据管理能力；
– 鉴权设备的鉴权能力；
– 授权设备的授权（访问控制）能力；
– 实施基于轻量密码算法的安全协议的能力。

物联网设备以资源（诸如计算和通信能力）的限制为特征。物联网设备的性质给满足物联网系统的安全要求带来新挑战。在考虑物联网安全解决方案时，容易部署、轻量管理操作和分布式认证是尤为重要的因素。

正如[b-ITU-T X.1361]所述，鉴权、访问控制以及数据完整性和保密性是确保物联网安全所需的必不可少的业务。对称密钥和公共密钥密码机制均能够用于提供此类服务。

基于对称密钥的安全解决方案相对简单。然而，该方案并不十分适合点对点场景，例如物联网中没有线上业务作为信任代理或者未在设备之间成对预共享秘密的机器对机器应用中。不对对等方暴露用户机密的跨系统安全通信亦十分复杂。

传统的基于证书的公钥密码解决方案涉及包括证书分发、查询、分配、验证和撤销在内的重量密钥管理操作。此类系统在跟上日益增加的接入物联网（IoT）设备的步伐的同时维持良好的性能方面面临巨大的困难。在安全协议中交换证书的开销亦带来问题，尤其是在分组数据单元较小的窄带物联网（NB-IoT）网络中。

基于身份的密码（IBC）是另一类型的技术。该技术采用一个实体的身份作为一个公钥。物联网的一个关键特征是所有物品都有一个唯一标识符（ID）。采用这些标识符作为公钥无需使用证书。因此，IBC安全解决方案采用更简便的密钥管理，推动分散的管理机构控制自身设备并大量扩展至庞大数量的端点和各类设备。由于无需传输证书，安全协议可被更高效地执行。

在IBC系统中，被称为密钥管理业务（KMS）的受信方负责生成每个实体的私钥。在提供私钥生成业务之前，KMS通过调用一个**IBSetup**函数启动一个系统初始化流程，被给予一个安全参数，确定一套系统参数并生成一个主密钥（MSK）和一个主公钥（MPK）。注意，KMS与私钥生成器（PKG）的函数相同。因此，为了表述方便，在本建议书中交替使用KMS和PKG，且系统函数和MPK的组合被称为公共参数。KMS使MSK保持严格保密，并使公共参数公开可获得。如有需要，公共参数可由专用服务公共参数服务器（PPS）发布。

一个典型的IBC安全系统可使用包括基于身份的加密（IBE）、基于身份的签名（IBS）和基于身份的授权密钥协议（IBAKA）在内的一系列IBC机制来提供包括数据保密性、实体鉴权和安全信道建立在内的各类安全业务。所有这些IBC算法可被视为两套函数的组合。一套函数由密钥生成函数构成，该函数生成基于身份的公共和私钥对。私钥生成函数（**IBExtract**）从一个ID、MSK和公共参数中生成一个私钥。身份公钥导出函数（**IBDerivate**）从一个ID和公共参数中计算出一个公钥。另一套函数，例如加密或解密（**IBEnc/IBDec**）、签名或验证（**IBSign/IBVerify**）和授权会话密钥建立协议，使用生成的密钥对来完成对应的密码操作。

IBC技术已经被包括国际标准化组织（ISO）、国际电工委员会（IEC）、互联网工程任务组（IETF）、电气和电子工程师协会（IEEE）、欧洲电信标准学会（ETSI）和中国国家标准化管理委员会（SAC）在内的各类标准制定组织标准化。参考书目中提供了这些组织制定的一些相关标准的列表。OneM2M也正在考虑在Release 4中使用IBC技术用于物联网网络，其安全性分析见[b-ETSI TR 118 508]。

本建议书为使用IBC技术来为电信网络的物联网服务提供安全能力描述了一个安全框架。该框架涵盖了身份管理、密钥管理架构、密钥管理操作和鉴权，以及使用IBC的密钥协商协议等方面。

7 电信网络物联网服务系统参考架构

本条款提供了电信网络物联网服务的通用系统参考架构。图1展示了物联网服务的概念系统参考架构。该系统由三个域组成：物联网设备、接入系统（AS）和物联网服务平台（ISP）。

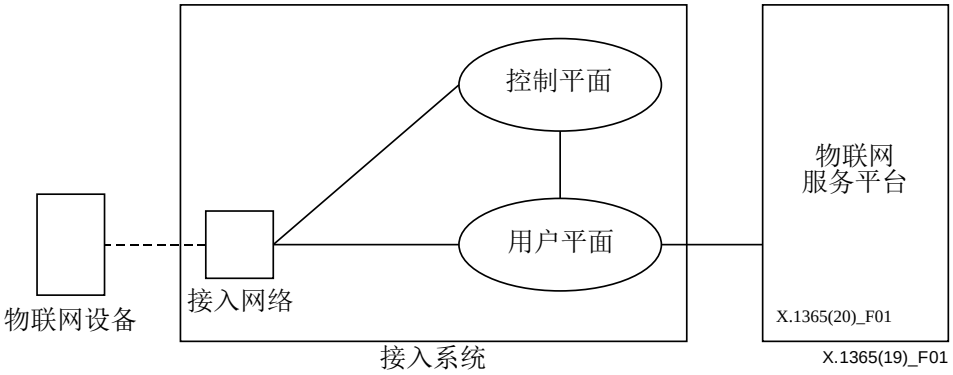


图1 – 物联网服务概念系统架构

物联网设备负责数据收集或者执行操作。大部分物联网设备可与一个电信系统建立联系，并与ISP通信。如今，大部分物联网设备通过在电信网络建立的无线链接连接至ISP。在本建议书中，AS指的是电信网络。它通常由两部分构成：接入网络（AN）和核心网络。核心网络可进一步细分为两部分：控制平面和用户平面，分别用于控制信令和数据传输。

作为一种传统的无线连接，电信网络已经被使用了多代。历史上来看，电信网络被设计用于支持人类的以无缝漫游为特征的移动通信。近些年，从第四代（4G）长期演进（LTE）网络开始，在设计中亦考虑到支持物联网设备。例如，在4G-LTE中，类别M1（LTE-M）和NB-IoT技术都被开发用于支持物联网设备。

今天的大部分电信系统都由三个部分构成，即终端或用户设备（UE）、一个接入网络和核心网络。在此，假设接入网络和核心网络均属于图1中展示的接入系统。物联网服务通常在电信网络之外，带有一些用于数据传输和服务管理的接口。为了给物联网服务提供更好的支持，电信网络正在将更多的特定物联网设计包含在其系统规范中。电信网络和物联网服务之间的集成在近些年已经变得更加紧密。

伴随着为第五代（5G）网络开发的系统规范，公钥技术被支持用于物联网服务，包括网络接入鉴权。正如第6款所说，与其他公钥技术相比，IBC管理更为简单，传输效率更高。因此，将IBC用于电信网络的物联网服务需要将其规范作为现有规范的补充标准。

8 对电信网络物联网服务使用基于身份的密码的框架

本条款提供了电信网络物联网服务使用IBC公钥技术的框架。该框架包含一个包括在使用IBC技术时所需的必要网络组件在内的系统架构。不仅如此，还规定了IBC的密钥管理框架，因为这对于使用IBC技术的系统来说至关重要。本框架亦涉及其他关键问题，例如密钥管理、身份命名和鉴权协议。

8.1 基于身份的密码的物联网系统架构

对于通过电信网络运行物联网服务，IBC可被用于网络接入鉴权或业务接入鉴权，或二者同时鉴权。网络接入鉴权处理是否允许设备接入网络，而业务接入鉴权处理是否允许设备接入一个ISP。

物联网设备可直接或间接接入电信网络。因此，共有两种接入模式：

– 直接连接模式：物联网设备直接与AS连接；

– 间接连接模式：物联网设备通过一个集总网关（AGW）连接至AS。

图2显示了一个将IBC用于AS和ISP安全保护的物联网系统参考架构。从安全的角度来看，AS和ISP对于物联网服务均有各自的安全要求。考虑到安全证书可由AS或者ISP提供，使用IBC用于物联网网络有三种场景，如下所示：

– 在AS安全保护场景中使用IBC：

  在这一场景下，存储在物联网设备的网络接入的安全证书由AS提供和管理。物联网设备在连接至AS时被其鉴权。例如，一台物联网设备基于AS提供的私钥计算IBS签名并发送签名至AS。相应的，AS可基于鉴权信息中提供的IBS签名鉴权物联网设备。如果验证成功，AS从物联网设备发送数据至物联网服务器；

– 使用IBC用于ISP安全保护：

  存储在物联网设备中的用于业务接入的IBC证书由ISP提供和管理。物联网设备由ISP基于使用IBC证书生成的签名鉴权；

– 在AS和ISP安全保护场景中均使用IBC：

  存储在物联网设备中的IBC安全证书由AS或ISP或二者共同提供和管理。物联网设备可由AS和ISP使用同一套证书进行鉴权。

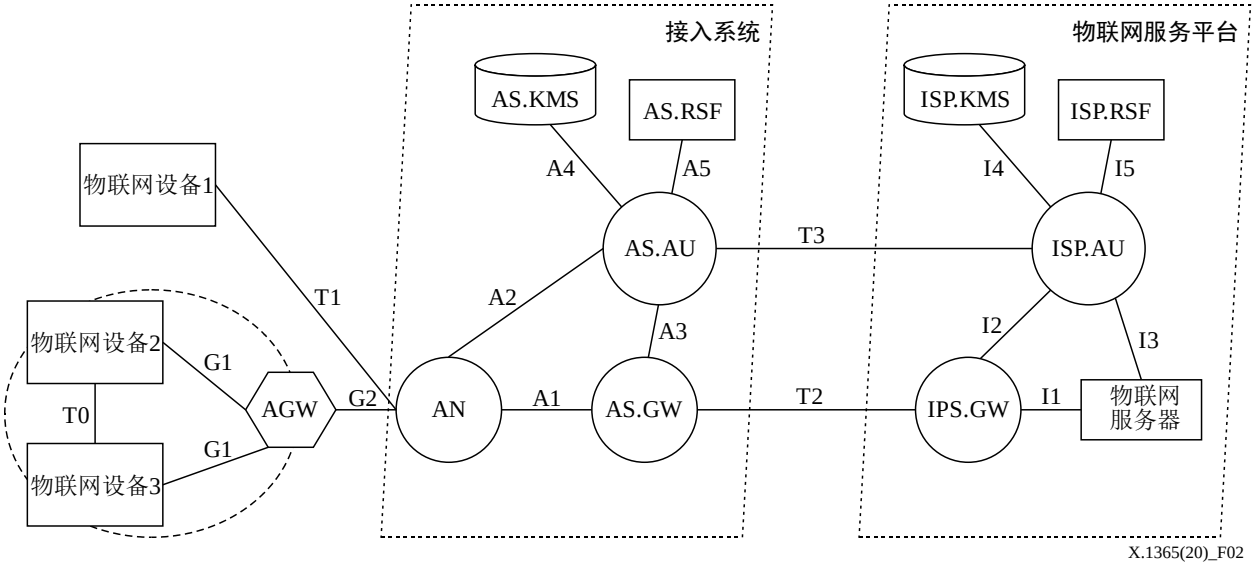


图2 – 接入系统和物联网服务平台安全保护场景中的基于身份密码的物联网系统架构

上述三种场景覆盖了用于网络和业务接入的IBC的大部分使用案例。然而，本建议书范围之外的其他场景亦可能存在。

基于IBC的物联网系统架构由以下网络函数（NF）和设备构成：

– 接入系统（AS）：接入物联网设备或AGW的系统，包括接入节点（AS.AN）、密钥管理系统（AS.KMS）函数、鉴权单元（AS.AU）、撤销服务器功能（AS.RSF）和网关（AS.GW）；

– 物联网服务平台（ISP）：用于物联网服务管理的平台，包括密钥管理系统函数（ISP.KMS）、鉴权单元（isp.au）、撤销服务器函数（ISP.RSF）、网关（ISP.GW）和物联网服务器。ISP须支持密钥管理、分配、身份鉴权、加密或解密，以及签名签署或验证等；

– 集总网关（AGW）：负责物联网设备连接、集总和发送所有物联网设备数据至AS的聚合节点。AGW发挥物联网设备和AN之间数据传输的代理作用；

– 接入节点（AN）：物联网设备或AGW的接入节点，可以是无线或者固网接入点；

– 密钥管理系统（KMS）函数：负责IBC密钥和物联网设备及网络函数参数的密钥的生成、分配和更新的管理系统；

– 鉴权单元（AU）：AU基于IBC系统对物联网设备进行鉴权；

– 撤销服务器函数（RSF）：维护身份撤销列表（IRL）的服务器。撤销列表中的公钥或身份被排除在使用之外；

注 – AS和ISP均可能拥有各自的KMS、AU和RSF；

– 接入系统网关（AS.GW）：连接至物联网GW的网元，负责物联网用户数据传输；

– 物联网网关（IoT GW）：负责转发或汇集数据并传输数据至物联网服务器，或从物联网服务器向物联网设备转发数据/信令的GW；

– 物联网服务器：位于物联网服务提供商侧的服务器，从物联网GW收集物联网数据；
– 物联网设备：用于数据收集和与AN以及物联网服务器建立连接的终端设备，提供包括密钥协商、加密或解密，和签名签署或验证在内的数据保护。

图2显示的参考点的函数描述如下：

– G1：物联网设备和AGW之间的参考点，用于鉴权和安全通信；
– G2：AGW和AN之间的参考点，用于AGW和AN之间的信令和数据通信；
– T0：物联网设备之间的参考点，用于信令和数据交换；
– T1：物联网设备和AN之间的参考点，用于鉴权和安全通信；
– T2：AS.GW和ISP.GW之间的参考点，提供AS.GW和ISP之间的用户平面数据隧道；
– T3：AS.AU和ISP.AU之间的参考点，用于信令交换，包括身份交换或密钥提供；
– A1：AN和AS.GW之间的参考点，用于用户平面数据隧穿；
– A2：AS.AU和AN之间的参考点，用于控制平面信令；
– A3：AS.AU和AS.GW之间的参考点，用于AS中的GW分配和管理协议；
– A4：AS.AU和AS.KMS之间的参考点，用于AS中的密钥提供协议；
– A5：AS.AU和AS.RSF之间的参考点，用于AS中的身份或密钥撤销协议；
– I1：物联网服务器和ISP.GW之间的参考点，用于用户平面数据隧穿；
– I2：ISP.AU和ISP.GW之间的参考点，用于ISP中的GW分配和管理协议；
– I3：ISP.AU和物联网服务器之间的参考点，用于信息交换，例如从物联网服务器传输至与ISP.AU的业务相关订阅信息、ISP.AU至物联网服务器的鉴权通知信息；
– I4：ISP.AU和ISP.KMS之间的参考点，用于ISP中的密钥提供协议；
– I5：ISP.AU和ISP.RSF之间的参考点，用于ISP中的身份或密钥撤销协议。

8.2 密钥管理架构

本条款描述了在物联网中使用IBC机制时支持密钥管理所需的函数架构。基于物联网设备是否嵌入有通用集成电路卡（eUICC）[b-GSMA SGP.02]组件，考虑使用两类密钥管理架构：1)嵌有eUICC的物联网设备的IBC和2)未嵌有eUICC的物联网设备的IBC。

如果在嵌有eUICC的物联网设备上使用IBC，则架构通过增加两个新的函数实体（即KMS和PPS）遵守[b-GSMA SGP.02]规定的通用eUICC远程提供的架构。该案例进一步分为以下两个子案例，取决于KMS的位置。

1) KMS由负责移动网络运营商（MNO）的实体进行管理 – 见图3；
2) KMS由负责订阅管理器数据准备（SM-DP）的实体进行管理 – 见图4。

在两个子案例中，当MNO发出一个文件命令时，就会生成包括私钥和公共参数在内的密钥。这些密钥之后在根据[b-GSMA SGP.02]中当前有效的远程密钥提供规范在安装时被远程提供给eUICC设备。eUICC远程提供的规则、相关函数和接口的详情见[b-GSMA SGP.02]。eUICC中的这些密钥的文件规格、存储格式和使用在本建议书的范围之外。

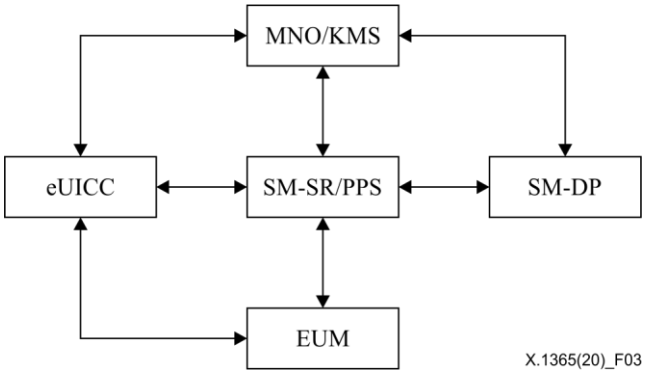


图3 – 装有嵌入式通用集成电路卡的物联网设备基于身份的密码密钥管理架构A

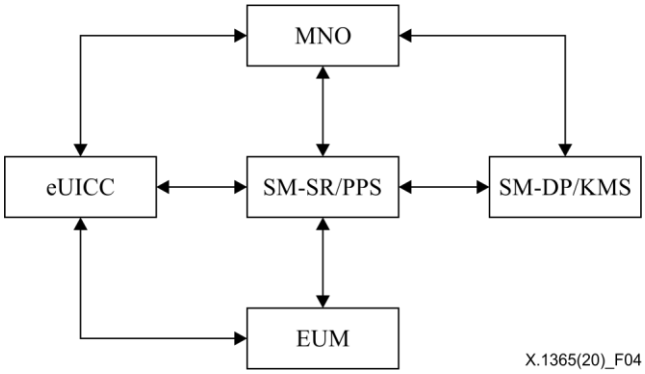


图4 – 装有嵌入式通用集成电路卡的物联网设备基于身份的密码密钥管理架构B

图5提供了在未嵌有eUICC的物联网设备中使用IBC的通用架构，其组件如下：

– SecM：一个安全模块（SecM）表示一个可安全地存储密钥和使用存储的密钥执行安全机制来完成安全操作的单元。一台物联网设备须拥有一个SecM。

– IdP：一个身份提供商（IdP）是一个创建、维护和管理身份信息的实体。

– AuC：鉴权中心（AuC）以提供实体鉴权为业务。

IdP依靠AuC提供的鉴权业务鉴权物联网设备。在初始鉴权流程之后，IdP为SecM提供包括身份创建、指定、替换和撤销在内的业务。在新身份创建并被指定给一台物联网设备之后，IdP调用KMS提供的私钥生成业务来生成与最新分配的ID相应的私钥并将私钥安全地分配给SecM。IdP亦从KMS中提取公共参数并将参数馈送至向外部实体发布公共参数的PPS。IdP还可以通过执行特定的SecM鉴权协议（包括本建议书定义的鉴权协议在内）对其他实体提供鉴权业务。

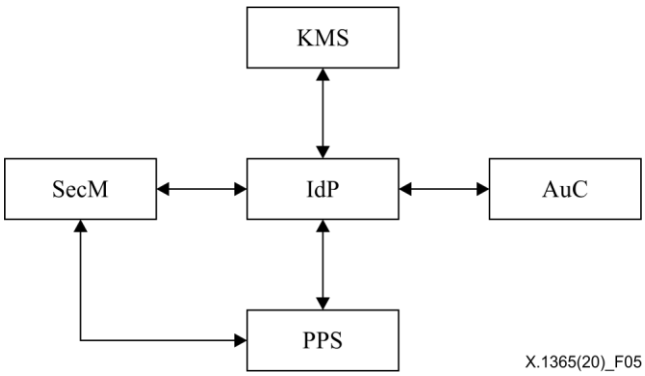


图5 – 未带有嵌入式通用集成电路卡的物联网设备基于身份的密码密钥管理架构

8.3 身份命名

当采用IBC技术用于电信网络的物联网服务时，身份命名能够提供有用信息来帮助运营商管理网络。各类信息，例如业务类型、位置、设备ID和有效时间可被嵌入至一个实体中。当使用IBC技术时需要使用部分信息，例如有效时间。使用身份信息，运营商能够优化网络管理，例如，基于业务类型为具体网络片段分配连接。基于设备位置信息来定位设备也十分简单。附录I提供了身份定义的例子。

8.4 密钥管理

除了身份值以外，IBC系统还涉及三种类型的密码密钥值：MSK、公钥参数和私钥。附件B提供了这些密钥结构的抽象句法记法一（ASN.1）定义。

为管理这些密钥，IBC系统采用五个密钥管理操作：

1) 系统初始化操作；
2) 设备初始化；
3) 公共参数查找；
4) 身份和密钥提供；
5) 身份和密钥撤销。

可使用密钥管理互操作性协议（KMIP）[b-OASIS KMIP]在管理实体和KMS之间交换信息。然而，KMIP满足**IBSetup**和**IBExtract**函数的新要求所需的扩展需要定义。对于带有eUICC的物联网设备来说，[b-GSMA SGP.02]采用远程密钥提供的标准流程。对于非eUICC物联网设备，SecM和管理实体之间互动的协议被基于超文本传输协议（HTTP）定义。这些操作的规范见附件C。

这些系统初始化操作通过生成MSK和公共参数来初始化IBC系统。IBC系统初始化流程被假设由管理实体，例如IdP、SM-DP或MNO来负责。其建立一个与KMS实体之间执行**IBSetup**函数的安全信道。双方采用创建密钥对操作来执行KMIP。管理实体为KMS调用**IBCSetup**函数和生成MSK和公共参数提供必要信息。KMIP被扩展以支持建立函数，包括各类标准化的IBC算法的函数。这些操作的详情见第C.1款。

设备初始化操作是为了让物联网设备为身份和密钥提供做好准备。有两种情况：有eUICC物联网设备的初始化和无eUICC物联网设备的初始化。对于带有eUICC的设备，需要eUICC在订阅管理器安全路由（SM-SR）完成注册，从而使其为文件下载[b-GSMA SGP.02]做好准备。对于标准eUICC设备无额外操作要求。对于非eUICC物联网设备，SecM应首先在AuC注册以获得一个提供ID（PROV.ID）和提供证书（PROV.CRED）。PROV.ID/PROV.CRED被用于身份/密钥提供流程的实体鉴权。若物联网设备无法使用传输层安全协议（TLS）与IdP建立安全信道，则设备初始化期间进一步要求在SecM中安装属于IdP的密钥身份IdP.ID或相关公钥IdP.PUK。这些操作的详情见第C.2款。

公共参数查找操作是为了读取IBC公共参数。物联网设备须使用身份和密钥提供流程来获取其所属的IBC系统的公共参数。可遵照[IETF RFC 5408]第4款定义的规格从已知PPS中读取另一个IBC系统的公共参数。这些操作的详情见第C.3款。

身份和密钥提供操作包括身份指配、私钥提取和密钥分配流程。物联网设备在初始化流程之后仅有一个临时身份。IdP或SM-DP或MNO应确定为提出请求的设备指派哪个身份，之后与KMS通信以生成相应的私钥，并最终安全地分配实体、私钥和公共参数至设备。这些操作的详情见第C.4款。

当严格的安全政策要求身份必须被即时撤销时使用身份和密钥撤销。若一个身份被撤销，则该身份须被设置为已撤销状态。若输入询问已撤销身份的状态，IdP或SM-DP或MNO须按照在线身份状态协议（OISP）的定义返回正确的值。欲更加高效地查找一批身份状态，实体可定期从IdP或SM-DP或MNO读取IRL并将其存储在本地，实体无需在线查询每个实体的状态即可查询新鲜IRL以确定一个实体是否被撤销。这些操作的详情见第C.5节。

8.5 鉴权

鉴权是确定实体（设备或用户）是否有权接入某些资源的流程。在电信网络中，有两种与物联网设备相关的鉴权类型：网络接入鉴权和业务鉴权。网络接入鉴权处理是否允许设备接入网络，而业务鉴权则处理设备是否能够接入ISP。

基于IBC技术建立的鉴权协议适用于电信网络中的物联网鉴权。这是由于IBC能极大地减轻对于大量物联网设备的身份和密钥管理的负担。IBC的另一个优势是使分布式鉴权成为可能，这不仅能够大幅减少鉴权时间，还可以用于新的应用场景，例如设备到设备鉴权、车辆到车辆鉴权。对于当前的电信网络，例如4G LTE网络来说，IBC能够被用于物联网设备和ISP之间的鉴权。对于5G蜂窝网络来说，IBC可被用于网络接入鉴权和业务接入鉴权。当前对于5G安全性的规范 — [b-ETSI TS 133.501]规定了支持可扩展的鉴权协议（EAP）方式的统一鉴权框架。[b-ETSI TS 133.501]的附件进一步规定了在5G网络如何使用EAP-TLS用于物联网网络。

EAP框架是开放的，并支持包括EAP-TLS在内的多个鉴权协议。EAP鉴权方式可支持对称式和非对称式密钥。

作为一种相对较新的公钥技术，IBC在现有的鉴权协议中未获得很好的支持。因此，在附件D中，四种现有的协议被修订，以支持对IBC的鉴权：

1） 第D.1款：一次处理的秘密传输协议[ISO/IEC 11770-3]；

2) 第D.2款：带有原始公钥的TLS [IETF RFC 8446]；

3) 第D.3款：EAP-TLS [IETF RFC 5216]；

4) 第D.4款：EAP-PSK [IETF RFC 4764IETF RFC 4764]。

9 安全要求

本建议书仅关注在物联网中使用IBC的安全要求。物联网的通用安全威胁和要求见[b-ITU-T X.1361]规定。作为一个密码系统，最重要的安全问题就是所使用的公钥的完整性和可靠性，以及使用的长期和临时密钥的保密性。IBC系统涉及以下部件：MSK、公共参数、ID、私钥和用于密码操作的临时密值。

9.1 对主密钥的安全要求

所有私钥均由MSK生成。尤其是，若MSK被破解，攻击者就可以重建任何实体的私钥，从而破解受到相应公钥保护的所有信息或仿冒任何实体。任何对MSK的非法访问都可能损害IBC系统的安全性。因此，MSK须被存储在防护环境，例如硬件安全模块（HSM）中。任何对于密钥的访问都应由强安全机制鉴权。

9.2 对公共参数的安全要求

公钥从公共参数和带有**IBDerivate**操作的ID计算得出。因此，使用攻击者生成的一套错误的公共参数来加密信息或验证签名会导致对于加密信息的保密性的破解，或得出对签名发起人的错误结论。因此，公共参数须通过安全信道或在有效签名的情况下传输。实体在接受公共参数之前须验证安全信道的对等实体或可信公钥的验证签名的有效性。

9.3 对标识符的安全要求

在物联网中，每个实体都拥有一个ID。若相同ID被分配给超过一个实体而对应的私钥被提供给每一个实体，会导致敏感信息泄露或假冒攻击。因此，每台设备须被指配一个独一无二的ID。

9.4 对私钥的安全要求

若物联网设备的安全环境被攻破，私钥就可能泄露。因此，私钥须通过安全信道分发，并存储在一个安全的环境中。

9.5 对临时密值的安全要求

若物联网设备的安全环境被攻破，则临时密值，例如用于加密或签名流程的随机密值就可能泄露。因此，须保证临时密值的随机性。

附件A

基于身份的密码的通用公式和算法

（本附件是本建议书不可分割的组成部分。）

本附件提供了IBC的通用公式和本建议书支持的IBC算法列表。遵守这一通用公式但未在下文列出的算法在未来也可作为对该框架的扩展方便地补充进来。在此规定的通用公式亦对相关附件B到附件D中定义的密钥数据结构、密钥管理操作以及鉴权和密钥建立协议的描述提供指导。

IBC密码系统涉及以下密钥数据类型。这些密钥的分类遵守[ISO/IEC 18033-5]：

– *ib.msk*：MSK是KMS用来计算基于身份的私钥的密值。*ib.msk*在系统初始化流程期间生成，且仅为KMS所知；

– *ib.mpk*：仅由对应MSK唯一确定的MPK。*ib.mpk*由KMS在系统初始化过程中计算得出；

– *ib.sysparam*：用于包括从一系列加密方案或函数，或一系列数学空间中精选特定加密方案或函数用于密码计算的系统参数。*ib.sysparam*由KMS在系统初始化过程中选择；

– *ib.pubparam*：公共参数是系统参数*ib.sysparam*与MPK *ib.mpk*的结合。此类型密钥被定义为国际标准（例如[ISO/IEC 18033-5]）和与IBC相关的RFC（例如[IETF RFC 5091]）提供统一视图；

– *ib.prk*：基于身份的私钥，由KMS与*ib.msk*和*ib.pubparam*生成，与标识符*ID*对应；

– *ib.pub*：基于身份的公钥，从标识符*ID*和*ib.pubparam*通过基于身份的密码方案的函数计算得出。

IBC密码系统可包含以下由输入和输出指定的函数：

IBSetup

输入：安全参数

输出：*ib.pubparam, ib.msk*

IBExtract

输入：*ib.pubparam, ib.msk, ID*

输出：*ib.prk*

IBDerivate

输入：*ib.pubparam, ID*

输出：*ib.puk*

IBEnc

输入：*ib.pubparam*、*ID*、信息*M*

输出：密文*C*

IBDec

输入：*ib.pubparam*、*ID*、*ib.prk*、密文*C*

输出：明文*M*或错误

IBSign

输入：*ib.pubparam*、*ID*、*ib.prk*、信息*M*

输出：签名*S*

IBVerify

输入：*ib.pubparam*、*ID*、信息 *M*、签名*S*

输出：有效或无效

本建议书须支持一下基于身份的算法的使用，包括：

– BB1-KEM（密钥封装机制）[IETF RFC 5091]；

– BF-IBE [IETF RFC 5091]；

– SK-KEM [IETF RFC 6508]；

– SM9-IBE [b-GM/T 0044.2]；

– Cha-Cheon-IBS (IBS2) [ISO/IEC 14888-3]；

– ECCSI（用于基于身份的加密的基于椭圆曲线的无证书签名）[IETF RFC 6507]；

– Hess-IBS (IBS1) [ISO/IEC 14888-3]；

– SM9-IBS (Chinese IBS) [ISO/IEC 14888-3]；

– Fujioka-Suzuki-Ustaoglu-AKA（经验证的密钥协议）[ISO/IEC 11770-3]；

– Smart-Chen-Cheng-AKA [ISO/IEC 11770-3]；

– SM9-AKA [b-GM/T 0044.2]；

– Wang-AKA [b-IEEE P1363.3]。

所有这些算法都基于离散对数假设，通常在椭圆曲线上的点群上执行。这些算法中的大多数亦利用椭圆曲线上[b-Galbraith]上的“密码配对”。密码配对*e*是一个高效可计算的双线性映射*e*: *G*1×*G*2→*G*3，满足方程：

$$e([a]P1, [b]P2) = e(P1, P2)^{a*b}$$

其中P1和P2分别为循环群*G*1和*G*2的产生常式。[*a*]P1表示*a*乘以P1的群运算，同样，[*b*]P2为乘以P2的群运算。

密码配对可由Weil配对、Tate配对、最佳Ate配对等在配对友好椭圆曲线[b-Freeman]上发起。通常使用的配对友好椭圆曲线包括超奇椭圆曲线、Barreto-Naehrig（BN）曲线和Barreto-Lynn-Scott嵌入式12度（BLS-12）曲线、Kachisa-Schaefer-Scott嵌入式16度（KSS-16）曲线、Kachisa-Schaefer-Scott嵌入式18度（KSS-18）曲线和Barreto-Lynn-Scott嵌入式24度（BLS-24）曲线[b-Freeman]。所有这些曲线*E*基于一个素域，一个有限素特征域p、F_p，其中P是一个素数。*G*1是曲线*E*上的点子群。*G*2或者与*G*1相同（若使用超奇曲线），或者是扭曲曲线*E*上的一个点子群。*E*从基域F_p的某个扩展域中构建。*G*3是基域的域扩展F_p^k，其中k是嵌入次数。

有的IBC算法采用其他数学机制，例如点阵（如[b-Ducas]）。这一类型的算法在计算方面非常高效，同时具备比基于椭圆曲线上的离散对数更大的密钥和输出规格。该算法同行被认为是可抵御在量子计算机上运行的攻击。然而，该类型的算法仍在发展中，因此将其标准化的考虑似乎尚未成熟，但这些基于点阵的IBC算法可被考虑在未来纳入。

附件B

基于身份的密码密钥数据说明

（本附件是本建议书不可分割的组成部分。）

使用标准ASN.1方式，[IETF RFC5408]为包括*ib.pubparam*和其他辅助信息在内的通用系统参数制定通用结构，而[IETF RFC 5091]已为两个IBE算法，即BF-IBE和BB1-IBE定义了两套密钥数据结构，包括*ib.msk*和*ib.prk*。在维护与既有定义的兼容性的同时，本建议书扩展了系统参数定义，并定义了新的密钥数据结构，以支持更多算法和与不同曲线和配对的高效应用。

通用系统参数结构定义如下。

```
IBSysParams ::= SEQUENCE {
    version                 INTEGER { v3(3) },
    domainName              IA5String,
    domainSerial            INTEGER,
    validity                ValidityPeriod,
    ibPublicParameters      IBPublicParameters,
    ibIdentityType          OBJECT IDENTIFIER,
    ibParamExtensions       [0] IMPLICIT IBParamExtensions OPTIONAL,
    signatureAlgorithm      [1] IMPLICIT AlgorithmIdentifier OPTIONAL,
    signature               [2] IMPLICIT BIT STRING OPTIONAL
}
```

IBSysParams对应[IETF RFC 5408]中定义的IBESysParams，但版本变更至v3 (3)并添加了两个额外字段。districtName和districtSerial被分别重命名为domainName和domainSerial。IBPublicParameter的定义被从OCTET STRING类型修改至最新定义的IBParameterData类型，这是由pkgAlgorithm值决定的CHOICE。该定义移除了由不必要的先前定义导致的双重编码，即，举例来说，将publicParameterData作为BFPublicParameters的一个SEQUENCE来编码，并进一步将结果作为一个OCTET STRING来编码。除了两个新增字段，其他字段的含义仍然保留[IETF RFC 5408]规定的含义不变。两个新增字段的含义如下。

– 签名算法指定用于生成签名值的签名算法。该字段可选，因为签名称段非强制。

– 签名字段包含从字段版本到*ibParamExtensions*的根据ASN.1唯一编码规则（DER）结果计算的数字签名。此字段作为BIT STRING编码并且可选。

如有，则使用签名字段帮助实体检查系统公共参数的真实性而无需借助其他方式。例如，若物联网设备无法创建[IETF RFC 5408]所要求的基于TLS的安全信道来读取其他IBC系统的公共参数，则可能使用HTTP来查询其PPS。在这种情况下，提供服务的PPS须使用其私人签署密钥对请求的公共参数进行签名。物联网设备能够验证该签名以检查响应的真实性。若一个PPS要发布另一个IBC系统的公共参数到其服务的实体上，建议将签名信息视为一个实体，采用**IBExtract**算法作为签名算法，以生成私钥作为相应签名值。以这种方式，物联网设备验证签名值是否是对应从字段版本到*ibParamExtensions*的ASN.1 DER结果的合法私钥，无需额外验证公钥以验证签名。

```
ValidityPeriod ::= SEQUENCE {
        notBefore      GeneralizedTime,
        notAfter       GeneralizedTime
}
IBPublicParameters ::= SEQUENCE SIZE (1..MAX) OF IBPublicParameter
IBPublicParameter ::= SEQUENCE {
        pkgAlgorithm            OBJECT IDENTIFIER,
        publicParameterData     IBParameterData
}
```

publicParameterData的值由pkgAlgorithm定义，可以是如下选择之一。

```
IBParameterData ::= CHOICE{
        bb1ParameterData    [0] IMPLICIT BB1PublicParameters,
        bfParameterData     [1] IMPLICIT BFPublicParameters,
        eccsiParameterData  [2] IMPLICIT ECCSIPublicParameters,
        skParameterData     [3] IMPLICIT SKPublicParameters,
        sm9ParameterData    [4] IMPLICIT SM9PublicParameters
}
IBParamExtensions ::= SEQUENCE OF IBParamExtension
IBParamExtension ::= SEQUENCE {
        ibParamExtensionOID       OBJECT IDENTIFIER,
        ibParamExtensionValue     OCTET STRING
}
AlgorithmIdentifier  ::= SEQUENCE {
        algorithm           OBJECT IDENTIFIER,
        parameters          ANY DEFINED BY algorithm OPTIONAL
}
```

在[IETF RFC 5091]中，两套MSK，公共参数和私钥块，即：

– BB1MasterSecret、BB1PublicParameters、BB1PrivateKeyBlock;

– 为BF和BB1密钥生成函数定义BFMasterSecret、BFPublicParameters、BFPrivateKeyBlock。这些指配仅适用于带有素域上定义的超奇椭圆曲线上的对称配对的函数的执行。本建议书规范了新的结构，版本号变更至v3以支持非对称配对算法的执行。对于超奇异椭圆曲线上的对称配对，BB1和BF密钥数据结构上的对应字段仍保留[IETF RFC 5091]规定的含义不变。分别为ECCSI、SM9和SK-KEM定义另外三套密钥数据结构。

```
BB1MasterSecret ::= SEQUENCE {
        version     INTEGER { v3(3) },
        alpha       INTEGER,
        beta        INTEGER,
        gamma       INTEGER
}
```

– 为执行非对称配对，[ISO IEC 18033-5]第9.3款中的alpha须为s1，beta须为s2，gamma须为s3。

```
BB1PublicParameters ::= SEQUENCE {
        version     INTEGER { v3(3) },
        curve       OBJECT IDENTIFIER,
        hashfcn     OBJECT IDENTIFIER,
        pairing     PAIRING OPTIONAL,
        p           INTEGER OPTIONAL,
        q           [0] IMPLICIT INTEGER OPTIONAL,
        pointP      FpPoint,
        pointQ      [1] EXPLICITFpxPoint OPTIONAL
       pointP1      FpPoint,
        pointP2     [2] EXPLICITFpxPoint OPTIONAL,
        pointP3     FpPoint,
        v           FpxElement
}
```

– 配对规定应对生成的参数使用哪类双线性映射。支持三类配对：Weil配对、Tate配对和最优Ate配对。

– P和q为可选。对于一些类型的曲线，例如BN、BLS-12等，p和q由曲线对象标识符（OIDs）预先确定，因此没有必要再次对其进行规定。

– 为使用非对称配对的执行，pointP和pointQ应为[ISO IEC 18033-5]第9.3款的*G*1中的Q1和*G*2中的Q2。对于对称配对，pointP等于pointQ，因此pointQ为OPTIONAL。

– 为使用非对称配对的执行，PointP1和pointP3应为[ISO/IEC 18033-5]第9.3款的R和T。

– 为使用非对称配对的执行（例如BN曲线上的最优Ate配对），pointP2从F_p的扩展字段取值。pointP2可选，因为若提供v，则BB1-KEM算法就无需执行pointP2。

– v是配对结果，为F_p的扩展字段的一个元。为使用非对称配对的执行（例如BN曲线上的最优Ate配对），扩展字段为F_p^k，其中，k是嵌入次数。在这一情况下，v应为[ISO/IEC 18033-5]的第9.3款中的J。

– 其他字段仍保留[IETF RFC 5091]中规定的含义不变。

```
PAIRING ::= ENUMERATED{
        weil        (1),    --Weil pairing
        tate        (2),    --Tate pairing
        optimalAte  (3)     --Optimal Ate pairing
}
FpPoint ::= SEQUENCE{
        x    INTEGER,
        y    INTEGER
}
```

FpPoint定义一个素域上的椭圆曲线上的一个点。一个点有两个坐标，指定为x坐标和y坐标。两个坐标都取大整数值。

```
FpxPoint ::= CHOICE{
        fpPoint [1]     EXPLICIT FpPoint,
        fp2Point        [2] EXPLICIT Fp2Point,
        fp3Point        [3] EXPLICIT Fp3Point,
        fp4Point        [4] EXPLICIT Fp4Point
}
```

– Fp2Point定义F_p^2字段上的椭圆曲线上的一个点。点的每个坐标都从F_p^2的一个元中取值。

– Fp3Point定义F_p^3字段上的椭圆曲线上的一个点。点的每个坐标都从F_p^3的一个元中取值。

– Fp4Point定义F_p^4字段上的椭圆曲线上的一个点。点的每个坐标都从F_p^4的一个元中取值。

```
Fp2Point ::= SEQUENCE{
        x    Fp2Element,
        y    Fp2Element
}
```

– Fp2Point定义F_p^2字段上的椭圆曲线上的一个点。一个点有两个坐标，名为x坐标和y坐标。两个坐标都从F_p^2取值。

```
Fp3Point ::= SEQUENCE{
        x    Fp3Element,
        y    Fp3Element
}
```

– Fp3Point定义F_p^3字段上的椭圆曲线上的一个点。一个点的两个坐标都从F_p^3取值。

```
Fp4Point ::= SEQUENCE{
        x    Fp4Element,
        y    Fp4Element
}
```

– Fp4Point定义F_p^4字段上的椭圆曲线上的一个点。一个点的两个坐标都从F_p^4取值。

```
Fp2Element ::= SEQUENCE{
        a    INTEGER,
        b    INTEGER
}
```

– Fp2Element定义字段F_p^2的一个元，表达为a+bα，其中α为F_p中的非平方根。

```
Fp3Element ::= SEQUENCE{
        a    INTEGER,
        b    INTEGER,
        c    INTEGER
}
```

– Fp3Element定义字段F_p^3的一个元，表达为a+bβ+cβ^2，其中β为F_p中的非立方根。

```
Fp4Element ::= SEQUENCE{
        a    Fp2Element,
        b    Fp2Element
}
```

– Fp4Element定义字段F_p^4的一个元，表达为F_p^2的两个元的塔。

```
FpxElement ::= CHOICE{
        fp2Elemt    [1] EXPLICIT Fp2Element,
                    --用于超奇异椭圆曲线执行
        fp12Elemt   [2] EXPLICIT Fp12Element,
                    --使用p->F_p^2->F_p^6->F_p^12塔表示
        fp16Elemt   [3] EXPLICIT Fp16Element,
                    --使用F_p->F_p^2->F_p^4->F_p^8->F_p^16塔表示
        fp18Elemt   [4] EXPLICIT Fp18Element,
                    --使用F_p->F_p^3->F_p^6->F_p^18塔表示
        fp24Elemt   [5] EXPLICIT Fp24Element
                    --使用F_p->F_p^2->F_p^6->F_p^12->F_p^24塔表示
}
```

– FpxElement定义*G*3中一个元的塔表示。配对e分别映射*G*1和*G*2到*G*3中的一个元的两个输入。对于常用的配对友好型曲线，*G*3的元通常用塔式法来表示。不同的嵌入次数有不同的塔式表示。本建议书为嵌入次数12、16、18和24的字段的元定义了一个常用的塔表达。

Fp12Element ::= SEQUENCE{

a Fp6Element,

b Fp6Element

}

– Fp12Element定义了2x3x2塔表达的F_p^12的一个元，须被用于使用BN曲线或BLS-12曲线或BLS-24曲线的执行。

Fp6Element ::= SEQUENCE{

a Fp2Element,

b Fp2Element,

c Fp2Element

}

– Fp6Element定义了3x2塔表达的F_p^6的一个元，须被用于使用BN曲线或BLS-12曲线或BLS-24曲线的执行。

Fp16Element ::= SEQUENCE{

a Fp8Element,

b Fp8Element

}

– Fp16Element定义了2x2x2x2塔表达的F_p^16的一个元，须被用于使用KSS-16曲线的执行。

Fp8Element ::= SEQUENCE{

a Fp4Element,

b Fp4Element

}

– Fp8Element定义了2x2x2塔表达的F_p^8的一个元，须被用于使用KSS-16曲线的执行。

Fp18Element ::= SEQUENCE{

a Fp6bElement,

b Fp6bElement,

c Fp6bElement

}

– Fp18Element定义了3x2x3塔表达的F_p^18的一个元，须被用于使用KSS-18曲线的执行。

Fp6bElement ::= SEQUENCE{

a Fp3Element,

b Fp3Element

}

– Fp6bElement定义了2x3塔表达的F_p^6的一个元，须被用于使用KSS-18曲线的执行。

Fp24Element ::= SEQUENCE{

a Fp12Element,

b Fp12Element

}

– Fp24Element定义了2x2x3x2塔表达的F_p^24的一个元，须被用于使用BLS-24曲线的执行。

BB1PrivateKeyBlock ::= SEQUENCE {

version INTEGER { v3(3) },

pointD0FpxPoint,

pointD1FpxPoint

}

– pointD0和pointD1仍保留[IETF RFC 5091]中规定的含义不变，但，如果使用非对称配对执行BB1-KEM，则pointD0和pointD1从*G*2取值。在这种情况下，pointD0和pointD1应分别为[ISO/IEC 18033-5]第9.3款的dID0和dID1。

BFMasterSecret ::= SEQUENCE {

version INTEGER {v3(3) },

masterSecret INTEGER

}

– 每个字段的含义仍保留[IETF RFC 5091]中规定的含义不变。

BFPublicParameters ::= SEQUENCE {

version INTEGER { v3(3) },

curve OBJECT IDENTIFIER,

hashfcn OBJECT IDENTIFIER,

pairing PAIRING OPTIONAL,

p INTEGER OPTIONAL,

q [0] IMPLICIT INTEGER OPTIONAL,

pointP FpxPoint,

pointPpub FpxPoint

}

– 每个字段的含义仍保留[IETF RFC 5091]中规定的含义不变，但，如果使用非对称配对执行BF-IBE，则pointP和pointPpub从*G*2取值。在这种情况下，pointP和pointPpub应分别为[ISO/IEC 18033-5]第8.2款的Q和R。

BFPrivateKeyBlock ::= SEQUENCE {

version INTEGER { v3(3) },

privateKey FpPoint

}

– 每个字段的含义仍保留[IETF RFC 5091]中规定的含义不变。为了使用非对称配对的执行，privateKey应为[ISO/IEC 18033-5]第8.2款中的skID。

```
ECCSIMasterSecret ::= SEQUENCE {
        version         INTEGER {v3(3) },
        masterSecret    INTEGER
}
```

– masterSecret应为[IETF RFC 6507]中的KSAK。

```
ECCSIPublicParameters ::= SEQUENCE {
        version     INTEGER { v2(2) },
        curve       OBJECT IDENTIFIER,
        hashfcn     OBJECT IDENTIFIER,
        pointP      FpPoint,
        pointPpub   FpPoint
}
```

– pointP应为[IETF RFC 6507]中的G。

– pointPpub应为[IETF RFC 6507]的KMS公共鉴权密钥（KPAK）。

```
ECCSIPrivateKeyBlock ::= SEQUENCE {
        version     INTEGER { v2(2) },
        ssk         INTEGER ,
        pvt         OCTET STRING
}
```

– ssk和pvt应分别为[IETF RFC 6507]中的秘密签名密钥（SSK）和公共验证令牌（PVT）。

```
SKMasterSecret ::= SEQUENCE {
        version     INTEGER {v3(3) },
        masterSecret  INTEGER
}
```

– masterSecret应为[IETF RFC 6508]中的z_T和[ISO/IEC 18033-5]第9.2款中的s。

```
SKPublicParameters ::= SEQUENCE {
        version         INTEGER { v3(3) },
        curve           OBJECT IDENTIFIER,
        hashfcn         OBJECT IDENTIFIER,
        pairing         PAIRING OPTIONAL,
        p               INTEGER OPTIONAL,
        q               [0] IMPLICIT INTEGER OPTIONAL,
        pointP1         FpPoint,
        pointP1pub      [1] EXPLICIT FpPoint OPTIONAL,
        pointP2         [2] EXPLICIT FpxPoint OPTIONAL,
        pointP2pub      [3] EXPLICIT FpxPoint OPTIONAL,
```

```
    v               [4] EXPLICIT FpxElement
}
```

– 对于超奇曲线上的对称配对的执行，p和q在[IETF RFC 5091]中进行了定义。对于非对称配对的执行，p和q由使用的曲线预定义，且可选。

– pointP1和Q1应分别为[IETF RFC 6508]中的P和[ISO/IEC 18033-5]第9.2款中的*G*1。

– pointP1pub应为[IETF RFC 6508]中的Z_T和[ISO/IEC 18033-5]第9.2款的R。pointP1pub对于基于Sakai-Kasahara （SK）生成函数的其他算法（例如签名算法）可能非必要，因此可选。

– 若SK-KEM使用非对称分配来执行，pointP2应为[ISO/IEC 18033-5]第9.2款*G*2中的Q2。pointP2对于SK-KEM执行非必要，因此可选。

– pointP2pub应为[*ib.msk*]Q2，对于SK-KEM非必要，但对于基于SK密钥生成函数的其他算法（例如签名算法）可能必要，因此可选。

```
SKPrivateKeyBlock ::= SEQUENCE {
    version     INTEGER { v3(3) },
    privateKey  FpxPoint
}
```

– privateKey应为[IETF RFC 6508]中的RSK和[ISO/IEC 18033-5]第9.2款的skID。

```
SM9MasterSecret ::= SEQUENCE {
    version         INTEGER {v3(3) },
    masterSecret    INTEGER
}
```

– masterSecret应为*ib.msk*，[b-ISO/IEC 14888-3a]第7.4款定义的U。

```
SM9PublicParameters ::= SEQUENCE {
    version         INTEGER { v3(3) },
    curve           OBJECT IDENTIFIER,
    hashfcn         OBJECT IDENTIFIER,
    pairing         PAIRING OPTIONAL,
    p               INTEGER OPTIONAL,
    q               [0] IMPLICIT INTEGER OPTIONAL,
    pointP1         FpPoint,
    pointP1pub      [1] EXPLICIT FpPoint OPTIONAL,
    pointP2         [2] EXPLICIT FpxPoint OPTIONAL,
    pointP2pub      [3] EXPLICIT FpxPoint OPTIONAL,
    v               [4] EXPLICIT FpxElement
}
```

– 对于超奇曲线上的对称配对的执行，p和q在[IETF RFC 5091]中进行了定义。对于非对称配对的执行，p和q由使用的曲线预定义。

– pointP1应为[ISO/IEC 14888-3]第7.4款的P。

– pointP1pub对于SM9-IBS非必要，但对于SM9-IBE必要，在这种情况下pointP2pub应为[*ib.msk*] P。

– pointP2应为[ISO/IEC 14888-3]第7.4款的Q。pointP2对于**SM9-IBE**的执行非必要，因此可选。

– pointP2pub应为[ISO/IEC 14888-3a]第7.4款的V。pointP2pub对于**SM9-IBE**的执行非必要，因此可选。

```
SM9PrivateKeyBlock ::= SEQUENCE {
        version      INTEGER { v3(3) },
        privateKey   FpxPoint
}
```

– privateKey用于签名应为[ISO/IEC 14888-3a]第7.4款的X，用于SM9-IBE和SM9-AKA应为*G*1的*ib.prvk*。

BFMasterSecret、BFPublicParameters和BFPrivateKeyBlock定义应被用于使用Sakai-Ohgishi-Kasahara（SOK）密钥生成的算法，例如BF-IBE、Cha-Cheon-IBS、Hess-IBS、Fujioka-Suzuki-Ustaoglu-AKA、Smart-Chen-Cheng-AKA和Wang-AKA。BB1MasterSecret、BB1PublicParameters和BB1PrivateKeyBlock定义应被用于使用BB1密钥生成的算法，例如BB1-KEM。SKMasterSecret、SKPublicParameters和SKPrivateKeyBlock应被用于SK-KEM，以及可能的其他基于SK密钥生成函数的算法。SM9MasterSecret、SM9PublicParameters和SM9PrivateKeyBlock应被用于包括SM9-IBE、SM9-IBS和SM9-AKA在内的SM9算法。ECCSIMasterSecret、ECCSIPublicParameters和ECCSIPrivateKeyBlock应被用于ECCSI。

若私钥需要被保护，应使用[IETF RFC 5958]定义的EncryptedPrivateKeyInfo结构。

```
EncryptedPrivateKeyInfo ::= SEQUENCE {
        encryptionAlgorithm      EncryptionAlgorithmIdentifier,
        encryptedData            EncryptedData
}
EncryptionAlgorithmIdentifier ::= AlgorithmIdentifier
EncryptedData ::= OCTET STRING
AlgorithmIdentifier ::= SEQUENCE {
        algorithm       OBJECT IDENTIFIER,
        parameters      ANY DEFINED BY algorithm OPTIONAL
}
```

附件C

密钥管理操作

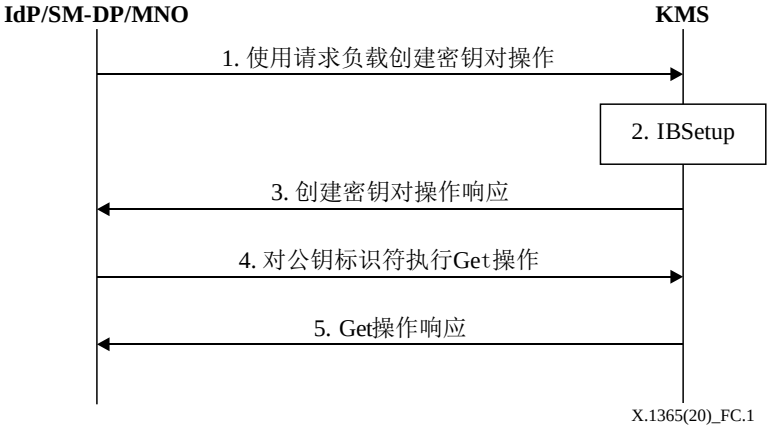
（本附件是本建议书不可分割的组成部分。）

在IBC系统中，密钥管理操作包括系统初始化、身份或私钥提供、身份或私钥撤销和系统参数发布。系统初始化涉及调用**IBSetup**函数的步骤，私钥提供涉及调用**IBExtract**函数的步骤。这些操作要求管理实体和KMS之间的互动。本建议书使用KMIP来交换这两者之间的信息。必要的扩展得到规定，以满足支持的**IBSetup**和**IBExtract**算法的新要求，见附录II。SecMs和管理实体之间的互动协议基于非eUICC物联网设备的HTTP定义。对于eUICC，如有需要，使用和扩展[b-GSMA SGP.02]标准。

C.1 系统初始化

在每个IBC系统中，系统初始化流程须在向用户提供KMS之前完成。在这一过程中，KMS执行一个或更多**IBSetup**函数来生成一套或更多套*ib.msk*和*ib.pubparam*密钥对。加固KMS的安全性的方法不在本建议书的范围内。作为良好实践，*ib.msk*须由HSM生成并存储其中。如有可能，可部署在多个KMS上使用秘密共享体制来拆分*ib.msk*并传播秘密共享和私钥生成函数的分布式密钥生成方案。在这种情况下，只有超过一个KMS的阈值数正常使用，对应ID的私钥才可被正确生成。

见图C.1。



图C.1 – 密钥管理互操作协议的系统初始化

启动条件：

假定IdP/SM-DP/MNO为系统启动器，负责系统的初始化流程。在IdP/SM-DP/MNO能够触发KMS中的**IBSetup**函数之前，须满足以下条件。

a) 在 IdP/SM-DP/MNO 和 KMS 之间建立一条安全信道。

b) IdP/SM-DP/MNO 完成与 KMS 的鉴权流程，经鉴权的 IdP/SM-DP/MNO 被授权执行 **IBSetup** 请求。

流程：

1) IdP/SM-DP/MNO 须准备请求负载（Request Payload）并调用创建密钥对操作来向 KMS 发送经过编码的请求信息。

2) KMS 须检查请求的有效性，以及 IdP/SM-DP/MNO 被授权调用这一操作。若这些条件中的任何一条未被满足，则 KMS 须返回一个响应，表明验证失败。否则，KMS 须执行 **IBSetup** 和请求中规定的参数。

3) KMS 须向 IdP/SM-DP/MNO 返回执行响应。若操作成功，则 KMS 须至少分别向 *ib.msk* 和 *ib.pubparam* 返回一个私钥唯一 ID 和一个公钥唯一 ID。

4) 或者，若创建密钥对操作成功，IdP/SM-DP/MNO 使用从最后一个响应中获得的公钥唯一 ID 调用 get 操作，以读取公钥参数 *ib.pubparam*。

5) KMS 须返回最新生成的公共参数的密钥值。

用于支持这一操作的KMIP扩展见附录II。

结束条件：KMS被成功初始化，IdP/SM-DP/MNO获得私钥唯一ID和公钥唯一ID以分别接入生成的MSK *ib.msk*和公共参数*ib.pubparam*。IdP/SM-DP/MNO须使用私钥唯一ID来唤起签名操作，以生成身份私钥，须使用公钥唯一ID来唤起get操作，以读取公共参数。

C.2 设备初始化

设备初始化操作是让设备为身份和密钥提供做好准备。对于eUICC和其他非eUICC物联网设备，之后的初始化流程不同。

C.2.1 案例1：eUICC的初始化

对于eUICC，身份和对应私钥*ib.prk*和公共参数*ib.sysparam*被从主安全域（ISD）文件中下载。因此，在设备初始化过程之后，eUICC须准备好ISD文件创建。须根据[b-GSMA SGP.02]完成注册操作。以下重复了[b-GSMA SGP.02]第3.5.1款。

- **eUICC在SM-SR上注册**

启动条件：

a) 在提供运营商的网络中生成 eUICC，加载并激活一个配置文件。这些都经过检验并准备用于运送。每个 eUICC 均有一个相应的 eUICC 信息组（EIS）。

流程：

1) eUICC 制造商（EUM）向所选择的 SM-SR 发送包含 EIS 的 eUICC 注册请求。

2) SM-SR 将 EIS 存储在其数据库中，使用 eUICC-ID（EID）作为密钥参数。

3) SM-SR 向 EUM 确认注册成功。确认信息中包含 EID。

结束条件：eUICC在SM-SR上注册，并为文件下载做好准备。现在可以被运送给机对机设备制造商。

C.2.2 案例2：非eUICC物联网设备的初始化

对于非eUICC物联网设备，应完成以下注册操作。

- AuC上的SecM注册

启动条件：

a) 生成 SecM，物联网设备须能够在运营商网络中与 IdP 通信。

流程：

1) SecM 向 AuC 发送 SecM 提供数据采集请求。

2) AuC 为请求的 SecM 生成提供 ID（PROV.ID）和相关鉴权证书(PROV.CRED)。

3) AuC 向 SecM 发送 PROV.ID 和 PROV.CRED。若 SecM 无法执行 TLS 协议，在同一条信息中，AuC 亦向 SecM 发送一个密钥身份 IdP.ID 和一个相关公钥 IdP.PUK 或 *ib.sysparam*。

4) SecM 安全地存储 PROV.ID 和 PROV.CRED，若提供，IdP.ID 和 IdP.PUK 或 *ib.sysparam* 亦同时存储。SecM 须保护 IdP.ID 和 dP.PUK 或 *ib.sysparam* 不受授权更改的影响。

结束条件：SecM在AuC上注册，并为身份和密钥提供做好准备。

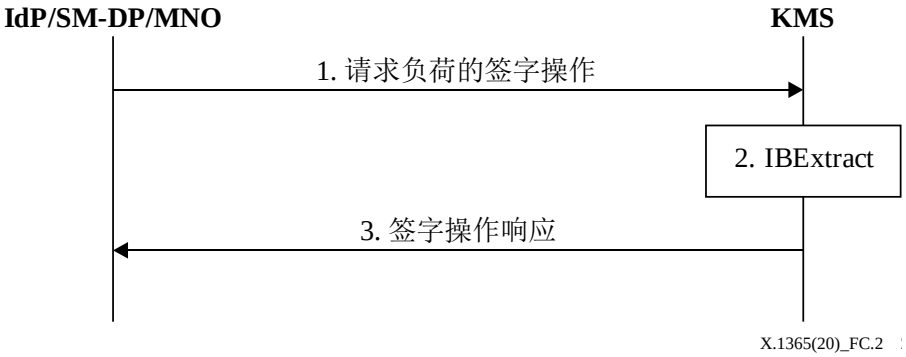
C.3 公共参数查找

实体须使用身份或密钥提供流程来为实体注册的IBC系统获取公共参数。实体可以是物联网设备或一个IBC系统的管理实体，须按照[IETF RFC 5408]第4款规定的规格从已知PPS上读取另一IBC系统的公共参数。应使用本建议书中定义的IBSysParams来替换在[IETF RFC 5408]中响应的IBESysParams。[IETF RFC 5408]假定查询物联网设备能够与请求的PPS建立一条基于TLS的安全信道。若该要求无法被满足，IBSysParams中的signatureAlgorithm和签名字段应存在并有效。一旦IBSysParams被读取，应遵守正确的签名验证流程，只有在IBSysParams中的签名有效且签名验证公钥真实有效的情况下，读取的公共参数才可被接受。

C.4 身份和密钥提供

身份和密钥提供包括身份指配、私钥提取和密钥分配流程。设备在初始化流程之后只有一个临时身份。IdP或SM-DP或MNO应确定为提出请求的设备指派哪个身份，之后与KMS通信以生成相应的私钥，并最终安全地将实体、私钥和公共参数分配给设备。

见图C.2。



图C.2 – 密钥管理互操作协议的私钥生成

- **使用KMIP生成私钥**

启动条件：

假设IdP/SM-DP/MNO生成私钥*ib.prk*。在IdP/SM-DP/MNO能够在KMS中调用IBExtract函数之前，须满足以下条件。

a) IdP/SM-DP/MNO 和 KMS 之间建立安全的信道。

b) IdP/SM-DP/MNO 已完成对 KMS 的鉴权过程。经鉴权的 IdP/SM-DP/MNO 被授权执行 IBExtract 请求。

流程：

1) IdP/SM-DP/MNO 应准备请求负载，并调用签名操作，从而向 KMS 发送编码的请求信息。

2) KMS 须检查请求的有效性，以及 IdP/SM-DP/MNO 被授权调用这一操作。若这些条件中的任何一条未被满足，则 KMS 须返回一个响应，表明验证失败。否则，KMS 须使用 *ib.mskk, ib.pubparam* 执行 **IBExtract**，以及请求中规定的参数。

3) KMS 须向 IdP/SM-DP/MNO 返回执行响应。若操作成功，则 KMS 须以 IBPrivateKeyBlock（这是用 ASN.1 定义的一个 CHOICE）的形式返回如下生成的私钥 *ib.prk*：

```
IBPrivateKeyBlock ::= CHOICE{
    bb1PrivateKeyBlock      BB1PrivateKeyBlock,
    bfPrivateKeyBlock       BFPrivateKeyBlock,
    eccsiPrivateKeyBlock    ECCSIPrivateKeyBlock,
    skPrivateKeyBlock       SKPrivateKeyBlock,
    sm9PrivateKeyBlock      SM9PrivateKeyBlock
}
```

支持这一操作的KMIP扩展见附录II。

结束条件：IdP/SM-DP/MNO检索对应于请求身份的私钥。

- **eUICC的身份/密钥提供**

启动条件：

a) UICC 在 SM-SR 注册，为文件下载做好准备。

b) SM-DP 已基于 MNO 提供的文件描述创建一个非个性化文件。

c) MNO 已请求 eUICC 文件的数量。

d) 非个性化文件已被在目标 eUICC 类型上使用非个性化文件验证流程验证。

流程：

1) MNO 向一个所选择的 SM-DP 提供文件排序。文件排序流程的详情见[b-GSMA SGP.02]的第 3.5.3 款。

2) SM-DP 使用从 MNO 读取的数据创建个性化文件。特别是，SM-DP 须使用所选择的国际移动订阅身份（IMSI）作为身份，采用在使用 KMIP 生成私钥时指定的 KMS 来完成签名操作，为选定 IMSI 生成私钥。生成的私钥和 IBSysParams 中的 ibPublicParameters 须作为密钥包含在文件中。

3) 目标文件由 MNO 在 eUICC 上提供。文件的下载和安装流程的详情见[b-GSMA SGP.02]第 3.5.4 款。

4) eUICC 的目标文件通过 SM-SR 或通过 SM-DP 和 SM-SR 启用。文件启用的具体步骤见[b-GSMA SGP.02]第 3.5.6 或 3.5.7 款。

结束条件：目标文件在eUICC上启用。先前启用的文件被禁用。EIS是最新的。

- **非eUICC物联网设备的身份和密钥提供**

案例1：SecM能够与IdP建立TLS会话

启动条件：

a. SecM 已在 AuC 注册。

流程：

1) SecM 与 IdP 建立一个 TLS 会话，并且须成功地验证 IdP TLS 证书的有效性。

2) SecM 使用 PROV.ID 和 PROV.CRED 执行 IdP 的网络验证程序。

3) IdP 选择一个指配给请求设备的身份，根据采用在使用 KMIP 生成私钥时指定的 KMS 来完成选定身份的签名操作。

4) IdP 通过 TLS 会话发送指配的身份、生成的私钥和公共参数至 SecM。

5) SecM 安全地存储私钥，公共参数须被保护不受未经授权的变更。

结束条件：目标密钥在SecM上提供。

SecM和IdP应遵守第5款规定的协议和[IETF RFC 5408]以完成身份和密钥提供程序。在响应中，[IETF RFC 5408]中定义的IBEPrivateKeyReply结构须被IBPrivateKeyReply替换。

```
IBPrivateKeyReply ::= SEQUENCE SIZE (1..MAX) OF IBPrivateKey
IBPrivateKey ::= SEQUENCE {
        pkgIdentity         IBIdentityInfo OPTIONAL,
        pkgAlgorithm        OBJECT IDENTIFIER,
        pkgKeyData          IBPrivateKeyBlock,    --defined by pkgAlgorithm
        pkgOptions          SEQUENCE SIZE (1..MAX) OF PKGOption,
        ibSysParams         IBSysParams OPTIONAL
}
PKGOption ::=  SEQUENCE  {
        optionID        OBJECT IDENTIFIER,
        optionValue     OCTET STRING
}
```

案例2：SecM没有TLS应用

启动条件：

a SecM 已在 AuC 上注册。

流程：

1) SecM 生成密钥加密密钥（KEK）并编码密钥提供请求（IBKeyProvRequest）。该请求包括 KEK、使用 IdP.ID 识别的 IdP 公钥加密的提供 ID（PROV.ID）和证书（PROV.CRED）。加密结果被编码为 EncryptedMsg。它将加密请求作为 HTTP POST 请求的主文发送给 IdP。

2) IdP 通过使用请求中的 IdP.ID 识别的密钥来解密密文，并检查时戳的新鲜度或者计数器的正确性，或同时检查二者。若请求未能通过这些检查，IdP 须返回一个响应，表明验证失败。IdP 进一步使用 AuC 检查 PROV.ID 和 PROV.CRED 的正确性。若检查失败，IdP 须返回一个响应，表明失败。IdP 选择一个指配给请求设备的身份，根据采用在使用 KMIP 生成私钥时指定的 KMS 来完成所选择身份的签名操作。

3) IdP 采用使用请求中传达的指定算法（keyProtAlg）的密钥加密密钥（KEK）加密生成的私钥，以及被编码为 IBKeyProvisionData 的身份和公共参数（如有必要）。密文被加密为 EncryptedMsg。IdP 向 SecM 发送加密响应作为 HTTP 响应主文。

4) SecM 解密响应并获得指定身份、私钥和公共参数。其安全地存储私钥，公共参数须被保护不受未经授权的变更。

结束条件：在SecM上提供目标密钥。

```
IBKeyProvisionRequest ::= SEQUENCE{
        version     INTEGER { v1(1) },
        timer       Time OPTIONAL,
        counter     INTEGER       OPTIONAL,
        identity    OCTET STRING,
        credential  OCTET STRING,
        keyProtAlg OBJECT IDENTIFIER,
        kek         OCTET STRING
}
Time ::= CHOICE {
    utcTime       UTCTime,
    generalTime   GeneralizedTime
}
IBKeyProvisionResponse ::= SEQUENCE SIZE(1..MAX) OF IBKeyProvisionData
IBKeyProvisionData ::= SEQUENCE{
        identity          OCTET STRING OPTIONAL,
        ibSysParams       IBSysParams OPTIONAL,
        ibPrivateKey      IBPrivateKeyBlock
```

}

EncryptedMsg ::= SEQUENCE {

encryptionAlgorithm EncryptionAlgorithmIdentifier,

encryptedData EncryptedData

}

EncryptionAlgorithmIdentifier ::= AlgorithmIdentifier

EncryptedData ::= OCTET STRING

C.5 身份和密钥撤销

若身份由于种种原因（例如，由于身份的所有者取消订购该业务或对应私钥被破解）未被IBC系统接受，该身份须被撤销，而对应私钥出于安全原因需要被销毁。若一个身份被撤销，该身份须被设置为已撤销状态。若一个输入要查询已撤销身份的状态，IdP/SM-DP/MNO须返回OISP定义的正确的值。欲更高效地查询身份状态，实体可定期从IdP/SM-DP/MNO读取IRL并将其存储在本地，并且实体可与新鲜IRL核对来确定实体是否被撤销而无须在线查询每个身份的状态。对于eUICC，销毁私钥的过程可以先禁用，而后从eUICC中删除文件。

- **eUICC上的身份和密钥撤销**

启动条件：

a) 目标文件在 eUICC 上启用。

流程：

1) MNO 通过 SM-DP 流程启动文件禁用。文件禁用流程的详情见[b- GSMA SGP.02]第 3.5.8 款。SM-DP 须将身份设置在撤销状态。

2) .MNO 启动文件删除流程。ISD-P 删除的具体步骤见[b- GSMA SGP.02]的第 3.5.10 条。SM-DP 须将身份设置为已撤销，若 ISD-P 删除过程成功，身份亦被设置为已删除状态。当实体查询身份的状态时，SM-DP 须根据状态记录正确响应。在此期间，SM-DP 须定期发布撤销身份的身份状态列表。

结束条件：目标文件被禁用并从eUICC中删除。

- **非eUICC物联网设备的身份和密钥撤销**

若身份被撤销，IdP须将身份设置为撤销状态。在实体查询身份状态时，IdP须根据状态记录正确响应。在此期间，IdP须定期发布撤销身份的身份状态列表。

撤销触发过程和身份状态维护在本建议书的范围之外。

- **在线身份状态协议**

随着大量物联网设备连接至电信运营商，SM-DP、IdP或物联网设备可能需要获得关于某物联网设备实体的撤销状态的即时信息。在本建议书中，OISP被指定用于使SM-DP、IdP或物联网设备通过在线查询的方式确定一个实体的当前状态。OISP客户端向OISP响应器发出一个状态请求，在响应器响应之前暂停接受正在请求的身份。OISP与在线证书状态协议（OCSP）[IETF RFC 6960]共享相似性。

OISP请求包含以下数据：

```
OISPRequest ::= SEQUENCE {
        version         INTEGER { v1(1) },
        identity        IBIdentityInfoSet
}
```

– Version表示协议版本，在本文件中为v1(1)。

– identity为OISP请求。

```
IBIdentityInfoSet ::= SEQUENCE SIZE(1..MAX) OF IBIdentityInfo
IBIdentityInfo ::= SEQUENCE {
        domainName          IA5String OPTIONAL,
        domainSerial        INTEGER OPTIONAL,
        identityType        OBJECT IDENTIFIER OPTIONAL,
        identityData        OCTET STRING
}
```

– domainName可选（OPTIONAL），IA5String表示URI [b-URI]或IRI [b-IRI]。

– domainSerial可选（OPTIONAL），包括在一个单域使用超过一套参数的情况下定义一套独特IBC公共参数的标识符（INTEGER）。

– identityType可选（OPTIONAL），包含定义identityData字段编码采用的格式的对象标识符（OBJECT IDENTIFIER）。若该字段缺失，则使用默认身份类型。

– identityData是目标对象数据。

在接受请求时，OISP响应器检查信息是否符合格式，以及请求是否包含响应器所需的信息。若检查失败，OISP响应器生成出错信息；否则，根据请求中查询的身份的状态返回明确回复。

```
OISPResponse ::= SEQUENCE {
        responseStatus      OISPResponseStatus,
        responseData        OISPResponseData OPTIONAL
}
```

– responseStatus表示预先请求的处理状态。

– responseData可选（OPTIONAL），包含请求的回复数据。若responseStatus的值是误差状态之一，则responseData字段不设置。

```
OISPResponseStatus ::= ENUMERATED {
    successful          (0),  -- 回复收到有效确认
    malformedRequest    (1),  -- 无效确认请求
    internalError       (2),  -- 发出者内部错误
    tryLater            (3),  -- 稍候再次尝试
```

```
                        --(4) 未使用
    unauthorized        (5)   -- 请求未授权
}
OISPResponseData ::= SEQUENCE {
    version             INTEGER { v1(1) },
    producedAt          GeneralizedTime,
    hashAlgorithm       AlgorithmIdentifier OPTIONAL,
    tbsIdStatus         SEQUENCE OF SingleIdStatus,
    signatureAlgorithm  AlgorithmIdentifier OPTIONAL,
    signature           BIT STRING OPTIONAL,
    certs               [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL
}
```

– 这一版本的基本响应句法版本必须为v1(1)。

– producedAt是OISP响应器签署这一响应的时间。

– hashAlgorithm定义在tbsIdStatus中生成idHash的散列算法（如果存在此字段）。该字段可选，无参数的SHA256的默认值为OBJECT IDENTIFIER。

– tbsldStatus表示一个请求中每个身份的响应。

– signatureAlgorithm可选（OPTIONAL），包含用于签署响应的算法。

– 签名（signature）基于字段producedAt到tbsIdStatus生成的ASN.1 DER结果使用指定签名算法计算。本字段可选（OPTIONAL），若OISP客户端有其他方式来确保响应的真实性可不设置。例如，响应通过TLS安全信道在客户端和响应器之间传输。

– certs可选（OPTIONAL），表述帮助OISP客户端验证响应器的签名的证书。[IETF RFC 5280]中规定了证书结构。

```
SingleIdStatus ::= SEQUENCE {
    idHash          OCTET STRING OPTIONAL,
    identityID      IBIdentityInfo OPTIONAL,
    identityStatus  IdentityStatus,
}
```

– idHash可选（OPTIONAL），包括请求身份的散列。若identityID过长，idHash可被用于表示被查询的身份。identityID可选，包含查询的目标身份的IBIdentityInfo字段。

– identityStatus说明预先请求的身份的状态。

```
IdentityStatus ::= CHOICE {
    good                [0]   IMPLICIT NULL,
    revoked             [1]   IMPLICIT RevokedInfo,
    unknown             [2]   IMPLICIT UnknownInfo,
    updated             [3]   IMPLICIT IBIdentityInfo,
    revokedAndDeleted   [4]   IMPLICIT RevokedInfo
```

}

UnknownInfo ::= NULL

– “good（好）”状态说明对状态查询的积极响应。

– “revoked（已撤销）”状态说明身份已被撤销（要么暂时要么永久），值为撤销信息。

– “unknown（未知）”状态说明响应器不知道正在被查询的证书。

– “updated（已更新）”说明身份已被更新，值是最新指配给被查询身份的身份。

– “revokedAndDeleted（已撤销并删除）”状态说明身份已被撤销，并且私钥已经被从远程设备中销毁。

```
RevokedInfo ::= SEQUENCE {
    revocationTime      GeneralizedTime,
    revocationReason    [0] EXPLICIT IRLReason OPTIONAL
}
IRLReason ::= ENUMERATED {
        unspecified             (0),
        keyCompromise           (1),
        pkgCompromise           (2),
        affiliationChanged      (3),
        superseded              (4),
        cessationOfOperation    (5),
        identityHold            (6),
                                -- 值7未使用
        removeFromIRL           (8),
        privilegeWithdrawn      (9)
}
```

- **身份撤销列表**

除了使用OSIP来响应状态查询之外，诸如IdP或SM-DP之类的实体可定期发布撤销的实体的完整列表，一个IRL。为加快身份状态检查流程，大容量的状态检查实体可查询该IRL并本地存储。检查实体可确认身份是否被某些操作接受，例如基于IRL的网络接入授权。若该身份未在IRL中，则假设该身份有效。为提高系统效率，IdP/SM-DP/MNO可仅发布自某个特定时间以来的最新撤销的身份，这被称为delta IRL。delta IRL包含自一个完整IRL发布以来撤销的身份信息。delta IRL的使用可极大减少通信开支和IRL的处理时间。IRL与证书撤销列表（CRL）[IETF RFC 5280]类似。

IRL的定义如下

```
IdentityRevocationList ::= SEQUENCE {
    tbsIdentityList         TBSIdentityRevocationList,
```

```
    signatureAlgorithm      AlgorithmIdentifier OPTIONAL,
    signatureValue          BIT STRING OPTIONAL
}
```

– tbsIdentityList是带有附加信息的被撤销的身份列表，例如撤销时间。

– signatureAlgorithm定义用于发放列表的IRL的发布者的算法。本字段可选，若不存在signatureValue，则本字段不存在。

– signatureValue定义tbsIdentityList上的发布者声称的签名的值。本字段可选，如果请求客户端由其他方式保证所读取的列表是真实的，则本字段不存在。

```
TBSIdentityRevocationList  ::=  SEQUENCE  {
    version                 INTEGER { v1(1) },
    issuer                  Name,
    irlNumber               INTEGER OPTIONAL,
    deltaList               BOOLEAN OPTIONAL,
    thisUpdate              Time,
    nextUpdate              Time OPTIONAL,
    domainName              IA5String OPTIONAL,
    domainSerial            INTEGER OPTIONAL,
    revokedIdentities       SEQUENCE OF SEQUENCE  {
        identity                IBIdentityInfo,
        revocationDate          Time,
        irlEntryExtensions      Extensions OPTIONAL
    } OPTIONAL,
    irlExtensions               [0] EXPLICIT Extensions OPTIONAL
}
Name ::= CHOICE {--imported from [IETF RFC 5280]
    rdnSequenceRDNSequence
}
RDNSequence ::= SEQUENCE OF RelativeDistinguishedName
RelativeDistinguishedName ::= SET SIZE (1..MAX) OF AttributeTypeAndValue
AttributeTypeAndValue ::= SEQUENCE {
    type    AttributeType,
    value   AttributeValue
}
AttributeType ::= OBJECT IDENTIFIER
AttributeValue ::= ANY -- DEFINED BY AttributeType
Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension
```

```
Extension ::=  SEQUENCE  {--imported from [IETF RFC 5280]
   extnID      OBJECT IDENTIFIER,
   critical    BOOLEAN DEFAULT FALSE,
   extnValue   OCTET STRING
            -- 包含一个ASN.1的值的DER编码
            -- 对应确定的扩展类型
            -- 通过extnID
}
```

– Version（版本）表示IRL结构的版本。
– 发布者是发布IRL的实体的名称。
– irlNumber是当前IRL发布者的数字。从0开始。每个完整的IRL发布使数量增加1。可选。
– deltaList表示当前IRL是否是delta IRL。该列表仅包含自一个由irlNumber作为指引的完整的IRL发布以来撤销的实体的信息。
– thisUpdate规定生成此IRL的时间。
– nextUpdate定义了生成下个IRL的时间。可选。
– domainName定义IBC身份域。
– domainSerial定义IBC身份域数字。
– revokedIdentities是已撤销的身份集。
  • 身份是已撤销的身份的数据。
  • revocationDate是身份被撤销的时间。
  • irlEntryExtensions定义可能的revokedIdentity扩展。当前未定义任何扩展。
– irlExtensions为IRL定义可能的扩展。当前未定义任何扩展。

附件D

鉴权

（本附件是本建议书不可分割的组成部分）

本附件提供了四个现有的鉴权协议来支持IBC。

D.1 一次处理的秘密传输协议

本协议对应[ISO/IEC 11770-3]中的密钥传输机制2。其根据从实体A到实体B的明式密钥鉴权和从实体B到实体A的隐式密钥鉴权从实体A向实体B传输一个由实体A生成、加密和签字的密钥。从实体A到实体B的明式密钥鉴权由签署加密密钥和时变参数（TVP）的实体A实现。从实体B到实体A的隐式密钥鉴权通过使用B的ID加密实现，这意味着只有B能够还原密钥。见图D.1。

为执行协议，须满足以下条件：

– 实体A拥有一个与其ID对应的签名私钥*A.ib.prk*和相关公共参数*A.ib.pubparam*。

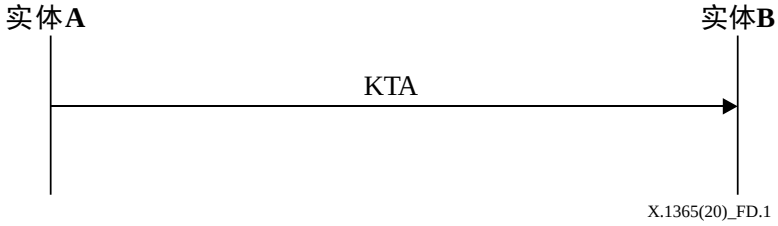
– 实体B拥有一个与其ID对应的签名私钥*B.ib.prk*和相关公共参数*B.ib.pubparam*。

– 实体A可接入实体B的公共参数的鉴权副本，用于加密*B.ib.pubparam*和B的ID。

– 实体B可接入实体A的公共参数的鉴权副本，用于*A.ib.pubparam*和A的ID签名。

– 可选的TVP须为时戳或序列号。若使用时戳，则实体A和B需要保持同步时钟或可信的第三方时戳。

– A和B可共享相同的公共参数，即*A.ib.pubparam = B.ib.pubpara*。



图D.1 – 一次处理的秘密传输协议

1) 实体 A 生成所需长度的随机密钥 *K*。

2) 实体 A 生成 *BE*=**IBEnc**(*B.ib.pubparam, ID_B,* [*ID_A*]||*K*||*Text1*)。若实体 B 有其他方式获得实体 A 的 ID，则 Text1 可为空，*ID_A* 可选。

3) 实体 A 生成 *S*=**IBSign**(*A.ib.pubparam, ID_A, A.ib.prk,* [*ID_B*]||TVP||BE||*Text2*)。若实体 B 知道使用 *ID_B* 用于加密的 ID，则 Text2 可为空，*ID_B* 可选。

4) 实体 A 生成令牌 KTA=[*ID_B*]||TVP||BE|| *Text2*|| S||*Text3*。

5) 当 TVP 为时戳时，实体 B 检查 TVP 是否在允许的时间差异之内。若否，实体 B 拒绝令牌。

6) 若实体 B 可通过其他方式获得 *ID_A* 而 TVP 是序列号，则实体 B 首先检查序列号是否大于为实体 B 保留的序列号。若否，实体 B 拒绝令牌。

7) 若实体 B 可通过其他方式获得 *ID_A*，实体 B 通过 **IBVerify**(*A.ib.pubparam, ID_A,* [*ID_B*]||TVP||BE||*Text2,* S)验证 KTA 中的签名 *S*。若签名无效，实体 B 拒绝令牌。

8) 实体 B 通过*[ID_A]||K||Text1*=**IBDec**(*B.ib.pubparam, ID_B, B.ib.prk,* BE)解密 *BE*。

9) 若实体 B 只能在步骤 8 之后获得 *ID_A*，实体 B 要检查 TVP 的新鲜度（若 TVP 是序列号）。若 TVP 不新鲜，实体 B 拒绝令牌。实体 B 进一步验证签名 *S*。若签名无效，实体 B 拒绝令牌。

10) 若所有的检查和验证均通过，实体 A 和实体 B 使用 *K* 来保护之后的信息。两个实体均使用密钥导出函数（KDF）[b-IEEE 1363]来生成用于加密和信息鉴权的密钥。

注1 – 可通过将BE从实体A和KTA发放的信息中移除的方式转换为单边实体鉴权协议。这一修改为[b-ISO/IEC 9798-3]定义的一次处理的实体鉴权方案。

注2 – 可通过要求实体B将*K*返还给实体A的方式转换为单边实体鉴权协议。实体B通过展示其能够恢复*K*（这需要其拥有私钥*B.ib.prk*）来被实体A鉴权。

注3 – 于身份的签密算法（例如BLMQ签密算法[b-Barreto]、Chen-Malone-Lee签密算法[b-Chen]）可被用于提高效率。

D.2 TLS-IBS

本条款规定了另一个名为TLS-IBS的鉴权协议。假设向服务器侧和物联网设备侧都提供了基于身份的证书，包括身份、用于签名的私钥和KMS公共参数（例如[IETF RFC 6507]中规定的KPAK作为一个计算参数）。附件B提供了被支持的算法的KMS公共参数结构定义。

TLS-IBS是基于[IETF RFC 7250]而开发的。传统上来看，公钥基础设施（PKI）证书TLS客户端和服务器交换公钥支持。使用PKI证书被认为是复杂的，且可能导致安全漏洞。为简化证书交换，[IETF RFC 7250]规定在TLS中采用原始公钥，即客户端和服务器之间的TLS信息中只交换公钥而不传输完整的证书信息。不过，假设公钥使用带外机制和身份绑定。对于物联网网络来说，采用原始公钥的TLS尤其具有吸引力，但是身份域公钥绑定可能带来挑战。维持大型身份表的成本和在服务器侧映射的公钥会产生额外维护费用，例如，设备必须在服务器上预注册。为简化公钥和显示公钥的实体之间的绑定，更好的方式是使用IBC，例如[IETF RFC 6507]中规定的ECCSI公钥进行鉴权。与ITU-T X.509证书和原始公钥不同，IBC中的公钥采用实体身份的形式。这有助于消除公钥和显示公钥实体之间绑定的必要性。

IBS被用作TLS的原始公钥时，签名和散列算法在握手期间协商。TLS客户端和服务器之间的握手遵守[IETF RFC 7250]定义的流程和[IETF RFC 8446]的TLS 1.3，但受到作为签名方案的IBS算法的支持。

接下来，基于[IETF RFC 7250]开发的TLS-IBS协议，和使用ECCSI [IETF RFC 6507]、IBS1 (Hess-IBS)、IBS1 (Cha-Cheon-IBS)以及SM9-IBS [ISO/IEC 14888-3]作为签名算法的TLS 1.3规定如下：

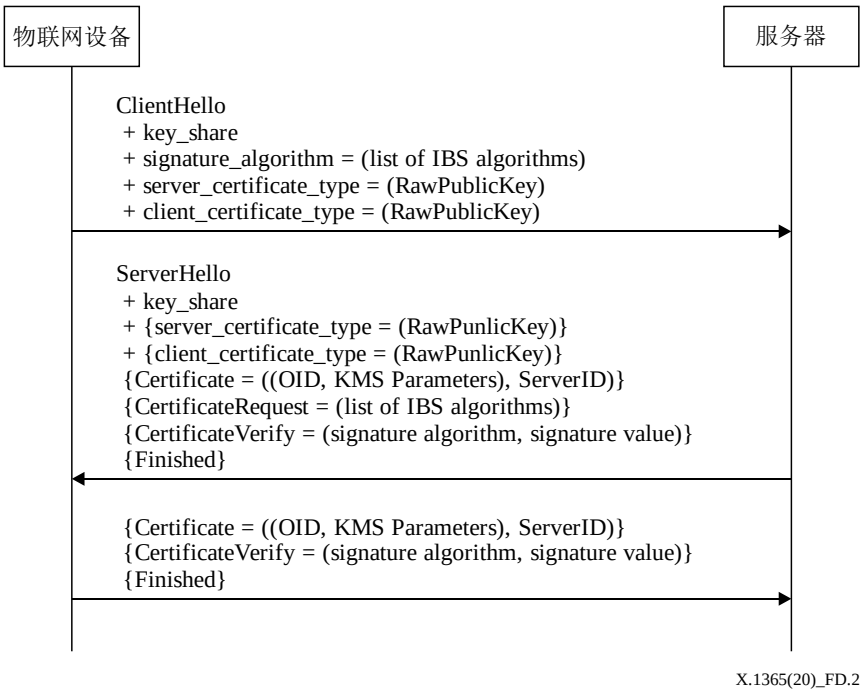
1) 物联网设备发送包括 extension key_share、signature_algorithms、server_certificate_type 和 client_certificate_type 在内的 ClientHello 至服务器，表明其支持原始公钥和 IBS 算法。

2) 服务器发送包括 extension key_share、server_certificate_type、client_certificate_type、Certificate、CertificateRequest、CertificateRequest 和 Finished 在内的 ServerHello 至物联网设备，表示原始公钥受到支持，并在证书部分包括其身份（ServerID）、KMS 参数（OID、KMS 参数）。第 D.2.3 款规定了 KMS 参数的数据结构。服务器拥有的使用私钥生成的签名被包括在 CertificateVerify 信息中。

3) 在验证服务器的身份和签名之后，物联网设备发送其原始公钥（Certificate、CertificateVerify 和 Finished）至服务器。物联网设备在证书区域包含其身份（ClientID）和 KMS 参数（OID、KMS 参数），这是客户端的原始密钥。第 D.2.3 款规定了 KMS 参数的数据结构。使用客户端私钥生成的签名涵盖在内。

4) 剩余步骤与[IETF RFC 8446]中的 TLS 1.3 相同。

见图 D.2。



图D.2 – TLS-IBS

D.2.1 ClientHello

ClientHello信息格式与TLS 1.3 [IETF RFC 8446]中规定的相同，但需要为IBS扩展签名算法的值。

ClientHello信息告诉服务器客户端支持的证书或原始公钥类型，以及客户端期待从服务器收到的证书类型。ClientHello信息包括期望的基于客户端偏好顺序的IBS算法。在TLS 1.3中为签名算法定义了名为SignatureScheme的数据结构。为支持IBS算法，必须按照如下进行扩展：

```
enum {
    ...
  /* IBS signature algorithm */
   eccsi_sha256 (0x0704),
   ibs1_sha256(0x0705)
```

ibs2_sha256(0x0706)

sm9_ibs_sm3(0x0707)

/* Reserved Code Points */

private_use (0xFE00..0xFFFF),

(0xFFFF)

} SignatureScheme;

扩展签名算法的代码点详情见the TLS registry [b-IANA TLS REG]。

D.2.2 ServerHello

ServerHello信息格式与TLS 1.3 [IETF RFC 8446]中规定的相同。SignatureScheme被按照与Client_Hello相同的方式扩展。

D.2.3 服务器证书

对于服务器证书，[b-IEF RFC 7250]中定义证书结构为RawPublicKey。同[IETF RFC 7250]中一样，使用数字结构subjectPublicKeyInfo来规定原始公钥及其密码算法。在subjectPublicKeyInfo结构中定义了两个字段：算法和参数。算法规定了原始公钥用的密码算法，以OID代表；参数字段提供了与算法相关的必要参数。服务器身份应位于subjectPublicKey部分。

注 – 身份须遵守附录I定义的形式。

```
subjectPublicKeyInfo ::= SEQUENCE {
        algorithm                   AlgorithmIdentifier,
        subjectPublicKey                    BIT STRING
}
AlgorithmIdentifier ::= SEQUENCE {
        algorithm           OBJECT IDENTIFIER,
        parameters          ANY DEFINED BY algorithm OPTIONAL
}
```

当使用IBS算法时，身份被用作原始公钥，可以被转换成为OCTET字符串。因此，证书和subjectPublicKey结构可以被重复使用而无需更换。

AlgorithmIdentifier结构的算法字段是使用的IBS算法的对象ID。除此之外，还有必要告诉同级发放者使用的公共参数集。信息可携带在AlgorithmIdentifier的参数字段的负载中。对应上述算法，公共参数结构分别为ECCSIPublicParameters、BFPublicParameters、BFPublicParameters和SM9PublicParameters，如附件B所定义。

为支持基于TLS协议的IBS算法协议生成信息CeritificateVerify，需要为签名值定义一个数据结构。

- ECCSI的数据结构定义如下（基于[IETF RFC 6507]）：

```
ECCSI-Sig-Value ::= SEQUENCE {
   r INTEGER,
   s INTEGER,
   pvt  OCTET STRING
```

}

其中，vt ([IETF RFC 6507]定义的PVT) 被编码为0x04 || x-coordinate of [v]G || y-coordinate of [v]G。

- IBS1数据结构定义如下：

```
IBS1-Sig-Value ::= SEQUENCE {
    r INTEGER,
    s ECPoint
  }
ECPoint ::= OCTET STRING 定义于[IETF RFC 5480]
```

- IBS2数据结构定义如下：

```
IBS2-Sig-Value ::= SEQUENCE {
    r ECPoint,
    s ECPoint
  }
```

- SM9-IBS的数据结构定义如下：

```
SM9-Sig-Value ::= SEQUENCE {
    r INTEGER,
    s ECPoint
  }
```

欲在TLS中使用签名算法，签名算法需要OID。表D.1显示了被用于TLS的IBS签名算法所需的基本信息。

表D.1 – 基于身份的签名算法

密钥类型	文件	OID
ISO/IEC 14888-3 ibs-1	ISO/IEC 14888-3：BS-1机制	1.0.14888.3.0.7
ISO/IEC 14888-3 ibs-2	ISO/IEC 14888-3：IBS-2机制	1.0.14888.3.0.8
SM9-IBS	ISO/IEC 14888-3：中国IBS机制	1.2.156.10197.1.302.1
基于身份的基于椭圆曲线的无签名（ECCSI）	[IETF RFC 6507]第5.2节	1.3.6.1.5.5.7.6.29

D.2.4 客户端证书

为支持IBS，客户端证书采用与服务器证书相同的方式被扩展。

D.3 EAP-TLS-IBS

在本条款中，EAP-TLS鉴权协议被扩展以支持IBS。网络侧和UE侧都被提供了基于身份的证书，包括身份、用于签名的私钥和KMS公共参数（例如，[IETF RFC 6507]中定义的KPAK）。见图D.3。

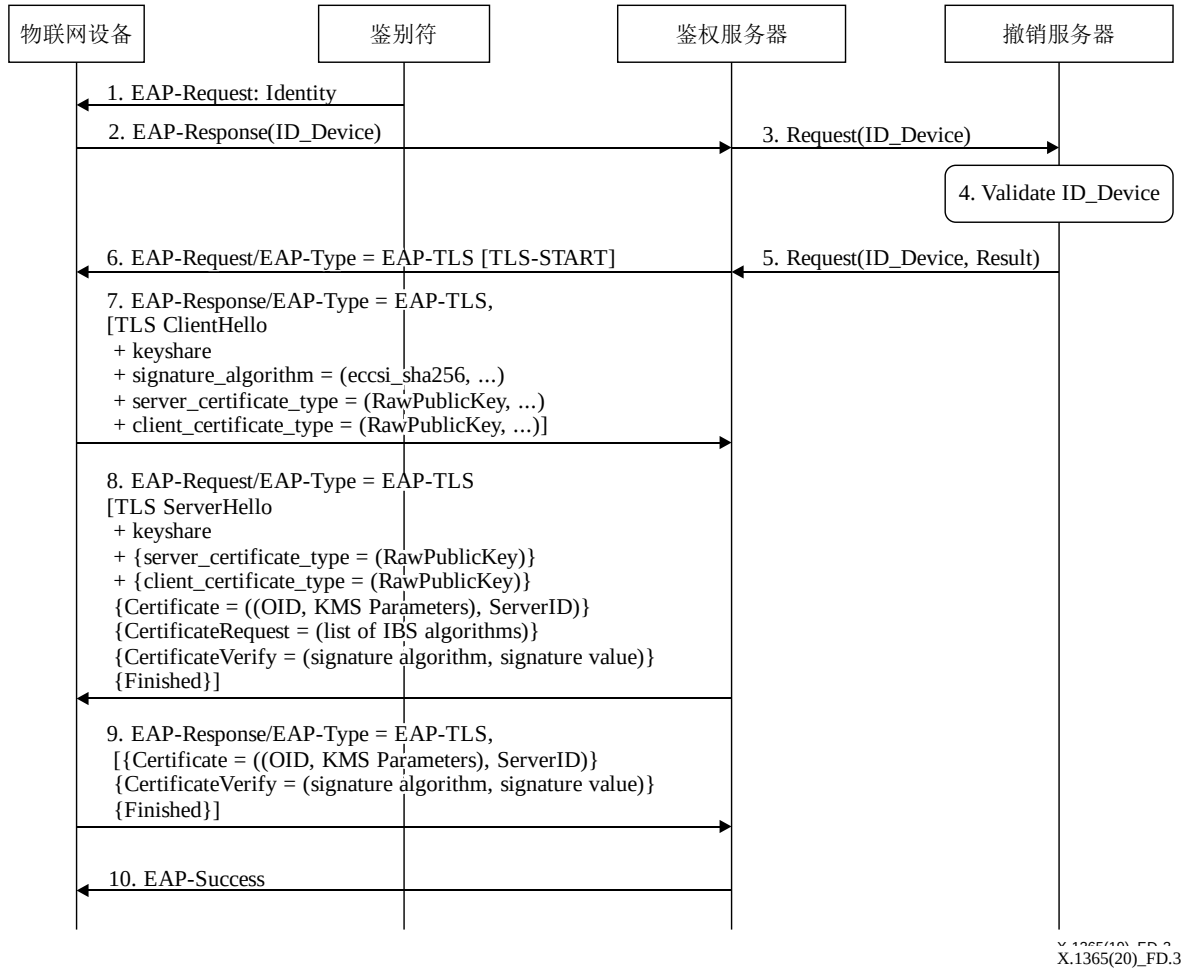
EAP-TLS被按照如下修改。

1) 与EAP-TLS相同；
2) 在接到与UE身份（ID_UE）相关的EAP-response之后；
3) AU向RSF发送ID_UE用于验证；
4) RSF基于存储的撤销清单验证ID_UE；
5) RSF将验证结果返回给AU；

6) 若ID_UE有效，则AU向UE发送EAP-TLS启动信息；

7-9) 与上述描述的TLS-IBS相同；

10 EAP-Success。



图D.3 – AP-TLS-IBS

D.3.1 EAP-Request

EAP-Request信息格式与[IETF RFC 5216]中规定的相同。

D.3.2 EAP-Response

EAP-Response信息格式与[IETF RFC 5216]中规定的相同。

D.3.3 ClientHello

ClientHello信息格式与第D.2.1款中的信息相同。

D.3.4 ServerHello

ServerHello信息格式与第D.2.2.款中的信息相同。

D.3.5 服务器证书

服务器证书格式与第D.2.3款中的格式相同。

D.3.7 客户端证书

客户端证书格式与第D.2.4款中的格式相同。

D.4 EAP-PSK-ECCSI

在本条款中，EAP-PSK被扩展以支持对IBS算法之一的ECCSI进行验证。UE和AU都被提供了基于身份的证书，包括身份、SSK、PVT和[IETF RFC 6507]中定义的作为计算参数的KPAK。

采用提供的证书，UE和AU能够基于静态Diffie-Hellman，通过交换身份信息和PVT来导出对称密钥，之后使用各实体的SSK。例如，一个UE可在收到AU的身份及其PVT之后得出一个密钥，分别用ID_AU和PVT_AU表示如下：

K_UE = [SSK_UE](KPAK+[hash(G || KPAK || ID_AU || PVT_AU)]PVT_AU))

其中，G是KMS用于为UE和网络生成密钥使用的椭圆曲线的生成点，由KMS同SSK、PVT和KPAK等一起被提供给UE和AU。散列函数的使用遵守[IETF RFC 6507]的附件A。

同样的，AU在收到UE提供的身份和PVT之后也可以得出如下K_AU：

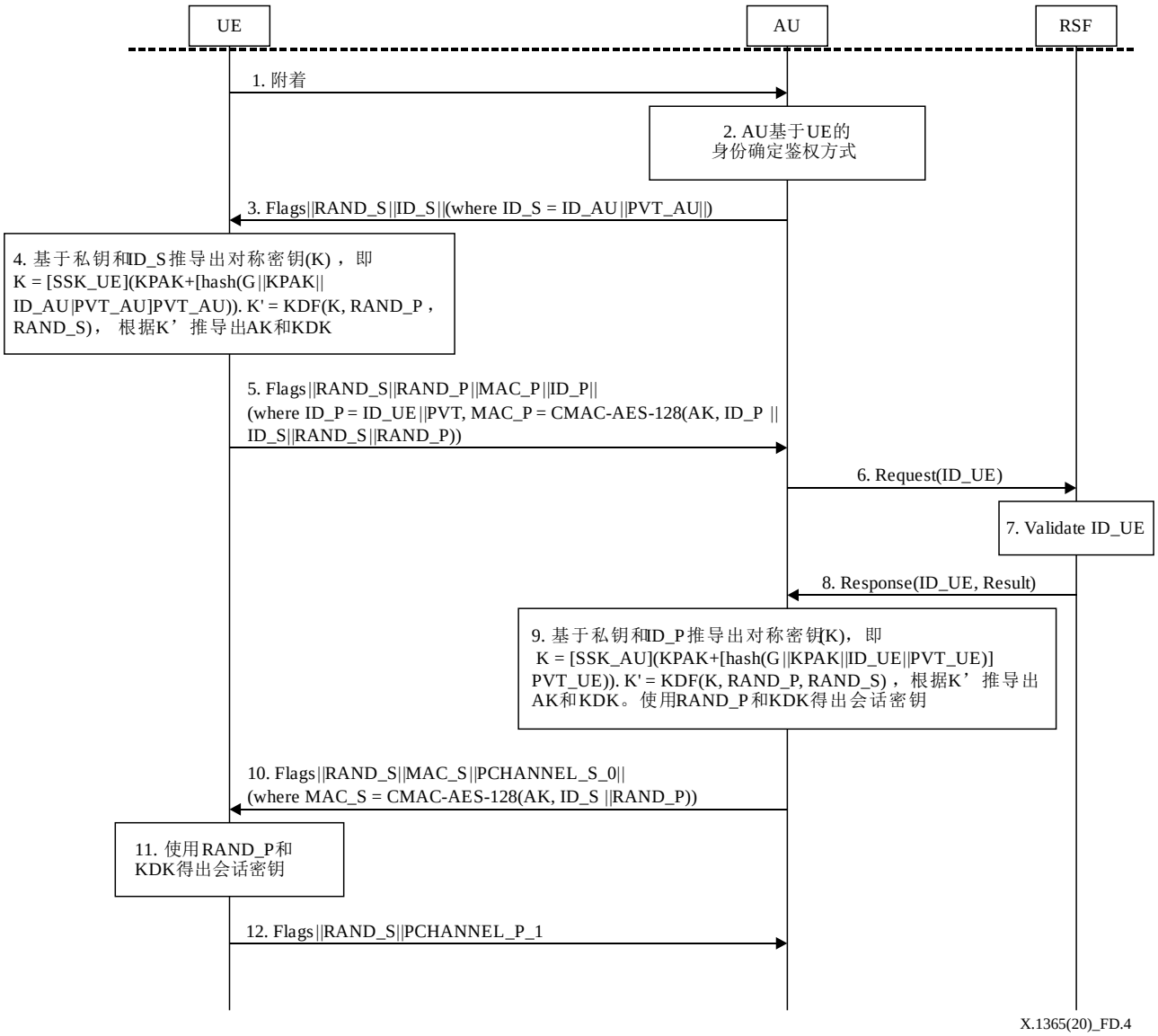
K_AU = [SSK_AU](KPAK+[hash(G || KPAK || ID_UE || PVT_UE)]PVT_UE))

可证明K_UE事实上等于K_AU。

利用上述属性，EAP-PSK可被用于如下手动鉴权。

1) UE 向 AU 发送一个附着请求，表明 EAP-PSK 须被用于手动鉴权。
2) AU 验证鉴权类型，并决定鉴权方式。
3) AU 向 UE 发送关于 EAP-PSK 的首条信息，其中一个身份字段包含 ID_AU 和 PVT_AU，以及 EAP-PSK 所要求的一个随机数 RAND_S。
4) UE 推导出一个对称密钥 K = [SSK_UE](KPAK+[hash(G || KPAK || ID_AU || PVT_AU)]PVT_AU))。UE 生成一个随机数 RAND_P，并进一步得出 K' = KDF(K, RAND_P, RAND_S)。UE 基于[b-IETF RFC4764]为 EAP-PSK 推导出鉴权密钥（AK）和密钥推导密钥（KDK）。
5) UE 向 AU 发送关于 EAP-PSK 的第二条信息，其中包含用于鉴权的 RAND_S、RAND_P、MAC_P (MAC_P=CMAC-AES-128(AK, ID_P||ID_S||RAND_S||RAND_P))，以及一个由 ID_UE 和 PVT_UE 构成的身份字段。
6) AU 发送 ID_UE 至 RSF 用于验证。
7) RSF 根据其撤销列表验证 ID_UE。
8) RSF 将验证结果发回 AU。
9) 若 ID 有效，则 AU 得出一个对称密钥 K = [SSK_AU](KPAK+[hash(G || KPAK || ID_UE || PVT_UE)]PVT_UE))。AU 进一步得出 K' = KDF(K, RAND_P, RAND_S)。AU 基于[IETF RFC 4764]从信息中得出 AK 和 KDK。AU 基于从信息接收的 MAC_P 对 UE 鉴权。AU 进一步基于 RAND_P 和 KDK 得出会话密钥。
10) AU 发送关于 EAP-PSK 的第三条信息至 UE，使用 MAC_S (MAC_S=CMAC-AES-128(AK, ID_S||RAND_P))用于鉴权以及 EAP-PSK 要求的其他字段。
11) UE 使用收到的 MAC_S 来鉴权 AU，并使用之前推导出的 RAND_P 和 KDK 导出会话。
12) UE 发送关于 EAP-PSK 的最后一条信息至 AU 以结束 EAP-PSK 鉴权流程。

见图D.4。



图D.4 – EAP-PSK--ECCSI

D.4.1 附着

本信息模仿鉴权流程。

D.4.2 EAP-PSK--ECCSI首条信息（图D.4的信息3）

首条EAP-PSK--ECCSI信息由服务器发送给对等网络。格式如下：

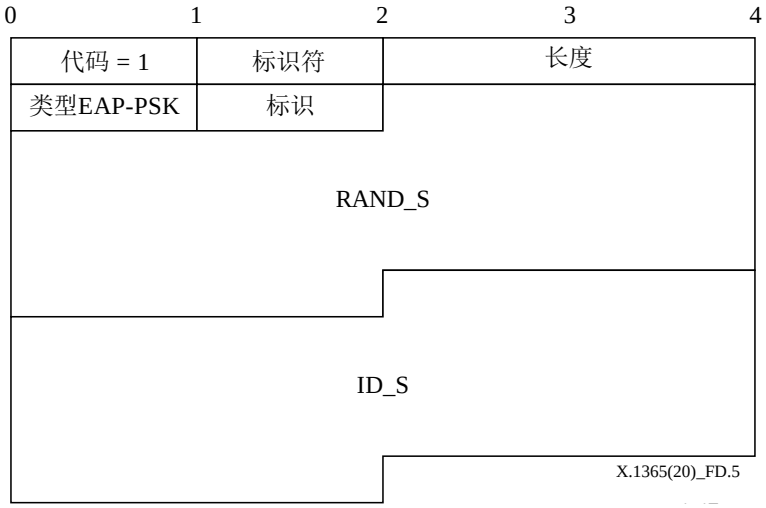
首条EAP-PSK--ECCSI信息由如下部分组成：

一个1字节标记字段

一个16字节随机数：RAND_S

一个可变长字段传达服务器的NAI：ID_S。这一字段的长度从EAP长度字段推导。这一NAI的长度不得超过966字节。这一限制旨在避免存储碎片问题。

图D.5显示了关于EAP-PSK的首条信息的格式范例。



图D.5 – EAP-PSK格式

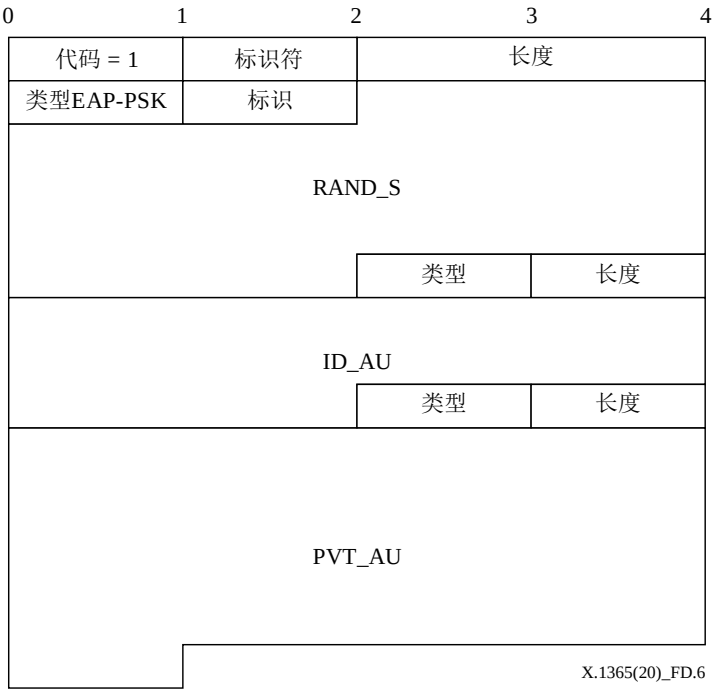
为支持基于IBC的EAP-PSK鉴权，EAP-PSK协议的ID_S被用于携带ID_AU和PVT_AU。ID_S和PVT_AU在标签、长度和矢量（TLV）数据结构中携带，其中首个八位字节携带标签指示器，第二个是长度字节，表示依据的字节长度。矢量字段携带值。

表D.2定义了与EAP-PSK一同使用的ID和PVT的TLV

表D.2 – 身份和公共验证令牌的标签、长度和矢量

	标签	长度	值
身份	1	可变 (≤255)	由服务提供商定义
PVT	2	65	十六进制数字

图D.6显示在ID_S字段携带身份和PVTEAP-PSK—ECCSImessage的格式。



图D.6 – M EAP-PSK--ECCSI的信息格式

D.4.3 EAP-PSK--ECCSI第二条信息（图D.4信息5）

第二条EAP-PSK-ECCSI信息由对等网络发送给服务器。格式由以下部分组成：

– 一个1字节标记字段；

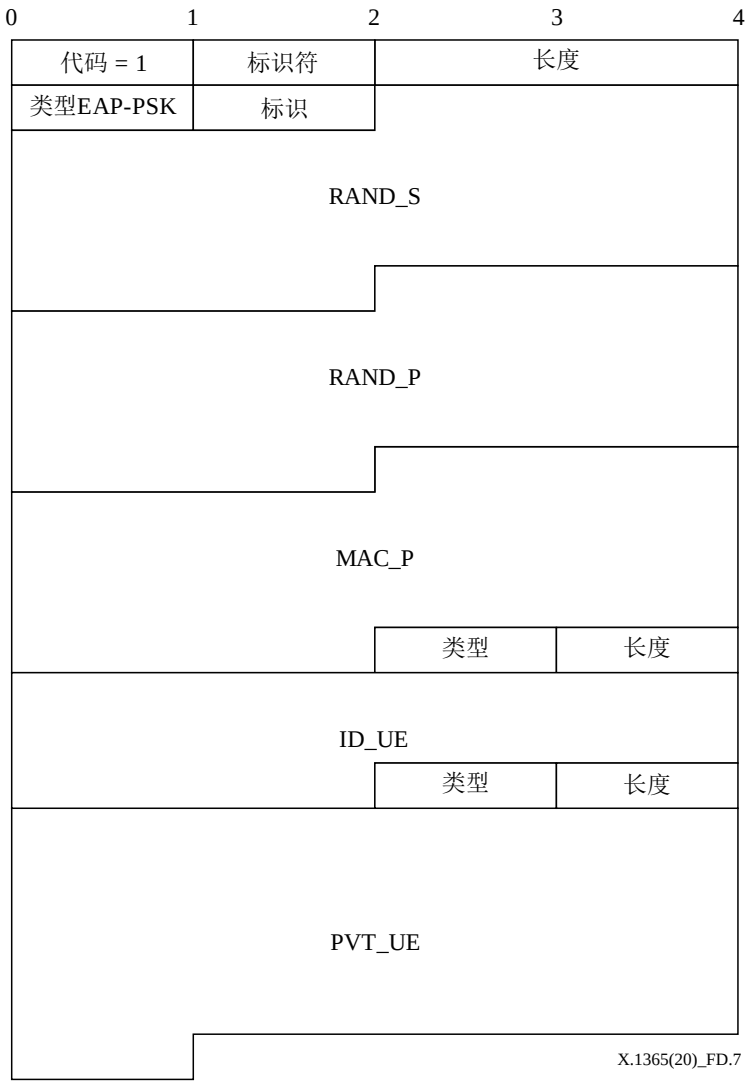
– 服务器在作为会话ID的首个EAP-PSK--ECCSImessage (RAND_S)中发送的16字节随机数；

– 一个16字节随机数：RAND_P；

– 一个16字节媒体接入控制（MAC）：MAC_P；

– 一个传达对等网络NAI的可变长度字节：ID_P。这一字段的长度从EAP长度字段推导。这一NAI的长度不得超过966字节。

同样的，EAP-PSK的ID_S字段被用于承载ID_UE和PVT_UE字节。图D.7显示第二条EAP-PSK信息的格式。



图D.7 – EAP-PSK--ECCSI的第二条信息格式

D.4.4 EAP-PSK--ECCSI第三条信息（图D.4信息10）

第三条EAP-PSK--ECCSI信息由服务器发送给对等网络。格式与[IETF RFC 4764]提供的格式相同。

D.4.5 EAP-PSK--ECCSI第四条信息（图D.4-1信息12）

第四条EAP-PSK-ECCSI信息由对等网络发送给服务器。格式与[IETF RFC 4764]提供的格式相同。

附录I

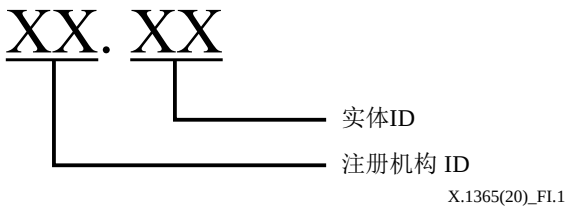
身份命名

（本附录非本建议书不可分割的组成部分）

物联网应用中的ID可以是终端或者物联网平台的ID。ID是服务于识别目的的名称。ID是对物体的方便表示，并允许该物体，比如，在数据库或通信协议中被引用或定址。为了实现这一功能，ID必须唯一，或者在一个独立的系统中唯一。例如，邮编在一个国家中是唯一的，ID的唯一性是在某个范围之内。此外，ID不仅仅用于一个单独物体，也可以用于实现对一组物体的统一管理和对这一群组的操作。

OID [b-ITU-T X.660]、[b-ITU-T X-Sup.31]由ISO/IEC和ITU-T共同制定，具有多个特性。OID具有分层树状结构，可灵活地扩展其层次和ID长度。一个OID对应OID树的一个节点，能够识别万物（物理或虚拟、设备或非设备），并能够将它们与全球信息和通信基础设施相连。树根包含以下三个弧：0（ITU-T）、1（ISO）和2（joint-iso-itu-t）。树上的每个节点都由被句点隔开的一系列整数表示，对应从根部通过一系列祖先节点到节点的路径。注册机构ID的每个层级都应由上一层级的注册机构分配。例如，表示中国国家IC卡注册中心的OID1.2.156.20005是由1.2.156 （ISO.member.china），中国国家OID注册中心的OID分配。

一个完整的OID可以是注册机构ID和实体ID的结合，这两个组成部分由句点隔开，如图I-1所示。若公司由上级注册机构注册，只需设计实体ID。



图I.1 – 对象完整OID结构

例如，实体ID须具备表I.1所列结构。

表I.1 – 实体ID的详细信息

字节	组成部分	解译
1	版本和保留	实体ID的版本为4比特，未来保留位数为4比特
2	业务	业务类型
3~11	失效时间	身份的失效时间，Unix时间的发布时间为5字节，有效期（秒）为4字节
12	类型	无意义数字值为0，MAC为1，IMSI为2
13	长度（值*l*）	数值部分大小（比特），MAC为6，IMSI为8.
14~13+*l*	值	个人识别号

当使用MAC作为个人识别号时实体ID为19字节，当使用IMSI时为21字节。IMSI通常以15位数表示，第一个数字不为零，除非是测试网络[b-ITU-T E.212]。在IMSI之前填充零至16位数，一位数使用4比特，8字节足够一个IMSI使用。

物联网平台维护一个寻址列表。在终端设备首次注册时，平台将增加包含设备ID和IP地址的一行。通过所有列表中的设备的ID，将获取与设备对应的IP地址。见表I.2。

表I.2 – 寻址列表示例

标识符	IP地址
1.2.9c.4e25.10.1.5b3e408003c26700.1.6.38B1DBC3156F	192.168.0.1

附录II

支持IBC的KMIP扩展

（本附录非本建议书不可分割的组成部分）

KMIP可被按照如下扩展来支持所需的KMS的IBC操作，尤其是分别在C.1和C.4中定义的使用KMIP的系统初始化和KMIP操作的私钥生成。

创建密钥对的请求负载由表II.1中的部分构成。

表II.1 – 请求负载

对象	是否必须	描述
私钥模板属性	是	规定当**IBSetup**函数生成*ib.msk*和*ib.pubparam*的属性。

私钥模板属性须包括表II.2列出的属性。

表II.2 – 私钥模板属性

对象	是否必须	编码	描述
密码算法	是	枚举，见表II.3	规定**IBSetup**函数
密码长度	否	整数	规定作为椭圆曲线基础的素域的特征的比特长度
密码使用掩膜	是	整数	规定应为密钥生成签名的*ib.msk*的使用。**IBExtract**本质上是签名过程。
密码域参数	是	对象	为选择系统参数（例如所使用的椭圆曲线）规定更多参数。
密码参数	是	对象	规定其他函数，例如散列函数，须与**IBExtract**函数一起使用。

密码算法须为表II.3所列的值之一。

表II.3 – 密码算法（密钥生成）

名称	值
IBC-KGA-BB1	00000030
IBC-KGA-BF	00000031
IBC-KGA-ECCSI	00000032
IBC-KGA-SK	00000033
IBC-KGA-SM9	00000034

密码长度须为等于或大于110的值。

密码使用须被设置为00000001（签名）。

密码域参数须包括表II.4所列属性。

表II.4 – 密码域参数

对象	是否要求	编码	描述
QLength	否	INTEGER	规定选中*ib.msk*的群组的顺序的比特长度
建议的曲线	是	枚举，见表II.5	规定使用的曲线
配对类型	否	枚举，见表II.6	若使用，规定一个基于身份的算法中的配对
域名	否	TEXT STRING	为生成的系统参数*ib.pubparam*规定唯一名称。
域串行	否	INTEGER	为生成的系统参数*ib.pubparam*规定版本号。

建议的曲线须为表II.5所列的值之一。

表II.5 – 建议的曲线

名称	值
IBC-CURVE-SS1	00000070
IBC-CURVE-SS2	00000071
IBC-CURVE-BN-254-1	00000072
IBC-CURVE-BN-256-1	00000073
IBC-CURVE-BN-256-2	00000074
IBC-CURVE-BN-382-1	00000077
IBC-CURVE-BLS-12-381-1	0000007A
IBC-CURVE-BLS-12-442-1	0000007B
IBC-CURVE-BLS-12-455-1	0000007C
IBC-CURVE-BLS-12-461-1	0000007D
IBC-CURVE-KSS-16-340-1	0000007E
IBC-CURVE-KSS-18-348-1	0000007F

配对类型须为表II.6所列的值之一。

表II.1-6 – 配对类型

名称	值
Weil-Pairing	00000001
Tate-Pairing	00000002
Optimal-Ate-Pairing	00000003

密码参数须包括表II.7所列属性。

表II.7 – 密码参数

对象	是否要求	编码	描述
散列算法	是	枚举，见表II.8	规定须被用于密钥生成函数的散列函数。
密钥组	否	枚举，见表II.9	规定若使用配对，私钥钥须在哪个群组生成。

散列算法须为表II.8的值之一。

表II.8 –密码算法（散列）

名称	值
SHA224	00000040
SHA256	00000041
SHA384	00000042
SHA512	00000043
SHA3-224	00000044
SHA3-256	00000045
SHA3-384	00000046
SHA3-512	00000047
SM3	00000048

私钥组须为表II.9所列值之一。

表II.9 – 私钥组

名称	值
IBC-PRK-GROUP1	00000001
IBC-PRK-GROUP2	00000002
IBC-PRK-TWOGROUPS	00000003

创建密钥对的响应负载构成见表II.10。

表II.10 – 响应负载

对象	是否必须	描述
私钥唯一标识符	是	可被用于接入*ib.msk*的新创建的私钥对象的唯一标识符。标识符编码为文本字符串。
公钥唯一标识符	是	可被用于接入*ib.pubparam*的新创建的公钥对象的唯一标识符。标识符编码为文本字符串。

get操作的请求负载构成见表II.11。

表II.11 –请求负载

对象	是否必须	描述
公钥唯一标识符	是	可用于接入*ib.pubparam*的公钥对象的唯一标识符。标识符编码为文本字符串。

get响应负载构成如表II.12：

表II.12 – 响应负载

对象	是否必须	描述
对象类型	是	对象类型
唯一标识符	是	对象的唯一标识符
公钥	是	公钥结构包含IBC公共参数*ib.pubparam*的数据

唯一ID须与get请求负载中发送的公钥唯一ID相同。

对象类型须为00000003 （公钥）

公钥字段的密钥块构成见表II.13。

表II.13 – 公共密钥字段中的密钥块

对象	是否必须	编码	描述
密钥格式类型	是	枚举，见表II.14。	规定密钥值格式。
密钥压缩	否	枚举。	规定密钥值是否应被压缩。
密钥值	是	IBC公共参数透明密钥结构。	新定义的IBC公共参数透明密钥结构。
密码算法	是	枚举，见表II.15。	与创建密钥对请求负载相同。

密钥格式类型须为表II.14的值。

表II.14 –密钥格式类型

名称	值
透明IBC公共参数	00000016

密钥压缩须为00000001（未压缩）或00000002（压缩素数）。

密钥值须具备表II.15的属性。

表II.15 – 密钥值

对象	是否必须	编码	描述
P	否	大整数	对于基于素域的曲线，P是素域的特征(p)。
Q	否	大整数	Q是计算密码操作的点子群(*G*1)的阶。
J	否	大整数	J是J*Q = X-1的代数余子式，其中X是指定曲线的点子群。
P1 STRING	是	字符串	对于基于配对的算法，P1是配对群组*G*1的发生器。对于非基于配对的算法，P1是工作点子群的发生器。
P2 STRING	否	字符串	对于基于配对的算法，P2是配对群组*G*2的生成器。

表II.15 – 密钥值

对象	是否必须	编码	描述
sP1 STRING	否	字符串	sP1是[*ib.msk*]P1的纯量结果或*ib.msk*与P1的整数部分的纯量结果。
sP2 STRING	否	字符串	对于基于配对的算法，sP2是[*ib.msk*]P2的纯量结果或*ib.msk*与P2的整数部分的纯量结果。
sP3 STRING	否	字符串	对于一些基于配对的算法，尤其是使用BB1密钥生成函数的算法，sP3是*ib.msk*与P1的另一个整数部分的纯量结果。
公共对 STRING	否	字符串	对于一些基于配对的算法，公共配对是pairing(P1, [s]P2) 或pairing([s]P1, P2)或pairing(P1, P2)的结果，其中s是*ib.msk* ，对于SM9、SK-KEM或SK-KEM或([s1]P1, [s2]P2)之类的BB1-KEM，s1、s2是*ib.msk*的整数部分。

表II.16中列出新的标签定义。

表II.16 – 标签定义

对象	标签值
配对类型	420100
私钥群组	420101
域名	420102
域串行	420103
P1字符串	420104
sP1字符串	420105
P2字符串	420106
sP2字符串	420107
sP3字符串	420108
公共配对字符串（STRING）	420109

签名请求负载构成如表II.17。

表II.17 – 签名请求负载

对象	是否必须	描述
唯一标识符	否	*ib.msk*密钥用于**IBExtract**操作的可管理的密码对象的唯一标识符。若忽视，则服务器须使用ID占位符值作为唯一标识符。
密码参数	否	密码参数可规定须用来生成私钥的群组。
数据	是	数据规定须被提取密钥的身份值。

密码参数须包括表II.18所列属性。

表II.18 – 密码参数

对象	是否必须	密码	描述
私钥群组	否	枚举，见表II.9。	规定须被生成私钥的群组(*G*1或*G*2)

参考书目

[b-ITU-T E.101] ITU-T E.101建议书 (2009)，E系列建议书中用于公众电信业务和网络的标识符（名称、号码、地址和其它标识符）的术语定义。

[b-ITU-T E.212] ITU-T E.212建议书（2016年），公共网络和订阅的国际识别计划。

[b-ITU-T X.509] ITU-T X.509建议书（2019年），信息技术 – 开放系统互联 – 目录：公钥和属性证书框架。

[b-ITU-T X.660] ITU-T X.660建议书（2011年），信息技术 – 对象标识符注册机构操作流程：国际对象标识符树的通用程序和顶层弧。

[b-ITU-T X.1361] ITU-T X.1361建议书（2018年），基于网关模型的物联网安全框架。

[b-ITU-T X-Sup.31] ITU-T X系列建议书 – 增补31（2017年），ITU-T X.660 –关于物联网使用对象标识符指南的增补。

[b-ITU-T Y.2720] ITU-T Y.2720建议书 (2009)，NGN身份管理框架。

[b-ITU-T Y.4000] ITU-T Y.4000/Y.2060建议书（2012年），物联网概述。

[b-ITU-T Y.4100] ITU-T Y.4100/Y.2066建议书（2014年），物联网的共同要求。

[b-ISO/IEC 9798-3] ISO/IEC 9798-3:2019. *IT Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques*.

[b-ETSI TR 118 508] ETSI TR 118 508 V1.0.0 (2014), *Analysis of Security Solutions for the oneM2M System*.
<https://www.etsi.org/deliver/etsi_tr/118500_118599/118508/01.00.00_60/tr_118508v010000p.pdf>

[b-ETSI TS 133.501] ETSI TS 133 501 V15.2.0 (2018), *5G; Security architecture and procedures for 5G system (3GPP TS 33.501 version 15.1.0 Release 15)*.
<https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.01.00_60/ts_133501v150100p.pdf>

[b-GM/T 0044.2] GM/T 0044.2-2016, *Identity-based cryptographic algorithms SM9 – Part 2: Digital signature algorithm*.

[b-GSMA SGP.02] GSMA Official Document SGP.02 Version 3.1 (2016), *Remote Provisioning Architecture for Embedded UICC – Technical Specification*.

[b-IANA TLS REG] Internet Assigned Numbers Authority (IANA), *Transport Layer Security (TLS) Parameters*. Website available, last viewed 2019-07-12.
<https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml>

[b-IEEE 1363] IEEE 1363-2000, *IEEE Standard Specifications for Public-Key Cryptography*.

[b-IEEE P1363.3] IEEE P1363.3/D9 (May 2013), *IEEE Standard for Identity-Based Cryptographic Techniques using Pairings*.

[b-IETF RFC 3748] IETF RFC 3748 (2004). *Extensible Authentication Protocol (EAP)*.

[b-OASIS KMIP] OASIS (2016), *Key Management Interoperability Protocol Specification Version 1.3*. <http://docs.oasis-open.org/kmip/spec/v1.3/os/kmip-spec-v1.3-os.pdf>

[b-Barreto] Barreto, P. S. L. M., Libert, B., McCullagh, N., Quisquater, J.-J. (2005). Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In: Roy B. (ed.). *Advances in Cryptology – ASIACRYPT 2005, pp. 515-532. Lecture Notes in Computer Science*, vol. 3788. Berlin: Springer

[b-Chen] Chen, L., Malone-Lee, J. (2005). Improved identity-based signcryption. In: Vaudenay S. (ed). *Public Key Cryptography – PKC 2005, pp. 362-379. Lecture Notes in Computer Science*, vol. 3386. Berlin: Springer.

[b-Ducas] Ducas, L., Lyubashevsky, V., Prest, T. (2014). Efficient identity-based encryption over NTRU lattices. In: Sarkar P., Iwata T. (eds). *Advances in Cryptology – ASIACRYPT 2014, pp. 22-41. Lecture Notes in Computer Science*, vol. 8874. Berlin: Springer.

[b-Freeman] Freeman, D., Scott, M., Teske, E. (2010). A taxonomy of pairing-friendly elliptic curves. *J. Cryptol*. **23**, pp. 224–280.

[b-Galbraith] Galbraith, S.D., Paterson, K.G., Smart, N.P. (2008). Pairings for cryptographers. *Discrete Appl. Math*., **156**, pp. 3113-3121.

ITU-T系列建议书

系列A	ITU-T工作的组织
系列D	资费及结算原则和国际电信/ICT的经济和政策问题
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	电话传输质量、电话设施及本地线路网络
系列Q	交换和信令 ，以及相关的测量和测试
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	**数据网、开放系统通信和安全性**
系列Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列Z	用于电信系统的语言和一般软件问题

瑞士印刷
2020年，日内瓦