ICS 35.040
L 80

GM

中华人民共和国密码行业标准

GM/T 0097—2020

射频识别电子标签统一名称解析服务安全技术规范

Security technical specifications for unified name resolution service of RFID

2020-12-28 发布　　2021-07-01 实施

国家密码管理局　　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：中国电力科学研究院有限公司、成都卫士通信息产业股份有限公司、北京智芯微电子科技有限公司、上海复旦微电子集团股份有限公司、北京中电华大电子设计有限责任公司、南方电网科学研究院。

本标准主要起草人：赵兵、许斌、梁晓兵、吕英杰、翟峰、刘鹰、李保丰、曹永峰、孔令达、徐萌、冯云、罗俊、胡川、付建峰、绍兴、杨祎巍、兰天。

射频识别电子标签统一名称解析服务安全技术规范

1 范围

本标准规定了射频识别电子标签统一名称解析服务的系统架构、关键业务流程和安全性要求，定义了名称解析服务器的注册流程、产品电子代码的安全查询流程及相应消息报文格式。

本标准适用于射频识别电子标签统一名称解析服务系统的开发和使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 17901.1 信息技术 安全技术 密钥管理 第1部分：框架

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32915 信息安全技术 二元序列随机性检测方法

GB/T 32918(所有部分) 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 35276—2017 信息安全技术 SM2密码算法使用规范

GM/Z 4001—2013 密码术语

3 术语和定义

GM/Z 4001—2013界定的以及下列术语和定义适用本文件。

3.1

产品电子代码 electronic product code

存储在RFID标签上，为物品提供唯一标识。

3.2

产品电子代码应用系统 electronic product code application system

为访问和持久保存产品电子代码相关数据提供了一个标准的接口，已授权用户可以通过它来读写产品电子代码相关数据，具有高度复杂的数据存储与处理过程，支持多种查询方式。

3.3

产品电子代码信息服务器 electronic product code information service server

保存物品详细信息的服务器，一般由生产商或者产品使用者管理和维护。

3.4

名称解析服务 object name service

提供产品电子代码与存放物品具体信息的服务地址之间的映射关系。

3.5

密钥 key

控制密码变换操作的关键信息或参数。

3.6

密钥管理　key management

密钥的生成、存储、使用、更新、导入、导出和销毁等过程的管理。

4　符号和缩略语

4.1　符号

下列符号适用于本文件。

cert_A：服务器 A 的设备证书

HDR_ans：响应消息头

HDR_req：请求消息头

Hmac(k,msg)：使用密钥 k 对消息 msg 计算消息认证码

ip_A：服务器 A 地址

ip_EPCIS：EPCIS 服务器地址

k_AB：服务器 A 与服务器 B 的会话密钥

k1_AB：服务器 A 与服务器 B 对称加密的会话密钥

k2_AB：服务器 A 与服务器 B 消息认证码校验的会话密钥

MAC_A：服务器 A 生成的消息认证码

PCODE：产品电子代码

pri_A：服务器 A 的设备私钥

prf()：密钥导出函数

prf(msg)：密钥导出函数，对消息 msg 进行数据摘要运算

pub_A：服务器 A 的设备公钥

rand_A：服务器 A 生成的随机数

SIG_A：服务器 A 生成的签名数据

SM2_Enc(pub_key,msg)：使用 SM2 非对称算法，pub_key 作为密钥对输入信息 msg 加密

SM2_Sign (pri_key,msg)：使用 SM2 非对称算法，pri_key 作为密钥对 msg 进行数字签名

SM4_Enc(key,msg)：使用 SM4 对称算法(CBC 模式)，key 作为密钥对消息 msg 加密

u_AB：服务器 A 与服务器 B 的工作密钥

u1_AB：服务器 A 与服务器 B 对称加密的工作密钥

u2_AB：服务器 A 与服务器 B 消息认证码校验的工作密钥

[x]：x 为可选

x|y：x 与 y 串接

4.2　缩略语

下列缩略语适用于本文件。

CA：数字证书认证中心(certificate authority)

CBC：密码分组链接(cipher-block chaining)

EPCIS：产品电子代码信息服务(electronic product code information service)

ONS：对象名称解析服务(object name service)

RFID：射频识别(radio frequency identification)

5 电子标签编码

电子标签的编码规则参见附录 A。

6 ONS 系统架构

ONS 系统由电子标签、标签阅读器、ONS 客户端、本地 ONS 服务器、ONS 基础架构服务器、EPCIS 服务器六部分组成，其中，椭圆区域是 ONS 基础架构服务器，采用三级部署，由各级 ONS 服务器提供产品电子代码到 EPCIS 服务器的地址映射，如图 1 所示。

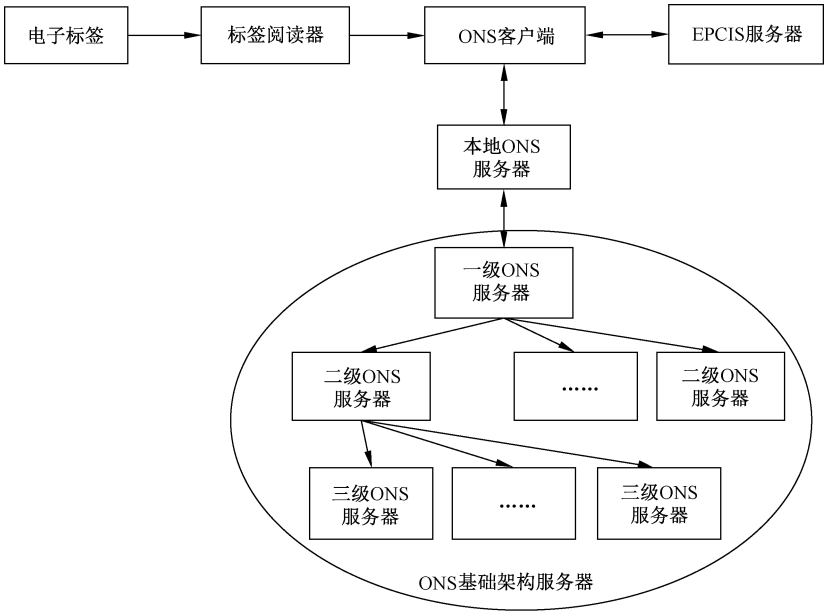

图 1 ONS 系统架构示意图

箭头方向指示了电子标签名称解析服务的查询处理过程。标签阅读器读取物品的产品电子代码后发送到 ONS 客户端，ONS 客户端通过本地 ONS 服务器，向 ONS 基础架构服务器中的各级 ONS 服务器查询，得到存有此物品信息的 EPCIS 服务器地址，然后访问该 EPCIS 服务器获取物品的详细信息。

7 ONS 系统关键业务流程

7.1 ONS 服务器注册

当本地 ONS 服务器加入系统时，应向一级 ONS 服务器注册，使用双方设备证书验证身份合法性，并协商出会话密钥。

当下级 ONS 服务器加入系统时，应向上级 ONS 服务器注册，注册过程中，使用双方设备证书验证身份合法性，并协商出会话密钥。

箭头指示 ONS 服务器间的注册关系，协商产生的会话密钥标识在对应的连线上，例如 k_CA 表示服务器 C 向服务器 A 注册时协商的会话密钥，如图 2 所示。

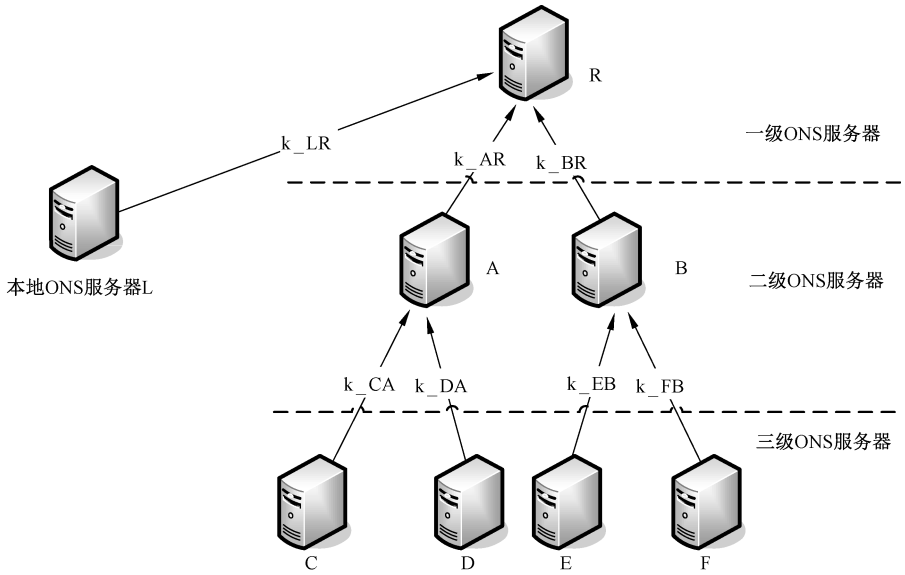

图 2　ONS 服务器注册示意图

ONS 服务器的注册流程见附录 B，通信协议见附录 C。

7.2　安全查询处理

本地 ONS 服务器收到来自 ONS 客户端的产品电子代码查询请求时，首先在本地缓存中查找对应 EPCIS 服务器信息，如果没有找到，则从一级 ONS 服务器开始，通过迭代查询的方式进行解析，直到获得查询结果为止，最后将查询结果返回该 ONS 客户端。

如图 3 所示，典型的 ONS 查询处理流程分为三级迭代 8 个步骤（如果迭代的级数不同，处理步骤相应变化）。

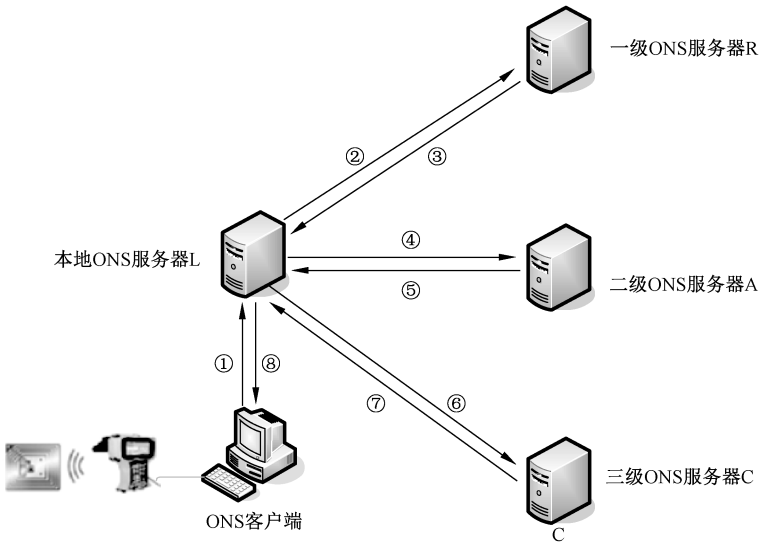

图 3　ONS 查询处理示意图

本地 ONS 服务器与一级 ONS 服务器通信过程中，使用本地 ONS 服务器注册时协商的会话密钥（包含用于数据加密的密钥和用于计算消息认证码的密钥），对 ONS 查询报文进行机密性、完整性、数

据源有效性验证等安全保护。

在向下级服务器迭代查询时，上级 ONS 服务器产生下级 ONS 服务器与本地 ONS 服务器通信的下级工作密钥。该密钥由上级工作密钥加密保护分发给本地 ONS 服务器，同时该密钥使用下级 ONS 服务器注册时协商的会话密钥加密保护，通过本地 ONS 服务器查询消息分发至下级 ONS 服务器，本地 ONS 服务器与下级 ONS 服务器通信过程中，使用该密钥（包含用于数据加密的密钥和用于计算消息认证码的密钥），对 ONS 查询报文进行机密性、完整性、数据源有效性验证等安全保护。

查询报文的交互流程见附录 D，通信协议见附录 C。

8 安全性要求

8.1 密码算法

ONS 系统使用的密码算法应符合密码国家标准和行业标准的要求。

公钥密码算法采用 SM2 椭圆曲线公钥密码算法，应遵循 GB/T 32918。

对称密码算法采用 SM4 分组密码算法，应遵循 GB/T 32907。

密码杂凑算法采用 SM3 密码杂凑算法，应遵循 GB/T 32905。

8.2 随机数安全

ONS 系统使用的随机数应符合密码国家标准和行业标准的要求。

随机数检验应符合 GB/T 32915 的要求。

8.3 密钥管理安全

8.3.1 总体要求

ONS 系统应配置完整的密钥管理措施，在密钥的生成、存储、分发、备份、更新、销毁等内容应符合 GB/T 17901.1 的相关要求。

8.3.2 密钥种类及用途

ONS 系统应遵循“专钥专用”原则，按种类及用途分为设备密钥、会话密钥和工作密钥，密钥类型如表 1 所示。

表 1 密码种类及用途

密钥名称	用途	密钥长度	支持算法
设备密钥	a) 非对称算法使用的设备公私钥对； b) 用于 ONS 服务器注册时设备身份认证和会话密钥协商过程保护	256 比特	SM2
会话密钥	a) 包含用于数据对称加密的密钥和用于计算消息认证码的密钥； b) 用于本地 ONS 服务器与一级 ONS 服务器数据传输加密和完整性保护； c) 用于上级 ONS 服务器向下级 ONS 服务器分发下级工作密钥时加密保护	128 比特	SM4、SM3

表 1（续）

密钥名称	用途	密钥长度	支持算法
工作密钥	a) 包含用于数据对称加密的密钥和用于计算消息认证码的密钥； b) 由上级 ONS 服务器生成，用于下级 ONS 服务器与本地 ONS 服务器之间数据传输加密和完整性保护	128 比特	SM4、SM3

8.3.3 密钥结构

ONS 系统采用三层密钥体系，遵循“逐层保护、专钥专用”原则。位于顶层的设备密钥保护其下层的会话密钥，位于中间层的会话密钥保护底层的工作密钥。

密钥结构层次如图 4 所示。

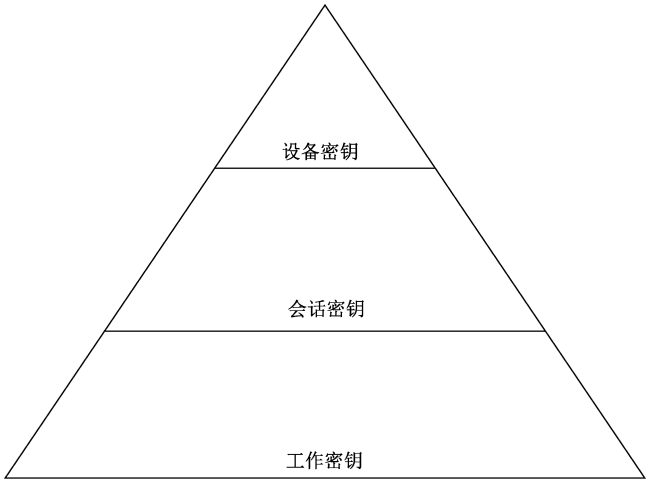

图 4 密钥结构层次图

8.3.4 密钥生成

设备密钥由各 ONS 服务器自己产生，包括设备私钥和设备证书。

会话密钥由 ONS 服务器注册时协商产生，协商过程见附录 B。

工作密钥由上级 ONS 服务器产生，产生过程见附录 D。

8.3.5 密钥分发

各级 ONS 服务器的设备公钥应能被导出，由密钥管理系统签发设备证书后导入设备中，设备私钥无需分发。

会话密钥产生后，无需分发。

工作密钥由上级 ONS 服务器产生后，使用下级 ONS 服务器的会话密钥进行保护，分发给下级 ONS 服务器及本地 ONS 服务器，分发过程见附录 D。

8.3.6 密钥存储

设备密钥应保存在设备非易失性存储装置中，其中设备私钥应有安全保护措施，在任何情况下不能以明文形式出现在设备外部。

会话密钥、工作密钥存储在设备易失性存储装置中，掉电应丢失，应有安全措施保护密钥存储期间的安全。

8.3.7 密钥更新

设备证书有效期一般不大于5年，在设备证书过期前，应提前由数字证书系统重新签发设备证书。

会话密钥有效期不大于24 h，会话密钥过期前，应由下级ONS服务器重新注册，协商新的会话密钥。

工作密钥有效期不大于1 h，在本次查询后过期，下次查询时应由上级ONS服务器重新产生及分发。

8.3.8 密钥备份和恢复

ONS服务器应支持设备密钥备份和恢复功能。备份时应以密文方式备份到安全存储介质中；从安全存储介质恢复时，应提供身份鉴别机制。

会话密钥、工作密钥无需进行备份和恢复。

8.3.9 密钥销毁

ONS服务器应支持设备密钥销毁功能，应提供物理保护机制，当机箱被破坏时，自动置于毁钥状态，并将设备中的密钥销毁。

会话密钥、工作密钥过期后自动销毁。

8.4 硬件安全

ONS服务器应提供安全措施，保证密码算法、密钥、关键数据的存储安全。

所有密码运算应在独立的密码部件中进行。

除必需的通信接口和管理接口以外，不提供任何可供调试、跟踪的外部接口。内部的调试、检测接口应在产品定型后封闭。

8.5 软件安全

ONS服务器所有的安全协议及管理软件应自主实现。

操作系统应进行安全加固，关闭所有不需要的端口和服务。

任何操作指令及其任意组合，不能泄露密钥和敏感信息。

附 录 A
（资料性附录）
射频识别电子标签统一编码规则

A.1 概述

本附录规定了射频识别电子标签的编码规则，包括版本号、行业、省份、管理者、对象种类、单品序列号六部分组成，其中行业代码应符合 GB/T 4754 的规定，省份代码应符合 GB/T 2260 的规定。

A.2 编码原则

表 A.1 编码格式

版本号	行业	省份	管理者	对象种类	单品序列号
2	6	6	22	20	40

如表 A.1 所示，电子标签编码由版本代码、行业、省份、管理者、对象种类、单品序列号 6 个字段组成。版本号 2 位，行业占 6 位(可容纳 64 个行业代码，应符合 GB/T 4754 的规定)，行业有 20 个门类，省份占 6 位(应符合 GB/T 2260 的规定)，管理者占 22 位(可容纳 400 多万个管理者代码)，对象种类占 20 位(可容纳 100 多万个对象种类代码)，单品序列号占 40 位(可容纳一万多亿个单品代码)。

A.3 管理者代码

建议国家权威机构对所有企业单位颁布企业管理代码，用 22 位表示。

A.4 对象种类

每个企业单位对自己拥有物品种类进行分类编码，用 20 位表示。

A.5 单品序列号

每个企业单位对自己的同一种类物品进行顺序编码，用 40 位表示。

附 录 B
（规范性附录）
ONS 服务器注册流程

B.1 概述

本附录规定了服务器的注册流程，包括本地 ONS 服务器向一级 ONS 服务器注册，以及下级 ONS 服务器向上级 ONS 服务器注册两种处理流程。

服务器发起注册请求前，应预先导入所注册服务器的设备证书。服务器注册时，使用双方设备证书验证身份合法性，并使用设备密钥进行保护，协商出会话密钥。

由于本地 ONS 服务器注册和下级 ONS 服务器注册的处理流程是相同的，本标准仅选择其中的本地 ONS 服务器注册过程进行说明。

B.2 注册过程

B.2.1 本地 ONS 服务器注册过程

本地 ONS 服务器 L（以下简称“服务器 L”）向一级 ONS 服务器 R（以下简称“服务器 R”）的注册处理过程如图 B.1 所示。

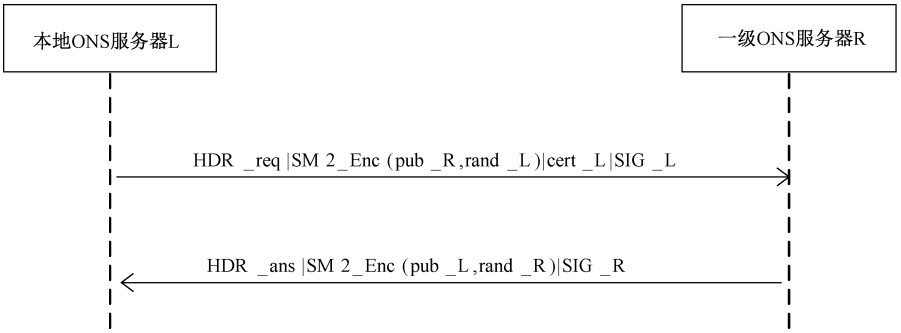

图 B.1 本地 ONS 服务器注册过程

B.2.2 步骤 1 服务器 L 发送注册请求

处理流程如下：

a) 服务器 L 生成随机数 rand_L，长度为 6 字节，使用服务器 R 设备公钥进行 SM2 加密保护，得到随机数 rand_L 密文；

b) 服务器 L 向服务器 R 发送注册请求消息，包含随机数 rand_L 密文、服务器 L 设备证书，并用设备私钥对请求消息进行 SM2 签名；

c) 服务器 R 收到请求消息后，首先验证服务器 L 设备证书身份合法性，验证消息签名是否有效，如果验证不通过，则注册失败；

d) 服务器 R 使用设备私钥，对随机数 rand_L 密文进行 SM2 解密，得到明文 rand_L；

e) 服务器 R 产生随机数 rand_R；

f) 服务器 R 以随机数 rand_L 及 rand_R 作为密钥素材，生成会话密钥 k_LA；

g） 服务器 R 按 B.2.3 要求，向服务器 L 返回注册响应消息。

B.2.3 步骤 2 服务器 R 返回注册应答

处理流程如下：

a） 服务器 R 使用服务器 L 设备公钥进行 SM2 加密保护，得到随机数 rand_R 密文；

b） 服务器 R 向服务器 L 发送注册响应消息，包含随机数 rand_R 密文，并用设备私钥对响应消息进行 SM2 签名；

c） 服务器 L 收到响应消息后，使用服务器 R 的设备证书验证签名是否有效，如果验证不通过，则注册失败；

d） 服务器 L 使用设备私钥，对随机数 rand_R 密文进行 SM2 解密，得到明文 rand_R；

e） 服务器 L 以随机数 rand_L 及 rand_R 作为密钥素材，生成会话密钥。

附 录 C
（规范性附录）
消息协议规范

C.1 概述

本附录定义了 ONS 服务器注册、安全查询等报文格式。

消息协议采用请求响应模式，协议模型由请求者、响应者和它们之间的交互协议组成。通过本协议，请求者将 ONS 服务器注册、安全查询等请求发送给响应者，等待响应者响应返回；响应者接收到请求消息后，检查请求的合法性，处理请求并将结果返回给请求者。

C.2 消息格式

请求消息及响应消息报文格式如下定义：

a） 请求消息报文

请求消息报文格式如图 C.1 所示。

图 C.1 请求消息结构图

版本号：由 1 字节组成。当前版本为 0x0。

消息类型：由 1 字节组成，如表 C.1 定义。

表 C.1 消息类型定义

值	消息类型
1	服务器注册
2	查询本地服务器
3	查询各级服务器

载荷长度：由 2 字节组成，网络字节序，表示请求载荷的长度。

序列号：由 4 字节组成，网络字节序，由请求方维护，从 1 开始递增，可用于防重放。

请求载荷：根据不同的消息类型具体内容不同，由多个字节组成，长度由载荷长度指定。

b） 响应消息报文

响应消息报文格式如图 C.2 所示。

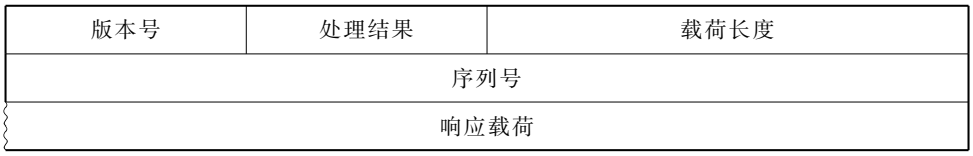

图 C.2 请求消息结构图

版本号：由 1 字节组成。当前版本为 0x0。

处理结果：由 1 字节组成，值为 0 时处理成功，非 0 时处理失败且响应载荷为空（为 0x8 时除外），如表 C.2 定义。

表 C.2　消息类型定义

错误 ID	错误描述
0x00	处理成功
0x01	协议版本错误
0x02	无效的报文类型
0x03	载荷格式无效
0x04	验签失败
0x05	非对称解密错误
0x06	对称解密失败
0x07	MAC 校验失败
0x08	查找失败，返回下级 ONS 服务器地址递归查询
0x09	查找失败，查询结束
0x0A-0xFF	保留

载荷长度：由 2 字节组成，网络字节序，表示请求载荷的长度。

序列号：由 4 字节组成，网络字节序，与请求消息中的序列号值相同，可用于防重放。

响应载荷：根据不同的消息类型具体内容不同，由多个字节组成，长度由载荷长度指定。

C.3　服务器注册消息

本地 ONS 服务器应向一级 ONS 服务器注册，下级 ONS 服务器应向上级 ONS 服务器注册，使用双方设备证书验证身份合法性，并协商出会话密钥。

若发起注册请求的服务器为 L，响应注册请求的服务器为 R，描述消息报文定义如下：

a)　请求消息定义：

HDR_req| SM2_Enc(pub_R, rand_L)| cert_L|SIG_L

各字段含义如下：

HDR_req：请求消息头。

SM2_Enc(pub_R, rand_L)：请求方随机数密文，使用响应方服务器 R 设备公钥，对请求方服务器 L 生成的随机数 rand_L 进行非对称加密，应符合 GB/T 35276 的规定。

cert_L，请求方服务器 L 的设备证书。

SIG_L：签名值，SM2_sign(pri_L, HDR_req|SM2_Enc(pub_R, rand_L)|cert_L)，使用请求方服务器 L 设备私钥对消息进行签名，遵循 GB/T 35276。

b)　响应消息定义

HDR_ans| SM2_Enc(pub_L, rand_R)| SIG_R

各字段含义如下：

HDR_ans：响应消息头。

SM2_Enc(pub_L, rand_R)：响应方随机数密文，使用请求方服务器 L 设备公钥，对请求方服务器

R 生成的随机数 rand_R 进行非对称加密，应符合 GB/T 35276—2017 的规定。

SIG_R：签名值，SM2_sign(pri_R, HDR_ans| SM2_Enc(pub_L, rand_R))，使用响应方服务器 R 设备私钥对消息进行签名，遵循 GB/T 35276。

c) 计算会话密钥

服务器注册消息通信过程中，双方交换得到的随机数 rand_L 和 rand_R，双方使用随机数作为密钥素材，使用密钥导出函数 prf()，计算服务器 L 和服务器 R 的会话密钥 k_LR，包括用于对称加密的 k1_LR 和用于消息认证码计算的 k2_LR：

k1_LR= prf(rand_L|rand_R)

k2_LR= prf(rand_L|rand_R|k1_LR)

C.4 查询本地服务器

ONS 客户端向本地 ONS 服务器发送产品电子代码查询请求，本地 ONS 服务器从本地缓存或者向各级 ONS 服务器中查找对应的 EPCIS 服务器信息，最后将查询结果返回 ONS 客户端。

查询本地服务器的请求信息和响应消息定义如下：

a) 请求消息定义

HDR_req| PCODE

各字段含义如下：

HDR_req：请求消息头。

PCODE：产品电子代码。

b) 响应消息定义

HDR_ans| ip_ EPCIS

各字段含义如下：

HDR_ans：响应消息头。

ip_EPCIS：EPCIS 服务器地址。

C.5 查询各级服务器

本地 ONS 服务器从本地缓存中查找产品电子代码失败时，本地 ONS 服务器从一级 ONS 服务器开始，进行迭代查询，上级 ONS 服务器返回本级 ONS 服务器地址，查询本级 ONS 服务器时，若查询成功，则返回对应的 EPCIS 服务器地址，否则返回下级 ONS 服务器地址，继续迭代查询，直到获得查询结果为止。

若本地 ONS 服务器为 L，上级 ONS 服务器为 R，本级 ONS 服务器为 A，下级 ONS 服务器为 C，描述消息报文定义如下：

a) 请求消息定义

HDR_req| SM4_Enc(u1_LA, PCODE)|[SM4_enc(k1_AR,u_LA)]|MAC_L

各字段含义如下：

HDR_req：请求消息头。

SM4_Enc(k1_LA, PCODE)：产品电子代码的密文，使用服务器为 L 与服务器 A 的工作密钥 u1_LA 对称加密保护。

SM4_enc(k1_AR,u_LA)：服务器为 L 与本级服务器 A 工作密钥密文，该密文由上级服务器 R 产生，使用本级服务器 A 与上级服务器 R 的会话密钥 k1_AR 对称加密保护。查询一级服务器时，本字段为空。

MAC_L：hmac(u2_LA，HDR_req| SM4_Enc(u1_LA，PCODE)|[SM4_enc(k1_AR,u_LA)]），使用服务器 L 与服务器 R 的会话密钥 u2_LA 生成的消息认证码。

b） 响应消息定义

HDR_ans| SM4_Enc(u1_LA，ip_C|u_LC)|[SM4_enc(k1_CA,u_LC)]| MAC_A

各字段含义如下：

HDR_ans：响应消息头。

SM4_Enc(u1_LA，ip_C|u_LC)：如果查询成功，本字段为 EPCIS 服务器地址的密文，如果需继续查询(消息头中处理结果为 0x8)时，本字段为下级服务器 C 地址和下级工作密钥 u_LC 的密文，使用服务器 L 与服务器 R 的工作密钥对称加密。

SM4_enc(k1_CA,u_LC)：如果查询成功，本字段为空，如果需继续查询，本字段为下级工作密钥 u_LC 密文，使用本级服务器 A 与下级服务器 C 的会话密钥 k2_CA 对称加密。

MAC_R：hmac(u2_LA，HDR_ans| SM4_Enc(u1_LA，ip_C|u_LC)|[SM4_enc(k1_CA,u_LC)]），使用服务器 L 与本级服务器 A 的会话密钥 k2_LA 生成的消息认证码。

c） 计算工作密钥

如果需要继续查询，由本级服务器 A 生成随机数 rand_A，使用该随机数及产品电子代码作为密钥素材，使用密钥导出函数 prf()，计算下级服务器 C 及本地服务器 L 的工作密钥 u_LC，包括用于对称加密的 u1_LC 和用于消息认证码计算的 u2_LC：

u1_LC＝prf(rand_L|rand_A)

u2_LC＝prf(rand_L|rand_A| u1_LC)

附 录 D
（规范性附录）
安全查询处理流程

D.1 概述

本附录规定了产品电子代码的安全查询流程。

本地 ONS 服务器收到来自 ONS 客户端的产品电子代码查询请求时，首先在本地缓存中查找对应 EPCIS 服务器信息，如果没有找到，则从一级 ONS 服务器开始，通过迭代查询的方式进行解析。

D.2 查询处理流程

D.2.1 查询处理流程图

ONS 客户端向本地 ONS 服务器 L（以下简称“服务器 L”）发起产品电子代码查询请求，服务器 L 依次向一级 ONS 服务器 R（以下简称“服务器 R”）、二级 ONS 服务器 A（以下简称“服务器 A”）、三级 ONS 服务器 C（以下简称“服务器 C”），进行迭代查询，最后将查询结果返回 ONS 客户端，如图 D.1 所示。

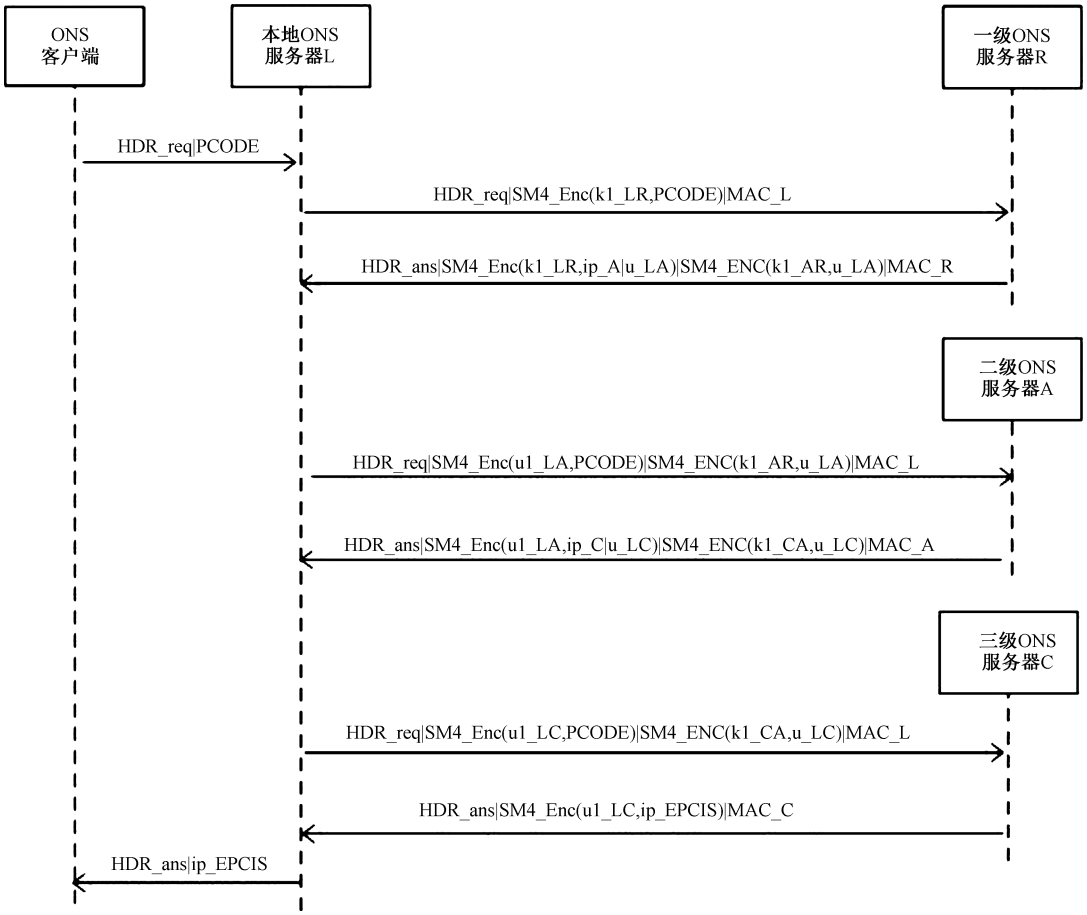

图 D.1 查询报文的交互流程图

D.2.2 步骤 1 ONS 客户端向服务器 L 发送查询请求

处理流程如下：

a) ONS 客户端从物品电子标签中读取产品电子代码；
b) ONS 客户端向服务器 L 发送查询请求，报文内容为符合附录 A 编码格式的产品电子代码；
c) 服务器 L 收到请求后，首先在本地缓存中查询产品电子代码，若查到对应的 EPCIS 服务器信息，则按 D.2.9 要求向 ONS 客户端返回查询结果；
d) 若本地缓存查询失败，则按 D.2.3 要求向服务器 R 发起查询请求。

D.2.3 步骤 2 服务器 L 向服务器 R 发送查询请求消息

处理流程如下：

a) 服务器 L 使用会话密钥 k1_LR，对产品电子代码进行对称加密，得到产品电子代码密文；
b) 服务器 L 向服务器 R 发送查询请求消息，包含产品电子代码密文，并使用会话密钥 k2_LR 生成消息认证码；
c) 服务器 R 收到请求消息后，使用会话密钥 k2_LR，对消息认证码进行完整性及数据源有效性验证，若验证无效，则查询失败；
d) 服务器 R 使用会话密钥 k1_LR，对产品电子代码密文进行对称解密，得到产品电子代码明文；
e) 服务器 R 按 D.2.4 要求，向服务器 L 返回查询结果。

D.2.4 步骤 3 服务器 R 向服务器 L 返回查询应答消息

处理流程如下：

a) 服务器 R 查询产品电子代码对应的二级 ONS 服务器，假设为服务器 A；
b) 服务器 R 为服务器 L 及下级服务器 A 生成下级工作密钥 u_LA；
c) 服务器 R 使用服务器 L 的会话密钥 k1_LR 对称加密保护，得到下级服务器 A 地址和下级工作密钥密文：SM4_Enc(k1_LR,ip_A|u_LA)；
d) 服务器 R 使用下级服务器 A 会话密钥 k1_AR 对称加密保护，得到下级工作密钥密文：SM4_Enc(k1_AR, u_LA)；
e) 服务器 R 向服务器 L 返回应答消息，包含密文 SM4_Enc(k1_LR,ip_A|u_LA)及密文 SM4_Enc(k1_AR, u_LA)，并使用会话密钥 k2_LR 生成消息认证码；
f) 服务器 L 收到应答消息后，使用会话密钥 k2_LR，对消息认证码进行完整性及数据源有效性验证，若验证无效，则查询失败；
g) 服务器 L 使用会话密钥 k1_LR，对密文 SM4_Enc(k1_LR,ip_A|u_LA)进行解密，得到下级服务器 A 地址及下级工作密钥 u_LA；
h) 服务器 L 按 D.2.5 要求，向服务器 A 发送查询请求。

D.2.5 步骤 4 服务器 L 向服务器 A 发送查询请求消息

处理流程如下：

a) 服务器 L 使用工作密钥 u1_LA 进行对称加密保护，得到产品电子代码密文；
b) 服务器 L 向服务器 A 发送查询请求消息，包含产品电子代码密文，以及上级服务器分发的工作密钥密文 SM4_Enc(k1_AR, u_LA)，并使用工作密钥 u2_LA 生成消息认证码；
c) 服务器 A 收到请求消息后，使用会话密钥 k1_AR，对工作密钥密文 SM4_Enc(k1_AR, u_LA)进行解密，得到工作密钥明文 u_LA；
d) 服务器 A 使用工作密钥 u2_LA，对消息认证码进行完整性及数据源有效性验证，若验证无效，则查询失败；
e) 服务器 A 使用工作密钥 u1_LA，对产品电子代码密文进行对称解密，得到产品电子代码明文；
f) 服务器 A 按 D.2.6 要求，向服务器 L 返回查询结果。

D.2.6 步骤5 服务器A向服务器L返回查询应答消息

处理流程如下：

a) 服务器A查询产品电子代码对应的三级ONS服务器，假设为服务器C；
b) 服务器A为服务器L及下级服务器C生成下级工作密钥u_LC；
c) 服务器A使用服务器L的工作密钥u1_LA对称加密保护，得到下级服务器C地址和下级工作密钥密文：SM4_Enc(u1_LA,ip_C|u_LC)；
d) 服务器A使用下级服务器C会话密钥k1_CA对称加密保护，得到下级工作密钥密文：SM4_Enc(k1_CA, u_LC)；
e) 服务器A向服务器L返回查询应答消息，包含密文SM4_Enc(u1_LA,ip_C|u_LC)及密文SM4_Enc(k1_CA, u_LC)，并使用会话密钥u2_LA生成消息认证码；
f) 服务器L收到应答消息后，使用工作密钥u2_LA，对消息认证码进行完整性及数据源有效性验证，若验证无效，则查询失败；
g) 服务器L使用工作密钥u1_LA，对密文SM4_Enc(u1_LA,ip_C|u_LC)进行解密，得到下级服务器C地址及下级工作密钥u_LC；
h) 服务器L按D.2.7要求，向服务器C发送查询请求。

D.2.7 步骤6 服务器L向服务器C发送查询请求报文

处理流程如下：

a) 服务器L使用工作密钥u1_LC进行对称加密保护，得到产品电子代码密文；
b) 服务器L向服务器C发送查询请求消息，包含产品电子代码密文，以及上级服务器A分发的工作密钥密文SM4_Enc(k1_CA, u_LC)，并使用工作密钥u2_LC生成消息认证码；
c) 服务器C收到请求消息后，使用会话密钥k1_CA，对工作密钥密文SM4_Enc(k1_CA, u_LC)进行解密，得到工作密钥明文u_LC；
d) 服务器C使用工作密钥u2_LC，对消息认证码进行完整性及数据源有效性验证，若验证无效，则查询失败；
e) 服务器C使用工作密钥u1_LC，对产品电子代码密文进行对称解密，得到产品电子代码明文；
f) 服务器C按D.2.8要求，向服务器L返回查询结果。

D.2.8 步骤7 服务器C向服务器L返回查询应答报文

处理流程如下：

a) 服务器C查询产品电子代码对应的EPCIS服务器地址；
b) 服务器C使用服务器L的工作密钥u1_LC对称加密保护，得到EPCIS服务器地址密文；
c) 服务器C向服务器L返回查询应答消息，包含EPCIS服务器地址密文，并使用工作密钥u2_LC生成消息认证码；
d) 服务器L收到应答消息后，使用工作密钥u2_LC，对消息认证码进行完整性及数据源有效性验证，若验证无效，则查询失败；
e) 服务器L使用会话密钥u1_LC，对EPCIS服务器地址密文进行解密，得到EPCIS服务器地址明文；
f) 服务器L按D.2.9要求，向ONS客户端发送查询结果。

D.2.9 步骤8 服务器L向ONS客户端返回查询结果

处理流程如下：

a) 服务器L向ONS客户端发送查询结果，报文内容为EPCIS服务器地址；
b) ONS客户端收到报文后，访问该EPCIS服务器获取物品的详细信息。

中华人民共和国密码
行业标准
射频识别电子标签统一名称
解析服务安全技术规范
GM/T 0097—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.5 字数 38 千字
2021年3月第一版 2021年3月第一次印刷
*
书号:155066·2-35850 定价 24.00 元

GM/T 0097-2020

码上扫一扫 正版服务到