ICS 35.110
L 78

中华人民共和国国家标准

GB/T 31491—2015

无线网络访问控制技术规范

Wireless network access control technical specification

2015-05-15 发布　　2016-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前言 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 2
4　缩略语 …… 3
5　网络访问的一般模型 …… 4
6　网络访问控制机制 …… 5
6.1　概述 …… 5
6.2　共享信息管理 …… 5
6.3　控制策略协商 …… 6
6.4　鉴别协议 …… 6
6.5　共享信息协商 …… 6
6.6　数据传输保护 …… 6
7　控制策略协商 …… 6
7.1　概述 …… 6
7.2　控制策略协商请求分组 …… 7
7.3　控制策略协商响应分组 …… 7
8　鉴别协议 …… 8
8.1　概述 …… 8
8.2　二实体鉴别机制 …… 8
8.3　三实体鉴别机制 …… 14
9　共享信息协商协议 …… 20
9.1　单播共享信息协商 …… 20
9.2　组播共享信息协商 …… 22
附录A（规范性附录）　应用领域 …… 25
附录B（资料性附录）　工作模式 …… 29
参考文献 …… 34

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本标准主要起草单位:西安西电捷通无线网络通信股份有限公司、无线网络安全技术国家工程实验室、国家无线电监测中心检测中心、中国电子技术标准化研究所、西安邮电大学、西安电子科技大学、国家密码管理局商用密码检测中心、信息安全国家重点实验室、中国信息安全认证中心、国家信息安全工程技术研究中心、国家计算机网络应急技术处理协调中心、中国人民解放军信息安全测评认证中心、广州杰赛科技股份有限公司、重庆邮电大学、宇龙计算机通信科技(深圳)有限公司、中国人民大学、桂林电子科技大学、中国电信集团公司、国家信息中心、北京大学深圳研究生院、北京中电华大电子设计有限责任公司、东南大学、深圳市明华澳汉科技股份有限公司、北京六合万通微电子技术有限公司、北京网贝合创科技有限公司、弘浩明传科技(北京)有限公司、中国人民解放军信息工程大学、江南计算技术研究所、北京邮电大学、北京五龙电信技术公司、北大方正集团公司、北京市政务网络管理中心、北京城市热点资讯有限公司、北京华安广通科技发展有限公司、迈普通信技术有限公司、北京天一集成科技有限公司、宽带无线 IP 标准工作组、WAPI 产业联盟。

本标准主要起草人:黄振海、铁满霞、赖晓龙、宋起柱、王育民、曹军、朱志祥、冯登国、李大为、陈晓桦、文仲慧、卓兰、肖跃雷、舒敏、胡亚楠、李广森、高波、刘平、杜志强、吴亚非、李琴、梁朝晖、梁琼文、张变玲、罗旭光、龙昭华、张伟、徐平平、仇洪冰、朱跃生、潘峰、兰天、王志坚、王轲、张国强、杨宏、田小平、田辉、张永强、寿国梁、毛立平、曹竹青、郭志刚、高宏、韩康、陈志峰、李大伟、王立仁、高原。

引　言

在通信网络，尤其是无线网络中，非授权的终端设备能物理地连接到网络上，或者授权的终端设备所物理连接的网络不一定是终端所期望的。因此，在终端和网络通信前，需要先相互鉴别对方的身份，再进行授权访问，以保证通信的可靠。

本标准描述了无线网络访问控制机制，规范了网络的接入控制。

本文件的发布机构提请注意，声明符合本文件时，可能涉及 8.2.2.2、8.3.2 等与“一种三步握手协议方法”、“一种实现实体的公钥获取、证书验证及双向鉴别的方法”等相关的专利的使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构保证，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本文件发布机构备案。相关信息可通过以下联系方式获得：

专利权人：西安西电捷通无线网络通信股份有限公司

地址：西安市高新区科技二路 68 号　西安软件园秦风阁 A201

联系人：刘长春

邮政编码：710075

电子邮件：ipri@iwncomm.com

电　　话：029-87607836

传　　真：029-87607829

网　　址：http://www.iwncomm.com

请注意除上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

无线网络访问控制技术规范

1 范围

本标准规定了网络访问过程中安全访问控制的一般方法。

本标准适用于 WLAN、WPAN、WSN、RFID 等各种无线网络访问控制领域，也适用于 LAN、PLC、PON 等各种有线网络访问控制领域。

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 15629.2—2008 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 2 部分：逻辑链路控制

GB/T 15629.3—2014 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 3 部分：带碰撞检测的载波侦听多址访问(CSMA/CD)的访问方法和物理层规范

GB 15629.11—2003 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范

GB 15629.11—2003/XG1—2006 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范 第 1 号修改单

GB 15629.1101—2006 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范：5.8 GHz 频段高速物理层扩展规范

GB 15629.1102—2003 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范：2.4 GHz 频段较高速物理层扩展规范

GB/T 15629.1103—2006 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范：附加管理域操作规范

GB 15629.1104—2006 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范：2.4 GHz 频段更高数据速率扩展规范

GB/T 15629.15—2010 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 15 部分：低速无线个域网(WPAN)媒体访问控制和物理层规范

GB/T 15843.1—2008 信息技术 安全技术 实体鉴别 第 1 部分：概述

GB/T 15843.2—2008 信息技术 安全技术 实体鉴别 第 2 部分：采用对称加密算法的机制

GB/T 15843.3 信息技术 安全技术 实体鉴别 第 3 部分：采用数字签名技术的机制

GB/T 28455—2012 信息安全技术 引入可信第三方的实体鉴别及接入架构规范

GB/T 28925—2012 信息技术 射频识别 2.45 GHz 空中接口协议

GB/T 29768—2013 信息技术 射频识别 800/900 MHz 空中接口协议

GB/T 29828—2013 信息安全技术 可信计算规范 可信连接架构

GB/T 30001.1—2013 信息技术 基于射频的移动支付 第 1 部分：射频接口

GM/T 0002—2012 SM4 分组密码算法

ISO/IEC 9798-3:1998/Amd.1:2010 信息技术 安全技术 实体鉴别 第 3 部分：采用数字签名

技术的机制　第1号修改单(Information technology—Security techniques—Entity authentication—Part 3:Mechanisms using digital signature techniques—Amendment 1)

ISO/IEC 11770-1　信息技术　安全技术　密钥管理　第1部分 框架(Information technology—Security techniques—Key management—Part 1:Framework)

ISO/IEC 20009-2:2013　信息技术　安全技术　匿名实体鉴别　第2部分:基于群组公钥签名的机制(Information technology—Security techniques—Anonymous entity authentication—Part 2:Mechanisms based on signatures using a group public key)

RFC 768 用户数据报协议(User Datagram Protocol,August 1980)

RFC 793 传输控制协议(Transmission Control Protocol,September 1981)

3　术语和定义

下列术语和定义适用于本文件。

3.1

DH交换　Diffie-Hellman exchange

Differ和Hellman提出的基于离散对数难题的密钥交换技术。

3.2

密文　ciphertext

经过变换,信息内容被隐藏起来的数据。

3.3

密码校验函数　cryptographic check function

以秘密密钥和任意字符串作为输入,并以密码校验值作为输出的密码变换。

3.4

解密　decryption

把一个密文转换为一个明文的处理,该转换需要一套算法和一套输入参量。

3.5

加密　encryption

把一个明文转换为一个密文的处理,该转换需要一套算法和一套输入参量。

3.6

鉴别　authentication

证实一个实体就是所声称的实体。

3.7

双向鉴别　mutual authentication

向双方实体提供身份保证的实体鉴别。

3.8

密钥　key

控制密码变换操作(例如加密、解密、密码校验函数计算、签名生成和签名验证)的符号序列。

3.9

密钥协商　key agreement

在实体之间建立一个共享密钥的过程,在这个过程中,任何一个参与实体都不能事先决定共享密钥的值。

3.10

共享信息　shared information

通信双方或多方共享的信息，可以是公开的也可以是秘密的，如：密钥等。

3.11

私钥　private key

一个实体的非对称密钥对中只由该实体使用的密钥。

3.12

签名私钥　private signature key

规定私有签名变换的私有密钥。

3.13

公钥　public key

一个实体的非对称密钥对中能够被公开的密钥。

3.14

公钥证书　public key certificate

实体的公开密钥信息，它由认证机构签名，因而不可伪造。

3.15

验证公钥　public verification key

规定公开验证变换的公开密钥。

3.16

随机数　random number

其值不可预测的时变参数。

3.17

权标　token

由与特定的通信相关的数据字段构成的信息，它包含已使用密码技术进行了变换的信息。

3.18

单向鉴别　unilateral authentication

只向一个实体提供另一个实体身份保证，而不向后者提供前者身份保证的实体鉴别。

3.19

杂凑函数　hash function

散列函数

将位串映射成固定长度位串的函数，满足两个性质：对于一个给定的输出，要找到其对应的输入，在计算上是不可行的；对于一个给定的输入，要找到对应其输出的第二个输入，在计算上是不可行的。计算上的可行性依赖于用户的具体安全要求和环境。

3.20

密钥加密密钥　key encryption key

用于加密密钥数据的密钥。

4　缩略语

下列缩略语适用于本文件。

3G LTE　3G 长期演进(3G Long Term Evolution)

AP　访问点(Access Point)

AS　鉴别服务器(Authentication Server)

BK 基密钥(Base Key)

CCM 计数器模式及密码区块链信息认证码(Counter mode with Cipher-block chaining Message authentication code)

GCM Galois 计数器模式(Galois/Counter Mode)

LAN 局域网(Local Area Network)

MAN 城域网(Metropolitan Area Network)

MIC 消息完整性校验(Message Integrity Check)

MPAS 移动支付空中接口安全(Mobile Payment Air interface Security)

NEAU NFC 实体鉴别(NFC Entity Authentication)

ONU 光网元(Optical Network Unit)

PLC 电力线通信(Power Line Communication)

PON 无源光网络(Passive Optical Network)

REP 响应者(Responser)

REQ 请求者(requester)

RFID 射频识别(Radio Frequency Identification)

SN 传感器网络(Sensor Network)

TCA 可信连接架构(Trusted Connect Architecture)

TePA 三元对等架构(Tri-element Peer Architecture)

TePA-AC 基于三元对等架构的访问控制(TePA-based Access Control)

TISec 可信 IP 安全(Trusted IP layer security)

TLSec 基于三元对等架构的局域网媒体访问控制安全(TePA-based LAN MAC Security)

TPLS 基于三元对等架构的电力线通信网络安全(TePA-based PLC Security)

TPSec 基于三元对等架构的无源光网络安全(TePA-based PON Security)

TRAIS 标签和读写器空中接口安全(Tag and Reader Air-Interface Security)

TSSI 基于三元对等架构的传感器网络安全基础设施(TePA-based SN Security Infrastructure)

UWB 超宽带(Ultra WideBand)

VPN 虚拟专用网络 (Virtual Private Network)

WAPI 无线局域网鉴别与保密基础结构(Wireless LAN Authentication and Privacy Infrastructure)

WLAN 无线局域网(Wireless LAN)

WMAN 无线城域网(Wireless MAN)

WPAN 无线个域网(Wireless PAN)

WSAI WPAN 安全访问基础设施(WPAN Security Access Infrastructure)

5 网络访问的一般模型

网络访问可以使用多种形式,包括无线、有线等物理链路及 IP 逻辑链路等,比如 WPAN、WLAN、WMAN、3G/LTE、RFID、LAN、PON、PLC 等均可作为网络访问方式。每种网络形式都有各自的组成方式,包含的网元种类也不同,但它们的基本结构都是相同的,如图 1 所示。

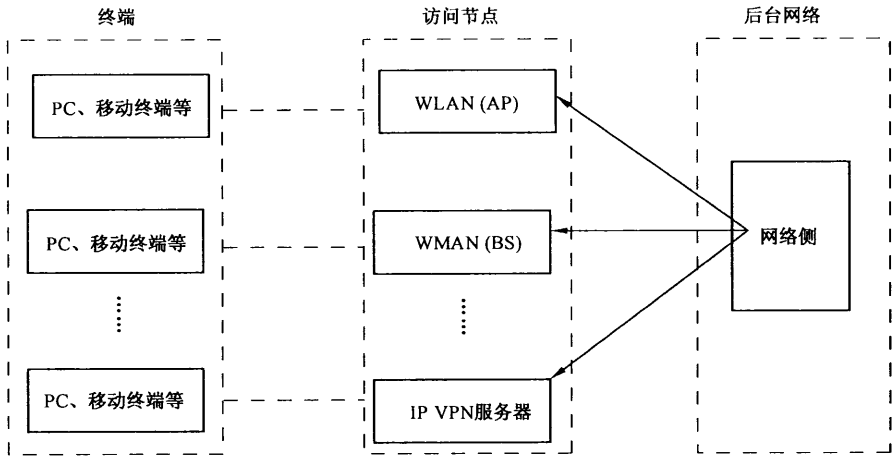


图 1　网络访问基本结构

网络在其网络边缘提供一个访问节点，比如 WLAN 的 AP(其定义应符合 GB 15629.11—2003、GB 15629.11—2003/XG1—2006、GB 15629.1101—2006、GB 15629.1102—2003、GB/T 15629.1103—2006、GB 15629.1104—2006 的规定)、PON 的 ONU、3G/LTE 的基站和 IP VPN 服务器等，终端通过该访问节点与网络连接；因此网络从结构上基本可以划分三个部分：终端、访问节点和后台网络。网络访问就是通过终端、访问节点和后台网络三部分的交互，实现终端和网络之间的通信控制。

6　网络访问控制机制

6.1　概述

如第 5 章描述，不同网络访问的结构基本类似，虽然各种网络在物理和链路特性上都各有自身的特殊性。

网络访问控制管理通过下面所述的控制技术，按照设定的控制机制，实现终端到访问节点的连结被合法的使用，其中的数据传输受到保护。

网络访问控制机制一般包含以下五大模块：

——共享信息管理；

——控制策略协商；

——鉴别协议；

——共享信息协商；

——数据传输保护。

本标准定义的网络访问控制机制可应用于链路层、网络层或应用层等，所定义的安全协议报文传递时，可以使用管理报文或控制报文，也可以使用数据报文。如果使用数据报文，需要使用特定的标记用以区分安全协议报文和普通的数据报文。具体实现时，对于以太网络，可使用以太类型字段 0x891b 进行安全协议交互；对于 TCP/UDP 应用，可使用 TCP/UDP 端口号 5111 完成安全协议交互。其中以太类型字段应符合 GB/T 15629.2—2008 的规定，TCP 定义应符合 RFC 793 的规定，UDP 定义应符合 RFC 768 的规定。在引入可信第三方时，网络访问控制的架构见 GB/T 28455—2012。

本标准定义的网络访问控制机制可应用不同网络，实现合法用户访问合法网络，见附录 A。

6.2　共享信息管理

共享信息管理是网络访问控制机制的基础一步，它指终端和访问点、终端和终端之间的初始共享信

息的管理，定义共享信息管理对象，共享信息管理机制，包括密钥的产生、注册、分配、安装、存储、存档、更新、恢复、撤销、导出、销毁等。其定义应符合 ISO/IEC 11770-1 的规定。

共享信息管理可以有多种方式，可根据网络规模、场景、安全需求等多种条件选择合适的管理方式。

共享信息管理：定义共享信息管理对象，共享信息管理机制所基于的总体模型，共享信息管理基本概念，共享信息管理服务，共享信息管理机制特征，共享信息材料管理需求，共享信息材料管理框架，共享信息管理机制等。

6.3 控制策略协商

当选择好共享信息管理方式后，终端和访问点还需要协商两者使用的控制策略机制，包括鉴别机制、密码算法等机制的协商。这种协商可以通过人工制定、带外通道协商、带内通道自动协商等多种通道完成，自动协商需要通过一定的协议实现。第 7 章对控制策略协商进行描述。

6.4 鉴别协议

鉴别协议是网络访问控制机制的核心部分，它完成终端和访问点的身份的鉴别，保证双方都是合法的使用者，是网络访问控制的重要一步。

根据控制策略协商结果，鉴别协议需要使用不同的方案。每种鉴别协议都有自身的特点，安全性也有区别。第 8 章对鉴别协议进行描述。

6.5 共享信息协商

通过鉴别协议完成身份鉴别，为保护数据在链路上的传输，终端和访问点需要使用协商的共享信息对数据进行保护。共享信息协商完成双方的共享信息协商一致、更新和同步，根据协商的共享信息用途可以分为单播共享信息协商和组播共享信息协商。单播共享信息用于保护点对点数据包的加密及完整性保护，而组播共享信息用于点到多点数据包的加密及完整性保护。第 9 章对共享信息协商进行描述。

6.6 数据传输保护

数据传输保护是指数据在传输过程中不被非授权的实体利用或窃取，网络中传输数据的机密性、完整性、认证性的要求由数据传输保护机制提供，通过使用合适的密码算法、算法模式提供数据传输保护。

数据传输保护过程中常用的对称加密算法有很多，其中 GM/T 0002—2012 规范的 SM4 算法应用较为广泛。不同的应用环境下使用的对称加密算法的输出数据长度和采用的工作模式也有所变化。

附录 B 提供了数据传输保护方式中 4 种典型的工作模式。

7 控制策略协商

7.1 概述

请求者 REQ 和响应者 REP 通过控制策略协商过程协商所使用的鉴别机制、密钥协商机制以及数据保护机制，还包括协商这些机制中所使用的密码套件，如鉴别密码算法、密钥协商密码算法、单播密码套件及组播密码套件等信息。控制策略协商过程由控制策略协商请求分组和控制策略协商响应分组构成，见图 2。

注：在网络中客户一般作为请求者，网络访问设备作为响应者。控制策略协商是网络访问设备提供多个选择，由客户进行选择，因此控制策略协商请求一般由响应者发起。但是根据实际的网络需求，控制策略协商请求也可以由请求者发起。

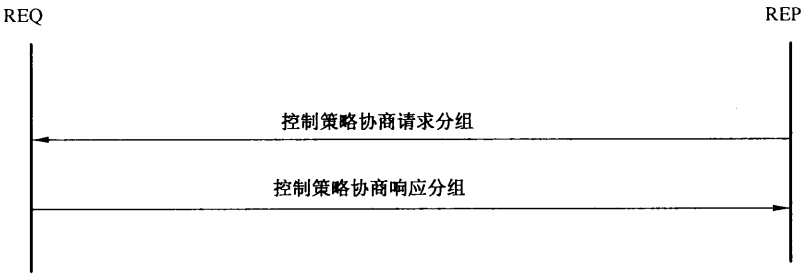


图 2　控制策略协商过程

7.2　控制策略协商请求分组

当用户设备访问网络时，响应者 REP 向请求者 REQ 发送控制策略协商请求分组。

控制策略协商请求分组包含能力信息 CI_{REP}，表示 REP 所支持的鉴别和密钥协商、数据保护套件以及密码算法套件等信息。

能力信息 CI_{REP} 定义如图 3 所示。

鉴别套件计数	鉴别套件	密钥协商套件计数	密钥协商套件	数据保护机制套件计数	数据保护机制套件	单播密码套件计数	单播密码套件	组播密码套件

图 3　REP 能力信息

图 3 中：

——鉴别套件计数字段：表示响应者 REP 支持的鉴别套件的个数；

——鉴别套件字段：表示响应者 REP 支持的鉴别套件列表；

——密钥协商套件计数字段：表示响应者 REP 支持的密钥协商套件的个数；

——密钥协商套件字段：表示响应者 REP 支持的密钥协商套件列表；

——数据保护机制套件计数字段：表示响应者 REP 支持的数据保护机制套件的个数；

——数据保护机制套件字段：表示响应者 REP 支持的数据保护机制套件列表；

——单播密码套件计数字段：表示响应者 REP 支持的单播密码套件个数；

——单播密码套件字段：表示响应者 REP 支持的单播密码套件列表；

——组播密码套件字段：表示响应者 REP 支持的组播密码套件。

7.3　控制策略协商响应分组

当请求者 REQ 收到响应者 REP 发来的控制策略协商请求分组时，根据控制策略协商请求分组中的 CI_{REP} 元素选择一种双方共有的鉴别、密钥管理、数据保护及密码套件，组成控制策略协商响应分组发送给响应者 REP。

控制策略协商响应分组包括能力信息 CI_{REQ}，表示 REQ 选择的鉴别套件、密钥协商套件、数据保护套件以及密码套件等信息。

能力信息 CI_{REQ} 定义如图 4 所示。

鉴别套件	密钥协商套件	数据保护机制套件	单播密码套件	组播密码套件

图 4 REQ 能力信息

图 4 中：

——鉴别套件字段：表示请求者 REQ 选择的鉴别套件列表；

——密钥协商机制套件字段：表示请求者 REQ 选择的密钥协商机制套件列表；

——数据保护机制套件字段：表示请求者 REQ 选择的数据保护机制套件列表；

——单播密码套件字段：表示请求者 REQ 选择的单播密码套件列表；

——组播密码套件字段：表示请求者 REQ 选择的组播密码套件。

当 REP 收到 REQ 回应的控制策略协商响应分组时，判断其中的 CI_{REQ} 字段是否有效，即 REQ 是否支持 REP 选择的鉴别、密钥协商、数据保护及密码套件，若不支持，则丢弃该分组；否则，根据 REQ 选择的套件开始相应的鉴别、密钥管理、数据保护等过程。

8 鉴别协议

8.1 概述

本章描述的鉴别协议根据参与者的数量分为二实体鉴别机制和三实体鉴别机制，根据网络的应用场景、安全需求可以在本章描述的鉴别协议中选择适合其需求的鉴别协议，其中包括支持隐私保护的匿名鉴别协议。

本章描述的鉴别协议中的 Text 是可选的，是 REP 和 REQ 在鉴别协议中传递的一些其他信息，与鉴别协议的安全性无关。本章描述的单向鉴别是指使用该机制时 REP 和 REQ 两个实体只有一方被鉴别，而双向鉴别是指使用该机制时 REP 和 REQ 两个实体都被鉴别。本章使用的定义和记法应符合 GB/T 15843.1—2008、GB/T 15843.2—2008、GB/T 15843.3、GB/T 28455—2012、ISO/IEC 9798-3:1998/Amd.1:2010 和 ISO/IEC 20009-2:2013 的规定。

8.2 二实体鉴别机制

8.2.1 基于异或运算的鉴别机制

8.2.1.1 单向鉴别

在基于异或运算的单向鉴别机制中，要求 REQ 和 REP 之间拥有共享密钥 K，鉴别过程的唯一性/时效性通过产生和校验随机数来控制。该机制在图 5 中说明，REQ 被 REP 鉴别，但通过简单更换 REP 和 REQ 的角色，REP 也可被 REQ 鉴别。该鉴别机制属轻量级安全机制，仅适用于对安全性要求较低的应用场景。

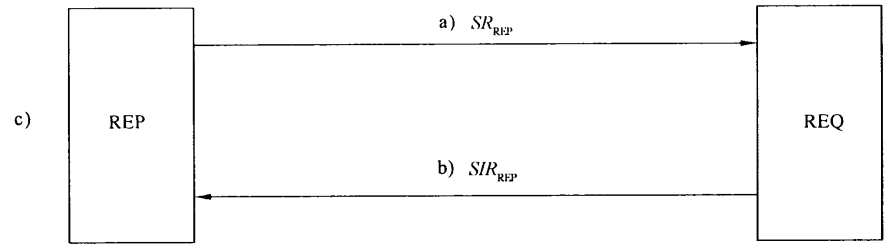


图 5　单向鉴别

图 5 中：

——SR_{REP}字段：表示 REP 将随机数 R_{REP}和 O_n 相加后与共享密钥 K 异或的结果，O_n=5555 5555 5555 5555$_h$，下同。

——SIR_{REP}字段：表示 REQ 用共享密钥 K 异或 SR_{REP}减去 O_n 后得到 R_{REP}，将 R_{REP}和 K 向左循环移位 n 位得到 R'_{REP}和 K'，n 的取值为 R_{REP}中值为 1 的位的个数，然后再用 R'_{REP}与 K'加 O_n 后的结果进行异或得到 SIR_{REP}。

该机制的执行过程如下：

a) REP 发送 SR_{REP}到 REQ；

b) REQ 发送 SIR_{REP}到 REP；

c) REP 收到来自 REQ 的信息后，REP 通过以下方式验证 SIR_{REP}：REP 分别计算 $SIR_{REP} \oplus R'_{REP}$和 $K'+O_n$，比较 $SIR_{REP} \oplus R'_{REP}$和 $K'+O_n$ 是否相等，如果不相等，则丢弃该分组；如果相等，则完成 REP 对 REQ 的单向鉴别。

8.2.1.2　双向鉴别

在基于异或运算的双向鉴别机制中，要求 REQ 和 REP 之间拥有共享密钥 K，鉴别过程的唯一性/时效性通过产生和校验随机数来控制，见 GB/T 15843.1—2008 的附录 B。该鉴别机制在图 6 中说明。该鉴别机制属轻量级安全机制，仅适用于对安全性要求较低的应用场景。

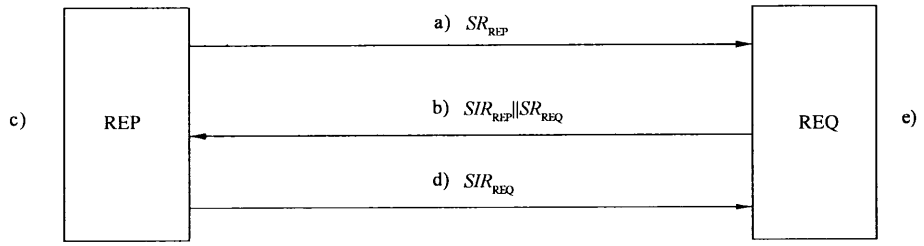


图 6　双向鉴别

图 6 中：

——SR_{REP}字段：表示 REP 将随机数 R_{REP}和 O_n 相加后与共享密钥 K 异或的结果；

——SIR_{REP}字段：表示 REQ 用共享密钥 K 异或 SR_{REP}减去 O_n 后得到 R_{REP}，将 R_{REP}和 K 向左循环移位 n 位得到 R'_{REP}和 K'，n 的取值为 R_{REP}中值为 1 的位的个数，然后再用 R'_{REP}与 K'加 O_n 后的结果进行异或得到 SIR_{REP}；

——SR_{REQ}字段：表示 REQ 将随机数 R_{REQ}和 O_n 相加后与共享密钥 K 异或的结果；

——SIR_{REQ}字段：表示 REP 用共享密钥 K 异或 SR_{REQ}减去 O_n 后得到 R_{REQ}，将 R_{REQ}和 K 向左循环移位 n 位得到 R'_{REQ}和 K'，n 的取值为 R_{REQ}中值为 1 的位的个数，然后再用 R'_{REQ}与 K'加 O_n 后的结果进行异或得到 SIR_{REQ}。

该机制的执行过程如下：

a) REP 发送 SR_{REP} 到 REQ；

b) REQ 发送 $SIR_{REP} \| SR_{REQ}$ 到 REP；

c) 收到来自 REQ 的信息后，REP 完成下列步骤：

1) 通过以下方式验证 SIR_{REP}：REP 分别计算 $SIR_{REP} \oplus R'_{REP}$ 和 $K' + O_n$，比较 $SIR_{REP} \oplus R'_{REP}$ 和 $K' + O_n$ 是否相等，如果不相等，则丢弃该分组；如果相等，则继续执行下面的步骤；

2) 计算 SIR_{REQ}。

d) REP 发送 SIR_{REQ} 到 REQ；

e) 收到来自 REP 的信息，REQ 通过以下方式验证 SIR_{REQ}：REQ 分别计算 $SIR_{REQ} \oplus R'_{REQ}$ 和 $K' + O_n$，比较 $SIR_{REQ} \oplus R'_{REQ}$ 和 $K' + O_n$ 是否相等，如果不相等，则丢弃该分组；如果相等，则完成 REQ 与 REP 之间的双向鉴别。

8.2.2 基于杂凑算法的鉴别机制

8.2.2.1 单向鉴别

在基于杂凑算法的单向鉴别机制中，要求 REQ 和 REP 之间拥有共享密钥 K，鉴别过程的唯一性/时效性通过产生和校验随机数来控制。该鉴别机制在图 7 中说明，REQ 被 REP 鉴别，但通过简单更换 REP 和 REQ 的角色，REP 也可被 REQ 鉴别。

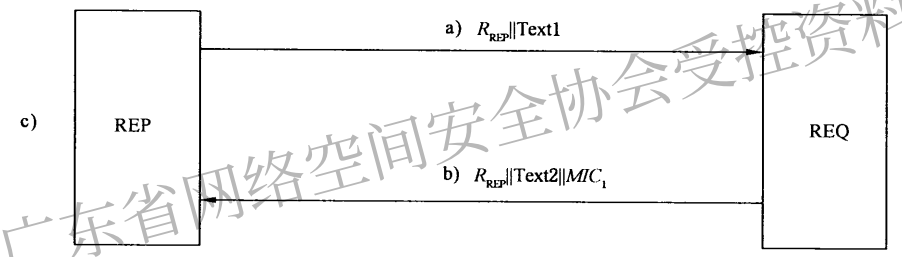


图 7 单向鉴别

图 7 中：

——R_{REP} 字段：表示 REP 的随机数；

——MIC_1 字段：表示 REQ 利用与 REP 之间的共享密钥 K 或 K 的导出密钥对 $R_{REP} \| \text{Text2}$ 利用杂凑算法计算得到的杂凑值。

该机制执行过程如下：

a) REP 发送随机数 $R_{REP} \| \text{Text1}$ 到 REQ；

b) 收到 REP 的信息后，REQ 完成如下步骤：

1) 利用与 REP 之间的共享密钥 K 或 K 的导出密钥计算得到 MIC_1 字段；

2) 发送 $R_{REP} \| \text{Text2} \| MIC_1$ 到 REP。

c) 收到来自 REQ 的信息后，REP 完成下列步骤：

1) 校验收到的随机数 R_{REP} 与步骤 a)中发送给 REQ 的随机数 R_{REP} 相一致；若不一致，则丢弃该分组；若一致，执行下面的步骤；

2) 利用与 REQ 之间的共享密钥 K 或 K 的导出密钥校验 MIC_1 字段的正确性，若不正确，则丢弃该分组；若正确则完成 REP 对 REQ 的鉴别。

8.2.2.2 三次传递双向鉴别

在基于杂凑算法的三次传递双向鉴别机制中，要求 REQ 和 REP 之间拥有共享密钥 K，鉴别过程

的唯一性/时效性通过产生和校验随机数来控制。该鉴别机制在图 8 中说明。

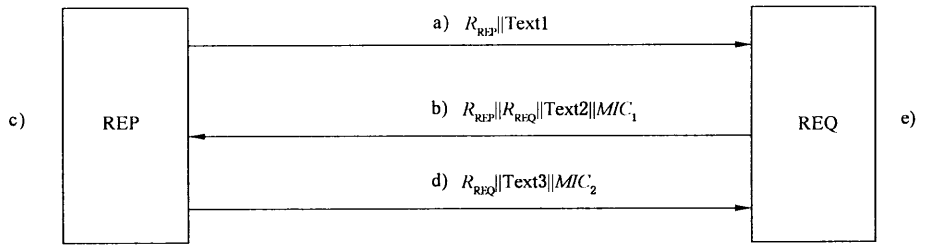


图 8　三次传递双向鉴别

图 8 中：

——R_{REP}字段：表示 REP 的随机数；

——R_{REQ}字段：表示 REQ 的随机数；

——MIC_1 字段：表示 REQ 利用与 REP 之间的共享密钥 K 或 K 的导出密钥对 $R_{REP} \| R_{REQ} \| \text{Text2}$ 利用杂凑算法计算得到的杂凑值；

——MIC_2 字段：表示 REP 利用与 REQ 之间的共享密钥 K 或 K 的导出密钥对 $R_{REQ} \| \text{Text3}$ 利用杂凑算法计算得到的杂凑值。

该机制的执行过程如下：

a) REP 发送随机数 $R_{REP} \| \text{Text1}$ 到 REQ。

b) 收到 REP 的信息后，REQ 完成如下步骤：

1) 生成随机数 R_{REQ}；

2) 发送 $R_{REP} \| R_{REQ} \| \text{Text2} \| MIC_1$ 到 REP。

c) 收到来自 REQ 的信息后，REP 完成下列步骤：

1) 校验收到的随机数 R_{REP} 与步骤 a)中发送给 REQ 的随机数 R_{REP} 相一致；

2) 利用与 REQ 之间的共享密钥 K 或 K 的导出密钥校验 MIC_1 字段的正确性，若不正确，则丢弃该分组；若正确，则完成 REP 对 REQ 的鉴别。

d) REP 发送 $R_{REQ} \| \text{Text3} \| MIC_2$ 到 REQ。

e) 收到来自 REP 的信息，REQ 完成下列步骤：

1) 校验收到的随机数 R_{REQ} 与步骤 b)中发送给 REP 的随机数 R_{REQ} 相一致；

2) 利用与 REP 之间的共享密钥 K 或 K 的导出密钥校验 MIC_2 字段的正确性，若不正确，则丢弃该分组；若正确，则完成 REQ 对 REP 的鉴别。

8.2.2.3　四次传递双向鉴别 1

在基于杂凑算法的四次传递双向鉴别 1 机制中，要求 REQ 和 REP 之间拥有共享密钥 K，鉴别过程的唯一性/时效性通过产生和校验随机数来控制。该鉴别机制在图 9 中说明。

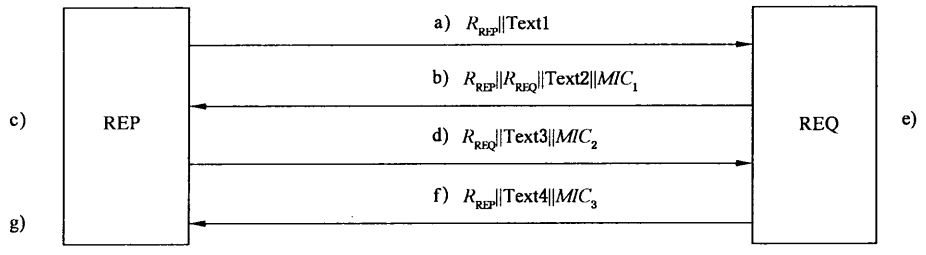


图 9　四次传递双向鉴别 1

图 9 中：

——R_{REP}字段：表示 REP 的随机数；

——R_{REQ}字段：表示 REQ 的随机数；

——MIC_1 字段：表示 REQ 利用与 REP 之间的共享密钥 K 或 K 的导出密钥对 $R_{REP} \| R_{REQ} \| Text2$ 利用杂凑算法计算得到的杂凑值；

——MIC_2 字段：表示 REP 利用与 REQ 之间的共享密钥 K 或 K 的导出密钥对 $R_{REQ} \| Text3$ 利用杂凑算法计算得到的杂凑值；

——MIC_3 字段：表示 REQ 利用与 REP 之间的共享密钥 K 或 K 的导出密钥对 $R_{REP} \| Text4$ 利用杂凑算法计算得到的杂凑值。

该机制的执行过程如下：

a) REP 发送随机数 $R_{REP} \| Text1$ 到 REQ。

b) 收到 REP 的信息后，REQ 完成如下步骤：

1) 生成随机数 R_{REQ}；

2) 发送 $R_{REP} \| R_{REQ} \| Text2 \| MIC_1$ 到 REP。

c) 收到来自 REQ 的信息后，REP 完成下列步骤：

1) 校验收到的随机数 R_{REP} 与步骤 a)中发送给 REQ 的随机数 R_{REP} 相一致；

2) 利用与 REQ 之间的共享密钥 K 或 K 的导出密钥校验 MIC_1 字段的正确性。

d) REP 发送 $R_{REQ} \| Text3 \| MIC_2$ 到 REQ。

e) 收到来自 REP 的信息后，REQ 完成下列步骤：

1) 校验收到的随机数 R_{REQ} 与步骤 b)中发送给 REP 的随机数 R_{REQ} 相一致；

2) 利用与 REP 之间的共享密钥 K 或 K 的导出密钥校验 MIC_2 字段的正确性，若不正确，则丢弃该分组；若正确，则完成 REQ 对 REP 的鉴别。

f) REQ 发送 $R_{REP} \| Text4 \| MIC_3$ 到 REP。

g) 收到来自 REQ 的信息后，REP 完成下列步骤：

1) 校验收到的随机数 R_{REP} 与步骤 a)中发送给 REQ 的随机数 R_{REP} 相一致；

2) 利用与 REQ 之间的共享密钥 K 或 K 的导出密钥校验 MIC_3 字段的正确性，若不正确，则丢弃该分组；若正确，则完成 REP 对 REQ 的鉴别。

8.2.2.4 四次传递双向鉴别 2

在基于杂凑算法的四次传递双向鉴别 2 机制中，要求 REQ 和 REP 之间拥有共享密钥 K，鉴别过程的唯一性/时效性通过产生和校验随机数来控制。该鉴别机制在图 10 中说明。

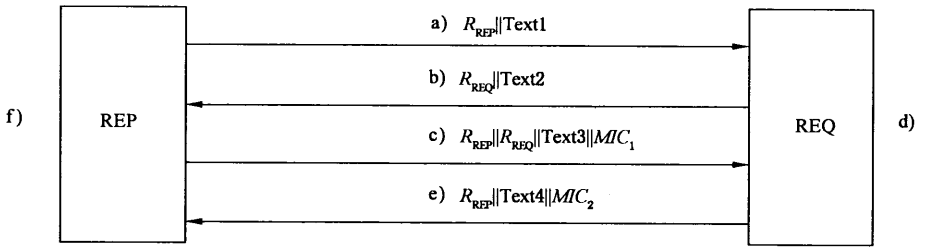


图 10 四次传递双向鉴别 2

图 10 中：

——R_{REP}字段：表示 REP 的随机数；

——R_{REQ}字段：表示 REQ 的随机数；

——MIC_1 字段：表示 REP 利用与 REQ 之间的共享密钥 K 或 K 的导出密钥对 $R_{REP} \| R_{REQ} \| Text3$ 利用杂凑算法计算得到的杂凑值；

——MIC_2 字段：表示 REQ 利用与 REP 之间的共享密钥 K 或 K 的导出密钥对 $R_{REP} \| Text4$ 利用杂凑算法计算得到的杂凑值。

该机制的执行过程如下：

a) REP 发送随机数 $R_{REP} \| Text1$ 到 REQ。

b) 收到 REP 的信息后，REQ 发送 $R_{REQ} \| Text2$ 到 REP。

c) 收到来自 REQ 的信息后，REP 发送 $R_{REP} \| R_{REQ} \| Text3 \| MIC_1$ 到 REQ。

d) 收到来自 REP 的信息，REQ 完成下列步骤：

1) 校验收到的随机数 R_{REQ} 与步骤 b)中发送给 REP 的随机数 R_{REQ} 相一致；

2) 利用与 REP 之间的共享密钥 K 或 K 的导出密钥校验 MIC_1 字段的正确性，若不正确，则丢弃该分组；若正确，则完成 REQ 对 REP 的鉴别。

e) REQ 发送 $R_{REP} \| Text4 \| MIC_2$ 到 REP。

f) 收到来自 REQ 的信息后，REP 完成下列步骤：

1) 校验收到的随机数 R_{REP} 与步骤 a)中发送给 REQ 的随机数 R_{REP} 相一致；

2) 利用与 REQ 之间的共享密钥 K 或 K 的导出密钥校验 MIC_2 字段的正确性，若不正确，则丢弃该分组；若正确，则完成 REP 对 REQ 的鉴别。

8.2.3 基于加密算法的鉴别机制

8.2.3.1 单向鉴别

基于加密算法的单向鉴别机制中，要求 REQ 和 REP 之间拥有共享密钥 K，鉴别过程的唯一性/时效性通过产生和校验随机数来控制。该鉴别机制在图 11 中说明，REQ 被 REP 鉴别，但通过简单更换 REP 和 REQ 的角色，REP 也可被 REQ 鉴别。

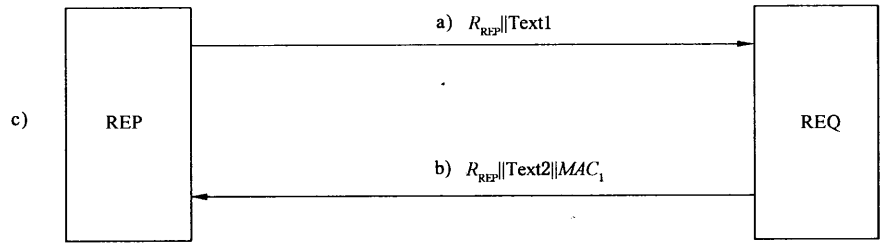


图 11 单向鉴别

图 11 中：

——R_{REP} 字段：表示 REP 的随机数；

——MAC_1 字段：表示 REQ 利用与 REP 之间的共享密钥 K 或 K 的导出密钥对 $R_{REP} \| Text2$ 利用分组加密算法计算得到的密文值。

该机制的执行过程如下：

a) REP 发送随机数 $R_{REP} \| Text1$ 到 REQ。

b) REQ 发送 $R_{REP} \| Text2 \| MAC_1$ 到 REP。

c) 收到来自 REQ 的信息后，REP 完成下列步骤：

1) 校验步骤 a)中发送给 REQ 的随机数 R_{REP} 与接收到的 R_{REP} 相一致；

2) 利用与 REQ 之间的共享密钥 K 或 K 的导出密钥解密 MAC_1 字段得到 $R_{REP}\|$Text2；校验步骤 a)中发送给 REQ 的随机数 R_{REP} 与解密得到的 R_{REP} 相一致。

8.2.3.2 双向鉴别

在该鉴别机制中，唯一性/时效性通过产生和校验随机数来控制。该鉴别机制在图 12 中说明。

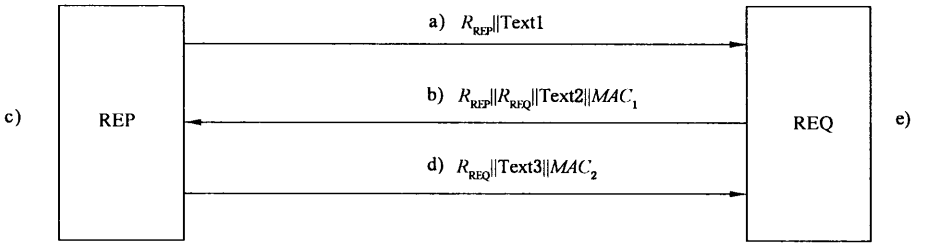


图 12 双向鉴别

图 12 中：

——R_{REP} 字段：表示 REP 的随机数；

——R_{REQ} 字段：表示 REQ 的随机数；

——MAC_1 字段：表示 REQ 利用与 REP 之间的共享密钥 K 或 K 的导出密钥对 $R_{REP}\|R_{REQ}\|$Text2 利用分组加密算法计算得到的密文值；

——MAC_2 字段：表示 REP 利用与 REQ 之间的共享密钥 K 或 K 的导出密钥对 $R_{REQ}\|$Text3 利用分组加密算法计算得到的密文值。

该机制的执行过程如下：

a) REP 发送随机数 $R_{REP}\|$Text1 到 REQ。

b) REQ 发送 $R_{REP}\|R_{REQ}\|$Text2$\|MAC_1$ 到 REP。

c) 收到来自 REQ 的信息后，REP 完成下列步骤：

1) 校验步骤 a)中发送给 REQ 的随机数 R_{REP} 与接收到的 R_{REP} 相一致；

2) 利用与 REQ 之间的共享密钥 K 或 K 的导出密钥解密 MAC_1 字段得到 $R_{REP}\|R_{REQ}\|$Text2；校验步骤 a)中发送给 REQ 的随机数 R_{REP} 与解密得到的 R_{REP} 相一致。

d) REP 发送 $R_{REQ}\|$Text3$\|MAC_2$ 到 REQ。

e) 收到来自 REP 的信息，REQ 完成下列步骤：

1) 校验步骤 b)中发送给 REP 的随机数 R_{REQ} 与收到的 R_{REQ} 相一致；

2) 利用与 REP 之间的共享密钥 K 或 K 的导出密钥解密 MAC_2 字段得到 $R_{REP}\|$Text3；校验步骤 b)中发送给 REP 的随机数 R_{REP} 与解密得到的 R_{REP} 相一致。

8.3 三实体鉴别机制

8.3.1 基于共享信息的鉴别机制

该鉴别机制在图 13 中说明。该鉴别机制中的 E 用于表示对称加密算法，H 用于表示杂凑函数。

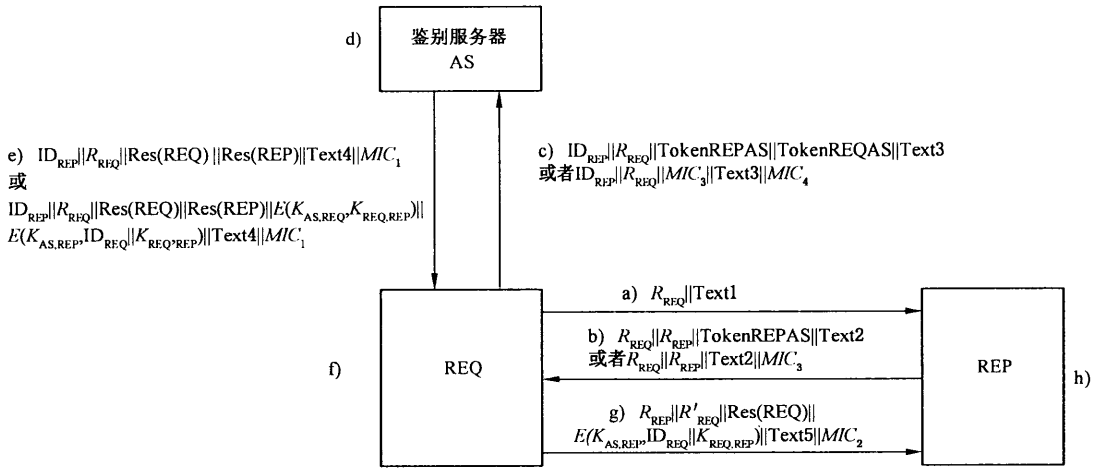


图 13　基于共享信息的三元对等鉴别机制

图 13 中的符号定义如下：

$TokenREPAS=E(K_{AS,REP},R_{REQ})$

$TokenREQAS=E(K_{AS,REQ},R_{REQ})$

$Res(REQ)=E(K_{AS,REP},R(REQ))$

$Res(REP)=E(K_{AS,REQ},R(REP))$

$MIC_1=H(K_{AS,REQ},ID_{REP}\|R_{REQ}\|Res(REQ)\|Res(REP)\|Text4)$(适用于 REQ 或 REP 之一不合法或都不合法时)或者 $MIC_1=H(K_{AS,REQ},ID_{REP}\|R_{REQ}\|Res(REQ)\|Res(REP)\|E(K_{AS,REQ},K_{REQ,REP})\|E(K_{AS,REP},ID_{REQ}\|K_{REQ,REP})\|Text4)$(适用于 REQ 和 REP 均合法的情况)

$MIC_2=H(K_{REQ,REP},R_{REP}\|R'_{REQ}\|Res(REQ)\|E(K_{AS,REP},ID_{REQ}\|K_{REQ,REP})\|Text5)$

$MIC_3=H(K_{AS,REP},R_{REQ}\|Text2)$

$MIC_4=H(K_{AS,REQ},ID_{REP}\|R_{REQ}\|MIC_3\|Text3)$

在这里，鉴别服务器 AS 已与实体 $X(X=\{REQ,REP\})$共享密钥，其中与被鉴别实体 REQ 共享密钥 $K_{AS,REQ}$，与鉴别实体 REP 共享密钥 $K_{AS,REP}$。$R(X)(X=\{REQ,REP\})$的值根据表 1 确定。

表 1　$R(X)$的值

域	选项
IX	X
$R(X)$	True or False

该机制的执行过程如下：

a) REQ 发送随机数 $R_{REQ}\|Text1$ 到 REP。

b) REP 发送 $R_{REQ}\|R_{REP}\|TokenREPAS\|Text2$ 到 REQ。

c) 收到来自 REP 的信息，REQ 完成下列步骤：

1) 校验收到的 R_{REQ}与在步骤 a)中发送给 REP 的随机数 R_{REQ}相一致；

2) 发送 $ID_{REP}\|R_{REQ}\|TokenREPAS\|TokenREQAS\|Text3$ 给 AS。

d) 收到来自 REQ 的信息后，AS 搜索与 REQ 以及 REP 的共享密钥；解密 TokenREQAS 和 TokenREPAS；若解密 TokenREQAS 得到的结果与收到的来自 REQ 的 R_{REQ}相等，则 REQ 合法，否则非法；若解密 TokenREPAS 后得到的结果与收到的来自 REQ 的 R_{REQ}相等，则 REP 合法，否则非法。

e) AS 发送 $ID_{REP} \| R_{REQ} \| Res(REQ) \| Res(REP) \| Text4 \| MIC_1$ 给 REQ。当 Res(REQ)和 Res(REP)均为 True 时，该信息中还包含 $E(K_{AS,REQ}, K_{REQ,REP})$和 $E(K_{AS,REP}, ID_{REQ} \| K_{REQ,REP})$，其中 $K_{REQ,REP}$为 REQ 与 REP 的共享密钥。

f) 收到来自 AS 的信息，REQ 完成下列步骤：

1) 校验收到的 R_{REQ}与在步骤 c)中发送给 AS 的随机数 R_{REQ}相一致；

2) 通过 MIC_1 验证信息的完整性；

3) 根据 Res(REP)判断 REP 的合法性；

4) 解密 $E(K_{AS,REQ}, K_{REQ,REP})$获得 $K_{REQ,REP}$。

g) REQ 发送 $R_{REP} \| R'_{REQ} \| Res(REQ) \| E(K_{AS,REP}, ID_{REQ} \| K_{REQ,REP}) \| Text5 \| MIC_2$ 到 REP。

h) 收到来自 REQ 的信息后，REP 执行下列步骤：

1) 校验收到的 R_{REP}与在步骤 b)中发送给 REQ 的随机数 R_{REP}相一致；

2) 解密 $E(K_{AS,REP}, ID_{REQ} \| K_{REQ,REP})$获得 $K_{REQ,REP}$；

3) 通过 MIC_2 验证信息的完整性；

4) 根据 Res(REQ)判断 REQ 的合法性。

上述步骤 b)～d)也可采用如下实现方式：

b′) REP 发送 $R_{REQ} \| R_{REP} \| Text2 \| MIC_3$ 到 REQ。

c′) 收到来自 REP 的信息，REQ 完成下列步骤：

1) 校验收到的 R_{REQ}与在步骤 a)中发送给 REP 的随机数 R_{REQ}相一致；

2) 发送 $ID_{REP} \| R_{REQ} \| MIC_3 \| Text3 \| MIC_4$ 给 AS。

d′) 收到来自 REQ 的信息后，AS 搜索与 REQ 以及 REP 的共享密钥；根据 MIC_3 和 MIC_4 验证 REQ 和 REP 的合法性。

8.3.2 基于证书的鉴别机制

基于证书的鉴别过程包含 6 个分组，该鉴别过程见图 14。

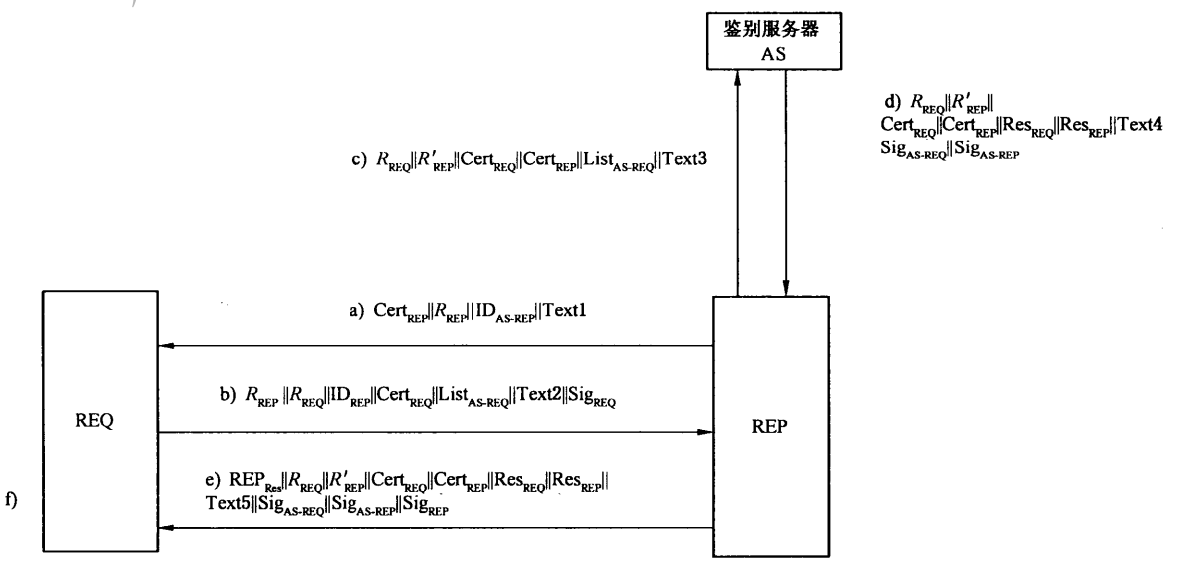


图 14 基于证书的鉴别过程

图 14 中：

R_{REP}字段：表示 REP 的随机数，是 REP 对鉴别过程的新鲜性标识；

R_{REQ}字段：表示 REQ 的随机数，是 REQ 对鉴别过程的新鲜性标识；

R'_{REP}字段：表示 REP 的另一随机数，是 REP 对向 AS 请求证书验证过程的新鲜性标识，可以与R_{REP}字段相同，也可以不同；

ID_{REP}字段：表示 REP 的身份标识；

ID_{REQ}字段：表示 REQ 的身份标识；

$ID_{AS\text{-}REP}$字段：表示 REP 信任的 AS 的标识；

$List_{AS\text{-}REQ}$字段：表示 REQ 信任的 AS 的标识的列表；

$Cert_{REP}$字段：表示 REP 的证书，REP 的证书中包含 ID_{REP}字段；

$Cert_{REQ}$字段：表示 REQ 的证书，REQ 的证书中包含 ID_{REQ}字段；

Res_{REQ}字段：表示 AS 对 REQ 证书的验证结果；

Res_{REP}字段：表示 AS 对 REP 证书的验证结果；

REP_{Res}字段：表示 REP 对 REQ 的验证的结果；

Sig_{REP}字段：表示 REP 对消息 e)中除 Sig_{REP}字段外所有字段的签名；

Sig_{REQ}字段：表示 REQ 对消息 b)中 $R_{REP} \| R_{REQ} \| ID_{REP} \| Cert_{REQ} \| List_{AS\text{-}REQ} \| Text2$ 的签名；

$Sig_{AS\text{-}REQ}$字段：表示 REQ 信任的 AS 对消息 d)中除 $Sig_{AS\text{-}REQ} \| Sig_{AS\text{-}REP}$字段外所有字段的签名；

$Sig_{AS\text{-}REP}$字段：表示 REP 信任的 AS 对消息 d)中除 $Sig_{AS\text{-}REP}$字段外所有字段的签名。

注：REQ 信任的 AS 和 REP 信任的 AS 是同一个 AS 时，就只需要该 AS 对消息 d)中 $R_{REQ} \| R'_{REP} \| Cert_{REQ} \| Cert_{REP} \| Res_{REQ} \| Res_{REP} \| Text4 \| Sig_{AS\text{-}REQ} \| Sig_{AS\text{-}REP}$进行签名即可；对应的消息 e)中也只需要包含一个签名即可。

该机制的执行过程中消息交互如下：

a) REP 发送 $Cert_{REP} \| R_{REP} \| ID_{AS\text{-}REP} \| Text1$ 到 REQ；

b) REQ 发送 $R_{REP} \| R_{REQ} \| ID_{REP} \| Cert_{REQ} \| List_{AS\text{-}REQ} \| Text2 \| Sig_{REQ}$到 REP；

c) REP 发送 $R_{REQ} \| R'_{REP} \| Cert_{REQ} \| Cert_{REP} \| List_{AS\text{-}REQ} \| Text3$ 到 AS；

d) AS 发送 $R_{REQ} \| R'_{REP} \| Cert_{REQ} \| Cert_{REP} \| Res_{REQ} \| Res_{REP} \| Text4 \| Sig_{AS\text{-}REQ} \| Sig_{AS\text{-}REP}$到 REP；
REP 发送 $REP_{Res} \| R_{REQ} \| R'_{REP} \| Cert_{REQ} \| Cert_{REP} \| Res_{REQ} \| Res_{REP} \| Text5 \| Sig_{AS\text{-}REQ} \| Sig_{AS\text{-}REP} \| Sig_{REP}$到 REQ。

该机制的执行过程如下：

a) REP 本地生成一随机数 R_{REP}，发送 $Cert_{REP} \| R_{REP} \| ID_{AS\text{-}REP} \| Text1$ 到 REQ；

b) REQ 收到由 REP 发送的分组后，根据分组中的 $ID_{AS\text{-}REP}$字段选择由该鉴别服务器 AS 实体颁发的证书或者根据本地策略选择证书，本地生成一个随机数 R_{REQ}，发送 $R_{REP} \| R_{REQ} \| ID_{REP} \| Cert_{REQ} \| List_{AS\text{-}REQ} \| Sig_{REQ} \| Text2$ 到 REP；

c) REP 收到由 REQ 发送的分组后，验证分组中 R_{REP}字段与之前 REP 发给 REQ 的随机数是否一致，若不一致，则丢弃该分组；若一致，则验证 REQ 的签名 Sig_{REQ}字段的正确性，若验签失败，则丢弃该分组；若验签成功，REP 本地新生成一个随机数 R'_{REP}，并发送 $R_{REQ} \| R'_{REP} \| Cert_{REQ} \| Cert_{REP} \| List_{AS\text{-}REQ} \| Text3$ 到 AS；

d) AS 收到由 REP 发送的分组后，验证 REQ 的证书 $Cert_{REQ}$和 REP 的证书 $Cert_{REP}$的有效性，发送 $R_{REQ} \| R'_{REP} \| Cert_{REQ} \| Cert_{REP} \| Res_{REQ} \| Res_{REP} \| Text4 \| Sig_{AS\text{-}REQ} \| Sig_{AS\text{-}REP}$到 REP；

e) REP 收到 AS 发送的分组后，验证 $R_{REQ} \| R'_{REP}$与之前发给 AS 的分组中的两个随机数字段是否一致，若不一致，则丢弃该分组；若一致，则验证 REP 信任的 AS 的签名 $Sig_{AS\text{-}REP}$字段的正确性，若验签失败，则丢弃该分组；若验签成功，查看分组中 REQ 证书验证结果 Res_{REQ}字段，并根据该字段给出 REP 对 REQ 的鉴别结果对 REP_{Res}字段进行赋值，发送 $REP_{Res} \| R_{REQ} \| R'_{REP} \| Cert_{REQ} \| Cert_{REP} \| Res_{REQ} \| Res_{REP} \| Text5 \| Sig_{AS\text{-}REQ} \| Sig_{AS\text{-}REP} \| Sig_{REP}$到 REQ；

f) REQ 收到 REP 发送的分组后，验证 R_{REQ}字段与之前发送给 REP 的分组中的 REQ 的随机数是否一致，若不一致，则丢弃该分组；若一致，则验证 REP 的签名 Sig_{REP}字段的正确性，若 Sig_{REP}字段验签失败，则丢弃该分组；若 Sig_{REP}字段验签成功，则进一步验证 REQ 信任的 AS

的签名 $Sig_{AS\text{-}REQ}$ 字段的正确性，若 $Sig_{AS\text{-}REQ}$ 字段验签失败，则丢弃该分组；若 $Sig_{AS\text{-}REQ}$ 字段验签成功，则查看 REP 的证书验证结果 Res_{REP} 字段，若 REP 证书无效，则 REQ 对 REP 身份鉴别失败；若 REP 证书有效，则查看 REP 对 REQ 的鉴别结果 REP_{Res} 字段，若 REP 对 REQ 的鉴别结果失败，则身份鉴别过程失败；若 REP 对 REQ 的鉴别结果成功，则完成双向的身份鉴别过程。

在实体需要匿名时，基于证书的鉴别机制应参照 ISO/IEC 20009-2:2013 采用匿名数字签名算法提供匿名实体鉴别服务。

8.3.3 基于 ID 签名的鉴别机制

该鉴别机制如图 15 所示。

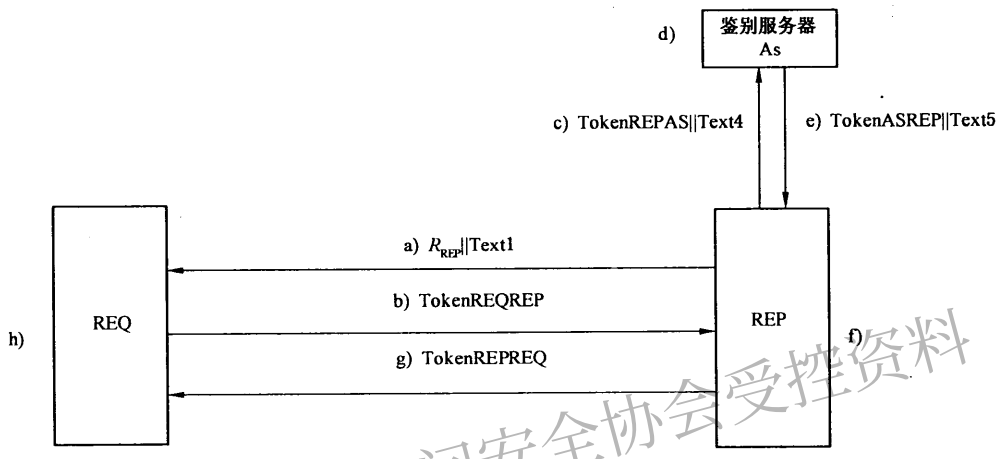


图 15 基于 ID 签名的鉴别机制

权标可以是下面的四种形式：

选项 1：

$TokenREQREP=R_{REP}\|R_{REQ}\|g^{x}\|ID_{REP}\|P_{REQ}\|Text3\|sS_{REQ}(R_{REP}\|R_{REQ}\|g^{x}\|ID_{REP}\|P_{REQ}\|Text2)$

$TokenREPAS=R_{REQ}\|R'_{REP}\|P_{REQ}\|P_{REP}$

$TokenASREP=R'_{REP}\|Re_{REQ}\|Res_{REP}$

$TokenREPREQ=R_{REQ}\|g^{y}\|ID_{REQ}\|P_{REP}\|Res_{REP}\|Text7\|sS_{REP}(R_{REQ}\|g^{y}\|ID_{REQ}\|P_{REP}\|Res_{REP}\|Text6)$

选项 2：

$TokenREQREP=R_{REP}\|R_{REQ}\|g^{x}\|ID_{REP}\|P_{REQ}\|Text3\|sS_{REQ}(R_{REP}\|R_{REQ}\|g^{x}\|ID_{REP}\|P_{REQ}\|Text2)$

$TokenREPAS=R'_{REP}\|P_{REQ}$

$TokenASREP=R'_{REP}\|Re_{REQ}$

$TokenREPREQ=R_{REQ}\|g^{y}\|ID_{REQ}\|P_{REP}\|Text7\|sS_{REP}(R_{REQ}\|g^{y}\|ID_{REQ}\|P_{REP}\|Text6)$

选项 3：

$TokenREQREP=R_{REP}\|R_{REQ}\|g^{x}\|ID_{REP}\|P_{REQ}\|Text3\|sS_{REQ}(R_{REP}\|R_{REQ}\|g^{x}\|ID_{REP}\|P_{REQ}\|Text2)$

$TokenREPAS=R_{REQ}\|R'_{REP}\|P_{REP}$

$TokenASREP=R'_{REP}\|Res_{REP}$

$TokenREPREQ=R_{REQ}\|g^{y}\|ID_{REQ}\|P_{REP}\|Res_{REP}\|Text7\|sS_{REP}(R_{REQ}\|g^{y}\|ID_{REQ}\|P_{REP}\|Res_{REP}\|Text6)$

选项 4：

$TokenREQREP=R_{REP}\|R_{REQ}\|g^{x}\|ID_{REP}\|P_{REQ}\|Text3\|sS_{REQ}(R_{REP}\|R_{REQ}\|g^{x}\|ID_{REP}\|P_{REQ}\|Text2)$

$TokenREPREQ=R_{REQ}\|g^{y}\|ID_{REQ}\|P_{REP}\|Text7\|sS_{REP}(R_{REQ}\|g^{y}\|ID_{REQ}\|P_{REP}\|Text6)$

Re_{REQ}和 Res_{REP}字段的值如下：

$Re_{REQ}=Status$

$Res_{REP}=R_{REQ}\|P_{REP}\|Re_{REP}\|Text9\|sS_{AS}(R_{REQ}\|P_{REP}\|Re_{REP}\|Text8)$

其中，Re_{REP} = Status，Status = True or False。若基于 ID 的公钥是被撤销的，则该字段的值是 False，否则该字段的值是 True。

该鉴别机制的执行过程如下：

a) REP 发送随机数 $R_{REP}\|Text1$ 到 REQ。

b) REQ 发送 TokenREQREP 到 REP。

c) 若 REQ 要求验证 REP 的基于 ID 的公钥 P_{REP}的有效性或 REP 要求验证 REQ 的基于 ID 的公钥 P_{REQ}的有效性，则 REP 发送 TokenREPAS ‖ Text4 到 AS；否则，REP 获得 REQ 的基于 ID 的公钥 P_{REQ}，然后验证包含在权标 TokenREQREP 中 REQ 的签名，检查在步骤 a)中发送给 REQ 的随机数 R_{REP}是否与包含在 TokenREQREP 中的随机数 R_{REP}一致，检查包含在 TokenREQREP 中的签名数据中的身份标识 ID_{REP}是否与 REP 的身份标识 ID_{REP}一致，最后跳至步骤 h)。

d) 收到来自 REP 的信息后，若 TokenREPAS 中包含 REQ 的基于 ID 的公钥 P_{REQ}，则 AS 检查 P_{REQ}的有效性并生成相应的公钥撤销结果 Re_{REQ}；若 TokenREPAS 中包含 REP 的基于 ID 的公钥 P_{REP}，则 AS 检查 P_{REP}的有效性并生成相应的公钥撤销结果 Re_{REP}和公钥撤销查询结果 Res_{REP}。

e) AS 发送 TokenASREP ‖ Text5 到 REP。

f) 收到来自 AS 的信息后，REP 完成以下步骤：

1) 检查在步骤 c)中发送给 AS 的随机数 R'_{REP}是否与包含在 TokenASREP 中的随机数 R'_{REP}一致；

2) 获得 REQ 的基于 ID 的公钥 P_{REQ}，然后验证包含在权标 TokenREQREP 中 REQ 的签名，检查在步骤 a)中发送给 REQ 的随机数 R_{REP}是否与包含在 TokenREQREP 中的随机数 R_{REP}一致，检查包含在 TokenREQREP 中的签名数据中的身份标识 ID_{REP}是否与 REP 的身份标识 ID_{REP}一致。

g) REP 发送 TokenREPREQ 到 REQ。

h) 收到来自 REP 的信息后，REQ 完成以下步骤：

1) 若 TokenREP_{REQ}中包含 Res_{REP}，则验证包含在 Res_{REP}中的 AS 的签名，检查在步骤 b)中发送给 REP 的随机数 R_{REQ}是否与包含在 Res_{REP}中的随机数 R_{REQ}一致；

2) 获得 REP 的基于 ID 的公钥 P_{REP}，然后验证包含在权标 TokenREPREQ 中 REP 的签名，检查在步骤 b)中发送给 REP 的随机数 R_{REQ}是否与包含在 TokenREPREQ 中的随机数 R_{REQ}一致，检查包含在 TokenREPREQ 中的签名数据中的身份标识 ID_{REQ}是否与 REQ 的身份标识 ID_{REQ}一致。若不一致，则身份鉴别过程失败；若一致，则完成双向的身份鉴别过程。

在上述鉴别机制中，REP 和 AS 之间的数据交换被保护，提供该保护的机制超出了本标准的范围。

在上述鉴别机制中，REQ 和 REP 分别计算基密钥 $BK=H(g^{xy},R_{REQ}\|R_{REP}\|Text10)$。

9 共享信息协商协议

9.1 单播共享信息协商

9.1.1 基于共享基密钥的单播密钥协商

9.1.1.1 鉴别消息交互过程

该鉴别过程如图 16 所示。

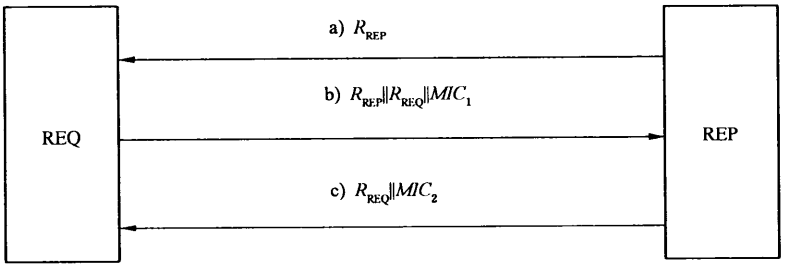


图 16 基于共享基密钥的单播密钥协商

该机制的执行过程中消息交互如下：

a) REP 发送 R_{REP} 到 REQ；

b) REQ 发送 $R_{REP}\|R_{REQ}\|MIC_1$ 到 REP；

c) REP 发送 $R_{REQ}\|MIC_2$ 到 REQ。

或者是：

a) REQ 发送 R_{REQ} 到 REP；

b) REP 发送 $R_{REQ}\|R_{REP}\|MIC_1$ 到 REP；

c) REQ 发送 $R_{REP}\|MIC_2$ 到 REP。

也即 REP 和 REQ 均可主动发起该密钥协商过程；以 REP 发起为例进行说明：

图 16 中：

R_{REP} 字段：表示 REP 的随机数，是 REP 对密钥协商过程的新鲜性标识；

R_{REQ} 字段：表示 REQ 的随机数，是 REQ 对密钥协商过程的新鲜性标识；

MIC_1 字段：表示 REQ 对消息 b)中 $R_{REQ}\|R_{REP}$ 利用与 REP 之间通过该过程最新协商得到的单播密钥计算得到的完整性校验值；

MIC_2 字段：表示 REP 对消息 c)中 R_{REQ} 利用与 REQ 之间通过该过程最新协商得到的单播密钥计算得到的完整性校验值。

9.1.1.2 鉴别机制的执行过程

该机制的执行过程如下：

a) 当 REP 需要发起与 REQ 之间的基于共享基密钥的单播密钥协商过程时，REP 本地生成一随机数 R_{REP}，发送 R_{REP} 到 REQ；

b) REQ 收到 REP 发送的分组后，本地生成一随机数 R_{REQ}，并使用密钥导出算法对 R_{REP}、R_{REQ}、BK 等密钥材料计算得到与 REP 之间最新协商的单播密钥；并发送 $R_{REQ}\|R_{REP}\|MIC_1$ 到 REP；

c) REP 收到 REQ 发送的分组后，验证分组中的 R_{REP} 字段与之前发送给 REQ 的随机数是否一致，若不一致，则丢弃该分组；若一致，则验证分组中 MIC_1 字段的正确性，若不正确，则丢弃该分组；否则，REP 使用密钥导出算法对 R_{REP}、R_{REQ}、BK 等密钥材料计算得到与 REP 之间最新协商的单播密钥，并发送 $R_{REQ} \| MIC_2$ 到 REQ；

d) REQ 收到 REP 发送的分组后，验证分组中的 R_{REQ} 字段与之前发送给 REP 的随机数是否一致，若不一致，则丢弃该分组；若一致，则利用之前计算得到的最新协商的单播密钥验证 MIC_2 字段的正确性，若不正确，则丢弃该分组；否则，确认 REP 已建立和自己一致的单播密钥，完成此次单播密钥的协商过程。

9.1.2 基于 DH 交换的单播密钥协商

9.1.2.1 基于 DH 交换的单播密钥协商过程如图 17 所示。

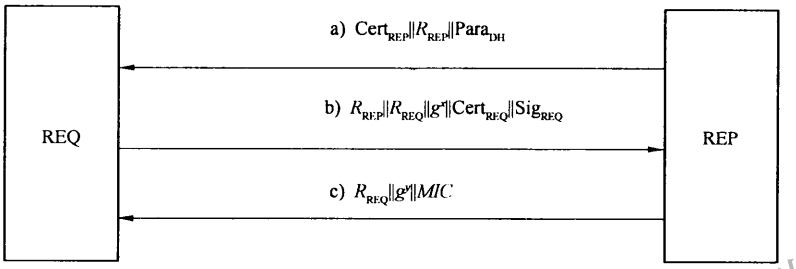


图 17 基于 DH 交互的单播密钥协商

该机制的执行过程中消息交互如下：

a) REP 发送 $Cert_{REP} \| R_{REP} \| Para_{DH}$ 到 REQ；

b) REQ 发送 $R_{REP} \| R_{REQ} \| g^x \| Cert_{REQ} \| Sig_{REQ}$ 到 REP；

c) REP 发送 $R_{REQ} \| g^y \| MIC$ 到 REQ。

图 17 中：

R_{REP} 字段：表示 REP 的随机数，是 REP 对密钥协商过程的新鲜性标识；

R_{REQ} 字段：表示 REQ 的随机数，是 REQ 对密钥协商过程的新鲜性标识；

$Cert_{REP}$ 字段：表示 REP 的证书，REP 的证书中包含 REP 的公钥信息；

$Cert_{REQ}$ 字段：表示 REQ 的证书，REQ 的证书中包含 REQ 的公钥信息；

g^x 字段：表示 REQ 的临时公钥，用于 DH 交换；

g^y 字段：表示 REP 的临时公钥，用于 DH 交换；

$Para_{DH}$ 字段：表示 DH 参数；

Sig_{REQ} 字段：表示 REQ 对消息 b)中 $R_{REP} \| R_{REQ} \| g^x \| Cert_{REQ}$ 的签名；

MIC 字段：表示 REP 利用最新协商得到的单播密钥对消息 c)中 $R_{REQ} \| g^y$ 计算得到的完整性校验值。

9.1.2.2 基于 DH 交换的单播密钥协商机制的执行过程如下：

a) 当 REP 需要发起与 REQ 之间的基于 DH 交换的单播密钥协商时，REP 本地生成一随机数 R_{REP}，REP 发送 $Cert_{REP} \| R_{REP} \| Para_{DH}$ 到 REQ；

b) REQ 收到 REP 发送的分组后，本地生成一随机数 R_{REQ}，并产生用于 DH 交换的临时私钥 x、临时公钥 g^x，发送 $R_{REP} \| R_{REQ} \| g^x \| Cert_{REQ} \| Sig_{REQ}$ 到 REP；

c) REP 收到 REQ 发送的分组后，首先验证分组中的 R_{REP} 字段与之前发送给 REQ 的分组中的 REP 的随机数是否一致，若不一致，则丢弃该分组；若一致，则验证 REQ 的签名 Sig_{REQ} 字段的

正确性，若验签失败，则丢弃该分组；若验签成功，则产生用于 DH 交换的临时私钥 y、临时公钥 g^y，使用自己的临时私钥 y 和接收到的分组中 REQ 的临时公钥 g^x 进行 DH 计算，进而使用密钥导出算法对(DH(g^{xy})，R_{REP}，R_{REQ})进行计算扩展得到最新协商的单播密钥，并发送 $R_{REQ} \| g^y \| MIC$ 到 REQ；

d) REQ 收到 REP 发送的分组后，首先验证分组中 R_{REQ} 字段与之前发送给 REP 的分组中的 REQ 的随机数是否一致，若不一致，则丢弃该分组；若一致使用自己的临时私钥 x 和接收到的分组中 REP 的临时公钥 g^y 进行 DH 计算，进而使用密钥导出算法对(DH(g^{xy})，R_{REP}，R_{REQ}))进行计算扩展得到最新协商的单播密钥，并利用该密钥验证 MIC 字段的正确性，若不正确，则丢弃该分组；否则，即可确认已和 REP 协商得到一致的单播密钥，完成此次密钥协商过程。

9.2 组播共享信息协商

9.2.1 基于会话密钥的组播密钥协商

9.2.1.1 基于会话密钥的组播密钥协商过程如图 18 所示。

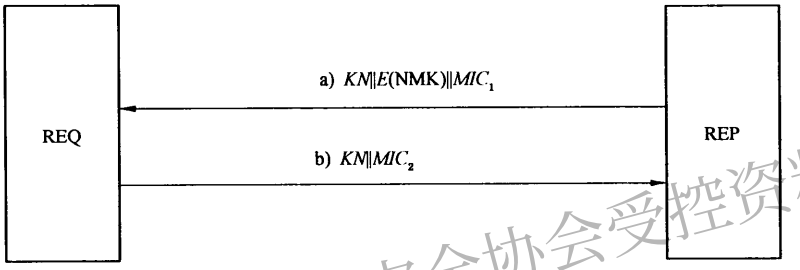


图 18 组播密钥通告

该机制的执行过程中消息交互如下：

a) REP 发送 $KN \| E(NMK) \| MIC_1$ 到 REQ；

b) REQ 发送 $KN \| MIC_2$ 到 REP。

图 18 中：

KN 字段：表示密钥通告标识，表示一个整数，在每次密钥更新通告时该字段值加 1；若通告的密钥不变，则本字段值保持不变；该字段还用作密钥通告数据的 IV；

E(NMK) 字段：表示密钥通告数据，是 REP 利用与 REQ 之间的单播密钥对通告主密钥 NMK 加密(不带 MIC)后的密文，通告主密钥 NMK 为 REP 生成的随机数；

MIC_1 字段：表示 REP 对消息 a)中 $KN \| E(NMK)$利用与 REQ 之间的单播密钥计算得到的完整性校验值；

MIC_2 字段：表示 REQ 对消息 b)中 KN 利用与 REP 之间的单播密钥计算得到的完整性校验值。

9.2.1.2 基于会话密钥的组播密钥协商机制的执行过程如下：

a) 当 REP 需要将组播密钥通告给 REQ 时，REP 本地生成一随机数作为通告主密钥 NMK，REP 利用与 REQ 之间的单播密钥对通告主密钥 NMK 加密，发送 $KN \| E(NMK) \| MIC_1$ 到 REQ；

b) 当 REQ 收到 REP 发送的分组后，REQ 验证 KN 是否单调递增，若不是，则丢弃该分组；若是，则验证 MIC_1 字段是否正确，若不正确，则丢弃该分组；若正确，则解密 E(NMK) 字段，即可得到通告主密钥 NMK，利用密钥导出算法扩展 NMK 即可得到组播密钥，发送 $KN \| MIC_2$ 到 REP；

c) REP 收到 REQ 发送的分组后，验证分组中的 KN 字段与之前发送给 REQ 的分组中的 KN

是否一致，若不一致，则丢弃该分组；若一致，则验证 MIC_2 字段是否正确，若不正确，则丢弃该分组；若正确，则完成对 REQ 的组播密钥通告过程。

9.2.2 基于密钥加密密钥的组播密钥协商

9.2.2.1 基于密钥加密密钥的组播密钥协商机制分为两个步骤，步骤 1：组播密钥加密密钥 GKEK 分发和步骤 2：组播密钥通告，如图 19 所示。

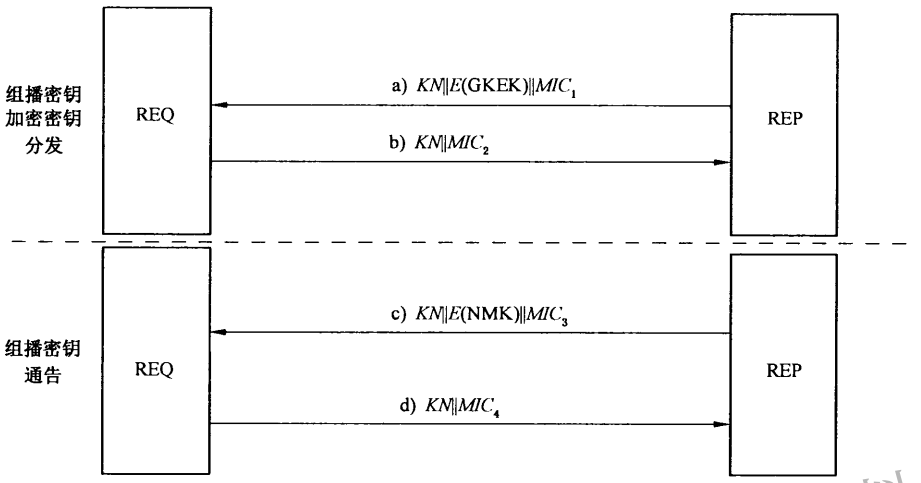


图 19 组播密钥通告

步骤 1 组播密钥加密密钥 GKEK 分发的执行过程中消息交互如下：

a) REP 发送 $KN \| E(\text{GKEK}) \| MIC_1$ 到 REQ；

b) REQ 发送 $KN \| MIC_2$ 到 REP。

图 19 中：

KN 字段：表示密钥通告标识，表示一个整数，在每次密钥更新通告时该字段值加 1；若通告的密钥不变，则本字段值保持不变；该字段还用作密钥通告数据的 IV；

$E(\text{GKEK})$ 字段：表示密钥通告数据，是 REP 利用与 REQ 之间的单播密钥对组播密钥加密密钥 GKEK 加密（不带 MIC）后的密文，组播密钥加密密钥 GKEK 分发为 REP 生成的随机数；

MIC_1 字段：表示 REP 对消息 a）中 $KN \| E(\text{GKEK})$ 利用与 REQ 之间的单播密钥计算得到的完整性校验值；

MIC_2 字段：表示 REQ 对消息 b）中 KN 利用与 REP 之间的单播密钥计算得到的完整性校验值；

步骤 2 组播密钥通告的执行过程中消息交互如下：

c) REP 发送 $KN \| E(\text{NMK}) \| MIC_3$ 到 REQ；

d) REQ 发送 $KN \| MIC_4$ 到 REP。

图 19 中：

KN 字段：表示密钥通告标识，表示一个整数，在每次密钥更新通告时该字段值加 1；若通告的密钥不变，则本字段值保持不变；该字段还用作密钥通告数据的 IV；

$E(\text{NMK})$ 字段：表示密钥通告数据，是 REP 利用与 REQ 之间步骤 1 中分发的组播密钥加密密钥 GKEK 对通告主密钥 NMK 加密（不带 MIC）后的密文，通告主密钥 NMK 为 REP 生成的随机数；

MIC_3 字段：表示 REP 对消息 c）中 $KN \| E(\text{NMK})$ 利用与 REQ 之间的组播密钥加密密钥 GKEK 计算得到的完整性校验值；

MIC_4 字段：表示 REQ 对消息 d)中 KN 利用与 REP 之间的组播密钥加密密钥 GKEK 计算得到的完整性校验值。

9.2.2.2 基于密钥加密密钥的组播密钥协商机制的执行过程如下：

a) 当 REP 需要将组播密钥通告给 REQ 时，REP 本地生成一随机数作为组播密钥加密密钥 GKEK(同一组内使用的组播密钥加密密钥 GKEK 相同)，REP 利用与 REQ 之间的单播密钥对组播密钥加密密钥 GKEK 加密，发送 $KN \| E(\text{GKEK}) \| MIC_1$ 到 REQ；

b) 当 REQ 收到 REP 发送的分组后，REQ 验证 KN 是否单调递增，若不是，则丢弃该分组；若是，则验证 MIC_1 字段是否正确，若不正确，则丢弃该分组；若正确，则解密 $E(\text{GKEK})$ 字段，即可得到组播密钥加密密钥 GKEK，利用密钥导出算法扩展组播密钥加密密钥 GKEK 即可得到分别用于计算完整性校验值和机密性保护功能的组播密钥加密密钥，发送 $KN \| MIC_2$ 到 REP；

c) REP 收到 REQ 发送的分组后，验证分组中的 KN 字段与之前发送给 REQ 的分组中的 KN 是否一致，若不一致，则丢弃该分组；若一致，则验证 MIC_2 字段是否正确，若不正确，则丢弃该分组；若正确，则完成步骤 1 对 REQ 的组播密钥加密密钥 GKEK 分发过程；

d) 当 REP 完成对 REQ 的组播密钥加密密钥 GKEK 分发过程后，REP 本地生成一随机数作为通告主密钥 NMK(同一组内使用的通告主密钥 NMK 相同)，REP 利用与组内所有 REQ 之间相同的组播密钥加密密钥 GKEK 加密，发送 $KN \| E(\text{NMK}) \| MIC_3$ 到 REQ，在 $E(\text{NMK})$ 的计算过程中 REP 可利用与组内所有 REQ 之间相同的组播密钥加密密钥 GKEK 一次处理产生；

e) 当 REQ 收到 REP 发送的分组后，REQ 验证 KN 是否单调递增，若不是，则丢弃该分组；若是，则验证 MIC_3 字段是否正确，若不正确，则丢弃该分组；若正确，则解密 $E(\text{NMK})$ 字段，即可得到通告主密钥 NMK，利用密钥导出算法扩展 NMK 即可得到组播密钥，发送 $KN \| MIC_4$ 到 REP；

f) REP 收到 REQ 发送的分组后，验证分组中的 KN 字段与之前发送给 REQ 的分组中的 KN 是否一致，若不一致，则丢弃该分组；若一致，则验证 MIC_4 字段是否正确，若不正确，则丢弃该分组；若正确，则完成对 REQ 的组播密钥通告过程。

附 录 A
（规范性附录）
应 用 领 域

A.1 概述

本标准可应用于 WPAN、WLAN、WMAN、RFID、WSN、LAN、IP 网络等，建立网络节点/设备之间的可靠连接，说明如下。

A.2 三元访问鉴别与授权（TAAA）

基于三元对等架构的无线城域网安全访问架构，完成终端和基站之间的双向身份鉴别或者基站对终端的单向身份鉴别，确保通信双方身份的合法性。

基于三元对等架构的无线城域网安全访问架构，采用 8.3.2 规定的基于证书的鉴别机制实现了终端和基站之间的身份鉴别。

基于三元对等架构的无线城域网安全访问架构，采用 9.1.1 规定的基于共享基密钥的单播协商为终端和基站提供共享的会话密钥。

基于三元对等架构的无线城域网安全访问架构，采用 9.2.2 规定的基于密钥加密密钥的组播协商实现组播密钥的分发和更新。

基于三元对等架构的无线城域网安全访问架构采用 9.1.1 及 9.2.2 所规定的机制建立的会话密钥和组播密钥为无线城域网提供保密通信服务。

A.3 可信连接架构（TCA）

可信连接架构，见 GB/T 29828—2013，基于三元对等架构的可信网络连接架构，为终端访问受保护网络提供可信网络连接服务。

基于三元对等架构的可信网络连接架构，采用第 8 章规定的各种鉴别协议实现了用户身份鉴别。

基于三元对等架构的可信网络连接架构，采用 9.1 规定的各种单播密钥协商协议实现单播密钥协商。

基于三元对等架构的可信网络连接架构，采用 9.2 规定的各种组播密钥协商协议实现组播密钥协商。

A.4 可信 IP 安全（TISec）

可信 IP 安全，通过安全鉴别、密钥管理和保密通信服务，在 IP 网络上实现 VPN。

可信 IP 安全，采用 8.3.2 所规定的基于证书的鉴别机制实现用户终端和接入点之间的双向身份鉴别，确保通信双方身份的合法性和准入性。

A.5 基于三元对等架构的局域网媒体访问控制安全（TLSec）

基于三元对等架构的局域网媒体访问控制安全，见 GB/T 15629.3—2014，为有线局域网提供 MAC

层的安全鉴别、密钥管理和保密通信服务。

基于三元对等架构的局域网媒体访问控制安全解决方案，采用 8.3.2 所规定的基于证书的鉴别机制实现用户终端和交换设备之间以及交换设备和交换设备之间的双向身份鉴别，或者采用 8.2.2.2 所规定的基于杂凑算法的三次传递双向鉴别机制实现用户终端和交换设备之间以及交换设备和交换设备之间的双向身份鉴别；以确保合法的局域网设备接入合法的局域网。

基于三元对等架构的局域网媒体访问控制安全解决方案，采用 9.1.1 所规定的基于共享基密钥的单播密钥协商过程为用户终端和交换设备之间以及交换设备和交换设备之间建立共享的单播密钥；采用 9.2.1 所规定的基于会话密钥的组播密钥协商机制完成局域网组播密钥的分发和更新。

基于三元对等架构的局域网媒体访问控制安全解决方案，采用 9.1.1 及 9.2.1 所规定的机制建立的单播密钥以及组播密钥为局域网提供保密通信服务。

A.6 基于三元对等架构的电力线通信网络安全(TPLS)

基于三元对等架构的电力线通信网络安全，为电力线通信提供安全鉴别、密钥管理和保密通信服务。

基于三元对等架构的电力线通信网络安全解决方案，采用 8.3.2 所规定的基于证书的鉴别机制实现用户终端/隐藏的用户终端与网络中心协调管理器/代理协调管理器之间的双向身份鉴别，或者采用 8.2.2.2 所规定的基于杂凑算法的三次传递双向鉴别机制实现用户终端/隐藏的用户终端与网络中心协调管理器/代理协调管理器之间的双向身份鉴别；以确保合法的用户终端接入合法的电力线通信网络。

基于三元对等架构的电力线通信网络安全解决方案，采用 9.1.1 所规定的基于共享基密钥的单播密钥协商过程为用户终端/隐藏的用户终端与网络中心协调管理器/代理协调管理器之间建立共享的单播密钥。

基于三元对等架构的电力线通信网络安全解决方案，采用 9.1.1 所规定的机制建立的单播密钥为电力线通信提供保密通信服务。

A.7 基于三元对等架构的以太无源光网络安全(TPSec)

基于三元对等架构的以太无源光网络安全，为以太无源光网络提供安全鉴别、密钥管理和保密通信服务。

基于三元对等架构的以太无源光网络安全解决方案，采用 8.3.2 所规定的基于证书的鉴别机制实现光线路终端 OLT 和光网络单元 ONU 之间的双向身份鉴别，或者采用 8.2.2.2 所规定的基于杂凑算法的三次传递双向鉴别机制实现光线路终端 OLT 和光网络单元 ONU 的双向身份鉴别；以确保合法的光网络单元 ONU 接入合法的光线路终端 OLT。

基于三元对等架构的以太无源光网络安全解决方案，采用 9.1.1 所规定的基于共享基密钥的单播密钥协商过程为光线路终端 OLT 和光网络单元 ONU 之间建立共享的单播密钥；采用 9.2.2 所规定的基于密钥加密密钥的组播密钥协商机制完成局域网组播密钥的分发与更新。

基于三元对等架构的以太无源光网络安全解决方案，使用采用 9.1.1 及 9.2.2 所规定的机制建立的单播密钥以及组播密钥为以太无源光网络提供保密通信服务。

A.8 标签和读写器空中接口安全(TRAIS)

基于三元对等架构架构的 RFID 空中接口安全解决方案，见 GB/T 28925—2012 或 GB/T 29768—2013，为读写器和标签之间提供身份鉴别、密钥协商和信息机密性等安全服务。

射频识别空中接口安全方案采用 8.2.1 所规定的基于异或运算的鉴别机制，或者 8.2.2 所规定的基于杂凑算法的鉴别机制，或者 8.2.3 所规定的基于加密算法的鉴别机制，或者 8.3.2 所规定的基于证书的鉴别机制，实现读写器与电子标签之间单向或双向的身份鉴别，确保通信过程中读写器和电子标签身份的合法性。

射频识别空中接口安全方案采用 9.1.1 所规定的基于共享基密钥的单播密钥协商过程为读写器和电子标签提供共享的会话密钥。

射频识别空中接口安全方案采用 9.1.1 所规范的机制建立的会话密钥为读写器和电子标签提供保密通信服务。

A.9 传感器网络安全基础结构（TSSI）

基于三元对等架构的传感器网络安全整体解决方案，为传感器网络提供密钥管理、鉴别和访问控制等安全服务。

传感器网络安全基础结构采用 8.2.1 所规定的基于异或运算的鉴别机制，或者 8.2.2 所规定的基于杂凑算法的鉴别机制，或者 8.2.3 所规定的基于加密算法的鉴别机制，或者 8.3.2 所规定的基于证书的鉴别机制，实现传感器网络节点之间的双向身份鉴别，确保通信节点双方身份的合法性。

传感器网络安全基础结构采用 9.1.1 所规定的基于共享基密钥的单播密钥协商过程为读写器和电子标签提供共享的会话密钥，采用 9.2.1 所规定的基于会话密钥的组播密钥协商机制实现传感器网络中组播密钥的分发和更新。

传感器网络安全基础结构采用 9.1.1 及 9.2.1 所规范的机制建立的会话密钥和组播密钥为传感器网络节点间提供保密通信服务。

A.10 无线局域网鉴别与保密基础结构（WAPI）

无线局域网鉴别与保密基础结构，见 GB 15629.11—2003/XG1—2006，为终端和无线接入点 AP 之间提供身份鉴别、密钥协商和信息机密性等安全服务。

无线局域网鉴别与保密基础结构，采用 8.3.2 规定的鉴别协议实现了终端和无线接入点 AP 的身份鉴别。

无线局域网鉴别与保密基础结构，采用 9.1.1 规定的单播密钥协商协议实现单播密钥协商。

无线局域网鉴别与保密基础结构，采用 9.2.2 规定的组播密钥协商协议实现组播密钥协商。

无线局域网鉴别与保密基础结构，采用 9.1.1 及 9.2.2 所规范的机制建立的会话密钥和组播密钥为无线局域网提供保密通信服务。

A.11 WPAN 安全访问基础设施（WSAI）

实现 WPAN 中设备通过协调器安全访问网络的基础设施，见 GB/T 15629.15—2010。

WPAN 安全访问基础设施，采用 8.2.2.2 规定的三次传递双向鉴别或者 8.3.3 规定的基于 ID 签名的鉴别方法实现了身份鉴别。

WPAN 安全访问基础设施，采用 9.1.1 规定的基于共享基密钥单播密钥协商协议实现单播密钥协商。

WPAN 安全访问基础设施，采用 9.2.1 规定的基于会话密钥的组播密钥协商协议实现组播密钥协商。

WPAN 安全访问基础设施，采用 9.1.1 及 9.2.1 所规范的机制建立的单播密钥以及组播密钥为

WPAN 提供保密通信服务。

A.12 NFC 实体鉴别(NEAU)

基于三元对等架构的 NFC 空中接口安全,为 NFC 设备之间提供身份鉴别和密钥协商等安全服务。

NFC 实体鉴别,采用 8.2.2.2 规定的三次传递双向鉴别或者 8.3.2 规定的基于证书的鉴别机制实现身份鉴别。

NFC 实体鉴别,采用 9.1.2 规定的基于 DH 交换的单播密钥协商协议实现单播密钥协商,用于为 NFC 空中接口提供保密通信服务。

A.13 移动支付空中接口安全(MPAS)

基于三元对等架构的移动支付空中接口安全,见 GB/T 30001.1—2013,为移动支付设备之间提供身份鉴别和密钥协商等安全服务。

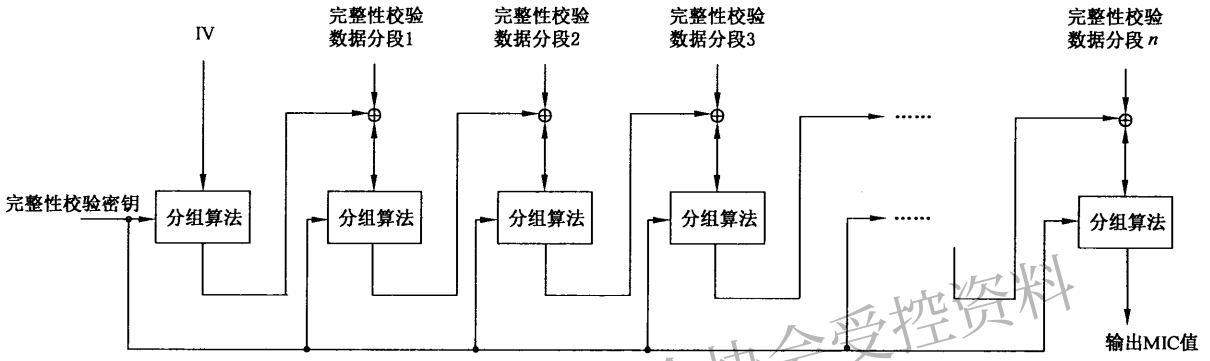
移动支付空中接口安全,采用 8.2.2.2 规定的三次传递双向鉴别或者 8.3.2 规定的基于证书的鉴别机制实现身份鉴别。

移动支付空中接口安全,采用公钥加密的方式实现单播密钥传输,用于为移动支付空中接口提供保密通信服务。

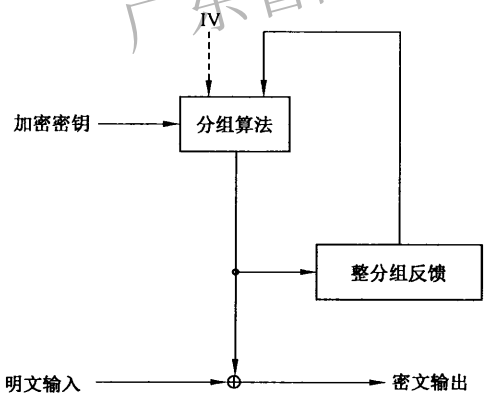
附 录 B
（资料性附录）
工 作 模 式

B.1 工作模式一

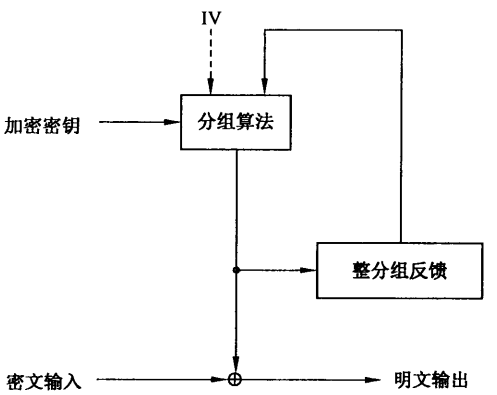
完整性校验算法工作在CBC-MAC模式，数据保密采用的对称加密算法工作在OFB模式。两种模式如图B.1所示，图中符号⊕表示异或运算。



a) CBC-MAC模式



b) OFB加密模式

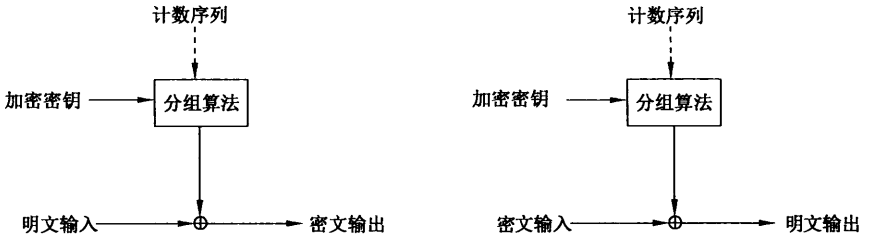


c) OFB解密模式

图 B.1 工作模式一

B.2 工作模式二

数据保密通常还采用计数器CTR模式，其具体的工作模式如图B.2所示。



a) CTR加密模式　　b) CTR解密模式

图 B.2　工作模式二

图 B.2 中计数序列的长度与输入的明文长度相同。

B.3　工作模式三

完整性校验算法和数据保密采用 CCM 模式，其中完整性校验算法采用 CBC-MAC 模式，数据保密采用 CTR 模式。该加密模式如图 B.3 所示。

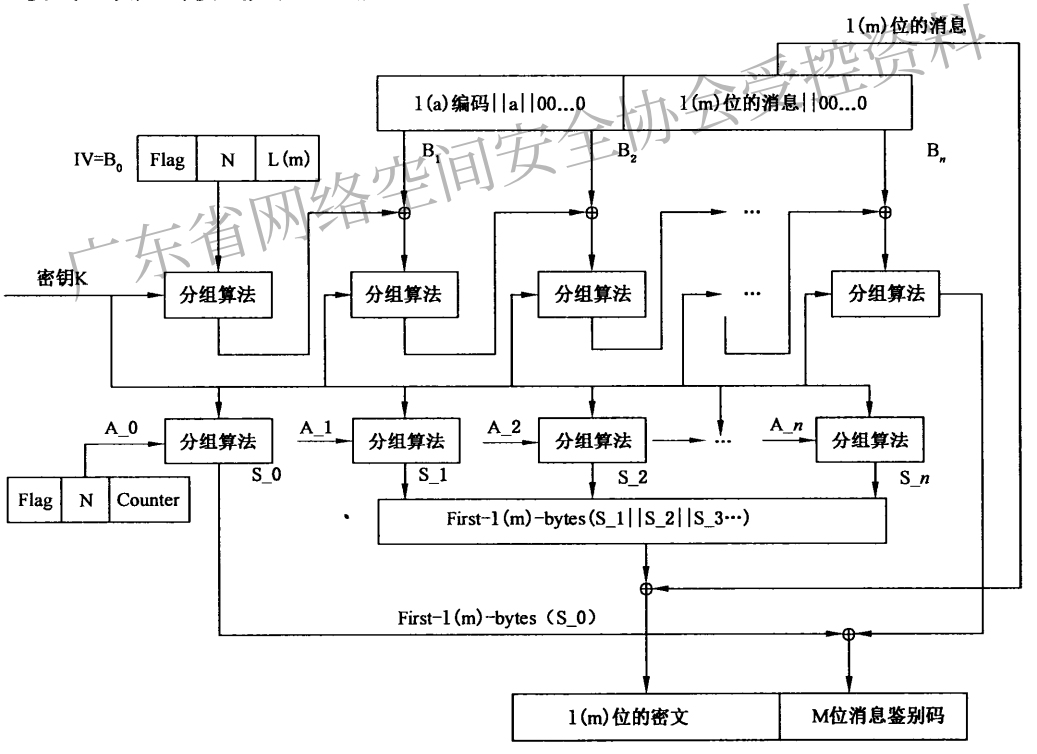


图 B.3　工作模式三

CCM 模式中的参数包括：

N：随机数 Nonce；

m：用来加密和产生消息鉴别码的消息，长度为 1(m)个八位位组；

a：附加鉴别数据，长度为 1(a)个八位位组，例如数据包号；

M：消息鉴别码的长度，表示 M 个八位位组；

L：表示需要加密的消息长度 1(m)的长度，表示 L 个八位位组。

B.4 工作模式四

B.4.1 GCM 加密认证模式

GCM 的加密认证模式如图 B.4 所示。

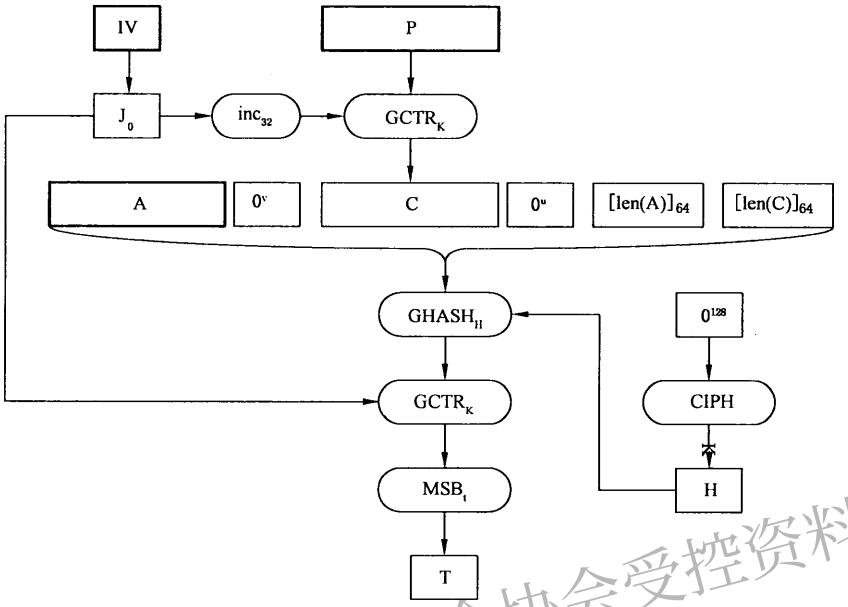


图 B.4 GCM 加密认证模式

GCM 加密认证模式中，输入为：

——明文 P，且 $len(P) \leqslant 2^{39}-256$，其中 len(X)表示比特流 X 的长度；

——初始化向量 IV，且 $1 \leqslant len(A) \leqslant 2^{64}-1$；

——附加认证数据 A，且 $len(A) \leqslant 2^{64}-1$；

——密钥 K，长度为 128 位。

GCM 加密认证模式中，输出为：

——消息鉴别码 T，其中 t 为消息鉴别码 T 的长度；

——密文 C，密文 C 的长度和明文 P 的长度一样。

GCM 模式中的函数如下定义：

a) $X \cdot Y$ 表示 $GF(2^{128})$ 域上的乘法。

b) $MSB_s(X)$表示比特流 X 最左边的 s 位。

c) $LSB_s(X)$表示比特流 X 最右边的 s 位。

d) $inc_s(X)=MSB_{len(X)-s}(X) \| [int(LSB_s(X))+1 \bmod 2^s]_s$，这里 inc_s 是一个增加函数，表示左边 len(X)-s 位不变，右边的 s 位增加 1 后 $\bmod 2^s$。

e) $CIPH_K(X)=E(K,X)$即用密钥 K 对块 X 进行加密后的结果。

f) $GHASH_H(X)$是一个泛哈希函数，其中 $len(X)=128m$，m 为一个正整数；

步骤：

1) $X=X_1 \| X_2 \| \cdots \| X_{m-1} \| X_m$；

2) $Y_0=0^{128}$，其中 0^s 表示 s 个‘0’组成的比特流；

3) For $i=1,\cdots,m$，$Y_i=(Y_{i-1} \oplus X_i) \cdot H$；

4) $GHASH_H(X)=Y_m$。

g) $GCTR_k(ICB,X)$是一个加密函数。

步骤：

1) 如果 X 是空字符串，则返回一个空字符串作为 Y；

2) $n=\lceil len(X)/128 \rceil$，其中$\lceil X \rceil$，表示不小于 X 的最小整数；

3) $X=X_1 \| X_2 \| \cdots \| X_{n-1} \| X_n^*$，其中 $X_1,\cdots,X_{n-1}$是一个 128 位的完整的块，X_n^*既不是完整的块，也不是空字符串，即 $1 \leqslant len(X) \leqslant 128$。

4) 令 $CB_1=ICB$；

5) For i=2 to n, let $CB_i=inc_{32}(CB_{i-1})$；

6) For i=1 to n-1, let $Y_i=X_i \oplus CIPH_K(CB_i)$；

7) Let $Y_n^*=X_n^* \oplus MAB_{Len(X_n^*)}(CIPH_K(CB_n))$；

8) $Y=Y_1 \| Y_2 \| \cdots \| Y_{n-1} \| Y_n^*$；

9) $GCTR_k(ICB,X)=Y$。

GCM 中常量的定义：

——J_0 的定义为：

如果 $len(IV)=96$，那么 $J_0=IV \| 0^{31} \| 1$；

如果 $len(IV) \neq 96$，那么 $s=128\lceil len(IV)/128 \rceil - len(IV)$ 令 $J_0=GHASH_H(IV \| 0^{s+64} \| [len(IV)]_{64})$。

——$u=128\lceil len(C)/128 \rceil - len(C)$。

——$v=128\lceil len(A)/128 \rceil - len(A)$。

——$H=CIPH_K(0^{128})$。

B.4.2 GCM 解密认证模式

GCM 的解密认证模式如图 B.5 所示。

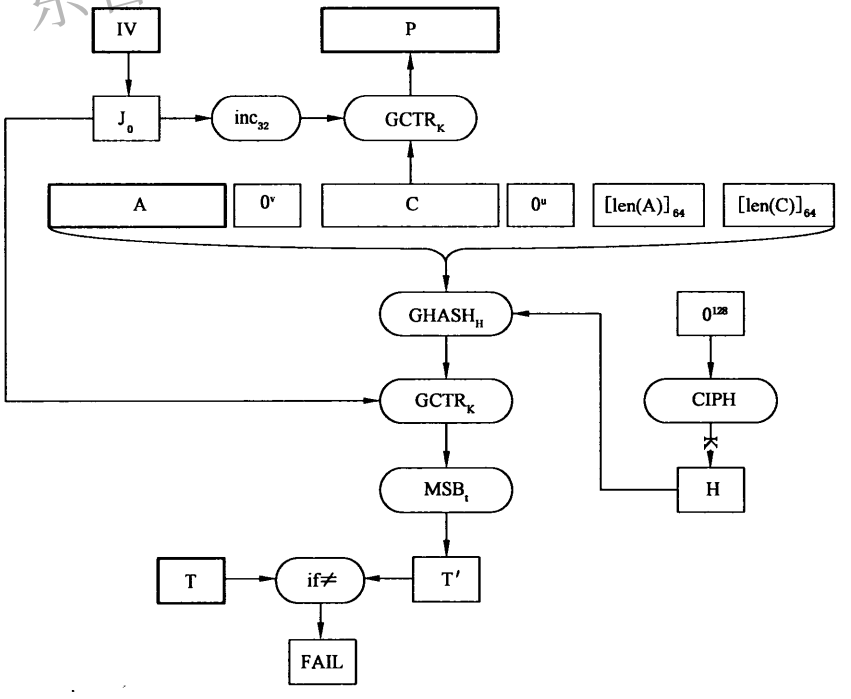


图 B.5 GCM 解密认证模式

GCM 加密认证模式中，输入为：

——密文 P，且 len(P)≤$2^{39}-256$，其中 len(X)表示比特流 X 的长度，密文与输入明文的长度一致；
——初始化向量 IV，且 1≤len(A)≤$2^{64}-1$；
——附加认证数据 A，且 len(A)≤$2^{64}-1$；
——密钥 K，长度为 128 位；
——消息鉴别码 T，长度为 t。

GCM 解密认证模式中，输出为：

解密后输出明文 P 或者当消息鉴别码 T≠T'时输出 FAIL。

参 考 文 献

[1] IEEE Std 802.3—2012 IEEE Standard for Local and Metropolitan Area Networks—Specific Requirements—Part 3:Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications

[2] IEEE Std 802.3ah—2004 IEEE Standard for Local and Metropolitan Area Networks—Specific requirements—Part 3:Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment:Media Access Control Parameters, Physical Layers,and Management Parameters for Subscriber Access Networks

[3] IEEE Std 802.3av—2009 IEEE Standard for Local and Metropolitan Area Networks—Specific requirements—Part 3:Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment 1:Physical Layer Specifications and Management Parameters for 10 Gb/s Passive Optical Networks

中 华 人 民 共 和 国
国 家 标 准
无线网络访问控制技术规范
GB/T 31491—2015
*
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 2.5 字数 68 千字
2015年5月第一版 2015年5月第一次印刷
*
书号:155066·1-51509 定价 36.00 元

GB/T 31491-2015