ICS 35.110
L 79

中华人民共和国国家标准

GB/T 30269.808—2018

信息技术　传感器网络　第808部分：测试：低速率无线传感器网络网络层和应用支持子层安全

Information technology—Sensor network—Part 808：Testing：Network layer and application support sublayer security for low-rate wireless sensor network

2018-12-28 发布　　2019-07-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

中 华 人 民 共 和 国
国 家 标 准
信息技术 传感器网络 第808部分：
测试：低速率无线传感器网络
网络层和应用支持子层安全
GB/T 30269.808—2018
*
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 4.25 字数 126 千字
2018年12月第一版 2018年12月第一次印刷
*
书号：155066·1-61819 定价 57.00 元

目　　次

前　言

GB/T 30269《信息技术　传感器网络》拟分为以下部分：

——第1部分：参考体系结构和通用技术要求；

——第2部分：术语；

——第301部分：通信与信息交换：低速无线传感器网络网络层和应用支持子层规范；

——第302部分：通信与信息交换：高可靠性无线传感器网络媒体访问控制和物理层规范；

——第303部分：通信与信息交换：基于IP的无线传感器网络网络层规范；

——第304部分：通信与信息交换：声波通信系统技术要求；

——第401部分：协同信息处理：支撑协同信息处理的服务及接口；

——第501部分：标识：传感节点标识符编制规则；

——第502部分：标识：传感节点标识符解析；

——第503部分：标识：传感节点标识符注册规程；

——第504部分：标识：传感节点标识符管理规范；

——第601部分：信息安全：通用技术规范；

——第602部分：信息安全：低速率无线传感器网络网络层和应用支持子层安全规范；

——第701部分：传感器接口：信号接口；

——第702部分：传感器接口：数据接口；

——第801部分：测试：通用要求；

——第802部分：测试：低速无线传感器网络媒体访问控制和物理层；

——第803部分：测试：低速无线传感器网络网络层和应用支持子层；

——第804部分：测试：传感器接口；

——第805部分：测试：传感器网关；

——第806部分：测试：传感节点标识符解析；

——第807部分：测试：网络传输安全；

——第808部分：测试：低速率无线传感器网络网络层和应用支持子层安全；

——第809部分：测试：基于IP的无线传感器网络网络层协议；

——第901部分：网关：通用技术要求；

——第902部分：网关：远程管理技术要求；

——第903部分：网关：逻辑接口；

——第1001部分：中间件：传感器网络节点接口。

本部分为GB/T 30269的第808部分。

本部分按照GB/T 1.1—2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本部分主要起草单位：中国信息安全认证中心、山东省标准化研究院、中国电子技术标准化研究院、无锡物联网产业研究院、山东省计算中心(国家超级计算济南中心)、重庆邮电大学、中国传媒大学。

本部分主要起草人：甘杰夫、公伟、王曙光、王庆升、陈书义、苏静茹、寇春晓、邢涛、李昭、郑潇潇、汪付强、吴晓明、谢昊飞、李红胜、刘剑波、田佳音、杨成。

引　言

GB/T 30269 的本部分针对 GB/T 30269.602—2017《信息技术　传感器网络　第 602 部分：信息安全：低速率无线传感器网络网络层和应用支持子层安全规范》描述了低速率无线传感器网络网络层和应用支持子层安全的测试例。鉴于某一测试例可能涉及若干协议要求，某一协议要求可能对应若干测试例，因此本部分描述的测试例未与 GB/T 30269.602—2017 的条款一一对照。

信息技术　传感器网络　第808部分：测试：低速率无线传感器网络网络层和应用支持子层安全

1　范围

GB/T 30269的本部分针对GB/T 30269.602—2017规定了低速率无线传感器网络网络层和应用支持子层安全的测试例。

本部分适用于声称符合GB/T 30269.602—2017的产品一致性测试和针对特定产品的特定测试例设计。

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 17178.1—1997　信息技术　开放系统互连　一致性测试方法和框架　第1部分：基本概念

GB/T 30269.301—2014　信息技术　传感器网络　第301部分：通信与信息交换：低速无线传感器网络网络层和应用支持子层规范

GB/T 30269.601—2016　信息技术　传感器网络　第601部分：信息安全：通用技术规范

GB/T 30269.602—2017　信息技术　传感器网络　第602部分：信息安全：低速率无线传感器网络网络层和应用支持子层传输安全规范

GB/T 30269.801—2017　信息技术　传感器网络　第801部分：测试：通用要求

3　术语和定义

GB/T 17178.1—1997、GB/T 30269.301—2014、GB/T 30269.601—2016界定的以及下列术语和定义适用于本文件。

3.1

被测设备　device under test；DUT

被测实现所位于的设备。

[GB/T 30269.803—2017，定义3.4]

3.2

密钥材料　keying material

确立和维持密码密钥关系所必需的数据。

3.3

共享密钥　shared key

两个或多个节点之间在初始密钥材料的基础上建立的长期共同使用的密钥。

3.4

会话密钥　session key

为保证一对节点之间的保密通信或消息鉴别而随机产生的密钥。

3.5

密钥更新　key update

一种机制，通过给同一个组提供另外一个密钥，在两个或多个设备之间实施共享密钥的更换。

3.6

密钥建立　key establishment

为一个或多个实体产生一个可用的、共享的密钥的过程。

3.7

直接密钥　direct key

邻居节点之间建立的共享的对密钥。

3.8

路径密钥　path key

在没有直接密钥的情况下，在存在多跳安全的节点之间建立的共享的对密钥。

3.9

信任中心　Trust Center

被网络内设备信任的设备，为网络和端到端应用配置进行密钥管理或安全数据融合等安全操作。

3.10

网络协调器　network coordinator

负责网络构建的首要网络控制设备。

3.11

路由器　router

传感器网络中，一种提供设备之间选路消息，并支持关联的全功能设备。

注：路由器虽不是协调器，但在其操作范围内可完成协调器承担的工作。

4　缩略语

下列缩略语适用于本文件。

ACFS：应用支持子层安全命令帧(application support sublayer command frame of security)

ADFS：应用支持子层安全数据帧(application support sublayer data frame of security)

AFS：应用支持子层安全功能(application support sublayer function of security)

APS：应用支持子层(application support sublayer)

APSME：应用支持子层管理实体(application support sublayer management entity)

DUT：被测设备(device under test)

FDT：功能设备类型(function device type)

MAC 媒体访问控制(medium access control)

NCFS：网络层安全命令帧(network layer command frame of security)

NDFS：网络层安全数据帧(network layer data frame of security)

NIB：网络层信息库(network layer information base)

NLDE：网络层数据实体(network layer data entity)

NLME：网络层管理实体(network layer management entity)

NLFS：网络层安全功能(network layer function of security)

NWK：网络层(network layer)

OSI：开放系统互联(open system interconnect)

PAN：个域网(personal area network)

PICS:协议实现一致性声明(protocol implementation conformance statement)
rSC:参考的传感器网络协调器(reference sensor network coordinator)
rSED:参考的传感器网络终端设备(reference sensor network end device)
rSR:参考的传感器网络路由器(reference sensor network router)
rSTC:参考的传感器网络信任中心(reference sensor network trust center)
SC 传感器网络协调器 (sensor network coordinator)
SED 传感器网络终端设备 (sensor network end device)
SR 传感器网络路由器(sensor network router)
STC:传感器网络信任中心(sensor network trust center)

5 总体描述

本部分使用拓扑图的形式描述测试例的设备角色和无线通信关系,如图 1 所示。图中包括 DUT(可能是 SC、SR、SED 或 STC)和已证明符合 GB/T 30269.602—2017 的设备(在前述设备标识前加 r 表示)。

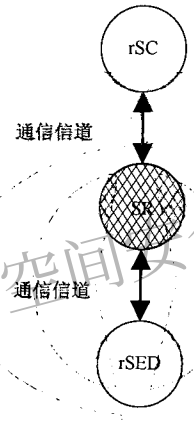


图 1 拓扑图

本部分包括 NWK 安全测试和 APS 安全测试两部分,如表 1 所示。NWK 安全测试规定了发起路由安全过程等测试内容。APS 安全测试规定了信任中心配置分发初始化密钥材料到终端设备、信任中心配置分发初始化值到终端设备、手持设备分发初始化密钥材料到终端设备、手持设备分发初始化值到终端设备、基于随机密钥池的方法建立直接密钥、基于多项式池的方法建立直接密钥、基于同一簇内路径密钥建立的方法建立路径密钥、基于不同簇内路径密钥建立的方法建立路径密钥、更新初始化密钥材料、更新初始化值、更新共享密钥、更新会话密钥、撤销密钥、在网关处对数据资源采用自主访问方法启动访问控制过程、在网关处对节点资源采用自主访问方法启动访问控制过程、在网关处对数据资源采用强制访问方法启动访问控制过程、在网关处对节点资源采用强制访问方法启动访问控制过程、在节点处对节点资源采用强制访问方法启动访问控制过程、基于异或算法的身份鉴别、基于哈希运算的身份鉴别、基于分组密码算法的身份鉴别、基于非对称密码算法的身份鉴别、启动广播消息鉴别、启动安全数据融合服务、安全数据融合撤销等测试内容。

第 6 章和第 7 章关于测试例的描述按照 GB/T 30269.801—2017 中 6.3 的要求,附录 A 中给出的实现一致性声明符合 GB/T 30269.801—2017 中第 7 章的要求。

附录 A 给出了 GB/T 30269.602—2017 中实现的一致性声明,测试方应根据被测厂商所填写的附录 A 中的声明项来选取本部分的测试例。

本部分根据附录 A 协议实现一致性声明 PICS 表给出对应的测试例。

表 1 中测试例是通用的，作用是指导测试方对符合 GB/T 30269.602—2017 的产品开展一致性测试，测试方可根据需要对测试例进行裁剪。

表 1 中“测试例类别”是对 NWK 和 APS 安全测试进行分类。“测试例编号”按照 TC_无线传感器网络层次_SEXY 形式进行，其中 TC 是 Test Case 测试例的缩写，无线传感器网络层次是 NWK 或 APS，SE 是 Security 是安全取前两个字母，XY 表示序号，X、Y 取值范围均为 0～9。“测试例名”是针对对应编号测试例给予的名称。“描述测试例的条款”是给出对应编号测试例给出具体测试环境配置、测试过程和测试判决的条款。在测试判决中，如无特殊说明，只要失败判决中任意一项发生，则该测试例不通过。

示例：TC_APS_SE05，是 APS 的 05 号安全测试例，测试例名是“基于随机密钥池的方法建立直接密钥”，对应测试例的条款是 7.5。

表 1 NWK 安全与 APS 安全的一致性测试例列表

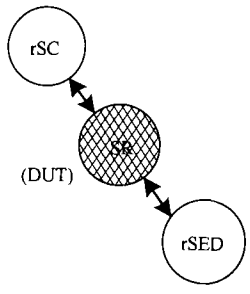
测试例类别	测试例编号	测试例名	描述测试例的条款
NWK 安全	TC_NWK_SE01	发起路由安全过程	第 6 章
APS 安全	TC_APS_SE01	信任中心配置分发初始化密钥材料到终端设备	7.1
	TC_APS_SE02	信任中心配置分发初始化值到终端设备	7.2
	TC_APS_SE03	手持设备分发初始化密钥材料到终端设备	7.3
	TC_APS_SE04	手持设备分发初始化值到终端设备	7.4
	TC_APS_SE05	基于随机密钥池的方法建立直接密钥	7.5
	TC_APS_SE06	基于多项式池的方法建立直接密钥	7.6
	TC_APS_SE07	基于同一簇内路径密钥建立的方法建立路径密钥	7.7
	TC_APS_SE08	基于不同簇内路径密钥建立的方法建立路径密钥	7.8
	TC_APS_SE09	更新初始化密钥材料	7.9
	TC_APS_SE10	更新初始化值	7.10
	TC_APS_SE11	更新共享密钥	7.11
	TC_APS_SE12	更新会话密钥	7.12
	TC_APS_SE13	撤销密钥	7.13
	TC_APS_SE14	在网关处对数据资源采用自主访问方法启动访问控制过程	7.14
	TC_APS_SE15	在网关处对节点资源采用自主访问方法启动访问控制过程	7.15
	TC_APS_SE16	在网关处对数据资源采用强制访问方法启动访问控制过程	7.16
	TC_APS_SE17	在网关处对节点资源采用强制访问方法启动访问控制过程	7.17
	TC_APS_SE18	在节点处对节点资源采用强制访问方法启动访问控制过程	7.18
	TC_APS_SE19	基于异或算法的身份鉴别	7.19
	TC_APS_SE20	基于哈希运算的身份鉴别	7.20
	TC_APS_SE21	基于分组密码算法的身份鉴别	7.21
	TC_APS_SE22	基于非对称密码算法的身份鉴别	7.22
	TC_APS_SE23	启动广播消息鉴别	7.23
	TC_APS_SE24	启动安全数据融合服务	7.24
	TC_APS_SE25	安全数据融合撤销	7.25

6 NWK 安全测试

6.1 环境配置

DUT SR 分别与 rSC 和 rSED 之间建立通信关系。网络层信息库 NIB 中 nwkSecureAllFrames 应为 TURE。TC_NWK_SE01 的环境配置如表 2 所示。

表 2 TC_NWK_SE01 的环境配置

测试拓扑结构	设备	配置
	SR (DUT)	PANID = 0x1AAA Logical Address 随机生成，有效范围：0x0001～0xFFF7 MAC address = 0x00 00 00 01 00 00 00 00
	rSED	PANID = 0x1AAA Logical Address 随机生成，有效范围：0x0001～0xFFF7 MAC address = 0xBB BB BB BB BB BB BB BB
	rSC	PANID = 0x1AAA Logical Address=0x0000 MAC address = 0xAAAAAAAAAAAA AAAAAA

6.2 测试过程

TC_NWK_SE01 的测试过程如表 3 所示。

表 3 TC_NWK_SE01 的测试过程

步骤	描述	说明
0a[a]	所有设备复位	—
0b	rSC 建立 PAN，DUT SR 加入 PAN，rSED 通过 DUT SR 加入 PAN	—

1	rSED 邻近高层发送 NLME-SEC-ROUTE.request
	{
	Request Device Address=rSED 的地址
	Request Identifier Type=0x00 或 0x01
	}
		本步骤的通过判决见 6.3 a)中 1)、2)

2	rSED 发送标识符请求命令	本步骤的通过判决见 6.3 a)中 3)

3	rSED 对 DUT SR 进行鉴别，并向邻近高层发送 NLME-SEC-ROUTE.confirm
	{
	Status=SUCCESS
	}
		本步骤的通过判决见 6.3 a)中 4)

4	DUT SR 向邻近高层发送 NLME-SEC-ROUTE.indication
	{
	Request Device Address=DUT SR 的地址
	Request Identifier Type=0x00 或 0x01
	}
		本步骤的通过判决见 6.3 a)中 5)

表 3（续）

步骤	描述	说明

5	DUT SR 邻近高层发送 NLME-SEC-ROUTE.request
	{
	Request Device Address=DUT SR 的地址
	Request Identifier Type=0x00 或 0x01
	}
		本步骤的通过判决见 6.3 a)中 6)、7)

6	DUT SR 发送标识符响应命令到 rSED	本步骤的通过判决见 6.3 a)中 8)

7	DUT SR 对 rSED 进行鉴别，并向邻近高层发送 NLME-SEC-ROUTE.confirm
	{
	Status=SUCCESS
	}
		本步骤的通过判决见 6.3 a)中 9)

[a] GB/T 30269 的本部分中测试例的步骤 0x(x=a,b,c…)表示测试的准备阶段。		

6.3 测试判决

本测试例通过与否的判决条件如下：

a) 通过判决：

1) rSED 能够向 DUT SR 发送安全路由请求命令；
2) rSED 发出的 NWK 数据中，NWK 帧中存在辅助帧头和信息完整性校验码；
3) rSED 发出的 NWK 数据中，NWK 帧负载字段中命令标识符为 0x0f(设备标识符请求命令帧)；
4) rSED 能够对 DUT SR 成功鉴别；
5) DUT SR 能够收到标识符请求命令；
6) DUT SR 能够向 DUT SR 发送安全路由响应命令；
7) DUT SR 发出的 NWK 数据中，NWK 帧中存在辅助帧头和信息完整性校验码；
8) rSED 接收的 NWK 数据中，NWK 帧负载字段中命令标识符为 0x10(设备标识符响应命令帧)；
9) DUT SR 能够对 rSED 成功鉴别。

b) 失败判决：

1) rSED 不能向 DUT SR 发送安全路由请求命令；
2) rSED 发出的 NWK 数据中，NWK 帧中不存在辅助帧头和信息完整性校验码；
3) rSED 发出的 NWK 数据中，NWK 帧负载字段中命令标识符不为 0x0f(设备标识符请求命令帧)；
4) rSED 不能对 DUT SR 成功鉴别；
5) DUT SR 不能收到标识符请求命令；
6) DUT SR 不能向 DUT SR 发送安全路由响应命令
7) DUT SR 发出的 NWK 数据中，NWK 帧中不存在辅助帧头和信息完整性校验码；
8) rSED 接收的 NWK 数据中，NWK 帧负载字段中命令标识符不为 0x10(设备标识符响应命令帧)；
9) DUT SR 不能对 rSED 成功鉴别。

6.4 说明

本测试例覆盖附录 A 中的部分声明项，如表 4 所示。

表 4 TC_NWK_SE01 的 PICS 声明项

PICS 声明项	描述
NLFS1	NWK 是否支持邻近高层发起路由安全过程
NDFS1	设备是否支持生成安全的 NWK 数据帧，即增加了辅助帧头和信息完整性校验码的 NWK 数据帧
NCFS1	设备是否支持接收设备标识符请求命令帧
NCFS2	设备是否支持生成设备标识符响应命令帧

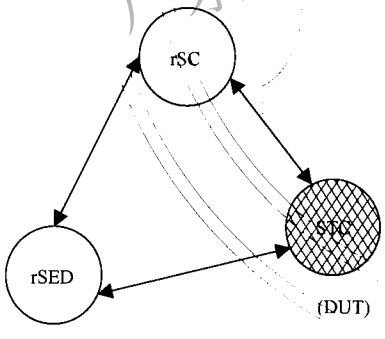
7 APS 安全测试

7.1 TC_APS_SE01 信任中心配置分发初始化密钥材料到终端设备

7.1.1 环境配置

TC_APS_SE01 的环境配置如表 5 所示。

表 5 TC_APS_SE01 的环境配置

测试拓扑结构	设备	配置
	STC (DUT)	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xAA AA AA AA AA AA AA AA
	rSED	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0x00 00 00 01 00 00 00 00
	rSC	PANID=0x1BBB Logical Address=0x0000 MAC address =0xBB BB BB BB BB BB BB BB

7.1.2 测试过程

TC_APS_SE01 测试过程如表 6 所示。

表 6 TC_APS_SE01 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN，rSED 加入 PAN，DUT STC 加入 PAN	—

表 6（续）

步骤	描述	说明

1	DUT STC 邻近高层发送 APSME-DISTRIBUTE-KEY.request
	{
	DistributeType =0x00
	KeyType = 0x00
	NodeID = rSED 的地址
	KeyData = 0xAA BB CC DD
	}
		本步骤的通过判决见 7.1.3 a)中 1)

2	DUT SC APSME 直接分发初始化密钥材料到 rSED	本步骤的通过判决见 7.1.3 a)中 2)

3	rSED 接收初始化密钥材料并向邻近高层发送 APSME-DISTRIBUTE-KEY.indication
	{
	KeyType = 0x00
	NodeID = DUT STC 的地址
	TransportKeyData=0xAA BB CC DD
	}
		本步骤的通过判决见 7.1.3 a)中 3)

7.1.3 测试判决

本测试例通过与否的判决条件如下：

a) 成功判决：

1) DUT STC 能够发送直接分发初始化密钥材料命令；

2) DUT STC APSME 能够直接分发初始化密钥材料到 rSED；

3) 收到初始化密钥材料后，rSED 能够告知邻近高层并更新 AIB 中 Initializationkey、KeyID、Key 等相关属性。

b) 失败判决：

1) DUT STC 不能发送直接分发初始化密钥材料命令；

2) DUT STC APSME 不能直接分发初始化密钥材料到 rSED；

3) 收到初始化密钥材料后，rSED 不能告知邻近高层并更新 AIB 中 Initializationkey、KeyID、Key 等相关属性。

7.1.4 说明

本测试例覆盖附录 A 的部分声明项，如表 7 所示。

表 7 TC_APS_SE01 的 PICS 声明项

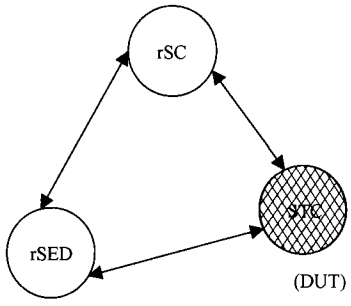
PICS 声明项	描述
AFS1	APS 是否支持使用信任中心分发密钥材料到其他设备

7.2 TC_APS_SE02 信任中心配置分发初始化值到终端设备

7.2.1 环境配置

TC_APS_SE02 的环境配置如表 8 所示。

表 8　TC_APS_SE02 的环境配置

测试拓扑结构	设备	配置
	STC (DUT)	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xAA AA AA AA AA AA AA AA
	rSED	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0x00 00 00 01 00 00 00 00
	rSC	PANID=0x1BBB Logical Address=0x0000 MAC address =0xBB BB BB BB BB BB BB BB

7.2.2　测试过程

TC_APS_SE02 测试过程如表 9 所示。

表 9　TC_APS_SE02 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN，rSED 加入 PAN，DUT STC 加入 PAN	—

1	DUT STC 邻近高层发送 APSME-DISTRIBUTE-KEY.request
	{
	DistributeType =0x00
	KeyType = 0x01
	NodeID = rSED 的地址
	KeyData = 0xAA BB CC DD
	}
		本步骤的通过判决见 7.2.3 a)中 1)

2	DUT SC APSME 直接分发初始化值到 rSED	本步骤的通过判决见 7.2.3 a)中 2)

3	rSED 接收初始化值并向邻近高层发送 APSME-DISTRIBUTE-KEY.indication
	{
	KeyType = 0x01
	NodeID = DUT STC 的地址
	TransportKeyData=0xAA BB CC DD
	}
		本步骤的通过判决见 7.2.3 a)中 3)

7.2.3　测试判决

本测试例通过与否的判决条件如下：

a)　成功判决：

1)　DUT STC 能够发送直接分发初始化值命令；

2)　DUT STC APSME 能够直接分发初始化值到 rSED；

3)　收到初始化值后，rSED 能够告知邻近高层并更新 AIB 表中 Initializationvalue，Key 等相

关属性。

b) 失败判决：

1) DUT STC 不能发送直接分发初始化值命令；

2) DUT STC APSME 不能直接分发初始化值到 rSED；

3) 收到初始化值后，rSED 不能告知邻近高层并更新 AIB 表中 Initializationvalue，Key 等相关属性。

7.2.4 说明

本测试例覆盖附录 A 的部分声明项，如表 10 所示。

表 10 TC_APS_SE02 的 PICS 声明项

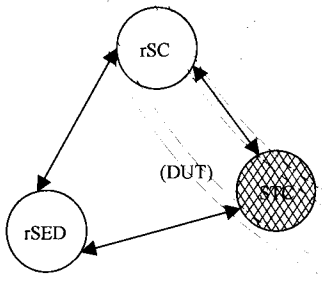
PICS 声明项	描述
APS1	APS 是否支持使用信任中心分发密钥材料到其他设备

7.3 TC_APS_SE03 手持设备分发初始化密钥材料到终端设备

7.3.1 环境配置

TC_APS_SE03 的环境配置如表 11 所示。

表 11 TC_APS_SE03 的环境配置

测试拓扑结构	设备	配置
	STC (DUT)	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xAA AA AA AA AA AA AA AA
	rSED	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0x00 00 00 01 00 00 00 00
	rSC	PANID=0x1BBB Logical Address=0x0000 MAC address =0xBB BB BB BB BB BB BB BB

7.3.2 测试过程

TC_APS_SE03 测试过程如表 12 所示。

表 12 TC_APS_SE03 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN，rSED 加入 PAN，DUT STC 加入 PAN	—

表 12（续）

步骤	描述	说明

1	DUT STC 邻近高层发送 APSME-DISTRIBUTE-KEY.request
	{
	DistributeType =0x01
	KeyType = 0x00
	NodeID = rSED 的地址
	KeyData = 0xAA BB CC DD
	}
		本步骤的通过判决见 7.3.3 a)中 1)

2	DUT SC APSME 通过手持设备分发初始化密钥材料到 rSED	本步骤的通过判决见 7.3.3 a)中 2)

3	rSED 接收初始化密钥材料并向邻近高层发送 APSME-DISTRIBUTE-KEY.indication
	{
	KeyType = 0x01
	NodeID = DUT STC 的地址
	TransportKeyData=0xAA BB CC DD
	}
		本步骤的通过判决见 7.3.3 a)中 3)

7.3.3 测试判决

本测试例通过与否的判决条件如下：

a) 成功判决：

1) DUT STC 能够发送通过手持设备分发初始化密钥材料命令；

2) DUT STC APSME 能够通过手持设备分发初始化密钥材料到 rSED；

3) 收到初始化密钥材料后，rSED 能够告知邻近高层并更新 AIB 中 Initialization key，KeyID，Key 等相关属性。

b) 失败判决：

1) DUT STC 不能发送发送通过手持设备分发初始化密钥材料命令；

2) DUT STC APSME 不能通过手持设备分发初始化密钥材料到 rSED；

3) 收到初始化密钥材料后，rSED 不能告知邻近高层并更新 AIB 中 Initialization key，KeyID，Key 等相关属性。

7.3.4 说明

本测试例覆盖附录 A 的部分声明项，如表 13 所示。

表 13 TC_APS_SE03 的 PICS 声明项

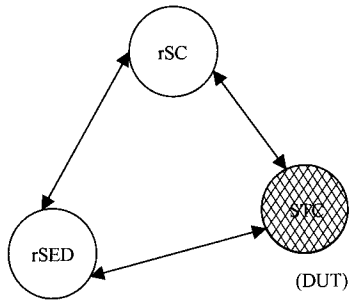
PICS 声明项	描述
AFS1	APS 是否支持使用信任中心分发密钥材料到其他设备

7.4 TC_APS_SE04 手持设备分发初始化值到终端设备

7.4.1 环境配置

TC_APS_SE04 的环境配置如表 14 所示。

表 14　TC_APS_SE04 的环境配置

测试拓扑结构	设备	配置
	STC (DUT)	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xAA AA AA AA AA AA AA AA
	rSED	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0x00 00 00 01 00 00 00 00
	rSC	PANID=0x1BBB Logical Address=0x0000 MAC address =0xBB BB BB BB BB BB BB BB

7.4.2　测试过程

TC_APS_SE04 测试过程如表 15 所示。

表 15　TC_APS_SE04 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN，rSED 加入 PAN，DUT STC 加入 PAN	—

1	DUT STC 邻近高层发送 APSME-DISTRIBUTE-KEY.request
	{
	DistributeType =0x01
	KeyType = 0x01
	NodeID = rSED 的地址
	KeyData = 0xAA BB CC DD
	}
		本步骤的通过判决见 7.4.3 a)中 1)

2	DUT SC APSME 通过手持设备分发初始化值到 rSED	本步骤的通过判决见 7.4.3 a)中 2)

3	rSED 接收初始化值并向邻近高层发送 APSME-DISTRIBUTE-KEY.indication
	{
	KeyType = 0x01
	NodeID = DUT STC 的地址
	TransportKeyData=0xAA BB CC DD
	}
		本步骤的通过判决见 7.4.3 a)中 3)

7.4.3　测试判决

本测试例通过与否的判决条件如下：

a)　成功判决：

1)　DUT STC 能够发送通过手持设备分发初始化值命令；

2)　DUT STC APSME 能够通过手持设备分发初始化值到 rSED；

3)　收到初始化值后，rSED 能够告知邻近高层并更新 AIB 中 Initialization key，KeyID，Key

等相关属性。

b) 失败判决：

1) DUT STC 不能发送通过手持设备分发初始化值命令；

2) DUT STC APSME 不能通过手持设备分发初始化值到 rSED；

3) 收到初始化值后，rSED 不能告知邻近高层并更新 AIB 中 Initialization key，KeyID，Key 等相关属性。

7.4.4 说明

本测试例覆盖附录 A 的部分声明项，如表 16 所示。

表 16 TC_APS_SE04 的 PICS 声明项

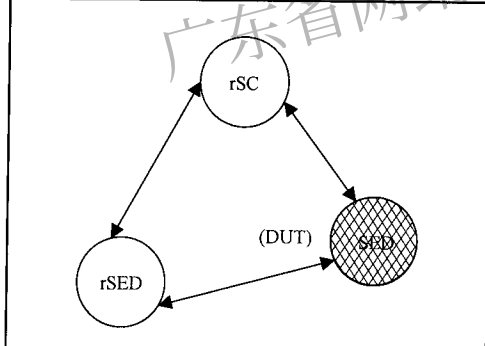
PICS 声明项	描述
AFS1	APS 是否支持使用信任中心分发密钥材料到其他设备

7.5 TC_APS_SE05 基于随机密钥池的方法建立直接密钥

7.5.1 环境配置

TC_APS_SE05 的环境配置如表 17 所示。

表 17 TC_APS_SE05 的环境配置

测试拓扑结构	设备	配置
	SED (DUT)	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xAA AA AA AA AA AA AA AA
	rSED	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0x00 00 00 01 00 00 00 00
	rSC	PANID=0x1BBB Logical Address=0x0000 MAC address =0xBB BB BB BB BB BB BB BB

7.5.2 测试过程

TC_APS_SE05 测试过程如表 18 所示。

表 18 TC_APS_SE05 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN，rSED 加入 PAN，DUT SED 加入 PAN	—

表 18（续）

步骤	描述	说明

1	DUT SED 邻近高层发送 APSME-ESTABLISH-KEY.request
	{
	KeyType = 0x00
	DestAddress = DUT SED 的地址
	ResponderAddress = 0xFFFF(广播地址)
	KeyEstablishmentMethod = 0x00
	KeyData = 0xAA BB CC DD
	}
		本步骤的通过判决见 7.5.3 a)中 1)、2)、3)

2	DUT SED APSME 执行基于密钥池的预分配协议	—

3	rSED 接收密钥建立信息并向邻近高层发送 APSME-ESTABLISH-KEY.indication
	{
	InitiatorAddress=DUT SED 的地址
	KeyEstablishmentMethod = 0x00
	KeyType = 0x00
	KeyData = 0xAA BB CC DD
	}
		本步骤的通过判决见 7.5.3 a)中 4)

4	rSED 邻近高层发送 APSME-ESTABLISH-KEY.Response
	{
	InitiatorAddress=DUT SED 的地址
	Accept=TRUE
	}
		本步骤的通过判决见 7.5.3a)中 5)

5	rSED 选取与自身 Initialization key ID 元素相同的密钥材料建立所需密钥。
	DUT SED 向邻近高层发送 APSME-ESTABLISH-KEY.confirm
	{
	Address=DUT SED 的地址
	Status=SUCCESS
	}
	rSED 向邻近高层发送 APSME-ESTABLISH-KEY.confirm
	{
	Address=DUT SED 的地址
	Status=SUCCESS
	}
		本步骤的通过判决见 7.5.3 a)中 6)

7.5.3 测试判决

本测试例通过与否的判决条件如下：

a） 成功判决：

1） DUT SED 能够向 rSED 发送密钥建立请求命令；

2） DUT SED 发出的 APS 数据中，APS 帧中存在辅助帧头和信息完整性校验码；

3） DUT SED 发出的 APS 数据中，命令标识符为 0x01(密钥建立命令帧)；

4) rSED 能够根据基于密钥池的密钥预分配方法和 DUT SED 地址确定是否与发起者建立密钥连接；
5) rSED 能够对与 DUT SED 建立密钥连接进行响应；
6) rSED 能够与 DUT SED 建立共享密钥。

b) 失败判决：
1) DUT SED 不向 rSED 发送密钥建立请求命令；
2) DUT SED 发出的 APS 数据中，APS 帧中不存在辅助帧头和信息完整性校验码；
3) DUT SED 发出的 APS 数据中，命令标识符不为 0x01(密钥建立命令帧)；
4) rSED 不能根据基于密钥池的密钥预分配方法和 DUT SED 地址确定是否与发起者建立密钥连接；
5) rSED 不能对与 DUT SED 建立密钥连接进行响应；
6) rSED 不能与 DUT SED 建立共享密钥。

7.5.4 说明

本测试例覆盖附录 A 的部分声明项，如表 19 所示。

表 19 TC_NWK_SE05 的 PICS 声明项

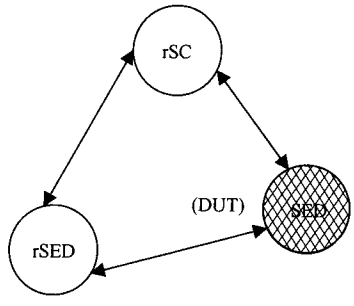
PICS 声明项	描述
AFS2	APS 是否支持两个设备之间手动建立一个共享密钥
ADFS1	APS 是否支持生成安全的 APS 数据帧，即增加了辅助帧头和信息完整性校验码 MIC 的 APS 数据帧
NCFS1	设备是否支持生成密钥建立命令帧

7.6 TC_APS_SE06 基于多项式池的方法建立直接密钥

7.6.1 环境配置

TC_APS_SE06 的环境配置如表 20 所示。

表 20 TC_APS_SE06 的环境配置

测试拓扑结构	设备	配置
	SED (DUT)	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xAA AA AA AA AA AA AA AA
	rSED	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0x00 00 00 01 00 00 00 00
	rSC	PANID=0x1BBB Logical Address=0x0000 MAC address =0xBB BB BB BB BB BB BB BB

7.6.2 测试过程

TC_APS_SE06 测试过程如表 21 所示。

表 21　TC_APS_SE06 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN，rSED 加入 PAN，DUT SED 加入 PAN	—

1	DUT SED 邻近高层发送 APSME-ESTABLISH-KEY.request
	{
	KeyType = 0x00
	DestAddress = DUT SED 的地址
	ResponderAddress = 0xFFFF(广播地址)
	KeyEstablishmentMethod = 0x01
	KeyData = 0xAA BB CC DD
	}
		本步骤的通过判决见 7.6.3 a)中 1)、2)、3)

2	DUT SED APSME 执行基于多项式池预分配协议	

3	rSED 接收密钥建立信息并向邻近高层发送 APSME-ESTABLISH-KEY.indication
	{
	InitiatorAddress= DUT SED 的地址
	KeyEstablishmentMethod = 0x00
	KeyType = 0x00
	KeyData = 0xAA BB CC DD
	}
		本步骤的通过判决见 7.6.3 a)中 4)

4	rSED 邻近高层发送 APSME-ESTABLISH-KEY.Response
	{
	InitiatorAddress=DUT SED 的地址
	Accept=TRUE
	}
		本步骤的通过判决见 7.6.3 a)中 5)

5	rSED 选取与自身 Polynomial ID 元素相等的密钥材料建立所需密钥。
	DUT SED 向邻近高层发送
	APSME-ESTABLISH-KEY.confirm
	{
	Address=DUT SED 的地址
	Status=SUCCESS
	}
	rSED 向邻近高层发送 APSME-ESTABLISH-KEY.confirm
	{
	Address=DUT SED 的地址
	Status=SUCCESS
	}
		本步骤的通过判决见 7.6.3 a)中 6)

7.6.3　测试判决

本测试例通过与否的判决条件如下：

a)　成功判决：

1) DUT SED 能够向 rSED 发送密钥建立请求命令；
2) DUT SED 发出的 APS 数据中，APS 帧中存在辅助帧头和信息完整性校验码；
3) DUT SED 发出的 APS 数据中，命令标识符为 0x01(密钥建立命令帧)；
4) rSED 能够根据基于多项式池的方法和 DUT SED 地址确定是否与发起者建立密钥连接；
5) rSED 能够对与 DUT SED 建立密钥连接进行响应；
6) rSED 能够与 DUT SED 建立共享密钥。

b) 失败判决：
1) DUT SED 不向 rSED 发送密钥建立请求命令；
2) DUT SED 发出的 APS 数据中，APS 帧中不存在辅助帧头和信息完整性校验码；
3) DUT SED 发出的 APS 数据中，命令标识符不为 0x01(密钥建立命令帧)；
4) rSED 不能根据基于多项式池的方法和 DUT SED 地址确定是否与发起者建立密钥连接；
5) rSED 不能对与 DUT SED 建立密钥连接进行响应；
6) rSED 不能与 DUT SED 建立共享密钥。

7.6.4 说明

本测试例覆盖附录 A 的部分声明项，如表 22 所示。

表 22 TC_NWK_SE06 的 PICS 声明项

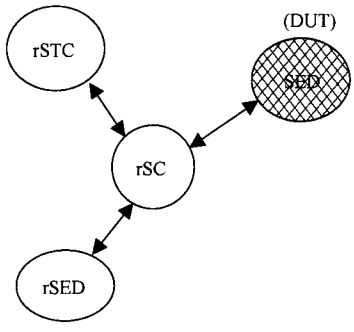
PICS 声明项	描述
AFS2	APS 是否支持两个设备之间手动建立一个共享密钥
ADFS1	APS 是否支持生成安全的 APS 数据帧，即增加了辅助帧头和信息完整性校验码 MIC 的 APS 数据帧
NCFS1	设备是否支持生成密钥建立命令帧

7.7 TC_APS_SE07 基于同一簇内路径密钥建立的方法建立路径密钥

7.7.1 环境配置

TC_APS_SE07 的环境配置如表 23 所示。

表 23 TC_APS_SE07 的环境配置

测试拓扑结构	设备	配置
	SED (DUT)	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xAA AA AA AA AA AA AA AA
	rSED (DUT)	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xCCCCCCCCCCCCCC CC
	rSTC	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0x00 00 00 01 00 00 00 00
	rSC	PANID=0x1BBB Logical Address=0x0000 MAC address =0xBB BB BB BB BB BB BB BB

7.7.2 测试过程

TC_APS_SE07 测试过程如表 24 所示。

表 24 TC_APS_SE07 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN，rSTC 加入 PAN，DUT SED1 和 rSED2 加入 PAN	—

1	DUT SED 的邻近高层发送 APSME-ESTABLISH-KEY.request
	{
	KeyType = 0x00
	DestAddress = DUT SED 的地址
	ResponderAddress = rSED 的地址
	KeyEstablishmentMethod = 0x02
	KeyData = 0xAA BB CC DD
	}
		本步骤的通过判决见 7.7.3 a)中 1)、2)、3)

2	rSTC 接收密钥建立信息并向邻近高层发送 APSME-ESTABLISH-KEY.indication
	{
	InitiatorAddress=rSTC 地址
	KeyEstablishmentMethod = 0x02
	KeyType = 0x00
	KeyData = 0xAA BB CC DD
	}
		本步骤的通过判决见 7.7.3 a)中 4)

3	rSTC 邻近高层发送 APSME-ESTABLISH-KEY.request
	{
	KeyType = 0x00
	DestAddress = rSTC 的地址
	ResponderAddress = rSED 的地址
	KeyEstablishmentMethod = 0x02
	KeyData = 0xAA BB CC DD
	}
		本步骤的通过判决见 7.7.3 a)中 5)

4	rSED 接收密钥建立信息并向邻近高层发送 APSME-ESTABLISH-KEY.indication
	{
	InitiatorAddress= DUT SED 的地址
	KeyEstablishmentMethod = 0x02
	KeyType = 0x00
	KeyData = 0xAA BB CC DD
	}
		本步骤的通过判决见 7.7.3 a)中 6)

5	rSED 邻近高层发送 APSME-ESTABLISH-KEY.Response
	{
	InitiatorAddress=DUT SED 的地址
	Accept=TRUE
	}
		本步骤的通过判决见 7.7.3 a)中 7)

表 24（续）

步骤	描述	说明

6	rSED 建立基于信任中心路径密钥。
	DUT SED 向邻近高层发送 APSME-ESTABLISH-KEY.confirm
	{
	Address＝DUT SED 的地址
	Status＝SUCCESS
	}
	rSED 向邻近高层发送 APSME-ESTABLISH-KEY.confirm
	{
	Address＝DUT SED 的地址
	Status＝SUCCESS
	}
		本步骤的通过判决见 7.7.3 a)中 8)

7.7.3 测试判决

本测试例通过与否的判决条件如下：

a） 成功判决：

1） DUT SED 能够发送密钥建立请求命令；
2） DUT SED 发出的 APS 数据中，APS 帧中存在辅助帧头和信息完整性校验码；
3） DUT SED 发出的 APS 数据中，命令标识符为 0x01(密钥建立命令帧)；
4） rSTC 能够为 DUT SED 生成密钥信息及其相应的标识符；
5） rSTC 能够为 rSED 发送密钥；
6） rSED 能够根据基于同一簇内路径密钥建立的方法和通过信任中心与 DUT SED 地址确定是否与发起者建立密钥连接；
7） rSED 能够对与 DUT SED 建立密钥连接进行响应；
8） rSED 能够与 DUT SED 通过信任中心建立路径密钥。

b） 失败判决：

1） DUT SED 不向 rSED 发送密钥建立请求命令；
2） DUT SED 发出的 APS 数据中，APS 帧中不存在辅助帧头和信息完整性校验码；
3） DUT SED 发出的 APS 数据中，命令标识符不为 0x01(密钥建立命令帧)；
4） rSTC 不能为 DUT SED 生成密钥信息及其相应的标识符；
5） rSTC 不能为 rSED 发送密钥；
6） rSED 不能根据基于同一簇内路径密钥建立的方法通过信任中心与 DUT SED 地址确定是否与发起者建立密钥连接；
7） rSED 不能对与 DUT SED 建立密钥连接进行响应；
8） rSED 不能与 DUT SED 通过信任中心建立路径密钥。

7.7.4 说明

本测试例覆盖附录 A 的部分声明项，如表 25 所示。

表 25 TC_NWK_SE07 的 PICS 声明项

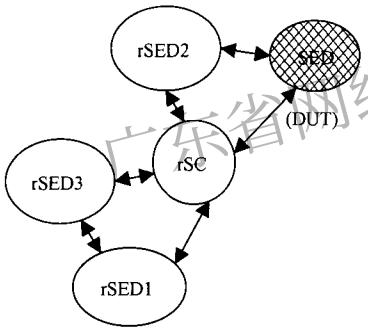
PICS 声明项	描述
AFS2	APS 是否支持两个设备之间手动建立一个共享密钥
ADFS1	APS 是否支持生成安全的 APS 数据帧，即增加了辅助帧头和信息完整性校验码 MIC 的 APS 数据帧
NCFS1	设备是否支持生成密钥建立命令帧

7.8 TC_APS_SE08 基于不同簇内路径密钥建立的方法建立路径密钥

7.8.1 环境配置

rSED2、rSED3 分别为可信节点。TC_APS_SE08 的环境配置如表 26 所示。

表 26 TC_APS_SE08 的环境配置

测试拓扑结构	设备	配置
	SED (DUT)	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xAA AA AA AA AA AA AA AA
	rSED1	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xCC CC CC CC CC CC CC CC
	rSED2	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0x00 00 00 01 00 00 00 00
	rSED3	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0x00 00 00 02 00 00 00 00
	rSC	PANID=0x1BBB Logical Address=0x0000 MAC address =0xBB BB BB BB BB BB BB BB

7.8.2 测试过程

TC_APS_SE08 测试过程如表 27 所示。

表 27 TC_APS_SE08 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN，rSR 加入 PAN，rSED1，DUT SED 和 rSED2 通过 rSR 加入 PAN	—

表 27（续）

步骤	描述	说明

1	DUT SED 的邻近高层发送 APSME-ESTABLISH-KEY.request
	{
	KeyType = 0x00
	DestAddress = DUT SED 的地址
	ResponderAddress = rSED1 的地址
	KeyEstablishmentMethod = 0x03
	KeyData = 0xAA BB CC DD
	}
		本步骤的通过判决见 7.8.3 a)中 1)、2)、3)

2	rSED2 接收密钥建立信息并向邻近高层发送 APSME-ESTABLISH-KEY.indication
	{
	InitiatorAddress=rSED2 地址
	KeyEstablishmentMethod = 0x03
	KeyType = 0x00
	KeyData = 0xAA BB CC DD
	}
		本步骤的通过判决见 7.8.3 a)中 4)

3	rSED2 邻近高层发送 APSME-ESTABLISH-KEY.request
	{
	KeyType = 0x00
	DestAddress = rSED2 的地址
	ResponderAddress = rSED3 的地址
	KeyEstablishmentMethod = 0x03
	KeyData = 0xAA BB CC DD
	}
		本步骤的通过判决见 7.8.3 a)中 5)

4	rSED3 邻近高层发送 APSME-ESTABLISH-KEY.request
	{
	KeyType = 0x00
	DestAddress = rSED3 的地址
	ResponderAddress = rSED1 的地址
	KeyEstablishmentMethod = 0x03
	KeyData = 0xAA BB CC DD
	}
		本步骤的通过判决见 7.8.3 a)中 6)

5	rSED 接收密钥建立信息并向邻近高层发送 APSME-ESTABLISH-KEY.indication
	{
	InitiatorAddress= DUT SED 的地址
	KeyEstablishmentMethod = 0x03
	KeyType = 0x00
	KeyData = 0xAA BB CC DD
	}
		本步骤的通过判决见 7.8.3 a)中 7)

表 27（续）

步骤	描述	说明

6	rSED 邻近高层发送 APSME-ESTABLISH-KEY.Response
	{
	InitiatorAddress=DUT SED 的地址
	Accept=TRUE
	}
		本步骤的通过判决见 7.8.3 a)中 8)

7	rSED 建立基于信任节点路径密钥。
	DUT SED 向邻近高层发送 APSME-ESTABLISH-KEY.confirm
	{
	Address=DUT SED 的地址
	Status=SUCCESS
	}
	rSED1 向邻近高层发送 APSME-ESTABLISH-KEY.confirm
	{
	Address=DUT SED 的地址
	Status=SUCCESS
	}
		本步骤的通过判决见 7.8.3 a)中 9)

7.8.3 测试判决

本测试例通过与否的判决条件如下：

a) 成功判决：

1) DUT SED 能够向 rSED1 发送密钥建立请求命令；
2) DUT SED 发出的 APS 数据中，APS 帧中存在辅助帧头和信息完整性校验码；
3) DUT SED 发出的 APS 数据中，命令标识符为 0x01(密钥建立命令帧)；
4) rSED2 能够与 rSED3 进行密钥的协商；
5) rSED2 能够向 rSED3 发送密钥；
6) rSED3 能够向 rSED1 发送密钥；
7) rSED1 能够根据基于不同簇内路径密钥建立的方法(通过 rSED2)和 DUT SED 地址确定是否与发起者建立密钥连接；
8) rSED1 能够对与 DUT SED 建立密钥连接进行响应；
9) rSED1 能够与 DUT SED 通过可信节点建立路径密钥。

b) 失败判决：

1) DUT SED 不向 rSED1 发送密钥建立请求命令；
2) DUT SED 发出的 APS 数据中，APS 帧中不存在辅助帧头和信息完整性校验码；
3) DUT SED 发出的 APS 数据中，命令标识符不为 0x01(密钥建立命令帧)；
4) rSED2 不能与 rSED3 进行密钥的协商；
5) rSED2 不能向 rSED3 发送密钥；
6) rSED3 不能向 rSED1 发送密钥；
7) rSED1 不能根据基于不同簇内路径密钥建立的方法(通过 rSED2)和 DUT SED 地址确定是否与发起者建立密钥连接；
8) rSED1 不能对与 DUT SED 建立密钥连接进行响应；

9） rSED1 不能与 DUT SED 通过可信节点建立路径密钥。

7.8.4 说明

本测试例覆盖附录 A 的部分声明项，如表 28 所示。

表 28 TC_NWK_SE08 的 PICS 声明项

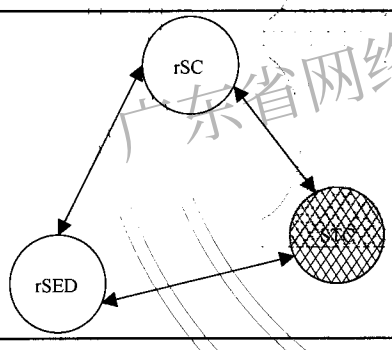
PICS 声明项	描述
AFS2	APS 是否支持两个设备之间手动建立一个共享密钥
ADFS1	APS 是否支持生成安全的 APS 数据帧，即增加了辅助帧头和信息完整性校验码 MIC 的 APS 数据帧
NCFS1	设备是否支持生成密钥建立命令帧

7.9 TC_APS_SE09 更新初始化密钥材料

7.9.1 环境配置

TC_APS_SE09 的环境配置如表 29 所示。

表 29 TC_APS_SE09 的环境配置

测试拓扑结构	设备	配置
	STC（DUT）	PANID =0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xAA AA AA AA AA AA AA AA
	rSED	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xDDDDDDDDDDDDDDDD
	rSC	PANID=0x1BBB Logical Address=0x0000 MAC address =0xBB BB BB BB BB BB BB BB

7.9.2 测试过程

TC_APS_SE09 测试过程如表 30 所示。

表 30 TC_APS_SE09 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN，rSED 加入 PAN，DUT STC 加入 PAN	—

1	DUT STC 邻近高层发送 APSME-UPDATE-KEY.request
	{
	DestAddress =rSED 的地址
	KeyType = 0x00
	KeyData =0xAA BB CC DD
	}
		本步骤的通过判决见 7.9.3 a)中 1)、2)、3)

表 30（续）

步骤	描述	说明

2	rSED 向邻近高层发送 APSME-UPDATE-KEY.indication
	{
	DestAddress ＝rSED 的地址
	KeyType ＝ 0x00
	KeyData ＝0xAA BB CC DD
	}
		本步骤的通过判决见 7.9.3 a)中 4)

3	rSED 更新密钥为 KeyData，Initialization key 和 Initialization key ID 元素设置为 KeyData 参数中的初始化密钥材料及其相应的标识符	本步骤的通过判决见 7.9.3 a)中 5)

7.9.3 测试判决

本测试例通过与否的判决条件如下：

a） 成功判决：

1） DUT STC 能够向 rSED 发送密钥更新请求命令；

2） DUT STC 发出的 APS 数据中，APS 帧中存在辅助帧头和信息完整性校验码；

3） DUT STC 发出的 APS 数据中，命令标识符为 0x02(密钥更新命令帧)；

4） rSED 能够收到密钥更新命令帧；

5） rSED 能够更新密钥为 keyData。

b） 失败判决：

1） DUT STC 不能向 rSED 发送密钥更新请求命令；

2） DUT STC 发出的 APS 数据中，APS 帧中不存在辅助帧头和信息完整性校验码；

3） DUT STC 发出的 APS 数据中，命令标识符不为 0x02(密钥更新命令帧)；

4） rSED 不能收到密钥更新命令帧；

5） rSED 不能更新密钥为 0xAA 0xBB 0xCC 0xDD。

7.9.4 说明

本测试例覆盖附录 A 的部分声明项，如表 31 所示。

表 31 TC_NWK_SE09 的 PICS 声明项

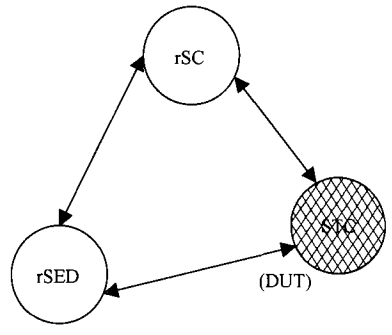
PICS 声明项	描述
AFS4	APS 是否支持使用信任中心去通知其他设备更换到一个新的密钥
ADFS1	APS 是否支持生成安全的 APS 数据帧，即增加了辅助帧头和信息完整性校验码 MIC 的 APS 数据帧
NCFS2	设备是否支持接收密钥更新命令帧

7.10 TC_APS_SE10 更新初始化值

7.10.1 环境配置

TC_APS_SE10 的环境配置如表 32 所示。

表 32　TC_APS_SE10 的环境配置

测试拓扑结构	设备	配置
	STC (DUT)	PANID =0x1BBB Logical Address 随机分配,有效范围:0x0001～0xFFF7 MAC address =0xAA AA AA AA AA AA AA AA
	rSED	PANID=0x1BBB Logical Address 随机分配,有效范围:0x0001～0xFFF7 MAC address =0xDDDDDDDDDDDDDDDD
	rSC	PANID=0x1BBB Logical Address=0x0000 MAC address =0xBB BB BB BB BB BB BB BB

7.10.2　测试过程

TC_APS_SE10 测试过程如表 33 所示。

表 33　TC_APS_SE10 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN,rSED 加入 PAN,DUT STC 加入 PAN	—

1	DUT STC 邻近高层发送 APSME-UPDATE-KEY.request
	{
	DestAddress =rSED 的地址
	KeyType = 0x01
	KeyData =0xAA BB CC DD
	}
		本步骤的通过判决见 7.10.3 a)中 1)、2)、3)

2	rSED 向邻近高层发送 APSME-UPDATE-KEY.indication
	{
	DestAddress =rSED 的地址
	KeyType = 0x01
	KeyData =0xAA BB CC DD
	}
		本步骤的通过判决见 7.10.3 a)中 4)

3	rSED 更新密钥为 KeyData,Initialization value 元素设置为 KeyData 参数中的初始化值	本步骤的通过判决见 7.10.3 a)中 5)

7.10.3　测试判决

本测试例通过与否的判决条件如下：

a)　成功判决：

1)　DUT STC 能够向 rSED 发送密钥更新请求命令；

2)　DUT STC 发出的 APS 数据中,APS 帧中存在辅助帧头和信息完整性校验码；

3） DUT STC 发出的 APS 数据中，命令标识符为 0x02(密钥更新命令帧)；
4） rSED 能够收到密钥更新命令帧；
5） rSED 能够更新密钥为 keyData。

b） 失败判决：
1） DUT STC 不能向 rSED 发送密钥更新请求命令；
2） DUT STC 发出的 APS 数据中，APS 帧中不存在辅助帧头和信息完整性校验码；
3） DUT STC 发出的 APS 数据中，命令标识符不为 0x02(密钥更新命令帧)；
4） rSED 不能收到密钥更新命令帧；
5） rSED 不能更新密钥为 keyData。

7.10.4 说明

本测试例覆盖附录 A 的部分声明项，如表 34 所示。

表 34 TC_NWK_SE10 的 PICS 声明项

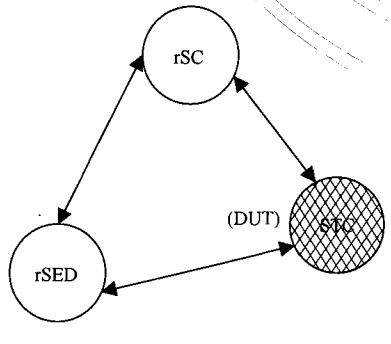
PICS 声明项	描述
AFS4	APS 是否支持使用信任中心去通知其他设备更换到一个新的密钥
ADFS1	APS 是否支持生成安全的 APS 数据帧，即增加了辅助帧头和信息完整性校验码 MIC 的 APS 数据帧
NCFS2	设备是否支持接收密钥更新命令帧

7.11 TC_APS_SE11 更新共享密钥

7.11.1 环境配置

TC_APS_SE11 的环境配置如表 35 所示。

表 35 TC_APS_SE11 的环境配置

测试拓扑结构	设备	配置
	STC (DUT)	PANID =0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xAA AA AA AA AA AA AA AA
	rSED	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xDDDDDDDDDDDDDDDD
	rSC	PANID=0x1BBB Logical Address=0x0000 MAC address =0xBB BB BB BB BB BB BB BB

7.11.2 测试过程

TC_APS_SE11 测试过程如表 36 所示。

表 36 TC_APS_SE11 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN，rSED 加入 PAN，DUT STC 加入 PAN	—

1	DUT STC 邻近高层发送 APSME-UPDATE-KEY.request
	{
	DestAddress ＝rSED 的地址
	KeyType ＝ 0x02
	KeyData ＝0xAA BB CC DD
	}
		本步骤的通过判决见 7.11.3 a)中 1)、2)、3)

2	rSED 向邻近高层发送 APSME-UPDATE-KEY.indication
	{
	DestAddress ＝rSED 的地址
	KeyType ＝ 0x02
	KeyData ＝0xAA BB CC DD
	}
		本步骤的通过判决见 7.11.3 a)中 4)

3	rSED 更新密钥为 KeyData，Shared key 和 Shared key ID 元素设置为 KeyData 参数中的初始化密钥材料及其相应的标识符	本步骤的通过判决见 7.11.3 a)中 5)

7.11.3 测试判决

本测试例通过与否的判决条件如下：

a) 成功判决：

1) DUT STC 能够向 rSED 发送密钥更新请求命令；
2) DUT STC 发出的 APS 数据中，APS 帧中存在辅助帧头和信息完整性校验码；
3) DUT STC 发出的 APS 数据中，命令标识符为 0x02(密钥更新命令帧)；
4) rSED 能够收到密钥更新命令帧；
5) rSED 能够更新密钥为 keyData。

b) 失败判决：

1) DUT STC 不能向 rSED 发送密钥更新请求命令；
2) DUT STC 发出的 APS 数据中，APS 帧中不存在辅助帧头和信息完整性校验码；
3) DUT STC 发出的 APS 数据中，命令标识符不为 0x02(密钥更新命令帧)；
4) rSED 不能收到密钥更新命令帧；
5) rSED 不能更新密钥为 keyData。

7.11.4 说明

本测试例覆盖附录 A 的部分声明项，如表 37 所示。

表 37 TC_NWK_SE11 的 PICS 声明项

PICS 声明项	描述
AFS4	APS 是否支持使用信任中心去通知其他设备更换到一个新的密钥

表 37（续）

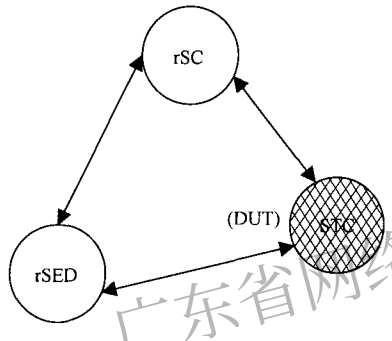
PICS 声明项	描述
ADFS1	APS 是否支持生成安全的 APS 数据帧，即增加了辅助帧头和信息完整性校验码 MIC 的 APS 数据帧
NCFS2	设备是否支持接收密钥更新命令帧

7.12 TC_APS_SE12 更新会话密钥

7.12.1 环境配置

TC_APS_SE12 的环境配置如表 38 所示。

表 38 TC_APS_SE12 的环境配置

测试拓扑结构	设备	配置
	STC (DUT)	PANID =0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xAA AA AA AA AA AA AA AA
	rSED	PANID=0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xDDDDDDDDDDDDDDDD
	rSC	PANID=0x1BBB Logical Address=0x0000 MAC address =0xBB BB BB BB BB BB BB BB

7.12.2 测试过程

TC_APS_SE12 测试过程如表 39 所示。

表 39 TC_APS_SE12 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN，rSED 加入 PAN，DUT STC 加入 PAN	—

1	DUT STC 邻近高层发送 APSME-UPDATE-KEY.request
	{
	DestAddress =rSED 的地址
	KeyType = 0x03
	KeyData =0xAA BB CC DD
	}
		本步骤的通过判决见 7.12.3 a)中 1)、2)、3)

表 39（续）

步骤	描述	说明

2	rSED 向邻近高层发送 APSME-UPDATE-KEY.indication
	{
	DestAddress ＝rSED 的地址
	KeyType ＝ 0x03
	KeyData ＝0xAA BB CC DD
	}
		本步骤的通过判决见 7.12.3 a)中 4)

3	rSED 更新密钥为 KeyData，Session key ID 和 Session key 元素应该设置为 KeyData 参数中的初始化值	本步骤的通过判决见 7.12.3 a)中 5)

7.12.3 测试判决

本测试例通过与否的判决条件如下：

a) 成功判决：

1) DUT STC 能够向 rSED 发送密钥更新请求命令；
2) DUT STC 发出的 APS 数据中，APS 帧中存在辅助帧头和信息完整性校验码；
3) DUT STC 发出的 APS 数据中，命令标识符为 0x02(密钥更新命令帧)；
4) rSED 能够收到密钥更新命令帧；
5) rSED 能够更新密钥为 keyData。

b) 失败判决：

1) DUT STC 不能向 rSED 发送密钥更新请求命令；
2) DUT STC 发出的 APS 数据中，APS 帧中不存在辅助帧头和信息完整性校验码；
3) DUT STC 发出的 APS 数据中，命令标识符不为 0x02(密钥更新命令帧)；
4) rSED 不能收到密钥更新命令帧；
5) rSED 不能更新密钥为 keyData。

7.12.4 说明

本测试例覆盖附录 A 的部分声明项，如表 40 所示。

表 40 TC_NWK_SE12 的 PICS 声明项

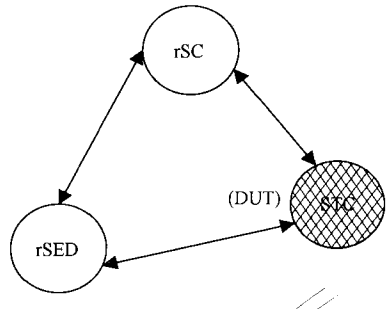
PICS 声明项	描述
AFS4	APS 是否支持使用信任中心去通知其他设备更换到一个新的密钥
ADFS1	APS 是否支持生成安全的 APS 数据帧，即增加了辅助帧头和信息完整性校验码 MIC 的 APS 数据帧
NCFS2	设备是否支持接收密钥更新命令帧

7.13 TC_APS_SE13 撤销密钥

7.13.1 环境配置

TC_APS_SE13 的环境配置如表 41 所示。

表 41　TC_APS_SE13 的环境配置

测试拓扑结构	设备	配置
	STC (DUT)	PANID =0x1BBB Logical Address 随机分配,有效范围:0x0001～0xFFF7 MAC address =0xAA AA AA AA AA AA AA AA
	rSED	PANID=0x1BBB Logical Address 随机分配,有效范围:0x0001～0xFFF7 MAC address =0xDDDDDDDDDDDDDDDD
	rSC	PANID=0x1BBB Logical Address=0x0000 MAC address =0xBB BB BB BB BB BB BB BB

7.13.2　测试过程

TC_APS_SE13 测试过程如表 42 所示。

表 42　TC_APS_SE13 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN,rSED 加入 PAN,DUT STC 加入 PAN	—

1	DUT STC 邻近高层发送 APSME-REVOCATION-KEY.request
	{
	DestAddress =rSED 的地址
	Key ID = 0x0000
	Revocation Time = 2017-05-01
	Revocation Reason=0xFF
	}
		本步骤的通过判决见 7.13.3 a)中 1)、2)、3)

2	rSED 向邻近高层发送 APSME-REVOCATION-KEY.indication
	{
	SrcAddress =DUT STC 的地址
	Key ID = 0x0000
	Revocation Time = 2017-05-01
	Revocation Reason=0xFF
	}
		本步骤的通过判决见 7.13.3 a)中 4)

3	rSED 删除存储的相关密钥信息	本步骤的通过判决见 7.13.3 a)中 5)

7.13.3　测试判决

本测试例通过与否的判决条件如下：

a)　成功判决：

1)　DUT STC 能够向 rSED 发送密钥撤销请求命令；

2)　DUT STC 发出的 APS 数据中,APS 帧中存在辅助帧头和信息完整性校验码；

3)　DUT STC 发出的 APS 数据中,命令标识符为 0x03(密钥撤销命令帧)；

4) rSED 能够收到密钥撤销命令帧；
5) rSED 能够删除存储的相关密钥信息。

b) 失败判决：
1) DUT STC 不能向 rSED 发送密钥撤销请求命令；
2) DUT STC 发出的 APS 数据中，APS 帧中不存在辅助帧头和信息完整性校验码；
3) DUT STC 发出的 APS 数据中，命令标识符不为 0x03(密钥撤销命令帧)；
4) rSED 不能收到密钥撤销命令帧；
5) rSED 不能删除存储的相关密钥信息。

7.13.4 说明

本测试例覆盖附录 A 的部分声明项，如表 43 所示。

表 43 TC_NWK_SE13 的 PICS 声明项

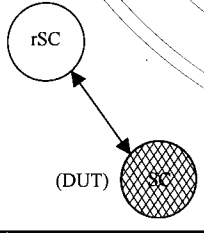
PICS 声明项	描述
AFS5	APS 是否支持使用信任中心去通知相关设备撤销使用特定密钥信息
ADFS1	APS 是否支持生成安全的 APS 数据帧，即增加了辅助帧头和信息完整性校验码 MIC 的 APS 数据帧
NCFS3	设备是否支持接收密钥撤销命令帧

7.14 TC_APS_SE14 在网关处对数据资源采用自主访问方法启动访问控制过程

7.14.1 环境配置

TC_APS_SE14 的环境配置如表 44 所示。

表 44 TC_APS_SE14 的环境配置

测试拓扑结构	设备	配置
	SC (DUT)	PANID= 0x1BBB Logical Address=0x0000 MAC address =0xAA AA AA AA AA AA AA AA
	rSC	PANID = 0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xBB BB BB BB BB BB BB BB

7.14.2 测试过程

TC_APS_SE14 测试过程如表 45 所示。

表 45 TC_APS_SE14 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	DUT SC 建立 PAN，rSC 加入 PAN	—

表 45（续）

步骤	描述	说明

1	DUT SC 邻近高层产生 APSME-ACCESS-CONTROL.request
	{
	ResponderAddress = DUT SC 的地址
	Action = INITIATE
	AccessObject = 0x00
	AccessControlMethod =0x00
	}
		本步骤的通过判决见 7.14.3 a)中 1)

2	rSC 向邻近高层发送 APSME-ACCESS-CONTROL.indication
	{
	InitiatorAddress = DUT SC 的地址
	AccessObject = 0x00
	AccessControlMethod=0x00
	}
		本步骤的通过判决见 7.14.3 a)中 2)、3)

3	DUT SC 邻近高层发送 APSME-ACCESS-CONTROL.request
	{
	ResponderAddress = rSC 的地址
	Action = RESPOND_ACCEPT
	AccessObject = 0x00
	AccessControlMethod =0x00
	}
		本步骤的通过判决见 7.14.3 a)中 4)

4	DUT SC 决定 rSC 对数据资源自主访问控制，
	rSC 向邻近高层发送 APSME-ACCESS-CONTROL.confirm
	{
	Address = DUT SC 的地址
	Status = SUCCESS
	}
		本步骤的通过判决见 7.14.3 a)中 5)

7.14.3 测试判决

本测试例通过与否的判决条件如下：

a) 成功判决：

1) DUT SC 能够向 rSC 发送对数据资源自主访问控制请求命令；

2) rSC 能够收到 DUT SC 的访问控制请求并通知邻近高层；

3) rSC 发出的 APS 数据中，命令标识符为 0x04(访问控制请求命令帧)；

4) DUT SC 收到的 APS 数据中，命令标识符为 0x05(访问控制响应命令帧)；

5) DUT SC 能够对 rSC 请求的数据资源进行自主访问控制。

b) 失败判决：

1) DUT SC 不能向 rSC 发送对数据资源自主访问控制请求命令；

2) rSC 不能收到 DUT SC 的访问控制请求并通知邻近高层；

3) rSC 发出的 APS 数据中，命令标识符不为 0x04(访问控制请求命令帧)；

4) DUT SC 收到的 APS 数据中，命令标识符不为 0x05(访问控制响应命令帧)；

5) DUT SC 不能对 rSC 请求的数据资源进行自主访问控制。

7.14.4 说明

本测试例覆盖附录 A 的部分声明项，如表 46 所示。

表 46 TC_NWK_SE14 的 PICS 声明项

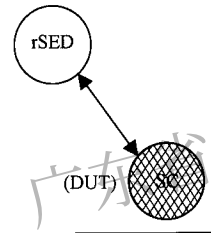
PICS 声明项	描述
AFS6	APS 是否支持控制用户对传感网的节点资源和数据资源的访问
NCFS4	设备是否支持生成访问控制请求命令帧
NCFS5	设备是否支持接收访问控制响应命令帧

7.15 TC_APS_SE15 在网关处对节点资源采用自主访问方法启动访问控制过程

7.15.1 环境配置

TC_APS_SE15 的环境配置如表 47 所示。

表 47 TC_APS_SE15 的环境配置

测试拓扑结构	设备	配置
	SC (DUT)	PANID= 0x1BBB Logical Address=0x0000 MAC address =0xAA AA AA AA AA AA AA AA
	rSED	PANID = 0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xBB BB BB BB BB BB BB BB

7.15.2 测试过程

TC_APS_SE15 测试过程如表 48 所示。

表 48 TC_APS_SE15 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	DUT SC 建立 PAN，rSED 加入 PAN	—

1	DUT SC 邻近高层产生 APSME-ACCESS-CONTROL.request
	{
	ResponderAddress = DUT SC 的地址
	Action = INITIATE
	AccessObject = 0x01
	AccessControlMethod =0x00
	}
		本步骤的通过判决见 7.15.3 a)中 1)

表 48（续）

步骤	描述	说明

2	rSED 向邻近高层发送 APSME-ACCESS-CONTROL.indication
	{
	InitiatorAddress = DUT SC 的地址
	AccessObject = 0x01
	AccessControlMethod=0x00
	}
		本步骤的通过判决见 7.15.3 a)中 2)、3)

3	DUT SC 邻近高层发送 APSME-ACCESS-CONTROL.request
	{
	ResponderAddress = rSED 的地址
	Action = RESPOND_ACCEPT
	AccessObject = 0x01
	AccessControlMethod = 0x00
	}
		本步骤的通过判决见 7.15.3 a)中 4)

4	DUT SC 决定对 rSED 自主访问控制，
	rSED 向邻近高层发送 APSME-ACCESS-CONTROL.confirm
	{
	Address = DUT SC 的地址
	Status = SUCCESS
	}
		本步骤的通过判决见 7.15.3 a)中 5)

7.15.3 测试判决

本测试例通过与否的判决条件如下：

a) 成功判决：

1) DUT SC 能够向 rSED 发送对节点资源自主访问控制请求命令；
2) rSED 能够收到 DUT SC 的访问控制请求并通知邻近高层；
3) rSED 发出的 APS 数据中，命令标识符为 0x04(访问控制请求命令帧)；
4) DUT SC 收到的 APS 数据中，命令标识符为 0x05(访问控制响应命令帧)；
5) DUT SC 能够对 rSED 资源进行自主访问控制。

b) 失败判决：

1) DUT SC 不能向 rSED 发送对节点资源自主访问控制请求命令；
2) rSED 不能收到 DUT SC 的访问控制请求并通知邻近高层；
3) rSED 发出的 APS 数据中，命令标识符不为 0x04(访问控制请求命令帧)；
4) DUT SC 收到的 APS 数据中，命令标识符不为 0x05(访问控制响应命令帧)；
5) DUT SC 不能对 rSED 资源进行自主访问控制。

7.15.4 说明

本测试例覆盖附录 A 的部分声明项，如表 49 所示。

表 49　TC_NWK_SE15 的 PICS 声明项

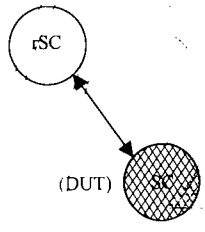
PICS 声明项	描述
AFS6	APS 是否支持控制用户对传感网的节点资源和数据资源的访问
NCFS4	设备是否支持生成访问控制请求命令帧
NCFS5	设备是否支持接收访问控制响应命令帧

7.16　TC_APS_SE16 在网关处对数据资源采用强制访问方法启动访问控制过程

7.16.1　环境配置

TC_APS_SE16 的环境配置如表 50 所示。

表 50　TC_APS_SE16 的环境配置

测试拓扑结构	设备	配置
	SC (DUT)	PANID= 0x1BBB Logical Address=0x0000 MAC address =0xAA AA AA AA AA AA AA AA
	rSC	PANID = 0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xBB BB BB BB BB BB BB BB

7.16.2　测试过程

TC_APS_SE16 测试过程如表 51 所示。

表 51　TC_APS_SE16 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	DUT SC 建立 PAN，rSC 加入 PAN	—

1	DUT SC 邻近高层产生 APSME-ACCESS-CONTROL.request
	{
	ResponderAddress = DUT SC 的地址
	Action = INITIATE
	AccessObject = 0x00
	AccessControlMethod =0x01
	}
		本步骤的通过判决见 7.16.3 a)中 1)

2	rSC 向邻近高层发送 APSME-ACCESS-CONTROL.indication
	{
	InitiatorAddress = DUT SC 的地址
	AccessObject = 0x00
	AccessControlMethod=0x01
	}
		本步骤的通过判决见 7.16.3 a)中 2)、3)

表 51（续）

步骤	描述	说明

3	DUT SC 邻近高层发送 APSME-ACCESS-CONTROL.request
	{
	ResponderAddress = rSC 的地址
	Action = RESPOND_ACCEPT
	AccessObject = 0x00
	AccessControlMethod =0x01
	}
		本步骤的通过判决见 7.16.3 a)中 4)

4	DUT SC 决定 rSC 对数据资源强制访问控制，
	rSC 向邻近高层发送 APSME-ACCESS-CONTROL.confirm
	{
	Address = DUT SC 的地址
	Status = SUCCESS
	}
		本步骤的通过判决见 7.16.3 a)中 5)

7.16.3 测试判决

本测试例通过与否的判决条件如下：

a) 成功判决：

1) DUT SC 能够向 rSC 发送对数据资源强制访问控制请求命令；
2) rSC 能够收到 DUT SC 的访问控制请求并通知邻近高层；
3) rSC 发出的 APS 数据中，命令标识符为 0x04(访问控制请求命令帧)；
4) DUT SC 收到的 APS 数据中，命令标识符为 0x05(访问控制响应命令帧)；
5) DUT SC 能够对 rSC 请求的数据资源进行强制访问控制。

b) 失败判决：

1) DUT SC 不能向 rSC 发送对数据资源强制访问控制请求命令；
2) rSC 不能收到 DUT SC 的访问控制请求并通知邻近高层；
3) rSC 发出的 APS 数据中，命令标识符不为 0x04(访问控制请求命令帧)；
4) DUT SC 收到的 APS 数据中，命令标识符不为 0x05(访问控制响应命令帧)；
5) DUT SC 不能对 rSC 请求的数据资源进行强制访问控制。

7.16.4 说明

本测试例覆盖附录 A 的部分声明项，如表 52 所示。

表 52 TC_NWK_SE16 的 PICS 声明项

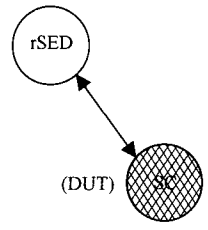
PICS 声明项	描述
AFS6	APS 是否支持控制用户对传感网的节点资源和数据资源的访问
NCFS4	设备是否支持生成访问控制请求命令帧
NCFS5	设备是否支持接收访问控制响应命令帧

7.17 TC_APS_SE17 在网关处对节点资源采用强制访问方法启动访问控制过程

7.17.1 环境配置

TC_APS_SE17 的环境配置如表 53 所示。

表 53 TC_APS_SE17 的环境配置

测试拓扑结构	设备	配置
	SC (DUT)	PANID= 0x1BBB Logical Address=0x0000 MAC address =0xAA AA AA AA AA AA AA AA
	rSED	PANID = 0x1BBB Logical Address 随机分配,有效范围:0x0001～0xFFF7 MAC address =0xBB BB BB BB BB BB BB BB

7.17.2 测试过程

TC_APS_SE17 测试过程如表 54 所示。

表 54 TC_APS_SE17 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	DUT SC 建立 PAN,rSED 加入 PAN	—

1	DUT SC 邻近高层产生 APSME-ACCESS-CONTROL.request
	{
	ResponderAddress = DUT SC 的地址
	Action = INITIATE
	AccessObject = 0x01
	AccessControlMethod =0x01
	}
		本步骤的通过判决见 7.17.3 a)中 1)

2	rSED 向邻近高层发送 APSME-ACCESS-CONTROL.indication
	{
	InitiatorAddress = DUT SC 的地址
	AccessObject = 0x01
	AccessControlMethod=0x01
	}
		本步骤的通过判决见 7.17.3 a)中 2)、3)

3	DUT SC 邻近高层发送 APSME-ACCESS-CONTROL.request
	{
	ResponderAddress = rSED 的地址
	Action =RESPOND_ACCEPT
	AccessObject = 0x01
	AccessControlMethod =0x01
	}
		本步骤的通过判决见 7.17.3 a)中 4)

表 54（续）

步骤	描述	说明

4	DUT SC 决定对 rSED 强制访问控制，
	rSED 向邻近高层发送 APSME-ACCESS-CONTROL.confirm
	{
	Address = DUT SC 的地址
	Status = SUCCESS
	}
		本步骤的通过判决见 7.17.3 a)中 5)

7.17.3 测试判决

本测试例通过与否的判决条件如下：

a) 成功判决：

1) DUT SC 能够向 rSED 发送对节点资源强制访问控制请求命令；
2) rSED 能够收到 DUT SC 的强制访问控制请求并通知邻近高层；
3) rSED 发出的 APS 数据中，命令标识符为 0x04(访问控制请求命令帧)；
4) DUT SC 收到的 APS 数据中，命令标识符为 0x05(访问控制响应命令帧)；
5) DUT SC 能够对 rSED 资源进行强制访问控制。

b) 失败判决：

1) DUT SC 不能向 rSED 发送对节点资源强制访问控制请求命令；
2) rSED 不能收到 DUT SC 的强制访问控制请求并通知邻近高层；
3) rSED 发出的 APS 数据中，命令标识符不为 0x04(访问控制请求命令帧)；
4) DUT SC 收到的 APS 数据中，命令标识符不为 0x05(访问控制响应命令帧)；
5) DUT SC 不能对 rSED 资源进行强制访问控制。

7.17.4 说明

本测试例覆盖附录 A 的部分声明项，如表 55 所示。

表 55 TC_NWK_SE17 的 PICS 声明项

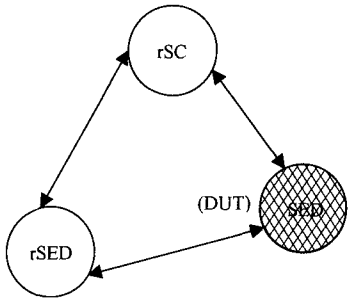
PICS 声明项	描述
AFS6	APS 是否支持控制用户对传感网的节点资源和数据资源的访问
NCFS4	设备是否支持生成访问控制请求命令帧
NCFS5	设备是否支持接收访问控制响应命令帧

7.18 TC_APS_SE18 在节点处对节点资源采用强制访问方法启动访问控制过程

7.18.1 环境配置

TC_APS_SE18 的环境配置如表 56 所示。

表 56　TC_APS_SE18 的环境配置

测试拓扑结构	设备	配置
	rSC	PANID= 0x1BBB Logical Address=0x0000 MAC address =0xAA AA AA AA AA AA AA AA
	SED (DUT)	PANID = 0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xBB BB BB BB BB BB BB BB
	rSED	PANID = 0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0x00 00 00 01 00 00 00 00

7.18.2　测试过程

TC_APS_SE18 测试过程如表 57 所示。

表 57　TC_APS_SE18 的测试过程

步骤	描述	说明
0a	所有设备复位	
0b	rSC 建立 PAN，DUT SED、rSED 加入 PAN	—

1	DUT SED 邻近高层产生 APSME-ACCESS-CONTROL.request
	{
	ResponderAddress = DUT SED 的地址
	Action = INITIATE
	AccessObject = 0x01
	AccessControlMethod =0x01
	}
		本步骤的通过判决见 7.18.3 a)中 1)

2	rSED 向邻近高层发送 APSME-ACCESS-CONTROL.indication
	{
	InitiatorAddress = DUT SED 的地址
	AccessObject = 0x01
	AccessControlMethod=0x01
	}
		本步骤的通过判决见 7.18.3 a)中 2)、3)

3	DUT SED 邻近高层发送 APSME-ACCESS-CONTROL.request
	{
	ResponderAddress = rSED 的地址
	Action =RESPOND_ACCEPT
	AccessObject = 0x01
	AccessControlMethod =0x01
	}
		本步骤的通过判决见 7.18.3 a)中 4)

表 57（续）

步骤	描述	说明

4	DUT SED 决定对 rSED 强制访问控制，
	rSED 向邻近高层发送 APSME-ACCESS-CONTROL.confirm
	{
	Address = DUT SED 的地址
	Status = SUCCESS
	}
		本步骤的通过判决见 7.18.3 a)中 5)

7.18.3 测试判决

本测试例通过与否的判决条件如下：

a) 成功判决：

1) DUT SED 能够向 rSED 发送对节点资源强制访问控制请求命令；
2) rSED 能够收到 DUT SED 的强制访问控制请求并通知邻近高层；
3) rSED 发出的 APS 数据中，命令标识符为 0x04(访问控制请求命令帧)；
4) DUT SED 收到的 APS 数据中，命令标识符为 0x05(访问控制响应命令帧)；
5) DUT SED 能够对 rSED 资源进行强制访问控制。

b) 失败判决：

1) DUT SED 不能向 rSED 发送对节点资源强制访问控制请求命令；
2) rSED 不能收到 DUT SED 的强制访问控制请求并通知邻近高层；
3) rSED 发出的 APS 数据中，命令标识符不为 0x04(访问控制请求命令帧)；
4) DUT SED 收到的 APS 数据中，命令标识符不为 0x05(访问控制响应命令帧)；
5) DUT SED 不能对 rSED 资源进行强制访问控制。

7.18.4 说明

本测试例覆盖附录 A 的部分声明项，如表 58 所示。

表 58 TC_NWK_SE18 的 PICS 声明项

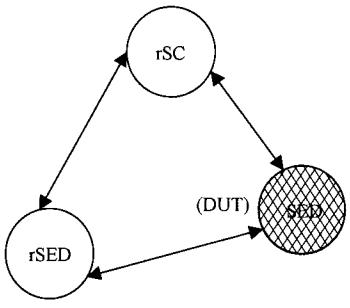
PICS 声明项	描述
AFS6	APS 是否支持控制用户对传感网的节点资源和数据资源的访问
NCFS4	设备是否支持生成访问控制请求命令帧
NCFS5	设备是否支持接收访问控制响应命令帧

7.19 TC_APS_SE19 基于异或算法的身份鉴别

7.19.1 环境配置

TC_APS_SE19 的环境配置如表 59 所示。

表 59　TC_APS_SE19 的环境配置

测试拓扑结构	设备	配置
	rSC	PANID = 0x1BBB Logical Address =0x0000 MAC address =0xAA AA AA AA AA AA AA AA
	SED (DUT)	PANID = 0x1BBB Logical Address 随机分配,有效范围:0x0001～0xFFF7 MAC address =0xBB BB BB BB BB BB BB BB
	rSED	PANID = 0x1BBB Logical Address 随机分配,有效范围:0x0001～0xFFF7 MAC address =0xCC CC CC CC CC CC CC CC

7.19.2　测试过程

TC_APS_SE19 测试过程如表 60 所示。

表 60　TC_APS_SE19 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN,DUT SED 和 rSED 加入 PAN	—

1	DUT SED 的邻近高层发起 APSME-IDENTITY-AUTHENTICATE.request
	{
	DestAddress = rSED 的地址
	AuthenticateMethod = 0x00
	RandomChallenge =0x00 00110000000000
	}
	DUT SED 使用 MCPS-DATA.request 原语发送基于异或算法身份鉴别请求命令,请求与 rSED 进行基于异或算法身份鉴别的过程
		本步骤的通过判决见 7.19.3 a)中 1)、2)

2	rSED 向邻近高层发送 APSME-IDENTITY-AUTHENTICATE.indication
	{
	InitiatorAddress = DUT SED 的地址
	AuthenticateMethod = 0x00
	RandomChallenge =0x00 00110000000000
	}
		本步骤的通过判决见 7.19.3 a)中 3)

3	rSED 邻近高层对 rSED 进行基于异或算法身份鉴别	本步骤的通过判决见 7.19.3 a)中 4)

4	rSED 的邻近高层发起 APSME-IDENTITY-AUTHENTICATE.request
	{
	DestAddress =DUT SED 的地址
	AuthenticateMethod = 0x00
	RandomChallenge =0x00 00110000000000
	}
		本步骤的通过判决见 7.19.3 a)中 5)、6)

表 60（续）

步骤	描述	说明

5	DUT SED 向邻近高层发送 APSME-IDENTITY-AUTHENTICATE.indication
	{
	InitiatorAddress = DUT SED 的地址
	AuthenticateMethod = 0x00
	RandomChallenge =0x00 00110000000000
	}
		本步骤的通过判决见 7.19.3 a)中 7)、8)、9)

6	DUT SED 邻近高层对 DUT SED 进行基于异或算法身份鉴别
	DUT SED 向邻近高层发送 APSME-IDENTITY-AUTHENTICATE.confirm
	{
	Address=DUT SED 的地址
	Status=SUCCESS
	}
	rSED 向邻近高层发送 APSME-IDENTITY-AUTHENTICATE.confirm
	{
	Address= rSED 的地址
	Status=SUCCESS
	}
		本步骤的通过判决见 7.19.3 a)中 10)

7.19.3 测试判决

本测试例通过与否的判决条件如下：

a) 成功判决：

1) DUT SED 邻近高层能够向 rSED 发送基于异或算法身份鉴别请求命令；
2) DUT SED 发出的 APS 数据中，命令标识符为 0x06(身份鉴别请求命令帧)；
3) rSED 能够收到 DUT SED 基于异或算法身份鉴别请求并通知邻近高层；
4) DUT SED 能够对 rSED 进行基于异或算法身份鉴别；
5) rSED 邻近高层能够向 DUT SED 发送对基于异或算法身份鉴别响应命令；
6) rSED 发出的 APS 数据中，命令标识符为 0x07(身份鉴别响应命令帧)；
7) DUT SED 能够收到 rSED 基于异或算法身份鉴别响应并通知邻近高层；
8) DUT SED 能够对 rSED 基于异或算法身份鉴别响应确认；
9) DUT SED 向 rSED 发出的基于异或算法身份鉴别响应确认 APS 数据中，命令标识符为 0x08(身份鉴别响应确认命令帧)；
10) rSED 能够对 DUT SED 进行基于异或算法身份鉴别。

b) 失败判决：

1) DUT SED 邻近高层不能向 rSED 发送基于异或算法身份鉴别请求命令；
2) DUT SED 发出的 APS 数据中，命令标识符不为 0x06(身份鉴别请求命令帧)；
3) rSED 不能收到 DUT SED 基于异或算法身份鉴别请求并通知邻近高层；
4) DUT SED 不能对 rSED 进行基于异或算法身份鉴别；
5) rSED 邻近高层不能向 DUT SED 发送对基于异或算法身份鉴别响应命令；
6) rSED 发出的 APS 数据中，命令标识符不为 0x07(身份鉴别响应命令帧)；

7) DUT SED 不能收到 rSED 基于异或算法身份鉴别响应并通知邻近高层；
8) DUT SED 不能对 rSED 基于异或算法身份鉴别响应确认；
9) DUT SED 向 rSED 发出的基于异或算法身份鉴别响应确认 APS 数据中，命令标识符不为 0x08(身份鉴别响应确认命令帧)；
10) rSED 不能对 DUT SED 进行基于异或算法身份鉴别。

7.19.4 说明

本测试例覆盖附录 A 的部分声明项，如表 61 所示。

表 61 TC_NWK_SE19 的 PICS 声明项

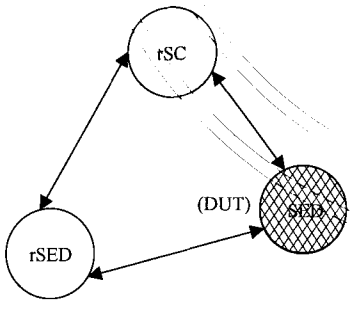
PICS 声明项	描述
AFS7	APS 是否支持两个设备之间进行身份鉴别
NCFS6	设备是否支持生成身份鉴别请求命令帧
NCFS7	设备是否支持接收身份鉴别响应命令帧
NCFS8	设备是否支持生成身份鉴别响应确认命令帧

7.20 TC_APS_SE20 基于哈希运算的身份鉴别

7.20.1 环境配置

TC_APS_SE20 的环境配置如表 62 所示。

表 62 TC_APS_SE20 的环境配置

测试拓扑结构	设备	配置
	rSC	PANID = 0x1BBB Logical Address = 0x0000 MAC address = 0xAA AA AA AA AA AA AA AA
	SED (DUT)	PANID = 0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address = 0xBB BB BB BB BB BB BB BB
	rSED	PANID = 0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address = 0xCC CC CC CC CC CC CC CC

7.20.2 测试过程

TC_APS_SE20 测试过程如表 63 所示。

表 63 TC_APS_SE20 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN，DUT SED 和 rSED 加入 PAN	—

表 63（续）

步骤	描述	说明

1	DUT SED 的邻近高层发起 APSME-IDENTITY-AUTHENTICATE.request
	{
	DestAddress = rSED 的地址
	AuthenticateMethod = 0x01
	RandomChallenge =0x00 00110000000000
	}
	DUT SED 使用 MCPS-DATA.request 原语发送基于哈希运算身份鉴别请求命令，请求与 rSED 进行基于哈希运算身份鉴别的过程
		本步骤的通过判决见 7.20.3 a)中 1)、2)

2	rSED 向邻近高层发送 APSME-IDENTITY-AUTHENTICATE.indication
	{
	InitiatorAddress = DUT SED 的地址
	AuthenticateMethod = 0x01
	RandomChallenge =0x00 00110000000000
	}
		本步骤的通过判决见 7.20.3 a)中 3)

3	rSED 邻近高层对 rSED 进行基于哈希运算身份鉴别	本步骤的通过判决见 7.20.3 a)中 4)

4	rSED 的邻近高层发起 APSME-IDENTITY-AUTHENTICATE.request
	{
	DestAddress =DUT SED 的地址
	AuthenticateMethod = 0x01
	RandomChallenge =0xCC 00110000000000
	}
		本步骤的通过判决见 7.20.3 a)中 5)、6)

5	DUT SED 向邻近高层发送 APSME-IDENTITY-AUTHENTICATE.indication
	{
	InitiatorAddress = DUT SED 的地址
	AuthenticateMethod = 0x01
	RandomChallenge =0x00 00110000000000
	}
		本步骤的通过判决见 7.20.3 a)中 7)、8)、9)

6	DUT SED 邻近高层对 DUT SED 进行基于哈希运算身份鉴别
	DUT SED 向邻近高层发送 APSME-IDENTITY-AUTHENTICATE.confirm
	{
	Address=DUT SED 的地址
	Status=SUCCESS
	}
	rSED 向邻近高层发送 APSME-IDENTITY-AUTHENTICATE.confirm
	{
	Address= rSED 的地址
	Status=SUCCESS
	}
		本步骤的通过判决见 7.20.3 a)中 10)

7.20.3 测试判决

本测试例通过与否的判决条件如下：

a) 成功判决：

1) DUT SED 邻近高层能够向 rSED 发送基于哈希运算身份鉴别请求命令；
2) DUT SED 发出的 APS 数据中，命令标识符为 0x06(身份鉴别请求命令帧)；
3) rSED 能够收到 DUT SED 基于哈希运算身份鉴别请求并通知邻近高层；
4) DUT SED 能够对 rSED 进行基于哈希运算身份鉴别；
5) rSED 邻近高层能够向 DUT SED 发送对基于哈希运算身份鉴别响应命令；
6) rSED 发出的 APS 数据中，命令标识符为 0x07(身份鉴别响应命令帧)；
7) DUT SED 能够收到 rSED 基于哈希运算身份鉴别响应并通知邻近高层；
8) DUT SED 能够对 rSED 基于哈希运算身份鉴别响应确认；
9) DUT SED 向 rSED 发出的基于哈希运算身份鉴别响应确认 APS 数据中，命令标识符为 0x08(身份鉴别响应确认命令帧)；
10) rSED 能够对 DUT SED 进行基于哈希运算身份鉴别。

b) 失败判决：

1) DUT SED 邻近高层不能向 rSED 发送基于哈希运算身份鉴别请求命令；
2) DUT SED 发出的 APS 数据中，命令标识符不为 0x06(身份鉴别请求命令帧)；
3) rSED 不能收到 DUT SED 基于哈希运算身份鉴别请求并通知邻近高层；
4) DUT SED 不能对 rSED 进行基于哈希运算身份鉴别；
5) rSED 邻近高层不能向 DUT SED 发送对基于哈希运算身份鉴别响应命令；
6) rSED 发出的 APS 数据中，命令标识符不为 0x07(身份鉴别响应命令帧)；
7) DUT SED 不能收到 rSED 基于哈希运算身份鉴别响应并通知邻近高层；
8) DUT SED 不能对 rSED 基于哈希运算身份鉴别响应确认；
9) DUT SED 向 rSED 发出的基于哈希运算身份鉴别响应确认 APS 数据中，命令标识符不为 0x08(身份鉴别响应确认命令帧)；
10) rSED 不能对 DUT SED 进行基于哈希运算身份鉴别。

7.20.4 说明

本测试例覆盖附录 A 的部分声明项，如表 64 所示。

表 64 TC_NWK_SE20 的 PICS 声明项

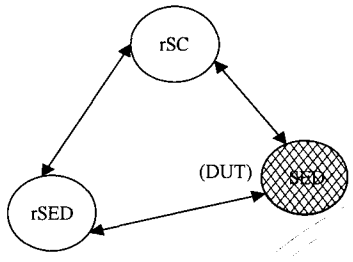
PICS 声明项	描述
AFS7	APS 是否支持两个设备之间进行身份鉴别
NCFS6	设备是否支持生成身份鉴别请求命令帧
NCFS7	设备是否支持接收身份鉴别响应命令帧
NCFS8	设备是否支持生成身份鉴别响应确认命令帧

7.21 TC_APS_SE21 基于分组密码算法的身份鉴别

7.21.1 环境配置

TC_APS_SE21 的环境配置如表 65 所示。

表 65 TC_APS_SE21 的环境配置

测试拓扑结构	设备	配置
	rSC	PANID = 0x1BBB Logical Address =0x0000 MAC address =0xAA AA AA AA AA AA AA AA
	SED (DUT)	PANID = 0x1BBB Logical Address 随机分配,有效范围:0x0001～0xFFF7 MAC address =0xBB BB BB BB BB BB BB BB
	rSED	PANID = 0x1BBB Logical Address 随机分配,有效范围:0x0001～0xFFF7 MAC address =0xCC CC CC CC CC CC CC CC

7.21.2 测试过程

TC_APS_SE21 测试过程如表 66 所示。

表 66 TC_APS_SE21 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN,DUT SED 和 rSED 加入 PAN	—

1	DUT SED 的邻近高层发起 APSME-IDENTITY-AUTHENTICATE.request
	{
	DestAddress = rSED 的地址
	AuthenticateMethod = 0x02
	RandomChallenge =0x00 00110000000000
	}
	DUT SED 使用 MCPS-DATA.request 原语发送基于分组密码算法身份鉴别请求命令,请求与 rSED 进行基于分组密码算法身份鉴别的过程
		本步骤的通过判决见 7.21.3 a)中 1)、2)

2	rSED 向邻近高层发送 APSME-IDENTITY-AUTHENTICATE.indication
	{
	InitiatorAddress = DUT SED 的地址
	AuthenticateMethod = 0x02
	RandomChallenge =0x00 00110000000000
	}
		本步骤的通过判决见 7.21.3 a)中 3)

3	rSED 邻近高层对 rSED 进行基于分组密码算法身份鉴别	本步骤的通过判决见 7.21.3 a)中 4)

表 66（续）

步骤	描述	说明

4	rSED 的邻近高层发起 APSME-IDENTITY-AUTHENTICATE.request
	{
	DestAddress ＝DUT SED 的地址
	AuthenticateMethod ＝ 0x02
	RandomChallenge ＝0x00 00110000000000
	}
		本步骤的通过判决见 7.21.3 a)中 5)、6)

5	DUT SED 向邻近高层发送 APSME-IDENTITY-AUTHENTICATE.indication
	{
	InitiatorAddress ＝ DUT SED 的地址
	AuthenticateMethod ＝ 0x02
	RandomChallenge ＝0x00 00110000000000
	}
		本步骤的通过判决见 7.21.3 a)中 7)、8)、9)

6	DUT SED 邻近高层对 DUT SED 进行基于分组密码算法身份鉴别
	DUT SED 向邻近高层发送 APSME-IDENTITY-AUTHENTICATE.confirm
	{
	Address＝DUT SED 的地址
	Status＝SUCCESS
	}
	rSED 向邻近高层发送 APSME-IDENTITY-AUTHENTICATE.confirm
	{
	Address＝ rSED 的地址
	Status＝SUCCESS
	}
		本步骤的通过判决见 7.21.3 a)中 10)

7.21.3 测试判决

本测试例通过与否的判决条件如下：

a) 成功判决：

1) DUT SED 邻近高层能够向 rSED 发送基于分组密码算法身份鉴别请求命令；
2) DUT SED 发出的 APS 数据中，命令标识符为 0x06(身份鉴别请求命令帧)；
3) rSED 能够收到 DUT SED 基于分组密码算法身份鉴别请求并通知邻近高层；
4) DUT SED 能够对 rSED 进行基于分组密码算法身份鉴别；
5) rSED 邻近高层能够向 DUT SED 发送对基于分组密码算法身份鉴别响应命令；
6) rSED 发出的 APS 数据中，命令标识符为 0x07(身份鉴别响应命令帧)；
7) DUT SED 能够收到 rSED 基于分组密码算法身份鉴别响应并通知邻近高层；
8) DUT SED 能够对 rSED 基于分组密码算法身份鉴别响应确认；
9) DUT SED 向 rSED 发出的基于分组密码算法身份鉴别响应确认 APS 数据中，命令标识符为 0x08(身份鉴别响应确认命令帧)；
10) rSED 能够对 DUT SED 进行基于分组密码算法身份鉴别。

b) 失败判决：

1) DUT SED 邻近高层不能向 rSED 发送基于分组密码算法身份鉴别请求命令；
2) DUT SED 发出的 APS 数据中，命令标识符不为 0x06(身份鉴别请求命令帧)；
3) rSED 不能收到 DUT SED 基于分组密码算法身份鉴别请求并通知邻近高层；
4) DUT SED 不能对 rSED 进行基于分组密码算法身份鉴别；
5) rSED 邻近高层不能向 DUT SED 发送对基于分组密码算法身份鉴别响应命令；
6) rSED 发出的 APS 数据中，命令标识符不为 0x07(身份鉴别响应命令帧)；
7) DUT SED 不能收到 rSED 基于分组密码算法身份鉴别响应并通知邻近高层；
8) DUT SED 不能对 rSED 基于分组密码算法身份鉴别响应确认；
9) DUT SED 向 rSED 发出的基于分组密码算法身份鉴别响应确认 APS 数据中，命令标识符不为 0x08(身份鉴别响应确认命令帧)；
10) rSED 不能对 DUT SED 进行基于分组密码算法身份鉴别。

7.21.4 说明

本测试例覆盖附录 A 的部分声明项，如表 67 所示。

表 67 TC_NWK_SE21 的 PICS 声明项

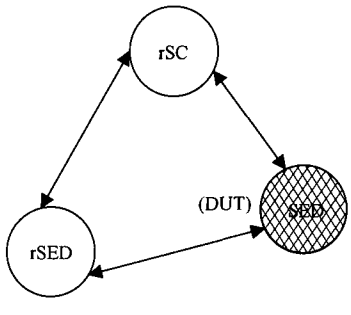
PICS 声明项	描述
AFS7	APS 是否支持两个设备之间进行身份鉴别
NCFS6	设备是否支持生成身份鉴别请求命令帧
NCFS7	设备是否支持接收身份鉴别响应命令帧
NCFS8	设备是否支持生成身份鉴别响应确认命令帧

7.22 TC_APS_SE22 基于非对称密码算法的身份鉴别

7.22.1 环境配置

TC_APS_SE22 的环境配置如表 68 所示。

表 68 TC_APS_SE22 的环境配置

测试拓扑结构	设备	配置
	rSC	PANID = 0x1BBB Logical Address =0x0000 MAC address =0xAA AA AA AA AA AA AA AA
	SED (DUT)	PANID = 0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xBB BB BB BB BB BB BB BB
	rSED	PANID = 0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xCC CC CC CC CC CC CC CC

7.22.2 测试过程

TC_APS_SE22 测试过程如表 69 所示。

表 69　TC_APS_SE22 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN，DUT SED 和 rSED 加入 PAN	—

1	DUT SED 的邻近高层发起 APSME-IDENTITY-AUTHENTICATE.request
	{
	DestAddress = rSED 的地址
	AuthenticateMethod = 0x03
	RandomChallenge =0x00 00110000000000
	}
	DUT SED 使用 MCPS-DATA.request 原语发送基于非对称密码算法身份鉴别请求命令，请求与 rSED 进行基于非对称密码算法身份鉴别的过程
		本步骤的通过判决见 7.22.3 a)中 1)、2)

2	rSED 向邻近高层发送 APSME-IDENTITY-AUTHENTICATE.indication
	{
	InitiatorAddress = DUT SED 的地址
	AuthenticateMethod = 0x03
	RandomChallenge =0x00 00110000000000
	}
		本步骤的通过判决见 7.22.3 a)中 3)

3	rSED 邻近高层对 rSED 进行基于非对称密码算法身份鉴别	本步骤的通过判决见 7.22.3 a)中 4)

4	rSED 的邻近高层发起 APSME-IDENTITY-AUTHENTICATE.request
	{
	DestAddress =DUT SED 的地址
	AuthenticateMethod = 0x03
	RandomChallenge =0x00 00110000000000
	}
		本步骤的通过判决见 7.22.3 a)中 5)、6)

5	DUT SED 向邻近高层发送 APSME-IDENTITY-AUTHENTICATE.indication
	{
	InitiatorAddress = DUT SED 的地址
	AuthenticateMethod = 0x03
	RandomChallenge =0x00 00110000000000
	}
		本步骤的通过判决见 7.22.3 a)中 7)、8)、9)

6	DUT SED 邻近高层对 DUT SED 进行基于非对称密码算法身份鉴别
	DUT SED 向邻近高层发送 APSME-IDENTITY-AUTHENTICATE.confirm
	{
	Address=DUT SED 的地址
	Status=SUCCESS
	}
	rSED 向邻近高层发送 APSME-IDENTITY-AUTHENTICATE.confirm
	{
	Address= rSED 的地址
	Status=SUCCESS
	}
		本步骤的通过判决见 7.22.3 a)中 10)

7.22.3 测试判决

本测试例通过与否的判决条件如下：

a) 成功判决：

1) DUT SED 邻近高层能够向 rSED 发送基于非对称密码算法身份鉴别请求命令；
2) DUT SED 发出的 APS 数据中，命令标识符为 0x06(身份鉴别请求命令帧)；
3) rSED 能够收到 DUT SED 基于非对称密码算法身份鉴别请求并通知邻近高层；
4) DUT SED 能够对 rSED 进行基于非对称密码算法身份鉴别；
5) rSED 邻近高层能够向 DUT SED 发送对基于非对称密码算法身份鉴别响应命令；
6) rSED 发出的 APS 数据中，命令标识符为 0x07(身份鉴别响应命令帧)；
7) DUT SED 能够收到 rSED 基于非对称密码算法身份鉴别响应并通知邻近高层；
8) DUT SED 能够对 rSED 基于非对称密码算法身份鉴别响应确认；
9) DUT SED 向 rSED 发出的基于非对称密码算法身份鉴别响应确认 APS 数据中，命令标识符为 0x08(身份鉴别响应确认命令帧)；
10) rSED 能够对 DUT SED 进行基于非对称密码算法身份鉴别。

b) 失败判决：

1) DUT SED 邻近高层不能向 rSED 发送基于非对称密码算法身份鉴别请求命令；
2) DUT SED 发出的 APS 数据中，命令标识符不为 0x06(身份鉴别请求命令帧)；
3) rSED 不能收到 DUT SED 基于非对称密码算法身份鉴别请求并通知邻近高层；
4) DUT SED 不能对 rSED 进行基于非对称密码算法身份鉴别；
5) rSED 邻近高层不能向 DUT SED 发送对基于非对称密码算法身份鉴别响应命令；
6) rSED 发出的 APS 数据中，命令标识符不为 0x07(身份鉴别响应命令帧)；
7) DUT SED 不能收到 rSED 基于非对称密码算法身份鉴别响应并通知邻近高层；
8) DUT SED 不能对 rSED 基于非对称密码算法身份鉴别响应确认；
9) DUT SED 向 rSED 发出的基于非对称密码算法身份鉴别响应确认 APS 数据中，命令标识符不为 0x08(身份鉴别响应确认命令帧)；
10) rSED 不能对 DUT SED 进行基于非对称密码算法身份鉴别。

7.22.4 说明

本测试例覆盖附录 A 的部分声明项，如表 70 所示。

表 70 TC_NWK_SE22 的 PICS 声明项

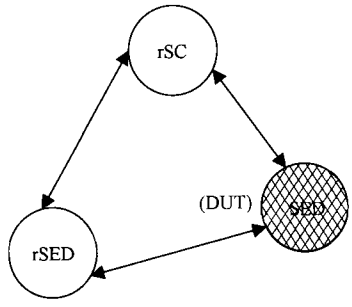
PICS 声明项	描述
AFS7	APS 是否支持两个设备之间进行身份鉴别
NCFS6	设备是否支持生成身份鉴别请求命令帧
NCFS7	设备是否支持接收身份鉴别响应命令帧
NCFS8	设备是否支持生成身份鉴别响应确认命令帧

7.23 TC_APS_SE23 启动广播消息鉴别

7.23.1 环境配置

TC_APS_SE23 的环境配置如表 71 所示。

表 71　TC_APS_SE23 的环境配置

测试拓扑结构	设备	配置
	rSC	PANID = 0x1BBB Logical Address =0x0000 MAC address =0xAA AA AA AA AA AA AA AA
	SED (DUT)	PANID = 0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xBB BB BB BB BB BB BB BB
	rSED	PANID = 0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xCC CC CC CC CC CC CC CC

7.23.2　测试过程

TC_APS_SE23 测试过程如表 72 所示。

表 72　TC_APS_SE23 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN，DUT SED 和 rSED 加入 PAN	—

1	DUT SED 的邻近高层产生 APSME-MESSAGE-AUTHENTICATE.request
	{
	PartnerAddress = DUT SED 的地址
	RandomChallenge =0x00 00110000000000
	}
		本步骤的通过判决见 7.23.3 a)中 1)、5)

2	rSED 向邻近高层发送 APSME-MESSAGE-AUTHENTICATE.indication
	{
	InitiatorAddress = DUT SED 的地址
	RandomChallenge = 0x00 00110000000000
	}
		本步骤的通过判决见 7.23.3 a)中 2)、3)

3	rSED 对广播消息鉴别。
	DUT SED 向邻近高层发送 APSME-MESSAGE-AUTHENTICATE.confirm
	{
	Address = rSED 的地址
	Status = SUCCESS
	}
	rSED 向邻近高层发送 APSME-MESSAGE-AUTHENTICATE.confirm
	{
	Address = rSED 的地址
	Status = SUCCESS
	}
		本步骤的通过判决见 7.23.3 a)中 4)

7.23.3 测试判决

本测试例通过与否的判决条件如下：

a) 成功判决：

1) DUT SED 能够向 rSED 发送广播消息鉴别请求命令；

2) DUT SED 发出的 APS 数据中，命令标识符为 0x09(广播消息鉴别命令帧)；

3) rSED 能够对广播消息进行鉴别。

b) 失败判决：

1) DUT SED 不能向 rSED 发送广播消息鉴别请求命令；

2) DUT SED 发出的 APS 数据中，命令标识符不为 0x09(广播消息鉴别命令帧)；

3) rSED 不能对广播消息进行鉴别。

7.23.4 说明

本测试例覆盖附录 A 的部分声明项，如表 73 所示。

表 73 TC_NWK_SE23 的 PICS 声明项

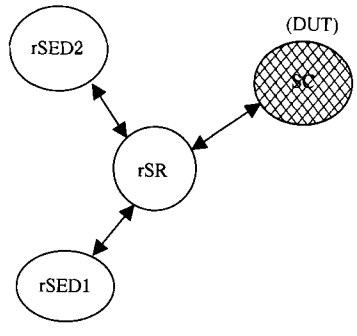
PICS 声明项	描述
AFS8	APS 是否支持两个设备之间进行广播消息鉴别
NCFS9	设备是否支持生成广播消息鉴别命令帧

7.24 TC_APS_SE24 启动安全数据融合服务

7.24.1 环境配置

TC_APS_SE24 的环境配置如表 74 所示。

表 74 TC_APS_SE24 的环境配置

测试拓扑结构	设备	配置
	SC (DUT)	PANID 随机分配，在这里假设为 0x1AAA Logical Address=0x0000 MAC address =0xAA AA AA AA AA AA AA AA
	rSR	PANID 随机分配，在这里假设为 0x1AAA Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0x00 00 01 00 00 00 00 00
	rSED2	融合设备 PANID 随机分配，在这里假设为 0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xBBBBBBBBBBBBBBBB
	rSED1	监督设备 PANID 随机分配，在这里假设为 0x1CCC Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xCC CC CC CC CC CC CC CC

7.24.2 测试过程

TC_APS_SE24 测试过程如表 75 所示。

表 75 TC_APS_SE24 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN，rSR 加入 PAN，rSED1 和 rSED2 通过 rSR 加入 PAN	—

1	DUT SC 的邻近高层产生 APSME-SECURE-DATA-AGGREGATION-START.request
	{
	AggregationNodeAddress ＝rSED2 的地址
	SupervisorNodeAddress ＝rSED1 的地址
	AggregationCycleTime ＝1 月
	}
		本步骤的通过判决见 7.24.3 a)中 1)、2)

2	RSED2 向邻近高层发送
	APSME-SECURE-DATA-AGGREGATION-START.indication
	{
	InitiatorAddress＝DUT SC 的地址
	Function＝0x00
	Time＝1 month
	}
	rSED1 发送到邻近高层
	APSME-SECURE-DATA-AGGREGATION-START.indication
	{
	InitiatorAddress＝DUT SC 的地址
	Function＝0x01
	Time＝1 月
	}
		本步骤的通过判决见 7.24.3 a)中 3)、4)

3	融合设备 rSED2 邻近高层产生
	APSME-SECURE-DATA-AGGREGATION-START.response
	{
	InitiatorAddress＝DUT SC 的地址
	Function＝0x00
	Accept＝TRUE
	}
	监督设备 rSED1 邻近高层产生
	APSME-SECURE-DATA-AGGREGATION-START.response
	{
	InitiatorAddress＝DUT SC 的地址
	Function＝0x01
	Accept＝TRUE
	}
		本步骤的通过判决见 7.24.3 a)中 5)、6)、7)、8)

表 75（续）

步骤	描述	说明

4	DUT SC 发送到邻近高层
	APSME-SECURE-DATA-AGGREGATION-START.confirm
	{
	Address＝DUT SC 的地址
	Status＝SUCCESS
	}
	RSED1 发送到邻近高层 APSME-SECURE-DATA-AGGREGATION-START.confirm
	{
	Address＝rSED1 的地址
	Status＝SUCCESS
	}
	RSED2 发送到邻近高层 APSME-SECURE-DATA-AGGREGATION-START.confirm
	{
	Address＝rSED2 的地址
	Status＝SUCCESS
	}
		本步骤的通过判决见 7.24.3 a)中 9)、10)

5	融合设备 rSED2 执行融合功能；监督设备 rSED1 执行监督功能	本步骤的通过判决见 7.24.3 a)中 11)、12)

7.24.3 测试判决

本测试例通过与否的判决条件如下：

a) 成功判决：

1) DUT SC 能够向 rSED1 和 rSED2 发送安全数据融合请求；
2) DUT SC 发出的 APS 数据中，命令标识符为 0x10（安全数据融合启动请求命令帧）；
3) 融合设备 rSED2 能够收到安全数据融合请求命令；
4) 监督设备 rSED1 能够收到安全数据融合请求命令；
5) 融合设备 rSED2 邻近高层能够向 DUT SC 发送执行融合功能的响应；
6) 监督设备 rSED1 邻近高层能够向 DUT SC 发送执行监督功能的响应；
7) rSED2 邻近高层发送的 APS 数据中，命令标识符为 0x11（融合设备响应命令帧）；
8) rSED1 邻近高层发送的 APS 数据中，命令标识符为 0x12（监督设备响应命令帧）；
9) DUT SC 能够确定安全数据融合服务启动结果，向 rSED1 和 rSED2 发送启动确认；
10) DUT SC 发送的 APS 数据中，命令标识符为 0x13（安全数据融合启动请求确认命令帧）；
11) 融合设备 rSED2 能够启动融合功能；
12) 监督设备 rSED1 能够启动监督功能。

b) 失败判决：

1) DUT SC 不能向 rSED1 和 rSED2 发送安全数据融合请求；
2) DUT SC 发出的 APS 数据中，命令标识符不为 0x10（安全数据融合启动请求命令帧）；
3) 融合设备 rSED2 不能收到安全数据融合请求命令；
4) 监督设备 rSED1 不能收到安全数据融合请求命令；
5) 融合设备 rSED2 邻近高层不能向 DUT SC 发送执行融合功能的响应；
6) 监督设备 rSED1 邻近高层不能向 DUT SC 发送执行监督功能的响应；

7) rSED2 邻近高层发送的 APS 数据中，命令标识符不为 0x11(融合设备响应命令帧)；
8) rSED1 邻近高层发送的 APS 数据中，命令标识符不为 0x12(监督设备响应命令帧)；
9) DUT SC 不能确定安全数据融合服务启动结果，向 rSED1 和 rSED2 发送启动确认；
10) DUT SC 发送的 APS 数据中，命令标识符不为 0x13(安全数据融合启动请求确认命令帧)；
11) 融合设备 rSED2 不能启动融合功能；
12) 监督设备 rSED1 不能启动监督功能。

7.24.4 说明

本测试例覆盖附录 A 的部分声明项，如表 76 所示。

表 76 TC_NWK_SE24 的 PICS 声明项

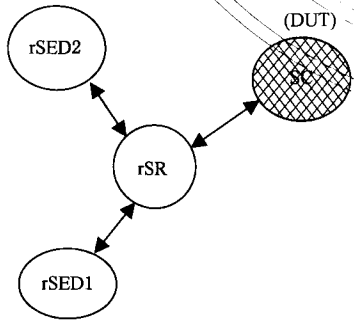
PICS 声明项	描述
AFS9	APS 是否支持发起设备(网络协调器)和响应设备进行安全数据融合
NCFS10	设备是否支持生成安全数据融合启动请求命令帧
NCFS11	设备是否支持生成融合设备响应命令帧
NCFS12	设备是否支持生成监督设备响应命令帧
NCFS13	设备是否支持生成安全数据融合启动请求确认命令帧

7.25 TC_APS_SE25 安全数据融合撤销

7.25.1 环境配置

TC_APS_SE25 的环境配置如表 77 所示。

表 77 TC_APS_SE25 的环境配置

测试拓扑结构	设备	配置
	SC (DUT)	PANID 随机分配，在这里假设为 0x1AAA Logical Address=0x0000 MAC address =0xAA AA AA AA AA AA AA AA
	rSR	PANID 随机分配，在这里假设为 0x1AAA Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0x00 00 01 00 00 00 00 00
	rSED2	融合设备 PANID 随机分配，在这里假设为 0x1BBB Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xBBBBBBBBBBBBBBBB
	rSED1	监督设备 PANID 随机分配，在这里假设为 0x1CCC Logical Address 随机分配，有效范围：0x0001～0xFFF7 MAC address =0xCC CC CC CC CC CC CC CC

7.25.2 测试过程

TC_APS_SE25 测试过程如表 78 所示。

表 78 TC_APS_SE25 的测试过程

步骤	描述	说明
0a	所有设备复位	—
0b	rSC 建立 PAN，rSR 加入 PAN，rSED 通过 rSR 加入 PAN	—

1	DUT SC 邻近高层发送
	APSME-SECURE-DATA-AGGREGATION-REVOKE.request
	{
	AggregationNodeAddress ＝rSED2 的地址
	SupervisorNodeAddress ＝rSED1 的地址
	}
		本步骤的通过判决见 7.25.3 a)中 1)、2)

2	融合设备 rSED 向邻近高层发送
	APSME-SECURE-DATA-AGGREGATION-REVOKE.indication
	{
	InitiatorAddress ＝DUT SC 的地址
	AggregationNodeAddress ＝rSED2 的地址
	SupervisorNodeAddress ＝rSED1 的地址
	Command ＝0x00
	}
	监督设备 rSR 向邻近高层发送
	APSME-SECURE-DATA-AGGREGATION-REVOKE.indication
	{
	InitiatorAddress ＝DUT SC 的地址
	AggregationNodeAddress ＝rSED2 的地址
	SupervisorNodeAddress ＝rSED1 的地址
	Command ＝0x01
	}
		本步骤的通过判决见 7.25.3 a)中 3)

3	融合设备 rSED2 终止融合功能，监督设备 rSED1 终止监督功能	本步骤的通过判决见 7.25.3 a)中 4)

7.25.3 测试判决

本测试例通过与否的判决条件如下：

a) 成功判决：

1) DUT SC 能够向 rSED1 和 rSED2 发送安全数据融合撤销请求；

2) DUT SC 发出的 APS 数据中，命令标识符为 0x14(安全数据融合撤销请求命令帧)；

3) 响应设备 rSED1 和 rSED2 能够接收到撤销融合节点以及对应的监督节点命令并发送给邻近高层；

4) rSED1 和 rSED2 能够结束融合/监督功能。

b) 失败判决：

1) DUT SC 不能向 rSED1 和 rSED2 发送安全数据融合撤销请求；

2) DUT SC 发出的 APS 数据中，命令标识符不为 0x14(安全数据融合撤销请求命令帧)；

3) 响应设备 rSED1 和 rSED2 不能接收到撤销融合节点以及对应的监督节点命令并发送给

邻近高层；

4） rSED1 和 rSED2 不能结束融合/监督功能。

7.25.4 说明

本测试例覆盖附录 A 的部分声明项，如表 79 所示。

表 79 TC_NWK_SE25 的 PICS 声明项

PICS 声明项	描述
AFS11	APS 是否支持发起设备(网络协调器)和响应设备进行安全数据融合的撤销
NCFS14	设备是否支持接收安全数据融合撤销命令帧

附 录 A
（规范性附录）
协议实现一致性声明

A.1 NWK 安全 PICS

A.1.1 设备类型

功能设备类型(FDT)如表 A.1 所示。

PICS 表项的状态表示法如下所示：

M：必备

O：可选

O.n：可选，至少支持一组功能中的一种(n=1,2,3……)

N/A：不适用

X：禁止

表 A.1 功能设备类型(FDT)

项	描述	状态
FDT1	设备能否充当协调器	O.1
FDT2	设备能否充当路由器	O.1
FDT3	设备是否是终端设备	O.1

A.1.2 NWK 主要安全功能

A.1.2.1 NWK 安全功能

NWK 安全功能如表 A.2 所示。

表 A.2 NWK 安全功能

项	描述	引用	状态
NLFS1	NWK 是否支持邻近高层发起路由安全过程	GB/T 30269.602—2017 中 6.2.2.1、6.2.2.2、6.2.2.3	FDT1：O FDT2：M FDT3：O

A.1.2.2 NWK 安全帧

NWK 安全数据帧如表 A.3 所示。

表 A.3 NWK 安全数据帧

项	描述	引用	状态
NDFS1	设备是否支持生成安全的 NWK 数据帧，即增加了辅助帧头和信息完整性校验码的 NWK 数据帧	GB/T 30269.602—2017 中 6.3.1、6.3.2、6.3.3	FDT1：M FDT2：M FDT3：M

NWK 安全命令帧如表 A.4 所示。

表 A.4 NWK 安全命令帧

项	描述	引用	状态
NCFS1	设备是否支持接收设备标识符请求命令帧	GB/T 30269.602—2017 中 6.4.2	FDT1：M FDT2：M FDT3：M
NCFS2	设备是否支持生成设备标识符响应命令帧	GB/T 30269.602—2017 中 6.4.3	FDT1：M FDT2：M FDT3：M

A.2 APS 安全 PICS

A.2.1 设备类型

功能设备类型(FDT)如表 A.5 所示。

表 A.5 功能设备类型(FDT)

项	描述	状态
FDT1	设备是否作为协调器	O.1
FDT2	设备是否作为路由器	O.1
FDT3	设备是否是终端设备	O.1
FDT4	设备是否是信任中心	O.1

A.2.2 APS 主要安全功能

A.2.2.1 APS 安全功能

APS 功能如表 A.6 所示。

表 A.6 APS 安全功能

项	描述	引用	状态
AFS1	APS 是否支持使用信任中心分发密钥材料到其他设备	GB/T 30269.602—2017 中 7.2.2.2、7.2.2.3	FDT1:O.1 FDT2:O.1 FDT3:O.1 FDT4:M
AFS2	APS 是否支持两个设备之间建立一个共享密钥	GB/T 30269.602—2017 中 7.2.3.2、7.2.3.3、7.2.3.4、7.2.3.5	FDT1:M FDT2:M FDT3:M FDT4:O
AFS3	APS 是否支持使用信任中心去通知其他设备更换到一个新的密钥	GB/T 30269.602—2017 中 7.2.4.2、7.2.4.3	FDT1:O.1 FDT2:O.1 FDT3:O.1 FDT4:M
AFS4	APS 是否支持使用信任中心去通知相关设备撤销使用特定密钥信息	GB/T 30269.602—2017 中 7.2.5.1、7.2.5.2	FDT1:O.1 FDT2:O.1 FDT3:O.1 FDT4:M
AFS5	APS 是否支持控制用户对传感器网络的节点资源和数据资源的访问	GB/T 30269.602—2017 中 7.2.6.2、7.2.6.3、7.2.6.4	FDT1:M FDT2:M FDT3:M FDT4:N/A
AFS6	APS 是否支持两个设备之间进行身份鉴别	GB/T 30269.602—2017 中 7.2.7.2、7.2.7.3、7.2.7.4	FDT1:M FDT2:M FDT3:M FDT4:N/A
AFS7	APS 是否支持两个设备之间进行广播消息鉴别	GB/T 30269.602—2017 中 7.2.8.2、7.2.8.3、7.2.8.4	FDT1:M FDT2:M FDT3:M FDT4:N/A
AFS8	APS 是否支持发起设备(网络协调器)和响应设备(包括融合设备和监督设备)进行安全数据融合	GB/T 30269.602—2017 中 7.2.9.1、7.2.9.2、7.2.9.3、7.2.9.4	FDT1:M FDT2:M FDT3:M FDT4: O
AFS9	APS 是否支持发起设备(网络协调器)和响应设备(包括融合设备和监督设备)进行安全数据融合的撤销	GB/T 30269.602—2017 中 7.2.9.5、7.2.9.6	FDT1:M FDT2:M FDT3:M FDT4:O

A.2.2.2 APS 安全帧

APS 安全数据帧如表 A.7 所示。

表 A.7 APS 安全数据帧

项	描述	引用	状态
ADFS1	APS 是否支持生成安全的 APS 数据帧，即增加了辅助帧头和信息完整性校验码 MIC 的 APS 数据帧	GB/T 30269.602—2017 中 7.3.1、7.3.2、7.3.3	FDT1：M FDT2：M FDT3：M FDT4：M

APS 安全命令帧如表 A.8 所示。

表 A.8 APS 安全命令帧

项	描述	引用	状态
ACFS1	设备是否支持生成密钥建立命令帧	GB/T 30269.602—2017 中 7.4.1、7.4.2	FDT1：M FDT2：M FDT3：M FDT4：O
ACFS2	设备是否支持接收密钥更新命令帧	GB/T 30269.602—2017 中 7.4.3	FDT1：0.1 FDT2：0.1 FDT3：0.1 FDT4：M
ACFS3	设备是否支持接收密钥撤销命令帧	GB/T 30269.602—2017 中 7.4.4	FDT1：0.1 FDT2：0.1 FDT3：0.1 FDT4：M
ACFS4	设备是否支持生成访问控制请求命令帧	GB/T 30269.602—2017 中 7.4.5	FDT1：M FDT2：M FDT3：M FDT4：N/A
ACFS5	设备是否支持接收访问控制响应命令帧	GB/T 30269.602—2017 中 7.4.6	FDT1：M FDT2：M FDT3：M FDT4：N/A
ACFS6	设备是否支持生成身份鉴别请求命令帧	GB/T 30269.602—2017 中 7.4.7	FDT1：M FDT2：M FDT3：M FDT4：N/A
ACFS7	设备是否支持接收身份鉴别响应命令帧	GB/T 30269.602—2017 中 7.4.8	FDT1：M FDT2：M FDT3：M FDT4：N/A

表 A.8（续）

项	描述	引用	状态
ACFS8	设备是否支持生成身份鉴别响应确认命令帧	GB/T 30269.602—2017 中 7.4.9	FDT1:M FDT2:M FDT3:M FDT4:N/A
ACFS9	设备是否支持生成广播消息鉴别命令帧	GB/T 30269.602—2017 中 7.4.10	FDT1:M FDT2:M FDT3:M FDT4:N/A
ACFS10	设备是否支持生成安全数据融合启动请求命令帧	GB/T 30269.602—2017 中 7.4.11	FDT1:M FDT2:M FDT3:M FDT4:O
ACFS11	设备是否支持生成融合设备响应命令帧	GB/T 30269.602—2017 中 7.4.12	FDT1:M FDT2:M FDT3:O FDT4:O
ACFS12	设备是否支持接收监督设备符响应命令帧	GB/T 30269.602—2017 中 7.4.13	FDT1:M FDT2:O FDT3:M FDT4:O
ACFS13	设备是否支持生成安全数据融合启动请求确认命令帧	GB/T 30269.602—2017 中 7.4.14	FDT1:M FDT2:M FDT3:M FDT4:O
ACFS14	设备是否支持接收安全数据融合撤销命令帧	GB/T 30269.602—2017 中 7.4.15	FDT1:M FDT2:M FDT3:M FDT4:O

GB/T 30269.808-2018

*
书号:155066・1-61819
定价:　57.00 元