基于

基于 LTE 的车联网无线通信技术

PC5 安全协议一致性测试用例

版本:v0.6.0

生效日期:2019-08

编写:

批准:

1 | 18基于

目录

基于 ............................................... 1

前言 .................................................................................................................................................. 3

1 范围........................................................................................................................................... 3

2 引用........................................................................................................................................... 3

3 缩略语 ....................................................................................................................................... 4

4 测试系统架构 ........................................................................................................................... 5

5 PC5 通信安全测试用例 ........................................................................................................... 5

5.1

DUT 签发 SPDU 测试 ................................................................................................ 5

5.1.1

安全消息版本号信息测试 ............................................................................... 5

5.1.2

签名方式测试 ................................................................................................... 6

5.1.3

数字证书版本号信息测试 ............................................................................... 6

5.1.4

数字证书签发者信息测试 ............................................................................... 7

5.1.5

假名证书主题信息测试 ................................................................................... 7

5.1.6

应用数字证书主题信息测试 ........................................................................... 8

5.1.7

数字证书主题属性信息测试 ........................................................................... 9

5.1.8

假名证书有效性限定信息测试 ....................................................................... 9

5.1.9

应用证书有效性限定信息测试 ..................................................................... 10

5.1.10 数字证书签名信息测试 ................................................................................. 10

5.1.11 待签数据头信息测试 ..................................................................................... 11

5.1.12 待签数据内容测试 ......................................................................................... 11

5.1.13 安全消息签名信息测试 ................................................................................. 12

5.1.14 签名证书父子证书一致性测试 ..................................................................... 12

5.1.15 签名证书证书链测试 ..................................................................................... 13

5.2

DUT 验签 SPDU 测试 .............................................................................................. 14

5.2.1

基于假名证书签名的 SPDU 信息解析测试 .................................................. 14

5.2.2

基于应用证书签名的 SPDU 信息解析测试 .................................................. 14

5.2.3

包含可选参数的 SPDU 信息解析测试 .......................................................... 15

5.3

安全消息验证测试 ................................................................................................. 15

5.3.1

安全消息版本号非法测试 ............................................................................. 15

5.3.2

待签数据产生时间非法测试 ......................................................................... 16

5.3.3

待签数据杂凑算法非法测试 ......................................................................... 17

5.3.4

待签数据应用信息非法测试 ......................................................................... 17

5.3.5

安全消息签名信息非法测试 ......................................................................... 18

2 | 18基于

前言

本部分起草单位:中国信息通信研究院、东软集团股份有限公司。

1 范围

该本部分规定了基于LTE的车联网无线通信技术通信安全检测方法,对基于LTE的车联网

PC5通信安全的检测参数与指标、检测方法、检测规则进行了规范。

本部分适用于测试服务提供商,终端厂商以及测试仪表制造商。

2 引用

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,仅所注日期的版本

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。

1) GB/T 37376-2019 交通运输 数字证书格式

2) GB/T 37374-2019 智能交通 数字证书应用接口规范

3) 2018-0173T-YD 基于LTE的车联网无线通信技术总体技术要求

4) 3GPP TS 33.210 3G安全;网络域安全;IP网络层安全(3G security; Network

Domain Security (NDS); IP network layer security)

5) 3GPP TS 33.223 通用认证架构;通用引导架构推送功能(Generic Authentication

Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push

function)

6) 3GPP TS 33.246 3G安全;多媒体广播/多播业务(3G Security; Security of

Multimedia Broadcast/Multicast Service (MBMS))

7) IEEE Std 1363 IEEE公钥加密标准规范 (IEEE Standard Specifications for

Public-Key Cryptography)

8) IEEE Std 1363a IEEE公钥加密标准规范 - 修正1:附加技术(IEEE Standard

Specifications for Public-Key Cryptography — Amendment 1: Additional

Techniques)

9) IEEE Std 1609.2-2016 IEEE车载环境无线接入标准 应用和管理消息的安全服务

(IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—

Security Services for Applications and Management Messages)

10) IETF RFC 5639椭圆曲线密码(ECC)Brainpool标准曲线和曲线生成(Elliptic

Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation)

11) FIPS-197 先进的加密标准(ADVANCED ENCRYPTION STANDARD)

12) FIPS PUB 180 安全散列标准(SECURE HASH STANDARD)

13) FIPS PUB 186-4 数字签名标准 (Digital Signature Standard)

14) GM/T 0002 SM4分组密码算法

15) GM/T 0003 SM2椭圆曲线公钥密码算法

16) GM/T 0004 SM3密码杂凑算法

3 | 18基于

17) GM/T 0015 基于SM2密码学算法的数字证书格式规范

18) NIST SP 800-38C 分组密码操作模式的建议:用于认证和机密性的 CCM模式

(Recommendation for Block Cipher Modes of Operation: the CCM Mode for

Authentication and Confidentiality)

3 缩略语

缩略语 全称 中文释义

TS Test System 测试系统

TTCN-3 Testing and Test Control Notation-3 测试与测试控制第三版

DUT Device Under Test 被测实体

AID Application ID 应用标识

DSM Dedicated Short Message 专用短消息

DSMP Dedicated Short Message Protocol 专用短消息协议

LTE Long Term Evolution 长期演进技术

LTE-V2X LTE Vehicle to Everything 基于 LTE 的车用无线通信技术

AA Authorization Authority 授权机关

CA Certificate Authority 证书管理机构

EA Enrollment Authority 注册机构

EM Equipment Manufacturer 设备生产厂商

SPDU Secured Protocol Data Unit 安全协议数据单元

4 | 18基于

4 测试系统架构

基于LTE的车联网无线通信测试系统架构如图 1所示。测试系统主要由PC主机和系统模

拟器两个部分组成,二者通过以太网进行通信。

PC主机是测试系统中的上位机,实现设备运行、系统自检以及TTCN-3可执行测试用例的

运行,并且可通过相关命令接口对被测终端实现自动化测试及控制;

系统模拟器上实现基于LTE的车联网无线通信技术的底层协议栈功能,系统模拟器与终

端之间通过空口进行通信。

测试系统如需被测实体反馈测试过程中相关测试状态或测试结果信息,被测实体通过以

太网反馈相关信息。

图 1 测试系统架构

注 1:被测实体可以是 OBU 或者 RSU 中任何一种。

5 PC5 通信安全测试用例

5.1 DUT 签发 SPDU 测试

5.1.1 安全消息版本号信息测试

|  |  |
| --- | --- |
| 测试编号: | TC\_SPDU\_TS\_BV\_01 |
| 测试项目: | DUT 签发 SPDU 测试 |
| 测试目的: | 验证 DUT 产生的 SPDU 中安全消息版本号信息是否正确 |
| 预置条件: | 1) DUT 已加电启动;  2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;  3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;  4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;  5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;  6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。 |
| 测试结构: | 参见图 1 测试系统架构 |
| 测试步骤: | 步骤1:配置DUT发送SPDU消息;  步骤2:验证DUT发送的SPDU是否可OER正确编码;  步骤3:验证DUT发送的SPDU消息中安全消息版本号信息是否正确。 |
| 预期结果: | 步骤2中,TS接收到的SPDU可以OER正确解码;  步骤3中,SPDU消息结构正确,且SecureMessage.version值为2。 |

5.1.2 签名方式测试

测试编号:TC\_SPDU\_TS\_BV\_02

测试项目:DUT 签发 SPDU 测试

测试目的:验证 DUT 产生的 SPDU 中签名方式是否正确

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT发送SPDU消息;

步骤2:验证DUT发送的SPDU是否可OER正确编码;

步骤3:验证DUT发送的SPDU消息中签名方式测试是否正确。

预期结果:

步骤2中,TS接收到的SPDU可以OER正确解码;

步骤3中,SPDU消息结构正确,且签名方式测试为:包含1个数字证书的签名方式。

5.1.3 数字证书版本号信息测试

测试编号:TC\_SPDU\_TS\_BV\_03

测试项目:DUT 签发 SPDU 测试

测试目的:验证 DUT 产生的 SPDU 中数字证书的版本号信息是否正确

预置条件:

1) DUT 已加电启动;

6 | 18基于

2)

3)

4)

5)

6)

DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT发送SPDU消息;

步骤2:验证DUT发送的SPDU是否可OER正确编码;

步骤3:验证DUT发送的SPDU消息中数字证书的版本号信息是否正确。

预期结果:

步骤2中,TS接收到的SPDU可以OER正确解码;

步骤3中,SPDU消息结构正确,且Certificate.version值为2。

5.1.4 数字证书签发者信息测试

测试编号:TC\_SPDU\_TS\_BV\_04

测试项目:DUT 签发 SPDU 测试

测试目的:验证 DUT 产生的 SPDU 中数字证书的签发者信息是否有效

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT发送SPDU消息;

步骤2:验证DUT发送的SPDU是否可OER正确编码;

步骤3:验证DUT发送的SPDU消息中数字证书的签发者信息是否有效。

预期结果:

步骤2中,TS接收到的SPDU可以OER正确解码;

步骤3中,SPDU消息结构正确,且签名者信息满足如下要求:

 签发者签名算法为SM3;

 签名杂凑值长度为8字节;

 签发者有效可信。

5.1.5 假名证书主题信息测试

测试编号:TC\_SPDU\_TS\_BV\_05

测试项目:DUT 签发 SPDU 测试

7 | 18基于

测试目的:验证 OBU 类型的 DUT 产生的 SPDU 中数字证书主题信息是否正确

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT发送通过假名证书签名的SPDU消息;

步骤2:验证DUT发送的SPDU是否可OER正确编码;

步骤3:验证DUT发送的SPDU消息中假名证书主题信息是否正确。

预期结果:

步骤2中,TS接收到的SPDU可以OER正确解码;

步骤3中,SPDU消息结构正确,且假名证书主题信息满足如下要求:

 主题类型为:pseudonymTicket;

 主题名称参数长度合规,PCA生成的8字节随机数。

5.1.6 应用数字证书主题信息测试

测试编号:TC\_SPDU\_TS\_BV\_06

测试项目:DUT 签发 SPDU 测试

测试目的:验证 RSU 类型的 DUT 产生的 SPDU 中数字证书主题信息是否正确

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT发送通过应用证书签名的SPDU消息;

步骤2:验证DUT发送的SPDU是否可OER正确编码;

步骤3:验证DUT发送的SPDU消息中应用证书主题信息是否正确。

预期结果:

步骤2中,TS接收到的SPDU可以OER正确解码;

步骤3中,SPDU消息结构正确,且假名证书主题信息满足如下要求:

 主题类型为:authorizationTicket;

 主题名称参数长度合规。

8 | 18基于

5.1.7 数字证书主题属性信息测试

测试编号:TC\_SPDU\_TS\_BV\_07

测试项目:DUT 签发 SPDU 测试

测试目的:验证 DUT 产生的 SPDU 中数字证书主题属性信息是否正确

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT发送SPDU消息;

步骤2:验证DUT发送的SPDU是否可OER正确编码;

步骤3:验证DUT发送的SPDU消息中数字证书主题属性信息是否正确。

预期结果:

步骤2中,TS接收到的SPDU可以OER正确解码;

步骤3中,SPDU消息结构正确,且数字证书主题属性信息满足如下要求:

 签名公钥算法为SM2;

 verificationKey字段:公钥选用压缩后填充,

 verificationKey内的ECCPoint 在证书生成时根据压缩计算结果的奇

偶校验值具体选择。奇数选择compressed-y-0,偶数选取compressed-

y-1。

5.1.8 假名证书有效性限定信息测试

测试编号:TC\_SPDU\_TS\_BV\_08

测试项目:DUT 签发 SPDU 测试

测试目的:验证 OBU 类型的 DUT 产生的 SPDU 中数字证书有效性限定信息是否正确

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT发送通过假名证书签名的SPDU消息;

步骤2:验证DUT发送的SPDU是否可OER正确编码;

9 | 18基于

步骤3:验证DUT发送的SPDU消息中数字证书有效性限定信息是否正确。

预期结果:

步骤2中,TS接收到的SPDU可以OER正确解码;

步骤3中,SPDU消息结构正确,且数字证书有效期限信息中包含合法的证书起始时

间和证书截止时间,时限不超过1周。

5.1.9 应用证书有效性限定信息测试

测试编号:TC\_SPDU\_TS\_BV\_09

测试项目:DUT 签发 SPDU 测试

测试目的:验证 RSU 类型的 DUT 产生的 SPDU 中数字证书有效性限定信息是否正确

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT发送通过应用证书签名的SPDU消息;

步骤2:验证DUT发送的SPDU是否可OER正确编码;

步骤3:验证DUT发送的SPDU消息中数字证书有效性限定信息是否正确。

预期结果:

步骤2中,TS接收到的SPDU可以OER正确解码;

步骤3中,SPDU消息结构正确,且数字证书有效期限信息中包含合法的证书起始时

间和证书截止时间,时限不超过1周。

5.1.10 数字证书签名信息测试

测试编号:TC\_SPDU\_TS\_BV\_10

测试项目:DUT 签发 SPDU 测试

测试目的:验证 DUT 产生的 SPDU 中数字证书签名信息是否正确

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

10 | 18基于

步骤1:配置DUT发送SPDU消息;

步骤2:验证DUT发送的SPDU是否可OER正确编码;

步骤3:验证DUT发送的SPDU消息中数字证书签名信息是否正确。

预期结果:

步骤2中,TS接收到的SPDU可以OER正确解码;

步骤3中,SPDU消息结构正确,且签名信息满足如下要求:

 签名算法为SM2

 签名值正确。

5.1.11 待签数据头信息测试

测试编号:TC\_SPDU\_TS\_BV\_11

测试项目:DUT 签发 SPDU 测试

测试目的:验证 DUT 产生的 SPDU 中待签数据头信息是否正确

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT发送SPDU消息;

步骤2:验证DUT发送的SPDU是否可OER正确编码;

步骤3:验证DUT发送的SPDU消息中待签数据头信息是否正确。

预期结果:

步骤2中,TS接收到的SPDU可以OER正确解码;

步骤3中,SPDU消息结构正确,且待签数据信息满足如下要求:

 待签数据头信息中包含itsAid信息,且aid值与网络层AID值相同;

 擦凑算法为SM3;

 消息产生时间有效。

5.1.12 待签数据内容测试

测试编号:TC\_SPDU\_TS\_BV\_12

测试项目:DUT 签发 SPDU 测试

测试目的:验证 DUT 产生的 SPDU 中待签数据内容是否正确

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

11 | 18基于

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT发送SPDU消息;

步骤2:验证DUT发送的SPDU是否可OER正确编码;

步骤3:验证DUT发送的SPDU消息中待签数据内容是否正确。

预期结果:

步骤2中,TS接收到的SPDU可以OER正确解码;

步骤3中,SPDU消息结构正确,且待签数据内容与TS配置的内容一致。

5.1.13 安全消息签名信息测试

测试编号:TC\_SPDU\_TS\_BV\_13

测试项目:DUT 签发 SPDU 测试

测试目的:验证 DUT 产生的 SPDU 中安全消息签名信息是否正确

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT发送SPDU消息;

步骤2:验证DUT发送的SPDU是否可OER正确编码;

步骤3:验证DUT发送的SPDU消息中安全消息签名信息是否正确。

预期结果:

步骤2中,TS接收到的SPDU可以OER正确解码;

步骤3中,SPDU消息结构正确,且签名信息满足如下要求:

 签名算法为SM2

 签名值正确(待签数据OER编码后的密码杂凑值&签名者证书OER编码

后的密码杂凑值合并值)。

5.1.14 签名证书父子证书一致性测试

测试编号:TC\_SPDU\_TS\_BV\_14

测试项目:DUT 签发 SPDU 测试

测试目的:验证 DUT 产生的 SPDUT 中签名证书的父子证书一致性是否正确

预置条件:

12 | 18基于

1)

2)

3)

4)

5)

6)

DUT 已加电启动;

DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT发送SPDU消息;

步骤2:验证DUT发送的SPDU是否可OER正确编码;

步骤3:验证DUT发送的SPDU消息中签名证书的父子证书一致性是否正确。

预期结果:

步骤2中,TS接收到的SPDU可以OER正确解码;

步骤3中,SPDU消息结构正确,且子证书的有效时间范围是发布证书的有效时间范

围的子集。

5.1.15 签名证书证书链测试

测试编号:TC\_SPDU\_TS\_BV\_15

测试项目:DUT 签发 SPDU 测试

测试目的:验证 DUT 产生的 SPDU 中签名证书证书链是否有效

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT发送SPDU消息;

步骤2:验证DUT发送的SPDU是否可OER正确编码;

步骤3:验证DUT发送的SPDU消息中签名证书证书链是否有效。

预期结果:

步骤2中,TS接收到的SPDU可以OER正确解码;

步骤3中,SPDU消息结构正确,且证书链满足如下要求:

 可以在该证书和可信证书之间构建证书链

 可信证书必须是有效证书

 所有的有效证书必须由有效证书发布

 证书链中前一个证书是后一个证书的发布证书。

13 | 18基于

5.2 DUT 验签 SPDU 测试

5.2.1 基于假名证书签名的 SPDU 信息解析测试

测试编号:TC\_SPDU\_RV\_BV\_01

测试项目:DUT 验签 SPDU 测试

测试目的:验证 DUT 是否正确解析 TS 产生的基于假名证书的签名的 SPDU 消息

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT接收SPDU消息;

步骤2:TS发送基于假名证书的签名的SPDU消息;

步骤3:验证DUT是否接收到SPDU消息;

步骤4:验证DUT针对接收的SPDU消息的有效性判断是否正确;

步骤5:验证DUT接收到的待签数据信息是否正确。

预期结果:

步骤3中,DUT接收到TS发送的SPDU消息

步骤4中,DUT判断接收到SPDU消息有效;

步骤5中,DUT接收到的待签数据信息与TS发送的内容一致。

5.2.2 基于应用证书签名的 SPDU 信息解析测试

测试编号:TC\_SPDU\_RV\_BV\_02

测试项目:DUT 验签 SPDU 测试

测试目的:验证 DUT 是否正确解析 TS 产生的基于应用证书的签名的 SPDU 消息

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT接收SPDU消息;

14 | 18基于

步骤2:TS发送基于应用证书的签名的SPDU消息;

步骤3:验证DUT是否接收到SPDU消息;

步骤4:验证DUT针对接收的SPDU消息的有效性判断是否正确;

步骤5:验证DUT接收到的待签数据信息是否正确。

预期结果:

步骤3中,DUT接收到TS发送的SPDU消息

步骤4中,DUT判断接收到SPDU消息有效;

步骤5中,DUT接收到的待签数据信息与TS发送的内容一致。

5.2.3 包含可选参数的 SPDU 信息解析测试

测试编号:TC\_SPDU\_RV\_BV\_02

测试项目:DUT 验签 SPDU 测试

测试目的:验证 DUT 是否正确解析包含可选参数的 SPDU 信息

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT接收SPDU消息;

步骤2:TS发送包含了可选参数的SPDU消息;

步骤3:验证DUT是否接收到SPDU消息;

步骤4:验证DUT针对接收的SPDU消息的有效性判断是否正确;

步骤5:验证DUT接收到的待签数据信息是否正确。

预期结果:

步骤3中,DUT接收到TS发送的SPDU消息

步骤4中,DUT判断接收到SPDU消息有效;

步骤5中,DUT接收到的待签数据信息与TS发送的内容一致。

5.3 安全消息验证测试

5.3.1 安全消息版本号非法测试

测试编号:TC\_SPDU\_RV\_BI\_01

测试项目:安全消息验证测试

15 | 18基于

测试目的:验证 DUT 是否能正确识别包含非法安全消息版本号的 SPDU 消息

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT接收SPDU消息;

步骤2:TS发送包含非法安全消息版本号的SPDU消息;

步骤3:验证DUT针对接收的SPDU消息的有效性判断是否正确;

步骤4:验证DUT接收到的无效SPDU消息非法原因是否正确。

预期结果:

步骤3中,DUT判断接收到SPDU消息无效;

步骤4中,DUT反馈的SPDU消息无效原因为:安全消息版本号信息错误。

5.3.2 待签数据产生时间非法测试

测试编号:TC\_SPDU\_RV\_BI\_02

测试项目:安全消息验证测试

测试目的:验证 DUT 是否正确识别包含了非法数据产生时间的 SPDU 消息

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT接收SPDU消息;

步骤2:TS发送包含了非法数据产生时间的SPDU消息;

步骤3:验证DUT针对接收的SPDU消息的有效性判断是否正确;

步骤4:验证DUT接收到的无效SPDU消息非法原因是否正确。

预期结果:

步骤3中,DUT判断接收到SPDU消息无效;

步骤4中,DUT反馈的SPDU消息无效原因为:待签数据中数据产生时间信息非法。

16 | 18基于

5.3.3 待签数据杂凑算法非法测试

测试编号:TC\_SPDU\_RV\_BI\_03

测试项目:安全消息验证测试

测试目的:验证 DUT 是否正确识别包含了非法杂凑算法的 SPDU 消息

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT接收SPDU消息;

步骤2:TS发送包含了非法杂凑算法的SPDU消息;

步骤3:验证DUT针对接收的SPDU消息的有效性判断是否正确;

步骤4:验证DUT接收到的无效SPDU消息非法原因是否正确。

预期结果:

步骤3中,DUT判断接收到SPDU消息无效;

步骤4中,DUT反馈的SPDU消息无效原因为:待签数据中杂凑算法信息非法。

5.3.4 待签数据应用信息非法测试

测试编号:TC\_SPDU\_RV\_BI\_04

测试项目:安全消息验证测试

测试目的:验证 DUT 是否正确识别包含了非法 AID 信息的 SPDU 消息

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT接收SPDU消息;

步骤2:TS发送包含了非法AID信息的SPDU消息;

步骤3:验证DUT针对接收的SPDU消息的有效性判断是否正确;

步骤4:验证DUT接收到的无效SPDU消息非法原因是否正确。

预期结果:

步骤3中,DUT判断接收到SPDU消息无效;

17 | 18基于

步骤4中,DUT反馈的SPDU消息无效原因为:待签数据中AID信息非法。

5.3.5 安全消息签名信息非法测试

测试编号:TC\_SPDU\_RV\_BI\_05

测试项目:安全消息验证测试

测试目的:验证 DUT 是否正确识别包含了非法安全签名信息(Signature)的 SPDU 消息

预置条件:

1) DUT 已加电启动;

2) DUT 已锁定了基于 GNSS 的位置,并完成与 GNSS 时钟同步;

3) DUT 或测试系统无线信号捕获工具范围内没有其他同类型设备;

4) DUT 已预置了支持 C-V2X 消息传输或接收的安全证书;

5) DUT 上运行的是基于 LTE 的车联网无线通信技术安全通信的应用;

6) DUT 除接收测试系统发出的相关指令外,DUT 不会主动发送消息。

测试结构:参见图 1 测试系统架构

测试步骤:

步骤1:配置DUT接收SPDU消息;

步骤2:TS发送包含了非法安全签名信息(Signature)的SPDU消息;

步骤3:验证DUT针对接收的SPDU消息的有效性判断是否正确;

步骤4:验证DUT接收到的无效SPDU消息非法原因是否正确。

预期结果:

步骤3中,DUT判断接收到SPDU消息无效;

步骤4中,DUT反馈的SPDU消息无效原因为:安全消息中签名信息非法。

18 | 18