

**Conformance test specifications for**

**Wireless Access in  
Vehicular Environments (WAVE) —  
Security Services**

**Test Suite Structure and Test Purposes (TSS & TP)**

|  |  |
| --- | --- |
| Document Mnemonics: | WAVE-16092-TSS&TP |
| Revision: | [V1.2] |
| Revision Date: | 4/28/2017 |

**Table of Contents**

[1 Scope 4](#_Toc459988677)

[2 References 4](#_Toc459988678)

[2.1 Normative References 4](#_Toc459988679)

[2.2 Informative References 4](#_Toc459988680)

[3 Definitions and abbreviations 5](#_Toc459988681)

[3.1 Definitions 5](#_Toc459988682)

[3.2 General Convention 5](#_Toc459988683)

[3.3 Abbreviations 5](#_Toc459988684)

[4 Prerequisites and Test Configurations 5](#_Toc459988685)

[4.1 Test Configurations 5](#_Toc459988686)

[4.1.1 Global Test Parameters: 6](#_Toc459988687)

[4.1.2 SPDUBSM Global Test Parameters 6](#_Toc459988688)

[4.1.3 SPDUWSA Global Test Parameters 8](#_Toc459988689)

[4.2 Feature Restriction and Pre-Enrolment 10](#_Toc459988690)

[4.2.1 Feature Restriction 10](#_Toc459988691)

[4.3 States in Initial Conditions 10](#_Toc459988692)

[4.3.1 Conditions for the Initial State 10](#_Toc459988693)

[5 Test Suite Structure (TSS) 11](#_Toc459988694)

[5.1 Structure for security tests 11](#_Toc459988695)

[5.2 Test groups 11](#_Toc459988696)

[5.2.1 Root 12](#_Toc459988697)

[5.2.2 Groups 12](#_Toc459988698)

[5.2.3 Sub-Groups 12](#_Toc459988699)

[5.2.4 Categories 12](#_Toc459988700)

[6 Test Purposes (TP) 12](#_Toc459988701)

[6.1 Introduction 12](#_Toc459988702)

[6.1.1 TP definition conventions 12](#_Toc459988703)

[6.1.2 TP Identifier naming conventions 13](#_Toc459988704)

[6.1.3 Rules for the behaviour description 13](#_Toc459988705)

[6.1.4 References 13](#_Toc459988706)

[6.1.5 PICS selection and mnemonics for reference 13](#_Toc459988707)

[6.1.6 Mnemonics for PICS reference 14](#_Toc459988708)

[6.1.7 Sources of TP definitions 14](#_Toc459988709)

[6.1.8 Secure Protocol Data Unit for Basic Safety Messages (SPDUBSM) 15](#_Toc459988710)

[6.1.9 Secure Protocol Data Unit for WAVE Service Advertisements Messages (SPDUWSA) 23](#_Toc459988711)

[7 Messages and information element content 29](#_Toc459988712)

[7.1 Secure Protocol Data Uunit for Basic Safety message (SPDUBSM) 29](#_Toc459988713)

[7.1.1 SPDUBSM defaults 29](#_Toc459988714)

[7.1.2 SPDUBSM Message Details 29](#_Toc459988715)

[7.1.3 SPDUBSM Security Header information 29](#_Toc459988716)

[7.1.4 SPDUBSM Signed with Certificate Digest 30](#_Toc459988717)

[7.1.5 SPDUBSM Signed with Implicit Certificate 30](#_Toc459988718)

[7.1.6 SPDUBSM Security Signature 31](#_Toc459988719)

[7.1.7 SPDUWSA Message Details 31](#_Toc459988720)

[7.1.8 SPDUWSA Security Header information 31](#_Toc459988721)

[7.1.9 SPDUWSA Signed with Implicit Certificate 32](#_Toc459988722)

[7.1.10 SPDUWSA Signed with Certificate Digest 33](#_Toc459988723)

[7.1.11 SPDUWSA Security Signature 33](#_Toc459988724)

[Appendix A: 34](#_Toc459988725)

[Traceability Matrix 34](#_Toc459988726)

[8 Revision History 43](#_Toc459988727)

# Scope

The scope of this document provides Test Suite Structure (TSS) and Test Purposes (TP’s) for WAVE Security Services as defined in IEEE 1609.2 [8]. Furthermore, the document defines a set of Test Purposes including Test Descriptions and the structure for the Test Suite. The TP’s covers the Security Services requirements for BSM as specified SAE J2945/1 [1] and WSA as specified in IEEE 1609.3 [5]. The ISO standard for the methodology of conformance testing (ISO/IEC 9646‑1 [3] and ISO/IEC 9646‑2 [4]) as well as the ETSI rules for conformance testing (ETS 300 406 [7]) are used as a basis for the test methodology.

# References

## Normative References

The following referenced documents are necessary for the application of the present document.

[1] SAE J2945/1 MAR2016: “Surface Vehicle Standard - On-board System Requirements for V2V Safety Communications”

[2] IEEE Std. 1609.12-2016 “IEEE Standard for Wireless Access in Vehicular Environments – Identifier Allocations”

[3] ISO/IEC 9646-1 (1994): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework - Part 1: General concepts".

[4] ISO/IEC 9646-2 (1994): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 2: Abstract Test Suite specification".

[5] IEEE Std 1609.3-2016 “IEEE Standard for Wireless Access in Vehicular Environments (WAVE) — Network Services”.

[6] ISO/IEC 9646-7 (1995): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".

[7] ETSI ETS 300 406 (1995): "Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

[8] IEEE Std. 1609.2-2016: "IEEE Standard for Wireless Access in Vehicular Environments - security Services for Applications and Management Messages".

## Informative References

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI EG 202 798 (V1.1.1): "Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperability testing".

# Definitions and abbreviations

## Definitions

For the purposes of the present document, the terms and definitions given in IEEE 1609.2 [8] , ISO/IEC 9646‑1 [3] and in ISO/IEC 9646‑7 [6] apply.

## General Convention

***Parameters*** and ***its value*** defined in SAE J2945/1 [1], IEEE 1609.12 [2], IEEE 1609.3 [5] and IEEE 1609.2 [8] used in this document are donated as **BOLD** and *ITALIC.*

## Abbreviations

For the purposes of the present document, the following abbreviations apply:

BSM Basic Safety Message

BI Behaviour Invalid

BV Behaviour Valid

CERTCH Change Certificate

CA Certificate Authority

EA Enrolment Authority

ITS Intelligent Transport Systems

IUT Implementation Under Test

TC Test Configuration System

TP Test Purposes

TS Test System

TSS Test Suite Structure

PSID Provider Service Identifier

PDU Protocol Data Unit

SPDU Secure Protocol Data Unit.

WAVE Wireless Access in Vehicular Environments

WME WAVE Management Entity

WSM WAVE Short Message

WSA WAVE Service Advertisement Message

SEND Send message

SPDUBSM Represents a BSM with security credentials as per IEEE 1609.2 Standard

SPDUWSA Represents a WSA with security credentials as per IEEE 1609.2 Standard

SUT System Under Test

RECV Receive message

16092 Security Credentials

# Prerequisites and Test Configurations

## Test Configurations

This clause introduces the test configurations that is used to run the conformance testing for these definition of test purposes. These tests will be run in a lab environment in an automated fashion and controlled by the test system as shown in figure (1). The test configurations cover the various scenarios of the IEEE 1609.2 [8] test purposes.



WAVE

Host



IUT

TS

TS control interface

Figure 1: TC (1) Test Configuration System

### Global Test Parameters:

Default value parameters listed in this section will be used as a global test system parameters. These values are selected based on BSM and WSA relevant security profiles as indicated in the reference column for each value.

### SPDUBSM Global Test Parameters

Below are listed global test parameters / conditions that are applicable to all SPDUBSM test cases in this specification[[1]](#footnote-1).

#### Value for crlSeries Parameters:

Select the default values for ***crlSeries***according to the following table.

Table 4‑1: *CrlSeries*

| **Parameter Name** | **Range of Values** | **Default** | **Reference** |
| --- | --- | --- | --- |
| *crlSeries* | ***Unit16 -***  any positive integer value in the range of (0..65535)) | *1* | [8]  section 5.1.3 |

#### Number of psid included in the certificate:

Select the default value for psid according to the following table. While PSID is p-encoded in WSM headers [5], it is encoded as a hex value according to [2] in security headers and in permissions in certificates used in [8].

Table 4‑2: *psid*

| **Parameter Name** | **Range of Values (p-encoded)** | **Default** | **Reference** |
| --- | --- | --- | --- |
| *psid* | *1byte PSID: 0p00 to 0p7F*  *2byte PSID: 0p80-00 to 0pBF-FF*  *3byte PSID: 0pC0-00-00 to 0pDF-FF-FF*  *4byte PSID: 0pE0-00-00-00 to 0pEF-FF-FF-FF* | BSM messages include certificates containing psid  0x20 “BSM”  0x26 “Misbehaviour for common applications.”  WSA messages include certificates containing psid  0x87 “WSA” | [2]  Section “4.1.3“  Table 2 |

#### duration Life Time Unit:

Select the default value for ***duration*** according to the following table.

Table 4‑3: *duration life time unit*

| **Parameter Name** | **Range of Values** | **Default** | **Reference** |
| --- | --- | --- | --- |
| *duration* | *microseconds*  *milliseconds*  *seconds*  *minutes*  *hours*  *sixtyHours*  *years* | *hours* | [8]  Section “D.5.2.3” |

#### reconstructionValue:

Select the default value for ***reconstructionValue*** default value according to the following table.

Table 4‑4: *reconstructionValue*

| **Parameter Name** | **Range of Values** | **Default** | **Reference** |
| --- | --- | --- | --- |
| *reconstructionValue* | *x-only*  *fill*  *compressed-y-0*  *compressed-y-1*  *uncompressed* | *compressed-y-0 or compressed-y-1* | [8]  Section “D.5.2.3” |

#### signature type:

Select the default value for ***signature*** according to the following table.

Table 4‑5: *signature*

| **Parameter Name** | **Range of Values** | **Default** | **Reference** |
| --- | --- | --- | --- |
| *signature* | *ecdsaNistP256Signature*  *ecdsaBrainpoolP256r1Signature* | *ecdsaNistP256Signature* | [8]  Section “5.3.1” |

#### “r” default value:

Select the default value for ***r*** according to the following table.

Table 4‑6: *“r” value*

| **Parameter Name** | **Range of Values** | **Default** | **Reference** |
| --- | --- | --- | --- |
| *r* | *x-only*  *fill*  *compressed-y-0*  *compressed-y-1*  *uncompressed* | *compressed-y-0*  *or*  *compressed-y-1* | [8]  Section “D.5.2.3” |

#### Other Default values:

Select the default value for the parameter names listed on Table 4-10. The values for the parameter names listed on table 4-10 were obtained from

Table 4‑7: *default values*

| **Parameter Name** | **Value** | **Reference** |
| --- | --- | --- |
| *vMaxCertDigestInterval* | 450 milliseconds | [1]  Section “7” Table 21 |
| *+/-DE\_DSecond/2* | 30 Seconds | [1]  Section “6.1.2.2.3” Table 11 |
| *vCertChangeInterval* | 5 minutes | [1]  Section “7” Table 21 |

### SPDUWSA Global Test Parameters

Below are listed global test parameters and conditions that are applicable to all SPDUWSA test cases in this specification[[2]](#footnote-2).

#### id default value:

Select the default value for ***id***according to the following table

Table 4‑8: *id*

| **Parameter Name** | **Range of Values** | **Default** | **Reference** |
| --- | --- | --- | --- |
| *id* | *name*  *binaryId*  *none* | *none* | [8]  Section “ 5.1.3” |

#### Value for cracaId & crlSeries Parameters:

Select the default values for ***cracaId*** *&* ***crlSeries*** according to the following table.

Table 4‑9: *cracaId & CrlSeries*

| **Parameter Name** | **Range of Values** | **Default** | **Reference** |
| --- | --- | --- | --- |
| *cracaId* | *Octet String size(3)* | *0* | [8]  Section “5.1.1.3“ |
| *crlSeries* | *Integer (0 . . 65535)* | *0* |

#### duration Life Time Unit:

Select the default value for ***duration*** according to the following table.

Table 4‑10: *duration life time unit*

| **Parameter Name** | **Range of Values** | **Default** | **Reference** |
| --- | --- | --- | --- |
| *duration* | *microseconds*  *milliseconds*  *seconds*  *minutes*  *hours*  *sixtyHours*  *years* | *minutes* | [8] |

#### Certificate region type:

Select the default value for ***region*** according to the following table.

Table 4‑11: *region*

| **Parameter Name** | **Range of Values** | **Default** | **Reference** |
| --- | --- | --- | --- |
| *region* | *none*  *identified*  *circularRegion* | *circularRegion* | [5]  Annex “H” Table H.1.1.4 |

#### reconstructionValue:

Select the default value for ***reconstructionValue*** according to the following table.

Table 4‑12: *reconstructionValue*

| **Parameter Name** | **Range of Values** | **Default** | **Reference** |
| --- | --- | --- | --- |
| *reconstructionValue* | *x-only*  *fill*  *compressed-y-0*  *compressed-y-1*  *uncompressed* | *compressed-y-0*  *or*  *compressed-y-1* | [8]  Section “D.5.2.3” |

#### signature type:

Select the default value for ***signature*** according to the following table.

Table 4‑13: *signature*

| **Parameter Name** | **Range of Values** | **Default** | **Reference** |
| --- | --- | --- | --- |
| *signature* | *ecdsaNistP256Signature*  *ecdsaBrainpoolP256r1Signature* | *ecdsaNistP256Signature* | [8]  Section “5.3.1” |

#### “r” default value:

Select the default value for ***r*** parameter according to the following table.

Table 4‑14: *r* default value

| **Parameter Name** | **Range of Values** | **Default** | **Reference** |
| --- | --- | --- | --- |
| *r* | *x-only*  *fill*  *compressed-y-0*  *compressed-y-1*  *uncompressed* | *compressed-y-0*  *or*  *compressed-y-1* | [5]  Annex “H”  Table H.1.1.4 |

## Feature Restriction and Pre-Enrolment

### Feature Restriction

In this clause all feature restrictions are listed:

* Encrypted PDUs are not considered
* Decrypting encrypted SPDUs are not considered.
* Peer to peer certificate distribution (P2PCD) is not considered
* Service Access Points (SAPs) are not considered.
* Certificate Revocation List (CRL) Verification Entity is not considered.

## States in Initial Conditions

The description of the TP is built according to EG 202 798 [i.1].

Test purposes use a generic "Initial State" that corresponds to a state where the IUT is ready for starting the test execution. Furthermore, the IUT shall be left in this "Initial State", when the test is completed.

Being in the "Initial State" refers to the starting point of the initial device configuration. There are no pending actions, no instantiated buffers or variables, which could disturb the execution of a test.

### Conditions for the Initial State

Figure 2 depicts the overall state diagram for a test system below.

State 2

IUT is in “Initial State”

State 1

IUT is powered off

State 3

Test Purpose Initial Conditions/Pre-test Conditions

State 4

Test Execution

Figure 2: State Diagram

Each TP contains an initial condition. The initial condition defines the initial state in which the IUT has to be to apply the actual TP. Most of the TPs start from the “initial state” which is defined as follows:

* The IUT is powered up.
* The IUT is not transmitting or receiving messages
* The IUT is provisioned with the appropriate security credentials to enable transmission or reception of messages. That is, the IUT is configured with a valid signer credentials (certificate) as specified in SAE J2945/1 [1] and IEEE 1609.3 [5] security profiles for BSM and WSA.

Some TPs start from a different initial condition which is explicitly defined in the TP such as if an invalid behavior needs to be tested by the IUT. However, the “initial state” defined above is the starting point before the different initial conditions are established.

When the execution of the initial condition does not succeed, it leads to the assignment of an Inconclusive verdict.

# Test Suite Structure (TSS)

## Structure for security tests

The test suite is structured as a tree with the root defined as 16092. The tree is of rank 4 with the first rank is Root, 16092 second is Group, third is Sub-group and the fourth rank is the standard ISO conformance test categories. The Sub-Group (third rank) belongs to any Group member in the second rank.

## Test groups

The test suite has a total of four levels. The first level is the root. The second level separates the root into various functional areas. The third level is the sub‑functional areas if necessary. The fourth level is the standard ISO conformance test categories.

### Root

The root identifies the 1609.2 protocol given in IEEE 1609.2 [8].

### Groups

This level contains two message types identified as:

SPDUBSM

SPDUWSA

### Sub-Groups

This level contains functional areas identified in Table 5‑1.

Table 5‑1: Functional areas

|  |  |
| --- | --- |
| **Functional areas** | **Description** |
| Send/Transmit | The IUT signs and transmit WSM |
| Receive | The IUT receive and verifies WSM |
| Change Certificate | The IUT changes the signing certificate for BSM as per 2945/1 requirement |

### Categories

This level contains the standard ISO conformance test categories limited to the behaviour valid event and behaviour invalid event.

# Test Purposes (TP)

## Introduction

### TP definition conventions

A Test Purpose (TP) is a prose description of a well-defined objective of testing. Applying to conformance testing, it focuses on a single conformance requirement or a set of related conformance requirements from the base standards [i.1]..The TP definition is built according to EG 202 798 [i.1].

The TPs are defined by the rules shown in Table 6‑1.

Table 6‑1: TP definition rules

|  |  |
| --- | --- |
| Test Purpose ID | The Test Purpose ID is a unique identifier. It shall be specified according to the TP naming conventions defined in the clause below. |
| Test objective | Short description of test purpose objective according to the requirements from the base standard. |
| References | The reference indicates the sub-clauses of the reference standard specifications in which the conformance requirement is expressed. |
| Test Configuration | The Config Id references the test configuration selected for this TP. |
| PICS Selection | Reference to the PICS statement involved for selection of the TP. It may contain a Boolean expression. |
| Pre-Test Conditions | A list of test specific pre-conditions that need to be met by the SUT including information about equipment configuration, i.e. precise description of the initial state of the SUT required to start executing the test sequence |
| Test Sequence | An ordered list of equipment operation and observations. In case of a conformance test description the test sequence contains also the conformance checks as part of the observations |
| **Event Types** | |
| Stimulus | Corresponds to an event that enforces an IUT to proceed with a specific protocol action, like sending a message for instance. |
| Check | Ensures the receipt of protocol messages on reference points with valid content. |
| Verify | Consists of verifying that the IUT behaves according to the expected behavior (for instance the IUT behavior shows that it receives the expected message). |
| Configure | Corresponds to an action to modify the IUT configuration. |

When a conformance test has a sequencing requirement, these are described using a format in the table 3 derived from [i.1]

### TP Identifier naming conventions

The identifier of the TP is built according to Table 6‑2.

Table 6‑2:TP naming convention

| **Identifier** | **TP-<root>-<gr>-<sgr>-<x>-<nn> or TP-<root>-<gr>-<x>-<nn> when no <sgr>** |  |  |
| --- | --- | --- | --- |
|  | <root> = root | 16092 | 1609.2 |
|  | <gr> = group | SPDUBSM | Secure Basic Safety Message |
|  |  | SPDUWSA | Secure Wave Service Advertisement message |
|  | <sgr> =sub- group | SEND | Send Message |
|  |  | RECV | Receive Message |
|  |  | CERTCH | Change Certificate |
|  | <x> = type of testing | BV | Valid Behaviour tests |
|  |  | BI | Invalid Syntax or Behaviour Tests |
|  | <nn> = sequential number |  | 01 to 99 |

### Rules for the behaviour description

The description of the TP is built according to EG 202 798 [i.1].

The base standards are not using finite state machine concept. As consequence, the test purposes use a generic "Initial State" that corresponds to a state where the IUT is ready for starting the test execution. Furthermore, the IUT shall be left in this "Initial State", when the test is completed.

Being in the "Initial State" refers to the starting point of the initial device configuration. There are no pending actions, no instantiated buffers or variables, which could disturb the execution of a test.

### References

All Test Purposes are derived from requirements defined in 1609.2 [8]. Traceability between TPs and sub-clauses of referenced standard specifications is established in Table A- 1 for BSM and Table A-2 for WSA messages. For each PICS, a reference section from 1609.2 [8] is listed and applicable test purposes are identified in the TP ID column.

### PICS selection and mnemonics for reference

Table A- 1 and Table A- 2 includes a subset of PICS defined in 1609.2 [8] with a traceability to TPs included in the TP ID column. Some TPs are directly derived from SAE J2945/1[1] requirements and do not refer to any PICS from 1609.2[8]. In this case the SAE J2945/1[1] requirement that is used to generate the test purpose is listed in the “Reference section” of the TP.

Table 6‑3 lists mnemonic names and maps them to a subset of PICS item number. This is a partial list of PICS used in selecting of certain TPs or TPs which incorporated variances.

### Mnemonics for PICS reference

The following table lists mnemonic names and maps them to the PICS item number. This is a partial list of PICS used in selecting TPs. The complete list of PICS with traceability to TPs is included in Appendix A.

Table 6‑3: Mnemonics for PICS reference

|  |  |
| --- | --- |
| **Mnemonic** | **PICS** **item** |
| PIC\_Generate\_SignedData | [8] Annex A, S1.2.2 |
| PIC\_Generate\_Using\_Valid\_HashAlgorithm | [8] Annex A, S1.2.2.1 |
| PIC\_Generate\_Signing\_With\_SHA256 SHA-256 | [8] Annex A, S1.2.2.1.1 |
| PIC\_Generate\_Signed\_Data\_payload | [8] Annex A, S1.2.2.2 |
| PIC\_Generate\_With\_Payload\_Containing\_Data | [8] Annex A, S1.2.2.2.1 |
| PIC\_Generate\_With\_generationTime\_In\_security\_headers headers | [8] Annex A, S1.2.2.2.3 |
| PIC\_Generate\_With\_generationLocation\_In\_security\_headers 16092urity\_Headers | [8] Annex A, S1.2.2.2.5 |
|  |  |
| PIC\_Generate\_Support\_SignerIdentifier | [8] Annex A, S1.2.2.3 |
| PIC\_Generate\_Of\_Type\_digest | [8] Annex A, S1.2.2.3.1 |
| PIC\_Generate\_Of\_Type\_certificate | [8] Annex A, S1.2.2.3.2 |
| PIC\_Generate\_Max\_Number\_Of\_Certificates\_In\_The\_chain | [8] Annex A, S1.2.2.3.2.1 |
|  |  |
| PIC\_Generate\_Signature | [8] Annex A, S1.2.2.4 |
| PIC\_Generate\_Ecdsa256\_Signature | [8] Annex A, S1.2.2.4.1 |
| PIC\_Generate\_Ecdsa256\_Signature\_Using\_ NIST p256 | [8] Annex A, S1.2.2.4.1.1 |
| PIC\_Generate\_Signature\_With\_Compressed\_r\_value | [8] Annex A, S1.2.2.4.1.5 |
| PIC\_Generate\_Support\_signing\_Implicit\_Certificate | [8] Annex A, S1.2.2.8 |
|  |  |
| PIC\_Verify\_Ieee1609DoT2Data\_Containing\_SignedData | [8] Annex A, S1.3.2 |
| PIC\_Verify\_Using\_Valid\_HashAlgorithm | [8] Annex A, S1.3.2.1 |
| PIC\_Verify\_Signing\_With\_SHA256 | [8] Annex A, S1.3.2.1.1 |
| PIC\_Verify\_Signed\_Data\_payload | [8] Annex A, S1.3.2.2 |
| PIC\_Verify\_With\_Payload\_Containing\_Data | [8] Annex A, S1.3.2.2.1 |
| PIC\_Verify\_With\_generationTime\_In\_security\_headers | [8] Annex A, S1.3.2.2.3 |
| PIC\_Verify\_With\_generationLocation\_In\_security\_headers | [8] Annex A, S1.3.2.2.5 |
|  |  |
| PIC\_Verify\_Support\_SignerIdentifier | [8] Annex A, S1.3.2.3 |
| PIC\_Verify\_Of\_Type\_digest | [8] Annex A, S1.3.2.3.1 |
| PIC\_Verify\_Of\_Type\_certificate | [8] Annex A, S1.3.2.3.2 |
| PIC\_Verify\_Max\_Number\_Of\_Certificates\_In\_The\_chain | [8] Annex A, S1.3.2.3.2.1 |
|  |  |
| PIC\_Verify\_Signature | [8] Annex A, S1.3.2.4 |
| PIC\_Verify\_ecdsa256\_Signature | [8] Annex A, S1.3.2.4.1 |
| PIC\_Verify\_ecdsa256\_Signature\_Using\_ NIST\_p256 | [8] Annex A, S1.3.2.4.1.1 |
| PIC\_Verify\_Signature\_With\_Compressed\_r\_value | [8] Annex A, S1.3.2.4.1.4 |
| PIC\_Verify\_SignedData\_fails\_if\_certificate\_is\_not\_valid | [8] Annex A, S1.3.2.5 |
| PIC \_Verify\_Reject\_data if\_certificate\_doesn’t\_have\_proper\_appPermissions | [8] Annex A, S1.3.2.5.2 |
| PIC\_Verify\_Reject\_data\_if\_generationTime\_not\_available | [8] Annex A,S 1.3.2.10.4 |
| PIC\_Verify\_Reject\_data\_if\_generationLocation\_not\_available | [8] Annex A, S1.3.2.10.5 |

### Sources of TP definitions

All TPs are specified according to IEEE 1609.2 [8] and SAE J2945/1 [1]. Test purposes for 1609.2

### Secure Protocol Data Unit for Basic Safety Messages (SPDUBSM)

#### Transmission of packets

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092- SPDUBSM-SEND-BV-01 | |
| **Summary** | | Validate that the IUT will generate a valid SPDUBSM security header. Security header shall include, ***protocolVersion***, ***content***, ***signedData***, ***hashId***, ***tbsData***, ***headerInfo*** and doesn’t include ***expiryTime*** nor ***generationLocation***. | |
| **Test Configuration** | | TC (1) | |
| **IUT** | | IUT | |
| **Reference:** | |  | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT being initialized | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to transmit more than one SPDUBSM per second as defined in Table 7‑1 |  |
| 2 | Stimulus | The IUT transmits SPDU’sBSM |  |
| 3 | Verify | SPDUBSM ***Ieee1609Dot2Data*** contains ***protocolVersion*** indicating value = ***0x03*** | Pass/Fail |
| 4 | Verify | SPDUBSM ***Ieee1609Dot2Data*** contains ***content*** indicating signedData | Pass/Fail |
| 5 | Verify | SPDUBSM ***signedData*** contains ***hashId*** indicating ***sha256*** | Pass/Fail |
| 6 | Verify | SPDUBSM ***tbsData*** contains ***protocolVersion*** indicating value = ***0x03*** | Pass/Fail |
| 7 | Verify | SPDUBSM ***tbsData*** contains ***content*** indicating ***unsecuredData*** (Payload Data> 0) | Pass/Fail |
| 8 | Verify | SPDUBSM ***headerInfo*** contains ***psid*** indicating value = ***0x20*** | Pass/Fail |
| 9 | Verify | SPDUBSM ***headerInfo*** contains ***generationTime*** indicating a ***Time64*** (non-zero value of size 8 octets) | Pass/Fail |
| 10 | Verify | SPDUBSM ***headerInfo*** doesn’t include ***expiryTime*** | Pass/Fail |
| 11 | Verify | SPDUBSM ***headerInfo*** doesn’t include ***generationLocation*** | Pass/Fail |

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092- SPDUBSM-SEND-BV-02 | |
| **Summary** | | Validate that the SPDUBSM digitally signed by certificate contains a valid 1609.2 certificate data structure. The certificate shall include a valid ***signer*** info, ***toBeSigned*** ***linkageData*** information, valid ***region*** information and ***ecdsaP256Signature*** type. | |
| **Test Configuration** | | TC (1) | |
| **IUT** | | IUT | |
| **Reference:** | |  | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT being initialized | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to transmit more than one BSM per second as defined in Table 7‑3 |  |
| 2 | Stimulus | The IUT transmits SPDUBSM |  |
| 3 | Verify | SPDUBSM ***signer*** contains ***certificate*** indicating ***version*** value = ***0x03*** | Pass/Fail |
| 4 | Verify | SPDUBSM ***signer*** contains ***type*** indicating ***implicit*** | Pass/Fail |
| 5 | Verify | SPDUBSM ***signer*** contains ***issuer*** containing ***sha256AndDigest*** indicating HashedId8 (a non-zero value of size 8 octets) | Pass/Fail |
| 6 | Verify | SPDUBSM ***toBeSigned*** contains ***id*** indicating linkageData | Pass/Fail |
| 7 | Verify | SPDUBSM ***linkageData*** contains ***iCert*** indicating a value of size 2 octets | Pass/Fail |
| 8 | Verify | SPDUBSM ***linkageData*** contains ***linkage-value*** indicating value of size 9 octets | Pass/Fail |
| 9 | Verify | SPDUBSM ***linkageData*** contains ***group-linkage-value*** containing ***jValue*** indicating a value of size 4 octets | Pass/Fail |
| 10 | Verify | SPDUBSM ***linkageData*** contains ***group-linkage-value*** containing ***value*** indicating a value of size 9 octets | Pass/Fail |
| 11 | Verify | SPDUBSM ***toBeSigned*** contains ***cracaId*** indicating a non-zero value of size 3 octets | Pass/Fail |
| 12 | Verify | SPDUBSM ***toBeSigned*** contains ***crlSeries*** indicating a value =***0x01*** | Pass/Fail |
| 13 | Verify | SPDUBSM ***toBeSigned*** contains ***start*** indicating ***Time32*** (a non-zero value of size 4 octets) | Pass/Fail |
| 14 | Verify | SPDUBSM ***toBeSigned*** contains ***duration*** containing ***hours*** indicating Unit16 (a non-zero Integer value of size 2 octets) | Pass/Fail |
| 15 | Verify | SPDUBSM ***toBeSigned*** contains ***region*** containing a sequence of ***identifiedRegion*** indicating ***countryOnly*** values ***0x7C, 0x1E4*** and ***0x348*** | Pass/Fail |
| 16 | Verify | SPDUBSM ***toBeSigned*** contains a sequence of ***appPermission*** with PSIDs indicating values of 0x***20*** and ***0x26*** | Pass/Fail |
| 17 | Verify | SPDUBSM ***toBeSigned*** contains ***verificationKeyIndicator*** containing ***reconstructionValue*** indicating ***compressed-y-0*** or ***compressed-y-1*** (value of size 32 octets) | Pass/Fail |
| 18 | Verify | SPDUBSM ***signature*** contains ***ecdsaP256Signature*** indicating ***r*** (***compressed-y-0 or compressed-y-1*** consists of octet size 32) | Pass/Fail |
| 19 | Verify | SPDUBSM ***signature*** contains opaque ***s*** indicating non-zero value of size 32 octets | Pass/Fail |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Identifier** | | TP-16092- SPDUBSM-SEND-BV-03 | | |
| **Summary** | | Validate that the SPDUBSM signed by certificate digest contains a valid 1609.2 data structure. The SPDUBSM shall include, ***protocolVersion***, ***content***, ***signedData***, ***hashId***, ***tbsData***, ***headerInfo***, ***signer***, ***ecdsaP256Signature*** and doesn’t include ***expiryTime*** nor ***generationLocation***. | | |
| **Test Configuration** | | TC (1) | | |
| **IUT** | | IUT | | |
| **Reference:** | |  | | |
| **PICS Selection** | |  | | |
| **Pre-test conditions** | | | | |
| * The IUT is being initialized | | | | |
| **Test Sequence** | | | | |
| **Step** | **Type** | | **Description** | **Verdict** |
| 1 | Configure | | The IUT is configured to transmit more than one SPDUBSM per second as defined in Table 7‑2 |  |
| 2 | Stimulus | | The IUT transmits SPDU’sBSM |  |
| 3 | Verify | | SPDUBSM ***Ieee1609Dot2Data*** contains ***protocolVersion*** indicating value = ***0x03*** | Pass/Fail |
| 4 | Verify | | SPDUBSM ***Ieee1609Dot2Data*** contains ***content*** indicating ***signedData*** | Pass/Fail |
| 5 | Verify | | SPDUBSM ***signedData*** contains ***hashId*** indicating ***sha256*** | Pass/Fail |
| 6 | Verify | | SPDUBSM ***tbsData*** contains ***protocolVersion*** indicating value = ***0x03*** | Pass/Fail |
| 7 | Verify | | SPDUBSM ***tbsData*** contains ***content*** indicating ***unsecuredData*** (Payload Data> 0) | Pass/Fail |
| 8 | Verify | | SPDUBSM ***headerInfo*** contains ***psid*** indicating value = ***0x20*** | Pass/Fail |
| 9 | Verify | | SPDUBSM ***headerInfo*** contains ***generationTime*** indicating a ***Time64*** (non-zero value of size 8 octets) | Pass/Fail |
| 10 | Verify | | SPDUBSM ***headerInfo*** doesn’t include ***expiryTime*** | Pass/Fail |
| 11 | Verify | | SPDUBSM ***headerInfo*** doesn’t include ***generationLocation*** | Pass/Fail |
| 12 | Verify | | SPDUBSM contains ***signer*** containing ***digest*** indicating HashedId8 (a non-zero value of size 8 octets) | Pass/Fail |
| 13 | Verify | | SPDUBSM ***signature*** contains ***ecdsaP256Signature*** indicating ***r*** (***compressed-y-0 or compressed-y-1*** consists of octet size 32) | Pass/Fail |
| 14 | Verify | | SPDUBSM ***signature*** contains opaque ***s*** indicating non-zero value of size 32 octets | Pass/Fail |

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092- SPDUBSM-SEND-BV-04 | |
| **Summary** | | Validate that the SPDUBSM is digitally signed by certificate at least every ***vMaxCertDigestInterval***. | |
| **Test Configuration** | | TC (1) | |
| **IUT** | | IUT | |
| **Reference:** | | SAE J2945 [1] Table 10 “Security Profile for TransmittingBSMs”. | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT being initialized | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to transmit more than one SPDUBSM per ***vMaxCertDigestInterval*** interval as defined in Table 7‑3 |  |
| 2 | Stimulus | The IUT transmits SPDU’sBSM |  |
| 3 | Verify | IUT transmitted SPDUBSM at TIME\_1 contains ***signer*** indicating ***certificate*** where the low order 8 octets of the sha256 hash is calculated for the signer Certificate and identified as ID1 | Pass/Fail |
| 4 | Verify | IUT transmitted the next successive SPDUBSM at TIME\_2 (TIME\_2>TIME\_1) which contains ***signer*** indicating ***certificate***  where the low order 8 octets of the sha256 hash is calculated for the signer Certificate and identified as ID2 | Pass/Fail |
| 5 | Verify | ID2 is equal ID1 | Pass/Fail |
| 6 | Verify | Interval (TIME\_2 - TIME\_1) is ‘smaller or equal to' ***vMaxCerDigestInterval*** | Pass/Fail |

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092- SPDUBSM-SEND-BV-05 | |
| **Summary** | | Validate that a SPDUBSM containing a certificate ***digest*** is signed using a valid digital signature computed over entire payload using ***ecdsaP256Signature*** type. | |
| **Test Configuration** | | TC (1) | |
| **IUT** | | IUT | |
| **Reference:** | |  | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT is being initialized | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to transmit more than one SPDUBSM per second |  |
| 2 | Stimulus | The IUT transmits SPDUBSM |  |
| 3 | Verify | The IUT transmitted SPDU’sBSM contains ***signer*** containing ***digest*** indicating ***HashedId8***  where HashedId8 is referenced to a pre-loaded certificate on the IUT | Pass/Fail |
| 4 | Verify | SPDUBSM Signature contains ***ecdsaP256Signature*** indicating ***r*** and ***s*** values verifiable using the pre-loaded certificate identified in step 3 | Pass/Fail |

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092-SPDUBSM-SEND-BV-06 | |
| **Summary** | | Validate that a SPDUBSM digitally signed by certificate contains a valid ***signature*** computed over entire payload using ***ecdsaP256Signature*** type. | |
| **Test Configuration** | | TC (1) | |
| **IUT** | | IUT | |
| **Reference:** | |  | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT being initialized | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to transmit more than one SPDUBSM per second as defined in Table 7‑3 |  |
| 2 | Stimulus | The IUT transmits SPDUBSM |  |
| 3 | Verify | SPDUBSM ***signer*** contains certificate indicating ***type*** ***implicit*** | Pass/Fail |
| 4 | Verify | SPDUBSM ***toBeSigned*** contains ***psid*** indicating a value=***0x20*** | Pass/Fail |
| 5 | Verify | SPDUBSM **toBeSigned** contains ***verificationKeyIndicator*** containing ***reconstructionValue*** indicating ***compressed-y-0*** or ***compressed-y-1*** value (RECVAL) of size 32 octets. RECVAL creates the public key (KEY) by invoking the 1609.2 reconstruction function on (RECVAL) and the public key of the certificate stored on IUT | Pass/Fail |
| 6 | Verify | SPDUBSM ***signature*** contains ***ecdsaP256Signature*** indicating ***r*** and ***s*** values verifiable using a public key (KEY) | Pass/Fail |

#### Reception of packets

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092-SPDUBSM-RECV-BV-01 | |
| **Summary** | | Validate that the IUT will indicate a valid security credentials for a well-formed SPDUBSM security header. Security header shall include ***protocolVersion, signedData, tbsData, headerInfo*** and doesn’t include ***expiryTime*** nor ***generationLocation***. | |
| **Test Configuration** | | TC (1) | |
| **IUT** | | IUT | |
| **Reference:** | |  | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT is being initialized | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to receive more than one SPDUBSM per second |  |
| 2 | Check | SPDUBSM ***Ieee1609Dot2Data*** contains ***protocolVersion*** indicating value = ***0x03*** |  |
| 3 | Check | SPDUBSM Ieee1609Dot2Data contains ***content*** indicating ***signedData*** |  |
| 4 | Check | SPDUBSM ***signedData*** contains ***hashId*** indicating ***sha256*** |  |
| 5 | Check | SPDUBSM ***tbsData*** contains ***protocolVersion*** indicating value = ***0x03*** |  |
| 6 | Check | SPDUBSM ***tbsData*** contains ***content*** indicating ***unsecuredData*** (Payload Data> 0) |  |
| 7 | Check | SPDUBSM ***headerInfo*** contains ***psid*** indicating value = ***0x20*** |  |
| 8 | Check | SPDUBSM ***headerInfo*** contains ***generationTime*** indicating a ***Time64*** (non-zero value of size 8 octets) |  |
| 9 | Check | SPDUBSM ***headerInfo*** doesn’t include ***expiryTime*** |  |
| 10 | Check | SPDUBSM ***headerInfo*** doesn’t include ***generationLocation*** |  |
| 11 | Stimulate | The IUT receives SPDU’sBSM |  |
| 12 | Verify | IUT indicate that the security header for SPDUBSM is formed correctly | Pass/Fail |

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092-SPDUBSM-RECV-BV-02 | |
| **Summary** | | Validate that the IUT will indicate a valid security credential for a well-formed SPDUBSM signed by implicit certificate. The BSM shall include ***protocolVersion, signedData, tbsData, headerInfo, signer***, ***toBeSigned, linkageData, ecdsaP256Signature*** type and doesn’t include ***expiryTime*** nor ***generationLocation***. | |
| **Test Configuration** | | TC (1) | |
| **IUT** | | IUT | |
| **Reference:** | |  | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT is being initialized | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to receive more than one SPDUBSM per second as defined in Table 7‑3 |  |
| 2 | Check | SPDUBSM ***signer*** contains ***certificate*** indicating ***version*** value = ***0x03*** |  |
| 3 | Check | SPDUBSM ***signer*** contains ***type*** indicating ***implicit*** |  |
| 4 | Check | SPDUBSM ***signer*** contains ***issuer*** containing ***sha256AndDigest*** indicating ***HashedId8*** a non-zero value of size 8 octets |  |
| 5 | Check | SPDUBSM ***toBeSigned*** contains ***id*** indicating linkageData |  |
| 6 | Check | SPDUBSM ***linkageData*** contains ***iCert*** indicating a value of size 2 octets |  |
| 7 | Check | SPDUBSM ***linkageData*** contains ***linkage-value*** indicating value of size 9 octets |  |
| 8 | Check | SPDUBSM ***linkageData*** contains ***group-linkage-value*** containing ***jValue*** indicating a value of size 4 octets |  |
| 9 | Check | SPDUBSM ***linkageData*** contains ***group-linkage-value*** containing ***value*** indicating a value of size 9 octets |  |
| 10 | Check | SPDUBSM ***toBeSigned*** contains ***cracaId*** indicating a non-zero value of size 3 octets |  |
| 11 | Check | SPDUBSM ***toBeSigned*** contains ***crlSeries*** indicating a value =***0x01*** |  |
| 12 | Check | SPDUBSM ***toBeSigned*** contains start indicating ***Time32*** (a non-zero value of size 4 octets) |  |
| 13 | Check | SPDUBSM ***toBeSigned*** contains ***duration*** containing ***hours*** indicating ***Unit16*** (a non-zero Integer value of size 2 octets) |  |
| 14 | Check | SPDUBSM ***toBeSigned*** contains ***region*** containing a sequence of ***identifiedRegion*** indicating ***countryOnly*** values ***0x7C, 0x1E4*** and ***0x348*** |  |
| 15 | Check | SPDUBSM ***toBeSigned*** contains a sequence of ***appPermission*** with PSIDs indicating values of ***0x20*** and ***0x26*** |  |
| 16 | Check | SPDUBSM ***toBeSigned*** contains ***verificationKeyIndicator*** containing ***reconstructionValue*** indicating ***compressed-y-0*** or ***compressed-y-1*** (value of size 32 octets) |  |
| 17 | Check | SPDUBSM ***signature*** contains ***ecdsaP256Signature*** indicating ***r*** (***compressed-y-0*** or ***compressed-y-1*** consists of octet size 32) |  |
| 18 | Check | SPDUBSM ***signature*** contains opaque ***s*** indicating non-zero value of size 32 octets |  |
| 19 | Stimulate | The IUT receives SPDUBSM. |  |
| 20 | Verify | IUT indicates that the SPDUBSM holds a valid security credentials. | Pass/Fail |

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092-SPDUBSM-RECV-BV-03 | |
| **Summary** | | Validate that the IUT will indicate a valid security credential for a well-formed SPDUBSM signed by certificate ***digest*** of known certificate. The SPDUBSM shall include***, protocolVersion, content, signedData, tbsData, headerInfo, signer, ecdsaP256Signature*** type and doesn’t include ***expiryTime*** nor ***generationLocation***. | |
| **Test Configuration** | | TC (1) | |
| **IUT** | | IUT | |
| **Reference:** | |  | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT is being initialized | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to receive more than one SPDUBSM per second as defined in Table 7‑2 |  |
| 2 | Check | SPDUBSM Ieee1609Dot2Data contains ***protocolVersion*** indicating value = ***0x03*** |  |
| 3 | Check | SPDUBSM Ieee1609Dot2Data contains ***content*** indicating ***signedData*** |  |
| 4 | Check | SPDUBSM ***signedData*** contains hashId indicating ***sha256*** |  |
| 5 | Check | SPDUBSM ***tbsData*** contains ***protocolVersion*** indicating value = ***0x03*** |  |
| 6 | Check | SPDUBSM ***tbsData*** contains ***content*** indicating ***unsecuredData*** (Payload Data> 0) |  |
| 7 | Check | SPDUBSM ***headerInfo*** contains ***psid*** indicating value = ***0x20*** |  |
| 8 | Check | SPDUBSM ***headerInfo*** contains ***generationTime*** indicating a ***Time64*** (non-zero value of size 8 octets) |  |
| 9 | Check | SPDUBSM ***headerInfo*** doesn’t include ***expiryTime*** |  |
| 10 | Check | SPDUBSM ***headerInfo*** doesn’t include ***generationLocation*** |  |
| 11 | Check | SPDU’sBSM contains ***signer*** containing ***digest*** indicating ***HashedId8*** (a non-zero value of size 8 octets) |  |
| 12 | Check | SPDUBSM ***signature*** contains ***ecdsaP256Signature*** indicating ***r*** (***compressed-y-0*** or ***compressed-y-1*** (consists of octet size 32) |  |
| 13 | Check | SPDUBSM ***signature*** contains opaque ***s*** indicating non-zero value of size 32 octets |  |
| 14 | Stimulate | IUT receives SPDU’sBSM |  |
| 15 | Verify | IUT indicates that the SPDUBSM holds a valid security credentials. | Pass/Fail |

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092-SPDUBSM-RECV-BV-04 | |
| **Summary** | | Validate that the IUT will indicate a valid security credential for a SPDUBSM digitally signed by ***certificate***, which includes ***generationTime*** within ***+/-DE\_DSecond/2*** of the current time and the BSM ***generationTime*** is earlier than the expiration time of the signing certificate. | |
| **Test Configuration** | | TC (1) | |
| **IUT** | | IUT | |
| **Reference:** | | SAE J2945 [1] Table 11 “Security Profile for Receiving BSMs” | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT being initialized | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to receive more than one SPDUBSM per second as defined in Table 7‑3 |  |
| 2 | Check | SPDUBSM ***headerInfo*** contains ***psid*** indicating value = ***0x20*** |  |
| 3 | Check | SPDUBSM ***headerInfo*** contains ***generationTime*** indicating a TIME\_1 where (CUR\_TIME - DE\_DSecond/2 'less or equal' TIME\_1 'less or equal' CUR\_TIME + DE\_DSecond/2) |  |
| 4 | Check | SPDU’sBSM ***signer*** contains ***certificate*** indicating ***type implicit*** |  |
| 5 | Check | SPDUBSM ***toBeSigned*** contains ***start*** & ***duration*** indicating EXP\_TIME where (CUR\_TIME 'less or equal' EXP\_TIME) |  |
| 6 | Stimulate | The IUT receives SPDU’sBSM. |  |
| 7 | Verify | IUT indicates that the SPDUBSM holds a valid security credentials. | Pass/Fail |

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092-SPDUBSM-RECV-BV-05 | |
| **Summary** | | Validate that the IUT will indicate a valid security credential for a SPDUBSM digitally signed by certificate ***digest*** which includes ***generationTime*** within ***+/-DE\_DSecond/2*** from the current time, and the SPDUBSM is generated before the expiration time of the signing certificate digest pre-stored on the device. | |
| **Test Configuration** | | TC (1) | |
| **IUT** | | IUT | |
| **Reference:** | | SAE J2945 [1] Table 11 “Security Profile for Receiving BSMs” | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT is being initialized | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to receive more than one SPDUBSM per second as defined in Table 7‑2 |  |
| 2 | Check | SPDUBSM ***headerInfo*** contains ***psid*** indicating value = ***0x20*** |  |
| 3 | Check | SPDUBSM contains ***signer*** containing ***digest*** indicating ***HashedId8*** (ID1) |  |
| 4 | Stimulate | The IUT receives SPDU’sBSM |  |
| 5 | Check | SPDUBSM ***headerInfo*** contains ***generationTime*** indicating TIME\_1 where (CUR\_TIME – DE\_DSecond/2 'less or equal' TIME\_1 'less or equal' CUR\_TIME + DE\_DSecond/2) |  |
| 6 | Check | SPDUBSM contains ***signer*** containing ***digest*** indicating ***HashedId8*** (ID1) |  |
| 7 | Check | SPDUBSM ***toBeSigned*** contains ***start*** & ***duration*** indicating EXP\_TIME where (CUR\_TIME 'less or equal' EXP\_TIME) |  |
| 8 | Stimulate | The IUT receives SPDU’sBSM |  |
| 7 | Verify | IUT indicates that the SPDUBSM holds a valid security credentials. | Pass/Fail |

#### Certificate Rotation Validation

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092-SPDUBSM-CERTCHG-BV-01 | |
| **Summary** | | Validate that the SPDUBSM contains either ***certificate*** or certificate ***digest*** referencing the same certificate for (***vCertChangeInterval***) minutes and BSM changes the referenced certificate after (***vCertChangeInterval***). | |
| **Test Configuration** | | TC (1) | |
| **IUT** | | IUT | |
| **Reference:** | | SAE J2945 [1] section 6.3.5 “6.5.3-V2V-SECPRIV-CERTCHG-001” | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT being initialized * Time is set at the moment when digest changes | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to transmit more than one SPDUBSM per second |  |
| 2 | Stimulus | The IUT transmits SPDUBSM at TIME\_1 |  |
| 3 | Verify | SPDU’sBSM contains **signer** containing **digest** indicating **HashedId8** (ID1) if yes go to step 5 | Pass/Fail |
| 4 | Verify | SPDUBSM signer contains ***certificate*** where the low order 8 octets of the sha-256 hash is calculated for the certificate (ID1) | Pass/Fail |
| 5 | Verify | The IUT sends the next SPDUBSM at TIME\_2 where (TIME\_2-TIME\_1) 'less' 1sec | Pass/Fail |
| 6 | Verify | SPDU’sBSM contains **signer** containing **digest** indicating HashedId8(ID2) if yes go to step 8 | Pass/Fail |
| 7 | Verify | SPDUBSM **signer** contains ***certificate*** where the low order 8 octets of the **sha-256 hash** is calculated for the certificate (ID2) | Pass/Fail |
| 8 | Verify | where ID2 = ID1 | Pass/Fail |
| 9 | Verify | IUT sends SPDUBSM at TIME\_3 | Pass/Fail |
| 10 | Verify | SPDU’sBSM contains **signer** containing **digest** indicating HashedId8 (ID3) if yes go to step 12 | Pass/Fail |
| 11 | Verify | SPDUBSM signer contains ***certificate*** where the low order 8 octets of the sha-256 hash is calculated for the certificate (ID3) | Pass/Fail |
| 12 | Verify | where ID3! = ID2 | Pass/Fail |
| 13 | Verify | vCertChangeInterval 'less or equal' (TIME\_3 - TIME\_2) 'less or equal' vCertChangeInterval+ 30 sec | Pass/Fail |

#### Reception of packets – invalid behaviour tests

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092-SPDUBSM-RECV-BI-01 | |
| **Summary** | | Validate that the IUT will indicate an invalid security credentials for a SPDUBSM signed by certificate digest, which failed verification due to incorrect signature. | |
| **Test Configuration** | | TC (1) | |
| **IUT** | | IUT | |
| **Reference:** | |  | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT is being initialized | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to receive more than one SPDUBSM per second |  |
| 2 | Check | SPDUBSM ***headerInfo*** contains ***psid*** indicating value = ***0x20*** |  |
| 3 | Check | SPDU’sBSM contains ***signer*** containing ***digest*** indicating HashedId8 (a non-zero value of size 8 octets) |  |
| 4 | Check | SPDUBSM ***signature*** contains ***ecdsaP256Signature*** type indicating ***r*** and **s** ***signature*** not verifiable using the public key (KEY) corresponding to the certificate identified by ***digest*** and stored on IUT |  |
| 5 | Stimulate | The IUT receives SPDU’sBSM |  |
| 6 | Verify | IUT indicates that the SPDUBSM holds an invalid security credentials | Pass/Fail |

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092-SPDUBSM-RECV-BI-02 | |
| **Summary** | | Validate that the IUT will indicate an invalid SPDUBSM signed by implicit certificate which failed verification due to incorrect signature. | |
| **Test Configuration** | | TC (1) | |
| **IUT** | | IUT | |
| **Reference:** | |  | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT being initialized | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to receive more than one SPDUBSM per second |  |
| 2 | Check | SPDU’sBSM ***signer*** contains ***certificate*** indicating ***type implicit*** |  |
| 3 | Check | SPDUBSM ***toBeSigned*** contains ***psid*** indicating a value=***0x20*** |  |
| 4 | Check | SPDUBSM ***toBeSigned*** contains ***verificationKeyIndicator*** containing ***reconstructionValue*** indicating ***compressed-y-0*** or ***compressed-y-1*** value (RECVAL) of size 32 octets. RECVAL creates the public key (KEY) by invoking the 1609.2 reconstruction function on (RECVAL) and the public key of the certificate stored on IUT |  |
| 5 | Check | SPDUBSM ***signature*** contains ***ecdsaP256Signature*** type indicating ***r*** and ***s*** ***signature*** not verifiable using KEY |  |
| 6 | Stimulate | The IUT receives SPDU’sBSM |  |
| 7 | Verify | IUT indicates that the SPDUBSM holds an invalid security credentials | Pass/Fail |

### Secure Protocol Data Unit for WAVE Service Advertisements Messages (SPDUWSA)

#### Transmission of packets

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Identifier** | | TP-16092- SPDUWSA-SEND-BV-01 | | |
| **Summary** | | Validate that the IUT will generate a correct SPDUWSA security header structure. That is, the WSA security header shall include ***protocolVersion, content, signedData, tbsData and headerInfo***. | | |
| **Test Configuration** | | TC (1) | | |
| **IUT** | | IUT | | |
| **Reference:** | |  | | |
| **PICS Selection** | |  | | |
| **Pre-test conditions** | | | | |
| * The IUT is being initialized | | | | |
| **Test Sequence** | | | | |
| **Step** | **Type** | | **Description** | **Verdict** |
| 1 | Configure | | The IUT is configured to transmit one or more SPDUWSA per second as defined in Table 7‑5 |  |
| 2 | Stimulus | | The IUT transmits WSAs |  |
| 3 | Verify | | SPDUWSA ***Ieee1609Dot2Data*** contains ***protocolVersion*** indicating value = ***0x03*** | Pass/Fail |
| 4 | Verify | | SPDUWSA ***Ieee1609Dot2Data*** contains ***content*** indicating ***signedData*** | Pass/Fail |
| 5 | Verify | | SPDUWSA ***signedData*** contains ***hashId*** indicating ***sha256*** | Pass/Fail |
| 6 | Verify | | SPDUWSA ***tbsData*** contains ***protocolVersion*** indicating value = ***0x03*** | Pass/Fail |
| 7 | Verify | | SPDUWSA ***tbsData*** contains ***content*** indicating ***unsecuredData*** (Payload Data> 0) | Pass/Fail |
| 8 | Verify | | SPDUWSA ***headerInfo*** contains ***psid*** indicating value =***0x87*** | Pass/Fail |
| 9 | Verify | | SPDUWSA ***headerInfo*** contains ***generationTime*** indicating a ***Time64*** (non-zero value of size 8 octets) | Pass/Fail |
| 10 | Verify | | SPDUWSA ***headerInfo*** contains ***expiryTime*** indicating a ***Time64*** (non-zero value of size 8 bytes | Pass/Fail |
| 11 | Verify | | SPDUWSA ***headerInfo*** contains ***generationLocation*** indicating  ***latitude*** (-900000000 . . 900000000)  ***longitude*** (-1799999999 . . 1800000000)  ***elevation*** Unit16 | Pass/Fail |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Identifier** | | TP-16092-SPDUWSA-SEND-BV-02 | | |
| **Summary** | | Validate that the IUT will generate a correct SPDUWSA certificate data structure. The SPDUWSA shall include ***signer*** information, ***toBesigned*** data structure and a valid ***ecdsaP256Signature*** type. | | |
| **Test Configuration** | | TC (1) | | |
| **IUT** | | IUT | | |
| **Reference:** | |  | | |
| **PICS Selection** | |  | | |
| **Pre-test conditions** | | | | |
| * The IUT is being initialized | | | | |
| **Test Sequence** | | | | |
| **Step** | **Type** | | **Description** | **Verdict** |
| 1 | Configure | | The IUT is configured to transmit one or more SPDUWSA per second as defined in Table 7‑6 |  |
| 2 | Stimulus | | The IUT transmits SPDU’sWSA |  |
| 3 | Verify | | SPDUWSA ***signer*** contains ***certificate*** indicating ***version*** value= ***0x03*** |  |
| 4 | Verify | | SPDUWSA ***signer*** contains ***type*** indicating ***implicit*** | Pass/Fail |
| 5 | Verify | | SPDUWSA ***signer*** contains ***issuer*** containing ***sha256AndDigest*** indicating ***HashedId8*** (a non-zero value of size 8 octets) | Pass/Fail |
| 6 | Verify | | SPDUWSA ***toBeSigned*** contains ***id*** indicating ***none*** | Pass/Fail |
| 7 | Verify | | SPDUWSA ***toBeSigned*** contains ***cracaId*** indicating value = ***0x0*** | Pass/Fail |
| 8 | Verify | | SPDUWSA ***toBeSigned*** contains ***crlSeries*** indicating value=***0x0*** | Pass/Fail |
| 9 | Verify | | SPDUWSA ***toBeSigned*** contains ***start*** indicating ***Time32*** (a non-zero value of size 4 octets) | Pass/Fail |
| 10 | Verify | | SPDUWSA ***toBeSigned*** contains ***duration*** containing ***minutes*** indicating ***Unit16*** (a non-zero value of size 2 bytes) | Pass/Fail |
| 11 | Verify | | SPDUWSA ***toBeSigned*** contains ***region*** containing ***circularRegion*** indicating  ***latitude*** INTEGER (-900000000..900000000)  ***longitude*** INTEGER (-1799999999..1800000000)  ***radius*** INTEGER (0 .. 65535) | Pass/Fail |
| 12 | Verify | | SPDUWSA ***toBeSigned*** contains ***appPermission*** indicating ***psid*** value= ***0x87*** | Pass/Fail |
| 13 | Verify | | SPDUWSA ***toBeSigned*** contains ***verificationKeyIndicator*** containing ***reconstructionValue*** indicating ***compressed-y-0*** or ***compressed-y-1*** (value of size 32 octets) | Pass/Fail |
| 14 | Verify | | SPDUWSA ***signature*** contains ***ecdsaP256Signature*** indicating ***r*** (a value of ***compressed-y-0*** or ***compressed-y-1*** size of 32 octets) | Pass/Fail |
| 15 | Verify | | SPDUWSA ***signature*** contains opaque ***s*** indicating non-zero value of size 32 octets | Pass/Fail |

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092-SPDUWSA-SEND-BV-03 | |
| **Summary** | | Validate that the IUT will generate a well-formed SPDUWSA signed by certificate ***digest*** of known certificate. The SPDUWSA shall include***, protocolVersion, content, signedData, tbsData, headerInfo, signer, ecdsaP256Signature***. | |
| **Test Configuration** | | TC (1) | |
| **IUT** | | IUT | |
| **Reference:** | |  | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT is being initialized | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to transmit one or more SPDUWSA per second as defined in Table 7‑7 | Pass/Fail |
| 2 | Stimulus | The IUT transmits SPDU’sWSA | Pass/Fail |
| 4 | Verify | SPDUWSA Ieee1609Dot2Data contains ***content*** indicating ***signedData*** | Pass/Fail |
| 5 | Verify | SPDUWSA ***signedData*** contains hashId indicating ***sha256*** | Pass/Fail |
| 6 | Verify | SPDUWSA ***tbsData*** contains ***protocolVersion*** indicating value = ***0x03*** | Pass/Fail |
| 7 | Verify | SPDUWSA ***tbsData*** contains ***content*** indicating ***unsecuredData*** (Payload Data> 0) | Pass/Fail |
| 8 | Verify | SPDUWSA ***headerInfo*** contains ***psid*** indicating value =***0x87*** | Pass/Fail |
| 9 | Verify | SPDUWSA ***headerInfo*** contains ***generationTime*** indicating a ***Time64*** (non-zero value of size 8 octets) | Pass/Fail |
| 10 | Verify | SPDUWSA ***headerInfo*** contains ***expiryTime*** indicating a ***Time64*** (non-zero value of size 8 bytes | Pass/Fail |
| 11 | Verify | SPDUWSA ***headerInfo*** contains ***generationLocation*** indicating  ***latitude*** (-900000000 . . 900000000)  ***longitude*** (-1799999999 . . 1800000000)  ***elevation*** Unit16 | Pass/Fail |
| 12 | Verify | SPDUWSA contains ***signer*** containing ***digest*** indicating ***HashedId8*** (a non-zero value of size 8 octets) | Pass/Fail |
| 13 | Verify | SPDUWSA ***signature*** contains ***ecdsaP256Signature*** indicating ***r*** (***compressed-y-0*** or ***compressed-y-1*** consists of octet size 32) | Pass/Fail |
| 14 | Verify | SPDUWSA ***signature*** contains opaque ***s*** indicating non-zero value of size 32 octets | Pass/Fail |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Identifier** | | TP-16092-SPDUWSA-SEND-BV-04 | | |
| **Summary** | | Validate that the IUT will generate SPDUWSA message digitally signed by ***certificate*** that contains a valid ***signature*** computed over the entire payload using ***ecdsaP256Signature*** type***.*** | | |
| **Test Configuration** | | TC (1) | | |
| **IUT** | | IUT | | |
| **Reference:** | |  | | |
| **PICS Selection** | |  | | |
| **Pre-test conditions** | | | | |
| * The IUT is being initialized | | | | |
| **Test Sequence** | | | | |
| **Step** | **Type** | | **Description** | **Verdict** |
| 1 | Configure | | The IUT is configured to transmit one or more SPDUWSA per second as defined Table 7‑6 |  |
| 2 | Stimulus | | The IUT transmits SPDU’sWSA |  |
| 3 | Verify | | SPDUWSA ***headerInfo*** contains ***psid*** indicating value =***0x87*** | Pass/Fail |
| 4 | Verify | | SPDUWSA ***signer*** contains ***certificate*** indicating ***version*** value = ***0x03*** | Pass/Fail |
| 5 | Verify | | SPDUWSA ***signer*** contains ***type*** indicating ***implicit*** | Pass/Fail |
| 6 | Verify | | SPDUWSA ***signer*** contains ***issuer*** containing ***sha256AndDigest*** indicating ‘CERTID’ | Pass/Fail |
| 7 | Verify | | SPDUWSA ***toBeSigned*** contains ***verificationKeyIndicator*** containing ***reconstructionValue*** indicating (RECVAL)  which creates the public key (KEY) by invoking the 1609.2 reconstruction function on (RECVAL) and the public key of the certificate stored on IUT and identified by (CERTID) | Pass/Fail |
| 8 | Verify | | SPDUWSA ***signature*** contains ***ecdsaP256Signature*** verifiable using (KEY) | Pass/Fail |

#### Reception of packets

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092-SPDUWSA-RECV-BV-01 | |
| **Summary** | | Validate that the IUT will indicate a valid security credentials for a well-formed SPDUWSA security header. That is, the SPDUWSA shall include ***protocolVersion***, ***content***, ***signedData***, ***tbsData*** and ***headerInfo***. | |
| **Test Configuration** | | TC1 | |
| **IUT** | | IUT | |
| **Reference:** | |  | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT is being initialized | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to receive more than one SPDUWSA per second as defined in Table 7‑5 |  |
| 2 | Check | SPDUWSA ***Ieee1609Dot2Data*** contains ***protocolVersion*** indicating (value = ***0x03***) |  |
| 3 | Check | SPDUWSA ***Ieee1609Dot2Data*** contains ***content*** indicating ***signedData*** |  |
| 4 | Check | SPDUWSA ***signedData*** contains ***hashId*** indicating ***sha256*** |  |
| 5 | Check | SPDUWSA ***tbsData*** contains ***protocolVersion*** indicating value = ***0x03*** |  |
| 6 | Check | SPDUWSA ***tbsData*** contains ***content*** indicating ***unsecuredData*** (Payload Data> 0) |  |
| 7 | Check | SPDUWSA ***headerInfo*** contains ***psid*** indicating value =***0x87*** |  |
| 8 | Check | SPDUWSA ***headerInfo*** contains ***generationTime*** indicating a ***Time64*** (non-zero value of size 8 octets) |  |
| 9 | Check | SPDUWSA ***headerInfo*** contains ***expiryTime*** indicating a ***Time64*** (non-zero value of size 8 bytes |  |
| 10 | Check | SPDUWSA ***headerInfo*** contains ***generationLocation*** indicating  ***latitude*** (-900000000 . . 900000000)  ***longitude*** (-1799999999 . . 1800000000)  ***elevation*** Unit16 |  |
| 11 | Stimulate | The IUT receives SPDU’sWSA |  |
| 12 | Verify | IUT indicates that the SPDUWSA message holds a valid security credentials. | Pass/Fail |

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092-SPDUWSA-RECV-BV-02 | |
| **Summary** | | Validate that the IUT will indicate a valid security credentials for a well-formed SPDUWSA signed by implicit certificate. That is, the certificate data structure shall include ***signer, toBesigned*** data structure and ***ecdsaP256Signature*** type. | |
| **Test Configuration** | | TC1 | |
| **IUT** | | IUT | |
| **Reference:** | |  | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT is being initialized | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to receive more than one SPDUWSA per second as defined in Table 7‑6. |  |
| 2 | Check | SPDUWSA ***signer*** contains ***certificate*** indicating ***version*** value = ***0x03*** |  |
| 3 | Check | SPDUWSA ***signer*** contains ***type*** indicating ***implicit*** |  |
| 4 | Check | SPDUWSA ***signer*** contains ***issuer*** containing ***sha256AndDigest*** indicating ***HashedId8*** a non-zero value of size 8 octets |  |
| 5 | Check | SPDUWSA ***toBeSigned*** contains ***id*** indicating ***none*** |  |
| 6 | Check | SPDUWSA ***toBeSigned*** contains ***cracaId*** indicating a value = ***0x0*** |  |
| 7 | Check | WSA ***toBeSigned*** contains ***crlSeries*** indicating a value=***0x0*** |  |
| 8 | Check | SPDUWSA ***toBeSigned*** contains ***start*** indicating ***Time32*** (a non-zero value of size 4 octets) |  |
| 9 | Check | SPDUWSA ***toBeSigned*** contains ***duration*** containing ***minutes*** indicating ***Unit16*** (a non-zero value of size 2 bytes) |  |
| 10 | Check | SPDUWSA ***toBeSigned*** contains ***region*** containing ***circularRegion*** indicating  ***latitude*** INTEGER (-900000000..900000000)  ***longitude*** INTEGER (-1799999999..1800000000)  ***radius*** INTEGER (0 .. 65535) |  |
| 11 | Check | SPDUWSA ***toBeSigned*** contains ***appPermission*** indicating ***psid*** value=***0x87*** |  |
| 12 | Check | SPDUWSA ***toBeSigned*** contains ***verificationKeyIndicator*** containing ***reconstructionValue*** indicating ***compressed-y-0*** or ***compressed-y-1*** (value of size 32 octets) |  |
| 13 | Check | SPDUWSA ***signature*** contains ***ecdsaP256Signature*** indicating ***r*** (a value of ***compressed-y-0*** or ***compressed-y-1*** (size of 32 octets) |  |
| 14 | Check | SPDUWSA ***signature*** contains opaque ***s*** indicating non-zero value of size 32 octets |  |
| 15 | Stimulate | The IUT receives SPDU’sWSA |  |
| 16 | Verify | IUT indicates that the SPDUWSA message holds a valid security credentials. | Pass/Fail |

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092-SPDUWSA-RECV-BV-03 | |
| **Summary** | | Validate that the IUT will indicate a valid security credentials for a well-formed SPDUWSA signed by certificate ***digest*** of known certificate. The SPDUWSA shall include***, protocolVersion, content, signedData, tbsData, headerInfo, signer, ecdsaP256Signature***. | |
| **Test Configuration** | | TC (1) | |
| **IUT** | | IUT | |
| **Reference:** | |  | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT is being initialized | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to receive more than one SPDUWSA per second as defined in Table 7‑6. |  |
| 2 | Check | SPDUWSA Ieee1609Dot2Data contains ***protocolVersion*** indicating value = ***0x03*** |  |
| 3 | Check | SPDUWSA Ieee1609Dot2Data contains ***content*** indicating ***signedData*** |  |
| 4 | Check | SPDUWSA ***signedData*** contains hashId indicating ***sha256*** |  |
| 5 | Check | SPDUWSA ***tbsData*** contains ***protocolVersion*** indicating value = ***0x03*** |  |
| 6 | Check | SPDUWSA ***tbsData*** contains ***content*** indicating ***unsecuredData*** (Payload Data> 0) |  |
| 7 | Check | SPDUWSA ***headerInfo*** contains ***psid*** indicating value = ***0x87*** |  |
| 8 | Check | SPDUWSA ***headerInfo*** contains ***generationTime*** indicating a ***Time64*** (non-zero value of size 8 octets) |  |
| 9 | Check | SPDUWSA ***headerInfo*** contains ***expiryTime*** indicating a ***Time64*** (non-zero value of size 8 bytes |  |
| 10 | Check | SPDUWSA ***headerInfo*** contains ***generationLocation*** indicating  ***latitude*** (-900000000 . . 900000000)  ***longitude*** (-1799999999 . . 1800000000)  ***elevation*** Unit16 |  |
| 11 |  | SPDUWSA contains ***signer*** containing ***digest*** indicating ***HashedId8*** (a non-zero value of size 8 octets) |  |
| 12 | Check | SPDUWSA ***signature*** contains ***ecdsaP256Signature*** indicating ***r*** (***compressed-y-0*** or ***compressed-y-1*** consists of octet size 32 ) |  |
| 13 | Check | SPDUWSA ***signature*** contains opaque ***s*** indicating non-zero value of size 32 octets |  |
| 14 | Stimulate | IUT receives SPDU’sWSA |  |
| 15 | Verify | IUT indicates that the SPDUWSA message holds a valid security credentials. | Pass/Fail |

#### Reception of packets – invalid behaviour tests

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | | TP-16092-SPDUWSA-RECV-BI-01 | |
| **Summary** | | Validate that the IUT will indicate an invalid SPDUWSA signed by implicit certificate, which failed verification due to incorrect signature. | |
| **Test Configuration** | | TC1 | |
| **IUT** | | IUT | |
| **Reference:** | |  | |
| **PICS Selection** | |  | |
| **Pre-test conditions** | | | |
| * The IUT is being initialized | | | |
| **Test Sequence** | | | |
| **Step** | **Type** | **Description** | **Verdict** |
| 1 | Configure | The IUT is configured to receive more than one SPDUWSA per second |  |
| 2 | Check | SPDUWSA ***headerInfo*** contains ***psid*** indicating ***value =0x87*** |  |
| 3 |  | SPDUWSA ***signer*** contains ***certificate*** indicating ***version*** value= ***0x03*** |  |
| 4 | Check | SPDUWSA ***signer*** contains ***type*** indicating ***implicit*** |  |
| 5 | Check | SPDUWSA ***signer*** contains ***issuer*** containing ***sha256AndDigest*** indicating ***HashedId8*** |  |
| 6 | Check | SPDUWSA ***toBeSigned*** contains ***verificationKeyIndicator*** containing ***reconstructionValue*** indicating ‘RECVAL’  which creates the public key ‘KEY’ by invoking the 1609.2 reconstruction function on ‘RECVAL’ and the public key of the certificate stored on IUT and identified by ‘DG1’ |  |
| 7 | Check | SPDUWSA ***signature*** contains ***ecdsaP256Signature*** indicating ***r*** and ***s*** not verifiable using (KEY) |  |
| 8 | Stimulate | The IUT receives the SPDU’sWSA |  |
| 9 | Verify | IUT indicates that the SPDUWSA message holds an invalid security credentials. | Pass/Fail |

# Messages and information element content

This section contains basic message structure that will be used in the TP’s.

## Secure Protocol Data Uunit for Basic Safety message (SPDUBSM)

### SPDUBSM defaults

The following assumptions apply to all messages defined in this section.

* All default values are listed in section 4.1
* The ASN.1 presentation in this section depicts the 1609.2 [8] secure message formats structure of WSM message.

### SPDUBSM Message Details

* Table 7‑1 describes 1609.2[8] security header information of BSM which includes the payload.
* Table 7‑2 and Table 7‑3 describes 1609.2[8] signer credentials information of BSM.
* Table 7‑4 describes 1609.2[8] security signature information of BSM.

### SPDUBSM Security Header information

Table 7‑1: SPDUBSM Header Information

|  |  |  |
| --- | --- | --- |
| Information Element | Value/Remark | Comment |
| Ieee1609Dot2Data SEQUENCE { |  |  |
| ***protocolVersion*** | ***3*** |  |
| ***content signedData*** SEQUENCE { |  |  |
| ***hashId*** | ***sha256*** |  |
| ***tbsData*** SEQUENCE{ |  |  |
| ***payload*** SEQUENCE { |  |  |
| ***data*** { |  |  |
| ***protocolVersion*** | ***3*** |  |
| ***content*** | Any valid BSM payload including 1609.3 WAVE message information. | BSM payload created according to 2945/1 and 2735 standards |
| } |  |  |
| } |  |  |
| ***headerInfo*** { |  |  |
| ***Psid*** | 32 (PSID=***0p20***) | PSID value for BSM is 0p20 |
| ***generationTime*** | Any valid value |  |
| } |  |  |
| } |  |  |
| Require signer credentials information in Table 7‑2 or Table 7‑3 |  |  |
| Require Security Signature information in Table 7‑4 |  |  |

### SPDUBSM Signed with Certificate Digest

Table 7‑2: SPDUBSM Signed by Signer type of Certificate Digest

|  |  |  |
| --- | --- | --- |
| Information Element | Value/Remark | Comment |
| Requires BSM Security header information in Table 7‑1 |  |  |
| ***signer*** { } | ***digest*** | ***HashedID8*** |
| Require Security Signature information in Table 7‑4 |  |  |

### SPDUBSM Signed with Implicit Certificate

Table 7‑3: SPDUBSM Signed by Signer type of Implicit Certificate

|  |  |  |
| --- | --- | --- |
| Information Element | Value/Remark | Comment |
| Requires BSM Security header information in Table 7‑1 |  |  |
| ***signer*** SEQUENCE { | ***certificate*** |  |
| ***certificate*** { |  |  |
| ***version*** | ***3*** |  |
| ***type*** | ***implicit*** |  |
| ***issuer*** | ***ecdsaNistP256AndDigest*** | HashedID8 |
| ***toBeSigned*** SEQUENCE{ |  |  |
| ***id*** { | ***linkageData*** |  |
| ***iCert*** | Any valid value |  |
| ***linkage-value*** | Any Valid value |  |
| ***group-linkage-value*** SEQUENCE{ |  |  |
| ***jValue*** | Any valid value |  |
| ***Value*** | Any valid value |  |
| } |  |  |
| } |  |  |
| ***cracaId*** | Any valid value |  |
| ***crlSeries*** | ***1*** |  |
| ***validityPeriod*** SEQUENCE{ |  |  |
| ***start*** | Any valid value |  |
| ***duration hours*** | Any valid value |  |
| } |  |  |
| ***region identifiedRegion*** SEQUENCE { |  |  |
| ***countryOnly*** | ***124 (0X7C)*** |  |
| ***countryOnly*** | ***484 (0X1E4)*** |  |
| ***countryOnly*** | ***840 (0X348)*** |  |
| }, |  |  |
| ***appPermissions*** SEQUENCE{ |  |  |
| { |  |  |
| ***psid*** | 32 (PSID=***0p20***) | BSM |
| } |  |  |
| { |  |  |
| ***psid*** | 38 (PSID=***0p26***) | Misbehaviour for common applications |
| } |  |  |
| } |  |  |
| ***verifyKeyIndicator*** | ***reconstructionValue*** | ***compressed-y-0 or compressed-y-1*** |
| } |  |  |
| } |  |  |
| } |  |  |
| Require Security Signature information in Table 7‑4 |  |  |

### SPDUBSM Security Signature

Table 7‑4: SPDUBSM Security Signature

|  |  |  |
| --- | --- | --- |
| Information Element | Value/Remark | Comment |
| Requires BSM Security header information in Table 7‑1 |  |  |
| Require signer credentials information in Table 7‑2 or Table 7‑3 |  |  |
| ***signature*** SEQUENCE { | ***ecdsa256Signature*** | EccP256CurvePoint |
| ***r*** | ***compressed-y-0* or *compressed-y-1*** | Octet size of 32 |
| ***s*** |  | Octet size of 32 |
| } |  |  |

### SPDUWSA Message Details

* Table 7‑5 describes 1609.2[8] security header information of WSA which includes valid payload.
* Table 7‑6 and Table 7‑7 describes 1609.2[8] signer credentials information of WSA.
* Table 7‑8 describes 1609.2[8] security signature information of WSA.

### SPDUWSA Security Header information

Table 7‑5 SPDUWSA Header Information

|  |  |  |
| --- | --- | --- |
| Information Element | Value/Remark | Comment |
| Ieee1609Dot2Data SEQUENCE { |  |  |
| ***protocolVersion*** | ***3*** |  |
| ***content signedData*** SEQUENCE { |  |  |
| ***hashId*** | ***sha256*** |  |
| ***tbsData*** SEQUENCE { |  |  |
| ***payload*** SEQUENCE { |  |  |
| ***data*** { |  |  |
| ***protocolVersion*** | ***3*** |  |
| ***content*** | Valid WSA payload |  |
| } |  |  |
| } |  |  |
| ***headerInfo*** SEQUENCE{ |  |  |
| ***psid*** | ***135*** (PSID=***0p8007***) |  |
| ***generationTime*** | Any valid value |  |
| ***expiryTim***e | Any valid value |  |
| ***generationLocation*** SEQUENCE { |  |  |
| ***latitude*** | Any valid value |  |
| ***longitude*** | Any valid value |  |
| ***elevation*** | Any valid value |  |
| } |  |  |
| } |  |  |
| } |  |  |
| Require signer credentials information in Table 7‑6 or 7-7 |  |  |
| Require Security Signature information in Table 7‑8 |  |  |
| } |  |  |

### SPDUWSA Signed with Implicit Certificate

Table 7‑6: SPDUWSA Signed by Signer type of Implicit Certificate

|  |  |  |
| --- | --- | --- |
| Information Element | Value/Remark | Comment |
| Requires WSM Security header information in Table 7‑5 |  |  |
| ***signer*** SEQUENCE { |  |  |
| ***certificate*** { |  |  |
| ***Version*** | ***3*** |  |
| ***type*** | ***implicit*** |  |
| ***issuer*** | ***ecdsaNistP256AndDigest*** | ***HashedID8*** |
| ***toBeSigned*** SEQUENCE { |  |  |
| ***id*** | ***none*** |  |
| ***cracaId*** | ***Value = 0*** |  |
| ***crlSeries*** | ***Value=0*** |  |
| ***validityPeriod***  SEQUENCE { |  |  |
| ***start*** | Any valid value |  |
| ***duration minutes*** | Any valid value |  |
| } |  |  |
| ***region circularRegion*** SEQUENCE { |  |  |
| ***centre*** { |  |  |
| ***latitude*** | Any valid value |  |
| ***longitude*** | Any valid value |  |
| } |  |  |
| ***radius*** | Any valid value |  |
| } |  |  |
| ***appPermissions*** { |  |  |
| { |  |  |
| ***psid*** | 135 (PSID=***0p8007***) |  |
| } |  |  |
| } |  |  |
| ***verifyKeyIndicator*** | ***reconstructionValue*** | ***compressed-y-0 or compressed-y-1*** |
| } |  |  |
| } |  |  |
| } |  |  |
| Require Security Signature information in Table 7‑8 |  |  |

### SPDUWSA Signed with Certificate Digest

Table 7‑7: SPDUWSA Signed with Certificate digest

|  |  |  |
| --- | --- | --- |
| Information Element | Value/Remark | Comment |
| Requires WSA Security header information in Table 7‑5 |  |  |
| ***signer*** { } | ***digest*** | ***HashedID8*** |
| Require Security Signature information in Table 7 8 |  |  |

### SPDUWSA Security Signature

Table 7‑8: SPDUWSA Security Signature

|  |  |  |
| --- | --- | --- |
| Information Element | Value/Remark | Comment |
| Requires WSM Security header information in Table 7‑5 |  |  |
| Require signer credentials information in Table 7‑6 or Table 7‑7 |  |  |
| ***signature*** SEQUENCE { | ***ecdsa256Signature*** | EccP256CurvePoint |
| ***r*** | ***compressed-y-0 or compressed-y-1*** | Octet size of 32 |
| ***s*** | Any valid value | Octet size of 32 |
| } |  |  |



Traceability Matrix

This section of the document contains the traceability matrix for BSM and WSA security requirements. As shown below, Table A- 1 lists BSM IEEE 1609.2[8] traceability to TPs. In Page (# 40) Table A- 2 lists WSA IEEE 1609.2 traceability to TPs where PICS for WSA was derived from “IEEE 1609.2[8] security specification for WSA requirements” listed under Annex H in 1609.3[5].

The current test specification doesn’t include any TP’s that requires Security Credential Management System (SCMS) due to the fact that the new standard is not available and will be available in 2016. Accordingly, not all the mandatory requirements by 2945/1 is tested at this time.

Table A- 1: BSM IEEE 1609.2 PICS traceability to TPs

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **1609.2 PICS from [8]** | **Features in [8]** | **Reference section in [8]** | **Status (J2945-1 [1])** | **Support  (J2945-1 [1])** | **TP ID** | **TP Description** |
| S1.2.2 | **Create Ieee1609Dot2Data containing valid SignedData** | 4.2.2.2.3, 5.2, 5.3.1, 5.3.3,5.3.7,6.3.4,6.3.9,9.3.9.1 | S1.2:O3 | Y | TP-16092-BSM-SEND-BV-01 | To verify that the IUT will generate a valid signedData as per 1609.2[8] specifications |
| S1.2.2.1 | Using a valid HashAlgorithm | 6.3.5 | S1.2.2:M | Y | TP-16092-BSM-SEND-BV-01 | To verify that the IUT will generate a valid signedData using sha256 hash |
| TP-16092-BSM-SEND-BV-03 | To verify that the IUT will generate signed using certificate digest generated by hash 256 |
| S1.2.2.1.1 | Support signing with hash algorithm SHA-256 | 6.3.5 | S1.2.2:M | Y | Refer to S1.2.2.1 |  |
| S1.2.2.2 | Containing a Signed Data payload | 6.3.6 | S1.2.2:M | Y | TP-16092-BSM-SEND-BV-01 | To verify that the IUT will generate a signedData with BSM payload is included |
| S1.2.2.2.1 | with payload containing data | 6.3.7 | S1.2.2.2:O4 | Y | Refer to S1.2.2.2 |  |
| S1.2.2.2.3. | … with generationTime in the security header | 6.3.9, 6.3.11 | S1.2.2.2: O | Y | TP-16092-BSM-SEND-BV-01 | To verify that the IUT will generate BSM security header that includes generationTime |
| TP-16092-BSM-SEND-BV-03 | To verify that the IUT will generate BSM security header that includes generationTime signed by certificate digest |
| S1.2.2.3. | Support a SignerIdentifier | 6.3.24 | S1.2.2:M | Y | TP-16092-BSM-SEND-BV-02 | To verify that the IUT will generate aBSM signed with signer type of certificate |
| TP-16092-BSM-SEND-BV-03 | To verify that the IUT will generate BSM signed with signer type of certificate digest |
| S1.2.2.3.1. | … of type digest | 6.3.26 | S1.2.2.3:O6 | Y | Refer to S1.2.2.3 |  |
| S1.2.2.3.2. | … of type certificate | 6.4.2 | S1.2.2.3:O6 | Y | Refer to S1.2.2.3 |  |
| S1.2.2.3.2.1 | Maximum number of Certificates in the chain | 5.1.2.2 | S1.2.2.3.2  8:M  > 8:O | 1 | TP-16092-BSM-SEND-BV-02 | To verify that the IUT will generate BSM signed with signer type of certificate With a Maximum number of certificates in the chain is equal to 1. |
| S1.2.2.4. | Support a Signature | 6.3.28 | S1.2.2:M | Y | TP-16092-BSM-SEND-BV-05 | To verify that the IUT will generate a valid signature to sign BSM message generated by signer of type certificate digest |
| TP-16092-BSM-SEND-BV-06 | To verify that the IUT will generate a valid signature to sign BSM messages generated by signer of type certificate |
| S1.2.2.4.1. | … a ecdsa256Signature | 6.3.29 | S1.2.2.4:M | Y | TP-16092-BSM-SEND-BV-02 | To verify that the IUT will generate a valid signature using ecdsa256Signature type. Where it uses the NIST p256 algorithm to generate the compressed r value. The signer type used to sign the BSM message is certificate |
| TP-16092-BSM-SEND-BV-03 | To verify that the IUT will generate a valid signature using ecdsa256Signature type. Where it uses the NIST p256 algorithm to generate the compressed r value. The signer type used to sign the BSM message is digest |
| S1.2.2.4.1.1. | … … using NIST p256 | 6.3.29 | S1.2.2.4.1:O7 | Y | Refer to S1.2.2.4.1 |  |
| S1.2.2.4.1.4. | … … with a compressed r value | 6.3.23 | S1.2.2.4.1:O8 | Y | Refer to S1.2.2.4.1 |  |
| S1.2.2.5.1. | Determine that the region is correct | 6.4.8, 6.4.17 | S1.2.2.5:O | Y | TP-16092-BSM-SEND-BV-02 | To verify that the certificate region is defined as " identifiedRegion" with a minimum number of 3 countries as specified in SAE J2945/1 |
| S1.2.2.5.1.4 | Support identifiedRegion | 6.4.17, 6.4.22 | S1.2.2.5.1:O9 | Y | Refer to S1.2.2.5.1 |  |
| S1.2.2.5.1.4.1. | Maximum number of identifiedRegions supported | 6.4.17 6.4.22 | S1.2.2.5.1.4: 8:M >8:O | Minimum of 3 Note: US, Canada, Mexico supported as defined by the United Nations Statistics Division, October 2013 edition | Refer to S1.2.2.5.1 |  |
| S1.2.2.5.1.4.2. | Support IdentifiedRegion of type Country Only | 6.4.22, 6.4.23 | S1.2.2.5.1.4:O1 | Y | Refer to S1.2.2.5.1 |  |
| S1.2.2.5.2 | Determine that the certificate has the proper appPermissions | 6.4.8 6.4.28 | S1.2.2.5:O | Y | TP-16092-BSM-SEND-BV-02 | verify that the IUT will generate a signedData using implicit certificate that contains the appropriate appPermissions |
| S1.2.2.8. | Support signing with implicit certificate | 5.3.2, 6.4.5 | S1.2.2.5:O11 | Y | Refer to S1.2.2.5.2 |  |
| S1.3.2. | Verify Ieee­­1609­Dot2­­Data containing Signed­Data | 4.2.2.2.3, 5.2, 5.3.1, 5.3.3 5.3.7, 6.3.4,6.3.9 | S1.3:O17 | **Y** | TP-16092-BSM-RECV-BV-01 | To verify that the IUT will accept a valid BSM contains signedData. |
| S1.3.2.1. | Using a valid HashAlgorithm |  | S1.3.2:M | **Y** | TP-16092-BSM-RECV-BV-01 | To verify that the IUT will accept BSM message signed by a digest of type sha256 |
| TP-16092-BSM-RECV-BV-03 | To verify that the IUT will accept BSM messages signed by a signer credential of type certificate digest using sha256 |
| S1.3.2.1.1. | Verify signed data using Hash Algorithm SHA-256 | 6.3.5 | S1.3.2.1:M | Y | Refer to S1.3.2.1 |  |
| S1.3.2.2. | Containing a Signed Data payload | 6.3.6 | S1.3.2:M | **Y** | Refer to S1.3.2 |  |
| S1.3.2.2.1. | … with payload containing data | 6.3.7 | S1.3.2.2:O18 | **Y** | Refer to S1.3.2 |  |
| S1.3.2.2.3. | … with generation Time in the security header | 6.3.9, 6.3.11 | S1.3.2.2:O | **Y** | TP-16092-BSM-RECV-BV-01 | To verify that the IUT will accept BSM message with the correct security header information. That is, it must contain generationTime. |
| S1.3.2.3. | Support a SignerIdentifier | 6.3.24 | S1.3.2:M | **Y** | TP-16092-BSM-RECV-BV-02 | To verify that the IUT will accept BSM message signed with the correct signer credential of type certificate. . |
| TP-16092-BSM-RECV-BV-03 | To verify that the IUT will accept BSM message signed with the correct signer credential of type certificate digest. |
| S1.3.2.3.1. | … of type digest | 6.3.26 | S1.3.2.3:O20 | **Y** | Refer to S1.3.2.3 |  |
| S1.3.2.3.2 | … of type certificate | 6.4.2 | S1.3.2.3:O20 | **Y** | Refer to S1.3.2.3 |  |
| S1.3.2.3.2.1. | … … Maximum number of Certificates in the chain | 5.1.2.2 | S1.3.2.3.2 1:M >1:O | 1 | TP-16092-BSM-RECV-BV-02 | To verify that the IUT will accept a BSM message with a maximum certificate chain is equal to 1. |
| S1.3.2.4. | Support a Signature | 6.3.28 | S1.3.2:M | **Y** | TP-16092-BSM-RECV-BV-02 | To verify that the IUT will accept BSM message signed by ecdsa256Signature type. Where it uses the NIST p256 algorithm to generate the compressed r value. The signer credential type used to sign the BSM message is certificate |
| TP-16092-BSM-RECV-BV-03 | To verify that the IUT will accept BSM message signed by ecdsa256Signature type. Where it uses the NIST p256 algorithm to generate the compressed r value. The signer credential type used to sign the BSM message is certificate digest. |
| S1.3.2.4.1. | … a ecdsa256Signature | 6.3.29 | S1.3.2.4:M | **Y** | Refer to S1.3.2.4 |  |
| S1.3.2.4.1.1. | … … using NIST p256 | 6.3.29 | S1.3.2.4.1:O21 | **Y** | Refer to S1.3.2.4 |  |
| S1.3.2.4.1.4. | … … with a compressed r value | 6.3.23 | S1.3.2.4.1:O22 | **Y** | Refer to S1.3.2.4 |  |
| S1.3.2.10.14. | … SPDU-Crypto: Verification failure | 5.3.1 | S1.3.2.10:M | **Y** | TP-16092-BSM-RECV-BI-01 | To verify that the IUT will reject a BSM message signed with invalid ecdsa256Signature. The signer credential of type certificate digest is used to sign the BSM message. |
| TP-16092-BSM-RECV-BI-02 | To verify that the IUT will reject a BSM message signed with invalid ecdsa256Signature. The signer credential of type certificate is used to sign the BSM message. |

Table A- 2: WSA IEEE 1609.2 PICS traceability to TPs

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **1609.2 PICS from** [8] | **Features in** [8] | **Reference section in** [8] | **Status** [8] | **Support 1609.3**[5] | **TP ID** | **TP Description** |
| S1.2.2 | Create Ieee1609Dot2Data containing valid SignedData | 4.2.2.2.3, 4.2.2.2.3, 5.2, 5.3.1  5.3.3, 5.3.7, 6.3.4, 6.3.9, 9.3.9.1 | S1.2:O3 | Y | TP-16092-WSA-SEND-BV-01 | To verify that the IUT will generate a valid WSA signedData as per 1609.2[8] specifications |
|
|
|
|
|
|
| S1.2.2.1. | Using a valid HashAlgorithm | 6.3.5 | S1.2.2:M | Y | TP-16092-WSA-SEND-BV-01 | To verify that the IUT will generate a valid WSA signedData using sha256 hash |
| S1.2.2.1.1. | Support signing with hash algorithm sha-256 | 6.3.5 | S1.2.2:M | Y | Refer to S1.2.2.1 |  |
|
| S1.2.2.2. | Containing a Signed Data payload | 6.3.6 | S1.2.2:M | Y | TP-16092-WSA-SEND-BV-01 | To verify that the IUT will generate a valid signedData with WSA payload is included |
| S1.2.2.2.1. | … with payload containing data | 6.3.7 | S1.2.2.2:O4 | Y | Refer to S1.2.2.2 |  |
| S1.2.2.2.3. | … with generationTime in the security headers | 6.3.9, 6.3.11 | S1.2.2.2: O | Y | TP-16092-WSA-SEND-BV-01 | To verify that the IUT will generate a valid WSA headerinfo data structure that include Generation time |
|
| S1.2.2.2.4. | … with expiryTime in the security headers | 6.3.9, 6.3.11 | S1.2.2.2: O | Y | TP-16092-WSA-SEND-BV-01 | To verify that the IUT will generate a valid WSA headerinfo data structure that includes Expiry Time. |
|
| S1.2.2.2.5. | … with generationLocation in the security headers | 6.3.9, 6.3.12 | S1.2.2.2: O | Y | TP-16092-WSA-SEND-BV-01 | To verify that the IUT will generate a valid WSA headerinfo data structure that include Generation location. |
|
| S1.2.2.3. | Support a SignerIdentifier | 6.3.24 | S1.2.2:M | Y | TP-16092-WSA-SEND-BV-02 | To verify that the IUT will generate WSA signed with signer type of implicit certificate |
| TP-16092-WSA-SEND-BV-03 | To verify that the IUT will generate WSA signed with signer type of certificate digest |
| S1.2.2.3.1. | … of type digest | 6.3.26 | S1.2.2.3:O6 | Y | Refer to S1.2.2.3 |  |
| S1.2.2.3.2. | … of type certificate | 6.4.2 | S1.2.2.3:O6 | Y | Refer to S1.2.2.3 |  |
| S1.2.2.3.2.1. | … … Maximum number of Certificates in the chain | 5.1.2.2 | S1.2.2.3.2 8:M >8O | 1 | TP-16092-WSA-SEND-BV-02 | To verify that the IUT Will generate WSA signed with certificate chain =1 |
|
|
| S1.2.2.4. | Support a Signature | 6.3.28 | S1.2.2:M | Y | TP-16092-WSA-SEND-BV-04 | To verify that the IUT Will generate WSA signed with a valid signature. The signature will be generated using NISTp256 and using Compressed r value |
| S1.2.2.4.1. | … a ecdsa256Signature | 6.3.29 | S1.2.2.4:M | Y | Refer to S1.2.2.4. |  |
| S1.2.2.4.1.1. | … … using NIST p256 | 6.3.29 | S1.2.2.4.1:O7 | Y | Refer to S1.2.2.4. |  |
| S1.2.2.4.1.4. | … … with a compressed r value | 6.3.23 | S1.2.2.4.1:O8 | Y | Refer to  S1.2.2.4. |  |
| S1.2.2.5.1. | Determine that the region is correct | 6.4.8, 6.4.17 | S1.2.2.5:O | Y | TP-16092-WSA-SEND-BV-02 | To verify that the IUT will generated a signer of type implicit certificate that contains a valid region. |
|
| S1.2.2.8. | Support signing with implicit certificates | 5.3.2, 6.4.5 | S1.2.2.5:O11 | Y | Refer to S1.2.2.3 |  |
|
| S1.3.2. | Verify Ieee1609Dot2Data containing SignedData | 4.2.2.2.3, 5.2, 5.3.1  5.3.3, 5.3.7, 6.3.4 6.3.9 | S1.3:O17 | Y | TP-16092-WSA-RECV-BV-01 | To verify that the IUT will accept a valid WSA contains signedData. |
|
|
|
|
|
| S1.3.2.1. | Using a valid HashAlgorithm |  | S1.3.2:M | Y | TP-16092-WSA-RECV-BV-01 | To verify that the IUT will accept WSA message signed by a digest of type sha256 |
| TP-16092-WSA-RECV-BV-03 | To verify that the IUT will accept BSM messages signed by a signer credential of type certificate digest using sha256 |
| S1.3.2.1.1. | Verify signed data using HashAlgorith SHA-256 | 6.3.5 | S1.3.2.1:M | Y | Refer to S1.3.2.1 |  |
| S1.3.2.2. | Containing a Signed Data payload | 6.3.6 | S1.3.2:M | Y | TP-16092-WSA-RECV-BV-01 | To verify that the IUT will accept a WSA signed message containing Payload |
| S1.3.2.2.1. | … with payload containing data | 6.3.7 | S1.3.2.2:O18 | Y | Refer to S1.3.2.2 |  |
| S1.3.2.2.3. | … with generationTime in the security headers | 6.3.9, 6.3.11 | S1.3.2.2:O | Y | TP-16092-WSA-RECV-BV-02 | To verify that the IUT will accept a valid WSA headerinfo data structure that include Generation time |
|
| S1.3.2.2.4. | … with expiryTime in the security headers | 6.3.9, 6.3.11 | S1.3.2.2:O | Y | TP-16092-WSA-RECV-BV-02 | To verify that the IUT will accept a valid WSA headerinfo data structure that include Expiry time. |
|
| S1.3.2.2.5. | … with generationLocation in the security headers | 6.3.9, 6.3.12 | S1.3.2.2:O | Y | TP-16092-WSA-RECV-BV-02 | To verify that the IUT will accept a valid WSA headerinfo data structure that include Generation location |
|
| S1.3.2.3. | Support a SignerIdentifier | 6.3.24 | S1.3.2:M | Y | TP-16092-WSA-RECV-BV-02 | To verify that the IUT will accept a valid WSA message signed with signer type of implicit certificate |
| TP-16092-WSA-RECV-BV-02 | To verify that the IUT will accept a valid WSA message signed with signer type of certificate digest. |
| S1.3.2.3.1. | … of type digest | 6.3.26 | S1.3.2.3:O20 | Y | Refer to S1.3.2.3 |  |
| S1.3.2.3.2. | … of type certificate | 6.4.2 | S1.3.2.3:O20 | Y | Refer to  S1.3.2.3. |  |
| S1.3.2.3.2.1. | … … Maximum number of Certificates in the chain | 5.1.2.2 | S1.3.2.3.2 1:M >1:O | 1 | TP-16092-WSA-RECV-BV-02 | To verify that the IUT will accept a valid WSA message signed with certificate chain = 1 |
|
|
| S1.3.2.4. | Support a Signature | 6.3.28 | S1.3.2:M | Y | TP-16092-WSA-RECV-BV-02 | To verify that the IUT Will accept WSA signed with a valid signature. The signature will be generated using NISTp256 and using Compressed r value |
| S1.3.2.4.1. | … a ecdsa256Signature | 6.3.29 | S1.3.2.4:M | Y | Refer to S1.3.2.4 |  |
| S1.3.2.4.1.1. | … … using NIST p256 | 6.3.29 | S1.3.2.4.1:O21 | Y | Refer to S1.3.2.4 |  |
| S1.3.2.4.1.4. | … … with a compressed r value | 6.3.23 | S1.3.2.4.1:O22 | Y | Refer to S1.3.2.4 |  |
| S1.3.2.5.1.1. | … using a circularRegion | 6.4.17, 6.4.18 | S1.3.2.5.1:O23 | Y | TP-16092-WSA-RECV-BV-02 | To verify that the IUT will accept a WSA message signed by a signer of type implicit certificate with a region of type circular. |
|
| S1.3.2.7. | Support verifying SPDUs signed with implicit authorization certificates | 5.3.2, 6.4.5 | S1.3.2:O25 | Y | Refer to S1.3.2.3. |  |
|
| S1.3.2.10.14. | … SPDU-Crypto: Verification failure | 5.3.1 | S1.3.2.10:M | Y | TP-16092-WSA-RECV-BI-01 | To verify that the IUT will reject a WSA message signed with invalid ecdsa256Signature. The signer credential of type certificate is used to sign the BSM message. |

# Revision History

|  |  |  |
| --- | --- | --- |
| V0.1.0 | Sep 17, 2015 | Initial Draft – BSM test cases |
| V0.2.0 | Sep 30, 2015 | Added test cases for WSA messages |
| V0.3.0 | Oct 5, 2015 | Updated BSM and WSA messages |
| V.0.4.0 | Oct 23, 2015 | Updated Test Cases to the new format |
| V.0.5.0 | Dec 31, 2015 | Updated TP to the new Standard  Added Tractability Matrix for BSM and WSA |
| V.0.6.0 | Feb 5, 2016 | Based on peer review, multiple changes were made to the document. |
| V.1.0 | March 23, 2016 | Incorporated comments from industry reviewers |
| V1.1 | Oct 10, 2016 | Incorporated comments from CAMP reviewers. |
| V1.2 | Apr 28, 2017 | Replaced p-encoded PSID values with hex encoded values  Added compressed-y-1 where compressed-y-0 is mentioned  Changes in TP-16092- SPDUBSM-SEND-BV-[04-06], TP-16092-SPDUBSM-RECV-BI-01. Small edits in others. |

◙ End of Document ◙

1. SPDUBSM will have certificates with a lifetime of a week and will be revocable. ***cracaId*** will be non-zero, ***crlSeries*** value will be 1 and ***linkageData*** is used to determine if the cert is revoked. ***reconstructionValue*** and ***r*** values will use ***compressed-y-0*** or ***compressed-y-1*** for elliptic curve point is encoding. [↑](#footnote-ref-1)
2. All SPDUWSA test cases are written with the assumption that the signer credentials (certificate) are non-revocable, because they will have short lifetimes. Certificate geographical ***region*** will be ***circularRegion*** type ***reconstructionValue*** and ***r*** values will use ***compressed-y-0 or compressed-y-1*** for elliptic curve point encoding. [↑](#footnote-ref-2)