



# SURFACE VEHICLE STANDARD

J2945™/5

FEB2020

Issued

2020-02

## Service Specific Permissions and Security Guidelines for Connected Vehicle Applications

### RATIONALE

The Technical Committees under the SAE Vehicle to Everything (V2X) Steering Committee are developing a series of standards that specify a set of applications that use message sets from the SAE J2735 data dictionary. The communications for these applications are secured using digital signatures and IEEE 1609.2 digital certificates, which indicate the permissions of the senders using Provider Service Identifiers (PSID) and (optionally) Service Specific Permissions (SSPs). The PSID in a certificate governs the certificate holder's permissions to engage in any communications activities associated with that application; the SSP allows more specific statements of the holder's permissions within the universe of that application. For any given application based on SAE J2735, a complete application specification will include a specification of how the contents of the PSID and (if present) SSP fields in a given certificate correspond to the application activities that certificate holder is entitled to carry out. This document establishes principles that can be used by future application specifiers to (1) specify the syntax of SSPs, and (2) determine which fields and activities should be subject to SSP constraints. It also addresses the development of SSPs for scenarios not addressed in the original application specification; for example, arising from regional extensions, changes in application functionality, or future expansions of the base SAE J2735 standard.

### TABLE OF CONTENTS

|       |                                                                                   |    |
|-------|-----------------------------------------------------------------------------------|----|
| 1.    | SCOPE.....                                                                        | 3  |
| 2.    | REFERENCES.....                                                                   | 3  |
| 2.1   | Applicable Documents .....                                                        | 3  |
| 2.1.1 | SAE Publications.....                                                             | 3  |
| 2.1.2 | IEEE Publications.....                                                            | 3  |
| 2.1.3 | ISO Publications.....                                                             | 4  |
| 2.1.4 | NIST Publications.....                                                            | 4  |
| 2.1.5 | Other References .....                                                            | 4  |
| 3.    | DEFINITIONS .....                                                                 | 5  |
| 4.    | ABBREVIATIONS AND ACRONYMS.....                                                   | 8  |
| 5.    | SSP DEVELOPMENT PROCESS (NORMATIVE) .....                                         | 9  |
| 5.1   | Overview .....                                                                    | 9  |
| 5.2   | SSP Overview .....                                                                | 10 |
| 5.2.1 | Security Deployment Lifecycle for Applications Using 1609.2 Certificates.....     | 13 |
| 5.2.2 | SSP Encoding Options and Recommended SSP Type.....                                | 14 |
| 5.3   | Security Specification through the Systems Engineering Process (Informative)..... | 17 |
| 5.3.1 | Systems Engineering Process Overview .....                                        | 17 |
| 5.3.2 | Security Specification through the Systems Engineering Process (Informative)..... | 18 |

SAE Technical Standards Board Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2020 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

**TO PLACE A DOCUMENT ORDER:** Tel: 877-606-7323 (inside USA and Canada)  
Tel: +1 724-776-4970 (outside USA)  
Fax: 724-776-0790  
Email: CustomerService@sae.org  
http://www.sae.org

**SAE WEB ADDRESS:**

Full document details: SAE J2945\_5\_202002

SAE values your input. To provide feedback on this Technical Report, please visit [http://standards.sae.org/J2945/5\\_202002](http://standards.sae.org/J2945/5_202002)

Documents  
Document Sharing Hub

|            |                                                                                                                              |    |
|------------|------------------------------------------------------------------------------------------------------------------------------|----|
| 5.4        | SSP Development Process: Overview.....                                                                                       | 22 |
| 5.4.1      | Background .....                                                                                                             | 22 |
| 5.4.2      | SSP Design Principles .....                                                                                                  | 23 |
| 5.4.3      | Recommended Process: Summary .....                                                                                           | 23 |
| 5.5        | SSP Development Process: Design .....                                                                                        | 25 |
| 5.5.1      | Application Roles .....                                                                                                      | 25 |
| 5.5.2      | Identify Information Flows .....                                                                                             | 25 |
| 5.5.3      | Receiver Behavior Assumptions and Entity Activities.....                                                                     | 26 |
| 5.5.4      | Perform Risk Analysis .....                                                                                                  | 28 |
| 5.5.5      | Create Entity Activity Groups (SSP Roles) .....                                                                              | 29 |
| 5.5.6      | Validate Results through Review and Iterate.....                                                                             | 31 |
| 5.6        | SSP Development: Design .....                                                                                                | 32 |
| 5.6.1      | The Omitted SSP Encoding .....                                                                                               | 33 |
| 5.7        | Regionality and Extensibility .....                                                                                          | 34 |
| 5.7.1      | Background .....                                                                                                             | 34 |
| 5.7.2      | Changes to Application Functionality Based on Existing Fields .....                                                          | 34 |
| 5.7.3      | ITIS Phrases .....                                                                                                           | 35 |
| 5.7.4      | Extensibility via ASN.1 Extensions .....                                                                                     | 35 |
| 5.7.5      | Extensibility via Regional Extensions.....                                                                                   | 35 |
| 5.8        | SSP Version Number .....                                                                                                     | 36 |
| 5.9        | Identity.....                                                                                                                | 36 |
| 5.10       | Conclusion .....                                                                                                             | 37 |
| 6.         | OTHER CONSIDERATIONS FOR SSP DEPLOYMENT (INFORMATIVE) .....                                                                  | 37 |
| 6.1        | SSP Separation Privacy Guidance .....                                                                                        | 37 |
| 6.2        | Certification and Conformance Claims for Applications Using SSPs .....                                                       | 38 |
| 6.3        | SSP Design as Part of an Overall Security Control Strategy: Certificate Issuance and<br>Device Security .....                | 38 |
| 6.4        | PSIDs and Application Specifications: Ownership, Extensions, and Hygiene.....                                                | 39 |
| 7.         | NOTES .....                                                                                                                  | 40 |
| 7.1        | Revision Indicator.....                                                                                                      | 40 |
| APPENDIX A | SAE J2945/3: SECURITY ANALYSIS AND SSP DESIGN (INFORMATIVE) .....                                                            | 41 |
| Figure 1   | Sending/receiving architecture for applications using IEEE 1609.2 certificates to authorize<br>individual messages.....      | 10 |
| Figure 2   | 1609.2 consistency conditions: checked by security services and by application logic .....                                   | 11 |
| Figure 3   | Consistency conditions to be checked by the security services .....                                                          | 12 |
| Figure 4   | Consistency conditions to be checked by the application.....                                                                 | 12 |
| Figure 5   | Security deployment lifecycle for applications using 1609.2 certificates .....                                               | 14 |
| Figure 6   | Matching an entry in a CA certificate certIssuePermissions with an entry in an end-entity certificate<br>appPermissions..... | 15 |
| Figure 7   | Matching an entry in a CA certificate certIssuePermissions with an entry in an end-entity certificate<br>appPermissions..... | 16 |
| Figure 8   | Matching an entry in a CA certificate certIssuePermissions with an entry in an end-entity certificate<br>appPermissions..... | 16 |
| Figure 9   | Iteration of security analysis throughout the SEP .....                                                                      | 19 |
| Figure 10  | High level SSP development process flow .....                                                                                | 24 |
| Figure 11  | Establish actors.....                                                                                                        | 25 |
| Figure 12  | Establish information flows .....                                                                                            | 25 |
| Figure 13  | Perform sensitivity analysis.....                                                                                            | 29 |
| Figure 14  | Bitmap permissions encoding .....                                                                                            | 33 |
| Figure 15  | SSP versioned bitmap.....                                                                                                    | 36 |
| Table 1    | Risk analysis: use case name.....                                                                                            | 28 |
| Table 2    | Entity activity groups: application name.....                                                                                | 30 |
| Table 3    | Entity activity groups: application name.....                                                                                | 38 |

## 1. SCOPE

SAE is developing a number of standards, including the SAE J2945/x and SAE J3161/x series, that specify a set of applications using message sets from the SAE J2735 data dictionary. ("Application" is used here to mean "a collection of activities including interactions between different entities in the service of a collection of related goals and associated with a given IEEE Provider Service Identifier (PSID)"). Authenticity and integrity of the communications for these applications are ensured using digital signatures and IEEE 1609.2 digital certificates, which also indicate the permissions of the senders using Provider Service Identifiers (PSIDs) and Service Specific Permissions (SSPs). The PSID is a globally unique identifier associated with an application specification that unambiguously describes how to build interoperable instances of that application. If the application features multiple activities such that different activities have different security impacts, correspond to different roles, or require different capabilities, then the application specifier should define an SSP data structure such that the contents of the SSP in a given certificate indicate which activities the certificate holder is entitled to carry out.

This document establishes a security systems engineering process that can be used by future application specifiers to (1) determine which fields and activities should be subject to SSP constraints, and (2) specify a syntax and semantics for the SSPs for that application. It also addresses the development of SSPs for scenarios not addressed in the original application specification; for example, arising from regional extensions, changes in application functionality, or future expansions of the base SAE J2735 standard.

## 2. REFERENCES

### 2.1 Applicable Documents

The following publications form a part of this specification to the extent specified herein. Unless otherwise indicated, the latest issue of SAE publications shall apply.

#### 2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), [www.sae.org](http://www.sae.org).

- [1] SAE J2945: Dedicated Short Range Communication (DSRC) Systems Engineering Process Guidance for SAE J2945/x Documents and Common Design Concepts, December 2017
- [2] SAE J2735: Dedicated Short Range Communications (DSRC) Message Set Dictionary, March 2016
- [3] SAE J2540-2: ITIS Phrase Lists (International Traveler Information Systems), November 2009

#### 2.1.2 IEEE Publications

Available from IEEE Operations Center, 445 and 501 Hoes Lane, Piscataway, NJ 08854-4141, Tel: 732-981-0060, [www.ieee.org](http://www.ieee.org).

- [4] IEEE 1233-1998 (R2002): IEEE Guide for Developing System Requirements Specifications (Replaced by ISO/IEC/IEEE 29148:2011 (<https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:29148:ed-1:v1:en>))
- [5] IEEE 1609.0-2019: IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture
- [6] IEEE 1609.2-2016: IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages
- [7] IEEE 1609.2a-2017: IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages - Amendment 1
- [8] IEEE 1609.2b-2019: IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages Amendment 2 - PDU Functional Types and Encryption Key Management
- [9] IEEE 1609.12-2016: IEEE Standard for Wireless Access in Vehicular Environments - Identifier Allocations

It should be noted that there are additional standards in the 1609 suite which are not directly referenced here but may also be of assistance to implementers.

### 2.1.3 ISO Publications

Copies of these documents are available online at <http://webstore.ansi.org/>.

- [10] ISO/IEC 8824-1:1998: Information Technology - Abstract Syntax Notation One (ASN.1): Specification of Basic Notation
- [11] ISO/IEC 8824-2:1998: Information Technology - Abstract Syntax Notation One (ASN.1): Information Object Specification
- [12] ISO/IEC 8824-3:1998: Information Technology - Abstract Syntax Notation One (ASN.1): Constraint Specification
- [13] ISO/IEC 8824-4:1998: Information Technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 Specifications
- [14] ISO 14816-2019: Road Transport and Traffic Telematics - Automatic Vehicle and Equipment Identification - Numbering and Data Structure

### 2.1.4 NIST Publications

Available from NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD 20899-1070, Tel: 301-975-6478, [www.nist.gov](http://www.nist.gov).

- [15] NIST Standards for Security Categorization of Federal Information and Information Systems [FIPS PUB 199], February 2004

### 2.1.5 Other References

All documents cited here are considered informative with respect to SAE J2945/5.

- [16] Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT), U.S. DOT ITS JPO, 1200 New Jersey Avenue, SE, Washington, DC 20590, <http://local.iteris.com/arc-it/> (last accessed September 2017)
- [17] ETSI EN 302 637-2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service
- [18] ETSI TS 103 097: Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats
- [19] IETF Request for Comments (RFC) 8446, The Transport Layer Security (TLS) Protocol Version 1.3
- [20] IETF Request for Comments (RFC) 5246, The Transport Layer Security (TLS) Protocol Version 1.2
- [21] ISO TS 19091: Intelligent Transport Systems - Cooperative ITS - Using V2I and I2V Communications for Applications Related to Signalized Intersections
- [22] ISO TS 21177: Intelligent Transport Systems - ITS Station Security Services for Secure Session Establishment and Authentication Between Trusted Devices
- [23] SAE J2945/3: Requirements for V2I Weather Applications

### 3. DEFINITIONS

#### 3.1 General Statements

This outline section is included to comply with NTCIP format.<sup>1</sup> There is no content for this section in this standard.

#### 3.2 Terms

For the purposes of this document, the definitions, abbreviations, and acronyms found in SAE J2735 and SAE J2945 also apply. The following additional definitions, abbreviations, and acronyms supersede those found in SAE J2735 and SAE J2945 in the case of conflict. Any such conflicts are identified in the definitions below.

##### 3.2.1 ACCESS CONTROL POLICY

A policy stating the conditions under which an entity may carry out a particular application activity.

##### 3.2.2 ACTOR

Refer to SAE J2945.

##### 3.2.3 APPLICATION

A collection of activities including interactions between different entities in the service of a collection of related goals and related to a particular Provider Service Identifier (PSID).

NOTE: This term is overloaded and, in particular, some stakeholders would identify multiple different applications associated with a single PSID.

##### 3.2.4 APPLICATION ACTIVITY

A set of actions within an application intended to achieve a particular goal or set of goals.

##### 3.2.5 APPLICATION SPECIFICATION

A specification that can be used to implement an application.

##### 3.2.6 APPLICATION SPECIFIER

A stakeholder or group of stakeholders that produces an application specification.

##### 3.2.7 APPLICATION PROTOCOL DATA UNIT (APDU)

A well-structured set of data elements and data frames that can be sent as a unit between devices to convey some semantic meaning in the context of an application. The APDU does not include headers and footers added by network stack entities. Corresponds to: Message in SAE J2945.

##### 3.2.8 AUTHORIZATION

A security service demonstrating that an entity has particular permissions. Also used to refer to the specific permissions that an entity has.

---

<sup>1</sup> "NTCIP format" is used throughout this document to refer to the document structure defined in NTCIP 8002 Annex B, version 04.

### 3.2.9 CERTIFICATE AUTHORITY

A trusted entity that checks the entitlement of entities to digital certificates with particular contents and issues digital certificates to those entities.

NOTE: This is different from the definition in SAE J2945 and SAE J2735.

### 3.2.10 CERTIFICATE HOLDER

The “owner” of an IEEE 1609.2 certificate, i.e., the entity entitled to sign secured protocol data units (SPDUs) with the private key associated with a certificate such that the signature can be verified by that certificate.

### 3.2.11 CONCEPT OF OPERATIONS

Refer to SAE J2945.

### 3.2.12 CONFIDENTIALITY

A security service protecting against data being read by unauthorized actors.

### 3.2.13 CONNECTED VEHICLE

Refer to SAE J2945.

### 3.2.14 CORE APPLICATION SPECIFICATION TEAM

The subset of stakeholders within an application specifier responsible for specifying core application functionality, as opposed to (for example) management or security operations.

### 3.2.15 DATA CONCEPT

Refer to SAE J2735.

### 3.2.16 DATA DICTIONARY

Refer to SAE J2735.

### 3.2.17 DATA FRAME

Refer to SAE J2735.

### 3.2.18 DIGITAL CERTIFICATE

A digital document, issued by a trusted party known as a Certificate Authority (CA), that binds a cryptographic public key to an identity or set of permissions, so that, by carrying out an operation with the private key corresponding to that public key, the certificate holder can indicate that they have that identity or those permissions.

### 3.2.19 DRIVER

Refer to SAE J2945.

### 3.2.20 ENROLLMENT REQUIREMENTS

The requirements that an actor within the system must demonstrate that they satisfy in order to receive a certificate with particular permissions.

### 3.2.21 ENTITY

Refer to SAE J2945.

### 3.2.22 ENTITY ACTIVITY GROUP

A group of activities carried out within a particular application that have similar security impacts.

### 3.2.23 EXTENDED AUTHENTICATION (IN THE CONTEXT OF ISO TS 21177)

A security activity in which an entity, which has already presented evidence of its authorizations, presents additional evidence of additional authorizations.

### 3.2.24 EXTENSIBILITY MARKER

An ASN.1 feature used to indicate that an ASN.1 structure may have additional fields added in future versions of its specification.

### 3.2.25 IMPACT

A measure of the effect on a system of a failure of security in a particular application activity. In the context of a security analysis, the impact is usually categorized as low, medium, or high.

### 3.2.26 INFORMATION FLOW

A sequence of one or more messages which are exchanged in a known format between one or more sending actors and one or more receiving actors. Corresponds to: Dialog in SAE J2945.

### 3.2.27 INTEGRITY

A security service covering the reliability of received data. As used by the National Institute of Standards and Technology (NIST), integrity provides assurance that information is accurate and comes from an appropriate source. As used in a cryptographic context, integrity provides assurance that information has not been modified since it was generated by an appropriate source.

### 3.2.28 INTERNATIONAL TRAVELER INFORMATION SYSTEMS (ITIS)

Refer to SAE J2945.

### 3.2.29 ITIS CODE

A value defined in the ITIS context to have a particular meaning.

### 3.2.30 ITIS PHRASE

A sequence of ITIS codes.

### 3.2.31 PROVIDER SERVICE IDENTIFIER (PSID)

Refer to SAE J2735.

### 3.2.32 REGULATORY PRIVILEGE

The ability to request an activity such that if the receiver of the request fails to comply, there will be real-world law enforcement consequences.

### 3.2.33 SECURED PROTOCOL DATA UNIT (SPDU)

An Ieee1609Dot2Data as defined in IEEE 1609.2, of one of the types defined in IEEE 1609.2 (unsecured, signed, or encrypted), containing protocol data unit contents.

### 3.2.34 SECURITY CONTROL

A mechanism used to ensure that operations in the system meet the stated security requirements.

### 3.2.35 SECURITY SPECIFICATION TEAM

The subset of stakeholders within an application specifier responsible for analyzing security requirements and specifying security functionality.

### 3.2.36 SERVICE SPECIFIC PERMISSIONS (SSP)

A field in an IEEE 1609.2 certificate, bound to a specific Provider Service Identifier (PSID), indicating the permissions of the certificate holder to carry out specific activities within the set of activities defined by that PSID.

### 3.2.37 SSP ROLES

A synonym for entity activity groups. Contrast: Roles in SAE J2735.

### 3.2.38 SYSTEMS ENGINEERING PROCESS (SEP)

Refer to SAE J2945.

### 3.2.39 TRANSPORT LAYER SECURITY (TLS)

A protocol defined by the Internet Engineering Task Force (IETF) to provide end-to-end security for unicast application communications.

## 4. ABBREVIATIONS AND ACRONYMS

The additional abbreviations and acronyms cited below are terms related to this document (and the companion volumes and guides) unless specifically cited otherwise.

|        |                                               |
|--------|-----------------------------------------------|
| APDU   | Application Protocol Data Unit                |
| ASN.1  | Abstract Syntax Notation 1                    |
| BSM    | Basic Safety Message                          |
| CA     | Certificate Authority                         |
| C//I/A | Confidentiality/Integrity/Availability        |
| ConOps | Concept of Operations                         |
| FIPS   | Federal Information Processing Standards      |
| ISO    | International Standardization Organization    |
| ITIS   | International Traveler Information Systems    |
| PICS   | Protocol Implementation Conformance Statement |
| PDU    | Protocol Data Unit                            |
| PSID   | Provider Service Identifier                   |
| RSU    | Roadside Unit                                 |

|      |                              |
|------|------------------------------|
| SEP  | Systems Engineering Process  |
| SPaT | Signal Phase and Timing      |
| SPDU | Secured Protocol Data Unit   |
| SSP  | Service Specific Permissions |
| TLS  | Transport Layer Security     |

## 5. SSP DEVELOPMENT PROCESS (NORMATIVE)

### 5.1 Overview

This document provides a methodology that can be used to derive Service Specific Permissions (SSPs) for use with new connected vehicle applications based on SAE J2735. The goal of the methodology is to enable standards developers to specify security mechanisms and provide a solid rationale for those mechanisms.

This section provides:

- a. A detailed description of the SSP concept.
- b. An explanation of how SSPs fit into the larger context of security for a connected vehicle environment.
- c. A methodology that can be used by application specifiers to develop SSP specifications for their applications.

This section is intended for all users, including:

- a. Application specifiers.
- b. Application developers.
- c. Certificate and certification service providers.
- d. Transportation operations managers.
- e. Transportation operations personnel, including transportation weather specialists.
- f. Transportation engineers.
- g. System integrators.

Application specifiers will be assisted to understand what is involved in specifying a permissions model for their connected vehicle application's communications security approach. The permissions design is incorporated into application specification as part of a larger application security approach.

Application developers will gain a clearer understanding of the application logic to write when implementing security-related parts of the application specification, especially authorization decisions.

Certificate and certification service providers will gain a clearer understanding of distinct roles within an application and how the certification and the certificate-issuing process can be used to enforce those roles.

The remaining categories of users will gain a clearer understanding of how to think about communications security requirements for connected vehicle applications and what the security requirements may be for potential future deployments. For this audience, this section, and especially [5.3](#), serves as the starting point in the agency specification and procurement process.

## 5.2 SSP Overview

IEEE 1609.2 and its amendments, IEEE 1609.2a and IEEE 1609.2b, define security mechanisms to protect communications in the connected vehicle setting. IEEE 1609.2 defines a custom digital certificate format that allows the receiver of a protocol data unit (PDU) to determine the authorization of the sender of that PDU.

The Service Specific Permissions (SSP) field is a security control defined in the context of a particular connected vehicle application that uses IEEE 1609.2 certificates for communications security. The SSP is a field in a 1609.2 certificate, associated with a particular Provider Service Identifier (PSID), that indicates the permissions of the certificate holder to carry out particular activities in the application identified by the PSID.

“Application,” an overloaded term, means here “a collection of activities including interactions between different entities in the service of a collection of related goals and related to a particular Provider Service Identifier (PSID).” Application activities are carried out through information flows between actors. An information flow consists of the transmission and reception of one or more application protocol data units (APDUs). The IEEE 1609 suite of standards generally uses the term “service” or “higher layer” for what this document refers to as an application.

The sender of an application protocol data unit (APDU) demonstrates that they are authorized to send that APDU by the use of an IEEE 1609.2 certificate. There are two ways to use the certificate to demonstrate authorization:

- The certificate can be used to directly sign APDUs, resulting in a secure protocol data unit (SPDU) as defined in IEEE 1609.2.
- The certificate can be used in the context of a secure session to sign authentication packets that are transmitted separately from the APDUs themselves. Examples of this include signing the CertificateVerify message in Transport Layer Security (TLS) [\[19\]\[20\]](#) or Extended Authentication packets as defined in ISO 21177 [\[22\]](#).

The IEEE 1609.2 assumed architecture for sending and receiving directly signed APDUs is shown in [Figure 1](#). The 1609.2 security services are not a “layer” in the network stack, but instead are invoked directly by the receiving application. When a signed SPDU is received, the receiving application process may request that the 1609.2 security services determine its validity. This is done by carrying out several tests, including cryptographic verification, certificate validity (not expired, not revoked, etc.), and consistency between the certificate and the 1609.2 security “header info” added to the signed SPDU. If any of the tests fails, the SPDU is considered invalid. The 1609.2 security services return to the application an indication of the validity of the signed SPDU. Handling of invalid SPDUs is to be defined by the application, but at the very least a receiver should not cause an application activity to be carried out based on SPDUs that are determined to be invalid.

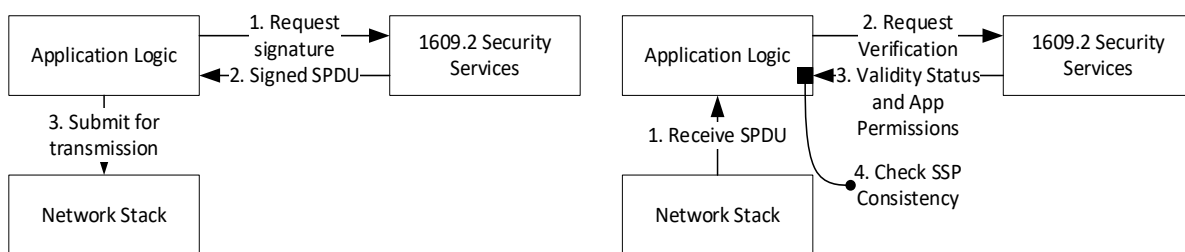


**Figure 1 - Sending/receiving architecture for applications using IEEE 1609.2 certificates to authorize individual messages**

If a signed SPDU passes the validity tests that can be carried out by the security services, there is one further step to be carried out before it can be accepted as valid by the application. This step is carried out by the application logic itself and is to check that the payload of the SPDU is consistent with the specific application permissions in the certificate.

A sender's permissions are encoded in a 1609.2 certificate by a combination of two identifiers:

- The Provider Service Identifier (PSID) identifies the “application,” in the sense of “a set of specific information flows.”
- The Service Specific Permissions (SSP) is associated with the PSID and identifies the specific *application activities* that a sender can carry out. This can include identifying:
  - The information flows within the application in which the certificate holder can act as the sender.
  - Particular constraints on what the certificate holder can send within each information flow. The constraints can take any form. Examples of possible constraints include: specific fields or substructures that can be included in individual messages; specific ranges of values that can appear in specific fields; and specific updates of receiver state or other responses by the receiver that can be requested, explicitly or implicitly, by the sender.

An application specification may define that no SSP is associated with the application if, following the analysis outlined in this document, it is determined that there is no need for an SSP. This could be the case, for example, if there is only a single role within the application, i.e., all actors do essentially the same thing.

[Figure 2](#) shows the processing model that fits the 1609.2 security model. The 1609.2 security services check the validity of the information available to those services. However, the match between the appPermissions in the certificate and the application contents of the SPDU is application-specific and so cannot be checked by the security services. Instead, the security services return the appropriate PSID and SSP from the certificate (selected by the PSID in the 1609.2 HeaderInfo field in the signed SPDU) and the application determines whether the contents of the APDU (or, more broadly, the action that the APDU is requesting) are consistent with the PSID and SSP, as defined by the application specification.

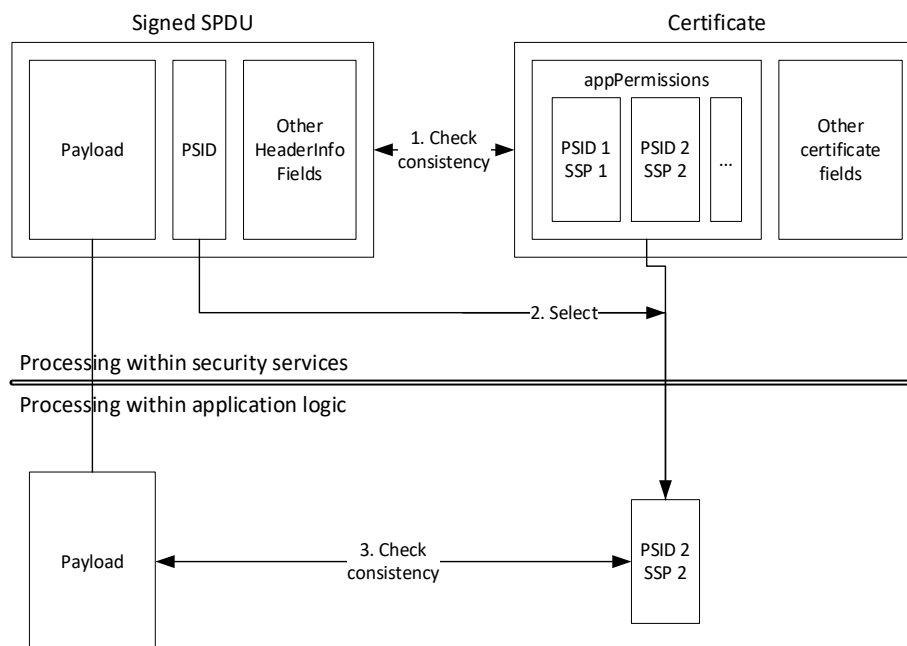


**Figure 2 - 1609.2 consistency conditions: checked by security services and by application logic**

[Figures 3](#) and [4](#) show this in more detail: the 1609.2 security services can check a number of consistency conditions ([Figure 3](#)), but the determination of consistency between the APDU contents and the PSID/SSP must be carried out by application logic ([Figure 4](#)).

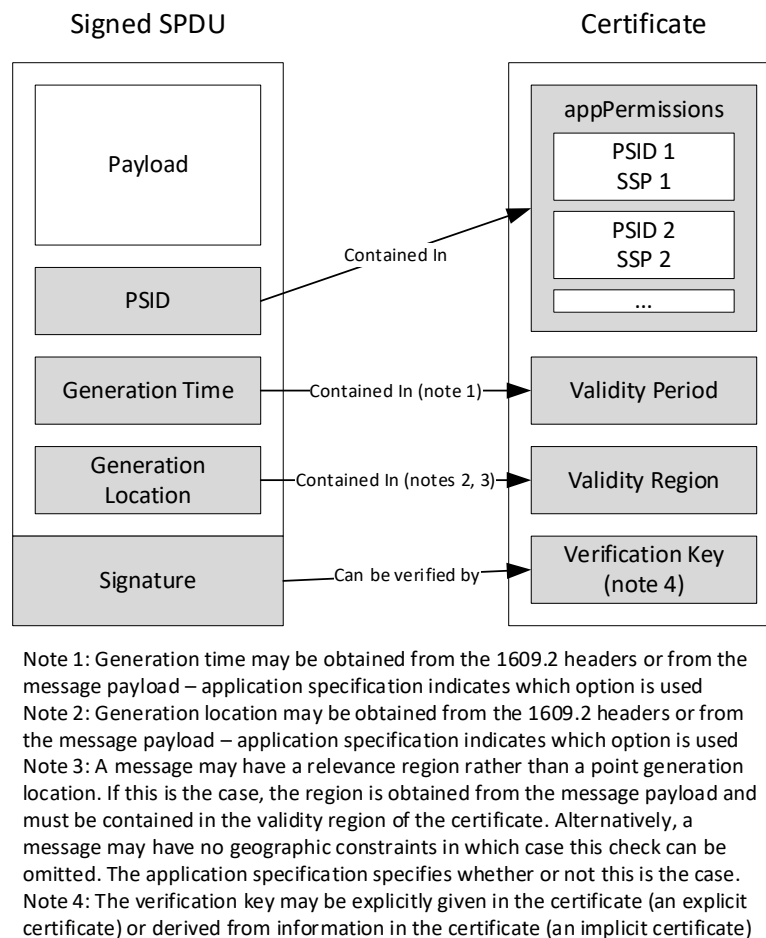


**Figure 3 - Consistency conditions to be checked by the security services**

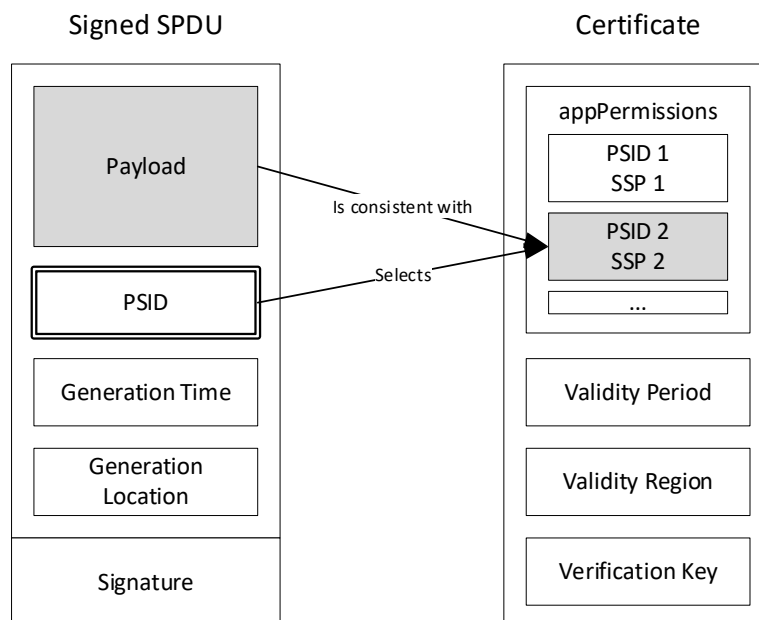


**Figure 4 - Consistency conditions to be checked by the application**

This discussion illustrates that:

- The SSP design (syntax and semantics) are part of the application specification.
- The specification of how a received APDU is determined to be consistent with the SSP is part of the application specification.

An application specification that uses 1609.2 certificates is not complete unless it specifies:

- Whether SSPs are to be used.
- If SSPs are to be used, their syntax, semantics, and consistency logic.

The mapping from a given SSP encoding to a set of permitted actions is part of the application specification and, as part of generating an application specification through a systems engineering process (SEP), the application specifiers are expected to provide a full specification of the syntax and semantics of the SSP for the application. The goal of this section of this document is to specify a methodology that can be used by application specifiers to develop the SSP syntax and semantics for their connected vehicle applications.

NOTE: The existence of a specific PSID/SSP that grants permission to send a particular APDU, and the existence of a valid certificate that includes that SSP, are not an absolute guarantee that all communications from a device that owns that certificate will be correct. SSPs and certificates with those SSPs cannot prevent (intentional or accidental) misbehavior of devices, but can only serve to limit the scope or impact of that misbehavior. This does not in any way eliminate the need for misbehavior detection and the action of a misbehavior authority to deal with rogue devices sending bogus or misleading messages with valid certificates, but the creation of unique SSPs is a way to acknowledge that certain messages or classes of messages (e.g., BSM) have a lower (but still non-zero) potential for abuse or misuse than other messages or classes of messages (e.g., SPaT, or messages related to emergency vehicle actions), and it is desirable to restrict certificates that include the SSPs for more “dangerous” messages to a smaller set of devices intended for installation in RSUs, emergency vehicles, or other specialized vehicles.

#### 5.2.1 Security Deployment Lifecycle for Applications Using 1609.2 Certificates

[Figure 5](#) illustrates the security deployment lifecycle for applications using 1609.2 certificates. The lifecycle has three steps. Step A is the Design step; Step B is the Security Provisioning step; Step C is the Operating step.

In Step A, Design, a stakeholder organization (the design actor in [Figure 5](#)) develops the application design. The stakeholder organization specifies:

- The application design itself, which includes a specification of the consistency rules to be applied when an end-entity actor (the “sender”) sends an authenticated message to another end-entity actor (the “receiver”). In other words, the design includes the syntax and semantics for the SSP. The SSP is associated with the PSID that identifies the application design; the intent is that the design stakeholder organization that develops the design does so with the knowledge and approval of the organization that owns (or has been assigned) the PSID. (One natural way to achieve this is for the design stakeholder organization to be the same as the PSID owning organization.)

This application design is embodied in the application implementations and installed on sending and receiving end-entities.

- The properties that a sender must demonstrate that they have in order to get a certificate with permission fields set. The certificate is issued by an authorization actor known as a Certificate Authority (CA). For example, for a sender to be provided with a certificate that shows it is an emergency vehicle, the CA must be satisfied that the sender is an emergency vehicle. The processes that the sending end entity uses to demonstrate its eligibility for a certificate, or at least the requirements for those processes, are specified by the design actor and made known to the CA and to developers of sender end entities. These processes and/or requirements are referred to as *enrollment requirements*.

NOTE: This document does not address how these requirements are to be developed.

In Step B, Security Provisioning, a sender end entity demonstrates to an authorization actor (a CA) that it meets the enrollment requirements for a set of application permissions. The authorization actor responds by issuing the sender with a certificate with those permissions.

In Step C, Operations, a sender end entity and a receiver end entity interact. The sender communicates with the receiver to send it data, requests, commands, or other interactions. For each interaction, the receiver determines whether the interaction is permitted by the sender's permissions, as shown in [Figures 1, 2, 3, and 4](#).

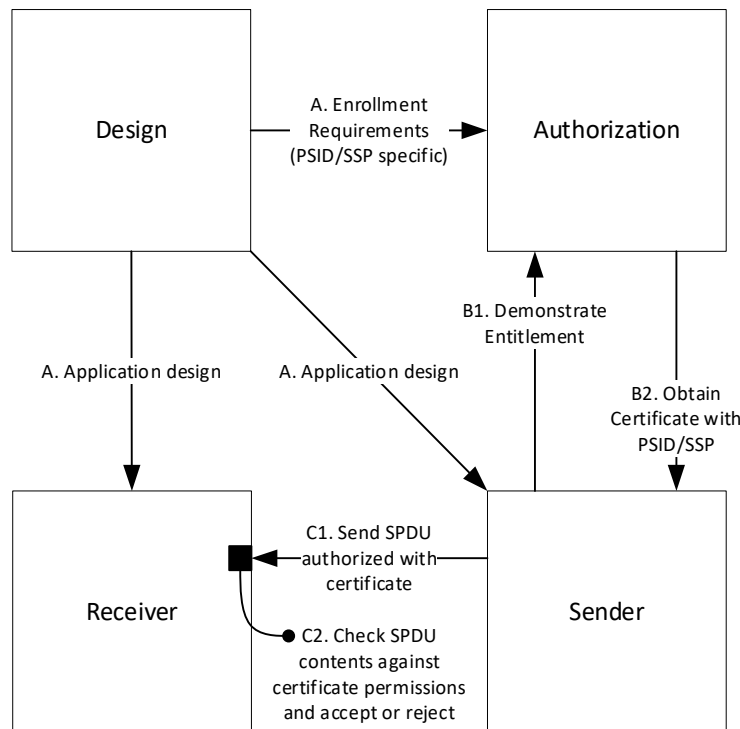


**Figure 5 - Security deployment lifecycle for applications using 1609.2 certificates**

As stated, the primary goal of this document is to assist design actors in creating the application permission related aspects of their application design via the specification of SSPs. The rest of this section provides a methodology for carrying out that design work. It is important to note, however, that SSPs only truly protect a receiver against a rogue sender if the enrollment requirements are also specified and rigorously enforced. The topic of enrollment requirements is out of scope for this document.

### 5.2.2 SSP Encoding Options and Recommended SSP Type

This section reviews types of SSP specified in IEEE 1609.2 and recommends the type that should be used for SSPs developed according to the methodology in this document.

IEEE 1609.2 certificates use PSID and SSP to express three different types of permissions:

- Application permissions, i.e., what the certificate holder can communicate in an application. These are contained in the 1609.2 certificate *appPermissions* field.
- Certificate request permissions, i.e., the permissions that an end entity is allowed to request in an application certificate request. These are contained in the 1609.2 certificate *certRequestPermissions* field.
- Certificate issuance permissions, i.e., the permissions a CA certificate holder is allowed to include in certificates it issues. These are contained in the 1609.2 certificate *certIssuePermissions* field.

1609.2 defines consistency rules to use to determine whether a CA certificate was permitted to issue a subordinate CA or an end-entity certificate. A 1609.2 certificate is invalid if the issuing CA did not have permissions to issue it. APDUs authorized by an invalid certificate should be considered invalid.