

Section 1 Overview

1.1 General

This document addresses the development of security material for application specifications in SAE V2X Technical Committees. The assumption in this document is that two groups with distinct missions contribute to the development of each standard: the “Application Specification Team” is in charge of specifying the application functionality and the “Security Specification Team” is in charge of specifying the security. The two teams may, of course, have a significant overlap of members.

1.2 Development of the Initial Specification

The phases in the systems engineering process should include the following security-related activities.

Phase 1, Concept of Operations: After the Application Specification Team has developed stable ConOps material, the security team should:

1. **Document assumptions**, especially about roles in the application, receive-side behavior, and whether a single device can take on multiple roles. The assumptions about receive-side behavior are important as they allow the Security Specification Team to understand the impact of false messages.
2. **Analyze and derive security requirements** as specified in Section 2.
3. **Iterate with the Application Specification Team**. For example, the assumptions documented may illustrate that use cases used as basis for the ConOps need to be updated. The steps above are iterated through until the ConOps and the security analysis are stable.

Phase 2, Requirements: Once the Application Specification Team has developed stable requirements, the Security Specification Team should:

1. **Review assumptions** to see if they have changed as a result of the requirements process.
2. **Analyze and derive security requirements** as specified in Section 2.
3. **Make requirements recommendations at the appropriate level of specificity**; for example, recommend whether authentication and authorization should be provided by IEEE 1609.2 certificates, some other means, or both. The requirements recommendations for an information flow within the application may be influenced by security requirements for similar information flows in different applications.
4. **Iterate with the Application Specification Team** to integrate security requirements into the specification. The steps above are iterated through until the application requirements and the security analysis of the requirements are stable.

Phase 3, Design: Once the Application Specification Team has developed stable design material, the security team should:

1. **Review assumptions** to see if they have changed as a result of the requirements process.
2. **Analyze and derive security requirements** as specified in Section 2. If there are roles in the application, and the application is using 1609.2 certificates, this step will derive the requirements for Service Specific Permissions (SSPs).
3. **Analyze whether design decisions have an impact on the security requirements** and recommend design changes if necessary.
4. **Specify security controls**
 - Specify the security mechanism(s) that will protect broadcast and unicast messages within the system. This includes security protocols and the authentication requirements, e.g., participants are authenticated via X.509 certificates, identified via 1609.2 certificates, or identified via username and password.
 - If the system uses 1609.2 certificates, specify the PSID and SSP structure and provide a 1609.2 security profile (or more than one, if different roles within the application require different security profiles). The security profile addresses topics including whether pseudonymity is necessary, whether misbehaving devices are to be revoked or allowed to age out of the system, and whether there should be geographic limitations on where actors can carry out the application activities.
 - If the system uses ISO 21177, specify all the items noted in the previous bullet point as to be specified for 1609.2, and additionally provide an ISO 21177 access control policy.

The security design for an information flow within the application may be influenced by the security design for similar information flows in different applications.

5. **Specify data operations at each functional element within the architecture**, as described in 2.2.
6. **Optionally, include informative material about future security controls.** The following controls do not need to be included in the first version of the specification, but that version may (and, if possible, should) contain informative considerations that will influence the development of those controls.
 - Enrollment processes.
 - Misbehavior detection and reporting: in particular, there should be a definition of what constitutes a misbehaving transmission, even if specific mechanisms for detection and reporting are not defined.
 - Revocation/restoration policy (and other end-of-life considerations).
7. **Iterate with the Application Specification Team** until the design, including the security controls, is stable.

1.3 Activities After the Initial Specification is Prepared

The following security procedures need not be part of the initial specification; but they should be carried out as deployment moves forward. This document assumes the following lifecycle for application deployments:

1. Initial specification produced following the principles above.
2. Initial small-scale deployment. In these deployments the impact of breaches of confidentiality or authentication is low, relative to a full deployment, and the goal is to establish that the application functionally works in practice. As such, the application can be deployed without a full security strategy being in place.
3. Full-scale deployment. At this stage, a full security strategy is required for the deployment to be secure.