Connected Vehicle Pilot Security Profiles

Provider Service Identifiers and Service Specific Permissions (SSPs) used by the CV Pilot Sites

www.its.dot.gov/index.htm

Report – May 2020
FHWA-JPO-19-778

U.S. Department of Transportation

1. Report No. FHWA-JPO-19-778	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle Connected Vehicles Pilot Security Profiles, Provider Service Identifier and Service Specific Permissions (SSPs) used by the CV Pilot Sites		5. Report Date May 2020 6. Performing Organization Code:
7. Author(s) J.D. Schneeberger (Noblis), Amy O'Hara (Noblis), David Benevelli (TransCore). Tony English (Neaera Consulting), Steve Johnson (HNTB), Steve Novosad (HNTB), and Bob Rausch (TransCore)		8. Performing Organization Report No.
9. Performing Organization Name and Address Noblis 500 L'Enfant Plaza, S.W., Suite 900 Washington, DC 20024		10. Work Unit No. 11. Contract or Grant No.
12. Sponsoring Agency Name and Address ITS Joint Program Office 1200 New Jersey Ave., SE Washington, DC 20590		13. Type of Report and Period Technical Primer 14. Sponsoring Agency code HOIT-1
15. Supplementary Notes Michelle Noch (COR)		

16. Abstract
This document provides Security profiles being used by the CV Pilot sites and is intended to be used to inform early deployers and guide them to make the best choices for their own deployments. The Connected Vehicle Pilot sites worked collaboratively with the USDOT, their roadside unit (RSU) and onboard unit (OBU) vendors, and their security credential management system (SCMS) vendor (which was the same for all three sites) to jointly develop Service Specific Permissions (SSP) guidance for all of the Provider Service Identifiers (PSIDs) they were implementing. Technical leads from the CV Pilot Sites –and some of their vendors—included members that had subject matter expertise with the SAE and IEEE standards associated with PSIDs and SSPs.

17. Key Words	18. Distribution Statement
CV Pilot, Connected Vehicles, Security Profiles, Basic Safety Message (BSM), Traveler Information Message (TIM), MAP, Signal Phase and Timing (SPaT), Signal Status Message (SSM), Signal Request Message (SRM), Wave Service Advertisement (WSA), Service Specific Permission (SSP)	This document is available to the public through the ITS JPO PCB website.

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 47	22. Price

U.S. Department of Transportation

Connected Vehicle Pilot Sites Security Profiles

Provider Service Identifiers and Service Specific Permissions (SSPs) used by the CV Pilot Sites

The USDOT's CV Pilot Sites – New York City, Tampa-Hillsborough Expressway Authority (THEA), and Wyoming Department of Transportation (WYDOT) – are the vanguard in moving the connected vehicle standards into practice and paving the way for future deployers. A key challenge for the CV Pilot Sites in implementing connected vehicle devices was the lack of specific SSP guidance for many of the applications that they were deploying. V2I messages associated with intersection safety and awareness applications – including SPAT, Map Data (MAP), Signal Request Message (SRM), Signal Status Message (SSM) and Traveler Information Message (TIM) – did not have performance requirements or SSP guidance defined in a SAE J2945/X series standard, yet. The guidance for implementing BSM Part 2 SSPs had not been formally published and was still in draft status. Finally, the CV Pilot Sites are the first entities trying to deploy these devices using PSIDs with a production level SCMS.

To overcome this challenge, the CV Pilot Sites worked collaboratively with the USDOT, their RSU and OBU vendors, and their SCMS vendor (which was the same for all three sites) to jointly develop SSP guidance for all of the PSIDs they were implementing. Technical leads from the CV Pilot Sites –and some of their vendors—included members that had subject matter expertise with the SAE and IEEE standards associated with PSIDs and SSPs.

The Security Profiles presented in Appendices A-G are based on the specific needs of the CV Pilot Sites. The information gleaned from the CV Pilot deployment experiences is provided in the following section to inform early deployers and guide them to make the best choices for their own deployments. SAE is currently developing guidance on creating SSPs. While that guidance is being developed, examples from the CV Pilot Sites are made available in this primer to assist early deployers in the meantime.

Additional information concerning PSIDs can be found at: https://standards.ieee.org/develop/regauth/psid/index.html. Links to PSID tutorial and FAQs are also listed at the link provided.

IEEE is the registrar for all PSIDs. The list of all PSIDs that have been registered to date can be found at: https://standards.ieee.org/develop/regauth/psid/public.html.

For Society of Automotive Engineers (SAE) owned PSIDs, the guidance for SSPs can be found in SAE J2945/5, although not all SAE owned PSIDs have SSP guidance as of this writing. Implementing SSPs is an important element of deploying secure applications.

Appendix A – CV Pilots Security Profile Summary

Below is a summary of the PSIDs and SSPs used for the CV Pilot Deployments

Table A-1: Summary of PSIDs and SSPs used by CV Pilot Deployments (Source: CV Pilot Sites)

Application (Message)	PSID Value (hex)	SSP
Basic Safety Message (BSM)	0x20	--
Traveler Information Message (TIM)	0x83	00 80 01 F0 40
MAP Message	0x20-40-97	00 80 01 20 40
Signal Phase and Timing (SPaT)	0x82	00 80 01 30 40
Signal Status Message (SSM)	0x20-40-95	00 00 01 E0 40
Signal Request Message (SRM)	0x20-40-96	00 80 01 D0 40
Distress Notification	0x40-82	00 80 01 F0 40
Mobile Probe Exchange (PVD) and Mobile Probe Exchange (PDM)	0x84	--
Wave Service Advertisements (WSA)	0x87	--

BSM Application Security Profile and SSPs for the Connected Vehicle Pilot Deployment Projects

Version 11, 2018-04-06

General

BSM Security Profile for CV Pilot

All BSM messages in CV pilot will use the SAE J2945/1 Security Profile.

References in this document to BSM Part 2 content refer to those Part 2 data elements beyond the Part 2 data elements identified in SAE J2945/1.

All certificates will be pseudonym certificates.

General SSP Requirements

In order to send BSMs, a device must have:

- A certificate
  - Containing an `appPermissions` field
    - Containing a `PsidSsp` structure
      - Where the `psid` field is 0x20 and the SSP is as specified below.

A BSM containing ONLY Part 1 content and NO Part 2 content does not need an SSP in the PsidSsp element. It only needs the PSID value of 0x20.

Table 1 and Table 2 contains a list of Part2 message content, aside the SAE J2945/1 Part 2 content, that is permitted for use in Pilot Deployments.

Any Part2 content that is not identified in Table1 or Table 2 is not permitted to be sent in Pilot Deployments.

Any Part2 content that is not identified in Table 1 or Table 2 is not permitted to be acted upon in Pilot Deployments.

- EXCEPTION: BSM receiving applications MAY be programmed to accept Part2 fields identified in J2945/2, with the appropriate SSP as defined in J2945/2.
- NOTE: If a BSM is received contains BOTH authorized fields AND unauthorized Part2 fields, the unauthorized Part2 fields should be rejected but the authorized fields should be accepted.

Senders do not need an SSP to send Part2 content that is identified in Table 1 or Table 2, i.e. these senders may have certificates with the PSID = 0x20 and the SSP omitted. In other words:

- All BSM receiving applications on Pilot Deployment devices are programmed to accept the Part2 fields identified in Table 1 or Table 2.
- All BSM receiving applications on Pilot Deployment devices are programmed to reject any other Part2 fields.
  - EXCEPTION: BSM receiving applications MAY be programmed to accept Part2 fields identified in J2945/2, with the appropriate SSP as defined in J2945/2.
- BSM sending applications may be configured to send the Part2 fields identified in Table 1 or Table 2. This is a decision up to the Pilot Deployment site and does not involve

intervention by the SCMS. The Pilot Deployment sites are responsible for ensuring that the configuration process is secure and will not result in any BSM sending application including incorrect fields.

Table B-1: BSM Part 2 Elements: Methods of Constraint and Pertinent Vehicle Type (Source: CV Pilot Sites)

Constrained BSM Part 2 Field	Applicable CV Pilot Vehicle Types
supplementalVehicleExt.keyType in range from 25-35 (truck-*)	Garbage Truck (NYC) Package Truck (NYC) Long-Haul Truck (NYC & WY) Asphalt Dump Truck (NYC) Sand/Snowplow (WY)
supplementalVehicleExt.keyType in range from 50-58 (transit-*)	MTA Bus (NYC) Bus (THEA: keyType == transit-TypeUnknown) Streetcar (THEA: keyType == transit-FixedGuideway)
supplementalVehicleExt.classDetails.hpmsType = 2 (special)	Streetcar (THEA)
supplementalVehicleExt.classDetails.hpmsType = 4 (car)	Taxi (NYC)
supplementalVehicleExt.classDetails.hpmsType =6 (bus)	Transit Bus (NYC and THEA)
supplementalVehicleExt.classDetails.hpmsType =7 (axleCnt2)	Garbage Truck (NYC)
supplementalVehicleExt.classDetails.hpmsType =8 (axleCnt3)	Garbage Truck (NYC) Asphalt Dump Truck (NYC) Sand/Snowplow (WY)
supplementalVehicleExt.classDetails.hpmsType =10 (axleCnt4Trailer)	Long-Haul Truck w/Trailer (WY)
supplementalVehicleExt.classDetails.hpmsType =11 (axleCnt5Trailer)	Long-Haul Truck w/Trailer (WY)
supplementalVehicleExt.classDetails.hpmsType =14 (axleCnt6MultiTrailer)	Long-Haul Truck (WY)
supplementalVehicleExt.classDetails.role =9 (truck)	Garbage Truck (NYC) Package Truck (NYC) Long-Haul Truck (NYC & WY) Asphalt Dump Truck (NYC) Sand/Snowplow (WY)
supplementalVehicleExt.classDetails.role =15 (dot)	DoT Pickup (NYC) DoT Pickup (WY) Asphalt Dump Truck (NYC) Sand / Snowplow (WY)
supplementalVehicleExt.classDetails.role =16 (transit)	Taxi (NYC) MTA Bus (NYC) Bus (THEA) Streetcar (THEA)

Table B-2: BSM Part 2 Elements: Additional Constrained Data Constructs (Source: CV Pilot Sites)

Constrained BSM Part 2 Data Constructs	Notes
specialVehicleExt.trailers including its child data frames and elements	Provides trailer descriptions
supplementalVehicleExt.vehicleData.height	Provides Overheight Vehicle information
supplementalVehicleExt.vehicleData.mass	Provides trailer descriptions
supplementalVehicleExt.vehicleData.trailerWeight	Provides trailer descriptions

MAP Application Security Profile and SSPs for the Connected Vehicle Pilot Deployment Projects

Version 10, 2018-05-21

MAP Description and Security Needs

Signal phase and timing messages in the CV pilots will be sent from supported intersection Roadside Equipment (RSE) at a rate of approximately once per second per intersection. MAP messages provide intersection geometry pertinent to driver applications that rely on detailed messaging regarding intersection state (e.g., Signal Phase and Timing [SPaT]).

While the RSE digitally signs SPaT messages, MAP messages are more static in nature. MAP messages can therefore be either locally signed by the RSE or 'centrally signed,' i.e., signed by the Traffic Management Center (TMC).

Note that the CV Pilots will use a unique MAP message PSID.

The security concerns this security profile should address include the following:

Table C-1: Application-specific Security Concerns (Source: CV Pilot Sites)

Application-Specific Security Concerns	**Mitigations Supported by Security Profile**
Replay	Receiving security application shall support detection of replay attack. In addition, replay is a concern if the replayed message indicates an old intersection MAP configuration that is still within the validity period of the signing certificate. For that reason, the MAP messages should contain a reasonable expiration time (assuming the signer's authorization cert has a long validity period).
Integrity errors	The sending application needs to digitally sign the messages. False intersection geometry descriptions could severely impact V2I applications.
Message spoofing	MAP messages need to be digitally signed by the RSE or TMC to ensure data origin and non-repudiation. There is no need to encrypt.
Signing certificate not authorized to provision MAP data for a given intersection or intersections within a given region.	The RSE or TMC should only be transmitting MAP messages for intersection(s) for which it has authority. The signing certificate needs to indicate a geographic restriction that definitively contains/overlaps the geographic constraint of the intersection(s).
Revoked RSE transmitting	End entities should have reasonably fresh CRL information with respect to the validity period of the RSE certificate (~2 months)

Application-Specific Security Concerns	Mitigations Supported by Security Profile
Incorrect entity signs message	Only either the RSE or TMC should be able to digitally sign MAP messages.
Unauthorized entity creates/signs a regulated speed value	Only an SSP-authorized entity (i.e., TMC or RSE, for region in question) will be able to sign a MAP message that indicates a regulated speed within the domain of the MAP.

IEEE 1609.2 Security Profile Identification

The following table provides the identification features for the CV Pilot MAP application security profile.

Table C-2: CV Pilot MAP Application Security Profile Identification (Source: CV Pilot Sites)

Name	Type	Recommended values	Description
Name	Text string	"CV Pilot MAP Security Profile"	
PSIDs	List of PSIDs	HEX: (0x20-40-97) P-ENC: (0pE0-00-00-17) DEC: (2,113,687)	The PSID to be used by SDEEs that use this profile.
Other considerations	Text string	This MAP security profile is designated for the Connected Vehicle Pilot Program	A description of the conditions under which this security profile is to be used.

Sending

The following table provides the security profile for message sending within the MAP PSID.

Table C-3: CV Pilot MAP Application Security Profile for Sending Messages (Source: CV Pilot Sites)

Name	Type	Recommended values	Notes
Sign Data	enumerated	True	Sign all MAP messages for data origin authentication and non-repudiation
Signed Data in Payload	Boolean	True	
External Data	Boolean	False	Otherwise we need to populate - tbsData.payload.extDataHash
External Data Source	Text	N/A	
External Data Hash Algorithm	enumerated	N/A	
Set Generation Time in Security Headers	Boolean	True	
Set Generation Location in Security Headers	Boolean	False	Signed messages do not need to indicate generation location. The signing certificate will indicate 'authority to sign' for a given region.

Name	Type	Recommended values	Notes
Set Expiry Time in Security Headers	Boolean	True	Lane closures or other intersection impediments may be somewhat dynamic, requiring multiple MAP message updates within the signer authorization certificate's validity period.
Signed SPDU Lifetime	Time interval	"72 Hours"	The signing application needs to set the time interval for this SPDU lifetime. 72 hours is the lifetime of the MAP message. Note that the NYC CV pilot anticipates refreshing the RSU every 4 hours as one aspect of its security program.
Signer Identifier Policy Type	Enumerated	Simple	
Simple Signer Identifier Policy: Minimum Inter Cert Time	Time interval (for example, "one second")	Always	All MAP messages will contain the signing public key certificate.
Simple Signer Identifier Policy: Exceptions	Boolean	False	
Simple Signer Identifier Policy: Signer Identifier Cert -Chain Length	Integer or enumerated	1	Will use the signer's authorization certificate only within the message. We will assume full pre-distribution of CA certs to the OBU/ASDs.
Text Signer Identifier Policy	Text	N/A	
Sign With Fast Verification	enumerated	Yes-Compressed	
EC Point Format	Enumerated	Compressed	
p2pcd_useInteractive-Form	Boolean	False	
p2pcd_max-ResponseBackoff	Time or n/a	N/A	
p2pcd_response-ActiveTimeout	Time or n/a	N/A	
p2pcd_request-ActiveTimeout	Time or n/a	N/A	
p2pcd_observed-RequestTimeout	Time or n/a	N/A	
p2pcd_currentlyUsed-TriggerCertificateTime	Time or n/a	N/A	
p2pcd_response-CountThreshold	Integer or n/a	N/A	
Repeat Signed SPDUs	Boolean	True	Following the initial, transmitted MAP PDU, each following one may be a re-transmit of the first so long as they are within the validity period of the message (as set by the signing application).
Time Between Signing	Time or n/a	Set to Message lifetime	
Encrypt Data	enumerated	No	MAP messages are in plaintext

Receiving

The following table provides the message reception security features for the MAP application security profile.

Table C-4: CV Pilot MAP Application Security Profile for Receiving Messages (Source: CV Pilot Sites)

Name	Type	Value	Notes
Use Preprocessing	Enumerated	True	The full cert chain will not be sent with MAP messages
Verify Data	Enumerated	True	Verify all MAP messages
Maximum Certificate Chain Length	Integer	4	
Relevance: Replay	Boolean	False	
Relevance: Generation Time in Past	Boolean	False	Security services won't take control. The app must decide.
Validity Period	Time interval	N/A	
Relevance: Generation Time in Future	Boolean	True	This allows a RSE or TMC to set future expectations for a given intersection (e.g., a planned lane closure) even if the message doesn't reflect the current intersection state.
Acceptable Future Data Period	Time	30 seconds	
Generation Time Source	Enumerated	Security Header	
Relevance: Expiry Time	Boolean	True	
Expiry Time Source	Enumerated	Security Header	
Consistency: Generation Location	Boolean	False	
Relevance: Generation Location Distance	Boolean or "Text"	False	
Validity Distance	Distance in meters or "Variable"	N/A	
Generation Location Source	Enumerated	N/A	
Overdue CRL Tolerance	Time period or text	N/A	No CRLs
Relevance: Certificate Expiry	Boolean	True	
Accept Encrypted Data	Enumerated or text	No	This entire message should be in plaintext

Security Management

The following table provides the security management features for the CV Pilot MAP application security profile.

Table C-5: CV Pilot MAP Application Security Management Security Profile (Source: CV Pilot Sites)

Name	Type	Value	Notes
Signing Key Algorithm	Enumerated	ecdsaNistP256withSha256	
Encryption Algorithm	Enumerated	N/A	
Implicit or Explicit Certificates	Enumerated	Implicit	What is supported by SCMS

Name	Type	Value	Notes
EC Point Format	Enumerated	Compressed	Point compression more vital on rapidly transmitted messages
SupportedGeographic Regions	Array of enumerated	Rectangular, Polygon, Identified: Country and Subregions	The type of geographic region supported for conformant certificates.
Maximum Certificate Chain Length	Integer	8	
Use Individual Linkage ID	Boolean	N/A	
Use Group Linkage ID	Boolean	N/A	
Signature Algorithms in Chain or CRL	Sequence of Enumerated	ecdsaNistP256withSha256	

Specific Permission (SSP) Expression and Syntax

Permissions for CV Pilot MAP messages are indicated in this section. These may be updated as PSID and SSP constructions are resolved between SAE and the CV Pilots.

J2945/2 Elements

The SSP associated with MAP for the Connected Vehicle Pilot Deployments is the UPER encoding of the following structure. See J2945/2 for definitions of structures not defined in this document.

```
DSRC-SSP ::= SEQUENCE {
    rev           DSRCSSP.SSPVersion(1),      -- version  1
    allowedSSPs   DSRCSSP.SSPallowedList,     -- sequence of
    SSPentrys
    ...
    }
```

In this structure:

- `version` is set to 1
- `allowedSSPs` is a SEQUENCE containing exactly two SSPentry fields, as follows:

```
SSPentry ::= SEQUENCE {
   index         INTEGER(msg-mapData),  --
                 integer=18 constraint
                 (SSPconstraintAll)     --  Boolean:
   True
   }
SSPentry ::= SEQUENCE {
   index         INTEGER(pilot-regulatory-SpeedAuth), --
                 integer=2045 constraint
                 (SSPconstraintAll)                   --  Boolean:
   True
   }
```

The following diagram indicates the J2945/2 SSP structural components (DSRC-SSP) for the CV Pilot MAP messages.

PDU Name/Identifier	Value	Typereference	Built-in Type	Default Value	Constraints
DSRC-SSP		DSRC-SSP	SEQUENCE		
rev	1	SSPrevision	INTEGER		(0..255)
allowedSSPs	2	SSPallowedList	SEQUENCE ...		(SIZE(1..128))
SSPentry 1		SSPentry	SEQUENCE		
index	18	SSPregistrationID	INTEGER		(0..2047)
constraint	all		CHOICE		
SSPentry 2		SSPentry	SEQUENCE		
index	2045	SSPregistrationID	INTEGER		(0..2047)
constraint	all		CHOICE		

Figure D-1: J2945/2 Conformant PSID-SSP Structure for CV Pilot MAPs (Source: CV Pilot Sites)

This structure, UPER-encoded in hexadecimal format is: 00 81 01 20 5F F4 10

This binary value is input as an OPAQUE OCTET STRING into the Canonical Octet Encoding Rules (COER) encoded1609.2 PsidSsp ssp structure, as described in the next section.

Completed PsidSsp Content

A CV Pilot MAP message meets the permission validity conditions to transmit MAP ***with*** the regulatory speeds if the signing certificate's `appPermissions` field includes a `PsidSsp` entry where:

- The PSID is 0x20-40-97 (integer 2113687) for CV-Pilot MAP messages
- The SSP is the 'opaque' UPER-encoded DSRC-SSP element described above.

This structure is indicated in the following diagram.

PDU Name/Identifier	Value	Typereference	Built-in Type	Default Value	Constraints
PsidSsp		PsidSsp	SEQUENCE		
psid	2113687	Psid	INTEGER		(0..MAX)
ssp	opaque	ServiceSpecificPermissions	CHOICE		
opaque	'0080013040'H		OCTET STRI...		(SIZE(0..4294967295))

Figure C-2: Completed 1609.2 PsidSsp Element (COER encoded) (Source: CV Pilot Sites)

The entire 1609.2 PsidSsp structure is thus the following binary containing 1) the complete COER-encoded PsidSsp structure and 2) its opaque, UPER-encoded DSRC-SSP payload.

80 03 20 40 97 80 07 00 81 01 20 5F F4 10

- (Blue -> 1609.2 COER-encoded PsidSsp Structure)
- (Red -> J2945/2 UPER-encoded DSRC-SSP Structure)

A CV Pilot MAP message meets the permission validity conditions to transmit the MAP ***without*** regulatory speeds if the signing certificate's `appPermissions` field includes a `PsidSsp` entry ***without*** the `pilot-regulatory-SpeedAuth` (value=2045) SSPentry 2 above. The entire 1609.2 PsidSsp structure is thus the following binary containing 1) the complete COER-encoded PsidSsp structure and 2) its opaque, UPER-encoded DSRC-SSP payload.

80 03 20 40 97 80 07 00 80 01 20 40

SPaT Application Security Profile and SSPs for the Connected Vehicle Pilot Deployment Projects

Version 8, 2018-04-06

SPaT Description and Security Needs

Signal phase and timing messages in the NYC pilot will be sent from supported intersection Roadside Equipment (RSU) at a rate equivalent to that of vehicle BSMs, namely 10Hz. SPaT messages are described as follows (CVRIA):

Current signal phase and timing information for all lanes at a signalized intersection. This flow identifies active lanes and lanes that are being stopped and specifies the length of time that the current state will persist for each lane. It also identifies signal priority and preemption status and pedestrian crossing status information where applicable.[1]

The security concerns this security profile should address include the following:

Table D-1: Application-specific Security Concerns (Source: CV Pilot Sites)

Application-Specific Security Concerns	Mitigations Supported by Security Profile
Replay	Receiving security application shall support detection of replay attacks
RSU transmitting outside of assigned area	Receiving security applications needs to check the declared message origin to determine if it is transmitting within a prescribed geo-fence indicated by the certificate's geographic restriction. Note: This is a 1609.2 'consistency check' in terms of the application security processing.
Strong association to correct intersection description	SPaT messages must be tightly indexed to the intersection in question so that ASD applications that receive MAP messages provide the correct information to the drivers. Note: This is a 1609.2 'relevance check' in terms of the application processing.
Revoked RSU transmitting	End entities should have reasonably fresh CRL information with respect to the validity period of the RSU certificate (~2 months)
Message spoofing	SPaT messages need to be signed. There is no need to encrypt.
Unauthorized advisory speeds	The RSU should only be transmitting regulator-approved speed advisory information (whether static or algorithmically determined). The RSU's signing certificate will need this authorization when providing such speed advisory information.

IEEE 1609.2 Security Profile Identification

The following table provides the identification features for the SPaT application security profile.

[1] http://local.iteris.com/cvria/html/applications/app67.html#tab-3

Table D-2: SPaT Application Security Profile Identification (Source: CV Pilot Sites)

Name	Type	Recommended values	Description
Name	Text string	"SPAT Security Profile"	The name to be used to refer to the profile. This should be unique among names used by security profiles that reference a particular PSID.
PSIDs	List of PSIDs	0x82	The PSIDs to be used by SDEEs that use this profile.
Other considerations	Text string	This SPAT security profile is designated for the Connected Vehicle Pilot Program	A description of the conditions under which this security profile is to be used.

Sending

The following table provides the security profile for message sending within the SPaT PSID.

Table D-3: SPaT Application Security Profile for Sending Messages (Source: CV Pilot Sites)

Name	Type	Recommended values	Notes
Sign Data	enumerated	True	Sign all SPaT messages for data origin authentication and non-repudiation
Signed Data in Payload	Boolean	True	
External Data	Boolean	False	Otherwise we need to populate - tbsData.payload.extDataHash
External Data Source	Text	N/A	
External Data Hash Algorithm	enumerated	N/A	
Set Generation Time in Security Headers	Boolean	True	Needed to determine if message lies within the validity period of the signing credential
Set Generation Location in Security Headers	Boolean	True	Needed for credential and SPDU consistency checks
Set Expiry Time in Security Headers	Boolean	False	
Signed SPDU Lifetime	Time interval	N/A	Short-lived messages, no lifetime
Signer Identifier Policy Type	Enumerated	Simple	
Simple Signer Identifier Policy: Minimum Inter Cert Time	Time interval (for example, "one second")	1 second	Comment: Default setting from 1609.2 SDEE Specifiers guidance seems reasonable. Also, SPAT is typically sent out at 10Hz so every 10 messages would get the cert vs. the cert hash as the signer identifier.
Simple Signer Identifier Policy: Exceptions	Boolean	False	
Simple Signer Identifier Policy: Signer Identifier Cert - Chain Length	Integer or enumerated	1	Will use the RSUs EE certificate only within the message. We will assume full pre-distribution of CA certs to the fleets.
Text Signer Identifier Policy	Text	N/A	
Sign With Fast Verification	enumerated	Yes-Compressed	
EC Point Format	Enumerated	Compressed	
p2pcd_useInteractive-Form	Boolean	False	

Name	Type	Recommended values	Notes
p2pcd_max-ResponseBackoff	Time or n/a	N/A	
p2pcd_response-ActiveTimeout	Time or n/a	N/A	
p2pcd_request-ActiveTimeout	Time or n/a	N/A	
p2pcd_observed-RequestTimeout	Time or n/a	N/A	
p2pcd_currentlyUsed-TriggerCertificateTime	Time or n/a	N/A	
p2pcd_response-CountThreshold	Integer or n/a	N/A	
Repeat Signed SPDUs	Boolean	True	Will sign each SPaT PDU when the PDU contents changes or once each second to limit resource consumption from signing
Time Between Signing	Time or n/a	1 second	Limit signings to when data changes or once per second.
Encrypt Data	enumerated	No	SPaT messages are in plaintext

Receiving

The following table provides the message reception security features for the SPaT application security profile.

Table D-4: SPaT Application Security Profile for Receiving Messages (Source: CV Pilot Sites)

Name	Type	Value	Notes
Use Preprocessing	Enumerated	True	The full cert chain will not be sent with SPAT messages
Verify Data	Enumerated	True	Verify all SPaT messages when first received from a newly encountered RSE and when acting based on the data within the SPaT message
Maximum Certificate Chain Length	Integer	4	Implementations are not required to support receiving a cert chain length > 4
Relevance: Replay	Boolean	False	SPaTs have generation time within them, so application behavior to detect replay is needed. Delayed SPaT messages need to be detected by the application.
Relevance: Generation Time in Past	Boolean	True	
Validity Period	Time interval	1 Minute	Within a one minute period, the application logic handles message latency issues. Beyond that, the security services will discard. This threshold is an important item for which 1609.2 can help provide guidance.
Relevance: Generation Time in Future	Boolean	True	
Acceptable Future Data Period	Time	30s	
Generation Time Source	Enumerated	Security Header	
Relevance: Expiry Time	Boolean	False	
Expiry Time Source	Enumerated	N/A	
Consistency: Generation Location	Boolean	True	The ASDs need to carry out consistency checks based on the SPAT's generation location.
Relevance: Generation Location Distance	Boolean or "Text"	True	

Name	Type	Value	Notes
Validity Distance	Distance in meters or "Variable"	1000m	Security services will reject if more than 1000m
Generation Location Source	Enumerated	Security Header	
Overdue CRL Tolerance	Time period or text	8 weeks	
Relevance: Certificate Expiry	Boolean	True	Assume that certs won't be on the CRL for long. Either way, check for cert. expiration.
Accept Encrypted Data	Enumerated or text	No	This entire message should be in plaintext

Security Management

The following table provides the security management features for the SPaT application security profile.

Table D-5: SPaT Application Security Management Security Profile (Source: CV Pilot Sites)

Name	Type	Value	Notes
Signing Key Algorithm	Enumerated	ecdsaNistP256withSha256	
Encryption Algorithm	Enumerated	N/A	
Implicit or Explicit Certificates	Enumerated	Implicit	10Hz messages consume more bandwidth
EC Point Format	Enumerated	Compressed	Point compression more vital on rapidly transmitted messages
SupportedGeographic Regions	Array of enumerated	Circular	The type of geographic region supported for conformant certificates.
Maximum Certificate Chain - Length	Integer	8	
Use Individual Linkage ID	Boolean	N/A	
Use Group Linkage ID	Boolean	N/A	
Signature Algorithms in Chain or CRL	Sequence of Enumerated	ecdsaNistP256withSha256	

Specific Permission (SSP) Expression and Syntax

Permissions for SPaT messages are indicated in this section. These may be updated as SSP constructions are resolved between SAE and the CV Pilots.

J2945/2 Elements

The SSPs associated with SPaT for the Connected Vehicle Pilot Deployments are the UPER encoding of the following structure. See J2945/2 for definitions of structures not defined in this document.

```
DSRC-SSP ::= SEQUENCE {
    rev             DSRCSSP.SSPVersion(1),      -- version 1
```

```
    allowedSSPs    DSRCSSP.SSPallowedList,      -- sequence of SSPentrys
    ...
    }
```

In this structure:

- `version` is set to 1
- `allowedSSPs` is a SEQUENCE containing exactly two SSPentry fields, as follows:

```
SSPentry ::= SEQUENCE {
   index          INTEGER(msg-signalPhaseAndTimingMessage),   --  integer=19
   constraint      (SSPconstraintAll)                         --  Boolean: True
   }
SSPentry ::= SEQUENCE {
   index          INTEGER(cvPilots-SpeedAuthorizations), --  integer=2045
   constraint      (SSPconstraintAll)                    --  Boolean: True
   }
```

If the SPaT enabled intersection provides advisory speeds (similar to MAP messages in CV pilot), then it must also contain the above SSPentry with SSPRegistrationID index of: `cvPilots-SpeedAuthorizations`. Advisory speed indications mean that the J2735 SPaT message's MovementEventList contains at least one MovementEvent with a populated AdvisorySpeed (speeds) element. If advisory speeds are not provided in the SPaT message, then this SSPEntry is not needed in the RSU's certificate.

The following diagram indicates the J2945/2 SSP structural components (DSRC-SSP) for the CV Pilot SPaT messages.

PDU Name/Identifier	Value	Typereference	Built-in Type	Default Value	Constraints
DSRC-SSP		DSRC-SSP	SEQUENCE		
rev	1	SSPrevision	INTEGER		(0..255)
allowedSSPs	2	SSPallowedList	SEQUENCE ...		(SIZE(1..128))
SSPentry 1		SSPentry	SEQUENCE		
index	19	SSPregistrationID	INTEGER		(0..2047)
constraint	all		CHOICE		
SSPentry 2		SSPentry	SEQUENCE		
index	2045	SSPregistrationID	INTEGER		(0..2047)
constraint	all		CHOICE		

Figure D-1: J2945/2 Conformant PSID-SSP Structure for CV Pilot SPaTs (Source: CV Pilot Sites)

The complete structure, UPER-encoded in hexadecimal format is:
00 81 01 30 5F F4 10

This binary value is input as an OPAQUE OCTET STRING into the Canonical Octet Encoding Rules (COER) encoded1609.2 PsidSsp ssp structure, as described in the next section.

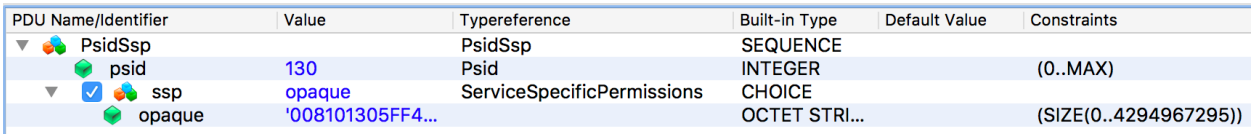
Completed PsidSsp Content

A SPaT message meets the permission validity conditions to transmit SPaT ***with*** the advisory speeds if the signing certificate's `appPermissions` field includes a `PsidSsp` entry where:

- The PSID is 0x82 (130 Integer) for SPaT messages

- The SSP element is opaquely populated by the UPER-encoded DSRC-SSP shown above

This structure is indicated in the following diagram.



PDU Name/Identifier	Value	Typereference	Built-in Type	Default Value	Constraints
PsidSsp		PsidSsp	SEQUENCE		
psid	130	Psid	INTEGER		(0..MAX)
ssp	opaque	ServiceSpecificPermissions	CHOICE		
opaque	'008101305FF4...		OCTET STRI...		(SIZE(0..4294967295))

Figure D-2: Completed 1609.2 PsidSsp Element (COER encoded) (Source: CV Pilot Sites)

The entire 1609.2 PsidSsp structure is thus the following binary containing 1) the complete COER-encoded PsidSsp structure and 2) its opaque, UPER-encoded DSRC-SSP payload. Its binary is represented as: 80 01 82 80 07 00 81 01 30 5F F4 10

- (Blue -> 1609.2 COER-encoded PsidSsp Structure)
- (Red -> J2945/2 UPER-encoded DSRC-SSP Structure)

A SPaT message meets the permission validity conditions to transmit the SPaT ***without*** the advisory speeds if the signing certificate's `appPermissions` field includes a `PsidSsp` entry without the `cvPilots-SpeedAuthorizations` (value=2045) SSPEntry above. The entire 1609.2 PsidSsp structure is thus the following binary containing 1) the complete COER-encoded PsidSsp structure and 2) its opaque, UPER-encoded DSRC-SSP payload.

80 01 82 80 07 00 80 01 30 40

SRM Application Security Profile and SSPs for the Connected Vehicle Pilot Deployment Projects

Version 5, 2018-04-06

SRM Description and Security Needs

Signal request messages in the CV pilot will be sent from supported vehicle OBE devices to RSUs in order to request signal priority. SRM messages are defined in SAE J2735. Note that SRM messages in the CV pilot will use a unique PSID.

The security concerns this security profile should address include the following:

Table E-1: Application-specific Security Concerns (Source: CV Pilot Sites)

Application-Specific Security Concerns	Mitigations Supported by Security Profile
Replay	Replay is a concern if the replayed message indicates a previously requested signal priority (e.g., that requested by a first responder vehicle), therefore the receiving security application shall support detection of replay attack.
Integrity errors	The sending application needs to digitally sign the messages. Modified SRM requests could seriously undermine critical safety operations.
Message spoofing	SRM messages need to be digitally signed by the authorized OBE to ensure data origin and non-repudiation. There is no need to encrypt.
Signing certificate not authorized to send a SRM message	Only authorized vehicles (e.g., first responder, public transit, etc.) should possess the authorizations necessary to request a signal preemption. 'Normal' vehicles should not have this permission.
Revoked OBE transmitting	The RSU should have reasonably fresh CRL information with respect to the validity period of the transmitting certificate.

IEEE 1609.2 Security Profile Identification

The following table provides the identification features for the SRM application security profile.

Table E-2: CV Pilot SRM Application Security Profile Identification (Source: CV Pilot Sites)

Name	Type	Recommended values	Description
Name	Text string	"SRM Security Profile"	
PSIDs	List of PSIDs	HEX: (0x20-40-96) P-ENC: (0pE0-00-00-16) DEC: (2,113,686)	The PSID to be used by SDEEs that use this profile. Note that this PSID is specific to the CV pilots for general use in conveying 'Priority Control' information.
Other considerations	Text string	This SRM security profile is designated for the Connected Vehicle Pilot Program	A description of the conditions under which this security profile is to be used.

Sending

The following table provides the security profile for message sending within the SRM PSID.

Table E-3: SRM Application Security Profile for Sending Messages (Source: CV Pilot Sites)

Name	Type	Recommended values	Notes
Sign Data	enumerated	True	Sign all SRM messages for data origin authentication and non-repudiation
Signed Data in Payload	Boolean	True	
External Data	Boolean	False	Otherwise we need to populate - tbsData.payload.extDataHash
External Data Source	Text	N/A	
External Data Hash Algorithm	enumerated	N/A	
Set Generation Time in Security Headers	Boolean	True	Needed to determine if message lies within the validity period of the signing credential (message's generation time only resolves to the minute)
Set Generation Location in Security Headers	Boolean	True	RSUs need to perform a geographic relevance check to determine whether the message needs to undergo full processing (i.e., determine that the message content indicates the specific intersection in question). The actual geographic relevance 'range' (distance from intersection RSU to OBE is to be determined by the application developer)
Set Expiry Time in Security Headers	Boolean	False	
Signed SPDU Lifetime	Time interval	Text	OBE signing application needs to set the time interval for this SPDU lifetime.
Signer Identifier Policy Type	Enumerated	Simple	
Simple Signer Identifier Policy: Minimum Inter Cert Time	Time interval (for example, "one second")	Always	All SRM messages will contain the signing public key certificate.
Simple Signer Identifier Policy: Exceptions	Boolean	False	
Simple Signer Identifier Policy: Signer Identifier Cert - Chain Length	Integer or enumerated	1	
Text Signer Identifier Policy	Text	N/A	
Sign With Fast Verification	enumerated	Yes-Compressed	
EC Point Format	Enumerated	Compressed	
p2pcd_useInteractive-Form	Boolean	False	
p2pcd_max-ResponseBackoff	Time or n/a	N/A	
p2pcd_response-ActiveTimeout	Time or n/a	N/A	
p2pcd_request-ActiveTimeout	Time or n/a	N/A	
p2pcd_observed-RequestTimeout	Time or n/a	N/A	
p2pcd_currentlyUsed-TriggerCertificateTime	Time or n/a	N/A	

Name	Type	Recommended values	Notes
p2pcd_response-CountThreshold	Integer or n/a	N/A	
Repeat Signed SPDUs	Boolean	False	SRM messages that need to be retransmitted for whatever reason must be re-generated (new location/time) and signed due to the short validity period, sensitivity and relevance of the request.
Time Between Signing	Time or n/a	N/A	
Encrypt Data	enumerated	No	SRM messages are in plaintext

Receiving

The following table provides the message reception security features for the SRM application security profile.

Table E-4: SRM Application Security Profile for Receiving Messages (Source: CV Pilot Sites)

Name	Type	Value	Notes
Use Preprocessing	Enumerated	True	The full cert chain will not be sent with SRM messages
Verify Data	Enumerated	True	Verify all SRM messages
Maximum Certificate Chain Length	Integer	4	
Relevance: Replay	Boolean	False	
Relevance: Generation Time in Past	Boolean	True	
Validity Period	Time interval	2 minutes	Validity period needs to accommodate vehicle delay due to high traffic volumes. After a period of 2 minutes, however, the transmitting vehicle will need to issue a new SRM.
Relevance: Generation Time in Future	Boolean	True	This allows a RSU to anticipate a forthcoming request and handle it as it becomes valid. Route generation and optimal traffic flows may dictate sequences SRMs through a dense urban area.
Acceptable Future Data Period	Time	15 minutes	Vehicles should not accept anticipated SRMs that are more than 15 minutes in the future. This should accommodate adaptive routing needs. If a future validity period is specified, a new SRM can always be transmitted by the sender to perform a 'priorityCancellation' and remove the prior request (and its future validity)
Generation Time Source	Enumerated	Security Header	
Relevance: Expiry Time	Boolean	False	
Expiry Time Source	Enumerated	N/A	
Consistency: Generation Location	Boolean	True	
Relevance: Generation Location Distance	Boolean or "Text"	"TBD"	This needs to be set by the application developer due to the variance in urban intersection density.
Validity Distance	Distance in meters or "Variable"	Meters	
Generation Location Source	Enumerated	Security Header	Indicated by OBE in security header
Overdue CRL Tolerance	Time period or text	1 month	CV Pilots only
Relevance: Certificate Expiry	Boolean	True	
Accept Encrypted Data	Enumerated or text	No	This entire message should be in plaintext

Security Management

The following table provides the security management features for the SRM application security profile.

Table E-5: SRM Application Security Management Security Profile (Source: CV Pilot Sites)

Name	Type	Value	Notes
Signing Key Algorithm	Enumerated	ecdsaNistP256withSha256	
Encryption Algorithm	Enumerated	N/A	
Implicit or Explicit Certificates	Enumerated	Implicit	What is supported by SCMS
EC Point Format	Enumerated	Compressed	Point compression more vital on rapidly transmitted messages
SupportedGeographic Regions	Array of enumerated	Rectangular, Polygon, Identified: Country and Subregions	The type of geographic region supported for conformant certificates.
Maximum Certificate Chain Length	Integer	8	
Use Individual Linkage ID	Boolean	N/A	
Use Group Linkage ID	Boolean	N/A	
Signature Algorithms in Chain or CRL	Sequence of Enumerated	ecdsaNistP256withSha256	

Specific Permission (SSP) Expression and Syntax

Permissions for SRM messages are indicated in this section. These may be updated as SSP constructions are resolved between SAE and the CV Pilots.

The SSP associated with SRM for the Connected Vehicle Pilot Deployments is the UPER encoding of the following structure. See J2945/2 for definitions of structures not defined in this document.

```
DSRC-SSP ::= SEQUENCE {
    rev            DSRCSSP.SSPVersion(1),       -- version 1
    allowedSSPs    DSRCSSP.SSPallowedList,      -- sequence of SSPentrys
    ...
    }
```

In this structure:

- `version` is set to 1
- `allowedSSPs` is a SEQUENCE containing exactly one SSPentry field, as follows:

```
SSPentry ::= SEQUENCE {
   index          INTEGER(msg-signalRequestMessage),  --  integer=29
   constraint      (SSPconstraintAll)                 --  Boolean: True
   }
```

Mapping from PSID / SSP to message

A SRM message meets the permission validity conditions if the signing certificate's `appPermissions` field includes a `PsidSsp` entry where:

- The PSID is 0x20-40-96 for CV-Pilot SRM messages
- The SSP is the UPER-encoded DSRC-SSP containing the SSPentry described above

1609.2 PsidSsp with J2945/2 SSP Binaries

The complete SAE J2945/2 DSRC-SSP binary blob (UPER-encoded) in hexadecimal format is:

00 80 01 D0 40

This binary value is input as an OPAQUE OCTET STRING into the Canonical Octet Encoding Rules (COER) encoded1609.2 PsidSsp ssp structure. The entire 1609.2 PsidSsp structure is thus a mixed encoding consisting of the following binary embedded in the 1609.2 certificate:

80 03 20 40 96 80 05 00 80 01 D0 40

SSM Application Security Profile and SSPs for the Connected Vehicle Pilot Deployment Projects

Version 5, 2018-04-06

SSM Description and Security Needs

Signal status messages in the CV pilot will be sent from RSUs to indicate priority status information typically in response to a vehicle's Signal Request Message. SSM messages are defined in SAE J2735. Note that the CV Pilots will use a unique PSID to transmit and process SSM messages.

The security concerns this security profile should address include the following:

Table F-1: CV Pilot SSM Application-specific Security Concerns (Source: CV Pilot Sites)

Application-Specific Security Concerns	Mitigations Supported by Security Profile
Replay	Replay is a concern if the replayed status message indicates stale signal status information, therefore the receiving security application shall support detection of replay attack. Possible signal response statuses from J2735 include: • Unknown • Requested • Processing • WatchOtherTraffic • Granted • Rejected • maxPresence • reserviceLocked
Integrity errors	The sending application needs to digitally sign the messages. Modified SSM requests could cause incorrect signal status information to be conveyed to vehicles.
Message spoofing	SSM messages need to be digitally signed by the authorized RSU to ensure data origin and non-repudiation. There is no need to encrypt.
Signing certificate not authorized to send a SSM message	Only authorized applications (RSUs) should possess the permissions necessary to send signal status information. RSUs running applications that accept and process SRM messages will need to contain the authorizations (SSP) necessary to respond using SSM messages.
Revoked RSU transmitting	OBEs should have reasonably fresh CRL information with respect to the validity period of the transmitting RSU certificate.

IEEE 1609.2 Security Profile Identification

The following table provides the identification features for the SSM application security profile.

Table F-2: SSM Application Security Profile Identification (Source: CV Pilot Sites)

Name	Type	Recommended values	Description
Name	Text string	"CV Pilot SSM Security Profile"	
PSIDs	List of PSIDs	HEX: (0x20-40-95) P-ENC: (0pE0-00-00-15) DEC: (2,113,685)	The PSID to be used by SDEEs that use this profile. Note that this PSID is specific to the CV pilots for general use in conveying 'Priority Status' information.
Other considerations	Text string	This SSM security profile is designated for the Connected Vehicle Pilot Program	A description of the conditions under which this security profile is to be used.

Sending

The following table provides the security profile for message sending within the SSM PSID.

Table F-3: SSM Application Security Profile for Sending Messages (Source: CV Pilot Sites)

Name	Type	Recommended values	Notes
Sign Data	enumerated	True	Sign all SSM messages for data origin authentication and non-repudiation
Signed Data in Payload	Boolean	True	
External Data	Boolean	False	Otherwise we need to populate - tbsData.payload.extDataHash
External Data Source	Text	N/A	
External Data Hash Algorithm	enumerated	N/A	
Set Generation Time in Security Headers	Boolean	True	
Set Generation Location in Security Headers	Boolean	True	OBEs need to perform a geographic relevance check to determine whether the message needs to undergo full processing. Intersection status information that is beyond a configurable range (or direction) should be discarded. The actual geographic relevance 'range' (distance from intersection RSU to OBE is to be determined by the application developer)
Set Expiry Time in Security Headers	Boolean	False	
Signed SPDU Lifetime	Time interval	N/A	
Signer Identifier Policy Type	Enumerated	Simple	
Simple Signer Identifier Policy: Minimum Inter Cert Time	Time interval (for example, "one second")	Always	All SSM messages will contain the signing public key certificate.
Simple Signer Identifier Policy: Exceptions	Boolean	False	

Name	Type	Recommended values	Notes
Simple Signer Identifier Policy: Signer Identifier Cert - Chain Length	Integer or enumerated	1	
Text Signer Identifier Policy	Text	N/A	
Sign With Fast Verification	enumerated	Yes-Compressed	
EC Point Format	Enumerated	Compressed	
p2pcd_useInteractive-Form	Boolean	False	
p2pcd_max-ResponseBackoff	Time or n/a	N/A	
p2pcd_response-ActiveTimeout	Time or n/a	N/A	
p2pcd_request-ActiveTimeout	Time or n/a	N/A	
p2pcd_observed-RequestTimeout	Time or n/a	N/A	
p2pcd_currentlyUsed-TriggerCertificateTime	Time or n/a	N/A	
p2pcd_response-CountThreshold	Integer or n/a	N/A	
Repeat Signed SPDUs	Boolean	False	SSM status messages may need to be retransmitted if the status hasn't changed.
Time Between Signing	Time or n/a	5 seconds	Even if no status has changed, a new SSM message should be generated at least every 5 seconds. Within a 5 second period, the RSU may re-transmit previously signed status information.
Encrypt Data	enumerated	No	SSM messages are in plaintext

Receiving

The following table provides the message reception security features for the CV Pilot SSM application security profile.

Table F-4: SSM Application Security Profile for Receiving Messages (Source: CV Pilot Sites)

Name	Type	Value	Notes
Use Preprocessing	Enumerated	True	The full cert chain will not be sent with SSM messages
Verify Data	Enumerated	True	Verify all SSM messages (note: 'replayed messages' within a 5 second interval do not need to be re-verified)
Maximum Certificate Chain Length	Integer	4	
Relevance: Replay	Boolean	False	
Relevance: Generation Time in Past	Boolean	True	Security services will need to reject SSM messages that are signed for a future period. Future state is unknown, therefore the relevance check that the message was generated in the past is necessary.
Validity Period	Time interval	5 seconds	After a period of 5 seconds, however, the RSU will need to issue a new SSM even though it may indicate the same signal state.
Relevance: Generation Time in Future	Boolean	True	
Acceptable Future Data Period	Time	30 seconds	
Generation Time Source	Enumerated	Security Header	

Name	Type	Value	Notes
Relevance: Expiry Time	Boolean	False	
Expiry Time Source	Enumerated	N/A	
Consistency: Generation Location	Boolean	True	
Relevance: Generation Location Distance	Boolean or "Text"	"TBD"	This needs to be set by the application developer due to the variance in urban intersection density.
Validity Distance	Distance in meters or "Variable"	Meters	
Generation Location Source	Enumerated	Security Header	Indicated by OBE in security header
Overdue CRL Tolerance	Time period or text	1 month	CV Pilots only
Relevance: Certificate Expiry	Boolean	True	
Accept Encrypted Data	Enumerated or text	No	This entire message should be in plaintext

Security Management

The following table provides the security management features for the SSM application security profile.

Table F-5: CV Pilot SSM Application Security Management Security Profile (Source: CV Pilot Sites)

Name	Type	Value	Notes
Signing Key Algorithm	Enumerated	ecdsaNistP256withSha256	
Encryption Algorithm	Enumerated	N/A	
Implicit or Explicit Certificates	Enumerated	Implicit	What is supported by SCMS
EC Point Format	Enumerated	Compressed	Point compression more vital on rapidly transmitted messages
SupportedGeographic Regions	Array of enumerated	Rectangular, Polygon, Identified: Country and Subregions	The type of geographic region supported for conformant certificates.
Maximum Certificate Chain Length	Integer	8	
Use Individual Linkage ID	Boolean	N/A	
Use Group Linkage ID	Boolean	N/A	
Signature Algorithms in Chain or CRL	Sequence of Enumerated	ecdsaNistP256withSha256	

Specific Permission (SSP) Expression and Syntax

Permissions for SSM messages are indicated in this section. These may be updated as SSP constructions are resolved between SAE and the CV Pilots.

The SSP associated with SSM for the Connected Vehicle Pilot Deployments is the UPER encoding of the following structure. See J2945/2 for definitions of structures not defined in this document.

```
DSRC-SSP ::= SEQUENCE {
    rev             DSRCSSP.SSPVersion(1),      -- version 1
```

```
    allowedSSPs    DSRCSSP.SSPallowedList,      -- sequence of SSPentrys
    ...
    }
```

In this structure:

- `version` is set to 1
- `allowedSSPs` is a SEQUENCE containing exactly one SSPentry field, as follows:

```
SSPentry ::= SEQUENCE {
   index          INTEGER(msg-signalStatusMessage),    --  integer=30
   constraint      (SSPconstraintAll)                  --  Boolean: True
   }
```

Mapping from PSID / SSP to message

A SSM message meets the permission validity conditions if the signing certificate's `appPermissions` field includes a `PsidSsp` entry where:

- The PSID is 0x20-40-95 for CV-Pilot SSM messages
- The SSP is the UPER-encoded DSRC-SSP containing the SSPentry described above

1609.2 PsidSsp with J2945/2 SSP Binaries

The complete SAE J2945/2 DSRC-SSP binary blob (UPER-encoded) in hexadecimal format is:

00 00 01 E0 40

This binary value is input as an OPAQUE OCTET STRING into the Canonical Octet Encoding Rules (COER) encoded1609.2 PsidSsp ssp structure. The entire 1609.2 PsidSsp structure is thus a mixed encoding consisting of the following binary embedded in the 1609.2 certificate:

80 03 20 40 95 80 05 00 00 01 E0 40

TIM Application Security Profile and SSPs for the Connected Vehicle Pilot Deployment Projects

Version 9, 2018-12-04

TIM Description and Security Needs

Traveler Information Messages (TIM) in the CV pilots will be generated and sent from the TMC to RSUs specifically selected to transmit the messages or will be generated locally (within the RSU) based on internal configuration and business logic. TIM messages provide a variety of traveler-related information according to SAE J2735.

While the RSU transmits the messages, TIM messages are more static in nature. TIM messages can therefore be either locally signed by the RSE or 'centrally signed,' i.e., signed by the Traffic Management Center (TMC).

The security concerns this security profile should address include the following:

Table G-1: Application-specific Security Concerns (Source: CV Pilot Sites)

Application-Specific Security Concerns	**Mitigations Supported by Security Profile**
Replay	TIM messages are expected to be replayed for a certain period of time by the RSU or satellite provider (as configured by the TMC). The receiving security application does not need to detect replay attacks but does need to perform geographic and temporal relevance checks.
Integrity errors	The sending application needs to digitally sign the messages. False descriptions could severely impact I2V applications.
Message spoofing	TIM messages need to be digitally signed by the RSE or TMC to ensure data origin and non-repudiation. There is no need to encrypt.
Signing certificate not authorized to provision TIM data for a given region	The RSE or TMC should only be signing TIM messages for RSUs to transmit within a confined geography for which it has authority. The signing certificate needs to indicate a geographic constraint that definitively contains/overlaps the location to which the TIM message pertains.
Revoked TMC cert is signing	End entities should have reasonably fresh CRL information with respect to the validity period of the RSE or TMC signing certificate
Incorrect entity signs message	Only the RSE or TMC should be able to digitally sign TIM messages, therefore the signing certificate will need to have specific application identifier and permissions to transmit TIM message.
Entity not authorized to sign TIM messages that cause vehicle ASDs to modify their BSM sending behavior	The NYC CV pilot requires the ability for the TMC to 'instruct' ASDs in specific areas to reduce their BSM transmission rates. Due to the safety sensitivity of this behavior, certain authorizations are required to allow the sending authority to manipulate ASD behavior in this manner.

IEEE 1609.2 Security Profile Identification

The following table provides the identification features for the TIM application security profile.

Table G-2: TIM Application Security Profile Identification (Source: CV Pilot Sites)

Name	Type	Recommended values	Description
Name	Text string	"TIM_Security Profile"	
PSIDs	List of PSIDs	0x83	From 1609.12. The PSIDs to be used by SDEEs that use this profile.
Other considerations	Text string	This TIM security profile is designated for the Connected Vehicle Pilot Program	A description of the conditions under which this security profile is to be used.

Sending

The following table provides the security profile for message sending within the TIM PSID.

Table G-3: TIM Application Security Profile for Sending Messages (Source: CV Pilot Sites)

Name	Type	Recommended values	Notes
Sign Data	enumerated	True	Sign all TIM messages for data origin authentication and non-repudiation
Signed Data in Payload	Boolean	True	
External Data	Boolean	False	Otherwise we need to populate - tbsData.payload.extDataHash
External Data Source	Text	N/A	
External Data Hash Algorithm	enumerated	N/A	
Set Generation Time in Security Headers	Boolean	True	Needed to determine if message lies within the validity period of the signing credential. In this case, the generation time is the time that the RSE or TMC encapsulated and signed the TIM source message for relay.
Set Generation Location in Security Headers	Boolean	False	Signed messages (RSE or TMC) do not need to indicate generation location. The signing certificate will indicate 'authority to sign' for a given region.
Set Expiry Time in Security Headers	Boolean	True	Update this to set the expiry time to match the TIM expiry time or the TMC/RSE certificate expiry time, whichever is sooner. Or default to 240 minutes
Signed SPDU Lifetime	Time interval	240 minutes	The signing application needs to set the time interval for this SPDU lifetime. Update this to set the expiry time to match the TIM expiry time or the TMC/RSE certificate expiry time, whichever is sooner. Or default to 240 minutes
Signer Identifier Policy Type	Enumerated	Simple	
Simple Signer Identifier Policy: Minimum Inter Cert Time	Time interval (for example, "one second")	Always	All TIM messages will contain the signing public key certificate.

Name	Type	Recommended values	Notes
Simple Signer Identifier Policy: Exceptions	Boolean	False	
Simple Signer Identifier Policy: Signer Identifier Cert - Chain Length	Integer or enumerated	1	Will use the RSE's or TMC's authorization certificate only within the message. We will assume full pre-distribution of CA certs to the fleets.
Text Signer Identifier Policy	Text	N/A	
Sign With Fast Verification	enumerated	Yes-Compressed	Matches convention established for other J2735 messages
EC Point Format	Enumerated	Compressed	Matches convention established for other J2735 messages
p2pcd_useInteractive- Form	Boolean	False	TIM doesn't fit the P2PCD paradigm where the device requesting the certs sends the same messages as the device using the certs, so P2PCD doesn't work here.
p2pcd_max-ResponseBackoff	Time or n/a	N/A	
p2pcd_response-ActiveTimeout	Time or n/a	N/A	
p2pcd_request-ActiveTimeout	Time or n/a	N/A	
p2pcd_observed-RequestTimeout	Time or n/a	N/A	
p2pcd_currentlyUsed-TriggerCertificateTime	Time or n/a	N/A	
p2pcd_response-CountThreshold	Integer or n/a	N/A	
Repeat Signed SPDUs	Boolean	True	Following the initial, transmitted TIM PDU, each following one may be a re-transmit of the first so long as they are within the validity period of the message (as set by the signing application).
Time Between Signing	Time or n/a	Set to Message lifetime	
Encrypt Data	enumerated	No	TIM messages are in plain text

Receiving

The following table provides the message reception security features for the TIM application security profile.

Table G-4: TIM Application Security Profile for Receiving Messages (Source: CV Pilot Sites)

Name	Type	Value	Notes
Use Preprocessing	Enumerated	True	The full cert chain will not be sent with TIM messages
Verify Data	Enumerated	True	Verify all TIM messages
Maximum Certificate Chain Length	Integer	4	Matches convention established for other J2735 messages
Relevance: Replay	Boolean	False	RSU will purposefully be replaying messages
Relevance: Generation Time in Past	Boolean	False	Security services won't take control. The app must decide.
Validity Period	Time interval	N/A	We use expiry time, not generation time, to decide whether to reject messages
Relevance: Generation Time in Future	Boolean	True	
Acceptable Future Data Period	Time	30 seconds	
Generation Time Source	Enumerated	Security Header	Due to J2735 timestamp and 1609.2 Time64 encoding mismatches – time will be re-expressed in a valid 1609.2 format by the sender in the security header
Relevance: Expiry Time	Boolean	True	
Expiry Time Source	Enumerated	Security Header	The RSE or TMC signing application will populate with a value that encompasses all of the J2735 TIM's Traveler Data Frame's startYear, startTime and duration values.
Consistency: Generation Location	Boolean	False	
Relevance: Generation Location Distance	Boolean or "Text"	False	
Validity Distance	Distance in meters or "Variable"	N/A	
Generation Location Source	Enumerated	N/A	
Overdue CRL Tolerance	Time period or text	N/A	RSE or TMC cert will not be revoked; it will expire.
Relevance: Certificate Expiry	Boolean	True	
Accept Encrypted Data	Enumerated or text	No	This entire message should be in plain text

Security Management

The following table provides the security management features for the TIM application security profile.

Table G-5: TIM Application Security Management Security Profile (Source: CV Pilot Sites)

Name	Type	Value	Notes
Signing Key Algorithm	Enumerated	ecdsaNistP256withSha256	
Encryption Algorithm	Enumerated	N/A	
Implicit or Explicit Certificates	Enumerated	Implicit	What is supported by SCMS
EC Point Format	Enumerated	Compressed	Point compression more vital on rapidly transmitted messages
SupportedGeographic Regions	Array of enumerated	Rectangular, Polygonal, Identified: Country and Subregions	The type of geographic region supported for conformant certificates.
Maximum Certificate Chain Length	Integer	8	
Use Individual Linkage	Boolean	N/A	
Use Group Linkage ID	Boolean	N/A	
Signature Algorithms in Chain or CRL	Sequence of Enumerated	ecdsaNistP256withSha256	

Specific Permission (SSP) Expression and Syntax

Permissions for TIM messages are indicated in this section. These may be updated as SSP constructions are resolved between SAE and the CV Pilots.
The SSP associated with TIM for the Connected Vehicle Pilot Deployments is the UPER encoding of the following structure. See J2945/2 for definitions of structures not defined in this document.

```
DSRC-SSP ::= SEQUENCE {
    rev           DSRCSSP.SSPVersion(1),      -- version  1
    allowedSSPs   DSRCSSP.SSPallowedList,     -- sequence of SSPentrys
    ...
    }
```

In this structure:

- `version` is set to 1
- `allowedSSPs` is a SEQUENCE containing exactly one SSPentry field, as follows:

```
SSPentry ::= SEQUENCE {
   index  INTEGER(msg-travelerInformation),  -- 31
   constraint  (SSPconstraintAll)            -- Boolean: True
   }
```

Mapping from PSID / SSP to message

A TIM message meets the permission validity conditions if the signing certificate's `appPermissions` field includes a `PsidSsp` entry where:

- The PSID is 0x83 (131 Integer) for TIM messages
- The SSP is the UPER-encoded DSRC-SSP containing the SSPentry described above

TIM Regional Extension SSPs

The TIM messages in NYC CV Pilot will additionally be used to indicate to participating NYC vehicles when and where to throttle their BSM transmission rates. This information will be included in a TIM extension 'Region' Module according to the following ASN.1 definition.

```
-- To be included in the REGION module:

Reg-TravelerInformation DSRC.REG-EXT-ID-AND-TYPE ::= {
      { TravelerInformation-addGrpA IDENTIIED BY DSRC.addGrpA} ,
           -- U.S. implements addGrpA for message extensions
       ...
}

-- To be included in the Profile_addGrpA module:

--    TIM J2735 Regional Message Rate Management Content for TIM
TravelerInformation-addGrpA ::=
    SEQUENCE OF MessageMgmtRegion (0..16), -- prefix by mmr
    ...
}

MessageMgmtRegion ::= SEQUENCE {
    mmrAnchor       Position3D,      -- J2735 type: anchor point for zone
```

```
    mmrPath          OffsetSystem,     -- J2735 type: outline of area
    mmrMessageType   DSRCmsgID,        -- J2735 message type to manage
    mmrInterval      Uint16,           -- Transmission interval
    mmrStartTime     MinuteOfTheYear,  -- J2735 type: Start time for rate management
    mmrDuratonTime   MinutesDuration,  -- J2735 type: Duration of rate management
    mmrVehSpeedMax   SpeedAdvice       -- J2735 type: Max rate applies if speed < this
    mmrVehAccMax     Acceleration      -- J2735 type: Max rate applies if acc < this
}
```

TIM Signing SSPentry

Any TIM message of any sort must be permitted by an SSPentry in the SSP associated with the TIM PSID 0x83, per SAE J2945/2. In this SSPentry:

- SSPregistrationId = 31
- constraint = all.

This SSPentry is required for signing any TIM.

TIM Extension SSPentry

Any TIM message containing an extension must be permitted by an SSPentry in the SSP associated with the TIM PSID 0x83, per SAE J2945/2. In this SSPentry:

- SSPregistrationId = 218
- constraint = all.

This SSPentry is required for signing any TIM containing message rate management fields.

High Velocity Message Rate Management SSPentry

If mmrVehSpeedMax indicates a speed greater than 8 KPH, then this must be permitted by an SSPentry in the SSP associated with the TIM PSID 0x83. In this SSPentry:

- SSPregistrationId = 700
- constraint = all.

If mmrVehSpeedMax is less than this value, this SSPentry need not be present in the certificate signing a TIM containing message rate management fields.

Acceleration SSPentry

If mmrVehAccMax indicates an acceleration greater than 1 m/s^2 then this must be permitted by an SSPentry in the SSP associated with the TIM PSID 0x83. In this SSPentry:

- SSPregistrationId = 701
- constraint = all.

If mmrVehAccMax is less than this value[1], this SSPentry need not be present in the certificate signing a TIM containing message rate management fields.

[1] This is a strawman value, based on the observation in https://ac.els- cdn.com/S2352146517307937/1-s2.0-S2352146517307937-main.pdf?_tid=b9d6dd5f-e726- 42ba-a196-5777eb3744a2&acdnat=1523609633_684735d3ada7342e566af047aba57f74 that max acceleration rates for petrol cars are around 2.7 m/s^2. It can be changed if there's any other value with a stronger rationale.

Large Geographic Area SSPentry

If mmrAnchor and mmrPath indicate a "large message management region", this must be permitted by an SSPentry in the SSP associated with the TIM PSID 0x83. A "large message management region" is defined as a region which is greater than one square kilometer, or 1000000 square meters. In this SSPentry:

- SSPregistrationId = 702
- constraint = all.

If the area for message rate management does not qualify as a "large message management region" by this definition, this SSPentry need not be present in the certificate signing a TIM containing message rate management fields.

1609.2 PsidSsp with Different SSP Binary Options

This section provides the different PsidSsp recipes based on the TIM signing authorizations of the sender.

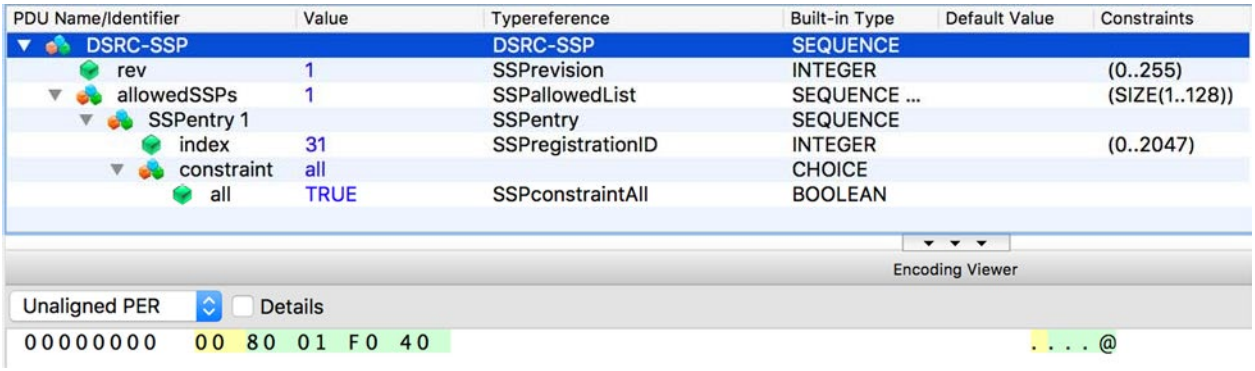


Figure G-1: SS for Basic TIM Signer with No Regional Extensions (Source: CV Pilot Sites)

SSP Binary is: 0x008001F040

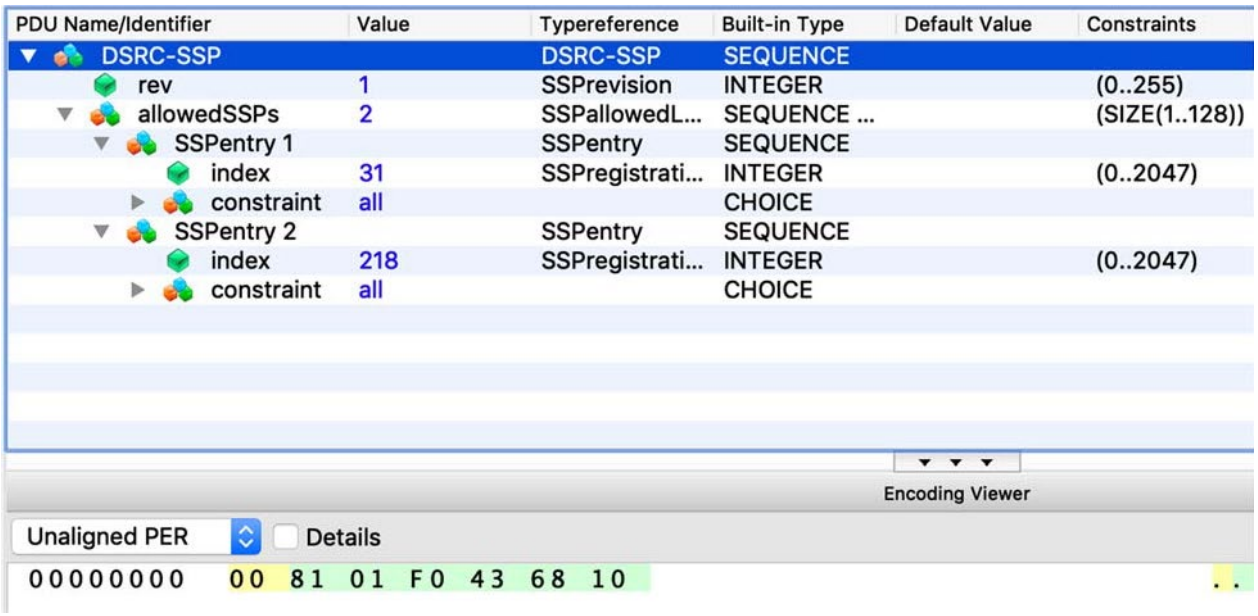


Figure G-2: SSP: TIM Signer with Low Velocity BSM Throttling Only (for areas less than 1 sq-km, low velocity and low acceleration) (Source: CV Pilot Sites)

SSP Binary is: 0x008101F0436810

The New York City TIM-signing application will use this SSP binary in its 1609.2 certificate PsidSsp structure.

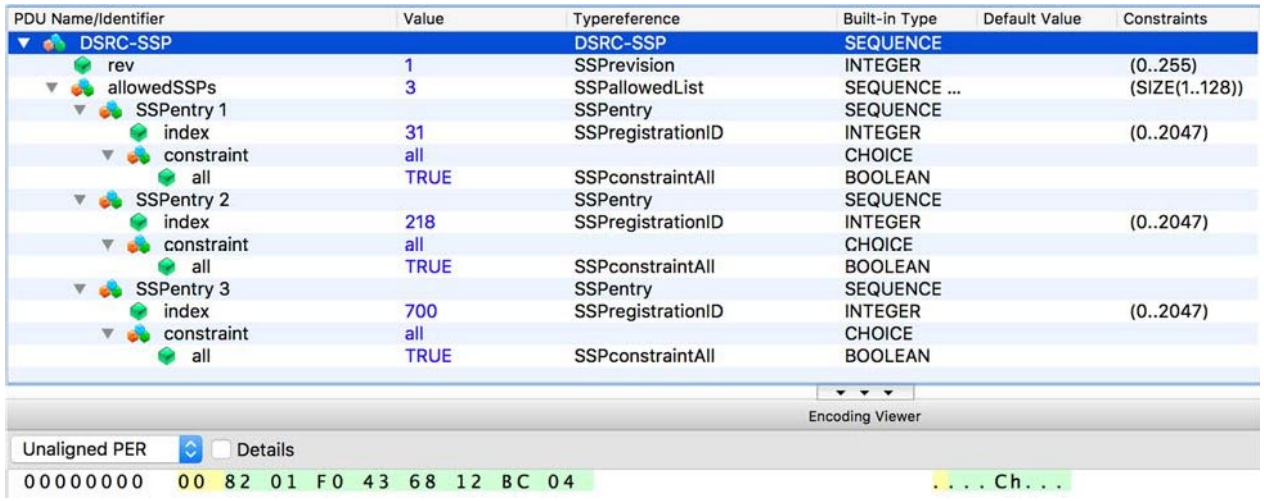


Figure G-3: SSP for TIM Signer with High Velocity BSM Throttling Extension Only (for areas less than 1 sq-km) (Source: CV Pilot Sites)

SSP Binary is: 0x008201F0436812BC04

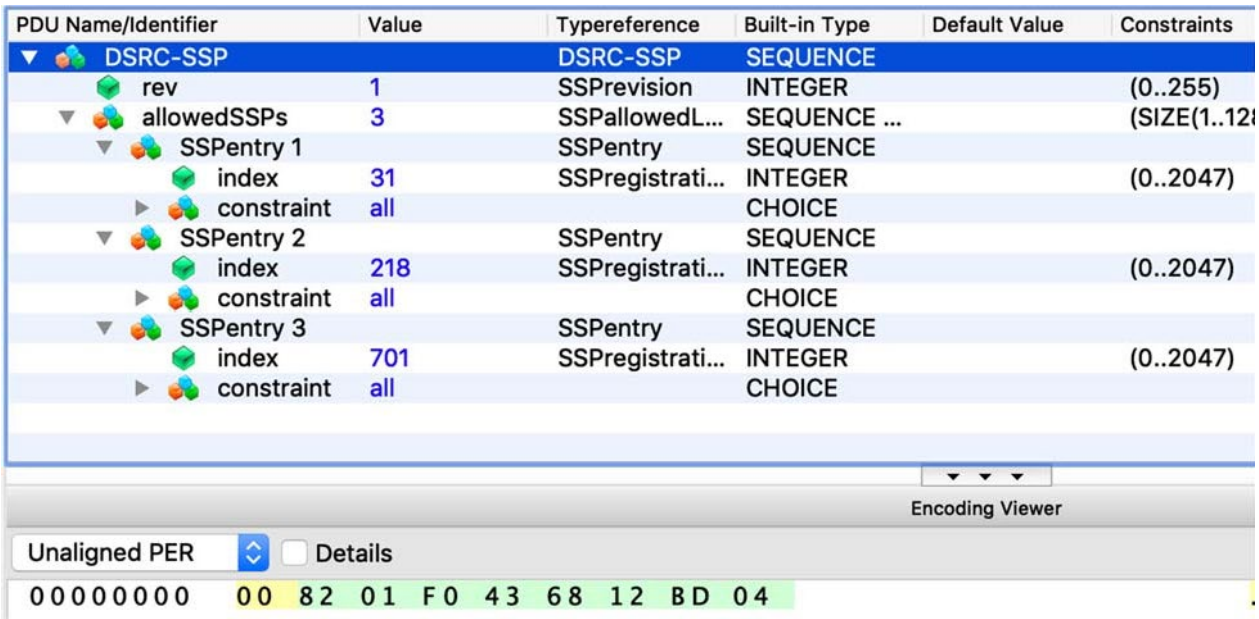


Figure G-4: SSP for TIM Signer with High Acceleration and Low Velocity SSP Only (Source: CV Pilot Sites)

SSP Binary is: 0x008201F0436812BD04

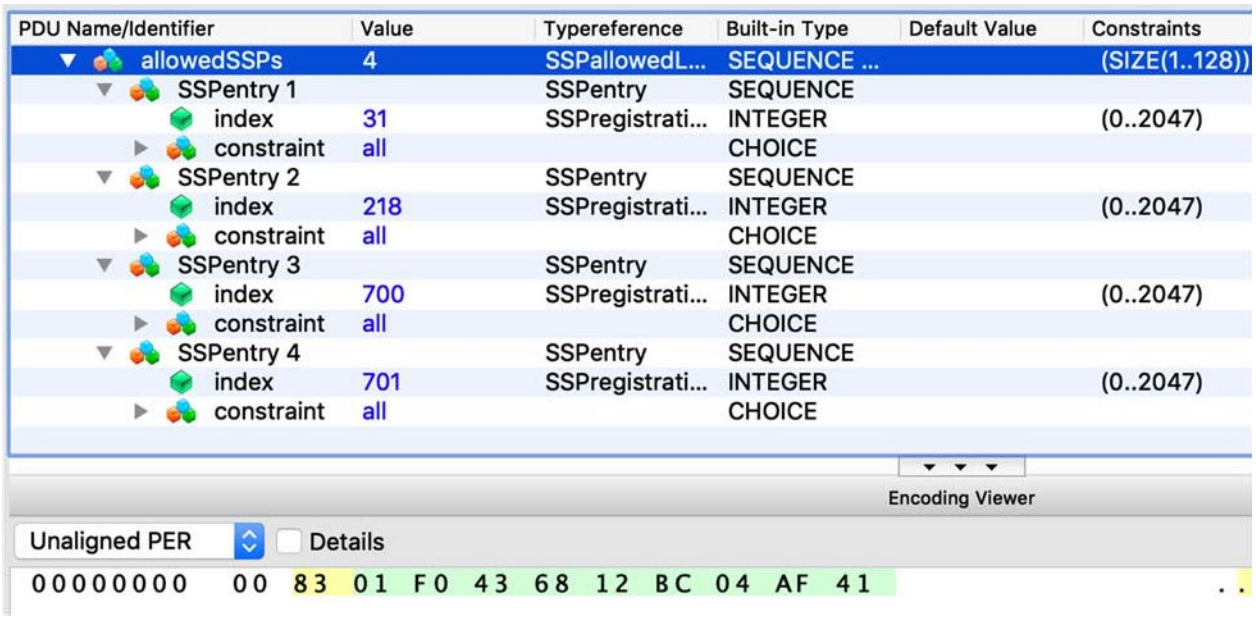


Figure G-5 SSP for TIM Signer with High Acceleration and High Velocity (Source: CV Pilot Sites)

SSP Binary is: 0x008301F0436812BC04AF41

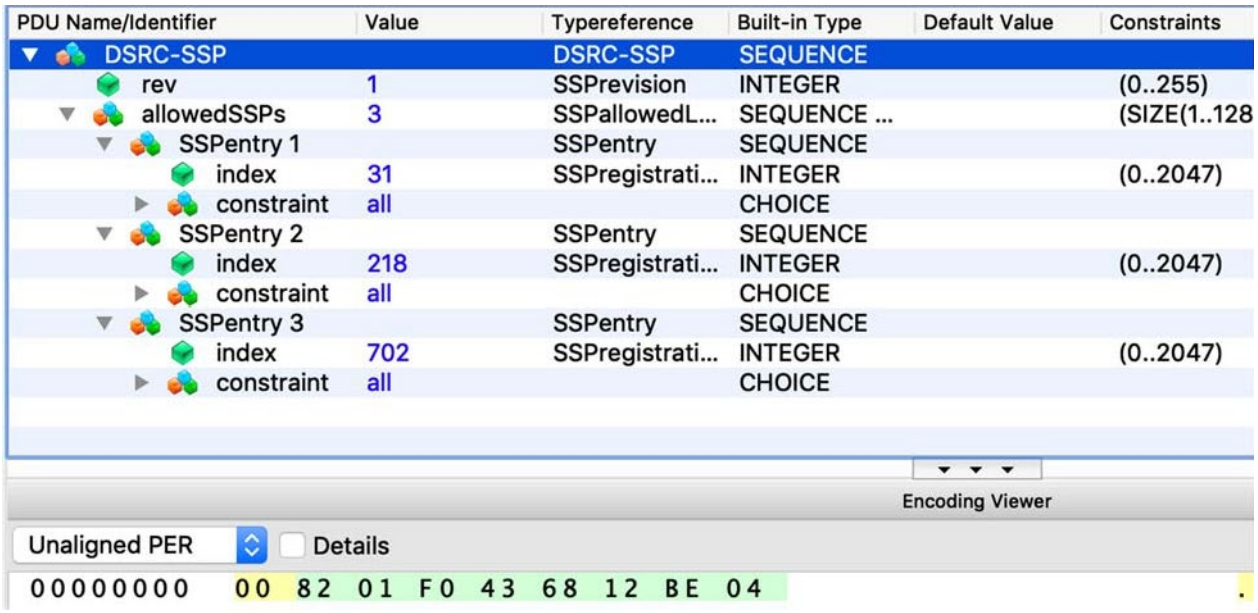


Figure G-6: SSP for TIM Signer with Large Geographic Area SSP Only (Source: CV Pilot Sites)

SSP Binary is: 0x008201F0436812BE04

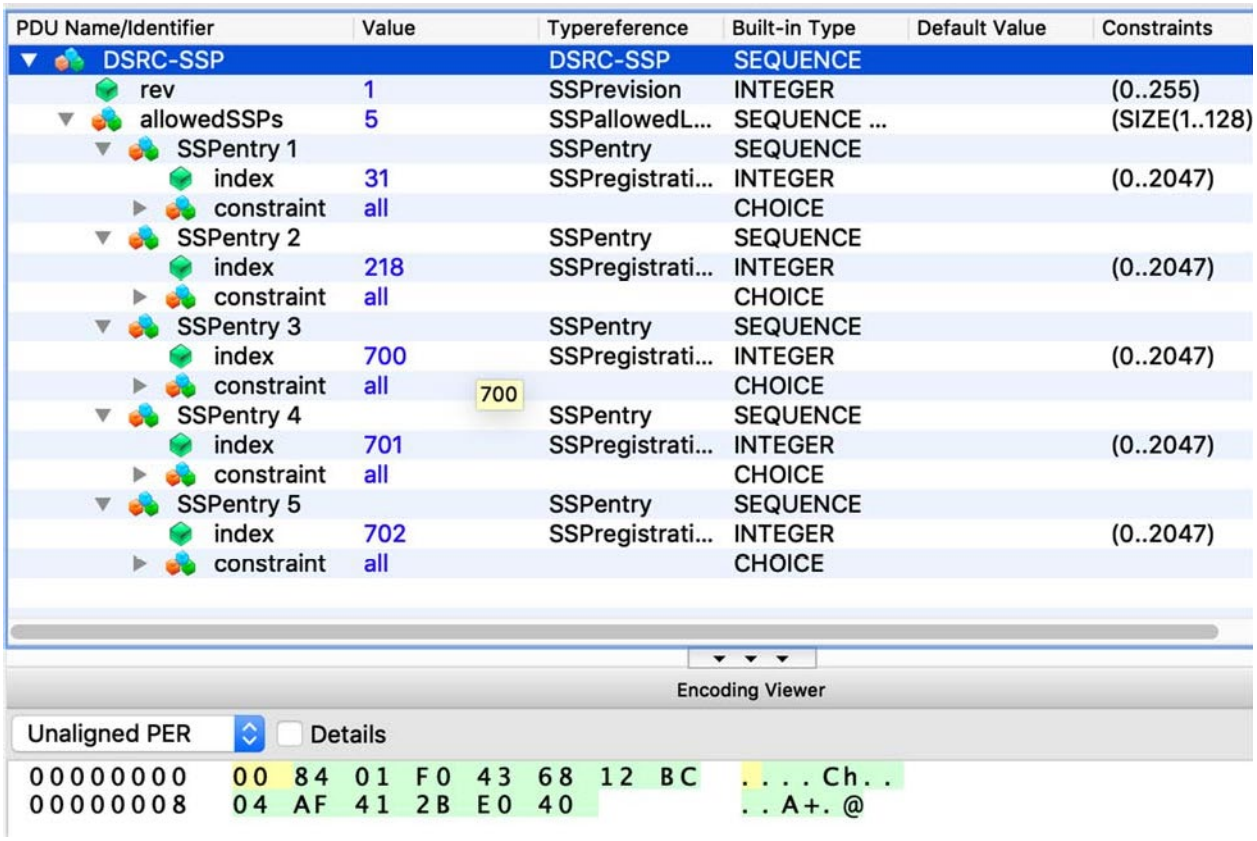


Figure G-7: SSP for TIM Signer with All BSM Throttling Rights (Large area, high velocity, high acceleration) (Source: CV Pilot Sites)

SSP Binary: 0x008401F0436812BC04AF412BE040

U.S. Department of Transportation
ITS Joint Program Office – HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487

www.its.dot.gov

FHWA-JPO-19-778

U.S. Department of Transportation