Connected Vehicle Deployment Technical Assistance

Provider Service Identifiers (PSID) and Service Specific Permissions (SSP) Technical Primer

www.its.dot.gov/index.htm

Report – November 2019
FHWA-JPO-19-777

U.S. Department of Transportation

1. Report No. FHWA-JPO-19-777	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle Connected Vehicles Deployment Technical Assistance, Provider Service Identifiers (PSID) and Service Specific Permissions (SSP) Technical Primer		5. Report Date November 2019 6. Performing Organization Code:
7. Author(s) J.D. Schneeberger (Noblis), Justin Anderson (Noblis), and Amy O'Hara (Noblis)		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
Authenticity and integrity of the communications for connected vehicle applications are ensured using digital signatures and IEEE 1609.2 digital certificates supported by the security credential management system (SCMS). The permissions of the senders are indicated using Provider Service Identifiers (PSID) and Service Specific Permissions (SSPs). The PSID is a globally unique integer value that is associated with a service being provided using a communications system such as 5.9 GHz DSRC WAVE. Associated with PSIDs is a SSP. This technical primer provides an overview of PSIDS and SSPs – including lessons learned from early deployers.

17. Key Words Connected Vehicles, Provider Service Identifiers (PSID), Service Specific Permissions (SSP), CV Pilots	18. Distribution Statement 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 8	22. Price

U.S. Department of Transportation

Introduction

Connected vehicle technologies enable vehicles, roadside infrastructure, and personal portable devices to communicate and share information through wireless communication technology. Onboard units (OBUs) installed on vehicles will continually broadcast information on the vehicle's position, direction, and speed in the form of a Basic Safety Message (BSM). These messages will be received by other vehicles and used active safety applications to assist in reducing traffic-related incidents. Roadside units (RSUs) installed along the roadway will also be able to receive and broadcast messages helping to further improve safety and enhance mobility.

Authenticity and integrity of the communications for connected vehicle applications are ensured using digital signatures and IEEE 1609.2 digital certificates supported by the security credential management system (SCMS). The permissions of the senders are indicated using Provider Service Identifiers (PSID) and Service Specific Permissions (SSPs). The PSID is a globally unique integer value that is associated with a service being provided using a communications system such as 5.9 GHz DSRC WAVE. Associated with PSIDs is a SSP. The SSP can grant certain devices special privileges, such as emergency vehicle preemption for emergency vehicles or transit signal priority for transit vehicles.

Provider Service Identifiers (PSIDs)

The PSID is a globally unique integer value that is associated with a service being provided. PSIDs have three uses:

1. A service provider identifies advertised service opportunities by the PSID values in WAVE Service Advertisement (WSA) messages it transmits.
2. The WAVE Short Message Protocol (WSMP) delivers WAVE Short Message (WSM) content to higher layer entities based on the PSID value set by the sender in the WSM message header.
3. A security certificate lists the PSID value(s) identifying applications for which a sender is authorized to generate signed secured messages.

A WAVE (Wireless Access in Vehicular Environment) system advertises available services by way of sending periodic messages known as WAVE Service Announcements (WSA). A device knows about available PSIDs based on WSA. WSAs advertise the availability of other information and services on other channels within the spectrum.

When a connected vehicle device is within range of a roadside unit (RSU) is must listen to the WSA to understand what services are offered by the RSU. Without WSA's connected vehicle devices and applications would not know how to apply messages being broadcast and thus would not be able to act on those messages. Each WSA may include a list of PSIDs for services that are available on the network, as well as information needed to receive and process the WAVE Short Messages (WSMs) pertaining to each service being advertised. A corresponding security certificate lists the PSID value(s) identifying applications for which a sender is authorized to generate signed, secured messages.

A PSID is a four-byte numeric string used by the IEEE 1609 set of standards announcing that it is providing a service to potential users of an application. PSIDs are generally represented in hexadecimal (numbers from 0 to 15, or 0 to F in ASCII) format. As an example, the vehicle-to-vehicle (V2V) safety applications (e.g., forward collision warning) all use the PSID 0x20 (represented in hexadecimal format

and equivalent to 32 in decimal format). The Basic Safety Message (BSM) will use PSID 0x20 and this allows all V2V safety related applications to receive this message. For intersection safety and awareness (e.g., intersection movement assist and red-light violation warning), the PSID is 0x82. In this case the Signal Phase and Timing (SPAT) message will use PSID 0x82. Upon receiving the PSID, the OBU will know to route these SPAT messages to the intersection safety and awareness applications running on the device. Specific guidance on what PSIDs are, how they are used and where they are provided in DSRC messages can be found in the IEEE 1609.3 and IEEE 1609.12 standards.

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.

Service Specific Permissions (SSPs)

Associated with PSIDs is a SSP. The SSP can grant certain devices special privileges, such as emergency vehicle preemption for emergency vehicles or transit signal priority for transit vehicles. PSIDs are not required to implement a SSP, but for applications that grant enhanced privileges to certain devices it is recommended for security reasons. Per the IEEE PSID registration process, the owner of a PSID is responsible for developing the SSPs associated with that PSID. The official PSID registry listed above also notes who owns a specific PSID and IEEE collects contact information for the owner of each PSID so it can be provided to organizations looking to implement that PSID. For Society of Automotive Engineers (SAE) owned PSIDs, the guidance for SSPs can be found in SAE J2945/5 (https://www.sae.org/standards/content/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. As an example, if an Infrastructure Owner Operator (IOO) is looking to deploy a transit signal priority application, SSPs are a way to ensure that RSUs will only accept signal priority request messages from authorized transit vehicles.

Implementing PSIDs and SSPs

Entities deploying connected vehicle technologies can follow the steps below to implement PSIDs and SSPs in a way that will reduce re-work and increase interoperability with other deployments around the United States. The process for implementing PSIDs and SSPs applies to software and application developers. Infrastructure Owners and Operators (IOOs) roles in the process are for general requirement awareness and coordination with other operating partners. Decisions about PSIDs, SSPs, and certificate types should be made in concert with device vendors and the SCMS vendor—and should be done before application development is finalized. The following steps should be considered.

- **Step 1: Determine the Applications to be Implemented:** Any entity looking to deploy connected vehicle devices should make sure they have a good understanding of the applications that they are planning on implementing in their deployment. This is especially important for V2I applications as that is where SSPs are more prevalent. Additionally, it is important to know what

other connected vehicle deployments a deployer wants to be interoperable with and gather PSID and SSP information from those deployments.

- **Step 2: Refer to the IEEE PSID Registry for Guidance:** Deployers can then start determining what SSP guidance needs to be implemented with the chosen connected vehicle applications. A good starting point is always the IEEE PSID registry to determine who owns the specific PSIDs and if they have already developed SSP guidance.
- **Step 3: If Guidance Doesn't Exist, Work with Other Deployers:** If there isn't any official guidance, then the next step is to work with the other deployments you want to be interoperable with to see if they have specific guidance for SSP implementations. If no one has created SSP guidance for the PSIDs chosen for implementation, then it is recommended that guidance is jointly developed with the deployments that a deployer wants to be interoperable with. Throughout this process it is beneficial for someone on the deployment team (either in the organization or associated with the organization as a vendor or contractor) to have a strong understanding of the SAE and IEEE DSRC related standards to help ensure that chosen solutions don't violate those standards or hamper interoperability.

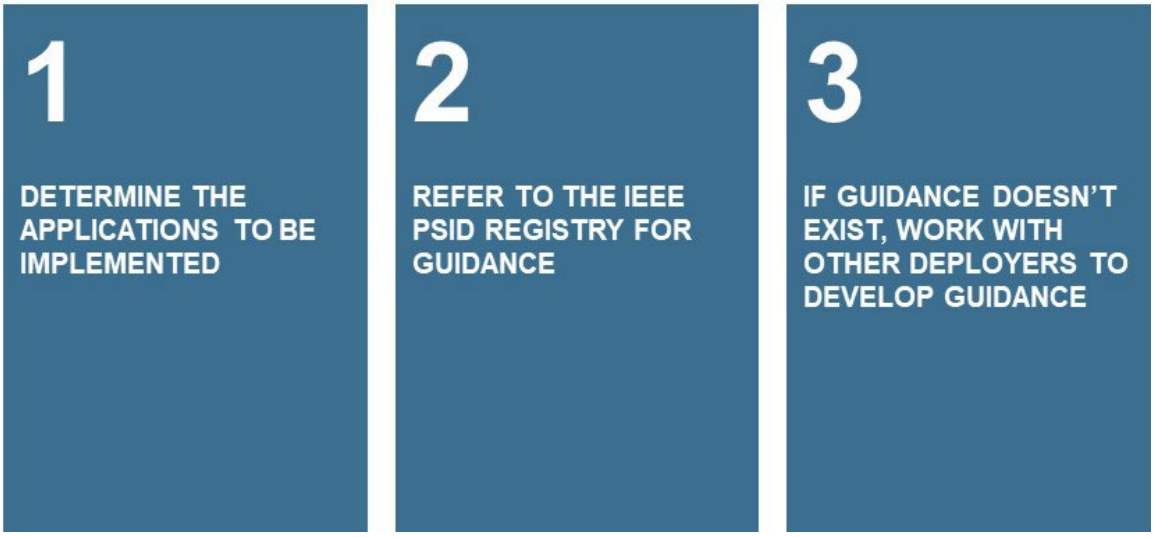

Figure 1. Approach for Implementing PSIDs and SSPs (Source: USDOT)

Lessons Learned and Key Decisions from the CV Pilot Sites

The United States Department of Transportation's (USDOT) 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 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 information gleaned from the CV Pilot deployment experiences is provided below to inform early deployers and guide them to make the best choices for their own deployments. SAE is currently developing guidance (https://www.sae.org/standards/content/j2945/5/) on creating SSPs. Other deployers considering using CV Pilot Security Profiles should may be interested in understanding the key decisions made by the CV Pilot Sites in developing security profiles. IOOs considering deploying connected vehicle technologies should be aware that the process of implementing Security Profiles is not an "off the shelf" process as connected vehicle devices and technologies are still immature. IOO's should fully expect and anticipate having to make changes to the technologies they deploy to maintain interoperability.

- **Understand What Applications Devices Will Be Supporting Early in the Process:** Prior to procuring a SCMS vendor, entities should know what applications their devices will be supporting. When deploying secure connected vehicle devices that are signing messages with certificates from a SCMS, knowing the applications the devices will support, and the messages utilized by those applications is extremely important. As part of the initialization/set-up process for these connected vehicle devices, they will need to enroll with the SCMS for specific PSIDs as well as specific SSPs (if necessary). If these devices are deployed without enrolling with the proper PSIDs and SSPs, re-initialization of those devices may be required, which could entail pulling down RSUs off of mast arms or removing OBUs from vehicles and bringing them back to a depot.
- **MAP Security Profile Considerations – Signing Messages at the TMC or RSU:** The NYC DOT CV Pilot Site is taking an approach to centrally sign messages at the TMC while the THEA CV Pilot Site is signing at the RSU. Originally, the CV Pilot Sites considered the option of developing separate security profiles, but it was later determined that it would be easier to develop a single MAP Security Profile that both sites could use. The RSU specification used did not support the remote signing of certificates. As a result, this will be addressed in NTCIP 1202 version 3 (current published version is NTCIP 1202 version 2). NYC had to work with their RSU vendor to develop a temporary approach while the standards process continues. The approach used by NYC DOT is to assign a separate block (index above 100) to indicate a pre-signed message from the TMC. Users of CV Pilot Security Profiles may find it difficult to understand what the CV Pilots did because this was not addressed in the current development of the new standard *NTCIP 1218: Object Definitions for Roadside Unit Standard (RSU)*.
- **CV Pilots Sites' Decision to Remove SSPs for BSMs:** The CV Pilot Sites thought as pilots it would be good practice to deploy SSPs using existing processes outlined in SAE 2945/2 to protect the messages and to protect what the CV Pilots wanted to accomplish with their deployments. This was not well received by the larger connected vehicle community as there are concerns within the community in defining what permissions a vehicle can have when going through the SCMS enrollment process. As a result, the BSM Security profile was dramatically modified to remove

SSPs. SSPs were used for the SPaT and MAP messages because the sites wanted to protect regulatory speed content from being spoofed by bad actors. NYC is using MAP to provide speed limit information using MAP instead of TIMs. THEA is using MAP to provide advisory speed information. These are all pre-standard usage using concepts from J2945/2 to avoid impacts to future standards decisions.

- **PSIDs for Over-the-Air Uploads and Downloads:** The NYC CV Pilot Site originally planned to have one PSID for both over-the-air (OTA) uploads and downloads; however, it was later decided to use separate PSIDs for uploads and downloads. This was done because of the density of RSUs in NYC where analysis determined that different channels were needed for channelization planning. More complex channelization plans were required because of the density of RSUs and separating the PSIDs allowed more flexibility. OTA downloads broadcast or perform on-demand functions but all use the same PSID

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-19-776

U.S. Department of Transportation