Secure Vehicle Interface (SVI)

Preserving Open Access to Vehicles and Ensuring Security

TECHNICAL PAPER

DATE: AUGUST 18, 2018

1 ABSTRACT

Today's vehicles are generating an enormous amount of data derived from the vehicle ECUs, sensors, drivers, and passengers. The amount and type of vehicle data generated by the vehicle will continue to grow as data such as driver and passenger biometrics is collected. As vehicles become more connected, all of this vehicle data will be communicated and potentially stored for use in applications such as vehicle-to-vehicle (V2V) communications, vehicle-to-infrastructure (V2I), diagnostics and maintenance, and big data, where it will be analyzed by transportation authorities, insurance companies, automotive industry, and others. As vehicles are networked to the Internet, to the traffic infrastructure, and to one another, it is imperative that the interface to the in-vehicle network (IVN) be secure from attack and abuse. It is also important that the interface to the vehicle be standardized and open to allow for direct access to time-sensitive data and for access by the open market for aftermarket services, such as maintenance and repair service providers, telematics service providers, etc. This forms the typical security versus productivity dichotomy that needs to be addressed and balanced to provide adequate security and safety while allowing for an open marketplace and the efficient exchange of data required to implement future V2V and V2I solutions that aim to reduce traffic congestion, pollution and improve transportation safety.

2 Introduction

The Secure Vehicle Interface (SVI) described in this paper leverages existing and evolving standards that, when implemented, establish a secure, open, and standardized solution. There are three basic principles that make up the SVI:

1. **Security:** A major goal of SVI is to continue to allow access and control of vehicle data by the vehicle owner, which requires that access to the vehicle's network and data be authorized by the owner. SVI helps to ensure that the vehicle owner has control of their vehicle data and the authorization for who and what systems can access their vehicle data. Just as a cell phone user can authorize who or what systems can access their cell phone data, including location and performance data. SVI provides the same ability for the vehicle owner. SVI achieves this by implementing a concept of a hierarchical structure of Certificate Authorities (CA) cryptographically issuing and signing identity certificates.

2. **Standard Data Format:** SVI implements standard vehicle data formats to facilitate timely and efficient communications between all network entities. This efficiency extends to the cost benefits of a standard language shared by all vehicle manufacturers for external communications between vehicles and between the vehicle and the transportation network as well as the aftermarket service providers and suppliers. A standard data library reduces the need for data translation and the need for multiple implementations of the same functionality to accommodate different proprietary implementations.

3. **Secure Communication Profiles**: SVI implements secure communication profiles that can be applied to existing and future communications standard protocols as they evolve, and SVI closes an existing gap by defining a direct, secure interface between the in-vehicle network (IVN) and the Intelligent Transport System (ITS).

Each of these core principles is defined in corresponding, evolving ISO standards documents, which are also a culmination of established international standards as depicted in Figure 1 SVI References.

1. **Standard Data Format –** ISO 21184 ITS Management of messages containing information on sensor and control networks specified in data dictionaries

2. **Security -** ISO 21117 Intelligent transport systems — ITS-station security services for secure session establishment and authentication between trusted devices

3. **Secure Communications Profiles:** - ISO 21185 Communication profiles for secure connections between trusted devices

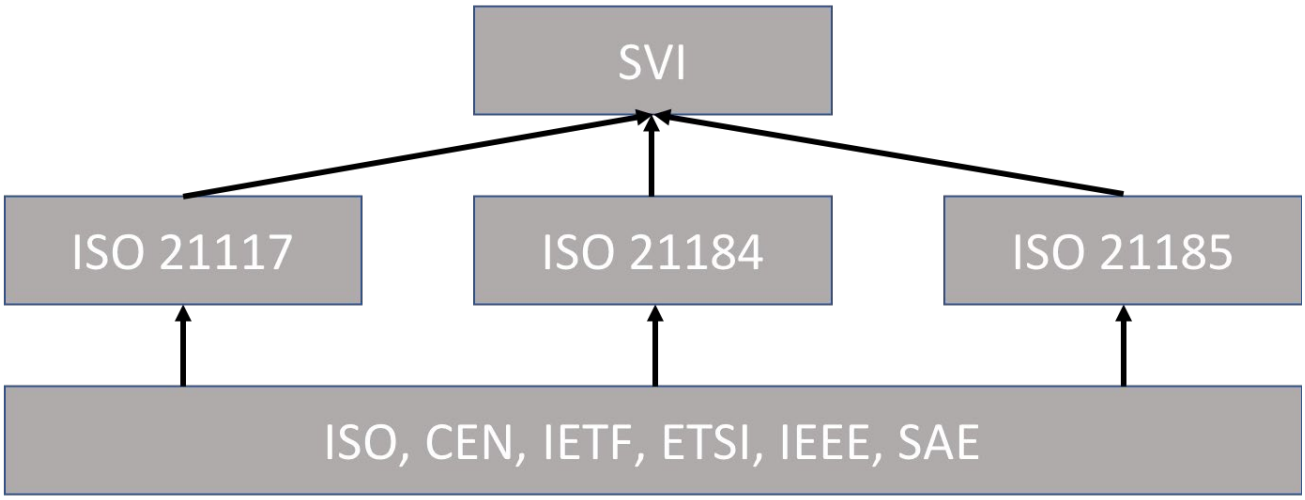


Figure 1 SVI References

3 SVI in the Intelligent Transport System (ITS) – Station, Overview

In order to fully grasp the principles of SVI, it is important to have a general understanding of ITS. Specifically, the ITS station and its architecture. ISO, CEN, and ETSI standards bodies agreed on a common Intelligent Transport System (ITS) architecture and terminology that is standardized in ISO 21217 and EN 302 3665. The ITS station architecture is based on a simplified OSI reference model, as seen in Figure 2.

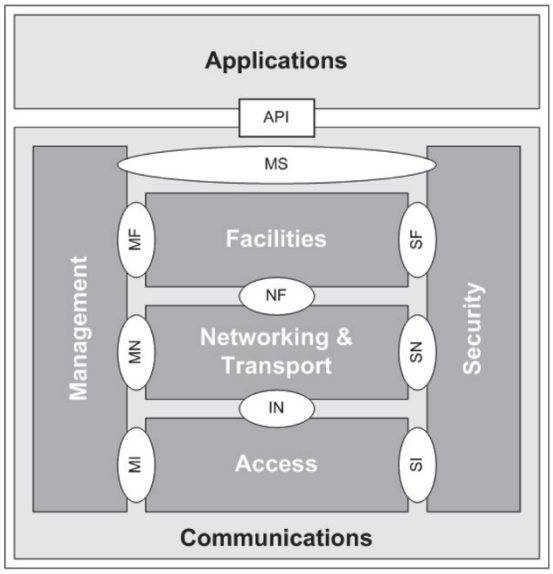


Figure 2 Simplified OSI Reference Model

The ITS station concept has many aspects discussed below that make it practical for use as the basis of the SVI.

- An ITS station is a concept that is defined and supported by several Standards organizations. Therefore, it is a long-term, trustable platform for all transport-related services that need stability and official support to ensure compatibility between all ITS entities, including the vehicle itself.
- An ITS station is defined as a Bounded, Secured, Managed Domain
    - Bounded means that there is a defined border, where everything on the inside belongs under the umbrella of the ITS station, and everything outside that border is not subject to this particular set of standards.
    - Secured means that everything on the inside of the boundary is secured and trusted.
    - Managed means that the Station must have a certain set of management functions, usually including remote secure management for operation, maintenance, and application loading and updating.
    - Domain means that an ITS station belongs to a family of stations where there is implicit trust and exchange of information between relevant applications/services.

- The ITS Station follows a strict, layered communication concept, which means that it supports different communication interfaces and protocols. Therefore, adding another protocol to the standard set is straightforward and does not require modifications to higher-layer functions.
- The exchange of information between ITS Stations occurs between Applications. This means an application in one ITS station is always the sender, and an application in another station is always the receiver. This ensures that only approved applications and services gain access to certain types of information.
- Applications may be end-user applications that are installed at the top to do one specific task or facility layer applications that handle information exchange without direct end-user involvement.
- An ITS station may be usage-specific and contain only one application, or it can act as a technical platform for multiple applications. The platform concept is similar to smartphones and apps, and this multi-application platform is the preferred solution in most implementations due to the added flexibility and cost reductions.
- Each application or service can have security provisions attached. These are called service-specific permissions (SSPs) and are tightly controlled by a hierarchy of trusted certificate authorities. Who gets the rights to information and how the approval process works is defined in a Security Policy that is defined for each subject area. There is also a related Certificate Policy that determines the more practical aspects of the certificate lifetime etc.
- Interfaces to the outside are facilitated by Gateways. A gateway will perform three main functions:
    - Connecting to the often proprietary, external world to send and receive information.
    - Translating the information between external formats and the standardized ITS format.
    - Secure and filter the link to the external world, which is often referred to as a firewall function.

The following drawing, adapted from ISO 21217, illustrates peer-to-peer connectivity between ITS Stations. The drawing shows many different components that are or may be involved in ITS communications. For the purposes of this paper, we are going to focus on the Vehicle ITS sub-system and how SVI can be implemented to provide the necessary secure interface to the proprietary in-vehicle network. It should be apparent that in order for the vehicle ITS station to function effectively within the ITS architecture, that information, e.g., vehicle speed, location, steering wheel position, etc., must be communicated to other peer systems. Since this information resides within the IVN proprietary network, an interface must be implemented. This interface should also be secure and standard, and the information should be formatted in a standard format.

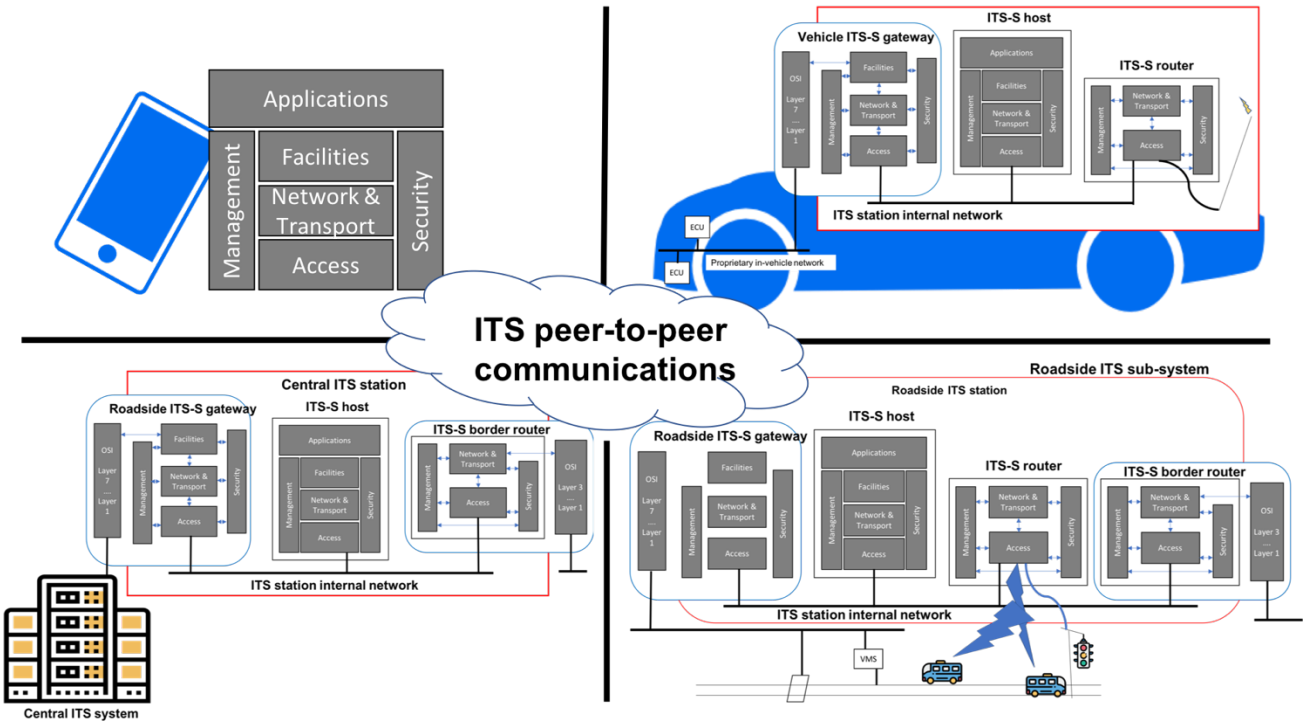


Figure 3 ITS Station

As we focus directly on the vehicle ITS station, it is important to point out that the roles within the ITS station can be combined, and in many instances, it is practical to at least combine the gateway and host in order to reduce complexity and costs. An example of this is depicted below in Figure 4.

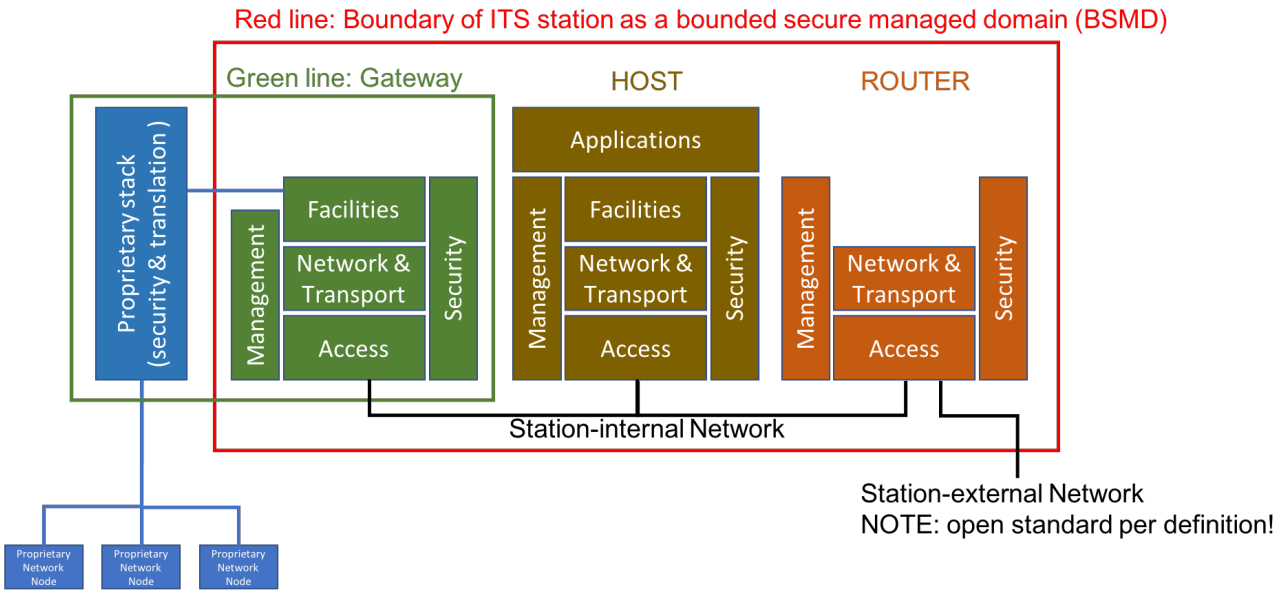


Figure 4 Boundary of ITS Station

As previously mentioned, an ITS station is a bounded secure managed domain (BSMD), and as seen above, the Gateway, Host, and Router functions reside within the secure domain, and the gateway extends from within the domain in order to perform its task of interfacing to the external proprietary network. In this drawing, the translation and firewall functionality are theoretically happening where the blue line from the proprietary stack crosses the red line toward the Facilities. In a practical implementation, the translation function is split between the proprietary stack and the relevant station facilities application, and the firewall functionality is distributed over most of the functional blocks within the ITS bounded domain.

The flexibility that the ITS station provides by not being limited to a single access technology or a specific networking transport protocol through its ability to support any technologies that have appropriate adaptation specifications makes it uniquely suitable for implementation as part of the SVI. This capability is important in the constantly evolving landscape of the modern, connected transportation system.

Where SVI Fits in ITS

The red arrow in Figure 5 shows where the SVI is placed in an ITS station. This means that the SVI will be a fully functional ITS station interface that can be connected to other ITS stations, either via a station-internal network or to any other ITS station via a router function.

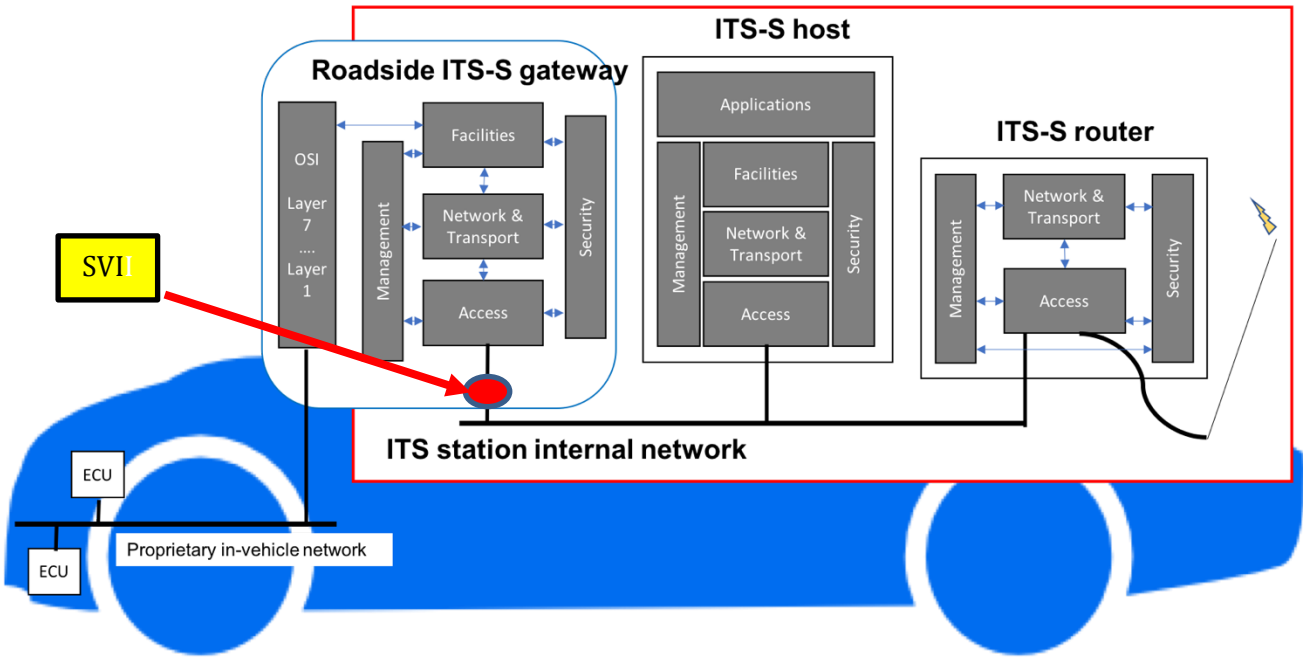


Figure 5 SVI Position in ITS Station

4 SVI Evolution

In the future, a full ITS station will likely be included in the vehicle design so that only the SVI will be exposed and accessible to the owner and other approved users, such as aftermarket service providers. Expanding on this long term view, we have the following depiction in Figure 6:

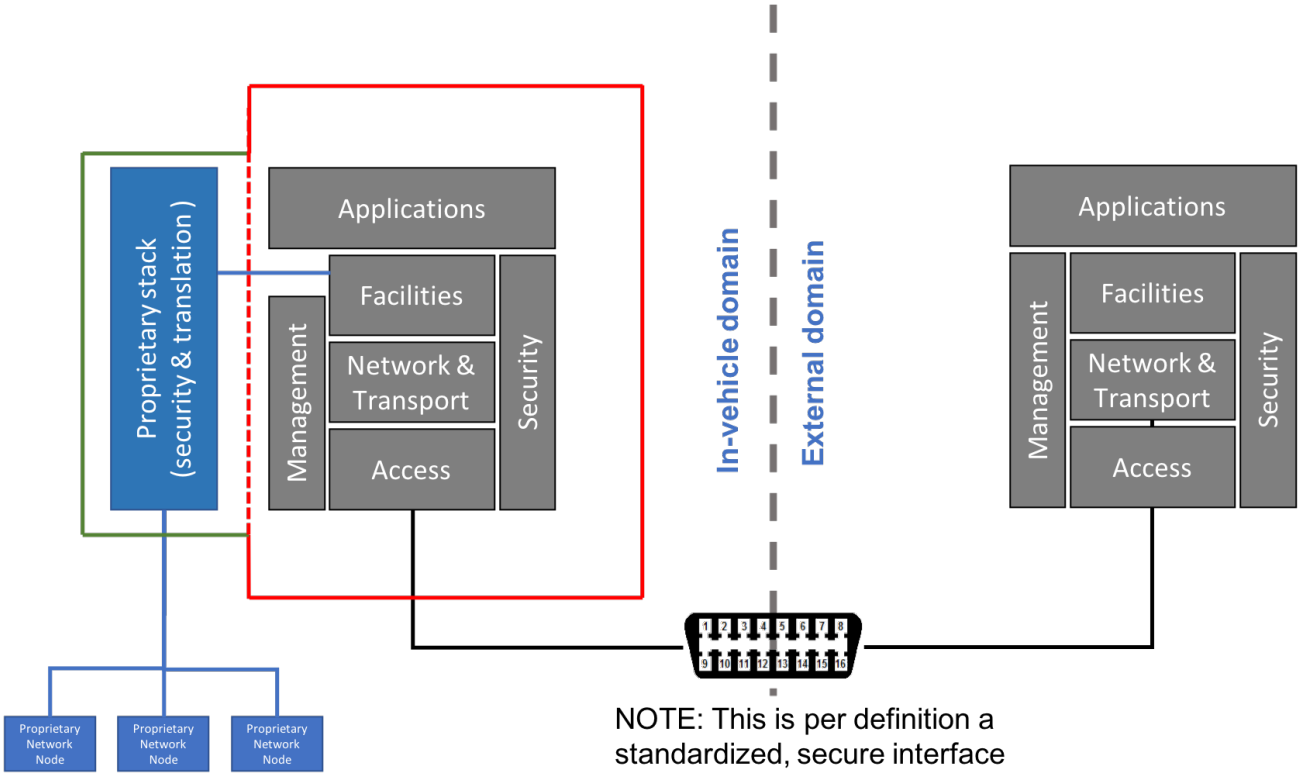


Figure 6 ITS Incorporated in Vehicle

In Figure 7, we can see the SVI symbolized as an exposed OBD-II connector, and this already mandated interface is intended to be extended with physical wired Ethernet. As additional SVI communications profiles are added, wireless access will also be supported if a Router is added, which makes the architecture future-proof. The vehicle manufacture may choose to implement light versions of the ITS station, but it is more likely that they implement a relatively complete version, as global regions, such as Europe, are likely to require a full version of SVI as a legal requirement. As the vehicle is a primary peer in ITS, intuitively, it would be equipped with the same standard interfaces and security standards as all other ITS peers. The following figure illustrates the concept of an IVN with an IVN gateway facing the SVI and a CAN allocated for ITS. The SVI functions are implemented logically separated from the IVN but optionally physically separated from the IVN Gateway.

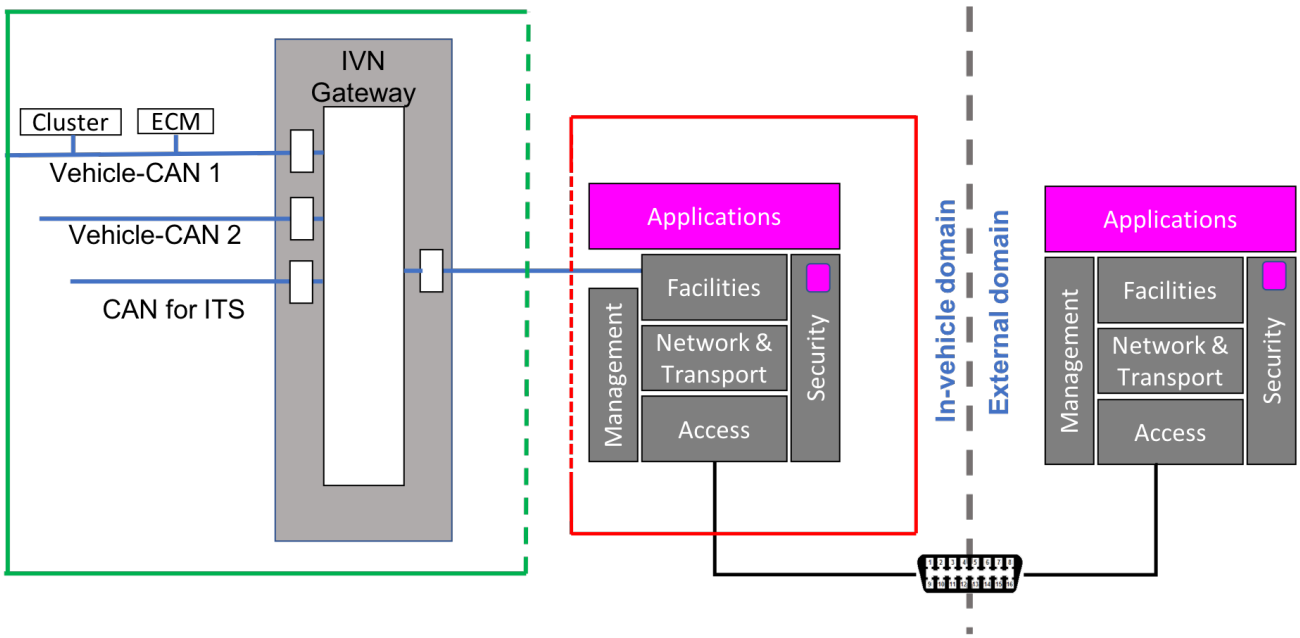


Figure 7 In-vehicle network gateway connected to internal ITS Station

5 Secure communications over SVI

Figure 8 shows secure communication flow over the exposed SVI. The applications layer on each side communicate with each other in a secure way, where data access and control mechanisms are handled by the security provisions in the Security management. These provisions are depicted by the violet box in the Security plane, which contains all relevant access rights and crypto material (keys, certificates). The technical security description is more thoroughly described in the SVI security section of this paper.

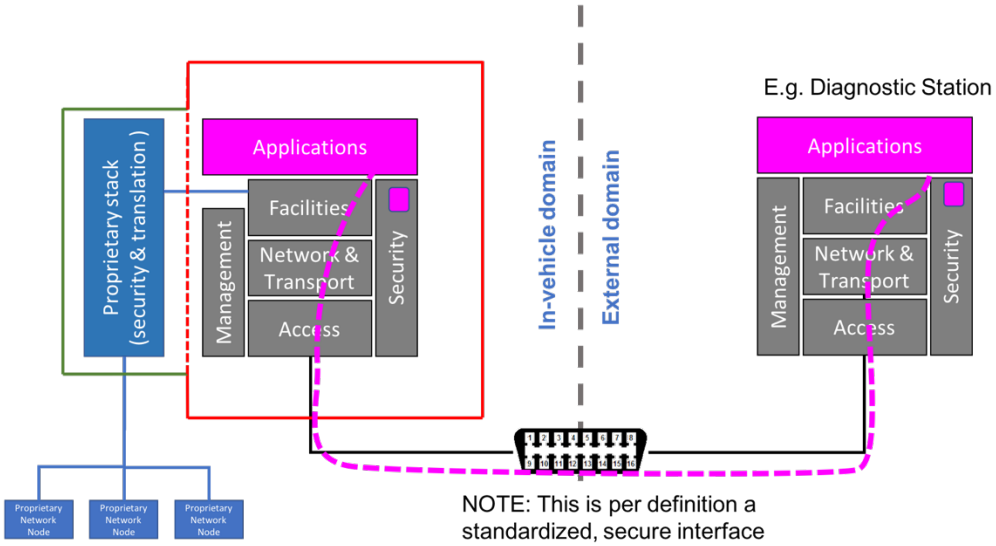


Figure 8 Secure Communications Over SVI

6 SVI Security Description

The objectives of ITS security are to ensure the authenticity of the source and confidentiality and integrity of application activities taking place between trusted devices. The trust relation between two devices is illustrated in figure 9. Two devices cooperate in a trusted way, i.e. exchange information with optional explicit bi-directional protection.

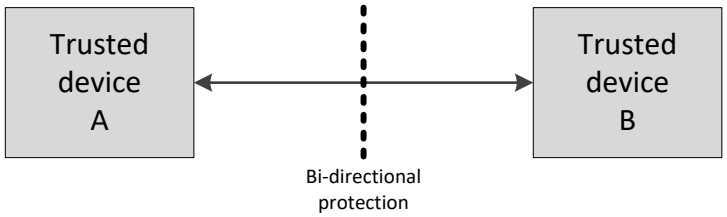


Figure 9 ITS Trust Relationship

In regard to SVI, the relationship is between an ITS station and an internal proprietary network as depicted in figure 10. This relationship is the same for all ITS communications network peers and associated proprietary internal networks and allows for the peers to participate in related ITS services e.g. sustainability, road safety and transportation efficiency. All of these services and services yet to be envisioned do and will rely on access to the Sensor and Control Networks (SCN) of the peers in order for ITS to function optimally and affectively and thereby maximizing transportation safety and efficiency.

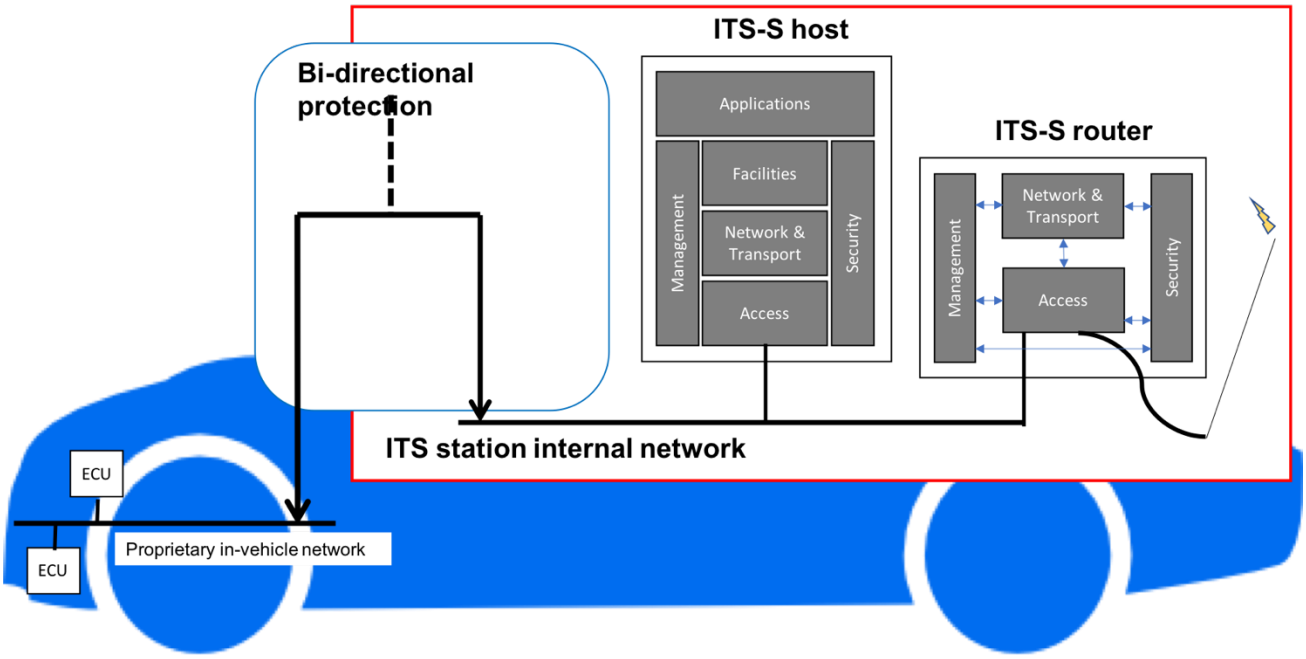


Figure 9 ITS Station to IVN Relationship

For reasons previously discussed in this paper, access to and from the SCNs must be secure. This requires the establishment of secure application sessions which in turn, requires either a-priori knowledge of the peers or the use of service announcement messages per ISO 22418. Additionally, other security means may be applied, e.g. encryption of messages.

Figure 11 illustrates the connection between and ITS station and a SCN residing on a proprietary internal network. The interface between the two networks is facilitated by an SVI that implements the necessary security to provide a trust relationship. The SVI may be a standalone device or may be part of the SCN which could be an IVN, or any other internal proprietary network.

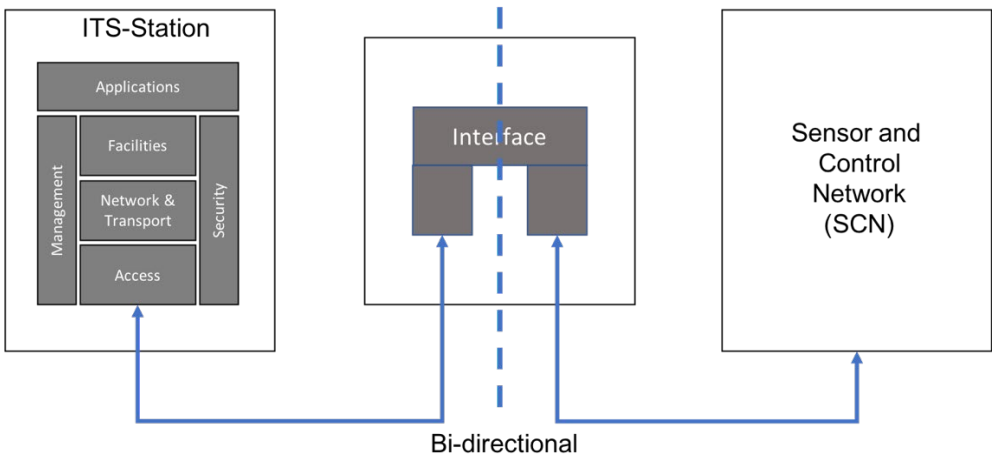


Figure 11 SVI Interface to SCN

Use cases of these ITS services have largely been derived from regulatory requirements and ITS operational needs, which include:

— secure real-time access to time-critical vehicle-related data for the safety of life and property applications, e.g. collision avoidance, emergency electronic brake light, and event determination.

— secure local access to detailed real-time data for efficiency applications (traffic management), e.g. intersection interaction, congestion avoidance, and dynamic priorities.

— protection of private data, e.g. in compliance with the European "General Data Protection Regulation" (GDPR).

— local access to certified real-time data for sustainability applications, e.g. dynamic emission zones (controlled zones as currently standardized in CEN TC278 within the Project Team PT1705 funded by the European Commission), intersection priorities based on emissions, interactive optimum vehicle settings to minimize fuel consumption.

There are many use cases of ITS services currently identified where real-time exchange of time-critical information between ITS stations in close proximity is essential, and the number will grow, e.g., the US National ITS Reference Architecture. It is critical that, ultimately, all ITS stations in a given area are able to be engaged in these distributed services. This, in turn, requires vehicle ITS stations to have real-time access to vehicle data and roadside ITS stations to have real-time access to infrastructure data.

The ITS standards allow for the communications between ITS compliant devices and external devices that are not compliant with ITS standards. In order to have trusted communications a certain minimum level of security measures must be shared between an ITS station and an external device. Examples of such external devices are a node in the Internet or a node in a sensor and control network. The assumption is made that ITS station application processes are issued certificates by a Certificate Authority (CA), and that the CA is a trusted third party in the sense that before issuing the certificate to the ITS station application process, it ensures that the ITS station application process meets the minimum-security requirements for that application. This allows peer ITS station application processes to observe that another ITS station application process possesses a valid certificate and is, in fact, secure and trustworthy.

ITS communications security services, specifically in regard to SVI, are listed below:

- (source) authenticity - did the data come from a trusted source?
- (data) integrity – was the data altered in transit?
- (data) availability - will the required information be available when it is needed?
- (data) confidentiality – is there any possibility that unauthorized entities got a hold of the data?
- (source) non-repudiation: Can it be proven to a third party that the data received actually originated from the source indicated in that data?

Figure 12 depicts the logical architecture of secure communications between ITS station applications.

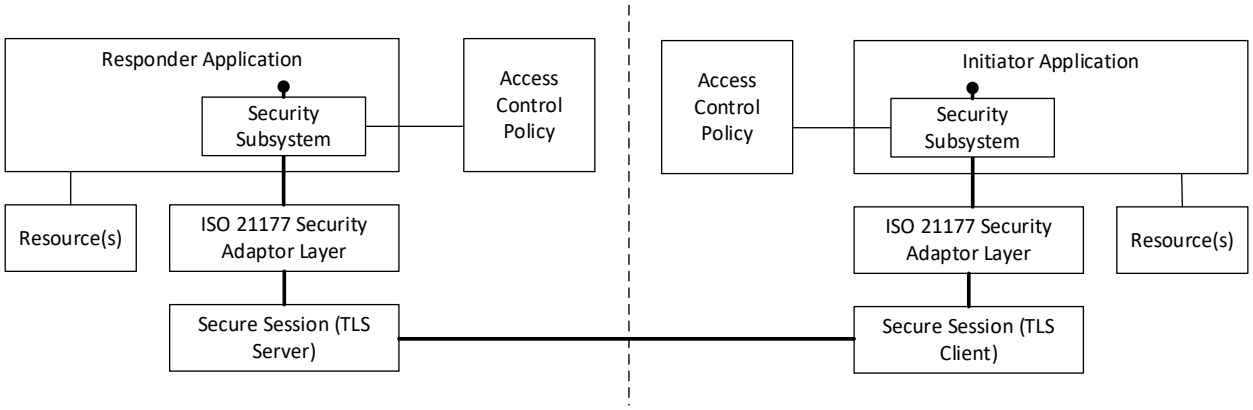


Figure 12 Logical Security Architecture

Functional entities are:

— **Resources:** These are endpoints of ITS-S application process activity and may be inside or outside the ITS station on which the ITS-S application process resides.

— **Application:** This is an ITS-S application process that uses input from resources, from a peer ITS-S application process (peer Application), and from its own state to carry out application activities.

— **Security Subsystem:** The security subsystem applies security mechanisms to determine what actions the peer Application is permitted to take and implements support functionality in support of making those decisions.

The Security Subsystem is configured using input from the Access Control Policy data source. For outgoing communications, it takes as input commands and data from the Application and applies appropriate security processing. For incoming communications, it takes as input commands and data from the Security Adaptor Layer and applies the appropriate access control policy; as a result of applying the access control policy it either passes the input to the application or generates an access control response.

— **Security Adaptor Layer:** This is a multiplexer/demultiplexer that allows both data, i.e. communications between the Applications themselves, and session control commands, i.e. communications between peer instances of Security Subsystem or the Security Adaptor Layer, to be sent over the same secure session.

— **Secure session:** This provides confidentiality, integrity, authentication, guaranteed in-order delivery, and replay protection on the datagrams that are passed over it. In this version of this document there are two types of secure session:

— **Cryptographic secure session:** this uses cryptography to achieve the listed security properties. Any secure session which passes outside the secure boundary of the ITS station shall be a cryptographic secure session.

— **Physical secure session**: this is a session between two Applications running in the same ITS station, i.e. the information flow does not pass outside the ITS station secure boundary. In this case, because the ITS station is a trusted domain, all the security properties listed above are

assumed to hold. This document does not provide a specification of a physical secure session but permits the use of a physical secure session.

These communications security mechanisms are used to provide access control functionality to ensure that access to resources is only carried out by parties that are entitled to that resource. The security in the SVI is focused on ensuring proper access control. An unauthorized device may not have any access to the in-vehicle network whatsoever, and different devices may have different types of access; one device may only have read access to a subset of diagnostic information, while another device may be permitted to send control messages to components within the in-vehicle network. ISO 21117 specifies access control policies and mechanisms for enforcing them, allowing different access control requirements for access to different resources. Figure 13 gives a high-level illustration of SVI in-vehicle network access control functionality.

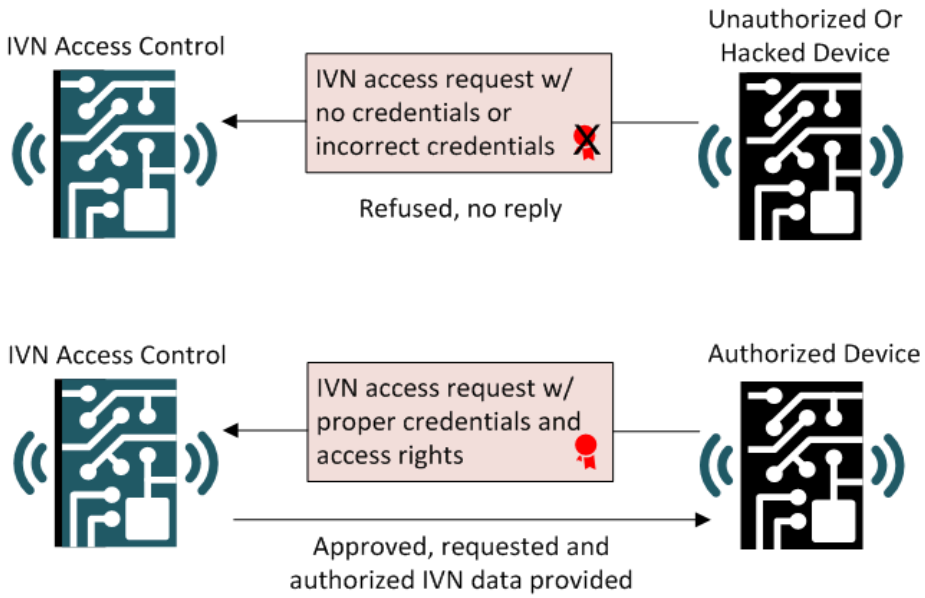


Figure 13 – The SVI in-vehicle network access control

For a complete description of the ITS station security services that are required to ensure the authenticity of the source and the integrity of the information exchanged between trusted entities please refer to **ISO 21117 Intelligent transport systems — ITS-station security services for secure session establishment and authentication between trusted devices**.

7 SVI Standard Data Format

The SVI data format function is a bi-directional data translator with a standardized and simple API (Application Programming Interface) supporting the Unified Gateway Protocol (ISO 13185-2 UGP). The IVNs of the vehicle, sensor and control networks of ITS stations, and networks used within ITS are

specialized to support the requirements of real-time measurements and controls. The complexity inside such systems differs between the domains and individual systems. A bi-directional data translation library is needed for each system to convert raw data to standardized data types and vice versa is therefore necessary for obvious efficiency and cost savings reasons.

The ISO 13185-2:2015 UGP has been developed in ISO TC204/WG17 – ITS Nomadic and Mobile Devices. Connecting e.g. Smartphones to IVNs is only possible utilizing the USB or the wireless connectivity of a mobile device. The protocols and messages implemented in the IVNs are vehicle-specific and optimized for its purpose. The solution for accessing IVN-specific data is the UGP application layer protocol, which has specified a superset of services for all known/standardized application layer protocol message functionality. UGP is supported by the SVI software. ISO 13185-3 specifies the UGP client and server API.

UGP supports the Vehicle Interface Data Format (VIDF) message format defined in ASN.1 (ISO/IEC 8825-1:2015 Abstract Syntax Notation One), see Annex of ISO 13185-2. VIDF is based on a standardized data model, which supports not only all types of diagnostic messages and data but also non-diagnostic message sets of other domains e.g. IVN, ITS, Smart Grid. Each VIDF data parameter uses a specific data type, which is based on a set of standardized data types. The actual data of a parameter is runtime optimized. Each data parameter has a time-stamp, which includes date and time of measurement/event occurrence.

Each vehicle has its own set of VIDF configurations. This is comparable to a vehicle-specific EPC (Electronic Parts Catalogue). The VIDF configurations for IVN would be published by the vehicle manufacturer/domain owner. Each VIDF configuration should have a certificate to prove authentication. Figure 14 shows an example of an IVN raw data conversion to VIDF value based on IVN configuration information.

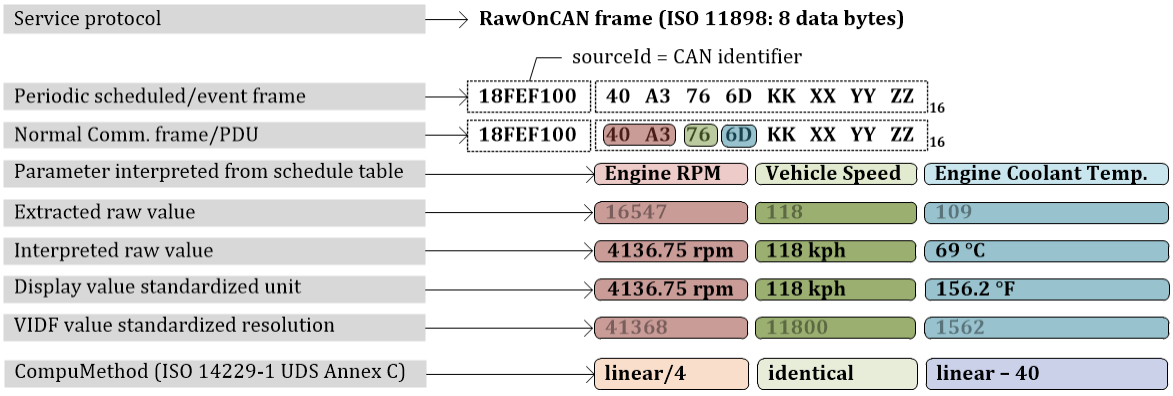


Figure 14 Raw Data Conversion to VIDF

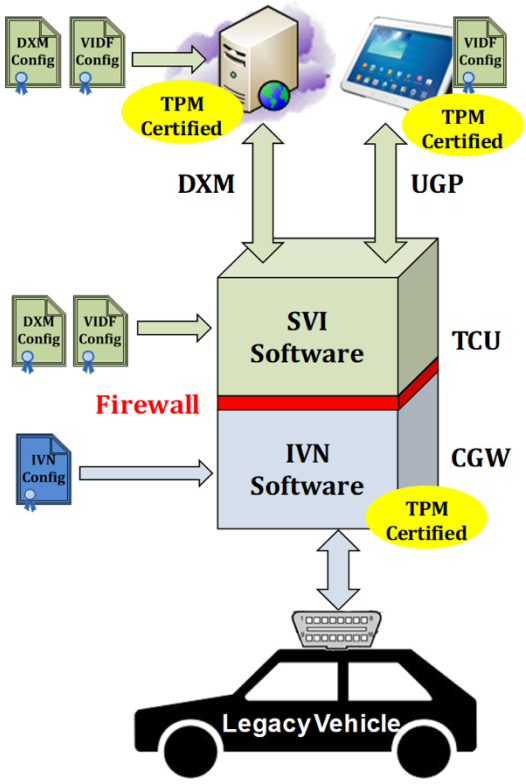
The IVN configuration data is key to the SVI standard formatting and includes all necessary information to access all types of raw data of any IVN connected with SVI-compatible IVN software. Most, but not all, raw data can be directly filtered at runtime from the IVNs. The majority of raw data occurs on event- or schedule-basis. Using this access method does not cause additional bandwidth and therefore is the preferred methodology for continuous refresh of all data defined in the IVN configuration.

The minority of data is diagnostics, which is mainly performed, while the vehicle is not being driven. Most diagnostic protocols require a request and response message scheme. Diagnostic protocols negatively impact the available bandwidth of the IVNs and are not recommended to be executed while the vehicle is being driven. The diagnostic data is mainly required while the vehicle is in the service repair shop.

Once the relevant raw data is extracted from the IVN, the IVN configuration information is used to convert the raw data into the VIDF-defined format. Each data parameter is mapped to an ECU identifier, has a data type, a value matching the data type, and a time stamp when posted to the data pool of the Data Provider inside the SVI software.

Flexibility is required for the support of additional data parameters at any time when new use cases require data, currently not included in the IVN configuration. This is a key element of the SVI-compatible IVN software for enabling future upgrades to support new applications with required data over the life cycle of the vehicle. An example could be, that a traffic management system initially only requires anonymous location information (GPS) but several years later may additionally require the vehicle type (passenger car, truck, ...) to improve traffic flow. Such a scenario might occur more than once over the life cycle of the vehicle.

Figure 15 depicts an aftermarket SVI implementation.



Key	Description
DXM	Data eXchange Message
UGP	Unified Gateway Protocol
VIDF	Vehicle Interface Data Format
TPM	Trusted Platform Module
SVI	Secured Vehicle Interface
TCU	Telematics Control Unit
IVN	In-Vehicle Network
CGW	Central GateWay

Figure 15 Aftermarket Implementations

In a fully integrated configuration of SVI, it is part of the vehicle's CGW (central gateway), which is connected to all IVNs, either directly or through domain gateway(s) including all necessary security

measures to provide a single access point for all data and control functionalities the vehicle systems provide.

The software consists of two major tasks:

(1) The IVN software (task (1)) consists of an IVN Manager and PDU Handler. It connects to IVN protocols to handle IVN data access, reads ignition on/off status, processes available inputs/outputs, and performs periodic updates on sensor data e.g. IMU (inertial measurement unit), GPS (global positioning sensor). Such data is very useful to reproduce vehicle system fault occurrences based on location and driving behaviour at the time of misbehaviour. The PDU Handler extracts the protocol data unit from any data source. The IVN Manager uses the information contained in the IVN configuration to mask data bytes from the PDU, convert to the VIDF runtime format and attaching a time stamp. Each data parameter with ECU identifier, data type identifier, data type specific parameter value, and time stamp since 1970 is posted to the data pool according to the schedule table or by event occurrence.

(2) The SVI software (task (2)) consists of the UGP Server, DXM Handler, Job Handler, and Data Provider. The Data Provider maintains the VIDF formatted data parameters of the data pool. The UGP Server handles all UGP client(s) request messages, which are inspected by the firewall. A deep packet inspection (DPI) is a form of computer network packet filtering, that examines the data part of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions, etc. If no matching information is found in the configurations, the UGP response message will include an error code for this data parameter. UGP clients, which e.g. request data parameters via the GetValueCall, will be served by the UGP server with the requested information, if available in the Data Provider data pool.

Both tasks run independently. Even if the UGP server task would be in an idle state, the IVN data access task would continue according to the schedule table in the IVN configuration.

Figure 16 shows the SVI software solution block diagram and data flow.

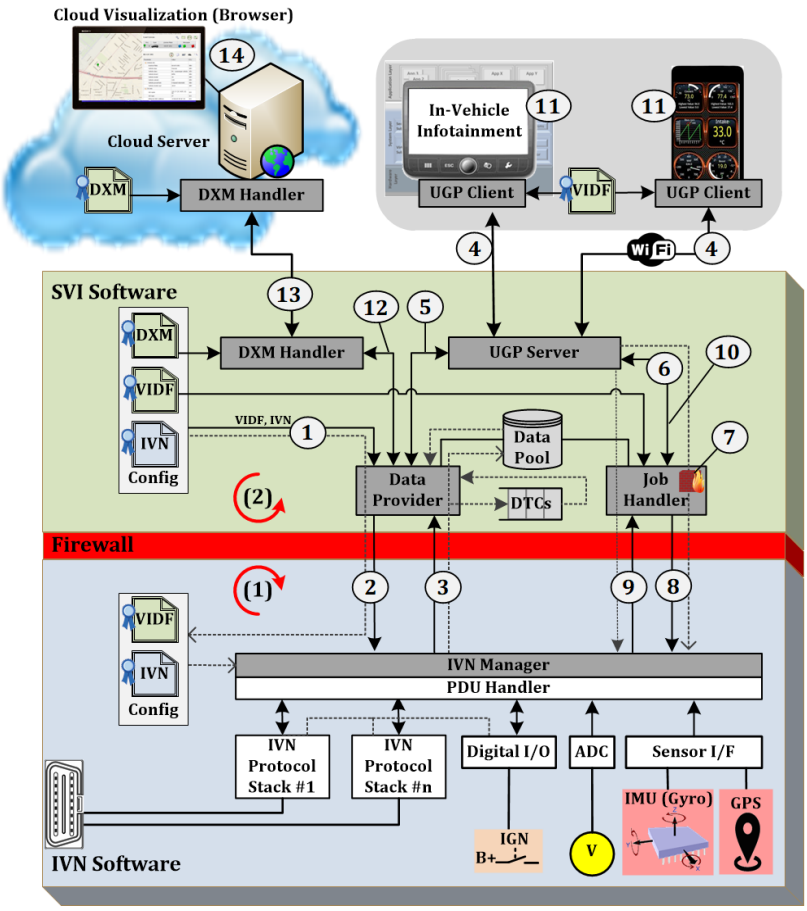


Figure 16 SVI Software Solution Block Diagram

Key	Data flow description
1	Read configurations
2	Send VIDF and IVN configurations
3	Send sensor data in VIDF format
4	Send UGP service request
5	Collect UGP service relevant sensor data (normal mode) and send UGP response
6	Call Job Handler (diagnostic mode)
7	Firewall checks authorization of UGP request message, checks support of data parameter in configuration
8	Send corresponding IVN raw protocol message based on IVN configuration and execute it
9	Send IVN raw protocol response message in VIDF
10	Receive job response and send UGP service response
11	Get UGP response and visualize data
12	Collect configured DXM sensor data
13	Send DXM message containing DXM configured sensor data
14	Receive DXM and Visualize sensor data

All VIDF formatted data parameters and associated runtime information is stored in the circular buffer (data pool) of the Data Provider. This includes the normal communication data as well as diagnostic protocol data, which require a request and response message scheme performed by the Job Handler. The Job Handler processes all UGP call messages (requests) with the exception of those UGP calls, which do not have associated VIDF and IVN configuration information. The firewall function inside the Job Handler checks all UGP client call messages.

Any UGP client call, which does not have an associated configuration, will not pass the firewall and therefore never appear as a transformed request message on the IVN.

For a complete description of the standard data formats, translations and methods refer to ISO **21184 ITS Management of messages containing information of sensor and control networks specified in data dictionaries**.

8 SVI Secure Communication Profiles

In order to enable interoperability between ITS stations from different manufacturers, and portability of ITS applications (that provide the ITS services), ITS Station Communication Profiles (ITS-SCP) used in Secure Sessions between Trusted Devices (SSTD) are standardized. Such ITS-SCPs are essential for many ITS applications and services including time-critical safety applications, automated driving, remote management of ITS-SUs (ISO 24102-2), and roadside / infrastructure related services.

IVN communication profiles typically deployed in in-vehicle networks are illustrated in figure 17. SVI can incorporate these profiles as required by evolving use-cases . An initial and non-exhaustive set of ITS-SCPs are defined in **ISO 21185 Communication profiles for secure connections between trusted devices** that provides data and message reguirements related to SCNs.

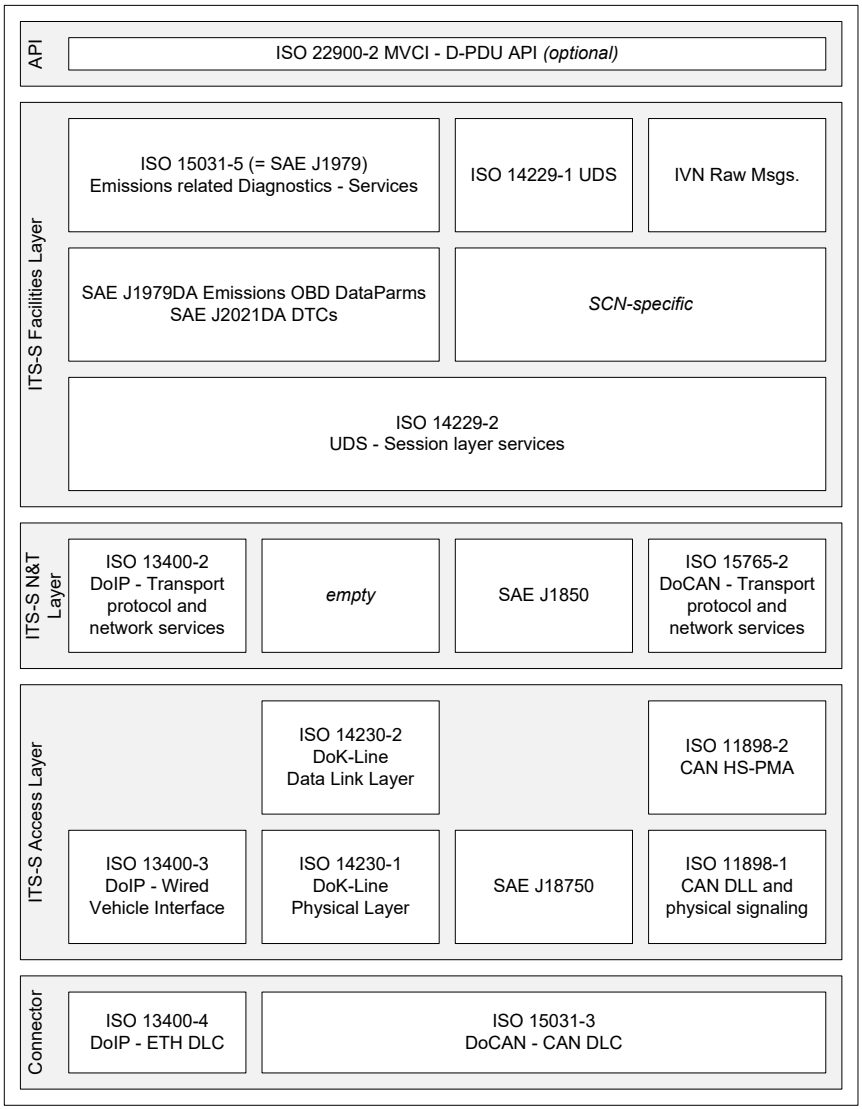


Figure 17 IVN protocol stacks used for in-vehicle networks

As we have already explained there are four classes of communication nodes in ITS communications networks that are identified in the ITS station and communication architecture ISO 21217. These nodes are defined as;

- Personal
- Vehicular
- Roadside
- central

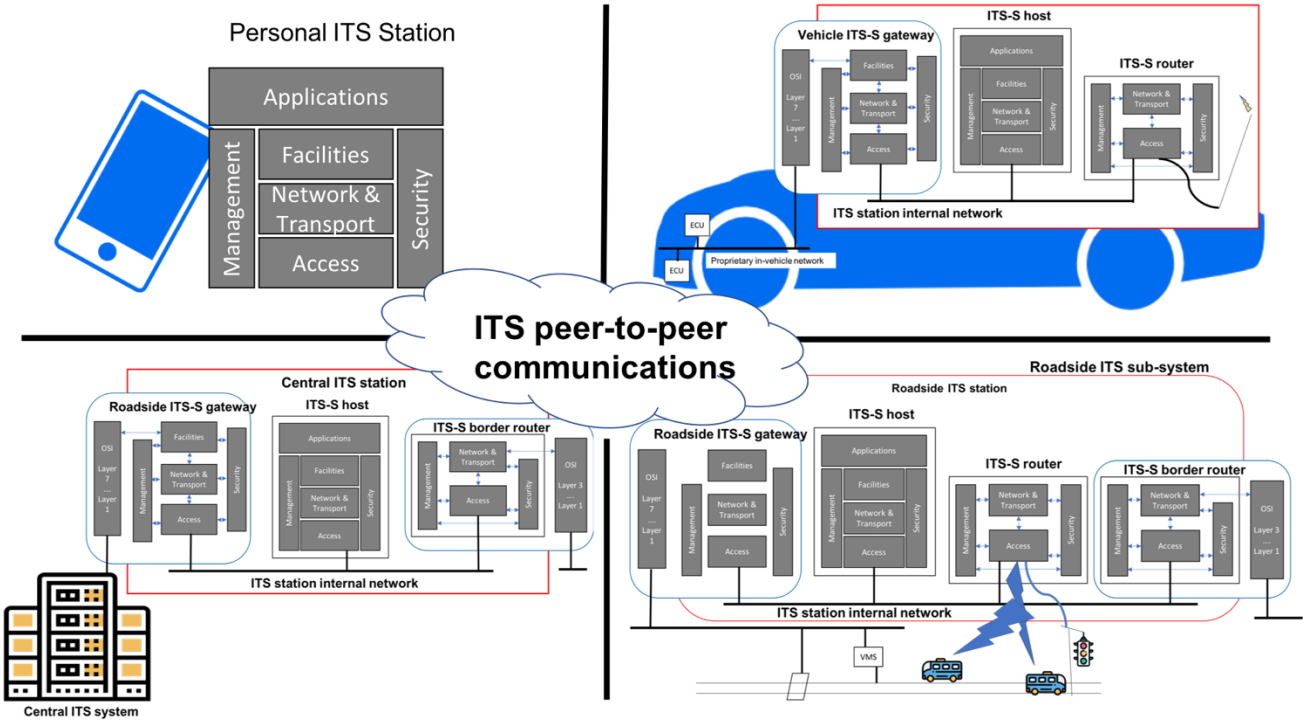


Figure 18 ITS Communication Nodes

As can be seen by the above diagram, varying communications protocols will be deployed and must be interoperable in a secure and efficient way to meet the strenuous time-critical and security requirements. Therefore ITS-SCPs must be standardized as specified in the evolving ISO 21185 standard. The following text provides some examples of this standardization and the methods for standardizing ITS-SCPs.

ITS communication protocol stacks and related ITS-SCPs are referenced by an Object Identifier (OID) value of the following structure

— { iso (1) standard (0) 21185 (21185) its-scps (2) its-scp-'*n*' ('*n*') }

with '*n*' being an Integer number unique in this document. ITS-SCPs specified in other documents require assignment of a unique identifier 'n' by means of registration in this document.

This OID value of an ITS communication protocol stack can be used in the CSP Protocol for the purpose specified in ISO 17423:2018.

The OID can identify:

- Communication protocols
- Communication protocol stacks
- Communication profiles

A suggested methodology for identifying ITS-SCP follows:

1. Identify protocols by means of an ITS protocol identifier.
2. Create an ITS-SCPS by combining the identified protocols (that creates an entry in a look-up table).

3. Create an ITS-SCP by adding parameterization to an ITS-SCPS (that creates an entry in a look-up table).

4. Map ITS-SCPs to specific use-cases, e.g.

    a. trust between ITS-SCUs;

    b. trust between ITS-SUs;

    c. trust towards SCNs.

An example of an ITS communication profile is described in table 1, which specifies the Ethernet for SCN-access profile.

Table 1 Profile "Ethernet for SCN-access"

The OID { iso(1) standard(0) 21185 (21185) its-scps (2) its-scp-1(1) } shall be used to identify the ITS-SCP

CSP_SpecificCommsProts		**Parameterization**	**Comments**
`ITSprotID.locationID`	**`ITSprotID.protocolID`**		
1: acLayer	{ iso (1) identified-organization (3) ieee (111) standards-association-numbered-series-standards (2) 802 (802) dot3 (3) document (0) its-prot-id (0) edition2015 (1) }	n.a.	Ethernet access technology
2: ntLayer	{ iso (1) standard (0) its-ipv6 (21210) document (0) its-prot-id (0) edition1(1) }		IPv6 communications
4: fcLayer	{ iso (1) standard (0) 21184 (21184) document (0) its-prot-id (0) edition1 (1) }	tbd once ISO 21148 will be available	Data and messages for sensor and control networks
8: mgEntity	None		No requirement on support by the ITS-S management entity
16: scEntity	{ iso (1) standard (0) 21177 (21177) document (0) its-prot-id (0) edition1 (1) }	n.a.	Manages secure session with a SCN

Table 2 Profile LTE access to Internet

The OID { iso(1) standard(0) 21185 (21185) its-scps (2) its-scp-2(2) } shall be used to identify the ITS-SCP specified in Table .

CSP_SpecificCommsProts		Parameterization	Comments
ITSprotID.locationID	**ITSprotID.protocolID**		
1: acLayer	{ iso (1) standard (0) lte (17515) part1 (1) document (0) its-prot-id (0) edition1 (1) }		General access to the Internet
2: ntLayer	{ iso (1) standard (0) its-ipv6 (21210) document (0) its-prot-id (0) edition1(1) }		IPv6 communications
4: fcLayer	None		No requirement on ITS-S facility layer protocols
8: mgEntity	None		No requirement on support by the ITS-S management entity
16: scEntity	{ iso (1) standard (0) 21177 (21177) document (0) its-prot-id (0) edition1 (1) }	n.a.	Manages secure sessions between ITS-S application processes in different ITS-SUs.

Even small differences in communications, e.g. usage of EPD instead of LPD (addressing methods at OSI Layer 2) disables data exchange, although the same radio technology, e.g. ITS-M5 (ISO 21215) is used by both trusted devices at the same channel, e.g. Safety Channel at 5,9 GHz. Extended negotiation of a common protocol for time-critical communications is not conducive to vehicle and traffic infrastructure safety applications and therefor needs to be standardized and advertised prior to a communication session. For detailed specifications and a list of current communication profiles, refer to **ISO 21185 Communication profiles for secure connections between trusted devices,** which is the first ITS standard aimed to standardised ITS-SCPs

9 SVI Service examples

1. Example of Multiple Services Connected to an SVI

In figure 19, we have expanded on the previous example by adding two more applications. The violet application is now made as an example Diagnostic Tool application. This would typically reside in the facilities layer, since there is usually no direct user interaction in the vehicle Human Machine Interface (HMI). Indeed, this application would normally put the relevant ECUs in a specific service mode. The yellow application in this example signifies an insurance company that has been granted access to certain driving parameters, but also strongly restricted to access other (driving behavior) parameters. The third green example depicts a fleet management application where for instance a taxi fleet operator gets access to the vehicle position and fuel level, and in this case, there is a full user interface where the fleet operator can communicate directly via the vehicle HMI. Access credentials for each of these services is stored in the in-vehicle ITS station as indicated by the color coded boxes in the security plane.

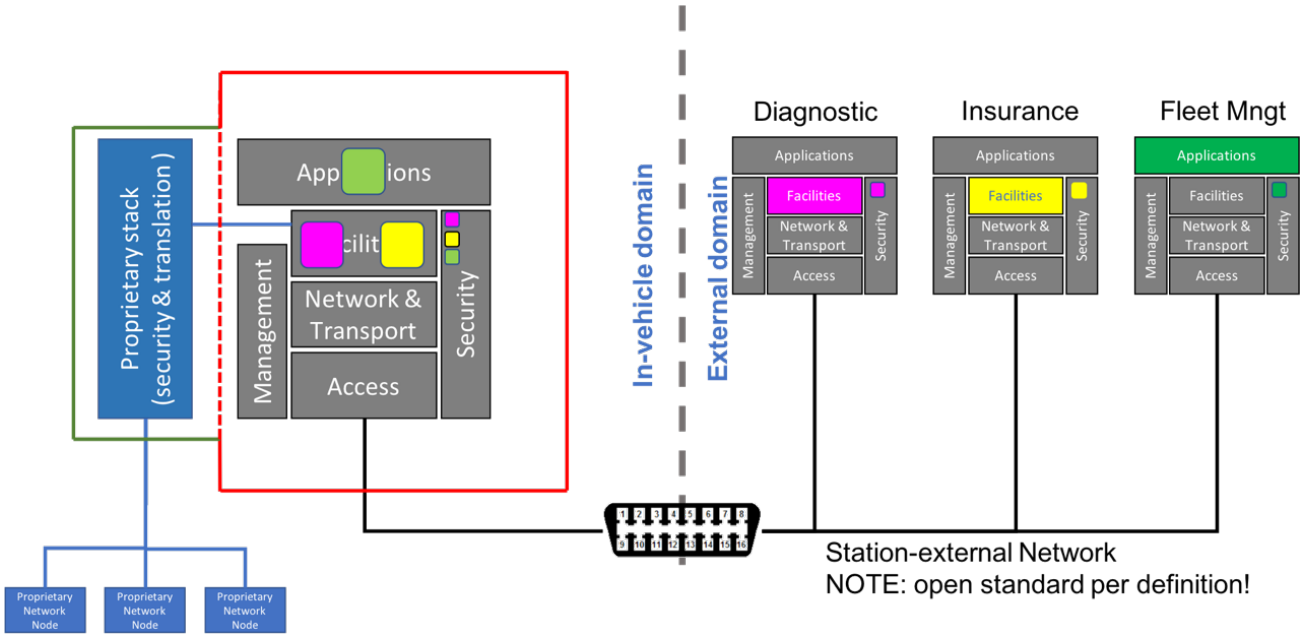


Figure 19 Multiple Applications

2. Example of Multi-application Supported External ITS Station

In the following example there are multiple applications supported in the in-vehicle station and exposed as a resource over the SVI. If the same applications are present in the external ITS station, and the security credentials allow, then secure communications may take place over the interface. Depending on capacity, several application sessions may take place simultaneously. Each session would have its own protection for confidentiality and integrity.

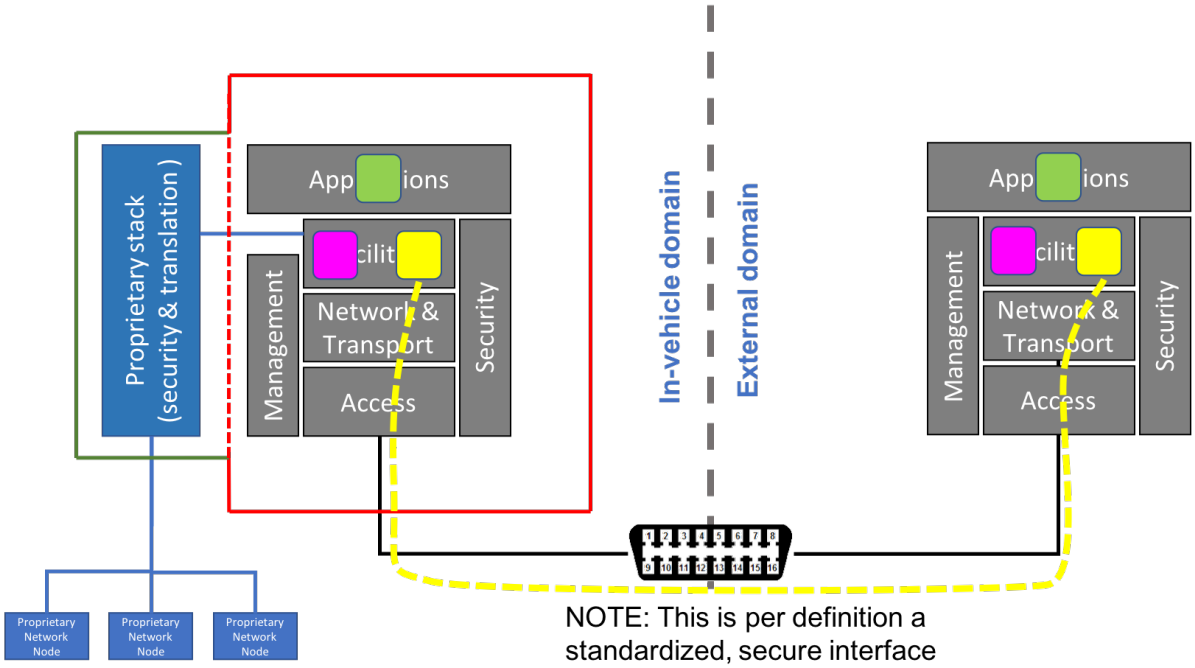


Figure 20 Multiple Internal Application Resources

3. Short Term Effect on the Aftermarket

   Most vehicles have a standardized OBD-II connector for diagnostics. However, there are challenges with this mandated interface:

   - The open OBD-II data set is limited to emissions diagnostics. Other data sets may be accessible, but is proprietary and both, types of data and access methods vary extensively.
   - Interfaces for diagnostics are limited to slow protocols. ITS will require high speed, low latency connectivity, and the current CAN bus is limited in these regards.
   - Security for other data sets is either proprietary or absent.
   - Connecting to unprotected data networks in a vehicle is high risk, so a strong firewall is an absolute requirement.
   - Data access is sometimes not possible while driving. The CAN buses in current generation vehicles are heavily loaded and adding data access may interfere with critical vehicle functions while in use.

   Figure 21 shows that an ITS station can be connected to the current OBD-II connector, and all required translators and security functions can be implemented in this external domain. Due to the proprietary nature of the non-emissions diagnostic data, the blue stack in the external domain will have to be implemented on a case-by-case basis. But this process is simplified by the table-driven translation mechanisms described in the SVI Standard data format section detailed later in this document. In the end, the facilities layer in the external ITS station will have available to it a certain set of data and access to whatever services are allowed on the in-vehicle domain.

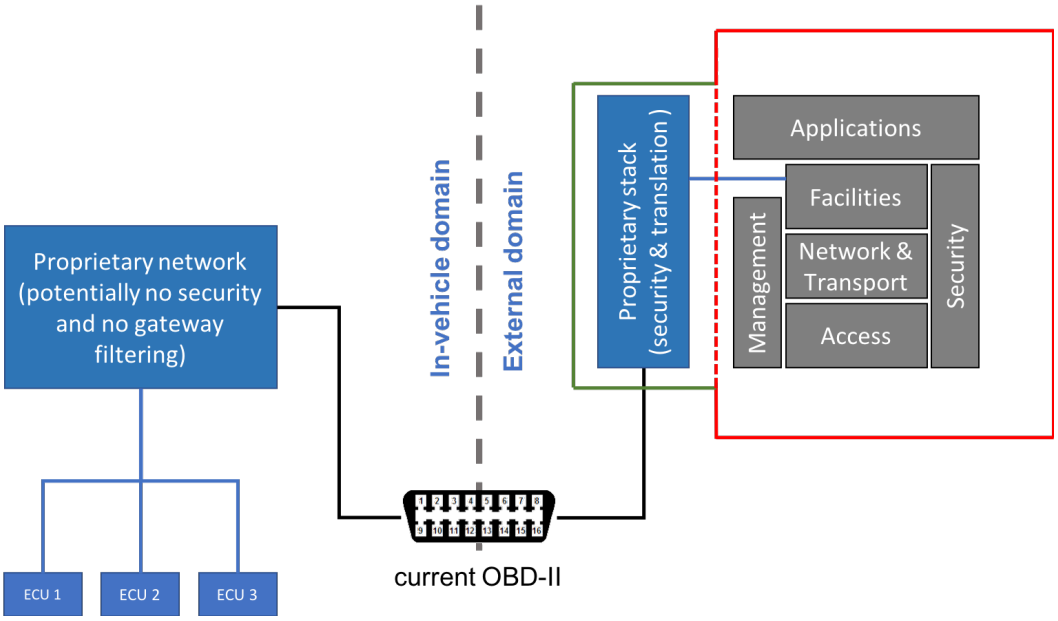


Figure 21 OBD II Connector

4. External ITS Station Running Multiple Applications

Figure 22 is similar to the embedded station example above, with one major difference. The access credentials in the security section may "open" the right to read proprietary data and translate these into standard format. This would allow VMs to protect unauthorized access to critical resources. The ITS applications (green, yellow, violet) will perform their task as usual.

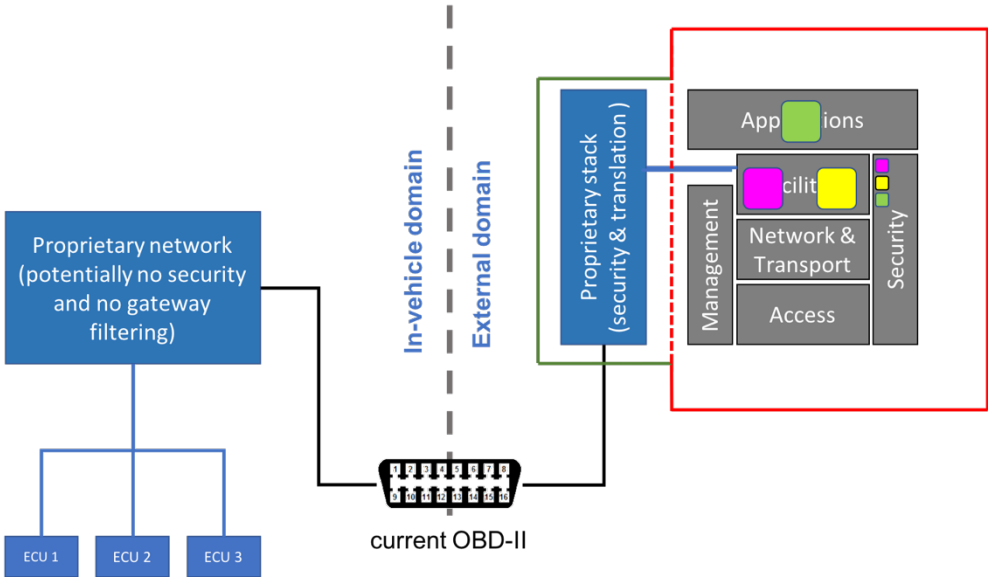


Figure 22

5. Retrofitting SVI to Existing Vehicles

In figure 23, the external ITS station has three roles:

- Controlling access and translating data over the OBD-II connector
- Operating the local applications
- Giving access to external ITS stations via an SVI port

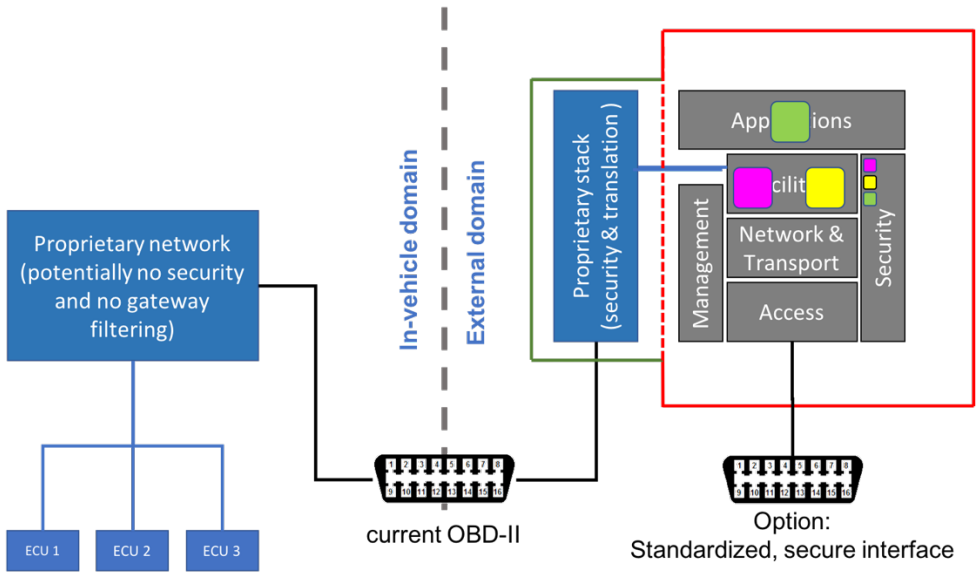


Figure 23 SVI with External SVI Port

6. Full aftermarket example

The functionality in figure 24 is similar to the "Multiple services connected to an SVI" example above. The main difference is the extra ITS station that is used as a gateway to the proprietary network. The challenge is that data access may be very limited over the OBD-II port, especially in older vehicles, so that external stations trying to access information over the SVI may not be fully capable of complying with data requests. Therefore, this solution will offer a transition mechanism so that new services can be implemented without waiting for a critical mass of newly equipped SVI vehicles to enter the market.

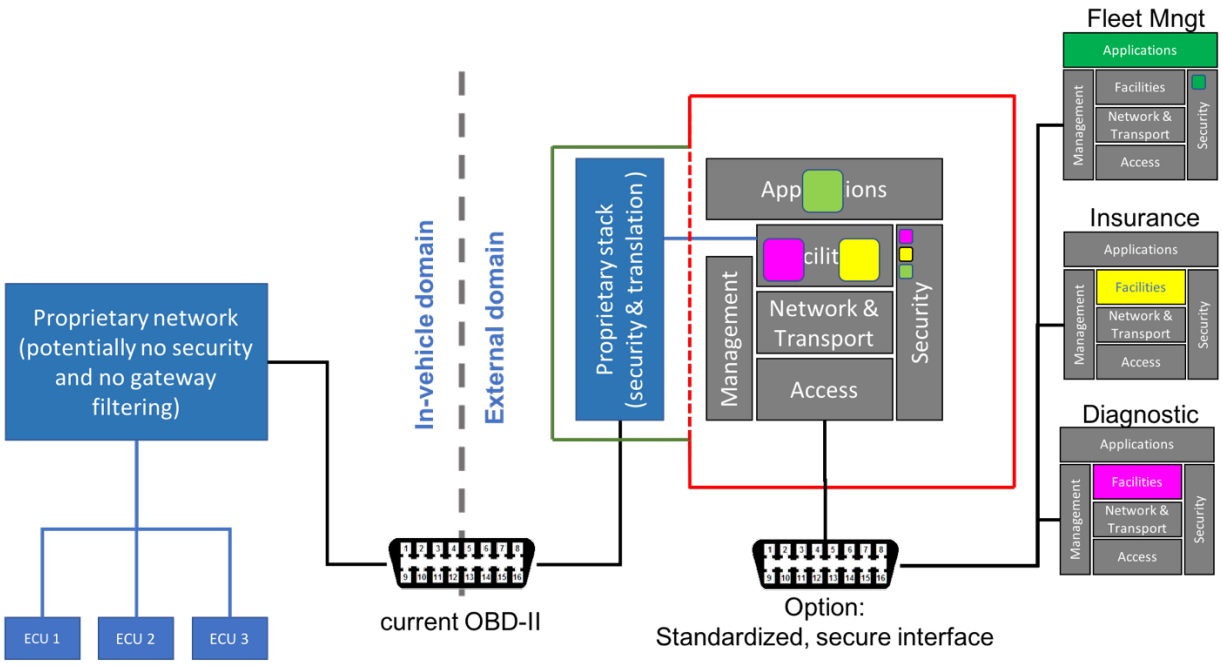


Figure 24 Full Aftermarket Retrofit

10 Conclusion

As vehicles (future and existing) are required to become more connected to each other and to the transportation infrastructure protection of the vehicle communications network becomes ever increasingly vital, for safety and privacy reasons. The implementation of proprietary and non-standardized solutions drives up costs for consumers and municipalities, and reduces the interoperability required for an efficient and dependable, fully integrated transportation system. The SVI implements evolving and existing international standards that provide the necessary security to protect the vehicle network, while providing for open access to the vehicle owner and authorized service providers.