Secure Vehicle Interface

Auto Care Association

March 5, 2018

ABSTRACT

Vehicular cyber security is the set of measures taken to protect in-vehicle communication and control networks against unauthorized access or attack. It is a global issue of continually increasing importance as the complexity of such networks and the autonomy of vehicles expands. This increasing complexity and autonomy make it necessary to connect in-vehicle networks (IVNs) to external networks for purposes such as remote monitoring and diagnostics, accessing maintenance and repair data, predictive services, location-relevant services, and utilizing real-time safety and operational data using telematics systems. This network access has the potential to expose new attack surfaces, making an otherwise secure and isolated in-vehicle network vulnerable to intrusion and to all other threats common to any publicly connected network. Yet the preservation and expansion of aftermarket telematics, diagnostic products, and services, and the vehicle owners' right to choose independent service providers, requires standardized interfaces for accessing IVNs. These interfaces must be standardized and secure to protect IVNs from attack by potential external threats. This paper describes techniques for implementing secure interfaces between in-vehicle networks and external networks that provide safe, secure, and equitable in-vehicle network access.

INTRODUCTION

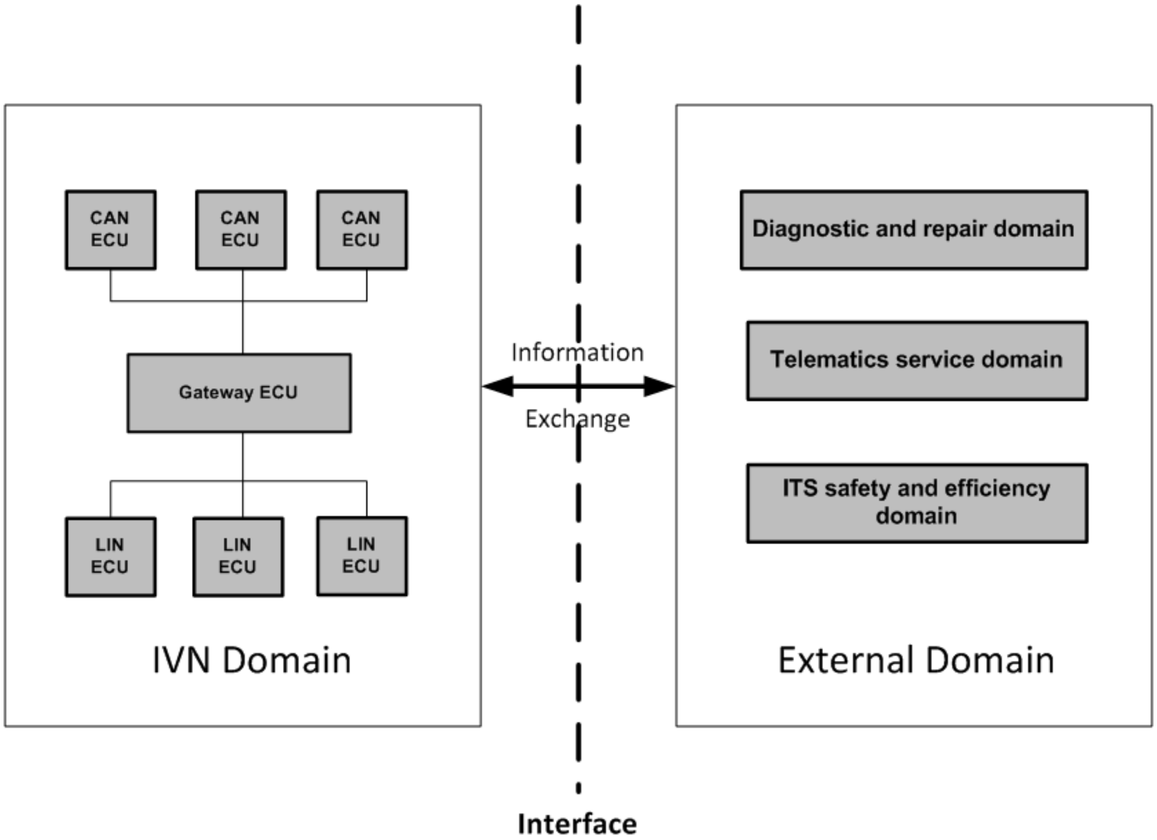
Over the last four decades, ground vehicles of all types have been evolving from simple mechanical machines to intelligent agents that are becoming increasingly connected to the outside world. Communication, control, and infotainment networks have become the third heaviest component of today's light-duty vehicles due to the miles of wiring required to connect each Electronic Control Unit (ECU), which are the "brains behind the operation". Modern vehicles have become so complex that auto technicians are studying computer networking to perform simple repair and diagnostic services. Scanning devices connecting to and communicating with these complex networks through existing standardized and open interfaces, such as the On-board diagnostics II port (OBD-II), have become essential tools in diagnosing problems and affecting repairs. Telematics device manufacturers and service providers also use these same connection points.

Today, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, more generally vehicle-to-anything (V2X) communications, are being deployed to improve the safety, efficiency, and comfort of vehicular operations. Wireless devices of various types, referred to as Onboard Units (OBUs), are required to support these communications. Such devices require real-time access to the IVNs to gather safety-critical information in a timely manner that can be sent to neighboring vehicles as well as to other entities such as traffic management and safety systems as well as repair facilities of the customer’s choosing.

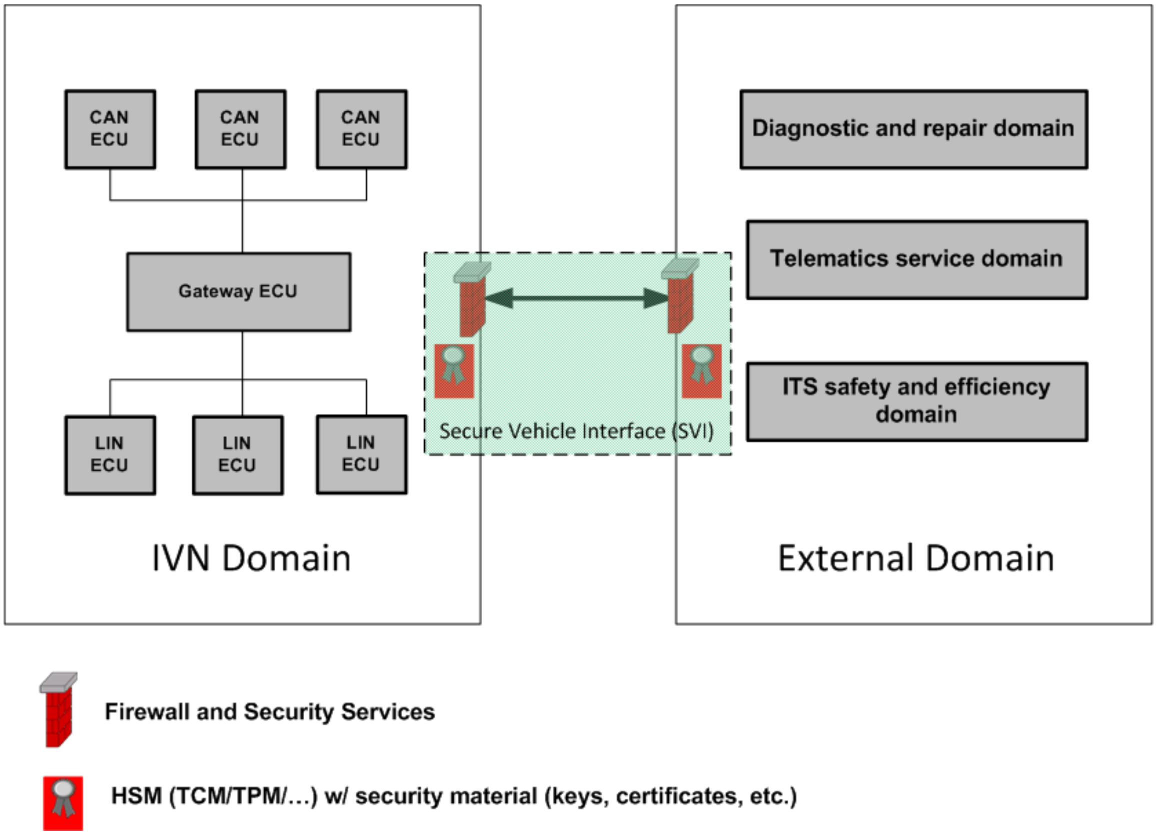
Regardless of whether the method used to connect a vehicle with the outside world is wired or wireless, the communication interface must be safe and secure and must not introduce additional attack surfaces into the IVNs or connected external devices. This paper provides a high-level overview of the techniques used to implement a secure interface. Some elements of the techniques presented are currently the subject of international standardization within several international standards development organizations (SDOs), including SAE, IEEE, ETSI, ISO, and CEN. These standards form the basis for implementation of the “Secure Vehicle Interface” (SVI).

What is an SVI?

An SVI is an implementation of an interface between an IVN, such as a communication, control, or infotainment network inside the vehicle, and an external device or network enabling secure information exchanges between the two. Theoretically, this “interface” is a shared boundary between two or more separate components of a system exchanging information.



Specifically, the interface is between two “gateways,” one in the IVN and the other in the external network, such as a diagnostic tool (DT) or telematics device (TD) connected to an IVN using an OBD-II connector and a CANbus interface. In this example, the communication interface used in the TD or DT, along with the software that controls that interface, forms the DT/TD gateway. Similar hardware and software in one or more ECUs in the IVN form the IVN gateway. Those two gateways augmented with security-related functionality, which includes Hardware Security Modules (HSMs) and supporting software, are the essential elements of the SVI illustrated below.


CAN ECU
CAN ECU
CAN ECU
Gateway ECU
LIN ECU
LIN ECU
LIN ECU
IVN Domain
Secure Vehicle Interface (SVI)
Diagnostic and repair domain
Telematics service domain
ITS safety and efficiency domain
External Domain
Firewall and Security Services
HSM (TCM/TPM/…) w/ security material (keys, certificates, etc.)

Enabling successful communication between entities across the interface requires that both gateways use the same hardware and software interface specifications. This is accomplished in SVI by developing the specifications into international standards.

Industry standards have proven to make it easier and cheaper for companies to gain access to new technologies by creating a common interface across all variations of a technology. Standards limit the need for negotiating multiple licensing agreements in order to access intellectual property for a single technology. Examples of where standards have been used to level the playing field are: telecommunications (voice, data, wireless, SMS), entertainment industry (DVD, Blu-ray, …), GPS, petroleum and solar panels, are just a few examples. Without these standards, manufacturers are likely to generate one-off variations of technologies, thereby limiting the ability for third-party developers to compete or offer aftermarket modifications by reducing the potential customer base to only one manufacturer's customers rather than all manufacturer's customers.

It is important to note that the requirement for a standardized interface has no impact on the design and implementation of the IVN or the external device or network except that these gateways must "speak the same language" and that their applications must share a "common dictionary."

An SVI is comprised of two gateways along with:

- the communication medium used to connect them,
- the hardware and software required to implement the necessary security functionality and
- means for uniquely and unambiguously interpreting the data/information exchanged through the gateways

The communication medium employed in an SVI can be wired or wireless, but to ensure equitable access, the specifications for the medium must be widely available. When the components of an SVI are built-in and tested for conformance to the same open specifications, telematics device suppliers, diagnostic tool suppliers, and OBU suppliers of V2X communication devices can be assured of the necessary level of interoperability

Security is a critical aspect of SVI, although security-related hardware and software requirements will vary depending on the level of security that's required. Security-related requirements depend on the:

- access and functionality of the networks/components/devices involved
- the importance of the information being exchanged
- the cost of implementation versus the security risk involved

Given the importance of security, the subject is discussed in depth in a later section of this paper.

As important as gateways secured by standardized security-related functionality are, they are of little use if the information they exchange is incorrectly or ambiguously interpreted. At present,, the details behind IVN designs and implementations are VM-specific, yet the ability to obtain information from IVNs in a standardized manner is crucial to maintain modern vehicles properly. The best means of assuring accurate information exchange and unambiguous interpretation of this information is, again, adherence to common specifications or standards for data object definitions and data exchange protocols. The good news is that such standards and specifications are available.

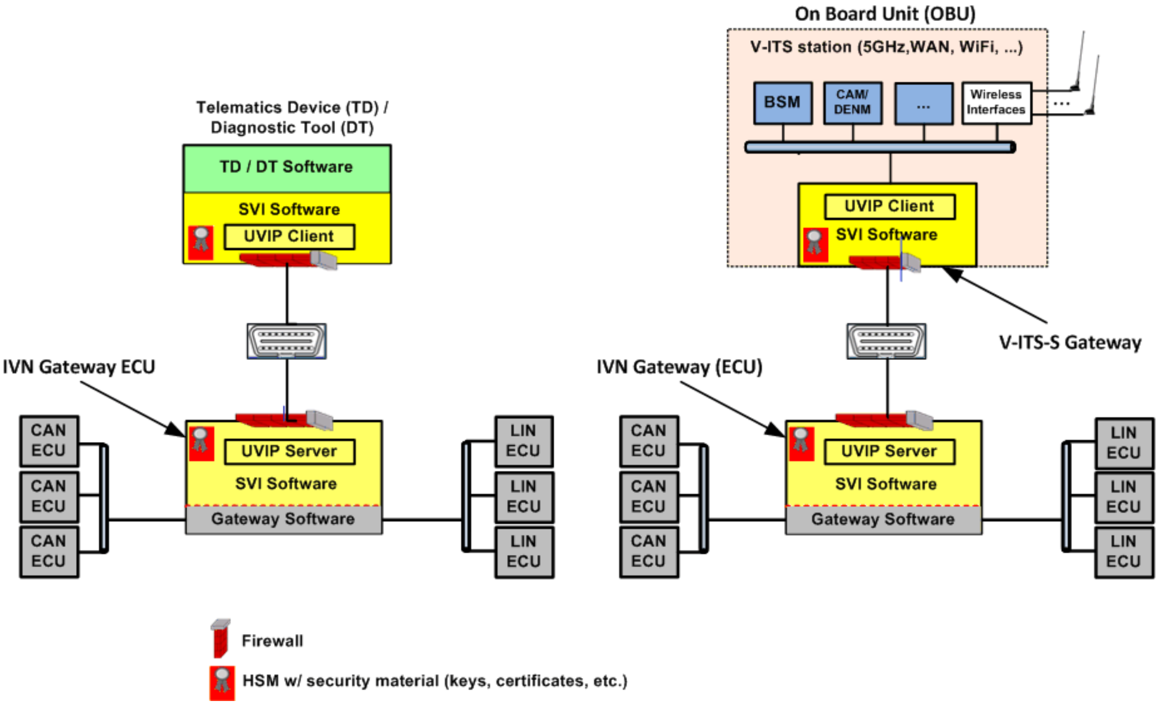
The development of a common specification for IVN information exchange is possible and practical because, at an abstract level, IVN control and sensor information is largely the same. A steering wheel angle sensor collects information on the steering wheel angle, which is fundamentally the same thing in all vehicles with a steering wheel. However, the actual definition and encoding of this information is most often vehicle make and model dependent. (As a technical example, data collected from one vehicle may be defined as a 12-bit two's-complement signed integer in degrees, and another a two-octet unsigned integer in hundredths of radians with a zero-offset of 32,768). Adherence to a common specification for data representation and a common protocol for data exchange across an SVI mitigates the need for external devices or networks (such as aftermarket telematics and diagnostic devices) to have multiple proprietary data specifications, as is the case today. An example of a set of such specifications is the set of ISO standards specifying the Unified Vehicle Interface Protocol (UVIP) (see illustration below), and this, or a similar set of specifications, is considered essential in any SVI implementation.

Who are the major stakeholders in SVI deployment?

In addition to vehicle manufacturers (VMs), the major stakeholders in SVI deployment include companies designing, manufacturing and/or marketing:

- IVN-connected telematics devices and diagnostic and repair tools,
- Intelligent Transport Systems (ITS) compliant vehicle and/or infrastructure components, and
- products or services that require the use of standardized, secure means for communicating with electronic control units (ECUs) in IVNs.

Vehicle manufacturers need to implement SVI standards-conformant IVN gateways in new IVN architectures to provide a single, secure, standards-based interface for the exchange of IVN information with other SVI standards-conformant device gateways in external devices/networks. This potentially includes the development of OBD-II retrofit modules that implement an SVI standardized IVN gateway for deployment in all existing vehicle makes and models currently on the road today or with onboard interoperable application platforms that are already (and increasingly) being implemented today by various VMs. Firewalls implemented in these IVN gateways will protect against the injection of malicious commands from unauthorized entities that might have access to the communication medium between the IVN and external device gateways. The figure below illustrates SVI implementations involving aftermarket telematics/diagnostic devices and ITS-compliant On-Board Units (OBUs).



Despite the fact that many vehicles on the road today have no means for implementing secure gateways because they lack the required security hardware (HSMs), SVI-conformant aftermarket devices can connect to IVNs through the (OBD-II) data link connector in most legacy vehicles and provide the necessary security. In many cases, it will also be possible to implement the UVIP for data exchange. However, the level of security that can be provided will be dependent on the IVN architecture and its inherent security functionality. Source authenticity and data integrity can't be guaranteed without hardware security deployed wherever attack surfaces are present throughout the IVN. Without secure hardware to store credentials, for example, a brake position sensor output can't be authenticated. This means the sensor outputs can't be "trusted" because data coming from that sensor could be forged. As a result, any decisions based on information from this sensor should take into account the fact that this information has a lower level of assurance and trustworthiness.

While vehicle owners are not stakeholders in the implementation of SVIs, they are the group most affected by the introduction of SVIs. Implementation of SVIs is essential in providing vehicle owners with an assurance of their ability to exercise their right-to-repair and a guarantee of the level of privacy and anonymity they expect.

What are the issues an SVI addresses?

Secure connection of external devices to IVNs using an SVI is becoming increasingly important for several reasons:

1. IVNs need to become accessible to the outside world by wireless and/or wired means to ensure equitable access by telematics system operators and repair facilities not directly affiliated with the vehicle manufacturer. Such access must be carefully controlled and secured to prevent access by actors with malicious intent and standardized so that the market for such products and services can develop independently.

2. Vehicles will need to share information from their IVN(s) with each other (V2V) and the transportation infrastructure (V2I) by wireless means to enable the deployment of safety and efficiency applications. The need for source authentication and data integrity assurance is obvious, and these functions are key components of the security functionality of an SVI.

3. Vehicle manufacturers wish to design their IVNs according to their own requirements, resulting in proprietary implementations. Much of the information that flows through these proprietary IVNs also needs to be shared with the outside world, and in some cases, such as V2V safety communications, this information needs to be exchanged continuously in real-time. This is most efficiently and securely accomplished by having a common data dictionary and set of specifications for information exchange between the IVNs and the outside world, as described above.

4. Software will soon control all critical driving functions. Because unauthorized modification or corruption of that software can lead to safety risks, all IVN software updates must be done in a secure manner by authenticated sources through a properly configured secure interface. Implementation of a standardized SVI interface reduces the cost and complexity associated with proprietary solutions.

5. Autonomous vehicles will operate more efficiently, safely, and effectively when they share information with each other and the transportation infrastructure using a wireless connection. Once again the need for source authentication and data integrity assurance is obvious and these functions are key components of the security functionality of an SVI.

All of the issues listed above, and many more, are directly or indirectly addressed by SVIs.

What makes an SVI secure?

It's necessary to have some understanding of the basics of security and the set of services that are possible in order to understand the implications of security on a SVI interface. Basic communications-related security services in a relative order of importance in a SVI implementation are:

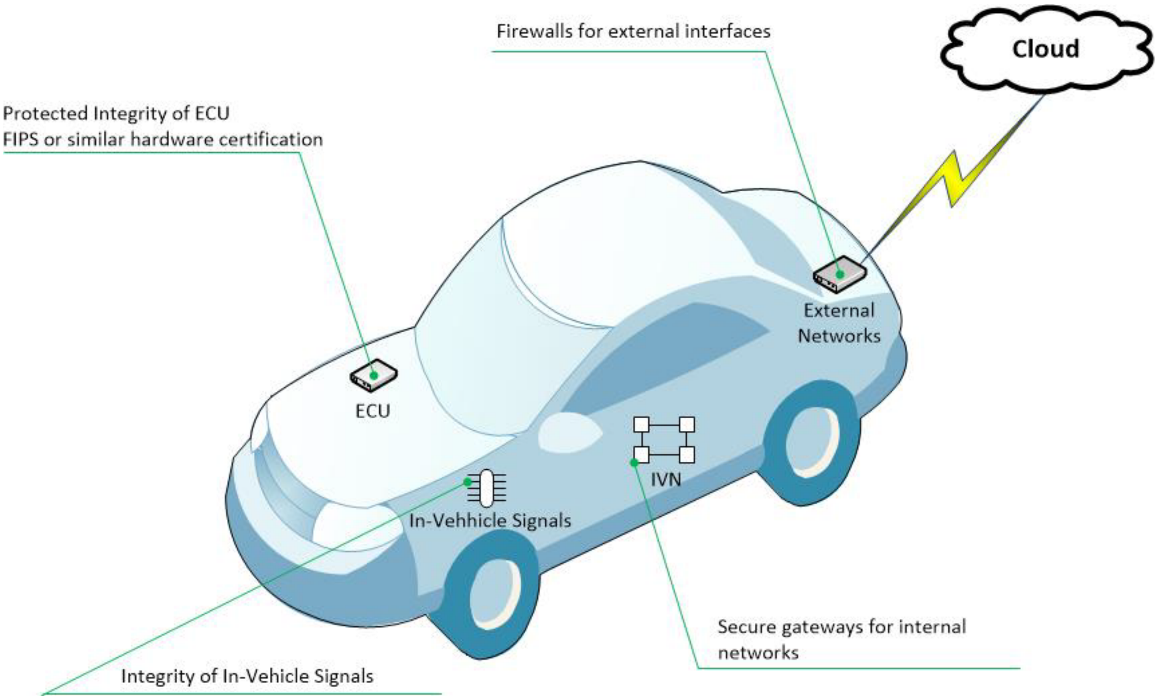
- (source) authenticity - did the data come from a trusted source?

- (data) integrity – was the data altered in transit?
- (data) availability - will the required information be available when it's 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?

Of these, availability, authenticity, integrity, and confidentiality are the most important for most application operations, while non-repudiation is most useful when investigating whether a device is misbehaving, i.e. injecting bad data into the system.

Cryptographic Security

Communications on an open network are generally secured using a secret as a cryptographic key. The secret is protected from distribution to parties outside the system by hardware and software mechanisms. Special hardware protects the key from being easily accessed by an attacker with physical access to the device(s) in which the key resides. Software prevents the key material from being exported from the special hardware and unauthorized processes from requesting use of the key material. The department of defense, finance and banking, telecommunications and most recently the Internet of Things (IOT) industries deploy hardware as well as software security mechanisms.


Firewalls for external interfaces
Cloud
Protected Integrity of ECU
FIPS or similar hardware certification
External
Networks
ECU
IVN
In-Vehhicle Signals
Secure gateways for internal networks
Integrity of In-Vehicle Signals

Recommended open standards for hardware protection of cryptographic keys include the Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS 140-2), "Security Requirements for Cryptographic Modules". This standard specifies multiple levels of security, allowing an implementer to choose the required level for their system based on a cost-benefit tradeoff. There are many suppliers of FIPS 140-2 hardware for each security level. FIPS 140-2 or a similar standard can provide a baseline of security for key storage and for cryptographic operations essential for an SVI implementation. It is important for implementers of IVNs and connected devices to remember that an SVI implementation only secures the connection between the two, and not the networks or platforms themselves. Generally, security functionality inside both the IVNs and the external devices is required at all levels to thwart attacks.

Once devices have cryptographic keys secured by hardware and software mechanisms, those keys are used to carry out critical cryptographic operations that provide integrity, authenticity, confidentiality, and non-repudiation. Keys can be either symmetric, in which case the secret must be known to all parties to a transaction, or asymmetric, in which case the secret is known only to one party, and the other parties are given a "public key" derived from that secret or private key.

Authenticity

In nearly all cases, the most important security service for an SVI is authenticity. For example, an IVN needs to trust that an application instance on an external device ("external application") connecting to an application instance in its IVN gateway ECU ("IVN application") is authorized to do so. In addition, the IVN gateway ECU needs to know which commands and data the external application is authorized to send and which data and commands the external application is authorized to receive, thus preventing malicious or unauthorized commands from passing through the IVN gateway ECU to the IVN, and preventing the release of IVN data to unauthorized external applications. The same is true of the external application. It requires assurance the IVN application is authorized and can be trusted to perform according to SVI specifications.

The challenge for an SVI is that the external device, along with all its applications, and the IVN gateway ECU, along with all its applications, are more than likely "strangers" without an established trust relationship. The solution is a Public Key Infrastructure (PKI) and third-party trust. While the details are beyond the scope of this paper, they can be summarized as follows. If there is an entity trusted by both parties, commonly known as a "certificate authority" (CA), and each party can prove they are trusted by that CA, then both parties can trust each other because they're part of the same "trust domain." Proof takes the form of a common certificate and a private-public key pair unique to each entity safely stored in secure hardware by each party. The creation and distribution of certificates from a trusted authority or authorities requires infrastructure that is commonly referred to as a Security Credential Management System (SCMS) or Public Key Infrastructure (PKI), and such a system is required for the successful implementation and secure operation of SVIs. SCMSs for ITS are currently under development and, once deployed, will meet the needs of those implementing SVIs in devices offering telematics and diagnostic services as well as V2X safety services.

The system will require that for an application instance to be issued a certificate, there must be some assurance that it is an instance of a validated application installed on a trusted (validated) device. For a device to be issued a certificate and consequently be trusted, it must conform to an accepted set of hardware security standards, including the presence of a suitable HSM. The certificates issued to application instances installed on trusted devices indicate behaviors in which the application instances have been authorized to engage. Both application instance and device validation are essential to the implementation of the SVI, and they both involve some level of certification and testing to ensure an appropriate level of trust.

Integrity

The next most important security service is integrity. While the technical details for ensuring data integrity are also beyond the scope of this paper, integrity is often combined with authenticity by using the sender's secret or private key to calculate a cryptographic checksum that can be used by the receiver to ensure data wasn't modified in transit. This approach can be implemented symmetrically, using the secret key known to the sender and receiver, or asymmetrically, using the public key corresponding to the sender's private key. In the asymmetric case, public key cryptographic procedures can be computationally complex, requiring special-purpose hardware in certain situations, e.g., when a large number of checks is required in a short period of time.

Confidentiality

Confidentiality is provided by encryption, which can be implemented using symmetric or asymmetric mechanisms. If communications between parties are encrypted with appropriately secure algorithms, other parties are unable to access or successfully alter the information being exchanged. To avoid incurring the computational cost of asymmetric cryptography, it is common practice for two communicating parties to securely exchange a shared symmetric key, which is subsequently used for encryption and decryption of information. When confidentiality over an SVI is required, the specification of a symmetric encryption-decryption algorithm and a protocol for symmetric key exchange are recommended. Many publicly available specifications support this approach.

Availability

While not directly involved in securing an interface, availability is a very important system service when deploying applications and services with stringent data availability requirements. Such requirements directly affect the choice of communication media used in implementing an SVI. As an example, when implementing an SVI supporting IVN ECU software updates, a highly reliable wired interface is preferred over a wireless interface that can be subject to periodic disruption from a variety of sources. When implementing an SVI connected to an OBU engaged in V2X safety services requiring large amounts of real-time information with minimal latency, a directly wired onboard communication medium is essential, as wireless media are unable to meet system availability requirements.

What if I want to know more?

A more detailed technical description of the functionality required to implement an SVI is available in the SVI Technical Paper. That paper contains a list of the many ISO and IEEE standards currently in publication specifying various aspects of the SVI, with more underway. Work on the SCMS in the US is currently being sponsored in part by the US DoT, and publicly available specifications are expected soon. Similar efforts are underway in Europe as well. The core work on the SVI is being conducted in ISO TC 204 WG18, and progress on the SVI-related standardization effort can be monitored on the ISO website.