The Secure Vehicle Interface (SVI) is a ready-to-deploy, CEN/ISO Standards-based technology.
SVI enables safe, cybersecure communication between the vehicle and service partners who have been chosen to obtain the data by the vehicle Owner/Users. SVI uses a standardised secure interface to connect recognised and authorised external systems to the network within a vehicle.
SVI then converts the vehicle manufacturer's proprietary vehicle data into a common language, which enables broad interoperability for competitive services irrespective of the manufacturer or brand of the vehicle. The next few years will be critical in shaping the future of mobility.

Source [https://www.svi-for-mobility.org/]

The Secure Vehicle Interface (SVI) is a ready-to-deploy technology, based on three CEN/ISO standards: **TS 21177, TS 21185 and TS 21184.** SVI enables safe, cybersecure communication between the vehicle and service partners who have been chosen to obtain the data by the vehicle Owner/Users. SVI uses a standardised secure interface to connect recognised and authorised external systems to the network within a vehicle. SVI then converts the vehicle manufacturer's proprietary vehicle data into a common language, which enables broad interoperability for competitive services irrespective of the manufacturer or brand of the vehicle.

[Source : overview of CEN/ISO standard used by SVI]

CEN/TS 21177: Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices

- This document contains specifications for a set of ITS station security services required to ensure the authenticity of the source and integrity of information exchanged between trusted entities:
- devices operated as bounded secured managed entities, i.e. "ITS Station Communication Units" (ITS-SCU) and "ITS station units" (ITS-SU) specified in ISO 21217
- between ITS-SUs (composed of one or several ITS-SCUs) and external trusted entities such as sensor and control networks
- These services include authentication and secure session establishment which are required to exchange information in a trusted and secure manner.
- These services are essential for many ITS applications and services including time-critical safety applications, automated driving, remote management of ITS stations (ISO 24102-2), and roadside / infrastructure related services.
- This document is complemented by guidelines (contained in CEN/TR 21186-3) on how security for C-ITS can work in general for all communication types (broadcast information dissemination and unicast sessions), considering especially what is needed in the infrastructure in addition to the technical features implemented in ITS station units.

CEN/TS 21184: Cooperative intelligent transport systems, Global transport and data management (GTDM) framework

- This document specifies a "Global Transport Data Management" (GTDM) framework composed of a global transport basic data model, a global transport function monitor data model, a global transport access control data model
- to support data exchange between ITS-S application processes and correct interpretation of these data.
- This document defines standardized data classes in a "Global Transport Data Format" (GTDF) and means for managing them.
- Data exchange between ITS stations is specified based on messages composed of a global unique identifier and the associated data part. The format of the data part is specified by a globally unique identifier pointing to a configuration including instructions for correct interpretation of the data part.
- Application and role-based access control to GTDF resources are specified in conformance with IEEE 1609.2 certificates.
- The set of ITS-S facility layer services is described as an ITS-S capability conformant with ISO 24102-6, which is an optional feature.

CEN/TS 21185: Cooperative intelligent transport systems - Communication profiles

- This document specifies a methodology to define ITS-S communication profiles (ITS-SCPs) based on standardized communication protocols to interconnect trusted devices. These profiles enable information exchange between such trusted devices, including secure low-latency information exchange, in different configurations. This document also normatively specifies some ITS-SCPs based on the methodology, yet without the intent of covering all possible cases, in order to exemplify the methodology.
- Configurations of trusted devices for which this document defines ITS-SCP's include the following units according to ISO 21217:
- ITS station communication units (ITS-SCU) of the same ITS station unit (ITS-SU), i.e. station-internal communications specified e.g. in ISO 24102-4
- an ITS-SU and an external entity such as a sensor and control network, or a service in the Internet
- ITS-SUs
- The specifications given in this document can be applied to secured and to unsecured communications, both in unicast and groupcast communications mode

Active partners

Friends of SVI

Observation.
The SVI website has very limited information. Hence for further analysis access to above mentioned ISO standards is required.