Securing Vehicle to Everything
**What is at stake with V2X?**

As cars are getting all connected and autonomous driving is every day becoming a stronger reality, car manufacturers are facing the challenge to trust the information that is received by each vehicle. In this perspective V2X communication will be a key factor to the success of autonomous cars.

‘Vehicle-to-everything’ also known as V2X refers to the passing of information from a vehicle to any entity that may affect the vehicle, and vice versa. V2X covers:

- **V2I or ‘Vehicle-to-Infrastructure’** which is the exchange of data between a car and equipment installed alongside roads and that are generally called ‘roadside units’ (RSU). V2I can be typically used to broadcast traffic conditions and emergency information to drivers.

- **V2V or ‘Vehicle-to-vehicle’** relates to the transfer of data in between vehicles. Compared to what sensors can provide to the vehicle, information transmitted via V2I technology can come from vehicles few hundred meters ahead or even hidden vehicles from behind trucks or buildings.

The automotive industry has worked with regulatory bodies to standardize V2X communication. The objective was to ensure interoperability between vehicle brands and with the road infrastructure so standardized messages can be managed by all stakeholders.

In most countries governments consider V2X as a key technology to achieve a next step into the reduction of road fatalities. So they are pushing the industry to shorten the deployment schedule for the technology. For car manufacturers, V2X and more specifically V2V, is a milestone in the path towards fully autonomous cars.

Beside the challenge of choosing the optimum communication bearer (DSRC, C-V2X or hybrid) that keeps the industry and the mobile community very active, the security of V2X communication comes also as a key topic. Regulators have pointed out the need to protect the messages against fraudulent or misleading use. They also request the user’s privacy to be protected and preserved so the journey of drivers cannot be easily tracked or reconstructed by listening and compiling all messages a car sent and received in a period of time.

**Leverage on Public Key Infrastructure to secure V2X**

The principle of V2X communication security is based on signed messages using Public Key Certificates. In Europe and in the US, ETSI ITS and IEEE have both respectively defined PKI architectures to secure all V2V and V2I communications. And for privacy protection purposes certificates have a fairly limited validity period and need to be changed regularly.
Optimize certificate issuance and management

As car manufacturers are working to prepare their vehicles to comply with V2X standards, they are working on new ECUs (Electronic Control Units) that manage all the communication flow as well as fetching certificates that are required to sign messages they broadcast.

For OEMs as they concentrate on building the V2X ECU, the backend system that is required to run the PKI infrastructure and generate certificates for their cars comes with two major challenges:

- First the certificate structure defined by ETSI-ITS and IEEE is very specific to the V2X use case and requires a complete new development, so most of existing PKI bricks cannot be reused.

- Second, because of the high frequency of certificate renewal for every vehicle, the quantity and availability of the certificate generation become a strong constraint when building the service. Even so, with the growing number of V2X ready vehicles coming on the roads, the number of certificate fetching requests to the store will grow exponentially.

Benefit from Gemalto V2X Cloud Services

With more than 15 PKI projects deployed and live, Gemalto has a strong experience in providing PKI infrastructures to its customers. Gemalto has also a deep expertise in developing secure services and operating large scale system that addresses hundred millions of users.

Thanks to this unique position Gemalto is developing V2X certificate services that combines state-of-the-art technologies for optimum scalability, advanced cryptographic expertise and its unrivalled HSM products.

As V2X standards have just been released and the V2X ecosystem is still very new, Gemalto is working in agile mode to be as close as possible to OEMs requirements and be able to adapt and pivot as needed.