Horus Security Suite for ITS

Build trusted and secure Intelligent Transportation Systems

Trusted partner for your Digital Journey
With the growing deployment of connected cars, vehicles are rising in complexity with new features, enabling them, among other things, to communicate with a huge ecosystem: intelligent transportation systems.

**What are ITS?**

Related to the smart city concept, intelligent transportation systems (ITS) are meant to improve security and safety, as well as efficiency, through different uses. Traffic monitoring, vehicle safety, transit signal priority... All these applications rely on sensors, data collection, analysis, control and communication technologies to enhance citizens’ daily life. Data collected via hardware devices on connected vehicles are transmitted to the system, designed to smartly treat information in real-time.

**The three pillars of ITS security**

The more the ITS are growing, the more potential vulnerabilities can be found, arising potential cyberattacks gateways for hackers. As these threats can expose dangerously city’s traffic systems, it is essential to implement the right security technologies. According to the Connected Vehicle Reference Implementation Architecture (CVRIA), the security solutions must focus on 3 core elements:

- **Confidentiality:** only authorized stakeholders should be allowed to access the content of the messages exchanged in a V2X(1) environment
- **Integrity:** to ensure the reliability of the messages exchanged, the security solutions must protect them from being altered by unauthorized stakeholder, otherwise ITS applications could be threatened
- **Availability:** operational systems and information must be provided, even in risky situations, especially for critical information

Moreover, trust and privacy management for ITS communication must also be achieved according to the ETSI TS-102941. Indeed, when tracking people and vehicles within transportation, private data such as the license plate or vehicle owner must not be disclosed to guarantee privacy protection for travelers.

---

**1.25 millions**

Connected cars with embedded connectivity are expected to ship worldwide by 2022(2)

**1 in 3**

Connected vehicle models will have built-in, function-level, over-the-air software update capabilities by the end of this decade according to Gartner(3)

**10 hacks in 10 week**

Is the number of hacks targeting connected vehicles highlighted in January and February 2018 by Upstream from identity theft in car-sharing services to keyless entry, system vulnerabilities exploitation in UK to steal cars(4)

---

(1) V2X refers to vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I)
(3) https://www.gartner.com/smarterwithgartner/staying-on-track-with-connected-car-security/
(4) https://www.upstream.auto/blog/q1-2018-automotive-cyber-hacks/
“There are so many different ways that cars connect to the internet and connect to the outside world, everything from the OBD2 port, to Bluetooth, to Wi-Fi, to 3G, 4G and eventually 5G. Hackers are always looking for the weakest link, so the more links you have and the more software you have, the more vulnerability you have. There’s a huge attack surface in cars.”

Alex Manea, BlackBerry’s chief security officer

Secured V2X communication is critical to set up reliable ITS. PKI solutions are key to secure exchanges between connected vehicles and roadside units.

**Traditional security for new automotive needs**

PKI solutions are nothing new, but they have been proven in many industries and can be a perfect fit for automotive industry. In ITS, connected vehicles need to be clearly identified to implement a trusted environment and then avoid risks related to access control and impersonation.

Electronic certificates are used to support strong authentication for devices and data confidentiality for data in transit or in storage. Connected vehicles are provided with a digital identity materialized by key pair (a public key and a private key) and a long-term certificate, generated by an Enrolment Authority (EA), that associates the registered vehicle with the digital identity.

After that, whenever the vehicle needs to be identified to communicate with another vehicle or a smart city application (traffic flow controls, payment application, roadway reporting…), an Authorization Authority (AA) will check the enrolment certificate of the vehicle with the EA. If the identity is confirmed, the concerned vehicle is provided with short-term certificates, allowing it to communicate securely with other stakeholders while through encrypted data. Its privacy is also ensured all along the process as the certificates do not reveal the identity of the user.
A proven and scalable solution

Benefiting from the legacy of its qualified PKI offer, Horus metapki, Atos paved the way to a new cloud-native micro-services architecture for PKI. Horus ITS-uPKI supplies PKI capabilities on demand for ITS services, such as devices registry, enrollment and authorization for V2X communication. Depending on your needs, our PKI experts can provide you with an adapted PKI solution hosted on the Cloud and easy to deploy:

- **Managed Enrollment Authority**: enable connected vehicles to request permission to access ITS communications by registering their credential information and provide them with a long-term enrollment electronic certificate
- **Managed Authorization Authority**: enable connected vehicles to request authorization to invoke ITS security services with short-term electronic certificates and verify their enrollment credentials

As a cloud-based service, Horus ITS-PKI eliminates the burden of managing in-house PKI solutions for the organizations. With this solution, you can:
- Eliminate the need to buy and install the required hardware and software technologies, as well as hiring a dedicated expert team, for PKI technologies with an easy-to-deploy solution
- Manage your costs with a fixed setup, easily adaptable to your growing organization
- Enjoy a high-available and compliant system enabling you to keep your PKI services available even during updates or maintenance and without business disruption
- Expand your business without worrying with a PKI-scalable solution

Deploy your offline Root Certificate Authorities

It is critical to ensure the integrity of your root CA by avoiding any unauthorized access to it. To mitigate this risk, Atos provides a secure and offline environment to keep your root private keys protected with the Horus PKI appliance based on a Trustway Proteccio Hardware Security Module (HSM). This HSM has been certified under the most stringent qualifications such as Common Criteria EAL4+ with CWA 14167-2-PP, allowing organizations to run security-sensitive processes in a highly performing manner.

Secure elements for the automotive industry

To enhance the integrity in ITS, the messages exchanged in V2X must be encrypted. Atos can provide dedicated secure elements (V2X-HSM) based on security controllers to be integrated into ECUs to answer this challenge. They do not affect the complete board design and sustain the required automotive qualifications and requested performance for automotive applications. To ease the integration into the V2X software stack Atos provides a software library (V2X SDK) to abstract the communication with the V2X-HSM. Atos Secure Elements (V2X-HSM) rely on CardOS®, which performs the cryptographic functionality over standard interfaces SPI or I2C and ISO 7816-3 T=1. CardOS is a multifunctional native operating system, which provides a high level of flexibility by adapting the file structure.

As modern vehicles use up to 120 ECUs to communicate in an ITS environment, it becomes prevalent to be able to generate quickly and efficiently cryptographic keys that will be used for signature creation, authentication, as well as message encryption and decryption. With CardOS, for IoT, all these state-of-the-art cryptographic functionalities are provided. Coupled with our solution Horus PKI-ITS, it becomes easy to implement certificate lifecycle management and ensure data integrity.

---

The connected automotive market is quickly evolving and is expected to reach USD 2.07 billion by 2023 at a CAGR of 29.44% by 2023. Both car manufacturers and smart city services providers will need a scalable solution to handle the billions of cars’ devices and sensors linked to smart cities.

The PKI-ITS architecture is using Docker for an easy-to-install environment and Kubernetes for automating deployment and management of these containerized applications. This enables organizations to set up PKI-ITS into their infrastructure quickly and simply.

The Horus security suite for ITS works in a SaaS mode with a hybrid Cloud architecture. It enables operators to elevate their performance whenever needed, adapting electronic certificates generation to the requests and helping to manage the costs. Moreover, this system helps to efficiently fight against cyberattacks targeting the availability of smart cities’ services, such as DDoS attacks.

Due to its flexible and modular approach, the Horus security suite can easily be integrated into an existing information system such as a fleet management organization.

The Horus security suite for ITS works in a SaaS mode with a hybrid Cloud architecture. It enables operators to elevate their performance whenever needed, adapting electronic certificates generation to the requests and helping to manage the costs. Moreover, this system helps to efficiently fight against cyberattacks targeting the availability of smart cities’ services, such as DDoS attacks.

Due to its flexible and modular approach, the Horus security suite can easily be integrated into an existing information system such as a fleet management organization.

An adaptive architecture tailored to your needs

Choosing the Horus security suite for its...

One-button deployment

The PKI-ITS architecture is using Docker for an easy-to-install environment and Kubernetes for automating deployment and management of these containerized applications. This enables organizations to set up PKI-ITS into their infrastructure quickly and simply.

High availability

Through its SaaS model, Horus PKI-ITS provides uniform high availability of its services. It is possible to perform updates and system maintenance without disrupting business.

Integration to SOC

The various Certificate Authorities can be integrated to a Security Operations Center (SOC) to identify abnormal behaviors and conduct the right remedial actions as soon as possible.
Standards and technical specifications:

- ETSI TS-102941
- ETSI TS-103097
- IEEE-1609.2a
- ITU-T-X.696
- C-ITS Certificate Policy

- The compliance of RCA, EA and AA certificates is based on ETSI TS-103097
- The compliance of CRL, CTL, Enrolment request, Authorization request is based on ETSI TS-102941
- Algorithms: ECDSA (Nist-256, Brainpool-256 and Brainpool-384)
About Atos

Atos is a global leader in digital transformation with 120,000 employees in 73 countries and annual revenue of €13 billion.

European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions through its Digital Transformation Factory, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies and industry knowledge, Atos supports the digital transformation of its clients across all business sectors. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Syntel, Unify and Worldline. Atos is listed on the CAC40 Paris stock index.

Find out more about us: atos.net/en/products/cyber-security/digital-identities

Let’s start a discussion together