thalesgroup.com

THALES

Building a future we can all trust


# Automotive digital IDs:

## Building digital trust for enhanced convenience

# Automotive digital IDs: **Building digital trust for enhanced convenience**

With the massive introduction of computing power and connectivity inside vehicles, our cars are connected to more and more devices, servers, apps and services. The diverse technologies can range from 5G and Bluetooth, to Wi-Fi and NFC. However, before exchanging data or engaging in a transaction, it is important to know what – or who - is on the other side of the connection.

Each one of us has multiple identities depending on the context, known as a digital identifier or digital ID. For example, our mobile phone digital ID is our phone number, whereas in a payment context our identity is our credit card number. Similarly, cars have multiple identities for various scenarios.

Beyond identification (i.e., assigning a unique ID to a person or object), an authentication phase is mandatory to ensure a remote entity is the one it claims to be. Finally, an authenticated entity with a given ID will be generally associated with a set of permissions depending on its role, status or service level. Permissions associated with an authenticated ID are a powerful way to implement value-added services and innovative business models.

In this paper, we will review the concepts of digital IDs, authentication and permissions in the automotive market through three concrete examples:

- **the digitalisation of the car key** to open and start the engine
- **the electric vehicle (EV) charging** subscription and
- **the peer-to-peer communication** between cars and related infrastructure (aka V2X communication)

For each use case, we will describe the associated cybersecurity risks and the attacks that could be set-up by potential hackers.

Clearly, risks did not appear with digitalisation alone. Car theft has always been a problem. However, new risks have been introduced with the possibility of cyber attacks at an industrial scale. The vast majority of hackers' motivation is financial gain. So, it's probably wise to be prepared for immense creativity from cyber criminals to extort money. Car-stealing ransomware that would make a vehicle unusable, fraudulent EV charging with incorrect billing or personal data reselling are just a few of the potential attacks in our new cyber world.

As the transport ecosystem is one of the pillars of modern society, it is of collective interest to build a trusted and cyber resilient environment. Otherwise, it will be a high-profile target for any potential hacker, spy or terrorist and the brand image of auto manufacturers could be irreparably damaged.

We will describe some security mechanisms available to deploy safe and trusted services for connected cars, EVs and the many new innovations coming to the auto industry.

# Automotive digital ID **use cases**

## Digital car key

Car keys have already evolved from plain metal keys to so-called key fobs that communicate wirelessly with a car to open it. However, a key fob has to be handed over to anyone who needs to use the car and no specific permissions can be attached to it. The next step is the virtualisation of the car key, or a digital car key. A digital car key can be stored in smartphones, and the car can be opened by simply tapping the smartphone on the door handle. The latest models allow smartphones to remain in a pocket or bag for seamless use.

Once a car key has been digitalised, it is easy to share it among family members´ smartphones without the hassle of passing around a physical key fob. Moreover, compared to a key fob, a smartphone is a personal device associated with an individual, that one can no longer do without. It then becomes possible to associate specific permissions to individual drivers easily. For a car shared by a family, a young driver may be given permission to use the car for only a short period of time, or a delivery person can be given temporary access to the trunk only to deliver a parcel.

Outside the family context, the advantage of the digital car key is even more obvious for car rental fleet management. Digital keys allow car rental companies to reduce friction and remove all key fob handling processes, while being able to sell additional car options or to more precisely control the authorised drivers of a rented car, e.g., only licenced or age-appropriate drivers. Additionally, fleet managers will be able to assign drivers to specific vehicles for specific tasks. For example, a remote moving company manager could easily match drivers to different-sized vehicles based on the project needs in various regions.

To implement this service, a standard has been created thanks to the work of the **Car Connectivity Consortium® (CCC)**, known as the **CCC Digital Key (CCC DK)**. The principle is smart and easy: each car and smartphone is assigned a CCC Digital ID, enabling mutual authentication between car and smartphone for single access, while ´unlocking´ specific permissions associated with a car user.

The driver simply has to enrol in a Digital Car Key platform to certify his ID before using the service. While the CCC standard does not use biometry for validation, adding this extra security layer can provide a very strong authentication step that is used in many other industries including banking and telecom. This authentication step is crucial to ensure the driver is the one associated with the specific smartphone.

On the driver´s side, the CCC DK can be stored in other smart devices, such as wearables (smart watch), contactless cards (for phone back-up purposes) or any other electronic equipment (in a parcel delivery terminal, for example).

### Main cyber risks associated with the digital car key

A common cyber threat is the simple extraction of a Digital Key (from a smartphone, for example). If this happens, the hacker can use the DK to impersonate a valid user and steal a car. An attack can be set up with a temporary access to a phone or, even worse, remotely. Concerning lost or stolen devices that could also have their DK extracted, it is important to be sure that the owner of the device is authenticated. This is generally the case with recent smartphones, which offer various authentication form factors, including biometrics. In fact, the situation can be similar to credit card digitalisation with services such as Apple Pay or Samsung Pay. Now the phone security level is high enough that credit card issuers consider the digitalisation risks acceptable. However, the risk is higher with the DK: the maximum amount of a payment transaction is always capped and risk management is part of the credit card issuers' core business. With cars, the value of the car is at stake (typically much higher than a credit card transaction) and the risk management will be up the card owner and its insurance company.

A DK inside the car (that ensures the mutual authentication between smartphone and car) has to be secured as well and protected from remote or local cyber attacks. Local attacks are especially concerning when the car is parked in a public and unmonitored location. It is more likely that an attack will take place against a parked car at night than against a smartphone placed beside its sleeping owner.

In addition to DK extraction, an existing cyber attack on key fobs might be transferred to phones or wearables: the relay attack. As its name suggests, relay attacks consist of opening a car parked away from the phone by relaying car messages on the phone side and phone messages on the car side. This is done by a pair of attack devices that are communicating wirelessly and acting as a car on the phone and as a phone on the car. This cyber attack extends the communication range between the phone and the car but does not change anything in the authentication traffic. In practice, this attack is relatively common against key fobs that do not require an action from the driver (aka Passive Entry Passive Start or PEPS).

The typical set-up for such an attack is when a car is parked in a house driveway where the owner has dropped the key fob near the front door. In order to mitigate this risk for mobile devices, the first generation of DKs utilizes only very short-range communication (Near-Field Communications or NFC), like what is used for digital payments. However, this does not provide the convenience of PEPS. For subsequent versions, Bluetooth communication has been introduced, but in combination with a new wireless technology called UWB (Ultra Wide Band) that allows checking the distance between the car and mobile phone with an accuracy of up to a few centimeters. With this set-up, the relay attacks can be thwarted.

# Automotive digital ID **use cases**

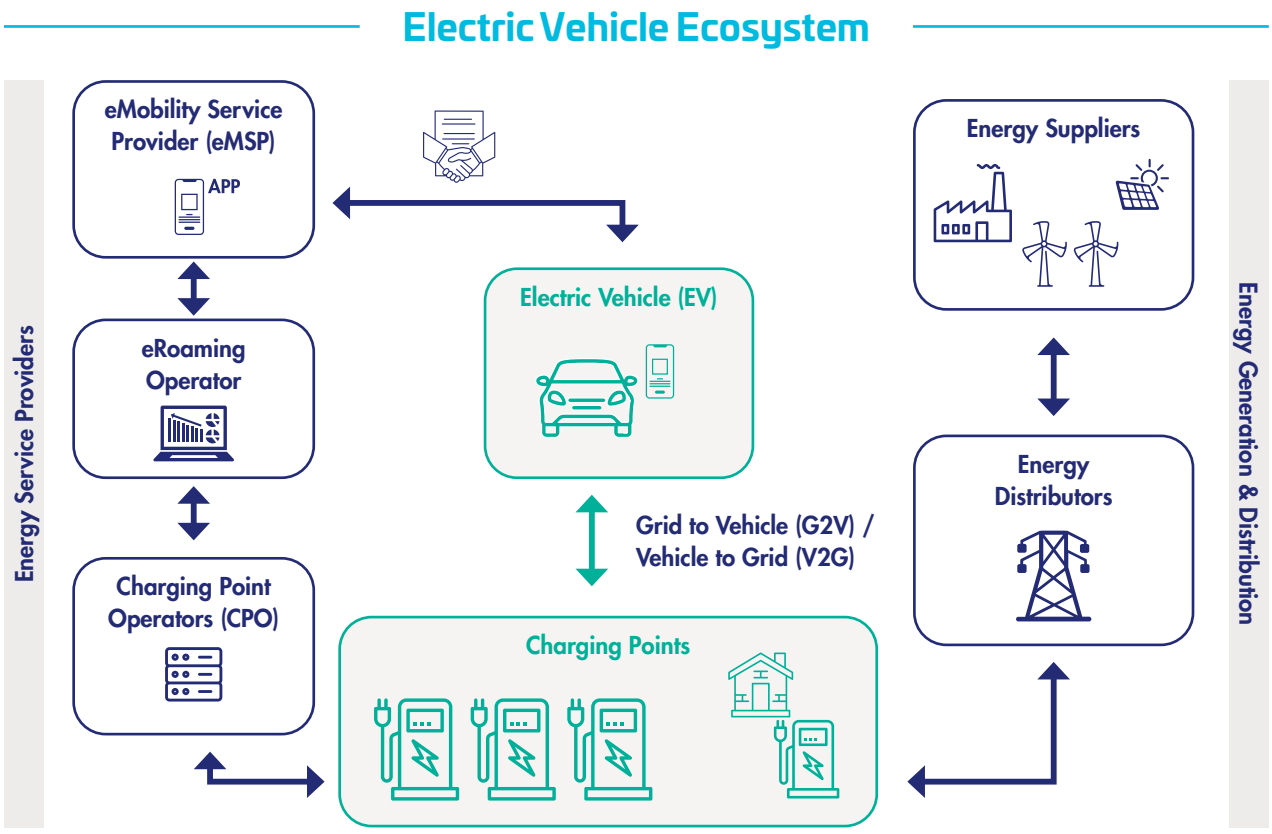
## Electric vehicle charging

The Electric Vehicle (EV) market is booming and there is no doubt that, due to climate change concerns and regulations, more and more EVs will replace Internal Combustion Engine (ICE) vehicles on the roads in the coming decades. The only remaining question is: at what rate? As almost all countries struggle to follow the path of the Paris Agreement in terms of greenhouse gas emissions, it is important to remove all potential roadblocks to massive EV adoption by customers. Beyond price and autonomy, EV charging has been identified as a pain point for end users.

Today, when traveling, not only does the EV owner have to find an available (and functional) charging station, but he/she also has to be able to pay for the transaction. And this is where the hassle starts. The market has been flooded with a wide range of incompatible solutions ranging from smartphone apps to classic credit card payments including contactless badges linked to a variety of subscriptions.

To simplify the current chaos and complexity, the next step is to enable the EV user to have a unique subscription from one electric Mobility Service Provider (eMSP) and receive an aggregated bill at the end of the month for all charges, encompassing all charging stations accessed. The parallel can be drawn with mobile phone communication where we all have one contract with a Mobile Network Operator (MNO) while being able to travel worldwide, use foreign mobile networks seamlessly, and still be billed by our home network operator (roaming).

The **ISO standard 15118** (aka plug and charge) makes this vision for EV charging a reality. According to ISO 15118, car and charging stations are assigned Digital IDs that are exchanged over the power cable (also called power line communication or PLC), enabling a mutual authentication, transparently performed each time the car is plugged in. In a second step, an extra authentication proof is given by the car to prove that it is associated with a valid eMSP subscription. Plugging your EV and charging it at any charging station is as seamless as switching on your mobile phone when landing in a foreign country.




To implement this service, each element of the ecosystem (car, charging station, eMSP) has a Digital ID. Authentication between these elements is performed before any charging transaction and permissions can be further associated to a contract, to grant charging priority, service level agreement, free parking time, etc.

### Main cyber risks associated with plug and charge

If opening the car with a mobile phone can be compared to the mobile payment use case, the EV charging landscape described above can be compared to the GSM subscription use case. One difference is that the Digital ID of the subscription is not contained in the mobile phone's SIM card, but within the car. One of the main threats is the extraction of credentials associated with an eMSP subscription and their injection into another car. This attack would allow the attacker to pose as the genuine contract subscriber and charge their EV at the expense of the genuine subscriber. In addition to the financial loss, this kind of attack would decrease the level of trust in the plug and charge ecosystem and slow down its adoption and the deployment of value-added services.

If transportation is an important part of our modern societies, the electricity grid is the cornerstone of charging stations. It is of utmost importance that the massive deployment of EVs and charging stations do not hurt its reliability. If hackers managed to take control of thousands of vehicles, one identified risk would be the launch of too many EV charging sessions at the same time. The grid balance could be lost resulting in a large blackout. The world watched as cyber attacks against some country grid caused long outages a few years ago, showing that this scenario is far from theoretical. Critical and essential operators are becoming valuable targets for cyber attackers considering the catastrophic impact and huge damage caused.

# Automotive digital ID **use cases**

## V2X communications

V2X communications encompass direct communications between cars (vehicle-to-vehicle, or V2V) and between cars and infrastructures (V2I). All of these communications are called direct (or device-to-device) as they do not go through any mobile network infrastructure, allowing communication outside cellular network coverage and low latency. Numerous use cases have been devised for V2X. Although the main purpose of V2X is to increase road safety, it may also decrease congestion and allow more dynamic traffic management. We review three V2X usage examples below.

The typical use case for V2V is collision avoidance. For this purpose, each vehicle will broadcast its position, speed, direction and a few other parameters, such as emergency braking, 10 times per second. All surrounding vehicles will receive this data and use them to construct a dynamic model of the traffic and detect potential collisions. For example, if a truck in front of my car blocks a vehicle that requires emergency braking, the V2X technology will warn me in advance or even automatically start to slow down my car.

V2I communications will also be used for safety purposes. For instance, speed limit and advanced warning broadcast devices can be fitted on temporary roadwork or accident signage. The information will be received by bypassing vehicles (and displayed in the dashboard or Heads Up Display, aka HUD) a few hundred meters in advance, which increases the time a driver has to react compared to exterior road signage only.

As for traffic enhancement, traffic lights can broadcast the delay before their state changes, which can help drivers adjust their speed to avoid braking or extreme speed changes. With the advance warning and correct speed adjustments, drivers can arrive just in time for the light to change green without stopping, helping to keep traffic moving. This application is called Signal Phase and Timing (SPaT).

V2X communications are starting to be deployed in the EU, Japan and China. They are also extensively discussed and tested in the USA. The applicable standards vary by region, with ETSI the driving force in Europe and IEEE leading in North America.

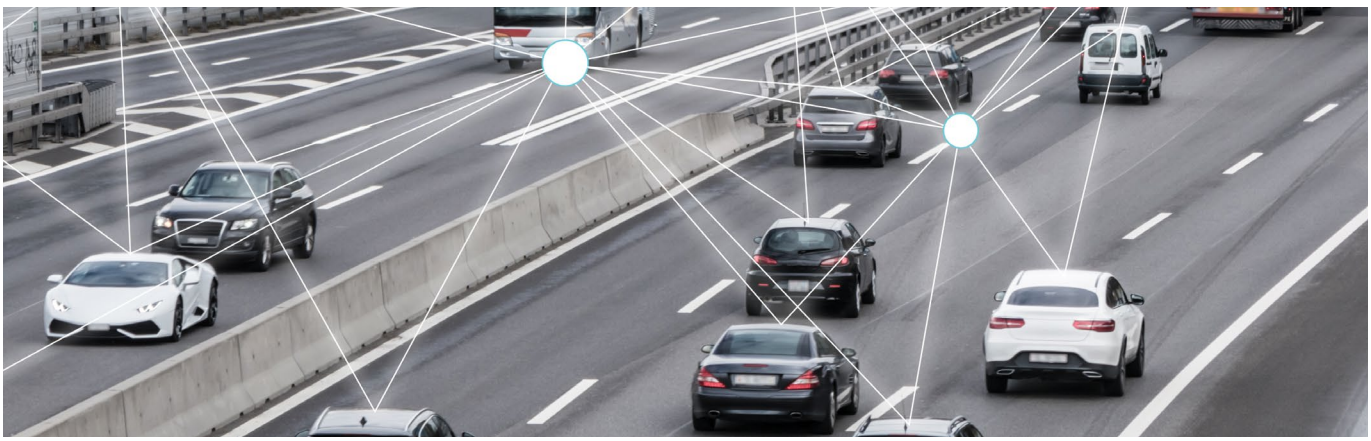
Behind the scenes, a Digital ID must be assigned to each vehicle and infrastructure element. Obviously, all data broadcasted by a node must be authenticated before being taken into account by the other surrounding nodes. This will prevent the creation of false messages transmitted by fake nodes. Permissions can also be helpful in this context: for example, an emergency vehicle approaching a traffic light will be immediately recognized as such and will switch its status to green, while keeping close-by traffic lights red, to avoid collision.

**Main cyber risks associated with V2X communications**

There is no need to review the danger of a general freeze of the transportation infrastructure caused by malicious messages (like a non-existing accident or ghost car routes). What is more specific to V2X communications is the importance of data privacy protection.

The cyber risk is obvious: each car will constantly broadcast its position making it a perfect tool for tracking across a town or region. Fortunately, this threat has been accounted for from day one and mitigated by the standards. First, if cars have long-term digital IDs related to V2X communication, these IDs are not used in publicly broadcasted messages. Short-term IDs (i.e., pseudonyms typically valid for a week) are used instead. Moreover, each car is given a set of pseudonyms (typically up to 100) that are used randomly throughout a trip, making it difficult to be tracked even for a short period of time. This trade-off between privacy, security and implementation cost has been publicly debated and is now agreed upon as acceptable.

When doing a rough estimation, it is immediately clear that allocating approximately 100 pseudonyms each week to millions of cars will result in billions of digital IDs and associated credentials each year. To accommodate this volume, very specific V2X solutions need to be developed to provide a high level of scalability, elasticity and, of course, security.



# Security solutions **to build automotive digital trust**

In light of the above-mentioned cyber risks, it is clear that privacy and security solutions must be built-in to enable trust from car owners, fleet managers, automotive service providers, e-Mobility users, and government entities. This will foster a healthy and safe automotive ecosystem into which innovative services can be deployed and bring resilient infrastructure for society.

Before diving into the specifics about the various security mechanisms that can be deployed for the automotive ecosystem, let's point out the generic principles that are implemented for a security-by-design methodology.

The main purpose is to make vehicle cyber attacks more costly and harder to set up in order to deter them. To that end, the security mechanisms will try to make automatic, massive and remote cyber attacks very difficult. If successful, this strategy will leave the attacker with only one option: to set up targeted attacks that need physical access to the devices in order to be attempted. The resulting cost / benefit ratio will likely deter the hacker.

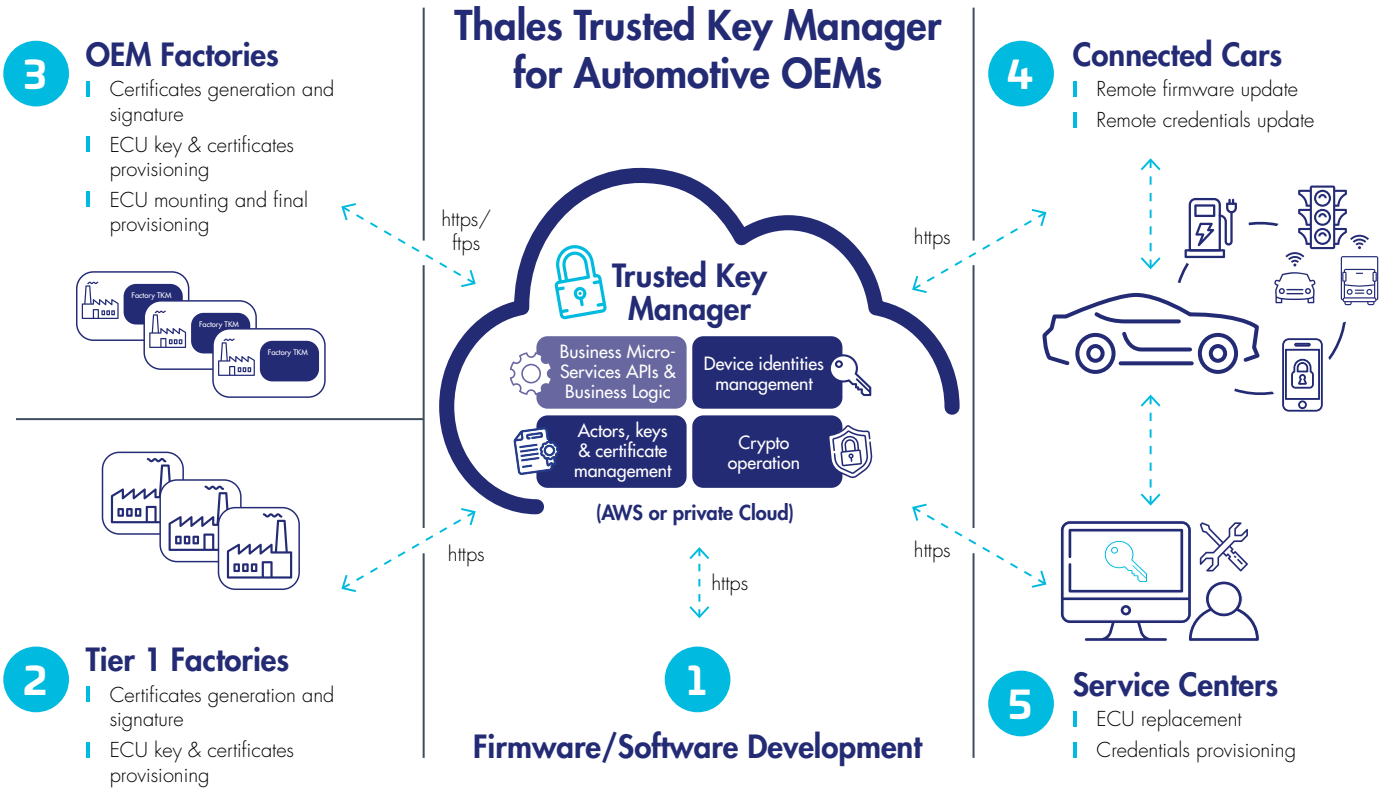
There will always be some residual risks, as zero risk does not exist, either because the cost to prevent them is not acceptable or because of technology vulnerabilities discovered afterwards. In any case, it is important to acknowledge those risks and to put in place mechanisms that will detect attacks as soon as possible and trigger a reaction to block propagation.

In the rest of this section, we will present the main security mechanisms to manage the digital IDs' lifecycle in a trusted way, to store IDs securely - either in devices or on the back-end side - and to monitor the automotive ecosystem's infrastructure security in real time.

## Trusted management of digital IDs and credentials

In all discussed use-cases, it is mandatory to create robust and diversified digitals IDs for the various actors in order to perform mutual authentication with associated credentials later on. This will enable data integrity and confidentiality protection. Underlying security and cryptography technologies are very heterogeneous, so it is important for any credential management solution to cope with this diversity and to be future proof as many more will come (such as post quantum cryptography).

Thales proposes such a solution with the Trusted Key Manager (TKM). It has been specifically tailored for the automotive and mobility market, which has some important requirements. First, the logistic chain of car manufacturing is complex, and IDs/credentials will need to be created and injected when numerous suppliers manufacture the car parts. Then, downstream, IDs and credentials will need to be renewed when the car will hit the road or when an embedded computer will have to be replaced in a maintenance center.



Simply put, the TKM can be seen as the security hub linking all car manufacturer partners to allow the smooth management of all digital IDs across the whole lifecycle of vehicles. Thales TKM leverages the below described Hardware Security Modules (HSM) for state-of-the-art protection of automotive infrastructures.

## Secure storage of digital IDs and credentials

As previously stated, a recurrent cyber threat is the potential extraction of credentials from a car or phone. The deployed technologies should resist such an attack, even if the attacker has physical access to the device for a long time and is able to dismantle it in a lab. Solutions that are able to resist an attack in that context are called tamper-resistant. In addition to the high level of resistance to attacks, technology providers must be able to prove their security claims in a transparent way. This is called security assurance and typically it is achieved through third-party product certification under standardised schemes like ISO 15408 (aka Common Criteria) or FIPS 140.

These issues are well known in other markets such as payment, mobile telecommunications or even sovereign identities like electronic passport. In all these markets, Thales provides tamper-resistant certified solutions and has adapted them for automotive and mobility.

On the embedded side, secure chips called Secure Elements (SE) are already present in mobile phones or other wearables and can be leveraged to securely store digital keys. These SEs are also introduced in car-embedded computers or in-road infrastructure such as charging stations, road signage, etc. Secure Elements are tamper-resistant environments that act as a vault to securely store very sensitive data, such as digital car keys. Being microprocessor-based platforms, they also host cryptographic applications that provide data and device access only to authorized applications and people. It represents a high level of security against both physical and remote attacks.

On the back-end side, a variety of servers also needs digital IDs to protect critical infrastructures and sensitive data, proceed to secure updates, and to access and manage the credentials that are embedded into the cars or other devices. Due to the number of end-points managed and the performance constraints, extremely powerful hardware is required, providing high computing power, high tamper-resistance properties and certifications. These products are called Hardware Security Modules (HSMs) – dedicated devices that are specifically designed to perform complex crypto operations and to protect the cryptographic keys that are routinely used in data centers.

Thales Luna HSMs answer international security standards (FIPS 140-2 Level 3, Common Criteria (CC) EAL4+) and provide a hardware root of trust for the Public Key Infrastructure (PKI) typically used to issue IDs to all devices, regardless of their complexity or scale. Luna HSMs enable automotive manufacturers to secure their production processes and assets by always generating, managing and storing high entropy, or "unhackable", encryption keys in hardware, securing communications and data.

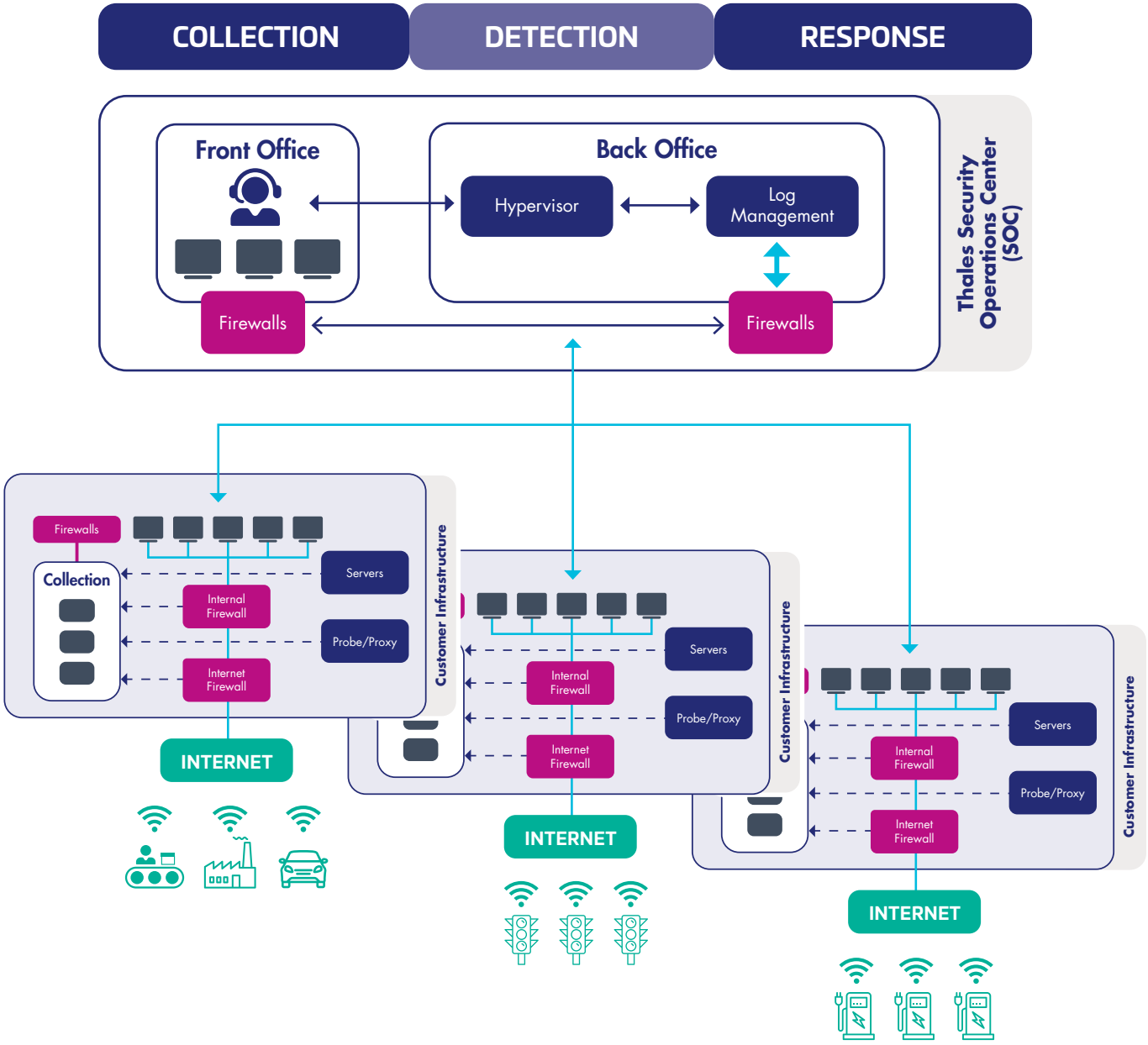
Strong access controls ensure that automotive resources are available to only those who are granted access, and device authentication ensures that each IoT device is manufactured with a unique identity to track your device throughout its lifecycle, communicate securely with it and revoke privileges when a device exhibits unexpected behavior. Lastly, Luna HSMs protect code signing keys, which in turn ensure authenticity and integrity of device firmware updates and patches.

## Monitoring infrastructure security

Finally, it would be foolish to design multiple security mechanisms to manage digital IDs, to roll them out in products and consider the work as being done. Security is a never-ending process, and the live deployment of a solution is only the beginning of the story.

New attack techniques appear on a daily basis. New vulnerabilities are constantly discovered and software is now deployed continuously. To cope with the residual risks and newly emerging ones, cyber security solutions are needed to supervise large IT and OT infrastructures, detect real-time incidents or attacks, classify them according to their dangerousness and launch the appropriate reaction for better effectiveness.

Thales provides such Security Operation Centres (SOC) that are composed of best-in-class cybersecurity components for a 360° cyber supervision: sector specific threat intelligence to understand the threat environment, real-time attack detection with IT and OT probes, big data analytics assisted by Artificial Intelligence (AI) for hunting and detecting unknown attacks. And because cybersecurity is not only a matter of technologies, and human expertise is paramount, Thales has a large pool of worldwide cyber experts available 24/7, skilled to manage and control a potential crisis and react properly.




## Building Digital Trust with Automotive Digital IDs

In this whitepaper, we have described how the multiple digital IDs in cars and, more generally, the transportation ecosystem can be used to deploy safe and trusted services despite some unavoidable risks. Thanks to a wide range of security products and services dedicated to the car and transportation industry, Thales has the right offering to help reduce these risks so end-consumers can benefit from innovative new features and society as a whole will benefit from a resilient, secure infrastructure.