



# Securing the connected vehicle



**ENTRUST**

SECURING A WORLD IN MOTION

# Securing the connected vehicle

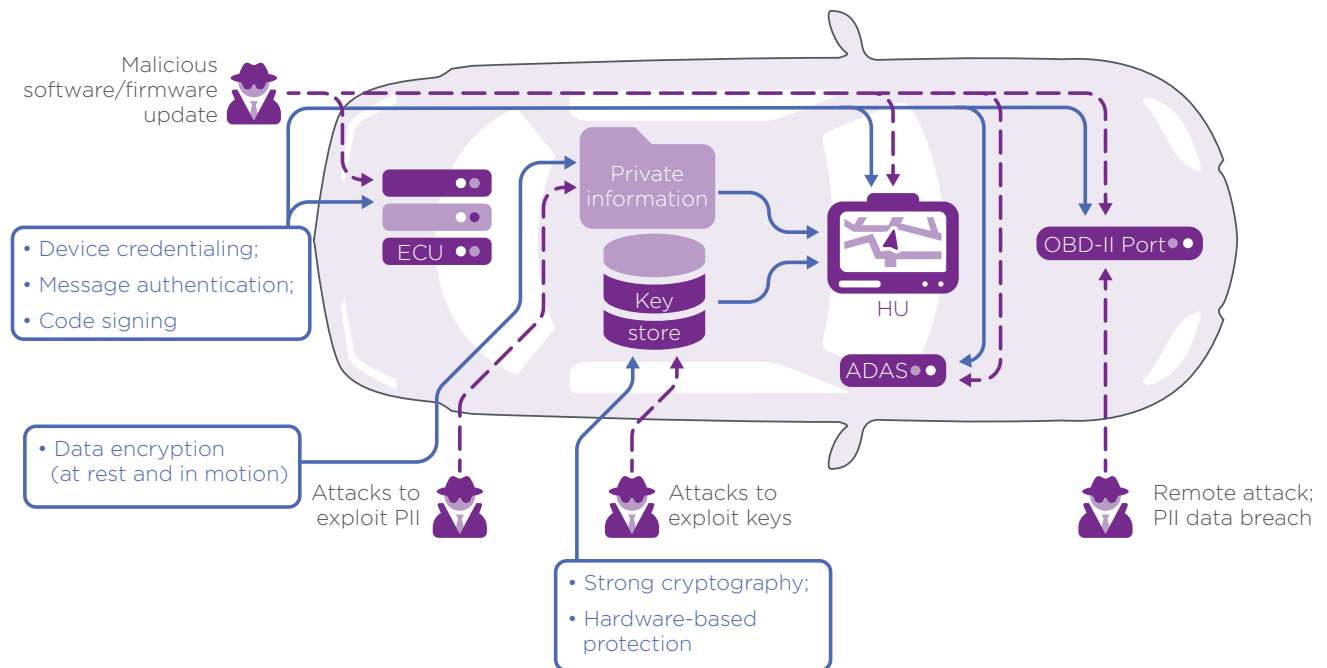
## The problem: new vehicles introduce security vulnerabilities

Today's automobile has as much in common with the Apple iPhone as it does with a '67 Ford Mustang. The trend toward increasing connectivity will only increase vehicles' complexity, resulting in new security vulnerabilities and challenges, including:

- The introduction of malware via software or firmware updates sent to vehicle safety, operational, and infotainment systems
- Unauthorized and insecure aftermarket components added to the vehicle – either deliberately or unknowingly – including widgets plugged into the vehicle's on-board diagnostics (OBD-II) port
- Valuable security personnel pulled away from high-priority activities to design and build a large public key infrastructure (PKI)
- Unauthorized production runs at remote factories that result in damaged revenues and brand reputation



Automotive original equipment manufacturers (OEMs) and their suppliers rely on Entrust for our expertise and experience in building data protection strategies. Our technology enables the root of trust needed to ensure a robust security infrastructure that will scale to meet the industry's evolving demands.



While some vehicle systems may be isolated, threat research has shown that advanced attackers can find vulnerabilities, so a breach of one subsystem could allow attackers to pivot to others.

Another challenge relates to the proper design of a scalable security infrastructure. Specifically, to help defend against certain attacks, connected components need to be authenticated.

While vehicle OEMs and their suppliers have recognized that cryptographically-based digital signatures provide the strongest form of authentication, this also necessitates the management and protection of certificates and the underlying keys. The rapid increase in connected components has created the need for broad-scale secure key management, supported by a PKI.

### Solution benefits:

- Ensures the authenticity of connected components
- Safeguards code updates against tampering
- Ensures that firmware and software code comply with internal policies
- Ensures PKI integrity, performance and manageability
- Provides opportunities for improved customer service and revenue streams
- Protects against unauthorized and erroneous production runs

Additionally, whereas software and firmware updates are commonplace for many kinds of consumer electronics, this is new territory for automotive OEMs and suppliers. These updates are increasingly necessary, and today they are typically performed at the dealership, resulting in unwelcome costs and negative customer impact.

Whether delivered over-the-air (OTA) or at a service center, code updates sent to connected components present the potential for malicious behavior, as well as unintended errors. Without proper security protocols, corrupted code can be introduced to the vehicle. Manufacturers also require assurances that code complies with organizational policies.

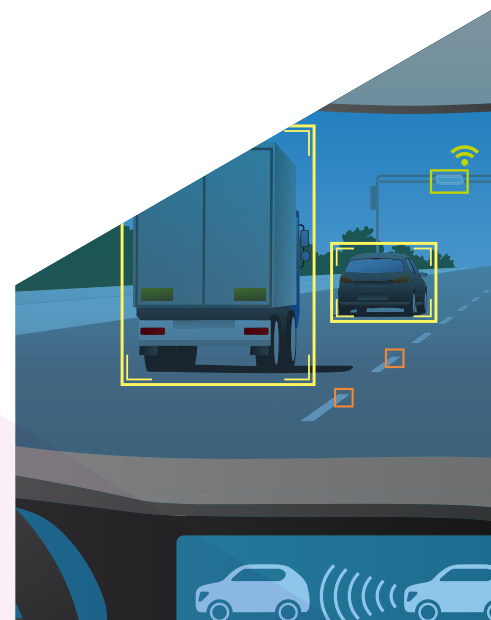
There are also battles to control systems and data, further complicating the security picture. For example:

- Right to repair legislation, which is supported by many consumers, requires vehicle manufacturers to allow non-dealer mechanics access to vehicle systems for repairs, potentially introducing security concerns
- While consumers want the functionality being offered by new OBD-II port devices (e.g. telemetry tracking for insurance discounts, teen driver tracking), auto manufacturers don't welcome the introduction of unfamiliar products to the vehicle environment

Connected vehicles produce large volumes of data, which introduce challenges. Specifically:

- Telemetry data, which can be used for maintenance tracking or consumer devices plugged into the OBD-II port, must be protected – in motion or at rest – in accordance with regional privacy mandates
- Data transmitted by connected components needs to be authenticated to be sure it's from a trusted source
- Data protection, while essential, must not interfere with analytics

Adding even further complexity, vehicle-to-vehicle and vehicle-to-infrastructure (V2X) communications, although first introduced in 2017 production vehicles, will soon become the norm, requiring manufacturers to identify and implement the necessary technologies. Vehicles in motion will need to be able to securely broadcast and receive telemetry data to and from other participants of the transportation ecosystem.





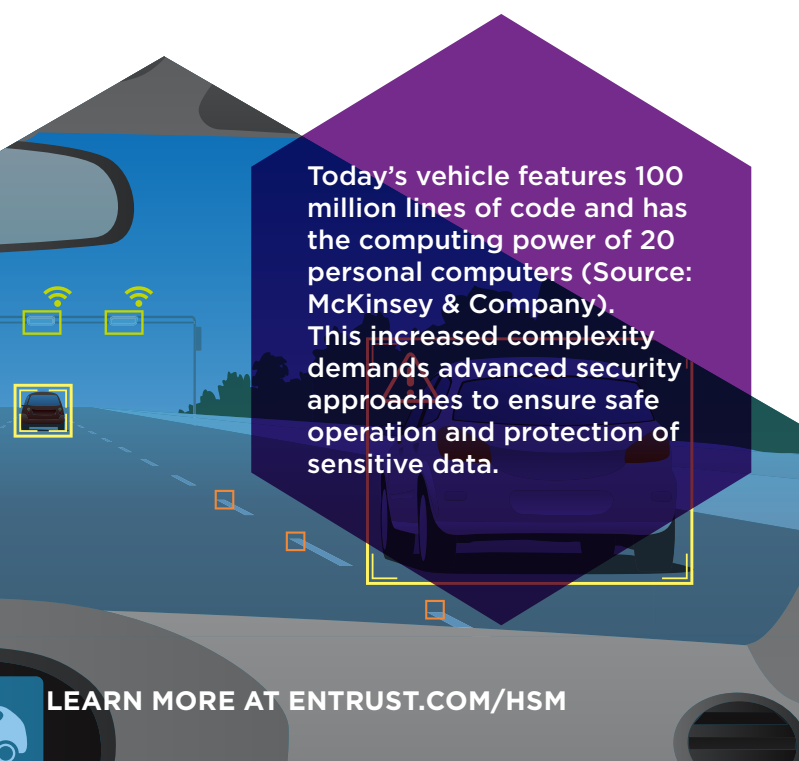
## The solution: Entrust nShield HSMs, code signing and PKI support

To address many of the security challenges posed by modern vehicles, Entrust nShield® hardware security modules (HSMs) enable manufacturers to give each connected component a unique identification – whether it’s introduced during original manufacture or as a replacement. Using the strongest cryptographic processing, key protection, and key management available, this security design enables:

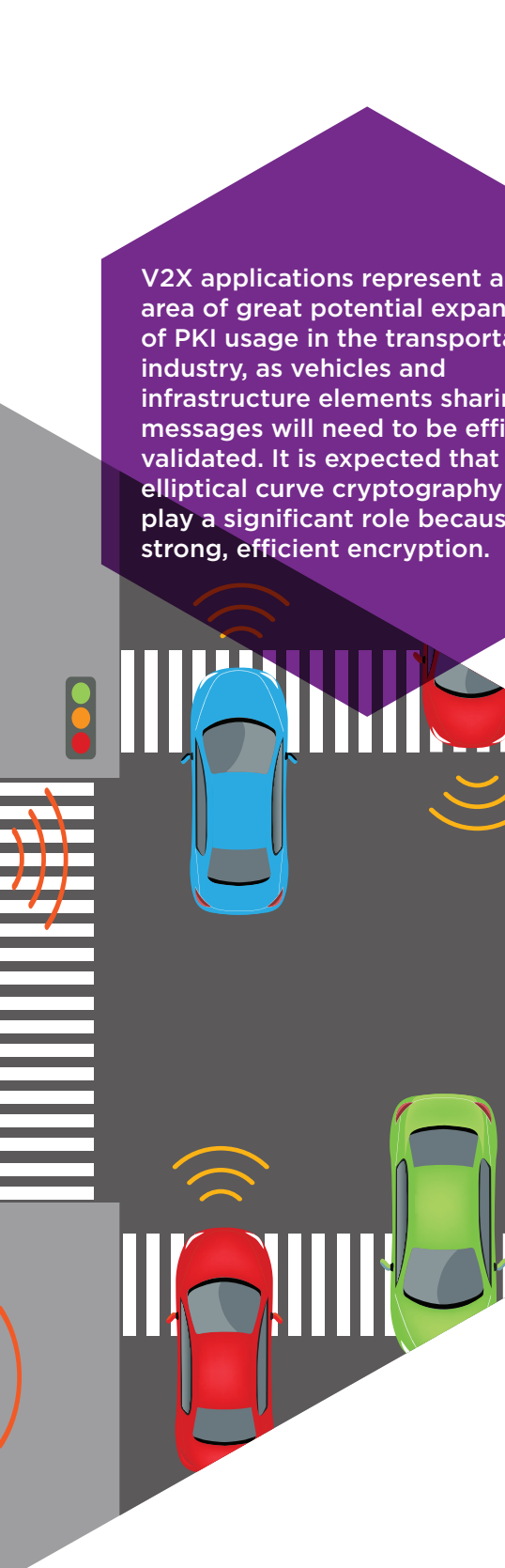
- Strong authentication of each component
- The trusted transmission of telemetry data as part of the V2X ecosystem and for applications such as maintenance tracking
- Authorized code updates
- The foundation for an effective PKI
- Stronger defense against fraudulent and faulty production

The most secure, industry-recognized method for establishing digital credentials for connected components starts by creating and protecting the underlying keys with a hardware security module. Combining the Entrust nShield with supporting security applications, manufacturers can control the provisioning of key material and associated digital certificates, and ensure that each is loaded with only authorized code. You can also defend against counterfeiting by controlling the number of units produced and the code that’s built into each, even in a geographically dispersed supply chain. Further, you can enjoy the added benefit of enhanced quality control by ensuring that all required certificates are in place as part of the vehicle’s final inspection.

With strong authentication in place, components can receive OTA software and firmware updates, presenting a significant opportunity for manufacturers, who could open up new revenue streams and enhance driver satisfaction with the introduction of new features, while reducing the cost of issuing updates.



Today's vehicle features 100 million lines of code and has the computing power of 20 personal computers (Source: McKinsey & Company). This increased complexity demands advanced security approaches to ensure safe operation and protection of sensitive data.

An illustration of a road intersection. A blue car is at the top, a red car is on the right, and a green car is at the bottom. A red car is also partially visible at the top right. Orange and yellow curved lines represent wireless signals emanating from the cars. A traffic light with green, yellow, and red lights is on the left. A purple hexagon is overlaid on the top left of the scene.

V2X applications represent an area of great potential expansion of PKI usage in the transportation industry, as vehicles and infrastructure elements sharing messages will need to be efficiently validated. It is expected that elliptical curve cryptography will play a significant role because of its strong, efficient encryption.

### Entrust's code signing

The best practice to confirm the integrity of code updates and defend against the risks associated with software tampering is to ensure that code is signed using highly secure signing processes with private signing keys protected by HSMs.

Entrust's Code Signing solution combines nShield HSMs with services from Entrust nShield professional services. The nShield provides tamper-resistant, certified protection for your private signing keys and a secure platform to perform critical digital signature processes.

### Support for public key infrastructures

Given the large scale of vehicle manufacturers' and suppliers' operations, they require a solution for managing digital certificates and protecting signing keys. Whether you work with one of our industry-leading PKI partners or tap into our nShield professional services for support, Entrust nShield HSMs enable a PKI that meets your needs, regardless of scale or complexity. By securing the process of issuing certificates and proactively managing signing keys, you prevent their loss or theft, thereby creating a high-assurance foundation for digital security. nShield HSMs are independently certified, tamper-resistant devices that are used to secure some of the most sensitive keys and business processes in the organization—a widely recognized PKI best practice.

## Potential PKI deployments at auto manufacturers might include:

- Ensuring the authenticity of connected components, which include digital certificates injected during the manufacturing process
- OTA updates; software and firmware update package are encrypted and signed, then distributed to fleets of vehicles
- V2X applications. The CA acts as the trusted source for issuing and managing certificates, which validate that the components are authentic

The V2X use case is notable, as it will entail a massive volume of certificates, thus requiring a robust PKI. It is also notable that leading organizations in the transportation community (e.g. US National Highway Transportation Authority; European Commission Joint Research Centre) are endorsing adopting elliptical curve cryptography for V2X because of its strong, efficient encryption.

### Automotive companies trust Entrust

Entrust customers include 2 of the top 3 North American OEMs and two thirds of the leading European suppliers.



## Summary

Entrust nShield HSMs enable car manufacturers to establish a unique identification for each connected component, and protect against the risks of unauthorized connected components and code updates. Entrust nShield HSMs and professional services also help to ensure the integrity, performance, and manageability of manufacturers' PKIs.

Visit [www.entrust.com](http://www.entrust.com) to learn how we can help you advance your vehicle security strategy.

To find out more about  
Entrust nShield HSMs

**HSMinfo@entrust.com**

**entrust.com/HSM**

## ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at  
**entrust.com/HSM**

