



**FORNETIX**

# Protecting the Integrity of Your Vehicles From Initial Production to the Open Road

**THE IMPORTANCE OF EFFECTIVE ENCRYPTION  
MANAGEMENT IN THE AUTOMOTIVE LIFECYCLE**

## Extending the Protection Chain Across Multiple Perimeters

*New technologies are being integrated into automotive OEM products every day as the industry experiences a dramatic demand for connectivity. Experts agree that this paradigm shift has created unique issues surrounding security which leaves vehicles vulnerable to a myriad of cyberattacks. If you think about it, the car in your driveway is a "mobile device" that weighs thousands of pounds and moves at speeds in excess of 200 miles per hour. Protecting this connected device now becomes more than just data security – it means preventing the loss of human life.*

With network boundaries becoming more skewed every day, protecting network architecture is no longer enough. Enterprises must also protect against vulnerabilities and threats that exist outside of the local network — specifically, those that exist within the networks of suppliers, dealerships, and customers themselves. The June 2017 IEEE interview of Dr. Christof Paar<sup>1</sup> explains that vehicle-to-everything (V2X) communications are an exercise in encryption-based authorization controls. V2X encompasses vehicle-to-vehicle (V2V), vehicle-to-dealership, and vehicle-to-infrastructure (V2I).

Another critical aspect of V2X is the introduction of encryption-based controls starting at manufacture and management of those keys through the supply chain of the vehicle. This is critical to provide a baseline for V2X communications by securing the supply chain of the components that provide secure and safe V2X communications. During manufacturing, assets are regularly transferred from one organization to another where they are exposed to threats in environments outside the data owner's control.

## Protecting the Jewels by Incorporating Encryption and Access Control

Despite being useful in some security planning approaches, traditional network security concepts such as defense in depth, perimeter protection, and dwell time don't address specifics based on what keeps a vehicle safe and the vehicle's information secure.

Whether it's healthcare, financials, military secrets, or even a car's entertainment system, the access to valuable data must be governed by security concepts and metrics. Mechanisms must be implemented to protect the vehicle from the point it drives off the assembly line to the point that the car is recycled. This begins with encryption and access control applied during manufacture and encryption management



# Jeep

**Note:** For safety's sake, we will demonstrate encryption solutions using the 2015 Jeep® hack by Miller and Valasek<sup>2</sup> as an example. This provides a practical target that has already been resolved and does not inadvertently expose vulnerabilities that could lead to harm.



### Defense in Depth

A layering tactic that defends a system from attack using several independent methods.

### Perimeter Protection

Refers to systems like routers and firewalls designed to tightly control access to networks from outside sources.

### Dwell Time

The amount of time an attacker is able to act unchecked on a network or resource after the initial compromise or unauthorized access.

<sup>1</sup> <https://cybersecurity.ieee.org/blog/2017/06/28/christof-paar-on-why-cryptography-is-key-for-automotive-cybersecurity/>

<sup>2</sup> <https://spectrum.ieee.org/cars-that-think/transportation/systems/jeep-hacking-101>

applied through the lifecycle of the vehicle. This aligns governance of the vehicle security controls with the need for vehicle-to-vehicle safety messages and certificate exchange.

When considering how vehicle-to-vehicle messages are to be signed and encrypted per standards like IEEE 1609.2, we must determine how the ECDH and ECDSA cryptography is controlled and managed. Not just for the confidentiality of information, but also for safeguarding the format and content of cryptographic information so that safety information can always be accurately relayed between vehicles without compromising the integrity and privacy of the data being relayed.

As approaches like IEEE 1609.2 rely on certificate authorities and intermediate certificate authorities, there is a corresponding need for a secure management framework that allows for controlled distribution of PKI information providing a framework of both trust and management. The need for consistent management from manufacture through end-of-life drives a need to incorporate and align key management with the lifecycle of the vehicle. This maintains the integrity of PKI-based trust as V2X support grows over time. To do otherwise is to introduce systemic brittleness into V2X communications.

In applying key management to vehicles, there is also consideration for telematics, sensors, and the dozens of electronic control units (ECU) that impact system behavior. Applied cryptography enables privacy and confidentiality for



customer information and intellectual property via encryption-based controls. Additionally, encryption-based signatures are used to validate the provenance of the software which supports the integrity of vehicular systems and the data that is being collected. This impacts the safety of the vehicle and provides legal protection for the manufacturers. Much like the V2X communications, there is a need to align management of the encryption with the services that protect information and guarantee the integrity of the software provided by the auto manufacturer. In regard to telematics systems, cryptography is applied in digital rights management, licensing for services such as satellite radio, GPS mapping services, and protection/integrity of communications between telematics and the ECUs on a vehicle's Controller Area Network (CAN bus). As with securing V2X communications, it is essential for key management to be applied from the point of assembly to the product's end of life. This alignment through the supply chain creates an association of the product, the consumer, and the manufacturer ensuring the vehicle provides the appropriate services in a safe and secure example.

## Concepts Applied – The “Acme Anvil Smasher 5000”

Let's imagine the Acme Anvil Smasher is a hypothetical luxury SUV with a hybrid powertrain plus numerous self-driving and safety features. Learning from past mistakes, Acme has invested in Fonetix VaultCore™ technology that allows for the integration of standards-based encryption and encryption key management. Acme extends this ecosystem out to its suppliers so subcomponents for telematics, sensors, and V2X communications can leverage secure integrated encryption services. It extends further to dealerships, customers, and secondary services like mechanics or independent used car sales.

## Making the Anvil Smasher

At the factory, the SUV is assembled and seeded with initial software. Additional third-party software is validated using Verify operations on the VaultCore appliance. The SUV receives its initial load of cryptographic material used for identity, authentication, verification, and authorization. At this beginning stage, the VaultCore appliance provides services that coordinate

the delivery of software with a named device, aligning manufacturing and software support through organization of IEEE 1609.2 IoT cryptography-based identity, authentication, and authorization services. Additionally, the associated key material for signing is applied to the software loaded onto the SUV so software updates can continue to be validated before use on the vehicle.

In our Jeep hack example, this is where the problems started. The seed value for WPA2 authentication of the vehicle's wireless network used system time as the cryptographic seed for the password. On startup, however, all the devices had the same time within a few seconds. If the Jeep telematics system had used a random seed value securely received from a VaultCore appliance, the number of passwords to try would have jumped from roughly a dozen to tens of millions. The other loaded keys for authentication on the Anvil Smasher for ECUs and sensors further limit the value of the Jeep hack as the attempts to update firmware would have had to circumvent signature verification on the corrupt software.

## From the Factory to the Driveway

The Anvil Smasher 5000 has a brand-new owner who is ready to experience all of the performance, security, and safety that comes from an orchestrated, connected car. As part of the buying process, the new owner interacts with a customer management system associated with the Anvil Smasher to provide information linking the SUV with the



new user. Acme's customer management system then prompts the VaultCore appliance to create a user account and associate that connection with the newly purchased vehicle. Cryptographic material for V2X comms, system integrity, and customer privacy are now associated with both the vehicle and the owner.

During the lifetime of the Anvil Smasher 5000, Acme continues to provide software updates associated with the SUV using cryptographic material and encryption/validation services provided by the VaultCore appliance. This includes having security controls in place that allow for safe and scalable over-the-air software updates.

In the Jeep scenario, the same controls that would prevent cracking WPA2 passwords or installing corrupt software remain in place as the vehicle continues to operate. Though the Jeep does not use V2X communications, the same type of encryption and integrity controls extend to IEEE 1609.2 wireless access. It's worth noting that Jeep owners had to go to the dealership

to have their software updated. Using the control and cryptographic security provided by VaultCore, over-the-air software updates would reduce vulnerabilities by increasing the adoption rate compared to a consumer who does not respond to in-person recalls from the dealer.

## When the Anvil Smasher Smashes No More Anvils

Over the next several years, the SUV may change hands, more mechanics might want to affect repairs on the vehicle, and the owner might just want to go to Jiffy-Lube® instead of the dealership for oil changes. In all of those circumstances, having control of the cryptographic material provides options in regard to making the maximum use of features while creating secondary markets for secure maintenance software used by mechanics and service shops. Finally, it is the accountability of knowing that when the Anvil Smasher is no more, Acme has traceability on what happened to its software – and they might even have a chance to sell it to someone who will like to work with “classic” cars.

## The Road Ahead for Secure Connected Vehicles

As for Jeep, or anyone else for that matter, this is uncharted territory. Solutions for V2X and system controls for secure communications and software integrity are only starting to come to the market. How these technologies change and adapt over time will be driven by technical, societal, and political changes. What can be certain is that a robust encryption ecosystem will ensure you're always ready. We believe VaultCore is the answer to securing connected vehicles both today and in the future.

## How Foretix and VaultCore Can Help

Foretix is helping organizations unleash the full potential of encryption by conquering the key management bottleneck. Our VaultCore ecosystem automates the key lifecycle across the entire enterprise with groundbreaking precision and speed.




Foretix is working with Micron to implement solutions for supply chain integrity. The innovation of Micron Authentia embedded memory solutions coupled with the scale, security, and ease-of-use of Foretix VaultCore. Both Micron and Foretix are committed to bringing standards-based security to the automotive industry.

As global use of encryption rapidly expands, you can be prepared for the future with unparalleled capacity and scalability. Our commitment to standards-based interoperability ensures your existing investments in encryption are fully realized and will continue to integrate seamlessly as your organization grows. Policy-driven automation of the key rotation lifecycle reduces human error and empowers your organization to remain secure and avoid costly data breaches.

If you're ready to orchestrate your encryption key management, we'd love to hear from you. Please call 1-844-539-6724 or visit [www.foretix.com](http://www.foretix.com) for more information.



## Find Out More About Foretix

-  [Foretix.com](http://Foretix.com)
-  [Facebook.com/foretix](https://Facebook.com/foretix)
-  [Twitter.com/foretix](https://Twitter.com/foretix)
-  [Linkedin.com/company/foretix](https://Linkedin.com/company/foretix)
-  1-844-539-6724
-  5728 Industry Lane,  
Frederick, MD 21704

For more information, please contact [marketing@foretix.com](mailto:marketing@foretix.com)