# Denying Hackers:
## *Unlocking Security Key Technology for Automated Vehicles*

MARK PETERS
Director, Automotive Business Development
OnBoard Security Inc., a Qualcomm Company

**Contents**



## INTRODUCTION

### Unlocking Security Key Technology for Automated Vehicles

As vehicles have become more complex, particularly with the development of automated vehicles, so has the issue of automotive cybersecurity. In particular, how will the security be assured of so many connected components in modern vehicles? How will automotive manufacturers protect their own proprietary systems while leaving them open enough to work with others? How will data providers protect their networks against attacks generated from a breached component in a single vehicle? How will manufacturers protect individual drivers from hackers who would seize control of a vehicle's components, much like the 2015 Jeep Cherokee incident where hackers exploited a vulnerability in the vehicle's connected entertainment system?

Without robust cybersecurity for vehicles, systems, and infrastructure, a viable mass-market for technologically advanced vehicles simply won't exist. Mcity researchers previously explored the nature of security threats and the vast landscape of potential risks in a 2018 whitepaper, "Assessing Risk: Identifying and Analyzing Cybersecurity Threats to Automated Vehicles." Now, new Mcity research zeroes in on one especially significant aspect of securing all modern vehicles: key management systems.

## SECURITY KEYS AND KEY MANAGEMENT

Modern vehicles need cryptographic keys for security. These are the small bits of information that safely determine the functional output of software applications. Currently there is no uniform process for key generation:  manufacturers design the vehicle and suppliers put together the required individual connected components, all of which require security keys. Each automaker has a completely different approach to working with suppliers; either the automakers create their own keys or have the suppliers create keys, resulting in no standard way to share and transmit these digital security codes. With each manufacturer depending on a network of up to 20 suppliers – who also provide components to other manufacturers – the key management process can quickly become an inefficient, expensive, and potentially insecure mess involving dozens of different key management approaches for any one vehicle.

"As cybersecurity is becoming more and more important for vehicles now, it's requiring developers to find ways to better secure the vehicle," said Mark Peters, one of the project's leaders and director of business development for OnBoard Security Inc., a Qualcomm Company, and Mcity Affiliate member. "Part of that is making sure that when you download software to a vehicle or one of its components, that it's the correct software and that it's coming from the right place. The way to do all of that is using, essentially, digital keys."

Coordinating those individual keys is where key management comes in.

Key management is administration of creation and subsequent activity associated with using cryptographic security keys within a system; this includes their storing, updating, and verification. Key management systems outline the definitions, protocols, and standards for creating and managing the digital keys used throughout a network. A secure and consistent key management system is an essential component for creating a secure and viable data and communications infrastructure to ensure the dependable operation of vehicles.

Automated vehicles will require dozens of these cryptographic keys, and even more as each new feature and function is added. At the moment, manufacturers and suppliers are using a variety of key management solutions to secure disparate systems, creating a situation where each company would need to install and manage a variety of keys and systems; creating complexity, incompatibility, and inefficiencies, as well as adding cost to the development and manufacturing of vehicles.

To illustrate this situation, imagine a family of five where each person uses their own individual kind of lock to enter their home. One person uses a standard key, another a fingerprint scanner, a third a combination lock, a fourth an iris scanner, and the fifth a digital keypad. The upshot of trying to accommodate each individual's key system means that either they use five different doors to enter the home, each person uses all five means to unlock the house, or they all agree on one particular standard for the keys they will use. The last is the obvious choice, but not necessarily the easiest one to implement.

## THE MCITY RESEARCH

Mcity researchers set out to solve the problem by creating one single, objective key management standard for automakers and suppliers to use across the industry. This standard would define how security keys are manufactured, which party is responsible for generating new keys, and how they are transmitted between automakers and their suppliers. The team approached the challenge by identifying four tasks:

- Identify use cases and relevant existing standards
- Specify requirements for all use cases
- Create technical specifications
- Initiate standardization

Let's take a closer look at each task.

### Task 1: Identify use cases and relevant existing standards

Researchers began the project with an initial survey of the many different key standards and products being used throughout the industry. They found a vast number of products and producers that forced the researchers to limit the study to auto manufacturers and top tier suppliers, known as Tier 1 suppliers.

"The biggest surprise was how quickly key management can go back through many layers," Peters explained. "There can be different requirements between the Tier 1 suppliers and their sub-suppliers, all the way down to the firms that make the semi-conductors. We felt that was far beyond what we could get our arms around and still be able to produce anything meaningful in the time period we were working with."

The team also found that each manufacturer was already approaching key management in ways that fit their needs, with some manufacturers and larger Tier 1 suppliers working far ahead of others in the industry, especially those with more experience dealing with cybersecurity issues. While older devices currently on the road lack security protections, most new components include some type of security provision.

As expected, the different uses, needs, and range of approaches was extremely diverse. Some manufacturers ordered keys and retrieved the source, while others generated the keys and distributed them to users. There were instances where key management was synchronized between manufacturers and suppliers, and others where the process was asynchronous. And while some key management processes were more centralized than others, every manufacturer utilized its own unique processes for supply chain logistics.

The survey also identified a few critical issues, such as the need to create a secure association with each electronic control unit, as well as finding that vehicle codes to lock and unlock specific features would be an essential security issue.

**Task 2: Specify requirements for all use cases**

After conducting workshops and surveys, Mcity researchers examined the situations where cryptographic keys would be used, then refined the list of use cases to a set of instances calling for key management. The team then produced a "concept of operations" document focusing on the functions and uses of key management in vehicles, and the relationship between key management and other security issues.

By drilling down to examine the key management use cases between manufacturers and products from Tier 1 suppliers, the team refined a list of factors involved in key management with the goal of creating a protocol to cover all the identified use cases that would work for all manufacturers. The main objective was to overcome the biggest obstacle the team identified in current key management systems – creating interoperability between all suppliers and manufacturers.

**Task 3: Create technical specifications**

With that in mind, Mcity researchers refined their findings to nine use cases covering key management issues in vehicles. They then looked to develop the technical requirements that would create a truly shareable solution that could be used to create industry standard protocols. The team documented all the basic use cases, recognizing that the business flows were different for each manufacturer, including supply chain and logistics, and set about finding a way to eliminate the myriad overlapping and conflicting key management systems currently in use.

Rather than start from scratch, the researchers first investigated whether an already existing protocol could be used as a starting point that could then be extended to the auto industry. What they discovered was the Key Management Interoperability Protocol, or KMIP, first released in 2010 by the Organization for the Advancement of Structured Information Standards (OASIS.) OASIS is a global nonprofit consortium focused on the adoption of open standards for security, Internet of Things, energy, content technologies, emergency management, and other areas.

According to OASIS, the KMIP is, "A single, comprehensive protocol for communication between clients that request any of a wide range of encryption keys and servers that store and manage those keys. By replacing redundant, incompatible key management protocols, KMIP provides better data security while at the same time reducing expenditures on multiple products."

KMIP manages objects, including cryptographic keys and digital certificates; defines their attributes, including unique identifiers; outlines actions; and manages links between keys, managed units, and operations. KMIP utilizes several other established standards and has become the dominant key management standard, with more than 40 companies offering commercial KMIP Products, including Dell, HPE, IBM, NetApp, Oracle and RSA.

By providing KMIP profiles that establish basic standards for interoperability, KMIP ensures that key servers and clients all provide:

- A minimal set of cryptographic algorithms to interoperate and manage
- Ability to engage an interoperable secure session
- Interoperable KMIP protocol encodings
- Interoperable key lifecycle designations
- Ability to manage opaque objects

With KMIP as a foundation, Mcity researchers could augment the existing profiles to include specific auto-industry objects, attributes and operations in a way that allows each manufacturer to adopt and configure the process to its own business practices.

"As we talked through this with all the manufacturers and Tier 1 suppliers, we found that the specification OASIS developed covered 90 percent of everything that we needed to create for automotive key management systems," Peters said. "All we needed to do was create profiles for the automotive industry that fit in with the KMIP basic specifications. We believe that this type of implementation will end up being a more

secure implementation than one where lots of companies are trying to do something on their own."

**Task 4: Initiate standardization**

Beyond this first effort, the next step in the project is to pass this newly developed specification to an existing standards organization that can further develop and implement the interoperability of an automotive KMIP system. The Mcity team has already arranged to work with SAE International to set-up the Vehicle Security Credentials Interoperability (VSCI) committee.

Once a standard protocol for interoperability is adopted, it will be pushed down through the supply chain, from manufacturers and Tier 1 suppliers, to other suppliers and vendors. In the case of automated vehicles, the standardized key management system protocol also will need to be coordinated across other aspects of vehicle operation to work with data providers – such as mapping and GPS systems – as well as roadside infrastructure networks.

At this point, manufacturers can now incorporate the Mcity team's use cases and extensions into their own supply chain practices. Manufacturers can:

- Develop their own client/server implementations according to KMIP and the Mcity profile
- Develop their own interoperable KMS/KMIP adapters
- Utilize existing off-the-shelf and commercial libraries
- Purchase and customize existing commercial KMIP server implementations
- Contract their own KMS equipment providers to augment systems with these interfaces

## CONCLUSION

The adoption of a unified, interoperable system to manage crypto keys in self-driving vehicles is a major component in achieving the very high level of cybersecurity needed to make autonomous vehicles successful. The current system of widely varying key management approaches can only add time, complexity and cost to vehicle development, while also creating security risks and threatening the dependability of these vehicles. Consumers will need to know that self-driving cars can't be hacked, breached or exploited

by scammers, data thieves or terrorists, and that the myriad of components and control units in each vehicle will work reliably and efficiently to safely get them to their destinations.

The Mcity research on key management has jump-started what is typically a years-long process to develop a global industry standard. Instead, the key management standard, which the automotive industry agrees is vital to the successful development of secure vehicles, could be adopted within a year after SAE issues a final specification.

## NEXT STEPS

This research is an example of the kind of collaborative, pre-competitive work with industry partners and researchers we do at Mcity to address the challenges in developing a viable working system of connected and automated vehicles.

If you are interested in the process of advancing the standards that this initiative inspired, please reach out to SAE's Vehicle Security Credential Interoperability Task Force.

***About Mcity***

*Mcity at the University of Michigan is leading the transition to connected and automated vehicles. Home to world-renowned researchers, a one-of-a-kind test facility, and on-road deployments, Mcity brings together industry, government, and academia to improve transportation safety, sustainability, and accessibility for the benefit of society.*