KEYFACTOR
SECURE EVERY DIGITAL IDENTITY

AUTOMOTIVE INDUSTRY USE CASE:

Scalability & Security Drive a Home Run

The promise of connected vehicles is tremendous - and so are the security measures required to keep drivers safe and maintain brand integrity. Highly complex, integrated systems from multiple vendors, often with legacy standards, equipment and infrastructure, make the automotive industry a presumably easy target for malicious actors. Security must be a top priority—bolstered by a strong foundation of digital identity management. Ensuring this underpinning is ready for the projected magnitude of IoT deployments is the difference between success and failure.

THE CHALLENGE

Every manufacturer faces the same challenge: keeping consumers interested, invested and loyal. For automotive manufacturers, that connection is critical. Pricepoints are high, time between first and next purchase is long, and keeping passengers safe every time they shut their doors is imperative. Driving innovation in a fast-paced, demanding market is a clear goal with a lot of complexity. Navigation, entertainment options, mobile connectivity, voice activated search, and push communications are just a few attributes consumers look for when they're making such a big purchase. Then there's the next level of advancement—self-driving and autonomous vehicles. Throughout it all, security must be the very first word spoken behind every feature and function across every vehicle.

There are serious financial consequences from a warranty return if the automaker can't remotely update its fleet. A large automotive manufacturer recently requested Keyfactor™ to engage in a scenario that would push the limits of what security means, helping to determine how managing a security breach successfully from afar could work ... or not.

THE PILOT

Keyfactor performed a pilot designed to secure a large fleet of simulated connected vehicles. The premise was based on a catastrophic re-enrollment scenario where the Root of Trust (RoT) was breached. The goal was to validate the ability to handle revocation & reissuance of 500 million certificates, and understand the time it would take to complete.

The set-up: All vehicles required an immediate update consisting of new certificates and keys from a new CA. The update of each device's trust store would replace the compromised root and shut off trust of its certificates. Keyfactor Control served as the orchestration layer between a third-party PKI and Keyfactor Control agents deployed on each vehicle Engine Control Unit (ECU).

The pilot ran in the Microsoft Azure cloud, on a single instance of Keyfactor Control running one standard-grade quad-core web server and one standard-grade 16-core database server.

> At this processing rate, it was estimated that the replacement for a typical two tier PKI (two chain certificates plus the end entity certificate) would operate at two million vehicles per-hour, excluding the time needed to actually issue the certificates from the certificate authority.

FINDINGS

The successful pilot demonstrated the ability to store, manage, and report on over 211 million certificates, and provided instructions to an equivalent load of 68 million vehicle agents checking in once per-day. Aggregate Keyfactor Command and Keyfactor Control rate processing rate with the single back end server was 800 operations per-second.

At this processing rate, it was estimated that the replacement for a typical two tier PKI (two chain certificates plus the end entity certificate) would operate at two million vehicles per-hour, excluding the time needed to actually issue the certificates from the certificate authority.

With a single backend Keyfactor Control server generating the above load, the underlying database was running at about 10% load. Performance scaled up linearly as more server capacity was added. Scaling the numbers by four times would generate a check-in rate of 3,200 per-second and keep the database load reasonably under 50%. Such scaling would process four million vehicles per-hour or 96 million vehicles a day, allowing all 500 million vehicles to have their PKI infrastructure replaced in a week.

TAKEAWAYS

Digital certificates were originally adopted within data centers and web farms followed by personal and network devices to secure the Intranet. With the IoT now mainstream, PKI's new assignment is to secure millions of devices, leading the convergence of information technology (IT) and operational technology (OT) security.

Including identity and security into a device shouldn't be an afterthought — it should be rooted in the design.

Scalable security is a key factor in ensuring your entire product line runs smoothly and has a prolonged shelf life. When you own a product line, there is nothing more meaningful, or more challenging, than securing every product on a global scale. Whether it is a controlled update, a new certificate configuration, or an unexpected breach, it's critical to stay on top of your entire device fleet.

Authentication, authorization and encryption are the lifeblood of successful digital identity security. Unique digital certificates validate that a device is authentic and assert with high assurance that its messages are genuine. The end user is counting on you to build a product that will stay secure every day, during every use.

*In this case, we tested the platform's ability to provide the connectivity, not the third-party CAs ability to issue certificates.

CONTACT US

- keyfactor.com
- 216.785.2990