cpl.thalesgroup.com

THALES
Building a future we can all trust

APAC Automotive Technology Manufacturer Digitally Secures Supply Chain

A large automotive technology supplier, which provides solutions for multiple automotive manufacturers in the Asia Pacific region, was going through a process of extensive digitalization, which included widespread adoption of internet of things (IoT) connected devices.

IoT now plays an extensive role in automotive manufacturing including connected cars, automotive maintenance systems, autonomous vehicles, in-vehicle infotainment and telematics, fleet management, and more. The addition of IoT infrastructure into manufacturing environments can help reduce manufacturing costs, improve supply chain efficiencies, and proficiently manage device lifecycles. However, because these applications are dependent on communication with the internet, they are also susceptible to hacking.

Challenge

This large automotive technology supplier needed to secure the supply chain for important automotive components to protect them from external hacking, malware, and loss of confidential information. To achieve this the supplier's IT team recognized the organization needed complete, on-premises control of cryptographic key management.

What is more, the solutions would need to be flexible enough to be implemented in multiple locations, given the distributed supply chain arrangements of auto manufacturers, and support multiple original equipment manufacturers throughout Asia Pacific.

Solution

The automotive technology supplier decided to work with Thales because it has decades of experience with every aspect of data security the supplier wanted to address.

The automotive supplier's digital security team put in place a FIPS 140-2 Level 3 validated Thales ProtectServer hardware security module (HSM) as root of trust for cryptographic keys. The ProtectServer HSM supports NIST SP800-90 TRNG and is deployed on-premises to generate cryptographic keys.

The ProtectServer HSMs include a cryptographic module that performs high assurance secure cryptographic processing. The appliances feature heavy-duty steel cases with tamper-protected security that safeguards against physical attacks. They deliver the highest levels of physical and logical protection to the storage and processing of highly sensitive information, such as cryptographic keys, personal identification numbers, and other data. Consequently, cryptographic keys are never exposed outside the HSM in clear form.

The ProtectServer HSM offered the automotive technology supplier a level of security unavailable from software alternatives, while providing a certified level of confidentiality and integrity that meets the security demands of government regulations and industry organizations.

Results

This Asia-Pacific automotive technology supplier was able to digitally secure manufacturing and its supply chain by:

- Creating a flexible Public Key Infrastructure (PKI) and HSM operation through the combination of on-premises deployment at multiple manufacturing and supplier locations as needed to meet operational requirements.
- Securing manufacturing with reliable on-premises control of cryptographic key management for automotive components throughout the supplier's entire manufacturing operation.
- Ensuring seamless deployment globally with entire supply chains in both manufacturing sites and external suppliers in multiple countries.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us