cpl.thalesgroup.com

THALES
Building a future we can all trust

亚太汽车技术制造商以数字方式确保供应链安全

一家为亚太地区多家汽车制造商提供解决方案的大型汽车技术供应商正在经历一个广泛数字化的过程，其中包括广泛采用物联网（IoT）连接设备。

IoT 现在在汽车制造中发挥着广泛的作用，包括联网汽车、汽车维修系统、自动驾驶汽车、车载信息娱乐和远程信息处理、车队管理等。将物联网基础设施添加到制造环境中可以帮助降低制造成本，提高供应链效率，并便捷地管理设备生命周期。然而，由于这些应用程序依赖于与互联网的通信，它们也容易受到黑客攻击。

挑战

这家大型汽车技术供应商需要保护重要汽车部件的供应链，以保护它们免受外部黑客攻击、恶意软件和机密信息的丢失。为了实现这一点，供应商的 IT 团队认识到组织需要对加密密钥管理进行完整的本地控制。

此外，鉴于汽车制造商的分布式供应链安排，这些解决方案需要足够灵活，以便在多个地点实施，并支持整个亚太地区的多个原始设备制造商。

解决方案

这家汽车技术供应商决定与 Thales 合作，因为它在供应商所需的数据安全各个方面都有几十年的经验。

汽车供应商的数字安全团队将 FIPS 140-2 三级验证的 Thales ProtectServer 硬件安全模块（HSM）作为加密密钥的信任根。ProtectServer HSM 支持 NIST SP800-90 TRNG用以在内部生成加密密钥。

ProtectServer HSM 包括一个加密模块，用于执行高度安全的加密操作。该设备采用重型钢制外壳，具有防篡改安全措施，防止物理攻击。它们为高度敏感信息的存储和处理提供了最高级别的物理和逻辑保护，如加密密钥、PIN码和其他数据。因此，密钥永远不会以明文形式暴露在 HSM 之外。

ProtectServer HSM 为汽车技术供应商提供了软件无法提供的安全级别，同时提供了满足政府法规和行业组织安全需求的满足认证要求的保密性和完整性等级。

结果

这家亚太汽车技术供应商能够通过以下方式实现制造及供应链的数字化安全：

- 根据需要，通过在多个制造基地和供应商设施的本地部署的结合，创建一个易操作的公钥基础设施（PKI）和 HSM 操作，以满足运营需求。
- 在供应商的整个生产过程中，通过对汽车零部件的加密密钥管理进行可靠的本地控制，确保生产的安全。
- 确保在多个国家的制造基地和外部供应商的整个供应链在全球范围内无缝部署。

关于 Thales

您依赖能够保护您隐私的专业人员，而他们都依赖 Thales 来保护数据。当涉及到数据安全时，企业面临越来越多的决定性时刻。从建立加密策略，迁移到云端，到满足合规性要求，面临这些决策时刻时，您都可以依靠 Thales 来保障您的数字化转型。

为决策时刻提供决定性技术。