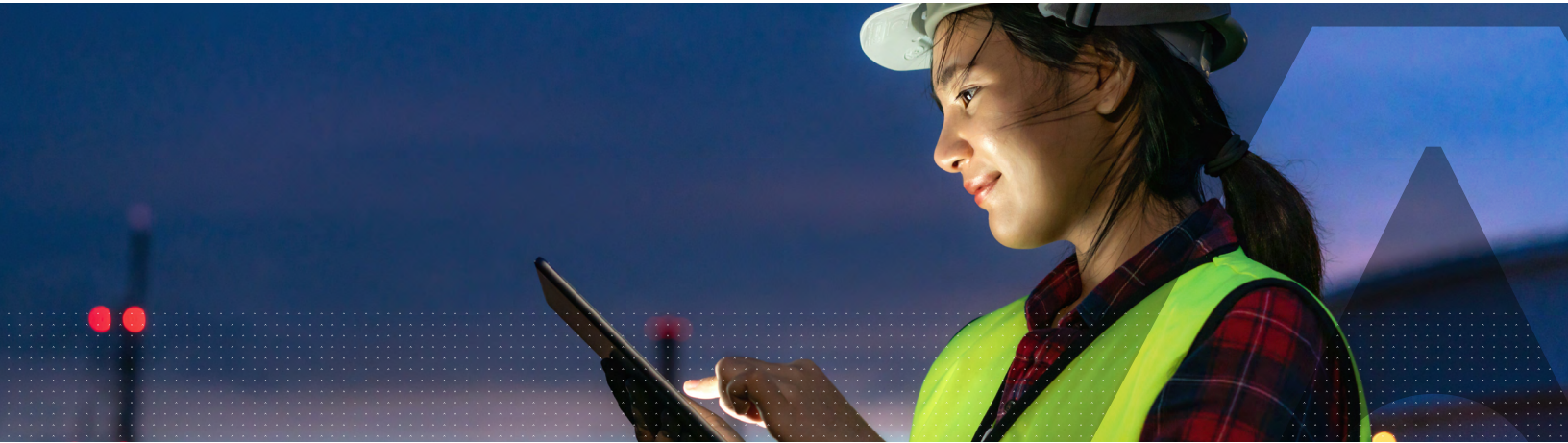


Secure Manufacturing



Overview

While remote or offshore manufacturing sites have their benefits, they also carry with them additional levels of risk since the security standards at these sites are not the same level as within the corporate network. Implementing a secure manufacturing environment requires protecting intellectual property (IP), device identity issuance and assurance, issuing and verifying certificates, and a strong network for communications. Additionally, with rising global inflation and supply chains issues, it is critical that CIOs reduce manufacturing costs and improve supply chain efficiencies by securing their manufacturing sites.

Common risks in with manufacturing:

- Remote or offshore sites
- Loss of IP
- Production of black-market replicas
- IP laws are not equally enforced globally
- Difficulty scaling or controlling production quantities
- Updating settings, configurations, credentials, and firmware of devices in the field

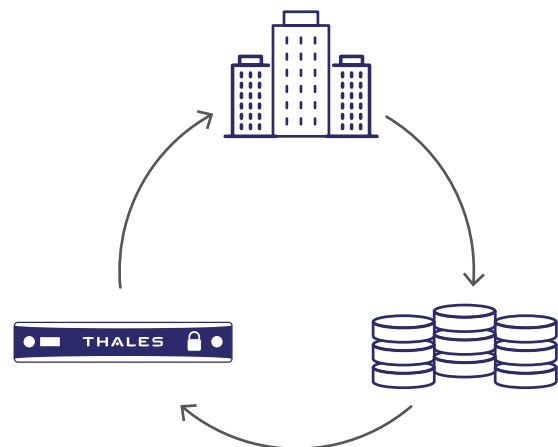
Security threat

- Privacy of IP data
- Limits on quantities or license features added at manufacturing time
- Authentication of manufactured components once deployed

- Enforcement of policy and procedures , especially at distributed operation sites

Thales value

With Thales Luna HSMs, whether on-premises, in the cloud or a hybrid environment, manufacturers are able to leverage the HSM for centralized control to all locations, as well as customize features to each manufacturing environment. In addition, Luna HSMs offer high availability, load balancing, and scalability and support suitable for both local and distributed operations. Importantly, Luna HSMs are crypto agile, giving the flexibility to choose whichever crypto is needed.



Benefits

- Specialized cryptographic electronics offload processing from the host system
- Protection of IP, particularly at remote or offshore manufacturing sites
- Greater control of manufacturing process
- Remote operational control with cryptographic policies, regardless of distance
- Cost reduction
- Improved time to market
- Improved quantity capabilities
- Improved quality
- Secure communications and device certifications
- Protection of the entire device identity life-cycle
- Streamlined management for device updates

Role of HSMs

HSMs are used throughout the manufacturing infrastructure to secure channels of communication, sign components, authenticate devices in the field, and protect the certificate issuance root keys. Using a Hardware Security Module (HSM) for key protection and management ensures the IP is protected both internally and amongst third parties who may or may not have their own security policies.

Since each manufacturing environment is different, Luna Functionalities Modules (FM) will enable manufacturers to customize their features/logic.

High availability and load balancing features assure production uptimes and efficient performance rates that will not bog down systems. In addition, the crypto agility of Luna HSMs enables the customer to use different key types such as ECC, which allows for smaller signed data footprints for constrained devices.

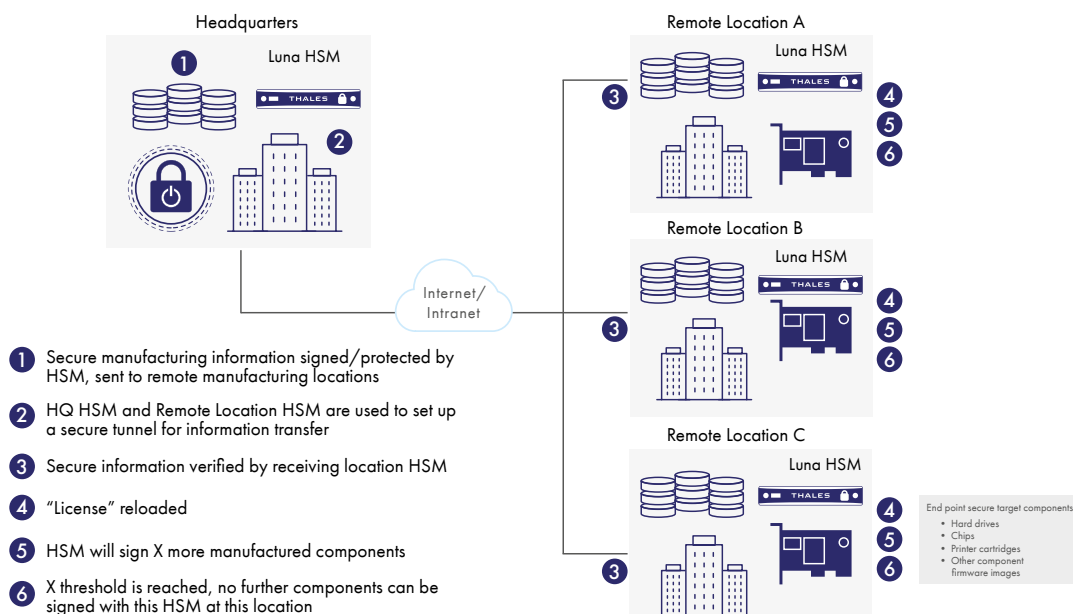
Use case





In order to guard against forgery, many manufacturers are relying on HSMs to protect their intellectual property, such as chips, hard drives, printer components, as well as protect against lost revenue. One manufacturer wanted to protect their phones from snooping, identity forgery, and other forms of network abuse that plague the cellular phone and satellite television industries. An IP phone manufacturer needed to integrate secure identification and authentication into its devices. The business also needed to integrate the issuance of digital identities and authentication into its manufacturing processes, which meant the organization would need to securely and cost-effectively create thousands of industry compliant digital identities.

The IP telephone manufacturer selected Microsoft Certificate Services software for managing the issuance of the digital identities, but needed a proven solution to deliver maximum security and performance. A highly secure hardware system was required to protect the certificate issuance root key—the basis of trust for all of the IDs issued to the phones—and prevent the possibility of a copy of that key being used to create illegitimate device identities. The solution also had to meet high performance standards to ensure that the computationally-intensive certificate issuance process did not create bottlenecks in the manufacturing process.

The manufacturer selected Luna HSM as the foundation for their digital identity issuance system for IP telephones. Their selected Luna HSM held both FIPS 140-2 and Common Criteria certifications, critical for compliance and auditing. With each IP telephone containing a unique, trusted digital identity, the manufacturer and its customers can be sure that the IP telephone they are connecting with is definitely the telephone it claims to be. The flexibility, scalability, and easy manageability of Luna HSMs provided this IP telephone manufacturer with a seamless integration of high-volume, high-speed digital ID issuance into its manufacturing process while maintaining full security.

Production Deployment



> cpl.thalesgroup.com <    

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