thalesgroup.com

THALES

Secured Manufacturing

Overview

The goal of implementing a secured manufacturing environment is to protect intellectual property (IP). With a projected year over year increase in IT spend of 3.6%, companies are moving towards secured manufacturing environments in an effort to reduce manufacturing costs, improve supply chain efficiencies, and protect their IP.

Risks/concerns with offshore manufacturing:

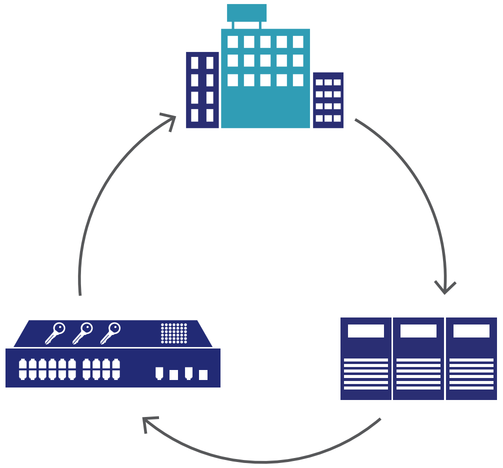
- Lack of control
- Loss of IP
- Production of black-market replicas
- IP laws are not equally enforced globally
- Complexity increases with distance
- Language barriers

Security threat

- Privacy of IP data
- Authentication of manufacturing tools
- Limits on manufacturing quantities
- Limits on license features, added at manufacturing time
- Authentication of manufactured components once deployed
- Enforcement of policy and procedures

Thales value

With Thales Luna HSMs, manufacturers are able to leverage the HSM for centralized control to remote locations, as well as customize features to each manufacturing environment. In addition, Luna HSMs offer high availability, load balancing, and ECC key limit size constraints for smaller crypto footprints, to ensure production uptimes and efficient performance rates that will not bog down systems.



Benefits gained

- Specialized cryptographic electronics offload processing from the host system
- Protection of IP
- Control of manufacturing process
- Remote operational control with cryptographic policies, regardless of distance
- Cost reduction
- Improved time to market
- Improved quantity capabilities
- Improved quality

HSM's role

Using a Hardware Security Module (HSM) for key protection and management ensures the IP is protected both internal and amongst third parties who may or may not have their own security policies. In addition, Thales Remote PED will provide centralized control.

Since each manufacturing environment is different, Luna Functionalities Modules (FMs) and the Luna Java applet will allow manufacturers to customize their features/logic.

High availability and load balancing features will assure production uptimes and efficient performance rates that will not bog down systems. In addition, next generation HSMs will include ECC keys limit size for smaller signed data footprints.

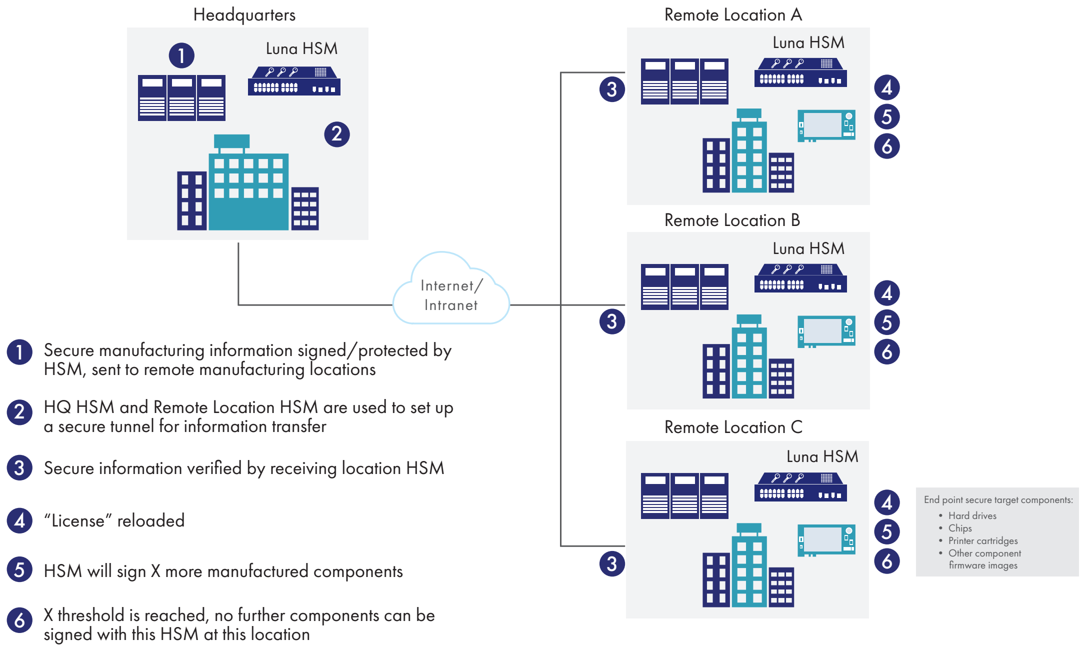
Use case

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 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 hardware 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 certification. With each IP telephone containing a unique, trusted digital identity, users can be sure that the IP telephone they are connecting with is definitely the telephone it claims to be. This IP telephone manufacturer's use of Luna HSMs demonstrates how high-volume, high-speed digital ID issuance can be seamlessly integrated into the manufacturing process without sacrificing security.

Production Deployment



1 Secure manufacturing information signed/protected by HSM, sent to remote manufacturing locations

2 HQ HSM and Remote Location HSM are used to set up a secure tunnel for information transfer

3 Secure information verified by receiving location HSM

4 "License" reloaded

5 HSM will sign X more manufactured components

6 X threshold is reached, no further components can be signed with this HSM at this location

End point secure target components:

- Hard drives
- Chips
- Printer cartridges
- Other component firmware images

> thalesgroup.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com