Hardware Security Modules

What they are and why it's likely that you've (indirectly) used one today

RWC 2015
Paul Hampton
8th January 2015

What Am I Going to Talk About?

What Is A HSM?

Where Will I Find One?

SafeNet

A Hardware Security Module is…

…a dedicated crypto processor…

…designed for the protection of keys throughout their lifecycle…

…validated as secure by third parties…

…a Trust Anchor…

SafeNet

A Hardware Security Module is…

…a source of high quality random numbers…

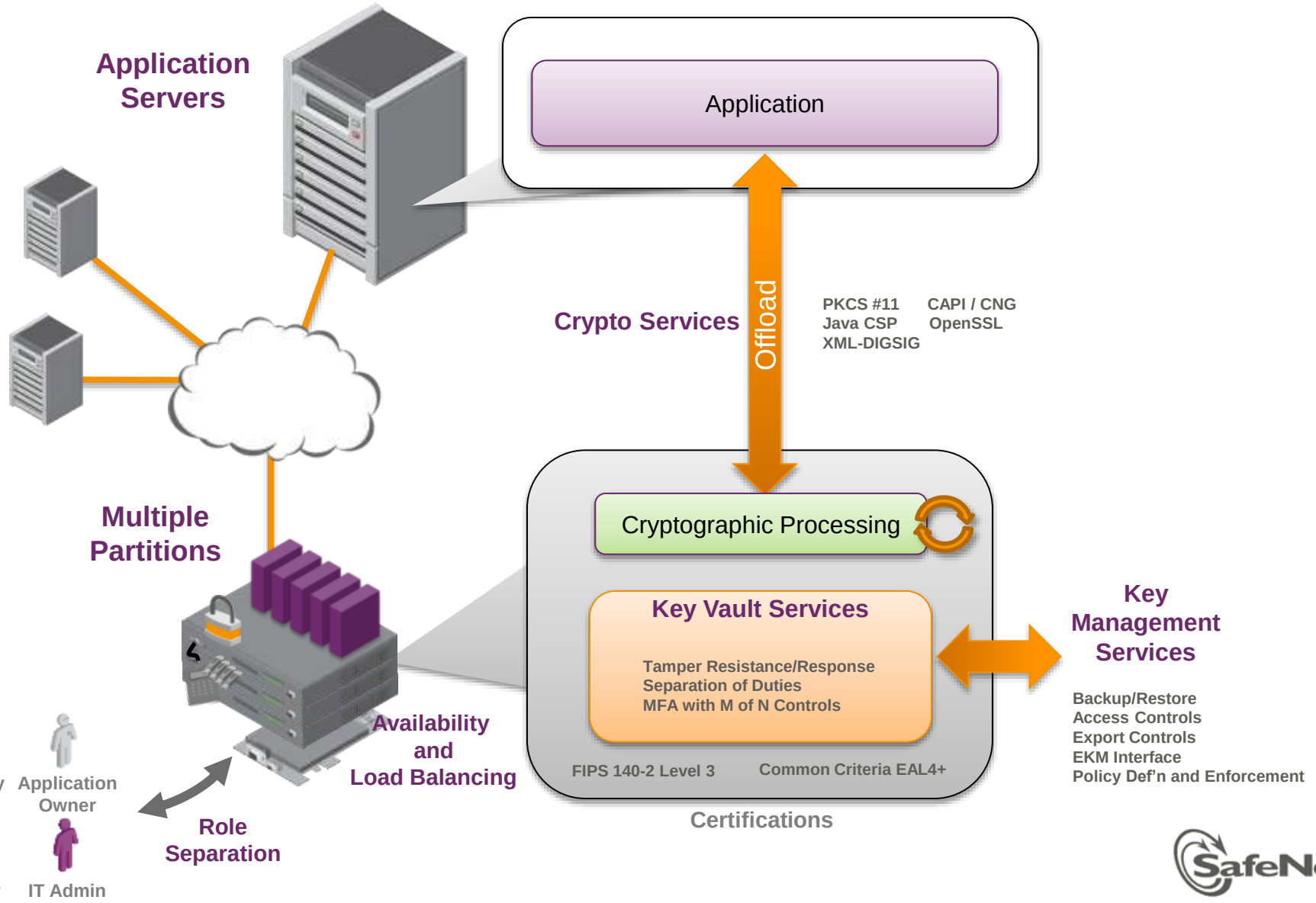
…a vault for holding cryptographic keys…

…Cryptographic Acceleration Hardware…

…a hardware solution that implements the cryptographic algorithms you want to use…

SafeNet

How is a HSM deployed?



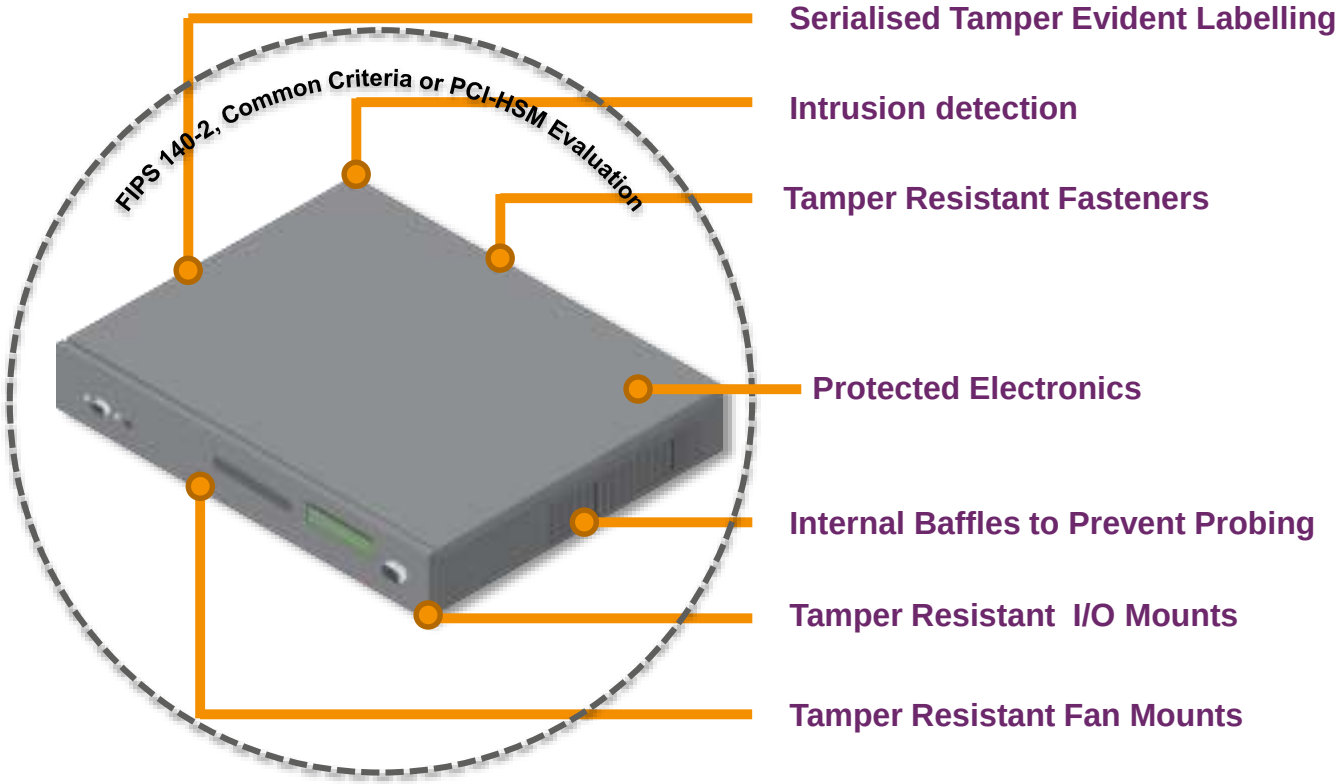
Certifications

- Provide independent verification of the security of a HSM

Common Criteria

Physical Security Features

Features of a Validated HSM Appliance



HSM Form Factors

SafeNet

So What Do HSMs Get Used For?
1. Secure Documents

SafeNet

HSMs secure passport issuance


HSMs secure documents for governments, hospitals, and the court system

Secure Manufacturing

HSMs secure entertainment devices, including videogame consoles and Personal Video Recorders

HSMs secure Smart Metering Systems and the delivery of Meter messages in our homes to Head End Utility systems

Banking and Payments

HSMs secure mobile money payments and verbal banking transactions made by telephone

HSMs secure card data and the delivery of Personal Identification Numbers (PINs)

HSMs secure the production of credit and debit cards and mobile phone SIM cards.

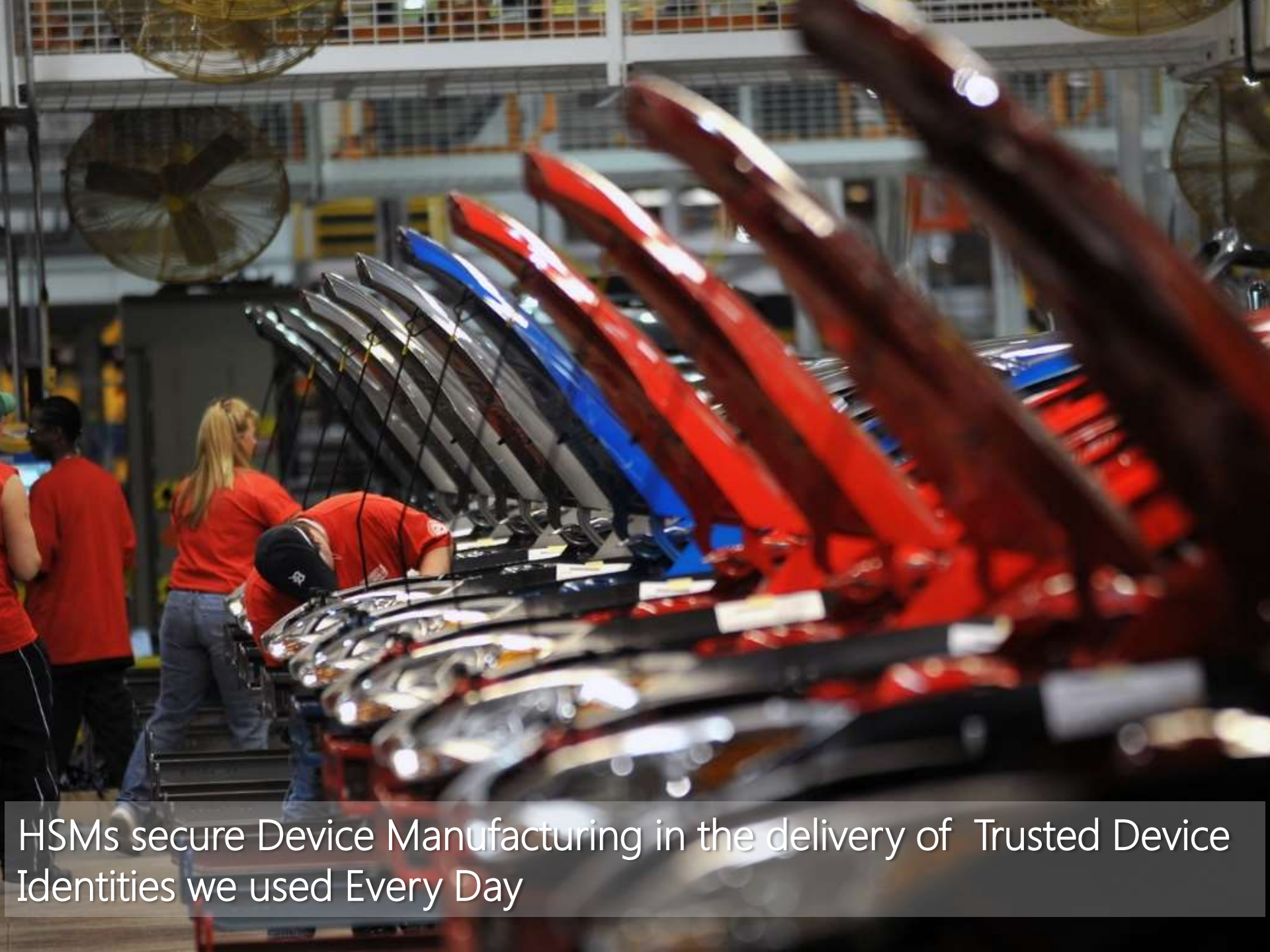
And Yet More Payments Use Cases…

SWIFT

SafeNet

HSMs secure SSL for the websites we use every day

Transport and Infrastructure

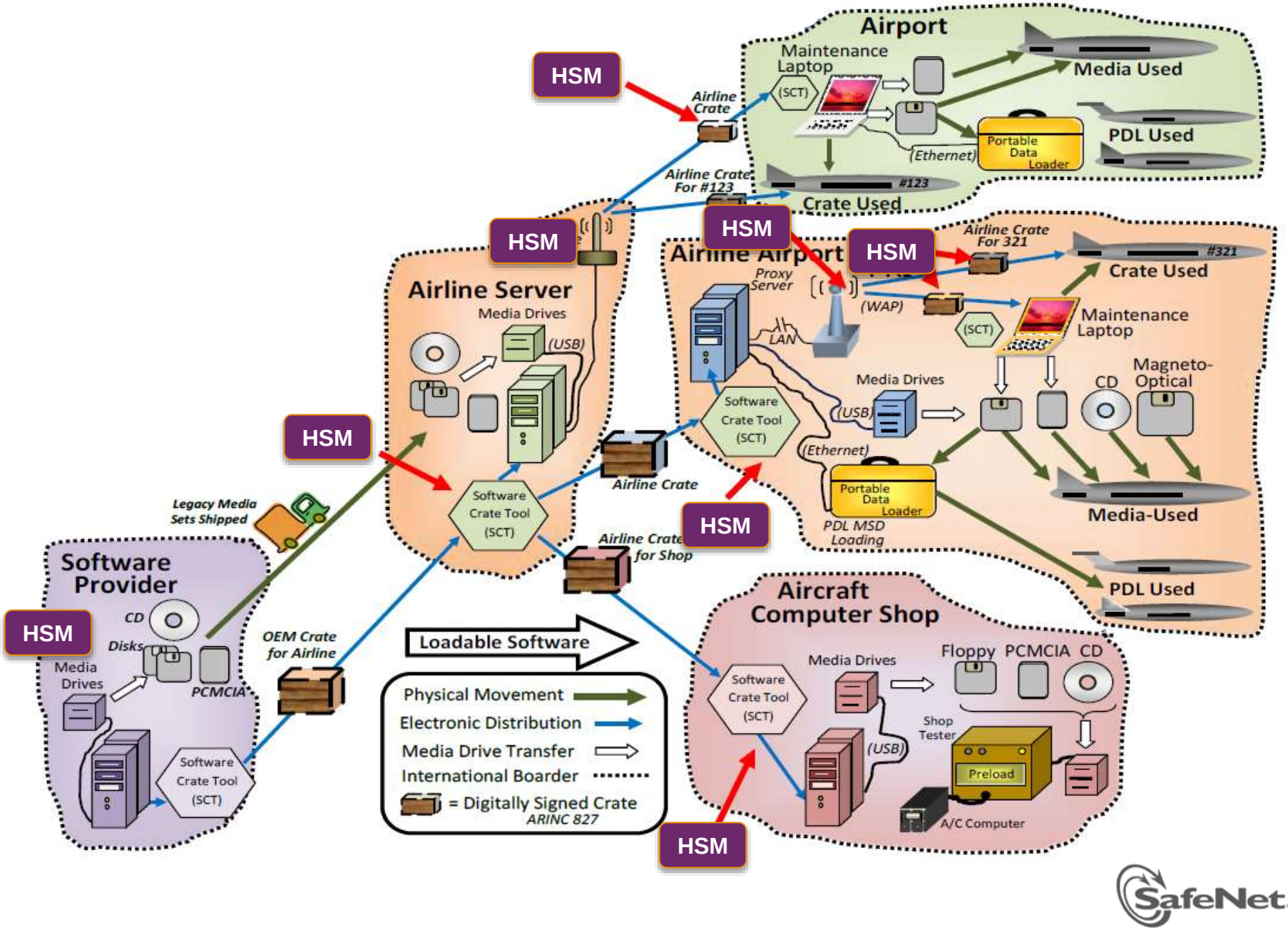


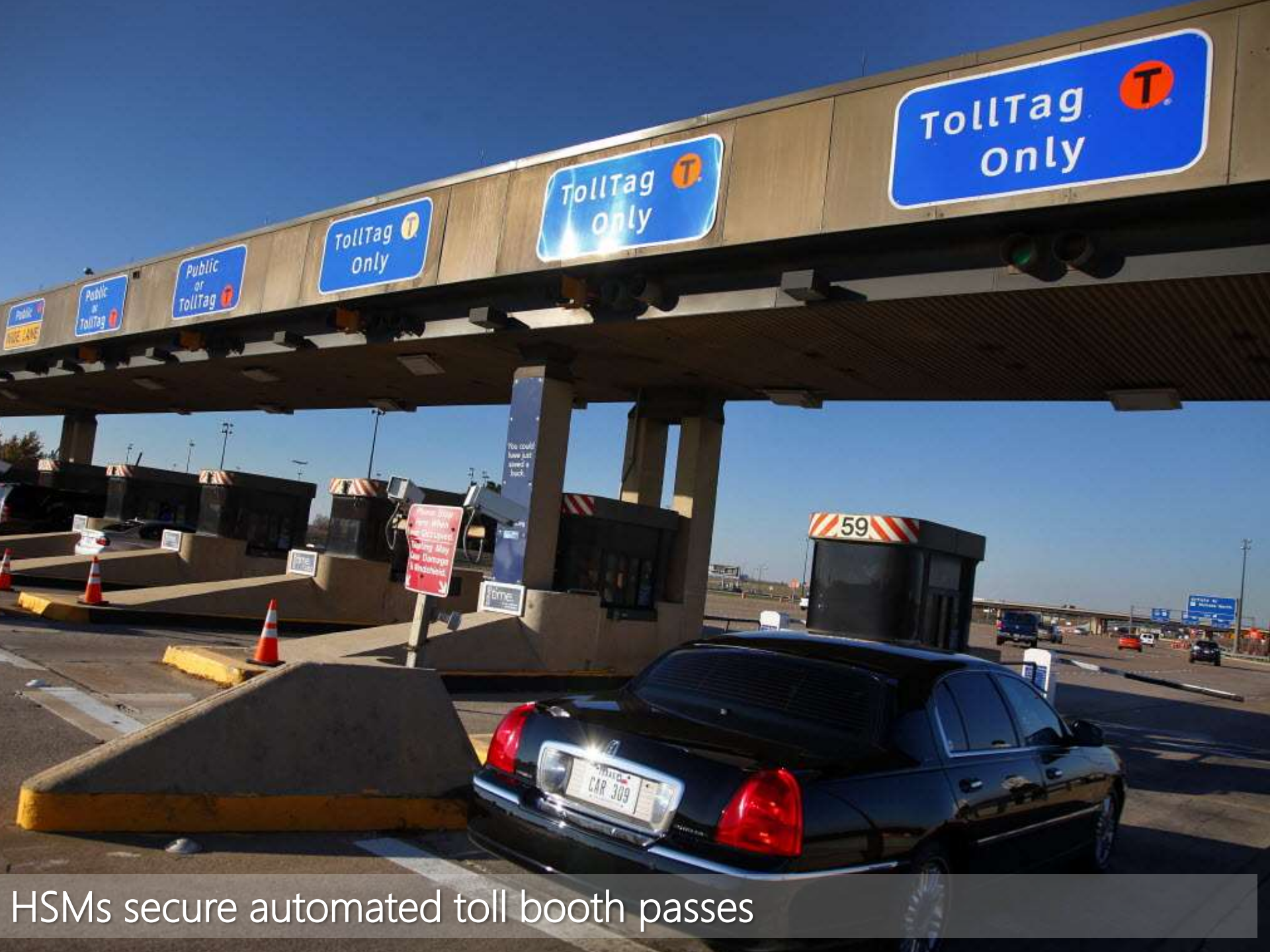
HSMs secure Device Manufacturing in the delivery of Trusted Device Identities we used Every Day

Railway signalling infrastructure is secured by Hardware Security Modules

HSMs are used to protect the communication protocols for large industrial equipment

HSMs secure the software and physical components of safety critical systems


Airport
Maintenance Laptop
(SCT)
Media Used
PDL Used
Portable Data Loader
(Ethernet)
#123
Crate Used
Airline Crate
Airline Crate For #123
HSM
Airline Server
Media Drives
(USB)
Software Crate Tool (SCT)
Airline Crate
Airline Crate for Shop
Airline Airport
Proxy Server
(WAP)
LAN
Airline Crate For 321
#321
Crate Used
Maintenance Laptop
Media Drives
(USB)
(Ethernet)
Portable Data Loader
PDL MSD Loading
CD
Magneto-Optical
Media-Used
PDL Used
Legacy Media Sets Shipped
Software Provider
CD
Disks
Media Drives
PCMCIA
Software Crate Tool (SCT)
OEM Crate for Airline
Loadable Software
Physical Movement
Electronic Distribution
Media Drive Transfer
International Boarder
= Digitally Signed Crate
ARINC 827
Aircraft Computer Shop
Media Drives
Floppy
PCMCIA
CD
Shop Tester
Preload
A/C Computer
(USB)



HSMs secure automated toll booth passes

Online Content

HSMs secure the delivery of streaming media

Thank You!