SECURING LPC55SXX PROVISIONING AND VOLUME PROGRAMMING WITH EPS GLOBAL

Clark Jarvis, Ecosystem Product Marketer, NXP
Brian Colgan, Field Application Engineer, EPS Global

MARCH 2021

SECURE CONNECTIONS
FOR A SMARTER WORLD

AGENDA

- **Protect your Valuable IP throughout your Product's Lifecycle**
  - The Importance of Security
  - LPC5500 MCU Series with Advanced Security
  - The Path to Production
  - Secure Provisioning in Volume on a Global Scale
- **Q & A**

How do you Protect your Valuable IP through your Product’s Lifecycle?

Volume Manufacturing flows for the LPC5500 MCU series

SECURE CONNECTIONS
FOR A SMARTER WORLD

PUBLIC

IMPORTANCE OF SECURITY: C-SUITE LEADERSHIP IS MANDATORY!

Gartner Predicts:

- 75% of CEOs Will be Personally Liable for Cyber-Physical Incidents by 2024.
- Financial impact of CPS (Cyber-Physical System) attacks resulting in fatal casualties will reach over **$50 billion by 2023**.

The scale and impact of industrial espionage and theft of trade secrets through cyber
Executive summary

Economic Impact of IP Theft

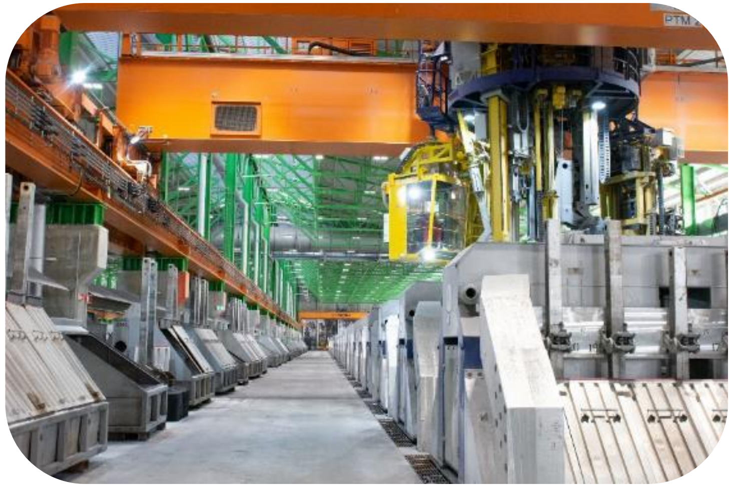
- **€60 billion** economic growth impact in EU due to cyber theft
- **289,000** potential job losses

TARGETS:

- Electronic Devices & Sub Assemblies
- Industrial Systems
- City Infrastructure
- Pharmaceutical Production

SOURCES:
https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl
https://op.europa.eu/en/publication-detail/-/publication/b3b5fcfb-4541-11e9-a8ed-01aa75ed71a1/language-en/format-PDF/source-90181868

INHIBITING MALWARE THROUGHOUT THE LIFECYCLE



Norsk Hydro

$52M+ impact

LockerGoga malware

2nd most expensive hack 2019

Real Costs

Real Impacts

Real Lives

Duesseldorf University Hospital
September 2020

First directly implicated death due to cyber attack

SECURITY DELIVERS MULTIPLE HIGH VALUE BENEFITS

Legislation

IP Protection

Production Control

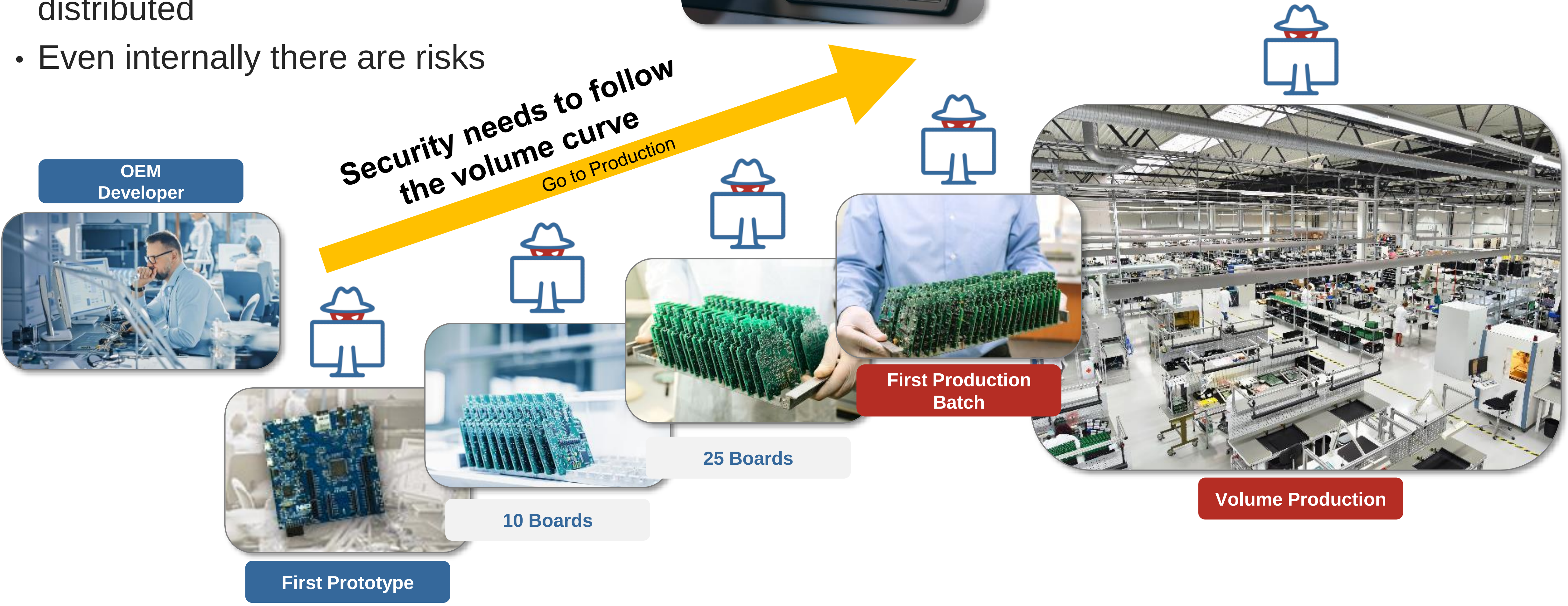
Inhibiting Malware

Secure Identity and Rapid Onboarding

Standards & Certification

TRANSFERRING FROM DESIGN TO PRODUCTION

- Tempting to think it’s easy…
- But roles and facilities are highly distributed
- Even internally there are risks



Security needs to follow the volume curve

Go to Production

OEM Developer

First Prototype

10 Boards

25 Boards

First Production Batch

Volume Production

TO ENABLE SECURE VOLUME PRODUCTION
AND PROTECT THE INTEGRITY OF YOUR PRODUCT THROUGHOUT ITS LIFECYCLE

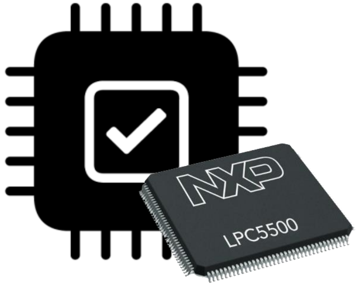
YOU NEED:

A microcontroller with enhanced security

A trusted development environment

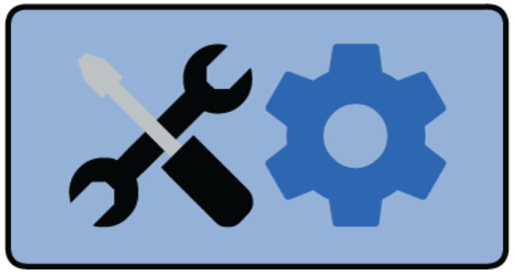
A trusted secure provisioning partner

A way to connect to them securely



NXP

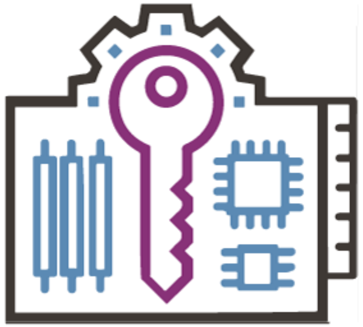
SECURITY-ENABLED MCU



SECURE THINGZ

SECURITY DEVELOPMENT TOOL

GLOBAL SECURITY PARTNER



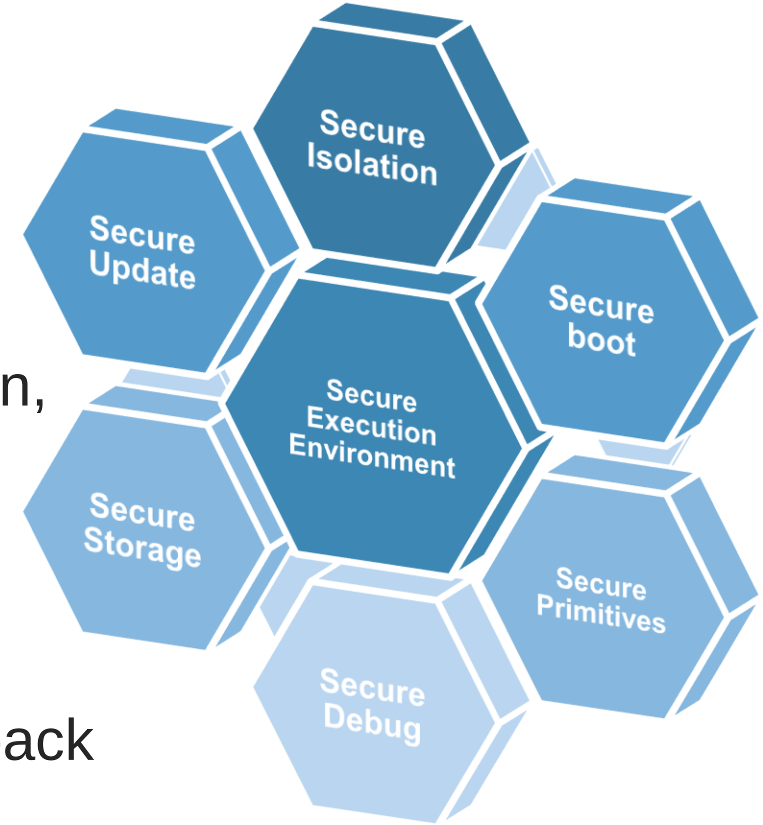
HARDWARE SECURITY MODULE (HSM)

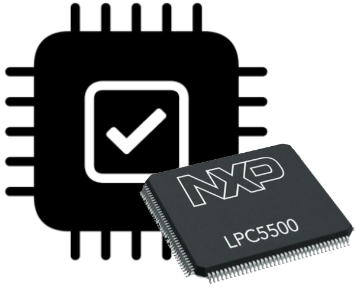
Software Development → Securely Package IP → Package Transfer → Provision Devices → Deploy Products

NXP LPC5500 MCU SERIES

A MICROCONTROLLER WITH ENHANCED SECURITY

- **Secure Isolation**
  Isolate secure and non-secure worlds
- **Secure Boot**
  Execute only authorized firmware
- **Secure Primitives**
  Cryptography primitives – hashing, encryption, decryption, authentication
- **Secure Storage**
  Secure keys, code and data confidentiality
- **Secure Update**
  OTA firmware update, revoke keys, anti-rollback
- **Secure Debug**
  Only authenticated parties allowed to debug

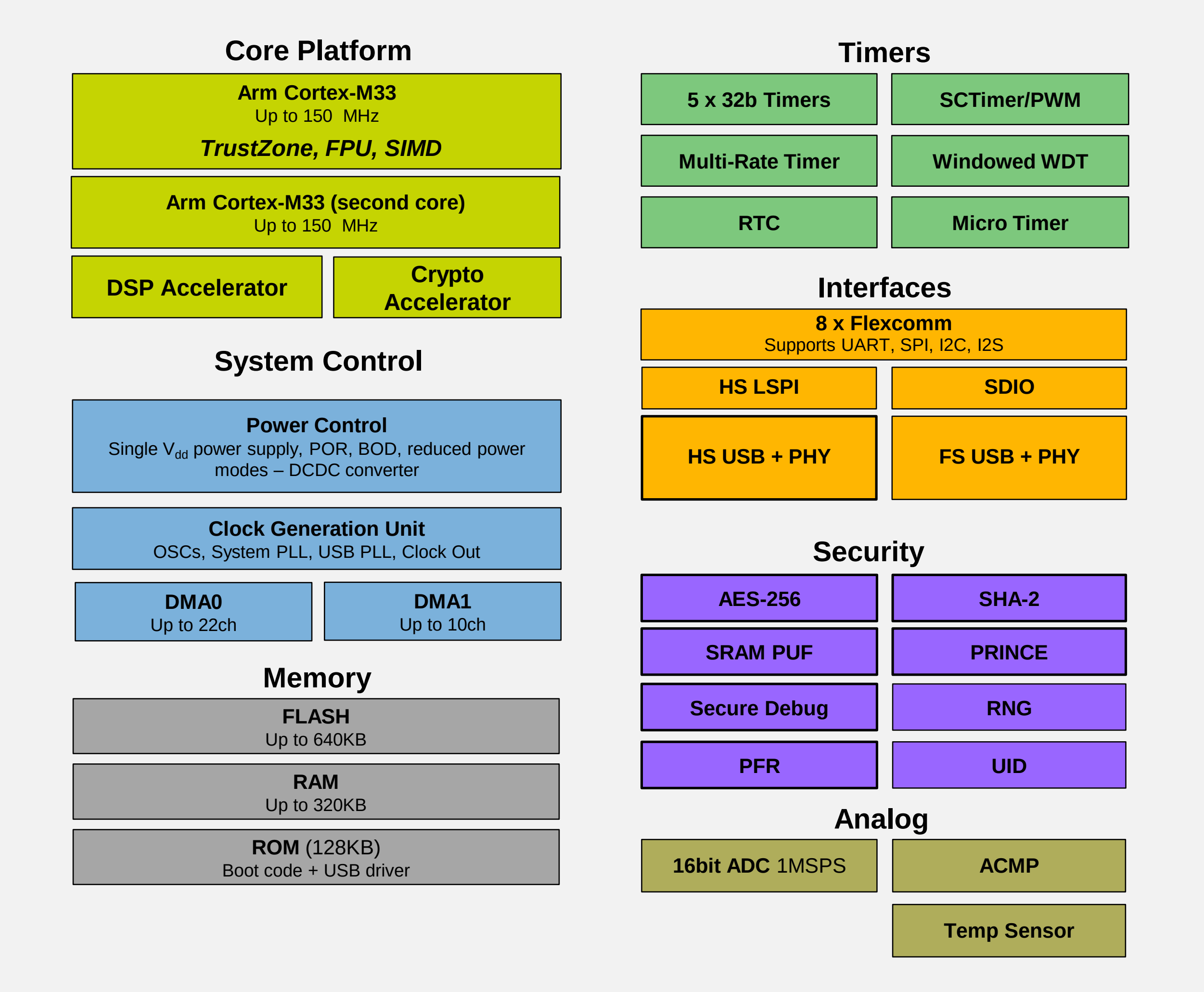




SECURITY-ENABLED MCU

LPC55S6X MCU FAMILY BLOCK DIAGRAM

- **Industrial & Building Automation**
  - Dual Core to boost performance & keep low power consumption
  - PowerQuad DSP as an accelerator
  - High precision ADC
- **Consumer**
  - HS/FS USB with PHY built-in for eBOM cost saving
  - High-Speed SPI for efficient module interface
  - Large SRAM for easy FW development
- **Smart Home**
  - Trust Zone for memory protection
  - Secure boot for user’s code protection
  - Built-in SRAM PUF for key storage
  - Low power consumption



Core Platform

- **Arm Cortex-M33** Up to 150 MHz *TrustZone, FPU, SIMD*
- **Arm Cortex-M33 (second core)** Up to 150 MHz
- **DSP Accelerator**
- **Crypto Accelerator**

System Control

- **Power Control** Single V_{dd} power supply, POR, BOD, reduced power modes – DCDC converter
- **Clock Generation Unit** OSCs, System PLL, USB PLL, Clock Out
- **DMA0** Up to 22ch
- **DMA1** Up to 10ch

Memory

- **FLASH** Up to 640KB
- **RAM** Up to 320KB
- **ROM** (128KB) Boot code + USB driver

Timers

- 5 x 32b Timers
- SCTimer/PWM
- Multi-Rate Timer
- Windowed WDT
- RTC
- Micro Timer

Interfaces

- **8 x Flexcomm** Supports UART, SPI, I2C, I2S
- HS LSPI
- SDIO
- HS USB + PHY
- FS USB + PHY

Security

- AES-256
- SHA-2
- SRAM PUF
- PRINCE
- Secure Debug
- RNG
- PFR
- UID

Analog

- **16bit ADC** 1MSPS
- ACMP
- Temp Sensor

FOUR PILLARS: RECOGNIZED FOR SECURITY ACROSS MANY MARKETS

EDGELOCK™
ASSURANCE
by NXP

PRODUCTS
Discrete and integrated solutions to meet your needs

SUPPORT
NXP and partner ecosystem support for end-to-end security

PROCESS
Security-by-design is integral to how we operate

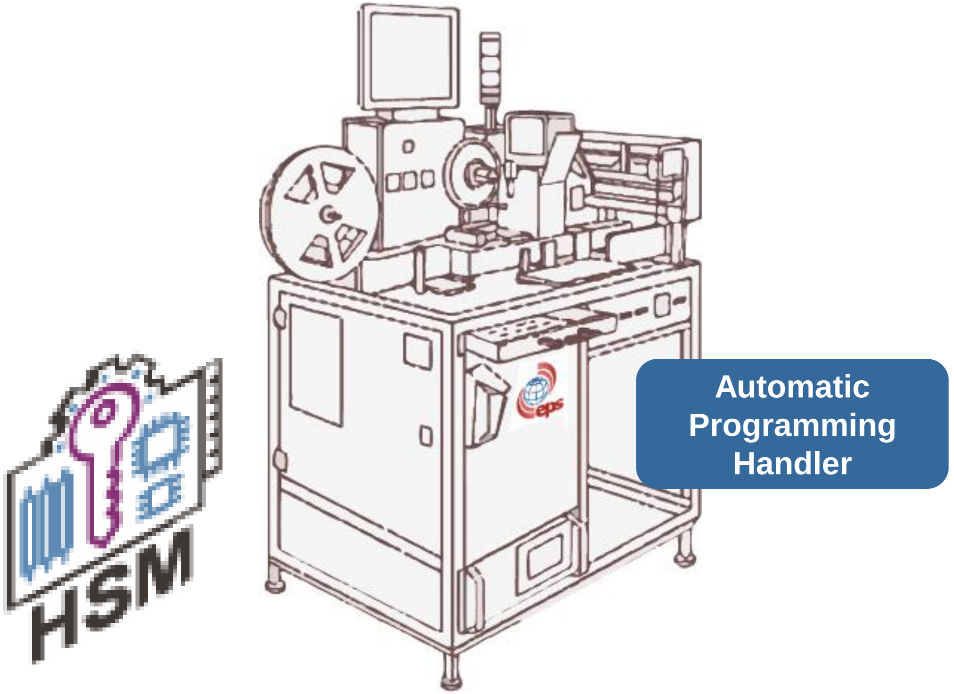
COMPLIANCE
Products designed to meet relevant industry standards

SECURE BOOT FOR LPC55SXX

- Chain of trust anchored directly in hardware
- Secure Key Storage for Root of Trust and Image Keys
- Booting of Public-Key signed images
  - 2048-bit or 4096-bit RSA keys and x.509 v3 certificates
- BootROM support for pre-configured TrustZone-M settings
- Support for Secure Boot Manager with immutable root of trust
  - Enabling the trusted development environment

For specifics, refer to NXP Application Note: AN12283

INTEGRATION OF HSM INTO AUTOMATIC MACHINES IN A VOLUME ENVIRONMENT



- The HSM is integrated into EPS Global’s high-volume automatic programming handlers.
- EPS has a global network of 19 programming centers in the Americas, EMEA, India and Asia.
- Full support for NXP LPC5500 MCU series.

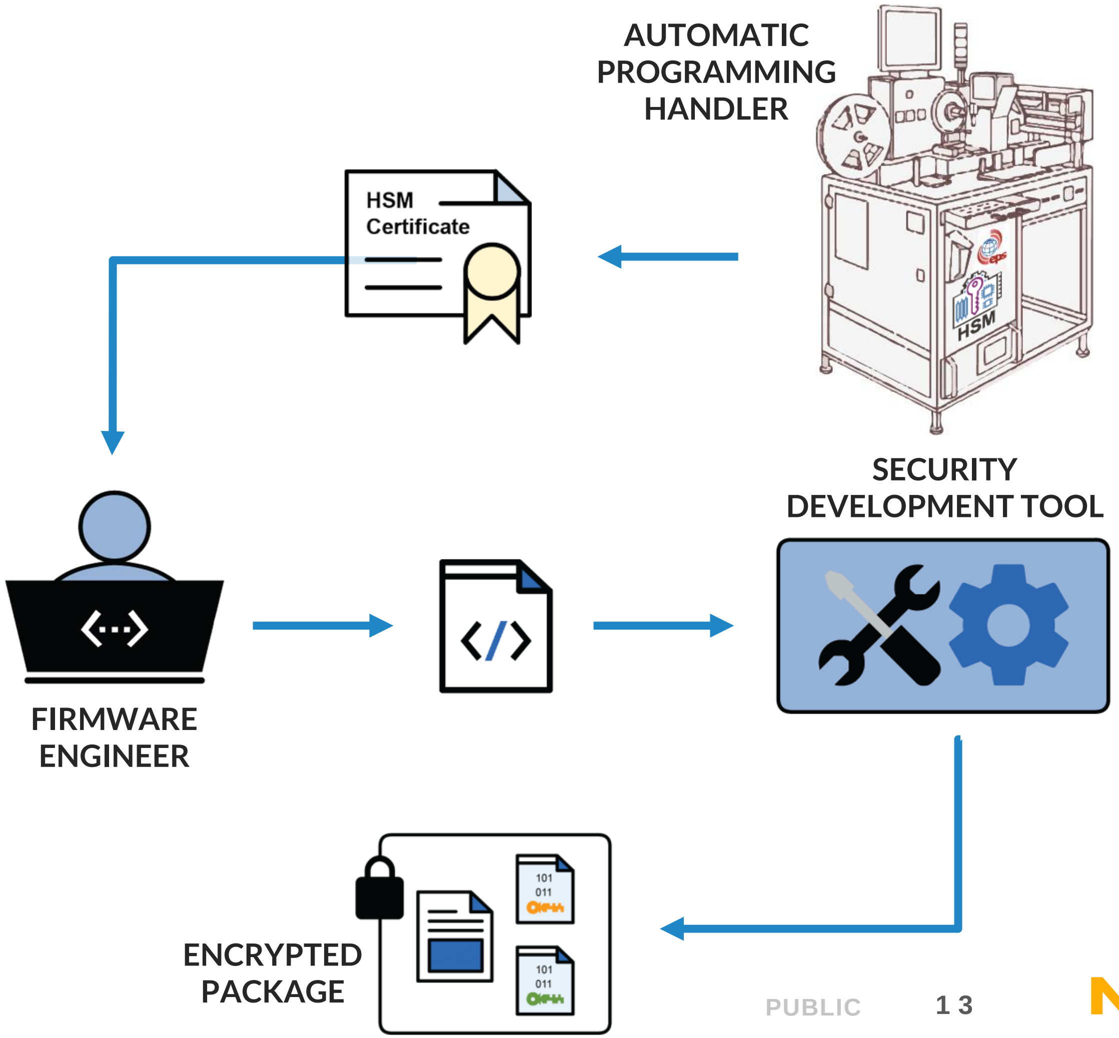
Cost effective solution. Why?

- EPS designs and builds their own automatic programming handlers in their R&D facility in Brno, Czech Republic

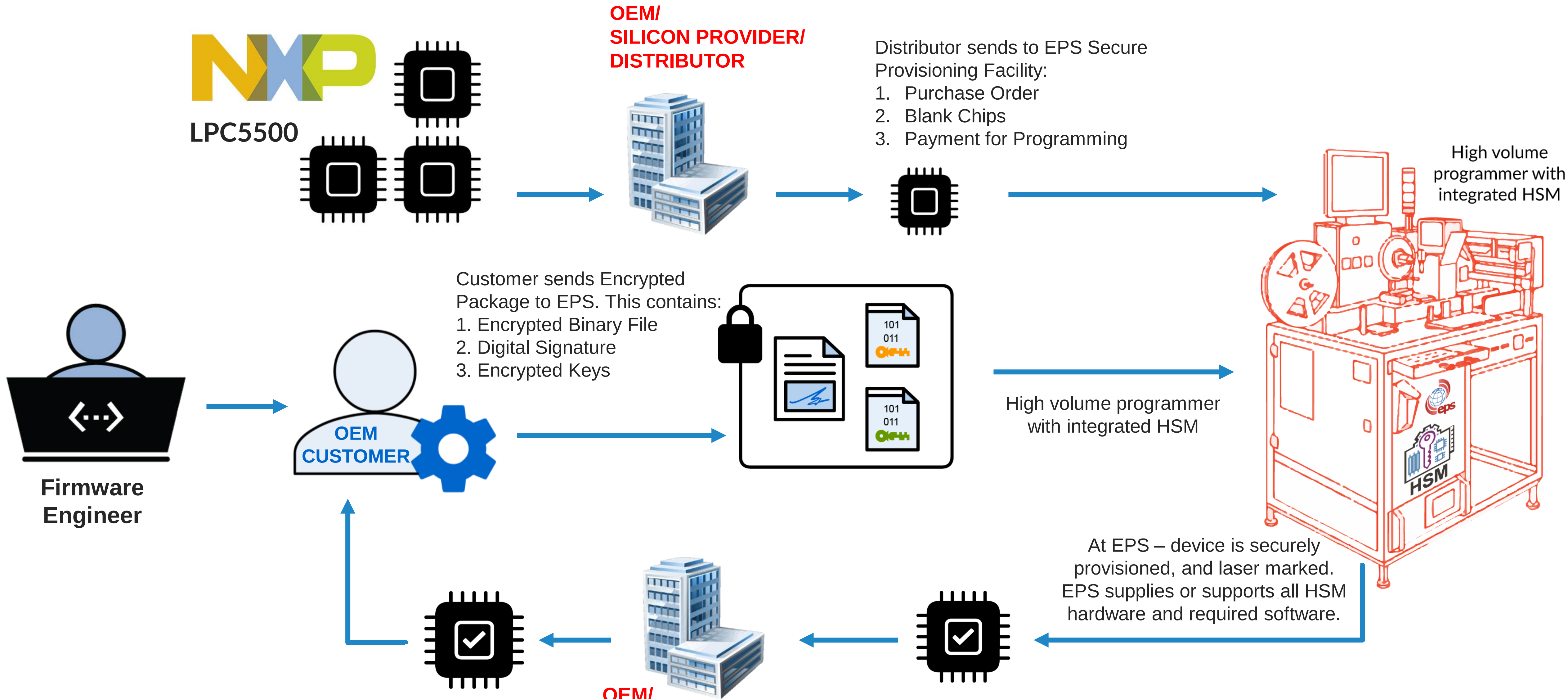
HOW IS AN IMAGE SECURELY TRANSFERRED?

SECURE PACKAGE:
HOW IT IS MADE, WHAT IT IS MADE OF?

- Firmware Engineer works with Secure Thingz Embedded Trust.
- EPS sends the public certificate of HSM to customer so file can be encrypted.
- The secure encrypted package (output from Embedded Trust) refers to the destination HSM inside the machine in the secure EPS programming center.
- Encrypted package is sent to EPS by preferred method.
- Only decryptable with the private key inside the HSM in the specified destination machine – EPS never has the unencrypted copy of the customer software.



HOW DOES SECURE PROVISIONING FIT INTO THE MANUFACTURING PROCESS?



LPC5500

OEM/
SILICON PROVIDER/
DISTRIBUTOR

Distributor sends to EPS Secure Provisioning Facility:

1. Purchase Order
2. Blank Chips
3. Payment for Programming

High volume programmer with integrated HSM

Customer sends Encrypted Package to EPS. This contains:

1. Encrypted Binary File
2. Digital Signature
3. Encrypted Keys

High volume programmer with integrated HSM

Firmware Engineer

OEM CUSTOMER

At EPS – device is securely provisioned, and laser marked. EPS supplies or supports all HSM hardware and required software.

These provisioned chips are sent to OEM/Silicon Provider/Distributor

OEM/
SILICON PROVIDER/
DISTRIBUTOR

HOW IS THE INTEGRITY OF SYSTEM MAINTAINED FROM START TO FINISH?

EPSGLOAL: SECURE TRUSTED ENVIRONMENT:

- Key card entry to enter facility
- Tamper-proof HSM in machine
- Limited number of operators permitted to use machine, access to machine is via Biometric ID
- Complete log file of who is operating each machine and when – full Traceability

LOT CODE <u>TRACEABILITY</u> MAINTAINED & RETAINED THROUGHOUT, I.E.:

- NXP Date code
- NXP Lot code
- NXP P/N
- Customer Blank P/N
- Customer Programmed P/N
- Shipping note #

WORLD-CLASS QUALITY LEVELS

Compliant with all International manufacturing quality control procedures: ISO 9001, 14001, 27001, VDA 6.3 (German Automotive standard)

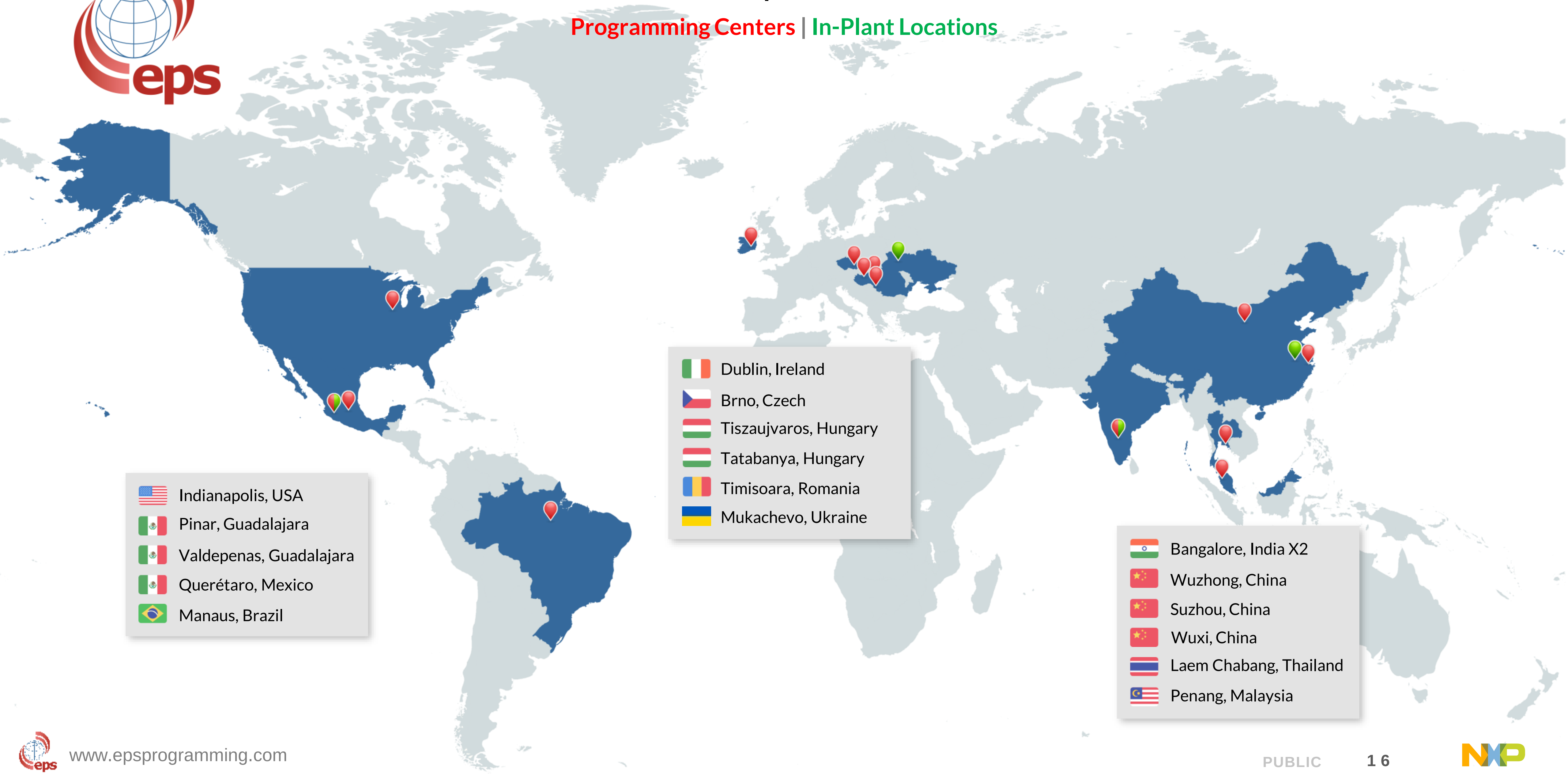
IoT Security Foundation Corporate Member

ISO 9001 ISO 27001 ISO 14001

VDA QMC Qualitäts Management Center im Verband der Automobilindustrie

GLOBAL REACH | LOCAL PRESENCE

Programming Centers | In-Plant Locations



- Indianapolis, USA
- Pinar, Guadalajara
- Valdepenas, Guadalajara
- Querétaro, Mexico
- Manaus, Brazil

- Dublin, Ireland
- Brno, Czech
- Tiszaujvaros, Hungary
- Tatabanya, Hungary
- Timisoara, Romania
- Mukachevo, Ukraine

- Bangalore, India X2
- Wuzhong, China
- Suzhou, China
- Wuxi, China
- Laem Chabang, Thailand
- Penang, Malaysia

NEXT STEPS…
GET IN TOUCH

Brian Colgan

FAE, Semiconductors

bcolgan@epsglobal.com

+353 87 646 5561

John Gleeson

Sales Director EMEA & Brazil

jgleeson@epsglobal.com

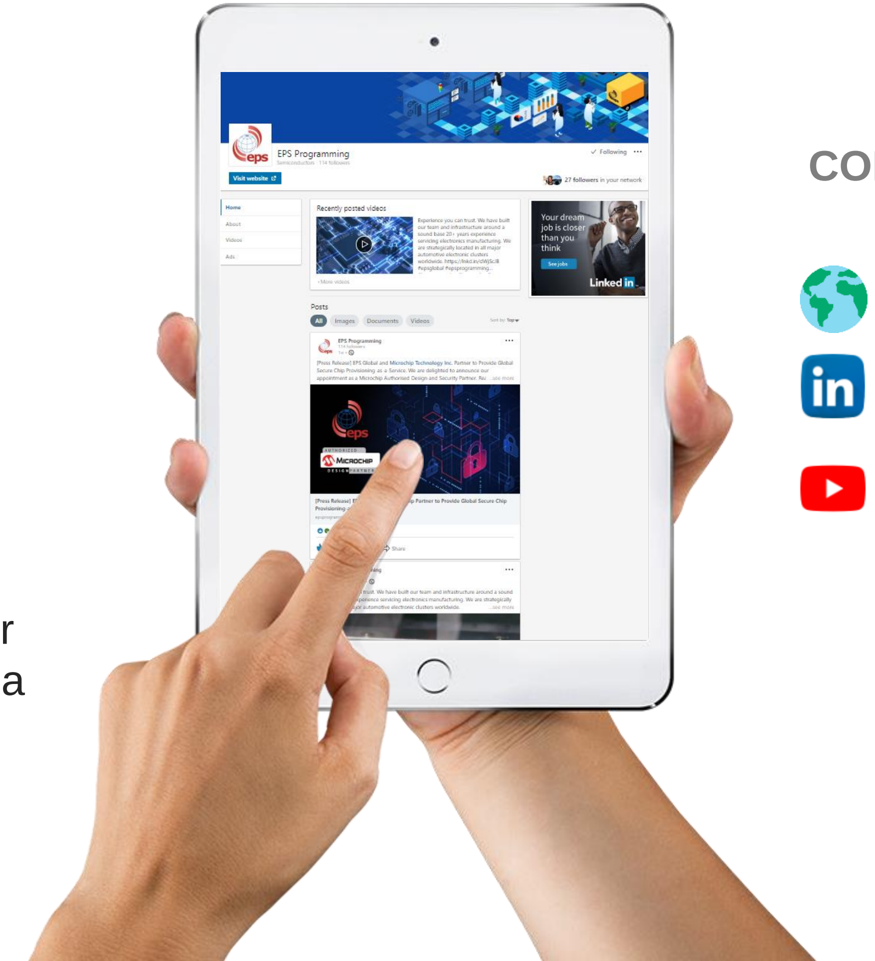
+353 872 594 128

Dean LoPresti

Business Development Director
IC Programming, North America

dlopresti@epsglobal.com

978-808-0323



CONNECT WITH US:

epsprogramming.com

/showcase/eps-programming

/c/epsprogramming1

Q&A

SECURE CONNECTIONS
FOR A SMARTER WORLD