CONNECT WITH CONFIDENCE

DIGI CONNECTCORE 6UL IOT EMBEDDED MODULE
TRUSTFENCE EMBEDDED IOT SECURITY FRAMEWORK

STRENGTH IN NUMBERS

285

PATENTS ISSUED AND PENDING

100M

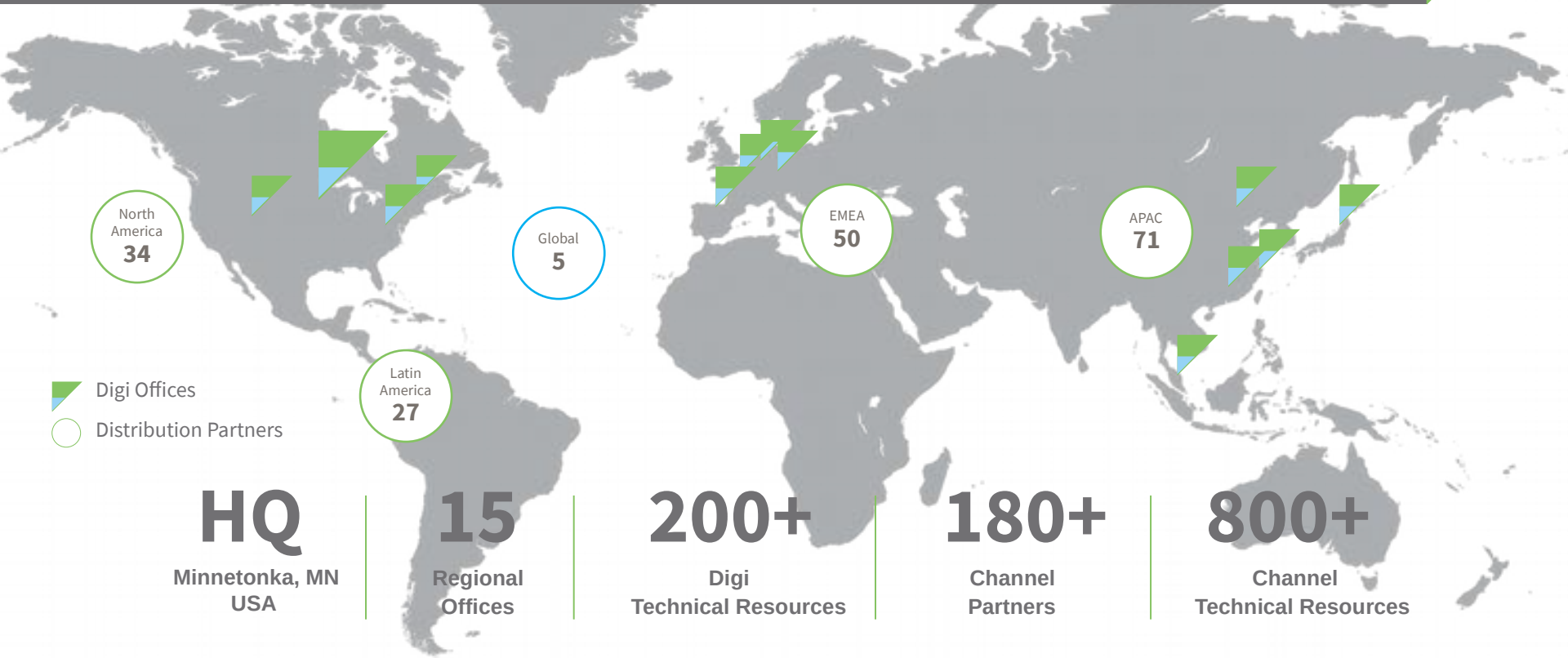
THINGS CONNECTED

25K

CUSTOMERS

DGII	1985	515	14	204	137
NASDAQ	Year Founded	Employees Worldwide	Consecutive Years of Profitability	Million In Revenue	Million In Cash

EXTENSIVE GLOBAL REACH



HQ
Minnetonka, MN
USA

15
Regional
Offices

200+
Digi
Technical Resources

180+
Channel
Partners

800+
Channel
Technical Resources

BRING CONNECTIVITY TO ANY DEVICE

CREATE

RF & EMBEDDED
MODULES & SBCs
CUSTOM DESIGN SERVICES

DEPLOY

CELLULAR ROUTERS
AND GATEWAYS
DEVICE NETWORKING

MANAGE

DIGI REMOTE MANAGER
DIGI DEVICE CLOUD
COLD CHAIN SOLUTIONS

DIGI EMBEDDED BENEFITS

Network Connectivity

- ✓ Integrated 802.11 a/b/g/n/ac networking options
- ✓ Bluetooth Smart Ready options on selected modules
- ✓ Single or dual Ethernet

Process Control and Reliability

- ✓ Design change notifications/approvals
- ✓ Strong 5-year hardware warranty
- ✓ Stringent environmental testing to meet reliability requirements

Quick Time-to-Market

- ✓ Design flexibility without the traditional complexity
- ✓ Pre-certified system on module solutions
- ✓ Complete out-of-box software support + design services

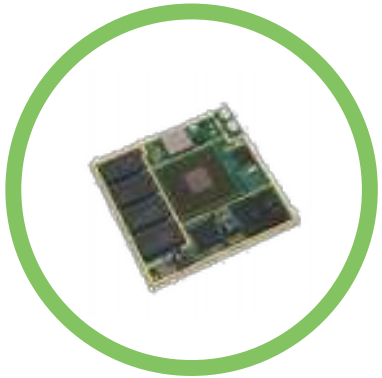
Long-Term Availability (7–10+ years)

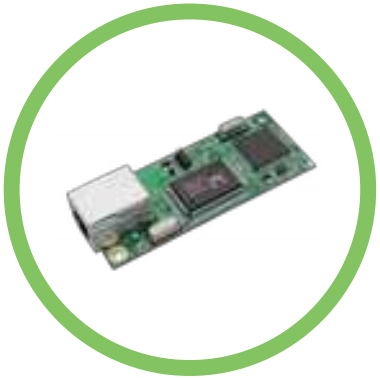
- ✓ Selected NXP i.MX application processors
- ✓ Long lifecycle connectors and memory components
- ✓ Multiple component supplier options

Digi TrustFence™ Security

- ✓ Complete Connected Device Security Framework
- ✓ Integrated, tested and future-proof
- ✓ Zero implementation effort

EMBEDDED MODULES AND SBC






Industrial grade ARM-based wireless SoM and SBCs

- ✓ Pre-certified Wi-Fi & Bluetooth capability
- ✓ Designed long-term availability
- ✓ Scalable architectures
- ✓ Linux, Android, Windows CE, and Dynamic C
- ✓ Low-profile and cost-effective ARM solutions
- ✓ On module power management

RF MODULES AND GATEWAYS

World's #1 selling RF module and gateway solution

- ✓ Over 10 million modules shipped globally
- ✓ Best-in-class range at over 100 miles
- ✓ More than 20,000 customers
- ✓ Large family of pin-compatible modules
- ✓ Easy to integrate
- ✓ Secure and scalable remote management

CELLULAR ROUTERS AND GATEWAYS




Secure and reliable wireless WAN

- ✓ 3G & 4G LTE support
- ✓ Industry-leading warranty
- ✓ Comprehensive remote management tools
- ✓ Hardened for environmental resilience
- ✓ Deployed in 95 countries globally
- ✓ Purpose-built for mission critical applications

DIGI MEETS CRITICAL MARKET REQUIREMENTS
Digi Meets Mission Critical Requirements

Reliability

- Performs in harsh environments
- Uptime is a must
- Very long system lifespans

- Long term product availability
- Built to last: free 5 year warranties
- Commercial and industrial grade

Scalability

- Start small. Grow large.
- Flexible, not one-size-fits-all approach
- Easy to integrate and deploy

- Range of external and embedded options
- 20+ connectivity interfaces supported
- Extensive provisioning and software tools

Security

- Mitigate risk and limit exposure
- Meet industry regulations
- Maintain compliance standards

- 175 security controls
- 20+ integrated hardware security features
- Industry compliance (PCI, HIPAA, NIST)

Manageability

- Meet service level commitments
- Monitor network health
- Minimize truck rolls

- Device profile enforcement
- Custom network health alerts and reports
- Turnkey firmware/software updates

PRE-CERTIFIED Pre-Certified

- Module certifications for unintentional radiation, immunity and safety minimize design risk and significantly accelerate product development cycle
  - FCC Class B, EN, RSS, IC, CE, VCCI, UL/UR
- Entirely pre-certified Wi-Fi radio design further simplifies product development and integration process
  - Eliminate certification costs for intentional radiation (radio)
    - Estimated cost of combined 802.11 a/b/g/n approval for North America, EU and Japan is ≥ US$50k
  - No radio design or homologation expertise required
  - No approval maintenance or monitoring of worldwide regulatory changes
  - Radio approved in US, Canada, EU, Japan, Australia/New Zealand

PRE-CERTIFIED Pre-Certified

- ConnectCore® 6UL, ConnectCard i.MX28 and ConnectCore 6 provide seamless integration and interoperability with common network infrastructure protocols for easy end device deployments
- Wi-Fi 802.11 Logo Certification Ready
  - Managed and defined by Wi-Fi Alliance
  - Interoperability tests, performance, connection reliability
- Cisco Compatible Extensions (CCX) v4 Certification Ready
  - Managed and defined by Cisco
  - Requires 802.11n Logo certification
  - Interoperability and validation of Cisco proprietary feature implementations, such as power management and Cisco Certificate Key Management (CCKM) for fast and secure roaming

KEY MARKETS TARGET

ENERGY ▸

Monitoring and management of smart grids, digital oil fields, and tank farms.

SMART CITIES ▸

Efficient, real-time protection and services for cities that never sleep.

MEDICAL ▸

Securely connecting patients in hospitals and homes to vigilant caregivers.

INDUSTRIAL ▸

Maximizing uptime and reducing costs for processes and heavy machinery.

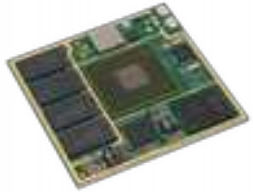
RETAIL ▸

Total security, reliability, and availability for a world of nonstop transactions.

TRANSPORTATION ▸

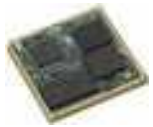
Rugged sensors, cellular devices, and onboard systems for applications constantly on the go.

CONNECTCORE I.MX SOM FAMILY



CONNECTCORE 6

- Scalable single to quad core performance
- 802.11 a/b/g/n + Bluetooth 4.0
- Ruggedized low-profile SMT design



CONNECTCORE for i.MX6UL

- Power-efficient ARM Cortex A7 performance
- 802.11 a/b/g/n/ac + Bluetooth 4.2
- Ruggedized low-profile SMTplus design

DIGI CONNECT ME 9210 FAMILY

- Digi ARM9 processor
- Scalable, compact, low-cost, off-the shelf module for intelligent Ethernet and Wi-Fi connectivity
- 10/100 Mbps Ethernet with built-in PoE pass-through option, or
- 802.11 bgn wireless networking

CONNECTCORE I.MX SBC FAMILY

CONNECTCORE 6UL SBC

- Build on ConnectCore 6UL
- Dual Ethernet, XBee and cellular optior
- LVDS and parallel display options
- Production-ready industrial grade Single Board Computer

CONNECTCORE 6 SBC

- Built on ConnectCore 6
- Additional XBee and cellular options
- Multiple display and camera interfaces
- Production-ready Single Board Computer with industrial grade option

CONNECTCORE 6UL SB

- Build on ConnectCore 6UL
- Multiple expansion connectors incl. Grove sensor interfaces
- 8-bit parallel LCD option
- Production-ready industrial grade Single Board Computer

DIGI TRUSTFENCE

BUILD SECURE CONNECTED EMBEDDED DEVICES

IOT MARKET AND DEVICE SECURITY

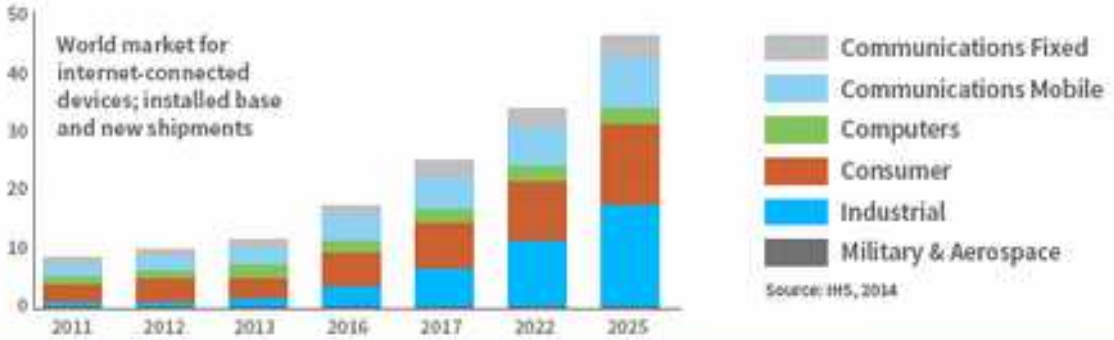
ARE YOU CONCERNED ABOUT CONNECTED DEVICE SECURITY?

70%

of IoT devices are vulnerable to attack

Source: HP Security Research

Non-consumer sectors will account for the majority of connected devices by 2025.



FOCUS ON CONNECTED DEVICE SECURITY, NOT “JUST” SECURE CONNECTIONS

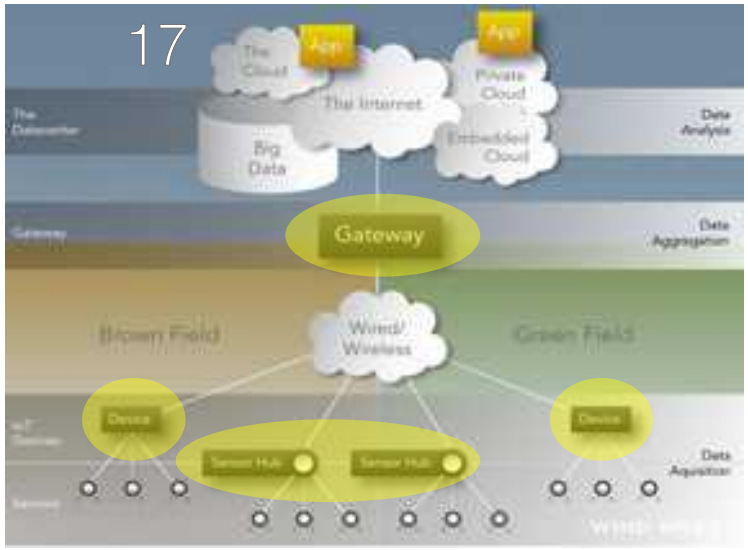


Image Source: Wind River

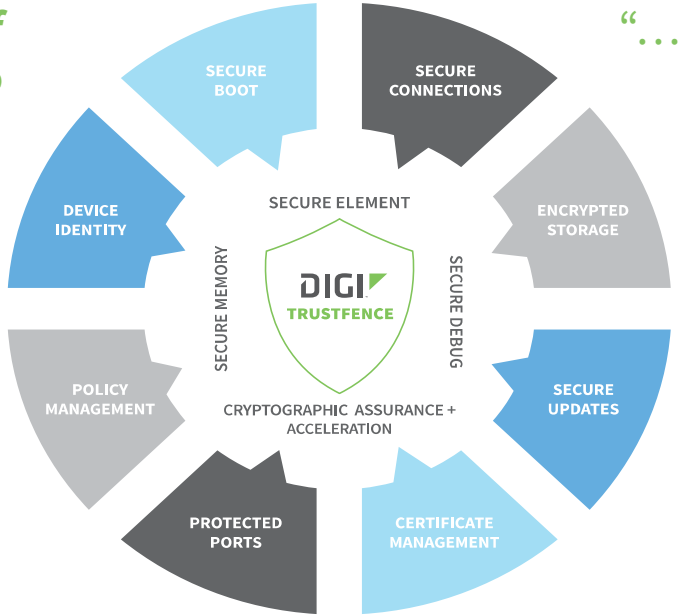
- Security by obscurity is an outdated “concept” - embedded devices are already a high profile target
- IoT already further amplifying existing concerns/issues
- Embedded devices require a device security approach supporting their 7-10+ year product lifecycles
- **Go beyond mandatory need for secure connections –** Secure Boot, Secure Storage, Access Control, ASLR, Device Identity/Authentication, Certificate Management, Secure Configuration/Updates, Tamper Detection …

Device Security is a critical design aspect

INTRODUCING DIGI TRUSTFENCE™

"…by 2020 more than 25% of identified attacks will involve IoT…"

Source: Gartner, 2016



"…70% of IoT devices are vulnerable to attack…"

Source: HP Security Research, 2016

Digi-exclusive Device Security Framework that protects connected devices

SIMPLIFY BUILDING SECURE CONNECTED PRODUCTS WITH DIGI TRUSTFENCE™

Let Digi TrustFence handle security for you with a full range of built-in features including:

- **Secure Boot**
  Ensures only signed software images can run on a device
- **Encrypted Storage**
  Local file system encryption keeps internal device data safe
- **Protected Ports**
  Access-controlled internal and external ports prevent unwanted "back doors"
- **Device Identity**
  Root of trust, certificate management, and secure key storage identity protection
- **Device Integrity**
  Tamper-proofing and device-integrity monitoring with low-power support protect against physical intrusion
- **Secure Connections**
  Enterprise-level data encryption for wired and wireless network privacy
- **Life-cycle Longevity**
  Rely on a Digi-maintained future-proof platform architecture

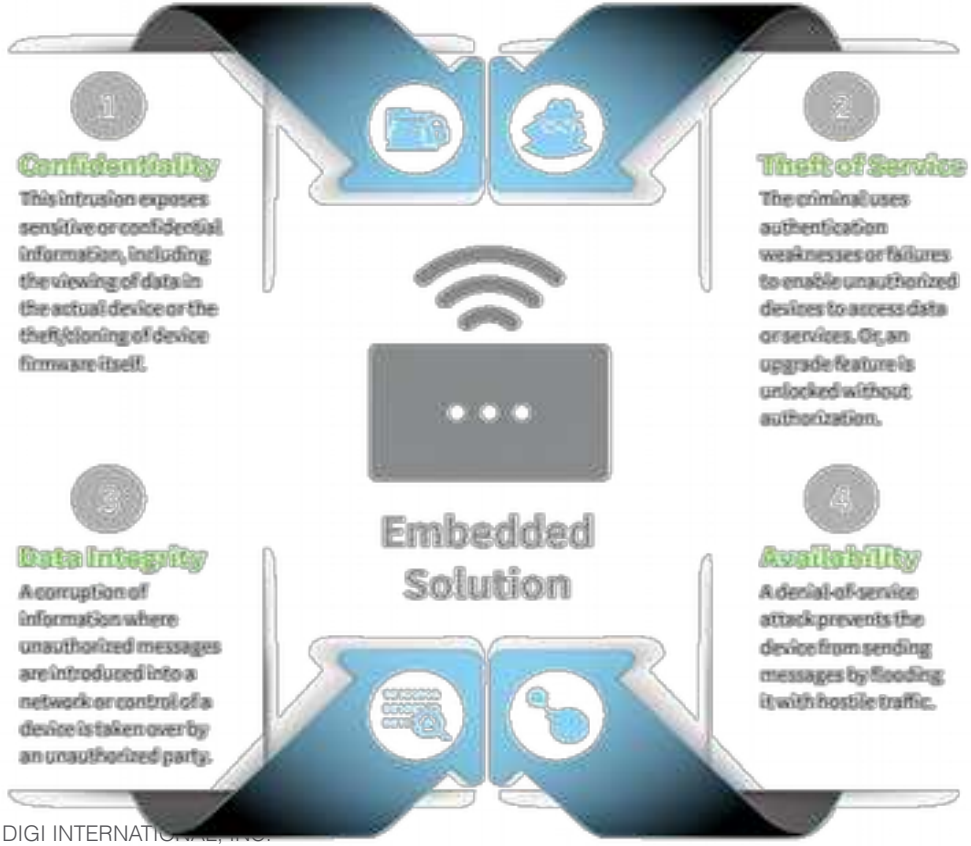
DIGI TRUSTFENCE™ AS AN UMBRELLA BRAND

Digi TrustFence™
IOT Device Security

Embedded	Cellular	RF	WDS	Cold Chain	Device Cloud	Technical Services
ConnectCore® 6UL	TransPort® LR54	Digi XBee® Cellular LTE Cat 1	TrustFence Security Audit	Honeycomb	Digi Remote Manager	Digi Security Center Scanning & Reporting
ConnectCore® 6	TransPort® LR11	Digi XBee® Cellular LTE Cat M1		FreshTemp		Professional Services and Support
	TransPort® LR21	Digi XBee® Cellular NB-IOT				
	TransPort® LR31					
	TransPort® LR54R					

IOT SECURITY – BALANCE BETWEEN ECONOMIC COST AND BENEFIT

FOUR KEY THREATS FOR IOT DEVICES



INCREASING PUBLIC ATTENTION ON IOT SECURITY

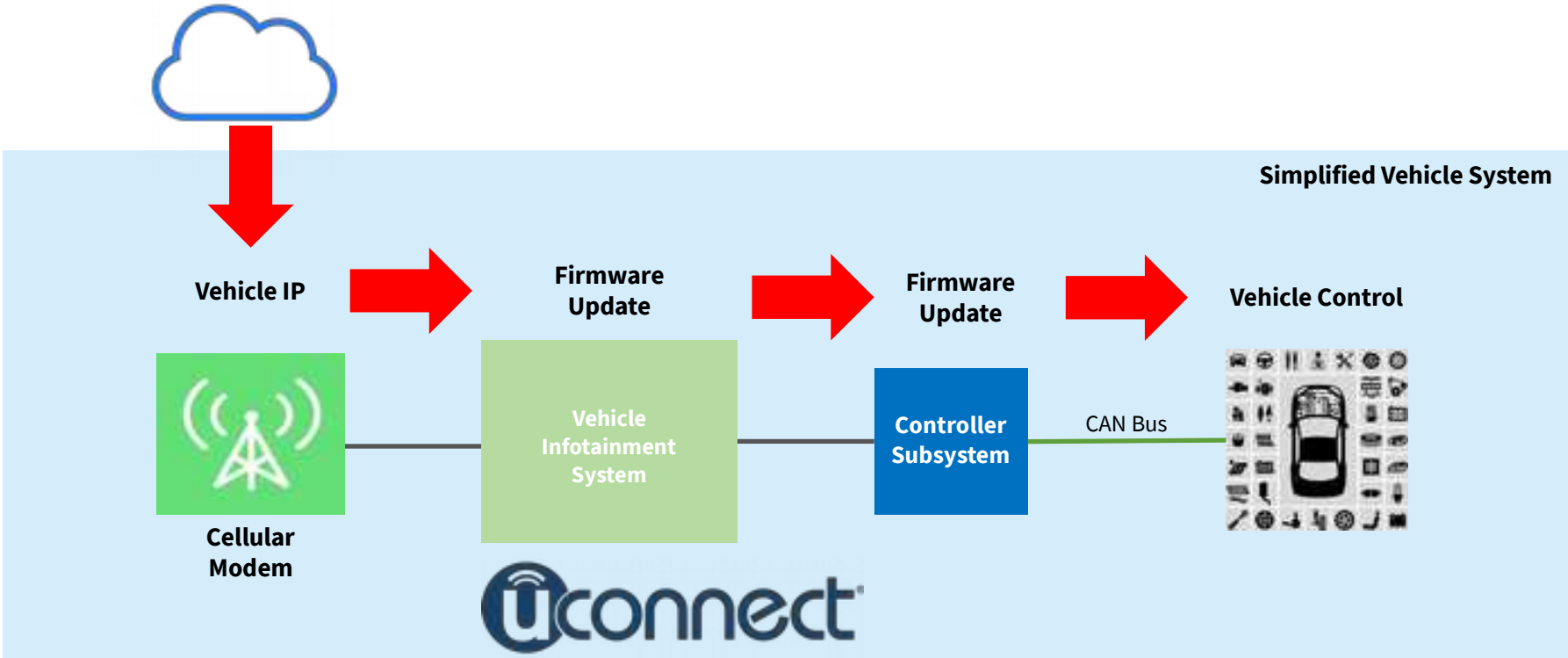
- FBI recently issued PSAs specifically related to IoT/connected device security concerns
  - I-091015-PSA INTERNET OF THINGS POSES OPPORTUNITIES FOR CYBER CRIME
  - I-031716-PSA Motor Vehicles Increasingly Vulnerable to Remote Exploits
- FTC released staff report urging adoption of best practices for security related design aspects of connected devices
- ICS issued advisories for software update and mitigation guidance regarding specific vulnerabilities present in connected devices such as hospital medical equipment and HVAC controllers
- Various examples demonstrating the vulnerability of connected device applications were widely publicized
  - Connected cars, ODB-II dongles, medical devices, CCTV cameras, baby monitors, HVAC units …

EXAMPLES: CONNECTED VEHICLE DEVICE ISSUES

- Widely publicized Fiat-Chrysler uconnect issue with Jeep Cherokee SUVs
  - Vehicles provide cellular connectivity for connected services
  - “Authentication” was mainly provided through the IP address of the vehicle
  - Access allowed silent update of the vehicle’s entertainment system firmware
  - Entertainment system was connected to another controller with CAN bus access
  - Modified firmware on entertainment system updated the controller firmware
  - Updated controller firmware allowed controlling critical vehicle functions via CAN bus
- Led to plans to introduce new legislation addressing digital attacks and privacy
- Other connected vehicle systems are already targets as well
  - For example, telematics solution in commercial vehicles

> *Recall Alert: Fiat Chrysler is recalling 1.4 million hackable vehicles. Check affected cars: http://t.co/sErjGgCxqL pic.twitter.com/8HuTxKYfY0*
> *— CNNMoney (@CNNMoney) July 25, 2015*

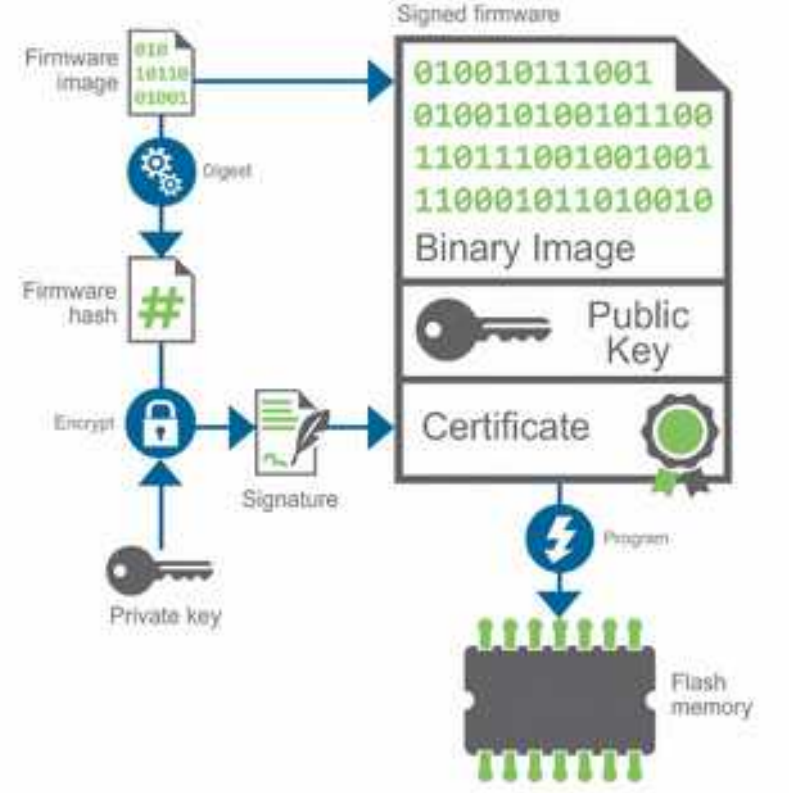
UCONNECT SYSTEM EXPLOIT



SECURE BOOT

- Secure Boot ensures authenticity and integrity of a device's boot image(s)
  - The firmware was created by a trusted source
  - The original image was not modified
  - CPU is booting a trusted bootloader
  - The bootloader is loading a trusted Linux kernel
  - The Linux kernel is mounting a trusted user space
- The implementation is done around NXP's High Assurance Boot (HAB)
  - Public key cryptography (RSA)
  - Digital signatures
- Additionally, the firmware can be encrypted
  - Signing and encrypting firmware is different and has different purposes

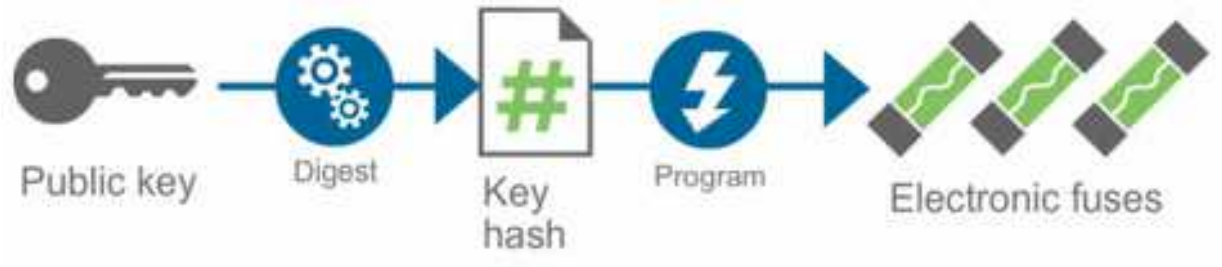
SECURE BOOT



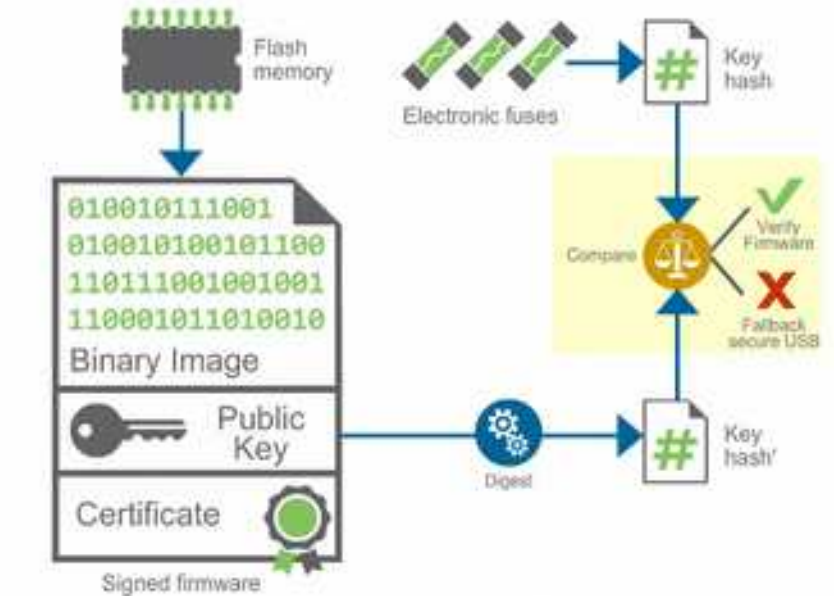
- Image Signature
  - Create hash of the firmware
  - Create signature by encrypting firmware hash using private key
  - Signature + signatory information = certificate
  - Attach certificate + public key to the binary firmware image to form the final signed image
  - Program signed firmware image to Flash Memory
- This process is fully automated
- Enabled by default

SECURE BOOT

- Additional Preparation
  - Create hash from public key
  - Program public key hash to eFuses during manufacturing
- Used during image verification process

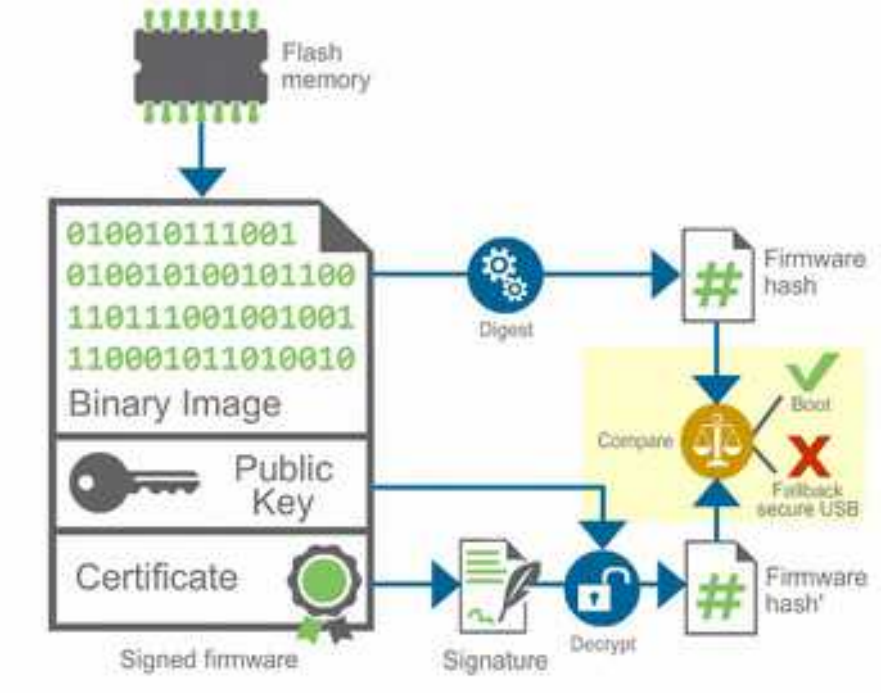


SECURE BOOT



- Image Validation during boot
  - Public key stored in the signed firmware image is validated by comparing its hash against a value stored in the eFuses
- Now we have established trust in the public key

SECURE BOOT



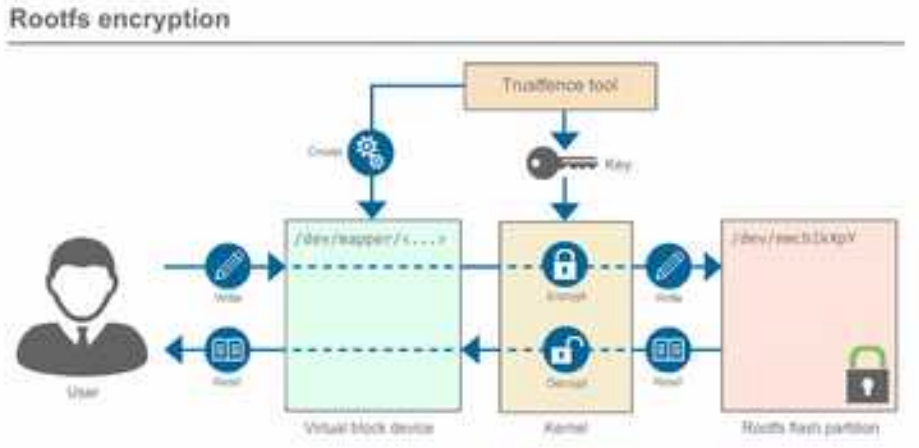
- Image Validation during boot
  - Public key is used to decrypt hash on the certificate
  - This hash is compared with hash computed from the image data
  - If they match, the device boots. If they do not match, the boot is aborted

Additionally, you can encrypt signed images to achieve even higher degree of security!

Secure Filesystem & Storage

- The ability of the system to encrypt the root and any other filesystem
- The implementation uses Linux encryption infrastructure dm-crypt
  - Encrypts/decrypts block devices on the fly
- Keeping the encryption key secure is crucial
  - The encryption key is encrypted by the Master Key of the processor
- At boot time, an application, running in a ramdisk:
  - Handles the key
  - Calls cryptsetup/cryptomount
  - Calls switch root
- Implemented on the CC6 / eMMC flash to encrypt root file system partition
- Filesystem encryption on NAND flashes (CC6UL) is more challenging and will be added in future releases

Secure Filesystem – Rootfs encryption



- Features
  - DEY provides encryption functionality when the image is flashed. No need to encrypt rootfs befo deploying it
  - Digi implemented specific tool for key handling and encryption at runtime
  - Kernel performs underlying encryption and decryption for data from the physical block devic
  - Applications access the file system through a virtual block device
- Usage
  - Developers boot into a ramdisk console application to call TrustFence tool
- Fully implemented and documented!

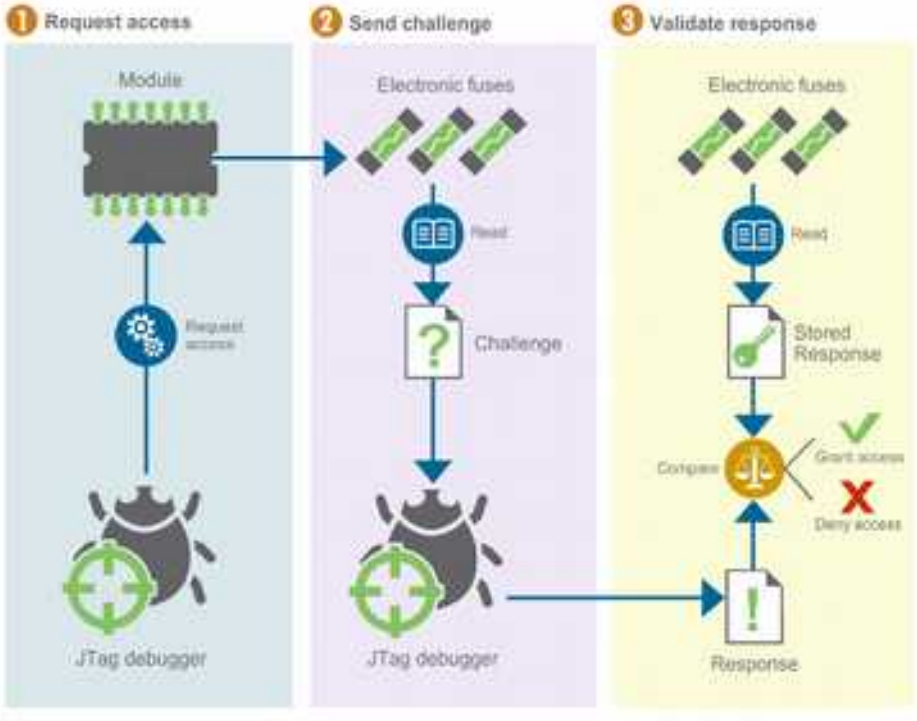
SECURE CONSOLE

- Attacking the (serial) console is one of the most typical attack vectors for embedded devices
- TrustFence allows to setup security for accessing the console in multiple levels:
  - Enabled: access to U-Boot shell over the serial console (default)
  - IO enabled: enabled/disabled based on the value of a GPIO
  - Secured: Access to console only with a passphrase, setup in the configuration of the Yocto project (cannot be accessed at OS runtime)
    - System will boot into silent mode and only if passphrase is entered after boot loader started access to console is enabled
  - Disabled: no console (recommended in production devices)
- U-Boot was extended to easily support these different console modes

SECURE JTAG

- i.MX6 family supports Secure JTAG modes
- Different levels of access can be set through the eFuses
  - Disabled JTAG: Maximum Security, no debugging nor boundary scan
  - Disabled Debugging: Allows boundary scan
  - Secure: Challenge-response required for debugging
  - Enabled: No restrictions. Default mode.
- Secure JTAG relies on challenge/response approach
  - Challenge based on processor-specific, unique ID assigned by NXP, programmed during manufactu
  - Secret Response provided by device manufacturer or at development time
  - Has to be programmed in the target and configured in the debug tool
- Secret Response must be unique to provide an effective solution
  - Unique key for all devices built by an OEM, or
  - A key per device, calculated from serial number, MAC, etc.

SECURE JTAG



- Preparation
  - Developer to calculate / define response key
  - Store response key in eFuses
  - Debugger has to be configured with response ke
- For debugging access
  - Debugger will request access
  - Challenge key is sent to debugger
  - If valid, debugger will send response key
  - Module will compare this with stored response key
  - If keys match, access is granted
- Fully implemented and documented!

TAMPER DETECTION

- Detect any unauthorized attempt to access the system, e.g. opening of the enclosure
- Tamper support for ConnectCore 6UL implemented in MCA includes:
  - Detect tamper events through IO pins
    - Tamper detection also works in low power modes, incl. power off, if battery backup (coin cell) p
  - Register tamper event(s) in non-volatile memory of MCA
  - Alert host CPU (IRQ, wake up, etc.) when tamper event occurs
  - Respond to tamper attack with custom actions such as erasing critical data partition and keys in flash
- Tamper pins
  - Two interfaces available (tamper 0 and tamper1)
    - 1 x Tamper pin to detect event
    - 1 x Tamper output (optional) - can be used to e.g. cut power of peripheral

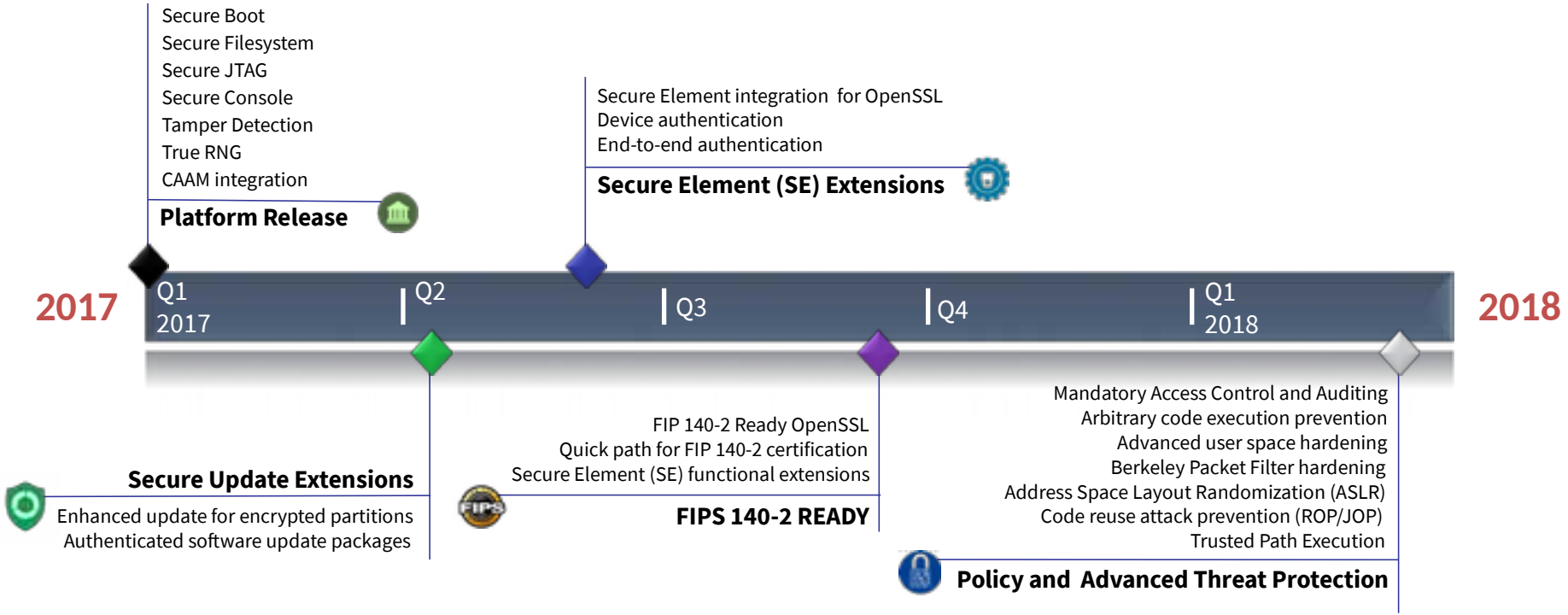
TRUE RANDOM NUMBER GENERATOR

- The i.MX6 has a True Hardware Random Number Generator
  - NIST compliant
- This is a critical component for the security of the system
  - Used for password creation, encryption and key management
- What has Digi done?
  - Ability to enable and disable it (it is disabled by default!!)
  - Made the hardware generator accessible through rng-tools (rngd)
    - “/dev/urandom” and “/dev/random” will benefit from that

CAAM & USER LAND

- The i.MX6 comes with a cryptographic engine that accelerates cryptographic operations
  - CAAM = Cryptographic Accelerator and Assurance Module
  - Cryptographic authentication (hash, MAC, ICV checking…)
  - Authenticated encryption algorithms (AES-CCM)
  - Symmetric key block ciphers (AES, DES, 3DES)
- If enabled, the kernel crypto-api will use it to offload the CPU
- What has Digi done?
  - Ability to enable and disable it (it is disabled by default)
  - Include crypto-dev driver so user space applications like OpenSSL can use crypto-api APIs.
  - Test it and characterize it (performance and power consumption) to understand the tradeoffs.
  - User applications can use it as well to offload security tasks

DIGI TRUSTFENCE™ ROADMAP (CY)



AT LEAST THREE KEY TAKEAWAYS

- Device security is as important as secure connections
  - Security by Obscurity does not work (anymore)
- Take ownership and care about locking down your device as much as you care about data privacy for connections
  - Implement Secure Boot, Secure Storage, Secure Ports, and Secure Updates
  - Device Security aspects will further affect how you manufacture products
- Security requirements will change over time, make sure your products have a chance to support those changes
  - Choose a hardware and software architecture with longevity in mind
  - Plan for and integrate a secure software upgrade path
  - Don't cost-optimize upgrade capabilities away, e.g. memory

Security issues directly affect your customers and the reputation + success of your company

Questions?

Neil PARKER
Account Manager Embedded

neil.parker@digi.com

