



FTF 2016
TECHNOLOGY FORUM

KINETIS MCU SECURITY TECHNOLOGY

FTF-DES-N1951

DONNIE GARCIA
SYSTEMS & APPLICATIONS ENGINEER
FTF-DES-N1951
MAY 16, 2016

PUBLIC USE

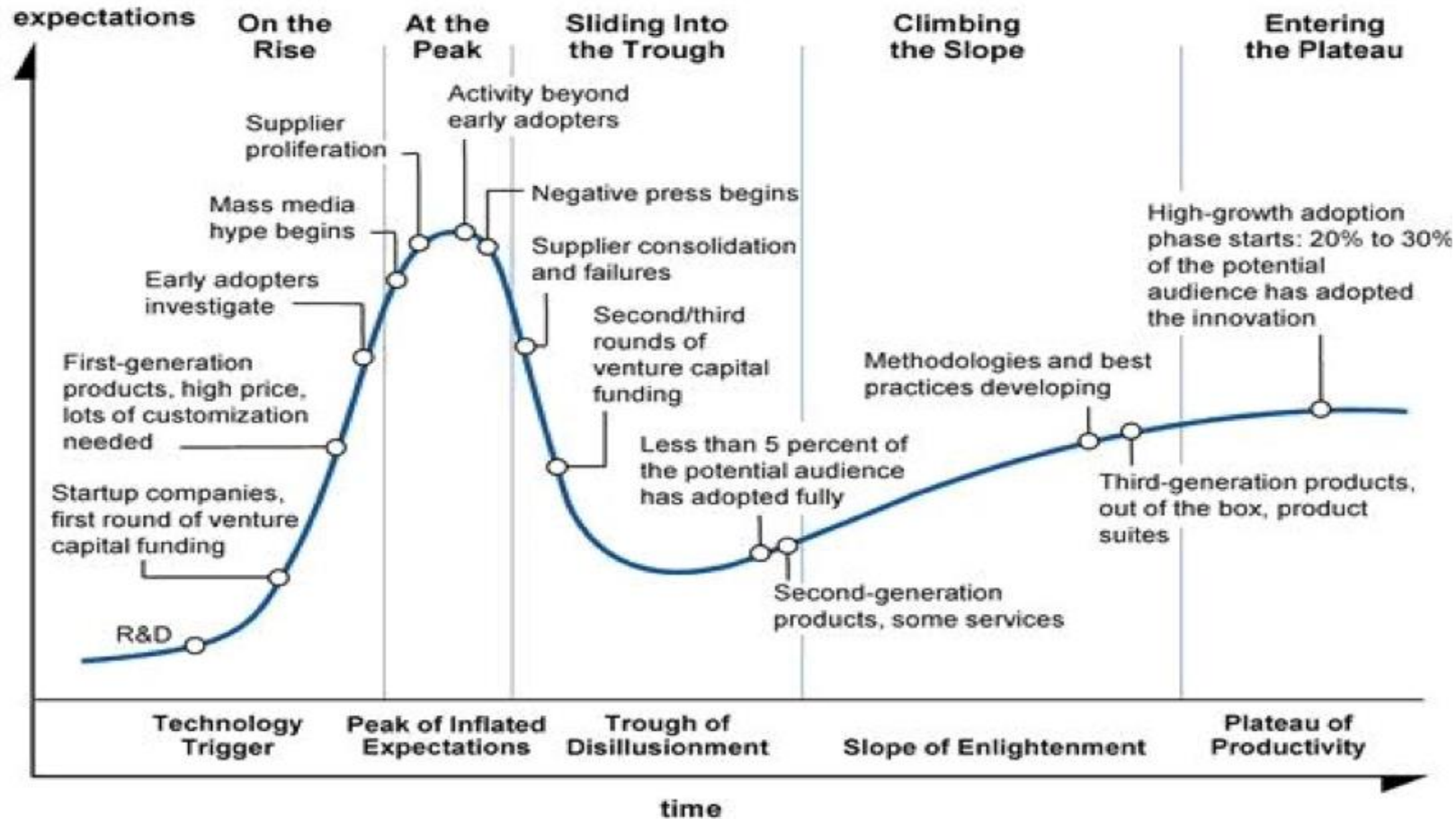


AGENDA

- The IoT
 - Security Challenges
- Security for Payment Applications
- Kinetis Security Technology
- Edge device implementation
- Conclusion

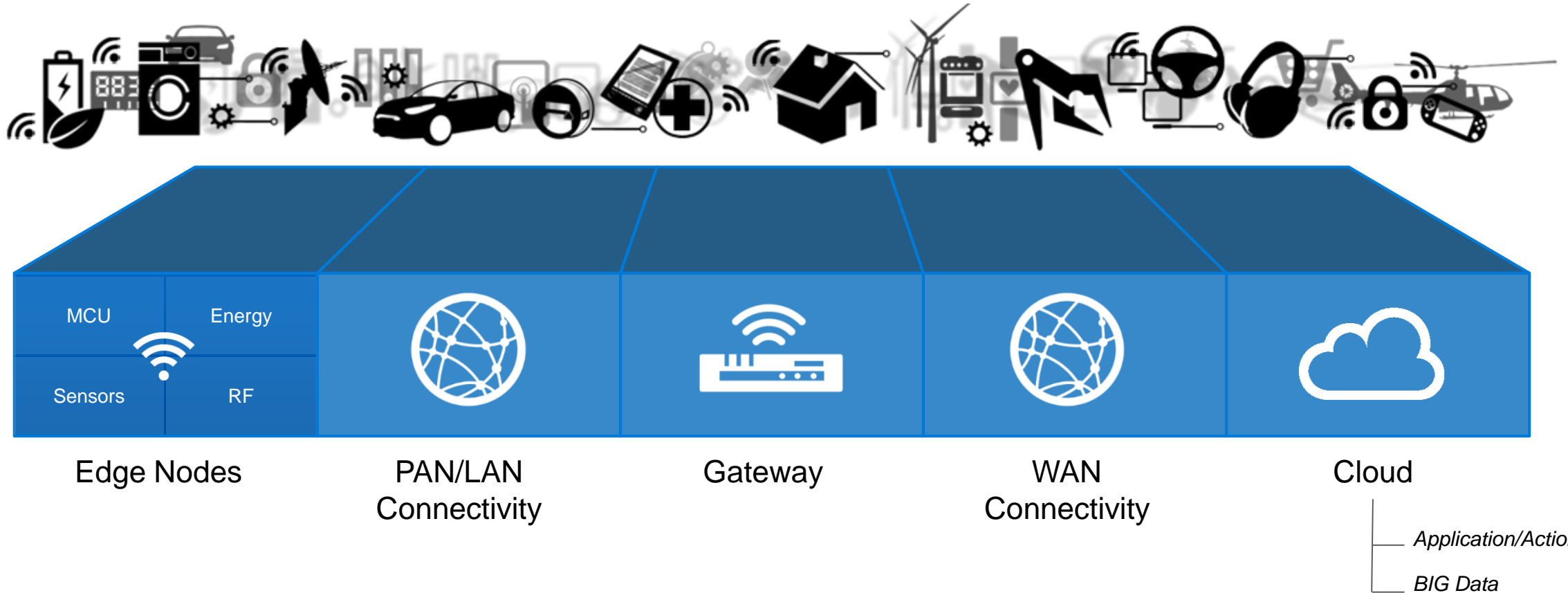


Technology Adoption

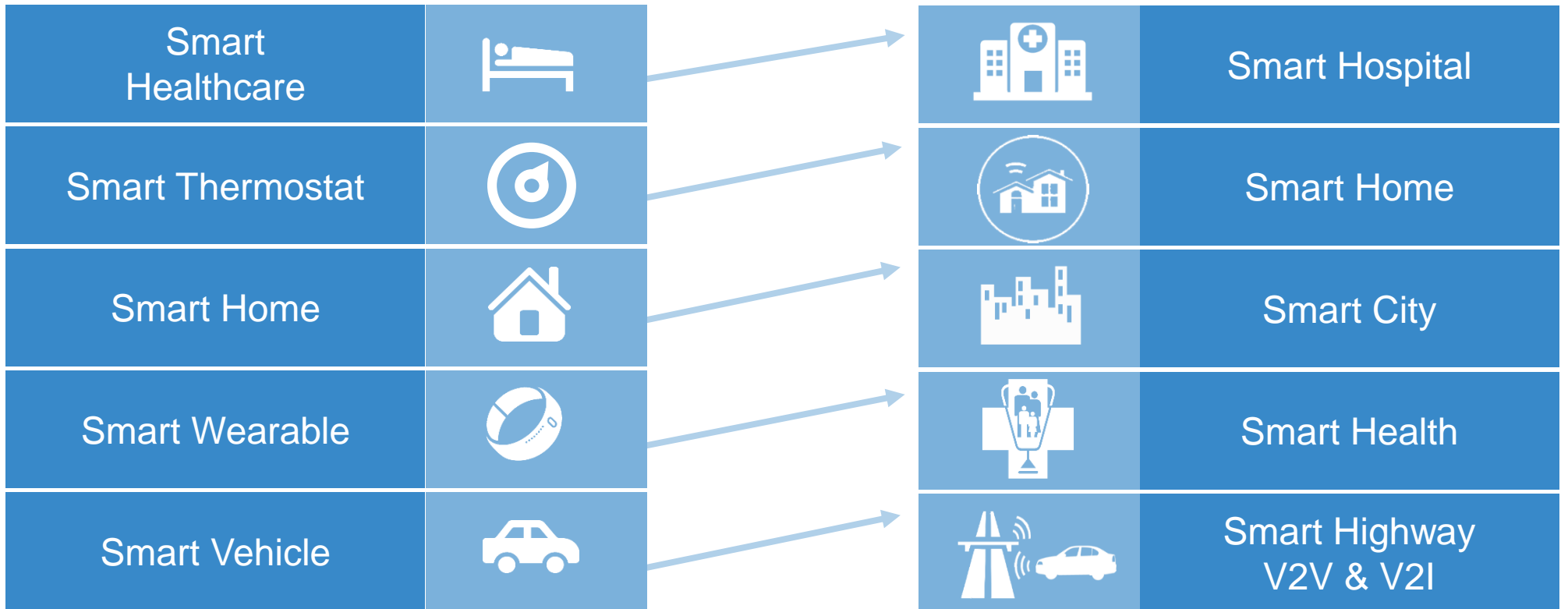


<http://semiengineering.com/limiters-to-the-internet-of-things/>

Connecting 'Things at the Edge' to the 'Cloud'

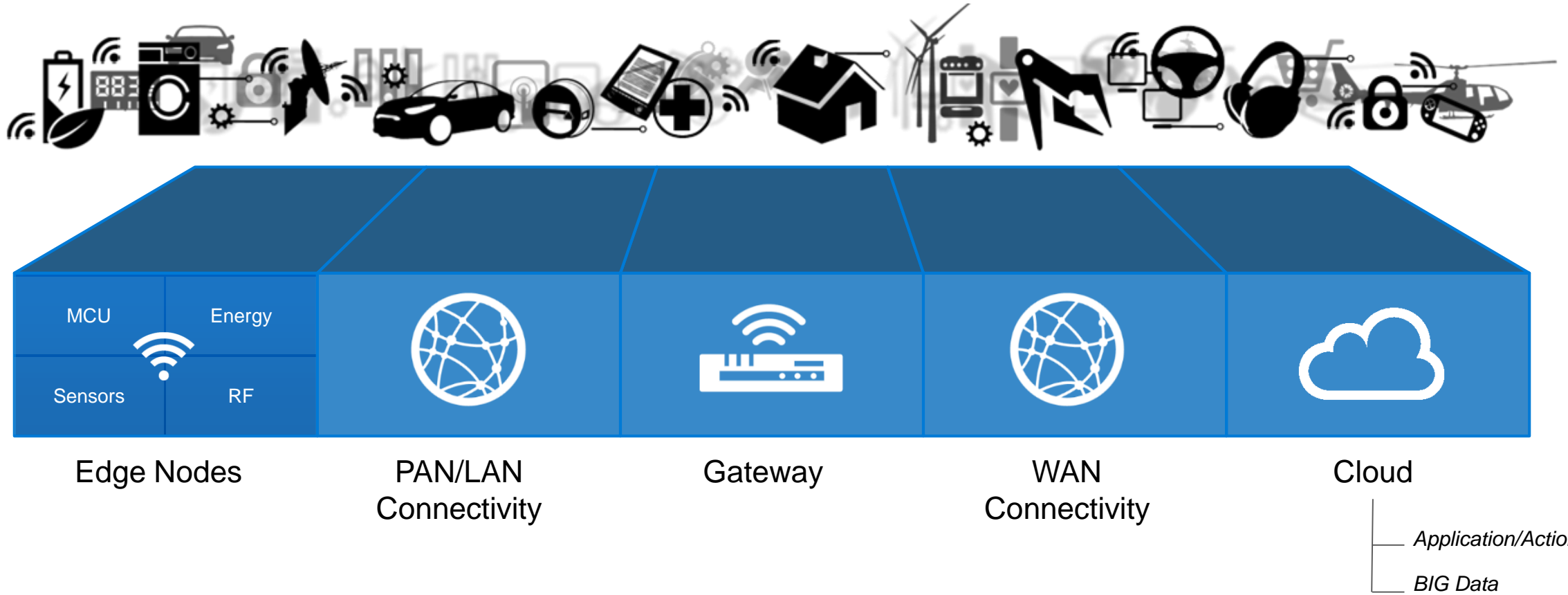


Internet of Tomorrow → Smart, Connected and Secure

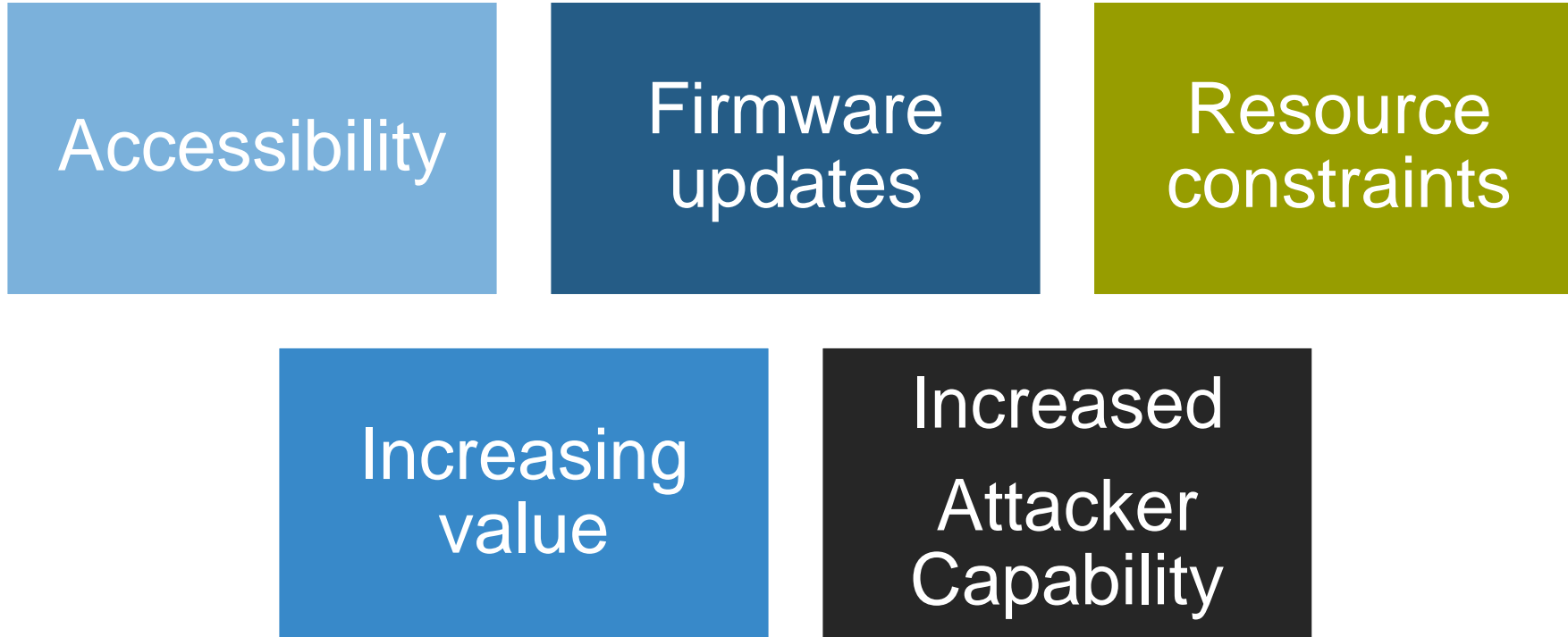


Increasing complexity of data collection,
handling & processing for delivering value added information.

Connecting 'Things at the Edge' to the 'Cloud'



Security Risk Multipliers



Security Needs?

Wearable Internet of Things (IoT) Device

- **Wearable LED Display**

- Battery operated
- Worn on the wrist
- Wireless connectivity
- Sensor (Accelerometer)

- **Limited Security Needed**

- No financial harm
- No legal ramifications
- Minor disruption

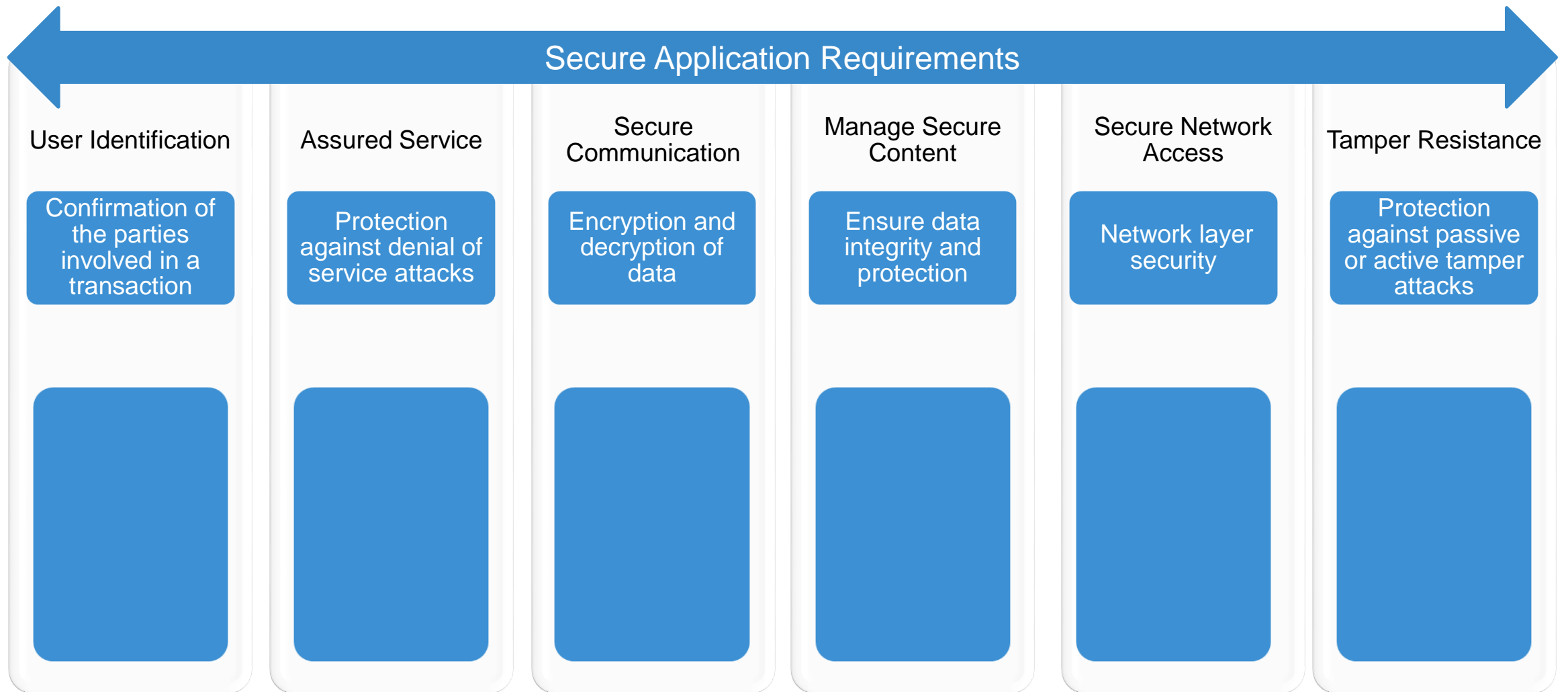
- **Wearable Health Tracker**

- Battery operated
- Worn on the wrist
- Wireless connectivity
- Sensors (GPS, Accelerometer, etc.)
- Data logging functionality

- **Significant Security Needed**

- Significant financial harm
- Serious legal ramifications
- Major disruptions

Payment Applications



Payment Applications

Secure Application Requirements

User Identification

Confirmation of the parties involved in a transaction



Assured Service

Protection against denial of service attacks



Secure Communication

Encryption and decryption of data



Manage Secure Content

Ensure data integrity and protection



Secure Network Access

Network layer security



Tamper Resistance

Protection against passive or active tamper attacks



Leveraging Standards and Certifications

- PCI PTS (PIN Transaction Security) – The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. [2] This includes system level requirements for hardware and software. Compliance with the PCI PTS security requirements reduces the likelihood and limits the potential impact of PIN compromise by establishing the minimum criteria for the design and manufacture of secure PEDs. The PCI PTS security requirements apply to Point of Sale (POS) devices and Encrypting PIN Pads (EPPs) used in ATMs and kiosks. [1]
- EMV (Europay, Mastercard, Visa) - EMVCo exists to facilitate worldwide interoperability and acceptance of secure payment transactions. It accomplishes this by managing and evolving the EMV® Specifications and related testing processes. This includes, but is not limited to, card and terminal evaluation, security evaluation, and management of interoperability issues. [2]
 - 3rd party lab certifications – the PCI Security Standards Council has established a tight (but not limiting) set of geographically disperse 3rd party certification laboratories. These labs require detailed supporting documents with each submission as well as thorough testing of the hardware. This can be accomplished in a time and cost effective manner.

[1] https://www.pcisecuritystandards.org/assessors_and_solutions/pci_recognized_laboratories

[2] <https://www.emvco.com/>

Payment Requirements Landscape

- Source: <https://usa.visa.com/dam/VCOM/download/merchants/visa-PED-Requirements-2013.pdf>
- Payment devices must be compliant to PCI (payment card industry) standards
 - These standards are updated every 3 years and if there is a significant threat
 - Whenever retailers purchase new POS devices, they are advised to purchase devices that have passed the latest standard
 - Every 7 years, the standard is retired and retailers are advised to replace the devices
- PCI security changes over time

- **V1 PCI PED or EPP Security Requirements*** - Baseline security requirements with independent lab evaluation. Tamper evident controls required to easily detect unauthorized access to the device.
- **V2 PCI PED or EPP Security Requirements** - Improved tamper evident controls by requiring tamper responsive controls that detect intrusion attempts and subsequently destroys the content, including encryption keys.
- **V3 PCI PTS POI Security Requirements** (includes PED and EPP combined) Introduced secure read and exchange of data (SRED) capabilities that ensures cardholder account data is encrypted at the point of acceptance. (Note: Visa has no mandates for the use of SRED but implementation is a best practice)
- **V4 PCI PTS POI Security Requirements** (includes PED and EPP combined) - Improves testing evaluations and incorporates controls that address communication vulnerabilities that can be remotely exploited to gain access to sensitive data or resources within the device.

**Note there are also V1 HSM and UPT security requirements. Currently these requirements are designated as best practices for their use.*

PCI Security Requirements: Related ISO Standards

Publication
ISO 9564: Personal Identification Number Management and Security
ISO 11568: Banking – Key Management (Retail)
ISO 11770–2: Information Technology – Security Techniques – Key Management, Part 2: Mechanisms Using Symmetric Key Management Techniques
ISO 13491: Banking – Secure Cryptographic Devices (Retail)
ISO 16609: Banking – Requirements for message authentication using symmetric techniques
ISO/IEC 18033-3: Information Technology – Security techniques – Encryption algorithms – Part 3: Block Ciphers
ISO TR19038: Guidelines on Triple DES Modes of Operation

Source: https://www.pcisecuritystandards.org/documents/PCI_PIN_Security_Requirements.pdf

PCI Security Requirements : Related ANSI Standards

Publication
ANSI X3.92: Data Encryption Algorithm
ANSI X9.24 (Part 1): Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
ANSI X9.42: Public-key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography
ANSI X9.44: Key Establishment Using Integer Factorization Cryptography
ANSI X9.62: Public Key Cryptography for the Financial Services ECDSA
ANSI X9.63: Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography
ANSI X9.65: Triple Data Encryption Algorithm (TDEA) Implementation
ANSI TR-31: Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

Source: https://www.pcisecuritystandards.org/documents/PCI_PIN_Security_Requirements.pdf

PCI Security Requirements: Related FIPS, NIST, EMV and PCI Standards

Publication

EMV: Integrated Circuit Card Specification for Payment Systems, version 4.2 (June 2008)—Book 2: Security and Key Management

FIPS PUB 140–2: Security Requirements for Cryptographic Modules

NIST Special Publication 800-22: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications

Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements

Payment Card Industry (PCI) PIN Transaction Security Point of Interaction Modular Derived Test Requirements

Payment Card Industry (PCI) Hardware Security Module (HSM) Security Requirements

Payment Card Industry (PCI) Hardware Security Module (HSM) Derived Test Requirements

Source: https://www.pcisecuritystandards.org/documents/PCI_PIN_Security_Requirements.pdf

Point of Sales

A Scalable Portfolio to Address a Wide Range of POS Solutions



Power efficient, secure and connected solutions

Risk Assessment

- Unbreakable security
 - With sufficient time, effort, resources, and motivation, security implementation can be defeated
 - Where is the tipping point between the effort to defeat the security and the possible payout for breaking it?
- Security should be based on a specific threat
 - What needs to be protected?
 - Why is it being protected?
 - Who is it being protected against?

Security Planning – Attacks

- Insider Attacks
 - Financial gain / fraud
 - Revenge / payback
 - Blackmail
- Midnight Attacks
 - Take place during a small window of time
- Focused Attacks
 - Time, money, and resources are not factors

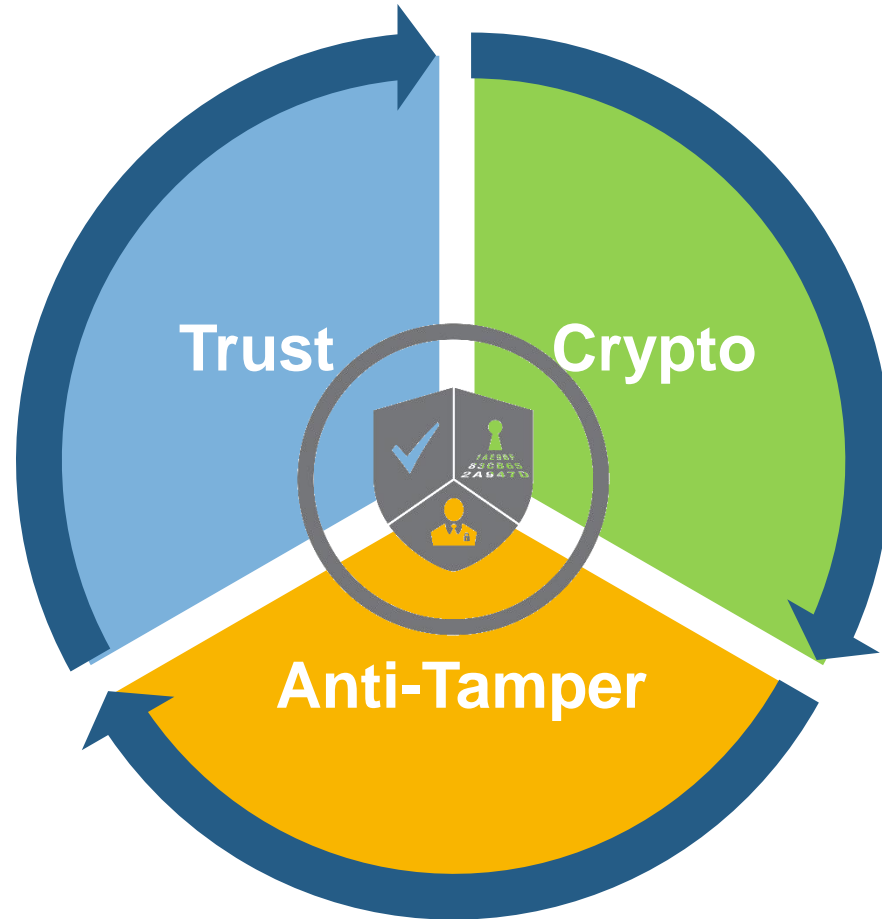


Security Planning – Attackers

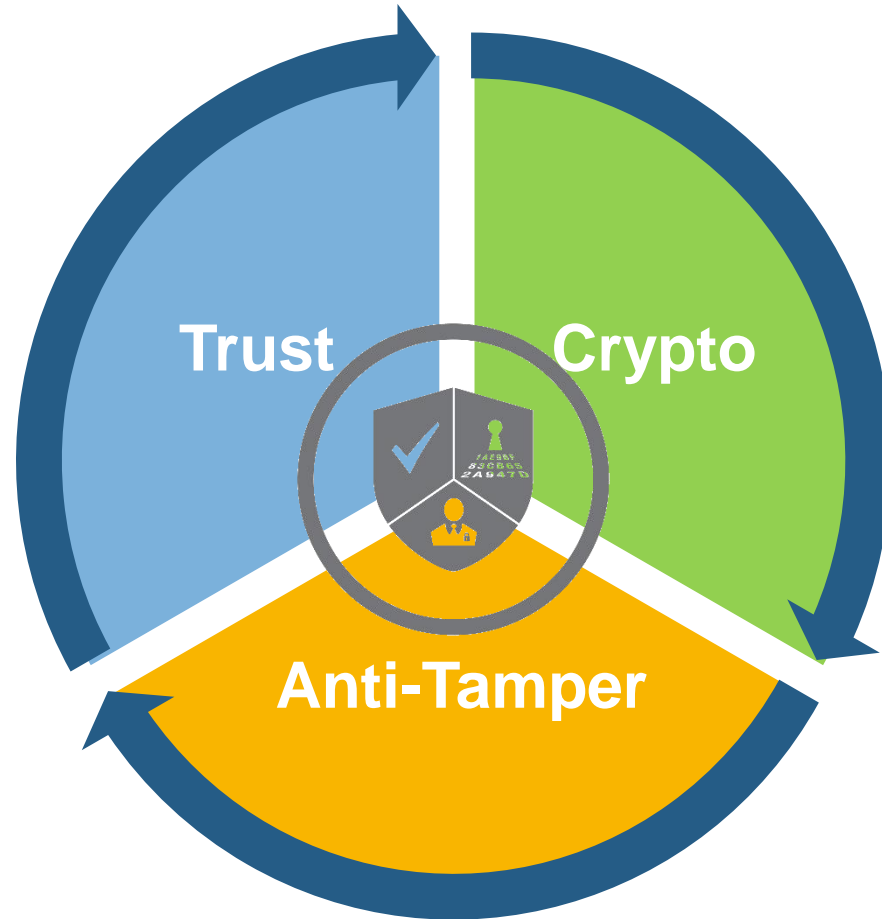
- Outsiders (Curious Hackers)
 - Intelligent, but limited knowledge of the system
 - Attempt to use existing security weaknesses
- Insiders (Professionals / Academics)
 - Have significant specialized technical experience
 - Access to sophisticated tools and instrumentation
- Organizations (Crime Syndicates / Governments)
 - Specialists with significant funding resources
 - Advanced analysis tools and in-depth analysis and attacks



Security Technology

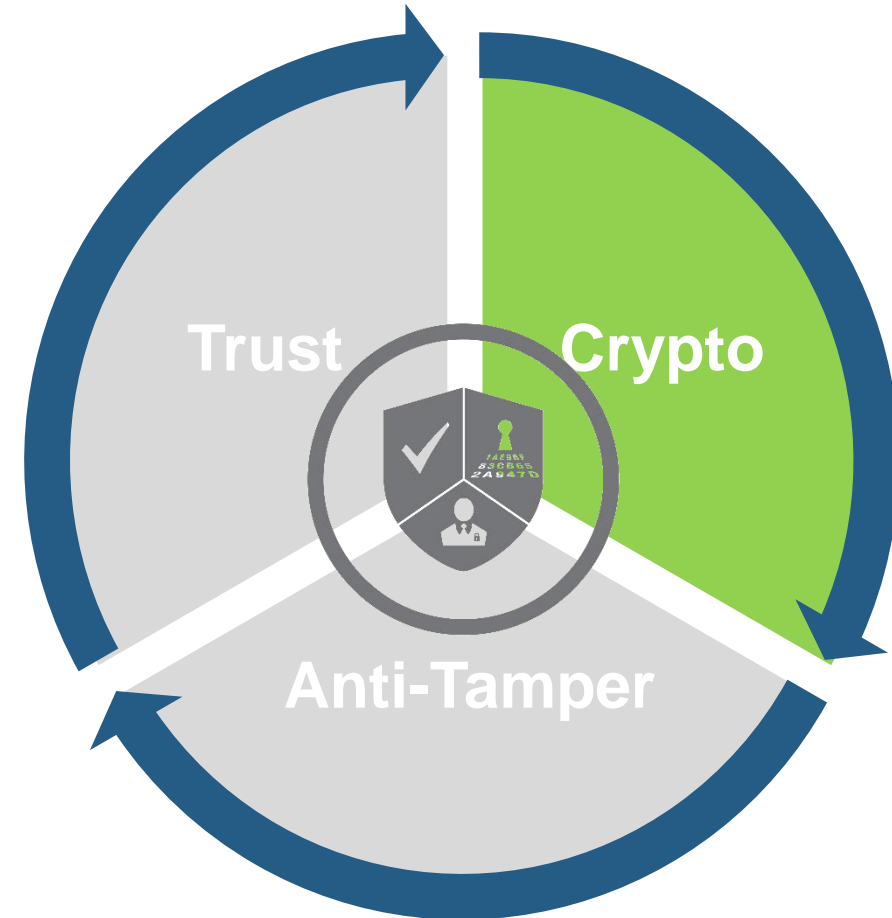


NXP'S Security Technology



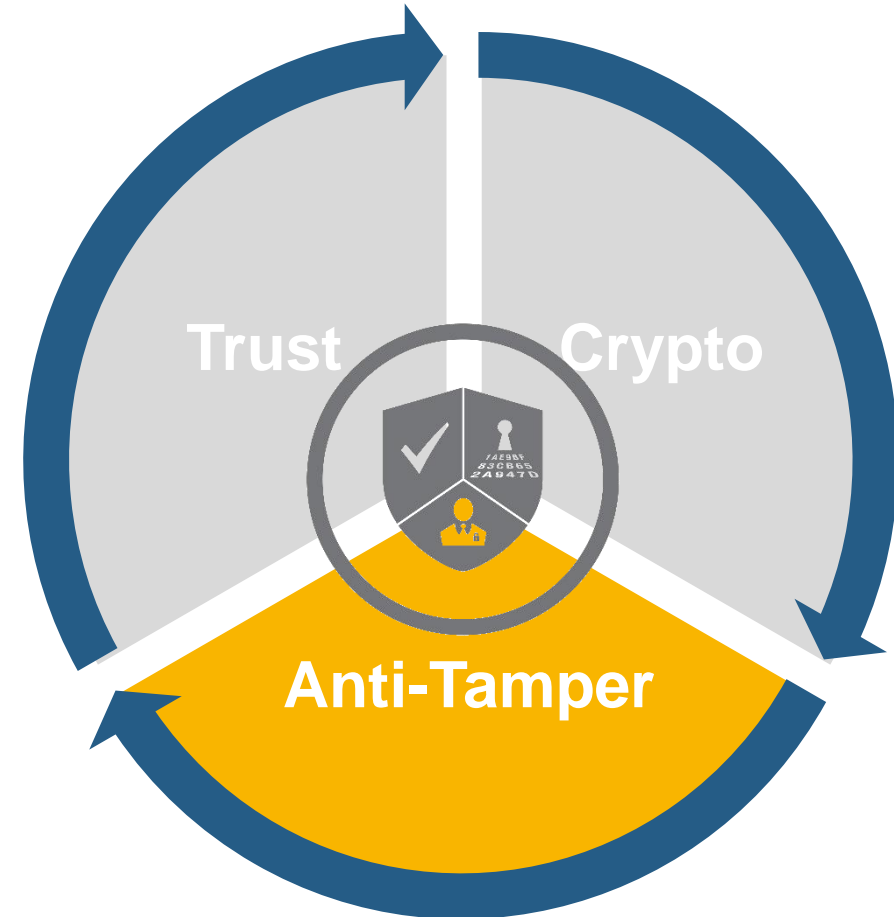
Cryptography

- The science of protecting data through encoding and decoding
- Symmetric Encryption
 - DES/DES3, AES
- Asymmetric Encryption
 - RSA, ECC
- Hashing
 - CRC, MD5, SHA
- True Random Number Generation
- Security Protocols
 - SSL, HomeKit, Thread



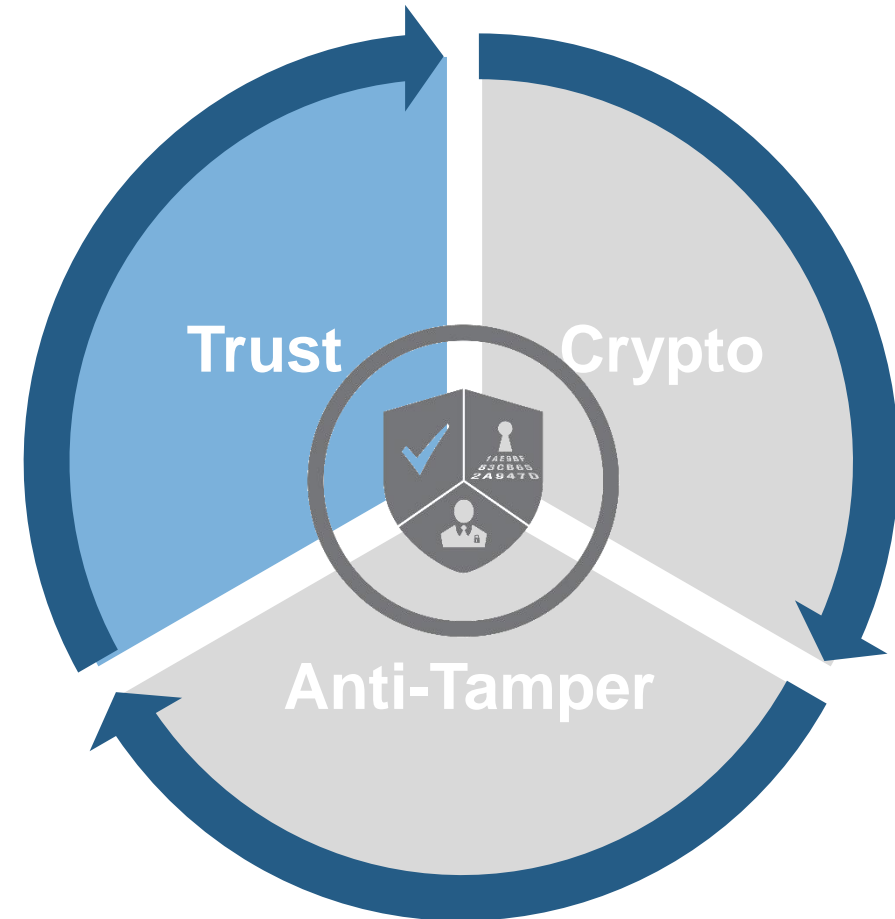
Anti-Tamper

- Proactive monitoring of physical and environmental system attacks
- Tamper Detection
 - Physical
 - Enclosure intrusion
 - Drilling and probing
 - Environmental
 - Voltage
 - Temperature
 - Frequency
- Secure Storage



Trust

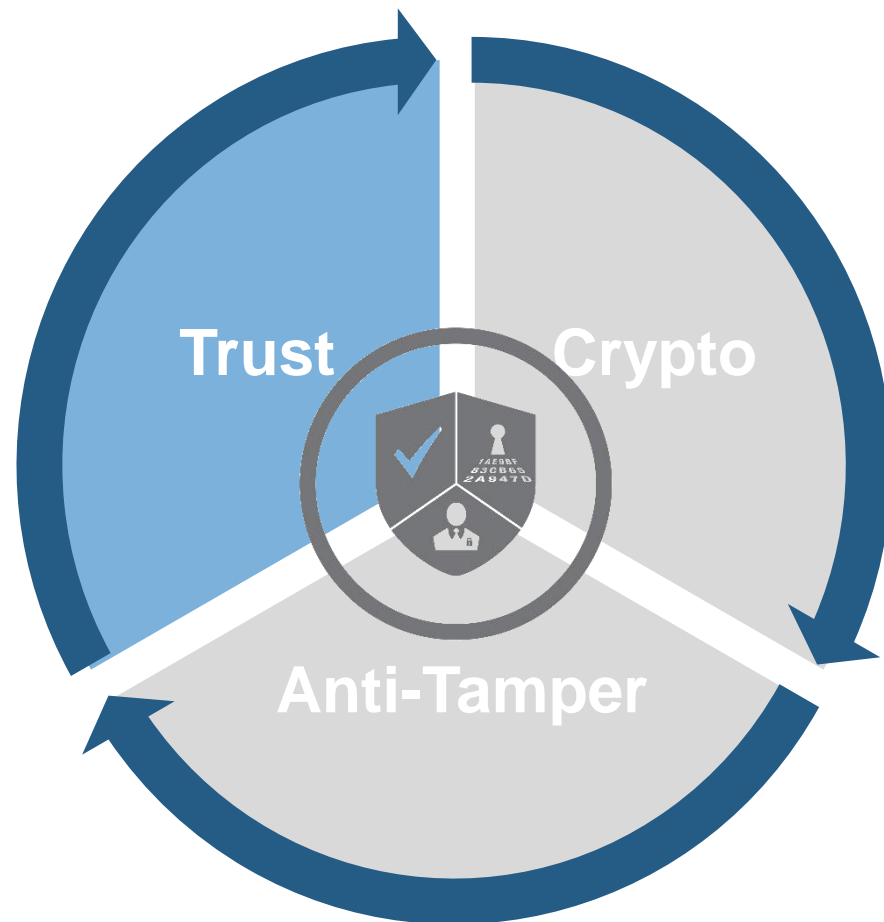
- The assurance that only access from a reliable source will occur
- Code I/P Protection
 - Internal memory protection
 - External memory protection
- Debug Port Protection
- Authentication
 - Software updates
 - Device verification
- Secure Boot



EDGE DEVICE IMPLEMENTATION



Trust: Ensuring Operation from Reliable Sources



Trust: All Kinetis Devices Support

FEATURE	BENEFIT	DETAILS	ENABLEMENT
On chip Flash security and protection mechanisms	Protection from firmware theft and application cloning	Ability to prevent debug access to the processor. Ability to set a 64-bit key to regain debug access.	AN4507: “Using the Kinetis Security and Flash Protection Features”
Debug port configuration	Block external access to debug or flash re-programming	Flash security disables debug port. JTAG pins can also be disabled via software	AN4507: “Using the Kinetis Security and Flash Protection Features”
Unique ID	Software can be used to uniquely identify the MCU as a trusted device	Kinetis L series: 80-bit unique ID All Others: 128-bit unique ID	
Boot from internal memory only	Controlled boot conditions to avoid attacks that use external memories	Boot from on-chip flash or ROM only	

Trust: A Handful of Kinetis Devices Support

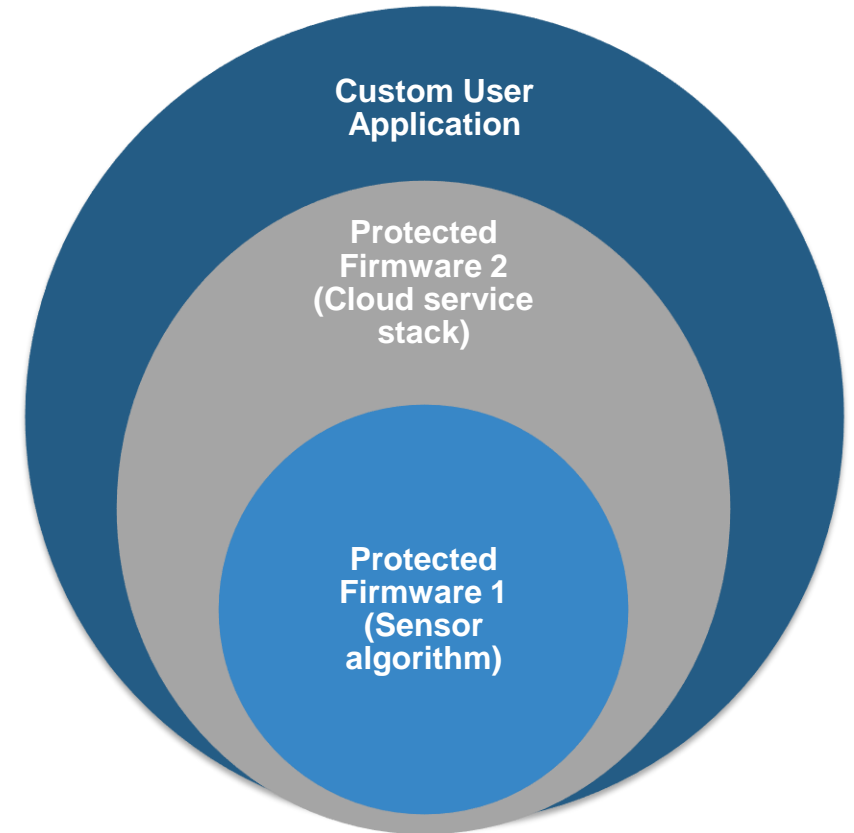
FEATURE	BENEFIT	DETAILS	ENABLEMENT
Execute and supervisor only access	Protection of software IP	Non-Volatile control registers to set access privileges of on chip flash resources. Supervisor or execute only access can be set for up to 64 different segments	AN5112: <i>“Using the Kinetis Flash Execute-only Access Control Feature”</i>
Encrypted firmware updates	Protection from firmware theft and application cloning	ROM enables encrypted image downloads for internal flash or external serial NOR. Code is stored in the clear on the device.	KBOOT
On-the-Fly AES Decryption (OTFAD)	Protection from firmware theft and application cloning	Code in external serial NOR flash can be stored encrypted in the external memory and is only decrypted as it is read by the processor	KBOOT

Flash Security and Protection Features

- Flash security and protection features are found on all Kinetis devices
- Security Features
 - Kinetis MCUs offer several levels of flash security
 - Flash security is a system-level feature
 - The flash is fully functional when secured (firmware updates are still possible if resident firmware is setup to program the flash)
 - Security effects are really a system level concern. The security setting determines what the SoC will allow.
 - Software IP is a large investment. Enabling security helps to protect that IP investment.
- Protection Features
 - Flash protection can be used to prevent accidental erase or programming
 - Initial protection values are loaded from the flash configuration field at reset

Execute-Only Application Code

- The concept of execute-only application code is:
- A primary developer (for example, Freescale or a 3rd-party software provider) creates useful, value added application(s) for a given MCU or MPU. Entry point and use information (for example, API details) is supplied, but source code is not. This code is assumed to be “trusted”.
- A method exists to load this software into a part without exposing it during the loading process and mark it “execute-only”.
- Other developers and/or users add more software to these parts and use these application(s).
- The user of the application(s) will not be able to see or expose any of the protected execute-only code.
- There may be multiple layers of “execute-only” application code added with all previously added layers protected.
- This feature is available on newer Kinetis devices and are controlled from the Flash FTF register set.

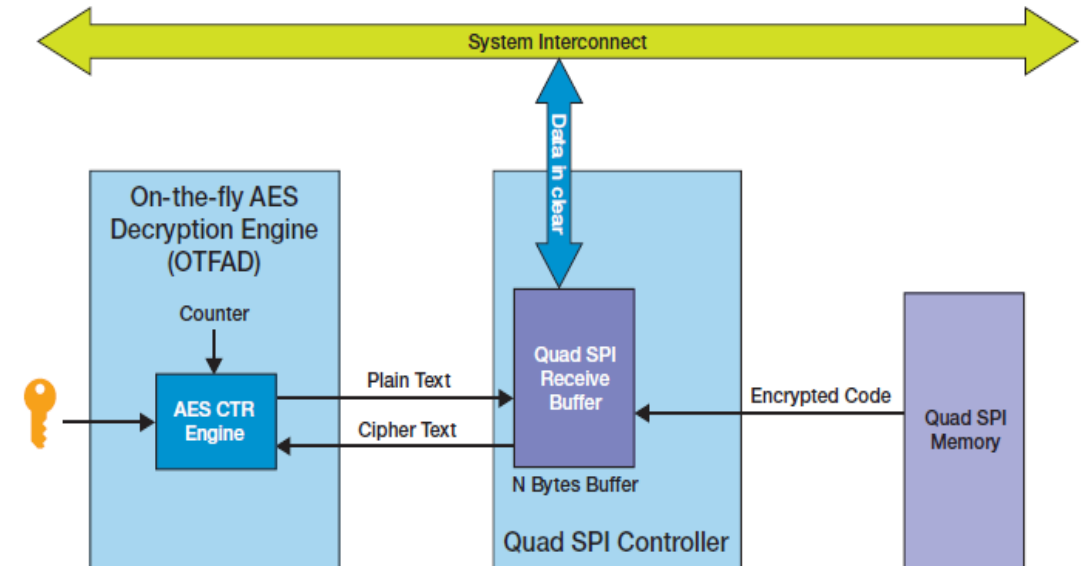


Encrypted Binary File Downloads (Kinetis K8x MCU Family)

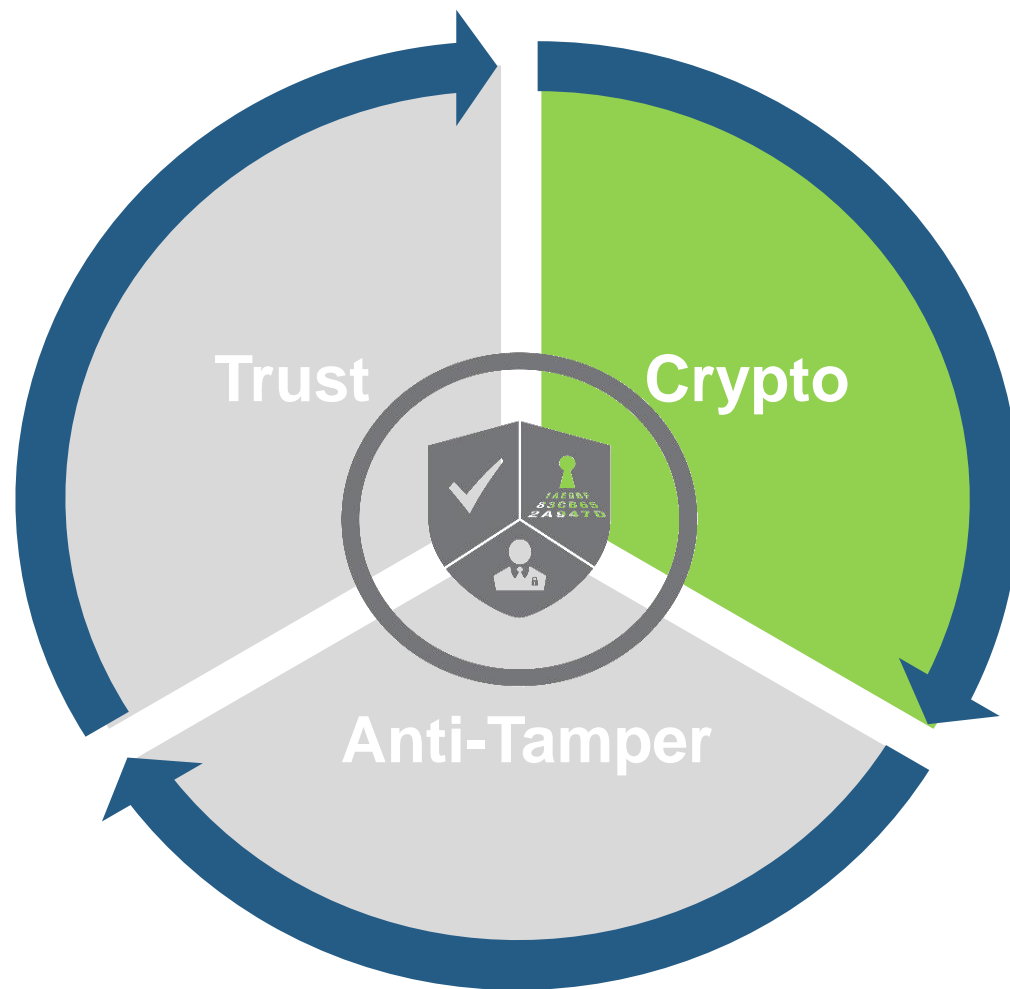
- The ROM supports downloading encrypted binary files in an Secure Binary (SB) file format (AES-128 encryption is used)
- Application is download encrypted, but stored to internal flash decrypted (there is also an option to download an encrypted file to external serial NOR flash too)
- A key value pre-programmed into the flash “eraseable program once” space is used for decryption
- Encrypted SB files can be downloaded when device is secure or unsecure, but if the device is secure, then the ROM disables all memory reads and writes with the exception of encrypted SB files.
- So if you enable security, encrypted binaries are the only way the ROM can be used to update the firmware
- Tools that generate encrypted binaries are available with the KBOOT software
- On Kinetis K81/K82 devices the LP Trusted Cryptography (LTC) module is used to decrypt the binary
- On Kinetis K80 devices the Memory Mapped Cryptographic Acceleration Unit (mmCAU) is used to decrypt the binary

On-The-Fly AES Decryption Features (Kinetis K8x MCU Family)




- Allows on-the-fly decryption of the encrypted code in Quad SPI
- Allows to Execute-in-Place encrypted code from Quad SPI
- Based on AES128-CTR Symmetric Algorithm
- OTFAD engine post decryption, transfers the data in clear back to QuadSPI Rx buffer that is then available for the system.
- Provides *anti-cloning* and *IP protection* capabilities by securing customer end product code and data
- Hardware support for 4 independent decryption segments, known as memory context
- Each context has a unique 128-bit key, 64-bit counter and 64-bit memory region descriptor



Crypto: Protecting Data with Encoding



Crypto: Algorithms/Protocols

	Required	Used
OTA secure firmware update Secure boot	RSA-2048 verify SHA-256 over firmware image	At each update At each boot
 HomeKit	SRP-3072 Ed22519 sign/verify Curve-25519 SHA-512 based KDF ChaCha20 cipher Poly-1305 MAC SHA-256	At first device pairing At first device pairing At each connection with accessory At each connection with accessory
 Thread	EC-JPAKE (NIST-P256) AES-128 CCM (TLS) HMAC-SHA256 based KGF SHA-256	At first device pairing
 AllJoyn	ECDHE-PSK ECDHE-ECDSA ECDHE-NULL NIST-P256 X509 Certificates SHA-256	At each connection

Kinetis MCU Hardware

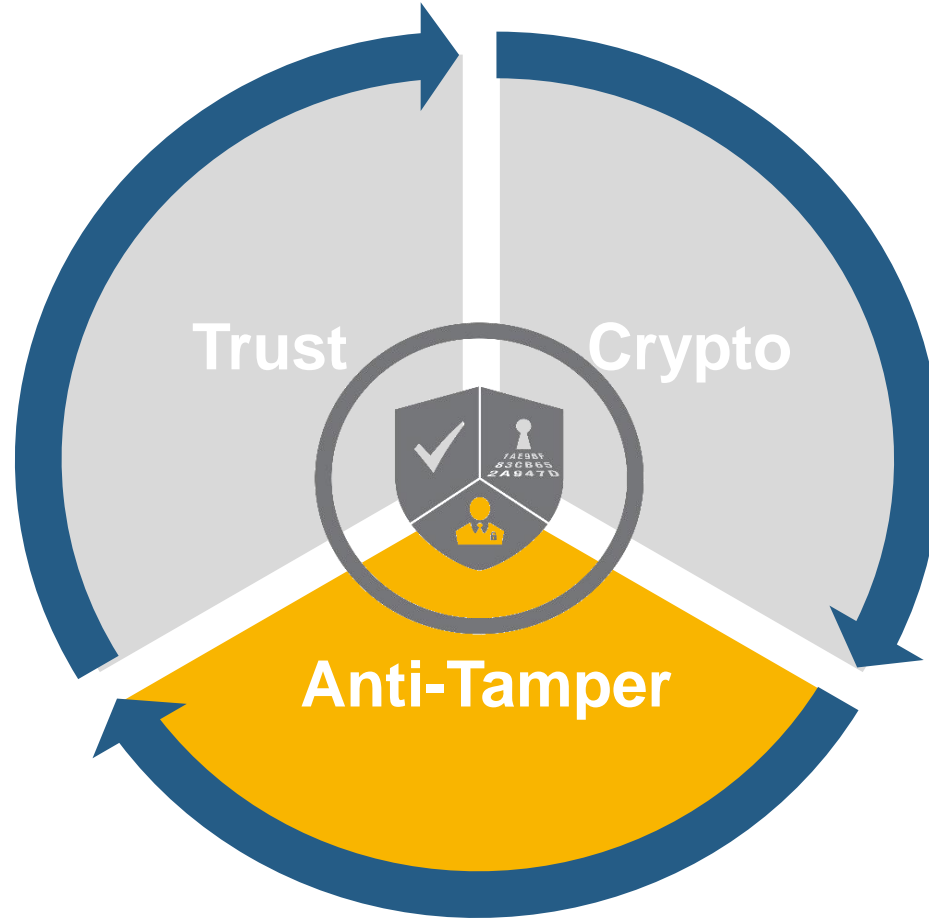
- Software
 - Any Kinetis device can use publically available cryptographic libraries for performing encryption, decryption, and hashing.
- Memory Mapped Cryptographic Acceleration Unit (mmCAU)
 - A hardware co-processor connected to the Private Peripheral Bus (PPB) used to accelerate software based cryptographic algorithms.
- LP Trusted Cryptography (LTC)
 - A DMA slave acceleration engine with dedicated hardware for each security algorithm that is supported.

Benefits of HW Crypto Vs. SW

	LTC	MMCAU
AES-CBC	15.4x	5.5x
AES-GCM	39.0x	1.5x
AES-CTR	13.4x	N/A
AES-CCM	15.8x	7.0x
Footprint	~10 KB smaller	~10 KB smaller
	LTC	MMCAU
3DES-CBC	81.8x	13.1x
Footprint	~ 2 KB smaller	~ 2.7 KB smaller

	LTC
RSA encryption	6.3x
RSA decryption	4.7x
Footprint	~ 5.5 KB smaller
	LTC
ECC 256 key generation	18.5x
EC-DHE key agreement	19.4x
EC-DSA sign	15.8x
EC-DSA verify	17.1x
Footprint	~ 2 KB smaller

Anti-Tamper: Detect and React to Attacks



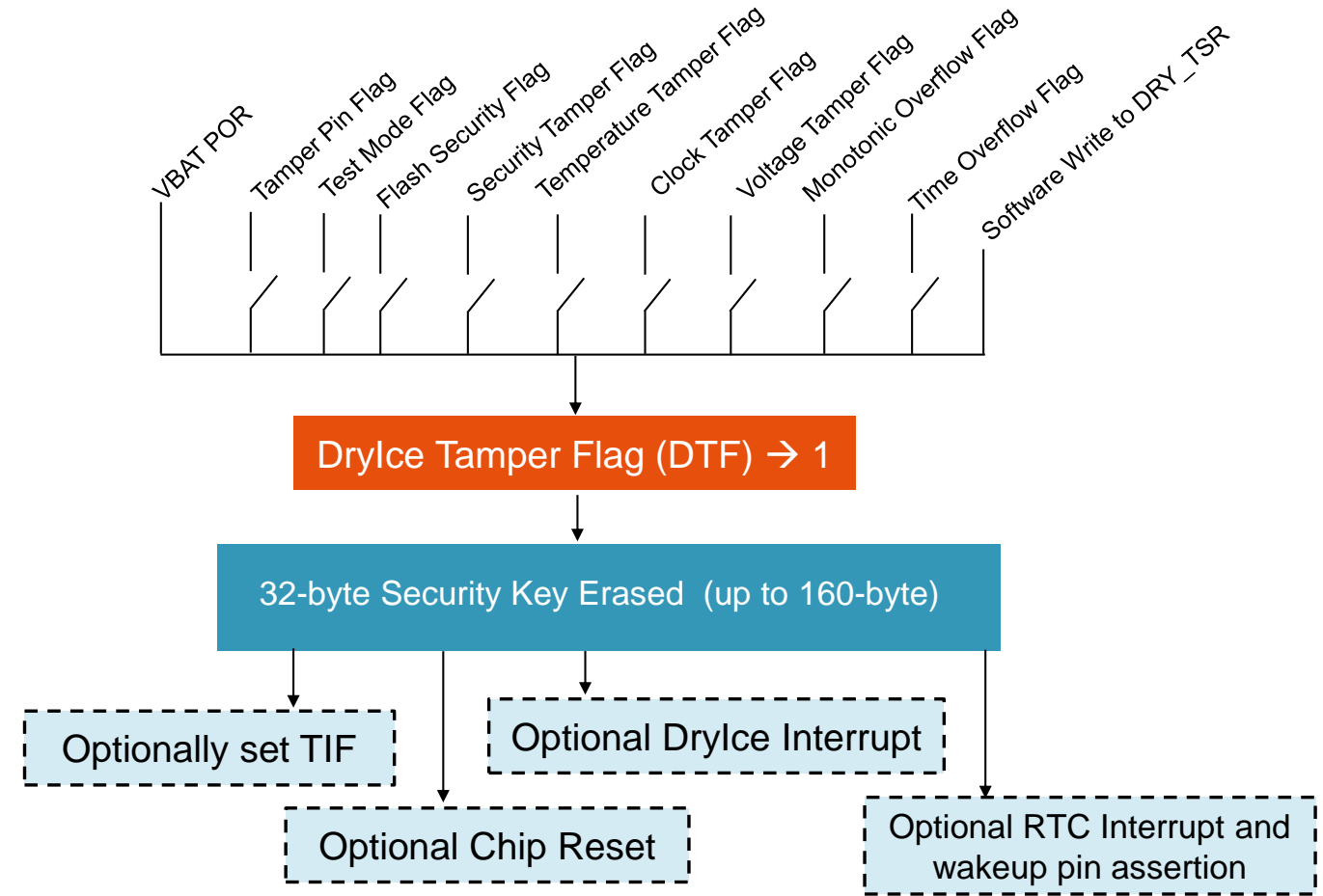
Anti-Tamper: A Handful of Kinetis Support

Feature	Benefit	Feature Details	Enablement
Tamper detect module with up to 8 tamper pins	Reduce external circuits needed to support Tamper Resistance mechanisms	Tamper detection for pin, temperature, voltage and clock. As well as active tamper.	Application note available for NDA customers
Secure storage	Key storage that is automatically erased on tamper (no software intervention required)	Secure key storage space with asynchronous erasure when external tamper events occur.	Application note available for NDA customers

Drylce Tamper Events

Events That Can Set Drylce Tamper Flag (DRY_SR[DTF])

External	
	VBAT Power-On Reset (POR)
	Assertion of Drylce Tamper Pin x Flag (TPFx) [Up to 8 pins]
Internal	
	Assertion of Drylce Test Mode Flag (TMF)
	Assertion of Drylce Flash Security Flag (FSF)
	Assertion of Drylce Security Tamper Flag (STF)*
	Assertion of Drylce Temperature Tamper Flag (TTF)
	Assertion of Drylce Clock Tamper Flag (CTF)
	Assertion of Drylce Voltage Tamper Flag (VTF)
	Assertion of Drylce Monotonic Overflow Flag (MOF)
	Assertion of Drylce Time Overflow Flag (TOF)
	Software-Initiated Write to DRY_TSR (no flag)



Secure Storage

- Amount of secure storage associated with the DryIce module can vary from device to device
- Latest Kinetis K8x MCU devices support:
 - 32-bytes of secure key storage in the DryIce block which is erased on tamper (battery backed)
 - 128-byte VBAT register file (battery backed memory that is optionally erased on tamper as determined by the DRY_CR[SRF] setting)
 - 2KB secure session RAM that is erased on a tamper and system reset

Enabling Secure implementations: Certifications/Testing

- PCI silicon pre-certification for Kinetis KL8x MCUs (in progress)
- PCI silicon pre-certification for Kinetis K8x MCUs (in progress)
- PCI hardware pre-certification for TWR-POS-K81 (in progress)

- Side channel attack testing for Kinetis KL8x LTC (in progress)
- Side channel attack testing for Kinetis K8x LTC (starting soon)

- CAVP (crypto assurance validation program) testing for LTC (starting soon)
- CAVP testing for mmCAU (starting soon)
- TRNG entropy evaluation (starting soon)

- Full PCI compliance certification testing for TWR-POS-K81 (planned start in Q12016)

CONCLUSION

Conclusions

- Every product needs security. Embedded developers must determine the level of security required for their implementation.
 - **A Risk Analysis Must be Performed:** What should be protected? Why is it being protected? Who would attack?
 - **Three Security Pillars:** Trust, Cryptography, and Anti-Tamper
 - **Kinetis MCU Portfolio has a Broad Range of Security Features:** From simple Flash protection to point-of-sale designs and security certifications



SECURE CONNECTIONS
FOR A SMARTER WORLD

ATTRIBUTION STATEMENT

NXP, the NXP logo, NXP SECURE CONNECTIONS FOR A SMARTER WORLD, CoolFlux, EMBRACE, GREENCHIP, HITAG, I2C BUS, ICODE, JCOP, LIFE VIBES, MIFARE, MIFARE Classic, MIFARE DESFire, MIFARE Plus, MIFARE Flex, MANTIS, MIFARE ULTRALIGHT, MIFARE4MOBILE, MIGLO, NTAG, ROADLINK, SMARTLX, SMARTMX, STARPLUG, TOPFET, TrenchMOS, UCODE, Freescale, the Freescale logo, AltiVec, C 5, CodeTEST, CodeWarrior, ColdFire, ColdFire+, C Ware, the Energy Efficient Solutions logo, Kinetis, Layerscape, MagniV, mobileGT, PEG, PowerQUICC, Processor Expert, QorIQ, QorIQ Qonverge, Ready Play, SafeAssure, the SafeAssure logo, StarCore, Symphony, VortiQa, Vybrid, Airfast, BeeKit, BeeStack, CoreNet, Flexis, MXC, Platform in a Package, QUICC Engine, SMARTMOS, Tower, TurboLink, and UMEMS are trademarks of NXP B.V. All other product or service names are the property of their respective owners. ARM, AMBA, ARM Powered, Artisan, Cortex, Jazelle, Keil, SecurCore, Thumb, TrustZone, and μ Vision are registered trademarks of ARM Limited (or its subsidiaries) in the EU and/or elsewhere. ARM7, ARM9, ARM11, big.LITTLE, CoreLink, CoreSight, DesignStart, Mali, mbed, NEON, POP, Sensinode, Socrates, ULINK and Versatile are trademarks of ARM Limited (or its subsidiaries) in the EU and/or elsewhere. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. The Power Architecture and Power.org word marks and the Power and Power.org logos and related marks are trademarks and service marks licensed by Power.org. © 2015–2016 NXP B.V.

