# IoT: Internet of Threats? Protect the Things!

## IoT Security principles and its reflection on Automotive Security

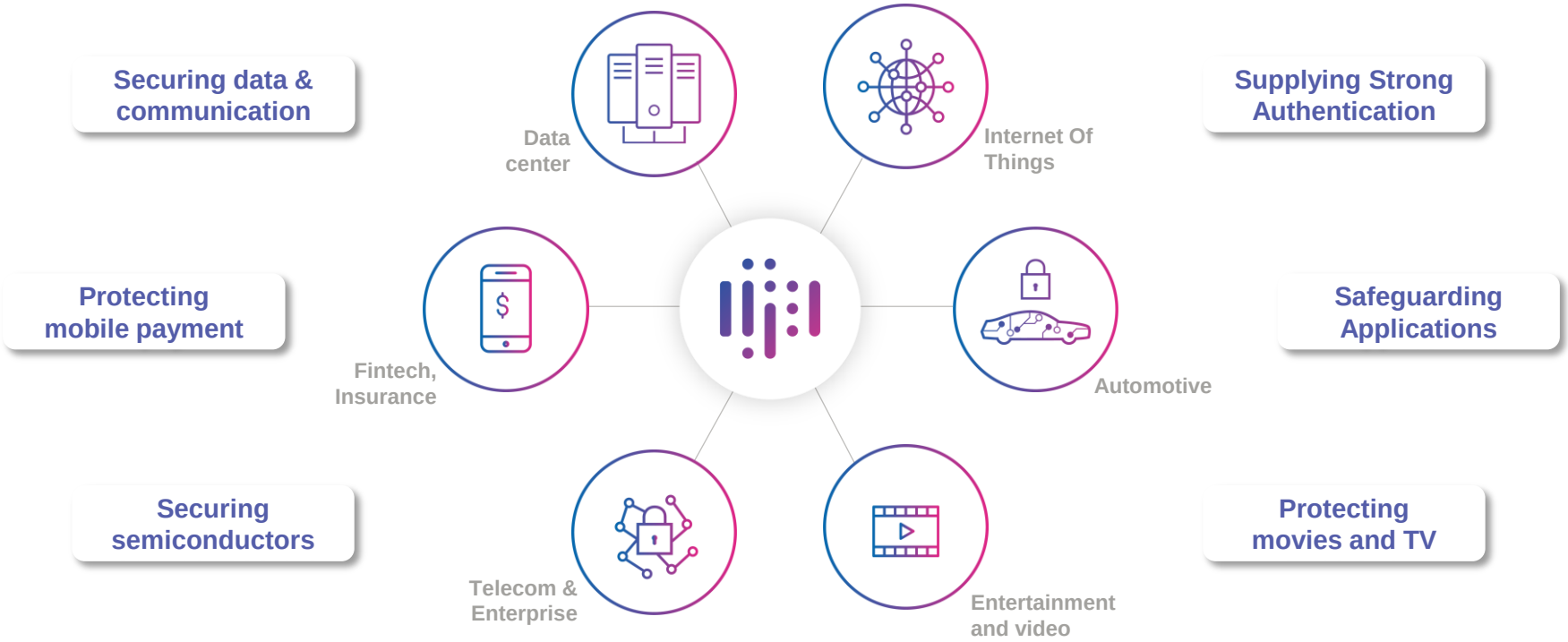
Inside Secure March 29, 2019

*George Kuan*



inside secure

# INSIDE SECURE IS UNIQUELY POSITIONED **TO HELP GROW BUSINESS SAFELY** IN HIGH POTENTIAL MARKETS






inside secure

# Trusted by the world's top companies

Banks and payment system


Content distributors


Top IT companies


Major semiconductor companies


Protecting the solutions of the broadest range of customers: service providers, content distributors, security system integrators, device makers, semiconductor companies



inside secure

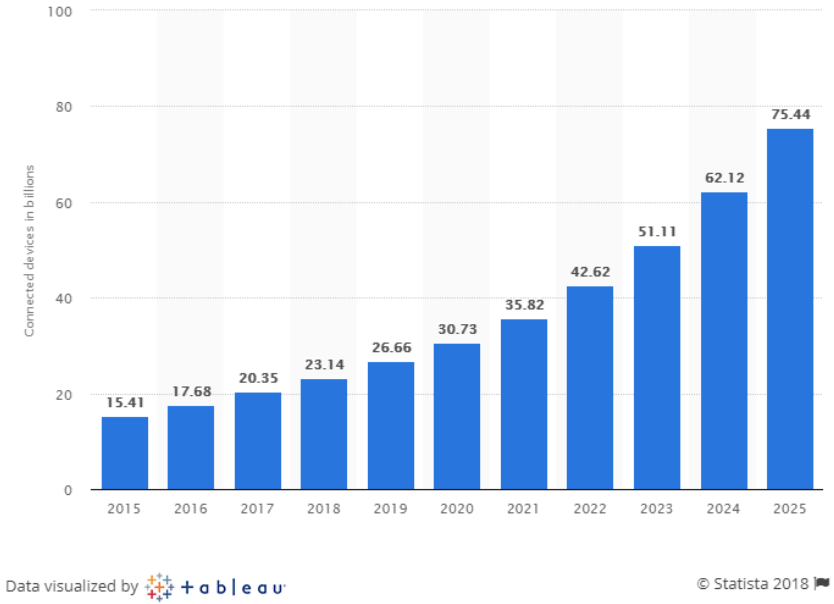
# With a worldwide team of security experts




inside secure

# Continued growth of connected devices and cloud services

- Internet of Things overtook # mobile phones in 2018
- Data center capacity doubles every 3-4yrs
- Edge devices must find right balance between local computation, power consumption & storage and security capabilities.




inside secure

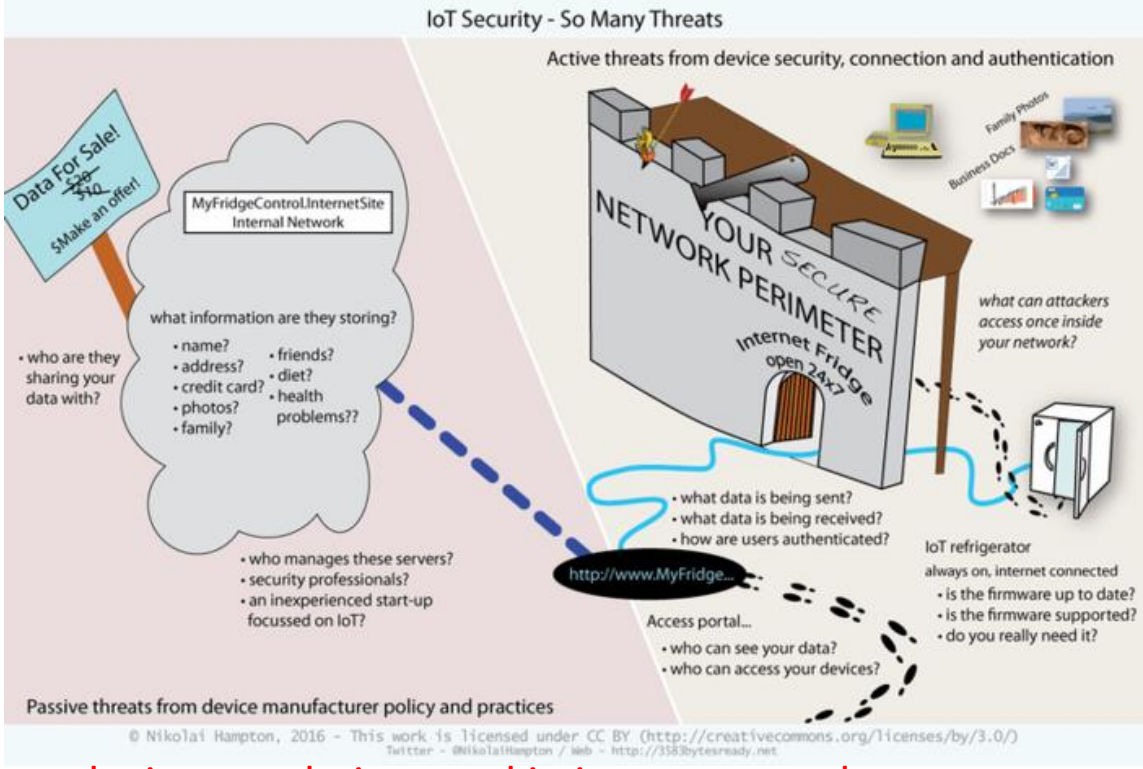
# Why IoT Security?

For device owners:

- IoT devices are typically connected in the trusted network
- IoT devices make connection to the cloud
- IoT devices collect private data

For service providers

- Trust the users of your service
- Understand/Know the source of the stored data
- For device manufactures: What if your devices are being used in internet attacks (DDOS, privacy violation, ransomware, ... )






inside secure

# Challenge #1: many different verticals

## Infotainment

- Video / gaming / VR
- Toys
- wearables

## Smart home

- Access control
- Surveillance and physical security
- Energy management
- Maintenance
- Appliance

## Smart City

- Parking meters
- Traffic control
- Waste management
- Public safety
- Lighting

## Retail

- Inventory management
- Smart payments
- Smart displays
- Shoppers tracking

## IIoT

- Robotic control
- Production monitoring
- Process control
- Maintenance

## Health

- Medication management
- Health monitoring
- Remote diagnostic
- Maintenance

## Transportation

- Vehicle diagnostics
- Autonomous driving car
- Fleet management

## Environment

- Air/water quality
- Noise
- Radiation
- flooding

## Agriculture

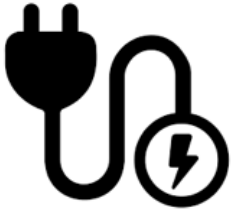
- Corp yield monitoring
- Soil monitoring
- Irrigation control



inside secure

# Challenge #2: Different devices, different constraints, different needs

Resource constrained

Resource rich

High volume; Low margins


Low volume; high margins

Consumer

Mission critical application

## Challenges:

**#3: Connectivity interoperability**






**#4: Fragmented device architecture**

**#5: Fragmented cloud architecture**

**#6: Huge supplier/device manufacturer base**

**#7: lack of standardization**



inside secure

# Still there are generic Security Requirements applicable for IoT, including automotive

## Automotive and IoT Security Essentials

- Keep it Simple
- Secure Boot
- Identity protection
- Device security
- Authentication
- Secure connection
- Data security
- Secure updates

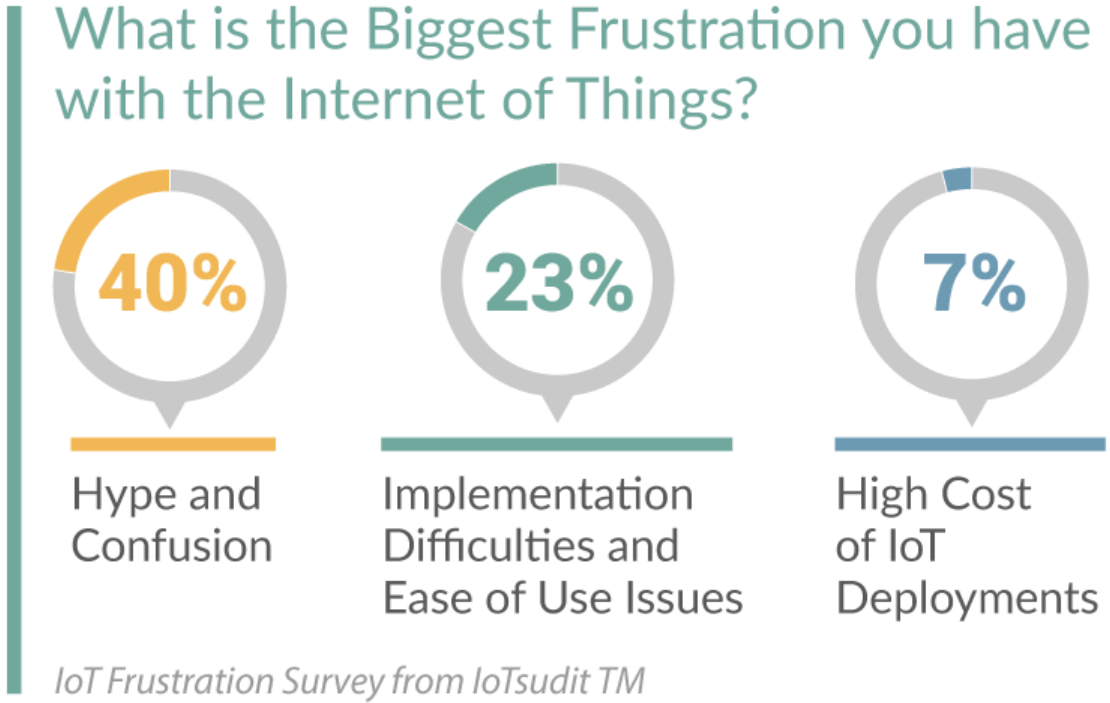
- Single step integration in the system architecture
- Prevent execution of unauthorized software
- Shield the ID from external software
- Protecting device assets, data and services
- Have a trusted identity to protect the service!
- TLS support, required by cloud services
- Encrypt data stored / created / accessed
- Secure updates and recovery; incl. attestation (measured boot)



inside secure

# Why Simple

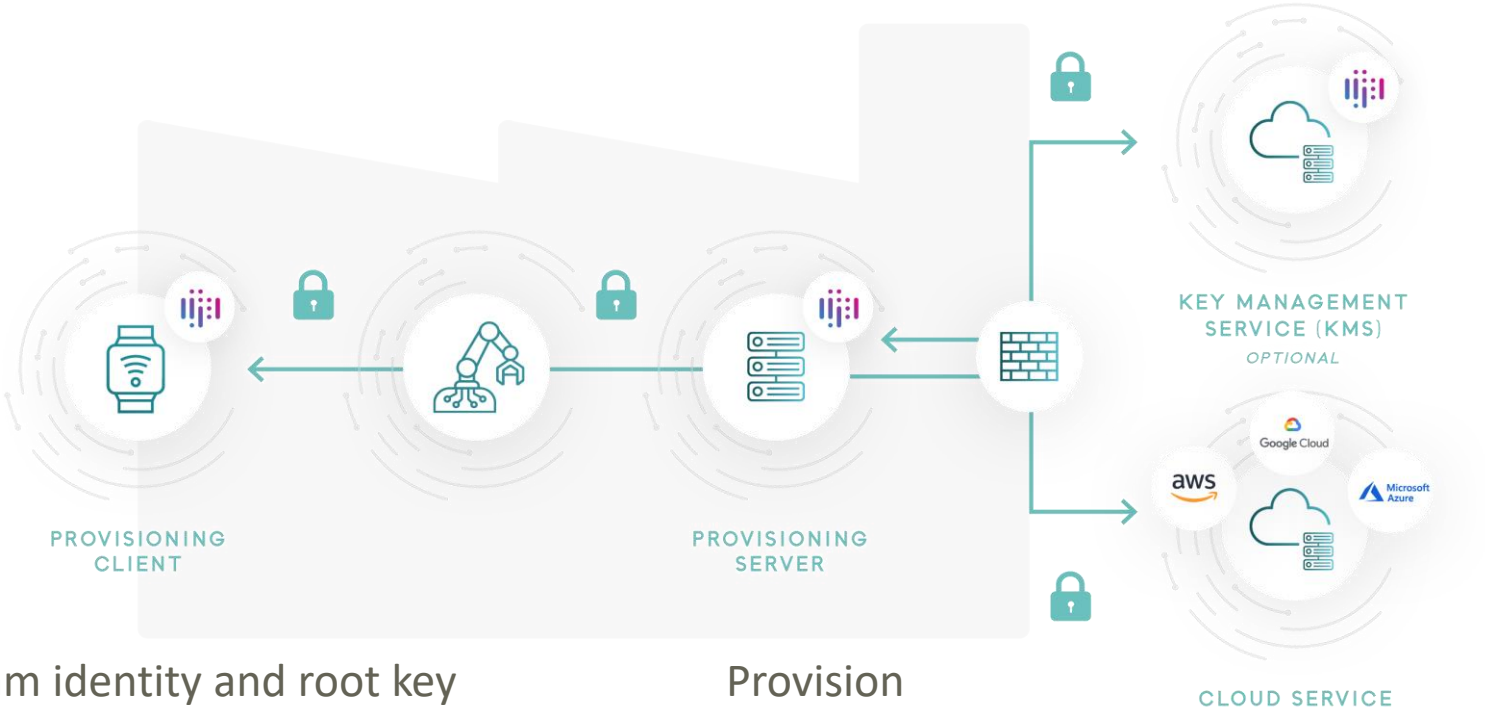
- Security knowledge is limited
  - Mistakes in deployment
  - Prevent enablement
- Implementation is difficult
  - Use complete solutions
  - Use standard integrations






inside secure

# #1: Provisioning -- create a trusted Identity




- Program identity and root key at manufacturer
- Program service/user keys during deployment

Provision

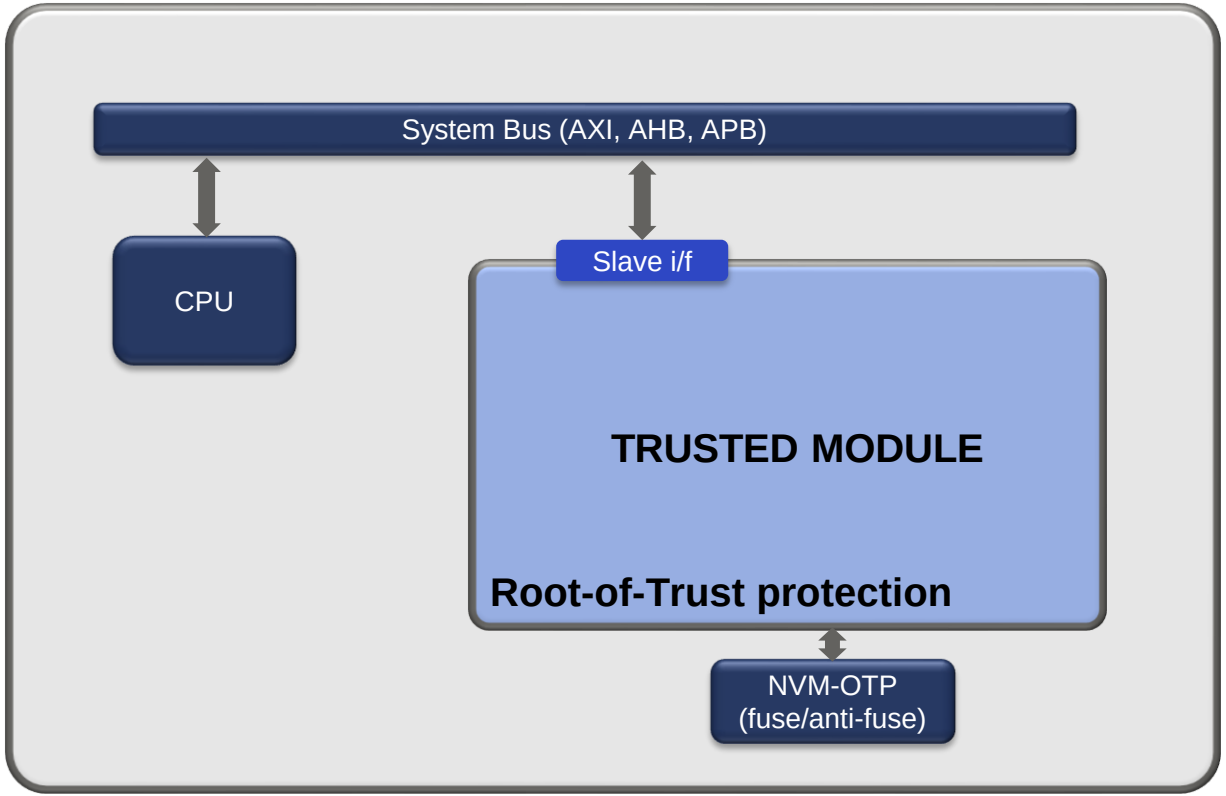
- Device identity
- Root Key



inside secure

# #2: Protect the identity of devices, such as sensors

- ID cloning gives unauthorized access to:
  - Services
  - Data
- A Root-of-Trust prevents:
  - Usage of fake parts: **Liability**
  - Misuse and Disruption of the service
  - Misuse of proprietary or personal data stored in the cloud

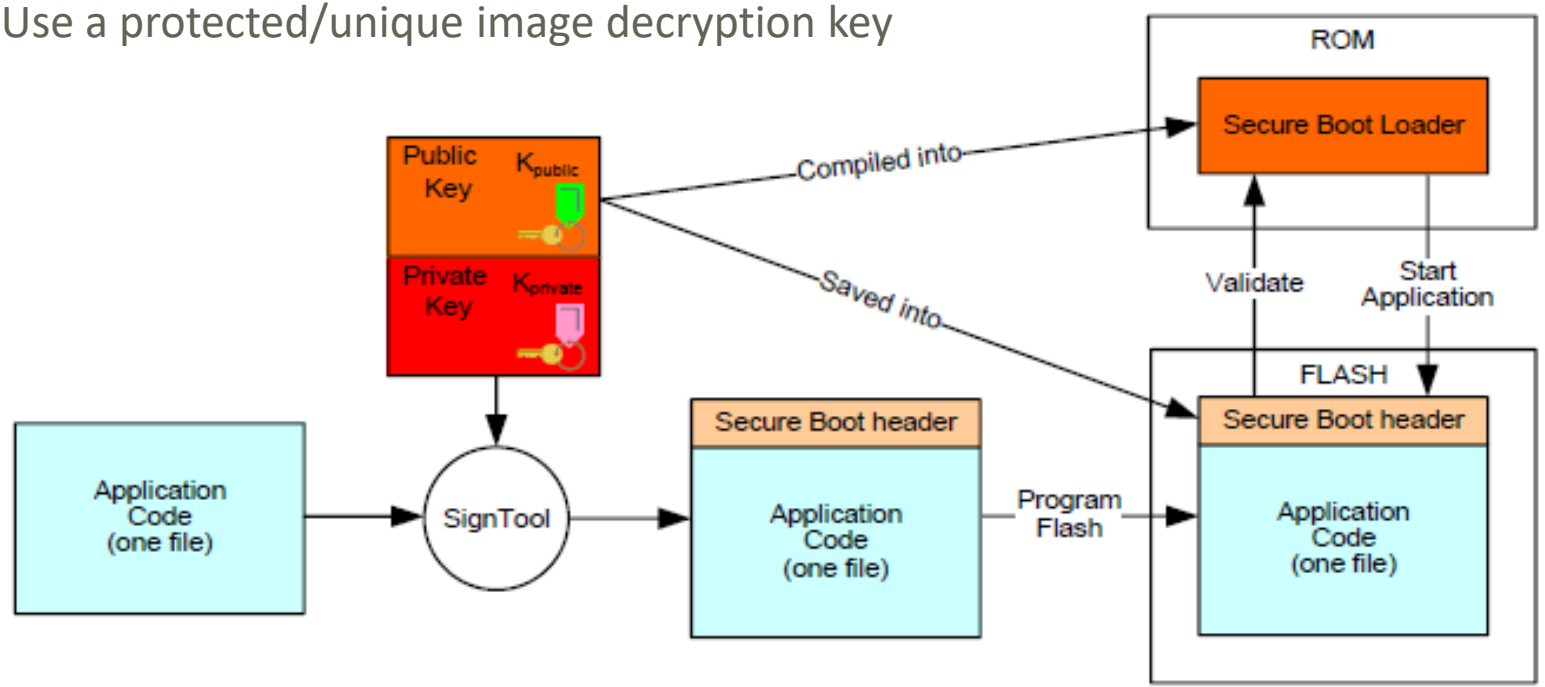





inside secure

# #3: Secure Boot

- Boot the device from an immutable source like a ROM
- Use a immutable (internally stored) public key to validate the downloaded SW image
  - Typically the hash of this key is stored in OTP or ROM
- Use a protected/unique image decryption key






inside secure

# Automotive Security (cybersecurity) specs (1)

- EVITA: *Design, verify, and prototype an architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data are protected against compromise when transferred inside a vehicle*
  - Full : Target is V2X Communications
    SW Crypto: ECDSA, ECDH, MAC/HMAC
    HW Crypto: ECC, AES, Whirlpool, TRNG
    Programmable CPU
  - Medium : Target is on-board communications
    SW Crypto: ECDSA, ECDH, MAC/HMAC
    HW Crypto: AES, TRNG
    Programmable CPU
  - Light : Target is on-board communications
    SW Crypto: AES, MAC
    HW Crypto: AES, PRNG (external seed)
    No programmable CPU

# Automotive Security (cybersecurity) specs (2)

- Secure Hardware Extension (SHE)
  - *Protect cryptographic keys from software attacks*
  - *Provide an authentic software environment*
  - *Security depend on the strength of the underlying algorithm and the confidentiality of the keys*
  - *Allow for distributed key ownerships*
  - *Keep the flexibility high and the costs low*
  - Hardware AES 128 (with CMAC)
  - AES & MAC crypto functions
  - Secure Boot (and associated OTP)
- Hardware Security Module (HSM)
- PRESERVE
  - Vehicle security architecture
  - Operates with an HSM / VaultIP model
  - Focus on typical security analysis
  - Risk assessment, Threat analysis, Policies etc, etc



inside secure

# Safety vs. Security

- **Safety** is the ability to manage risk and responses on malfunction
- **Security** is degree of resistance to attacks resulting in intentional failures

Several commonly used and referenced standards

- ISO26262 is a safety standard for automotive
- ISO19790 is a security requirement standard
- FIPS 140-2 is a security standardization
- ISO IEC62443 defines industrial processes that are also related to safety; 62443-4 is fully focused on security

- Fault detection for safety is not the same as fault injection detection

# ISO26262

- Defines development process
- Defines 4 different safety levels ASIL A…D
- Defines a requirement for an FMEDA
  - Failure Modes, Effects, and Diagnostic Analysis
- Dependent on the safety level, fault detection and fault management is required
- Requires certification by a lab

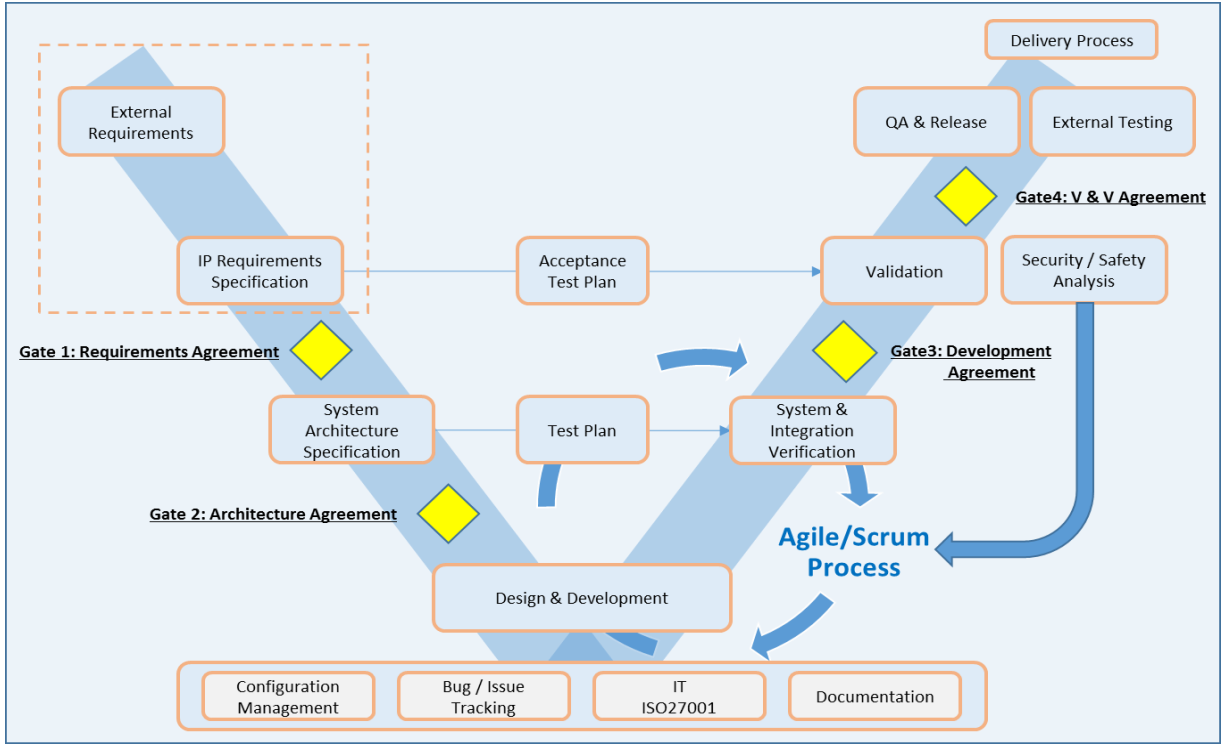
# What brings ISO26262 to Security (IPs)

Process

- Development process
- FMEDA
- Safety Manual

Design

- Redundancy
- Fault detection logic
- Fault management

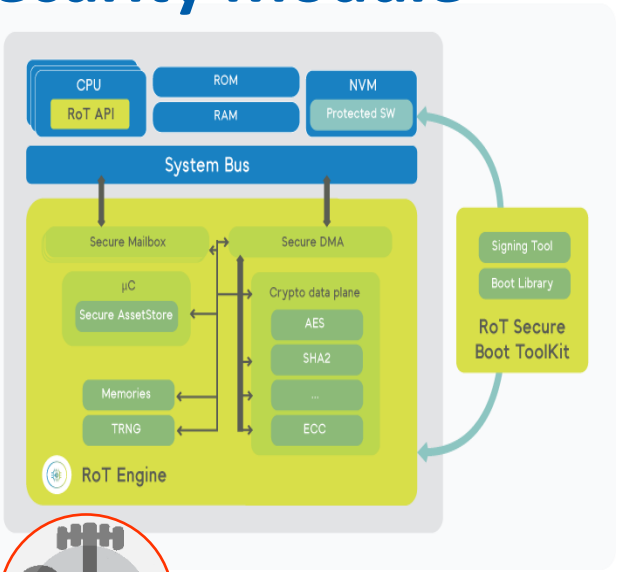


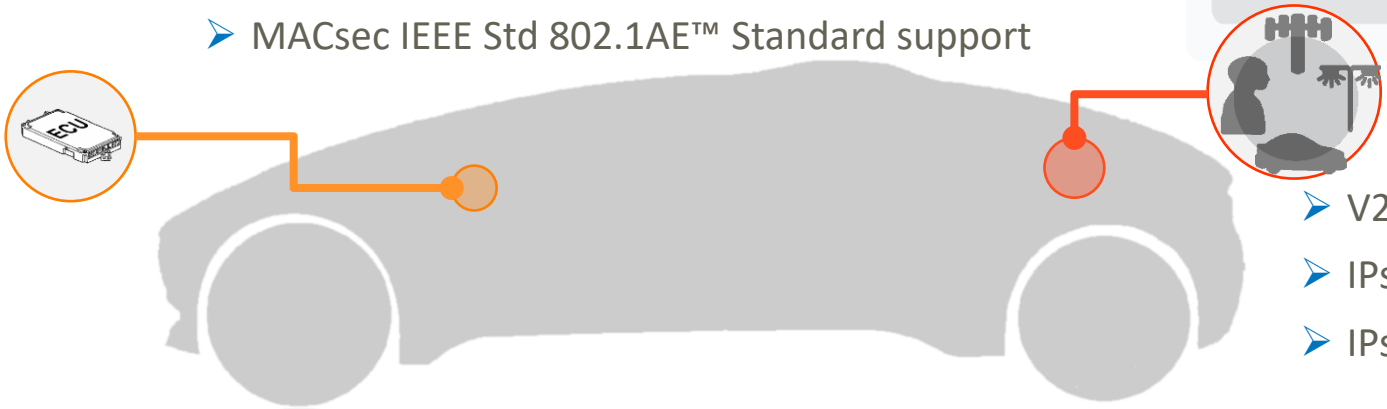



inside secure

# Solution for ECU and V2X: Flexible Security Module

- Embedded HSM
  - IP Cores for Evita Light, Medium, Full
- Secure Boot Image Encryption
  - Secure boot library
  - Software cryptography
  - Multi-stage boot support
- Secure CAN and Ethernet
  - MACsec IEEE Std 802.1AE™ Standard support




- V2V Public Key Engine
- IPsec, TLS/DTLS SW Toolkit
- IPsec, TLS/DTLS, 3GPP IP



inside secure

# #4: Chose a flexible hardware based security solution

Device:

- Supporting all cryptographic primitives!
- Protects the keys/assets

Device access:

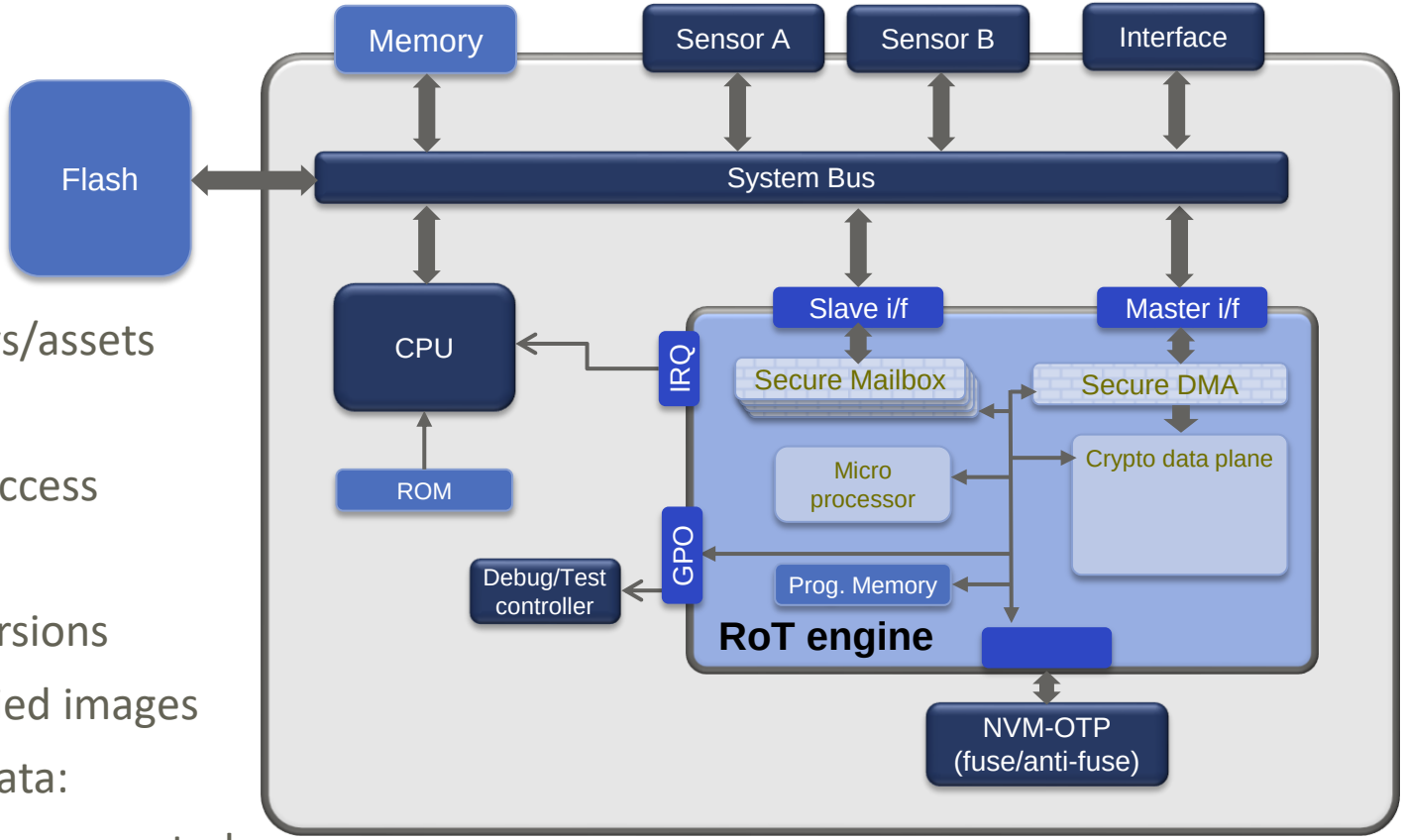
- Protect debug access

Device updates:

- Maintain FW versions
- Only allow verified images

Externally stored data:

- Store critical data encrypted

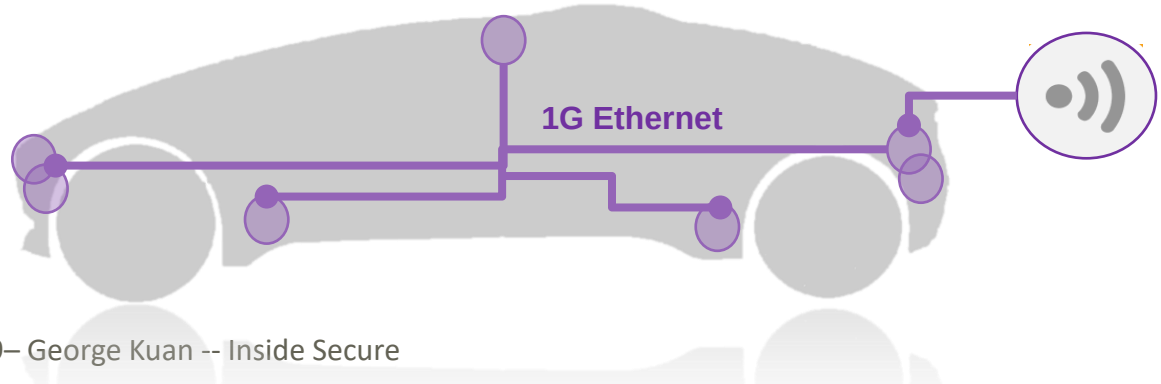





inside secure

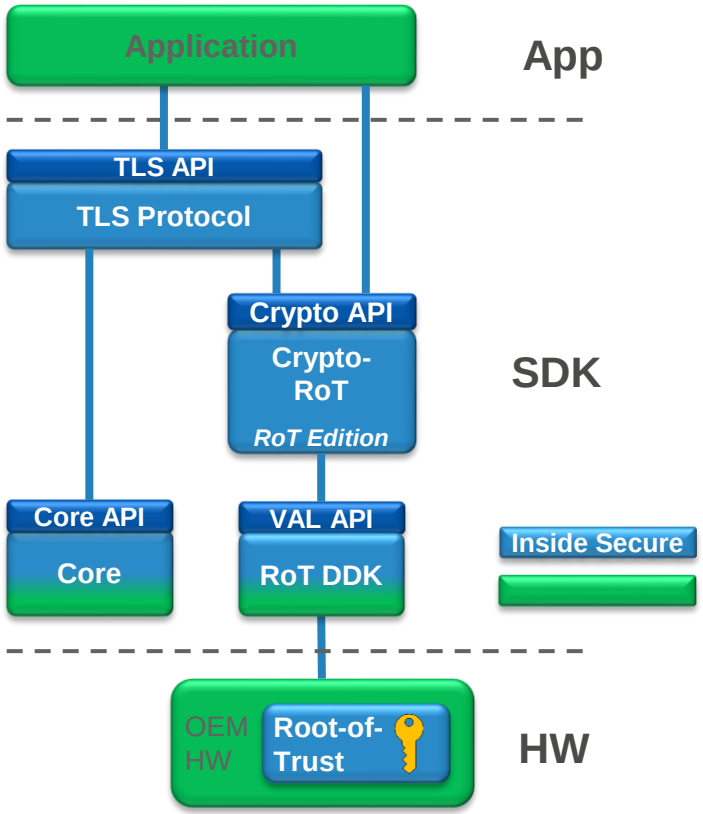
# Don’t forget to protect the network

- Data is generated, and must be available instantaneously
- Ethernet Infrastructure, but also LIDAR-sensor networks in a car require high-speed low latency links
- MACsec is very scalable and matches these requirements
- Inside Secure offers:
  - High-speed TLS / IPsec / MACsec engines ranging from 1Gbps for industrial and automotive networks to 50Gbps for gateways supporting full range of algorithms
  - MACsec / IPsec engines up to 400Gbps/800Gbps engines for data center security



# #5 Secure Connection and Data transfer

- Establish a secure connection with the infrastructure
  - Require a provisioned device.
  - (Almost) All cloud services require TLS
- Root-of-Trust provides **HW protection for the TLS Client/Server private key**
- Root-of-Trust Edition offloads cryptographic operations to Root-of-Trust HW
- Client/server authentication
- Shared secret generation
- Pseudo-random number generation for client_random and server_random






inside secure

# #6 V2X communication - Public Key Acceleration IP

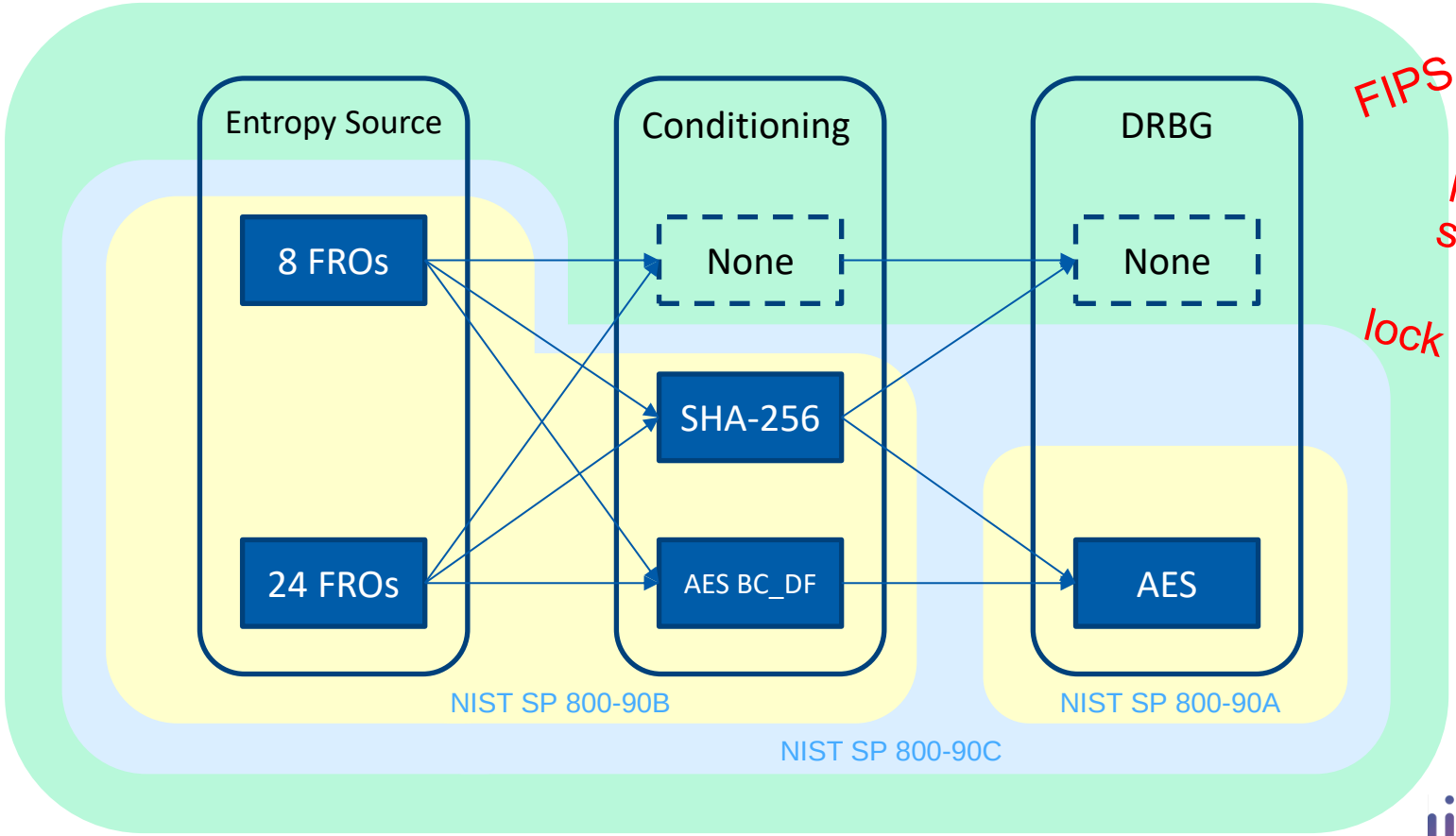
- ECC on all memories
- FIPS-140-2 compliant operations
  - Hardware zeroization logic for all memories containing sensitive data
  - Optional TRNG with SP800-90A (FIPS-140-2) compliant post processing using a separate AES-256 core and TRNG buffer RAM wiping
  - Capability to execute run-time the known-answer tests on local AES (if present), through firmware (high-level commands).
  - Capability to execute run-time the known-answer tests on the TRNG post-processor through direct access to the module registers.
- Optionally side channel attack counter measures available
- High Speed PKA engine with High Assurance Mode:
  - An external input can control or block access to the master controller
- High Speed PKA engine with Debug Mode



inside secure

# #7: Random Source: True Random Number Generator (TRNG)

## Without random data no secure communication!



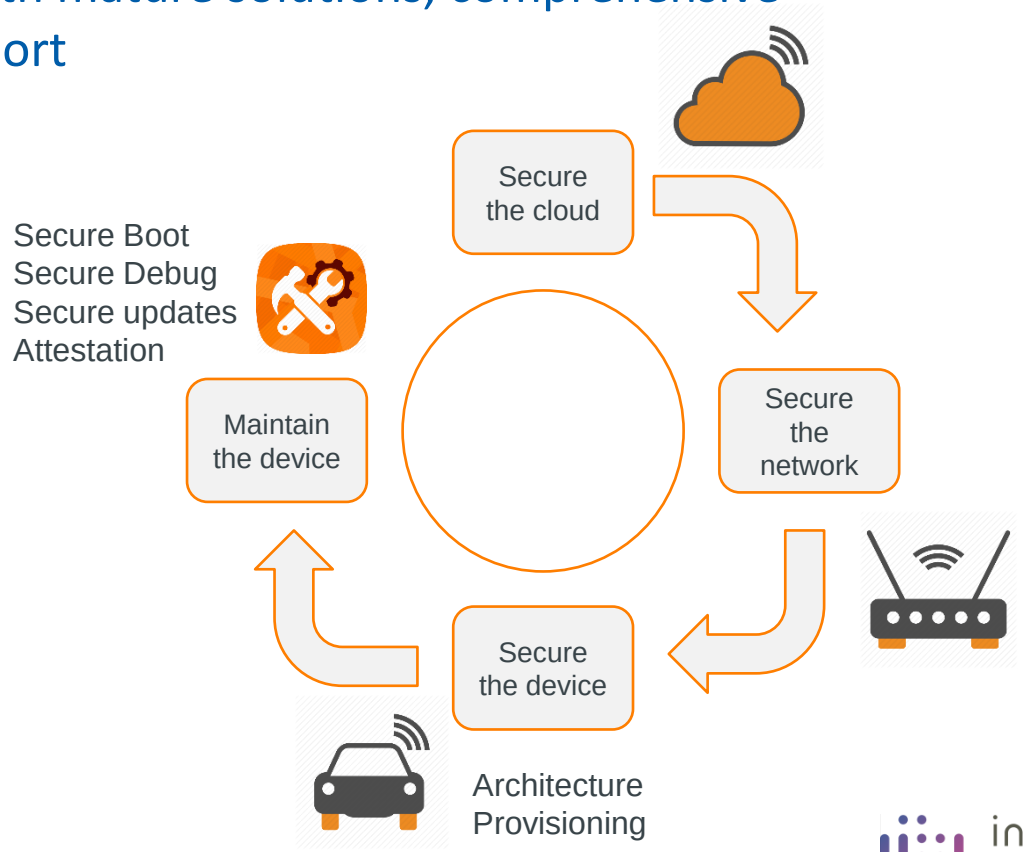



inside secure

# Was it simple?

Let us offload the complexity with mature solutions, comprehensive documentations, tests and support

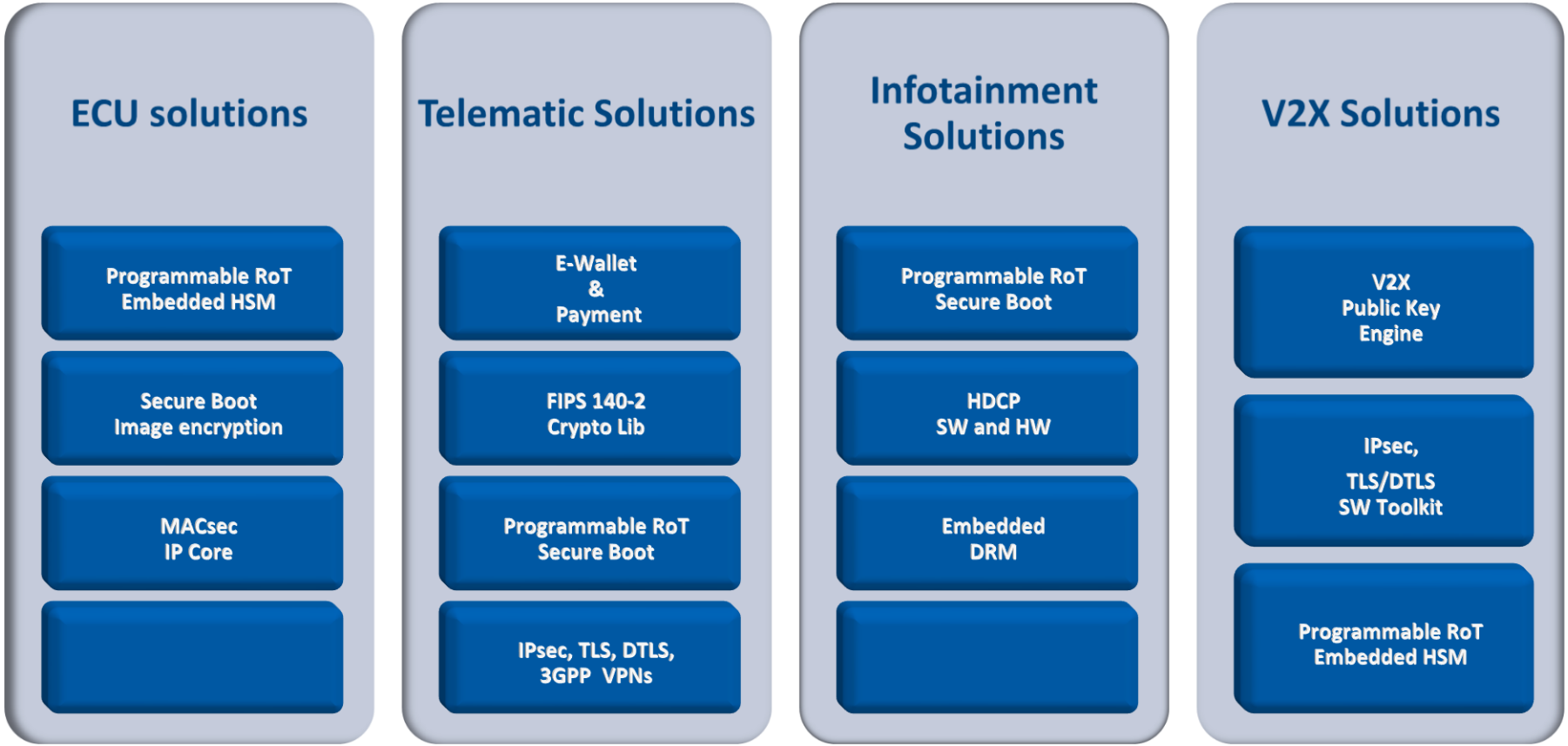
You are protected!






inside secure

# Inside Secure's Solutions for Automotive Market




Check it out on https://www.insidesecure.com/Markets/Automotive



inside secure