NXP | FTF 2016 TECHNOLOGY FORUM

SECURE CAN NETWORKS

FTF-AUT-N1783

REBECA DELGADO | FAE
JOHN COTNER | FAE
FTF-AUT-N1783
MAY 18, 2016

PUBLIC USE

AGENDA

- Introduction: Why Do We Need Security in the Vehicle?
- Functional Security Design Goals Definition
- Automotive Communication Security Concerns
  - Power Up Time
  - Secure Boot
  - Secure Key Storage and Revocation
  - Cryptography
- Conclusions

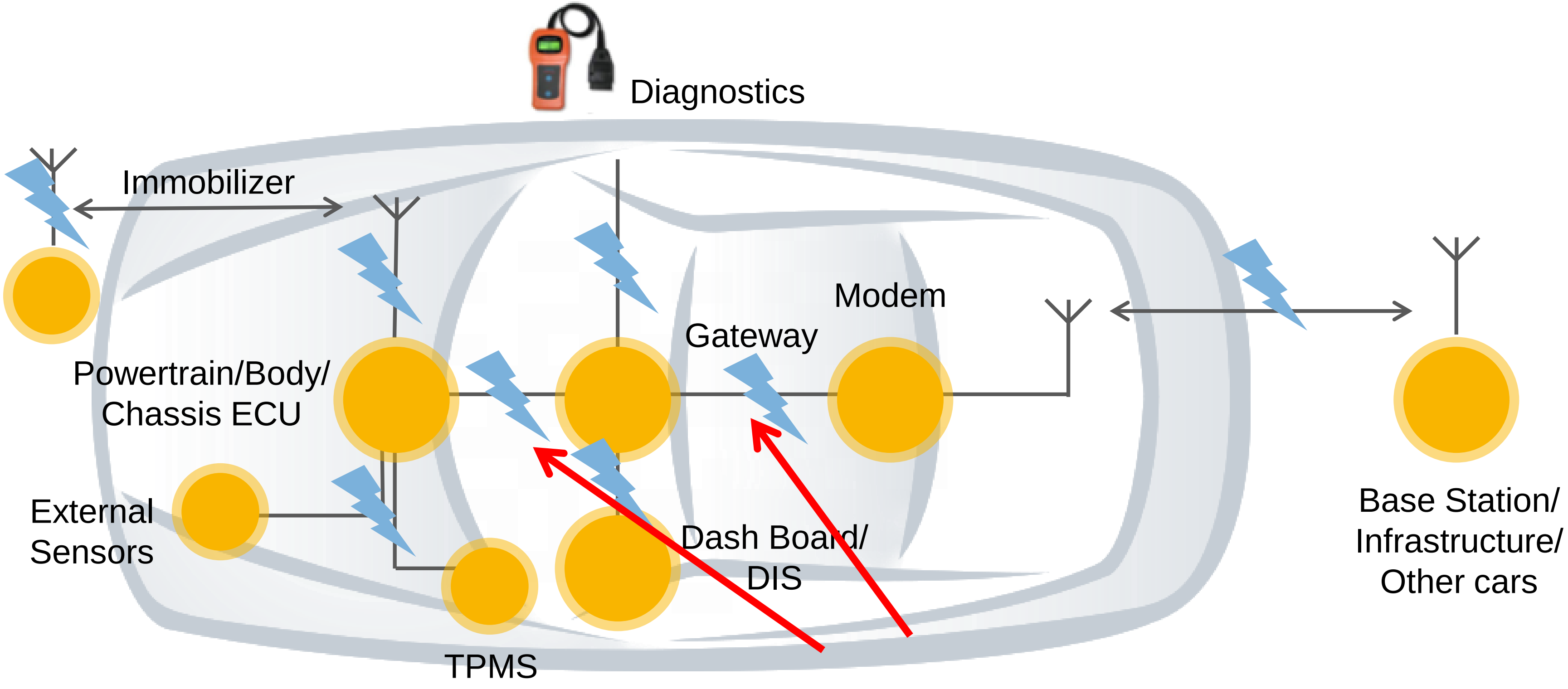
Introduction: Security – Necessity or Feature?

- What needs to be protected?
- What types of attack can be expected?
- What are the attack motivations and methods?

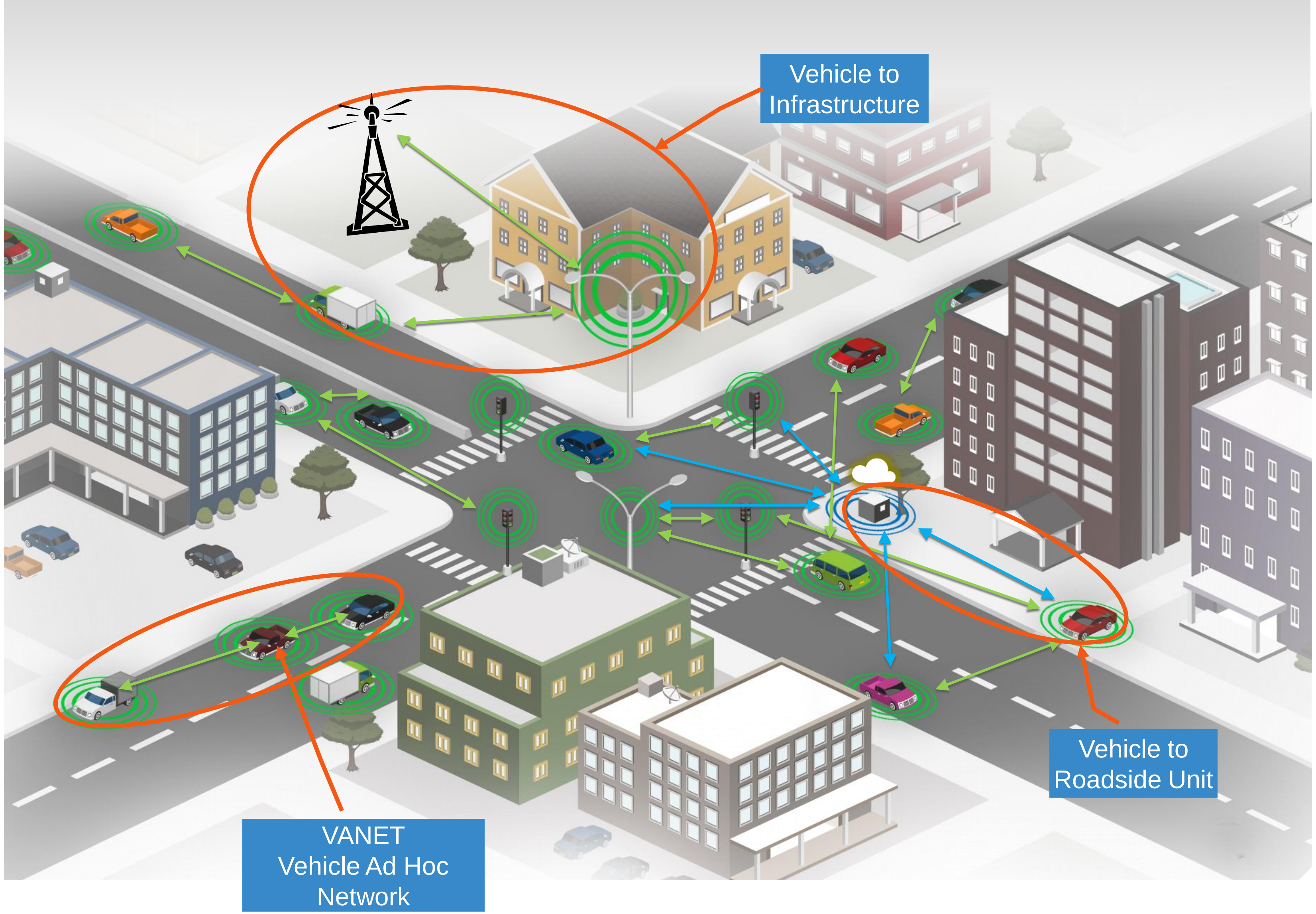
- How much security do we really want?
- How much are we willing to pay for it?

- What is the impact on system complexity?
- How can the security system be maintained and upgraded over time?

Introduction: Automotive Security Attack Surfaces



V2V & V2I Communications



Functional Security Design Goals Definition

Trustworthy System definition:

- A Trustworthy system is a system which does what its stakeholders expect it to do, resisting attackers with both remote and physical access, else it fails safe.

Security Enabled SoCs will provide OEM controlled silicon features which simplify the development of trustworthy systems.

- Security features are an opt in scheme
- OEM controlled trade-offs in cryptographic strength
- Debug visibility
- Sensitivity of tamper detection
- Anti-cloning mitigation

Functional Security Design Goals Definition

Secure Architecture Objectives

- **Objectives**
  - 100% Optional
  - Prevent unvalidated code from executing
  - Protect persistent and ephemeral device secrets against extraction or exposure
  - Protect persistent and ephemeral device secrets against mis-use
  - Support strong partitioning

- **Non objectives**
  - Preventing advanced physical attacks
  - Providing absolute partitioning
  - Operating as a single edged sword

Automotive Communication Security Concerns

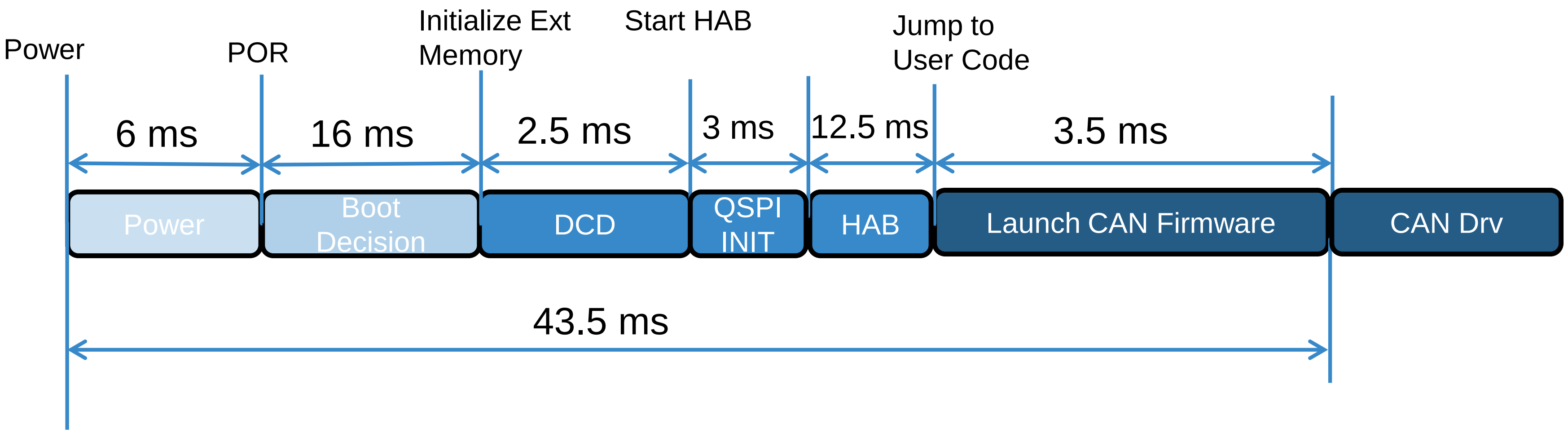
Secure communications require secure ECUs

- Power up time
  - ECU is ready, communication is ready
- Secure boot
  - Prevents unauthorized SW execution at reset
- Run time integrity check
  - Prevents unauthorized SW execution during runtime
- Secure key storage and revocation
  - Protects data confidentiality and integrity over time
- Latency
  - SW vs HW Cryptography
- Behavioral model
  - Focuses on identifying abnormal behavior vs preventing attacks.

→ **There is no safety without security**

Power Up and Secure Boot: Case Study

- i.MX 6SLX – DDR QSPI XIP
- Using 80 Mbytes/s DDR QSPI data rate

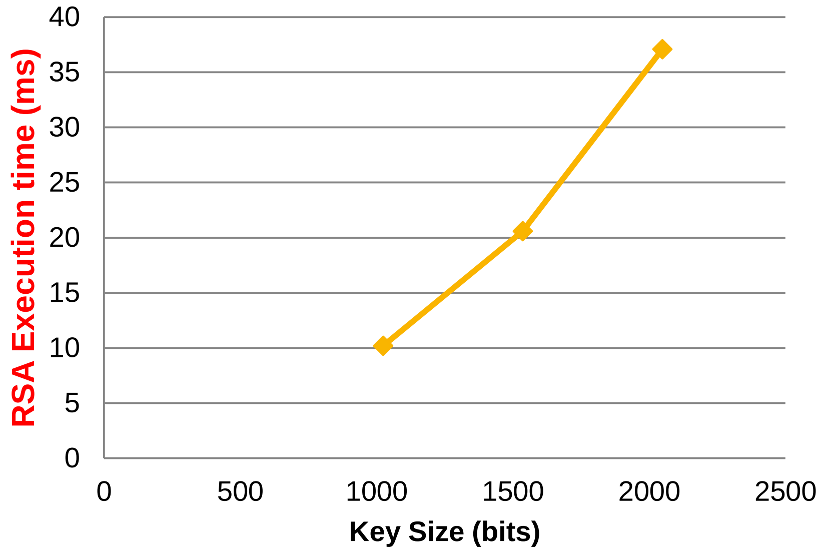


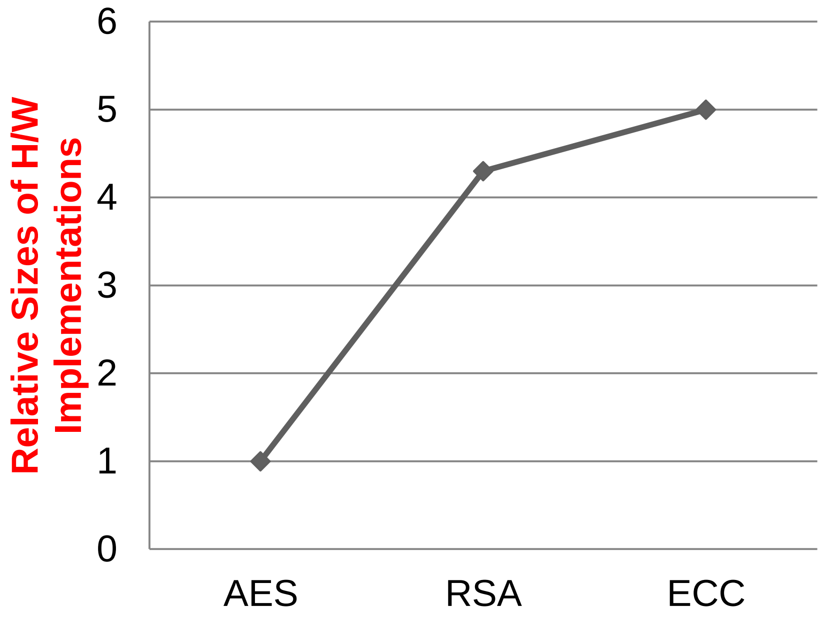
Secure Key Storage

- Required for Passwords, Cryptography Keys
- On-chip or in-package storage offers significant advantages
  - OTP flash memory is ideal from a security perspective
    - easy to provision
    - difficult to extract values
    - memory bus architecture requires careful design (firewalling)
    - can provide a degree of flexibility (revocation)
  - e-fuses are also used
    - might be more susceptible to attack (i.e. easier to read)
    - limited flexibility – not re-programmable
    - large structures, so limited number can be implemented cost effectively
  - Should not require encryption
- Off-chip storage can be subject to snooping attacks
  - requires keys to be encrypted/decrypted

Cryptography: Crypto Algorithm Metrics

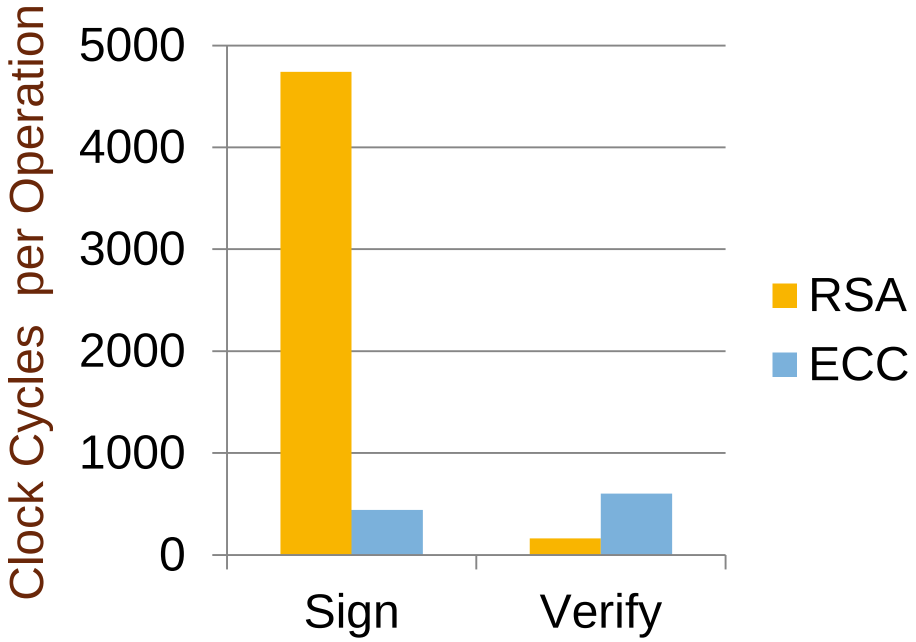
- AES-128, RSA2048, ECC224/256 are commonly used cryptographic algorithms
- Each of these can be accelerated by one to two orders of magnitude (depending on the complexity of the accelerator)
- Cost, performance, and key handling complexity tradeoffs need to be considered

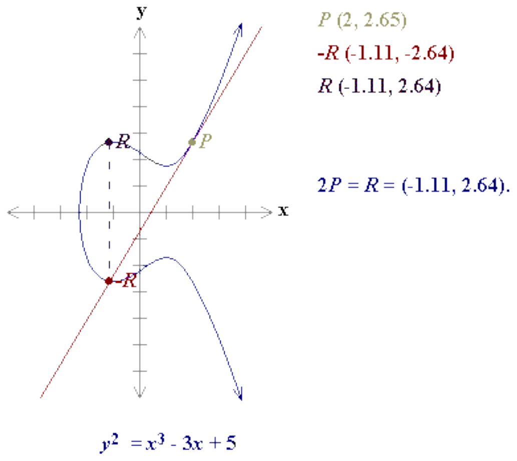




Cryptography: Relative Performance of Hardware RSA and ECC

- Compares equivalent security strength algorithms
  - RSA-2048 vs. ECC-224
- Example is for hardware implementations with 32 bit multipliers
  - Larger multipliers give higher performance, but at a cost
- Both performance and implementation size get closer between RSA and ECC as key sizes increase





Cryptography: Cipher Summary

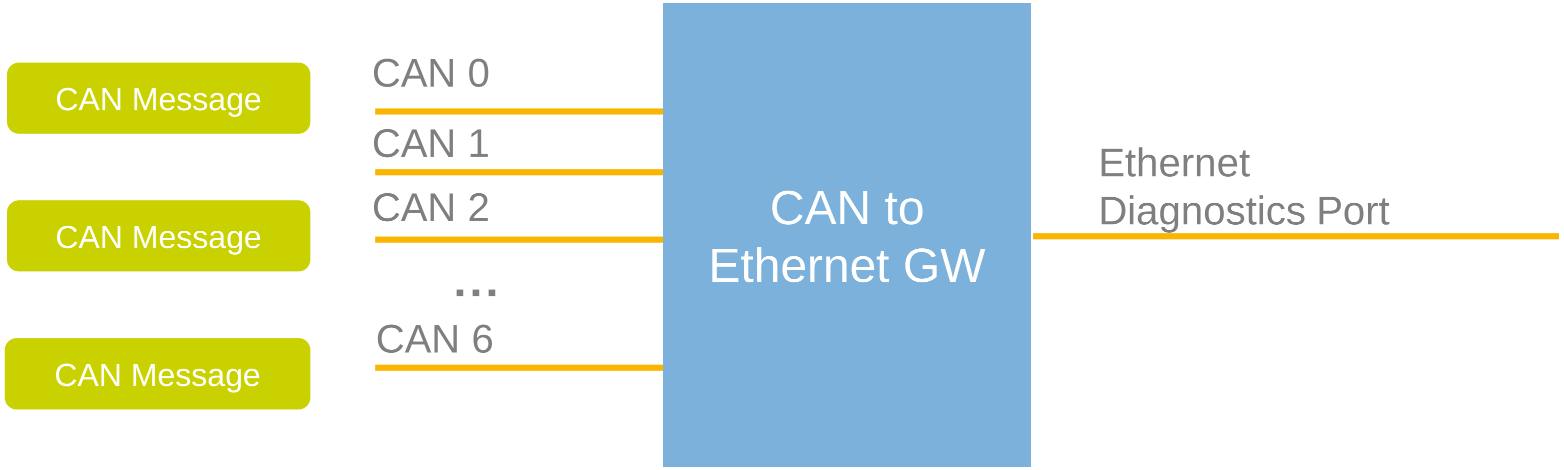
	AES	RSA	ECC
Secure for the next few years	☺	☺ Key size > 2048	☺
Type	symmetric	asymmetric	asymmetric
Typical key size [bits]	128, 192, 256	1024, 2048, 3072	180, 224, 256,320, 512
Execution time	short	long	long
Authentication / verification	😐	☺	☺
Implementation	HW / SW - good	Could combine into one module, req. big number math functions	
Key Management	☹	☺	

Encryption vs. Authentication

- Data Content
  - Should the data transmitted be obscured?
- Privacy
  - Is it important to keep the source anonymous?
- Verification of Source
  - Is this message from an authentic source?
- Latency
  - Is the protection of the data delaying its use outside of the requirement?

Bare Minimum: Diagnostics CAN to Ethernet Gateway

- MPC5748G: Power Architecture® z4 core @160 MHz
- Ethernet low level UDP packet builder: 1.3 us per packet
  - Payload 16 bytes = CAN ID: + DLC + Timestamp + 8 data bytes
  - 100% Traffic → One 8 byte CAN frame every 234 us, 7 CAN buses
    - 7*1.3 us/234 us = 4%



Bare Minimum CAN to Ethernet Gateway with HW Sign/Verify

- Verify AES CMAC algorithm is used to calculate a 128-bit MAC
  - Latency 30 us, for one message (128 bit, padded if needed)
  - Worst case scenario in this study, 7 CAN buses with Signature verification:
    - 30 us * 7 = 210 us
- Generate AES CMAC algorithm is used to calculate a 128-bit MAC
  - Latency 30 us, for one 128 bit message

Security to the Vehicle

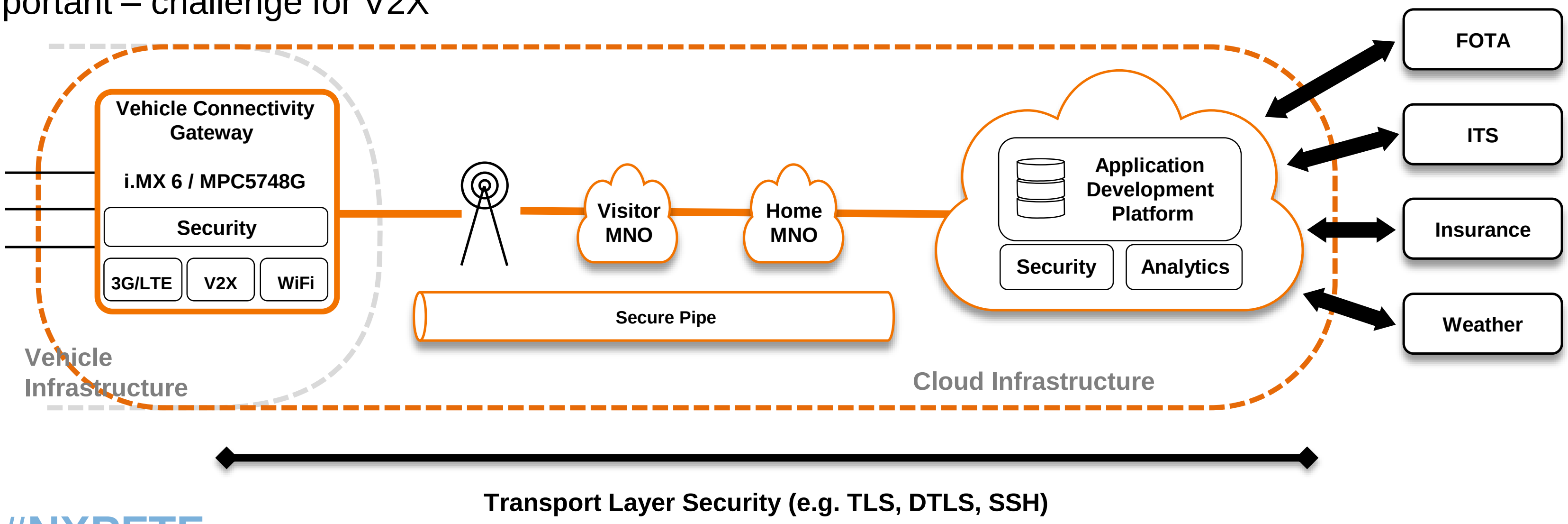
- Do not re-invent the wheel
  - Use industry standards
- Authentication Mandatory
  - Public Key based: ECC, RSA
- Encryption likely
  - Symmetric keys
- Strong Key Management advised
  - Key revocation important – challenge for V2X

Transport Layer Security Protocols

TLS (Transport Layer Security, i.e. SSL)
- HTTPS, MQTT

DTLS (Datagram TLS, i.e. TLS over UDP)
- IoT Protocols: MQTT-SN, CoAP

SSH (Secure Shell)
- Beyond just transport layer



Last Thoughts on Security

Implementing in the real world:

RISK vs COST

(of successful attack)

(of compromised data)

(of implementation)

NXP

SECURE CONNECTIONS
FOR A SMARTER WORLD

ATTRIBUTION STATEMENT