Infineon solutions for secure car communications and software over-the-air.

Antonio Monetti
Marketing Manager, Infineon Technologies Asia Pacific Pte Ltd
Megatrends in Automotive Market

Clean
› Clean Combustion Engines
› Efficient Energy Management
› Electrified Drivetrain
› Lighter vehicle

Smart
› Individual Convenience
› Secure Connectivity, Data Integrity and Privacy
› Advanced driver assistance, V2x and Autonomous Driving
The growing symbiosis between vehicle and environment offers plenty of opportunities.

- Software Update
- Remote Diagnostics
- Car Repair Shop
- Payment Systems
- eCall
- Traffic Information
- Infotainment
- Apps
- Internet Services
- Tablet & Smartphone
- Traffic Information
- Infotainment
- Apps
- CAR2CLOUD
- Onboard Safety & Security
- Car2Car
- Car2Infrastructure
- Consumer Device Integration
- Prioritization of Emergency Services
- Toll Control
- Traffic Jam Detection
- Accident Avoidance

Unwanted access must be denied.

Copyright © Infineon Technologies AG 2016. All rights reserved.
Security in the Cars Communications Network
Dependability (as defined by IFIP WG 10.4)

- Security
- Reliability
- Safety
- Availability

IFIP: International Federation for Information Processing
http://www.ifip.org/
Evolution of the board net architecture

**Distributed Control**
Almost one ECU per mechanical function – connected by multiple interfaces

- Considerable computing performance increase
- Integration of consumer devices
- External connectivity
- In-field upgradeability

**Distributed Computing**
Functions clustered in domains – connected by high-performance networks

**Dependability**
(new term set by the industry)
Basic security approaches discussed

Secure On-board Communication

Basic Protection of single ECUs (Immobilizer & Access)

Firewall & Gateway

Sandboxing

Connectivity Gateway/Data Fusion

Driving Domain
- Torque Control
- Dynamics Control
- Energy Management

ADAS Domain
- Radar
- Camera
- Lidar

Body & Comfort Domain
- HVAC
- Lighting
- Theft Protection

Infotainment Domain
- Navigation
- HMI
- Entertainment
Automotive security Architecture
Trust anchors with different security levels

Trust anchors
Protected Execution
Environments hosting
- Key storage and related cryptographic operation
- Security Applications

Integrated on MCU
- High speed
- Secure Onboard Communication
- Logical security

Discrete Security Controller
- External communication
- Protecting high value
- By certified hardware security

Enabling security for internal and external communication
Infineon’s Product Portfolio for a Security Architecture 2018++

- **Powertrain Domain Controller**
  - Engine Control
  - Battery Management
  - Inverter
- **Chassis Domain Controller**
  - Car2Car Com
  - ABS/ESP
  - ACC
- **Body Domain Controller**
  - Seat control
  - Door Module
  - Air Condition
  - Immobilizer
- **Infotainment Domain Controller**
  - Head Unit
  - E-Call/cell wireless
  - Connectivity ECU

**Integrated**
- **AUDO MAX** Application: Powertrain/Safety
- **AURIX™**
  - Driver: On Board Security

**Discrete Hardware Security**
- **SLI 76** Application: Cellular Com
  - Driver: Network auth.
- **SLI 97** Application: Car Services
  - Driver: Standards reuse
- **TPM** Application: Car2Car Communication
  - Driver: Network integrity, Privacy

**1 Integrated**

**2 Discrete Hardware Security**

Copyright © Infineon Technologies AG 2016. All rights reserved.
AURIX™ Hardware Security Module
A consequent security enhancement

Secure Platform

Hardware Security Module (HSM)

- A highly flexible and programmable solution
- AES128 HW accelerator matching performance for automotive protocols
- Crypto- and Algorithm Agility by Software
- AIS31 compliant True Random Number Generator (TRNG) with high Random Entropie over Lifetime

HSM: 32 bit CPU
AES Accelerator
Embedded µC security – AURIX™
SHE* versus HSM**

Secure Hardware Extention

**No asymmetric cryptography**
- PKC algorithms
- SHA-2

*Not Programmable*
- Platform integrity checks
- Signature checks on certificates
- Execution of secure protocols
- Secure logging

**HSM 1st generation**
- A highly flexible and programmable solution in addition to SHE
- Asymmetric crypto agility by software
- Broadly supported within the AURIX™ MCU portfolio

**HSM 2nd generation**
- ECC256 /SHA256 accelerators
  30 times more performance
- Supported by all Infineon AURIX™ 2G variants

---

* Secure Hardware Extension – SHE  ** Hardware Security Module - HSM

---

2016-09-09
Copyright © Infineon Technologies AG 2016. All rights reserved.
Infineon’s Product Portfolio for a Security Architecture 2018++

Gateway / Firewall

Powertrain Domain Controller
- Engine Control
- Battery Management
- Inverter
- ...

Chassis Domain Controller
- Car2Car Com
- ABS/ESP
- ACC
- ...

Body Domain Controller
- Seat control
- Door Module
- Air Condition
- Immobilizer
- ...

Infotainment Domain Controller
- Head Unit
- E-Call/Cell wireless
- Connectivity ECU
- ...

AUDO MAX
- Application: Powertrain/Safety
- Driver: On Board Security

AURIX™
- Application: Cellular Com
- Driver: Network auth.

SLI 76
- Application: Car Services
- Driver: Standards reuse

SLI 97
- Application: Car2Car Communication
- Driver: Network integrity, Privacy

SLI 97 V2V

Integrated

Discrete Hardware Security

Copyright © Infineon Technologies AG 2016. All rights reserved.
M2M Portfolio Overview

**SLM 97**
- 32-bit ARM® SC300™
- 600KB, 800KB and 1MB NVM
- 32 KB RAM
- 3DES, AES, RSA
- CC EAL 5+ High

**SLI 97**
- 32-bit ARM® SC300™
- 600KB, 800KB and 1MB NVM
- 32 KB RAM
- 3DES, AES, RSA
- CC EAL 5+ High

**SLM 76**
- 16-bit
- Up to 512 KB NVM
- 8 KB RAM
- 3DES, AES (SW)

**SLI 76**
- 16-bit
- Up to 512 KB NVM
- 8 KB RAM
- 3DES, AES (SW)

**Temp Range:**
- SLM 97: -40 – 105 °C
- 10 Year lifetime
- SLI 97: -40 – 105 °C
- 17 Year lifetime

**Subscription Options:**
- Multiple Subscription
- eUICC

- Single Subscription
## Testing Scope of SLx 97 Family

<table>
<thead>
<tr>
<th></th>
<th>SLE 97</th>
<th>SLI 97</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Quality</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consumer</td>
<td></td>
<td>In-Car</td>
</tr>
<tr>
<td><strong>Wafer Test @25°C</strong></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Wafer Test @105°C</strong></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>+ NVM pre-cycling @105°C</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td><strong>Wafer Test @-40°C</strong></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td><strong>Package test before Burn-in</strong></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>with extended test coverage for NVM</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Burn-In</strong></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td><strong>Package test after Burn-in</strong></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td><em><em>Post processing (PAT</em>, local yield, SBT</em>) according to AEC-Q100**</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>PPAP Documentation</strong></td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

*PAT…Part Average Testing
*SBT…Statistical Bin Analysis
Infineon’s Product Portfolio for a Security Architecture 2018++

1. Integrated
   - Application: Powertrain/Safety
   - Driver: On Board Security

2. Discrete Hardware Security
   - Application: Cellular Com
   - Driver: Network auth.

- Application: Car Services
  - Driver: Standards reuse

- Application: Car2Car Communication
  - Driver: Network integrity, Privacy

Copyright © Infineon Technologies AG 2016. All rights reserved.
Securing automotive services by Trusted Platform Module from Infineon

Better security and low integration effort and risk by:

1. using industry proven standards, drivers and applications

2. relying on 10 years of industry experience

Infineon Trusted Platform Module

1. World first TPM 2.0 implementation
2. Tamper resistant and Common Criteria Certified (EAL4+) on device level
3. Crypto-Agility to ensure long-term usability
4. Standards compliant and interoperability supported by leading role within TCG standardization
Infineon’s Product Portfolio for a Security Architecture 2018++

- **Powertrain Domain Controller**
  - Engine Control
  - Battery Management
  - Inverter

- **Chassis Domain Controller**
  - Car2Car Com
  - ABS/ESP
  - ACC

- **Body Domain Controller**
  - Seat control
  - Door Module
  - Air Condition
  - Immobilizer

- **Infotainment Domain Controller**
  - Head Unit
  - E-Call/cell wireless
  - Connectivity ECU

**Application:**
- **Powertrain/Safety**
  - Audo Max
  - AURIX™
  - SLI 76
  - SLI 97

**Driver:**
- **On Board Security**
- **Cellular Com**
  - Driver: Network auth.
- **Car Services**
  - Driver: Standards reuse

**Application:**
- **Car2Car Communication**
  - Driver: Network integrity, Privacy

**Integrated**

**Discrete Hardware Security**

Copyright © Infineon Technologies AG 2016. All rights reserved.
Better safety by
Vehicle to Vehicle Communication

› Increase situational awareness by communication between cars and roadside
› Derive driver warnings and (later) autonomous vehicle reactions.
› Control behavior of traffic lights
› Support of prioritization of ambulance and police vehicles

Source: CAR 2 CAR Communication Konsortium

Vehicle to Vehicle Communication

Vehicle to Roadside Communication
Vehicle to Vehicle Communication
Security Partitioning

Security Drivers
1. Network Integrity
2. Privacy

Security Engine
- Verification
- Signing
- Certificate Updates

Incoming Messages
Outgoing Messages
Pseudonymous Certificates
Benefits of Infineon Vehicle-to-Vehicle Communication Security Controller

- **Flexibility**
- **Stable Production**
- **Security**
- **Crypto Performance**
- **Automotive friendly interfaces**
- **Automotive Quality**

**Features**

- Up to 1 MB SOLID FLASH™
- High volume mass production
- Common Criteria EAL5+
- Crypto Acceleration
- SPI interface
- -40 - 105°C temperature range
- 17 year lifetime
- AEC-Q100 Qualified
- Automotive Qualification
Architecture and Security Partitioning

Security Engine

- Security Functions:
  - ECDSA Verification of incoming messages
- Performance:
  - EU: 400-1000 ECC/sec
  - US: 40-50 ECC/s
- Qualification
  - AEC-Q100 qualification

RF Transceiver

Baseband

ECC Accelerator
(> 400 Ver./sec)

Communication Processor

- Security Functions:
  - Store for pseudonym certificates and private keys
  - ECDSA Signatures for outgoing messages
  - Update for pseudonymous certificates
- Performance:
  - Sign 20 Messages/sec (ECDSA Gen <= 35 msec)
  - ~ 1 MB Flash
- Qualification
  - EAL 4 certified (Europe) Protection Profile: tbd.
  - AEC-Q100 qualification

SLI 97 V2X HSM
Security Controller

Copyright © Infineon Technologies AG 2016. All rights reserved.
Software Update Over the AIR (SOTA) Business Case

Potential for $35bn cost savings per year by 2022!

Source: IHS New Year's Briefing / January 2016
Software Over The Air (SOTA) repairing and enhancing the connected vehicle

Customer satisfaction
Better & faster

Lower cost
Fewer recalls

Safe and Secure

New Services/Business
Secured SOTA architecture
A brief explanation

Step 1: Download while driving
› Software download to central storage
› Unnoticed by the customer
› Vehicle shall be at any time safe and operational

Step 2: Update from central storage
› After customer approval
› In the background or at key-off
› Permissible update time (100s to 15min)
› Confirmation to backend

Safety and security must be ensured throughout the process
SOTA
Update Software OTA In Ten Steps

Over The Air
✓ Authentication btw. vehicle and server and agreement of a session key (TLS)
✓ Service pack is formatted and encrypted w. session key for wireless data transport

Over The Air – Telematics unit TCU
✓ Mutual authentication and session key agreement
✓ Service pack is received and decrypted from secure wireless data transport protocol

Service pack stored in central storage
✓ OEM signature is checked using HSM
✓ Integrity of Service pack is verified
✓ Service pack is split into individual service packs

Updating ECUs using UDS protocol
✓ Put vehicle into SW update mode (UDS programming session)
✓ Individual service packs are sent to specific ECUs in small blocks step by step using UDS protocol (and SecOC)

Update operation inside ECUs
✓ Erase Flash
✓ Decrypt and unzip blocks, write new code into Flash using the Secure Flash Bootloader and HSM
✓ Verify update
✓ Communicate success to update server

Restart car with new SW
✓ Exit update mode
✓ Restart all ECUs within the car

OEM Responsibility
✓ Individual service packs are integrated to one service pack that updates multiple ECUs
✓ Signed with OEM signature
✓ Service pack file is loaded into update server

UDS Formatting
✓ Individual service pack is wrapped to get handled by the protocol of the Universal Diagnostic Service (UDS, ISO 14229-1:2013)

Formatting for Secure Flash Bootloader
✓ Create out of new SW version an individual service pack which matches the Secure Flash Bootloader needs of the ECU: set of small blocks, zip, sign and encrypt

Tier 1 Responsibility
✓ Created in SW development
✓ Verified and released for ECU
Secured SOTA architecture
Security partitioning – IFX offering

Service Authentication
› Cellular network access
› Mutual authentication between car and OEM update server
› Encrypted transport channel
› Secure On-Board COM

Verification and central Storage
› Service pack reception
› 1st verification
› Encrypted storage in car central memory
› Secure On-Board COM

Update of Target ECU
› Service pack reception
› 2nd verification
› Flashing of code memory
› Secure On-Board COM
Secure Software update: SOTA versus OBD

**Commonalities:**
- New software version must be officially released and meet all legal requirements.
- ECUs receive the commands and service packs via their bus interfaces i.e. in UDS format.
- The onboard functions are handled i.e. by the Secure FLASH Bootloader.

**Main Differences:**
- For OBD an external diagnostics tool acts as the update server. For SOTA an **on-board update server must be implemented** (e.g. central gateway).
- The update flow must be power fail prove. Long update times are especially vulnerable for power fails.
Management of Flash Access protection

AURIX™ HSM: Flash Access Authorization

› The Flash Access Authorization prevents unauthorized read and write from internal or external:
  › Requires a 256-bit Password to get temporary unlocked.
  › ECU specific passwords can get created at band-end e.g. by usage of HSM’s TRNG function.
  › 256-bit passwords can get stored in the protected HSM Data Flash
  › The Flash access is only granted by the HSM after successful authentication of the central gateway and by sending appropriate programming command (using secure on-board communication)
Updating ECUs using UDS protocol

- Put vehicle into SW update mode (UDS programming session)

**Authentication:**
Update server (TPM) authenticates itself to target ECU and sends appropriate programming command by using secure on-board communication.

**Flash Access Authorization (target ECU):**
- AURIX™ w. HSM: HSM **temporary disables Flash write protection**
- Flash Erase

- Individual service packs are sent to specific ECU in small blocks step by step using UDS protocol (and SecOC)
Minimizing downtime is key but at what cost?

**Topology 1: Update from Central Storage**
- Downtime: Mins (CAN), Secs (Ethernet)
- AURIX™ supports today

**Topology 2: Update from Local Storage**
- Downtime: Secs
- AURIX™ supports today
- Auto grade serial flash available today

**Topology 3: Update from Double PFlash**
- Downtime: None
- Future generations
We make life easier, safer and greener – with technology that achieves more, consumes less and is accessible to everyone. Microelectronics from Infineon is the key to a better future.

Part of your life. Part of tomorrow.