Security in Automotive Applications

Fabrice Poulard, Technical Marketing
Automotive Business Group

Class ID: BC05I

Renesas Electronics America Inc.
© 2012 Renesas Electronics America Inc. All rights reserved.
Fabrice Poulard

Manager, Automotive Business Group
Renesas Electronics Europe

- Marketing and IP specification responsibility to address security requirements in Automotive applications
- Member of the Security WG within C2C-CC

Experience

- Four years in smart card applications (IT systems)
- Six years in smart card devices (secure MCUs)
- Eight years in the automotive industry (MCU for various apps)

Interests

- Tackle complex customer demands to offer state-of-the-art system solutions at the right cost
Renesas Technology & Solution Portfolio
Microcontroller and Microprocessor Line-up

### 2010

- **1200 DMIPS, Superscalar**
  - Automotive & Industrial, 65nm
  - 600µA/MHz, 1.5µA standby

- **500 DMIPS, Low Power**
  - Automotive & Industrial, 90nm
  - 600µA/MHz, 1.5µA standby

- **165 DMIPS, FPU, DSC**
  - Industrial, 90nm
  - 242µA/MHz, 0.2µA standby

- **25 DMIPS, Low Power**
  - Industrial & Automotive, 150nm
  - 190µA/MHz, 0.3µA standby

- **10 DMIPS, Capacitive Touch**
  - Industrial & Automotive, 130nm
  - 350µA/MHz, 1µA standby

### 2013

- **1200 DMIPS, Performance**
  - Automotive, 40nm
  - 500µA/MHz, 35µA deep standby

- **165 DMIPS, FPU, DSC**
  - Industrial, 40nm
  - 242µA/MHz, 0.2µA standby

- **Embedded Security, ASSP**
  - Industrial, 90nm
  - 1mA/MHz, 100µA standby

- **44 DMIPS, True Low Power**
  - Industrial & Automotive, 130nm
  - 144µA/MHz, 0.2µA standby
Microcontroller and Microprocessor Line-up

2010

1200 DMIPS, Superscalar
- Automotive & Industrial, 65nm
- 600µA/MHz, 0.2µA standby

50DMIPS, True Low Power
- Industrial, 65nm
- 2µA/MHz

10DMIPS, Capacitive Touch
- Industrial & Automotive, 130nm
- 350µA/MHz, 1µA standby

2013

1200 DMIPS, Performance
- Automotive, 40nm
- 1.5µA/MHz, 35µA deep standby

50DMIPS, FPU, DSC
- Automotive, 40nm
- 1µA/MHz, 0.2µA standby

1200 DMIPS, Embedded Security, ASSP
- Automotive & Industrial, 65nm
- 1.5µA/MHz, 100µA standby

1200 DMIPS, True Low Power
- Industrial & Automotive, 130nm
- 144µA/MHz, 0.2µA standby

32-Bit High Performance, High Scalability & High Reliability

© 2012 Renesas Electronics America Inc. All rights reserved.
‘Enabling The Smart Society’

**Challenge:**
“Future in-vehicle systems will contribute to safer cars, safer roads, more efficient driving, easier maintenance and more fun”

“... as long as sufficient trust can be established in those systems...”

**Solution:**
“This class introduces the security challenges ahead in the Automotive world and the solutions developing in the market to address them”
Agenda

- What is driving security in the automotive space?
- Automotive devices: the secure way forward
- SHE and EVITA: major security initiatives in the industry
- Renesas solutions
- Future developments
Introduction to Automotive Security
Security: One of Many Automotive Applications

Safety-relevant messages...

... must be secured! (so that they can be trusted)
Security Breach in Cars: *One* Consequence

**Step #1:**
Select your car brand and model...

**Step #2**
- get more horse power...
- ... or save fuel!

Can an engine break down just after 40,000km?

Yes, if used outside of the guaranteed configuration...
Automotive Security: Why Take it so Seriously?

- Electronic hobbyist: customization for fun
- Lab / University: reputation
- Professional: counterfeiting for money
- Competitor: gaining knowledge & expertise
- Criminal organization: black market, terrorist acts...

Revenue loss
Brand / reputation damage
Car safety at risk
Heavy costs (e.g. warranty)
Security-Enabled Automotive ECUs: The Vision

How to protect my virtual dashboard design?

How to secure radio communications?

How to protect the odometer?

How to secure the remote entry system and the immobilizer?

How to protect against illegal tuning?

How to secure the car diagnosis?

Toward a distributed in-vehicle security system
Automotive Devices: The (Secure) Way Forward
**Behind The Scene...**

**Electronic Control Unit (ECU)**
Handles a dedicated *in-vehicle function* (engine control, transmission, airbag, etc.)

**In-vehicle network**
Interconnects the ECUs together
Different bus types (CAN, LIN, Flexray, etc.)
Splits by *functional domains* (safety, body, ...)

**MCU / SoC**
The ECU intelligence
*MCU*: Microcontroller Unit with *on-chip Flash*
*SoC*: *Flash-less* System-on-Chip

The number of ECUs per car keeps on a steady growth
How to *secure* this increased IP value?
The 3 Security Objectives of a Secure System

In vehicle network

Proven Identity

Confidentiality

Integrity & Authenticity

Cryptographic Services

Computation power

Secret keys

Security → Cryptography → [Computation power + Keys]
# Measuring The Capabilities of a Secure ECU

<table>
<thead>
<tr>
<th>Cryptographic element</th>
<th>Metric</th>
<th>OEM / Tier1 interrogation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computation capabilities</td>
<td>Flexibility</td>
<td>How easy can cryptographic services be integrated in the overall system?</td>
</tr>
<tr>
<td>Secret keys</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Measuring The Capabilities of a Secure ECU

<table>
<thead>
<tr>
<th>Cryptographic element</th>
<th>Metric</th>
<th>OEM / Tier1 interrogation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computation capabilities</td>
<td><strong>Flexibility</strong></td>
<td>How easy can cryptographic services be integrated in the overall system?</td>
</tr>
<tr>
<td></td>
<td><strong>Performance</strong></td>
<td>How fast run the cryptographic services?</td>
</tr>
<tr>
<td>Secret keys</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* The quality of random number generators (RNG) is also considered to a certain extent.
# Measuring The Capabilities of a Secure ECU

<table>
<thead>
<tr>
<th>Cryptographic element</th>
<th>Metric</th>
<th>OEM / Tier1 interrogation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computation capabilities</td>
<td>Flexibility</td>
<td>How easy can cryptographic services be integrated in the overall system?</td>
</tr>
<tr>
<td></td>
<td>Performance*</td>
<td>How fast run the cryptographic services?</td>
</tr>
<tr>
<td>Secret keys</td>
<td>Tamper resistance</td>
<td>How secret are the secret keys? How difficult is it for an attacker to retrieve them?</td>
</tr>
</tbody>
</table>

Those metrics are normalized with the price of the secure ECU. (a low-cost BCM will target lower metrics than a high-end Gateway)

* The quality of random number generators (RNG) is also considered to a certain extent
The Corner Stones of a Secure ECU

OEMs & Tier1s

Secure protocols

Crypto services

Standardization Bodies

Flexibility

Performance

Tamper resistance

Firmware

MCU / SoC

Semiconductor Vendors

The MCU / SoC is the security enabler!
Automotive Devices: The (Secure) Way Forward

Cryptographic performances

Trend setters
- Concrete OEM & Tier1 requests W/W

Constraints
- Power dissipation (mA/MHz)
- Reliability (“AEC-Q100++”)
- Cost (die size, test, etc.)

Targeted area for security relevant applications

High

Mid

Low

SoC

MCU

Smart Card MCU

Low

Mid

High

Tamper resistance
In-Car Security: Fostering Market Acceptance
Toward Security Standards in Automotive

The establishment of standards is key to ensure the support of all key suppliers (Tier1s & MCU vendors)

Two important initiatives in Europe are setting the grounds for W/W standardization
Secure Hardware Extension (SHE)

- SHE: on-chip extension within a MCU
  - Provides a set of cryptographic services to the application layer
  - Isolates the secret keys from the rest of the MCU resources

- SHE objectives
  - “Secure anchor”
  - “Low cost”

- SHE: released in April 2009 as a public specification
  - Specification work driven by Audi
  - Endorsed by the German OEM consortium “HIS”

- SHE: now requested or (at least) referenced by OEMs W/W
SHE: Brief Overview

- Provides the application layer with a fixed set of cryptographic services based on AES-128
  - Encryption & decryption
  - CMAC generation & verification
  - Random number generation
  - Boot loader verification
  - Unique device identification

- Stores secret keys and certificates in a dedicated NVM not accessible by the application
  - The keys are referenced by an index (from 0 to 14)
  - Keys are updated in the secure memory with a specific procedure
The EVITA Project

- EVITA: an EC-sponsored project
  - Was running from 3 years, ended in November 2011
  - Project lead by BMW and Bosch

- EVITA scope: in-vehicular security hardware
  - Enforce ECU SW protection against SW & selected HW attacks
  - Accelerate security mechanism by HW acceleration
  - Support ECU to ECU communication protection

- EVITA specification: targets both HW & SW

- All deliverables publicly available on the EVITA web site
The EVITA HSM Concept

MCU (ECU) boundary

Application Core
- Application NVM
- Shared RAM
- Bus I/F
- Application CPU

Data

Secure CPU

Interrupts

EVITA interface

Secure Storage
- Internal RAM
- Internal NVM

Crypto HW acceleration
- Symmetric Crypto Engine
- Hash engine
- Asymmetric Crypto Engine
- TRNG / PRNG
- Counters

In-vehicle bus system

Source: EVITA project / Deliverable D3.2: Secure On-board Architecture Specification
Envisioning The Deployment of HSMs

**EVITA HSM “full” → securing extra-vehicular coms**
Supporting strong authentication (e.g. RSA, ECC) as well as complex block ciphers @ very high data throughputs

**EVITA HSM “medium” → securing internal coms, enforcing IP protection**
Supporting complex block ciphers @ high data throughput
Supporting signature verification in SW (e.g. RSA)

**EVITA HSM “small” → securing critical sensors / actuators**
Supporting simple block ciphers, low cost modules

Source: EVITA project / Deliverable D3.2: Secure On-board Architecture Specification
Security in Automotive: Picturing the Trend
Security-enabled Automotive MCU

**Master in the system:** has unrestricted accesses to all MCU resources

**New master in the system:** controls a (small) set of specific but exclusive resources for security relevant tasks
Application & Secure Domains

Application Domain
- Sense
- Actuate
- Communicate

Secure Domain
- Encrypt / Decrypt
- Verify Integrity
- Authenticate

Dedicated HW for efficient cryptography
Isolation of secret data
Parallel processing
Customized services
Potential use Case: Boot Loader Verification

Application Domain

- Initialize the application environment
- Initialize the communication stack
- Main application loop

Secure Domain

- Calculate hash value of boot loader (H)
- Verify boot loader signature (H’)
- H’ == H?
  - Boot loader verification failed: break the application loop
  - Boot loader verification successful: prepare for next security service

Execution time

HW Reset

Execution time enables systematic background check with no impact on application domain timings.
Potential use Case: Encrypted CAN Messages

Application Domain

- Main application loop
- Process the message received
- Prepare a message to send

Execution time

Secure Domain

- Wait for a CAN message
- Decrypt the mailbox
- Encrypt the mailbox
- Send the CAN message

Secret keys are never seen in the application domain
In-Vehicle Security: Renesas Solutions
The next generation of Renesas Automotive devices integrates a scalable range of security peripherals to support existing and emerging security requirements.

Security Peripherals for MCU with embedded Flash

- ICU-S
- ICU-M2
- ICU-M3

Security Peripherals for Flash-less SoC

- Crypto Engine

Renesas RH850
(low- to mid-end)

Renesas RH850
(mid- to high-end)

Renesas R-Car
SoC

Low power
Low cost

Flexibility and performances

High-performance
(stream ciphers)
Security-Enabled Automotive MCUs*: Renesas’ ICU Concept

*MCU: Microcontroller Unit with embedded Flash
ICU: Intelligent Cryptographic Unit

To tackle the need for security in automotive applications, Renesas introduces a **dedicated MCU peripheral** to support different security services.
ICU Types

- ICU-S
  - Slave unit
  - Private key cryptography
  - Control logic

- ICU-M
  - Master unit
  - Private key cryptography
  - Public key cryptography
  - Dedicated CPU

“EVITA HSM” type-of IP

“SHE” compliant IP

Cryptographic Capabilities

IP Complexity & Cost
ICU-S Block Diagram (Simplified View)

Inside view of the MCU

ICU-S

APB I/F

Finite State Machine (FSM)

INTC

DMA

INT_DO
INT_DI

DMARQ_DO
DMARQ_DI

SHE

RAM

AES

TRNG

Data Flash

ICU Exclusive Data Flash

Flash Control

Data Flash access path from CPU

ICU-S command access path from CPU
ICU-S Overview

- APB slave peripheral
- Commands and data transferred by the CPU or a DMA
  - Polling or interrupt handling possible

- Keys and certificates stored in a dedicated Data Flash area
  - Can be read, written and erased by the ICU-S only
  - Fail-safe mechanism in case of power fail during key update
  - CPU or ICU-S access to Data Flash arbitrated by ICU-S

- Device dependent data initialized by Renesas before shipment
  - Unique Identification Number, SECRET_KEY

- ICU-S operation complies to the SHE specification v1.1
ICU-M Block Diagram (Simplified View)

* Optional  CEG = Cryptographic Engine
ICU-M Overview

- Master peripheral: acts autonomously
- Has access to (almost) all internal MCU resources
- Programmable: can manage any type of security services
- Secure code and secret data stored in dedicated Flash areas
  - Can be read, written and erased by the ICU-M only
  - Smart Data Flash arbitration
- Powerful: embeds high-end cryptographic co-processors
### ICU-M: First Performance Estimations*

*based on simulation

#### AES encryption (@ 50MHz)

<table>
<thead>
<tr>
<th>Function</th>
<th>Test</th>
<th>Latency / 32-bit word</th>
<th>Estimated throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES (1) ECB / CBC</td>
<td>Read from far memory, encrypt and write back</td>
<td>5 clocks</td>
<td>~8 MB/s</td>
</tr>
</tbody>
</table>

(1) AES engine raw throughput ~50MB/s

#### Hashing (@ 50MHz)

<table>
<thead>
<tr>
<th>Function</th>
<th>Test</th>
<th>Latency / 32-bit word</th>
<th>Estimated throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA-1 (SW only)</td>
<td>Hash over Flash memory (iROM)</td>
<td>5 clocks</td>
<td>~1.5 MB/s</td>
</tr>
<tr>
<td>AES-based hash (HW+SW)</td>
<td>Hash over Flash memory (iROM)</td>
<td>5 clocks</td>
<td>~3.5 MB/s</td>
</tr>
</tbody>
</table>

#### RSA signature generation (@ 66MHz)

<table>
<thead>
<tr>
<th>Function</th>
<th>Test</th>
<th>Estimated timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA 2048 bits</td>
<td>Signature generation (w/o CRT (2))</td>
<td>~180ms (3)</td>
</tr>
<tr>
<td>RSA 2048 bits</td>
<td>Signature generation (w/ CRT (2))</td>
<td>~55ms (3)</td>
</tr>
<tr>
<td>RSA 2048 bits</td>
<td>Signature verification (e=2^{16}+1)</td>
<td>~1.4ms (3)</td>
</tr>
</tbody>
</table>

(2) CRT: Chinese Reminder Theorem
(3) As fast as a Pentium III @ 800MHz (source: “Secure Broadcast Communication” by A. Perrig)
## ICU Types And Variants (Summary)

<table>
<thead>
<tr>
<th></th>
<th>ICU-S</th>
<th>ICU-M2</th>
<th>ICU-M3</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICU Control</td>
<td><strong>FSM</strong></td>
<td><strong>CPU</strong> + Code Flash RAM: 24KB</td>
<td><strong>CPU</strong> + Code Flash RAM: 64KB</td>
</tr>
<tr>
<td>System Peripherals</td>
<td><strong>TRNG</strong></td>
<td><strong>TRNG</strong> <strong>TIMER</strong> <strong>WDT</strong></td>
<td><strong>TRNG</strong> <strong>TIMER</strong> <strong>WDT</strong></td>
</tr>
<tr>
<td>Cryptographic Accelerators</td>
<td><strong>AES</strong></td>
<td><strong>AES</strong></td>
<td><strong>AES</strong> <strong>CEG</strong></td>
</tr>
<tr>
<td>System Interfaces</td>
<td>slave</td>
<td>slave <strong>master</strong></td>
<td>slave <strong>master</strong></td>
</tr>
<tr>
<td>Accessible Resources</td>
<td>Data Flash (1KB)</td>
<td>All on-chip resources</td>
<td>All on-chip resources</td>
</tr>
<tr>
<td>Tamper Resistance</td>
<td>HW isolation of the ICU-S Data Flash</td>
<td>HW isolation of the ICU-M Code &amp; Data Flash</td>
<td>HW isolation of the ICU-M Code &amp; Data Flash</td>
</tr>
<tr>
<td>Compatibility</td>
<td><strong>SHE</strong></td>
<td><strong>SHE</strong> <strong>EVITA med.</strong></td>
<td><strong>SHE</strong> <strong>EVITA full</strong></td>
</tr>
</tbody>
</table>

CEG = Cryptographic Engine
ICU in RH850

Targeting all applications

Ultimately available in all device families
Security in *High-end Automotive SoC**: a Glimpse @ Renesas’ CryptoEngine

*SoC: System-on-Chip *without* embedded Flash
R-CAR-H1: High-end Automotive SoC

- 9 x 32-bit Timer
  - Cap/Comp, PWM
- 7 x 24-bit PWM
  - Programmable width
- WDT
- 4 x SD
- MMC
- 2 x USB Host
  - (480Mbps with PHY)
- USB Host/Funct
  - (480Mbps with PHY)
- Video Display:
  - WXGA
  - 4xRGB-in & IMR
  - 2xRGB-out
- JTAG/Coresight
- CryptoEngine
- 832pin FCBGA; 0.8mm pitch
- GPS BaseBand (option)
- Media Engine
- 2 x Cortex A9
  - 32KB i$, 32KB d$
  - Neon/FPU
  - 1GHz
  - 1MB L2$
- 2 x IMP-X3 (option)
- 32KByte RAM
- 2 x CAN
  - 32 Message Buffers
- IEBus
- MLB (MOST150)
  - 6-Pin I/F
- Ethernet MAC
- PCIe V2.0 (1 lane)
- SATA
- PATA
- 9 x I²S
- 4 x I²C (400Kbps)
- 3 x HSPI (26.6Mbps)
- 8 x UART
  - 6 x UART (1Mbps)
  - 2 x UART (10Mbps)
- 6 x UART (1Mbps)
- 2 x UART (10Mbps)
- 2 x HUART (3Mbps)
- 3 x HSPI (26.6Mbps)
- 32KByte RAM
- DDR3-1066 SDRAM
  - 2x1GB, 2x32 bit Data
- External Bus I/F/PATA
- DMA
- Gyro ADC IF
- GPIOs
- Media Engine
- 4 x Audio DSP (2xSPU2)
- Digital audio router & SRC
- 4 x IMR-X image renderer
- SH-4A for Media H/W control
- H/W HD video decoder (768KB RAM)
- 83MPoly/s; 2500MPix/s; 16GFlop/s
- R-GP2 map renderer
- HMI & 3D maps
- Dedicated cryptographic unit to provide high-end security services

*Note: IP from Imagination Technology
Outlook on Future Developments
Future: More Tamper Resistance

- Security is about being ahead of attacker capabilities

- HW isolation of secret Flash areas is a first level of security

- Other protections mechanisms are available in Renesas IP pool to countermeasure many kind of security attacks
  - Multiple circuits have designed within the last 15 years to counter invasive and non-invasive attacks in smart card ICs

- Careful assessments are required before integration into automotive MCUs
  - Relevance vs. technical constraints
  - Relevance vs. targeted security level
  - Cost impact
  - Regulations / enforcement of security in safety-relevant applications
Future: Dedicated HW Acceleration For C2X

- IEEE 1609 → Wireless Access in Vehicular Environment (WAVE)
  - IEEE 1609.2 → security protocols

- Message authentication method selected: ECDSA

- ECDSA throughput requirements:

- Existing solutions today?
  - FPGA-based @ very high freq.

- Renesas intends to develop a low-power solution to achieve several 100s of ECC signature verifications per second
  - Objective: integration into power-efficient automotive device
‘Enabling The Smart Society’

**Challenge:**
“Future in-vehicle systems will contribute to safer cars, safer roads, more efficient driving, easier maintenance and more fun”

“... as long as sufficient *trust* can be established in those systems...”

**Solution:**
“*Starts building trusted Automotive systems with Renesas solutions today!*”
Questions?
Please Provide Your Feedback...

- Please utilize the ‘Guidebook’ application to leave feedback

or

- Ask me for the paper feedback form for you to use...