

# **RESPONDING TO SECURITY THREATS IN THE SMART GRID**

Renesas Electronics Europe  
Secure MCU Centre

25th Oct 2010



# Agenda

- Introduction
- Smart Grid : Assets & Threats - Security implementation
- Renesas security experience - Products
- Security IC into networked environment
- Security considerations
- Conclusion

# What are the questions posed with this road sign ?

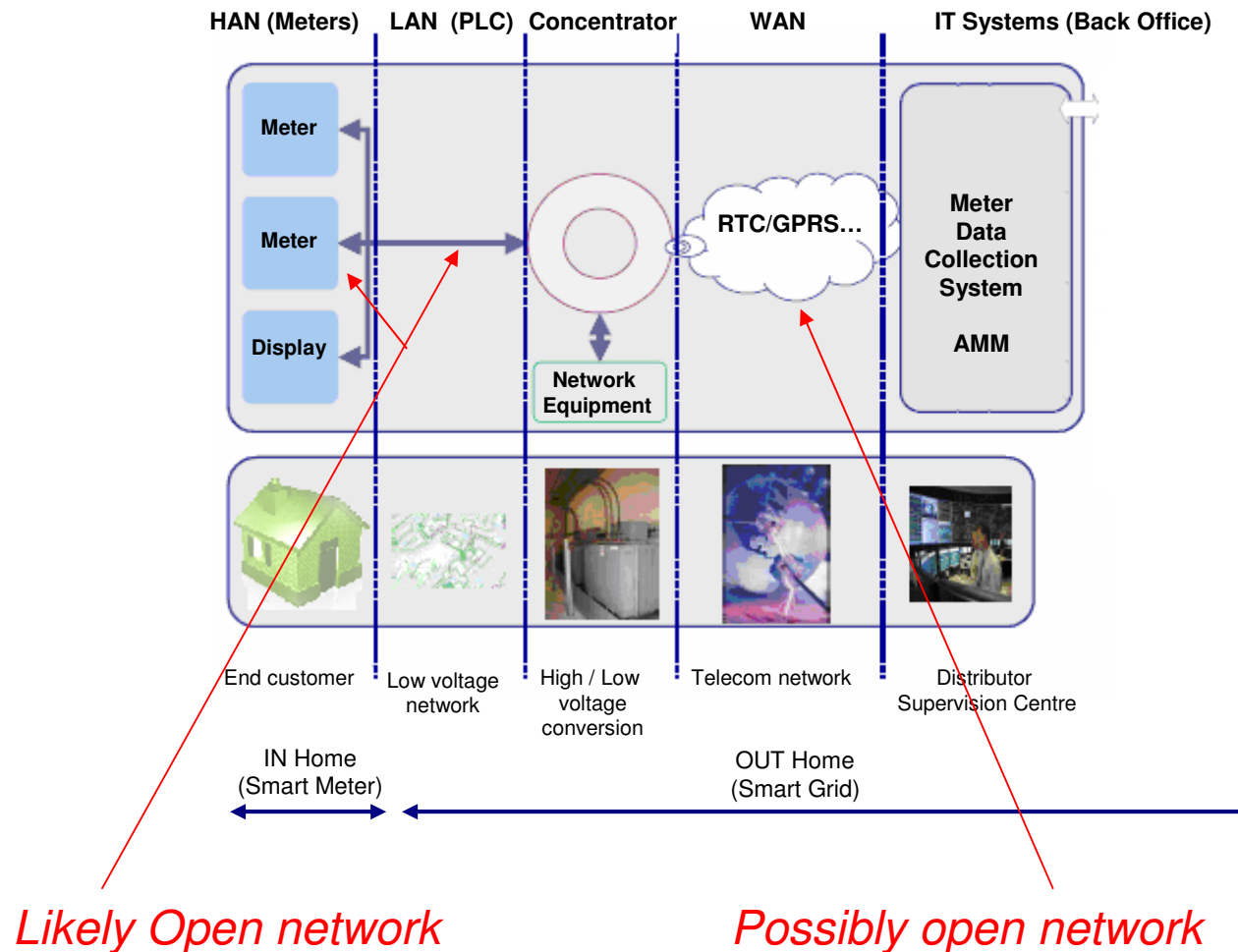
- Has the original message reached the display ?
- Does the display know who sent the message ?
- Is the message displayed the same as the original sent ?



AP Photo/Chris Nakashima-Brown

There are a lot of similarities between this visible example and AMI/Smart metering.

# Typical architecture for AMI



Hacking, fraud, cyber criminality are actual threats happening on open un-secure networks. Is there any reason why it would not happen on Smart Metering Infrastructure ?

# Security breaches - 3 main types

## Assets

- Energy value.
- Privacy.
- Energy supply dependability.

## Threats

- Fraud.  
Falsification of consumption index or tariffs, identity theft.
- Un-authorized parties accessing confidential/personal data.
- Mass cyber attacks through the networks.

## Fraud - Dispute

- Index consumption stored in the smart meter must not be altered.

→ *Memory protection, prevention of program code modification by un-authorized party is necessary.*

- Data (tariffs, index, time) must not be altered, deliberately or accidentally, during transmission.

- Identity of both sender & receiver must be verified.

*A well identified smart meter must only deal with a well identified Utility.*

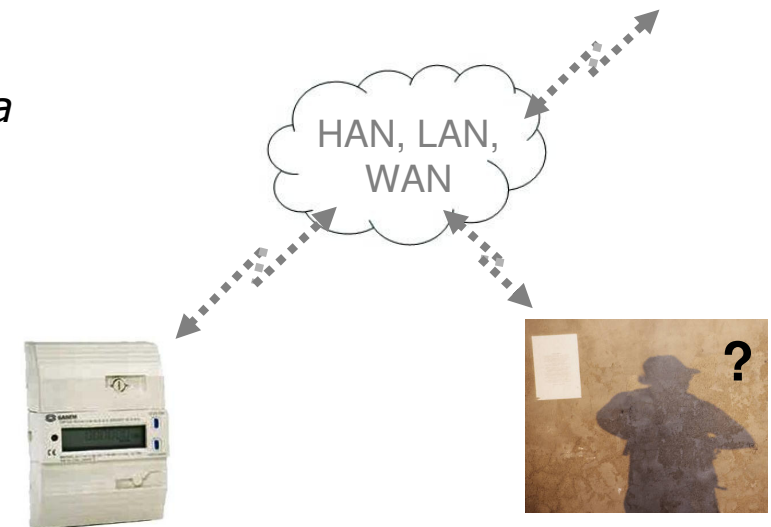
*It must be very difficult [impossible] to clone a smart meter.*

- Security implementation :

→ Tamper responsive or, better, tamper resistant device.

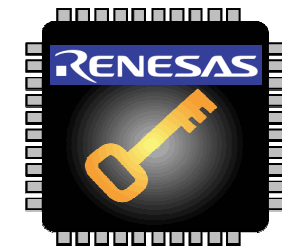
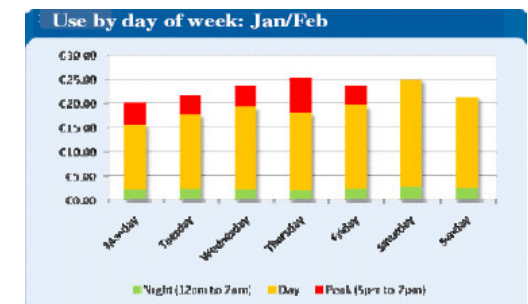
→ Mutual secure authentication between smart meter and Utility.

→ Hash function for data integrity.



# Privacy

- Traditional electricity (& gas) meters deal with simple tariff or a two part (day & night) basis
- Typical smart meter support ½ hourly measurement (48 measurements /day - Tariffs granularity can be the same)
  - It's possible to know if you are in or out, what you do (watching TV, going to sleep, getting up,...), at what time...
  - Your Personal profile/way of life is of high importance for several parties (Utilitie(s), commercial CIEs, others).
  - Use of these data by appointed energy providers is of top importance, but this is another debate : matter of ethics, best practices, regulation.
- All customer data must be kept confidential.
- Security implementation :
  - Encrypted communication.
  - State of the art : key protected in tamper resistant area, or temporary session key. Root key to be protected anyway.





# Mass cyber attack

- Modern societies absolutely require a dependable electricity supply.
- Smart meters can be remotely switched off/on, through open IP networks, for supporting both credit & prepayment tariffs, managing frequent resident changes, ...
- What if an attacker can send off-command to millions of meters ?  
Possible attackers : hostile government agency, terrorist organisation, militant group.
- In parallel, flexibility is requested :
  - it must be possible to add keys (new supplier entrant) into meters, or to remove keys (supplier bankruptcy, takeover, or even key compromise).
  - customers can move from one supplier to another one.
- Security implementation
  - Asymmetrical scheme / PKI / Certificates / Digital signature.
  - Symmetrical key (secret) architecture possible but more difficult to securely handle secret keys for all meters/customers.
  - Tamper resistant device to store private keys.
  - Ensuring secure firmware update.

This does not resolve all issues, but seems to be a solid basis to build on.

Who controls the off switch ? It MUST ONLY be the agreed Parties.  
Meter must reject commands from illegitimate sources.



# Security process for appropriate secure product

1. Identify assets to be protected
2. Identify threats (possible attacks) and vulnerabilities - Make relevant / sensible selection
3. Define and implement appropriate counter measure (hardware and/or software)

## So many possible attacks enabling access to platform assets...

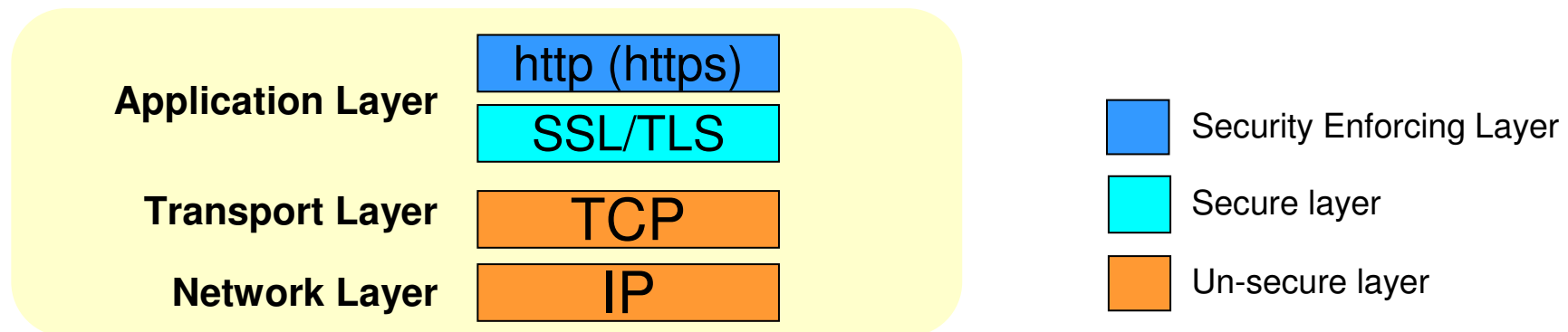
- Invasive attacks
  - Reverse engineering
  - Probing
  - FIB (Focused Ion beam)
- Passive attacks
  - Timing attacks
  - Side-channel analysis (Power, EM,...)
- Active attacks
  - Fault attacks
- Others

Which ones are relevant ?  
- In case of smart card applications : ALL !  
- And in case of **SMART METERING** ?

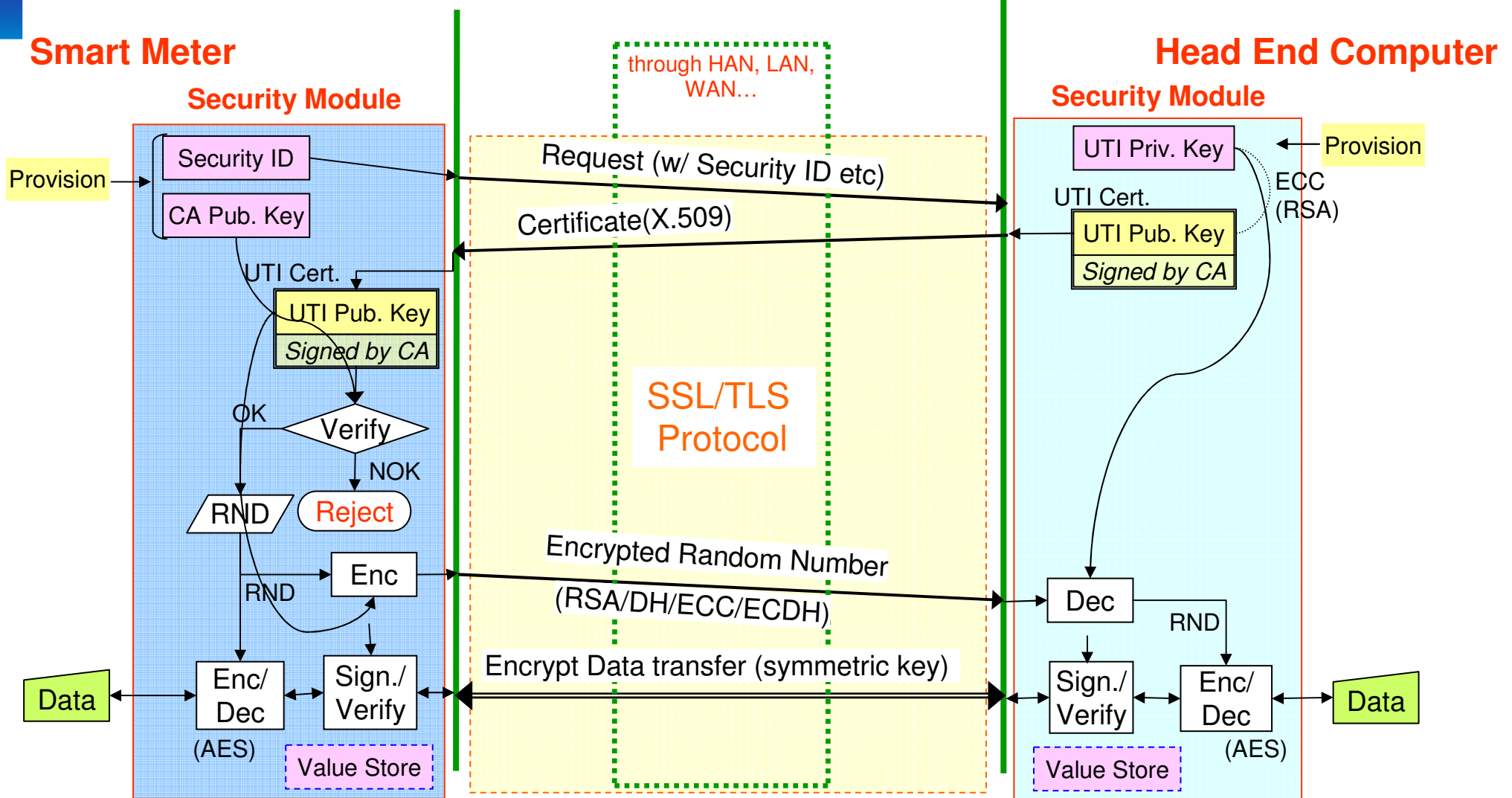
# Security IC into a Networked environment

- Several existing standards can be used to integrate a Security IC into a networked environment.
- Avoid developing proprietary formats / protocols.
- Example :
  - Public Key Infrastructure - Certificates : X509
  - SSL/TLS : encryption/decryption at application layer.
- See next slide an example of implementation by using X509 and TLS standards
- SSL/TLS on Web - Reminder :

*SSL/TLS are cryptographic protocols operating at the Application layer to ensure secure end to end transit at the Transport Layer.*

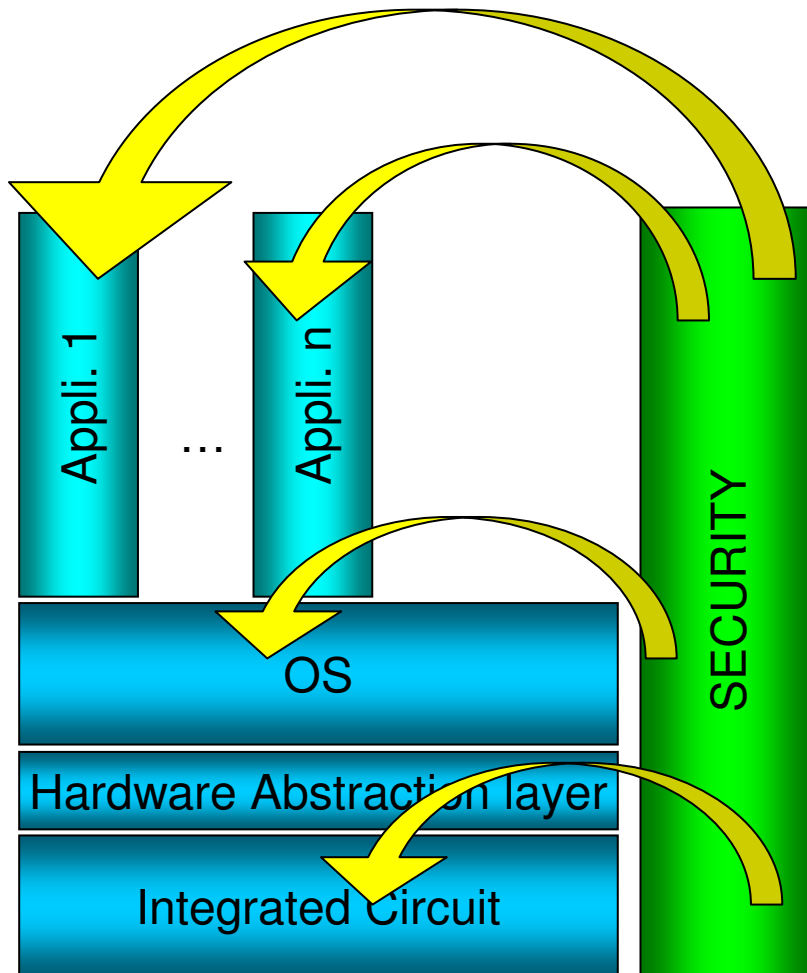


# Implementation example using existing standards



End to end communication is made perfectly secure, although going through un-secure networks

# Platform



## Platform assets to be protected :

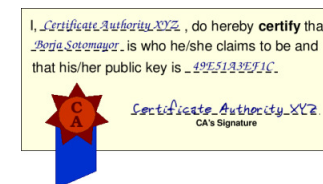
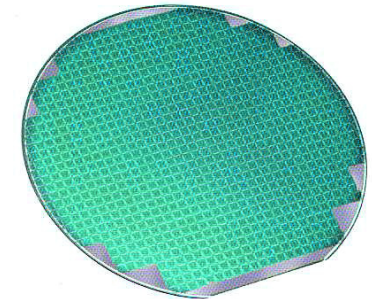
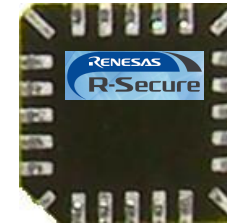
- Cryptographic keys
- Issuer data
- IPs: algorithm, code,...
- Private data

**Effective security implementation  
require Security features to be  
implemented at all levels**

# Security IC into Smart Grid - Sum up

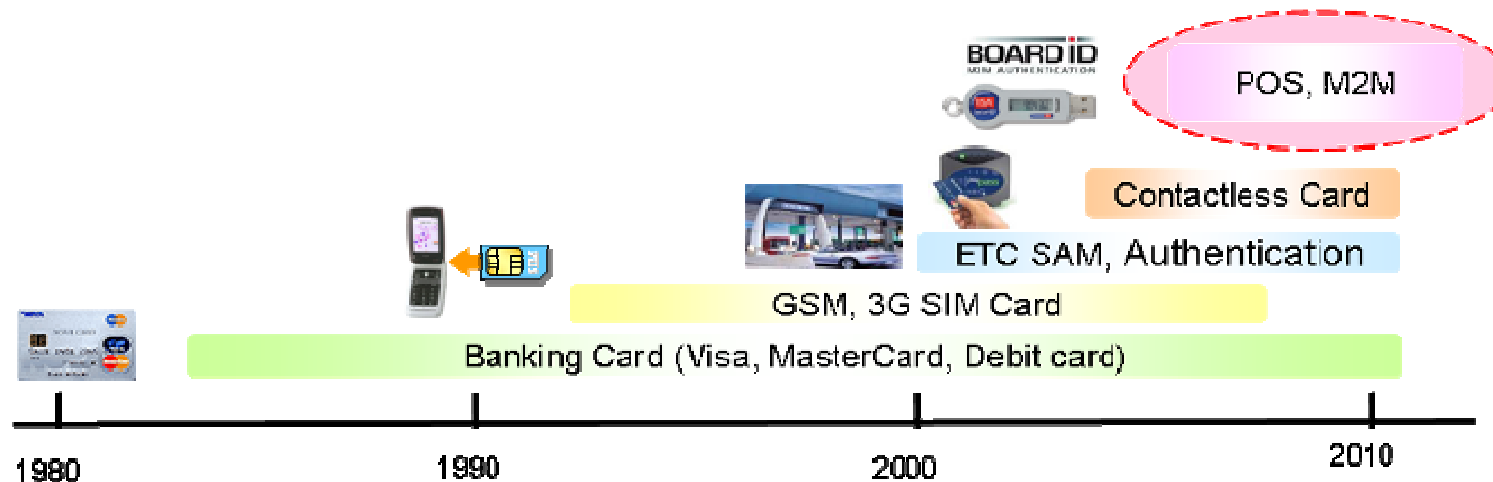
Renesas Secure microcontrollers can support :

- Strong authentication
  - Public Key (RSA, ECC)
  - Symmetric key (TDES, AES)
  - Data integrity (Hash)
  - Non-repudiation (Digital Signature)
  - True Random Number Generator
- Tamper resistance for secure key storage
- Secure download (eg: firmware upgrade)
- Security certifications (FIPS, CC, ...)
- Certificates standards (eg : X509)
- Secure connectivity (eg: SSL/TLS)



# Renesas security experience and support

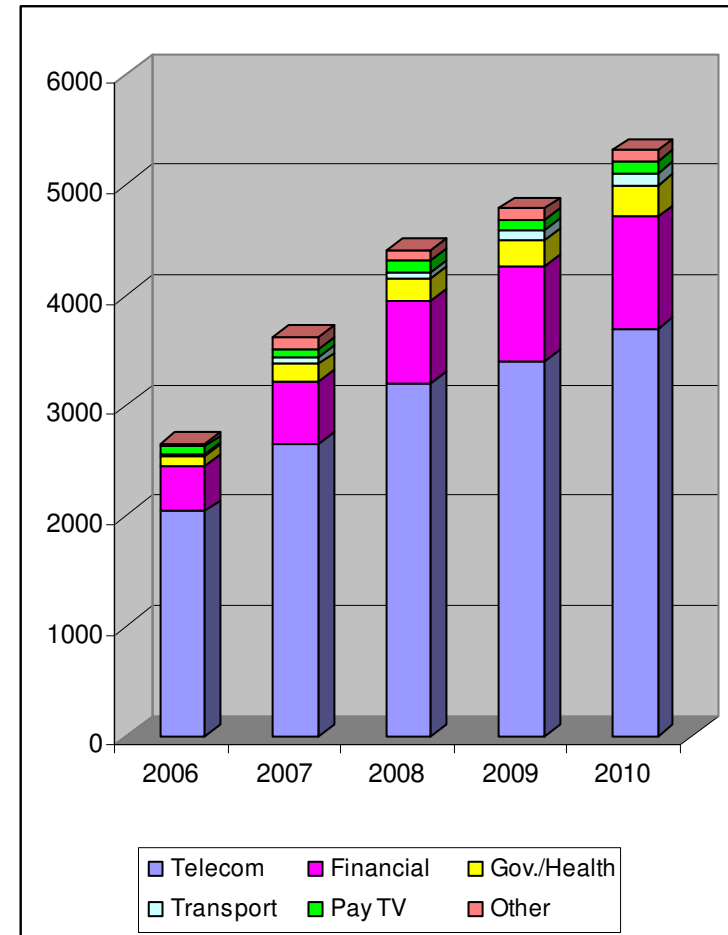
- Renesas has been designing and producing high-security ICs for the smartcard industry for many years
  - Several generations of secure MCUs have been developed over the years: H8/3xxx, AE-3, AE-4, AE-5 and the latest RS-4 devices. More than 3 Billion chips delivered ! (cumulative qty)
  - Specific versions of these ICs have been variously approved by MasterCard, Visa, ZKA, EMVCo and Common Criteria for use in security applications
  - Common Criteria evaluations have been carried out at the highest level of resistance to attack (VLA.4 - "no exploitable vulnerabilities")
  - **Embedded (non-smartcard) applications have also been supported, for authentication of accessories and for access controls**, for example.



- Renesas Electronics Europe Secure MCU Centre has resources to support Customers
  - Engineering (Crypto, security, tools), Product support (SAE Team), Sales & Marketing
  - Mainly located in Maidenhead (UK), Munich, Paris

# Secure Microcontroller Industry

- Volumes : >5 billions units shipped in 2010 !
- Applications :
  - Telecom
  - Finance
  - Governmental
  - Pay TV
  - Transport
  - ...now Embedded security/ New FF
- Secure supply chain
- Proven technologies & track records





## Renesas Electronics

can provide technologies bringing benefits to the Smart Grid sector,  
is ready to support Smart Grid security initiatives.

The Smart Grid sector is a strategic focus for  
Renesas Electronics, the #1 MCU company world wide.  
We are ready to support security requirements with a long term  
commitment.





Renesas Electronics Europe

© 2010 Renesas Electronics Corporation. All rights reserved.