M2M Secure Element
Short overview

March 2015

Where Security matters most

Software

- **Protected** environment
- **Trusted** users
- **Direct access** to data

Hardware

- **Unprotected** environment
- **Non trusted** users
- **No direct access** to data
- **Tamper resistant devices**

gemalto

Key functions of an M2M Secure element

Industry Leading Security Technology, Multiple Use Cases

Established form factors - 2FF, MFF2

Supports Consumer or Industrial Environment conditions

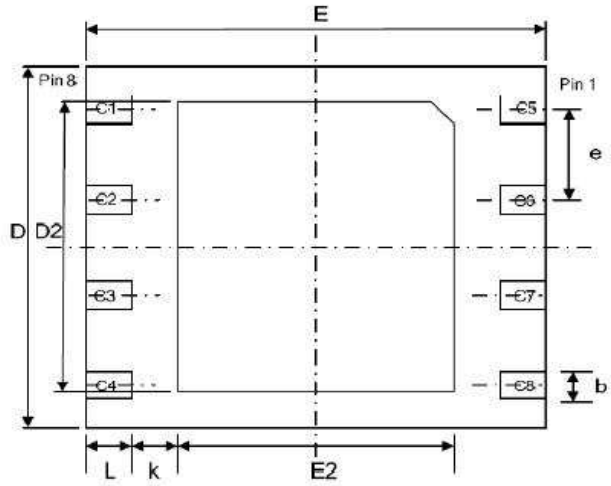
JavaCard allows custom application development

gemalto

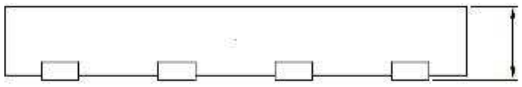
Which M2M SE form factor for which case?

2FF

for prototyping



Parameter	Dimensions (mm)
E	6,00 ± 0,15
D	5,00 ± 0,15
L	0,60 ± 0,15
b	0,40 ± 0,10
E2	min 3,30
D2	min 3,90
k	min 0,20
e	1,27 for tolerances see parameters bbb and ddd
bbb	0,10
ddd	0,05



Max 0,9mm

MFF2 (solderable)

for final Hardware development

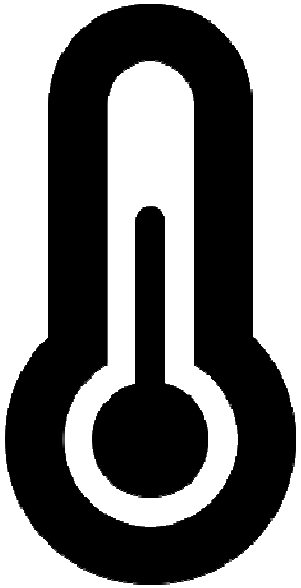
gemalto

M2M SE built on a reliable Hardware platform

- Minimum **500,000** write/erase cycles par page @ 25°C
- Common Criteria **EAL5+** certified

- M2M SE V1.0 Smart Grid
  - Operating temperature range: **-25 to +85°C**

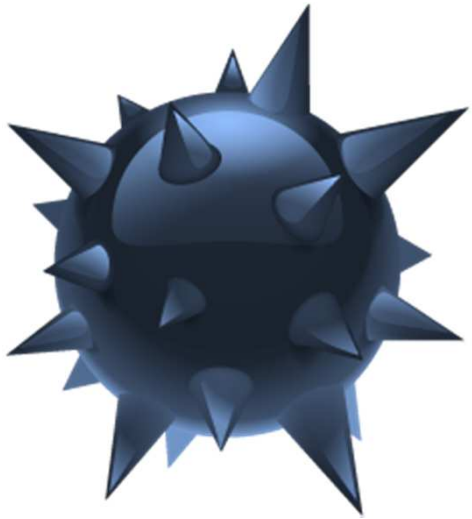
- M2M SE V1.0 Auto
  - Operating temperature range: **-40 to +105°C**
  - Extended Data retention: 17 years



M2M SE OS Security features

The OS includes multiple hardware and software **countermeasures against** various **attacks** such as:

- Side channel
- Invasive
- Advanced fault
- Other types : frequency, Light, Temperature, Glitch, Voltage, etc.



M2M SE Java Card Platform

- High security certification grade on chip-level and JavaCard Platform (both EAL5+)
  - Longer life expectancy
  - Higher resistance against attacks
- Common Criteria on JavaCard Platform
  - Upgradeability of the applets in the field without touching the chip
  - Quicker time-to-market in case of requested upgrades on applets running on the secure element
  - No full recertification required (only delta certif)
- Separate deployment of additional applets (e.g. for securing energy management and local controls)
  - No re-certification is required
  - If required the additional applets can be certified separtely
  - Ready for remote provisioning of new applets over lifetime

Exemple of a convenient cryptographic toolbox

MultiApp V3.0 Java card platform

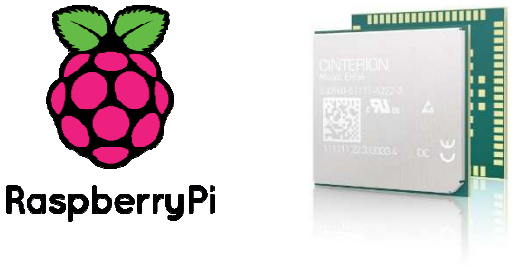
- Complies with **Global Platform 2.1.1** and **Javacard 2.2.2**
- Cryptographic features
  - algorithms: **3DES, RSA** up to **4096** bits, **AES** (128, 192, 256), **ECC** up to P**521** bits, **SHA1** & **SHA2** (224, 256, 384, 512)
  - **On board Key Generation**
- **Certified CC EAL5+ with Java Card protection profile**

Middleware: drivers & library

Gemalto provides:

- **drivers** for various host OS:

And Variety of platforms:



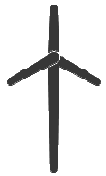
- **PKCS#11 library**

- Compliant with PKCS#11 v2.20
- Available for 32 bits and 64 bits OS
- Allows seamless integration with software accepting PKCS#11 tokens: OpenSSL, GnuTLS, Truecrypt, OpenSSH, Java Cryptography Extension (JCE) …

gemalto

Take Away

- M2M Secure Element provides:
  - **Strong Authentication /personalisation** of the edge device through a diversified ID scheme
  - **Toolbox** to ensure signature and encryption of data
  - Hardware tamper **resistance**



- To protect against
  - **Physical attacks** on the device,
  - **Remote software attacks** for use cases where the incentive to attack is strong, especially Smart Grid and Auto