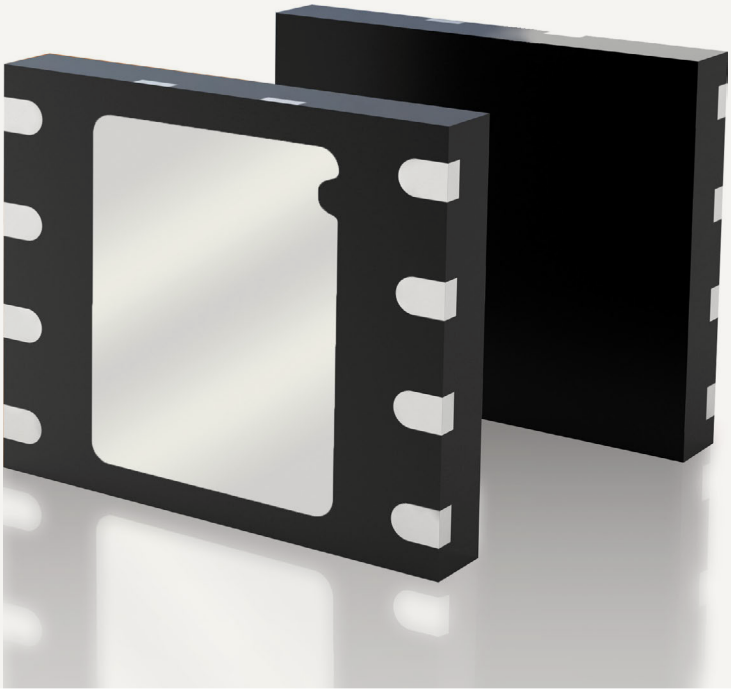
Cinterion® **Secure Element**



BUILDING A FOUNDATION OF TRUST: THE CINTERION® SECURE ELEMENT

Tamper-resistant, advanced protection for automotive and IoT solutions

Cinterion® **Secure Element.** **Tamper-resistant, advanced protection for automotive and IoT solutions**

The rise of the Internet of Things (IoT), smart cities, connected cars and smart homes has opened the door to a world of new possibilities - expanded productivity, improved safety, time and cost savings, enriched services, new business opportunities plus overall conveniences that simplify our lives. With billions of new connections expected in the next decade, it has never been more important to design solutions for trust.

The Gemalto Cinterion Secure Element provides a foundation of trust for IoT solutions. It is a tamper-resistant hardware component embedded in cars, industrial connected equipment and IoT solutions to deliver smart card level digital security and enable device lifecycle management. Part of advanced end-to-end security architecture, the Secure Element protects data integrity and defends against digital and physical attacks.

Ruggedized for reliability and longevity in the extreme environmental conditions typical of M2M and IoT applications, it ensures that data is stored in a safe place and that access is granted only to authorized applications and people.

It also enables over-the-air management of security credentials, software updates and evolving security capabilities across the lifecycle of solutions. The Cinterion Secure Element works with any vertical market application including connected cars, smart grids, smart city solutions and more. It provides a powerful key to help secure the entire IoT ecosystem.

Security by Design

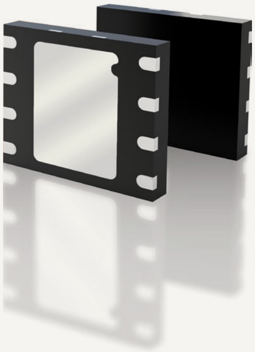
Gemalto secures the DNA of M2M and IoT solutions. Our security by design approach and suite of M2M optimized solutions protects the device, the data, the network and cloud ecosystem allowing people and enterprises to trust in our connected world. With decades of experience across a wide range of vertical markets and regions, Gemalto is your trusted partner for risk evaluation and security architecture that protects the right data at the right level and across the entire lifespan of the device.

WORLD SMART WEEK

2015 Innovation Award for Connected Security

Cinterion® Secure Element has won the **2015 Innovation Award for Connected Security** at World Smart Week (Marseille, France). Judged by a panel of leading industry analysts, influencers, and visionaries and presented at World Smart Week, the prestigious award honored the Cinterion Secure Element for innovation in smart connected security for mobile, Machine-to-Machine (M2M), Internet of Things (IoT) and cloud environments.

A ROOT OF TRUST



> Foundation of Trust
Ensures that data is stored in a safe place and that access is granted only to authorized applications and people

> Future Proof Security
Blends smart card level security with multi-application capabilities and allows for life cycle management and adaptive security for always up-to-date protection

> Tamper Resistant
Ruggedized for extreme environments and tamper resistant for high reliability and protection against physical attacks

Cinterion® **Secure Element Features**

GENERAL FEATURES

> Operating System
Javacard 3.0.1 Classic

> Global Platform 2.2
SCP01 implementations 5 and 15
SCP02 implementations 5, 15, 45 and 55

> Communication Interface
ISO/IEC 7816-3 compliant
T=0, PPS up to TA1=96
External clock from 1 to 5 Mhz

> Voltage & Current Consumption
Support From 1,62V up to 5,5V
Configurable current consumption profile: 2G / 3G / free mode
Support the Clock stop mode support (current consumption below <100µA)

> NVM
User NVM configurable from 80KB up to 480KB

SECURITY FEATURES

> Cryptographic features
DES, 3DES (ECB, CBC), AES up to 256 bits
RSA keys up to 2048 bits
Elliptic curves support from 224 bits to 384 bits
SHA-1, SHA-256, SHA-384 bits
RSA according to ISO 9796-2 or PKCS#1 v2.1 (PSS-OAEP)
On Board Key Generation
Cryptographic profile can be updated to client's needs

> Security
True RNG according to AIS31
The OS includes multiple hardware and software countermeasures against various attacks:
Side channel attacks (SPA, DPA, Timing attacks,...)
Invasive attacks
Advanced fault attacks
Other types of attacks (Frequency, Light, Temperature, Glitch, Voltage, etc)

ADDITIONAL FEATURES

> Solderability
MSL1 package (Jedec J-STD-020)
Ni/Pd/Au PPF plating
Package classification reflow temperature: 260°C
Lead free packaging compliant to the European Directive for Restriction of Hazardous Substances (RoHS directive).

> ESD
Protection > 4 kV (H

> Electric Personalization
The SE comes with a default profile loaded during the personalization process:
SE unique identifier
Issuer Security Domain with a 3 keys keyset

> This profile can be updated to match customer needs with:
- Supplementary security domains
- Customer Applets
- Supplementary keysets / keys
- Customer specific diversification algorithm
- Customer specific DF / EF

> Graphical Personalization

Gemalto proposes to personalize characters using laser technology on the top of the package.
- First line is reserved for silicon provider traceability
- 2 lines of 10 characters maximum for customer personalization. We strongly recommend printing a visual identifier
- 1 line for customer identifier (TRIGRAM)..

“The growing reliance on IoT solutions and high profile cyber-attacks are focusing industry minds on the necessity of security technology for continued growth. Security at this level does not work as an afterthought. It must be incorporated from the ground up at the start of new development projects. The Cinterion Secure Element provides for this, combining flexibility with high levels of security.“

- Robin Duke-Woolley, CEO at leading technology analyst firm Beecham Research

The information provided in this brochure contains merely general descriptions or characteristics of performance, which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. All product designations may be trademarks or product names of Gemalto M2M GmbH or supplier companies whose use by third parties for their own purposes could violate the rights of the owners. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. ARM9 is a registered trademark of ARM Limited.

micromax technology

1300 906 911
micromaxtechnology.com
info@micromaxtechnology.com

SUSTAINABLE CERTIFICATION
✓ ISO 9001
✓ AS/NZS 4801
✓ ISO 14001

JAS-ANZ

gemalto
security to be free