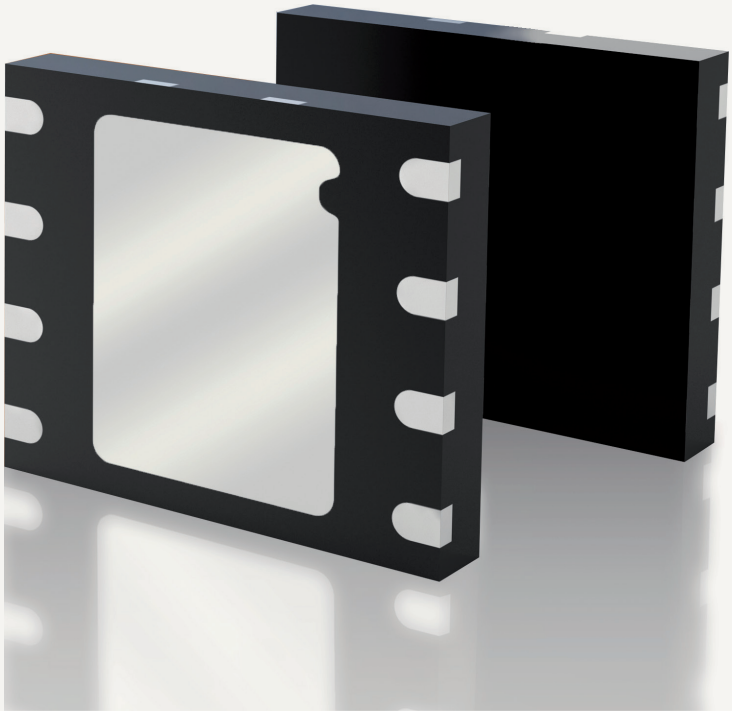
gemalto
security to be free



Cinterion® Secure Element

A Strong Foundation of Trust for IoT Solutions

"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 with high levels of security."

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

Cinterion® **Secure Element.**

Tamper-resistant, advanced protection for IoT applications and data

The Risk of IoT Cyber Attack is Expanding

As the number of IoT connections expands into the tens of billions, the potential for cyber-attacks is also on the rise. Because IoT devices are designed for long life with the majority being both physically accessible and unattended, they are particularly vulnerable to security breaches. The number of malicious IoT DDoS attacks increased 91% in 2017[1] alone while cloning and hacks into interconnected systems are also increasing. It has never been more important to secure IoT devices, applications and ecosystems with strong hardware security technology.

Building a Foundation of Trust

Gemalto's Cinterion Secure Element (SE) provides a solid foundation of trust for the most security-sensitive IoT solutions. It is a tamper-resistant platform embedded in IoT devices to ensure that sensitive data is stored, processed and protected in an isolated trusted environment.

It hosts confidential and cryptographic data according to strict industry security standards. As part of an advanced, end-to-end security architecture, the Secure Element ensures data confidentiality and integrity and defends against digital and physical attacks.

Cinterion Secure Element 4 Major Functions

Serving as a secure cyber vault, the Cinterion SE provides four key functions:

- **Protection of the device´s private key**
- **Storage of 3rd parties root certificates**
- **On-board cryptographic capabilities**
- **End-to-end authentication of devices and external IoT platforms** (mutual authentication and data encryption through TLS connection)

Inside-Out Protection for the IoT

END-TO-END CYBER DEFENSE

Inside: Software Protection

> True random number generation
> Sophisticated cryptographic computation
> Code/logic obfuscation: [a+b] or [(a*b)/a + (b/a)*a + ((a^b)/(a^(b-1)) – b]
> Constant-time programming
> Redundancy and consistency checks
> Data integrity verification
> Detection of wrong execution flow
> Encryption of secret data: cryptographic key protection
> Random delays in processing

Outside: Hardware Defense

> Single-component chip design
> Active shielding
> Glue logic design: mixed functional blocks on silicon
> Encrypted buses and memories
> Layered production: buried buses, scrambled memories
> Reduced power signal and electromagnetic emissions
> Analogical Sensors: voltage, frequency, light, temperature monitoring
> Logical sensors: detection of inconsistent processing
> Error correction code and memory integrity

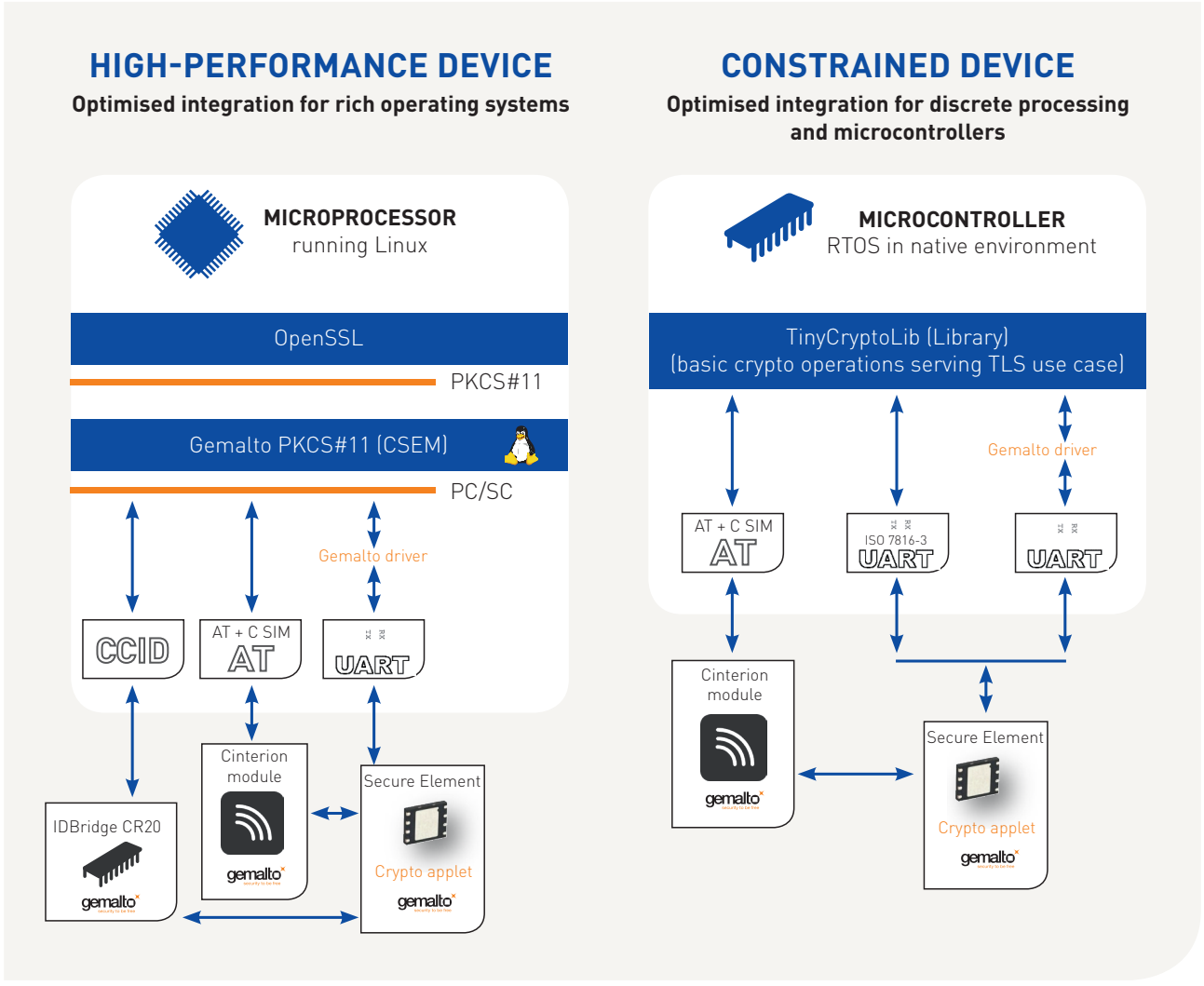
1 - https://www.techrepublic.com/article/ddos-attacks-increased-91-in-2017-thanks-to-iot/

Cinterion Secure Element Reference Platforms

The Cinterion SE is pre-integrated with major reference platforms, helping customers meet varying IoT security requests and supporting consumer, industrial and automotive IoT devices.

Ideal for both high performance devices, such as gateways, and constrained ones, the Cinterion SE mitigates risk for a variety of applications. It has been designed and reference tested with the most popular platforms, including the **iMX6UL for high-end devices** and the **STM32 for constrained ones.**

These platforms integrate seamlessly with IoT Modules via UART drivers. They are supported by a Gemalto SE Crypto Applet that performs the main cryptographic operations involved in a TLS connection.



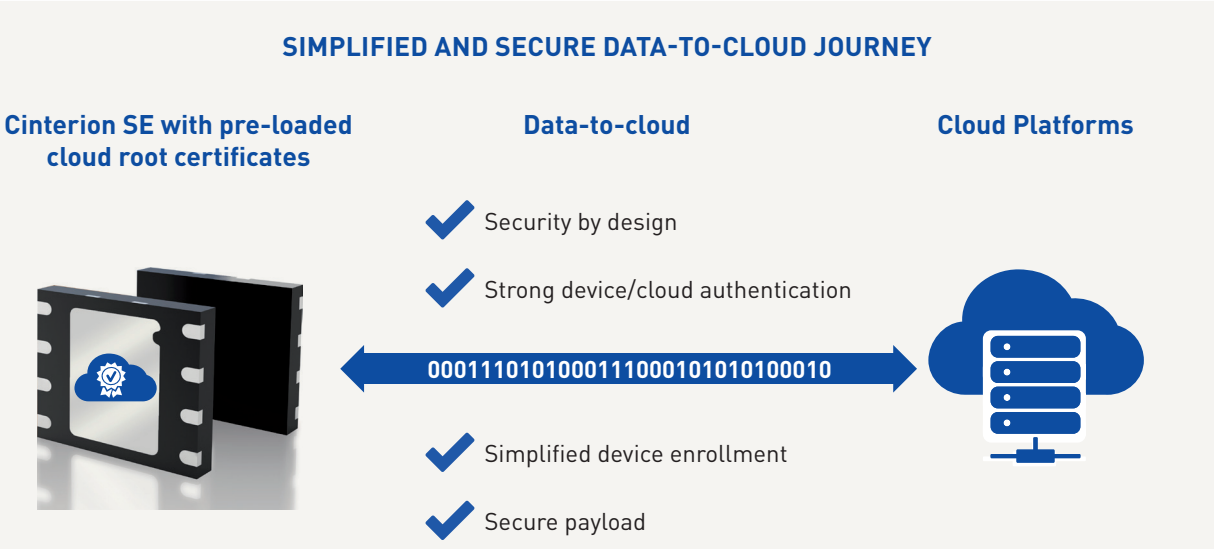
´Ready to Go´ Offer

Gemalto issues Gemalto-branded device certificates through a dedicated certification authority. These are loaded onto the Cinterion SEs during personalization, as well as IoT cloud platforms´ root certificates (trust anchor) which will simplify devices cloud onboarding.

Once devices are ready to exchange data with cloud applications, the pre-loaded certificates will enable a secure authentication between devices and external cloud platforms and thus simplify devices enrollment to the chosen platform (AWS, Microsoft Azure, IBM Watson to name a few).

Customers can focus on their core business as Gemalto takes the PKI (Public Key Infrastructure)-related burden off their shoulders and ensures that data can be exchanged securely.

SIMPLIFIED AND SECURE DATA-TO-CLOUD JOURNEY



GEMALTO.COM/IOT

gemalto
security to be free