Trusted Data

The IoT transforms big data into smart data but it´s only beneficial if it can be trusted. Gemalto ensures data integrity and privacy with advanced encryption, authentication and identification solutions

> **Cinterion Machine Identification Modules**, or MIM™, encrypt and authenticate data and securely identify devices on global mobile networks
> **Cinterion Secure Elements** provide a tamper-proof environment for secure storage of encryption keys and security credentials. Remote security updates further protect against evolving physical or digital attacks, insuring access is given only to authorized applications and people
> **Safenet KeySecure** platform provides flexible options for secure and centralized key management, deployed in physical, virtualized infrastructure and cloud environments
> **Safenet Hardware Security Modules** (HSMs) add an extra protection layer to safeguard centrally stored keys. The hardened, tamper-resistant appliance enables secure lifecycle management at the core, protecting most sensitive keys from compromise

Focus: mHealth Solutions You Can Trust

Highly sensitive mHealth solutions require Gemalto's strong encryption and authentication solutions to prevent data intrusion, protect intellectual property and provide access to authorized users only. Gemalto Cinterion Secure Elements provide an added layer of tamper-proof security to protect against physical and digital threats securing mission critical credentials and data. Gemalto's solutions protect IoT systems at the core and master devices to prevent attacks and defend against fraud.

Trusted Ecosystem

Gemalto extensive services and platforms establish a simplified environment where security can be remotely managed and updated over time, helping eliminate potential threats as they arise.
> Gemalto manages the secure storage and distribution of credentials across complex ecosystems and long-life solutions involving a large amount of stakeholders
> **Gemalto Trusted Service Hub** (TSH) acts as a central interconnection platform, allowing the secure deployment of new services and security updates towards devices already in the field

Focus: Protecting the Smart Energy Grid

Smart meters and smart home hubs provide the backbone for the emerging smart grid. Gemalto solutions ensure only authorized stakeholders have access to sensitive meter data. They also shield energy company infrastructure and IT systems from intrusion protecting against fraud and theft. In a highly regulated market, Gemalto solutions meet all requirements including the Common Criteria protection profile.

Gemalto secures the DNA of M2M IoT Solutions
Gemalto's security-by-design approach and array of solutions and services protect the device, the data, the network and the IoT ecosystem across the lifespan of M2M IoT applications. For a risk evaluation or security consulting services, contact us at: iot.query@gemalto.com

WWW.GEMALTO.COM/M2M

gemalto
security to be free

gemalto
security to be free

Trust is Everything
The Gemalto Pocket Guide to Securing the Industrial Internet of Things

micromax technology

1300 906 911
micromaxtechnology.com
info@micromaxtechnology.com

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

JAS-ANZ

In an age where everything is connected and cyber-attacks are inevitable, trust is essential. Gemalto delivers the solutions, services and platforms that protect Machine-to-Machine (M2M) and Internet of Things (IoT) applications from the edge to the core. Gemalto allows enterprises and people to trust in our increasingly connected world.

Security by design is the golden rule when it comes to enabling Trust. Gemalto helps mitigate threats at every level by building a foundation of trust that underpins the entire ecosystem protecting what matters, where it matters and when it matters most.

BIG DATA
DATA IN MOTION
DATA IN MOTION
DEVICE & DATA IN MOTION
DEVICE & DATA IN MOTION
DEVICE & DATA AT REST

M2M IoT Ecosystem

Trusted Devices

Gemalto Cinterion® M2M hardware solutions enable secure connectivity and strong encryption and authentication. They are optimized for long lifecycles and ruggedized for extreme industrial environments.

> **Cinterion M2M Modules** enable reliable communications over global wireless networks to support long lifecycles up to 10-15 years
> **Cinterion Machine Identification Modules**, or MIM™, encrypt and authenticate data and securely identify devices on global mobile networks
> **Cinterion Secure Elements** provide a tamper-proof environment on the device for secure storage of encryption keys and security credentials. Embedded cryptographic tools ensure high personalization of devices and thus strong authentication. Remote security updates can further protect devices against evolving physical or digital attacks across the lifecycle of solutions

Focus: Trusting Connected Cars

Security is integral to connected cars. Global automakers and Tier 1 suppliers rely on Gemalto to evaluate risk at every level of the ecosystem and develop customized, end-to-end security architecture to mitigate threats. With its ruggedized, auto-grade M2M technology, Gemalto provides secure connectivity and data access control to prevent unauthorized intrusions. Gemalto securely enables compelling features such as 4G LTE infotainment systems, advanced smart powertrain solutions, eCall for immediate roadside assistance, Advanced Driver Assistance Systems, secure NFC keyless entry and ignition, shared vehicle programs and much more.

Trusted Network

Gemalto optimizes mobile network quality of service enabling secure over-the-air updates that ensure the integrity and longevity of connected devices.

> **Cinterion M2M Modules** leverage industry standards such as TLS (Transport Layer Security) providing end-to-end security for environments needing it the most
> **Gemalto MIM Services** Platform enables regular MIM audit and hardware monitoring, allowing over-the-air MIM updates before service or security issues arise.
> **Gemalto Trusted Key Manager** provides an extra security layer allowing encryption key and credential management for the lifecycle of solutions, which simplifies production processes and device onboarding on non-cellular LPWAN networks
> **Gemalto LinqUs IoT Quality of Service** monitors smart device connectivity and performance in real-time, ensuring immediate troubleshooting if issues arise

Focus: Securing Connections in Smart Cities

Gemalto enables trust in Smart City solutions. Network security is reinforced with banking class TLS connections that ensure the privacy, confidentiality and integrity of the data exchanged between devices and applications. Gemalto's advanced authentication technology improves quality of service, enables preventive maintenance and helps ensure mobile networks are secure.