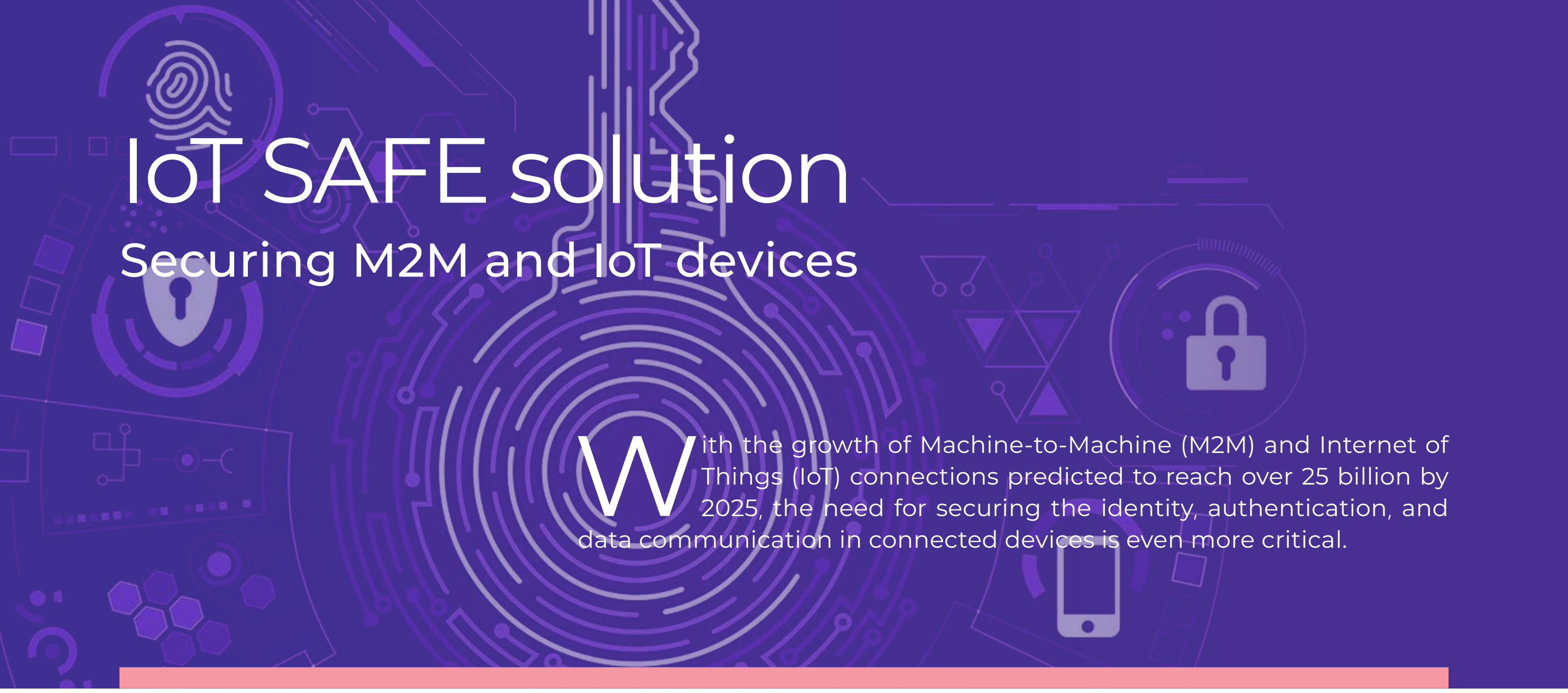


IoT SAFE solution

Securing M2M and IoT devices

With the growth of Machine-to-Machine (M2M) and Internet of Things (IoT) connections predicted to reach over 25 billion by 2025, the need for securing the identity, authentication, and data communication in connected devices is even more critical.

Securing the IoT ecosystem

The IoT is giving us more control over what we do. From consumer products, enterprise, or industrial needs, the use cases are endless. As this ecosystem continues to expand, mobile network operators, OEMs, and other service providers need a standardized secure solution that protects their IoT initiatives from cyberattacks and other security breaches. Driven by the mobile industry the GSMA introduced IoT security standards with the introduction of IoT SAFE.

Our offer

IDEMIA's IoT SAFE solution offers enhanced, end-to-end security for IoT deployments. It is designed to securely connect devices to the cloud by leveraging a hardware secure element or “Root of Trust” to establish end-to-end, chip-to-cloud security, as recommended by the GSMA IoT Security Guidelines. This includes SIM, eSIM and the Integrated SIM secure elements.

Our IoT SAFE technology provides other security services in addition to GSMA standard guidelines in order to ensure that the identity, authentication, and data communication from the client application on the device to the client server (i.e. in the cloud) is always secure.

Our solution enables Zero Touch Provisioning (ZTP) to eliminate most of the manual tasks involved with adding them to a network, thus simplifying the massive and automatic deployment of IoT devices.

Highly secure

Leverages the SIM as “Root of Trust” to securely store keys and certificates.

Simple deployment

IoT SAFE is based on (e)SIM interoperable and standard functionalities.

Remote management

Flexible remote provisioning management of IoT SAFE application.

Why IDEMIA?

Trusted by over 500 mobile operators globally, with 900 million SIM cards shipped in 2020 and over 5 million eSIM profiles activated, IDEMIA is leading the way in the IoT ecosystem with dedicated M2M/IoT SIMs and eSIMs for commercial, industrial, and automotive segments. Our ongoing commitment to innovation facilitates IoT SAFE implementation and the possibility of enabling other IoT security services, such as our OTA Quality of Service and Smart Connect Subscription Management platforms, to ensure optimized IoT deployment from small to large scale.

IDEMIA

IoT SAFE solutions for two different needs:

Applet #1 (eSIM)

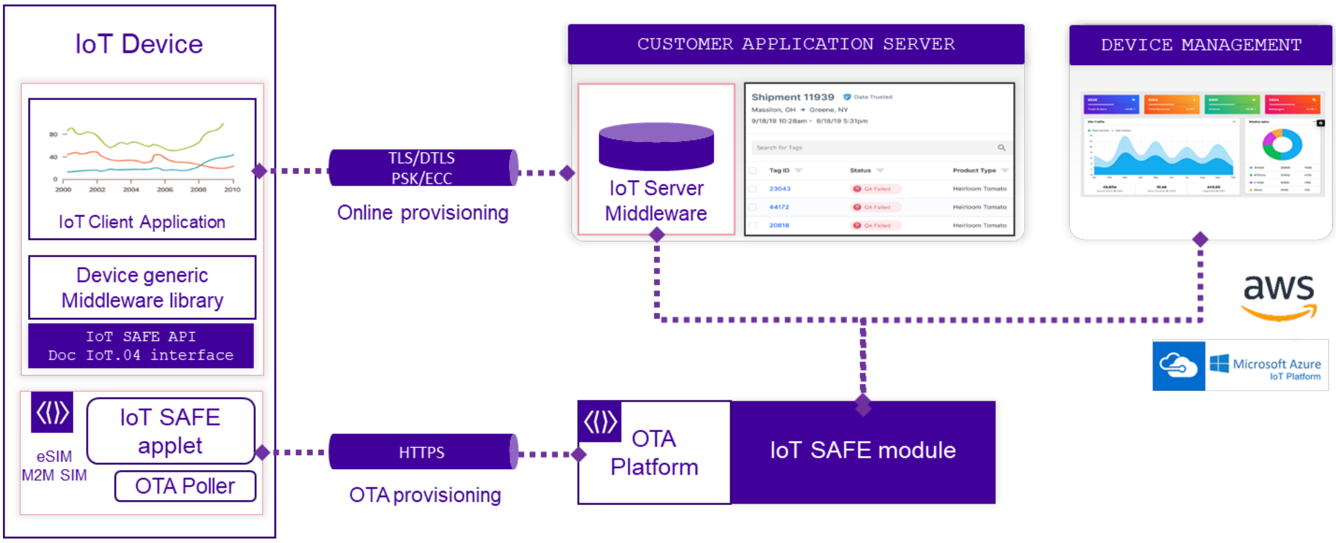
PSK-ECDHE scheme

- Enables the market de facto standard (D) TLS configuration, based upon PKI
- Secures access to all major cloud providers
- Facilitates cloud provider selection thanks to IoT Security Services
- Key-pairs are generated directly inside the application for a best-in-class security level

Applet #2 (SIM)

PSK scheme

- Overcomes limitations of constrained devices where RSA/ECC is not possible
- Enables security services on non-asymmetric secure elements
- Entry-level security approach
- Security based on pre-shared keys and symmetric cryptography



IoT Device

IoT Client Application

Device generic Middleware library

IoT SAFE API Doc IoT.04 interface

eSIM M2M SIM

IoT SAFE applet

OTA Poller

TLS/DTLS PSK/ECC

Online provisioning

HTTPS

OTA provisioning

CUSTOMER APPLICATION SERVER

IoT Server Middleware

DEVICE MANAGEMENT

aws

Microsoft Azure IoT Platform

OTA Platform

IoT SAFE module

GSMA IoT SAFE standards

- SIM serves as 'crypto-safe'
- Compatible with: SIM, eSIM, iSIM
- Helps solve challenge of provisioning millions of IoT devices
- Zero touch provisioning (ZTP)
- Provides a common API for the highly secure SIM to be used by IoT application running on the device
- Key rotation
- End-to-end data security
- Interoperable

And tomorrow?

- Integration with new device (D)TLS libraries
- E2E data security
- Firmware update authorization
- Continuously implement new standards and features