IoT SAFE

IoT **S**IM **A**pplet **F**or Secure **E**nd-to-End Communication

Leveraging a hardware secure element, or 'Root of Trust', to establish end-to-end, chip-to-cloud security for IoT products and services is a key recommendation of the GSMA IoT Security Guidelines. This requires both the provisioning and use of security credentials that are inside a secure place within the device.

The SIM is best suited to function as the hardware Root of Trust in an IoT device as it has advanced security and cryptographic features and is a fully standardised secure element, enabling interoperability across different vendors and consistent use by IoT device makers.

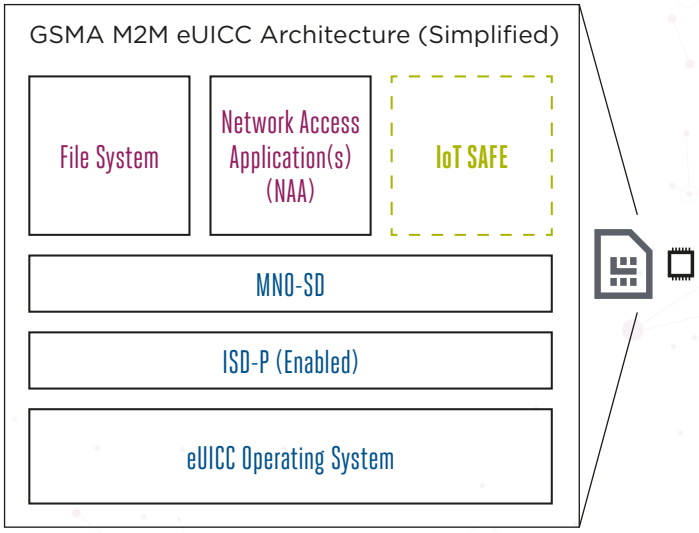
IoT SAFE (**IoT S**IM **A**pplet **F**or Secure **E**nd-to-End Communication) enables IoT device manufacturers and IoT service providers to leverage the SIM as a robust, scalable and standardised hardware Root of Trust to protect IoT data communications.

ROBUST AND EFFECTIVE IoT SECURITY AT SCALE

IoT SAFE provides a common mechanism to secure IoT data communications using a highly trusted SIM, rather than using proprietary and potentially less trusted hardware secure elements implemented elsewhere within the device.

IoT SAFE:

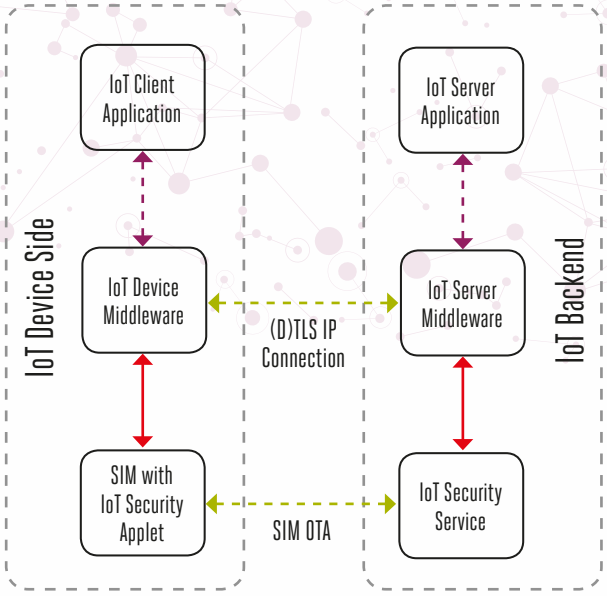
- Uses the SIM as a mini 'crypto-safe' inside the device to securely establish a (D)TLS session with a corresponding application cloud/server
- Is compatible with all SIM form factors (e.g. SIM, eSIM, iSIM)
- Provides a common API for the highly secure SIM to be used as a hardware 'Root of Trust' by IoT devices
- Helps solve the challenge of provisioning millions of IoT devices



IoT SAFE SIM Architecture (Example)

IoT SAFE PROVIDES SECURITY SERVICES THAT ENABLE:

- IoT devices to securely perform mutual (D)TLS authentication to a server using either asymmetric or symmetric security schemes
- IoT devices to compute shared secrets and keep long-term keys secret
- Provisioning and credential lifecycle management from a remote IoT security service



		IoT SECURITY APPLET 1	IoT SECURITY APPLET 2
TLS Version		(D)TLS 1.2 and 1.3	(D)TLS 1.2 and 1.3
Cryptography	RSA	Yes* (2048 bit)	No
	ECC	NIST P256	No
	ECDHE	Yes	No
	ECDSA	Yes	No
	PSK	Yes* (512 bits)	Yes (512 bits)
SHA-256		Yes	Yes
HMAC		Yes	Yes
HKDF		Yes	Yes

*optional

Download the IoT SAFE technical specifications from the GSMA website:
gsma.com/iot/iot-safe