IoT SAFE: Robust IoT security at scale

The why, what and how of securing IoT applications and data

June 2021

Table of Contents

Introduction

A recent GSMA intelligence survey[1] revealed that ninety-eight percent of enterprises want an end-to-end security solution that protects data integrity and confidentiality from IoT devices where data is collected, to the cloud where it is stored and processed. Seventy-two percent of enterprises consider device-to-cloud security as a very important feature when selecting a solution.

The most common method of protecting data from devices to the cloud is Transport Layer Security (TLS), or Datagram Transport Layer Security (DTLS[2]). This is especially true of IoT devices. Often the credentials needed to establish this TLS layer are stored in insecure locations in the IoT device. Credentials for access to mobile networks have, on the other hand, been securely stored in tamper-resistant hardware since the inception of GSM networks and SIM cards in the 1990s.

In this whitepaper, we review how a SIM, or any other Secure Element, can be leveraged as a root-of-trust to secure IoT device-to-cloud communications by implementing the world's most popular application layer security protocol. The approach avoids duplication of secure hardware functions, by loading an additional security service for storing and processing the sensitive credentials used to establish the TLS handshake on the worlds most deployed secure processor, the SIM or eSIM. It is vital for the trustworthiness of the Internet of Things (IoT) that we take a secure-by-design approach by properly protecting and processing the credentials used to secure data exchange between the IoT device and the cloud. Otherwise, enterprises will not be able to rely on the quality, accuracy or integrity of the data being collected, rendering it useless or even worse, dangerous.

This whitepaper describes IoT SAFE and its underlying technology and introduces the detailed technical specifications.

For more information about the IoT SAFE solution, including support material for organisations wishing to deploy it, please go to https://www.gsma.com/iot/IoT-SAFE/.

[1] GSMA intelligence: IoT security for enterprises: make it work, make it easy, December 2020

[2] TLS is used for TCP and DTLS is used when UDP is the underlying transport, IoT SAFE is suitable for both.

IoT End-to-End Security – a problem statement

Despite the importance of end-to-end security, there is a lack of commonly accepted standards for authentication and authorisation of IoT devices. Choosing from the many options and standards available may reduce interoperability, cause fragmentation, and prevent scalability of the security solution. Maintaining a fully functional IoT system over a long time will be a difficult task as well. The design of the IoT System architecture may quickly become a major challenge, with cost and time implications.

IoT SAFE is a technology that makes it easier to deploy and operate an IoT System that is secure, scalable, and manageable over time. How is this achieved?

Secure communication with TLS

Data exchange is at the basis of the IoT, with the *de-facto* standard for information transport being Transport Layer Security (TLS). TLS is an incredibly powerful and flexible secure protocol. The most common, often invisible, use of TLS is to allow secure and confidential connections between entities. TLS ensures both confidentiality and trust when performing sensitive operations such as online banking, or e-commerce. The identity of the server is validated by providing a digital certificate signed by a recognised Certificate Authority (CA). Browsers keep a long list of trusted CAs to validate server certificates. Finally, the user (or a security program), checks whether the certificate provided is consistent with the website owner. A “man-in-the-middle attack” occurs when the phishing website provides a “formally valid certificate”, which is not consistent with the displayed content.

Due to the limitations in IoT devices, not all TLS modes are applicable.

In addition to TLS used in the consumer space, IoT devices must be authenticated too.

IoT SAFE … performs all the security-critical operations during the TLS establishment phase.

TLS enables securing of TCP communications using the basic TLS protocol. However, for resource-constrained communications that use UDP, TLS also includes Datagram Transport Layer Security (DTLS), which is recommended. The use of UDP/DTLS is very common in the IoT space, especially for cellular LPWAN devices running on networks such as NB-IoT or LTE CAT-M.

(D)TLS in IoT applications

To ensure the end-to-end security, and to cope with limitations in IoT devices, specific (D)TLS modes should be used.

- IoT devices must be authenticated. This is necessary to ensure that only an authorised device can access the IoT service it’s connecting to. It prevents compromised IoT devices from entering the network.

- Servers running the IoT services must be authenticated also. It is not viable to hold a large set of CA certificates in the IoT device memory, as they tend to have constrained resources. An IoT application will connect to a specific cloud-hosted application with only one (or very few) server certificates to validate to overcome this issue.

- Hosting the Server Certificate in the device IoT application is neither secure nor effective. IoT spans a huge number of applications. Pre-loading Server certificates is not practical and complicates the device life-cycle management.

Fortunately, (D)TLS can be adapted to fulfil the IoT security needs. The IoT SAFE initiative is intended to leverage the flexibility of (D)TLS, providing a consistent mechanism to architect scalable security for manageable end-to-end IoT systems.

IoT SAFE Applet

IoT SAFE is embodied as an interoperable JavaCard Applet that resides inside the SIM of a mobile connected device[3] and it performs all the security critical operations during the TLS establishment phase, as explained later in this document.

The IoT SAFE applet holds valid and acceptable server and device access credentials that can be either a digital certificate or a pre-shared secret key. TLS has the option to use a pre-shared symmetric secret to validate a device identity, instead of a digital certificate.

The SIM is an ideal platform to perform the IoT SAFE tasks. It is a well standardised secure device, universally deployed. It is remotely manageable allowing the provisioning, and maintenance of the credentials and server certificate(s).

The major benefit for an IoT Device Application developer is that IoT SAFE is able to manage the complexity of setting up and on-going lifecycle of security credentials. The IoT Device Applications do not need to worry about any of the TLS security handshakes happening “under-the-hood”. Developers are then free to focus on their IoT applications, knowing that the lower layers of the device OS Middleware are taking care of the secure connection establishment.

To cope with different type of devices and security requirements, the IoT SAFE applet comes with two variants:

- IoT SAFE #1 uses digital certificates for authentication of server and devices

- IoT SAFE #2 uses pre-shared keys for authentication for more constrained devices.

[3] Or in alternative Tamper Resistant Elements in non-cellular connected devices.

IoT application security credentials

The IoT SAFE applets solve the problem of a secure and authenticated connection establishment. The loading of the credentials into an IoT SAFE enabled SIM is foreseen in two ways:

- If a business agreement is already in place before the devices are manufactured, the loading of the credentials into the SIM can happen at a secure personalisation plant.

- For all other cases, the credentials can be generated and provisioned ‘on-the-fly’ when the devices are put into operation.

Depending on the business logic, a device may host one or more IoT applications that in some cases may require an ‘application level’ validation with separate sets of credentials different from those used by TLS. IoT SAFE incorporates a *secure data vault* to store additional confidential information for the IoT application to use.

To provision those *application level* credentials, a device may use **Generic Bootstrap Authentication (GBA)**, a 3GPP standard. GBA exploits the firmly established challenge-response authentication to allow a user to gain access to the network. In an IoT context, the response from the SIM is used by the device to properly answer to the authentication requests.

Benefits of IoT SAFE

Benefit	Description	Cloud	IoT SP	MNO	eSIM	OEM
Improvement in security of solution offered or reduction in Device complexity	The majority of IoT Service Providers use basic device flash memory to store cloud credentials, which is not acceptable for security and integrity. Some OEMs add a dedicated secure element to store credentials which duplicates the secure element function in a cellular context. It is more cost effective, especially in a constrained device environment, to implement the IoT SAFE applet on the SIM and leverage its cryptographic, tamper resistant properties rather than doubling up.	✔	✔			✔
Provide secure, seamless cloud on-boarding with enterprise connectivity	Allow others to leverage the secure platform used to host network authentication credentials as a means of enabling seamless cloud provisioning and on-board key generation whilst boosting security			✔		✔
Extended certificate lifecycle management	Today public TLS certificate validity periods last up to a year, but regulations could soon impose that they be reduced to 3 months. With IoT SAFE, given the tamper-resistant storage of the private key, these constraints may be lengthened, and certificates be allowed to have longer validity periods.	✔	✔			✔
Zero-Touch Provisioning	Seamless unified remote SIM and cloud service provisioning while boosting security	✔	✔	✔		
Value-add to (e)SIM platform	IoT SAFE opens opportunities by allowing the SIM to be used for application-layer security, as well as its default purpose of mobile network authentication.				✔	✔

Benefit	Description	Cloud	IoT SP	MNO	eSIM	OEM
Portability, ease of deployment	Developed as a JavaCard application, IoT SAFE is portable between SIMs, eSIMs, integrated SIMs and other types of secure element.		✔		✔	✔
Inherent security	By employing IoT SAFE, IoT system architects, device designers, and application developers do not need to select a vendor specific security solution, or to implement ad-hoc mechanisms to secure device authentication and connection to an IoT cloud application. IoT SAFE will ensure the security measures will be executed as a background, invisible task.		✔			✔
Provisioning Flexibility	A subscription to an IoT Security Service provider will ensure that the security workflow will run smoothly for the deployment of a large number of devices. Depending on the business scenario, the security credentials can be pre-provisioned at manufacturing or later post-deployment.		✔			
Standards based, light integration efforts	IoT SAFE is designed around existing, commonly used TLS or DTLS security. It does not require specific network functions to be deployed or many-to-many integration scenarios between clouds, IoT service providers and/or mobile network operators.	✔	✔	✔	✔	✔

Benefit	Description	Cloud	IoT SP	MNO	eSIM	OEM
Connectivity agnostic	IoT SAFE is not limited to cellular-connected devices but can also be implemented on any devices supporting a JavaCard secure element and connected to the internet via Wi-Fi, Bluetooth, or any IP connection. The OEM or IoT Service Provider can leverage a common interface for the establishment of a (D)TLS connection in a fragmented environment where cellular and non-cellular devices coexist. This is extremely useful where network operators manage both mobile and fixed networks, to have a consistent approach to device security.		✔	✔		
Protocol agnostic	Multiple different IoT protocols can leverage the secure transport layer provided by IoT SAFE. Common protocols such as MQTT, CoAP, or even a simple HTTP session are supported.	✔	✔			✔
Persistence of IoT SAFE credentials	The IoT SAFE credentials remain present, even following events such as a Network Operator swap where an RSP-capable eSIM is employed.	✔	✔	✔		
Application layer security	IoT SAFE implements security-by-design practices by creating a native trust anchor, required by apps for secure OTA updates and continuous lifecycle management.	✔	✔	✔		✔
Unlocking the potential of IoT and bringing it to scale	IoT SAFE is fully specified, allowing all stakeholders to rely on the same root of trust in the device. TLS stack providers can all leverage the IoT SAFE applet credentials and cryptographic services the same way. IoT SAFE solves the problem of market fragmentation where a plethora of different operating systems and TLS stacks are used by different stakeholders in the IoT ecosystem.	✔	✔	✔	✔	✔

End-to-end security ecosystem and roles

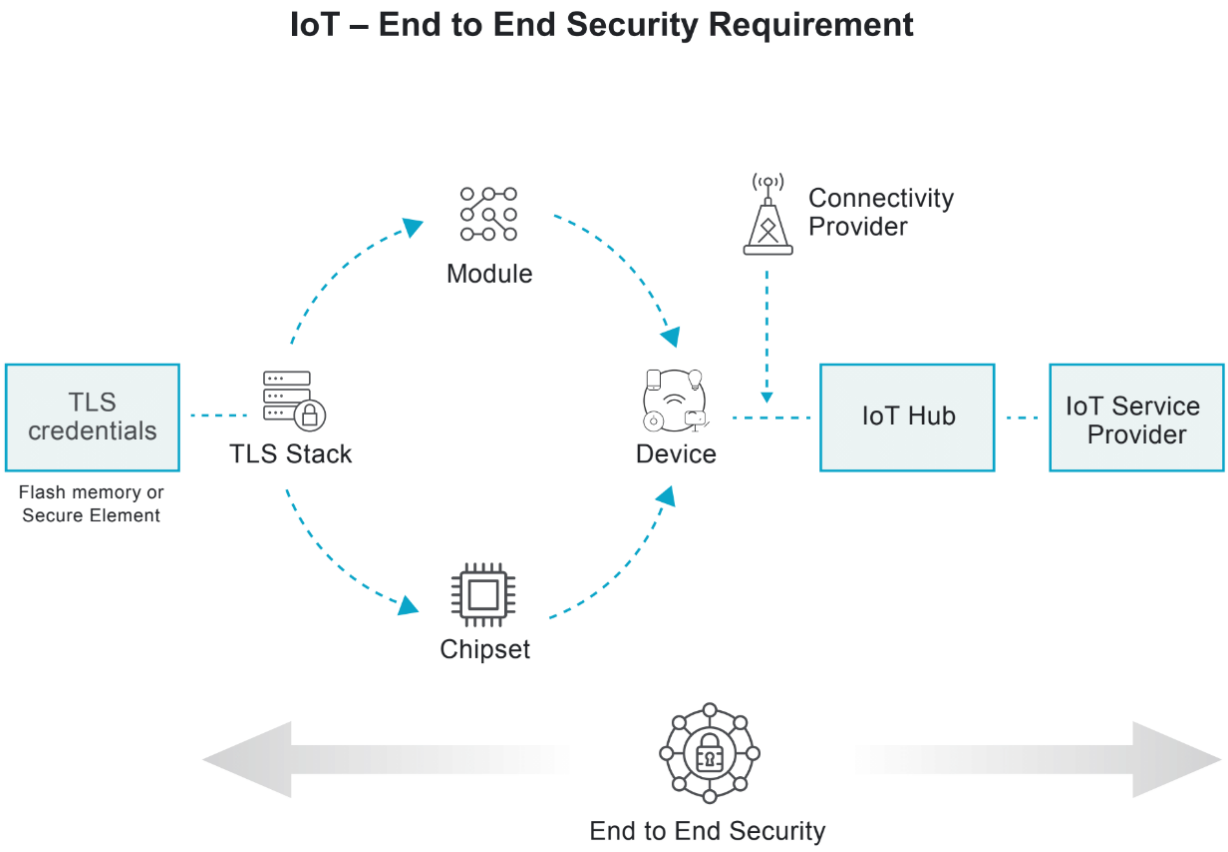


Figure 1 IoT End-to-End Security and TLS credential storage

TLS stack. End-to-end security is provided through Transport Layer Security (TLS) between a dedicated SW stack in the device, the TLS stack, and a remote cloud-based service. The TLS stack in the device establishes a set of session keys as part of a handshake procedure and then confidentiality protects data on the fly for transmission across the user/data plane of the network. The TLS stack can either run on the Microcontroller Unit (MCU) of a device or directly within the connectivity module. The TLS stack can support both TLS and DTLS protocols.

IoT Service Provider: brings together one or more devices, needing to communicate data securely to a given cloud, over a given network. The IoT Service Provider is the entity that benefits most from IoT SAFE as their device is being authenticated and their data is being protected from device-to-cloud in an end-to-end fashion without it being decrypted/re-encrypted anywhere along the chain.

IoT Hub: a cloud offering for IoT devices which hosts IoT Service Providers' innovative applications and provides data storage, application logic and advanced data analytics services.

The IoT Hub provides common endpoint side TLS functions that are leveraged by the IoT Service Provider and therefore must render the provisioning of credentials compatible with IoT SAFE, on behalf of the IoT Service Providers that they are hosting.

Connectivity Provider: A mobile network operator who provides connectivity services to the IoT Service Provider which carries data over a network between a device endpoint and an internet gateway to reach a hosted service in the cloud. The connectivity provider may choose to load the IoT SAFE application into their SIM/eSIM profile and offer it as a service to IoT Service Providers leveraging their connectivity.

Device OEM: builds devices hosting the application logic. Devices have a chipset with real-time operating system (RTOS) and a connectivity module allowing data to be exchanged with a remote cloud endpoint over a network.

Module manufacturer: Provides a connectivity module to the device OEM to integrate into their device. If the TLS layer securing the communications with the cloud endpoint is hosted within the module, then the module provider must ensure that the chosen TLS stack is IoT SAFE compatible.

SIM / eSIM Provider: Provides the (e)SIM to the module manufacturer to enable network authentication. The SIM / eSIM Provider must load the IoT SAFE application in the profile of the SIM (or as part of the eSIM profile to be downloaded remotely) to make it available for remote provision and use by the TLS stack.

How it Works

IoT Application Security Today

In current devices, end-to-end security is provided through Transport Layer Security (TLS) between a dedicated stack in the device, the TLS stack, and a remote cloud-based service. The TLS stack can either run on the processor of a device or directly within the connectivity module. A device may have more than one TLS stack residing on the device and it is up to either the OEM or the IoT application developer to select the one they wish to use.

-

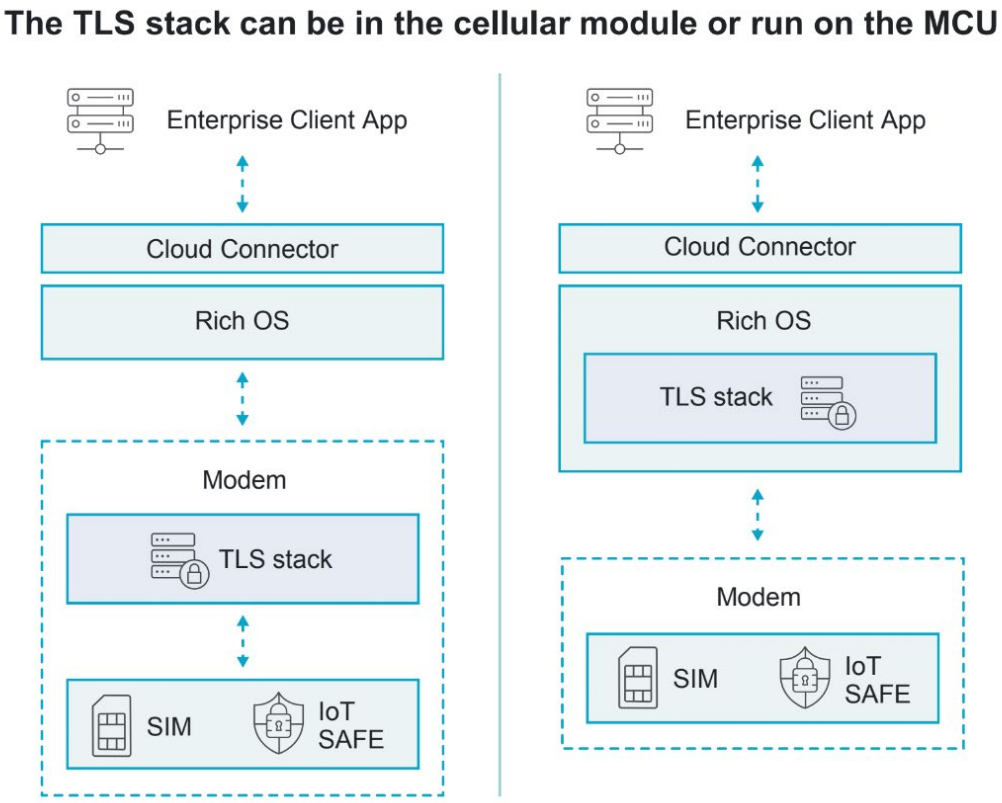


Figure 2 Comparison of TLS stack locations in IoT devices

Where credentials used to establish the TLS handshake are stored or processed in the device's memory, they are open to compromise. This could lead to a wide variety of cyber-attacks.

How does IoT SAFE help improve IoT security?

IoT SAFE brings a unified solution to secure credential storage and provides a set of standard interfaces to manage the TLS handshake, leading to the generation of session keys.

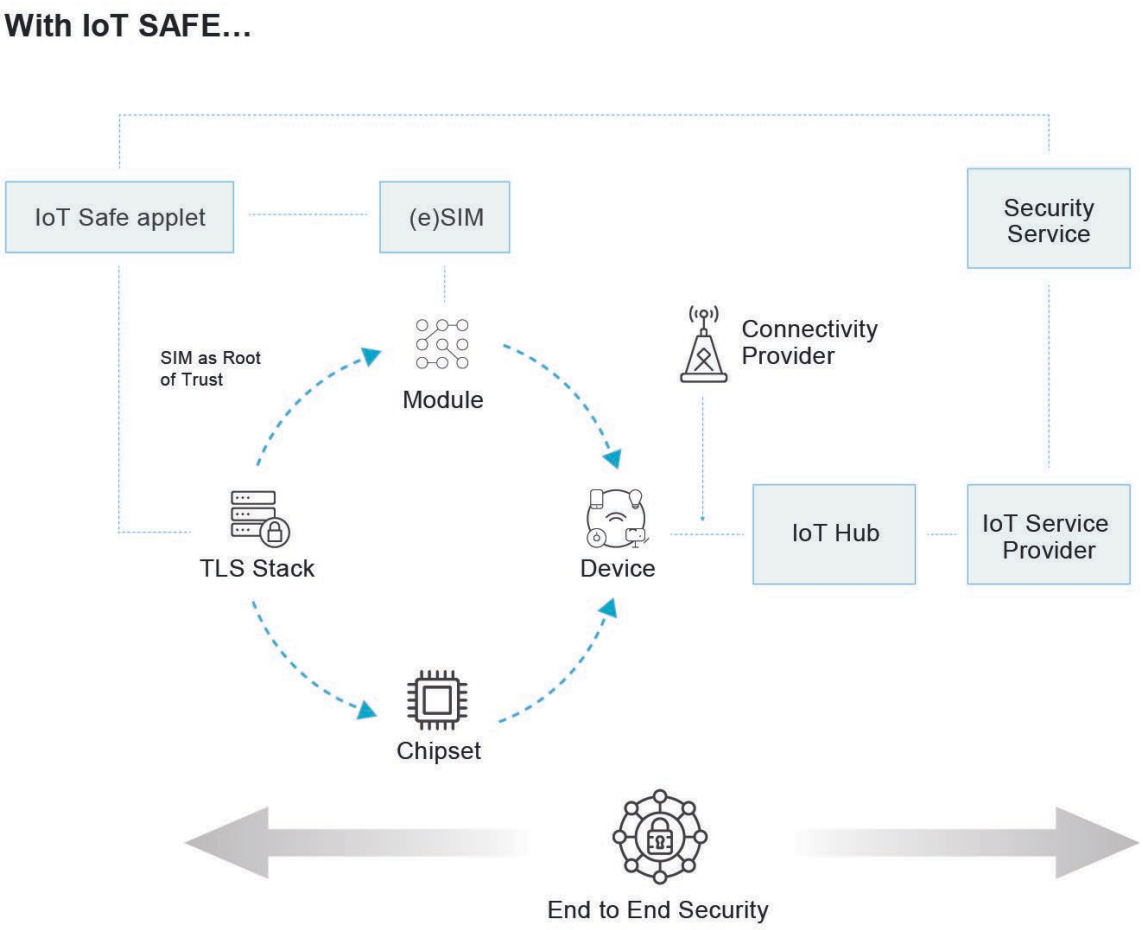


Figure 3 End-to-End Security using IoT SAFE to protect TLS credentials

As IoT SAFE is placed within the SIM card or another Secure Element, its physical and logical access is already well defined.

The IoT SAFE application can be leveraged whether the TLS stack is running directly within a thin-modem client (in the left hand image in Figure 3) or directly within the host processor (in the right hand image in Figure 3). If the TLS layer securing the communications with the cloud endpoint is hosted directly on the chipset, then the device OEM must ensure that the chosen TLS stack is IoT SAFE compatible. If the TLS layer securing the communications with the cloud endpoint is hosted within the module, then the device OEM has no changes to make on their side as they are being managed by the module manufacturer (see How to access the IoT SAFE applet from the device?). The extension made to the TLS stack to support IoT SAFE should be transparent to the end-developer of applications.

Overview of the Solution

Main System Elements

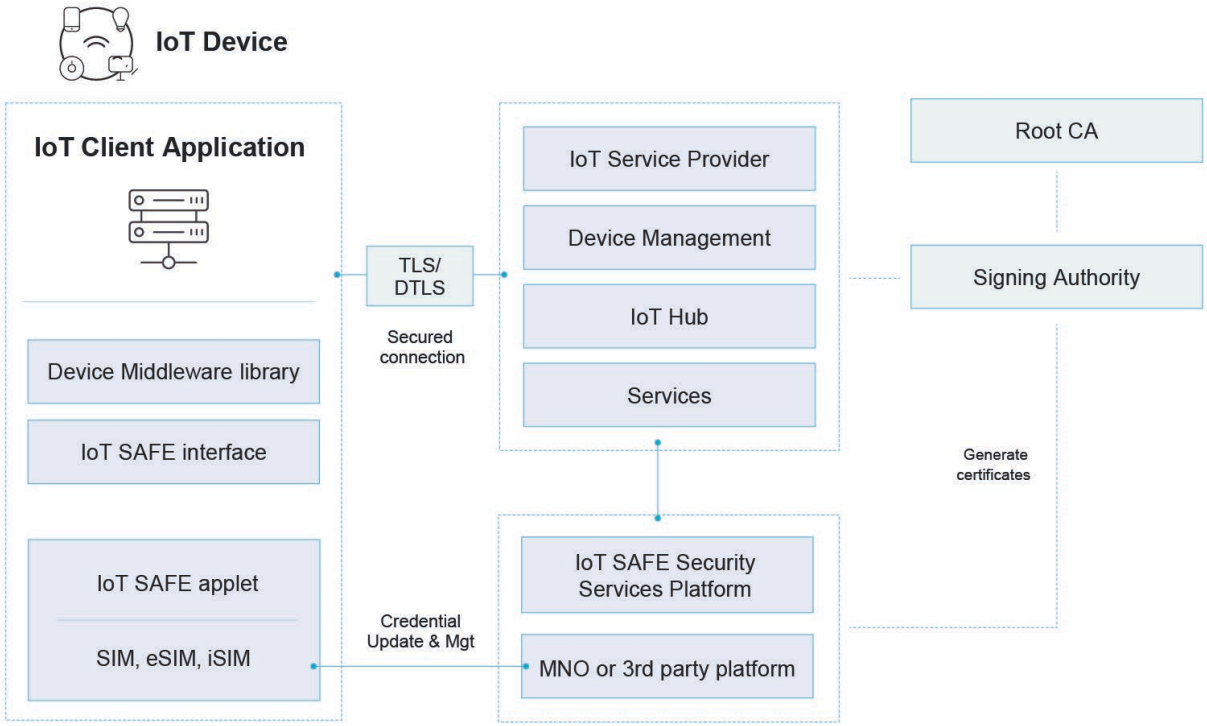


Figure 4 IoT SAFE Architecture

IoT Device

IoT Client Application

The goal of the IoT Client Application running on the OS is to retrieve data, manage the device or provide other functionalities. The IoT client application is typically re-using the security provided by the device (D)TLS stack and does not need to directly interact with IoT SAFE.

Device Middleware library (Modified (D)TLS stack middleware)

The Device Middleware library is a software security stack to provide secure data connectivity between the device and a remote server. It incorporates a standard D(TLS) stack, with a low layer IoT SAFE interface (according to [IoT .04]) providing a means to securely store Pre-Shared Keys (PSKs) and certificates used during the standard handshake operations with external entities.

The Device Middleware library can be implemented in different sub-elements of the device depending on the device's architecture and design.

SIM, eSIM, iSIM

A Standard SIM (Subscriber Identity Module) is available in different form factors (plug, soldered, embedded or integrated) depending on the device requirements. The SIM OS can host JavaCard applications that provide enhancements (for example MNO roaming capabilities or SIM card binding to a given device IMEI).

IoT SAFE applet type I or II

There are two types of IoT SAFE applet that a solution provider can choose from, depending on their preferred security scheme and device capabilities.

Type I applet uses asymmetric keys (also known as private and public key pairs) to manage digital certificates and uses them to setup the secure (D)TLS connection. Optionally, it can also handle pre-shared keys (PSK).

Type II applet uses symmetric (also known as pre-shared) keys to setup the secure (D)TLS connection.

Server Side

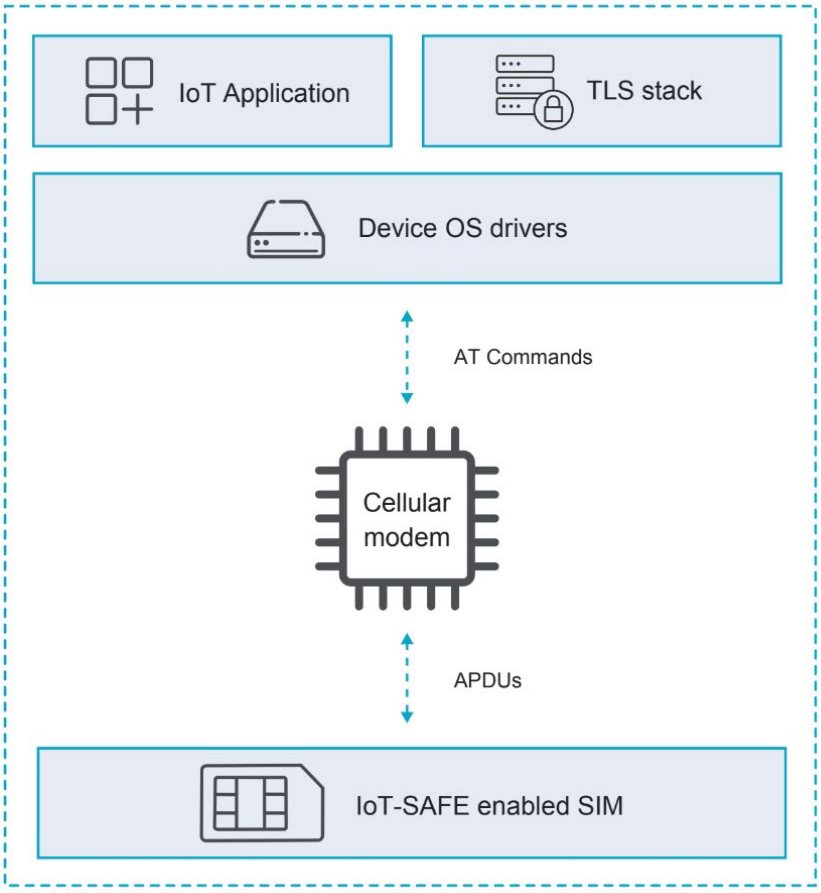
IoT Hub

The IoT Server Middleware is linked with the application server and the IoT SAFE security services platform for provisioning purposes. The IoT Hub establishes the TLS connection with the device.

IoT SAFE Security Services Platform.

The IoT SAFE Security Services Platform is connected with the IoT SAFE applet and the IoT Server Middleware (either directly or indirectly, through Device Management platforms for example). The platform enables provisioning of initial credentials at both the applet and Server Middleware at device switch-on (if they weren’t pre-provisioned), as well as the life cycle management of those credentials.

How to access the IoT SAFE applet from the device?



The most common way to access the IoT SAFE from the device is through the standard modem/module AT commands (described in [3GPP_AT]) that provides a mean to forward messages to the SIM. Encapsulated within the AT+CSIM command, the IoT SAFE messages are exchanged directly between the SIM and the device application using an ISO7816 interface located in modem/module.

At a higher level, the device middleware in charge of the TLS stack can now call upon the IoT SAFE application to manage the (D)TLS handshake. The interfaces are described in the document [IoT.05] and outlines all possible operations that are done by IoT SAFE during the (D)TLS session initialisation ensuring security of the critical phases.

IoT SAFE application provisioning

The [IoT.04] provides guidelines and examples of the IoT SAFE application credentials provisioning. It is possible to determine following options.

There are two aspects to be considered:

1) Loading of IoT SAFE applet in the SIM/Secure Element

The IoT SAFE applet can be securely loaded during the SIM card personalisation within GSMA SAS-UP certified premises by the SIM supplier with following two options:

- Factory provisioning and activation. The IoT SAFE application is loaded and provisioned with final credentials. In this option it is considered that the IoT SAFE service is active and operational. The prerequisite is that entities generating the secure credentials as well as the IoT Hub are known during the SIM personalisation phase.
  NOTE: In theory the IoT SAFE application could be run as a standalone application. However, in most cases it should be considered that the SIM supplier shall share the output file containing IoT SAFE necessary information with the IoT SAFE Security Services Platform.

- Factory provisioning. During the SIM card personalisation process in the SIM supplier premises the IoT SAFE application is loaded and provisioned with “bootstrap” credentials. Although the IoT SAFE application is active, to be operational the application credentials will have to be loaded remotely (see 2).

For an eSIM, the IoT SAFE application can be added as part of the eSIM profile to be downloaded remotely if it hasn’t been previously loaded as part of the factory provisioning process.

Note: A SIM card which is already in the field may be able to receive the IoT SAFE application via an Over-The-Air (OTA) download mechanism, subject to it meeting the respective requirements and being able to interact with the OTA enablers available.

2) In-Service IoT SAFE credentials provisioning and lifecycle management.

When the IoT SAFE application is already installed in the SIM card and the device is in the field, the credentials can be provisioned using an IoT SAFE Security Services Platform. The card/profile owner or IoT Service Provider can use this platform to provision the IoT SAFE application credentials.

Implementing IoT SAFE

The IoT SAFE ecosystem is made of components that must be properly orchestrated to achieve the desired function and security level. The key items being:

- IoT SAFE applet
- TLS credentials loaded at point of manufacture and/or using OTA services
- TLS stack / hardware drivers compatible with IoT SAFE
- Means of provisioning/managing the lifecycle of credentials remotely
- IoT SAFE ready hardware

Even more SAFE?

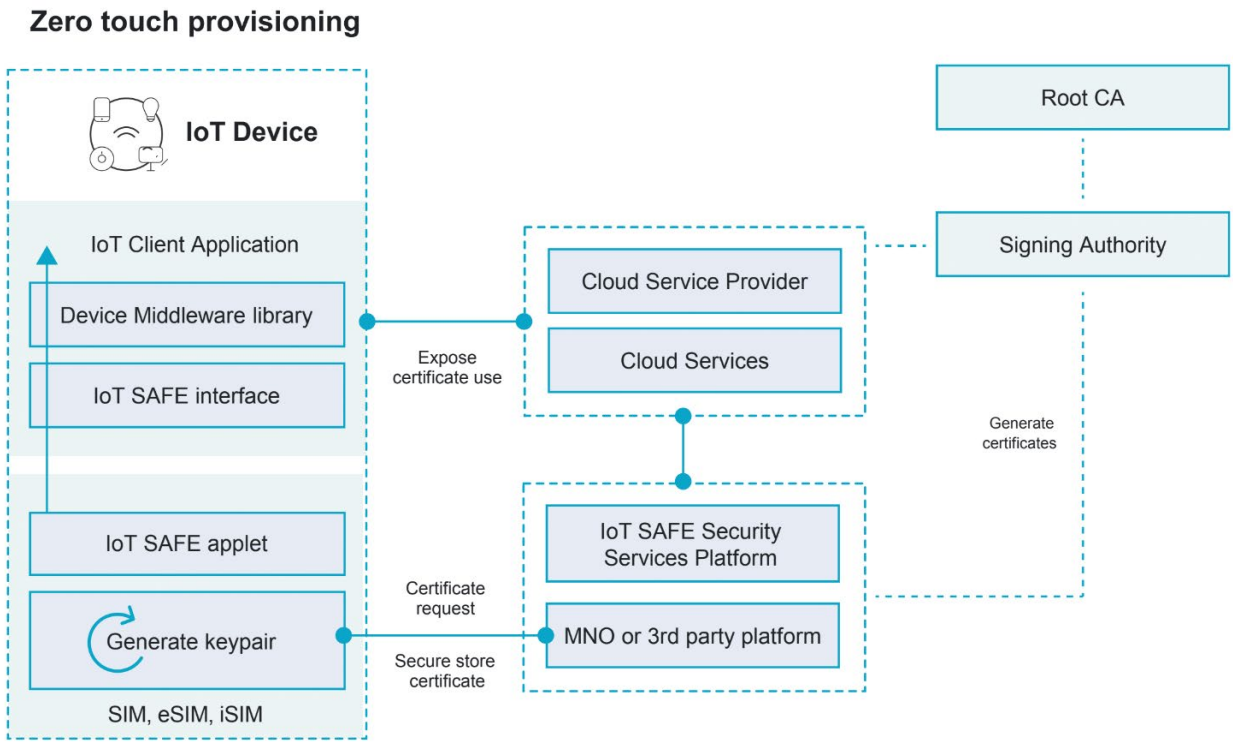
Extending data secrecy and end to end data protection

The IoT SAFE applet carries out mutual authentication of the device and a remote (cloud) server and establishes the session keys used for the data exchange. The bulk data exchange is left to the IoT device. If the expected quantity of data being exchanged is limited, the SIM cryptographic functions can be leveraged to also encrypt the data being exchanged on the user plane, for example a sensor transmitting a few bytes of data each day.

This scenario can further boost security to an even higher level than in typical usage where the application is only used for the TLS handshake, with the following benefits

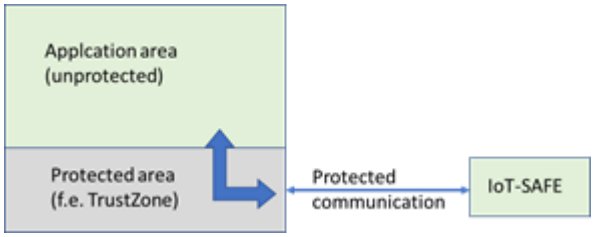
- Controlled access to IoT Service Provider data
- Secured data through the entire IoT communications network regardless of the transport security applied
- Can be integrated into various End-to-End protocol stacks

Zero-Touch Provisioning



Zero-Touch provisioning is allowing fast configuration of new devices and their enrolment to cloud services. IoT SAFE play an important role in automatic device on-boarding by using its ability to generate keys.

Secure Boot and Software Integrity Check



The secure boot process uses trusted hardware to verify the integrity of the application software, and the device proceeds to boot only if verification is successful.

The secure boot verification can leverage the IoT SAFE secure data store where valid certificates can store all the main software parameters including the memory span and trusted signature. The IoT device must be able to secure communications with IoT SAFE. Many mainstream IoT devices can do so as they incorporate technologies, such as ARM TrustZone, where a protected area controls the boot process and the communication channel with IoT SAFE.

The software integrity check is not limited to the boot process, it can also be done throughout the lifecycle of the device, providing an effective safety and integrity check.

Conclusion & Call to Action

IoT SAFE is taking the world's most popular end-to-end security protocol, Transport Layer Security and protecting the credentials used to put it in place, in the SAFEst place inside the device, the SIM, eSIM or secure element. This in turn enables the secure, seamless cloud-on boarding for enterprises leading to a full zero touch provision flow allowing cellular IoT connectivity to scale. IoT SAFE is connectivity agnostic meaning that it can work in the same way over the various categories of cellular network communications and any IP connected device featuring an (e)SIM or secure element.

A whole ecosystem of major actors in the IoT services space from chipset designers, module providers, (e)SIM providers, connectivity providers, software developers and IoT cloud service providers are already including support for IoT SAFE in their default offerings. The secure yet simple means of securing TLS combined with the potential for zero-touch provisioning that is brought by IoT SAFE will change the world of IoT device-to-cloud security forever.

Join us on the IoT SAFE journey by exploring the GSMA IoT SAFE website at https://www.gsma.com/iot/iot-safe/.

Annex – Frequently Asked Questions

Why is this initiative different to others?

The main goal of IoT SAFE was not to develop something specific to the telco environment and asking clouds to implement something defined by 3GPP or ETSI. Current cellular radio technologies ONLY encrypt traffic from the baseband in the modem to the eNodeB (LTE) or gNodeB (5G), which is usually close to the antenna in a local site or telco edge node. From them on, an enterprise depends on application layer security for their data to be confidentiality protected as far as their cloud or remote server. In rich devices, this is when you see the https:// in a URL and most browsers will indicate a secure connection with a lock where you can see that Transport Layer Security (TLS) is present, which was formerly known as Secure Socket Layer or SSL. IoT SAFE uses TLS so rather than building something new and cellular-specific, the group decided upon using existing security protocols.

Is IoT SAFE only relevant for cellular devices?

IoT SAFE is not limited to cellular-connected devices but can also be implemented on any devices supporting a JavaCard secure element and connected to the internet via Wi-Fi, Bluetooth, or any IP connection. The OEM or SP can leverage a common interface for the establishment of a (D)TLS connection in a fragmented environment where cellular and non-cellular devices coexist. Secure Element remote management procedures used to provision TLS credentials will differ from those of the SIM, but are fully standardised by GlobalPlatform.

Does IoT SAFE support TLS 1.3?

IoT SAFE is compatible with TLS v1.2 and v1.3.

Table of Definitions

Term	Description
Internet of Things	The Internet of Things describes the coordination of multiple machines, devices and appliances connected to the Internet through multiple networks. These devices include everyday objects such as tablets and consumer electronics, and other machines such as vehicles, monitors and sensors equipped with machine-to-machine (M2M) communications that allow them to send and receive data.
IoT Device	The combination of both the IoT Device Application and the Communications Module
IoT Device Application	The application software component of the IoT Device that controls the Communications Module and interacts with an IoT Service Platform via the Communications Module.
IoT SAFE Security Services Platform	The IoT SAFE Security Services Platform is connected with the IoT SAFE applet and the IoT Server Middleware. It enables provisioning of initial credentials at both the applet and Server Middleware at device switch-on (if they weren't pre-provisioned), as well as the life cycle management of those credentials.
IoT Service	The IoT service provided by the IoT Service Provider.
IoT Service Platform	The service platform, hosted by the IoT Service Provider which communicates to an IoT Device to provide an IoT Service. The IoT Service Platform can exchange data with the IoT Device Application over the Mobile Network and through the Communication Module, using (among others) IP-based protocols over a packet-switched data channel. Also, the IoT Service Platform typically offers Device Management capabilities, acting as a so-called Device Management Server. Finally, the IoT Service Platform typically offers APIs for IoT Server Applications to exchange data and interact with the IoT Device Applications over the IoT Service Platform.
IoT Service Provider	The provider of IoT services, often working in partnership with a Mobile Network Operator to provide an IoT Service to an End Customer. The provider could also be a Mobile Network Operator.
Secure Element	A Secure Element is a tamper-resistant platform capable of securely hosting applications and their confidential and cryptographic data (for example cryptographic keys) in accordance with the rules and security requirements set by well-identified trusted authorities.
SIM (and eSIM)	In the context of this whitepaper, we use the term SIM to refer to a UICC in a removable, embedded or integrated form, hosting a profile for mobile network authentication and optionally supporting GSMA eSIM architectures defined in SGP.01, SGP.21 or SGP.31.

Abbreviations

Term	Description
APDU	Application Protocol Data Unit
API	Application Programming Interface
CA	Certificate Authority
CoAP	Constrained Application Protocol
CSR	Certificate Signing Request
DTLS	Datagram Transport Layer Security
IoT	Internet of Things
IP	Internet Protocol
LPWAN	Low-Power Wide Area Network
NB-IoT	Narrow Band Internet of Things
OEM	Original Equipment Manufacturer
OTA	Over The Air
RSP	Remote SIM Provisioning
SP	Service Provider
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol

Table of References

Ref	Doc Number	Title
[IoT.04]	IoT.04	Common Implementation Guide to Using the SIM as a ‘Root of Trust’ to Secure IoT Applications
[IoT.05]	IoT.05	IoT Security Applet Interface Description
[3GPP_AT]	3GPP 27.007	AT command set for User Equipment (UE)

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
United Kingdom
www.gsma.com