

Design security



Protect your data at rest

Guard sensitive information on your device without the need of a specialized trusted chip

- Protect data via Authenticated Encryption with Associated Data (AEAD) and AES encryption and store information, even in a non-secure location
- Defend data at rest against bus sniffing and data injections by securing communication between modem and microcontroller
- Save space and simplify the design of your device

Design security services description

Space is precious. LPWA devices are not just constrained in memory space, but also in the number and size of components, which ultimately define design cost. When we talk about data protection, a crucial consideration is to guard the integrity of the data stored locally on the device, also known as the data at rest.

Design security offers a set of features that allow storage of sensitive information securely, even in a non-secure location such as the standard device memory. This offers a tremendous advantage as it avoids the use of dedicated hardware to store secrets, certificates and keys.

Further, chip-to-chip security protects the communication between the microcontroller and the u-blox module, safeguarding your device from external attacks such as bus sniffing and data injection.

In this way, design security simplifies the design of your device, protects your data at rest, and reduces cost.

Local data protection

Local data protection is a functionality made available through AT Commands that provides symmetric crypto functions to allow the device to locally encrypt/decrypt and authenticate critical data (e.g. certificates, tokens).

This method allows the secure local storage of sensitive information, even in a non-secure location (e.g. in "standard" device memory).

Local C2C security

Local C2C security is a method for a unique cryptographic pairing/binding between the microcontroller of the hosting device and the u-blox module by providing confidentiality, integrity, mutual authentication and anti-replay mechanisms for their communication channel.

Since a device microcontroller can only use the expected paired and authenticated u-blox module, and communications between the two components are authenticated and encrypted, the chip-to-chip communication is protected from bus sniffing and data injection.

IoT Security-as-a-Service features and services

Foundation security
Security root of trust
Secure boot
Secure production
Secure updates
Anti-cloning detection & rejection
Secure communication (D)TLS
Design security
Local data protection
Local C2C Security
End-to-end security
E2E symmetric KMS
E2E data protection
E2E data integrity
Certificate lifecycle control
Zero touch provisioning
IoT certificate manager

	LARA-R6 series	SARA-R410M-x3B	SARA-R422	SARA-R422S	SARA-R422M8S	SARA-R5 series	ALEX-R510M8S
TEE	TEE	TEE	TEE	TEE	TEE	SE	SE
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
□			□	□	□	•	•
□			□	□	□	•	•
□			□	□	□	•	•

C2C = chip-to-chip E2E = end-to-end KMS = key management system

TEE = trusted execution environment □ = Available in future FW version
SE = secure element

Legal Notice:

u-blox reserves all rights to this document and the information contained herein. Products, names, logos and designs described herein may in whole or in part be subject to intellectual property rights. Reproduction, use, modification or disclosure to third parties of this document or any part thereof without the express permission of u-blox is strictly prohibited.

The information contained herein is provided "as is". No warranty of any kind, either express or implied, is made in relation to the accuracy, reliability, fitness for a particular purpose or content of this document. This document may be revised by u-blox at any time. For most recent documents, please visit www.u-blox.com.
Copyright © 2022, u-blox AG

Further information

For contact information, see www.u-blox.com/contact-us.