Product summary

End-to-end security

Protect your data in transit

Ensure the true end-to-end privacy, integrity, and authenticity of your data in transit, powered by a proven scalable key management system

- Securely transfer data between device and cloud / end user without writing any security code or using additional hardware
- Leverage the u-blox symmetric key management system to generate infinite cryptographic keys for secure sessions
- Protect data with AEAD and AES encryption and reduce overhead by up to 8X on (D)TLS sessions
- Reduce power consumption and handshakes by entirely removing the need for certificates
- Keep the full control of cryptographic keys without the need for a PKI or PSK infrastructure

End-to-end security services description

Protecting your data in transit means that the confidentiality of your data is safeguarded all the way from the device to the cloud. Additionally, you need to be able to establish the integrity and authenticity of your data at all times. In IoT settings, which often involves thousands, if not millions, of devices, this requires highly efficient and scalable cryptographic methods.

The u-blox end-to-end security package provides smart methods to encrypt and transfer every type of application data from the device to your server/platform in the cloud with a few simple operations. This eliminates the need to implement a complex solution on the device microcontroller in order to establish secure communications to transfer sensitive data.

E2E symmetric KMS is a disruptive approach for secure key management that replaces the current public key infrastructure (PKI) or traditional pre-shared key (PSK) solutions.

The significant advantage of E2E symmetric KMS is in the session-unique keys that are generated out-of-the box both in the module and made available to your cloud application via a REST API, allowing the creation of an infinite number of keys per device. Keys are uniquely tied to the hardware and can be triggered on the module side and on the server/cloud side, entirely removing the need for creation, delivery, renewal, and revocation of certificates as well as the key storage. Development and operations are simplified by delegating the complexity of key management to a proven scalable system.

The full set of services are the best-in-class solution for LPWA constrained devices, because the optimized secure communications achieve up to 8 times reduction in data overhead and up to 2 times reduction in session handshakes. These optimizations translate to reductions in data usage, power consumption, and cost.

IoT Security-as-a-Service features and services	LARA-R6 series	SARA-R410M-x3B	SARA-R422	SARA-R422S	SARA-R422M8S	SARA-R5 series
Foundation security						
Security root of trust	TEE	TEE	TEE	TEE	TEE	SE
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	□			□	□	•

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

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

End-to-end security

End-to-end security features and services
E2E symmetric KMS
E2E data protection
E2E data integrity

E2E symmetric KMS	An end-to-end symmetric key management system is a highly scalable method to provision and manage a session-unique PSK in the module and in the cloud for application layer security. The PSK is generated and protected by the root of trust. E2E symmetric KMS uses a locally derived PSK for end-to-end communication security, such as DTLS, with the PSK available in the cloud via a REST API.
E2E data protection	Application data is encrypted in the module. The corresponding PSK for decryption is available in the cloud via a REST API. This method provides an efficient and scalable ability to encrypt data on a device and to decrypt data asynchronously in the cloud independent of protocols, servers, platforms, or time before reaching the final destination.
E2E data integrity	Application data is signed in the module and the corresponding PSK is available via a REST API in the cloud for signature verification. This method provides a robust way to sign data on a device and verify the signature asynchronously in the cloud independent of protocols, servers, platforms, or time before reaching the final destination.

Further information

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