Product summary

Foundation security

Trust and control of your device

A unique and immutable device identity and robust root of trust provide the foundation for a trusted set of advanced security functionality

- Production is performed using processes and methods designed with a focus on security
- Only trusted software issued by the authorized manufacturer can run on the device
- Authenticated firmware updates are delivered remotely via u-blox uFOTA client/server solution
- Clones are automatically identified and blocked

The foundation for your IoT security

The internet continually connects more physical objects, necessitating full trust and control your IoT devices.

To ensure that a module has a unique and immutable identity, it is tied with the root of trust. A root of trust is a source that can always be trusted in a cryptographic system, and from which a trusted set of advanced security functionalities can be based. The device identity is linked to a secure back-end in order to continuously monitor and detect compromised or cloned devices.

With the most secure provisioning process, we insert our root of trust in our fully controlled manufacturing environment.

Next, the secure boot sequence ensures that the module runs only authorized firmware, as well as any future authorized updates delivered over the air.

We then leverage our advanced set of secure libraries and hardware backed crypto functions, together with the root of trust, to derive an infinite number of trusted keys for each device to ensure the highest level of confidentiality to each single message to be delivered to the cloud.

Finally, the trusted keys are used to secure all functions, such as for data at rest locally or for sensitive data in transit to a cloud application platform.

These foundational principles ultimately protect the integrity, confidentiality and authenticity of your IoT solution.

Unique device identity	Immutable chip ID and robust root of trust provides the foundational security.
Secure boot sequence and updates	Only authenticated and authorized firmware and updates can run on the device.
Hardware-backed crypto functions	Secure Client Library generates keys & crypto functions to securely connect to the cloud.
Root of trust based authentication	SE or TEE protected, session unique keys ensure integrity and confidentiality of data at rest and communications.

IoT Security-as-a-Service features and services

	LARA-R6 series	SARA-R410M-x3B	SARA-R422	SARA-R422S	SARA-R422M8S	SARA-R5 series	ALEX-R510M8S
Foundation security							
Security root of trust	TEE	TEE	TEE	TEE	TEE	SE	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 □ = Available in future FW version
SE = secure element

Foundation security

Foundation security features and services

Foundation	Security root of trust Secure boot Secure production Secure updates Anti-cloning detection & rejection Secure communication (D)TLS

Detailed description

Security root of trust (RoT)	A security root of trust is a combination of a unique immutable identity together with the hardware and software cryptographic capabilities necessary to enable trusted functions. This provides the foundation for a trusted set of advanced security functionality.
Trusted execution environment (TEE)	A TEE is a trusted execution environment that has a trusted OS area, which is physically separated from the rich OS (rich execution environment) where apps are running. A TEE provides a very good level of robustness and is sufficient for many IoT applications. Combined with the security RoT, it gives a better level of robustness compared to competition.
Secure element (SE)	A secure element, or SE, is a dedicated hardware chip that stores sensitive data and runs secure applications. It acts as a vault, protecting what is inside the secure element (applications and data) from malware attacks that are typical in the host (i.e. the device operating system). A u-blox secure element is common criteria certified to EAL5+ level. This implementation is extremely robust and appropriate for mission critical IoT applications.
Secure boot	Secure boot is a security standard developed by the PC industry to make certain that a module will only boot or run trusted software issued by the original device manufacturer. The integrity of the code running on your module is ensured and the interfaces are protected from malicious attacks.
Secure production	Production is performed using processes and methods designed with a strong security focus and within our controlled manufacturing environment. The RoT is securely provisioned with personalization data (several keys). The personalization data is delivered utilizing multiple layers of encryption to protect it end-to-end. Each layer is only removed at the necessary step, with the final layer only removed within the module RoT itself. Best-in-class security protocols implemented in a controlled device production environment provides a reliable supply from which to protect your data and your business.
Secure updates (via FOTA or uFOTA)	FOTA allows a customer's chosen IoT platform to remotely and securely update module firmware (firmware is signed by u-blox, then authenticated in the module via secure boot). uFOTA is a complete end-to-end u-blox service that allows the customer to control the remote update of module firmware over-the-air, with additional security provided between module and server via PSK provisioning. Customers do not need to have servers to manage and deploy updates, since this is done by u-blox. Updates are always done with customer permission.
Anti-cloning detection and rejection	Anti-cloning detection and rejection allows immediate identification of devices that use the same RoT in order to allow just the first device to communicate with the server and to block all the others. The system automatically identifies and blocks clones.
Secure communications (D)TLS	DTLS and TLS are standards-based cryptographic protocols designed to provide communications security over a network. Having secure communications embedded in module firmware, ready and available for use by the end device, enables you to ensure authenticity, confidentiality and integrity for your data in transit.

Further information

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