LoRa Alliance Member™

AVNET® SILICA

LoRaWAN Security solutions

LoRaWAN Security solutions

WHAT IS A SECURE ELEMENT?

A secure element is a tiny chip able to perform cryptography primitives such as AES, SHA and ECC, and to keep secret keys safely hidden from the outside world. Unlike ordinary MCUs and memories, it is very robust against physical attacks and cannot be read or counterfeited.
Secure elements come programmed and personalized with unique IDs and secret keys, and are able to interface with its host MCU via an I^2C, a 1-Wire or an SPI bus.
Common examples of secure elements are SIM cards, banking smart cards, TPMs in computers, etc.

WHY IS THE TO136 SECURE ELEMENT SO SPECIAL?

The TO136 is Avnet Silica's exclusive secure element. It is manufactured on a hardware base supplied by OT-Morpho and is loaded with a firmware (defining its command set and features) developed by Trusted Objects and personalized with unique keys and IDs in a secure area at the heart of Avnet Logistics' European facility in Munich, Germany. The TO136 is the lowest-power secure element on the market: 2.8mA in active mode, 0µA in off mode and a start-up time under 500µs, orders of magnitude better than the competition, allowing it to be used in battery-powered applications without impacting energy consumption. Our production set-up is so flexible that it can be programmed to perform virtually any crypto function and personalized with the most complex key mapping. The TO136 HW is banking-grade EMVCo certified (Europay, Mastercard, Visa), which is equivalent to a Common Criteria CC EAL5+.

WHAT IS LoRaWAN 1.0.2 SECURITY?

There are two layers of security in LoRaWAN 1.0.2:

- A network security layer
- An application security layer

The network security layer is used to authenticate uplink and downlink messages on the network, to ensure that only network-registered devices can use it.

The application security layer ensures end-to-end confidentiality, from sensor to application server, so that network servers cannot read the data they convey.
Both network and application security layers use symmetric cryptography to respectively sign and encrypt messages with 128-bit symmetric keys:

- NtwSKey for network authentication
- AppSKey for end-to-end encryption

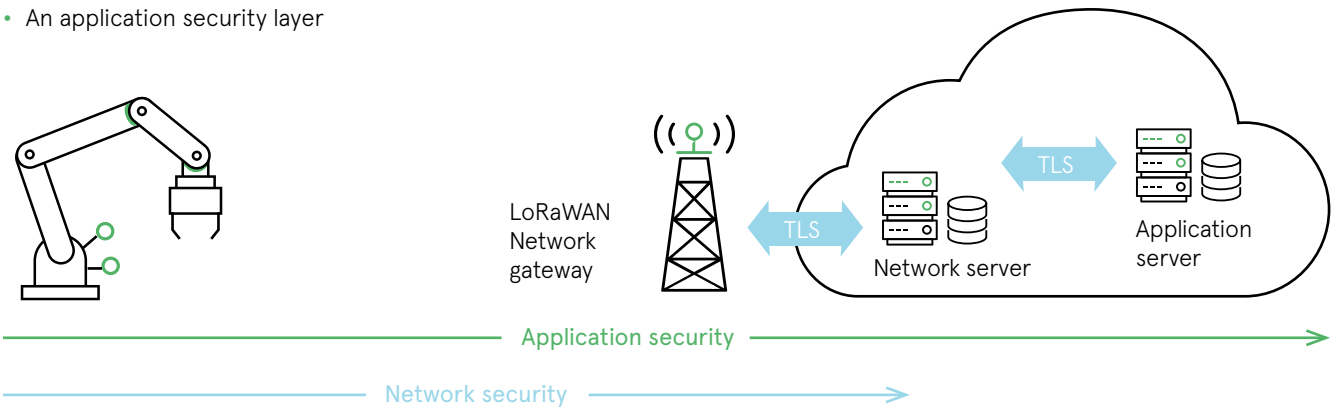
Both the NtwSKey and AppSKey are uniquely defined per sensor and need to be shared with the network server and the application server respectively. However, distributing the keys without exposing them is complex.

WHAT ARE THE PROVISIONING OPTIONS?

The LoRaWAN 1.0.2 specification defines two provisioning schemes for onboarding a LoRaWAN sensor:

- ABP: activation by personalization
- OTAA: over-the-air activation

ABP is the simplest but most restrictive option. Both the NtwSKey and the AppSKey are issued and shared with one network operator for one application server provider at end-device manufacturing. This option best applies to network- and application-specific devices, but does not fit objects that need to be able to roam or operate on different networks.



Using OTAA in conjunction with a third-party join server (JS) solves this problem. Via a join procedure with the JS sitting above the network operators, a device can attach to any network with a connection to the JS and any application server provider connecting to the JS. In this case, NtwSKey and AppSKey are derived by both the JS and the end-device simultaneously, from a pre-shared symmetric root key.However, in both cases, ABP and OTAA, symmetric keys need to be shared between the device manufacturer and outside third parties. If manufacturing is outsourced, it adds even more complexity to the key ceremonies and processes.

MANUFACTURING A NETWORK-SPECIFIC DEVICE

WITHOUT A SECURE ELEMENT	WITH THE TO136-LoRaWAN-ABP
The network operator, on which the device will operate, needs to issue a list of device addresses (DevAddr) to the OEM. The OEM then generates NtwSKey and AppSKey and builds two lists: - List 1: DevAddr + NtwSKey - List 2: DevAddr + AppSKey The OEM securely sends List 1 to the network operator, and List 2 to the application server provider for pre-provisioning of the devices. Then, the OEM aggregates both lists and sends the resulting file to the EMS manufacturing the physical devices, asking it to personalize the production as per the file. Once programmed, the OEM asks the EMS to destroy the keys.	The OEM orders TO136-LoRaWAN-ABP from Avnet Silica, referring the network operator and the application server provider. The network operator issues a list of DevAddr to Avnet Silica. Avnet Silica issues NwkSKey and AppSKey lists and personalizes secure elements accordingly. Avnet Silica securely shares information to compute the NwkSkey list and AppSKey list with the network operator and the application server provider respectively. Avnet Silica ships the batch of secure element to the EMS and destroys the key files.

MANUFACTURING A GENERIC DEVICE

WITHOUT A SECURE ELEMENT	WITH THE TO136-LoRaWAN-OTAA
The OEM needs to issue a list of device unique identifiers (DevEUI) to Avnet Silica, and also shares it with the join server behind the AppEUI. The OEM then generates unique device root keys AppKey and builds a list: DevEUI + AppKey The OEM securely sends the list to the join server provider for pre-provisioning of the devices. The OEM securely sends the list to the EMS manufacturing the physical devices, asking to personalize the production according to the list of keys. Once programmed, the OEM asks the EMS to destroy the list of keys.	The OEM orders TO136-LoRaWAN-OTAA from Avnet Silica and refers the join server provider to Avnet Silica. A list of device unique identifiers (DevEUI) can be generated by the OEM or the join server provider at will. This list of DevEUI is shared with Avnet Silica via a secure procedure. For each DevEUI, Avnet Silica issues a root key AppKey and personalizes secure elements accordingly. Avnet Silica securely shares the production information (DevEUI + AppKey) with the join server provider. Avnet Silica ships the batch of secure element to the EMS and destroys the key files.

HOW CAN I ORDER?

Two secure elements are available depending on the personalization scheme retained:

- TO136-LoRaWAN-ABP
- TO136-LoRaWAN-OTAA

Upon ordering, the customer will be asked to provide information regarding the workflow, as described above, so that Avnet Silica can smoothly manage the key ceremonies with the different parties involved.

Please contact your nearest Avnet Silica representative or email us at security-solutions@avnet.eu

Security partners

IDEMIA augmented identity

TRUSTED OBJECTS

Offices

AUSTRIA
Vienna
Phone: +43 186 642 300
Fax: +43 186 642 350
wien@avnet.eu

BELGIUM
Merelbeke
Phone: +32 9 210 24 70
Fax: +32 9 210 24 87
gent@avnet.eu

CZECH REPUBLIC (SLOVAKIA)
Prague
Phone: +420 234 091 031
Fax: +420 234 091 030
praha@avnet.eu

DENMARK
Herlev
Phone: +45 432 280 10
Fax: +45 432 280 11
herlev@avnet.eu

ESTONIA
(LATVIA, LITHUANIA)
Pärnu
Phone : +372 56 637737
paernu@avnet.eu

FINLAND
Espoo
Phone: +358 207 499 200
Fax: +358 207 499 280
helsinki@avnet.eu

FRANCE (TUNISIA)
Cesson Sévigné
Phone: +33 299 838 485
Fax: +33 299 838 083
rennes@avnet.eu

Illkirch
Phone: +33 390 402 020
Fax: +33 164 479 099
strasbourg@avnet.eu

Massy Cedex
Phone: +33 164 472 929
Fax: +33 164 470 084
paris@avnet.eu

Toulouse
Phone: +33 05 62 47 47
toulouse@avnet.eu

Vénissieux Cedex
Phone: +33 478 771 360
Fax: +33 478 771 399
lyon@avnet.eu

Germany
Berlin
Phone: +49 30 214 882 0
Fax: +49 30 214 882 33
berlin@avnet.eu

Freiburg
Phone: +49 761 881 941 0
Fax: +49 761 881 944 0
freiburg@avnet.eu

Hamburg
Phone: +49 40 608 235 922
Fax: +49 40 608 235 920
hamburg@avnet.eu

Holzwickede
Phone: +49 2301 919 0
Fax: +49 2301 919 222
holzwickede@avnet.eu

Lehrte
Phone: +49 5132 5099 0
braunschweig@avnet.eu

Leinfelden-Echterdingen
Phone: +49 711 782 600 1
Fax: +49 711 782 602 00
stuttgart@avnet.eu

Leipzig
Phone: +49 34204 7056 00
Fax: +49 34204 7056 11
leipzig@avnet.eu

Nürnberg
Phone: +49 911 24425 80
Fax: +49 911 24425 85
nuernberg@avnet.eu

Poing
Phone: +49 8121 777 02
Fax: +49 8121 777 531
muenchen@avnet.eu

Wiesbaden
Phone: +49 612 258 710
Fax: +49 612 258 713 33
wiesbaden@avnet.eu

HUNGARY
Budapest
Phone: +36 1 43 67215
Fax: +36 1 43 67213
budapest@avnet.eu

ITALY
Cusano Milanino
Phone: +39 02 660 921
Fax: +39 02 660 923 33
milano@avnet.eu

Firenze
Phone: +39 055 436 039 2
Fax: +39 055 431 035
firenze@avnet.eu

Modena
Phone: +39 059 348 933
Fax: +39 059 344 993
modena@avnet.eu

Padova
Phone: +39 049 807 368 9
Fax: +39 049 773 464
padova@avnet.eu

Rivoli
Phone: +39 011 204 437
Fax: +39 011 242 869 9
torino@avnet.eu

Roma Tecnocittà
Phone: +39 06 413 115 1
Fax: +39 06 413 116 1
roma@avnet.eu

NETHERLANDS
Breda
Phone: +31 765 722 700
Fax: +31 765 722 707
breda@avnet.eu

NORWAY
Asker
Phone: +47 667 736 00
Fax: +47 667 736 77
asker@avnet.eu

POLAND
Gdansk
Phone: +48 58 307 81 51
Fax: +48 58 307 81 50
gdansk@avnet.eu

Katowice
Phone: +48 32 259 50 10
Fax: +48 32 259 50 11
katowice@avnet.eu

Warszawa
Phone: +48 222 565 760
Fax: +48 222 565 766
warszawa@avnet.eu

PORTUGAL
Vila Nova de Gaia
Phone: +35 1 223 779 502
Fax: +35 1 223 779 503
porto@avnet.eu

ROMANIA (BULGARIA)
Bucharest
Phone: +40 21 528 16 32
Fax: +40 21 529 68 30
bucuresti@avnet.eu

RUSSIA (BELARUS, UKRAINE)
Moscow
Phone: +7 495 737 36 70
Fax: +7 495 737 36 71
moscow@avnet.eu

Saint Petersburg
Phone: +7 812 635 81 11
Fax: +7 812 635 81 12
stpetersburg@avnet.eu

SLOVENIA
(BOSNIA AND HERZEGOVINA, CROATIA, MACEDONIA, MONTENEGRO, SERBIA)
Ljubljana
Phone: +386 156 097 50
Fax: +386 156 098 78
ljubljana@avnet.eu

SPAIN
Barcelona
Phone: +34 933 278 530
Fax: +34 934 250 544
barcelona@avnet.eu

Galdàcano. Vizcaya
Phone: +34 944 572 777
Fax: +34 944 568 855
bilbao@avnet.eu

Las Matas
Phone: +34 913 727 100
Fax: +34 916 369 788
madrid@avnet.eu

SWEDEN
Sundbyberg
Phone: +46 8 587 461 00
Fax: +46 8 587 461 01
stockholm@avnet.eu

SWITZERLAND
Rothrist
Phone: +41 62 919 555 5
Fax: +41 62 919 550 0
rothrist@avnet.eu

TURKEY (GREECE, EGYPT)
Kadikoy Istanbul
Phone: +90 216 528 834 0
Fax: +90 216 528 834 4
istanbul@avnet.eu

UNITED KINGDOM (IRELAND)
Berkshire
Phone: +44 1628 512 900
Fax: +44 1628 512 999
maidenhead@avnet.eu

Bolton
Phone: +44 1204 547 170
Fax: +44 1204 547 171
bolton@avnet.eu

Bucks, Aylesbury
Phone: +44 1296 678 920
Fax: +44 1296 678 939
aylesbury@avnet.eu

Stevenage, Herts, Meadway
Phone: +44 1438 788 310
Fax: +44 1438 788 250
stevenage@avnet.eu

ISRAEL
Tel-Mond
Phone: +972 (0)9 7780280
Fax: +972 (0)3 760 1115
avnet.israel@avnet.com

SOUTH AFRICA
Cape Town
Phone: +27 (0)21 689 4141
Fax: +27 (0)21 686 4709
sales@avnet.co.za

Durban
Phone: +27 (0)31 266 8104
Fax: +27 (0)31 266 1891
sales@avnet.co.za

Johannesburg
Phone: +27 (0)11 319 8600
Fax: +27 (0)11 319 8650
sales@avnet.co.za