AVNET-TO136 data brief

Secure Element solutions designed for connected devices and peripherals

Hardware Platform

- 32-bit secure CPU core
- 136K bytes Flash
- Operating voltage: 1.62V - 5.5V
- Internal Oscillator
- Secure AES accelerator
- CRC-16, 16-bit counter
- True Random Generation
- Low power consumption (maximum 2.4mA)
- Fast boot mode (<1ms) enabling 0µA power consumption
- Operating temp : -25°C to 85°C
- Certified Hardware (EMVCo/Banking)

Cryptographic algorithms

- 64-bit unique identifier
- SHA256 hash
- HMAC-SHA256 with 128-bit key
- AES128 encryption/decryption using ECB, CBC, CTR, CCM, GCM modes
- AES-CMAC with 128-bit key
- Elliptic Curve P-256 (NIST)
- ECDSA : PKI authentication
- ECIES / Secure Messaging with P-256 (NIST), AES128 CBC, and HMAC
- On-board Key Generation (OBKG)
- Diffie-Hellman session key generation
- X.509 certificates / Short certificates

Supported Features

- Fast Mode I2C standard interface
- Certificate-based mutual authentication
- LoRaWAN 1.0 stack
- Full (D)TLS 1.2 stack (incl. session resume)
- Configurable command set
- Low MOQ for personalized products

Packaging

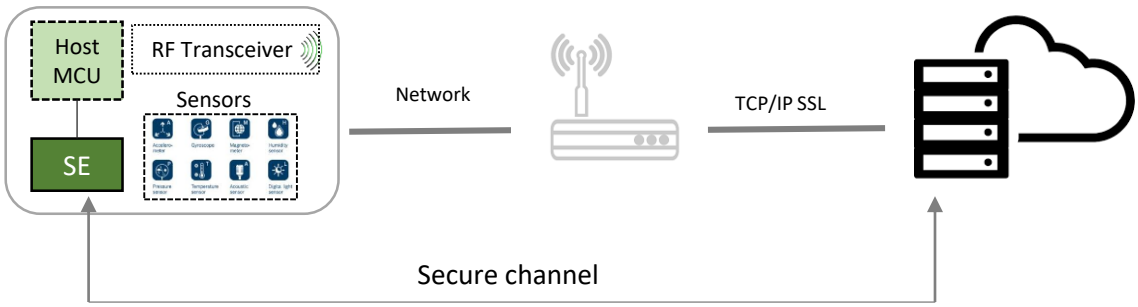
- Small footprint package
- DFN6 – 3 mm x 3 mm

TRUSTED OBJECTS
Secure firmware inside
www.trusted-objects.com

Summary Datasheet
Revision 1.0.5 30-jan-19

AVNET Reach Further™
www.avnet.com

End to end security in IoT networks



Credentials storage and IoT devices authentication

- Unique and strong identity assigned to each IoT device
- Keys securely stored and protected against logical and physical attacks
- Authentication scheme based on digital signature generation and verification
- ECDSA signature scheme associated with X.509 certificate
- Symmetric signature scheme with HMAC SHA256 and AES-CMAC
- Automatic renewal of pairing keys during the product lifecycle
- Compatible with LoRaWAN, Sigfox and TLS 1.2 authentication scheme

Network data integrity

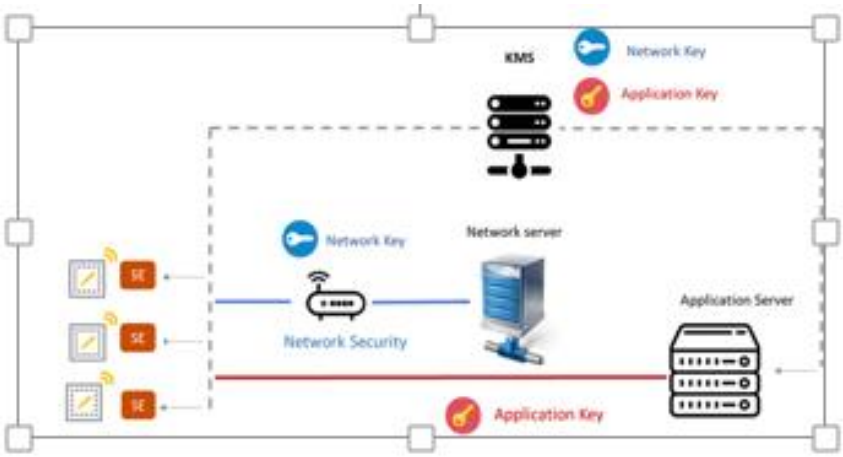
- Protection against unattended alteration or modification of the payload transmitted by the edge device into the network
- Only data sent by authorized servers are received by the IoT device
- Unique integrity code generated for each message using ECC cryptographic scheme (ECDSA with SHA256) or AES-CMAC and HMAC SHA256

Network data confidentiality

- Data protection against any authorized access
- Data encryption and/or decryption between the IoT device and the network gateway (AES 128 CBC/CTR/CCM/GCM modes)
- Data encryption and/or decryption between the IoT device and the application server (AES 128 CBC/CTR/CCM/GCM modes)
- Key session establishment with Diffie-Hellman schemes (ECDHE)

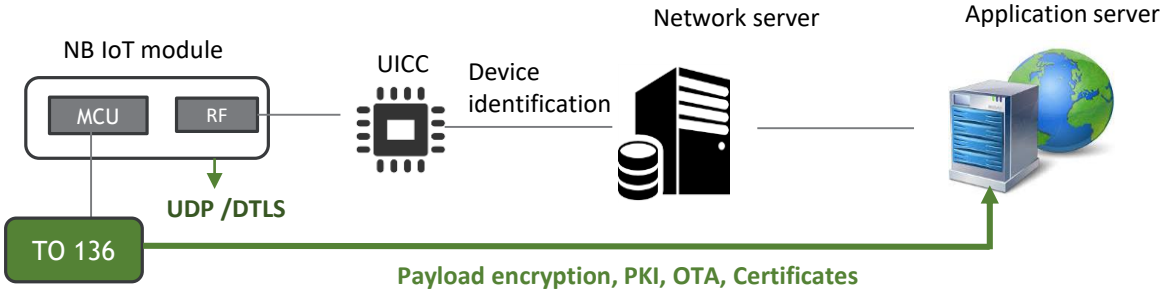
LoRaWAN and Sigfox secured connectivity

- Strong authentication between end-devices, gateways and cloud servers
- Payload encryption & decryption
- Secure storage of Network Keys and Applications Keys and Credentials
- Internal counter management implementation
  (up to 50M messages, freeing the MCU from wear-levelling management)
- Easy implementation with replacement of the host MCU security stack



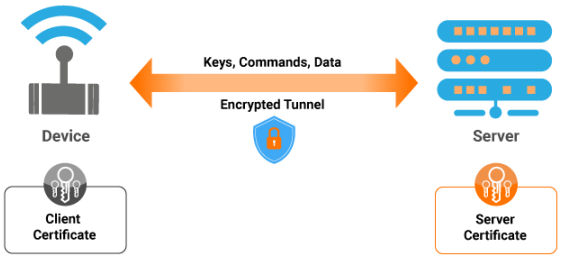
NB-IoT with UDP/DTLS protocol

- Secure implementation of DTLS protocol
- UDP-DTLS allowing faster data stream and better battery performance against TCP-TLS



TLS: full secure TLS stack implementation

- **Easy way to implement an end-to-end security layer** between an IP device and a server or between a non-IP device and a gateway/server
- **Secure TLS handshake**: mutual authentication with X.509 certificate and secure session key establishment, message confidentiality and integrity delegated to the host MCU
- **Full Secure TLS stack**: mutual authentication, secure session key establishment and messages encryption/decryption, all performed within the AVNET-TO136 Secure Element.



- **Supported Cipher Suites**:

ID	Standard Cipher Suite Name
C023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
C0AC	TLS_ECDHE_ECDSA_WITH_AES_128_CCM
C0AE	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
C02B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
00AE	TLS_PSK_WITH_AES_128_CBC_SHA256
C0A4	TLS_PSK_WITH_AES_128_CCM
C0A8	TLS_PSK_WITH_AES_128_CCM_8
00A8	TLS_PSK_WITH_AES_128_GCM_SHA256

Cloud connected devices – AWS (Amazon Web Services)

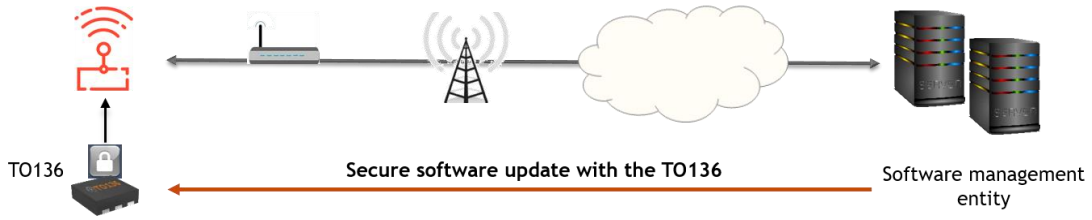
- Protection of connected devices credentials: secured access and secured data sent to AWS servers
- TLS 1.2 mutual authentication with X.509 Device Certificate

Off-line local network

- Peer to peer secure device connectivity, e.g. on a LAN
  (provided shared key have been established)
- ECIES shared key establishment scheme, with dynamic key renewal

Secure software update of the host MCU

- Control of software downloading into devices once deployed in the field
- Protection against unauthorized reprogramming of the devices (change/ control/ unlock functions)
- Software authenticity and integrity verification before allowing host MCU to proceed to update



Secure boot

- Root of trust to protect the integrity of the system
- Bootloader integrity or code integrity: computing secure bootloader hash at power up and comparing with the reference one

Secure data storage

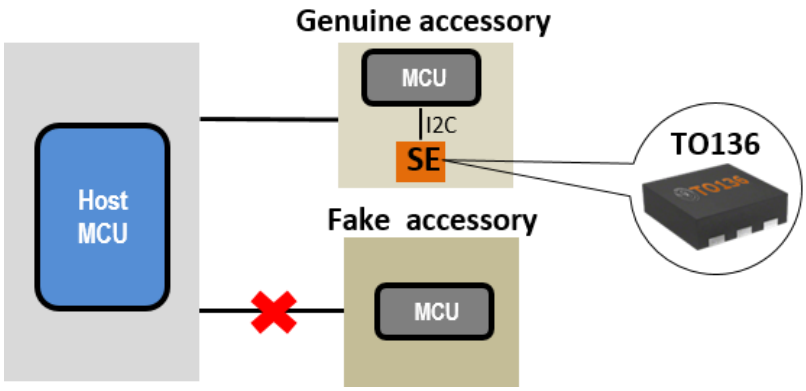
- Protection of application sensitive data
- Secure data storage inside the internal user memory
- Data encryption/decryption at rest using host MCU external Flash memory

Secure proprietary protocol

- Enhancement of the security level of a proprietary protocol

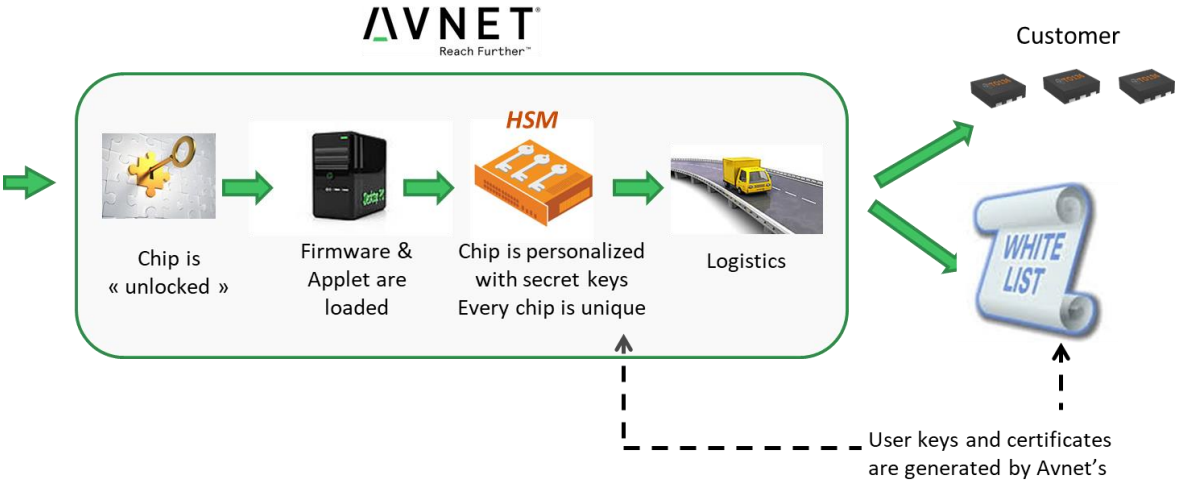
Brand protection and usage control

- Connection to server restricted to authorized devices or accessories (whitelist generated at production, available to customers)
- Over usage of a consumable accessory strictly controlled (secure counters)
- Discrimination between an original device/board and a fake copy
- Strong authentication used in production and in the field



Personalization with AVNET exclusive secure logistics

- Fully secure supply chain
- Keys and certificates generation (HSM), under a per-customer subCA
- Programming and personalization
- MOQ < 1 Ku
- Samples with the generic firmware
- Fast sampling with custom firmware
- Custom personalisation profile defined per-customer
- LoRaWAN personalization ready
- Security policies conforming with standards

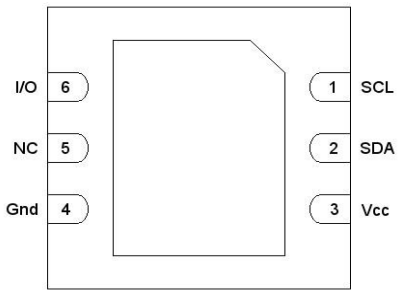


Source code helpers for integration

- libTO: 'C' Client library source code – for MCU or Linux hosts
- libTOsrv: Server-side API library (Java, Node.js, or C)
- Available on www.trusted-objects.com
  (password protected - get yours at TO136-support@avnet.eu)

Pinout & Packaging

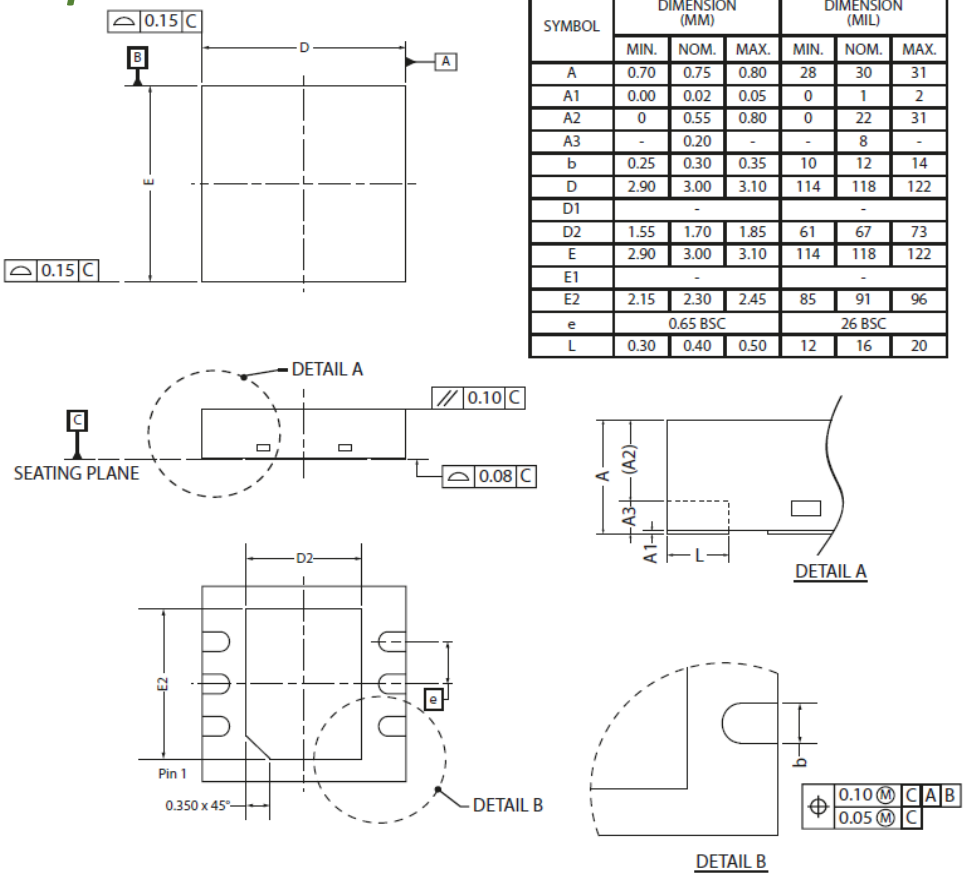
DFN6 package pinout



Bottom View

Pin Number	Pin Name	Role
1	SCL	I2C Serial Clock
2	SDA	I2C Serial Data
3	Vcc	Power supply from 1,62V to 5,5V
4	Gnd	Ground
5	NC	Not connected
6	I/O	Power management optimization

Mechanical Description



SYMBOL	DIMENSION (MM)			DIMENSION (MIL)		
	MIN.	NOM.	MAX.	MIN.	NOM.	MAX.
A	0.70	0.75	0.80	28	30	31
A1	0.00	0.02	0.05	0	1	2
A2	0	0.55	0.80	0	22	31
A3	-	0.20	-	-	8	-
b	0.25	0.30	0.35	10	12	14
D	2.90	3.00	3.10	114	118	122
D1		-			-	
D2	1.55	1.70	1.85	61	67	73
E	2.90	3.00	3.10	114	118	122
E1		-			-	
E2	2.15	2.30	2.45	85	91	96
e	0.65 BSC			26 BSC		
L	0.30	0.40	0.50	12	16	20

NOTE :
1. REFER TO JEDEC STD: MO-220.
2. DIMENSION "b" APPLIES TO METALLIZED TERMINAL AND IS MEASURED BETWEEN 0.15MM AND 0.30MM FROM THE TERMINAL TIP. IF THE TERMINAL HAS OPTIONAL RADIUS ON THE OTHER END OF THE TERMINAL, THE DIMENSION B SHOULD NOT BE MEASURED IN THAT RADIUS AREA.

Plastic Dual-Flat No-Leads 6 3x3x0.75mm Body [DFN6]

Absolute Maximum Ratings

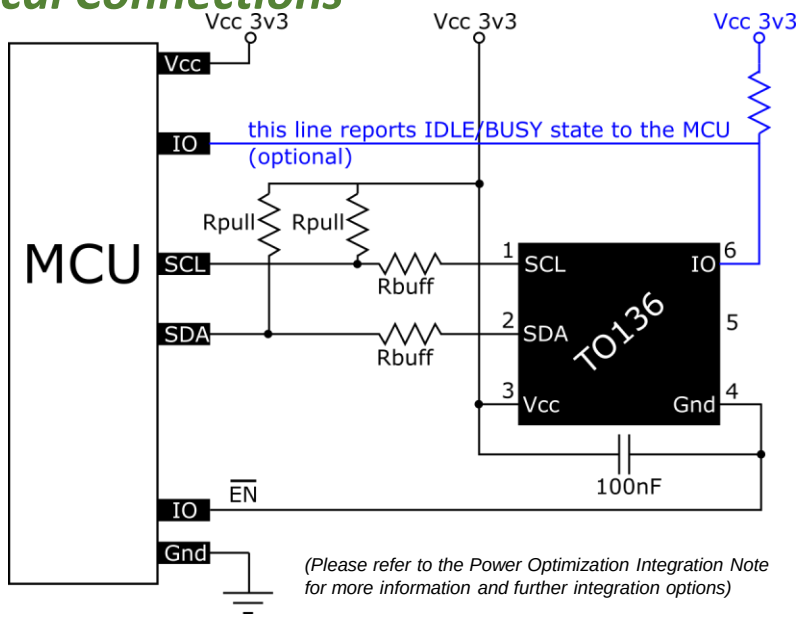
Symbol	Parameter	Condition	Min	Typ	Max	Unit
Vcc	Supply Voltage		-0.3		7.5	V
V	All pins		-0.3		Vcc+0.3	V
T_{stg}	Storage temperature		-40		105	°C
ESD	Electrostatic discharge resistance	Human Body mode*			6	kV

* Equivalent to discharging a 100pF capacitor through 1,5kΩ

Operating Parameters

Symbol	Parameter	Condition	Min	Typ	Max	Unit
Vcc	Operating Voltage		1.62		5.5	V
Icc	Output Current			2.4	2.6	mA
T_{op}	Operating temperature		-40	25	85	°C

Typical Electrical Connections



(Please refer to the Power Optimization Integration Note for more information and further integration options)

Communication

- I²C (Two Wire Interface) 400 kbit/s
- Custom protocol and command set

AVNET-TO136 features set

Subject	Features
Core	• Return the Serial or Product Identification Number • Return the Hardware or Software Version Number • True random numbers generation • Secure Write/Read data in user non-volatile memory
Cryptography	• Computes hash of the given data using SHA256 • Compute or verify HMAC or CMAC • Encrypt or decrypt data using AES (ECB/CBC/CTR/CCM/GCM modes)
Device Authentication	• Return the Avnet-TO136's certificate • Compute Elliptic Curve Digital Signature of a given challenge
Peer Authentication	• Verify signature of peer certificate and store the corresponding public key • Return random number to be signed by host • Elliptic Curve Digital Signature verification using peer public key
Key management	• Secure update of peer public key • On board ECC key pair generation • Diffie-Hellman or ECIES session keys computation • Key fingerprinting
LoRaWAN	• Return personalized values (APPEUI, DEVEUI, DEVADDR) • Handle LoRaWAN join process, computes NwkSkey and AppSkey • Handle secure counter • Compute or verify MIC • Encrypt or decrypt network or application data
Sigfox	• Return Sigfox ID • Verify/Generate Sigfox Message Authentication Code • Encrypt/decrypt messages, • Handle secure counter & Generate rsync frame
(D)TLS	• Full management of (D)TLS handshake process • Session keys generation • Data encryption / decryption and integrity protection • Packetization, ordering, and retransmission (DTLS only)