# Microchip's Trust Platform

Leverage Microchip's Secure Manufacturing Infrastructure
to Securely Provision Credentials in Your Products

Summary

For deployments as few as ten units up to many thousands of devices, the Trust Platform
is a cost-effective and flexible solution for on-boarding Microchip's Secure Elements
to your design and accelerating your product's time to market. The Trust Platform is
composed of a family of pre-provisioned, pre-configured or fully customizable secure
elements. Credentials are generated inside each secure element's boundary by leverag-
ing Microchip's Hardware Secure Modules (HSMs) installed in our factories. The devices
also come with hardware and software development tools to make prototyping easy and
fast track your development. The Trust Platform offers three tiers of secure elements—
Trust&GO, TrustFLEX and TrustCUSTOM—to provide you with the options and flexibility
to meet the requirements of your company's security model.
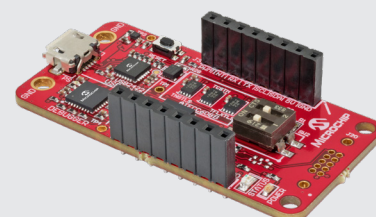
- Pre-configured and pre-provisioned devices
- Includes keys and generic certifi- cates for thumbprint authentication
- 10 units minimum order quantity including provisioning
- Full stack code examples available

- Pre-configured and pre-provisioned devices
- Upgrade default cerdential to use your own certificate chain
- 2,000 units minimum order quantity including provisioning
- Most commonly use cases available

- Blank devices
- Fully customizable device
- 4,000 units minimum order quantity including provisioning
- Full datasheet and configuration tool available under NDA

Key Highlights

- Easier embedded security on-boarding with pre-defined configurations and pre-provisioned keys and certificates
- Trust&GO for TLS networks
  - AWS IoT and Greengrass leveraging "Multi Accounts Registration"
  - Google Cloud Platform leveraging "Token authentication"
  - Microsoft Azure
  - Third-party TLS authentication
- Trust&GO for LoRaWAN™ networks
  - The Things Industry (TTI) join server
  - Actility join server
- Pre-defined use cases with TrustFLEX
  - Any cloud, any PKI, any certificate authority
  - Certificate-based/token authentication

- Firmware verification/OTA validation/secure boot verification
- Firmware IP protection
- Message encryption
- I/O protection key
- Accessory authentication
- Key rotation
- Fitted for mass market with low MoQ including secure key provisioning and Microchip certificates
- Architecture agnostic of any controller, any cloud, any connectivity
- Quick development with the Trust Platform Design Suite (use case selector, Python-based notebook, C-code, configurator for secret exchange)

MICROCHIP

Development Tools

- **Trust Platform Design Suite** – software tool helping to select the desired pre-defined use case(s), test your secure element setup leveraging python executable tutorials, accelerate your embedded prototype with the C code examples and be autonomous during secret exchange).
- **Trust Platform USB Kit (DM320118)** – base development kit with USB port integrating the ATECC608B Trust&GO, TrustFLEX and TrustCUSTOM.

- **ATECC608B Trust Kit (DT100104)** – add-on development board to the DM320118 to benefit from additional ATECC608B Trust Platform devices soldered on a PCB.
- From mikroe.com: **Secure click (uDFN: MIKROE-3746/ SOIC: MIKROE-3788)** – socketed-based extension board to the DM320118 to scale up your testing capabilities with the ATECC608B Trust Platform.

ATECC608B Trust&GO TLS	Description
ATECC608B-TNGTLSS-B	Trust&GO TLS, Provisioned, 8-SOIC, I²C (10 units bulk)
ATECC608B-TNGTLSU-B	Trust&GO TLS, Provisioned, 8-UDFN, I²C (10 units bulk)
ATECC608B-TNGTLSS-C	Trust&GO TLS, Provisioned, 8-SOIC, I²C (100 units Tape & Reel)
ATECC608B-TNGTLSU-C	Trust&GO TLS, Provisioned, 8-UDFN, I²C (100 units Tape & Reel)
ATECC608B-TNGTLSS-G	Trust&GO TLS, Provisioned, 8-SOIC, I²C (2K units Tape & Reel)
ATECC608B-TNGTLSU-G	Trust&GO TLS, Provisioned, 8-UDFN, I²C (2K units Tape & Reel)
ATECC608B TrustFLEX TLS	**Description**
ATECC608B-TFLXTLSS-Proto	TrustFLEX TLS, Provisioned Prototypes, 8-SOIC (10 units bulk)
ATECC608B-TFLXTLSU-Proto	TrustFLEX TLS, Provisioned Prototypes, 8-UDFN (10 units bulk)
ATECC608B-TFLXTLSS	TrustFLEX TLS, Provisioned, 8-SOIC (2K units Tape & Reel)
ATECC608B-TFLXTLSU	TrustFLEX TLS, Provisioned, 8-UDFN (2K units Tape & Reel)
ATECC608B TrustCUSTOM	**Description**
ATECC608B-TCSMS	TrustCUSTOM, Provisioned, 8-SOIC (4K units Tape & Reel)
ATECC608B-TCSMU	TrustCUSTOM, Provisioned, 8-UDFN (4K units Tape & Reel)
ATSHA204A TrustCUSTOM	**Description**
ATSHA204A-TCSMS	TrustCUSTOM, Provisioned, 8-SOIC (4K units Tape & Reel)
ATSHA204A-TCSMU	TrustCUSTOM, Provisioned, 8-UDFN (4K units Tape & Reel)
Trust&GO for The Things Industries	**Description**
ATECC608B-TNGLORAS-B	Trust&GO LORAWAN™, Provisioned Prototypes, 8-SOIC, I²C, (10 units bulk)
ATECC608B-TNGLORAU-B	Trust&GO LORAWAN, Provisioned Prototypes, 8-UDFN, I²C, (10 units bulk)
ATECC608B-TNGLORAS-C	Trust&GO LORAWAN, Provisioned, 8-SOIC, I²C (100 units Tape & Reel)
ATECC608B-TNGLORAU-C	Trust&GO LORAWAN, Provisioned, 8-UDFN, I²C (100 units Tape & Reel)
ATECC608B-TNGLORAS-G	Trust&GO LORAWAN, Provisioned, 8-SOIC, I²C (2K units Tape & Reel)
ATECC608B-TNGLORAU-G	Trust&GO LORAWAN, Provisioned, 8-UDFN, I²C (2K units Tape & Reel)
Trust&GO for Actility	**Description**
ATECC608B-TNGACTS-B	Trust&GO Actility LORAWAN, Provisioned Prototypes, 8-SOIC, I²C (10 units bulk)
ATECC608B-TNGACTU-B	Trust&GO Actility LORAWAN, Provisioned Prototypes, 8-UDFN, I²C (10 units bulk)
ATECC608B-TNGACTS-C	Trust&GO Actility LORAWAN, Provisioned, 8-SOIC, I²C (100 units Tape & Reel)
ATECC608B-TNGACTU-C	Trust&GO Actility LORAWAN, Provisioned, 8-UDFN, I²C (100 units Tape & Reel)
ATECC608B-TNGACTS-G	Trust&GO Actility LORAWAN, Provisioned, 8-SOIC, I²C (2K units Tape & Reel)
ATECC608B-TNGACTU-G	Trust&GO Actility LORAWAN, Provisioned, 8-UDFN, I²C (2K units Tape & Reel)

www.microchip.com/TrustPlatform

MICROCHIP