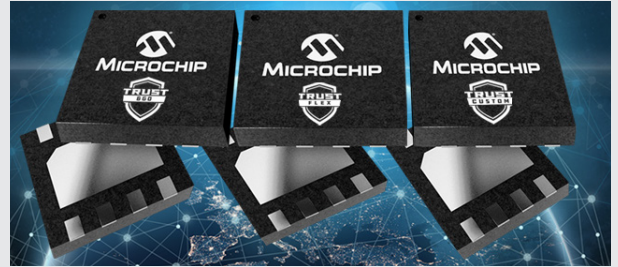# Microchip Trust Platform

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

Summary

For deployments of as few as ten units to up to many thousands of
devices, the Trust Platform is a cost-effective and flexible solution for
onboarding Microchip Secure Elements in your design and accelerat-
ing 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 ele-
ment's boundary by leveraging Microchip Hardware Secure Modules
(HSMs) installed in our factories. The devices also come with hard-
ware and software development tools to make prototyping easy and
to 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 Provisioning
- Trust&GO for TLS networks
  - AWS IoT and Greengrass leveraging "Multi Accounts Registration"
  - Google Cloud Platform leveraging "Token authentication"
  - Third-party TLS authentication
- Trust&GO for LoRaWAN networks
  - The Things Industry (TTI) Join Server
  - Actility join server
- Easier Embedded Security on-boarding with pre-defined Configurations and Provisioning with Trust&GO
  - 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 provisioning and Microchip certificates
- Architecture agnostic any controller, any connectivity
- Quick development with simple toolset 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** – free of charge – 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 (DM320119)** – $13 each – base development kit with USB port integrating the ATECC608A Trust&GO, TrustFLEX and TrustCUSTOM

- **ATECC608A Trust Kit (DT100104)** – $14 each – add-on development board to the DM320118 to benefit from additional ATECC608A Trust Platform devices soldered on a PCB.
- From mikroe.com: **Secure uDFN click (MiKROE-3746)** – socketed based extension board to the DM320118 to scale up your testing capabilities with the ATECC608A Trust Platform.

Trust&GO	Description
ATECC608A-TNGTLSS-B	Trust&GO TLS,Provisioined Proto Typing, 8-SOIC, I2C, (10 bulk)
ATECC608A-TNGTLSU-B	Trust&GO TLS, Provisioined Proto Typing, 8-UDFN, I2C, (10 bulk)
ATECC608A-TNGTLSS-C	Trust&GO TLS, Provisioned, 8-SOIC, I2C, (100 unit multiple)
ATECC608A-TNGTLSU-C	Trust&GO TLS, Provisioned, 8-UDFN, I2C, (100 unit multiple)
ATECC608A-TNGTLSS-G	Trust&GO TLS, Provisioned, 8-SOIC, I2C, 2K multiple
ATECC608A-TNGTLSU-G	Trust&GO TLS, Provisioned, 8-UDFN, I2C, 2K multiple
TrustFLEX	**Description**
ATECC608A-TFLXTLSS-Proto	TrustFLEX TLS, Provisioined Proto Typing, 8-SOIC (10 bulk)
ATECC608A-TFLXTLSU-Proto	TrustFLEX TLS, Provisioned Proto Typing, 8-UDFN, I2C, (10 bulk)
ATECC608A-TFLXTLSS	TrustFLEX TLS, Provisioned, 8-SOIC 2K MOQ
ATECC608A-TFLXTLSU	TrustFLEX TLS, Provisioned, 8-UDFN 2K MOQ
TrustCUSTOM	**Description**
ATECC608A-TCSMS	TrustCUSTOM, Provisioned, 8-SOIC, 4K MOQ
ATECC608A-TCSMU	TrustCUSTOM, Provisioned, 8-UDFN 4K MOQ
Trust&GO for The Things Industries	**Description**
ATECC608A-TNGLORAS-B	Trust&GO LORAWAN, Provisioined Proto Typing, 8-SOIC, I2C, (10 bulk)
ATECC608A-TNGLORAU-B	Trust&GO LORAWAN, Provisioined Proto Typing, 8-UDFN, I2C, (10 bulk)
ATECC608A-TNGLORAS-C	Trust&GO LORAWAN, Provisioned, 8-SOIC, I2C, (100 unit multiple)
ATECC608A-TNGLORAU-C	Trust&GO LORAWAN, Provisioned, 8-UDFN, I2C, (100 unit multiple)
ATECC608A-TNGLORAS-G	Trust&GO LORAWAN, Provisioned, 8-SOIC, I2C, 2K multiple
ATECC608A-TNGLORAU-G	Trust&GO LORAWAN, Provisioned, 8-UDFN, I2C, 2K multiple
TrustFLEX for LoRaWAN	**Description**
ATECC608A-TFLXLORAS-Proto	TrustFLEX LORAWAN, Provisioined Proto Typing, 8-SOIC (10 bulk)
ATECC608A-TFLXLORAU-Proto	TrustFLEX LORAWAN, Provisioined Proto Typing, 8-UDFN, I2C, (10 bulk)
ATECC608A-TFLXLORAS	TrustFLEX LORAWAN, Provisioned, 8-SOIC 2K MOQ
ATECC608A-TFLXLORAU	TrustFLEX LORAWAN, Provisioned, 8-UDFN 2K MOQ
Trust&GO for Actility	**Description**
ATECC608A-TNGACTS-B	Trust&GO Actility LORAWAN, Provisioined Proto Typing, 8-SOIC, I2C, (10 bulk)
ATECC608A-TNGACTU-B	Trust&GO Actility LORAWAN, Provisioined Proto Typing, 8-UDFN, I2C, (10 bulk)
ATECC608A-TNGACTS-C	Trust&GO Actility LORAWAN, Provisioned, 8-SOIC, I2C, (100 unit multiple)
ATECC608A-TNGACTU-C	Trust&GO Actility LORAWAN, Provisioned, 8-UDFN, I2C, (100 unit multple)
ATECC608A-TNGACTS-G	Trust&GO Actility LORAWAN, Provisioned, 8-SOIC, I2C, 2K multiple
ATECC608A-TNGACTU-G	Trust&GO Actility LORAWAN, Provisioned, 8-UDFN, I2C, 2K multiple
Trust Flex Actility	**Description**
ATECC608A-TFLXACTS-Proto	TrustFLEX Actility LoraWan, Provisioned Proto Typing, 8-SOIC (10 bulk)
ATECC608A-TFLXACTU-Proto	TrustFLEX Actility LORAWAN,Provsioned Proto Typing, 8-UDFN, I2C, (10 bulk)
ATECC608A-TFLXACTS	TrustFLEX Actility LORAWAN, Provisioned, 8-SOIC 2K MOQ
ATECC608A-TFLXACTU	TrustFLEX Actility LORAWAN, Provisioned, 8-UDFN 2K MOQ

MICROCHIP