
Secure Provisioning of TrustFLEX

Overview:

This document describes Microchip's secure provisioning process for TrustFLEX devices and shows you how to order devices that have been provisioned with your secrets, keys, and certificates.

After prototyping your use case with the [Trust Platform Design Suite](#), you are ready to place a device verification order. Microchip will have to provision these devices for you. This means you'll have to securely transmit your provisioning details (secrets, keys and certificates) to us using our secret exchange process. After verifying these devices perform as expected, you'll be ready to place your first production orders.

Table of Contents

Overview:	1
Create a technical support case.....	2
Secret Exchange Process.....	7
1) Obtain your encryption keys and your project part number.....	7
2) Create your provisioning file	7
3) Encrypt your provisioning file	10
4) Upload your provisioning file	12
Signature Exchange (optional)	13
Placing Verification Orders	14
Placing Production Orders	17

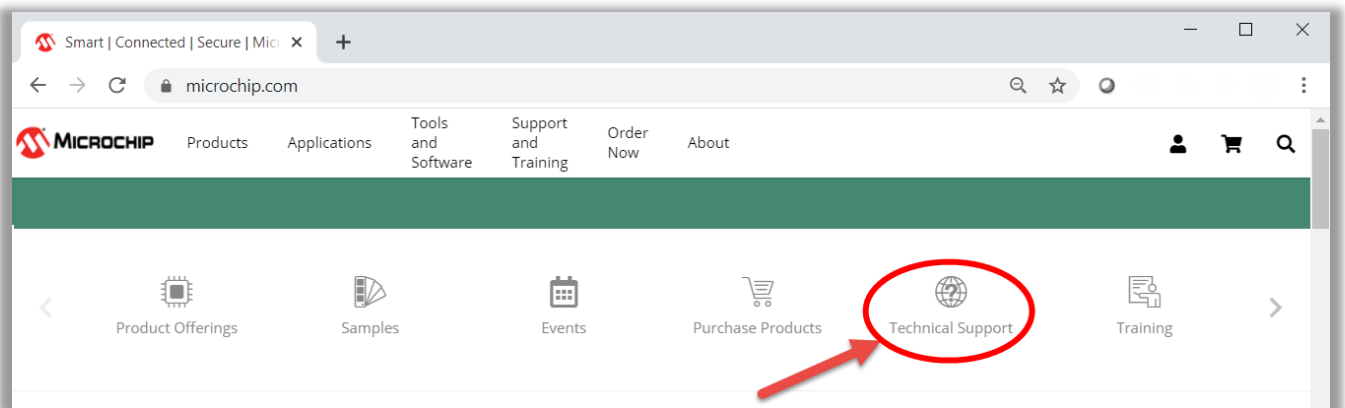
Create a technical support case

The Microchip Technical Support Portal (also known as myMicrochip) will be used to create a technical support case. The creation of this case enables you to:

- Obtain your TrustFLEX project part number
- Obtain the keys needed to encrypt your provisioning file
- Upload your encrypted provisioning file

You won't be able to order any provisioned devices without creating a support case first.

- 1) On the microchip.com homepage, click the **Technical Support** icon near the top of the page.

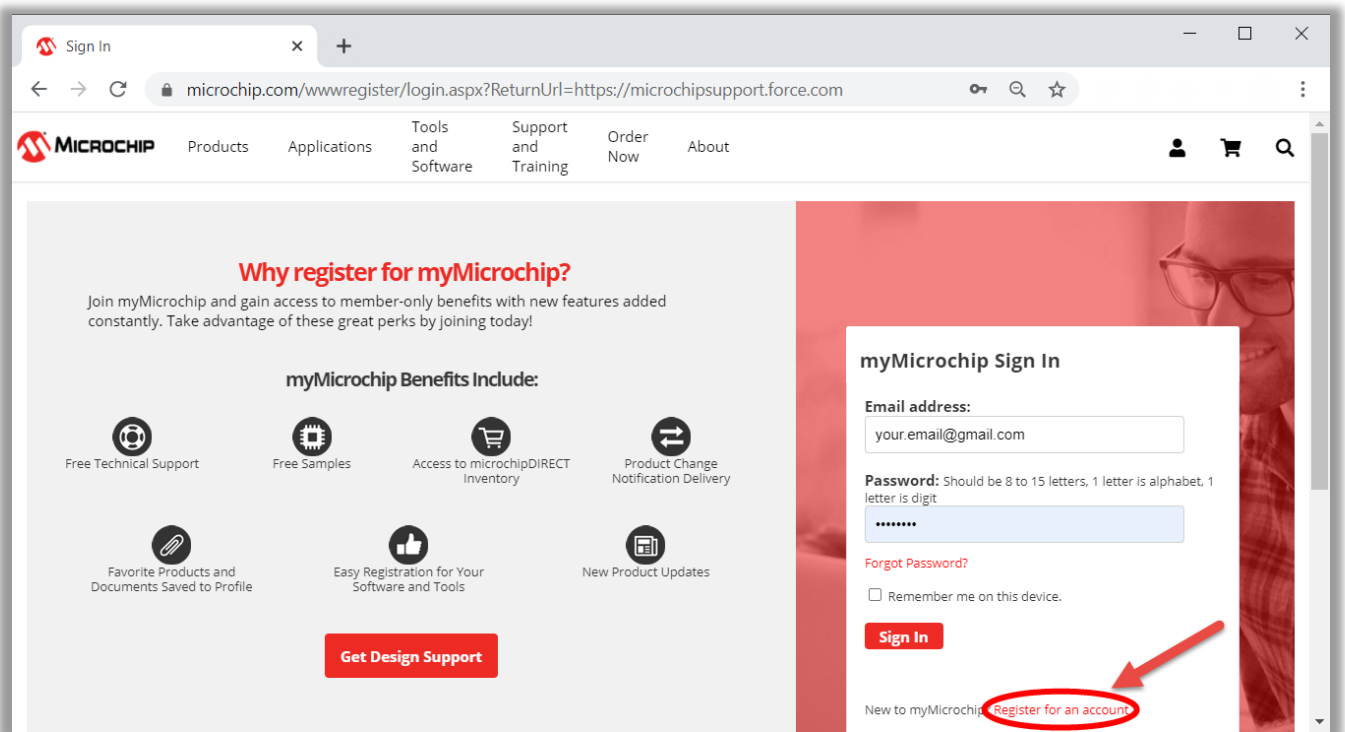


- 2) Click the **Log in** button (top right corner) to log into the technical support portal.

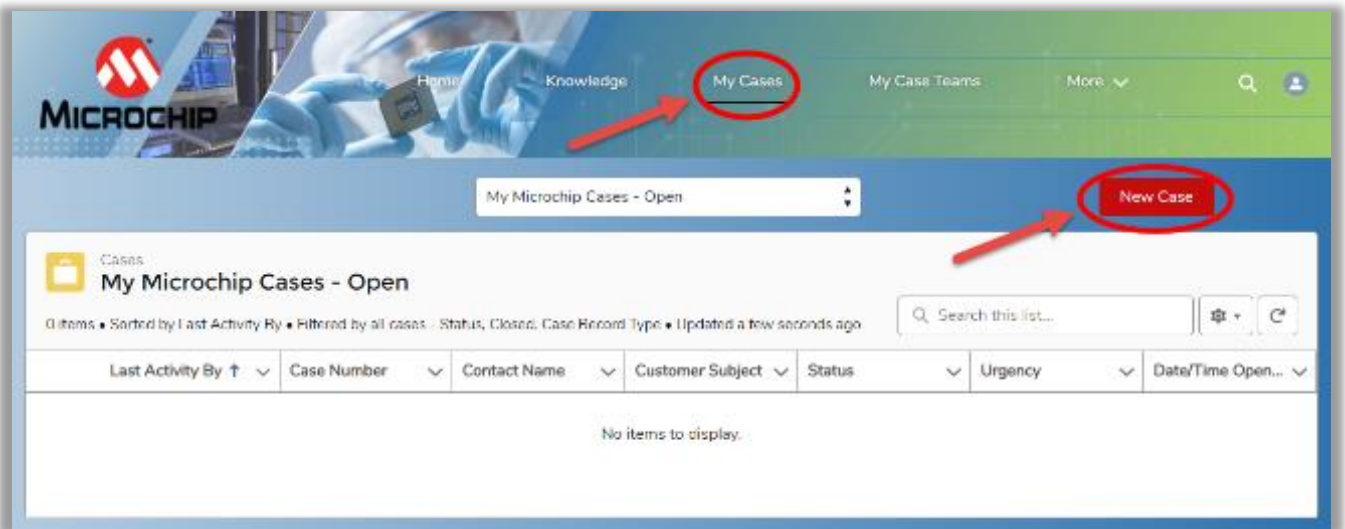
Note:

MicrochipDirect and myMicrochip share login credentials. Use your MicrochipDirect login credentials to log into this site. If you do not have a MicrochipDirect account, you can register for a new

myMicrochip account.



- 3) After logging into the technical support portal, click on **My Cases** at the top of the page, then click **New Case**.



- 4) In the “Let us know how we can help you” section, select **Value Added Services** as the case reason then click **Next**.

Let us know how we can help you

Case Reason*

☐ **Hardware/Firmware Support**
(Device, Peripherals, Modules, Code examples, Demo boards, Evaluation kits.)

☐ **Software Library**
(Harmony, Touch Library, Advanced Software Framework (ASF), Atmel Start, MPLAB® Code Configurator, Microchip Library of Applications, Bootloaders, Baremetal Softpack, Linux OS and drivers)

☐ **Development Tools**
(Development Environment - IDE, Compilers, Debugger, Emulator, Programmer, MPLAB Analog Designer, MPLAB Mindi Simulator)

☐ **Documentation**
(Datasheet, Errata, Application Notes, FRM, EOL, Soldering, Packaging, demo/kit design files)

☐ **Quality/Reliability**
(FIT, MTBF, MSL, RMA, Field Failures, MSL, EOL, Part Marking)

☐ **Product Selection**
(Help to select suitable product)

☒ **Value Added Services**
(Design Check, Secure Provisioning)

☐ **Website Issues**
(Support website related issues.)

Next **Cancel**

- 5) In the “Provide more specific information” section, provide the following then click **Next**:
- Subject: **Your Company Name**
- Target Device: Begin typing the part number you want to order. This window has an auto-complete function that will assist in selecting the appropriate device.
- Category: **Provisioning Services**
- Sub-Category: **TrustFLEX**

Provide more specific information

Subject*
Your Company Name

Target Device*
ATECC608A-TFLXTLS

Category*
Provisioning Services

Sub-Category*
TrustFlex

Previous **Next** **Cancel**

- 6) In the “Describe your issue here” section, please add the following details:

Program Name: Provide a short but descriptive name for this project so it will help distinguish between other projects you may have associated with your account.

Version Number: Provide a short name or numerical value for this program such as 1.0, etc.

Device Package: Provide your desired package (e.g. UDFN or SOIC).

Comments: Provide a short program description that will be displayed on the e-commerce portal.

MicrochipDirect Email Address: Provide all email addresses registered at [MicrochipDirect](#) that will be authorized to purchase product associated with this project. Make sure to include any distribution or contract manufacturer email addresses if they will be ordering parts for you. Please ensure all email addresses are accurate.

Attention:

You have total control over who can order your provisioned TrustFLEX devices. If a MicrochipDirect account is not associated with an email listed in this text box, the account will not be able to order TrustFLEX devices provisioned for your usecase.

Describe your issue here

Please add your issue description here*

I am looking for a TrustCustom device for my use case. Here are some additional details

Here are the program details as requested:

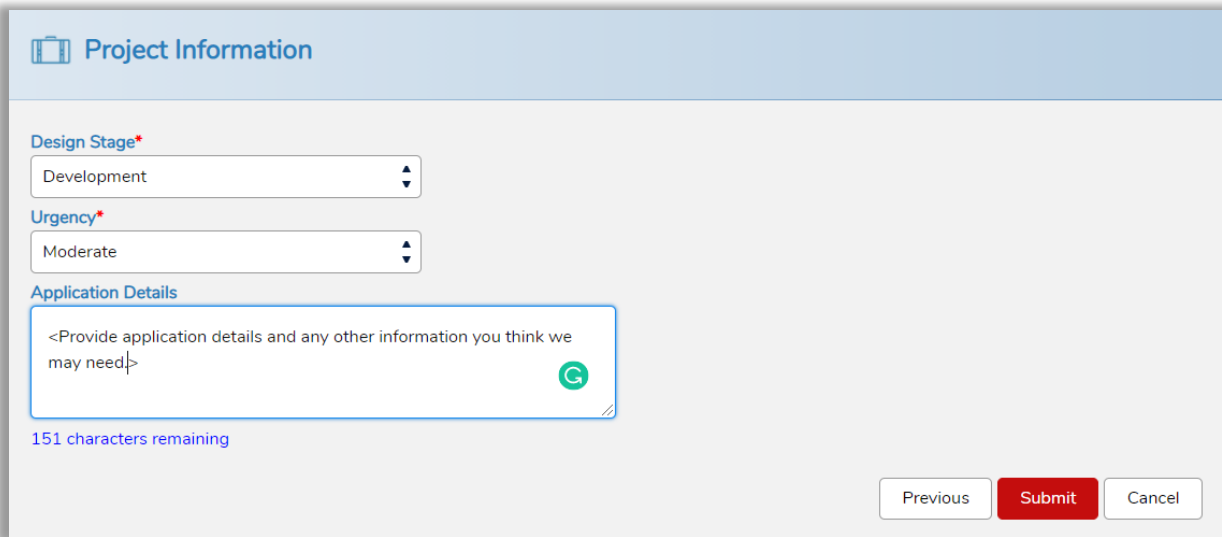
Program Name: Saturn
Version Number: x.x
Device Package: UDFN
Comments: Project 1
Microchip Direct Email Address: yyyyy@yyy

Microchip provides Trust Custom provisioning service for CryptoAuthentication device. For more details, please visit: www.microchip.com/TrustCustom. Please submit the case in this sub-category if your provisioning needs are based on TrustCustom configuration and are ready for secret exchange process.

- The user should have had NDA with Microchip to be able to continue with this case creation and need to provide confirmation in

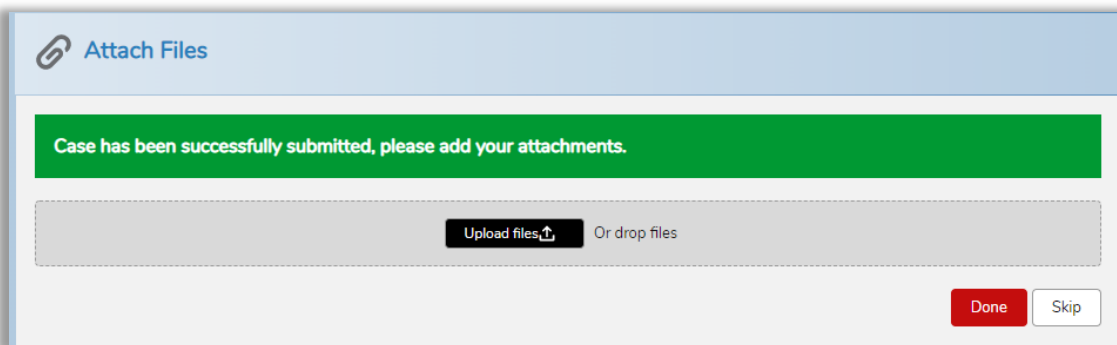
- 7) In the “*Project Information*” section enter the following and click **Submit**:
Design Stage and Urgency are automatically populated for you.

Application details: Add any additional relevant information you think we may need.



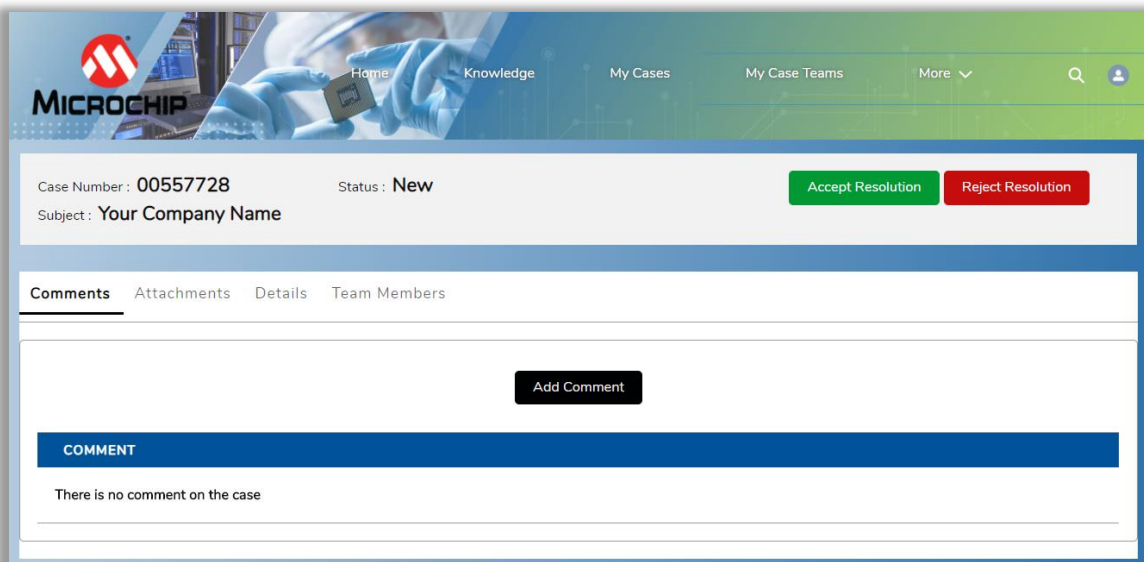
The 'Project Information' form contains two dropdown menus: 'Design Stage*' with 'Development' selected, and 'Urgency*' with 'Moderate' selected. Below these is a text area for 'Application Details' with the placeholder text '<Provide application details and any other information you think we may need>'. A green circular icon with a 'G' is to the right of the text area. Below the text area, it says '151 characters remaining'. At the bottom right are three buttons: 'Previous', 'Submit' (in red), and 'Cancel'.

- 8) After creating your technical support case, a window will open allowing you to attach files to it. If you have no files to attach just click **DONE**.



The 'Attach Files' window has a green banner at the top that says 'Case has been successfully submitted, please add your attachments.' Below this is a dashed box containing an 'Upload files' button with an upward arrow icon and the text 'Or drop files'. At the bottom right are two buttons: 'Done' (in red) and 'Skip'.

- 9) If you want to add a comment or a question to the case, click **Add Comment**.



The Microchip case details page shows the case number '00557728' and status 'New'. The subject is 'Your Company Name'. There are two buttons: 'Accept Resolution' (green) and 'Reject Resolution' (red). Below this is a tabbed interface with 'Comments', 'Attachments', 'Details', and 'Team Members'. The 'Comments' tab is active, showing an 'Add Comment' button. Below the button is a blue bar with the word 'COMMENT' and a text area that says 'There is no comment on the case'.

Secret Exchange Process

1) Obtain your encryption keys and your project part number

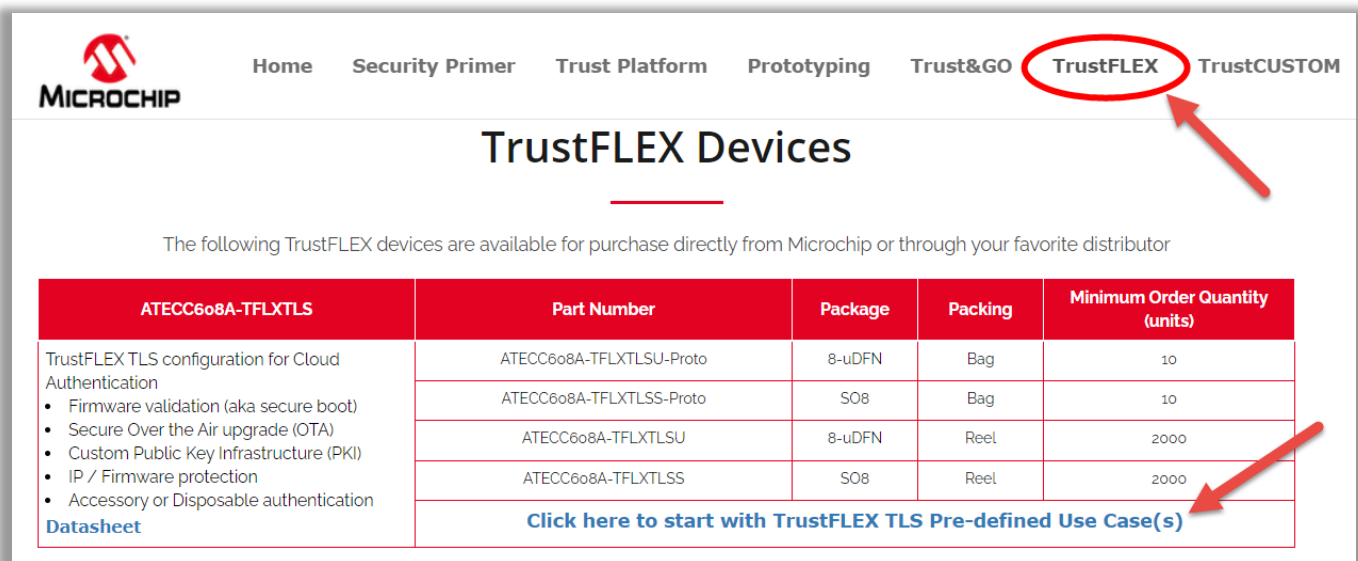
Your technical support case enables Microchip to assign you a project part number and provide you with keys used to encrypt your provisioning file. The project part number must be included in your provisioning file (instructions to do this are show below).

Microchip's hardware security modules (HSM) will generate the RSA public/private key pairs used to encrypt and decrypt your provisioning file. Each manufacturing location has its own HSM, so you'll need a one public key for each location. This means you will need to provide an encrypted provisioning file for each location, and the location name must be included in the file name. The details will be provided to you in the support case.

2) Create your provisioning file

The TrustFLEX homepage in the [Trust Platform Design Suite](#) contains a configurator tool that generates an XML file used to provision the TrustFLEX device.

Open the Trust Platform Design Suite homepage on your computer by clicking on the ****Getting Started**** button in the Trust Platform Design Suite program. Navigate to the TrustFLEX homepage by selecting TrustFLEX at the top of the page then "Click here to start with TrustFLEX TLS Pre-defined Use Case(s)".



MICROCHIP Home Security Primer Trust Platform Prototyping Trust&GO **TrustFLEX** TrustCUSTOM

TrustFLEX Devices

The following TrustFLEX devices are available for purchase directly from Microchip or through your favorite distributor

ATECC608A-TFLXTLS	Part Number	Package	Packing	Minimum Order Quantity (units)
TrustFLEX TLS configuration for Cloud Authentication <ul style="list-style-type: none">Firmware validation (aka secure boot)Secure Over the Air upgrade (OTA)Custom Public Key Infrastructure (PKI)IP / Firmware protectionAccessory or Disposable authentication Datasheet	ATECC608A-TFLXTLSU-Proto	8-uDFN	Bag	10
	ATECC608A-TFLXTLSS-Proto	SQ8	Bag	10
	ATECC608A-TFLXTLSU	8-uDFN	Reel	2000
	ATECC608A-TFLXTLSS	SQ8	Reel	2000
	Click here to start with TrustFLEX TLS Pre-defined Use Case(s)			

a) Select a use case (or multiple use cases) from the Use Case Library.

USE CASE LIBRARY

The following standard use cases are available completely pre-configured including transaction diagrams and example code.

Firmware validation Secure OTA	Secure Public Key Rotation	IP / Firmware Protection
<div>SELECT</div>	<div>SELECT</div>	<div>SELECT</div>
Accessory / Disposable Symmetric-Authentication	Custom Public Key Infrastructure	Cloud Connect Google - IoT
<div>SELECT</div>	<div>UNSELECT</div>	<div>SELECT</div>
Accessory / Disposable Asymmetric-Authentication		
<div>SELECT</div>		

b) The TrustFLEX Configuration section (near the bottom of the page) displays all the configuration slots in the TrustFLEX device. These slots are automatically configured for you based on your selection(s) of the use case(s). If a slot configuration may need additional information from you, it will be highlighted.

Click on these highlighted slots to add this information.

TrustFLEX CONFIGURATION			
TrustFLEX XML Generator			
Choose TrustFLEX device interface:			
<input checked="" type="radio"/> I2C			
<input type="radio"/> SWI			
Click on table rows for more info.			
Slot Number	Slot Use-case	Description	Slot Property
Slot 0	Primary private key	Primary authentication key.	Permanent, Ext Sign, ECDH
Slot 1	Internal sign private key	Private key that can only be used to attest internal keys and state of the a device. Can't be used to sign arbitrary messages.	Permanent, Int Sign
Slot 2	Secondary private key 1	Secondary private key for other uses.	Updatable, Ext Sign, ECDH, Lockable
Slot 3	Secondary private key 2	Secondary private key for other uses.	Updatable, Ext Sign, ECDH, Lockable
Slot 4	Secondary private key 3	Secondary private key for other uses.	Updatable, Ext Sign, ECDH, Lockable
Slot 5	Secret key	Storage for a secret key.	No Read, Encrypted write(6), Lockable, AES key
Slot 6	IO protection key	Key used to protect the I2C bus communication (IO) of certain commands. Requires setup before use.	No read, Clear write, Lockable
Slot 7	Secure boot digest	Storage location for secureboot digest. This is an internal function, so no reads or writes are enabled.	No read, No write
Slot 8	General data	General public data storage (416 bytes).	Clear read, Always write, Lockable
Slot 9	AES key	Intermediate key storage for ECDH and KDF output.	No read, Always write, AES key
Slot 10	Device compressed certificate	Certificate primary public key in the Crypto Authentication compressed format.	Clear read, No write
Slot 11	Signer public key	Public key for the CA (signer) that signed the device cert.	Clear read, No write
Slot 12	Signer compressed certificate	Certificate for the CA (signer) certificate for the device certificate in the CryptoAuthentication compressed format.	Clear read, No write
Slot 13	Parent public key or general data	Parent public key for validating/invalidating the validated public key. Can also be used just as a public key or general data storage (72 bytes).	Clear read, Always write, Lockable
Slot 14	Validated public key	Validated public key cannot be used (Verify command) or changed without authorization via the parent public key.	Clear read, Always write, Validated (13)
Slot 15	Secure boot public key	Secure boot public key.	Clear read, Always write, Lockable

If your use case requires certificates (i.e., custom PKI and accessory/disposable asymmetric authentication), a Microchip standard certificate will be selected by default. If you would like to use a custom certificate instead, click on slots 10 and 12 to add the additional information required. You will also have to enter additional information in the “Custom root CA provisioning” section.

- c) The “Part Number details” section enables you to add your project part number (provided to you in the technical support case) to your provisioning file. If you require a custom certificate you will also have to add the manufacturing identity (MAN ID) also provided to you in the support case.

Part Number details

Before generating the Secret Exchange Packet, its required to have MAN-ID and custom Part Number. When customer is availing MCHP provisioning services to load their secrets and certificates, MCHP assigns unique values. These can be requested through support ticket. Refer to [Secret Exchange Process](#) guide for details. For prototyping, one can leave these blank.

Only required if you need a custom certificate

- d) Create your XML provisioning file by clicking on the **Generate TFLXTLS provisioning package** button shown below. This provisioning package is a ZIP file (TFLXTLS_Provisioning_package.zip) that includes

your XML provisioning file as well as C source and header files that can be used with CryptoAuthLib.

The "Generate TFLXTLS provisioning package" button compiles all the data provided in the above slots into zip package containing .xml, .c and .h files.

'xml' file contains TFLXTLS device configuration and the data to be loaded into the slots.

'c, .h' are 'C' source files that are meant to be used with CryptoAuthLib. These files are required to use certificates in CryptoAuthLib.

Generate TFLXTLS provisioning package



After including the data and generating the provisioning package it can be sent to Microchip provisioning service through Microchip Support.

Below link will take you to microchip technical support portal where you can create a new case and send the provisioning package.

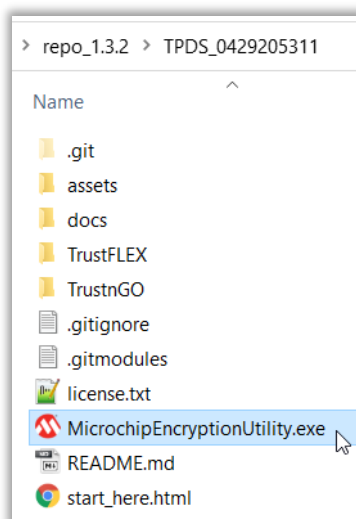
[Microchip Technical Support Portal](#)

Warning:

Your XML provisioning file at this stage contains secrets that are still **not encrypted**. Special handling of the file is required. No configuration files with secret data are to be shared with Microchip under any circumstance.

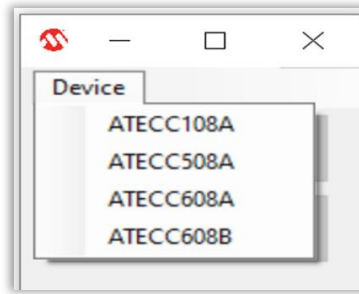
3) Encrypt your provisioning file

Open the Trust Platform repository folder on your computer to find and start the encryption utility (MicrochipEncryptionUtility.exe).

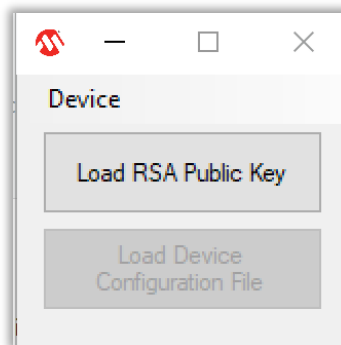


Each manufacturing location generates the RSA key pairs inside its HSM, so you'll need one public key for each location. You will encrypt your provisioning file using each key provided to you (creating one encrypted XML file per key). Each filename must include the manufacturing location name so we know which key goes with each file.

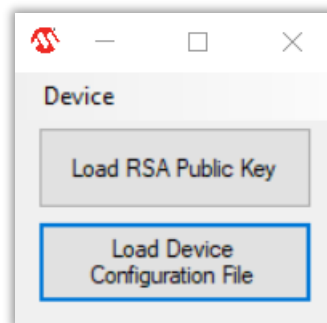
- In the utility, click the **Device** label. A dropdown menu will appear to select the appropriate secure element device.



- b) Click on the **Load RSA Public Key** button and select a public key XML file provided by Microchip via the support ticket.



- c) Extract the **TFLXTLS_Provisioning_package.zip** file you created in the previous step. Click the **Load Device Configuration File** button, browse to the extracted ZIP folder, and select your XML provisioning file.



- d) Another window will open asking you to choose a filename for your encrypted XML provisioning file. Use the following format to create the new file name:
 <project part number>-<RSA key site>.enc.xml (e.g., ATECC608A-MAHxx-COSP-T.enc.xml)

Note:

This Microchip encryption utility doesn't actually encrypt the whole XML file. It only encrypts your secrets. Feel free to open the encrypted file to see what is and is not encrypted.

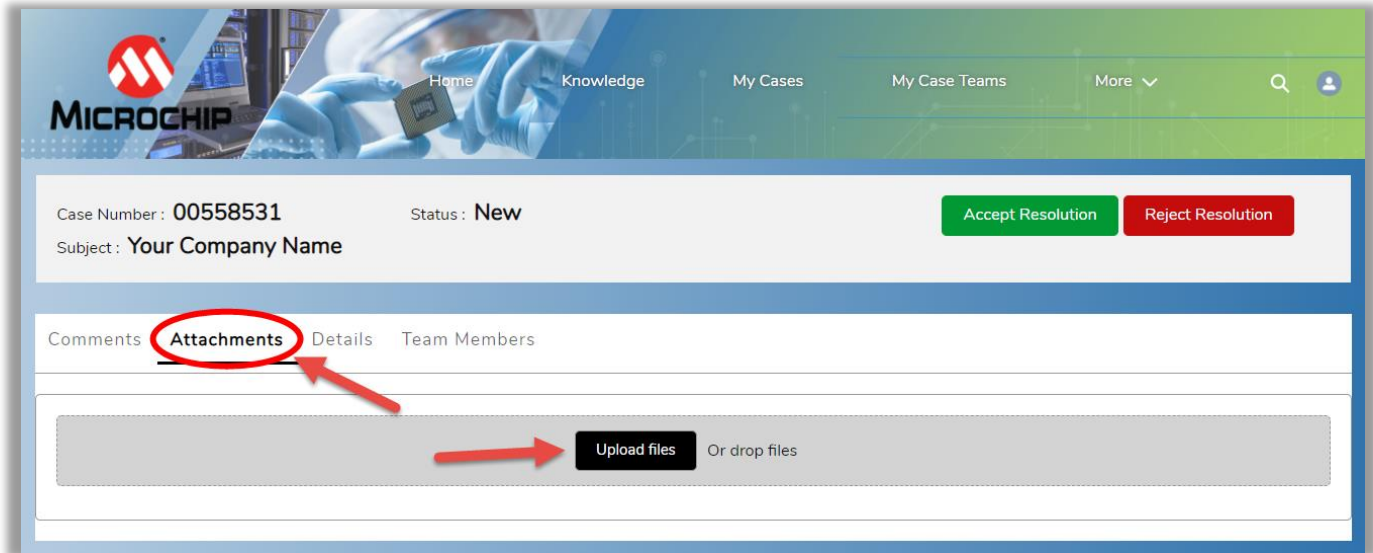
Attention:

Make sure you only upload files that have been encrypted with the Microchip Encryption Utility. Configuration files encrypted via other means cannot be accepted by Microchip.

4) Upload your provisioning file

Use your technical support case to upload your encrypted XML provisioning files. Your support case does not have the ability to upload XML files directly. Please add all your XML files to one ZIP file and upload that file instead.

Open your case, click on **Attachments** then click the **Upload files** button to upload the ZIP file containing your XML files.



Signature Exchange (optional)

If your use case requires a custom certificate, a signature exchange must be completed. This requires a Certificate Authority to be established for the product eco-system. This can be:

- A root certificate authority (with a self-sign certificate).
- An intermediate certificate authority that chains back to the root.

This certificate authority will be used to sign the Microchip production signers which will sign the device certificates.

Microchip will generate Certificate Signing Requests (CSRs) representing the different manufacturing sites (typically 160 CSRs) and upload them in the support case you created. These CSRs will need to be signed and uploaded back to the support case.

Note:

If you are using your own root certificate, careful security provisions must be observed. Protection of the root private key is very important as it forms the backbone of the entire authentication process. Microchip is not responsible for the setup of your root certificate and root private key protection.

Placing Verification Orders

Important Notes for placing orders:

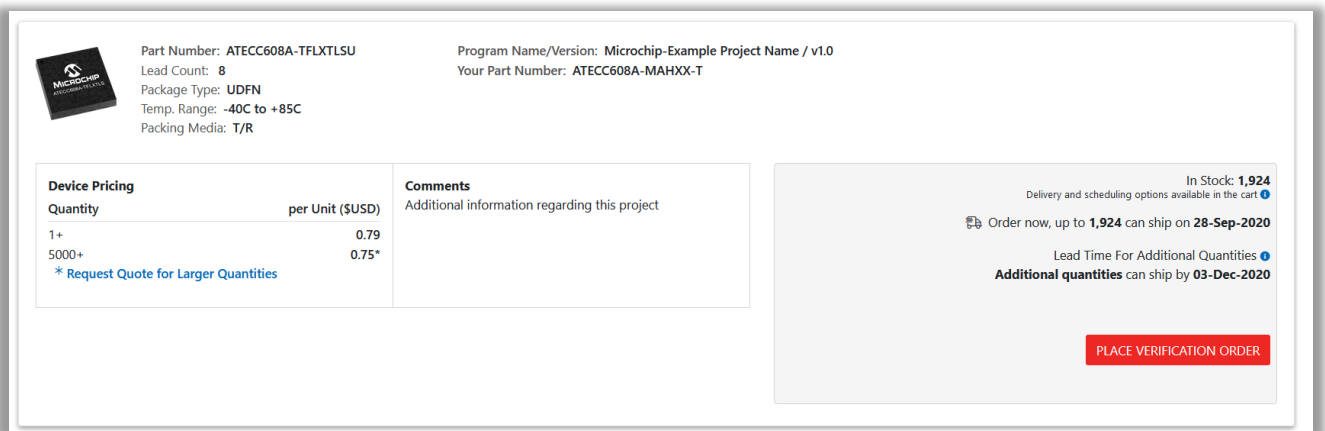
- Your project part number provided to you in your support case *is not a Microchip custom part number* and is not searchable through MicrochipDirect. It cannot be used to directly order units.
- Remember that you control which accounts can order these devices. Only accounts with emails listed in your support case can place orders.
- You will be ordering a standard TrustFLEX device that has your project part number (and therefore your provisioning file) associated with it. You won't be able to order these verification samples until Microchip has set this up for you.
- For distributors: The distributor email account must be the email address associated with the distributor trust account in the region the order will be placed.

After you've uploaded your encrypted provisioning files (and provided signed certificates if your use case requires custom certificates), you will be notified through your support case when provisioned verification samples are ready to be ordered.

- 1) Go to the Microchip Direct Trust Platform Products page and log into your Microchip Direct account:
<https://www.microchipdirect.com/trustplatform>

The page that opens will show your program name, project part number, and other information that was provided in your technical support case.

- 2) Click the **Place verification order** button to request validation samples.



The screenshot displays the Microchip Direct Trust Platform interface. At the top left is the Microchip logo. To its right, the following information is listed: Part Number: ATECC608A-TFLXTLSU, Lead Count: 8, Package Type: UDFN, Temp. Range: -40C to +85C, and Packing Media: T/R. Further right, the Program Name/Version is Microchip-Example Project Name / v1.0, and the Your Part Number is ATECC608A-MAHXX-T.


Below this information is a table with two columns: 'Device Pricing' and 'Comments'. The 'Device Pricing' column contains a sub-table with 'Quantity' and 'per Unit (\$USD)' headers. The 'Comments' column contains the text 'Additional information regarding this project'.

On the right side of the interface, there is a section for stock and shipping information. It states 'In Stock: 1,924' and 'Delivery and scheduling options available in the cart'. Below this, it says 'Order now, up to 1,924 can ship on 28-Sep-2020'. Further down, it indicates 'Lead Time For Additional Quantities' and 'Additional quantities can ship by 03-Dec-2020'. At the bottom right, there is a red button labeled 'PLACE VERIFICATION ORDER'.


Device Pricing		Comments
Quantity	per Unit (\$USD)	Additional information regarding this project
1+	0.79	
5000+	0.75*	

* Request Quote for Larger Quantities

- 3) Once the parts are ordered and are shipped by Microchip, log back into Microchip Direct and click on the **Order History** tab to find the option to **Download Manifest** for the shipped parts. Manifest file format details can be found in the Trust Platform Design Suite.


Order Date	PO Number	Order Status	Web Order Number	Recipient Name	Order Total (USD)
		Part Number: ATECC608A-TFLXLS Customer Part Number: N/A BUY IT AGAIN Cancel or Return Download Manifest		Quantity: 10 Unit Price: Line Total:	
		Line Status: Invoiced Request Arrival Date: 09-Sep-2019 Estimated Ship Date: 18-Sep-2019 Delivery Date: 21-Sep-2019 Shipping Method: FedEx Thailand to USA or US to USA Tracking Number: Invoice Number:			

- 4) Once the verification samples have been successfully validated, log back into Microchip Direct and click on the **Approve** button in the associated project.

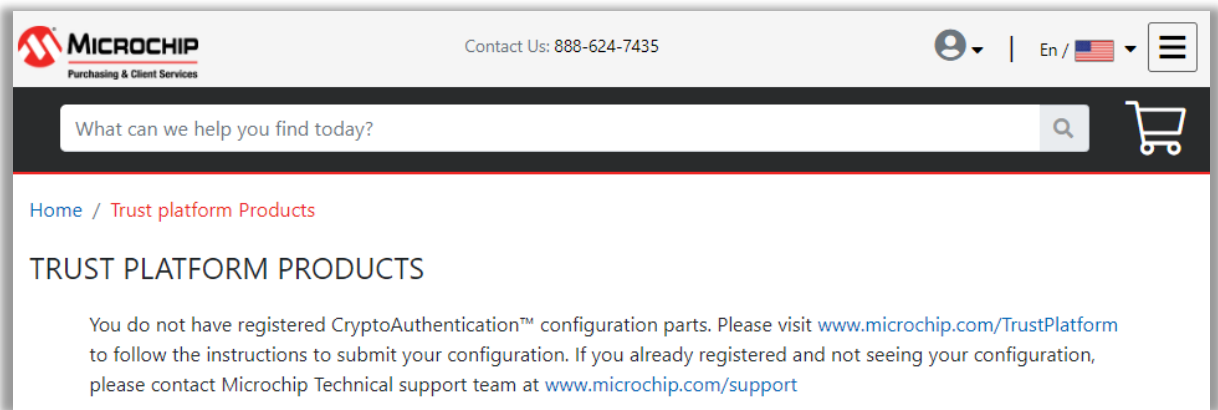
	Part Number: ATECC608A-TFLXLSU Lead Count: 8 Package Type: UDFN Temp. Range: -40C to +85C Packing Media: T/R	Program Name/Version: Microchip-Example Project Name / v1.0 Your Part Number: ATECC608A-MAHXX-T										
<table border="1"> <thead> <tr> <th>Device Pricing</th> <th>Comments</th> </tr> <tr> <th>Quantity</th> <th>per Unit (\$USD)</th> </tr> </thead> <tbody> <tr> <td>1+</td> <td>0.79</td> </tr> <tr> <td>5000+</td> <td>0.75*</td> </tr> <tr> <td colspan="2"> * Request Quote for Larger Quantities </td> </tr> </tbody> </table>		Device Pricing	Comments	Quantity	per Unit (\$USD)	1+	0.79	5000+	0.75*	* Request Quote for Larger Quantities		In Stock: 1,924 Delivery and scheduling options available in the cart i Order now, up to 1,924 can ship on 28-Sep-2020 Lead Time For Additional Quantities i Additional quantities can ship by 03-Dec-2020 PLACE VERIFICATION ORDER APPROVE REJECT
Device Pricing	Comments											
Quantity	per Unit (\$USD)											
1+	0.79											
5000+	0.75*											
* Request Quote for Larger Quantities												

If you log into Microchip Direct without going to the Trust Platform page, you can still order your verification devices, but it's a bit more work:

- Log into the microchipdirect.com main landing page.
- Type the TrustFLEX part number in the "What can we help you find today?" search window (e.g. ATECC608A-TFLXLS). This will open the generic TrustFLEX device page shown below.
- Select the "Please go to pre-provisioned part page to purchase" link. This should then re-direct you to the project ordering page shown above.

Part Number: ATECC608A-TFLXLSU Not Returnable/Cancellable			
Lead Count: 8	Package Type: UDFN	Temp Range: -40C to +85C	Packing Media: Tape and reel (1)
	Standard Pricing: i (Buy Now Price, Any Volume) Order Quantity: 1+ USD per Unit: \$0.79	*Estimated Pricing: i (Requires Approved Quote) Order Quantity: 5000+ USD per Unit: *\$0.75 *Request Quote for Larger Quantities	In Stock: 56,383 Delivery and scheduling options available in the cart i Order now, up to 56,383 can ship on 03-Oct-2020 Lead Time For Additional Quantities i Additional quantities can ship by 10-Dec-2020 Please go to pre-provisioned part page to purchase.
Design Services ▾	Associated Tools ▾	Associated Products ▾	Alternative Products ▾

If you log into a Microchip Direct account with an unregistered email (login email address not sent in the ticket support portal where the secret exchange steps are handled), you will not be able to see the specific configuration but instead will see a page similar to the one shown below. Ask the person that created the technical support case to add your email to the case.



Placing Production Orders

Important Notes for placing orders:

- Your project part number provided to you in your support case *is not a Microchip custom part number* and is not searchable through MicrochipDirect. It cannot be used to directly order units.
- Remember that you control which accounts can order these devices. Only accounts with emails listed in your support case can place orders.
- You will be ordering a standard TrustFLEX device that has your project part number (and therefore your provisioning file) associated with it. You won't be able to order production devices until you have approved your verification samples.
- For distributors: The distributor email account must be the email address associated with the distributor trust account in the region the order will be placed.

- 1) Go to the Microchip Direct Trust Platform Products page and log into your Microchip Direct account:
<https://www.microchipdirect.com/trustplatform>

The page that opens will show your program name, project part number, and other information that was provided in your technical support case.

- 2) Enter the requested order quantity in the project and click on the shopping cart icon.

The screenshot displays the Microchip Direct Trust Platform interface. At the top left, there is a Microchip logo and a list of device specifications: Part Number: ATECC608A-TFLXTL5U, Lead Count: 8, Package Type: UDFN, Temp. Range: -40C to +85C, and Packing Media: T/R. To the right, a red box highlights the 'Program Name/Version: Microchip-Example Project Name / v1.0' and 'Your Part Number: ATECC608A-MAHXX-T'. A red arrow points from the text 'Project Information' to this red box. Below the specifications, there is a table for 'Device Pricing' with columns for 'Quantity' and 'per Unit (\$USD)'. The table shows pricing for 1+ units at 0.79 and 5000+ units at 0.75*. A link for '* Request Quote for Larger Quantities' is also present. To the right of the pricing table is a 'Comments' section. On the far right, there is a section for 'In Stock: 1,924' and 'Delivery and scheduling options available in the cart'. It states 'Order now, up to 1,924 can ship on 28-Sep-2020' and 'Lead Time For Additional Quantities: Additional quantities can ship by 03-Dec-2020'. At the bottom right, there is a 'Quantity' input field with a red box around it and a shopping cart icon. The text 'a minimum of 2000' is displayed below the input field.

Quantity	per Unit (\$USD)
1+	0.79
5000+	0.75*

* Request Quote for Larger Quantities

Comments: Additional information regarding this project

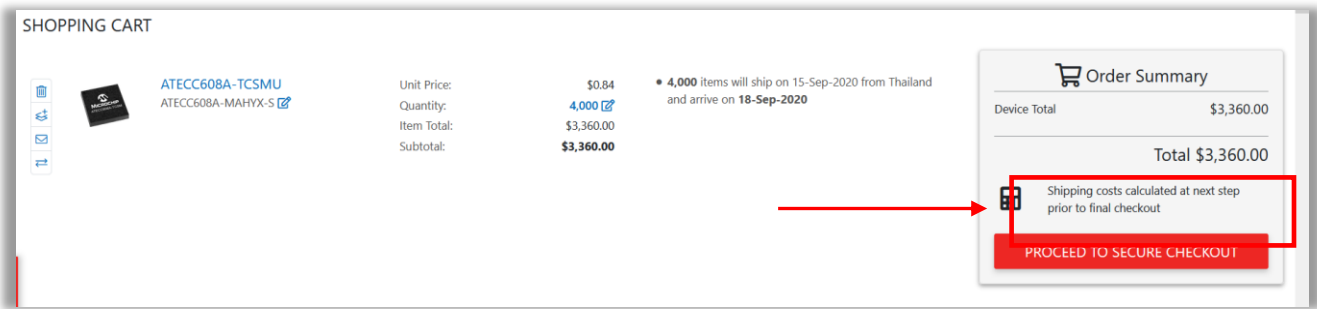
Quantity: a minimum of 2000

Note: The minimum order quantity (MOQ) for this device is 2k units.

- 3) Click on the shopping cart at the top of the page to review the shopping cart

The screenshot shows the top navigation bar of the Microchip Direct website. It includes the Microchip logo, contact information (888-624-7435), and a user profile dropdown labeled 'Microchip Demo'. There are links for 'PRODUCTS', 'VOLUME PRICING', 'PROGRAMMING SERVICES', and 'UTILITIES'. A search bar is present with the placeholder text 'What can we help you find today?'. On the right, there is a 'HOW CAN WE HELP?' section with links for 'Quote Status' and 'Request a Quote'. A shopping cart icon is highlighted with a red circle, showing '(1)' item and a total of '\$3,360.00'. The bottom of the header shows the breadcrumb 'Home / Trust platform Products'.

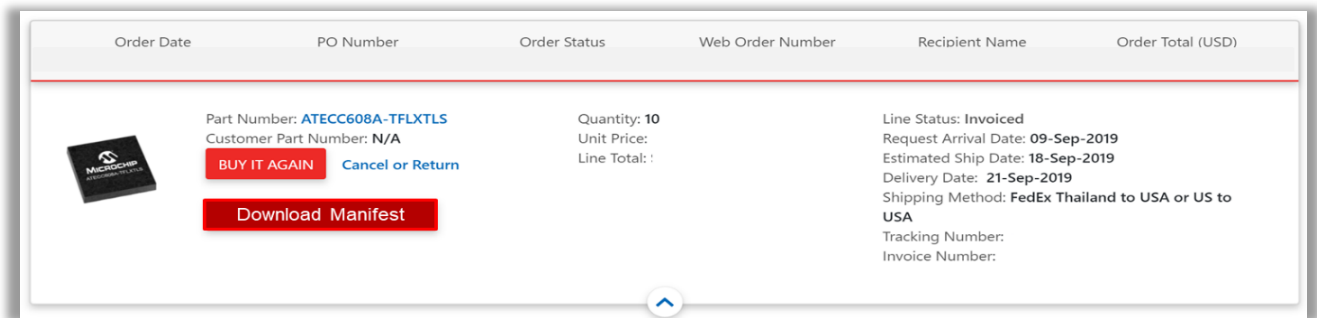
4) Click the “PROCEED TO SECURE CHECKOUT” button.



5) Once the parts are ordered and are shipped by Microchip, log back into Microchip Direct and click on the Order History tab to find the option to Download Manifest for the shipped parts.

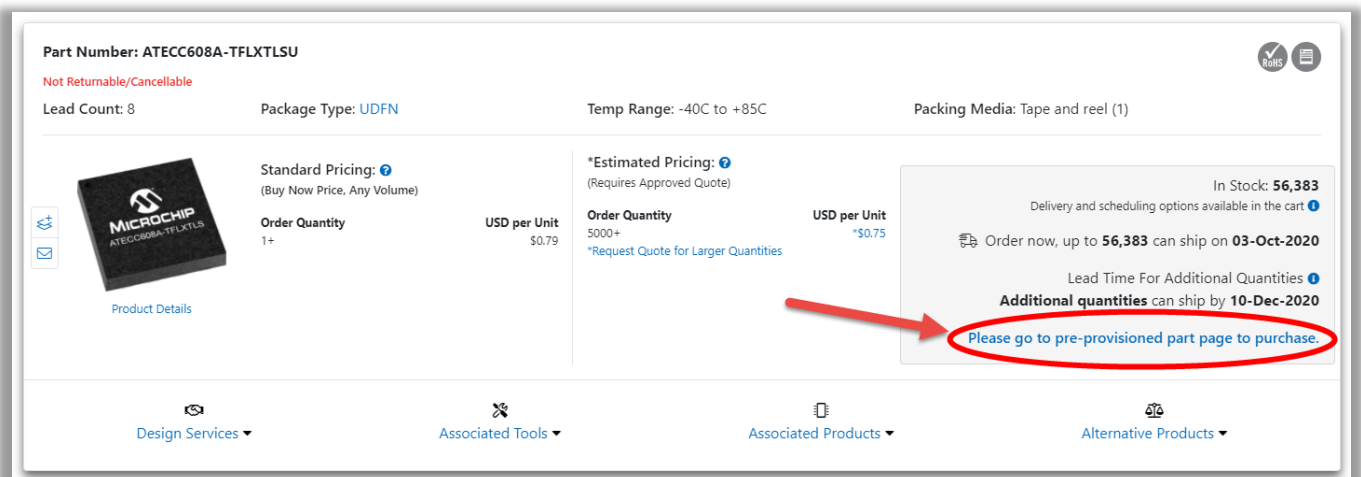
Note:

Manifest file format details can be found in the Trust Platform Design Suite.

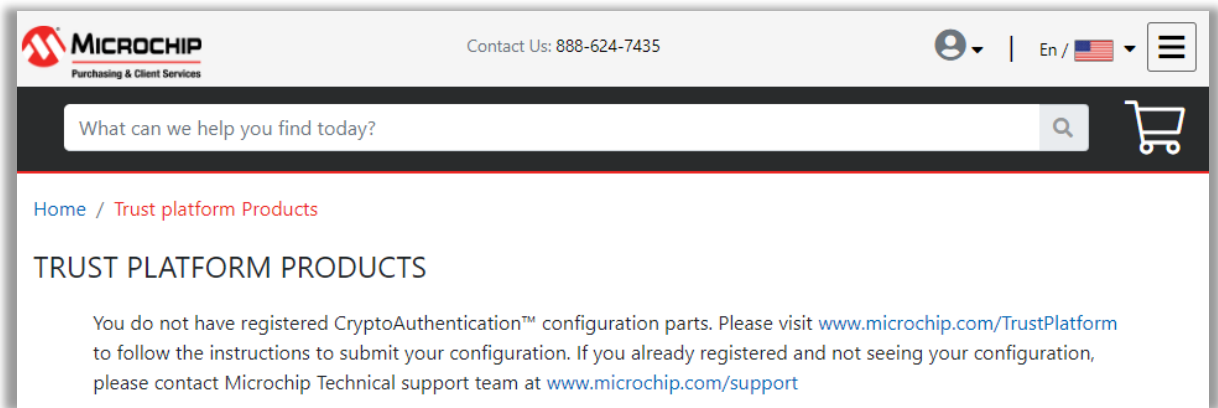


If you log into Microchip Direct without going to the Trust Platform page, you can still order your production devices, but it’s a bit more work:

- Log into the microchipdirect.com main landing page.
- Type the TrustFLEX part number in the “What can we help you find today?” search window (e.g. ATECC608A-TFLXTLS). This will open the generic TrustFLEX device page shown below.
- Select the “Please go to pre-provisioned part page to purchase” link. This should then re-direct you to the project ordering page shown above.



If you log into a MicrochipDirect account with an unregistered email (login email address not sent in the ticket support portal where the secret exchange steps are handled), you will not be able to see the specific configuration but instead will see a page similar to the one shown below. Ask the person that created the technical support case to add your email to the case.



The Microchip Web Site

Microchip provides online support via our web site at <http://www.microchip.com/>. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Customer Change Notification Service

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at <http://www.microchip.com/>. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or Field Application Engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: <http://www.microchip.com/support>

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the

code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, AnyRate, AVR, AVR logo, AVR Freaks, BitCloud, chipKIT, chipKIT logo, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, Helder, JukeBlox, KeeLoq, Kleeer, LANCheck, LINK MD, maXStylus, maXTouch, MediaLB, megaAVR, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, Prochip Designer, QTouch, SAM-BA, SpyNIC, SST, SST Logo, SuperFlash, tinyAVR, UNI/O, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

ClockWorks, The Embedded Control Solutions Company, EtherSynch, Hyper Speed Control, HyperLight Load, IntelliMOS, mTouch, Precision Edge, and Quiet-Wire are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, EtherGREEN, In-Circuit Serial Programming, ICSP, INICnet, Inter-Chip Connectivity, JitterBlocker, KleeerNet, KleeerNet logo, memBrain, Mindi, MiWi, motorBench, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICKit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, SAM-ICE, Serial Quad I/O, SMART-I.S., SQI, SuperSwitcher, SuperSwitcher II, Total Endurance, TSHARC, USBCheck, VariSense, ViewSpan, WiperLock, Wireless DNA, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

Silicon Storage Technology is a registered trademark of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

© 2018, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

ISBN:

Quality Management System Certified by DNV

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.