
Secret Exchange for TrustFLEX Platform

Overview:

This document explains the steps involved in secret exchange, Certificate signing and creating a support case to track the status of the secure provisioning of the TrustFLEX device selected.

If this document is being followed, then the following steps must have been completed:

- Defined the application and the use case with the Trust Platform Design Suite and ready to order pre-provisioned secure elements from Microchip with “production based crypto keys”
- myMicrochip account has been setup.

This document covers detailed steps that are carried out for Microchip to provision the TrustFLEX devices to the user-defined specifications.

1. myMicrochip Account Creation:

- If the account already exists, then you can skip this step.
- Create the myMicrochip account by clicking [HERE](#)
- Enter the details and complete the registration.
- There will be email confirming link sent to the email used for the registration.

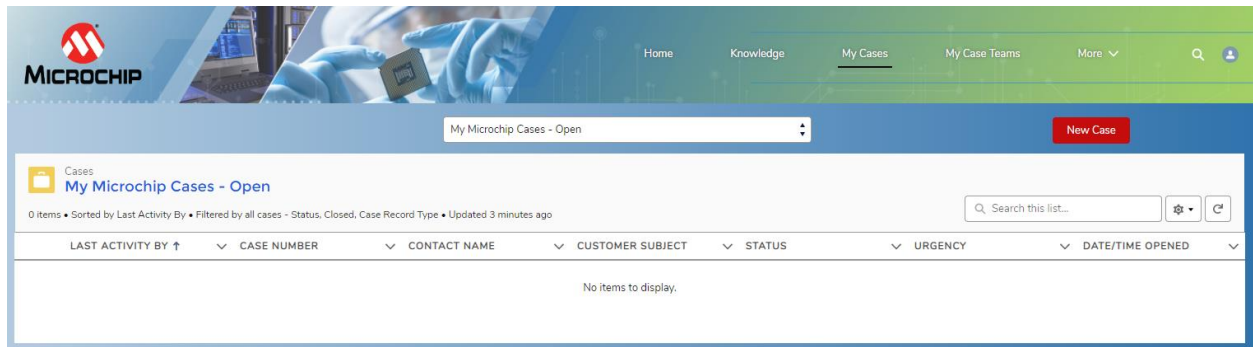
2. Support Case Creation:

- Once the account is created, the next step is to create support case

- Visit the Microchip [Case Console](#). Log in with the email address used to create the myMicrochip account

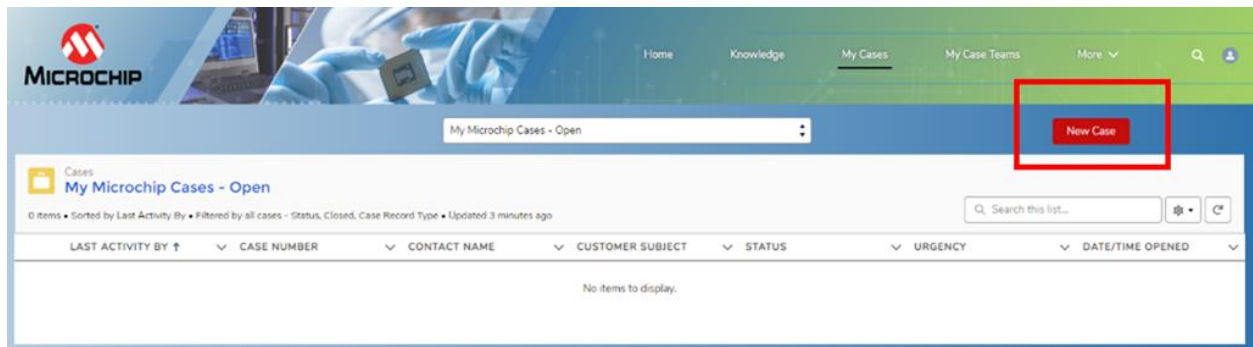
Note: The URL can also be visited in the later stage to check the support case status.

Fig 2.1: Login Page for the support case console



- Click on the New Case option on the top right corner of the page.

Fig 2.2: New Case



- Now select “Value Added Services” and then click on Next.

Fig 2.3: Selecting options

Let us know how we can help you

Case Reason*

<input type="radio"/> Hardware/Firmware Support <i>(Device, Peripherals, Modules, Code examples, Demo boards, Evaluation kits.)</i>	<input type="radio"/> Software Library <i>(Harmony, Touch Library, Advanced Software Framework (ASF), Atmel Start, MPLAB® Code Configurator, Microchip Library of Applications, Bootloaders, Baremetal Softpack, Linux OS and drivers)</i>
<input type="radio"/> Development Tools <i>(Development Environment - IDE, Compilers, Debugger, Emulator, Programmer)</i>	<input type="radio"/> Documentation <i>(Datasheet, Errata, Application Notes, FRM, EOL, Soldering, Packaging, demo/kit design files)</i>
<input type="radio"/> Quality/Reliability <i>(FIT, MTBF, MSL, RMA, Field Failures, MSL)</i>	<input type="radio"/> Product Selection <i>(Help to select suitable product)</i>
<input type="radio"/> Website Issues <i>(Support website related issues.)</i>	<input checked="" type="radio"/> Value Added Services <i>(Design Check, Secure Provisioning)</i>

Next Cancel

- In the subject line enter the company details, select the target device, enter “Provisioning Services” in the category selection, and “Secure Provisioning” in sub-category. Then click Next.

Fig 2.4: Adding the details

The screenshot shows the Microchip support portal interface. At the top, there's a header with the Microchip logo and navigation links for 'Home' and 'Knowledge'. Below this is a 'CREATE CASE' section with a briefcase icon and the text 'New Support Case (Step 2 of 4)'. A red asterisk indicates that certain fields are required. The main form area is titled 'Provide more specific information' and contains four input fields: 'Subject' (text box with 'JKLM Manf Custom provisioning Support'), 'Target Device' (text box with 'ATECC608A'), 'Category' (dropdown menu with 'Provisioning Services'), and 'Sub-Category' (dropdown menu with 'Secure Provisioning'). At the bottom right of the form are three buttons: 'Previous', 'Next' (highlighted in red), and 'Cancel'.

- In the Ticket Description, Enter the following details:
 - **Program Name:** This will be a short name that will help in differentiating the specific TrustFLEX configuration from several other TrustFLEX configurations present.
 - **Version Number:** This will be a shot number that will help to differentiate different configurations under the same program name.
 - **Comments:** This is a short description that will be displayed on the E-Commerce portal, that will help describe more about the program.
 - **MicrochipDirect Email address:** Please provide the email address that is used to register at www.microchipdirect.com this email address will be used to authorize the purchase of the product that contains the configuration/secrets that will be provides in this ticket portal.

Note: Please ensure that you provide correct email address(es), as this will be the only account that will be authorized to purchase product with the shared secret

Fig 2.5: Adding Description

Describe your issue here

Please add your issue description here*

I am working on an Trust Flex device and here are some of the details:

- I am using symmetric key slot. Please provide encryption keys for me to encrypt the file
- I am also using custom PKI certificate chain for device certificates.
- Please send the MAN ID
- List of CSRs (Certificate Signing Requests) for me to sign them with our Root key

Here are our program details:

- Program: xxxxxxxx
- Version: yy
- MicrochipDirect Registered Email address: zzzzzzzz@
- Comments: <Details of the program>

31225 characters remaining

Microchip provides Secure Factory Provisioning services for the ATECC608A, ATECC508A, and ATSHA204A family of CryptoAuthentication devices. Use this category to request information or service for Secure Factory Provisioning.

Previous Next Cancel

- The Design Stage and Urgency are default entered. They can be changed as required. Enter any other required information in Application Details option and click on “Submit”.

Fig 2.6: Project Information

Project Information

Design Stage*

Development

Urgency*

Moderate

Application Details

<Provide Application Details and any other information that will help MCHP team provide quicker response>

115 characters remaining

Previous Submit Cancel

- Once submitted, if there are any files to be uploaded it can be done now and then click “Done”.

Note: Make sure that while uploading the file, it must be encrypted with the RSA keys provided by Microchip that will be shared in the system. Uploading an unencrypted file leads to the probability of exposing the customer's sensitive data.

Fig 2.7: Final Submitted Page

The screenshot shows a light blue header with a paperclip icon and the text 'Attach Files'. Below this is a green banner with the text 'Case has been successfully submitted, please add your attachments.' Underneath the banner is a grey dashed box containing an 'Upload files' button with an upward arrow icon and the text 'Or drop files'. At the bottom right of the section are two buttons: a green 'Done' button and a white 'Skip' button with a grey border.

- Case home page after the case is created.

Fig 2.8: Case Homepage

The screenshot shows a case homepage with a light blue header. The header contains the case number '00463807', the subject 'JKLM Manf Custom provisioning Support', and the status 'New'. To the right of the status are two buttons: a green 'Accept Resolution' button and a red 'Reject Resolution' button. Below the header is a tabbed interface with 'Related' selected. Under the 'Related' tab, there are two main sections. The first is 'Case Comments', which has a blue header and an 'Add Comment' button. Below this is a 'COMMENT' input field. The second section is 'Files and Attachments (0)', which has a blue header and an upload area with 'Upload files' and 'Or drop files' options.

- Questions and comments can be added by clicking on the “Add Comment” option.

3. Secret Exchange:

- In order to begin with the Secret Exchange, user will have to enter their final production based crypto keys in the TrustFlex Configurator Tool that is available in the Trust Platform Design Suite.

- If custom PKI certificate option is selected, the tool will require you to enter MAN ID (Manufacturing ID).
 - You will receive this ID information in the support ticket from MCHP
- Once all crypto keys and details are entered in the TrustFlex Configurator tool, you can click on 'Generate TFLXTLS Provisioning Package' and this will download the XML file along with a few source files that are meant to be integrated into the embedded firmware project.
- Please note that the XML file at this stage contains secrets that are still not encrypted and so special handling of the file is required at this stage
 - The utility to encrypt the XML can be found in Trust Platform installation directory i.e. Users directory\DesignTools\ MicrochipEncryptionUtility.exe
- Microchip will send RSA encryption keys via support ticket portal, which are the public keys for the production HSMs (Hardware Security Module). This key should be used along with the XML file in a encryption utility that is also provided by MCHP and this generates an encrypted version of the XML file.
- The secrets that are entered in the XML file, once encrypted can only be decrypted by our process inside the protected memory of the HSM. They are never exposed.

Note: The unencrypted XML file having the secrets must be stored in a safe and secure location. Microchip does not take responsibility of the un-encrypted XML file.

4. Signature Exchange:

- Along with secret exchange, signature exchange must also be implemented if custom PKI certificate option is selected in the TrustFlex configurator.

Note: This step is required, if the user selects custom Certificate option in the TFLX configurator

Slot 10 Device compressed certificate Certificate primary public key in the Crypto Authentication compressed format Clear read, No write

SLOT 10

Slot Description:
Device compressed certificate is stored in this slot. This slot is written with certificate signed by Microchip signers and root.

It's permanent to support a "factory reset" option where the original credentials are always available. It also prevents Denial-Of-Service attacks where the cert is changed, either intentionally or by accident.

Provisioning:
The slot is provisioned by Microchip with its own root and signers. There are two options that customers can choose from (Microchip Standard Certificate or Custom certificate).

1. *Microchip standard certificate: Certificate elements like name, date, country..... will be filled by Microchip. The certificate will be signed with Microchip signers.*
2. *Custom Certificate: This option will allow the customer to define some of the certificate elements like name and data.*

Due to the way the certificates are stored/retrieved from the ECC608 device, using Custom certificates will require some knowledge on compressed certificates and certificate templates.

Select device certificate type:
☐ Microchip Standard Certificate
☒ Custom Certificate

- This requires a Certificate Authority to be established for the product eco-system.
 - Can be a root certificate authority (with self-sign certificate)
 - 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.
- If the own root certificate is established careful security provisions must be observed. Protection of the root private key is of at most importance as it forms the backbone of the entire authentication process.

Note: Microchip is not responsible for setting up of the root certificate and root private key protection.


- Microchip generates the signer certificates for our production signers to be used for the provisioning of the devices.
- Once the signer certificates are signed by the root signer they are locked and cannot be modified. These signed certificates will be sent back to Microchip.
- Microchip uses a large array of signers in parallel to get the throughput required for the production. Approximately 80-160 signers will be used depending on the volume.

5. Next Steps:

- Once MCHP onboards the configuration file, then we will respond back on the support case for you to proceed with ordering verification samples and the production units.
- There will be a default of 20 verification samples that will be shipped. If more than 20 samples are needed, then it must be mentioned in the description.
- Log into the microchipdirect.com account (with the email address provided in the case that is associated with the configuration file) and there will be a screen as shown below.

Fig 5.1: MicrochipDirect Device Page

PRODUCTION PARTS



Part Number: ATECC608A-TFLXTLSS-B
Lead Count: 8
Package Type: SOIC
Temp. Range: -40C to +85C
Packing Media: TUBE

Program Name/Version:
Customer Part Number:

Device Pricing		Comments
Quantity	per Unit (\$USD)	
1-25	1.32	
26-99	1.32	
100-999	1.32	
1000+	1.32*	
* Request Quote for Larger Quantities		

Estimated Ship Date: 18-Nov-2019

PLACE VERIFICATION ORDER


- By clicking on the “Place verification order” button, the verification parts can be ordered for confirming if it works with the application.
- Once the parts are tested and they are successfully working with the application, then log back to MicrochipDirect and click on Approve or Reject the verification samples.

- If approved is selected, then there will be screen as shown below where the production orders can be placed.

Note: For the TrustFLEX devices the minimum order quantity is 2000 units. Each order can contain any number of units above 2000. There will be MoQ limit for every order.

Fig 5.2: Ordering Production Parts


PRODUCTION PARTS



Part Number: ATECC608A-TFLXTL55-B
 Lead Count: 8
 Package Type: SOIC
 Temp. Range: -40°C to +85°C
 Packing Media: TUBE

Program Name/Version:
 Customer Part Number:

Device Pricing		Comments
Quantity	per Unit (\$USD)	
1-25	1.32	
26-99	1.32	
100-999	1.32	
1000+	1.32*	
* Request Quote for Larger Quantities		

Estimated Ship Date: 18-Nov-2019
 Quantity: 1 
 A minimum of 2000

- Once the parts are ordered and are shipped by Microchip, log back into MicrochipDirect and in the “Order History” tab there will be an option to “Download Manifest File” for the shipped parts that contain the pre-provisioned secrets.

Fig 5.3: Ordering the Manifest file

Order Date	PO Number
	<p>Part Number: ATECC608A-MAH Customer Part Number: N/A</p> <p>BUY IT AGAIN</p> <p>Download Manifest File</p>

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, Klear, 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, KlearNet, KlearNet 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.

ISBN:

Quality Management System Certified by DNV

ISO/TS 16949

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.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: http://www.microchip.com/support Web Address: www.microchip.com Atlanta Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 Austin, TX Tel: 512-257-3370 Boston Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 Chicago Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 Dallas Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 Detroit Novi, MI Tel: 248-848-4000 Houston, TX Tel: 281-894-5983 Indianapolis Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 Los Angeles Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 Raleigh, NC Tel: 919-844-7510 New York, NY Tel: 631-435-6000 San Jose, CA Tel: 408-735-9110 Tel: 408-436-4270 Canada - Toronto Tel: 905-695-1980 Fax: 905-695-2078	Australia - Sydney Tel: 61-2-9868-6733 China - Beijing Tel: 86-10-8569-7000 China - Chengdu Tel: 86-28-8665-5511 China - Chongqing Tel: 86-23-8980-9588 China - Dongguan Tel: 86-769-8702-9880 China - Guangzhou Tel: 86-20-8755-8029 China - Hangzhou Tel: 86-571-8792-8115 China - Hong Kong SAR Tel: 852-2943-5100 China - Nanjing Tel: 86-25-8473-2460 China - Qingdao Tel: 86-532-8502-7355 China - Shanghai Tel: 86-21-3326-8000 China - Shenyang Tel: 86-24-2334-2829 China - Shenzhen Tel: 86-755-8864-2200 China - Suzhou Tel: 86-186-6233-1526 China - Wuhan Tel: 86-27-5980-5300 China - Xian Tel: 86-29-8833-7252 China - Xiamen Tel: 86-592-2388138 China - Zhuhai Tel: 86-756-3210040	India - Bangalore Tel: 91-80-3090-4444 India - New Delhi Tel: 91-11-4160-8631 India - Pune Tel: 91-20-4121-0141 Japan - Osaka Tel: 81-6-6152-7160 Japan - Tokyo Tel: 81-3-6880-3770 Korea - Daegu Tel: 82-53-744-4301 Korea - Seoul Tel: 82-2-554-7200 Malaysia - Kuala Lumpur Tel: 60-3-7651-7906 Malaysia - Penang Tel: 60-4-227-8870 Philippines - Manila Tel: 63-2-634-9065 Singapore Tel: 65-6334-8870 Taiwan - Hsin Chu Tel: 886-3-577-8366 Taiwan - Kaohsiung Tel: 886-7-213-7830 Taiwan - Taipei Tel: 886-2-2508-8600 Thailand - Bangkok Tel: 66-2-694-1351 Vietnam - Ho Chi Minh Tel: 84-28-5448-2100	Austria - Wels Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 Denmark - Copenhagen Tel: 45-4450-2828 Fax: 45-4485-2829 Finland - Espoo Tel: 358-9-4520-820 France - Paris Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 France - Saint Cloud Tel: 33-1-30-60-70-00 Germany - Garching Tel: 49-8931-9700 Germany - Haan Tel: 49-2129-3766400 Germany - Heilbronn Tel: 49-7131-67-3636 Germany - Karlsruhe Tel: 49-721-625370 Germany - Munich Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 Germany - Rosenheim Tel: 49-8031-354-560 Israel - Ra'anana Tel: 972-9-744-7705 Italy - Milan Tel: 39-0331-742611 Fax: 39-0331-466781 Italy - Padova Tel: 39-049-7625286 Netherlands - Drunen Tel: 31-416-690399 Fax: 31-416-690340 Norway - Trondheim Tel: 47-7289-7561 Poland - Warsaw Tel: 48-22-3325737 Romania - Bucharest Tel: 40-21-407-87-50 Spain - Madrid Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 Sweden - Gothenberg Tel: 46-31-704-60-40 Sweden - Stockholm Tel: 46-8-5090-4654 UK - Wokingham Tel: 44-118-921-5800 Fax: 44-118-921-5820