Description

The PL360 is a programmable modem for narrow-band Power Line Communication (PLC), able to run any PLC protocol in the frequency band below 500 kHz.

This device has been designed to comply with FCC, ARIB, KN60 and CENELEC EN50065 regulations matching requirements of Internet of Things and Smart Energy applications. It supports state-of-the-art narrow-band PLC standards such as ITU G.9903 (G3-PLC), ITU G.9904 (PRIME) as well as any other narrow-band PLC protocols, at the same time being a future-proof platform able to support the evolution of these standards.

The PL360 has been conceived to be driven by external Microchip host devices, thus providing an additional level of flexibility on the host side. The Microchip host device loads the proper PLC-protocol firmware before modem operation and controls the PL360 modem.

Security Features

• Cryptographic Engine and Secure Boot
  – AES 128, 192, 256 supported
  – Secure boot: supports AES-128 CMAC for authentication, AES-128 CBC for decryption
  – One-time programmable fuses programming control for decryption and authentication 128-bit keys
# Table of Contents

Description.......................................................................................................................1

Security Features............................................................................................................ 1

1. PL360 Security Features........................................................................................... 3

2. Hardware Requirements for Fuse Programming.......................................................4

3. How to Program the Fuses........................................................................................5
   3.1. OTP Fuses Registers...............................................................................................5
   3.2. Interface and Protocol............................................................................................5
   3.3. PHY Fuses Tool Embedded Application...............................................................7

4. How to Encrypt and Sign the PL360 Binary............................................................ 10
   4.1. Introduction.............................................................................................................10
   4.2. Encrypt and Sign Script.........................................................................................11

5. How to Include Secure Boot on Firmware Application.............................................13

6. Appendix A. How to Generate Keys Using Signature Functions.........................15

7. Revision History.......................................................................................................16
   7.1. Rev A - 07/2018....................................................................................................16

The Microchip Web Site.................................................................................................17

Customer Change Notification Service.........................................................................17

Customer Support........................................................................................................17

Microchip Devices Code Protection Feature...............................................................17

Legal Notice..................................................................................................................18

Trademarks...................................................................................................................18

Quality Management System Certified by DNV..........................................................19

Worldwide Sales and Service.......................................................................................20
1. **PL360 Security Features**

The PL360 contains a Secure Boot mechanism that guarantees the secure transfer of the firmware binary. To achieve this advanced functionality, the PL360 includes the following blocks:

- AES-CMAC: allows signature verification of binaries loaded on PL360
- AES-CBC: allows decryption of binaries loaded on PL360
- OTP Fuses block:
  - KEY_TAG: 128b signature key used to verify signature of binary
  - KEY_ENC: 128b encryption key used to decrypt binary
  - CONTROL_FUSES: 128b Control Fuse key for configuration

PL360 contains a One-Time-Programmable (OTP) fuses block which is a series of nonvolatile memory registers that can only be programmed once and where data is stored permanently.

The figure below shows the structure of the registers and data transfers for fuses and their control logic.

**Figure 1-1. Fuse Controller Structure**

To take advantage of the security capabilities of PL360, the following processes are involved:

- Program the KEY_TAG, KEY_ENC and CONTROL_FUSES fuses blocks
- Sign and encrypt the corresponding PL360 binary with KEY_TAG and KEY_ENC
- Include Secure Boot capabilities in the host application

The following sections describe each one of those processes in detail.
2. **Hardware Requirements for Fuse Programming**

To be able to permanently modify the control or key fuses, an external supply of DC 2.5V ±10% 50 mA must be connected to the VZC pin. If the programming is done in system, an adequate protection of the VZC circuitry should be implemented by means of a 10K resistor, as shown in the figure below:

*Figure 2-1. Hardware Requirements for Fuse Programming*

The PL360MB-EK evaluation kit is prepared for fuses programming. To generate the voltage of 2.5V to the VZC pin in the PL360MB board, it is necessary to mount the components shown in the figure below:

*Figure 2-2. Fuses Programming in PL360MB-EK*

The fuse programming commands are sent through SPI. In case of using an external fuses programming controller, the SPI port pins of the host MCU must be set in High Impedance mode as to not interfere in the connection between PL360 and the external fuses programming controller.
3. **How to Program the Fuses**

3.1 **OTP Fuses Registers**

PL360 contains an OTP fuses block which is a series of nonvolatile memory registers that can only be programmed once and where data is stored permanently. In this OTP fuses block, there are several 128-bit registers related to security.

KEY_TAG and KEY_ENC are 128-bit registers used by the AES128-CMAC and AES128-CBC modules inside the PL360 Bootloader to store the keys when Secure Boot is enabled in order to verify the signature and decrypt the loaded binary.

CONTROL_FUSES is a 128-bit fuse register that controls the security features of PL360. Only some of the bits are user-configurable as shown on the next table:

<table>
<thead>
<tr>
<th>Fuse Bit</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ENCRNOTPLAIN</td>
<td>If it is set, Secure mode is active. Only encrypted and signed binaries with the correct keys will be accepted by the bootloader</td>
</tr>
<tr>
<td>1</td>
<td>READ_AES_KEY</td>
<td>If it is set, KEY_ENC and KEY_TAG can't be read</td>
</tr>
<tr>
<td>2</td>
<td>WRITE_AES_KEY</td>
<td>If it is set, KEY_ENC and KEY_TAG can't be written</td>
</tr>
<tr>
<td>5</td>
<td>READ_CONTROL</td>
<td>If it is set, CONTROL_FUSES can't be read</td>
</tr>
<tr>
<td>6</td>
<td>WRITE_CONTROL</td>
<td>If it is set, CONTROL_FUSES can't be written</td>
</tr>
<tr>
<td>7</td>
<td>READ_RAM</td>
<td>If it is set, RAM memory can't be read</td>
</tr>
<tr>
<td>10</td>
<td>FORCE_IVNBINC</td>
<td>If it is set, initialization vector and number of blocks must be used in the calculation of the signature</td>
</tr>
<tr>
<td>16</td>
<td>DBG_DISABLE</td>
<td>If it is set, JTAG debug is disabled</td>
</tr>
</tbody>
</table>

3.2 **Interface and Protocol**

The bootloader interface with host controller is a SPI bus which works in SPI Mode 0 (CPHA=1 and CPOL=0). The basic data transfer is:
The bootloader requires a specific SPI frame format in order to interact with PL360 Bootloader to send commands and receive data. The SPI frame format used is shown in the following table:

**Table 3-2. Bootloader SPI Frame Format**

<table>
<thead>
<tr>
<th>Address</th>
<th>Command</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>32 bits</td>
<td>16 bits</td>
<td>n words of 32 bits</td>
</tr>
</tbody>
</table>

The PL360 bootloader implements the following SPI commands related to the security features of PL360:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Addr(31:0)</th>
<th>DATA(n*32-1:0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0007</td>
<td>Write 128 bits fuses value to the Buffer register</td>
<td>0x00000000</td>
<td>0xDDDDDDDDDDD</td>
</tr>
<tr>
<td>0x0008</td>
<td>Write Buffer register to the Tamper register for KEY_ENC_FUSES</td>
<td>0x00000000</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0x0009</td>
<td>Write Buffer register to the Tamper register for KEY_TAG_FUSES</td>
<td>0x00000000</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0x000B</td>
<td>Write Buffer register to the Tamper register for CONTROL_FUSES</td>
<td>0x00000000</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0x000C</td>
<td>Blow desired fuses</td>
<td>0x00000000</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0x000D</td>
<td>Write KEY_ENC_FUSES to the corresponding Tamper register</td>
<td>0x00000000</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0x000E</td>
<td>Write KEY_TAG_FUSES to the corresponding Tamper register</td>
<td>0x00000000</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0x0010</td>
<td>Write CONTROL_FUSES to the corresponding Tamper register</td>
<td>0x00000000</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0x0011</td>
<td>Read Tamper register</td>
<td>0x00000000</td>
<td>0x000...000</td>
</tr>
<tr>
<td>0x0012</td>
<td>Read bootloader status</td>
<td>0x00000000</td>
<td>0x00000000</td>
</tr>
</tbody>
</table>

To write a fuse box, the data must be written in advance in the Buffer register (CMD=0x0007) and then, the content of the buffer written on the Tamper registers KEY_ENC_BOX, KEY_TAG_BOX or
CONTROL_BOX by means of the corresponding command (CMD=0x0008, CMD=0x0009 and CMD=0x000B respectively).

As the last step, to blow the desired fuses with the values in the corresponding Tamper register, the command (CMD=0x000C) must be sent. It’s necessary to check the bootloader status (CMD=0x0012) to know when this writing process finishes. If the writing process is active, bit 0 of the answer is ‘1’; in any other case, all data of the answer is ‘0’.

To activate the features controlled by CONTROL_FUSES, it is necessary to write the CONTROL_FUSES values to the corresponding Tamper register (CMD=0x0010).

To read the fuses registers KEY_ENC, KEY_TAG or CONTROL_FUSES, it is necessary to write their content to the Tamper register using the corresponding command (CMD=0x000D, CMD=0x000E and CMD=0x0010 respectively). After that, it is possible to read the Tamper register (CMD=0x0011) with the desired fuses register value.¹

Note:
1. More information about this process can be found in the PL360 Datasheet.

3.3 PHY Fuses Tool Embedded Application

Microchip provides a firmware project example for the PL360 Evaluation Kit named “PHY Fuses Tool” in folder “thirdparty\PROTOCOL\phy\atpl360\apps\phy_fuses_tool” that could be used for fuse programming. The folder “common\components\plc\atpl360\mnf” contains the functions related to fuse programming.

Figure 3-2. PHY Fuses Tool Project Tree

When the firmware runs in the PL360MB-EK, the LCD shows the message “Phy fuses tool”.

Figure 3-3. LCD Content for PHY Fuses Tool Firmware on PL360MB Evaluation Kit

Then, connect the board’s USB-Serial port to a computer running a serial terminal application configured as 115200-8-N-1, no flow control. That will provide access to the embedded console menu, displayed after reset or when pressing Enter.
For information about how to generate the 128-bit keys see 6. Appendix A. How to Generate Keys Using Signature Functions.

To program the ENC_KEY, select option 4 in console menu. ENC_KEY must be in hexadecimal format (32 hexadecimal characters).

To program the TAG_KEY, select option 6 in console menu. TAG_KEY must be in hexadecimal format (32 hexadecimal characters).

Tip: Press ‘ESC’ in order to cancel the programming operation.

To program CONTROL_FUSES, select option 2 in console menu. CONTROL_FUSES must be in hexadecimal format (8 hexadecimal characters).
Important: Since only fuses bits from 0 to 17 are user configurable, CONTROL_FUSES mask is 8 hexadecimal characters.

Figure 3-7. CONTROL_FUSES Fuse Programming

```
FUSES-Console> Enter FUSES mask: 0x00010007
Write CTRL_FUSES: 0x100c7
FUSES-Console>
```
4. How to Encrypt and Sign the PL360 Binary

4.1 Introduction

An encrypted and signed binary is called “secured binary”. The process to get a secured binary is:

1. Encrypt the PL360 binary getting an “encrypted binary”
2. Sign the “encrypted binary”

To generate the “encrypted binary”, the original binary must be multiple of 16 bytes. In case of a non-multiple of 16 bytes binary, it must be padded. Padding consists of filling the binary with a '1' bit and all the necessary '0' bits up to reach a total size of the binary multiple of 16 bytes. Regarding the signature validation, the binary length must be specified as the number of 16-bytes blocks.

Figure 4-1. Padding of Non-Encrypted Binary

Depending on FORCE_IVNBINC fuse, the signature is calculated over the “encrypted binary” (if the fuse is not set) or over “encrypted binary + Initialization Vector + Number of blocks” (if the fuse is set).

Figure 4-2. Structure of Data Signed with FORCE_IVBINC=0
4.2 Encrypt and Sign Script

Microchip provides an example Python™ script to encrypt and calculate the signature of firmware binaries. You can find the Python script (pl360_encfile.py) in the folder “atpl\bin”. In the same folder, it is also included a windows batch file (pl360_encfile.bat) which launches the Python script with the suitable parameters.

To use it, Python version 2.7 or 3 must be installed on the computer including the "cryptography" package.

Tip: To install the cryptography library, run “pip install cryptography” at the Python terminal.

Tip: Launch the script with arguments “-h” or “—help” to see the required parameters.
The script requires the following parameters:

- Binary file to encrypt
- Output encrypted binary file
- KEY_ENC key programmed in the PL360 fuses (in the script, it is called CBC_KEY)
- KEY_TAG key programmed in the PL360 fuses (in the script, it is called CMAC_KEY)
- Initialization vector used for encryption/decryption (in the script, it is called CBC_IV)
- Boolean variable to indicate if signature is calculated over “encrypted binary + Initialization Vector + Number of blocks” (True) or not (False)

Important: ENC_KEY, TAG_KEY and IV_KEY must be in hexadecimal format characters.

Using the parameters as inputs, the script will encrypt and sign the PL360 firmware, generating a new binary inside the “PL360_ENCFILE” folder. The structure of this secured binary obtained as output file is the following:

**Figure 4-5. Structure of the Secured Binary**
5. How to Include Secure Boot on Firmware Application

PL360 projects include all the functions to implement “normal” and “secure” boot.

Figure 5-1. PL360 Common Components Tree

Once PL360 binary has been encrypted and signed, the way to work with it in the firmware application project is the following:

1. Copy secured binary in “atpl\bin\” folder with the name of the original PL360 binary file

Figure 5-2. Original PL360 Binary Substitution with Secured Version
2. Define “ATPL360_SEC_BOOT_MODE” on “conf_atpl360.h” file

Figure 5-3. Firmware Definitions to Work with Secured PL360

3. Compile and link the application project

4. Program the application binary in the host microcontroller

5. Run the binary in the host microcontroller
Appendix A. How to Generate Keys Using Signature Functions

The keys used in secured bootloader (ENC_KEY, TAG_KEY and IV_KEY) can be any combination of 128 bits (32 hexadecimal characters).

An easy way to generate customized and easily replicable keys is to use a Master Key file, calculate its MD5 and SHA256 hashes and use them as keys (as SHA256 is 256 bits long, 2 128-bit keys are obtained from it). MD5 and SHA256 hashes can be obtained from Windows® or Linux® terminal, or even from web-based tools. With this method, it is not necessary to store the keys in any place, just the Master Key file.

In the following example, a text file containing the word "Microchip" is used to obtain the ENC_KEY using MD5 and TAG_KEY & IV_KEY using SHA256.

- **Linux terminal**

  ```
  $ echo -n "Microchip" > Microchip.txt
  $ sha256sum -t Microchip.txt | cut -c 1-32
  230fe79bc18ef87cd51096e450c8c27f
  $ sha256sum -t Microchip.txt | cut -c 33-64
  10456fd785df2af08397a2eb69647888
  $ md5sum -t Microchip.txt | cut -c 1-32
  f7962ad60e8c8ec26481358db76f7f6a
  ```

- **Windows Powershell (version 3.0 or above)**

  ```
  PS C:\> "Microchip" | Out-File -encoding ascii Microchip.txt -NoNewline
  PS C:\> (Get-FileHash .\Microchip.txt -Algorithm SHA256).hash.SubString(0,32)
  230FE79BC18EF87CD51096E450C8C27F
  PS C:\> (Get-FileHash .\Microchip.txt -Algorithm SHA256).hash.SubString(32,32)
  10456FD785DF2AF08397A2EB69647888
  PS C:\> (Get-FileHash .\Microchip.txt -Algorithm MD5).hash
  F7962AD60E8C8EC26481358DB76F7F6A
  ```
7. Revision History

7.1 Rev A - 07/2018

| Document | Initial document release. |
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.


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, Heldo, JukeBlox, KeeLoq, Kleer, LANCheck, LINK MD, maXSylus, maXTouch, MediaLB, megaAVR, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, Prochip Designer, QTorch, 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.


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.
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, KEELQ® 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.
<table>
<thead>
<tr>
<th>AMERICAS</th>
<th>ASIA/PACIFIC</th>
<th>ASIA/PACIFIC</th>
<th>EUROPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Office</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2355 West Chandler Blvd.</td>
<td>Australia - Sydney</td>
<td>Tel: 61-2-9868-6733</td>
<td>Australia - Wels</td>
</tr>
<tr>
<td>Chandler, AZ 85224-6199</td>
<td>China - Beijing</td>
<td>Tel: 86-10-8569-7000</td>
<td>Tel: 43-7242-2244-39</td>
</tr>
<tr>
<td>Tel: 480-792-7200</td>
<td>China - Chongdu</td>
<td>Tel: 86-28-8665-5511</td>
<td>Fax: 43-7242-2244-393</td>
</tr>
<tr>
<td>Fax: 480-792-7277</td>
<td>China - Chongqing</td>
<td>Tel: 86-23-8980-9588</td>
<td>Tel: 45-4450-2828</td>
</tr>
<tr>
<td>Technical Support:</td>
<td>China - Dongguan</td>
<td>Tel: 86-769-8702-9880</td>
<td>Fax: 45-4485-2829</td>
</tr>
<tr>
<td><a href="http://www.microchip.com/">http://www.microchip.com/</a></td>
<td>China - Guangzhou</td>
<td>Tel: 86-20-8755-8029</td>
<td>Finland - Espoo</td>
</tr>
<tr>
<td>support</td>
<td>China - Hangzhou</td>
<td>Tel: 86-571-8792-8115</td>
<td>Tel: 358-9-4520-820</td>
</tr>
<tr>
<td></td>
<td>China - Hong Kong SAR</td>
<td>Tel: 852-2943-5100</td>
<td>France - Paris</td>
</tr>
<tr>
<td></td>
<td>China - Nanjing</td>
<td>Tel: 86-25-8473-2460</td>
<td>Tel: 33-1-69-53-63-20</td>
</tr>
<tr>
<td></td>
<td>China - Qingdao</td>
<td>Tel: 86-632-8502-7355</td>
<td>Fax: 33-1-69-30-90-79</td>
</tr>
<tr>
<td></td>
<td>China - Shanghai</td>
<td>Tel: 86-21-3326-8000</td>
<td>Germany - Garching</td>
</tr>
<tr>
<td></td>
<td>China - Shenyang</td>
<td>Tel: 86-24-2334-2829</td>
<td>Tel: 49-8931-9700</td>
</tr>
<tr>
<td></td>
<td>China - Shenzhen</td>
<td>Tel: 86-755-8864-2200</td>
<td>Germany - Haan</td>
</tr>
<tr>
<td></td>
<td>China - Suzhou</td>
<td>Tel: 86-186-6233-1526</td>
<td>Tel: 49-2129-3766400</td>
</tr>
<tr>
<td></td>
<td>China - Wuhan</td>
<td>Tel: 86-27-5980-5300</td>
<td>Germany - Heilbronn</td>
</tr>
<tr>
<td></td>
<td>China - Xian</td>
<td>Tel: 86-29-8833-7252</td>
<td>Tel: 49-71-3-67-3636</td>
</tr>
<tr>
<td></td>
<td>China - Xiam</td>
<td>Tel: 86-992-2388138</td>
<td>Germany - Karlsruhe</td>
</tr>
<tr>
<td></td>
<td>China - Zhuhai</td>
<td>Tel: 86-876-3210040</td>
<td>Tel: 49-72-1-625370</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Germany - Munich</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tel: 49-89-627-144-0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fax: 49-89-627-144-44</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Germany - Rosenheim</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tel: 49-8031-354-560</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Israel - Ra'anana</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tel: 972-9-744-7705</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Italy - Milan</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tel: 39-0331-742611</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fax: 39-0331-466781</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Italy - Padova</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tel: 39-049-7625286</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Netherlands - Drunen</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tel: 31-416-690399</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fax: 31-416-690340</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Norway - Trondheim</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tel: 47-7289-7561</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Poland - Warsaw</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tel: 48-22-3325737</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Romania - Bucharest</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tel: 40-21-407-87-60</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Spain - Madrid</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tel: 34-91-708-08-90</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fax: 34-91-708-08-91</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sweden - Gothenburg</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tel: 46-31-704-60-40</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sweden - Stockholm</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tel: 46-8-5090-4654</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UK - Wokingham</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tel: 44-118-921-5800</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fax: 44-118-921-5820</td>
</tr>
</tbody>
</table>