EVB-SEC1110/EVB-SEC1210/ EVB-SEC1212-DEV Evaluation Board User's Guide

© 2013 Microchip Technology Inc.

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.

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in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates.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.

Trademarks

The Microchip name and logo, the Microchip logo, dsPIC, FlashFlex, KEELOQ, KEELOQ logo, MPLAB, PIC, PICmicro, PICSTART, PIC32 logo, rfPIC, SST, SST Logo, SuperFlash and UNI/O are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

FilterLab, Hampshire, HI-TECH C, Linear Active Thermistor, MTP, SEEVAL and The Embedded Control Solutions Company are registered trademarks of Microchip Technology Incorporated in the U.S.A.

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

Analog-for-the-Digital Age, Application Maestro, BodyCom, chipKIT, chipKIT logo, CodeGuard, dsPICDEM, dsPICDEM.net, dsPICworks, dsSPEAK, ECAN, ECONOMONITOR, FanSense, HI-TIDE, In-Circuit Serial Programming, ICSP, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, mTouch, Omniscient Code Generation, PICC, PICC-18, PICDEM, PICDEM.net, PICkit, PICtail, REAL ICE, rfLAB, Select Mode, SQI, Serial Quad I/O, Total Endurance, TSHARC, UniWinDriver, WiperLock, ZENA and Z-Scale 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.

GestIC and ULPP are registered trademarks 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.

© 2013, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

ISBN: 9781620774649

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.

Object of Declaration: EVB-SEC1110/EVB-SEC1210/EVB-SEC1212-DEV User's Guide

EU Declaration of Conformity

This declaration of conformity is issued by the manufacturer.
The development/evaluation tool is designed to be used for research and development in a laboratory environment. This development/evaluation tool is not a Finished Appliance, nor is it intended for incorporation into Finished Appliances that are made commercially available as single functional units to end users under EU EMC Directive 2004/108/EC and as supported by the European Commission's Guide for the EMC Directive 2004/108/EC (8th February 2010).
This development/evaluation tool complies with EU RoHS2 Directive 2011/65/EU.
For information regarding the exclusive, limited warranties applicable to Microchip products, please see Microchip's standard terms and conditions of sale, which are printed on our sales documentation and available at www.microchip.com.
Signed for and on behalf of Microchip Technology Inc. at Chandler, Arizona, USA

Derek Carlson
VP Development Tools

16-July-2013
Date

NOTES:

© 2013 Microchip Technology Inc.

Table of Contents

Preface 7
Conventions Used in this Guide 8
The Microchip Web Site 9
Development Systems Customer Change Notification Service 9
Customer Support 9
Document Revision History 10

Chapter 1. Introduction
1.1 SEC1110 Features 11
1.1.1 Smartcard 11
1.1.2 USB 11
1.2 SEC1210 Features 12
1.2.1 SPI1 12
1.2.2 UART 12
1.3 SEC1212-DEV Features 12
1.4 Directory structure 13

Chapter 2. EVBPCBA Documentation
2.5 EVB-SEC2112-DEV 14
2.5.1 Board Layout 16
2.5.2 Inserting a Chip into the Socket 17
2.5.3 Connector Description 17
2.5.4 Switch Description 20
2.5.5 Test Points Description 20
2.5.6 Bond Options 20
2.5.7 Selecting the Code Fetch Source 21
2.6 EVB-SEC1210 21
2.6.1 Placing a Chip in the Socket 22
2.6.2 Connector Description 23
2.7 EVB-SEC1110 24
2.7.1 Placing a Chip in the Socket 25
2.7.2 Connector Description 26

Chapter 3. CCID Firmware
3.8 Features 27
3.9 Single Slot CCID Firmware 27
3.10 Dual Slot CCID Firmware 27
3.11 Smartcard Reader Driver Installation under Windows 27

Chapter 4. Checking Device Firmware Revision

Chapter 5. OTP Programming Procedures

Chapter 6. SPI Programming Procedures

© 2013 Microchip Technology Inc.

Worldwide Sales and Service 41

© 2013 Microchip Technology Inc.

Preface

NOTICE TO CUSTOMERS

All documentation becomes dated, and this manual is no exception. Microchip tools and documentation are constantly evolving to meet customer needs, so some actual dialogs and/or tool descriptions may differ from those in this document. Please refer to our web site (www.microchip.com) to obtain the latest documentation available.

Documents are identified with a "DS" number. This number is located on the bottom of each page, in front of the page number. The numbering convention for the DS number is "DSXXXXXA", where "XXXXX" is the document number and "A" is the revision level of the document.

For the most up-to-date information on development tools, see the MPLAB® IDE online help. Select the Help menu, and then Topics to open a list of available online help files.

© 2013 Microchip Technology Inc.

CONVENTIONS USED IN THIS GUIDE

This manual uses the following documentation conventions:

DOCUMENTATION CONVENTIONS

Description	Represents	Examples
Arial font:		
Italic characters	Referenced books	*MPLAB® IDE User's Guide*
	Emphasized text	...is the *only* compiler...
Initial caps	A window	the Output window
	A dialog	the Settings dialog
	A menu selection	select Enable Programmer
Quotes	A field name in a window or dialog	"Save project before build"
Underlined, italic text with right angle bracket	A menu path	*File>Save*
Bold characters	A dialog button	Click **OK**
	A tab	Click the **Power** tab
N'Rnnnn	A number in verilog format, where N is the total number of digits, R is the radix and n is a digit.	4'b0010, 2'hF1
Text in angle brackets < >	A key on the keyboard	Press <Enter>, <F1>
Courier New font:		
Plain Courier New	Sample source code	`#define START`
	Filenames	`autoexec.bat`
	File paths	`c:\mcc18\h`
	Keywords	`_asm, _endasm, static`
	Command-line options	`-Opa+, -Opa-`
	Bit values	`0, 1`
	Constants	`0xFF, 'A'`
Italic Courier New	A variable argument	*`file`*`.o`, where *`file`* can be any valid filename
Square brackets [ ]	Optional arguments	`mcc18 [options]` *`file`* `[options]`
Curly brackets and pipe character: { | }	Choice of mutually exclusive arguments; an OR selection	`errorlevel {0|1}`
Ellipses...	Replaces repeated text	`var_name [, var_name...]`
	Represents code supplied by user	`void main (void) { ... }`

© 2013 Microchip Technology Inc.

THE MICROCHIP WEB SITE

Microchip provides online support via our web site at 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 (FAQs), 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

DEVELOPMENT SYSTEMS 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 www.microchip.com, click on Customer Change Notification and follow the registration instructions.

The Development Systems product group categories are:

- **Compilers** – The latest information on Microchip C compilers, assemblers, linkers and other language tools. These include all MPLAB C compilers; all MPLAB assemblers (including MPASM assembler); all MPLAB linkers (including MPLINK object linker); and all MPLAB librarians (including MPLIB object librarian).
- **Emulators** – The latest information on Microchip in-circuit emulators.This includes the MPLAB REAL ICE and MPLAB ICE 2000 in-circuit emulators.
- **In-Circuit Debuggers** – The latest information on the Microchip in-circuit debuggers. This includes MPLAB ICD 3 in-circuit debuggers and PICkit 3 debug express.
- **MPLAB IDE** – The latest information on Microchip MPLAB IDE, the Windows Integrated Development Environment for development systems tools. This list is focused on the MPLAB IDE, MPLAB IDE Project Manager, MPLAB Editor and MPLAB SIM simulator, as well as general editing and debugging features.
- **Programmers** – The latest information on Microchip programmers. These include production programmers such as MPLAB REAL ICE in-circuit emulator, MPLAB ICD 3 in-circuit debugger and MPLAB PM3 device programmers. Also included are nonproduction development programmers such as PICSTART Plus and PIC-kit 2 and 3.

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

DOCUMENT REVISION HISTORY

Revision A (September 2013)

- Initial Release of this Document.

© 2013 Microchip Technology Inc.

Chapter 1. Introduction

The SEC1110/SEC1210/SEC1212-DEV is a family low power, OEM configurable, single-chip smartcard reader solutions. Three evaluation boards (EVBs) are available for device development:

- EVB-SEC2112-DEV
- EVB-SEC1210
- EVB-SEC1110

These EVBs demonstrate standalone solutions with all of the interfaces and features listed the following sub-sections. For details on each individual EVB, refer to Chapter 2.

1.1 SEC1110 FEATURES

1.1.1 Smartcard

- Single Smartcard slot
- Fully compliant with the ISO/IEC 7816, EMV and PC/SC standards
- Versatile ETU rate generation, supporting current and proposed rates (to 861 Kbps and beyond)
- Full support of both T=0 and T=1 protocols
- Full-packet FIFO (259 bytes) for transmit and receive
- Half-Duplex operation, with no software intervention required between transmit and receive phases of an exchange
- Very loose real-time response required of software
- (worst case scenario of approximately 180 ms)
- Dynamically programmable FIFO threshold, with byte granularity
- Time-out FIFO flush interrupt, independent of threshold
- Programmable Smart Card clock frequency
- UART-like register file structure
- Supports Class A, Class B, Class C, or Class AB Smart Cards (all 1.8 V, 3 V and 5 V cards)
- Automatic Character Repetition for T=0 protocol Parity Error recovery
- Automatic card deactivation on card removal and on other system events, including persistent Parity Errors

1.1.2 USB

- Supports Full-Speed data transfer
- Endpoints can be configured for control, bulk & interrupt transfer types
- Max packet size configurable for each endpoint
- (8 / 16/ 32/ 64 bytes are allowed)
- Ping pong buffers supported for non-control endpoints

- Supports Suspend, Resume, and Remote Wakeup per the USB specification requirements
- Endpoint buffer may be located anywhere in the 1.5K SRAM, as per the alignment requirements based on the max packet size

1.2 SEC1210 FEATURES

Along with the features mentioned in Section 1.1, the SEC1210 includes two Smartcard slots and the following additional features:

1.2.1 SPI1

- Supports full-duplex mode
- Supports master or slave mode
- Supports seven SPI1 Master baud rates
- Slave Clock rate up to spi1_clk/8
- Serial clock with programmable polarity and phase
- Master Mode fault error flag with MCU interrupt capability
- Write collision flag protection
- Byte Transfer/Receive APIs
- Bulk Transfer/ Receive APIs
- Simultaneous Transfer/ Receive APIs

1.2.2 UART

- Software compatible with Standard 16C450 and 16C550A
- Separate 16 byte FIFO for transmission and reception
  - Prevents buffer overrun
  - Helps software to be less time critical in handling transmission / reception
- Programmable baud rate generator - Up to 3 Mbps baud rate can be achieved
- Supports flow control using RTS / CTS signals
- Pin Polarity control
- Programmable communication parameters:
  - Word length - 5, 6, 7, 8 bits
  - Stop bits - 1, 1.5, 2 bits
  - Parity - None, Odd, Even, Mark, Space
- Low power sleep mode available

Note: A voltage level shifter board / cable is required to connect the UART port to the PC. An FTDI cable is used for this.

1.3 SEC1212-DEV FEATURES

Along with the features mentioned in section 1.1 and1.2 the following modules are also available in the SEC1212-DEV:

- Boot from SPI2 Interface
- The SVB is equipped with a 1Kbyte Atmel SPI flash (AT26DF081A-SSU). SPI flash from Atmel and Windbond are supported.
- On-board RS232 Transceiver for debugging as well as RS232 host interface
- On-board Reset button
- On-board EDP header for f/w debugging.
- On-board JTAG header for entering ASIC test mode and debugging

© 2013 Microchip Technology Inc.

1.4 DIRECTORY STRUCTURE

The EVB-SEC2112-DEV release package provides the following file/folder structure:

EVB Schematics & BOM

Contains EVB schematics and BOM

SW Tools/WinUSB Driver

This is the device driver required for BootROM USB Device

SW Tools/OTPProgrammer

Contains the OTP programming utility and user manual

SW Tools/Linux Libraries

Contains the required Linux libraries

SW Tools/SPIFlashUtitly

Contains utility to program the SEC1212-DEV SPI2 flash and the relevant user manual.

Firmware

This folder contains the firmware binary files for programming into the OTP / SPI Flash. Filenames with "SPI2" are intended to be programmed onto the SPI flash using SPI-FlashWriter application. Filenames with "OTP" are intended to be programmed onto the OTP using OTPProgrammer application. Similarly, "SINGLESLOT" or "DUALSLOT" in the file name indicates a single slot or dual slot reader, respectively.

Chapter 2. EVBPCBA Documentation

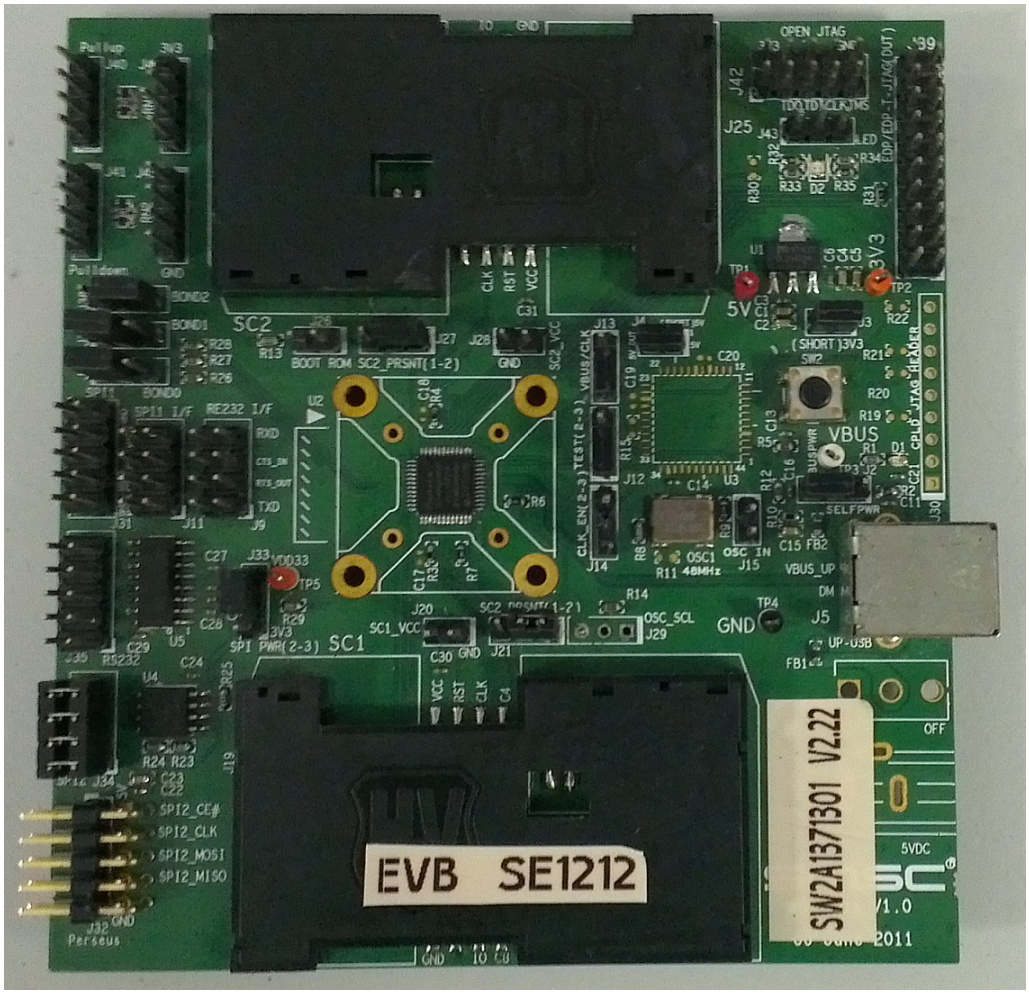
This chapter details the evaluation boards available for the SEC family of ASIC's and their hardware settings. A standard USB A-to-B cable is required to connect the EVB to the USB Host.

2.5 EVB-SEC2112-DEV

The EVB-SEC2112-DEV includes a 48-pin QFN SEC1212-DEV with the following interfaces and features:

- USB host interface
- Two smartcard slots
- SPI1
- SPI2 Code execution (Either from external or on board flash)
- UART
- Input bond options allow a single chip to function as either an SEC1110 or SEC1210.

FIGURE 2-1: EVB-SEC2112-DEV PROTOTYPE COMPONENT SIDE TOP LAYER

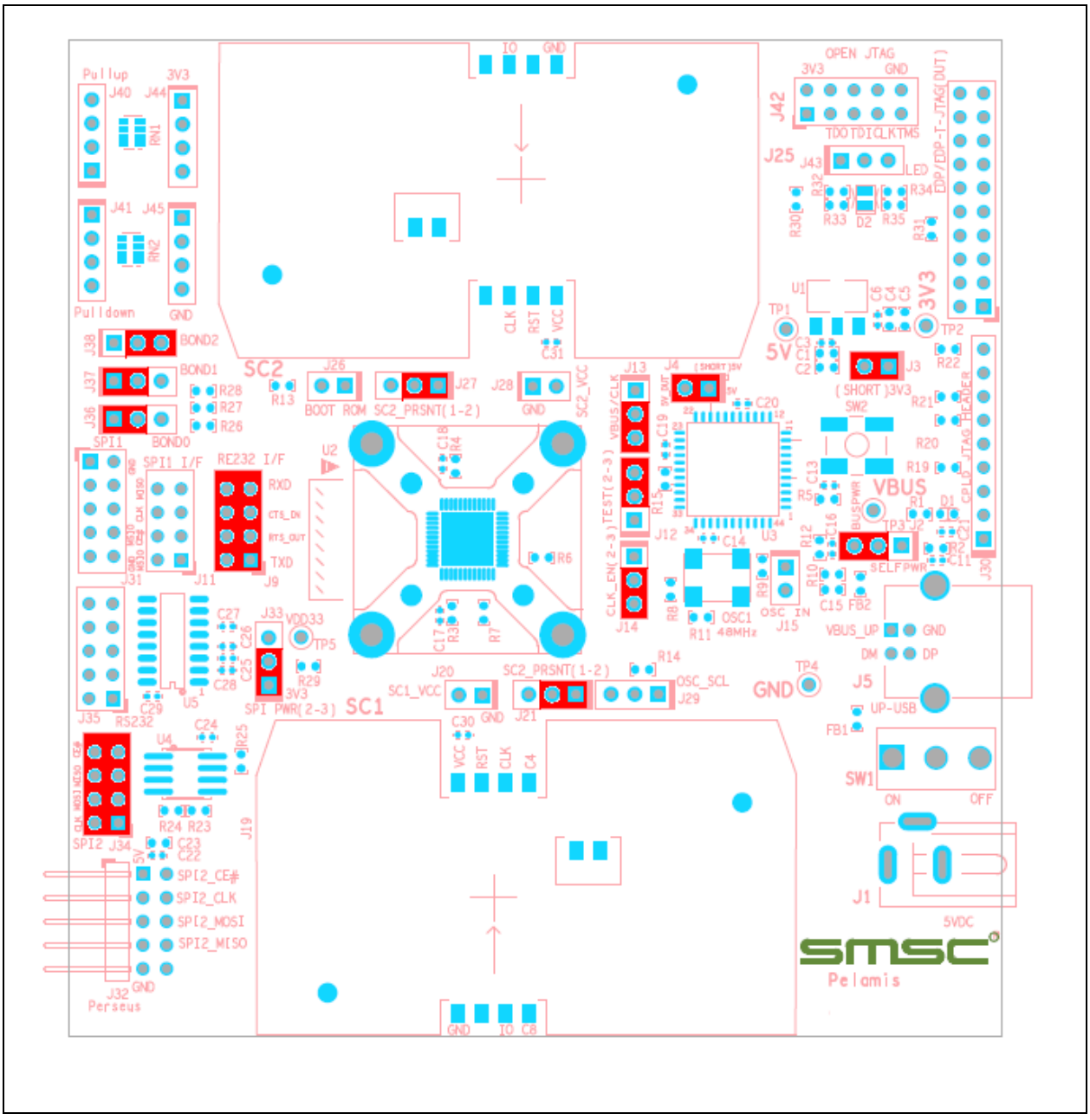


2.5.1 Board Layout

Please follow this legend to understand the following figure.

1. In each header, Pin 1 is represented by a thick band near the edge.
2. Pins filled in dark red indicate they are to be shorted by a jumper.

FIGURE 2-2: DEFAULT BOARD SETUP TO RUN FROM OTP USING INTERNAL OSCILLATOR IN SEC1212-DEV (QFN48) MODE



© 2013 Microchip Technology Inc.

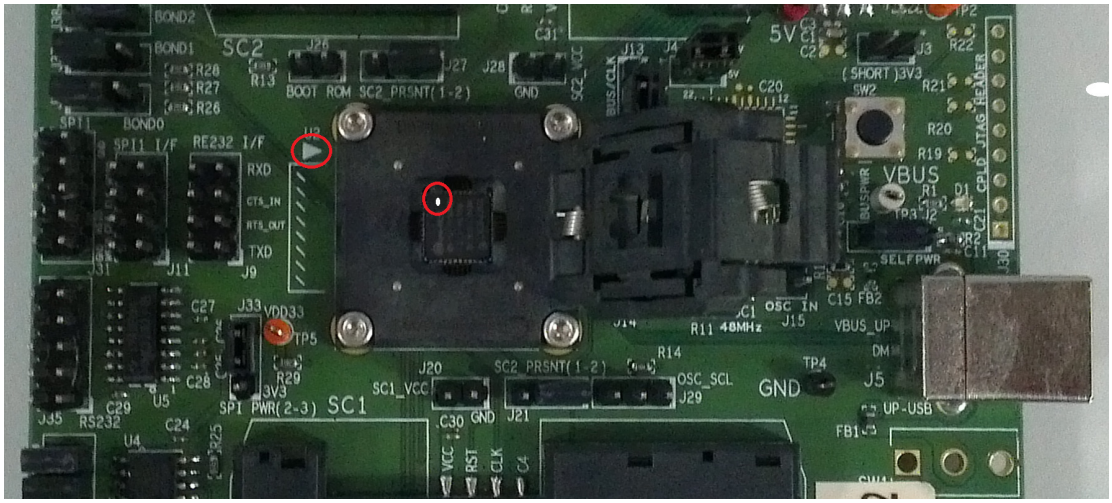
2.5.2 Inserting a Chip into the Socket

This section is applicable only if the ASIC is not directly soldered on the PCB and the EVB is equipped with a socket. The following guidelines must be followed when replacing the ASIC in the socket.

Place the ASIC in the socket in such a way that the Pin1 marking (dot) on the ASIC and the socket Pin1 marking on the PCB (triangle) align, as shown in Figure 2-3.

Note: The socket is manufactured by R&D Interconnect (P/N: 106458-0020).

FIGURE 2-3: EVB-SEC2112-DEV PIN 1 SOCKET ALIGNMENT



2.5.3 Connector Description

Note: The board's default settings are indicated in the *Settings* column.

Connector	Description	Settings	
J2	Self/Bus Power Header	1 --- 2 2 --- 3	Supplied Externally Supplied by Upstream VBUS (default)
J3	Power IN	1-2	Short (default)
J4	5V_DUT	1-2	Short (default)
J9	MUX'd RS232-I/F	1-2 3-4 5-6 7-8	Short (and open J11) to select RS232 interface

Connector	Description	Settings	
J11	MUX'd SPI1-I/F	1-2 3-4 5-6 7-8	Short (and open J9) to select SPI1 interface
J12	TEST	1-2 2-3	Chip will enter TEST mode Chip will enter functional mode (default)
J13	JTAG Select Header	1 --- 2 2 --- 3	JTAG_CLK (JTAG CLK is routed from J39 when this setting is selected) VBUS_DET(default)
J14	PCLK_ENABLE	1-2 2-3	Chip starts with external oscillator Chip starts with internal oscillator (default)
J15	OSC_IN	1-2	External oscillator is fed to PCLK_IN_48MHZ. To be shorted if the chip is to work from external oscillator
J20	SC1_Load	1-2	Open (default)
J21	SC1_PRSNT	1-2 2-3	SC1 Card detect pin routed from smartcard connector (default) SC1 card detect pin is permanently grounded
J26	BootROM select	1-2	Open (default)
J27	SC2_PRSNT	1-2 2-3	SC2 Card detect pin routed from smartcard connector (default) SC2 card detect pin is permanently grounded
J28	SC2_Load	1-2	Open (default)
J29	OSC_SEL	Unused	Open (default)
J31	SPI1_Interface	1-10	Open (default). Header for connecting Cheetah / Aardvark SPI host adapters
J34	SPI2_Internal Flash	1-8	Short to program SPI2 flash and execute code from
J35	RS232 10 pin header	1-10	Header to which Microchip's 10 pin serial cable to be connected

© 2013 Microchip Technology Inc.

Connector	Description	Settings	
J36	Bond 0 Configuration Header	1 --- 2 2 --- 3	Pulled high to VDD33 (default) Pulled down to GND
J37	Bond 1 Configuration Header	1 --- 2 2 --- 3	Pulled high to VDD33 (default) Pulled down to GND
J38	Bond 2 Configuration Header	1 --- 2 2 --- 3	Pulled high to VDD33 Pulled down to GND (default) for OTP / ROM execution
J19	Smart Card 1 (SC1 I/F – Credit Card)	10 9 8 4 7 3 6 2 5 1	CDSW2 (GND) SC1_PRSNT# SC1_C8 SC1_C4 SC1_IO SC1_CLK NC SC1_RST# GND SC1_VCC
J25	Smart Card 2 (SC2 I/F – Credit Card)	10 9 8 4 7 3 6 2 5 1	CDSW2 (GND) SC2_PRSNT# NC NC SC2_IO SC2_CLK NC SC2_RST# GND SC2_VCC
J39	DUT EDP/EDP-T JTAG Header	2,6,10,16 1,3,4,5,7,9,11,13,15,17,19,20 8 12 14 18	nc pins GND Test Points TCK (JTAG_CLK) TDO (PJTAG_TDO) TDI (PJTAG_TDI) TMS (PJTAG_TMS)
J40	General purpose pull up to 3.3V thru 1K ohm resistor	1-4	Open (default)

Connector	Description	Settings	
J41	General purpose pull down to GND thru 1K ohm resistor	1-4	Open (default)
J42	Open JTAG Header	Unused	Open (default)
J43	LED Polarity control	2-3	Short (default)
J44	3V3	1-4	Open (default). Connected to 3.3V
J45	GND	1-4	Open (default). Connected to GND

2.5.4 Switch Description

Ref. Des	Description	Settings
SW2	Reset Switch	Press : In Reset Release : Out of Reset

2.5.5 Test Points Description

Test Point	Description	Connection
TP1	5V	5V input to MIC37100 3.3V regulator (U1) & SEC1210 (U2)
TP2	3.3V	3.3V output of MIC37100 3.3V regulator (U1)
TP4	GND	GND
TP5	VDD33	VDD33 power output of internal regulator

2.5.6 Bond Options

Depending on the Bond option set on jumper J36, J37 and J38, the SEC1212-DEV prototype can work in SEC1210 (QFN24) and SEC1110 (QFN16) pin modes also.

PART No.	BOND0(J36)	BOND1(J37)	BONd2(J38)	Remarks
SEC1110	0	0	x	
SEC1210	0	1	x	
SEC1212-DEV	1	1	0	OTP/Internal ROM boot
SEC1212-DEV	1	1	1	External SPI2 Flash boot

© 2013 Microchip Technology Inc.

2.5.7 Selecting the Code Fetch Source

SEC1212-DEV can execute code from Internal /OTP ROM as well as from external serial SPI flash (one at a time).

The following sub-sections detail the pre-requisites to select the required code fetch source.

2.5.7.1 CODE EXECUTION FROM INTERNAL BOOT ROM

1. OTP_ROM_EN & FORCE_OTP_ROM bits are not programmed through OTP Programmer application
2. Pins 2-3 of J38 are to be shorted

2.5.7.2 CODE EXECUTION FROM INTERNAL OTP ROM

1. OTP should have been programmed through OTP Programmer application
2. OTP_ROM_EN bit is programmed through OTP Programmer application
3. Pins 2-3 of J38 are to be shorted

2.5.7.3 CODE EXECUTION FROM SPI FLASH

1. SPI Flash should have been programmed through SPI Flashwriter application
2. FORCE_OTP_ROM bit is not programmed through OTP Programmer application
3. Pins 1-2 of J38 are to be shorted

2.6 EVB-SEC1210

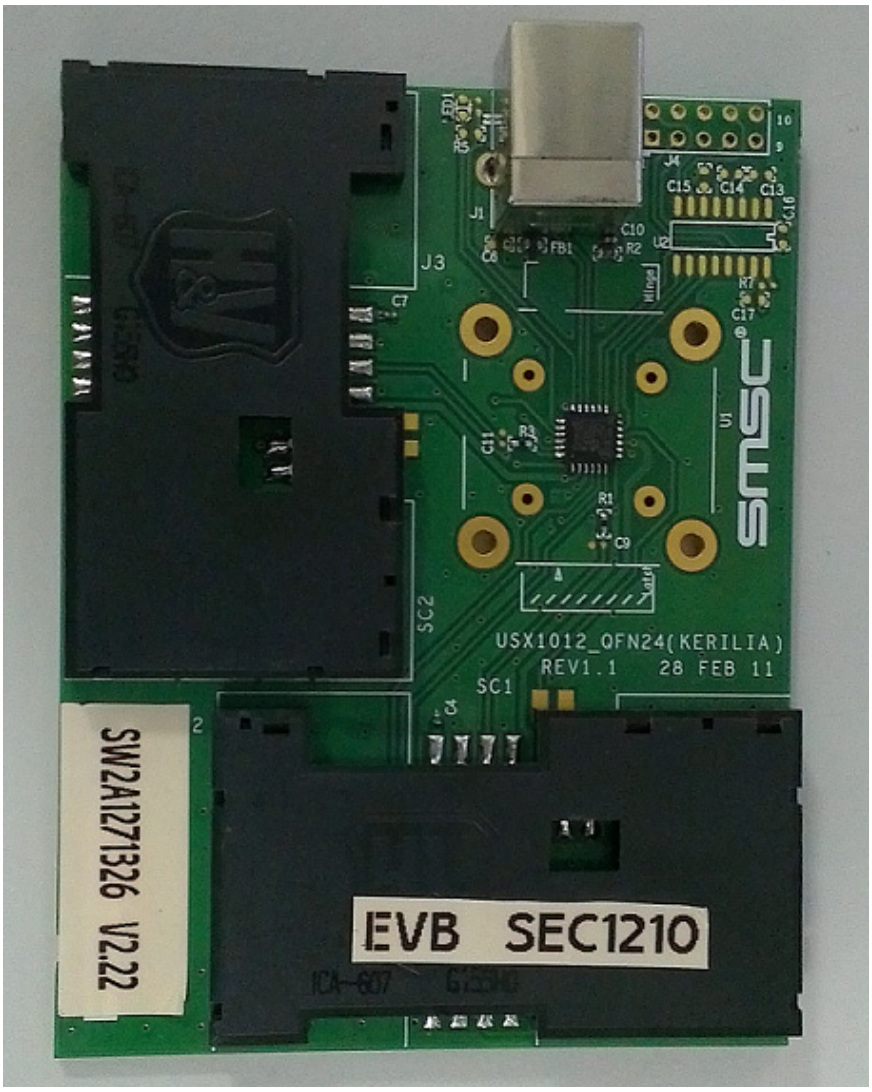
The EVB-SEC1210 utilizes the 24-pin QFN SEC1210 and includes the following interfaces and features.

- USB
- Two smartcard slots
- SPI1 or UART Interface

Note 1: A standard USB A-to-B cable is required to connect to the USB Host.

2: Code execution is possible only from internal SRAM or OTP.

FIGURE 2-4: EVB-SEC1210 COMPONENT SIDE TOP LAYER



2.6.1 Placing a Chip in the Socket

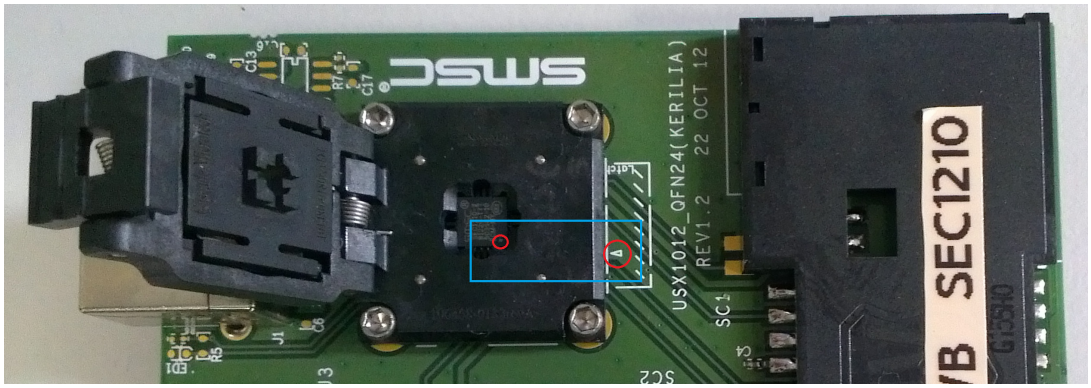
This section is applicable only if the ASIC is not directly soldered on the PCB and the EVB is equipped with a socket. The following guidelines must be followed when replacing the ASIC in the socket.

Place the ASIC in the socket in such a way that the Pin1 marking (dot) on the ASIC and the socket Pin1 marking on the PCB (triangle) align, as shown in Figure 2-5.

Note: The socket is manufactured by R&D Interconnect (P/N: 106458-0133).

© 2013 Microchip Technology Inc.

FIGURE 2-5: EVB-SEC1210 PIN 1 SOCKET ALIGNMENT



2.6.2 Connector Description

Ref. Des.	Description	Settings	
J1	USB-B Upstream Connector	5,6 1 2 3 4	Shield connections to earth GND VBUS_UP USBUP_DM USBUP_DP GND
J2	Smart Card 1 (SC1 I/F – Credit Card)	10 9 8 4 7 3 6 2 5 1	CDSW2 (GND) SC1_PRSNT# SC1_C8 SC1_C4 SC1_IO SC1_CLK NC SC1_RST# GND SC1_VCC
J3	Smart Card 2 (SC2 I/F – Credit Card)	10 9 8 4 7 3 6 2 5 1	CDSW2 (GND) SC2_PRSNT# NC NC SC2_IO SC2_CLK NC SC2_RST# GND SC2_VCC
J4	RS-232 D-sub9 connector	1-10	Header to which SMSC's 10 pin RS232 cable needs to be connected

2.7 EVB-SEC1110

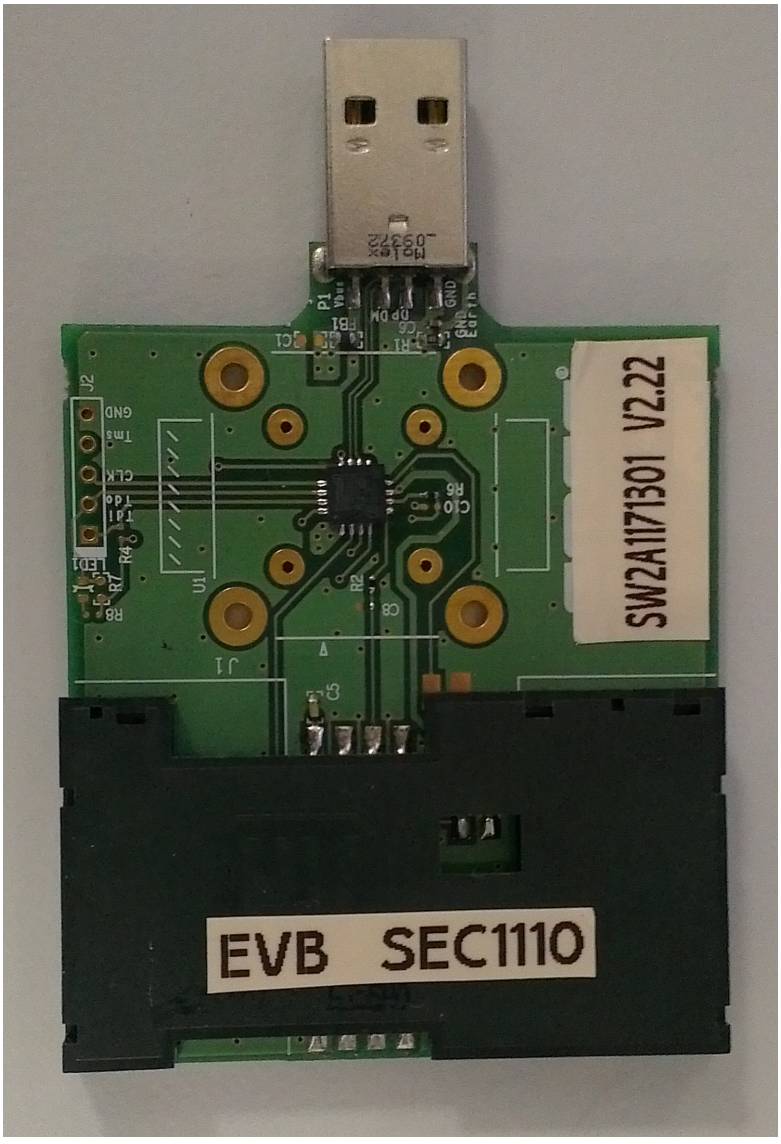
The EVB-SEC1110 utilizes the 16-pin QFN SEC1110 and includes the following interfaces and features.

- USB
- One smartcard slot

Note 1: A standard USB A-to-B cable is required to connect to the USB Host.

2: Code execution is possible only from internal SRAM or OTP.

FIGURE 2-6: EVB-SEC1110 COMPONENT SIDE TOP LAYER



© 2013 Microchip Technology Inc.

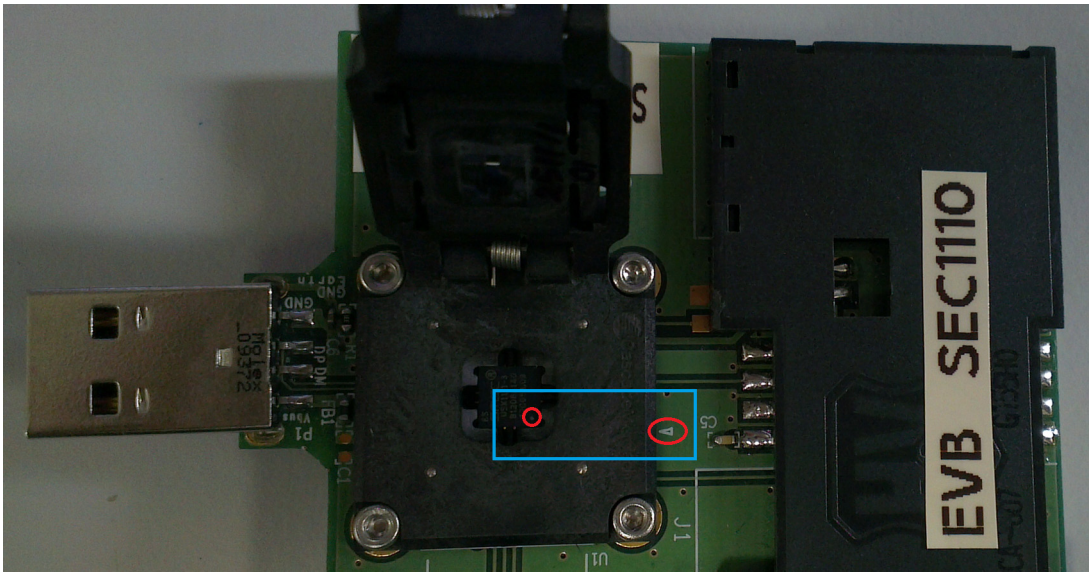
2.7.1 Placing a Chip in the Socket

This section is applicable only if the ASIC is not directly soldered on the PCB and the EVB is equipped with a socket. The following guidelines must be followed when replacing the ASIC in the socket.

Place the ASIC in the socket in such a way that the Pin1 marking (dot) on the ASIC and the socket Pin1 marking on the PCB (triangle) align, as shown in Figure 2-7.

Note:	The socket is manufactured by R&D Interconnect (P/N: 106458-0134).

FIGURE 2-7: EVB-SEC1110 PIN 1 SOCKET ALIGNMENT



2.7.2 Connector Description

Ref. Des.	Description	Settings	
P1	USB-A Upstream Connector	5,6 1 2 3 4	Shield connections to earth GND VBUS_UP USBUP_DM USBUP_DP GND
J1	Smart Card 1 (SC1 I/F – Credit Card)	10 9 8 4 7 3 6 2 5 1	CDSW2 (GND) SC1_PRSNT# SC1_C8 SC1_C4 SC1_IO SC1_CLK NC SC1_RST# GND SC1_VCC

© 2013 Microchip Technology Inc.

Chapter 3. CCID Firmware

3.8 FEATURES

- Supports smartcards of all voltages (1.8V, 3V and 5V)
- Supports T=0 and T=1 protocols
- Supports the fastest possible smartcards. (As per ISO Spec, ATR with TA1=17 is the maximum speed possible for a smartcard. This is equivalent to 826Kbps.)
- Has a maximum CCID command length of 271 bytes
- Supports suspending the device in order to save power
- Remote wake-up is possible through smartcard insertion. When host is in suspended state, on inserting a smartcard, the device will wake up the host.
- Support in-box drivers of all Windows and Linux versions

3.9 SINGLE SLOT CCID FIRMWARE

- USB CCID class compliant single slot firmware
- This firmware supports EVB-SEC1110, EVB-SEC1210 & EVB-SEC2112-DEV boards
- Card can be removed / re-inserted. Interrupt notification will be sent to host according to card changes in slot.

3.10 DUAL SLOT CCID FIRMWARE

- USB CCID class compliant dual slot firmware (enumerates as a composite USB device)
- This firmware supports EVB-SEC1210 & EVB-SEC2112-DEV boards
- In slot1, card removed / re-insertion is supported
- In slot2, card removal / re-insertion is not supported as no status change interrupt endpoint is supported for this interface

3.11 SMARTCARD READER DRIVER INSTALLATION UNDER WINDOWS

Most Windows OS installations include USBCCID drivers integrated by default. In these cases, as soon as the EVB is connected to the system, the usbccid.sys driver is loaded and the EVB-SEC1110/EVB-SEC1210/EVB-SEC1212-DEV smartcard reader will be listed in the Device Manager as shown below.

FIGURE 3-8: SEC1110 DEVICE ENUMERATION UNDER WINDOWS 7

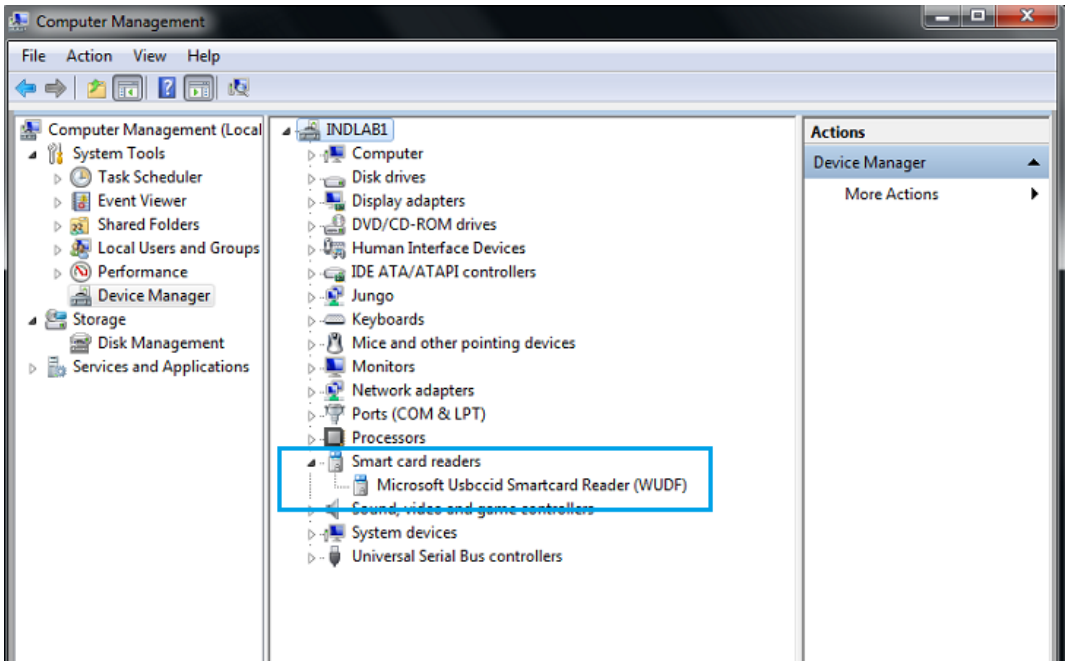
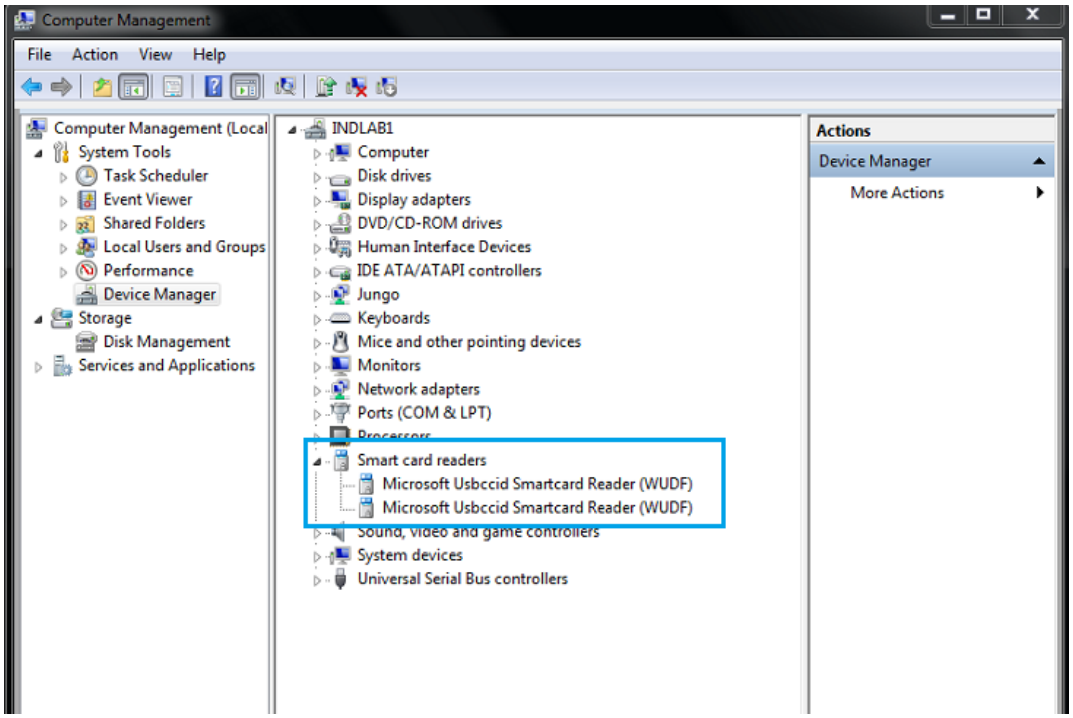


FIGURE 3-9: SEC1210/SEC1212-DEV DEVICE ENUMERATION UNDER WINDOWS 7



© 2013 Microchip Technology Inc.

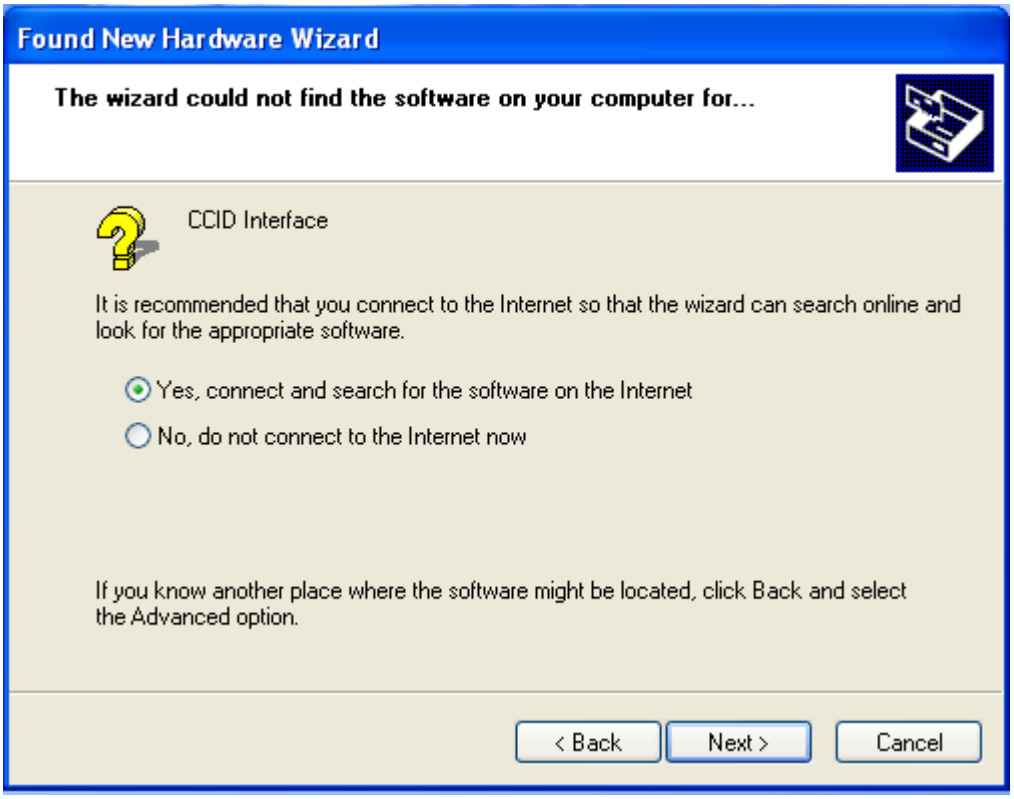
If the driver is has not been pre-installed on the PC, follow the steps below to install the driver via the Windows Update site (Shown for SEC1110 under Windows XP OS).

- Connect the reader to a free USB port on the PC.
- Once the smartcard reader is connected, Window reports that new hardware has been detected and will offer to connect to Windows Update to search for a suitable driver.
- Choose **Recommended Option** and click **Next** to continue.

FIGURE 3-10: FOUND NEW HARDWIRE WIZARD

- Choose **"Yes, Connect and search for software on the Internet"** and click **Next.**

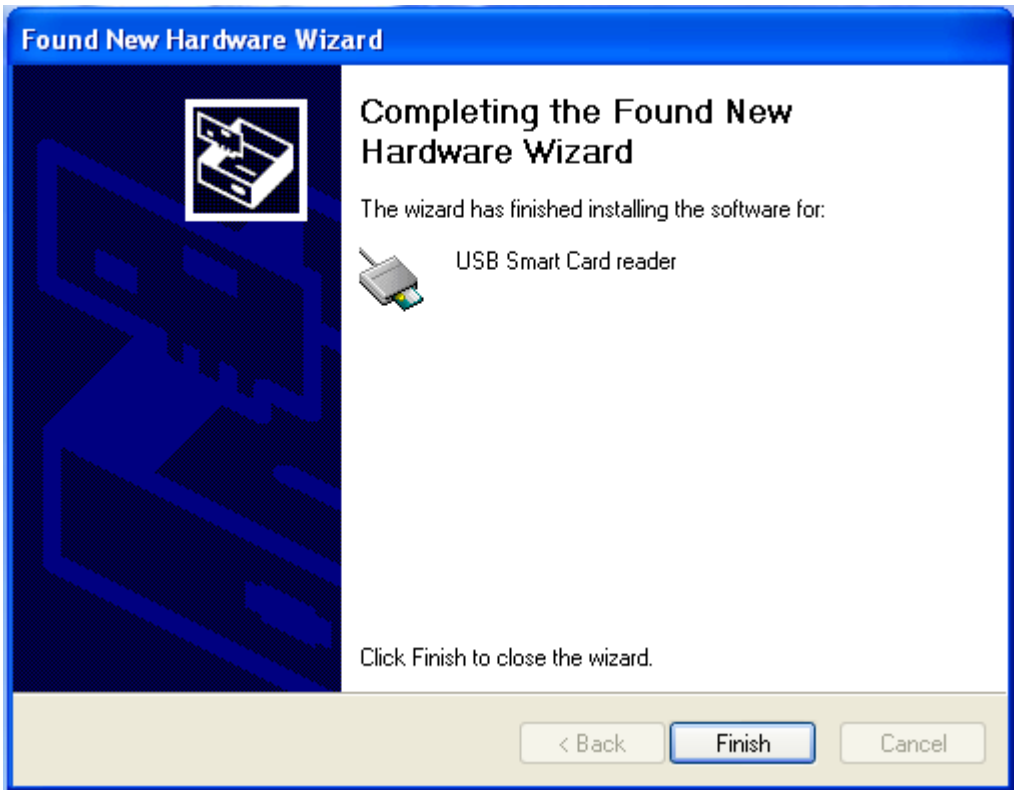
FIGURE 3-11: FOUND NEW HARDWARE WIZARD - OPTIONS



© 2013 Microchip Technology Inc.

FIGURE 3-12: FOUND NEW HARDWARE WIZARD - SEARCH

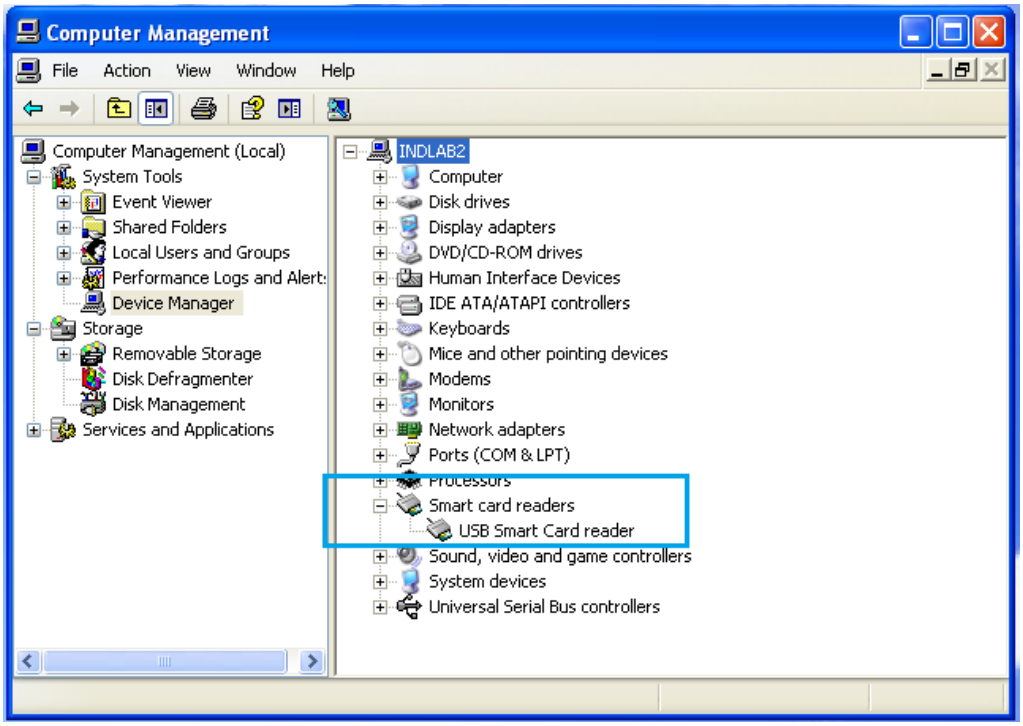
FIGURE 3-13: FOUND NEW HARDWARE WIZARD - COMPLETED



- Click **Finish** when the last window shows that the installation has finished.
- After successful driver installation, the device will be included in the Device Manager, as shown in Figure 3-14.

© 2013 Microchip Technology Inc.

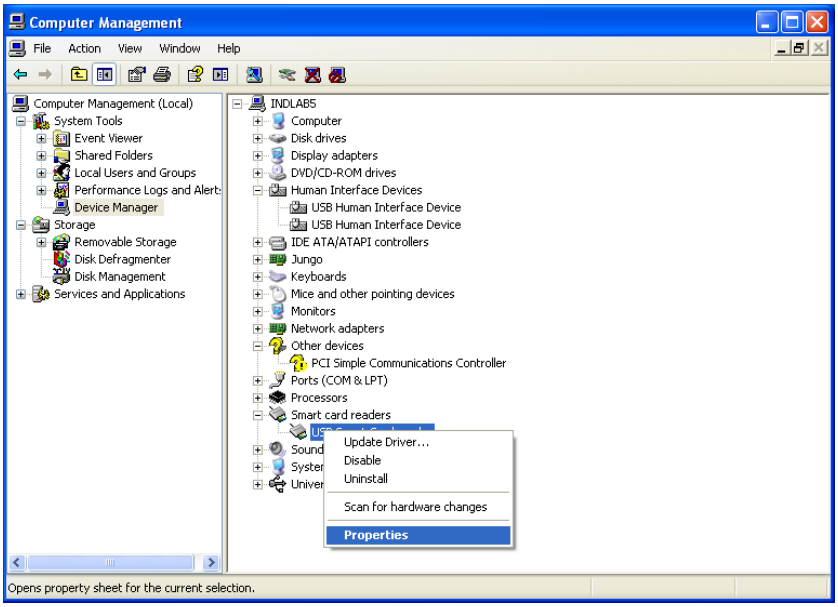
FIGURE 3-14: DEVICE MANAGER - NEW DEVICE



Chapter 4. Checking Device Firmware Revision

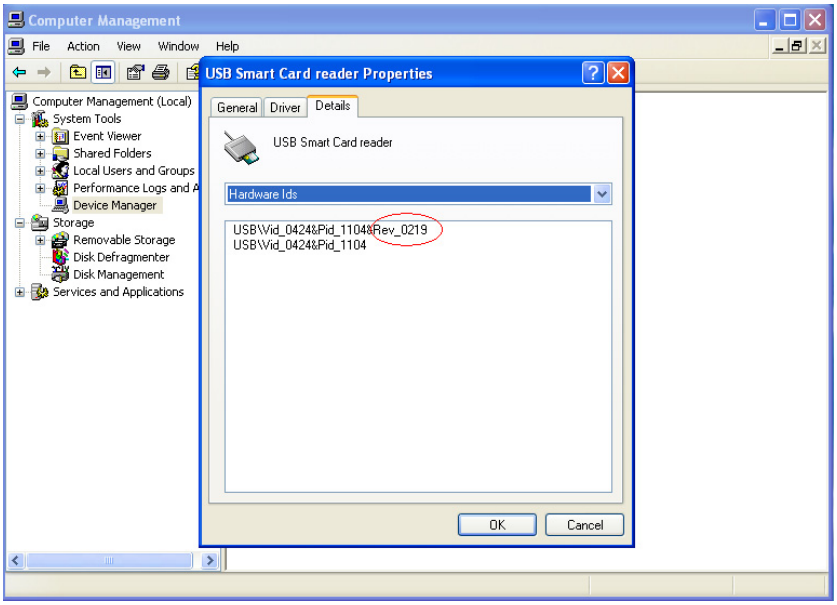
To check the device's firmware revision, go to Device Manager and select the smart card reader. Right click and select **Properties**.

FIGURE 4-15: DEVICE MANAGER - PROPERTIES



In the **Details** tab select **Hardware Ids**, where the revision number is listed.

FIGURE 4-16: DEVICE MANAGER - FIRMWARE REVISION



Note 1: F/W version in the above case is 2.19

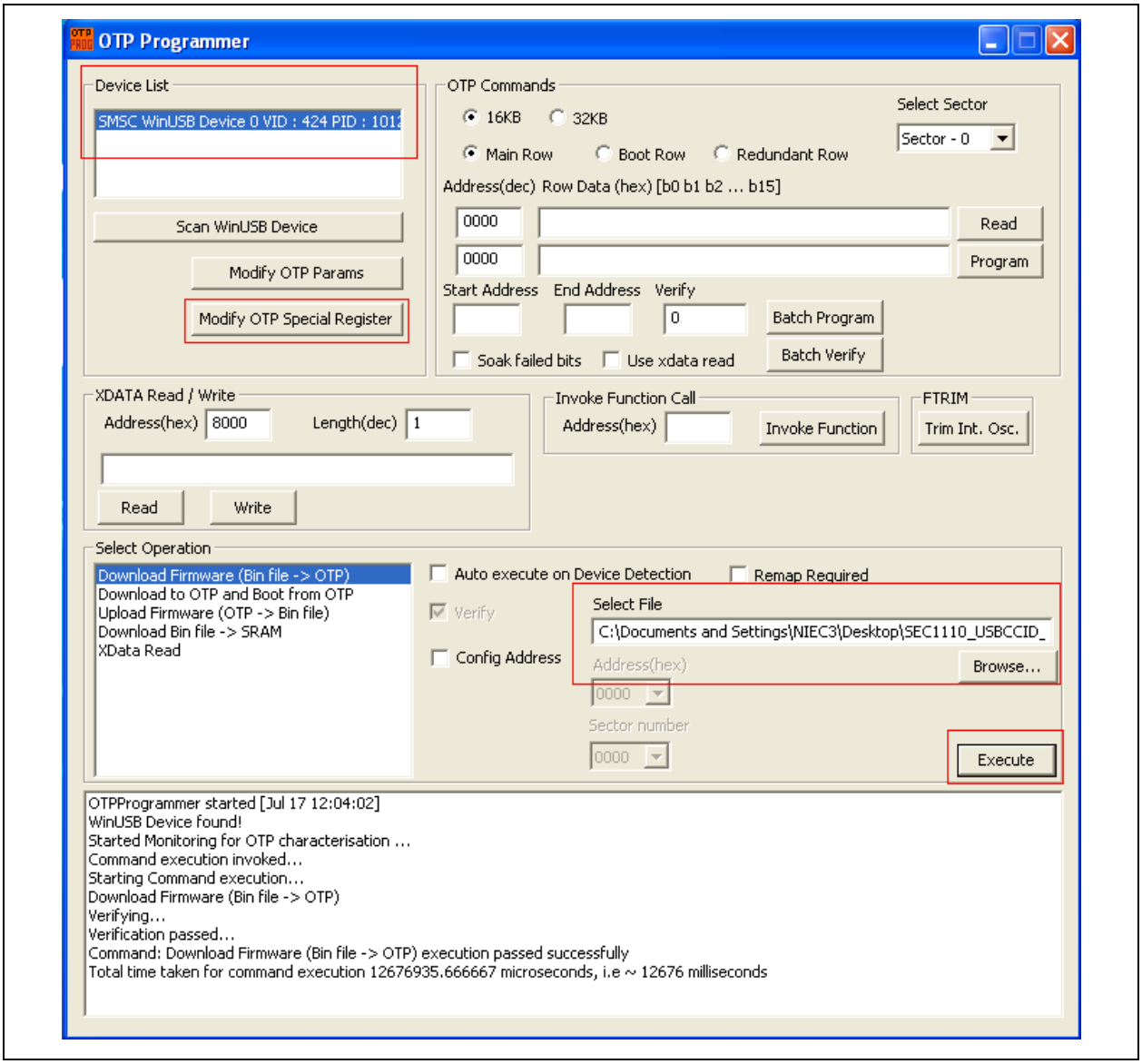
2: If the reader is enumerated as SMSC WINUSB, then the device is not programmed.

Chapter 5. OTP Programming Procedures

Note: This procedure is applicable only to EVB-SEC2112-DEV, as the EVB-SEC1110 and EVB-SEC1210 are pre-programmed with appropriate firmware. Only the EVB-SEC2112-DEV includes firmware loaded to SPI2 Flash - and user has an option to program the OTP only once. Once the OTP is programmed and the "OTP_ROM_EN" option is set as detailed in step 6 of the procedure below, the SPI flash cannot be updated again and the boot from OTP or SPI2 can be switched using Jumper J38.

1. The device should enumerate as "SMSC WINUSB". Otherwise the device can't be programmed.
2. Open the OTP Programmer and confirm the device enumerated
3. Select the .bin file using **Browse**… button
4. Click **Execute**

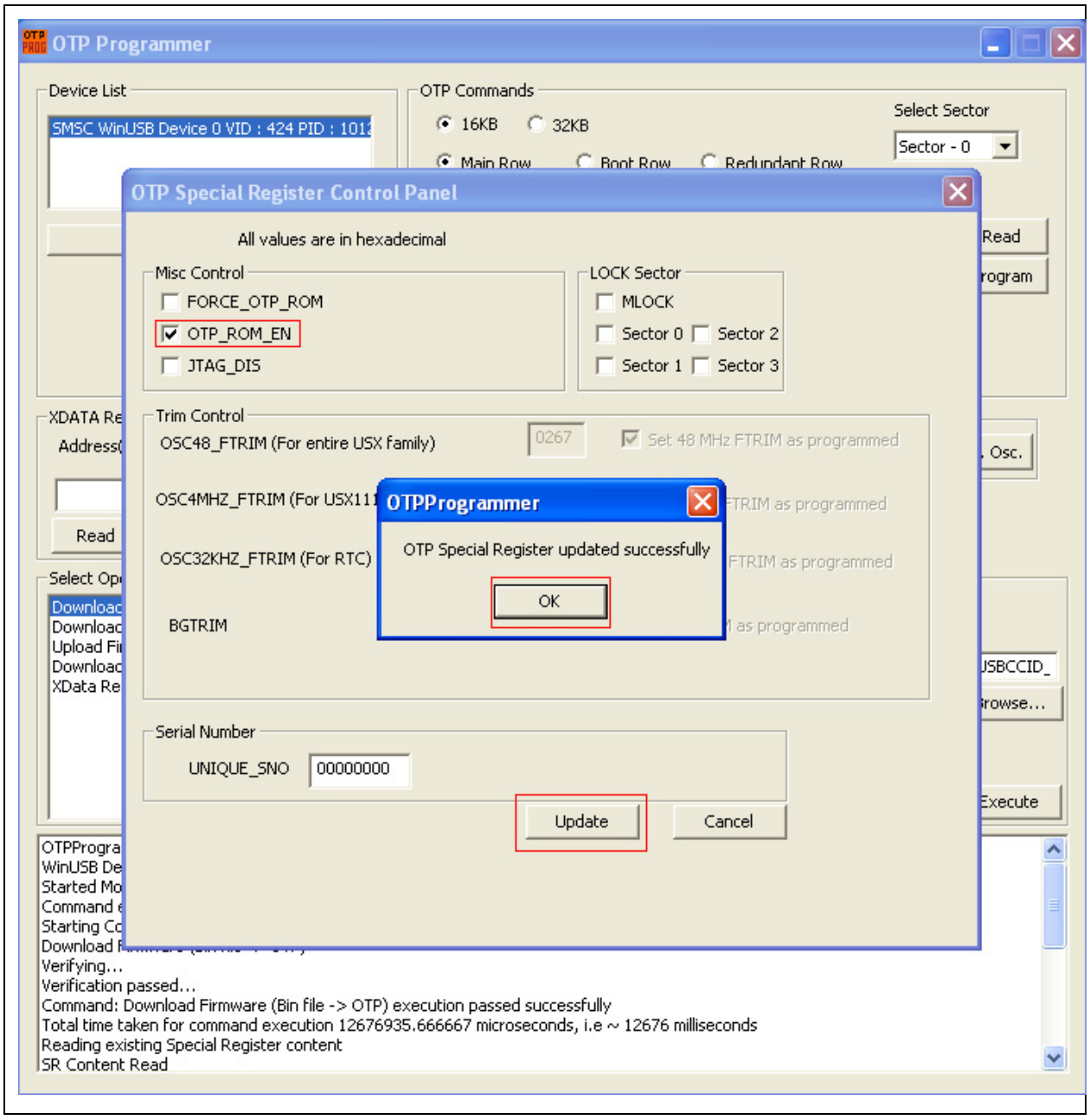
FIGURE 5-17: OTP PROGRAMMER - DEVICE LIST



5. After successful completion, the message shown in Figure 5-17 will be shown in the status box.
6. Select **Modify OTP Special Register** and click the OTP_ROM_EN check box, as shown in Figure 5-18.
7. Select Update and press OK.

Note: Steps 4, 5 and 6 must be performed without resetting the device after OTP programming. Otherwise, the device will enumerate as SMSC WINUSB.

FIGURE 5-18: OTP PROGRAMMER - SPECIAL REGISTER CONTROL PANEL



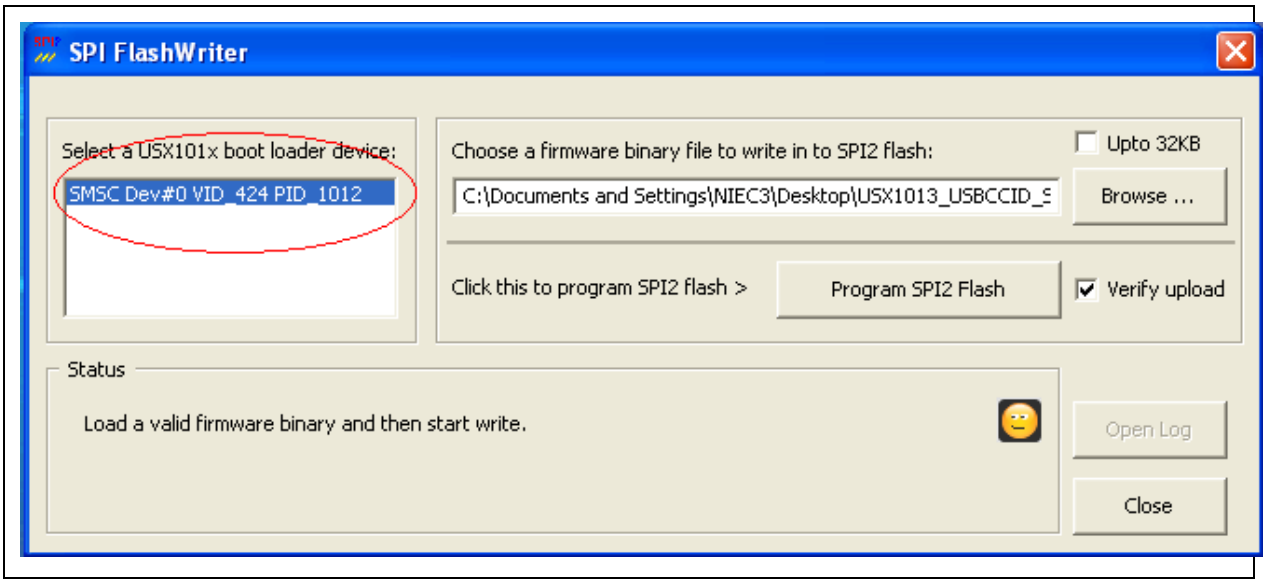
© 2013 Microchip Technology Inc.

Chapter 6. SPI Programming Procedures

Note: SPI Programming can only be performed on the EVB-SEC2112-DEV.

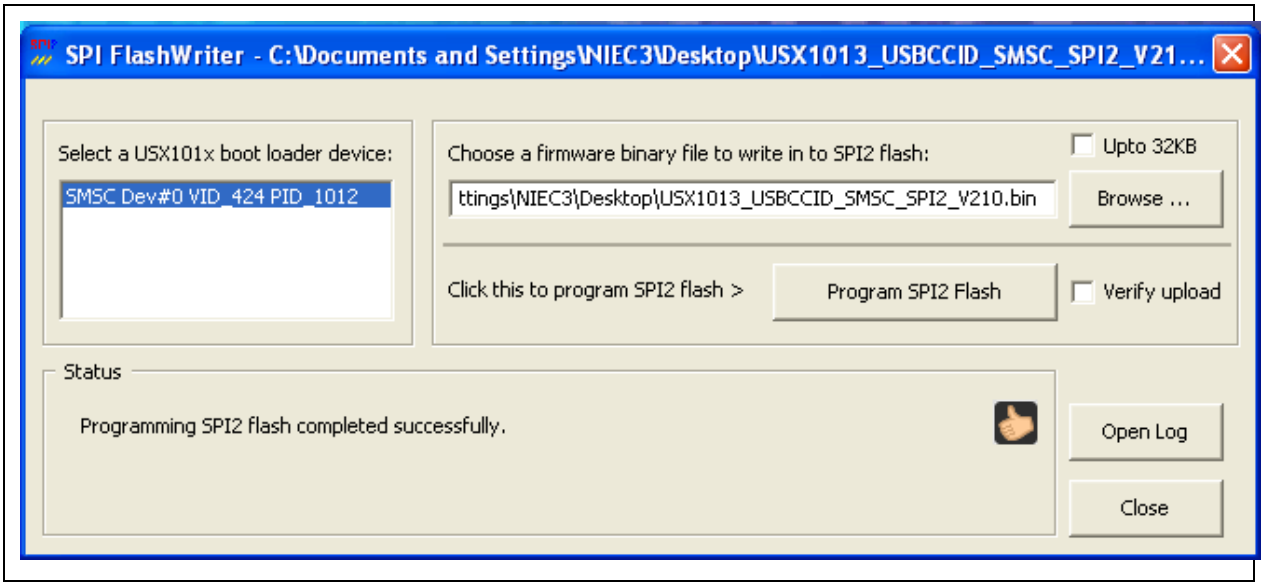
1. In order for the device to enumerate as "SMSC WINUSB", the Bond2 jumper (J38) must be set to 1-2 during power-up.
2. Open SPI Flashwriter and confirm the device has enumerated.
3. Select the .bin file using **Browse**… button
4. Click **Program SPI2 Flash**

FIGURE 6-19: SPI FLASH WRITER - SELECT DEVICE



5. After successful completion, the Status box will change to "Programming SPI2 flash completed successfully".

FIGURE 6-20: SPI FLASH WRITER - COMPLETED SUCCESSFULLY



6. Change the Bond2 jumper (J38) to 2-3 and reset the board. The EVB will now boot from SPI.

© 2013 Microchip Technology Inc.

Worldwide Sales and Service

AMERICAS

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

Boston
Westborough, MA
Tel: 774-760-0087
Fax: 774-760-0088

Chicago
Itasca, IL
Tel: 630-285-0071
Fax: 630-285-0075

Cleveland
Independence, OH
Tel: 216-447-0464
Fax: 216-447-0643

Dallas
Addison, TX
Tel: 972-818-7423
Fax: 972-818-2924

Detroit
Farmington Hills, MI
Tel: 248-538-2250
Fax: 248-538-2260

Indianapolis
Noblesville, IN
Tel: 317-773-8323
Fax: 317-773-5453

Los Angeles
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608

Santa Clara
Santa Clara, CA
Tel: 408-961-6444
Fax: 408-961-6445

Toronto
Mississauga, Ontario,
Canada
Tel: 905-673-0699
Fax: 905-673-6509

ASIA/PACIFIC

Asia Pacific Office
Suites 3707-14, 37th Floor
Tower 6, The Gateway
Harbour City, Kowloon
Hong Kong
Tel: 852-2401-1200
Fax: 852-2401-3431

Australia - Sydney
Tel: 61-2-9868-6733
Fax: 61-2-9868-6755

China - Beijing
Tel: 86-10-8569-7000
Fax: 86-10-8528-2104

China - Chengdu
Tel: 86-28-8665-5511
Fax: 86-28-8665-7889

China - Chongqing
Tel: 86-23-8980-9588
Fax: 86-23-8980-9500

China - Hangzhou
Tel: 86-571-2819-3187
Fax: 86-571-2819-3189

China - Hong Kong SAR
Tel: 852-2943-5100
Fax: 852-2401-3431

China - Nanjing
Tel: 86-25-8473-2460
Fax: 86-25-8473-2470

China - Qingdao
Tel: 86-532-8502-7355
Fax: 86-532-8502-7205

China - Shanghai
Tel: 86-21-5407-5533
Fax: 86-21-5407-5066

China - Shenyang
Tel: 86-24-2334-2829
Fax: 86-24-2334-2393

China - Shenzhen
Tel: 86-755-8864-2200
Fax: 86-755-8203-1760

China - Wuhan
Tel: 86-27-5980-5300
Fax: 86-27-5980-5118

China - Xian
Tel: 86-29-8833-7252
Fax: 86-29-8833-7256

China - Xiamen
Tel: 86-592-2388138
Fax: 86-592-2388130

China - Zhuhai
Tel: 86-756-3210040
Fax: 86-756-3210049

ASIA/PACIFIC

India - Bangalore
Tel: 91-80-3090-4444
Fax: 91-80-3090-4123

India - New Delhi
Tel: 91-11-4160-8631
Fax: 91-11-4160-8632

India - Pune
Tel: 91-20-3019-1500

Japan - Osaka
Tel: 81-6-6152-7160
Fax: 81-6-6152-9310

Japan - Tokyo
Tel: 81-3-6880- 3770
Fax: 81-3-6880-3771

Korea - Daegu
Tel: 82-53-744-4301
Fax: 82-53-744-4302

Korea - Seoul
Tel: 82-2-554-7200
Fax: 82-2-558-5932 or
82-2-558-5934

Malaysia - Kuala Lumpur
Tel: 60-3-6201-9857
Fax: 60-3-6201-9859

Malaysia - Penang
Tel: 60-4-227-8870
Fax: 60-4-227-4068

Philippines - Manila
Tel: 63-2-634-9065
Fax: 63-2-634-9069

Singapore
Tel: 65-6334-8870
Fax: 65-6334-8850

Taiwan - Hsin Chu
Tel: 886-3-5778-366
Fax: 886-3-5770-955

Taiwan - Kaohsiung
Tel: 886-7-213-7828
Fax: 886-7-330-9305

Taiwan - Taipei
Tel: 886-2-2508-8600
Fax: 886-2-2508-0102

Thailand - Bangkok
Tel: 66-2-694-1351
Fax: 66-2-694-1350

EUROPE

Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

Denmark - Copenhagen
Tel: 45-4450-2828
Fax: 45-4485-2829

France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

UK - Wokingham
Tel: 44-118-921-5869
Fax: 44-118-921-5820

08/20/13

© 2013 Microchip Technology Inc.

Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

Microchip:
EVB-SEC1110

OCEAN CHIPS
Океан Электроники
Поставка электронных компонентов

Компания «Океан Электроники» предлагает заключение долгосрочных отношений при поставках импортных электронных компонентов на взаимовыгодных условиях!

Наши преимущества:

- Поставка оригинальных импортных электронных компонентов напрямую с производств Америки, Европы и Азии, а так же с крупнейших складов мира;
- Широкая линейка поставок активных и пассивных импортных электронных компонентов (более 30 млн. наименований);
- Поставка сложных, дефицитных, либо снятых с производства позиций;
- Оперативные сроки поставки под заказ (от 5 рабочих дней);
- Экспресс доставка в любую точку России;
- Помощь Конструкторского Отдела и консультации квалифицированных инженеров;
- Техническая поддержка проекта, помощь в подборе аналогов, поставка прототипов;
- Поставка электронных компонентов под контролем ВП;
- Система менеджмента качества сертифицирована по Международному стандарту ISO 9001;
- При необходимости вся продукция военного и аэрокосмического назначения проходит испытания и сертификацию в лаборатории (по согласованию с заказчиком);
- Поставка специализированных компонентов военного и аэрокосмического уровня качества (Xilinx, Altera, Analog Devices, Intersil, Interpoint, Microsemi, Actel, Aeroflex, Peregrine, VPT, Syfer, Eurofarad, Texas Instruments, MS Kennedy, Miteq, Cobham, E2V, MA-COM, Hittite, Mini-Circuits, General Dynamics и др.);

Компания «Океан Электроники» является официальным дистрибьютором и эксклюзивным представителем в России одного из крупнейших производителей разъемов военного и аэрокосмического назначения «**JONHON**», а так же официальным дистрибьютором и эксклюзивным представителем в России производителя высокотехнологичных и надежных решений для передачи СВЧ сигналов «**FORSTAR**».

AVIC JONHON

«JONHON» (основан в 1970 г.)

Разъемы специального, военного и аэрокосмического назначения:

(Применяются в военной, авиационной, аэрокосмической, морской, железнодорожной, горно- и нефтедобывающей отраслях промышленности)

«FORSTAR» (основан в 1998 г.)

ВЧ соединители, коаксиальные кабели, кабельные сборки и микроволновые компоненты:

(Применяются в телекоммуникациях гражданского и специального назначения, в средствах связи, РЛС, а так же военной, авиационной и аэрокосмической отраслях промышленности).

FORSTAR®

Телефон: 8 (812) 309-75-97 (многоканальный)
Факс: 8 (812) 320-03-32
Электронная почта: ocean@oceanchips.ru
Web: http://oceanchips.ru/
Адрес: 198099, г. Санкт-Петербург, ул. Калинина, д. 2, корп. 4, лит. А