

dsPIC[®] Symmetric Key Embedded Encryption Library

Summary

Microchip offers a reliable security solution for embedded applications built on the dsPIC30F platform. This solution is provided by means of two libraries – Symmetric Key and Asymmetric Key Embedded Encryption libraries. The Symmetric Key library features the following:

- Hash Functions
 - SHA-1 Secure Hash Standard
 - MD5 Message Digest
- Symmetric-Key Encryption/Decryption Functions
 - Advanced Encryption Standard (AES)
 - Triple Data Encryption Algorithm (Triple-DES)
- Random Number Generator Functions
 - Deterministic Random Bit Generator ANSI X9.82

Typical Applications

The algorithms supported by this library have emerged as the de facto standard for many large-scale, secured applications like web access, e-mail, secure XML transactions and virtual private networks (VPN). These algorithms are also recommended by most Internet Engineering Task Force (IETF), Federal Information Processing Standards (FIPS) and IPsec Standards. Some typical applications for this library include:

- Mobile and Wireless Devices, PDAs
- Secure Banking
- Secure Web Transactions
 - Secure Socket Layer (SSL)
 - Transport Layer Security (TLS)
 - Secure Multipurpose Internet Mail Extensions (S/MIME)

Typical Applications (Continued)

- ZigBee™ technology and other monitoring and control applications
- Smart Card Readers/Trusted Card Readers
- Friend/Foe Identification
- Secure devices and peripherals interoperating with TCG and NGSCB PC's

The Trusted Computing Group (TCG) and related Microsoft Next-generation Secure Computing Base (NGSCB) both specify RSA and Triple-DES. RSA and other asymmetric solutions are featured in the dsPIC30F Asymmetric Key Embedded Encryption Library (SW300055).

Features

- C-callable library functions developed in MPLAB[®] ASM30 Assembly language
- Optimized for speed, code size and RAM usage:
 - RAM usage below 60 bytes
- Library functions extensively tested for adherence to applicable standards
- Symmetric Key Encryption/Decryption functions support multiple modes of operation:
 - Electronic Code Book (ECB) mode
 - Cipher Block Chaining with Message Authentication (CBC-MAC) mode
 - Counter (CTR) mode
 - Combined CBC-MAC and Counter (CCM) mode
- A comprehensive *dsPIC30F Embedded Encryption Libraries User's Guide* describing the required APIs for the library functions
- Several examples of use are provided for each library function

Cryptographic Functions

| Cryptographic Algorithm | Applicable Specification | Cryptographic Function ⁽²⁾ | Code Size (in bytes) | Data Rate ⁽⁴⁾ (Kbytes/sec) |
|-------------------------|--------------------------|-------------------------------------------|----------------------|---------------------------------------|
| RNG | ANSI X9.82, FIPS 180-2 | Deterministic Random Bit Generator | 1353 | – |
| SHA-1 | FIPS 180-2 | Secure Hash Algorithm – 160 bit | 909 | 423 |
| MD5 | RFC 1321 | Message Digest – 128 bit | 1428 | 656 |
| T-DES | FIPS 46-3 | Basic Encryption and Decryption | 8892 | 49 ⁽³⁾ |
| | FIPS 46-3 | ECB Wrapper ⁽⁴⁾ | 123 | |
| | NIST SP 800-38A | CBC Wrapper ⁽⁴⁾ | 903 | |
| | NIST SP 800-38A | CTR Wrapper ⁽⁴⁾ | 348 | |
| AES (128-bit) | FIPS 197 | Basic Encryption | 2505 | 232 ⁽³⁾ |
| | FIPS 197 | Basic Decryption | 2895 | |
| | FIPS 197 | ECB Wrapper ⁽⁴⁾ | 234 | |
| | FIPS 113 | CBC-MAC Encryption Wrapper ⁽⁴⁾ | 663 | |
| | NIST SP 800-38A | CBC Decryption Wrapper ⁽⁴⁾ | 357 | |
| | NIST SP 800-38A | CTR Wrapper ⁽⁴⁾ | 348 | |
| | IEEE 802.11i | CCM Wrapper ⁽⁴⁾ | 930 | |

Notes:

1. Wrapper functions are used in combination with the underlying basic encryption and/or decryption functions for the respective algorithm (AES,T-DES).
2. All library functions use the stack and require input and output message buffers to be set up by the calling application. Stack usage is below 60 bytes of RAM.
3. AES and T-DES data rate represents the average of the data rates for performing basic encryption and decryption functions for a single block of data.
4. All data rate statistics shown here assume device operation of 30 MIPS.



MICROCHIP

Development Systems

Microchip Technology Incorporated

Getting Started

- Review the dsPIC30F Symmetric Key Embedded Encryption Library web page at www.microchip.com
- Download the dsPIC30F Embedded Encryption Libraries User's Guide from the Microchip web site
- Purchase part number SW300050
- If Asymmetric Key Embedded Encryption Library support is required (part number SW300055), please visit www.microchip.com and review the applicable information

Host System Requirements

- PC-compatible system with an Intel Pentium® class or higher processor, or equivalent
- A minimum of 16 MB RAM
- A minimum of 40 MB available hard drive space
- Microsoft Windows® 98, Windows 2000 or Windows XP

Part Numbers and Ordering Information:

dsPIC® Symmetric Key Embedded Encryption Library

| Part Number | Description | Availability |
|---------------|------------------------------------------------------------------------------------------------------|--------------|
| SW300050-EVAL | dsPIC Symmetric Key Embedded Encryption Library Software License (Evaluation Only) ⁽⁴⁾ | Now |
| SW300050-5K | dsPIC Symmetric Key Embedded Encryption Library Software License (Up to 5K units) ⁽²⁾ | Now |
| SW300050-25K | dsPIC Symmetric Key Embedded Encryption Library Software License (5K+ to 25K units) ⁽²⁾ | Now |
| SW300050-100K | dsPIC Symmetric Key Embedded Encryption Library Software License (25K+ to 100K units) ⁽²⁾ | Now |

Note 1: The evaluation version offers the same functions and features as the other versions. The evaluation period is one year.

2: Quantities are per project, payable as a one-time license fee based on estimated lifetime volume for products resulting from the project. Please consult the factory for quantities above 100K.

dsPIC® Development Tools from Microchip

| | |
|-----------------------------------------------------------------------|------------------------------------------------------|
| MPLAB® IDE | Free |
| MPLAB® Visual Device Initializer (included in MPLAB® IDE) | |
| MPLAB® C30 C Compiler | SW006012 |
| MPLAB® ICD 2 In-Circuit Debugger/Programmer | DV164005, DV164007 |
| MPLAB® ICE 4000 | ICE4000 |
| MPLAB® PM3 Universal Device Programmer | DV007004 |
| dsPIC30F Math Library (included in download of MPLAB® C30 C Compiler) | Free |
| dsPIC30F DSP Library | Free |
| dsPIC30F Peripheral Library | Free |
| dsPICworks™ Data Analysis and DSP Software | Free |
| dsPIC® Digital Filter Design | SW300001 |
| dsPIC30F Soft-Modem Library | SW300002/3/4/5 |
| dsPIC® Speech Recognition Library | SW300010/11/12 |
| dsPIC® Symmetric Key Embedded Encryption Library | SW300050 |
| dsPIC® Asymmetric Key Embedded Encryption Library | SW300055 |
| dsPIC30F Acoustic Echo Cancellation Library | SW300060 |
| dsPIC30F Noise Suppression Library | SW300040 |
| CMX-RTX™ for dsPIC30F | SW300031 |
| CMX-Tiny+™ for dsPIC30F | SW300032 |
| CMX-Scheduler™ for dsPIC® Devices | Free at www.cmx.com |
| dsPICDEM™ Starter Demonstration Board | DM300016 |
| dsPICDEM™ 28-pin Starter Demonstration Board | DM300017 |
| dsPICDEM™ 1.1 General Purpose Development Board | DM300014 |
| dsPICDEM™ MC1 Motor Control Development System | DM300020 |
| dsPICDEM.net™ 1 Connectivity Development Boards | DM300004-1 |
| dsPICDEM.net™ 2 Connectivity Development Boards | DM300004-2 |

Americas: Atlanta (770) 640-0034 • Boston (978) 692-3848 • Chicago (630) 285-0071 • Dallas (972) 818-7423 • Detroit (248) 538-2250 • Kokomo (765) 864-8360 • Los Angeles (949) 462-9523 • Phoenix (480) 792-7200 • San Jose (650) 215-1444 • Toronto (905) 673-0699 • **Asia/Pacific:** Australia-Sydney 61-2-9868-6733 • China-Beijing 86-10-8528-2100 • China-Chengdu 86-28-8676-6200 • China-Fuzhou 86-591-8750-3506 • China-Hong Kong SAR 852-2401-1200 • China-Qingdao 86-532-502-7355 • China-Shanghai 86-21-5407-5533 • China-Shenyang 86-24-2334-2829 • China-Shenzhen 86-755-8203-2660 • China-Shunde 86-757-2839-5507 • India-Bangalore 91-80-2229-0061 • Japan-Kanagawa 81-45-471-6166 • Korea-Seoul 82-2-554-7200 • Singapore 65-6334-8870 • Taiwan-Taipei 886-2-2500-6610 • Taiwan-Kaohsiung 886-7-536-4818 • Taiwan-Hsinchu 886-3-572-9526 • **Europe:** Austria-Weis 43-7242-2244-399 • Denmark-Ballerup 45-4420-9895 • France-Massy 33-1-69-53-63-20 • Germany-Ismaning 49-89-627-144-0 • Italy-Milan 39-0331-742611 • Netherlands-Drunen 31-416-690399 • England-Berkshire 44-118-921-5869 (As of 11/04)

Microchip Technology Inc. • 2355 W. Chandler Blvd. • Chandler, AZ 85224-6199 USA • (480) 792-7200 • FAX (480) 792-7277

The Microchip name and logo, the Microchip logo, Accuron, dsPIC, KEELoQ, microID, MPLAB, PIC, PICmicro, PICSTART, PRO MATE, PowerSmart, rPIC, and SmartShunt are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries. AmpLab, FilterLab, MXDEV, MXLAB, PICMASTER, SEEVAL, SmartSensor and The Embedded Control Solutions Company are registered trademarks of Microchip Technology Incorporated in the U.S.A. Analog-for-the-Digital Age, Application Maestro, dsPICDEM, dsPICDEM.net, dsPICworks, ECAN, ECONOMONITOR, FanSense, FlexROM, fuzzyLAB, In-Circuit Serial Programming, ICSP, ICEPIC, Migratable Memory, MPASM, MPLIB, MPLINK, MPSIM, PICKit, PICDEM, PICDEM.net, PICLAB, PICtail, PowerCal, PowerInfo, PowerMate, PowerTool, rLAB, rPICDEM, Select Mode, Smart Serial, SmartTel and Total Endurance 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. All other trademarks mentioned herein are property of their respective companies.

© 2004, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved. 11/04

DS70128B

