dsPIC® Asymmetric 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 Asymmetric-Key library implements the following:

- Public Key Encryption/Decryption Functions
  - RSA (1024 and 2048 bit)
- Key Agreement Protocol
  - Diffie-Hellman (1024 and 2048 bit)
- Signing and Verification
  - DSA (1024 bit)
  - RSA (1024 and 2048 bit)
- Hash and Message Digest Functions
  - SHA-1, MD5
- Random Number Generator (RNG)
  - ANSI X9.82

Typical Applications

The algorithms supported by this library have emerged as the defacto 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)
- ZigBee™ technology and other monitoring and control applications
- Smart Card Readers
- Friend/Foe Identification
- Peripherals interoperating with TCG and NGSCB personal computers

The Trusted Computing Group (TCG) and related Microsoft Next Generation Secure Computing Base (NGSCB), both specify RSA and Triple-DES. AES, Triple DES and other symmetric solutions are featured in the dsPIC30F Symmetric Key Embedded Encryption Library (SW300050).

Execution Time

For a 1024-bit modulus, when the dsPIC30F device operates at 30 MIPS, average execution times are provided below (in milliseconds):

- RSA Encryption and Verification functions execute in 7 ms for a 17-bit exponent
- RSA Decryption and Signing functions execute in 152 ms for a 17-bit exponent
- DSA Signing function executes in 80 ms
- DSA Verification function executes in 151 ms
- Diffie-Hellman key agreement executes in:
  - 78 ms for 160-bit key
  - 487 ms for 1024-bit key

Features

- C-callable library functions developed in MPLAB ASM30 Assembly language
- Optimized for Speed, Code Size and RAM usage
  - RAM usage below 100 bytes
- Library functions extensively tested for adherence to applicable standards
- A comprehensive *dsPIC30F Embedded Encryption Libraries User's Guide* describing the required APIs for the library functions
- Several examples of use provided for each library function

Getting Started

- Review the dsPIC30F Asymmetric 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 SW300055
- If Symmetric Key Embedded Encryption Library support is required (part number SW300050), please visit www.microchip.com and review the applicable information

Cryptographic Functions

Cryptographic Algorithm	Applicable Specification	Cryptographic Function[1]	Security Strength (in bits)	Code Size[1] (in bytes)[2]
Primary Functions				
RSA	PKSC#1 v1.5	Encryption/Decryption	1024, 2048	2574
RSA	PKSC#1 v1.5	Signing/Verification	1024, 2048	2658
Diffie-Hellman	PKCS#3	Key Agreement Protocol	1024, 2048	2067
DSA	FIPS 186-2	Signing/Verification	1024	4341
Auxillary Functions				
Big Integer Arithmetic Package	–	Modulus Arithmetic Functions Inverse Modulus Arithmetic Montgomery Arithmetic	– – –	927 495 552
Deterministic Random Bit Generator	ANSI X9.82, FIPS 180-2	Random Number Generator	–	1353
SHA-1	FIPS 180-2	Secure Hash Algorithm	160	912
MD5	RFC 1321	Message Digest MD5	128	1428

Notes:

1. 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 100 bytes of RAM.
2. If more than one primary function is used in an application, code size required by the library will be less than the sum of code sizes for individual primary functions. For example, if RSA Signing/Verification and Diffie-Hellman Key Agreement are both used by an application, the library code size linked into the application is 3246 bytes, which is significantly lesser than (2658 + 2067) bytes.

MICROCHIP

Development Systems

Microchip Technology Incorporated

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® Asymmetric Key Embedded Encryption Library

Part Number	Description	Availability
SW300055-EVAL	dsPIC Asymmetric Key Embedded Encryption Library Software License (Evaluation Only)(1)	Now
SW300055-5K	dsPIC Asymmetric Key Embedded Encryption Library Software License (Up to 5K units)(2)	Now
SW300055-25K	dsPIC Asymmetric Key Embedded Encryption Library Software License (5K+ to 25K units)(2)	Now
SW300055-100K	dsPIC Asymmetric 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 MPLAB® Visual Device Initializer (included in MPLAB® IDE)	Free
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

DS70127B