

Features

- Portable ANSI C Implementation
- Software Cryptography Algorithm Implementations
- TeraFire Hardware Accelerator Drivers
- Sophisticated Configuration Management

Benefits

- Processor and Operating System Portable
- Same Code Base for Target Hardware and Software-Based Development Systems

Applications

- Encrypted data storage
- Secure communications
- Secure processing
- SSL and IPsec acceleration
- E-commerce
- VPN
- Mobile Platforms



Cryptographic Application Library

Athena delivers the cryptographic software and hardware drivers to jumpstart your development efforts. The TeraFire® Cryptographic Application Library (CAL) complements Athena's extensive family of cryptographic hardware accelerators by providing both a comprehensive library of software implementations of cryptographic algorithms and the drivers for TeraFire hardware accelerators. This allows you to choose the best combination of software and hardware implementations for your current product and protects your investment for your next application.

Product Description

The TeraFire CAL is a portable library that provides a standard API to access the performance and power advantages provided by TeraFire cryptographic core hardware, and it also provides software implementations of standard algorithms that do not need hardware acceleration. The TeraFire CAL is implemented in ANSI C, is portable to virtually any application environment, and may even be used for host-based development to jumpstart your software development efforts.

Asymmetric/Public Key Ciphers

The TeraFire CAL implements the most requested public key algorithms, including:

- RSA
- DSS
- Suite B Elliptic Curve, including EC-DSA Sign and Verify
- Diffie-Hellman
- IEEE 1363-2000 ECSVDP

Available Deliverables

- ANSI C Source
- Verification suite
- Support
- Documentation

Symmetric Ciphers and Modes

The TeraFire CAL implements the most common secret key ciphers and modes¹, including:

- AES with ECB, CBC, CFB, OFB, CTR, CCM, GCM, and XTS
- 3DES/DES with ECB, CBC, CFB, OFB, and CTR
- Kasumi with UEA1/f8
- SNOW 3G with UEA2
- IEEE 1363a-2004 DL/ECIES

Data Integrity - Hashes and Message Authentication Codes (MACs)

The TeraFire CAL implements multiple data integrity algorithms, including:

- AES with CMAC, CCM, GHASH, and GCM
- SHA-1/224/256/384/512
- MD5
- HMAC
- XCBC MAC
- UIA1/f9 (Kasumi)
- UIA2 (SNOW 3G)

Miscellaneous

Among the other important functions implemented by the TeraFire CAL are key derivation functions and random number generation.

Implementation

The TeraFire CAL has been implemented and tested on multiple platforms, including leading SoC microprocessors from ARM. Athena's sophisticated configuration management system enables rapid configuration of the TeraFire CAL for your mix of hardware accelerator and software implementation requirements.

X5200 Library for X5200 Family Cryptography Microprocessors

The X5200 Library implements high-level algorithms such as RSA with CRT, and elliptic curve operations such as point multiply and EC-DSA sign and verify, in native X5200 assembly language. These functions are designed to execute without host processor intervention, thus providing a complete fire-and-forget cryptographic offload solution for your application. The X5200 Library is packaged with the TeraFire CAL when pur-

1. Modes are implemented for all block ciphers using the same code. Modes are not valid for stream ciphers such as SNOW 3G.

chased with an X5200 family core product. Optional X5200 development tools are also available.

About The Athena Group, Inc.

Based in Gainesville, Florida, Athena innovates breakthrough technologies that achieve the optimum balance of power, performance, and silicon area in a wide range of applications such as wireless, satellite, and secure communications. Athena provides patented semiconductor intellectual property (IP) solutions, with products ranging from the market-leading TeraFire® security cores, to Atomic DSP™ cores, and Atomic SDR™ software defined radio cores.

Athena was founded in 1986 and is privately held.



The Athena Group, Inc.
408 W. University Ave., Suite 306
Gainesville, FL 32601

Phone: (352) 371-2567
Toll-free: (800) 741-7440
Fax: (352) 373-5182
www.athena-group.com
ipsales@athena-group.com

Copyright The Athena Group, Inc., 2011. All rights reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner. The information presented in this document does not form part of any quotation or contract, is believed to be accurate and reliable, and may be changed without notice. No liability will be accepted by the publisher for any consequence of its use. Publication thereof does not convey nor imply any license under patent or other industrial or intellectual property rights.