

## Features

- Comprehensive family of data security and integrity products
- Products optimized for speed, power, and area requirements
- Easy integration into any SoC design

## Benefits

- High-performance
- Low-power
- Rapid delivery via verified firm macro
- Synthesized to your target library and performance requirements
- Fully verified functionality and timing
- Compiled RTL simulation model included

## Applications

- Encrypted data storage
- Secure communications
- Secure processing
- IPsec acceleration
- E-commerce
- VPN
- Financial transactions

## *TeraFire Security Family* *Encryption and Data Integrity*



**The Athena Group delivers a comprehensive family of security processing functions, ready to use for your SoC application.**

Security is an ever-present concern in today's connected world. Hardware security acceleration is a requirement, not just for the server, but for cost and power sensitive mobile terminals such as PDAs and phones too. Hardware security functions provide many benefits over software security functions including increased throughput, and reduced latency, power, CPU load, and clock frequency.

Athena helps you realize these benefits with its comprehensive TeraFire® family of hardware security functions. The TeraFire family encompasses public key cryptography, secret key cryptography, secure hashes, and random number generation functions, which are compliant with the applicable Federal Information Processing Standards (FIPS), National Institute of Standards and Technology (NIST) publications, and Internet Engineering Task Force Request for Comments (IETF RFC). Athena is ready to help you analyze your security hardware requirements and customize a package of functions for your application. Athena's TeraFire security family is summarized in Table 1.

**Table 1: TeraFire Security Product Family**

Model	Description	Performance <sup>a</sup>
AES-A100	Advanced encryption standard (AES)	1.2 Gbps
AES-A200	Standard performance AES	256 Mbps
3DES-A100	Data encryption standard (DES)/triple DES	800/266 Mbps
MD5-A100	Message Digest 5 (MD5)	500 Mbps
SHA1-A100	Secure Hash Algorithm-1 (SHA-1)	640 Mbps
SHA2-A100	SHA-1, SHA-224, SHA-256	800 Mbps
SHA3-A100	SHA2-A100 plus SHA-384 and SHA-512	1.28 Gbps
RNG-A100	True random number generator	50 Mbps
TAI-A100	AHB Bus Interface for crypto functions	N/A
EXP-T500	Lightweight embedded public key cryptography accelerator family	200/s
EXP-T5000	Embedded public key cryptography family	2000/s
EXP-A1000	Ultra-high performance public key cryptography family	10000/s

a. Nominal performance at 100 MHz, higher/lower clock frequencies available. Public key processors specify private-key RSA-1024 operations/second at 250 MHz.

---

## Product Description

Athena's TeraFire public key cryptography solutions showcase the strongest features of Athena's proprietary high-precision multiplier technology: speed, power efficiency, and cost effectiveness. Athena supports your product succession strategy with multiple product families of TeraFire public key cryptography solutions, optimized for applications ranging from battery powered mobile terminals to ultra-high-performance servers.

Athena's market leading public key cryptography accelerators are complemented by AES and DES/3DES secret key cryptography accelerators for bulk data encryption. Athena also offers MD5 and SHA (SHA-1/224/256/384/512) cryptographic hash accelerators, which are required for data integrity verification.

Cryptographic-grade random numbers are required to serve as secret key material, and for negotiating shared keys with other parties using public key cryptography. Cryptographic-grade random numbers can only be produced by starting with non-deterministic sources of randomness, which means that cryptographic-grade random numbers cannot be produced in software only. This makes the Athena RNG-A100 hardware random number generator "must have" technology.

Athena's cryptography accelerators are offered with 'native' interfaces to simplify integration of the accelerators for bump-in-the-wire functionality. Athena also offers the TAI-A100 bus interface for microprocessor bus integration of the TeraFire family of cryptography accelerators.

Each TeraFire family core package is delivered as a firm core optimized to any customer-specified library. The package includes the core, verification suites, timing and simulation models, and documentation. Athena's IP cores are designed for efficient implementation and rapid delivery. The company's proprietary, automated implementation and verification methodology produces synchronous, testable IP cores of the highest quality. All Athena IP cores achieve a score of 95% or better on the OpenMore scale of IP reusability.



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](http://www.athena-group.com)

Copyright The Athena Group, Inc., 2005. 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.

## About The Athena Group, Inc.

The Athena Group, Inc. of Gainesville, Florida licenses high-performance DSP technology that delivers breakthrough performance, reduced area, and lower power consumption in a broad range of SoC products. Athena's proprietary technology powers leading edge applications such as secure e-commerce, wireless communications, and video compression. In addition to their high-value application level solutions, Athena also produces a full line of fundamental DSP functions suitable for SoC integration.

Athena was founded in 1986 and is privately held.

---