

Features

- Platform-Based Design for Anti-Tamper (AT) Applications
- Validated TeraFire® Security Cores
- Secure Boot Software
- Secure Services Software
- Crypto Service Software
- Cryptographic Protection of Application Firmware and Data
- Processor/Bus Portable Architecture
- Broad Standards Compliance
- FIPS 140-2 Certifiable

Benefits

- Defense in Depth Using Information Assurance (IA) and AT Techniques
- Reduced Time to Market
- Reduced Development Costs
- Customized Solution

Applications

- Trusted Platform Module (TPM)
- Encrypted Data Storage
- Secure Communications
- Secure Processing
- Financial Transactions



Anti Tamper (AT) Platform for Secure SoCs

The Athena Group solves the costly problem of deploying AT solutions. The first product of its kind, TeraFire AT circumvents the NRE, manufacturing, and time to market costs of conventional AT approaches. TeraFire AT uniquely combines the AT, design, and cost strengths of single-chip cryptographic modules with information assurance (IA) techniques, and delivers them as a standardized platform that includes both hardware and software. This approach finally bridges the return on investment gap for AT technology in digital electronic systems.

TeraFire AT provides cryptographic protection of application firmware and data, and even protects firmware and data stored off-chip in conventional storage such as RAM or Flash. TeraFire AT also secures interchip communications using strong IA techniques, enabling secure multi-chip systems without costly conventional volume protection. Varying levels of AT security are shown in the sidebar on the following page.

TeraFire AT SoC Environment

TeraFire AT can be used with most SoC microprocessors and bus environments, and is easily adapted to new environments. Figure 2 shows an example of the TeraFire AT-enabled SoC architecture. By separating the application from the security services and enabling hardware and software, the TeraFire AT platform gives application developers the freedom to concentrate on core competencies. TeraFire AT may be implemented in any standard cell ASIC technology, or any other technology that meets the physical requirements for CSP storage. Athena is partnering with silicon providers to enable these features.

TeraFire AT Platform-Based Design

The flexible TeraFire AT platform can be configured to optimally meet each application's unique functional and security requirements, with the minimum system impact. Athena has leveraged over a decade of experience in the implementation and delivery of configured IP cores, optimized to exacting customer requirements, to realize the automated

Why Anti Tamper?

Digital electronic systems embody the majority of the differentiated value of products in virtually every domain. As such, they are an obvious target for tampering attempts, including reverse engineering, firmware theft, manufacturing overproduction and counterfeiting, and modifying the system to operate outside design limits. The negative effects of tampering can be considerable, from loss of competitive advantages and shortened product lifetime, to product liability and increased government regulation.

FIPS 140 Implementation

FIPS 140 defines the requirements for cryptographic modules, but that is only the beginning. As many designers have discovered, FIPS 140 does not specify *how* to get there. FIPS 140 compliance not only requires the implementation of validated cryptographic solutions, but employing these in a systematic way to perform the specified security *processes*, which include management of cryptographic key material and the provision of security services.

Hardware, software, and *expertise* are required to implement this security in an SoC environment. Creation of the requisite hardware and software functionality, integration, and test is costly and time-consuming. The TeraFire AT platform provides hardware and software, *and* embodies the expertise needed to realize a secure FIPS 140 SoC design.

TeraFire AT Capability Stack

Level 1 Cryptography Accelerators

Public Key, AES, SHA, RNG

Level 2 Hardware Services

CSP Store Interface, Secure Clock, Tamper Response

Level 3 Software Services

Secure Services API, Crypto Service Port Monitor, Secure Boot Manager

Level 4 Extended Services

InCipher Memory Protection, Secure Interchip Communication

configuration and implementation system that translates your AT requirements into silicon.

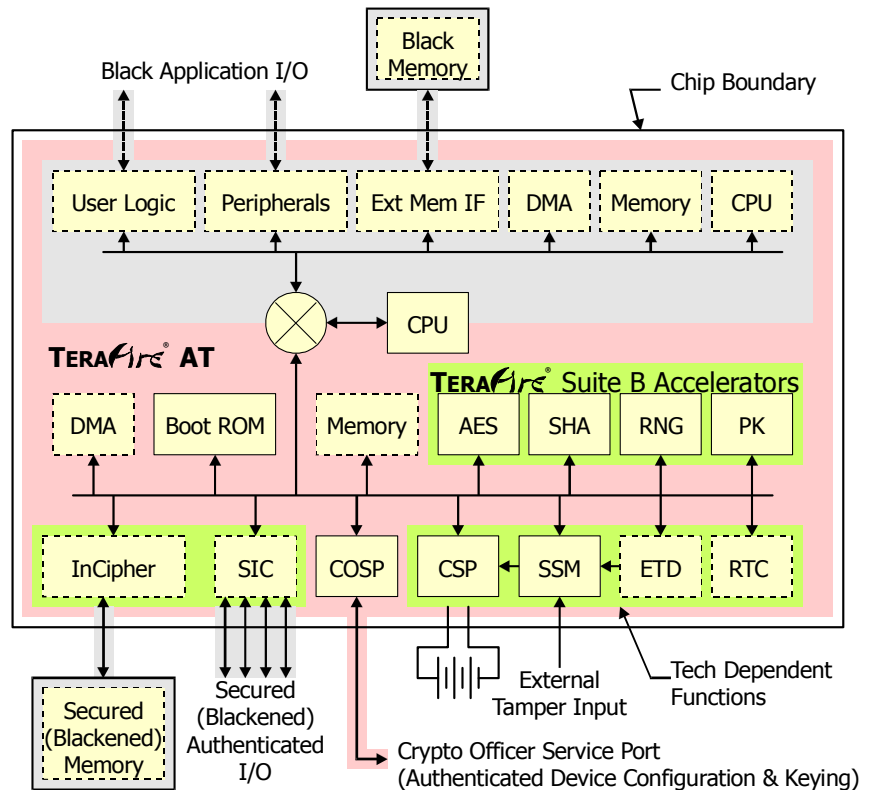


Figure 1: Example TeraFire AT-Enabled SoC

Rapid System Prototyping

TeraFire AT supports rapid system prototyping using the ARM Versatile™ platform. This enables developers to start implementing user-defined hardware and software immediately, with the benefits of at-speed or near at-speed execution prior to manufacturing.

Availability and Engagement Model

Starting in 4Q 2008, Athena is engaging with customers on multiple levels, ranging from turnkey implementation to supported IP configuration and delivery. With multiple licensing models, TeraFire AT platform benefits are within reach for virtually any application.

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.