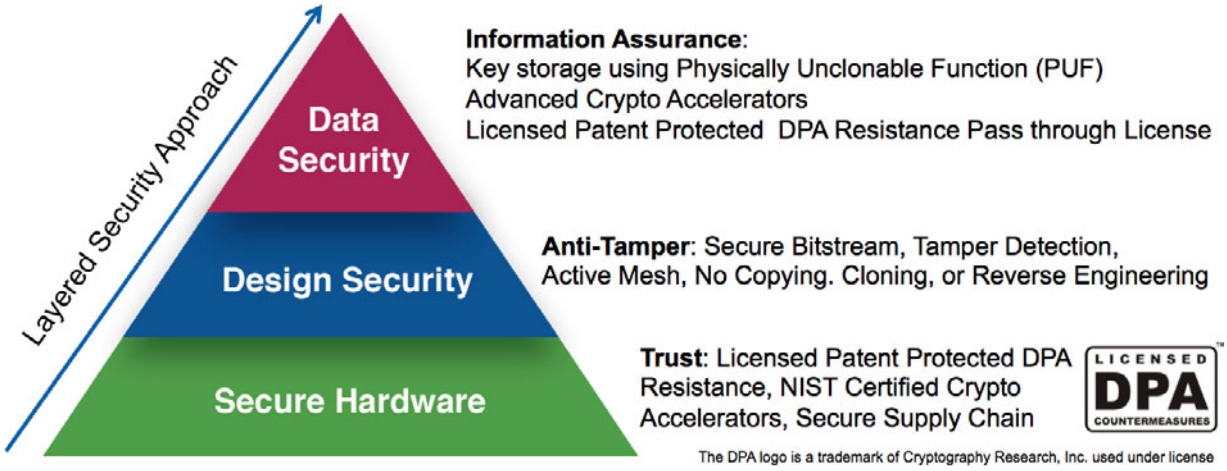
SmartFusion2 SoC and IGLOO2 FPGAs Security Features

Microsemi's fourth generation SmartFusion®2 SoC and IGLOO®2 FPGAs integrate a flash-based FPGA fabric, high-performance communications interface, and an ARM®Cortex®-M3 processor (in the SmartFusion2 devices only) on a single chip. Security is a key attribute for SmartFusion2 SoC and IGLOO2 FPGAs, and is included in all aspects of the device lifecycle—ensuring secure hardware, design security, and data security.

A foundation to secure embedded systems is that the underlying hardware is secure—that is, a level of trust that the underlying hardware is an authentic article from the device manufacturer. Secure hardware acts as the root-of-trust for the system and protects against threats that involve modification of the underlying hardware, such as the counterfeiting or malicious insertion of Trojan horses. Secure hardware is the baseline for protection of the underlying IP of a design (that is to say, design security). In the context of SmartFusion2 SoC and IGLOO2 FPGAs, this is the device configuration file that encapsulates the FPGA system design. Threats against the underlying system design can include tampering, reverse engineering, cloning, remarking, and overbuilding. Design security in turn acts as the baseline for robust security applications at the application layer—Data Security.



The implementation at each abstraction layer (Secure Hardware, Design Security, Data Security) requires a set of services to meet the requirements of cryptographic security—namely confidentiality, integrity, authentication and non-repudiation. As this is security in the context of embedded hardware systems, an additional layer for tamper protection is necessary to ensure a level of protection for physical security. SmartFusion2 SoC and IGLOO2 FPGAs implement a comprehensive feature in support of cryptographic security and anti-tamper protections.

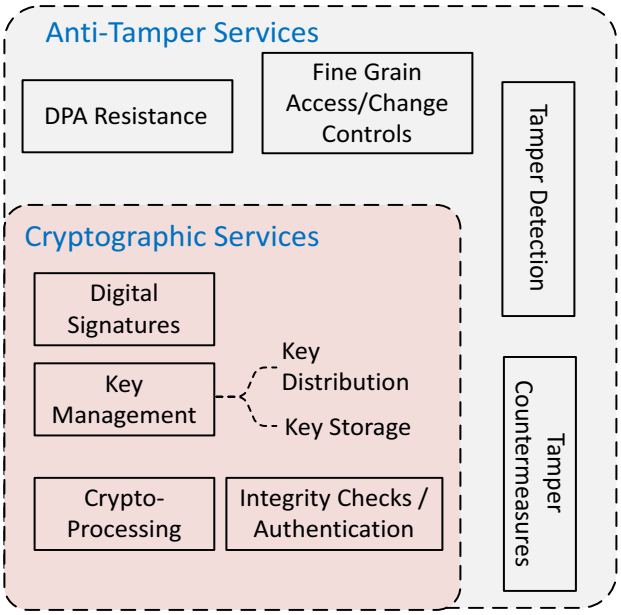
Cryptographic Services include the following:

- Digital Signatures
- Key Management
- Hardened Cores for Cryptographic Processing
- Integrity / Authentication Checks

Anti-tampering Services include the following:

- DPA Resistance
- Access and Change controls

Tamper Detection and Countermeasures



1 – Key Features Overview

Key Features for Secure Hardware

Table 1 • Secure Hardware

Services	Features
Key Management	Factory loaded public device-unique serial #/identifier.
	Encrypted loading of user secret key material (both Symmetric and Asymmetric encryption supported).*
	Key verification protocol to validate secret keys.
	Authenticated/encrypted loading of all factory keys.
	Factory keys and passcodes generated and loaded by Hardware Security Models (HSMs).
Digital Signature Validation	X.509 certificate bound to device serial number, device grading information, and device secret keys.
	Certificates digitally signed by factory HSMs.
	Certificate revocation list for scrapped or stolen devices.
Note: **Asymmetric encryption, and Physically Unclonable Functions (PUFs) are only supported on larger members of the device family (M2S090, M2S100, M2S150, M2GL090, M2GL100, M2GL150).*	

Key Features for Design Security

Table 2 • Design Security

Services	Features
Key Management	Encrypted loading of user secret key material (both Symmetric and Asymmetric encryption supported).[1]
	True Random Number Generators for nonces and private ECC key generation.
	Option to use ephemeral bitstream keys.
	Secure Storage of on-chip secret Keys (encrypted key storage and key storage based on Physically Unclonable Functions).[1]
	Support for disabling specific key mode(s).
Cryptographic Processing	Option to use Elliptic Cure Cryptography for establishing user secret keys.[1]
	All bitstreams are encrypted with AES-256 based encryption and fully authenticated with a 256-bit tag.
	No plaintext bitstreams are ever generated by EDA tools.

Notes:

1. *Asymmetric encryption, and Physically Unclonable Functions (PUFs) are only supported on larger members of the device family (M2S090, M2S100, M2S150, M2GL090, M2GL100, M2GL150).*
2. *ARM Cortex-M3 processors are only available on SmartFusion 2 devices*

Table 2 • Design Security (continued)

Services	Features
Authentication and Integrity	All bitstreams are authenticated with a secure boot process – Keyed-hash Message Authentication Code (HMAC) based on SHA-256.
	On-demand/power-up integrity checks on the fabric configuration array and embedded flash.
	External bitstream verification service, both through re-entry of bitstream and digest-based verification.
	Support for Configuration Variations, where a small part of a bitstream can be unique-per-device, but still authenticated as part of the whole bitstream.
	Fabric Configuration NVM and eNVM Integrity Tests.
	Back-Tracking Prevention (also known as versioning) to prevent reloading of obsolete bitstreams.
	Information services to readout device specific info (S/N, certificates, USERCODE, and so on).
	Digital Certificate-of-Conformance (C-of-C) validate correct bitstreams are loaded in the correct parts.
DPA Resistance	All design security keys and protocols and ECC point multiplication services have countermeasures in place to protect against Differential Power Analysis, with technology licensed from the Cryptographic™ Research Incorporated (CRI).
Access Controls	FlashLock security passcode (256-bit) to prevent unintended changes to security policies with an option to use a "One Time Passcode" challenge-response protocol.
	Option to have passcode-based access for debugging features.
	Flexible access control policies through setting flash lock-bits.
	Support for disabling specific key modes and Flashlock passcodes.
	Option to disable JTAG programming / boundary scan.
	ARM Software Memory Protection Unit.[2]
	Read back of bitstream is always disabled.
Tamper Detection Response	Configurable Zeroization options to clear and verify volatile and non-volatile memory on device.
	Global tri-state of I/O cells.
	Active monitoring of JTAG tap controller for activity.
	Redundancy in the security flash array to allow detection and reporting of any faults.

Notes:

1. *Asymmetric encryption, and Physically Unclonable Functions (PUFs) are only supported on larger members of the device family (M2S090, M2S100, M2S150, M2GL090, M2GL100, M2GL150).*
2. *ARM Cortex-M3 processors are only available on SmartFusion 2 devices.*

Key Features for Data Security

Data security features are only available in premium security device members. In the model number, the three digit capacity number is followed by an “S” designator.

Table 3 • Data Security

Services	Features
Key Management	User SRAM-PUF Enrollment Service[1]
	User SRAM-PUF Activation Code Export Service[1]
	SRAM-PUF Intrinsic Key Generation and Enrollment Service[1]
	SRAM-PUF Key Import and Enrollment Service[1]
	SRAM-PUF Key Regeneration Service[1]
Cryptographic Processing	Non-Deterministic Random Bit Generator Service
	AES-128/256 Service (ECB, OFB, CTR, CBC modes)
	PUF Emulation (Pseudo-PUF)[3]
	PUF Emulation (SRAM-PUF)[1]
	ECC Point-Multiplication Service[1]
	ECC Point-Addition Service[1]
Authentication and Integrity	SHA-256 Service
	HMAC-SHA-256 Service
DPA Resistance	CRI pass-through DPA patent license
	Key Tree Service
Access Controls	Hardware Firewalls protecting access to memories

Notes:

1. *Asymmetric encryption, and Physically Unclonable Functions (PUFs) are only supported on larger members of the device family (M2S090, M2S100, M2S150, M2GL090, M2GL100, M2GL150).*
2. *ARM Cortex™-M3 processors are only available on SmartFusion 2 devices.*
3. *Applicable only for devices without SRAM-PUF.*

2 – Product Brief Information

List of Changes

The following table lists critical changes that were made in each revision of the SmartFusion2 SoC and IGLOO2 FPGAs Security Features Product Brief.

Revision	Changes	Page
Revision 1 (September 2014)	Initial release	NA

Datasheet Categories

Categories

In order to provide the latest information to designers, some datasheet parameters are published before data has been fully characterized from silicon devices. The data provided for a given device is designated as either "Product Brief," "Advance," "Preliminary," or "Production." The definitions of these categories are as follows:

Product Brief

The product brief is a summarized version of a datasheet (advance or production) and contains general product information. This document gives an overview of specific device and family information.

Advance

This version contains initial estimated information based on simulation, other products, devices, or speed grades. This information can be used as estimates, but not for production. This label only applies to the DC and Switching Characteristics chapter of the datasheet and will only be used when the data has not been fully characterized.

Preliminary

The datasheet contains information based on simulation and/or initial characterization. The information is believed to be correct, but changes are possible.

Production

This version contains information that is considered to be final.

Export Administration Regulations (EAR)

The products described in this document are subject to the Export Administration Regulations (EAR). They could require an approved export license prior to export from the United States. An export includes release of product or disclosure of technology to a foreign national inside or outside the United States.

Safety Critical, Life Support, and High-Reliability Applications Policy

The products described in this advance status document may not have completed the Microsemi qualification process. Products may be amended or enhanced during the product introduction and qualification process, resulting in changes in device functionality or performance. It is the responsibility of each customer to ensure the fitness of any product (but especially a new product) for a particular purpose, including appropriateness for safety-critical, life-support, and other high-reliability applications. Consult the Microsemi SoC Products Group Terms and Conditions for specific liability exclusions relating to life-support applications. For more information covering all of the SoC Products Group's products refer to the *Reliability Report*. Microsemi also offers a variety of enhanced qualification and lot acceptance screening procedures. Contact your local *Sales* office for additional reliability information.

Microsemi Corporate Headquarters

One Enterprise, Aliso Viejo, CA 92656 USA. Within the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
Sales.Support@Microsemi.com

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo CA 92656 USA
Within the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
E-mail: sales.support@microsemi.com

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense & security, aerospace and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; security technologies and scalable anti-tamper products; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,400 employees globally. Learn more at www.microsemi.com.

51700129-1/09.14