

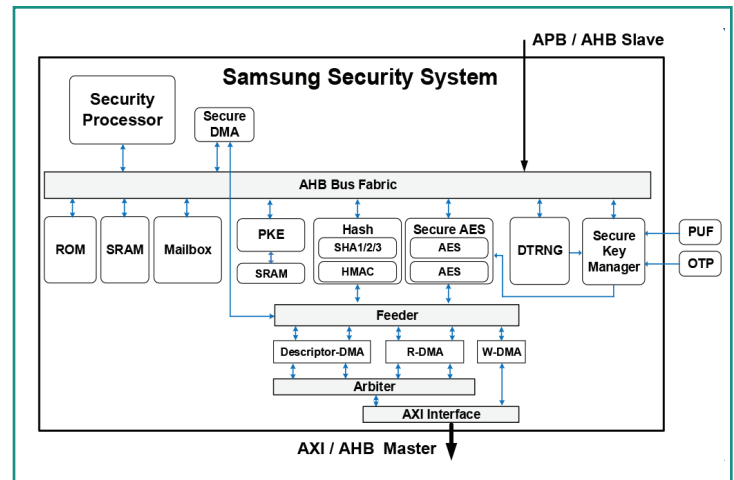
## Samsung Security System IoT

### OVERVIEW

The Samsung Security System (SSS) is a programmable hardware-based root of trust IP that targets a wide-range of Mobile, IoT and Automotive SoC devices. The processing in an isolated execution environment (TEE) secures the execution of sensitive code, processes and algorithms. The SSS offers the primary system processor a full array of security services, such as secure boot and runtime integrity checking, remote authentication and attestation, and hardware acceleration for symmetric and asymmetric cryptographic algorithms.

### KEY FEATURES

- Isolated Execution Environment (IEE)
  - o Security Processor, Secure Boot ROM
  - o RAM for Loadable FW
  - o Mailbox Communication
- Cryptographic Function
  - o Secure AES with Side Channel Attack Countermeasure
  - o SHA1, SHA2-256/384/512, SHA3-SHA224/256/384/512 with HMAC
  - o Public Key Engine (RSA/ECC)
  - o TRNG (NIST SP 800-90B Compliant), PRNG (NIST 800-90A Compliant)
- Secure Key Management
  - o Hardware Key Management using PUF KEY
  - o Key Derivation (SP 800-108) and Wrapping (SP 800-38F) using HW Unique Key
- System Function
  - o Parallel/Concurrent Cryptographic Processing
- ECC (Error Correction Code) Feature
- Power Efficient Scheme
  - o Low Power Features for Both ISP (Isolated Security Processor) and Crypto Engine
- All-in-one Security Solution Package combining SSS and Software Solution



### DELIVERABLES

- Encrypted RTL
- Data Sheet Document
- User Guide Document
- Integration Test C Code & Test Guide Document

### TARGET APPLICATIONS

- Secure Execution Environment
- Secure Booting
- Secure Key Management
- DRM (Digital Right Management)
- Cryptographic Processing

Feature		Description	Crypto System	Mobile	ADAS	IoT
BUS Interface		Master Interface (AMBA3)	AXI (1EA)	AXI (1EA)	AXI (2EA)	AHB (1EA)
		Slave Interface (AMBA3)	APB (2EA)	APB (3EA)	AHB (2EA)	APB (3EA)
Crypto Engine	AES	ECB/CBC/CTR/XTS/CCM/GCM/GMAC	●	●	●	●
		Multiple AES (2EA)		●	●	
		SCA Countermeasure		●	●	●
	(T)DES / RC4	Block Cipher / Stream Cipher	●			
	SM3/SM4	Hash / Block Cipher (ECB)				●
	HASH / HMAC	SHA1	●	●	●	
		SHA2-256/384/512	●	●	●	●
		SHA3-224/256/384/512		●	●	
	PKE	Public Key Engine for RSA / ECC <sup>1)</sup>	●	●	●	●
	PRNG	Pseudo Random Number Generator	●	●	●	
	TRNG <sup>1)</sup>	True Random Number Generator	●	●	●	●
	Key Manager	Secure Key Management	●	●	●	●
	PUF Key	PUF Key Interface		●	●	●
	DMA	For Block Cipher / Hash Engine	●	●	●	
Descriptor DMA	Scatter and Gather Function		●	●		
IEE <sup>6)</sup>	Processor	Security Processor		CM0+	CM7	CM0
	Memory	ROM		40KB	64KB	32KB
		SRAM		32KB	ITCM:256KB DTCM:256KB ICACHE:16KB DCACHE:32KB	16KB
		ECC (Error Correction Code)		●	● (SEC-DED) <sup>2)</sup>	
	Internal DMA	SRAM Backup / Restore		●	●	
WDT	Watchdog Timer			●	●	

1) Elliptic Curve Cryptosystem

2) Single Error Correction – Double Error Detection

# SAMSUNG Foundry

## Foundry Node

The Security System is for implementation in a Samsung Foundry process node. For more information please contact Silvaco at IP@Silvaco.com

# SILVACO

**HEADQUARTERS**  
2811 Mission College Boulevard, 6th Floor  
Santa Clara, CA 95054  
Phone: 408-567-1000  
Fax: 408-496-6080



CALIFORNIA

sales@silvaco.com  
408-567-1000

MASSACHUSETTS

masales@silvaco.com  
978-323-7901

TEXAS

txsales@silvaco.com  
512-418-2929

JAPAN

jpsales@silvaco.com

EUROPE

eusales@silvaco.com

FRANCE

eusales@silvaco.com

KOREA

krsales@silvaco.com

TAIWAN

twsales@silvaco.com

SINGAPORE

sgsales@silvaco.com

CHINA

cnsales@silvaco.com

WWW.SILVACO.COM