Trusted Edge Security Architecture (TESA)

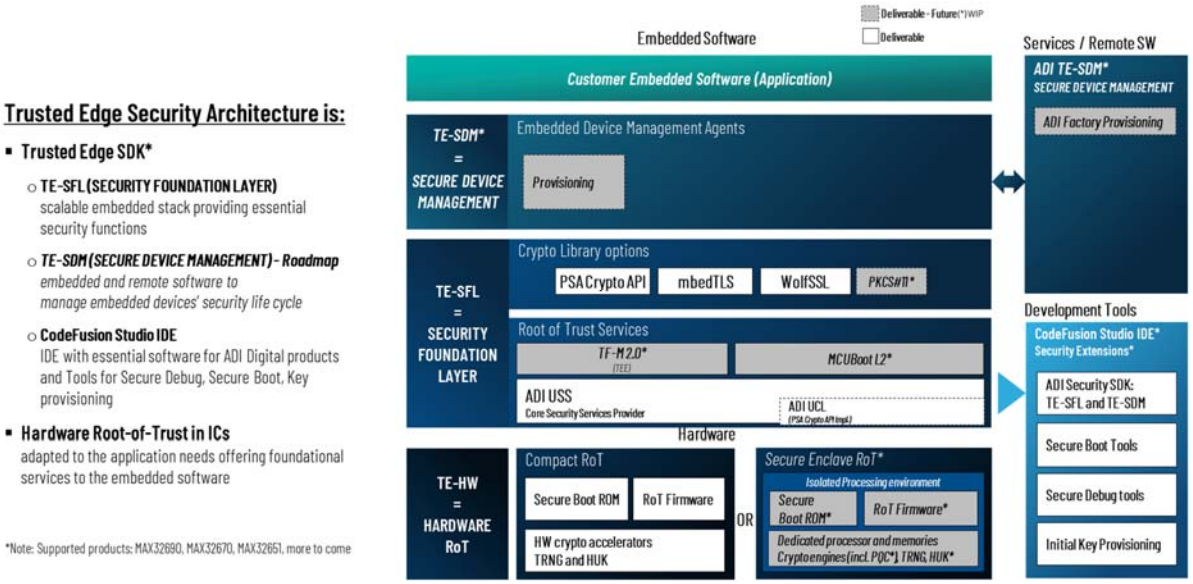
Product Brief

Overview

ADI's security offering for the Intelligent Edge, which is seamlessly bundled into CodeFusion Studio, is called "Trusted Edge Security Architecture" (TESA)

The offering covers the foundational layer of security for the customer by binding industry-standard crypto APIs with the hardware security capabilities of ADI security solutions.

The high-level representation of the offering is given below:



Trusted Edge Security Foundation Layer (TE-SFL)

The Trusted Edge provides flexibility to the user by supporting industry-standard crypto APIs out-of-the-box as part of the security installer: mbedTLS (free), wolfSSL (size optimized), and PSA (standard).

The major benefits of the architecture are:

- Simplicity for accessing the hardware security capabilities of the complete ADI digital portfolio regardless of being an MCU peripheral or discrete integrated circuit-based security solution
- Reduced time-to-market between product iterations

The Trusted Edge Security Foundation Layer contains ***Unified Security Software***, which includes a ***Universal Crypto Library*** for crypto as part of the offering.

Unified Security Software (USS)

Security services API backend for the ADI security offering that provides Secure Boot, Secure Channel, Lifecycle Management, Secure Storage, Cryptographic Toolbox, and Attestation.

The USS enables standalone security services solutions for ADI MCUs. The USS offers a one-stop-shop for security integration with ADI products as it glues the industry standard crypto APIs: mbedTLS, wolfSSL, and PSA. The physical posture of the security is hidden from the application developer, and the development of the security is identical across different postures. This makes the physical architecture transition seamless for ADI customers. This also eases the certification journey of the customers across different product development cycles by embracing re-use.

The USS supports MAX32650, MAX32670, and MAX32690 from the MCU portfolio and integrates the MAXQ1065 Connect Secure Element using the same API.

The examples provide references to help our customers during their development, certification, and manufacturing journey. The breadth of examples includes, but is not limited to provisioning, connected industrial sensors, PSA compliance reports, and crypto toolbox.

Table 1. USS Deliverables

ADI Unified Security Software examples	Provisioning, TLS, Encryption, Signature, Integrity examples.
ADI Unified Security Software Library	TE-SFL glue logic API including an abstraction layer for the physical interface for invoking the security services.
Documentation	Installation Guide, Readme, API Documentation, Benchmark, Example Documentation
Industry Standard Crypto Libraries	mbedTLS, wolfSSL(Download Scripts), PSA test infrastructure

Table 2. USS Target Platforms

MCU	SDK	IDE	Platforms
MAX32670	MSDK	CodeFusion Studio	• MAX32670EVKIT
MAX32690	MSDK	CodeFusion Studio	• AD-APARD32690-SL • MAX32690EVKIT
MAXQ1065	MSDK	CodeFusion Studio	• MAXQ1065EVKIT

Universal Crypto Library (UCL)

The UCL contains the state-of-the-art implementation of the crypto algorithms on ADI MCUs. The offering contains hashing, encryption/decryption, signature/verification, key exchange, and random number generation capabilities. The UCL implements countermeasures to harden the implementation against side-channel attacks. It also utilizes the hardware accelerator of the target ADI platform whenever applicable.

The cryptographic features supported by the UCL is given in table below:

Table 3. Crypto Toolbox Support

Algorithm Family	*Algorithm ID*		
Symmetric Cipher			
	AES	ECB, CBC, CTR, GCM, CCM, Keywrap	
	DES	ECB, CBC, OFB, CFB	
	3DES	ECB, CBC, OFB, CFB	
	SM4		
Public-Key Crypto			
	DSA		
	DH		
	RSA up to 4K bits		
		PKCS1_ES_OAEP	MD5, RIPEMD160, SHA1, SHA2
		PKCS1_MGF1	
		PKCS1_SSA_PKCS1v15	MD5, RIPEMD160, SHA1, SHA2
		PKCS1_SSA_PSS	MD5, RIPEMD160, SHA1, SHA2
	ECC		
		ECDSA	
		ECDH	
		ECIES	
		EDDSA	
		SM2	
HASH			
	SHA1		
	SHA2	SHA-224, SHA-256, SHA-384, SHA-512	
	SHA3		

		SHA3-224, SHA3-256, SHA3-384, SHA3-512
		SHAKE128, SHAKE256
	SIA-256	
	SM3	
	RIPEMD160	
	MD5	
MAC		
	HMAC	SHA1, SHA2, RIPEMD160, MD5
	CMAC	AES, 3DES, CBC-MAC, DES
KDF	HKDF	SHA1, SHA2
	PKCS5V20 PBKDF2	SHA2, SHA2
RNG	TRNG	
	SP800-90A HASH DRBG	

The crypto offering of the architecture contains examples, binary formed static object library for MSDK, and documentation for guiding the user for the utilization of the library and performance numbers as reference for the target platforms.

Table 4. UCL Deliverables

ADI Universal Crypto Library examples	Examples application for exercising features of the crypto toolbox
ADI Universal Crypto Library (object file)	Static Crypto library that includes implementation of the crypto toolbox features
Documentation	Installation Guide, API Documentation, Benchmark

The UCL is supported with MSDK and integrated into CodeFusion Studio. The list of platforms covered by the library is given in **Table *5*. UCL Target Platforms**.

Table 5. UCL Target Platforms

MCU	SDK	IDE	Platforms
MAX32670	MSDK	CodeFusion Studio	• MAX32670EVKIT
MAX32570	MSDK	CodeFusion Studio	• MAX32570-QNKIT

			• MAX32570-MNKIT
MAX32655	MSDK	CodeFusion Studio	• MAX32655EVKIT
MAX32662	MSDK	CodeFusion Studio	• MAX32662EVKIT
MAX32670	MSDK	CodeFusion Studio	• MAX32670EVKIT
MAX32672	MSDK	CodeFusion Studio	• MAX32672EVKIT
MAX32690	MSDK	CodeFusion Studio	• AD-APARD32690-SL • MAX32690EVKIT
MAX78000	MSDK	CodeFusion Studio	• MAX78000EVKIT

Revision History

REVISION NUMBER	REVISION DATE	DESCRIPTION
0	9/19/2024	Initial release