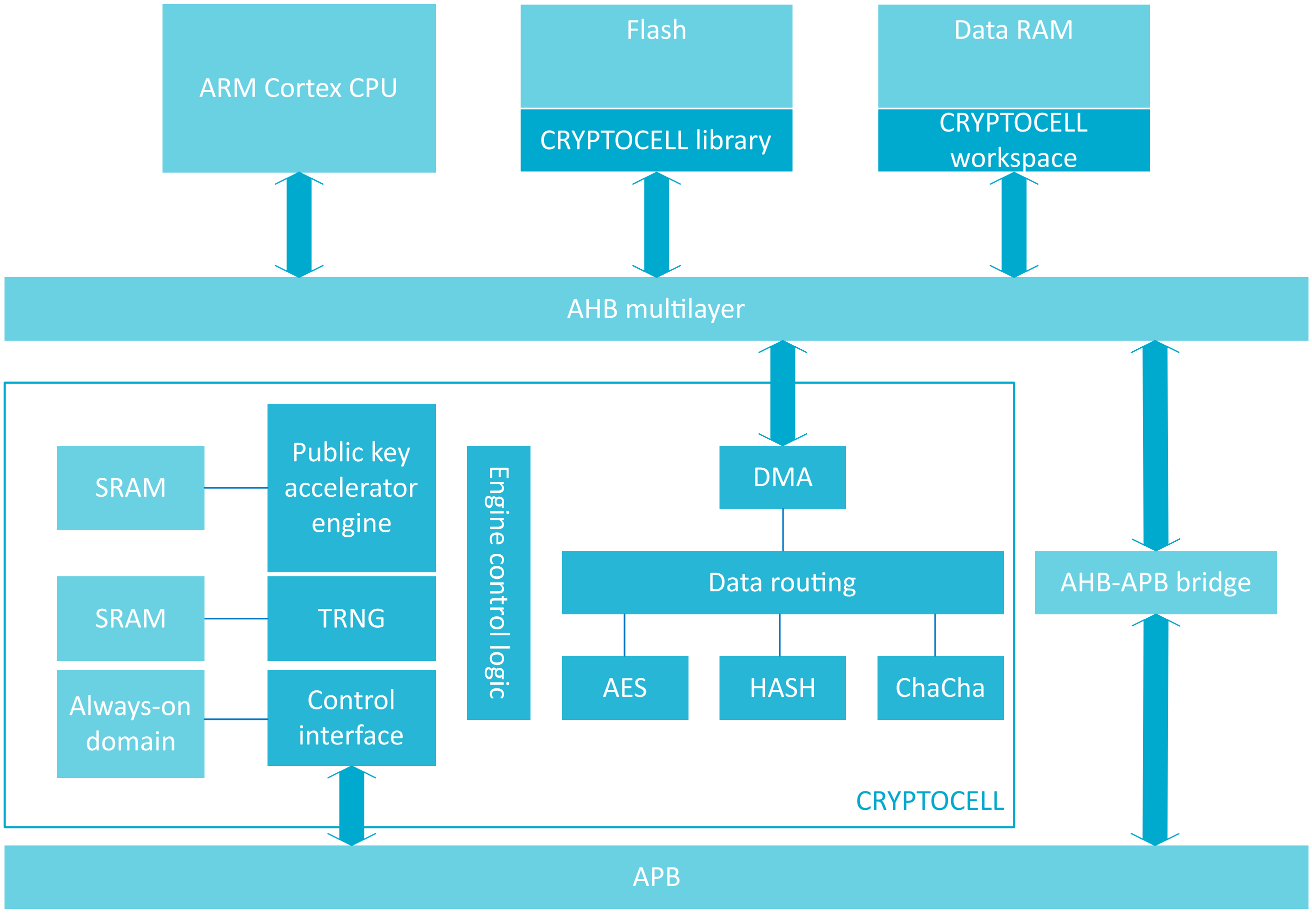
nRF9161 Product Specification

Contents

1. CRYPTOCELL — ARM TrustZone CryptoCell 310

ARM® TrustZone® CryptoCell 310 (CRYPTOCELL) is a security subsystem which provides root of trust (RoT) and cryptographic services for a device.

Figure 1. Block diagram for CRYPTOCELL



The following cryptographic features are provided:

- True random number generator (TRNG) compliant with NIST 800-90B, AIS-31, and FIPS 140-2
- Pseudorandom number generator (PRNG) using underlying AES engine compliant with NIST 800-90A
- RSA public key cryptography
  - Up to 2048-bit key size
  - PKCS#1 v2.1/v1.5

    - Optional CRT support
- Elliptic curve cryptography (ECC)
    - NIST FIPS 186-4 recommended curves using pseudorandom parameters, up to 521 bits:
        - Prime field: P-192, P-224, P-256, P-384, P-521
    - SEC 2 recommended curves using pseudorandom parameters, up to 521 bits:
        - Prime field: secp160r1, secp192r1, secp224r1, secp256r1, secp384r1, secp521r1
    - Koblitz curves using fixed parameters, up to 256 bits:
        - Prime field: secp160k1, secp192k1, secp224k1, secp256k1
    - Edwards/Montgomery curves:
        - Ed25519, Curve25519
    - ECDH/ECDSA support
- Secure remote password protocol (SRP)
    - Up to 3072-bit operations
- Hashing functions
    - SHA-1, SHA-2 up to 256 bits
    - Keyed-hash message authentication code (HMAC)
- AES symmetric encryption
    - General purpose AES engine (encrypt/decrypt, sign/verify)
    - 128-bit key size
    - Supported encryption modes: ECB, CBC, CMAC/CBC-MAC, CTR, CCM/CCM* (CCM* is a minor variation of CCM)
- ChaCha20/Poly1305 symmetric encryption
    - Supported key size: 128 and 256 bits
    - Authenticated encryption with associated data (AEAD) mode

Usage

The CRYPTOCELL state is controlled via a register interface. The cryptographic functions of CRYPTOCELL are accessible by using a software library provided in the device SDK, not directly via a register interface.

To enable CRYPTOCELL, use register ENABLE.

> Note: Keeping the CRYPTOCELL subsystem enabled will prevent the device from reaching the System ON, All Idle state.

Always-on (AO) power domain

The CRYPTOCELL subsystem has an internal always-on (AO) power domain for retaining device secrets when CRYPTOCELL is disabled.

The following information is retained by the AO power domain:

- 4 bits indicating the configured CRYPTOCELL lifecycle state (LCS)
- 1 bit indicating if the hard-coded RTL key, K_{PRTL} (see RTL key), is available for use
- 128-bit device root key, K_{DR} (see Device root key)

A reset from any reset source will erase the content in the AO power domain.

Lifecycle state (LCS)

Lifecycle refers to multiple states a device goes through during its lifetime. Two valid lifecycle states are offered for the device - debug and secure.

The CRYPTOCELL subsystem lifecycle state (LCS) is controlled through register HOST_IOT_LCS. A valid LCS is configured by writing either value Debug or Secure into the LCS field of this register. A correctly configured LCS can be validated by reading back the read-only field LCS_IS_VALID from the abovementioned register. The LCS_IS_VALID field value will change from Invalid to Valid once a valid LCS value has been written.

LCS field value	LCS_IS_VALID field value	Description
Secure	Invalid	Default reset value indicating that LCS has not been configured.
Secure	Valid	LCS set to secure mode, and LCS is valid. Registers HOST_IOT_KDR[0..3] can only be written once per reset cycle. Any additional writes will be ignored.
Debug	Valid	LCS set to debug mode, and LCS is valid. Registers HOST_IOT_KDR[0..3] can be written multiple times.

Table 1. Lifecycle states

Cryptographic key selection

The CRYPTOCELL subsystem can be instructed to operate on different cryptographic keys.

Through register HOST_CRYPTOKEY_SEL, the following key types can be selected for cryptographic operations:

- RTL key K_{PRTL}
- Device root key K_{DR}
- Session key

K_{PRTL} and K_{DR} are configured as part of the CRYPTOCELL initialization process, while session keys are provided by the application through the software library API.

RTL key

The ARM® TrustZone® CryptoCell 310 contains one hard-coded RTL key referred to as K_{PRTL}. This key is set to the same value for all devices with the same part code in the hardware design and cannot be changed.

The K_{PRTL} key can be requested for use in cryptographic operations by the CRYPTOCELL, without revealing the key value itself. Access to use of K_{PRTL} in cryptographic operations can be disabled until next reset by writing to register HOST_IOT_KPRTL_LOCK. If a locked K_{PRTL} key is requested for use, a zero vector key will be routed to the AES engine instead.

Device root key

The device root key K_{DR} is a 128-bit AES key programmed into the CRYPTOCELL subsystem using firmware. It is retained in the AO power domain until the next reset.

Once configured, it is possible to perform cryptographic operations using the CRYPTOCELL subsystem where K_{DR} is selected as key input without having access to the key value itself. The K_{DR} key value must be written to registers HOST_IOT_KDR[0..3]. These 4 registers are write-only if LCS is set to debug mode, and write-once if LCS is set to secure mode. The K_{DR} key value is successfully retained when the read-back value of register HOST_IOT_KDR0 changes to 1.

Direct memory access (DMA)

The CRYPTOCELL subsystem implements direct memory access (DMA) for accessing memory without CPU intervention.

Any data stored in memory type(s) not accessible by the DMA engine must be copied to SRAM before it can be processed by the CRYPTOCELL subsystem. Maximum DMA transaction size is limited to 2^{16}-1 bytes.

Standards

ARM® TrustZone® CryptoCell 310 (CRYPTOCELL) supports a number of cryptography standards.

Algorithm family	Identification code	Document title
TRNG	NIST SP 800-90B	*Recommendation for the Entropy Sources Used for Random Bit Generation*
	AIS-31	*A proposal for. Functionality classes and evaluation methodology for physical random number generators*
	FIPS 140-2	*Security Requirements for Cryptographic Modules*
PRNG	NIST SP 800-90A	*Recommendation for Random Number Generation Using Deterministic Random Bit Generators*
Stream cipher	Chacha	*ChaCha, a variant of Salsa20*, Daniel J. Bernstein, January 28th 2008
MAC	Poly1305	*The Poly1305-AES message-authentication code*, Daniel J. Bernstein *Cryptography in NaCl*, Daniel J. Bernstein
Key agreement	SRP	*The Secure Remote Password Protocol*, Thomas Wu, November 11th 1997
AES	FIPS-197	*Advanced Encryption Standard (AES)*
	NIST SP 800-38A	*Recommendation for Block Cipher Modes of Operation - Methods and Techniques*

Algorithm family	Identification code	Document title
	NIST SP 800-38B	*Recommendation for Block Cipher Modes of Operation. The CMAC Mode for Authentication*
	NIST SP 800-38C	*Recommendation for Block Cipher Modes of Operation. The CCM Mode for Authentication and Confidentiality*
	ISO/IEC 9797-1	AES CBC-MAC per ISO/IEC 9797-1 MAC algorithm 1
	IEEE 802.15.4-2011	*IEEE Standard for Local and metropolitan area networks - Part 15.4. Low-Rate Wireless Personal Area Networks (LR-WPANs)*, Annex B.4: *Specification of generic CCM* mode of operation*
Hash	FIPS 180-3	Secure Hash Standard (SHA1, SHA-224, SHA-256)
	RFC2104	*HMAC. Keyed-Hashing for Message Authentication*
RSA	PKCS#1	*Public-Key Cryptography Standards (PKCS) #1. RSA Cryptography Specifications* v1.5/2.1
Diffie-Hellman	ANSI X9.42	*Public Key Cryptography for the Financial Services Industry. Agreement of Symmetric Keys Using Discrete Logarithm Cryptography*
	PKCS#3	*Diffie-Hellman Key-Agreement Standard*
ECC	ANSI X9.63	*Public Key Cryptography for the Financial Services Industry - Key Agreement and Key Transport Using Elliptic Curve Cryptography*
	IEEE 1363	*Standard Specifications for Public-Key Cryptography*
	ANSI X9.62	*Public Key Cryptography For The Financial Services Industry. The Elliptic Curve Digital Signature Algorithm (ECDSA)*
	Ed25519	Edwards-curve, *Ed25519. high-speed high-security signatures*, Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang
	Curve25519	Montgomery curve, *Curve25519. new Diffie-Hellman speed records*, Daniel J. Bernstein
	FIPS 186-4	*Digital Signature Standard (DSS)*
	SEC 2	*Recommended Elliptic Curve Domain Parameters*, Certicom Research
	NIST SP 800-56A rev. 2	*Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*

Table 2. CRYPTOCELL cryptography standards

Registers

Instances

Instance	Base address	TrustZone			Split access	Description
		Map	Att	DMA		
CRYPTOCELL	0x50840000	HF	S	NSA	No	CryptoCell sub-system control interface

Register overview

Register	Offset	TZ	Description
ENABLE	0x500		Enable CRYPTOCELL subsystem

ENABLE

Address offset: 0x500

Enable CRYPTOCELL subsystem

Bit number	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4
ID																												
Reset 0x00000000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

ID	R/W	Field	Value ID	Value	Description
A	RW	ENABLE			Enable or disable the CRYPTOCELL subsystem
			Disabled	0	CRYPTOCELL subsystem disabled
			Enabled	1	CRYPTOCELL subsystem enabled. When enabled the CRYPTOCELL subsystem can be initialized and controlled t CryptoCell firmware API.

Host interface

This chapter describes host registers used to control the CRYPTOCELL subsystem behavior.

HOST_RGF block

The HOST_RGF block contains registers for configuring LCS and device root key K_{DR}, in addition to selecting which cryptographic key is connected to the AES engine.

Registers

Instances

Instance	Base address	TrustZone			Split access	Description
		Map	Att	DMA		
CC_HOST_RGF	0x50840000	HF	S	NSA	No	Host platform interface

Register overview

Register	Offset	TZ	Description
HOST_CRYPTOKEY_SEL	0x1A38		AES hardware key select
HOST_IOT_KPRTL_LOCK	0x1A4C		This write-once register is the K_PRTL lock register. When this register is set, K_PRTL cannot be used and a zeroed key will be used instead. The value of this register is saved in the CRYPTOCELL AO power domain.
HOST_IOT_KDR0	0x1A50		This register holds bits 31:0 of K_DR. The value of this register is saved in the CRYPTOCELL AO power domain. Reading from this address returns the K_DR valid status indicating if K_DR is successfully retained.
HOST_IOT_KDR1	0x1A54		This register holds bits 63:32 of K_DR. The value of this register is saved in the CRYPTOCELL AO power domain.
HOST_IOT_KDR2	0x1A58		This register holds bits 95:64 of K_DR. The value of this register is saved in the CRYPTOCELL AO power domain.

Register	Offset	TZ	Description
HOST_IOT_KDR3	0x1A5C		This register holds bits 127:96 of K_DR. The value of this register is saved in the CRYPTOCELL AO power domain.
HOST_IOT_LCS	0x1A60		Controls lifecycle state (LCS) for CRYPTOCELL subsystem

HOST_CRYPTOKEY_SEL

Address offset: 0x1A38

AES hardware key select

> Note: If the HOST_IOT_KPRTL_LOCK register is set, and the HOST_CRYPTOKEY_SEL register set to 1, then the HW key that is connected to the AES engine is zero

Bit number	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7
ID																									
Reset 0x00000000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

ID	R/W	Field	Value ID	Value	Description
A	RW	HOST_CRYPTOKEY_SEL			Select the source of the HW key that is used by the AES engine
			K_DR	0	Use device root key K_DR from CRYPTOCELL AO power domain
			K_PRTL	1	Use hard-coded RTL key K_PRTL
			Session	2	Use provided session key

HOST_IOT_KPRTL_LOCK

Address offset: 0x1A4C

This write-once register is the K_PRTL lock register. When this register is set, K_PRTL cannot be used and a zeroed key will be used instead. The value of this register is saved in the CRYPTOCELL AO power domain.

Bit number	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7
ID																									
Reset 0x00000000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

ID	R/W	Field	Value ID	Value	Description
A	RW	HOST_IOT_KPRTL_LOCK			This register is the K_PRTL lock register. When this register is set, K_P and a zeroed key will be used instead. The value of this register is sa CRYPTOCELL AO power domain.
			Disabled	0	K_PRTL can be selected for use from register HOST_CRYPTOKEY_SEL
			Enabled	1	K_PRTL has been locked until next power-on reset (POR). If K_PRTL i zeroed key will be used instead.

HOST_IOT_KDR0

Address offset: 0x1A50

This register holds bits 31:0 of K_DR. The value of this register is saved in the CRYPTOCELL AO power domain. Reading from this address returns the K_DR valid status indicating if K_DR is successfully retained.

Bit number	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5
ID	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
Reset 0x00000000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

ID	R/W	Field	Value ID	Value	Description
A	RW	HOST_IOT_KDR0			Write: K_DR bits 31:0. Read: 0x00000000 when 128-bit K_DR key value is not yet retained in the C power domain.

Bit number	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5
ID	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
Reset 0x00000000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

ID	R/W	Field	Value ID	Value	Description
					Read: 0x00000001 when 128-bit K_DR key value is successfully retained in th AO power domain.

HOST_IOT_KDR1

Address offset: 0x1A54

This register holds bits 63:32 of K_DR. The value of this register is saved in the CRYPTOCELL AO power domain.

Bit number	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5
ID	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
Reset 0x00000000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

ID	R/W	Field	Value ID	Value	Description
A	W	HOST_IOT_KDR1			K_DR bits 63:32

HOST_IOT_KDR2

Address offset: 0x1A58

This register holds bits 95:64 of K_DR. The value of this register is saved in the CRYPTOCELL AO power domain.

Bit number	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5
ID	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
Reset 0x00000000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

ID	R/W	Field	Value ID	Value	Description
A	W	HOST_IOT_KDR2			K_DR bits 95:64

HOST_IOT_KDR3

Address offset: 0x1A5C

This register holds bits 127:96 of K_DR. The value of this register is saved in the CRYPTOCELL AO power domain.

Bit number	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5
ID	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
Reset 0x00000000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

ID	R/W	Field	Value ID	Value	Description
A	W	HOST_IOT_KDR3			K_DR bits 127:96

HOST_IOT_LCS

Address offset: 0x1A60

Controls lifecycle state (LCS) for CRYPTOCELL subsystem

Bit number	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4
ID																								B				
Reset 0x00000002	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

ID	R/W	Field	Value ID	Value	Description
A	RW	LCS			Lifecycle state value. This field is write-once per reset.

Bit number	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4
ID																								B				
Reset 0x00000002	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

ID	R/ W	Field	Value ID	Value	Description
			Debug	0	CC310 operates in debug mode
			Secure	2	CC310 operates in secure mode
B	RW	LCS_IS_VALID			Read-only field. Indicates if CRYPTOCELL LCS has been successfully configured s reset.
			Invalid	0	Valid LCS not yet retained in the CRYPTOCELL AO power domain
			Valid	1	Valid LCS successfully retained in the CRYPTOCELL AO power domain