AN12297

APDU Specification of A71CL for Alibaba Cloud

Rev. 1.2 — 12 December 2018 Application note
511012 COMPANY PUBLIC

Document information

Information	Content
Keywords	Security Module, A71, APDU, ID2
Abstract	This document provides the APDU API specification for the A71CL-Ali security module.

1 Introduction

1.1 Scope

This specification describes the CL applet APDU interface to IoT devices, based on the A710x family with JCOP 2.4.2 R1. It is completely compatible with the ID2 (Internet Device ID) specification known as [ICA/T: 2017-202-01] which mainly supports device ID storage, sensitive data storage, cryptography, signature and message digest.

The ID2 functionality of A71CL supports the following uses cases:

- For device terminal: in terms of device, ID2 can serve as a trust anchor for implementing device authentication, deriving session keys, etc.
- For cloud service: ID2 can provide device authentication service to the clouds;
- For device to device: ID2 can provide offline mutual authentication between devices.

The figure below shows the ID2 system architecture between devices and clouds.

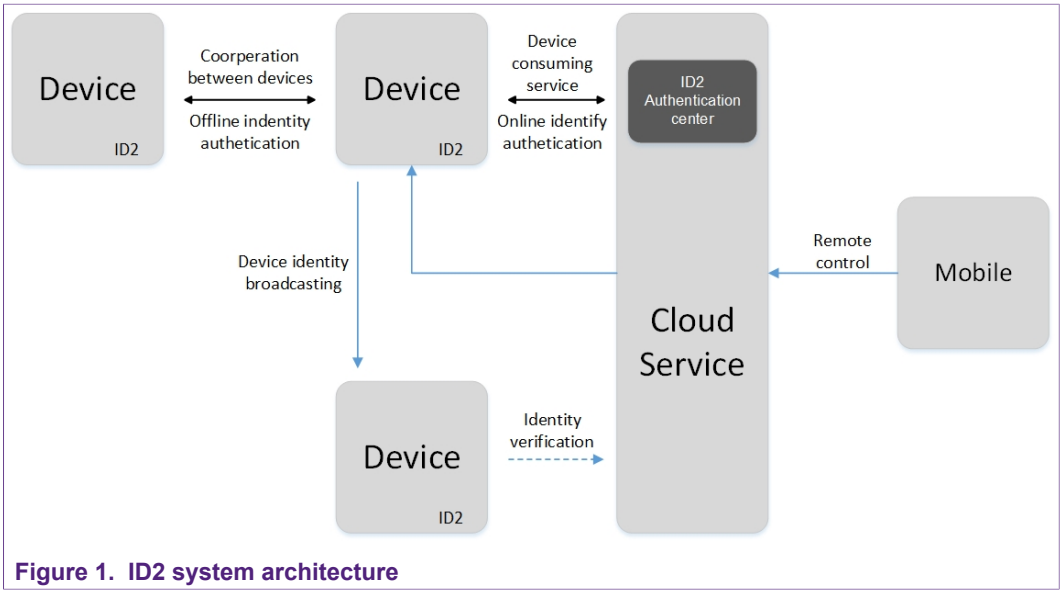

Figure 1. ID2 system architecture

A71CL also supports provisioning and personalization services without involving card-manager privileges using applet-specific keys.

1.2 Architecture

As shown in the architecture diagram below, A71CL consists of a crypto module and a security storage module.

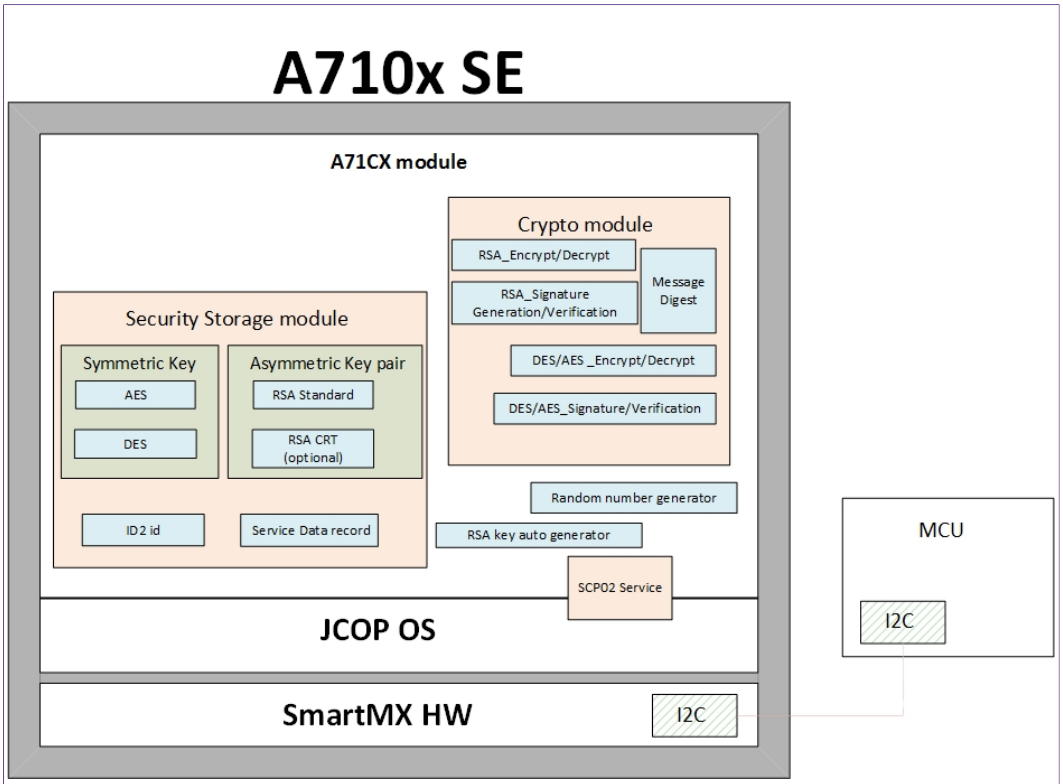

Figure 2. A71CL context

The security storage module acts as a data container. Sensitive data like ID2 ID, Service Data and keys are stored under SCP or RFC 5649 protection.

The crypto module provides cryptographic operations using Cryptography Commands (APDUs).

The provision mode is an alternative way to personalize sensitive data when the card manager is disabled. This service is activated through installation parameter.

1.3 Basic Product Features

The A71CL Security Module provides the following functionality based on [ICA/T: 2017-202-01]:

- Message Digest with SHA1, SHA224, SHA256.
- Random number generator.
- Symmetric Key Storage: one DES key or AES key.
- Asymmetric Key Storage: one RSA Standard keypair or one RSA CRT keypair.
- Auto RSA key generator ranges from 512-bit key length to 2048-bit key length. Including either RSA or RSA CRT.
- Symmetric encryption/decryption with DES_CBC_NOPADDING, DES_ECB_NOPADDING, AES_CBC_NOPADDING, AES_ECB_NOPADDING.
- Symmetric signature generation/verification with DES_CBC_ISO9797_M1, DES_CBC_ISO9797_M2, AES_CBC_ISO9797_M1, AES_CBC_ISO9797_M2.
- Asymmetric encryption/decryption with RSA_NOPADDING, RSA_ PKCS1.
- Asymmetric signature generation /verification with RSA_SHA1(PKCS1), RSA_SHA256.
- Service data storage: Service data record read and write by SCP protection.

- ID2 ID value in secure storage.
- SCP 02 service with option “i” = ‘55’[2].

1.4 A71CL Unsupported Feature

The A71CL Security Module does not support the following functionality described in [ICA/T: 2017-202-01]:

- SM2 and SM3 algorithms.[3]
- ECDSA algorithm.[4]
- SHA-384 and SHA-512 algorithms.[5]

1.5 A71CL Memory View

Table 1. Memory view

Memory type	Applet in A71CL
Number of symmetric keys	1
Number of Asymmetric keys	1
Service data storage size	~5 KB[1]

[1] This value is calculated under A71 with only A71CL applet on EEPROM without security domain.

1.6 Platform Characteristics

1.6.1 APDU Interface

The A71CL deploys an APDU interface as defined in [ISO/IEC 7816-4:2005].

The A71CL supports only standard APDUs. Extended APDUs are not supported.

1.6.1.1 Maximum APDU size

APDUs have a command data payload of maximum 255 bytes and a response data payload of maximum 255 bytes. This limitation applies to all commands when SCP is not active (see 2.4).

When SCP is active the maximum command payload is 239 bytes and the maximum response data payload is 239 bytes.

These limitations are applicable both for the Command APDU and the Response APDU.

2 Refer to E Secure Channel Protocol '02' in GlobalPlatform Card Specification 2.2.1
3 JCOP not supported.
4 No details about ECDSA in [ICA/T: 2017-202-01].
5 JCOP not supported.

2 A71CL configuration

2.1 Provisioning Mode

All the features mentioned in Product Basic Feature (see 1.3) follows [ICA/T: 2017-202-01].

The card manager is enabled. SCP keys are required to manage sensitive data.

2.1.1 APDU Command Reference

The following APDU commands are supported:

Table 2. A71CL APDU commands

Command	Command Supported
Free Read Service Data	yes
ID2_GetChallenge	yes
ID2_SecurityStorageData	yes
ID2_ComputeDigest	yes
ID2_GenerateKeyPair	yes
ID2_SymmetricEncrypt	yes
ID2_AsymmetricEncrypt	yes
ID2_GetID	yes
ID2_GetVendorInfo	yes

Note: commands started with “ID2_” follow [ICA/T: 2017-202-01].

2.2 Initial State

The initial state for all the object storing sensitive data are null unless personalized.

The initial state for mode configuration shall be set during the installation depending on the customers, else the installation will be failed.

2.3 Life Cycle

This section defines the following states applicable to A71CL:

1. UNPERSONALIZED
2. PERSONALIZED

The state is changed implicitly.

The A71CL life cycle coding state can be obtained through the associated Security Domain by the Global Platform command GET STATUS.

2.3.1 UNPERSONALIZED State:

This state indicates that Symmetric or Asymmetric key personalized and cryptography commands are not allowed. After the Symmetric or Asymmetric key is personalized by Sensitive Data Storage commands, the state switches to PERSONALIZED automatically.

A71CL application returns to UNPERSONALIZED automatically if an error occurs during the key personalization, or if triggered by the debug command in the PERSONALIZED state.

2.3.2 PERSONALIZED State:

When either a Symmetric or Asymmetric key is personalized the A71CL life cycle state switches from UNPERSONALZIED to PERSONALIZED.

This state indicated that the cryptography commands are allowed.

2.3.3 Life Cycle Coding[6]

The Life cycle has a bit-oriented code value on one byte as described in the following table. The code value can be read from the associated Security Domain by the Global Platform command GET STATUS.

Table 3. Life cycle coding

B8	B7	B6	B5	B4	B3	B2	B1	Meaning
0	0	0	0	0	0	1	1	UNPERSONALIZED
0	0	0	1	1	1	1	1	PERSONALIZED

2.4 Secure Channel Protocol (SCP)

The Security Module is connected to the Host CPU using, for example, an I2C link employing the SCI2C protocol (compare to [SCI^{2}C] and [A710x]).

The Host to Security Module communication is optionally protected by a Secure Channel Protocol (SCP) according to the [Global Platform SCP02] specification, using "i" = '55':

- Initiation mode explicit,
- C-MAC on modified APDU,
- ICV set to zero,
- ICV encryption for C-MAC session,
- 3 Secure Channel Keys of 128 bits,
- well-known pseudo-random algorithm (card challenge),
- no R-MAC.

2.4.1 Secure Channel Initiation

The Secure Channel initiation is done under the A71CL application by the SCP command pair INITIALIZE UPDATE and EXTERNAL AUTHENTICATE.

2.4.2 Secure Channel APDU Commands

Table 4 summarizes the minimum-security requirements for the APDU commands.

6 Life Cycle Coding is not acceptable for A71CL.

Table 4. Minimum-security

Command	Minimum-security
ID²_SecurityStorage	C-MAC
ID²_Generate Key Pair	Secure Channel initiation
Oher commands	None

2.4.3 Secure Channel Error Condition

Table 6 summarizes the error code Secure Channel initiation or unwrapping may return.

Table 5. Error Condition

SW1	SW2	Comment
0x63	0x00	Authentication of host cryptogram failed
0x67	0x00	Wrong length
0x69	0x82	Security is not satisfied
0x6A	0x88	Referenced data not found
0x90	0x00	Executed correctly

2.5 Security Feature

2.5.1 ID Integrity Protection

The ID² (Internet Device ID) is a character string which links to the unique identifier of equipment, corresponding key, certificate and ID² Server. It is solidified in an element chip and is resistant to tampering and prediction, and globally unique.

2.5.1.1 The Structure of ID Value

The ID value in A71CL is rommified during the first writing in the personalization. The length of ID depends on the user.

The struct below shows how ID is stored.

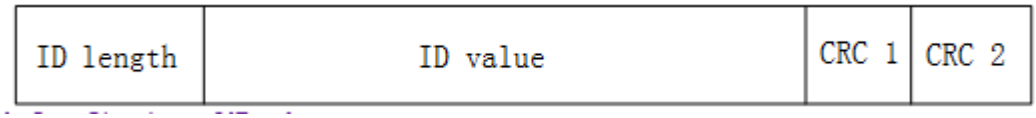

Figure 3. Structure of ID value

The first byte indicates the length of the ID value and the last two bytes is the CRC checksum. The checksum is calculated from ID length to ID value using the CRC-CCITT (0xFFFF) algorithm.

2.5.1.2 Integrity Protection

During the personalization, an ID value will be injected into the A71CL applet as well as its checksum.

The A71CL applet checks the CRC each time the ID2 value is read or used to see if it has been attacked.

2.5.2 Personalization Restriction

The following personalization restrictions apply to A71CL applet:

1. ID2_GenerateKeyPair cannot be executed as long as the ID2_SecurityStorageData command has been executed successfully or the asymmetric key already exists;
2. When the state is in UNPERSONALIZED , the commands ID2_SymmtricEncrypt, ID2_ComputeDigest and ID2_AsymmtricEncrypt cannot be executed.

3 A71CL Coding Rules

3.1 General Coding Rules

3.1.1 A71CL AID

3.1.1.1 Ali Yun configuaration

- Package AID is defined as follows[7]:

'AliYun.ID²':

0xA0, 0x00, 0x00, 0x00, 0x41, 0x6C, 0x69, 0x59, 0x75, 0x6E, 0x2E, 0x49, 0x44, 0x32

- Module ID is defined as follows

'com.nxp.ID2.app':

0x63,0x6f,0x6d,0x2e,0x6e,0x78,0x70,0x2e,0x49,0x44,0x32,0x2e,0x61,0x70,0x70

- Instance AID is defined as follows:

0xA0, 0x00, 0x00, 0x00, 0x41, 0x6C, 0x69, 0x59, 0x75, 0x6E, 0x2E, 0x49, 0x44, 0x32, 0x01

3.1.1.2 A71CL ID Value Configuration

The A71CL ID string is required by each OEM:

Table 6. A71CL ID string

OEM	ID vaule size	ID value
Alibaba	12 bytes	Provided by Alibaba

3.1.2 A71CL Security Application Instruction Set

A71CL security application instruction set is as listed in Table 7:

Table 7. Instruction sets

No	Instruction Name	CLA	INS	Function Description	Compatibility
1	ID²_GetChallenge	00	84	Take random number	ID² Proprietary
2	ID²_SecurityStoreData	84	E2	R/W instruction in secure channel	ID² Proprietary
3	ID²_ComputeDigest	80	F0	Calculate digest value (SHA1 / SHA256)	ID² Proprietary
4	ID²_GenerateKeyPair	80	F2	Generate key pair	ID² Proprietary
5	ID²_AsymmetricEncrypt	80	F4	Asym. algorithms	ID² Proprietary
6	ID²_SymmetricEncrypt	80	F6	Sym. Algorithm (3DES / AES)	ID² Proprietary
7	ID²_GetID	80	F8	Get ID² ID	ID² Proprietary

7 This AID is tentatively determined by IOT Connectivity Alliance.

No	Instruction Name	CLA	INS	Function Description	Compatibility
8	ID²_GetVendorInfo	80	FC	Get vendor information	ID² Proprietary
9	Initialize Update	80	50	To initiates the initiation of a Secure Channel Session	GP Proprietary
10	External Authenticate	84	82	To authenticate the host	GP Proprietary
11	Free Read Service Data	80	71	To be freely read service data	A71CL Proprietary

3.1.3 Key Type

Key type descriptions are as listed in Table 8:

Table 8. Key type

Key type	Value	Description
3DES	'00'	Triple-DES key, symmetric algorithm
AES	'01'	AES key, symmetric algorithm
RSA_Standard	'02'	RSA standard key, asymmetric algorithm
RSA_CRT	'03'	RSA Chinese remainder theorem key, asymmetric algorithm

3.1.4 Key Identifiers

Key element identifiers are as listed in Table 9:

Table 9. Definitions of ID² Security Application Key Storage Identifiers

Type	Flag	Length (byte)	Value
3DES	'40'	'10'or '18'	Key value
AES	'41'	'10'or '18'or'20'	Key value
RSA-CRT-INVQ	'49'	Key mod length/2	INVQ value
RSA-CRT-DP	'50'	Key mod length/2	DP value
RSA-CRT-DQ	'51'	Key mod length/2	DQ value
RSA-D	'64'	Private key value length	Private key value
RSA-E	'65'	'04'	Public key exponent
RSA-N	'6E'	Public key value length	Public key mod value
RSA-CRT-P	'70'	Key mod length/2	Prime P value
RSA-CRT-Q	'71'	Key mod length/2	Prime Q value

3.1.5 A71CL ID² Configuration Options

ID² configuration parameter called 'i' defines the functions the A71CL ID² module supports in the form of 4-byte bitmaps.

B3-B2 and B0 is defined as follows: (byte 0)

Table 10. ID² Configuration Option B0 of 'i'

b8	b7	b6	b5	b4	b3	b2	b1	Description
							1	3DES algorithm supported
						1		AES algorithm supported

B1 is defined as follows:

(byte1)

Table 11. ID² Configuration Option B1 of 'i'

b8	b7	b6	b5		b4	b3	b2	b1	Description
								1	RSA algorithm supported
							1		RSA CRT algorithm supported

B2 is defined as follows:

(byte 2)

Table 12. ID² Configuration Option B2

b8	b7	b6	b5	b4	b3	b2	b1	Description
							1	SHA-1 algorithm supported
						1		SHA-224 algorithm supported
					1			SHA-256 algorithm supported

The example of the 'i':

- i = 0x010101, 3DES, RSA, SHA1 algorithms supported.
- i = 0x000001, 3DES algorithm supported, asymmetric algorithm not supported.

3.1.6 Status Word

SW1 SW2 is the return code of the application execution command. The return information of any command is composed of at least one status word. The return data field is optional.

The status words are described in Table 14.

Table 13. Status Words

SW1	SW2	Description
90	**00**	Executed correctly
61	**xx**	Expected return data length of ISO7816 T0 protocol
62	**81**	The returned data may be wrong.
62	**83**	Selected file invalid, file or key validation error
63	**Cx**	x means the number of re-try times
63	**10**	There is still data not returned
64	**00**	Status flag not changed
65	**81**	Write EEPROM unsuccessfully
67	**00**	Wrong length

SW1	SW2	Description
69	**00**	CLA does not match line protection requirements.
69	**01**	Invalid status
69	**81**	The command is incompatible with the file structure.
69	**82**	Does not meet the secure state
69	**83**	The key is locked.
69	**84**	No random number
69	**85**	Conditions of use are not satisfied.
69	**86**	The selected file is not available.
69	**87**	No security message
69	**88**	Data item in security message is incorrect.
6A	**80**	Data structure error/signature verification failure
6A	**81**	Function not supported
6A	**82**	File not found
6A	**83**	Record not found
6A	**84**	Lack of space
6A	**86**	Parameter P1 P2 error
6B	**00**	The file ends before the Le / Lc byte is reached; the offset is incorrect.
6C	**xx**	Le error
6D	**00**	Instruction code not supported
6E	**00**	Invalid CLA
6E	**01**	Invalid command sequence
6E	**02**	No secure environment or invalid secure environment
6F	**00**	Invalid data
93	**03**	Application locked.
94	**01**	Algorithm not supported
94	**02**	Key type not supported
94	**03**	Key not found
94	**04**	ID input
94	**05**	The key type has existed
94	**06**	Required MAC is not available.
95	**xx**	XX indicates the number of bytes to be transmitted

4 A71CL APDU Interface

4.1 APDU Overview

There are six classified commands for the A71CL:

- Global Platform commands
- Sensitive Data Storage commands
- Cryptography commands
- Debug commands
- Read Information commands

This chapter explains these five classes in more detail.

4.1.1 Global Platform Commands

A71CL owns two Global Platform commands which are used to initiate secure channel.

Table 14. Global Platform commands

Function	Description
GP_INITIALIZE_UPDATE	See GP_InitializeUpdate
GP_EXTERNAL_AUTHENTICATE	See GP_ExternalAuthenticate

4.1.2 Sensitive Data Storage Commands

A71CL has specific commands that can store sensitive data (key or service data).

Table 15. Sensitive Data Storage commands

Function	Description
ID2_SecurityStorageData	See *ID2_SecurityStorageData*
ID2_GenerateKeyPair	*See ID2_GenerateKeyPair*

4.1.3 Cryptography Commands

A71CL offers commands for cryptographic operations.

Table 16. Cryptography commands

Function	Description
ID2_ComputeDigest	See ID2_ComputeDigest
ID2_SymmtricEncrypt	See ID2_SymmtricEncrypt
ID2_AsymmtricEncrypt	See ID2_AsymmtricEncrypt

4.1.4 Read Information Commands

A71CL offers commands that can retrieve information on SE.

Table 17. Read Information commands

Function	Description
ID2_GetChallenge	See ID2_GetChallenge
ID2_GetID	See ID2_GetID
Free Read Service Data	See Free Read Service Data
ID2_GetVendorInfo	See ID2_GetVendorInfo

4.2 APDU Instruction Coding

4.2.1 ID² Application Instruction

4.2.1.1 Get Challenge (Retrieve Random Number) Command

4.2.1.1.1 Definition and scope

The Get Challenge command is used to request a random number for the A71CL application's security process.

The random number can only be used for the next instruction. Whether the next command uses the random number or not, the random number will become invalid immediately.

4.2.1.1.2 Pre-condition

Secure message wrapped by SCP [8] can be used.

4.2.1.1.3 Post-condition

-

4.2.1.1.4 Command message

The command messages are as shown.

Table 18. Get Challenge Command message

Code	Value
CLA	0x00
INS	0x84
P1	0x00
P2	0x00
Lc	Not existing
Data	Not existing
Le	'04'~'10'

8 Secure message refers to the data message wrapped by SCP.

4.2.1.1.5 Command message data field

Command message data field does not exist.

4.2.1.1.6 Response message data field

Thee response message data field is the random number expected to return.

4.2.1.1.7 Response message status code

Table 19. Get Challenge– Status

SW1	SW2	Comment
0x67	0x00	Wrong length
0x6A	0x86	Parameter P1 P2 error
0x90	0x00	Executed correctly

See Secure Channel Error Condition for additional warning status code from SCP that A71CL may send back.

4.2.1.2 ID²_Compute Digest (Compute Digest) Command

4.2.1.2.1 Definition and scope

The Compute Digest command calculates a message digest of the data provided to the command using the specified digest algorithm provided by the command parameters. The ‘to-be-calculated’ data is sent to A71CL application by one or more Compute Digest commands. Upon receipt of all ‘to-be-calculated’ data blocks. The SE returns a fixed length digest of the data.

4.2.1.2.2 Pre-condition

Secure message can be used.

A71CL must be in state “PERSONALIZED”.

4.2.1.2.3 Post-condition

-

4.2.1.2.4 Command message

The ID²_Compute Digest command messages are as shown.

Table 20. ID²_Compute Digest Command message

Code	Value
CLA	0x80
INS	0xF0
P1	Block number (from 0)
P2	01: the last data; 00: the cascaded data (not the last one).
Lc	Length of data to be processed

Code	Value
Data	Data to be processed
Le	Not existing or the length of message digest value expected to return

4.2.1.2.5 Command message data field

The command message data field contains the data to be calculated.

Format definition:

When P1=0:

The command message data field is as shown in Table 21

Table 21. ID²_Compute Digest Command Message Data

Definition	Number of bytes	Description
Type	1	Digest algorithm type: 00: SHA1 01: SHA224 02: SHA256
Data	Lc-1	Block data defined in P1 to be digested

When P1 != ‘00’:

The command message data field is as shown in below table:

Table 22. Command message data field

Definition	Number of bytes	Description
Data	Lc	Data to be calculated

4.2.1.2.6 Response message data field

If the current command is not the last message digest calculation command, the response data field is empty;

If the current command is the last message digest calculation command, the response message is the calculated message digest value.

4.2.1.2.7 Response message status code

Table 23. ID²_Compute Digest– Status

SW1	SW2	Comment
0x6A	0x80	Wrong data
0x6A	0x86	Parameter P1 P2 error
0x6E	0x01	Chaining is invalid
0x94	0x01	Algorithm is not supported
0x90	0x00	Executed correctly

Where A71CL does not support digest algorithm specified by data field, the command returns the status word ‘9401’.(see 7.4.1 for details).

See Secure Channel Error Condition, the additional warning status code from SCP that A71CL may send back.

4.2.1.3 ID²_SecurityStorage (Security Data Operation) Command

4.2.1.3.1 Definition and scope

The ID²_SecurityStorage command is used to write the ID² sensitive data stored in the SE and read no-sensitive-related data.

Sensitive data include ID, keys and other associated sensitive data.

4.2.1.3.2 Pre-condition

Secure channel must be established before this command.

4.2.1.3.3 Post-condition

1. ID value once written cannot be updated.
2. The key data can be updated as long as the ID in the data field is equal to the existing ID.
3. The lifecycle transit to PERSONALIZED.

4.2.1.3.4 Command message

The ID²_SecurityStorage messages are as shown

Table 24. ID²_SecurityStorage Command message

Code	Value
CLA	0x84
INS	0xE2
P1	See P1 parameter description
P2	See P2 parameter description
Lc	Data field length
Data	ID² personalization data
Le	Not existing

P1, the read/write and block number control parameter, is described as follows:

Definition of most significant bit “Bit 7” of P1:

Table 25. Definition of most significant bit “Bit 7” of P1

Bit7	Description	
1	Read instruction	
0	Write instruction	

Definition of secondary significant bit "Bit 6" of P1:

Table 26. Definition of most significant bit “Bit 6” of P1

Bit6	Description
1	Service data instruction
0	Key operation instruction

Definition of P1 Bit5~Bit0:

Table 27. Definition of P1 Bit5~Bit0

Bit5~Bit0	Description
‘XX’	Value range of the block number of cascaded data: "00"~"20"

P2 parameter is cascade identification, which is defined as follows:

Table 28. P2 parameter cascade identification

Bit5~Bit0	Description
‘01’	The last data to be processed
‘00’	Cascade data to be processed

4.2.1.3.5 Command message data field

P1-Bit7 = 0, indicating write instruction:

The data format to be written into the command message data field is defined as follows:

a) If the data field is a key:

Key header data format:

Table 29. ID²_SecurityStorage Key header data format

Definition	Byte number	Description
ID²_id length	‘1’	
ID²_id	X	ID²_ID data
KEY_TYPE	1	See Table 8
KEY_ID	1	‘00’: indicating ID2.Key ‘01’~‘FF’: indicating business-related key
KEY	See table below	

KEY data field format is defined as follows:

Table 30. ID²_SecurityStorage Key data field format

Definition	Byte number	Description
KeyEl01 Tag	1	Tag of the first key element, as seen in Table 10 "Definitions of ID² Security Application Key Storage Identifiers"
KeyEl01 Length	2	Length of the first key element
KeyEl01 Value	KeyEl Length	Value of the first key element
KeyEl02 Tag	1	Tag of the second key element, as is seen in Table 10 "Definitions of ID² Security Application Key Storage Identifiers "

Definition	Byte number	Description
KeyEl02 Length	2	Length of the second key element
KeyEl02 Value	KeyEl Length	Value of the second key element
…		
KeyEln Tag	1	Tag of the nth key element, as is seen in Table 10 "Definitions of ID² Security Application Key Storage Identifiers "
KeyEln Length	2	Length of the nth key element
KeyEln Value	KeyEl Length	Value of the nth key element

Note:

1. If key data are loaded by chaining, the first data include Key header data and the first package of key value content and the following ones include only the key value;

2.When the length of the Key header data + key data value content is less than 256-byte length, all the key data must be loaded at one time.

3. KeyEl 01~KeyEln must be components of the same key.

b) When it comes to the non-key service data:

Table 31. Non-key service data

Definition	Byte number	Description
Data	Lc	Service data

Note:

1. Read instruction data field does not exist.

2. Key-related business correlation settings and data are placed in the service data and the data details are determined by communication between the 3rd party and the OEM. (For example, key attempt limit, key management and maintenance authority, except ID2 key.)

4.2.1.3.6 Response message data field

The response message data do not exist under the write instruction.

The response message data are business associated data under the read instruction.

Note:

1. It is forbidden to read key data by read instruction.

4.2.1.3.7 Response message status code

Table 32. ID²_SecurityStorage – Status

SW1	SW2	Comment
0x69	0x82	Security is not satisfied
0x69	0x84	Data is invalid
0x6A	0x81	Functionality is not supported
0x6A	0x84	Out of memory

SW1	SW2	Comment
0x6E	0x01	Chaining is invalid
0x90	0x00	Executed correctly
0x94	0x01	Algorithm is not supported

See Secure Channel Error Condition for information on the additional SCP warning status code A71CL may return.

4.2.1.3.8 Restriction for service data:

1.The service data should be written or read in chain, otherwise an error code is returned.

2 Each APDU command is atomically updated, and one failed APDU should not affect other segments in the chain

3.When in Plain Injection Mode, the read functionality for service data is forbidden. Instead it is recommended to use the PUT DATA command to write and read service data. Once the Plain Injection Mode changed to default mode, the service data could only be read by FREE READ SERVICE DATA.

4.When in Authentication Mode or Full Reset Mode, the command External Authentication must be executed before using the read functionality for service data.

4.2.1.4 ID²_Generate Key Pair Command

4.2.1.4.1 Definitions and scope

The Generate Key command is used to generate a complete asymmetric key public-private key pair. The specific key record is determined by the KID specified by data field. The public key value of the generated key pair is returned in the response message.

The generated key length is specified by the command data field, and the key length is in the range of 64 to 256 bytes and must be an integer multiple of 8. For example, RSA2048 is 256 bytes in length and 0x0800 in data field.

The KID of the public key must be consistent with that of the private key.

4.2.1.4.2 Pre-condition

The RSA key shall not exist.

This command must establish secure channel before it is executed.

4.2.1.4.3 Post-condition

The lifecycle will transit to PERSONALIZED.

Command message

ID²_Generate Key Pair command message is shown.

Table 33. ID²_Generate Key Pair Command message

Code	Value
CLA	0x80
INS	0xF2

Code	Value
P1	See P1 parameter description
P2	0x00
Lc	0x04
Data	See definition
Le	0x00

P1 parameter definition:

Table 34. P1 parameter definition

Value	Description
0x00	Generate key pair
0x01	Read public key value left when return data field is greater than 256 bytes

4.2.1.4.4 Response message data field

The response message data field contains the generated public key mode.

The response message data field public key data format is shown in Table 28.

Table 35. Response Message Data Field

Type	Tag (T)	Length (L)	Value (V)	Tag (T)	Length (L)	Value (V)
RSA	6E	00 (256bytes)	Public key value N	65	04	'00010001'

4.2.1.4.5 Response message status code

Table 36. ID²_SecurityStorage – Status

SW1	SW2	Comment
0x69	0x82	Security is not satisfied
0x6A	0x81	Functionality is not supported
0x90	0x00	Executed correctly

See Secure Channel Error Condition for information on the additional warning status code from SCP that A71CL may send back.

4.2.1.5 ID²_AsymmetricCrypt Command

4.2.1.5.1 Definition and scope

ID²_AsymmetricCryptcommand is used for asymmetric algorithms using asymmetric operations, including encryption and decryption and signature calculation and verification.

4.2.1.5.2 Pre-condition

Secure message can be used.

A71CL must be in state PERSONALIZED".

4.2.1.5.3 Post-condition

-

4.2.1.5.4 Command message

ID²_AsymmetricCrypt command message is shown.

Table 37. ID²_AsymmetricCrypt Command message

Code	Value
CLA	0x80
INS	0xF4
.P1	See P1 parameter defination
P2	'01': indicates the last data to be processed; '00': indicates cascade data to be processed
Lc	Length of data to be processed (length of data to be processed +5 byte data header, if P1= '00') or does not exist (if P1= '40', take the to-be-returned data left and LC does not exist)
Data	Data to be processed
Le	'00'/'XX'(if P1='40', read the to-be-returned data left)

P1 parameter definition:

Table 38. P1 parameter definition

Bit7~Bit6	Bit5~Bit0	Description
0	-	Application instruction
1	-	Read return value left when return data field is greater than 256 bytes
	'00'~ '20'	Block number: starting from '00'

4.2.1.5.5 Command message data field

The command message data field is the data to be encrypted. Table 31 shows the required content.

Table 39. ID²_AsymmetricCrypt Command message data field

Definition	Number of bytes	Description	Remarks
Mode	1	0x51: encryption 0x52: decryption 0x53: signature 0x54: signature verification	When P1='00', partial data field exists
Algorithm type	1	00: RSA_NOPADDING 01: RSA_SHA1(RSA_PKCS1) 02: RSA_SHA256	
KID	1	KEY index, '00'~ 'FF'	

Definition	Number of bytes	Description	Remarks
Length	2	Data length to be processed	
Data	Length	Data to be processed	

Note:

data field description

Table 40. Table

P1	P2	Mode	Algorithm types	Data	Description
0x00	0x00/01	0x51,0x52	0xx00,0x01	1-byte KID + 2 bytes length + data	P1 P2: 0001 indicates only one data block
		0x53,0x54	0x01,0x02,0x03,0x04,0x05,0x06		
0x01-0x20		——	——	Data	The nth data block
0x40	0x00	——	——	--	Le: xx more data to be returned

Note:

The signature verification data format shall be signature verification plaintext data + signature data.

4.2.1.5.6 Response message data field

Response message data field is an encrypted ciphertext and the Table 32 shows the required content:

Table 41. Response message data field

Definition	Requirements
Total response data length (2 bytes)	Return in the first response
RSA	Ciphertext length = algorithm mode length

4.2.1.5.7 Response message status code

Table 42. ID²_AsymmetricCrypt – Status

SW1	SW2	Comment
0x69	0x82	Security is not satisfied/ signature verification failed
0x6A	0x81	Functionality is not supported
0x90	0x00	Executed correctly

See Secure Channel Error Condition for more information on the error code.

4.2.1.6 ID²_SymmetricCrypt Command

4.2.1.6.1 Definition and scope

ID²_SymmetricCrypt command is used for symmetric encryption or MAC calculation.

4.2.1.6.2 Pre-condition

Secure message can be used.

When A71CL state is in state PERSONALZIED.

4.2.1.6.3 Post-condition

-

4.2.1.6.4 Command message

ID²_SymmetricCrypt message is shown.

Table 43. ID²_SymmetricCrypt Command message

Code	Value
CLA	0x80
INS	0xF6
P1	Block number: '00'~ '20' Starting from '00'
P2	'01': indicates the last to-be-processed data; '00': indicates cascade to-be-processed data
Lc	Length of to-be-processed data
Data	To-be-processed data
Le	Length of data which do not exist or are expected to be returned

4.2.1.6.5 Command message data field

Command message data field contains data to be processed.

Table 44. Command message data field

Definition	Number of byte	Description
Mode	1	0x51: encryption 0x52: decryption 0x53: calculate MAC 0x54: verify MAC
Algorithm type	1	0x00: DES_CBC_NOPADDING 0x01: DES_ECB_NOPADDING 0x02: AES_CBC_NOPADDING 0x03: AES_ECB_NOPADDING 0x04: DES_CBC_ISO9797_M1 0x05: DES_CBC_ISO9797_M2 0x06: AES_CBC_ISO9797_M1 0x07: AES_CBC_ISO9797_M2
KID	1	KEY index, '00'~ 'FF'
Length	2	Total length of data to be processed

Definition	Number of byte	Description
Data	Length	Data to be processed

Note:

1. *Complete data field description: if the length of the total data exceeds the maximum length of one command the data may be split into several cascading commands. Only the first package has algorithm pattern + algorithm types + KID.*
2. *By default, the symmetric algorithm's encryption and decryption padding option is set to No padding. All algorithm padding and calculation is completed outside A71CL and is then given to the A71 to calculate data.*
3. *MAC calculation of symmetric algorithm supports M1 and M2 Padding besides No padding mode.*
4. *Data field description:*

Table 45. Data field description

Definition	Mode	Algorithm types	Number of bytes	Description
IV	0x51,0x52 0x53,0x54	0x00	8	Initial vector
		0x02,0x04,0x05,0x06,0x07,0x10,0x12,0x14,0x15,0x16,0x17	16	
		Others	0	
Data	All	All		Data to be calculated
MAC	0x54	0x00	8	MAC to be verified
		0x02,0x04,0x05,0x06,0x07,0x10,0x12,0x14,0x15,0x16,0x17	16	
	Others	All	0	

4.2.1.6.6 Response message data field

Return of response message data field (symmetric algorithm result data or MAC value).

Calculated results description is as follows:

Table 46. Response message data field

Mode	Number of byte	Description
'0x51': encryption '0x52': decryption	integral multiple of 0 or 8/16	Encryption/decryption operation is made and returned upon receipt of the key algorithm block length data
'0x53': calculate MAC	0 or 8/16	Return MAC value after receiving all the data and MAC value is the last block in the CBC algorithm.
'0x54': verify MAC	0	No return

MAC algorithm refers to Annex B.

4.2.1.6.7 Response message status code

Table 47. ID²_SymmetricCrypt – Status

SW1	SW2	Comment
0x69	0x82	Security is not satisfied/MAC verification failed
0x6A	0x81	Functionality is not supported
0x90	0x00	Executed correctly

See Secure Channel Error Condition for more information on the error code.

4.2.1.7 ID²_GetID Command

4.2.1.7.1 Definition and scope

ID²_GetID command is used to read the ID value from ID² security application.

4.2.1.7.2 Pre-condition

Secure message can be used in default mode.

ID value is stored.

4.2.1.7.3 Post-condition

4.2.1.7.4 Command message

ID²_GetID command message is shown

Table 48. ID²_GetID Command message

Code	Value
CLA	0x80
INS	0xF8
P1	0x00
P2	0x00
Lc	Does not exist
Data	Does not exist
Le	'XX'

4.2.1.7.5 Command message data field

Command message data field does not exist.

4.2.1.7.6 Response message data field

The requirements for the response message data field are as follows:

The returned data is the OEM's information formatted as follows:

Table 49. Response message data field

Information	Number of byte	Description
OEM identification	2	-
Length	1	ID² ID Length
ID² ID	Length	ID² ID string

4.2.1.7.7 Response message status code

Table 50. ID²_GetID – Status

SW1	SW2	Comment
0x6A	0x80	Wrong data
0x6A	0x81	Functionality is not supported
0x90	0x00	Executed correctly

See Secure Channel Error Condition for more information on the error code.

4.2.1.8 ID²_GetVendorInfo Command

4.2.1.8.1 Definition and scope

The Get Vendor Info command is used to request information of OEM to the A71CL applet.

4.2.1.8.2 Pre-condition

Secure message can be used.

4.2.1.8.3 Post-condition

-

4.2.1.8.4 Command message

ID²_GetID command message is shown

Table 51. ID²_GetVendorInfo Command message

Code	Value
CLA	0x80
INS	0xFC
P1	0x00
P2	0x00
Lc	Does not exist
Data	Does not exist
Le	'XX'

4.2.1.8.5 Command message data field

Command message data field does not exist.

4.2.1.8.6 Response message data field

The requirements for the response message data field are as follows:

The returned data is the OEM's information formatted as follows:

Table 52. Response message data field

Information	Length
OEM identification	2 bytes
Version information	8 bytes
ID2 configuration options	4 bytes
Available space	2 bytes
Extension bit	4 bytes

4.2.1.8.7 Response message status code

Table 53. ID²_GetVendorInfo – Status

SW1	SW2	Comment
0x69	0x84	Data is invalid
0x90	0x00	Executed correctly

See Secure Channel Error Condition for more information on the error code.

4.2.1.9 Free Read Service Data

4.2.1.9.1 Definition and scope

The Free Read Service Data is used to read the service data written through PUT DATA. The Plain text return from this command can be freely read by off-card entity without authentication.

4.2.1.9.2 Security condition:

None.

4.2.1.9.3 Pre-condition

A71CL must be in state PERSONALIZED"

4.2.1.9.4 Post-condition

-

4.2.1.9.5 Command message

Table 54. Free Read Service Data command message

Code	Value
CLA	0x80
INS	0x71
P1	Record Number with high byte

Code	Value
P2	Record Number with low byte
Le	0x00

4.2.1.9.6 Response message data field

Table 55. Response message data field

Value	Comment
Plaintext data chunk	Byte array contains service data with plaintext controlled by record number.

4.2.1.9.7 Response message status code

Table 56. Response message status code

SW1	SW2	Comment
0x67	0x00	Length is incorrect
0x6A	0x82	Record not found
0x90	0x00	No error

5 A71CL Implementation Notes

5.1 Hardware Interface

A number of hardware interfaces are available. Refer to the hardware documentation for a full overview, but Table 57 lists the protocols in use.

Table 57. Hardware interface specifications

HW interface	Protocol specification	Protocol details
I2C	SCI2C	an195015 - Application note SCIIC Protocol Specification (1.5)

5.2 EEPROM Write Access

The hardware supports a limited number of EEPROM write accesses. Integrators have to take care to avoid unnecessary EEPROM writes due to calling commands that access & write to EEPROM. Table 58 gives an overview of commands that write to EEPROM.

Table 58. Commands writing to EEPROM

Command	Remark
ID2_SecurityStorageData	
ID2_GenerateKeyPair	

6 Annex A (Informative) OEM Identification

6.1 A.1 OEM Identification

The identification is shown as follows when the OEM in IOT Connectivity Alliance uses ID² security application commands:

Table 59. OEM Identification

Security OEM	OEM identification
NXP Semiconductors	8182

Note: The OEM identification of SE vendor shall be distributed by IOT Connectivity Alliance.

7 Annex B (Normative) CMAC Algorithm

7.1 B.1 CMAC Algorithm

CMAC algorithm adopts “MAC algorithm 1” as specified in ISO 9797-1.

8 Document Management

8.1 Abbreviations and Terminology

Table 60. Abbreviations

Abbreviation	Description
AID	Application Identifier
APDU	Application Protocol Data Unit
ATR	Answer to Reset
b	Binary
BER	Basic Encoding Rules
BWI	Block Waiting Time Integer
CLA	Class Byte of the Command Message
CWI	Character Waiting Time Integer
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DF	Dedicated File
EDC	Error Detection Code
EF	Elementary File
Etu	Elementary Time Unit
FCI	File Control Information
FID	File Identifier
GND	Ground
Hex.	Hexadecimal
IC	Integrated Circuit
ICC	Integrated Circuit Card
IEC	International Electrotechnical Commission
INS	Instruction Byte of Command Message
ISO	International Standardization Organization
Lc	the actual length of the command data field sent by terminal
Le	the maximum expected length of the response data
LEN	Length
MAC	Message Authentication Code
MF	Master File
P1	Parameter 1
P2	Parameter 2
PBOC	People’s Bank of China
PIN	Personal Identification Number

Abbreviation	Description
PIX	Proprietary Application Identifier Extension
PSA	Payment System Application
PSAM	Purchase Secure Access Module
PSE	Payment System Environment
RFU	Reserved for Future Use
RID	Registered Application Provider Identify
RSA	Rivest,Shamir,Adleman
RST	Reset
SAM	Secure Access Module
SFI	Short File Identifier
SHA	Secure Hash Algorithm
SW1	Status Word One
SW2	Status Word Two

8.2 Referenced Documents

Table 61. Referenced documents

Doc ID	Doc Title
[RFC5649]	Advanced Encryption Standard (AES) Key Wrap with Padding Algorithm [August 2009]
[RFC3394]	Advanced Encryption Standard (AES) Key Wrap Algorithm [September 2002]
[ISO/IEC 7816-4:2013]	Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange [2013-04-15]
[ICA/T: 2017-202-01]	Instruction Specification of ID² Application, Issue date: 2017-10-01

8.3 Revision history

Table 62. Revision history

Document ID	Release date	Document status	Change notice	Supersedes
511012	2018-12-12	Application note	Customized for A71CL-Ali	511011
511011	2017-07-10	Application note	Added ID type for each OEM supported	511010
511010	2017-01-31	Application note	Initial draft version	-

9 Legal information

9.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

9.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer. In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages. Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

9.3 Licenses

ICs with DPA Countermeasures functionality

LICENSED DPA COUNTERMEASURES™

NXP ICs containing functionality implementing countermeasures to Differential Power Analysis and Simple Power Analysis are produced and sold under applicable license from Cryptography Research, Inc.

9.4 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

Kinetis — is a trademark of NXP B.V.

AMBA, Arm, Arm7, Arm7TDMI, Arm9, Arm11, Artisan, big.LITTLE, Cordio, CoreLink, CoreSight, Cortex, DesignStart, DynamIQ, Jazelle, Keil, Mali, Mbed, Mbed Enabled, NEON, POP, RealView, SecurCore, Socrates, Thumb, TrustZone, ULINK, ULINK2, ULINK-ME, ULINK-PLUS, ULINKpro, µVision, Versatile — are trademarks or registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. The related technology may be protected by any or all of patents, copyrights, designs and trade secrets. All rights reserved.

Bluetooth — The Bluetooth word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by NXP Semiconductors is under license.

Tables

Figures

Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 12 December 2018
Document identifier: AN12297
Document number: 511012