A5000

EdgeLock Secure Authenticator

Rev. 1.6 — 5 August 2024
667616

Product data sheet

1 Introduction

The A5000 is a ready-to-use secure IoT authenticator. It provides a root of trust at the IC level and it gives an IoT authentication system state-of-the-art security capability right out of the box.

A5000 allows for securely storing and provisioning credentials and performing cryptographic operations for security critical communication and authentication functions. A5000 is versatile in IoT security use cases such as secure connection to public/private clouds, device-to-device authentication or counterfeit protection

A5000 has an independent Common Criteria EAL 6+ security certification up to OS level and supports ECC asymmetric cryptographic and AES/3DES symmetric algorithms. The latest security measures protect the IC even against sophisticated non-invasive and invasive attack scenarios.

The A5000 is a turnkey solution that comes with an authentication application optimized for authentication security use cases pre-installed. This is complemented by an authentication tailored product support package, enabling fast time to market & easy design-in with Plug & Trust middleware for host applications, easy to use development kits, reference designs, and documentation for product evaluation.

To implement inclusive language, the terms "master/slave" has been replaced by "controller/target", following the recommendation of MIPI.

1.1 A5000 use cases

- Device-to-device authentication
- Secure data protection and storage
- Secure connection to public/private clouds, edge computing platforms, infrastructure
- DLMS/COSEM Compliance for Smart Metering
- Secure key storage
- Secure provisioning of credentials
- Medical sensor and devices
- Qi 1.3 wireless charging authentication
- Matter Ready

1.2 A5000 target applications

- Smart Metering
- Smart Home
- Accessories and Smart Appliances
- Anti-Counterfeit

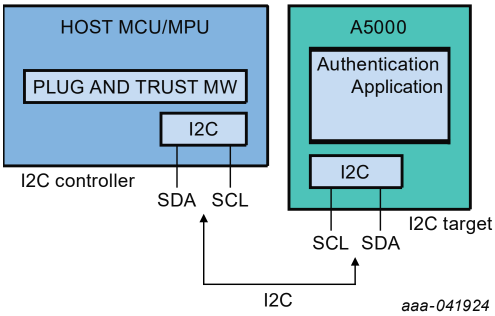


Figure 1. A5000 solution block diagram

Note: *A5000 is designed to be used as a part of an IoT or Authentication system. It works as an auxiliary security device attached to a host controller. The host controller communicates with A5000 through an I^2C interface (with the host being the controller and the A5000 being the target).*

1.3 A5000 naming convention

The following table explains the naming conventions of the commercial product name of the A5000 platform. Every A5000 product gets assigned a commercial name, which includes application specific data.

The A5000 commercial names have the following format.

A5000agddd/Zrrff

All letters are explained in Table 1 .

Table 1. A5000 commercial name format

Variable	Meaning	Values	Description
a	Product Config	C,R	Configuration options, refer to Configuration paragraph
g	Temperature range	2	Extended operational ambient temperature 2 = -40 °C - 105 °C
ddd	Delivery Type	HQ1	HX2QFN20
Zrrff		Letters and numbers	NXP internal code to identify individual configurations

2 Features and benefits

2.1 Key benefits

- Plug & Trust for fast and easy design with dedicated product support package for authentication use cases
- Easy integration with different MCU & MPU platforms and OSs (Linux, RTOS, Windows, Android, etc.)
- Turnkey solution ideal for many authentication use cases without the need to write security code
- Secure credential injection for proof of origin check
- Anti-counterfeit solution
- Secure, zero-touch connectivity to public & private clouds
- Real end-to-end security in authentication system from smart metering to smart home appliances
- Ready-to-use example code for each of the key use cases such as device-to-device authentication and originality check

2.2 Key features

The A5000 provides a secure and efficient protection for authentication and anti-counterfeit use cases. The efficiency of the security measures is proven by a Common Criteria EAL6+ certification.

The A5000 operates fully autonomously based on an authenticaton software ready to be used. The product comes with a dedicated authentication application. Direct memory access is possible by the fixed functionalities of the NXP Authentication application only. With that, the content from the memory is fully isolated from the host system.

- Built on NXP Integral Security Architecture 3.0 ™
- CC EAL 6+ certified HW and OS
- Effective protection against advanced attacks, including Power Analysis and Fault Attacks of various kinds
- Multiple logical and physical protection layers, including metal shielding, end-to-end encryption, memory encryption, tamper detection
- Support for ECC NIST asymmetric cryptography algorithms,
- Support for AES and DES symmetric cryptographic algorithms for encryption and decryption
- Support for AES Modes: CBC, ECB,CTR,GCM,CCM
- HMAC, CMAC, GMAC, SHA-256/384 operations
- HKDF key derivation function
- Small and very thin footprint HX2QFN20 package (3 × 3 mm) with max 0.33 mm height
- Extended temperature range (-40 °C to 105 °C)
- Standard physical interface I^2C Target (Fast mode, up to 1 Mbit/s)
- Secured user flash memory of 8kB for secure data or key storage
- Support for SCP03 protocol (bus encryption and encrypted credential injection) to securely bind the host with the secure authenticator
- TRNG compliant to NIST SP800-90B
- DRBG compliant to NIST SP800-90A
- Support for Automatic detection of the I^2C T=1 protocol implementation based on the initial message prologue. Supported protocols:
  - NXP SE05x T=1 Over I^2C Specification. See [1].
  - APDU Transport over SPI/I2C v1.0 | GPC_SPE_172. See [6].
- Matter Ready: A5000 provides the necessary cryptographic functions to support the upcoming Matter standard for connecting smart home devices.

2.3 Features in detail

Table 2. A5000 configuration

Categories		A5000
Security certification	CC EAL6+ (HW+OS)	x
JavaCard version	3.0.5	x
GlobalPlatform specification version	GP 2.3.1	x
ECC Crypto Schemes	ECDSA	x
	ECDH	x
	ECDHE	x
Supported Elliptic Curves	ECC NIST P256	x
	ECC NIST P384	x
Symmetric Crypto Algorithm	3DES (2K, 3K)	x
	AES (128, 192, 256)	x
AES Modes	CBC, ECB,CTR,GCM,CCM	x
Hash Function	SHA-256, SHA-384	x
MAC	HMAC, CMAC, GMAC	x
Key Derivation (KDF)	HKDF	x
Secure Channel	Secure Channel Host-SA (Platform SCP)	x
TRNG		NIST SP800-90B, AIS31
DRBG		NIST SP800-90A, AIS20
Memory reliability	up to 100 million write cycles / 25 years	x
User Memory		8kB
Pre-Provisioned		x
Interfaces	I^2C Target, up to 1 Mbit	x
Power saving modes	Power-Down (with state retention), 460 µA (I^2C)	Disabled [1]
	Deep Power-Down (no state retention), <5 µA	x
Temperature	Extended, -40 °C - 105 °C, see Section 1.3	x
Packaging	Plastic QFN, 3 mm x 3 mm (HX2QFN20) with max 0.33 mm height	x

[1] Power down mode can be enabled in custom part configuration.

3 Functional description

3.1 Functional diagram

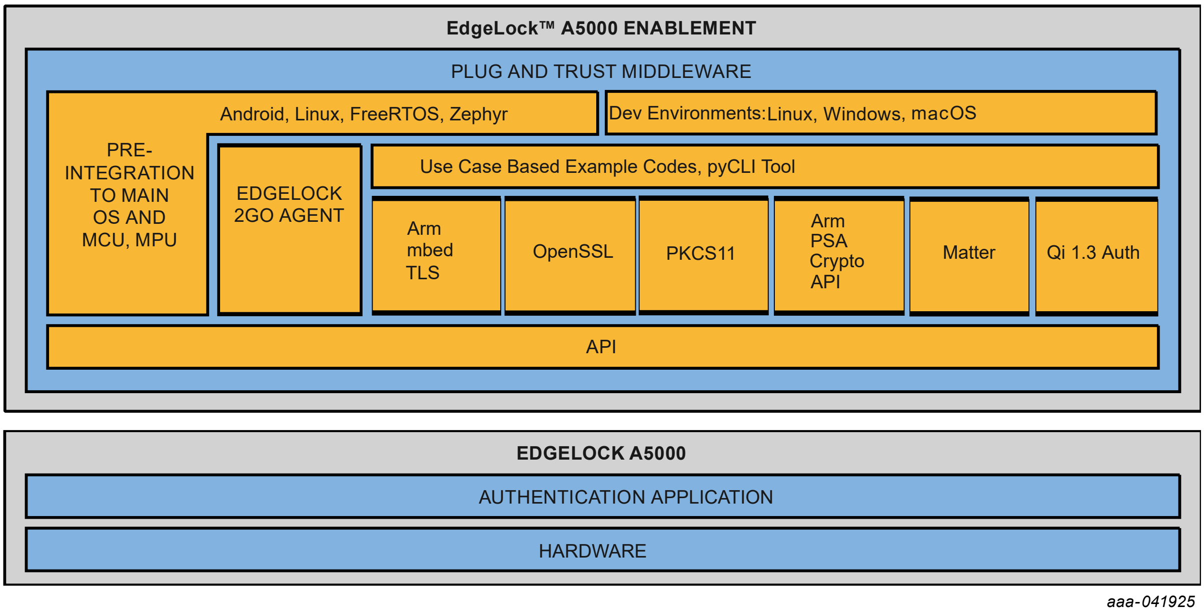


Figure 2. A5000 functional diagram

The A5000 uses I^2C as communication interface. Section 5 gives more details. The A5000 commands are wrapped using the Smartcard T=1 over I^2C (T=1o I^2C) protocol or the APDU Transport over SPI/I^2C v1.0 | GPC_SPE_172. Per default automatic detection of the I^2C T=1 protocol implementation based on the initial message prologue is activated. The detailed documentation of the A5000 commands (see [3]) and T=1 over I^2C protocol encapsulation is available on [1]. You may also check the APDU Transport over SPI/I2C v1.0 | GPC_SPE_172, in [4].

In order to simplify the product usage a host library which abstracts for A5000 commands and T=1 over I^2C protocol encapsulation is provided. The host library supporting various platforms is available for download including complete source code on the A5000 website.

A5000 Authentication application features a generic file system capable of securely storing secure objects and associated privilege management. All objects can either be stored in persistent memory or in RAM with the capability to securely export and import them to be stored in an externally provided storage. All secure objects feature basic file operations such as write, read, delete and update.

3.2 Authentication Application Functionality

3.2.1 Supported secure object types

A secure object is an entry in the file system of A5000. Each secure object has certain features and capabilities. The following secure object types are available:

- Symmetric Key (AES, 3DES)
- ECC Key
- HMAC Key
- Binary File

- User ID
- Counter
- Hash-Extend register

3.2.2 Access control

Each secure object can be linked to object specific access control policies. An access control policy associates a user identified by an authentication with a set of privileges such as read, write, allowed cryptographic operations and more. For details refer to [3].

To scale the functionality into a broad range of ecosystems, a set of different authentication options is provided:

- User-ID based authentication
- Symmetric key based authentication with secure messaging
- Asymmetric key based authentication with secure messaging
  At creation of a secure object, an optional set of policies is associated with that secure object. Each policy assigns a set of allowed operations on that object to an authentication object.

3.2.3 Locking the Device Configuration

The creation of new secure objects as well as the deletion or modification of existing secure objects can be controlled via a credential.

3.2.4 Sessions and multi-threading

The A5000 Authentication Application is prepared for ecosystems where multi-threading and multi-tenant use cases are needed on APDU level. To enable that, the application supports 2 simultaneous sessions that can span full secure messaging sessions, self-authenticated APDUs for tenants not requiring long-lasting sessions and on top one default session for single tenant use cases .

3.2.5 Application support

For specific ecosystems, A5000 Authentication Application has built-in crypto features to simplify the deployment of specific use cases such as

- ECC-Key based cloud connectivity (TLS)
- Remote attestation and trust provisioning

3.2.6 Random numbers

The A5000 IoT Applet provides random numbers using an AIS20 compliant pseudo random number generator (PRNG) with class DRG.4 generator initialized by a TRNG compliant to AIS31 class PTG.2. The PRNG is implemented according to NIST SP800-90Arev1.

DRG.3 functionality is a subset of DRG.4, therefore the TOE is also compliant to DRG.3.

3.2.7 Credential Storage & Memory

Within A5000, all credentials and secure objects are stored inside a dynamic file structure. At creation, a user has to associate a file identifier with the object created. This identifier is then used in subsequent operations to access the object. The number of objects that can be allocated is only limited by the available memory in the system. After usage, objects can be deleted and the associated memory is freed up again.

There is also the possibility to create transient objects. Transient objects have an object descriptor stored in non-volatile memory, but the object content is stored in RAM. Together with the import/export functionality of A5000, transient objects can be used securely store secret keys in a remote memory system.

When the creation of secure objects is interrupted by internal errors (e.g. insufficient space) or a tearing event, the memory is not freed up automatically. The memory can be freed up using garbage collection. An example to trigger garbage collection is included in the Plug & Trust Middleware (InvokeGarbageCollection) [5].

3.3 Startup behavior

If a supply voltage is applied to pins V_{IN}, V_{CC} within the specified supply voltage operating range the IC boots up.

4 Pre-provisioned ease of use configuration

A5000 variants with pre-provisioned credentials for ease of use are available and can be used during development phase or in the field. With this customers have all keys pre-injected in A5000 that are required for the main use cases as, e.g., originality check or cloud onboarding. The identifying information can be read out using the example "get info" from A5000 Plug&Trust MW package. This variant identifier is also known as OEF ID. This will allow to distinguish the delivered configuration.

For more information, see Table 3 and Table 4:

Table 3. Variant Identifiers

Variant	Variant Identifier (OEF ID)
A5000	A736
A5000 Arduino Dev. Kit.	A736

Table 4. Variant A5000

Key name and type	Certificate	Usage policy (keys)	Erasable by customer (keys) [1]	Identifier
Originality Key 0, ECC256, Die Individual	Certificate 0	Anybody, Read	No	`0xF0000000` (key) `0xF0000001` (cert)
Originality Key 1, ECC256, Die Individual	Certificate 1	Anybody, Read	No	`0xF0000002` (key) `0xF0000003` (cert)
Root of Trust signing key, ECC256, Die Individual (used to attest new generated keys)	N/A	Anybody Read and Attestation	No	`0xF0000012` (key)

[1] Certificates are always erasable by customer. Consider that their deletion prevents the device from connecting to the EdgeLock 2GO service over TLS.

4.1 A5000 Chain of Trust

4.1.1 Chain of Trust for Originality Keys

- Root Certificate
- Intermediate Certificate

4.2 Common keys

The keys in Table 5 are present in all configurations.

For the value of the Platform SCP please refer to Table 6.

A second set of Platform SCP keys are inserted with KVN 12. Key set 12 is a recovery key set. It can be used to establish a platform SCP connection in case key set 11 is lost. After authentication with key set 12, key set 11 can be updated again to the new values. Keep in mind that it is required that key set 12 shall be changed to a customer defined and owned value before the A5000 product is deployed in production. For generic products, NXP own the recovery key set. For customized products, the recovery key value can be retrieved from EdgeLock 2GO and customers can update them if recovery feature is not required. As an example for key update, please refer to "se05x_RotatePlatformSCP03Keys" in the Plug & Trust MW.

Table 5. Common objects

Key name	Details and type	Certificate	Erasable by customer	Identifier
Common files	UUID	N/A	No	`0x7FFF0206`
Platform SCP	Default Value needed to perform update of the key	N/A	No	N/A
Recovery SCP	Default Value needed to perform recovery	N/A	No	N/A
ECKey session	Establish an ECC256 based EC key session	N/A	No	`0x7FFF0201`
ECKey import	Used for ImportExternalObject	N/A	No	`0x7FFF0202`

Table 6. Default Platform SCP keys

Configuration	ENC	MAC	DEK
A5000	c9118500b5ffa1433a50226f489a0aa5	29d2fe28f7feeb153068be381f61bc01	6124d38402118060ed910360fc5a4278

4.3 NXP reserved keys and objects

Table 7. NXP reserved keys and objects

Key name	Erasable by customer	Identifier
NXP reserved key 1	No	`0x7FFF0204`
NXP reserved key 2	No	`0xF0000020`
NXP reserved key 3	No	`0xF0003394`

4.4 X.509 Certificate storage encoding

This paragraph provides details on the storage of X.509v3 Certificates in Binary Files on the Authentication application.

The command `ReadSize` can be used to read the size of the complete binary file containing a certificate.

Table 8. Content of certificate binary file

Name	Length [bytes]	Description
X.509 Certificate	variable (length encoded in X.509)	DER encoded X.509v3 Certificate. The length can be parsed from the first TLV sequence which spans over the complete certificate.
Zero padding	variable (remaining bytes up to the complete binary file size)	The file size of the binary file is constant over all devices of a type, while the specific device certificate can vary in size per device (due to the ASN.1 encoding of numbers).

5 Communication interfaces

The communication with the A5000 authenticator follows a command / response concept. This means that, after sending the full command to the authenticator all data needs to be retrieved fully until the next command can be sent.

5.1 I^2C Interfaces

The A5000 has one I^2C interface supporting target.

The I^2C target interface is used by the host controller to send arbitrary APDUs to the device. The I^2C interface is using the Smartcard T=1 over I^2C protocol.

The default target address of the A5000 is configured to 0x48.

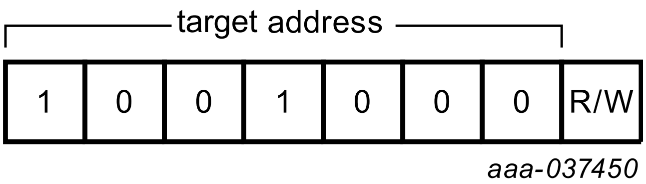


Figure 3. Target address

5.1.1 Supported I^2C frequencies

The A5000 I^2C target interface supports the I^2C fast-speed mode with a maximum SCL clock of up to 1 MHz.

5.1.2 Default I^2C communication parameters

The default I^2C interface parameters of the A5000 devices are chosen with the highest compatibility in mind:

- The used I^2C protocol is detected automatically on the first received frame amongst the two possible protocols:
  - NXP SE05x T=1 Over I^2C Specification. See [1].
  - APDU Transport over SPI/I2C v1.0 | GPC_SPE_172. See [4].
- Power-down mode is disabled. [1]

1 Power down mode can be enabled in custom part configuration.

6 Power-saving modes

The device can provide two power-saving operation modes:

1. Power-down mode (with state retention).
   By default this mode is globally disabled. It can be enabled in custom part configuration. Please contact your sales representative about this.
2. Deep Power-down mode (no state retention).
   Availability requires V_{CC} pin to be supplied like described in Section 6.2.

6.1 Power-down mode

The Power-down mode has the following properties:

- All internal clocks are frozen
- CPU enters power-saving mode with program execution being stopped
- CPU registers keep their contents
- RAM keeps its contents

Power-down mode is entered via the command; "End of APDU session request" (according to [1]) respectively "RELEASE request" (according to GP T=1oI2C [4]). In Power-down mode, all internal clocks are frozen. The IOs hold the logical states they had at the time Power-down mode was activated.

To exit from the Power-down mode an external interrupt edge must be triggered by a falling edge on I^2C_SDA[2].

6.2 Deep Power-down mode

The Deep Power-down mode enables maximum power saving. This mode is activated by pulling enable PIN (ENA) to a logic zero level.

While in Deep Power-down mode the internal power and V_{OUT} is switched off completely and only the I^2C pads stay supplied.

To leave the Deep Power-down mode pad ENA has to be pulled up to to a logic „1" level.

For usage of Deep Power-down mode the A5000 must be supplied via pin V_{in}, and pin V_{CC} needs to be supplied by pin V_{out}, as described in [6].

7 Ordering information

Table 9. Ordering information

12NC	Type number	A5000 Variant	Orderable part number
935426225472	A5000R2HQ1/Z016U	A5000	A5000R2HQ1/Z016UZ
935424319598	OM-A5000ARD	A5000 Arduino Board	OM-A5000ARD

2 In case ISO7816 is enabled a reset signal on RST_N exits the Power-down mode. After wake-up from Power-down mode via RST_N the device is in idle mode (see Table 17)

8 Pinning information

8.1 Pinning

8.1.1 Pinning HX2QFN20

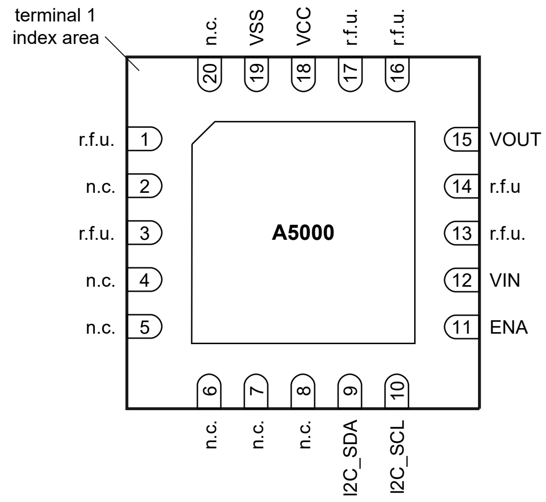


Figure 4. Pin configuration for HX2QFN20 (SOT1969-1)

Note: *Terminal 1 index area is marked on the bottom with a notch on the center pad and on the top with a printed dot.*

Table 10. Pin description HX2QFN20

Symbol	Pin	Description
r.f.u.	1	Connect to V_{SS}
n.c.	2	Not connected
r.f.u.	3	n.c. (recommended) or connect to V_{CC}
n.c.	4	Not connected
n.c.	5	Not connected
n.c.	6	Not connected
n.c.	7	Not connected
n.c.	8	Not connected
I^2C_SDA	9	I^2C target data
I^2C_SCL	10	I^2C target clock
ENA	11	Deep Power-down mode enable. Deep Power-down mode is enabled by pulling ENA PIN to a logic zero level.To leave the Deep Power-down mode pad ENA has to be pulled up to to a logic „1" level. Connect to V_{CC} if Deep Power-down mode is not used.
V_{IN}	12	Power supply voltage input for I^2C pads and logic supply in case Deep Power-down mode is used
r.f.u.	13	n.c. (recommended) or connect to V_{CC}

Table 10. Pin description HX2QFN20*...continued*

Symbol	Pin	Description
r.f.u	14	Connect to V_{SS}
V_{OUT}	15	Supply voltage output to be connected with pad V_{CC} on PCB level, if Deep Power-down mode is used. N. c. if not used.
r.f.u.	16	n.c. (recommended) or connect to V_{OUT}
r.f.u.	17	Connect to V_{SS}
V_{CC}	18	Logic power supply voltage input, to be connected with pad V_{OUT} on PCB level, if Deep Power-down mode to be used
V_{SS}	19	Ground
n.c.	20	Not connected

The center pad of the IC is not connected, although it is recommended to connect it to ground for thermal reasons.

Reference voltage for for I^2C SDA and SCL is V_{IN}.

9 Package

A5000 is offered in HX2QFN20 package. The dimensions are 3 mm x 3 mm x 0,32 mm with a 0,4 mm pitch.

Please refer to the package data sheet [2], SOT1969-1.

10 Marking

Table 11. Marking codes

Type number	Marking code
A5000	Line A: A50 Line B: **** (**** = 4-digit Batch code) Line C: nDyww D: RHF-2006 indicator n: Assembly Center Y: Year WW: Week

11 Packing information

11.1 Reel packing

The A5000 product is available in tape on reel.

Table 12. Reel packing options

Symbol	Parameter	Numbers of units per reel
HX2QFN20	7" tape on reel	3000

12 Electrical and timing characteristics

The electrical interface characteristics of static (DC) and dynamic (AC) parameters for pads and functions used for I^2C are in accordance with the NXP I^2C specification (see [1]).

13 Limiting values

Table 13. Limiting values

In accordance with the Absolute Maximum Rating System (IEC 60134). Voltages are referenced to V_{SS} (ground = 0 V).

Symbol	Parameter	Conditions	Min	Max	Unit
V_{IN}, V_{CC}	supply voltage		-0.3	6[1]	V
V_I	input voltage	any signal pad	-0.3	6	V
I_I	input current	pad I^2C_SDA, I^2C_SCL	-	10	mA
I_O	output current	pad I^2C_SDA, I^2C_SCL	-	10	mA
I_{lu}	latch-up current	V_I < 0 V or V_I > V_{IN}, V_{CC}	-	100	mA
V_{esd_hbm}	electrostatic discharge voltage (Human Body Model)	pads V_{CC}, V_{SS}, I^2C_SDA, I^2C_SCL [2]		± 2.0	kV
V_{esd_cdm}	electrostatic discharge voltage (Charge Device Model)	pads V_{CC}, V_{SS}, I^2C_SDA, I^2C_SCL [3]		± 500	V
P_{tot}	Total power dissipation	[4]	-	600	mW
T_{stg}	Storage temperature		-55	125	°C

[1] Maximum supported supply voltage is 6 V. The A5000 is characterized for the specified operating supply voltage range of 1.62 V to 3.6 V. In case of supply voltages above 3.6 V, Deep Power-down mode current <5 µA is not guaranteed.
[2] MIL Standard 883-D method 3015; human body model; C = 100 pF, R = 1.5 kΩ; T_{amb} = -40 °C to 105 °C.
[3] JESD22-C101, JEDEC Standard Field induced charge device model test method.
[4] Depending on appropriate thermal resistance of the package.

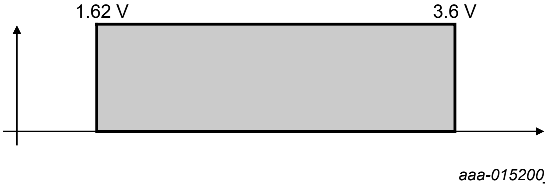
14 Recommended operating conditions

The A5000 is characterized by its specified operating supply voltage range of 1.62 V to 3.6 V.

Table 14. Recommended operating conditions

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
V_{IN}, V_{CC}	Supply voltage	Nominal supply voltage	1.62	1.8	3.6[1]	V
V_I	DC input voltage on digital inputs and digital I/O pads		-0.3		V_{CC}/V_{IN} + 0.3	V
T_{amb}	Operating ambient temperature[2]		-40		105	°C

[1] Maximum supported supply voltage is 6 V. In case of supply voltages above 3.6 V, Deep Power-down mode current <5 µA is not guaranteed.
[2] All product properties and values specified within this data sheet are only valid within the operating ambient temperature range.



Maximum supported supply voltage is 6 V. In case of supply voltages above 3.6 V, Deep Power-down mode current <5 μA is not guaranteed.

Figure 5. Characteristic supply voltage operating range

15 Characteristics

15.1 Thermal Characteristics

Table 15. Thermal characteristics

Rating	Board Type [1]	Symbol	Value	Unit
Junction to Ambient Thermal Resistance [2]	JESD51-9, 2s2p	$R_{\theta JA}$	70.2	°C/W
Junction to Package Top Thermal [2]	JESD51-9, 2s2p	Ψ_{JT}	8.3	°C/W
Junction to Case Thermal Resistance [3]	JESD51-9, 1s	$R_{\theta JC}$	32.9	°C/W

[1] Thermal test board meets JEDEC specification for this package (JESD51-9)
[2] Determined in accordance to JEDEC JESD51-2A natural convection environment. Thermal resistance data in this report is solely for a thermal performance comparison of one package to another in a standardized specified environment. It is not meant to predict the performance of a package in an application-specific environment
[3] Junction-to-Case thermal resistance determined using an isothermal cold plate. Case is defined as the bottom of the packages (exposed pad)

15.2 DC characteristics

Measurement conventions

Testing measurements are performed at the contact pads of the device under test. All voltages are defined with respect to the ground contact pad VSS. All currents flowing into the device are considered positive.

15.2.1 I²C Interface

Table 16. Electrical DC characteristics of I²C pads SDA, SCL.

Conditions: V_{CC}, V_{IN} = 1.62 V to 3.6 V; V_{SS} = 0 V; T_{amb} = -40 °C to 105 °C, unless otherwise specified. Maximum supported supply voltage is 6 V. In case of supply voltages above 3.6 V, Deep Power-down mode current <5 µA is not guaranteed. SSCL, SDA pads are in open-drain mode.

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
V_{IH}	HIGH level input voltage		0.7 V_{IN}	-	V_{IN} + 0.3	V
V_{IL}	LOW level input voltage		-0.3	-	0.25 V_{IN}	V
V_{HYS}	Input hysteresis voltage		0.081 V	-	-	V
$V_{OL(OD)}$	Low level output voltage (open-drain mode)	I_{OL} = 3 mA	0	-	0.4	V
$I_{OL(OD)}$	Low level output current (open-drain mode)	V_{OL} = 0.6 V	0.6	-	-	mA
I_{WPU}	weak pull-up current	V_{IO} = 0 V	-265	-180	-70	µA
I_{ILIH}	Leakage input current high level	V_{SDA} = 3.6 V, V_{SCL} = 3.6 V	-	0.27	15	µA

15.2.2 Power consumption

Table 17. Electrical characteristics of IC supply voltage

Conditions: V_{CC}; V_{SS} = 0 V; T_{amb} = -40 °C to 105 °C

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
Supply						
V_{CC}	supply voltage range	V_{CC} = 1.62 V - 3.6 V	1.62	1.8	3.6	V
operating mode: typical CPU						
I_{DD}	supply current	during Communication	-	3	3.7	mA
		during non asymmetric crypto operation	-	6.5	7.5	mA
		during asymmetric crypto operation	-	14.4	16.5	mA
$I_{DDD\ (DPD)}$	supply current Deep Power-down mode	$V_{CC(min)} \leq V_{IN} \leq V_{CC(max)}$; T_{amb} = 25°C	-	3	5	µA
$I_{DD\ (PD\text{-}I^2C)}$	supply current I²C Power-down mode (I²C wake-up source)	$V_{CC(min)} \leq V_{CC} \leq V_{CC(max)}$; Clock to input SCL stopped, T_{amb} = 25 °C SDA, SCL pads in pull-up Typical value with V_{CC}= 1.8 V	-	450	500	µA

15.3 AC characteristics

Table 18. Non-volatile memory timing characteristics

Conditions: V_{CC} = 1.62 V to 3.6 V; V_{SS} = 0 V; T_{amb} = -40 °C to 105 °C, unless otherwise specified.

Symbol	Parameter	Conditions	Min	Typ [1]	Max	Unit
t_{EEP}	FLASH erase and program time	[2]	-	2.3	-	ms
t_{EEE}	FLASH erase time		-	0.9	-	ms
t_{EEW}	FLASH program time		-	1.4	-	ms
t_{EER}	FLASH data retention time	T_{amb} = 55 °C	25	-	-	years
N_{EEC}	FLASH endurance (maximum number of programming cycles applied to the whole memory block performed by NXP static and dynamic wear leveling algorithm)		20×10^6	100×10^6		cycles

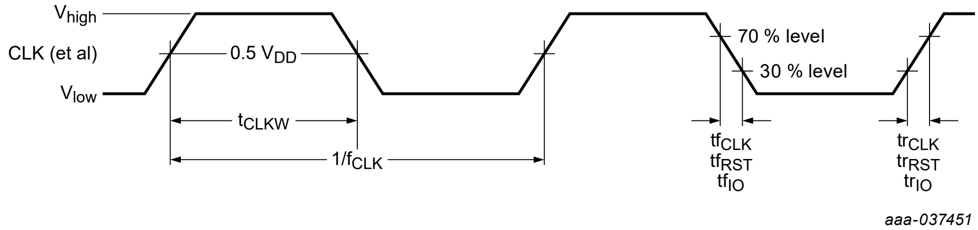
[1] Typical values are only referenced for information. They are subject to change without notice.
[2] Given value specifies physical access times of FLASH memory only.

Table 19. Electrical AC characteristics of I^2C_SDA, I^2C_SCL [1]

Conditions; V_{CC} = 1.8 V ± 10 % or 3 V ± 10 % V; V_{SS} = 0 V; T_{amb} = -40 °C to 105 °C, SCL, and SDA pads in open-drain mode.

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
Input/Output: I^2C_SDA, I^2C_SCL in open-drain mode						
tr_{IO}	I/O Input rise time	Input/reception mode [2]	-	-	1	µs
tf_{IO}	I/O Input fall time	Input/reception mode [2]	-	-	1	µs
$t_{f(OIO)}$	I/O Output fall time	Output/transmission mode; C_L = 30 pF [3]	-	-	0.3	µs
f_{CLK}	External clock frequency in I^2C applications	t_{CLKW}, T_{amb} and V_{CC} in their specified limits [4]	-	-	3.4	MHz
t_{PD}	Power down duration time (I^2C wake-up)	CPU clock = 48 MHz [5]	-	67	-	µs
t_{WKPD}	Wake-up from power down duration time (I^2C wake-up)	CPU clock = 48 MHz [6]	-	97	-	µs
C_{PIN}	Pin capacitances I^2C_SDA, / I^2C_SCL	Test frequency = 1 MHz; T_{amb} = 25 °C	-	-	10.5	pF
t_{ENalt}	ENA low time and V_{OUT}, V_{CC} low time for entering deep power down mode	[7]	-	2	-	µs
R_{on}	Resistance of power switch	T_{amb} = 105 °C, I_{load} = 25 mA, V_i = 1.62 V	-	-	1.1	Ω
I_{out}	maximum current driving capability of pin V_{OUT}	T_{amb} = 105 °C	-	-	25	mA
t_{WKPIO}	Pad LOW time for wake-up from Power-down mode	level triggered ext.int.	-	8	10	µs
		edge triggered ext.int.	-	8	10	µs
C_{PIN}	Pin capacitances I^2C_SDA, / I^2C_SCL	Test frequency = 1 MHz; T_{amb} = 25 °C	-	-	10.5	pF

[1] All appropriately marked values are typical values and only referenced for information. They are subject to change without notice.
[2] t_r is defined as rise time between 30 % and 70 % of the signal amplitude.t_f is defined as fall time between 70 % and 30 % of the signal amplitude.
[3] t_r is defined as rise time between 30 % and 70 % of the signal amplitude.
t_f is defined as fall time between 70 % and 30 % of the signal amplitude.
[4] 3.4 MHz can be enabled in customized A5000 with clock stretch enabled.
[5] Wakeup from power down: I²C_SCL = 400 kHz; the wakeup time will not be sufficient under the rare condition where host sends the first command during the time where SA is just entering power down; in this case the SA will send an R block to request retransmission from the host
[6] Wakeup from power down: I²C_SCL = 1 MHz; the wakeup time will not be sufficient to receive the first host command; the SA will send an R block to request retransmission from the host
[7] Low glitches below 0.4 V on pin ENA and V_{IN}, V_{OUT}, V_{CC} larger than 30 ns cause Power-On-Reset, respectively entering deep power-down mode.



1) During AC testing the inputs I²C_SDA, I²C_SCL are driven at 0 V to 0.3 V for a LOW input level and at V_{CC} -0.3 V to V_{CC} for a HIGH input level. Clock period and signal pulse (duty cycle) timing is measured at 50 % of V_{CC}.

2) t_r is defined as rise time between 30 % and 70 % of the signal amplitude. t_f is defined as fall time between 70 % and 30 % of the signal amplitude.

Figure 6. External clock drive and AC test timing reference points of I²C_SDA, I²C_SCL, (see 1) and 2)) in open-drain mode

15.4 I²C Bus Timings

Parameters defined in this chapter replace the parameter definitions of I²C bus, for specification see [4].

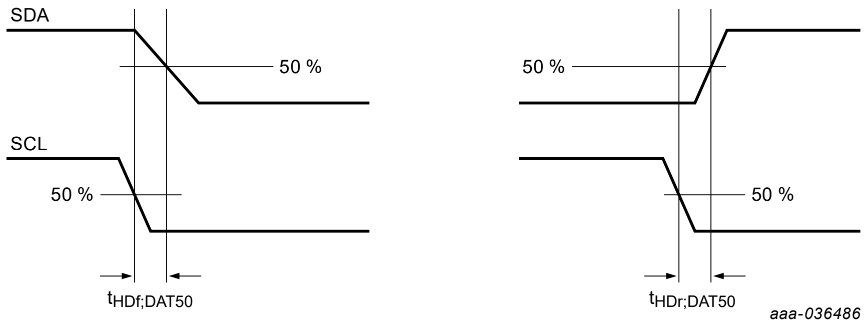


Figure 7. I²C Bus Timings

Table 20. I²C Bus Timing Specification

Symbol	Parameter	Condition	Min	Max	Unit
$t_{HDf;DAT50}$ [1]	data hold time 50 % SCL - 50 % SDA level	Fast mode	8	-	ns
$t_{HDr;DAT50}$ [2]	data hold time 50 % SCL - 50 % SDA level	Fast mode	24	-	ns

[1] $t_{HDf;DAT50}$, as defined in Figure 7, replaces parameter $t_{HD;DAT}$ defined in [4]
[2] $t_{HDr;DAT50}$, as defined in Figure 7, replaces parameter $t_{HD;DAT}$ defined in [4]

15.5 EMC/EMI

EMC and EMI resistance according to IEC 61967-4.

16 Product operation

Within this section guidelines for the operation of A5000 are described.

16.1 T1oI2C command and response pairs

T1oI2C protocol rely on alternating command-APDU response-APDU data pairs. Before the secure authenticator receives a new Command-APDU the previous response-APDU needs to be fetched entirely.

Ensure the response is fully read from the secure authenticator before sending the next command-APDU. This is especially important when the host is reset independently of the secure authenticator or used in multi-threaded/multi-processing applications. Independently of the secure authenticator, ensure the host/SA command response sequence is synchronized.

The Plug & Trust MW access Manager supports concurrent access from multiple linux processes to the A5000 Authenticaton application.

16.2 T1oI2C communication interface specifications

The Plug & Trust MW provides an example for the T1oI2C protocol implementation on the host. This reference implementation details also additions specific to the following available T1oI2C interfaces:

- NXP SE05x T=1 Over I^2C Specification. See [1].
- APDU Transport over SPI/I2C v1.0 | GPC_SPE_172. See [4].

The host implementation is required to fully comply to the specification to guarantee a seamless operation.

17 Abbreviations

Table 21. Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
CC	Common Criteria
CMAC	Cipher-based MAC
CRC	Cyclic Redundancy Check
CRI	Cryptography Research Incorporated
DES	Digital Encryption Standard
DPA	Differential Power Analysis
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
EMC	Electromagnetic compatibility
EMI	Electro Magnetic Immunity
FM	Fast-Mode
GP	Global Platform
GPIO	General-purpose input/output
HS	High-Speed-Mode
HKDF	HMAC-based Extract-and-Expand Key Derivation Function
HMAC	Keyed-Hash Message Authentication Code
HW	Hardware
IC	Integrated Circuit
I^2C	Inter-Integrated Circuit
I/O	Input/Output
IoT	Internet of Things
MAC	Message Authentication Code
MCU	Microcontroller unit
MPU	Microprocessor
MW	Middleware
OS	Operating System
NIST	National Institute for Standards and Technology
PCB	Printed Circuit Board
PKI	Public Key Infrastructure
PRF	Pseudo Random Function
RAM	Random Access Memory

Table 21. Abbreviations*...continued*

Acronym	Description
RST	Reset
SA	Secure Authenticator
SAM	Secure Access Module
SCL	Serial clock
SDA	Serial data
SPA	Simple Power Analysis
SFI	Single Fault Injection
SHA	Secure Hash Algorithm
SW	Software
TLS	Transport Layer Security
V_{CC}	Supply Voltage Input
V_{IN}	Voltage Input
V_{OUT}	Voltage Output
VSS	Ground

18 References

[1] NXP SE05x T=1 Over I^{2}C Specification User Manual, Document Number 11225. Available on NXP website
[2] SOT1969-1; HX2QFN20; Reel packing and package data sheet. Available on NXP website.
[3] A5000 Authentication Application APDU Specification, document number AN13187.
[4] APDU Transport over SPI/I2C v1.0 | GPC_SPE_172. Available here.
[5] Plug & Trust MW Documentation, AN 13030. Available on NXP website.
[6] EdgeLock A5000 User Guidelines, AN13266 NXP website

19 Revision history

Table 22. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
A5000 v.1.6	05 August 2024	Product data sheet	-	A5000 v.1.5
Modifications	• corrected [3] there was the wrong AN number and no link			
A5000 v.1.5	08 July 2024	Product data sheet	-	A5000 v.1.4
Modifications	• updated legal information • updated settings on Power saving modes in Table 2 • Updated the section Section 6, added that power-down is disabled by default.			
A5000 v.1.4	25 April 2023	Product data sheet		A5000 v.1.3
Modifications	• editorial updates			
A5000 v.1.3	18 November 2022	Product data sheet		A5000 v.1.2
Modifications	• Update Section 8.1.1			
A5000 v.1.2	17 October 2022	Product data sheet		A5000 v.1.1
Modifications	• Update Section 3.2.6			
A5000 v.1.1	21 April 2022	Product data sheet		A5000 v.1.0
Modifications	• Added Section 4.4			
A5000 v.1.0	28 March 2022	Product data sheet		-
Modifications	Initial version			

Legal information

Data sheet status

Document status[1][2]	Product status[3]	Definition
Objective [short] data sheet	Development	This document contains data from the objective specification for product development.
Preliminary [short] data sheet	Qualification	This document contains data from the preliminary specification.
Product [short] data sheet	Production	This document contains the product specification.

[1] Please consult the most recently issued document before initiating or completing a design.
[2] The term 'short data sheet' is explained in section "Definitions".
[3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL https://www.nxp.com.

Definitions

Draft — A draft status on a document indicates that 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 in a draft version of a document and shall have no liability for the consequences of use of such information.

Short data sheet — A short data sheet is an extract from a full data sheet with the same product type number(s) and title. A short data sheet is intended for quick reference only and should not be relied upon to contain detailed and full information. For detailed and full information see the relevant full data sheet, which is available on request via the local NXP Semiconductors sales office. In case of any inconsistency or conflict with the short data sheet, the full data sheet shall prevail.

Product specification — The information and data provided in a Product data sheet shall define the specification of the product as agreed between NXP Semiconductors and its customer, unless NXP Semiconductors and customer have explicitly agreed otherwise in writing. In no event however, shall an agreement be valid in which the NXP Semiconductors product is deemed to offer functions and qualities beyond those described in the Product data sheet.

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.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

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.

Suitability for use in non-automotive qualified products — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

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

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

Trademarks

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

NXP — wordmark and logo are trademarks of NXP B.V.

EdgeLock — is a trademark of NXP B.V.

I2C-bus — logo is a trademark of NXP B.V.

JCOP — is a trademark of NXP B.V.

Contents

Date of release: 5 August 2024
Document identifier: A5000
Document number: 667616