AN13283

AUTH Plug & Trust MW Documentation

Rev. 1.4 — 12 January 2023 Application note

Document information

Information	Content
Keywords	Plug & Trust, Middleware, A5000
Abstract	The document contains the documentation on A5000 Plug & Trust MW.

AUTH Plug & Trust MW Documentation

Release v04.03.00

NXP

Jan 12, 2023

CONTENTS

CHAPTER

ONE

NXP AUTH PLUG & TRUST MIDDLEWARE

This documentation covers Secure IoT Authenticator - A5000 (in following document, we refer it as AUTH). It's an addendum to NXP Plug & Trust MW Documentation (`v04.03.00`)

Documentation covers:

- Feature of AUTH.
- API defintion of AUTH.
- Demo Examples of AUTH.
- AUTH Building

A5000 documentation:

- A5000 Edge Lock R Secure Authenticator Data Sheet, document number 667601.
- A5000 Authentication Application APDU Specification Application Note, document number AN13157.
- Get started with EdgeLockTM SE05x support package Application Note, document number AN13256.

CHAPTER

TWO

AUTH FEATURES

This section provides the overview of functionalities of AUTH.

Note: The A5000 Authentication Application is referred as Applet in this document.

- **ECC Curves.**
    - NIST_P256
    - NIST_P384
- **Key management.**
    - ECC: AUTH supports NIST_P256 and NIST_P384.
    - AES: AUTH supports key of size 128, 192 or 256 bit
    - DES: AUTH supports key of size 8, 16 or 24 bytes respectively for DES, 2-key 3DES and 3-key 3DES.
- **Symmetric cryptographic operations.**
    - DES ECB, CBC
    - AES ECB, CBC, CTR
    - AES CCM, GCM
- **Asymmetric cryptographic operations.**
    - ECDAA sign and verify
    - ECDH with curve NIST_P256 and NIST_P384
- **Hash/HMAC/HKDF/TLSPerformPRF operations**
    - AUTH supports SHA-256 and SHA-384

CHAPTER

THREE

SSS APIS: AUTH

SSS API name	AUTH
sss_session_open()	Available
sss_session_close()	Available
sss_key_store_set_key()	For asymmKey object, only support those mentioned in Section 2 *AUTH Features* on SA.
sss_key_store_generate_key()	For asymmKey object, only support those mentioned in Section 2 *AUTH Features* on SA.
sss_key_store_get_key()	Available
sss_key_store_open_key()	Available
sss_key_store_erase_key()	Available
sss_key_store_context_free()	Available
sss_key_object_init()	Available
sss_key_object_allocate_handle()	Available
sss_key_object_get_handle()	Available
sss_key_object_free()	Available
sss_symmetric_context_init()	Available
sss_cipher_one_go()	Available
sss_cipher_init()	Available
sss_cipher_update()	Available
sss_cipher_finish()	Available
sss_cipher_crypt_ctr()	Available
sss_symmetric_context_free()	Available
sss_aead_context_init()	Available
sss_aead_one_go()	Available
sss_aead_init()	Available
sss_aead_update_aad()	Available
sss_aead_update()	Available
sss_aead_finish()	Available
sss_aead_context_free()	Available
sss_digest_context_init()	Available
sss_digest_one_go()	Available. Only works for SHA-256 and SHA-384 on SA.
sss_digest_init()	Available. Only works for SHA-256 and SHA-384 on SA.
sss_digest_update()	Available
sss_digest_finish()	Available
sss_digest_context_free()	Available
sss_mac_context_init()	Available

continues on next page

Table 1 – continued from previous page

SSS API name	AUTH
`sss_mac_one_go()`	Available. In case of HMAC, only works for SHA-256 and SHA-384 on SA.
`sss_mac_init()`	Available. In case of HMAC, only works for SHA-256 and SHA-384 on SA.
`sss_mac_update()`	Available
`sss_mac_finish()`	Available
`sss_mac_context_free()`	Available
`sss_asymmetric_context_init()`	Available
`sss_asymmetric_encrypt()`	Not availabe for SA.
`sss_asymmetric_decrypt()`	Not availabe for SA.
`sss_asymmetric_sign_digest()`	Available. Only support ECC curves mentioned in Section 2 *AUTH Features* on SA.
`sss_asymmetric_verify_digest()`	Available. Only support ECC curves mentioned in Section 2 *AUTH Features* on SA.
`sss_asymmetric_context_free()`	Available
`sss_derive_key_context_init()`	Available
`sss_derive_key_go()`	Deprecated. Only works for SHA-256 and SHA384 on SA.
`sss_derive_key_one_go()`	Only works for SHA-256 and SHA-384 on SA.
`sss_derive_key_sobj_one_go()`	Only works for SHA-256 and SHA-384 on SA.
`sss_derive_key_dh()`	Available
`sss_derive_key_context_free()`	Available
`sss_rng_context_init()`	Available
`sss_rng_get_random()`	Available
`sss_rng_context_free()`	Available

CHAPTER

FOUR

AUTH DEMO LIST

This section provides the overview of demos provided by MW. Some of them are not supported on AUTH.

4.1 SSS APIs Examples

Demo	AUTH supported
ECC Example: Inject ECC Key and use it for sign and verify operation	Yes
Symmetric AES Example: Inject AES key, encrypt and decrypt data with it	Yes
HKDF Example: HMAC Key derivation operation based on the info and salt. Inject HMAC key into SA and derive a key using HMAC from the SA into the host keystore	Yes
Message Digest Example: Message Digest hashing operation. Calculate SHA256 over data.	Yes
HMAC Example: Inject HMAC key and calculate a HMAC	Yes
ECDH Example: Inject ECC key into SA and derive a key using ECDH from the SA into the host keystore.	Yes

4.2 Cloud connectivity Examples

Demo	AUTH supported
AWS Demo for KSDK: Connect to Amazon Web Services IoT Core	Yes
AWS Demo for iMX Linux / RaspberryPi: Connect to Amazon Web Services	Yes
GCP Demo for KSDK: Connect to Google Cloud	Yes
GCP Demo for iMX Linux / Raspberry Pi: Connect to Google Cloud	Yes
IBM Watson Demo for KSDK: Connect to IBM Watson	Yes
IBM Watson Demo for iMX Linux / Raspberry Pi: Connect to IBM Watson	Yes
Azure Demo for KSDK: Connect to Microsoft Azure	Yes
Azure Demo for iMX Linux / Raspberry Pi: Connect to Microsoft Azure	Yes
Greengrass Demo for Linux: Connect as AWS Greengrass Core	Yes

4.3 OpenSSL Engine Examples

Demo	AUTH supported
OpenSSL Engine: TLS Client example for iMX/Rpi3: Setting up a TLS Link using OpenSSL Engine	Yes

4.4 mbedTLS Examples

Demos regarding the mbedTLS ALT implementation. See mbedTLS-alt

Demo	AUTH supported
SSL2 Client: Use extended SSL Client 2 & SSL Server 2 from mbedTLS	Yes
DTLS Client: Use extended dtls_client & dtls_server from mbedTLS	Yes

4.5 AUTH Specific Examples

Demo	AUTH supported
AUTH Minimal example: Showcase usage of AUTH low level APIs	Yes
AUTH Multiple Digest Crypto Objects example: Showcase Platform details of AUTH	Yes
APDU Player Demo: Send RAW APDUs to AUTH	Yes
Using policies for secure objects: Showcase usage of policies	Yes
Get Certificate from the SA: Read the certificate from the SA and store it on the file system.	Yes
AUTH Rotate PlatformSCP Keys Demo: Showcase Rotation of AUTH Platform-SCP03 Keys	Yes
AUTH Export Transient objects: Export transient objects	Yes
AUTH Import Transient objects: Import transient objects	Yes
Import External Object Prepare: Create ImportExternlObject raw APDU	Yes
AUTH Mandate SCP example	Yes
Read object with Attestation: Demonstrate how to read object with attestation	Yes
AUTH Transport Lock example: Show transport lock feature	Yes
AUTH Transport UnLock example: Show transport unlock feature	Yes
AUTH Timestamp: Demonstrate increment of timestamp inside SA	Yes
Write APDU to buffer: Demonstrate how to write APDU to buffer	Yes
Inject Certificate into SA: Example to showcase injection of certificates into SA	Yes
AUTH Read State example: Example to Read the LockState, RestrictMode and PlatformSCPRequest of SA	Yes
AUTH MultiThread demo: Showcase opening multiple sessions using multiple threads	Yes
AUTH Invoke Garbage Collection Example: Invoke Garbage Collection	Yes
ECC Concurrent Example	Yes
Symmetric Multi Step Concurrent Example	Yes

4.6 Examples that use OpenSSL

Demo	AUTH supported
Tool to create Reference key file: Native example to generate refKeys. (Only for NIST-P256 curve).	Yes
Building a self-signed certificate: Create self signed certificates	Yes

4.7 Ease of Use Configuration Examples

Seps for using the Ease Of Use Configuration of AUTH.

Demo	AUTH supported
Ease of Use configuration - IBM Watson	Yes
Ease of Use configuration - Google Cloud Platform	Yes
Ease of Use configuration - Azure IoT Hub	Yes
Ease of Use configuration - AWS IoT Console	Yes

4.8 LPC55S-PUF Based examples

Demo	AUTH supported
Key Injection to PUF: Example to demonstrate inject PlatformSCP keys into PUF	Yes
Key Rotation using PUF: Example to demonstrate PlatformSCP key rotation using PUF	Yes
Secure Boot Demo: Example to demonstrate Secure Binding with LPC55S and AUTH using PUF	Yes

4.9 EdgeLock 2GO Agent example

Demo	AUTH supported
EdgeLock 2GO Agent Examples: Example of usage of the EdgeLock 2GO Client	Yes

CHAPTER

FIVE

AUTH BUILDING

AUTH follows the same way(CMake) as SE051 to compile/build middleware. CMake Options Applet and SE05X_Ver should be selected for AUTH.

Applet
: `-DApplet=AUTH`: The Secure IoT Authenticator Applet - AUTH

SE05X_Ver
: `-DSE05X_Ver=07_02`: Selection of Applet version 07_02

5.1 Reference Commands

We recommend to use out of the source build of Cmake and run it from other directory.

A reference command to compiling for AUTH from Windows PC is:

```
cd <ROOT_DIR>
mkdir ..\build_auth
cd ..\build_auth
cmake ..\<ROOT_DIR> -DApplet=AUTH -DSE05X_Ver=07_02 -DHost=PCWindows
```

CHAPTER

SIX

INDICES AND TABLES

- genindex
- search

INDEX

2 Legal information

2.1 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.

2.2 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.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://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.

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 data sheet 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.

2.3 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.