AN13501

EdgeLock A5000 for secure connection to OEM cloud

Rev. 1.0 — 28 March 2022 Application note

Document information

Information	Content
Keywords	A5000, Secure cloud onboarding
Abstract	This document describes how to leverage A5000 to establish a secure connection with the private cloud of an Original Equipment Manufacturer (OEM).

Revision history

Revision history

Revision number	Date	Description
1.0	2021-03-28	Initial version

1 Device-to-cloud authentication

Security is a major aspect to take into account when deploying and managing IoT devices that connect to the cloud. As the number of connected devices grows, the higher the risk of confidential, sensitive or critical data leakage. Without security, any rogue user can sniff the communication and disclose private data.

With the expansion of IoT solutions, the number of devices that need to authenticate and send data to clouds grows exponentially. This is the case for industrial devices, sensor networks, IP cameras, smart home devices, home gateways, and smart cities. In these type of applications:

- The IoT device needs to authenticate the cloud that will be connected to.
- The cloud also needs to authenticate the IoT devices to trust them.

Therefore, to avoid rogue devices or data being compromised, it is essential to authenticate devices and clouds as well as protecting the data exchanged between an IoT device and the cloud.

TLS is one of the most used protocols to secure Internet connections, including the communication of IoT devices with the cloud. The A5000 supports TLS protocol using pre-shared secrets and provides a tamper-resistant platform to securely store keys and credentials needed for cloud authentication. Figure 1 depicts the device-to-cloud authentication scenario using TLS protocol and A5000.

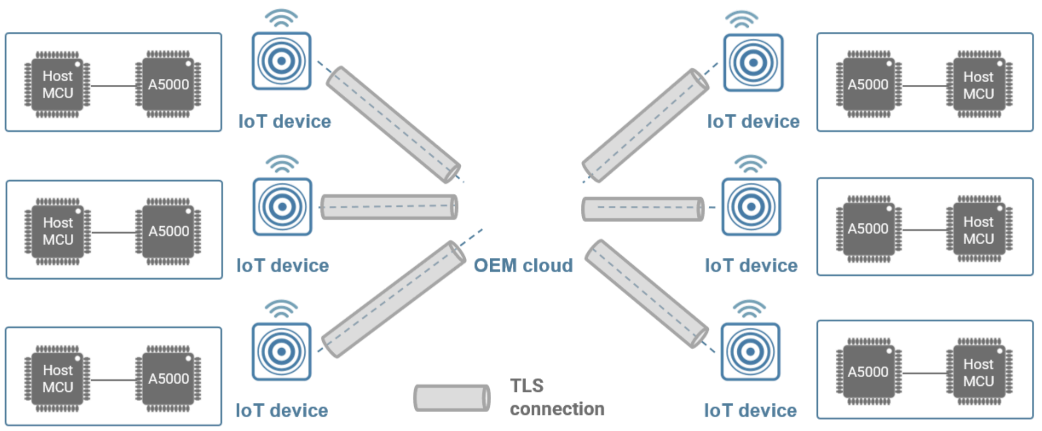

Figure 1. Device-to-cloud authentication scenario

The exchange of digital certificates is the basis of the authentication process during the TLS handshake protocol. The two parties check that the certificate is valid and was issued by a trusted authority, called Certificate Authority. Section 2 describes how certificates are verified using a chain of trust.

In addition, the TLS handshake protocol uses asymmetric encryption to generate a shared secret key that enables the encryption of the data exchange between two parties. Section 3 describes how to leverage A5000 to conduct the TLS handshake protocol.

2 Certificate chain of trust

IoT requires each device to possess a unique identity. For certificate-based authentication scheme, the identity is made of:

- Device certificate
- Device key pair

The digital certificate binds an identity with a public key. Digital certificates are verified using a chain of trust. The certificate chain of trust is a structure of certificates that enables the receiver to verify that the sender and all CA's are trustworthy. The trust anchor for the digital certificate is the root CA.

Certificates are issued and signed by certificates that reside higher in the certificate hierarchy, so the validity and trustworthiness of a given certificate is determined by the corresponding validity of the certificate that signed it. The certificate chain of trust results in a root CA signing an intermediate CA that in turn signs a leaf certificate as shown in Figure 2:

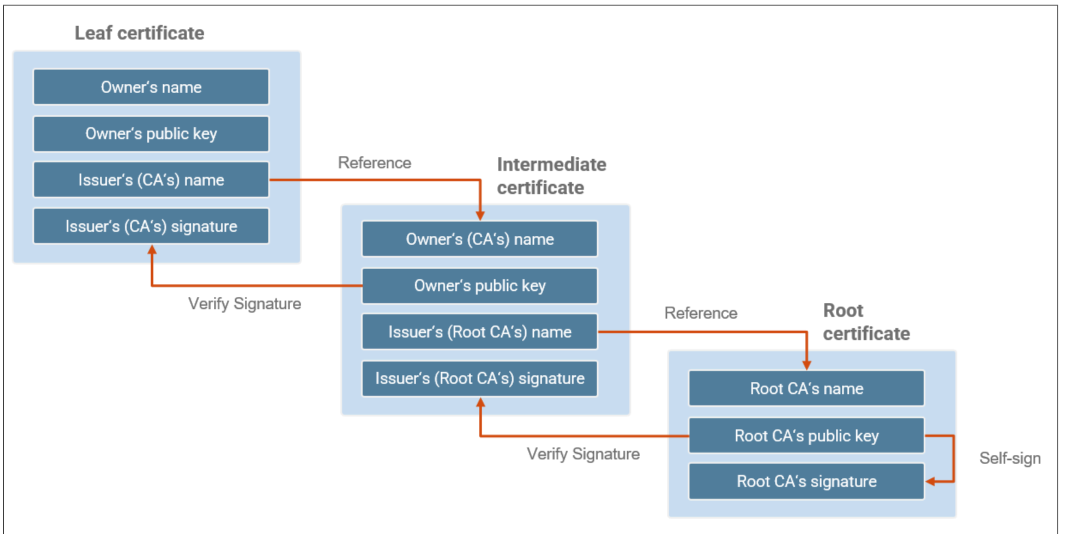

Figure 2. Certificate chain of trust

IoT devices manufactured by the OEM should be equipped with a unique key pair and a digital certificate signed by the OEM's CA certificate. The OEM's CA certificate is used to sign all the certificates of the devices manufactured by the OEM as shown in Figure 3. Precisely, this signature provides the means to verify the validity of device certificates in the field.

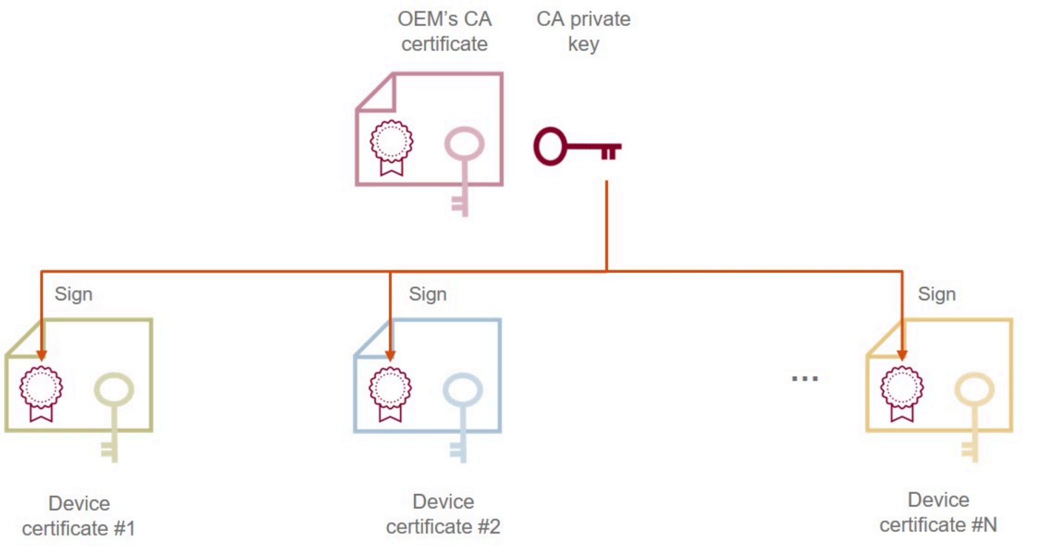

Figure 3. Certificate hierarchy

Before an IoT device manufactured by the OEM goes to the operation phase, they must possess the CA certificate, a device certificate and a key pair securely stored. Similarly, the OEM cloud platform must possess a certificated signed by the CA and its related private key as shown in Figure 4.

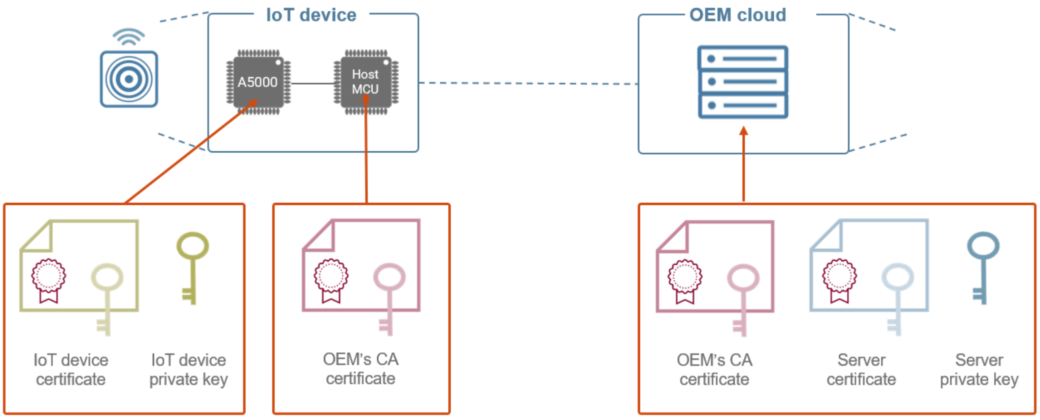

Figure 4. IoT device and OEM cloud credentials

Security ICs chips like A5000 are capable of internally protecting private keys in IoT devices. The CA certificate is typically stored outside the A5000. Section 4 outlines the A5000 trust provisioning models available.

3 TLS handshake

TLS is an industry standard designed to provide identification, authentication, confidentiality and integrity of the communication between two endpoints. Every TLS connection begins with a *TLS handshake* protocol that manages the cipher suite negotiation, the client and server authentication and the session key exchange. It consists of:

- The *hello* phase, where both parties negotiate the protocol version and cipher suite.
- The *client* and *server* key exchange phase.
- The session *secret key calculation* phase, where a pre-master secret and exchanged random values are used to calculate a session key that will be used for securing communication.

Figure 5 illustrates the phases involved in a TLS handshake negotiation:

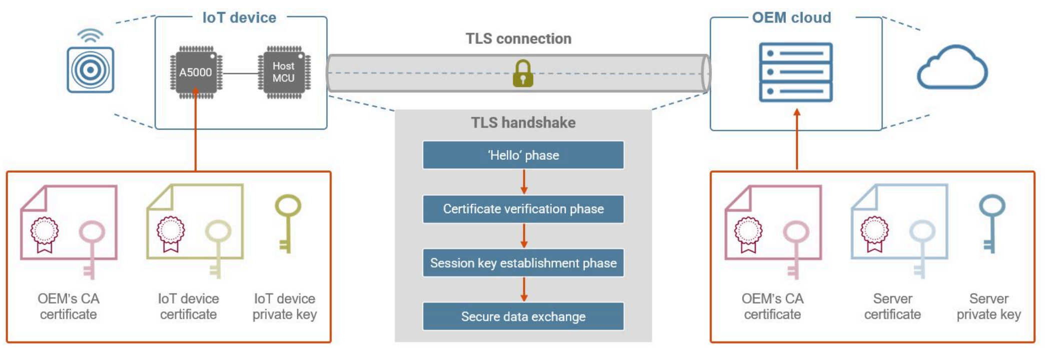

Figure 5. TLS handshake steps

This section briefly explains the use of Elliptic Curve Diffie-Hellman (ECDH) key agreement in a TLS handshake and the use of Elliptic Curve Digital Signature Algorithm (ECDSA) as an authentication mechanism. For more information, please refer to the RFC4492 [1].

3.1 *Hello* phase

The TLS handshake begins by sending a *client_hello* message. The *client_hello* message is sent by the IoT device and includes its supported *cipher suites*. It comprises three distinct algorithms:

- The *key exchange and authentication algorithm* used during the handshake (e.g. TLS_**ECDH_ECDSA**_WITH_AES_128_CBC_SHA256).
- The *encryption algorithm* used to encipher data (e.g. TLS_ECDH_ECDSA_WITH_**AES_128_CBC**_SHA256).
- The *MAC algorithm* used to generate the message digest (e.g. TLS_ECDH_ECDSA_WITH_AES_128_CBC_**SHA256**).

In addition, the *client_hello* message also includes a random number. This random number must be requested to the A5000 security IC.

The server responds with a *server_hello* message, which contains the cipher suite chosen, the session ID and another random number. Figure 6 illustrates the TLS handshake *hello* phase.

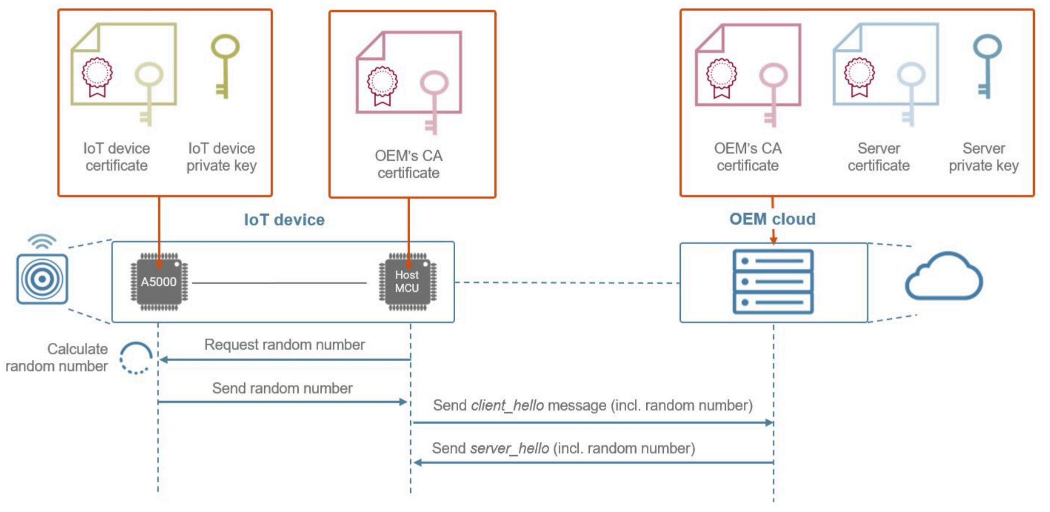

Figure 6. TLS handshake - *Hello* phase

3.2 Server key exchange phase

For the key exchange from the server side, the server sends:

- A *server_certificate* message, which is capable of carrying the whole server certificate chain (leaf certificate and CA certificate).
- A *serverKeyExchange* message, which contains the ephemeral ECDH public key and a specification of the corresponding curve. These parameters are signed with ECDSA using the private key corresponding to the public key in the server's certificate.
- A *client_certificate_request* message, which makes client authentication mandatory. This option is recommended to avoid unauthorized devices to connect to the IoT network.

The IoT device verifies the validity of the server certificate chain and then uses the public key in the server's certificate to verify the ECDSA signature of the parameters received in the *serverKeyExchange* message. A5000 can optionally be leveraged for verifying the ECDSA signature. A valid signature proves the server identity as shown in Figure 7.

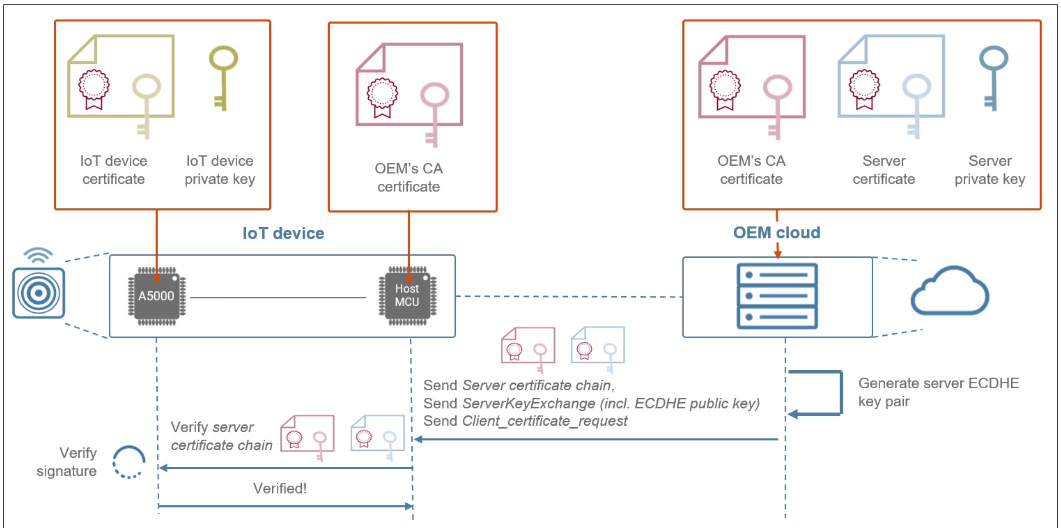

Figure 7. TLS handshake - *Server key exchange* phase

3.3 Client key exchange phase

For the key exchange from the client side, the IoT device sends:

- A *client_certificate* message, which is capable of carrying the whole client certificate chain (leaf certificate and CA certificate).
- A *proof of possession* message, which includes a signature used to prove that the IoT device is in possession of the private key. The signature is performed in A5000 using the IoT device private key.
- A *client_key_exchange* message, which includes a ECDH key public generated on the same curve as the server's ephemeral ECDH key. The ECDHE ephemeral keys are typically generated in the IoT device MCU.

The server verifies the IoT device certificate chain and uses the IoT device public key in the client certificate to verify the proof of possession. By performing this operation, the server verifies that the IoT device is actually in possession of the private key corresponding to the public key in the client certificate. The process is shown in Figure 8.

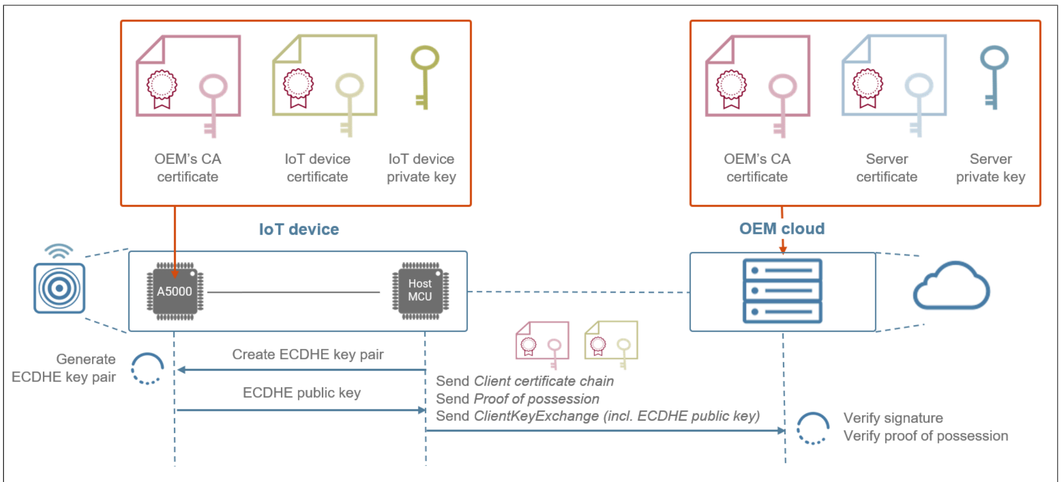

Figure 8. TLS handshake - Client key exchange phase

3.4 Secret key calculation phase

Both client and server perform an ECDH operation. The result is used as input to compute the premaster secret. The A5000 is in charge of calculating both the premaster and master secrets. The master secret is calculated using:

- The pre-master secret
- The client and server random numbers
- An identifier label

The process is shown in Figure 9.

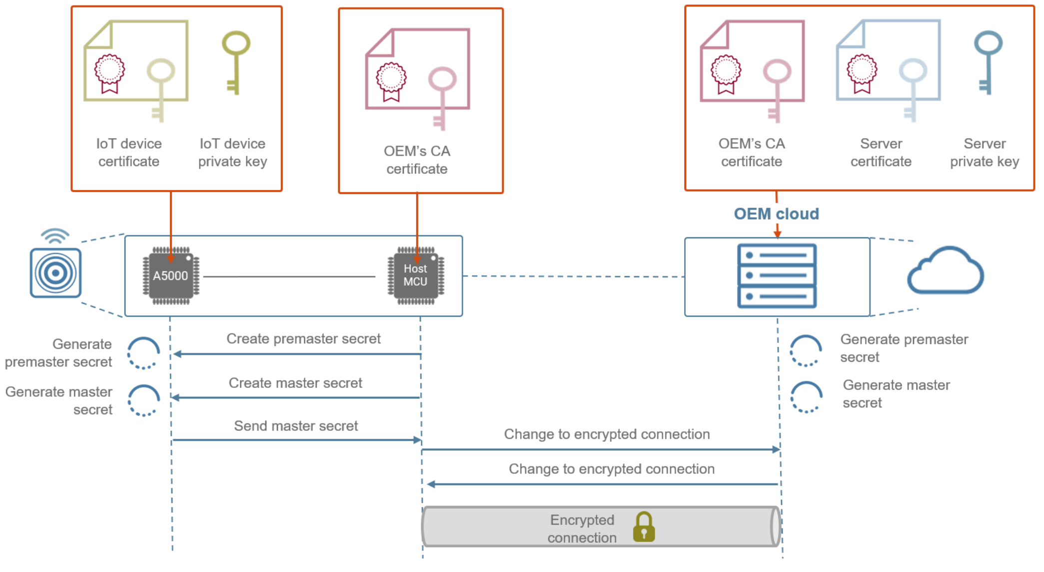

Figure 9. TLS handshake - Secret key calculation phase

At this point, both the IoT device and the OEM cloud are in possession of the shared secret key and can start to securely exchange data using a symmetric cryptographic algorithm.

4 A5000 secure provisioning

The IoT device identity should be unique, verifiable and trustworthy so that device registration attempts and any data uploaded to the OEM's servers can be trusted.

The A5000 is designed to provide a tamper-resistant platform to safely store keys and credentials needed for device authentication and registration to OEM's cloud service. Leveraging the A5000 security IC, OEMs can safely authenticate their devices without writing security code or exposing credentials or keys.

You can rely on any of the secure provisioning options for the A5000 security IC:

- **A5000 pre-configuration for ease of use**: Every A5000 product variant comes pre-provisioned with keys which can be used for all major use cases, including secure onboarding to clouds.
- **A5000 secure provisoning by NXP**: The NXP Trust Provisioning service offers customized and secure injection of die-individual keys and credentials into A5000 on behalf of the OEM. This service is available for high volume orders of more than 150K units.
- **A5000 secure provisioning by NXP distributors or third-party partners**: NXP has agreements with distributors and third-party partners to offer customized and secure injection of die-individual keys and credentials into A5000 for orders of any size.

Note: *A5000 provisioning can optionally be done by the OEM in case it owns or invests in PKI infrastructure at their facilities.*

5 References

[1] RFC4492: Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) - available in the web here.

6 Legal information

6.1 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.

6.2 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.

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.

Security — Customer understands that all NXP products may be subject to unidentified or documented vulnerabilities. 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.

6.3 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.

EdgeLock — is a trademark of NXP B.V.

Figures

Contents

Date of release: 28 March 2022
Document identifier: AN13501