AN12399

EdgeLock^{TM} SE05x for device-to-device authentication

Rev. 1.2 — 7 December 2020 Application note
534711

Document information

Information	Content
Keywords	EdgeLock SE05x, mutual authentication, proof of possession
Abstract	This document describes how to leverage EdgeLock SE05x for device-to-device authentication

Revision history

Revision history

Revision number	Date	Description
1.0	2019-06-08	First document release
1.1	2020-01-20	Added EdgeLock product name and other minor corrections
1.2	2020-12-07	Updated to new template and fixed broken URLs

1 Device-to-device authentication

The IoT environment increases the exposure of high value components to new security threats. OEM manufacturers need to protect themselves from non-authorized components, discriminate original devices from fake copies, avoid device misuse and over usage, and make sure customers purchase original equipment.

If we do not take security into account, attackers may try to compromise our devices by:

- Exploiting software bugs
- Extracting device keys
- Inserting counterfeit devices
- Abusing untrusted connections
- Disclosing confidential data, etc

These security threats are significantly serious for IoT systems dealing with real time processes, even risking safety in case of medical devices, industrial processes, energy grids or traffic lights automation, among others.

For illustrative purposes, let's assume an OEM which manufactures a certain type of machinery controlled by a centralized control unit as shown in Figure 1. As these machines perform some critical tasks in the manufacturing plant:

- The control unit authenticates the machine that is attempting to connect to it.
- The machines also authenticate the control unit that will manage it.

Therefore, only authenticated machines and control units will be used in the supply chain. This mechanism ensures protection against rogue devices that might damage production, degrading security levels or risking employee safety.

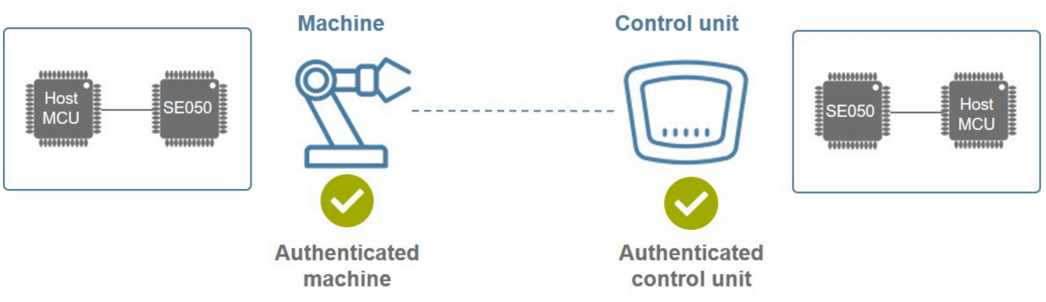

Figure 1. Device-to-device authentication scenario

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

Digital certificates, as public information, are susceptible to be intercepted and be misused. For this reason, a proof of possession of the certificate private key is an essential requirement to validate the certificate source. Section 3 describes how to leverage EdgeLock SE05x to conduct the proof of possession.

The private key must be kept secret and protected. The leakage of any private key compromises the identity verification and the overall system security. The EdgeLock SE05x provides a trust anchor at the silicon level, providing a tamper-resistant platform capable of securely storing keys and credentials needed for offline authentication.

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 enable the receiver to verity 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](#)

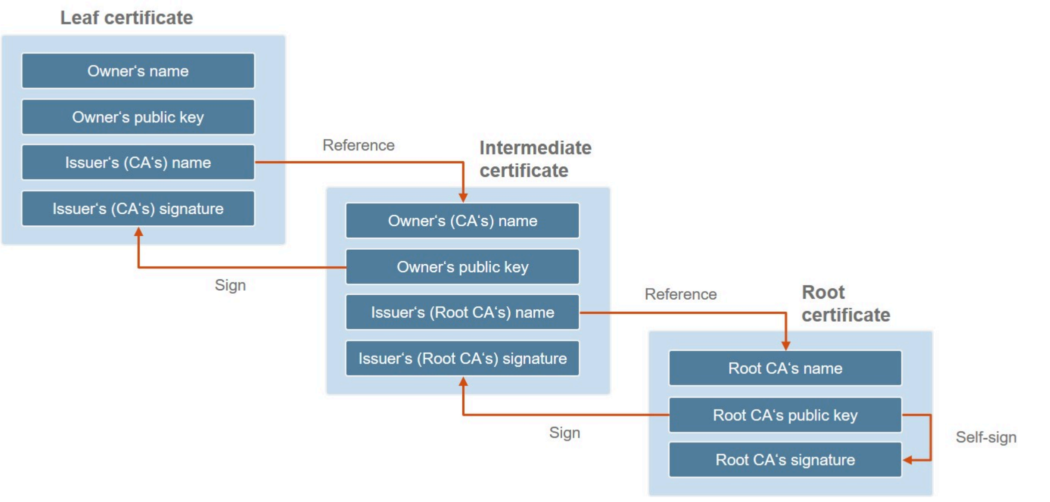

Figure 2. Certificate chain of trust

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. Precisely, this signature provides the means to verify the validity of device certificates in the field ([Figure 3](#)).

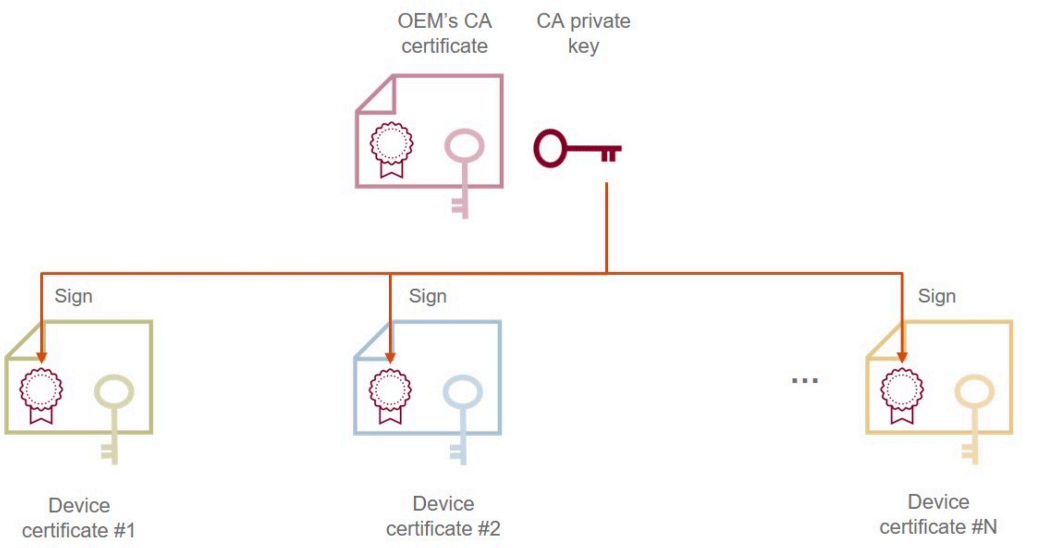

Figure 3. Certificate hierarchy

Before a machine or control unit manufactured by the OEM goes to the operation phase, they must possess the CA certificate, an individual certificate and a key pair securely stored as shown in Figure 4.

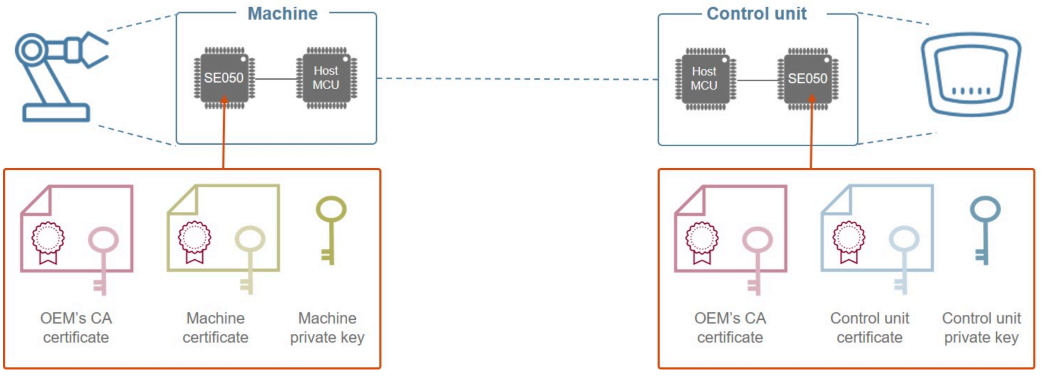

Figure 4. Machine and control unit credentials

Secure silicon chips like EdgeLock SE05x are capable of internally protecting private keys in IoT devices. The CA certificate could optionally be stored outside the EdgeLock SE05x. Section 4 outlines the EdgeLock SE05x trust provisioning models available.

3 Mutual authentication flow

The authentication flow consists of a mutual authentication procedure. First, the machine will authenticate the control unit that it will be connected to. After that, the control unit will authenticate the machine that attempts to connect.

3.1 Control unit authentication

The authentication of the control unit consists of two steps: the *certificate validation* and the private key *proof of possession* as shown in Figure 5.

Certificate validation:

The first step is the verification of the control unit digital certificate.

1. The control unit sends its device certificate together with its hierarchy of CA certificates.
2. The machine validates that the provided certificate chain of trust is valid by verifying the signatures of all the certificates in the chain up to the root CA

If the control unit certificate is valid, it means that the public key included in it can be trusted.

Proof of possesion:

The second step is the proof of possession. This procedure is needed to make sure that the certificate we verified belongs to the control unit. This proof of possession mechanism ensures that the uploader of the certificate also knows the associated private key. For that,

1. The machine generates a random challenge
2. The control unit returns the random challenge signed, using its private key stored inside EdgeLock SE05x.
3. The machine validates the random number signature with the public key obtained from the machine certificate

A successful response means that the control unit is authentic. Bear in mind that the trust relies on protecting the private key. For this reason, the use of EdgeLock SE05x is fundamental to make sure the private key is not compromised.

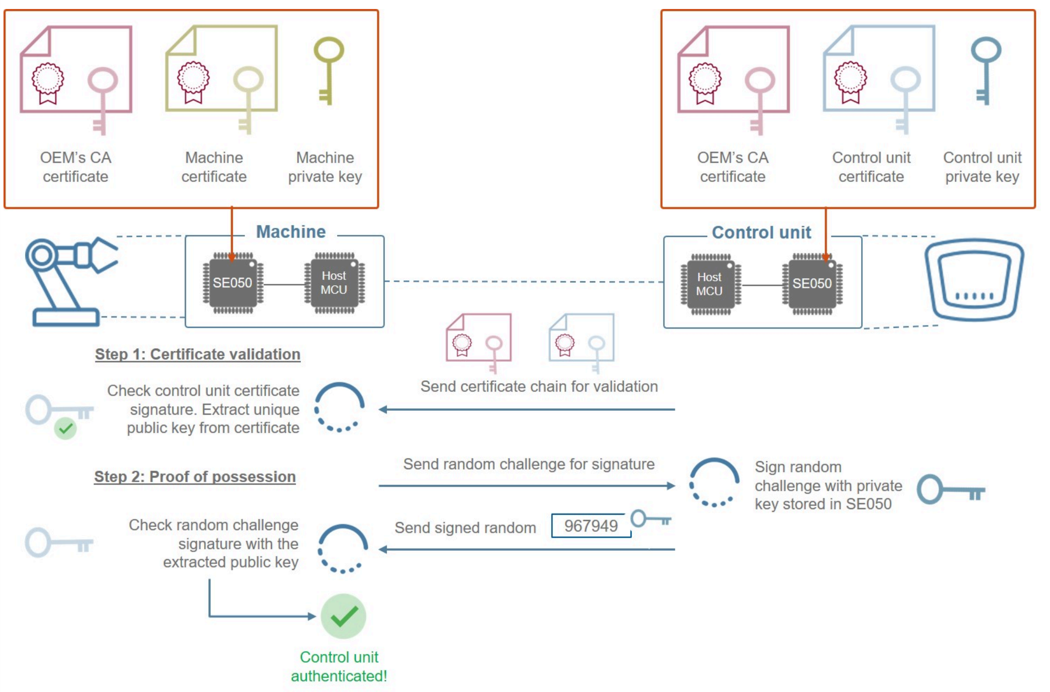

Figure 5. Control unit authentication flow

3.2 Machine authentication

The authentication of the machine also consists of two steps: the *certificate validation* and the private key *proof of possession* as shown in Figure 6. These two steps are equivalent to the ones performed for the control unit authentication.

Certificate validation:

The first step is the verification of the machine digital certificate.

1. The machine sends its device certificate together with its hierarhcy of CA certificates.
2. The control unit validates that the provided certificate chain of trust is valid by verifying the signatures of all the certificates in the chain up to the root CA

If the machine certificate is valid, it means that the public key included in it can be trusted.

Proof of possesion:

The second step is the proof of possession. This procedure is needed to make sure that the certificate we received belongs to the machine. This proof of possession mechanism ensures that the uploader of the certificate also knows the associated private key. For that,

1. The control unit generates a random challenge
2. The machine returns the random challenge signed, using its private key stored inside EdgeLock SE05x.
3. The control unit validates the random number signature with the public key obtained from the machine certificate

A successful response means that the machine is authentic. Bear in mind that the trust relies on protecting the private key. For this reason, the use of EdgeLock SE05x is fundamental to make sure the private key is not compromised.

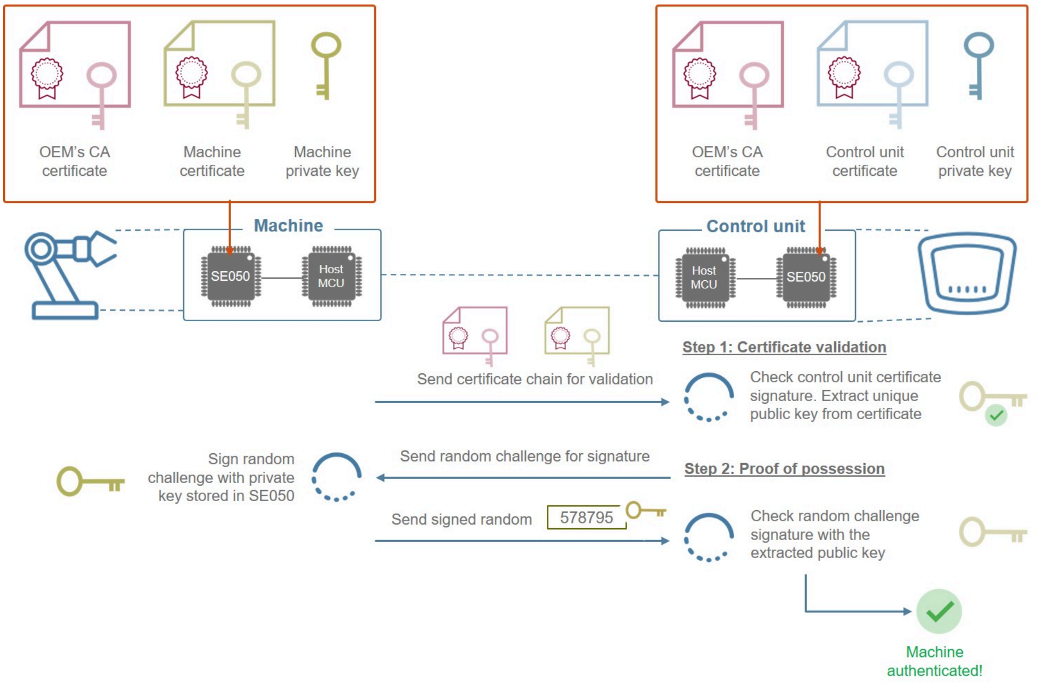

Figure 6. Machine authentication flow

4 EdgeLock SE05x 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 EdgeLock SE05x 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 EdgeLock SE05x 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 EdgeLock SE05x security IC:

- **EdgeLock SE05x pre-configuration for ease of use**: Every EdgeLock SE05x product variant comes pre-provisioned with keys which can be used for all major use cases, including device-to-device authentication.
- **EdgeLock SE05x secure provisoning by NXP**: The NXP Trust Provisioning service offers customized and secure injection of die-individual keys and credentials into EdgeLock SE05x on behalf of the OEM. This service is available for high volume orders of more than 150K units.
- **EdgeLock SE05x 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 EdgeLock SE05x for orders of any size.

Note: *EdgeLock SE05x provisioning can optionally be done by the OEM in case it owns or invests in PKI infrastructure at their facilities.*

5 Legal information

5.1 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.

5.2 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.

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.

5.3 Trademarks

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

Figures

Fig. 1. Device-to-device authentication scenario 3
Fig. 2. Certificate chain of trust 4
Fig. 3. Certificate hierarchy 5
Fig. 4. Machine and control unit credentials 5
Fig. 5. Control unit authentication flow 7
Fig. 6. Machine authentication flow 8

Contents

1 Device-to-device authentication 3
2 Certificate chain of trust 4
3 Mutual authentication flow 6
3.1 Control unit authentication 6
3.2 Machine authentication 7
4 EdgeLock SE05x secure provisioning 9
5 Legal information 10

Date of release: 7 December 2020
Document identifier: AN12399
Document number: 534711