Whitepaper

SEALSQ

Achieving U.S. Cyber Trust Mark using SEALSQ Products and Services

U.S. CYBER TRUST MARK

A review of SEALSQ products & services to meet the requirements of the US Cyber Trust Mark as outlined by NIST IR 8425.

Contents

Abstract

Cybersecurity has been neglected by many IoT deployments. Evidence of this fact can be seen in the news over the past few years with attacks against Google, AWS, and the famous Mirai botnet attack. The Mirai attack[i] recruited over 600,000 unprotected IoT devices to launch Distributed Denial of Service (DDoS) attacks. The frequency and targets of the attacks that include IoT devices like webcams, baby monitors, door locks, and health monitoring are hitting close to home for businesses and the consumer. According to one third-party estimate, there were more than 1.5 billion attacks against smart devices in the first six months of 2021 alone.

The vulnerability of IoT devices and their potential for public harm has prompted government agencies and standards organizations to develop guidelines, standards, and regulations.

In this Whitepaper, we will look at the cybersecurity "outcomes" and requirements. We will examine the NIST IR 8425[ii] document that will be the guiding document for FCC proposed Cyber Trust Mark[iii], and the *ETSI EN 303 645*[iv] that contains detailed requirements IoT cybersecurity. We will then show how the SEALSQ products and services can be used to meet the security requirements to achieve the label and simplify the certification process.

Background

Cybersecurity has been a problem since the early days of the internet. The attacks that include compromised communication, node impersonation of identity, software hacks, access control hacks, and data leaks have taken a new dimension with the advent of IoT devices. These IoT attacks have led to guidelines, standards, and regulations to ensure cybersecurity.

Internationally the Cyber Security Agency of Singapore has enacted the Cybersecurity Labelling Scheme for IoT[v] (CLS(IoT)). The CLS(IoT) labeling scheme uses the European Telecommunication Standards Institute (ETSI) standard *ETSI EN 303 645*[iv] *– Cyber Security for Consumer Internet of Things* as a basis for the specific requirements to determine certify their cybersecurity rating. Also, the European Commission has proposed the *EU Cyber Resilience Act*[vi] with the objective of enabling businesses and consumers to use products with digital elements securely.

Recently the FCC announced the "U.S. Cyber Trust Mark" initiative, a voluntary labeling program has been launched to increase awareness of consumer Internet of Things (IoT). The Cyber Trust Mark will help consumers make informed purchasing decisions, differentiate trustworthy products in the marketplace, and create incentives for manufacturers to meet higher cybersecurity standards.

Below are a couple of excerpts from the FCC Proposed Rulemaking document *FCC 23-65*[vii]:

"*We propose that the IoT security standards be developed jointly with the industry and other stakeholders*."

"*The NIST IoT criteria [defined in NIST IR 8425] are based on product-focused cybersecurity outcomes, rather than specific requirements*."

"*We propose that the IoT security requirements and standards would be developed and implemented through the following process:*

- *Collecting information: Conduct research, consult with experts, and review existing standards such as those developed and in use by international organizations.*
- *Establishing requirements: Informed by the new data, develop requirements that will help meet NIST core baseline criteria.*
- *Develop the standard: With the requirements established, the standard can be developed. This will involve creating a document that outlines the requirements in a clear and concise manner and a clear mapping between the standards and the device or product criteria.*
- *Reviewing and improving: Ensure that the standard is comprehensive, clear, and suitable for lab testing.*
- *Implementation: Conduct training, testing, and monitoring to ensure that the requirements are satisfied*."

Based on these excerpts, the Cyber Trust Mark requirements will be based partially on guidance from the National Institute of Standards (NIST) documents such as *NIST IR 85425* which defines the cybersecurity "outcomes" to be achieved by the labeling initiative. The requirements will also be based on "*standards such as those developed and in use by international organizations*". The FCC is seeking public commitment for the cybersecurity requirements and test procedures to achieve the Cyber Trust Mark label.

Security Requirements

Though the specific requirements are not yet determined for the Cyber Trust Mark, the cybersecurity "outcomes" defined int *NIST IR 8425* will certainly be covered. Additionally, the international cybersecurity requirements defined in *ETSI EN 303 645* will be taken into account. The combination of these documents defines the industry "Best Practices" for cybersecurity.

Both the *NIST IR 8425* and the *ETSI EN 303 645* documents include IoT product requirements. Additional requirements & criteria are defined for the IoT ecosystem, the documentation, and the manufacturer support. We will examine the outcomes and requirements from both of these documents focusing on identifying and comparing the testable *product requirements*.

NIST IR 8425 Outcomes

The outcomes that are defined in the NIST IR 8425 are as follows:

Asset Identification

The cybersecurity utility to facilitate asset management, firmware updates, data protection, and digital forensics for incident response.

The Asset Identification outcome covers two aspects of IoT device identity.

1. The identity of the IoT device itself
2. The identity and inventory of all IoT device components

Implied Requirements

1. IoT Device Credentials
    - This is usually the Factory Certificate (Initial DEVice Identifier or IDEVID[ix]) and takes the form of a public/private key pair with an X.509[viii] certificate signed by a trusted authority
    - This credential is referred to as the "Birth Certificate
2. Operational Credentials
    - This is cryptographically identical to the IoT Device Credential and is usually referred to as the Operational Certificate (Local DEVice Identifier or LDEVID[ix]), is used for operational and application-level use cases such as:
        i. Network Layer Credentials
        ii. Cloud Access

Product Configuration

The cybersecurity utility is to help customers tailer the functionality of the IoT product to meet their needs, and to avoid specific risks and threats. The following restrictions apply:

1. The reconfiguration can only be performed by "authorized individuals".
2. Once reconfigured, the ability to set the configuration back to "default" or "uninitialized" must be provided

Implied Requirements:

1. User role as a "authorized" configuration administrator

Data Protection

The cybersecurity utility is to maintain confidentiality, integrity and availability of data.

The contexts of data protection include:

1. Securely store data on the IoT device platform
2. Ability to delete customer data such as Name, address, family, etc.
3. Securely transmit data between platform components and other IoT nodes (including cloud)

Implied Requirements:

1. Provide secure and modifiable data storage on IoT platform
2. Provide secure storage and deletion of customer data
3. Provide secure communication between components on the IoT Platform

4. Provide secure communication between IoT platform and other ecosystem nodes
5. Verify data input for integrity

Interface Access Control

The cybersecurity utility is by controlling access to internal and external interfaces to the IoT device will facilitate the preservation of the confidentiality, integrity, and availability of the platform, it's components, and data.

The contexts for access control include:

- For all interfaces local or external during normal operation
    - Unique password or multi-factor authentication
    - Physical ports inaccessible
- Prevent access to interfaces and ports that are not consistent with the device intent
- For all administrative interfaces during configuration
- For initial connection (onboarding) or reconnection after disconnection

Implied Requirements:

1. Credentials based authentication
2. Role based authentication
3. Device intent enforcement
4. Unique password
5. Resilient onboarding and reinitialization

Software Update:

The cybersecurity utility is to enable enhancing features and fixing of vulnerabilities that were discovered after the product has been deployed. Software includes executable code, as well as software libraries, support packs, and other non-executable data.

The software updates must only be performed by authorized users. The following conditions must apply:

1. The IoT device must be able to receive, verify and apply verified software updates
2. The IoT device must implement mechanisms to keep the software up to date (e.g. automatic updates, notifications to user, etc)

Implied Requirements

1. Must have a mechanism to update software
2. The software must be verifiable at update time
3. The software must be verifiable at run time

ETSI EN 303 645 Requirements

The ETSI EN 303 645 document has overlapping requirements as the NIST IR 8425. The table below shows the mapping of the cybersecurity outcomes in NIST IR 8425 to the ETSI EN 303 645. While there may be nuances that are unique, the baseline requirements are overlapping.

ETSI VS NIST Requirements

ETSI EN 303 645 Requirement	NIST IR 8425 "Outcome"
No universal default passwords	Access Control
Keep software updated	Software Update
Securely store sensitive security parameters	Data Protection
Communicate Securely	Data Protection
Minimize exposed attack surfaces	Access Control
Ensure software integrity	Software Update
Ensure that personal data is secure	Data Protection
Make systems resilient to outages	Access Control
Examine system telemetry data	Cybersecurity State Awareness
Delete user data and reset are easy	Data Protection
Installation and Maintenance are easy	Access Control
Validate input data	Data Protection

Table 1: ETSI EN 303 645 Requirements Mapping to NIST IR 8425 Outcomes

Industry "Best Practices" Baseline Requirements

Below are the combined and consolidated "Implied Requirements" from NISTIR8425 and the requirements from the ETSE EN 303 645.

Best Practices Requirement	Description
Securely Store Credentials & Certificates	This applies to both the Birth (or factory) Certificate (IDEVID[ix]) and Operational Certificates (LDEVIDs) along with their associated public-private key pairs.
Credential based authentication	IDEVID (birth certificate) and LDEVIDs (application certificates
Unique password	Factory defined passwords must be unique
Specialized User Roles	Roles for administration, operation, etc.
Secure Storage and Update of data	Applies to configuration, user, and application data
Secure Communication	Includes communication on the bus, and communication to other IoT ecosystem nodes
Secure Software Update	Verify software package when downloading
Secure Boot	Verify software package in bootloader
Device Intent	Configuration to only intended Functionality of IoT device

Table 2: Consolidated Requirements from NISTIR8425 and ETSI EN 303 645

SEALSQ Products & Services

SEALSQ stands out as the only company in the market designing and selling a suite of Certified Secure Micro-Controllers, PKI and Identity Provisioning Services at the same time.

By combining all aspects of digital security in a vertically integrated offering, SEALSQ strives to streamline the design and operation of smart products. Our goal is to assist device manufacturers in incorporating security-by-design, ensuring compliance with the highest security standards, all while maintaining cost-effectiveness and minimizing time-to-market.

SEALSQ products and solutions are widely used by key players across all industries in a variety of applications today, from Home Automation Systems, Multi-Factor Authentication devices, and IT Network Infrastructure, to Automotive, Industrial Automation and Control Systems.

VaultIC with Firmware Library

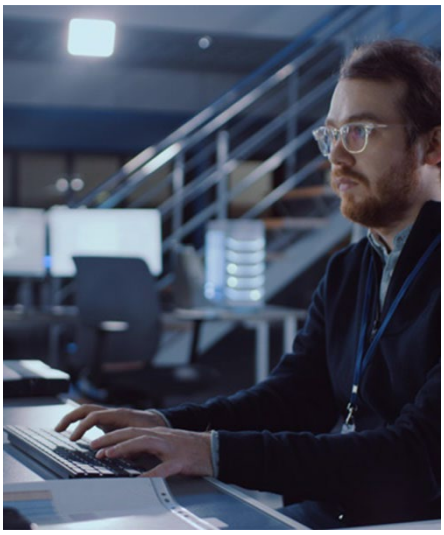
The VaultIC secure element combines hardware-based key storage with cryptographic accelerators to provide a wide array of cryptographic features including identity, authentication, encryption, key agreement, and data integrity. The hardware security protects against hardware attacks such as micro probing and side channel.

The fundamental cryptography of the VaultIC family includes the NIST-recommended algorithms and key lengths and is FIPS140-3 Level 3 (CMVP)[x] certified. Each of these algorithms, Elliptic Curve Cryptography (ECC), Rivest-Shamir-Adleman (RSA), and Advanced Encryption Standard (AES), is implemented on-chip and uses on-chip storage of the secret key material so the secrets are always protected in the secure hardware. Additionally, there is a NIST SP800-90B[xi] certified TRNG so that all IoT platform cryptographic calculations have top quality entropy.

The secure storage and cryptographic acceleration support use cases like network/IoT end node security, platform security, secure boot, secure firmware download, secure communication/TLS, data confidentiality, encryption key storage, and data integrity.

Additionally, a firmware library is provided to simplify the integration into virtually any MCU/MPU. The libraries include support for common use cases including TLS, sign/verify, secure read/write, etc.

INeS Certificate Management System (CMS)



SEALSQ's portfolio includes INeS, a Managed PKI-as-a-Service solution. INeS leverages the WISeKey Webtrust-accredited trust services platform, a Matter approved PAA, and private Certificate Authorities (CAs). These PKI technologies support large-scale IoT deployments. The endpoints of IoT will require certificates to establish their identities. The INeS CMS platform provides a secure, scalable, and manageable trust model.

INeS CMS provides certificate management, CA management, public cloud integration and automation, role-based access control (RBAC), and APIs for custom implementations.

INeS Code Signing Solution for secure Firmware OTA

SEALSQ's portfolio includes also within INeS platform, a code signing solution for Software developers. Code Signing is the process of applying a digital signature to a software binary or file. This digital signature validates the identity of the software author or publisher and verifies that the file has not been altered or tampered with since it was signed. Code signing can be performed manually or automated as part of a software development lifecycle such as a Continuous Integration / Continuous Integration (CI/CD) process.

Provisioning of the VaultIC

The VaultIC can be provisioned at wafer level at the Common Criteria certified SEALSQ factory or using SEALSQ "Personalization-On-Package" services. The provisioning includes one or more credentials and certificates along with configuration and product specific data. It can simplify & secure the production of the IoT device since the security requirements of the IoT device factory can be relaxed.

In Particular for Smart Home devices, SEALSQ uses the WISeKey Root-of-Trust which is certified by the Connectivity Standards Alliance (CSA) as a compliant Matter Product Attestation Authority (PAA)[xii]. This CSA certification enables the WISeKey Root of Trust to pre-load Matter compliant X509

Certificates (Matter DAC) in the VaultIC, accelerating the certification process for devices with the Matter Standard.

SEALSQ Cyber Trust Mark Service

The SEALSQ Cyber Trust Service consists of the components below. The service is intended to provide the tool suite and expert guidance to meet the security requirements, simplify the certification process, and ultimately achieve the label.

1. VaultIC secure element to provide secure storage of keys and data
    a. FIPS140-3 Certified technology
    b. Storage for keys and Certificates (IDEVID, LDEVIDs)
    c. Storage for passwords and application data
    d. Crypto acceleration
2. Firmware APIs that implement the "Baseline Requirements" on the VaultIC
3. Implementation guide
4. Cyber Trust Mark checklist
5. Expert guidance

Achieving the Cyber Trust Mark with SEALSQ

The consolidated "Baseline Requirements" are on the IoT device. We will examine each of the requirements in the following subsections and show how SEALSQ products and services can be used to fulfill the security requirements to achieve Cyber Trust Mark.

Securely Store Credentials & Certificates

This requirement applies to both the Birth Certificate (IDEVID[ix]) and Operational Certificates (LDEVIDs) along with their associated private keys. The IDEVID certificate becomes the fundamental identity for the IoT device and can be used to establish the trust required for LDEVID certificates to be issued

The VaultIC family of secure elements provide secure key storage along with crypto acceleration of NIST-recommended cryptography algorithms. The certificates are also securely stored on the VaultIC so it can be used as the cryptographically verifiable hardware root of trust for the IoT platform

The INeS CMS can provide IDEVIDs and LDEVID certificates for IoT devices. The certificates will be signed by the IoT ecosystem trusted Certificate Authority (CA). The IDEVID is usually provisioned on the VaultIC secure element in the Common Criteria certified SEALSQ factory. The LDEVIDs can be provisioned in the factory or in the field based on the use case.

Credential Based Authentication

This requirement applies to the IoT platform using credentials to configure, use, and communicate with the IoT platform. Certificates and public-private key pairs are used for this requirement.

The certificates and public-private keys are securely stored on the VaultIC family of secure elements. The VaultIC stores both the IDEVID credential for device identity, and multiple LDEVIDs for application layer authentication.

When the IoT device is being authenticated, the certificate is read from the VaultIC and presented to the authenticator. The authenticator will then perform a certificate validation back to the IoT ecosystem trusted Certificate Authority. Then the authenticator sends a random challenge to be signed by the VaultIC private key that is associated with the certificate. The signature of the random challenge can then be verified by the authenticator. The combination of the certificate validation with the trusted CA and the signature of the random challenge cryptographically proves the credential

Unique password

The requirement is that factory defined passwords must be unique. There are several ways that the VaultIC can be used to fulfill the uniqueness requirement. As pointed out earlier, the password applies to the IoT device platform, not the secure element. It is therefore the IoT device manufacturer's responsibility to use the VaultIC to fulfill this requirement.

Here are a few strategies for unique passwords:

- Random password generation using the NIST SP800
- Password storage and validation using xMAC functionality

Additionally, there are IoT ecosystems that use certificate-based authentication and never require passwords. This strategy implicitly fulfills this requirement.

Specialized User Roles

This requirement isolates the capability to modify the configuration and define users and access control to separate users as is required for normal operation. As with passwords, user roles apply to the IoT device platform, not directly to the secure element.

The VaultIC can be used to compliment this requirement as it has an access control model that includes multiple users with unique permissions. The VaultIC users include manufacturing user, administrative user, and operational users that can be configured with unique permissions.

The IoT device platform users can be given unique permissions for interacting with the VaultIC.

Secure Data Management

The "Baseline Requirements" for handling data are multifaceted. Data handling requirements include secure storage and update, but also securing data-at-rest, securing data-in-transit (see *Secure Communication*, and verification of input.

Secure Storage and Update / Secure Data-At-Rest

The VaultIC has non-volatile memory for secure data storage. The data storage memory is used to store keys, certificates, configuration, and user data. Base on permissions, the data can be set to read only or read/write depending on the type of data and the user accessing the data.

Additionally, the VaultIC can be used to encrypt and decrypt data stored in external memory. This enables virtually unlimited secure storage since the encryption keys remain in the VaultIC. This fulfills the Secure Data-At-Rest requirement.

Once the VaultIC is used for secure data storage, the data is protected with the hardware security of the VaultIC.

Data Input Validation

This is another IoT platform and application specific requirement that applies to configuration, user, and application data. The data can originate from any of multiple sources, but must be validated before being used. The VaultIC can assist in a few validation techniques such as validation of xMACs or signatures over the data. It is the IoT platform is ultimately responsible to use appropriate validation techniques for the use case.

Secure Communication

This requirement applies to securing all Data-In-Transit on the IoT platform and external communication. This includes communication on the IoT platform serial bus, and communication to other IoT ecosystem nodes and IoT cloud providers

Secure Serial Communication

The VaultIC provides mechanisms for the serial bus (I2C/SPI) communication to be encrypted. This encryption is in the form of a "Pairing Key" in the case of the VaultIC292 or using the Global Platform SCP03 communication in the case of the VaultIC408.

Transport Layer Security (TLS) Communication

TLS can be used to establish secure connection to cloud providers and for secure Device-To-Device communication. The VaultIC provides the private key protection and X.509 certificates required for TLS communication. The C-based firmware libraries for VaultIC have a pre-defined API specifically for TLS stack integration. In particular integration to TLS 1.2 & 1.3 stacks for WolfSSL and MbedTLS are provided.

Secure Software Update

This requirement involves the verifying of software package when downloading to the IoT platform. To secure this download the software update package is signed by a CA that is trusted by the IoT platform. The software package signature is verified by the IoT platform before continuing with the update. This prevents rogue software from being loaded on the IoT platform.

The VaultIC enables the validation by securely storing the trusted CA certificate or public key. This trusted public key will be used in the verification. Then the VaultIC provides the hashing and ECDSA verify cryptographic operations. The verification of the signed package effectively secures the software update.

Secure Boot

The secure boot requirement is similar to the *Secure Software Update* in that it verifies the signature from the last software update against the code that is ready to be loaded and executed. The secure boot operation is usually performed in the bootloader of the IoT platform.

As with the *Secure Software Update*, the VaultIC enables the validation by securely storing the trusted CA certificate or public key and the verifying the signature of the software that will be loaded and executed.

Device Intent

The objective of this requirement is to limit the IoT device to be used only for its intended purpose. As with other requirements, this cannot be directly supported by the secure element, or even by the IoT device platform. This is an IT and access permissions issue.

The NIST SP 1800-15[xiii] special publication addresses the issue of device intent by defining a Manufacturer Usage Description (MUD). This usage description is based on a MUD URL that the manufacturer provides. The VaultIC can securely store this MUD URL and present it when queried.

Conclusion

We examined the Cyber Trust Mark proposal by the FCC and the FCC Proposed Rulemaking document *FCC 23-65*[vii]. Since the specific requirements for the Cyber Trust Mark are still being developed, we used the combined requirements from NIST IR 8425 and ETSI EN 303 645 to establish the "Best Practices" cybersecurity requirements.

From these "Best Practices" requirement we showed how the SEALSQ products and services can be used to meet the security requirements to achieve the label and simplify the certification process. The specific SEALSQ products and services include the VaultIC family of FIPS140-3 certified secure elements, the INeS Certificate Management Service (CMS) and the WISeKey CA and Trust Services.

We also defined the SEALSQ Cyber Trust Mark Service that provides the tool suite, hardware, services, and expert guidance to help achieve the Cyber Trust Mark label.

References

[i] Inside the infamous Mirai IoT Botnet: A Retrospective Analysis https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

[ii] NIST IR 8425: Profile of the IoT Core Baseline for Consumer IoT Products https://csrc.nist.gov/pubs/ir/8425/final

[iii] FCC Proposes Cybersecurity Labeling Program for Smart Devices https://www.fcc.gov/document/fcc-proposes-cybersecurity-labeling-program-smart-device

[iv] ETSI EN 303 645: Cyber Security for Consumer Internet of Things: Baseline Requirements https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[v] Singapore Cybersecurity Labelling Scheme (CLS) https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme

[vi] European Commission: Cyber Resilience Act https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

[vii] FCC 23-65: Cybersecurity Labeling for Internet of Things – Proposed Rulemaking https://docs.fcc.gov/public/attachments/FCC-23-65A1.pdf

[viii] Internet X.509 Public Key Infrastructure Certificate https://datatracker.ietf.org/doc/html/rfc5280

[ix] IEEE, "802.1AR-2018 - IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity," 14 June 2018. [Online]. Available: https://standards.ieee.org/ieee/802.1AR/6995/.

[x] WISeKey Cryptographic Module Validation Program CMVP https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Basic&Vendor=WISeKey&CertificateStatus=Active&ValidationYear=0

[xi] WISeKey Entropy Certificate #E2 https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/2

[xii] CSA: Product Attestation Authorities https://csa-iot.org/certification/paa/

[xiii] NIST SP 1800-15: Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD) https://csrc.nist.gov/pubs/sp/1800/15/final