UG628: Understanding RED Security Compliance: How Silicon Labs Secure Vault™ SoCs Help You Meet EN 18031:2024 (E)

The European Union's Radio Equipment Directive (RED) 2014/53/EU, specifically Articles 3(3)(d), (e), and (f), introduces mandatory cybersecurity and privacy requirements for internet-connected radio equipment sold in the EU. As of **August 1, 2025**, compliance with these security-related clauses becomes legally enforceable. This guide is designed to support internal and external stakeholders—including customers, product teams, business units, and sales engineers—in understanding both the regulatory landscape and how **Silicon Labs' Series 2 Secure Vault™ High with Hardware Security Engine (HSE) SoCs** can be leveraged to meet these stringent requirements.

The RED compliance journey involves interpreting the newly harmonized standard **EN 18031:2024 (E)**, which provides the technical framework for self-assessment. Silicon Labs' Secure Vault™ platform is engineered with robust, certified security mechanisms—including secure boot, secure storage, tamper detection, secure communications, and hardware-based key management—that align with the EN 18031 evaluation structure.
Designed with flexibility in mind, this document empowers stakeholders to determine applicable security mechanisms through structured threat modeling and risk analysis, while offering technical clarity on integrating secure hardware features into RED-conformant devices. For product developers and integrators, it offers a practical, Silicon Labs-centric interpretation of EN 18031 and highlights best practices for achieving CE marking and maintaining long-term compliance in a dynamic regulatory environment.

Note: This User Guide is Silicon Labs' interpretation of EN 18031:2024 (E) and should be used in conjunction with the actual EN 18031-1 standard. Silicon Labs makes no claims to this User Guides accuracy, precision, or completeness in making an assessment of compliance to the standard."

KEY FEATURES

- The scope and intent of RED Articles 3 (3) (d), (e), and (f).
- The structure and use of EN 18031 Parts 1–3.
- The categorization of in-scope vs. out-of-scope equipment.
- Manufacturer responsibilities, including risk assessment and conformity documentation.
- How Silicon Labs SoCs and support services (e.g., CPMS, SESIP/PSA certifications) enable RED-aligned product designs.
- Practical security mappings between EN 18031 mechanisms and Silicon Labs Secure Vault™ capabilities.

Table of Contents

1. RED Delegated Act (Directive 2014/53/EU - Articles 3(3)(d,e,f)

Radio equipment was regulated under the R&TTE Directive (Radio and Telecommunication Terminal Equipment Directive) 1999/5/EC. It was adopted in 1999 and focused on ensuring the safety and electromagnetic compatibility (EMC) of telecom equipment and facilitating free movement of such equipment within the EU internal market.

While effective in harmonizing the market, the R&TTE Directive began to show limitations as technology rapidly evolved, especially with the convergence of telecom and IT. To address the challenges posed by new technologies, the Radio Equipment Directive (RED) 53 was adopted on 22 May 2014, replacing the R&TTE Directive. RED formally entered into force on June 13, 2016 with a compliance date a year later in June of 2017. Devices that do not comply with RED cannot carry the CE mark and cannot be sold legally in the EU.

In the context of security, a common misconception is that RED is only a security regulation. In fact, only Articles 3(3)(d), (e) and (f) of the RED that pertained to security and there was very limited in direction. The majority of RED regulates radio transmissions, not security. Below are the security relevant 3(3), (d), (e), and (f).

- **(d)** radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service; (example given: Denial of Service)
- **(e)** radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected
- **(f)** radio equipment supports certain features ensuring protection from fraud

Articles 3(3)(d), (e), and (f) remained dormant until October 29, 2021, when the European Commission issued supplement to these articles that made several clarifications which are summarized below.

- Deadline set for August 1st, 2024
- Compliance date depends on “Voluntary Harmonized Standards” being in place and industry adopted
- Any device must be “capable itself to communicate over the internet” (IPv(X) based comms i.e. WiFi or Thread)
- Exception: childcare, toys, and wearables are in scope even if connected to a gateway (i.e. ZigBee, Z-Wave, Proprietary)

2. Harmonized Standard (EN 18031)

In April of 2022, the European Electromechanical Committee for Standardization (CENELEC), whose membership is EU countries (not companies or individuals) was selected by the European Commission to draft and approve the ”Voluntary Harmonized Standards” that would provide much more detail on requirements RED cybersecurity. CENELEC formed the Joint Technical Committee (JTC) 13 / Workgroup 8 to develop the standards. Those harmonized standards became European Norm (EN) 18031 and was approved as the official “Harmonized Standard” for Articles 3(3)(d), (e), and (f) in January 28, 2025 with the extended compliance date now being August 1st, 2025.

Note: There are exemptions from RED Articles 3(3)(d), (e), and (f) because there are already other regulations for them:

- Medical Devices – regulated by EU 2017 / 745 and EU 2017 / 746
- For the following – NOT 3(3)(e) or (f), But 3(3)(d) still applies
  - Civil Aviation – regulated by EU 2018 / 1139
  - Vehicles - regulated by EU 2019 / 2144
  - Toll Collection – regulated by EU 2019 / 520

EN 18031 consists of three different standards to address the requirements of Articles 3(3(d)(e)(f):

Table 2.1. Scope of EN 18031-1/2/3

Document	Description
EN 18031-1 for 3(3) (d)	Internet-connected radio equipment
EN 18031-2 for 3(3) (e)	Radio equipment that processes Personal, Traffic, or Location Data that is internet-connected OR designed or intended for Childcare, Toys, or Wearables (even if non-internet-connected)
EN 18031-3 for 3(3) (f)	Radio equipment that processes Personal, Traffic, or Location Data that is internet-connected OR designed or intended for Childcare, Toys, or Wearables (even if non-internet-connected)

Table 2.2. EN 18031 Requirement Summary

Security Mechanism	Requirement Summary	-1	-2	-3
[ACM] Access Control	Access control of security/network assets	Applicable	Applicable	Applicable
[AUM] Authentication	Entity is what/who it claims to be	Applicable	Applicable	Applicable
[SUM] Secure Update	Patches can be installed securely	Applicable	Applicable	Applicable
[SSM] Secure Storage	Secure stored assets	Applicable	Applicable	Applicable
[SCM] Secure Communication	Securely communicate assets	Applicable	Applicable	Applicable
[LGM] Logging	Log events relevant to assets	Not Applicable	Applicable	Applicable
[DLM] Deletion	Delete assets	Not Applicable	Applicable	Not Applicable
[UNM] User Notification	Notify user of changes of assets	Not Applicable	Applicable	Not Applicable
[RLM] Resilience	Mitigate Denial of Service (DOS) attacks	Applicable	Not Applicable	Not Applicable
[NMM] Network Monitoring	Detect DOS and defend	Applicable	Not Applicable	Not Applicable
[TCM] Traffic Control	Detect malicious comms traffic	Applicable	Not Applicable	Not Applicable
[CCK] Cryptographic Keys	Guidance on key size, generation, and use	Applicable	Not Applicable	Not Applicable

Security Mechanism	Requirement Summary	-1	-2	-3
[GEC] General Equipment Capabilities	Up-to-date software and hardware with no known “exploitable” vulnerabilities, no unnecessary external interfaces	Applicable	Applicable	Applicable
[CRY] Cryptography	Shall use for Secure Update, Secure Storage, Secure Comms	Applicable	Applicable	Applicable

3. Types of Equipment in Scope and Not

All newly designed equipment placed on the market on August 1, 2025, or later will need to comply with RED Articles 3(3)(d), (e), and (f). Any equipment already on the market (already manufactured and made available, but not necessarily sold to an end user) before August 1, 2025, can remain on the market without change until the end of their life cycle. However, even those currently in production designs will need to be evaluated for compliance and re-designed, if necessary, by August 1, 2025. There is no requirement for equipment already deployed and in operation to comply with Articles 3(3)(d), (e), and (f).

What is “internet-connected radio equipment”? Per the “Commission Delegated Regulations (EU) 2022/30 supplementing Directive 2014/53/EU with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e), and (f):

“of radio equipment which: (i) is capable itself to communicate over the internet, regardless if it communicates directly or via any other equipment (‘internet-connected radio equipment’), i.e., such internet-connected equipment operates protocols necessary to exchange data with the internet either directly or by means of an intermediate equipment”

Certainly, any equipment that uses Internet Protocol (IP) communication standards such as WiFi, Thread, or Wi-SUN, is definitely in scope. What about protocols like ZigBee, Bluetooth, Z-Wave, and proprietary protocols that do not use IP addressing?

The common interpretation of most Notifying Bodies in the EU, is that any equipment that can be seen, interacted with, or communicated with individually (i.e. “itself”) from the internet are in scope, even if not using IP based protocols. An example of a piece of equipment NOT in scope would be Sub-GHz proprietary temperature sensor that is connected to a WiFi smart thermostat but its data only feeds the smart thermostat temperature control algorithm and cannot be seen from the internet. The smart thermostat would be in scope, but the Sub-Ghz temperature sensor would NOT BE due to it not being individually readable from the internet.

What about Silicon Labs Modules or Development boards… are they in scope? Again, the common interpretation of Notifying Bodies in the EU is that for the equipment to be in scope, it must be designed to communicate over the internet without further modification.

Since a module or development boards from Silicon Labs must be programmed to communicate over the internet, which is a further modification, they are NOT in scope. This interpretation makes even more sense when you consider that an EN 18031 security assessment requires the end equipment sold into undergo a rigorous Threat Modeling and Risk Analysis based on its intended operational environment. Silicon Labs modules and development boards must be programmed with the final equipment application to become operational; therefore, it would not make any sense for Silicon Labs to perform a Threat Model and Risk Assessment of a module or development kit without even knowing what the end device will be.

4. Manufacturer's Responsibility

The responsibility for RED DA compliance lies with the manufacturer of the final "internet-connected radio equipment" that is being sold on the EU market. No matter how many great security features an MCU may have, if not properly implemented or enabled, there really is no security to protect the end consumer. Even if you find a module or MCU that states that it is RED security compliant or pre-certified, you cannot simply inherit that certification and be done.

As an equipment manufacturer placing radio devices on the EU market, you have specific legal obligations under Articles 3(3)(d), (e), and (f) of the Radio Equipment Directive (RED) 2014/53/EU, as activated by Commission Delegated Regulation (EU) 2022/30. These requirements become mandatory for all in-scope radio equipment starting August 1, 2025.

To comply, manufacturers should integrate cybersecurity and data protection measures into the design and development of their products from the outset—this is known as the Security by Design approach. Devices must be capable of resisting unauthorized access, tampering, or exploitation that could compromise networks, violate user privacy, or facilitate fraudulent activity. Technical features such as secure boot, authenticated software updates, secure communications, and proper access control should be assessed and implemented as needed.

Manufacturers are also responsible for conducting and documenting a risk assessment and threat modeling process. This involves identifying potential threats related to connectivity, data handling, and misuse, and then applying appropriate mitigations. The results of this assessment must be included in the technical documentation (technical file) for the equipment, which must be made available to national market surveillance authorities upon request. If a harmonized standard such as EN 18031 is used, it can simplify the demonstration of compliance with Articles 3(3)(d), (e), and (f).

Furthermore, you must update the EU Declaration of Conformity (DoC) to reflect the application of these newly activated essential requirements. This document must explicitly reference compliance with Articles 3(3)(d)–(f), along with the applicable standards or procedures used to meet them. Finally, your quality management systems should be updated to ensure continued compliance, including during software or firmware updates, product line changes, or the introduction of new features.

By fulfilling these responsibilities, you ensure that your products remain eligible for CE marking and legal placement on the EU market after 1 August 2025. Non-compliance may result in enforcement actions including withdrawal from the market, fines, or reputational damage. Therefore, early planning, implementation of robust design practices, and alignment with recognized cybersecurity standards are essential for a successful and compliant product release.

5. RED Compliance Process Choices

Manufacturers have two paths they can take to comply with the RED Articles 3(3) (d), (e), and (f) cybersecurity requirements.

If they use officially approved “harmonized standards”, which are only EN 18031 currently, then they can do a self-assessment. Note: refer to the EN 18031 standard for details.

Or, a manufacturer can choose to work with an official Notified Body to do the security assessment. A Notified Body is an independent organization authorized by EU member states to evaluate whether products meet the requirements. Some Notifying Bodies are Applus, Deckra, SGS, and TUV.

On January 28, 2025 the European Commission not only approved EN 18031 as the “Harmonized Standard” that allows self-assessment if followed but also spelled out 3 scenario exceptions that require a Notified Body evaluation even if EN 18031 is followed. Those scenarios are the following:

- If a product requires a password for access, sections 6.2.5.1 and 6.2.5.2 of EN 18031-1/2/3 specify how passwords should be managed. However, if users can choose not to set a password, the product does not comply with RED DA, even if it follows the harmonized standard.
- Standard EN 18031-2 (sections 6.1.3 to 6.1.6) outlines four access control mechanisms for toys and childcare products. Some of these methods may not be compatible with parental or guardian controls. In such cases, adherence to the EN 18031 harmonized standard alone does not ensure compliance with RED DA.
- Standard EN 18031-3 (section 6.3.2.4) describes secure update mechanisms. It defines four implementation categories: digital signatures, secure communication, access control, and others. None of these methods alone is sufficient for handling financial assets. The criteria do not fully address authentication risks and therefore cannot ensure compliance with RED DA.

6. Assessment using EN 18031

The breadth and depth of Internet of Things (IoT) products is staggering… from simple open close contact switches in a home security system to very complex WiFi routers, video cameras, and smart speakers in that same home environment. Each of these devices doesn't need the same level of security. They need the "right" level of security.

The authors of the EN 18031 standards were very conscious of the need for a very flexible evaluation process that considered the various levels of security defenses needed depending on what was at stake if the device was hacked. Like all criminals, hackers are attracted to value of the assets they can gain by spending the time and energy necessary to perform the attack and there is also the chance of being caught and going to jail… classic risk vs reward. Therefore, all good equipment security designs begin with a risk analysis to identify the assets in the equipment and their value (or risk) if they fall into malicious hands. If there is nothing of value to protect, there is no security mechanism needed.

So, the EN 18031 standard begins by doing a risk analysis of your choice to establish what the assets are and their value. Once the list of assets are determined, you then apply the required security mechanisms spelled out in the standard and are evaluated on if the applied security mechanism is adequate in light of the value of the asset. This technique allows for a lot of flexibility and judgement to come into play so that at the end… the "right" amount of security is applied to protect the end user.

When performing risk analysis, there is often asset value that is overlooked because it has nothing to do with the protecting the end use or their assets. One of those is the value of your brand. If your equipment makes the front-page news or is a case study of "what not to do" in every security magazine, your brand and your company could be permanently damaged. Another important value is loss of revenue to your company if your device is counterfeited, which can be compounded by brand damage if the inferior products erode brand trust. These values are often hard to quantify which is why buying security is often equated to buying insurance… you don't need it till you need it. The take-away here is to consider these values to your business when doing your risk analysis.

To understand the type of assets that are in scope, you must examine the 3 categories of devices that are called out by the regulation.

RED 1024 Directive 53 – Article 3(3)(d),(e),and (f)

- d) general internet-connected radio equipment
- e) radio equipment that processes personal, traffic, or location data that is internet-connected OR designed or intended for childcare, toys, or wearables (even if NOT internet-connected
- f) Internet-connected radio equipment that enables user to transfer, monetary value, or virtual currency

For the d) category there are Security and Network Assets. For e) you add Privacy Assets. For f) you add Financial Assets.

According to EN 18031, protecting these assets is not just about protecting the specific data stored, communicated, or processed, but also includes the protection of functions and configurations that might affect those assets. For general cryptography for instance, this not only means protecting high value secret cryptographic keys, but also the cryptographic functions themselves that process those keys.

Public asymmetric keys and public certificate chains are usually in the category of not being secret, but still unchangeable or immutable.

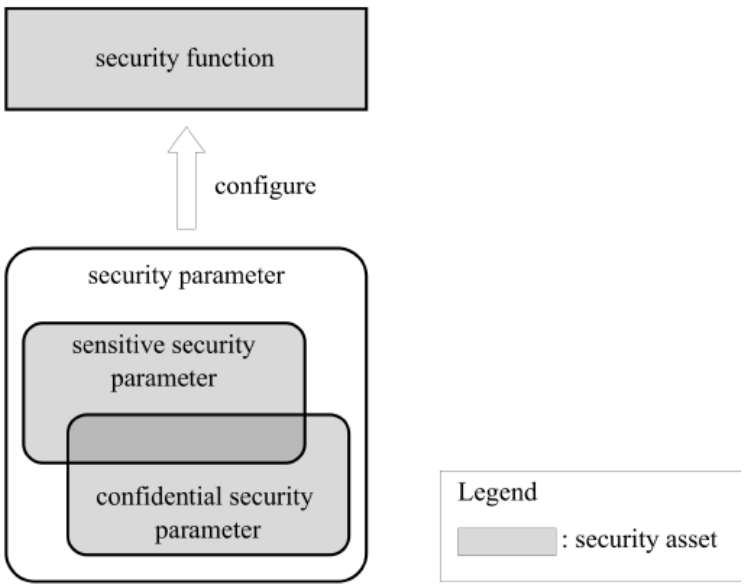


Figure 6.1.

6.1 Definition of Security Assets

A Confidential Security Parameter (CSP) per EN 18031 is secret security related information whose disclosure can compromise the security of and asset and must always remain confidential (secret). Examples would be PINs, passwords, symmetric keys, and public asymmetric keys. Sensitive Security Parameters (SSPs) are security related information whose manipulation can compromise the security of an asset. In security language that means it must remain immutable (not changed, modified, or deleted). A security parameter may need to be kept confidential AND remain immutable or it might be OK for it not to be confidential but still be immutable.

Public asymmetric keys and public certificate chains are usually in the category of not being secret, but still unchangeable or immutable.

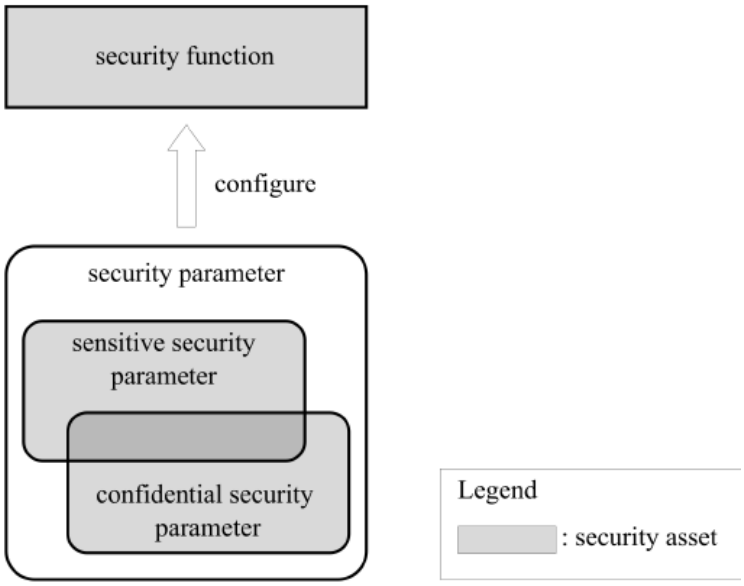


Figure 6.2. EN 18031 Definition of a Security Asset

6.2 Definition of Network Assets

Examples of a network function are a communication stack such as TCP/IP, ZigBee, Bluetooth, WiFi, etc. A DNS service providing network address resolution is another network function example.

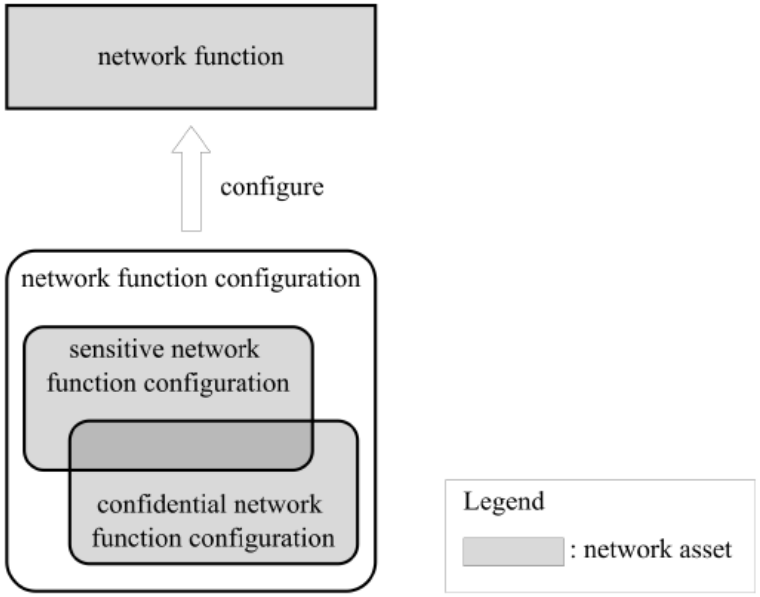


Figure 6.3. EN 18031 Definition of a Network Asset

6.3 Threat Modeling and Risk Analysis to Determine Which Assets Need to Be Protected

As the whole of the EN 18031 evaluation process depends on knowing the Security/Network Assets and their relative value, Security by Design and robust threat modeling and risk analysis are essential. The following standards, methods, and tools are particularly relevant within this regulatory framework:

RED-Relevant Standards and Frameworks

- **ISO/IEC 27005:2022 –** Provides a structured approach to information security risk management. It supports identifying and mitigating risks associated with network misuse and data protection—directly aligning with RED 3(3)(d) and (e).
- **ISO/SAE 21434:2021 –** While developed for the automotive sector, this standard offers useful guidance for embedded systems security, especially regarding asset-based risk evaluation and threat assessment consistent with RED compliance needs.
- **NIST SP 800-154 –** Focuses on data-centric threat modeling, making it highly applicable to RED Article 3(3)(e), which centers on user data protection.
- **ENISA Threat Landscape –** Provides sector-specific threat classifications and risk scenarios. These reports help anticipate the threat actors and attack techniques relevant to compliance with RED's fraud and privacy protection clauses.

Threat Modeling Methodologies for RED

To comply with RED Article 3(3), manufacturers should adopt one or more of the following structured methods:

- **STRIDE (Microsoft)–** Helps identify threats across network interaction boundaries. It is especially useful for analyzing risks related to data disclosure, network tampering, and elevation of privileges—risks central to RED Articles 3(3)(d) and (e).
- **PASTA (Process for Attack Simulation and Threat Analysis)–** A seven-step, risk-driven process that integrates both technical and business impact analysis. PASTA can directly support the creation of security documentation required under RED.
- **OCTAVE–** Offers an organizational risk perspective. This is useful when demonstrating due diligence in overall device lifecycle security, especially for manufacturers working across multiple product lines.
- **Attack Trees–** Help visualize how attacks can occur and which layers of protection must be added. These can be used in technical files to demonstrate fraud-prevention measures per RED 3(3)(f).
- **IEC 62443-4-1[1]–** Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements.
- **NIST 800-160[16]–** Systems Security Engineering; Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.
- **NIST 800-218[17]–** Secure Software Development Framework (SSDF)
- Microsoft Security Development Lifecycle (SDL)
- SAFECode Fundamental Practice for Secure Software Development
- GSMA FS.16 NESAS Development and Lifecycle Security Requirements

Tools for RED-Conformant Security Design

Several tools facilitate effective threat modeling and can help generate documentation to support the Technical Documentation and Declaration of Conformity (DoC) requirements under RED:

- **Microsoft Threat Modeling Tool –** Automates threat identification using STRIDE and is useful for producing traceable evidence of network and privacy risk evaluations.
- **OWASP Threat Dragon –** A free, open-source tool ideal for smaller manufacturers or design teams to implement security by design processes that map directly to RED requirements.
- **IriusRisk –** A commercial tool that enables automated threat modeling, risk scoring, and generation of security controls documentation, supporting both pre- and post-market RED obligations.

Learning Resources and Practical Guidance

For teams preparing for RED Article 3(3) compliance, the following are excellent references:

- **OWASP Threat Modeling Cheat Sheet –** Provides practical, lightweight guidance on integrating threat modeling into development lifecycles.
- **MITRE ATT&CK Framework –** A knowledge base of real-world tactics and techniques used by threat actors. This is useful for identifying realistic attack scenarios related to network compromise or data leakage.
- Key Books–
  - **"Threat Modeling: Designing for Security" by Adam Shostack –** Offers methodology and workflows that can directly support RED-compliant design documentation.
  - **"Engineering Trustworthy Systems" by Omar Santos –** Includes case studies on building secure systems and can help justify technical decisions in a RED conformity assessment.

6.4 Security Mechanisms are how you protect Assets

The EN 18031 evaluation methodology uses the concept of “Mechanisms” to protect the valued assets of a piece of equipment. As EN 18031 covers a wide range of products and use cases, the security objectives achieved need to vary depending on the intended use and operation of the equipment under evaluation. As we have discussed previously, the equipment needs to have the “right” amount of security. A specific security measure that might be appropriate for one piece of equipment may be too weak or strong for another. The EN 18031 assessment guides the user through questions and exceptions to decide if a particular mechanism is applicable or not. An example of a generic decision tree that you will see for each of the required Mechanisms.

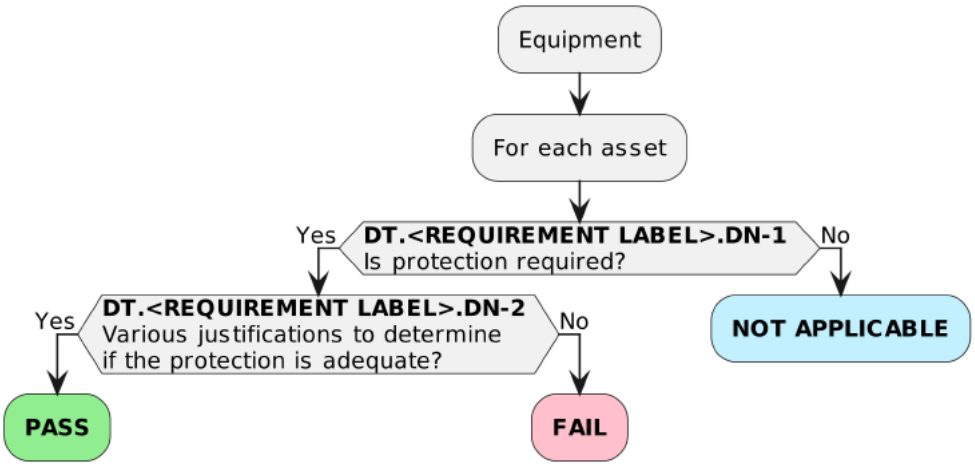


Figure 6.4. EN 18031 Generic Evaluation Decision Tree

6.5 Series 2 Secure Vault High (HSE) Mapping to EN 18031

The Series 2 Secure Vault™ High with Hardware Secure Engine (HSE) has many security features, services, and processes that are applicable in meeting the required security mechanisms. Please see table below for details:

Table 6.1. EN 18031 Requirement Mapping to Silicon Labs Security Features, Services, and Processes

Security Mechanism	Requirement Summary	Applicable Silabs Series 2 Secure Vault ™ High (HSE) Security Features/Services/Processes		-1	-2	-3
[ACM] Access Control	access control of security/network assets	Applicable	Secure Debug, Secure Engine (SE) Mailbox I/F, Key Management, Default Silicon Identities, Custom Identities w/ Custom Part Manufacturing Services (CPMS)	Applicable	Applicable	Applicable
[AUM] Authentication	entity is what/who it claims to be	Applicable	Default Silicon Identities, Custom Identities w/ CPMS	Applicable	Applicable	Applicable
[SUM] Secure Update	patches can be installed securely	Applicable	Secure Boot Root of Trust with Secure Loader (RTSL), Secure Firmware Upgrades (UG489)	Applicable	Applicable	Applicable
[SSM] Secure Storage	secure stored assets	Applicable	Key Management, Cryptography	Applicable	Applicable	Applicable
[SCM] Secure Communication	securely communicate assets	Applicable	Cryptography, Protocol Security	Applicable	Applicable	Applicable
[LGM] Logging	Log events relevant to assets	Applicable	Tamper Detection	Not Applicable	Applicable	Applicable
[DLM] Deletion	delete assets	Applicable	Tamper Detection deletion of secure keys and other assets	Not Applicable	Applicable	Not Applicable
[UNM] User Notification	Notify user of changes of assets	Not Applicable	Depends on final product design[1]	Not Applicable	Applicable	Not Applicable
[RLM] Resilience	Mitigate Denial of Service (DOS) attacks	Applicable	Secure Boot w/ RTSL, Watchdog Timer	Applicable	Not Applicable	Not Applicable
[NMM] Network Monitoring	Detect DOS and defend	Not Applicable	Depends on final product design[1]	Applicable	Not Applicable	Not Applicable
[TCM] Traffic Control	Detect malicious comms traffic	Not Applicable	Depends on final product design[1]	Applicable	Not Applicable	Not Applicable
[CCK] Cryptographic Keys	Guidance on key size, generation, and use	Applicable	TRNG, PUF, Cryptography	Applicable	Not Applicable	Not Applicable

Security Mechanism	Requirement Summary	Applicable Silabs Series 2 Secure Vault ™ High (HSE) Security Features/Services/Processes		-1	-2	-3
[GEC] General Equipment Capabilities	Up-to-date software and hardware with no known “exploitable” vulnerabilities, no unnecessary external interfaces	Applicable	Product Security Incident Reporting Process (PSIRP), Secure Debug, Depends on final product design[1]	Applicable	Applicable	Applicable
[CRY] Cryptography	Shall use for Secure Update, Secure Storage, Secure Comms	Applicable	Cryptography	Applicable	Applicable	Applicable

Note:

1. While no built-in security features exist to meet this requirement, application firmware can be written to address this requirement.

7. Platform Security Architecture (PSA) and Security Evaluation Standard for IoT Platforms (SESIP) Certifications for Series 2 Secure Vault™ High MCUs

Silicon Labs believes strongly that security is not something you can just put in a PowerPoint, Data Sheet, or Reference Manual. You must prove via a third-part security certification program that your security does what it has been designed to do but also at a high assurance level.

The oldest internationally recognized standard for evaluating security of IT products and systems is called Common Criteria (CC). This certification process has been most successfully utilized to evaluate and grade the security level of specialized very high security Secure Elements which are used in passports and credit cards.

However, this standard is far too rigorous and overcomplicated for most Internet of Things (IoT) products. Arm® Inc, knew that for IoT products to be successful they needed to be secure, but CC would be too much of a burden for those classes of devices with their advanced processing capabilities. So, Arm® set out many years ago to create a common Platform Security Architecture (PSA) standard to define for embedded processors. The most secure embedded processors on the market today follow this security architecture to various degrees.

But there also needed to be a standard way to evaluate the robustness of this architecture. Arm® then created a non-profit called psacertified.org to perform that certification. That certification process has three levels of certification. Level 1 is a self-certification that you meet the minimum requirements of the architecture. Level 2 adds security lab verification that you can withstand remote (device not in hand) security attacks for a set period. Level 3 adds local physical attacks to the remote and adds more time.

However, there was still a large amount of inertia behind Common Criteria certification and its processes, especially in Europe. Therefore, several European silicon companies developed a Common Criteria “Light” called Security Evaluation Scheme for IoT Platforms (SESIP). Like CC, SESIP uses the concept of standardized Protection Profiles (PPs). Protection Profiles are a standardized list of Security Functional Requirement(s) (SFRs) per type of device. The SESIP methodology is administered and maintained by GlobalPlatform.org.

Unfortunately, PSA and SESIP were competing processes for getting a security certification for an embedded processor. Subsequently, Arm® and GlobalPlatform agreed to create Protection Profiles that matched the SFRs required by PSA Level 2 and Level 3. PSAcertified.org will now recognize the SESIP-PSA Level 2 and Level 3 Protection Profiles so that a single lab evaluation can result in a combo SESIP/PSA Level 2 or Level 3 certification.

Since the European Union is partial to SESIP as it is Common Criteria based, EN 18031 references a SESIP to EN 18031 mapping in Annex D.

The two figures below help explain the advantages of the separate Secure Engine with its own core, flash, and RAM in achieving PSA/SESIP Level 3 with Series 2 Secure Vault™ High with HSE MCUs.

With this separate security sub-system, shown outlined in red in Figure 7.1, the PSA Immutable Root of Trust (RoT) functionality is provided by the Root of Trust Secure Loader (RTSL) ROM code (See Secure Boot with RTSL section of this User Guide for details). The PSA Updatable RoT functionality is provided by the Secure Engine (SE) firmware. The isolation barrier required between the PSA Updatable RoT and the Application RoT is provided by the HSE Application Interface (API) to the Host M33 core in the MCU.

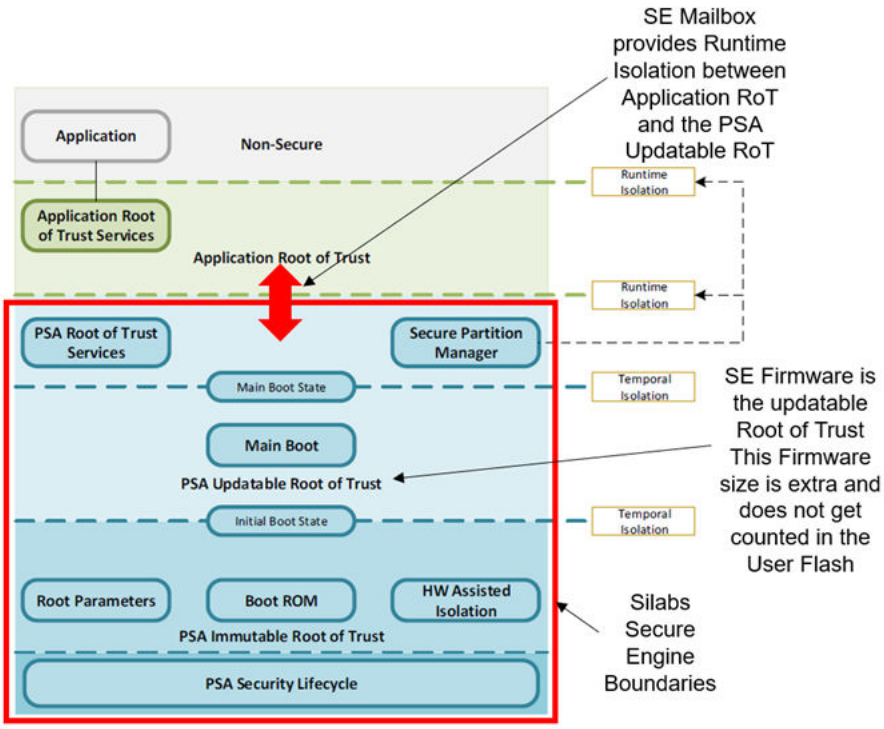


Figure 7.1. Silabs Secure Vault™ High PSA Level 3 Implementation

For contrast, Figure 7.2 illustrates a hard-gated security sub-system PSA/SESIP Level 3 implementation. Notice that to achieve the PSA Updatable RoT, the implementation requires the use of TrustZone or another similar Trusted Execution Environment (TEE) to achieve the separation between the PSA Updatable RoT and the Application RoT. The implementation of TrustZone in software comes with a hefty penalty in complexity and flash and RAM usage whereas with a Secure Vault™ with HSE part from Silicon Labs it has all that complexity, flash, and RAM built into the HSE.

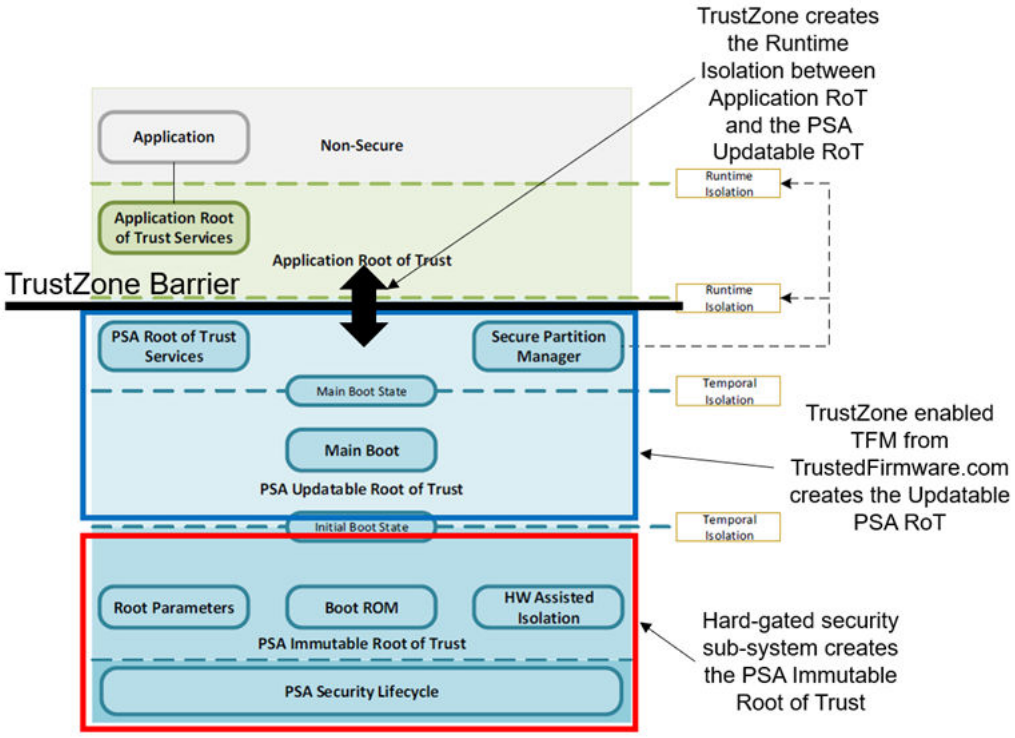


Figure 7.2. Hard-gated Security Sub-system PSA Level 3 Implementation

8. Custom Part Manufacturing Service (CPMS) and Security Programming

The Radio Equipment Directive 2014/53/EU - Articles 3(3)(d,e,f) must be enabled by programming of the Silicon Labs MCU. This programming may be done by whomever is manufacturing the “Equipment” under evaluation for RED security compliance. Or, Silicon Labs offers a service to create a custom part with all of the security features enabled/programmed in our secure manufacturing facility. We call this service the Custom Part Manufacturing Service or CPMS. With all of the Secure Vault™ features enabled in our factories, you can ensure a high degree of certainty that our silicon is not tampered with while in your manufacturing supply chain.

Table 8.1. Custom Part Manufacturing and Secure Programming Reference Documents

Reference	Title and Web Link
Docs.silabs.com	Custom Part Manufacturing Service (Link)
Docs.silabs.com	PKI Recommendations (Link)
http://www.silabs.com	CPMS Getting Started Web Link (Link)
AN1222	Production Programming of Series 2 Devices (Link)
AN1303	Programming Series 2 Devices using the Debug Challenge Interface (DCI) and Serial Wire Debug (SWD) (Link)

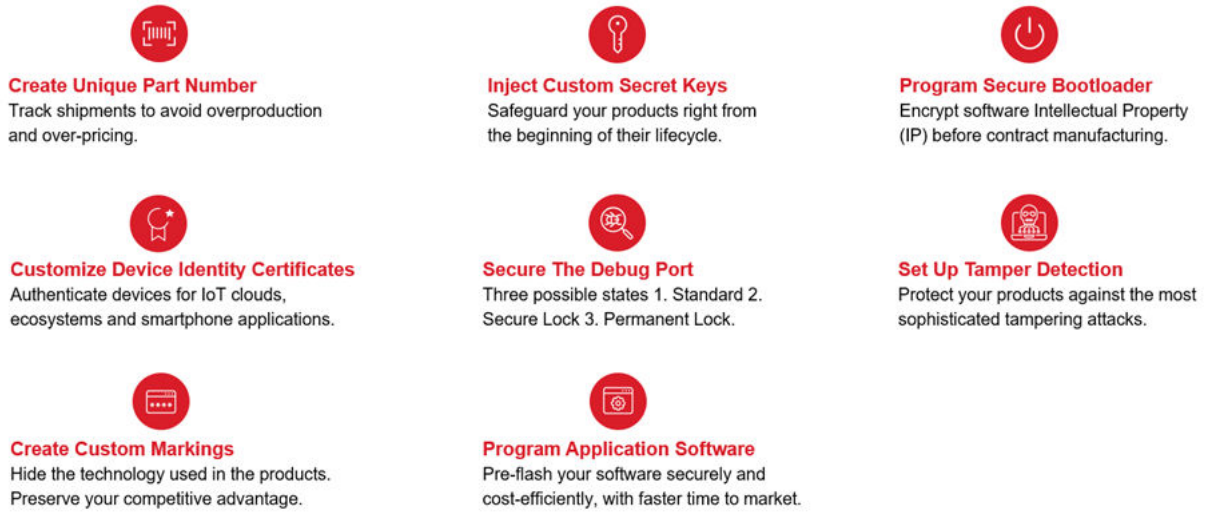


Figure 8.1. Silicon Labs CPMS Programming Options

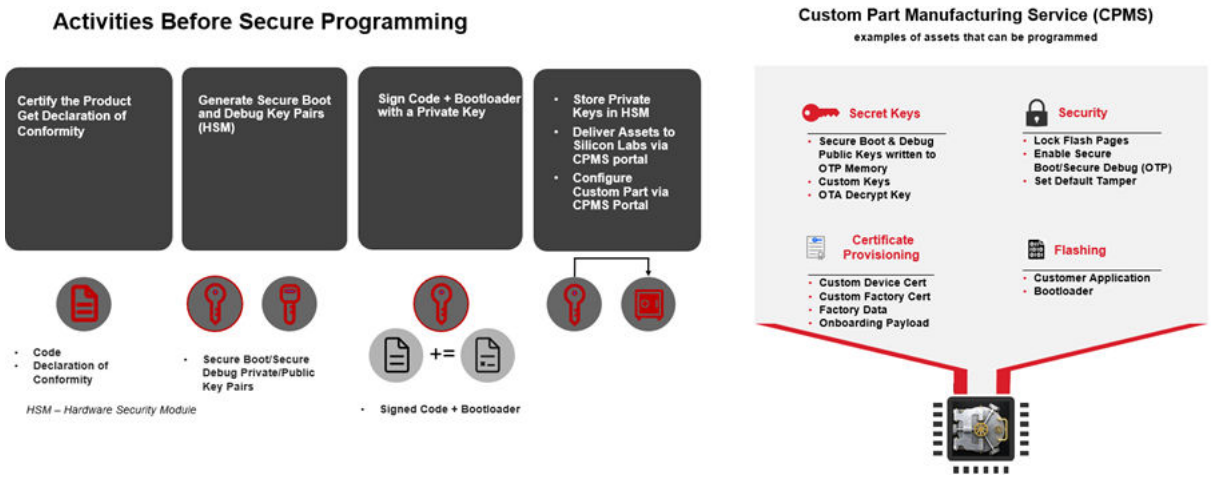


Figure 8.2. CPMS Process Flow

9. [ACM] – Access Control Mechanism (EN 18031 -1, -2, and -3)

Summary of Requirement:

The equipment shall use access control mechanisms to ensure that only authorized “entities” have access to protected security/network assets. Note: refer to the EN 18031 standard for details.

From EN 18031 Terms and definitions:

- “Entity” – user, “device”, equipment, or service
- “Device” – product external to the equipment

Access control mechanisms are usually thought of as Username and Password from an end equipment perspective. However, from the Silicon Labs SoC perspective, every external function/action/communication to or with the SoC itself is considered to be by another “Entity”.

There are many effective security features that can be applied to assure no external functions (“Entities”) can access any of the internal workings of the Silicon Labs System on Chip (SoC). Certificate identities can be used to authenticate external “Entities” before communicating with them. Locking the debug port is a very simple way to prevent easy physical access to the security and network assets contained in the SoC. Enabling Secure Boot w/ Root of Trust Secure Loader (RTSL) and triggering a secure boot periodically to authenticate the code base running on the SoC is an excellent way to assure that no malware has infected the SoC (see the [SUM] – Secure Update Mechanism section of this document for details). Secure Vault™ High tamper protection is an extremely effective way to prevent any local physical attack methods known today and in even in the future as those attacks become more sophisticated such as Laser glitching.

Also, as with all wireless technologies the communications protocol itself can be susceptible to man-in-the-middle attacks as well as replay attacks. All the major standards-based protocols used today on Silicon Labs parts, i.e. Wi-Fi, Bluetooth, ZigBee, Thread, Wi-SUN, Z-Wave, and Matter, have very sophisticated cryptographic based onboarding and operational processes that ensure devices are certified and trusted.

The layering of security in a secure MCU like Series 2 Secure Vault High is a very effective tool to frustrate a cyber-attack and limit access to security and network assets.

A physical world analogy for this type of security layering, is a secure building. The building has a top-notch security system with contact switches on all doors and windows as well as motion sensors throughout the building (Tamper Detection). The building has a guard and security barriers at the entry (Secure Debug). There is an even more secure room (the Hardware Secure Engine (HSE) within that secure building which houses all the security systems (Cryptography). To enter this room requires inherence authentication (what you are) like an iris scan or other biometrics (authentication) to enter this room also has one other major security feature that is not always appreciated, but critical… it only has one door in or out. Entering that room is tightly controlled… but, leaving that room is not. Anyone already in the room is considered a trusted individual and pretty much can go anywhere in the building once they leave the room (The Hardware Secure Engine (HSE) Mailbox). In this secure room, there is also a vault where all the security key cards, cash, and jewels are stored (PUF Wrapped Key Storage).

The following sections describe the security features in Series 2 Secure Vault™ High with a Hardware Security Engine (HSE) can be applied in an equipment-based access control mechanism.

9.1 Tamper Detection

As mentioned in our physical world analogy of a secure building, the first line of security defense for any commercial building you build today would be the security monitoring system. It's the first line of defense, because it is "automatically" going to warn you if there is anyone trying to break into the building. Similarly, for the Series 2 Secure Vault™ High parts, the front line of defense for our secure MCUs is our very sophisticated and effective Tamper Detection security feature. Just like the building secure monitoring system… it is "automatically" monitoring for any physical attack on the Silicon Labs MCU.

There are multiple sources of tamper events. Most are generated internally but there are also 8 external configurable tamper pins which can be used on external equipment cases, tamper meshes, or PCB bus traces to protect security or network assets. There is also a very sophisticated glitch detection circuitry mechanism in our Secure Vault™ High parts built into the upper layers of the silicon. Depending on the specific tamper, the user will be able to select the severity of the tamper response. The response can range from No Action… to an interrupt where the user application can do some reconnaissance and act… to a reset which allows the system to see if the glitch disappears and whether it may have been an anomaly. These levels of action allow the user application to ratchet up the response if a particular event is repetitive or take drastic action if certain things happen like the case of the device being opened.

The most extreme action is to erase the PUF reconstruction data which prevents the Key Encryption Key from ever being used again, which locks the key-blobs in their encrypted form. If developers choose to use this option in their design, it effectively 'bricks' a piece of equipment. Any customization of tamper settings, other than the default configuration, must be programmed into One-Time Programmable (OTP) memory during manufacturing. Silicon Labs' Custom Part Manufacturing Service (CPMS) can be used to do this programming if desired.

Table 9.1. Tamper Detection Reference Documentation

Reference	Title and Web Link
AN1247	Anti-Tamper Protection Configuration and Use (Link)

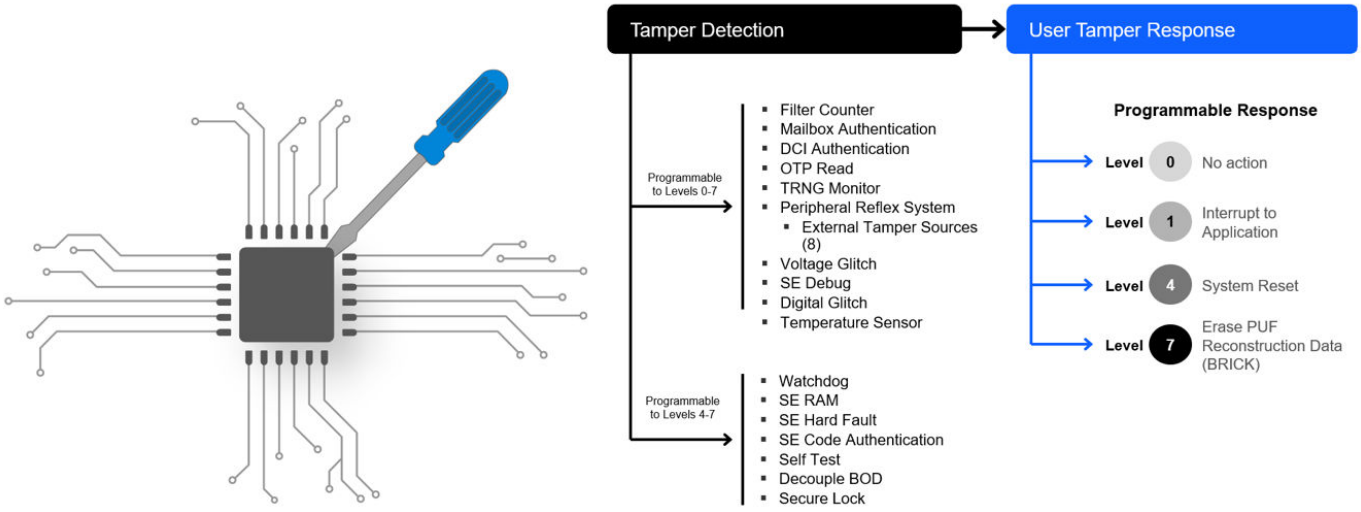


Figure 9.1. Secure Vault™ HSE Tamper Detection

9.2 Secure Debug

Using our physical world analogy of the secure building again, the Secure Vault™ High Secure Debug feature is like the security guard or badge reader at the front entrance of the building. You can present the reader or guard your badge credential, and if it validates, you are let into the building. This is very similar to our Secure Lock state of the debug port. If you present a cryptographic token to the debug port, and it validates, you can get access to the MCU assets. There are 4 lock states to a Silicon Labs Series 2 MCU which are defined below. Glitching open debug ports of MCUs has become trivial over the last few years and has become the easiest way to break open an MCU because you have access to all of its security and network assets. To prevent this from happening with Silicon Labs Series 2 SoCs, we have spent a large amount of effort to make sure that our debug states have been extensively glitch mitigated and tested by third-party labs.

Table 9.2. Secure Debug Reference Documentation

Reference	Title and Web link
AN1190	Series 2 Secure Debug (Link)

1. Unlocked can transition to any locked state
2. The Standard Lock state can revert to unlocked via Device Erase
3. Secure Lock can support a temporary unlock, but the state reverts to Secure Lock
4. Secure Lock can transition to Permanent Lock but cannot transition to a less secure configuration
5. Permanent Lock is a terminal state

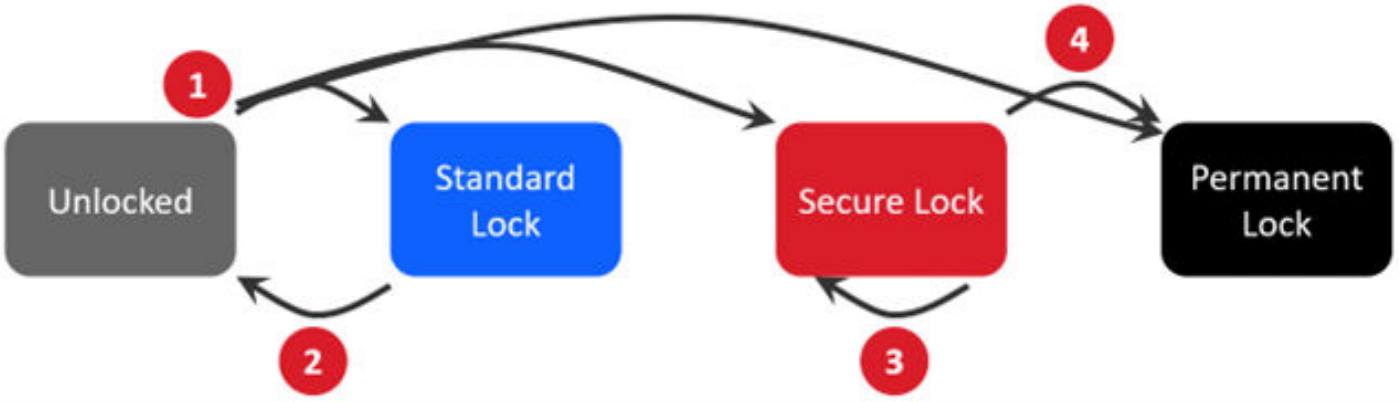


Figure 9.2. Debug Lock States

The Secure Lock state starts at the manufacturing facility where the customer's HSM creates a Command Private/Public Key pair. The secret Command Private Key stays in the HSM and the Command Public Key is programmed into the OTP of the Silicon Labs Series 2 chip. Silicon Labs can provide the service to program the OTP with the Command Public Key with its CPMS service.

Typically, all devices with the same model number will receive the same Command Public Key… but this is not a hard and fast rule and is up to the customer how granular they want to get with the Command Key Pairs.

Figure 9.3. Secure Lock State Requires a Public Key Generated by and HSM

The figure below demonstrates how a Secure Lock implementation can be used to send a part back to Silicon Labs for analysis with a cryptographic token that can be used to unlock the part without erasing the flash which is often necessary for failure analysis. This model could also be used with the equipment maker's own internal return and failure analysis department.

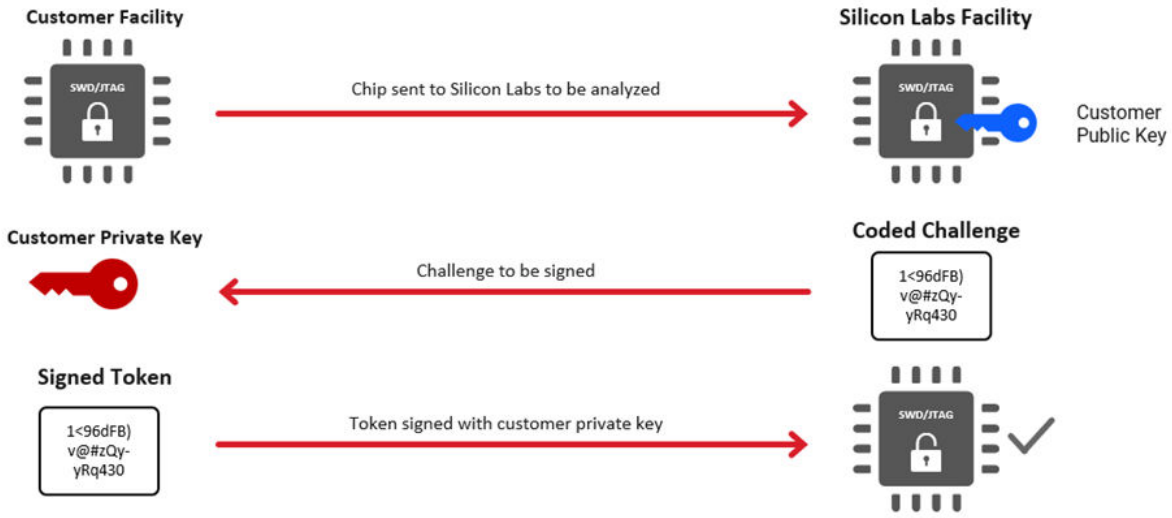


Figure 9.4. Secure Lock Use Case Example

9.3 Hardware Secure Engine (HSE) Mailbox Interface

In the physical world analogy of the secure building above, remember there is an even more secure room (the Hardware Secure Engine (HSE) within that secure building which houses all the security systems (Cryptography). To enter this room requires inherence authentication (what you are) like an iris scan or other biometrics (authentication) to enter this room also has one other major security feature that is not always appreciated, but critical… it only has one door in or out (The Hardware Secure Engine (HSE) Mailbox). But even a doorway is too broad of an analogy… it is more like a mail slot in the door that you can only pass very specific filled out pre-defined request forms through the mail slot for the personnel inside to perform the task associated with the request form. Anyone already in the room is considered a trusted individual and pretty much can send free-form cash, and jewels are stored (PUF Wrapped Key Storage).

Some of you may be familiar with chips that are called Secure Element's which are used in bank cards and passports. There are many companies selling secure elements and telling you to just put it next to your standard Non-secure MCU and you have a secure system. That is like saying, build a secure room separated by a very long walkway through a public park and your entire main building on the other side of the park will also be secure. What happens if someone mugs you in the park as you are walking to the main building. What if you have no security in the main building and the mugger has hidden in there.

With Secure Vault™ High, we have essentially pulled an external Secure Element into our silicon. But the beauty of our integrated system is that you don't need to worry about securing the connection to the external Secure Element as we have securely integrated it for you. The secure room is inside the secure building now.

Our Security Engine has its own independent MCU, Flash, RAM, and ROM and all the things it needs to do cryptography within the walls of the secure subsystem. The only way to get into this security subsystem is through a single, very tightly controlled interface, called the "Security Engine (SE) Mailbox". This mailbox is a means of limiting access to the most important security functions and assets in the MCU. Even if an intruder manages to get into the host CM33 core (the secure building), they cannot get into the secure room except to do very controlled transactions such as cryptography. But the security assets like private and secret keys, never leave the secure room. The CM33 interface is extensively "Fuzz" tested… which means we try as many variations of bogus commands as we can think up, to try and get the interface to do something unusual. Something unusual or unpredicted is usually what leads to vulnerability. We also trust the SE, so we allow it full Supervisory access to the CM33 world. Just like you would assume someone that originates from the secure room can pretty much go anywhere else in the building.

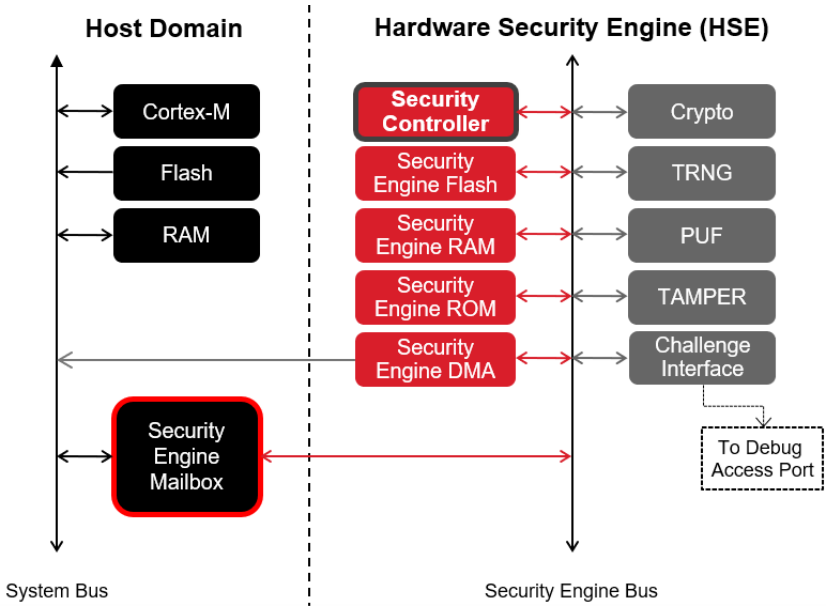


Figure 9.5. Secure Vault™ Hardware Security Engine (HSE)

9.4 Additional Application Isolation with TrustZone

While TrustZone is not necessary for obtaining PSA/SESIP certification (see section above), you may still want to create your own additional trusted services in the “Application Root of Trust” shown in the green area in the below figure as defined by the ARM Platform Security Architecture (PSA). This would allow even finer granularity of access control if needed by your equipment implementation. See the application note referenced below for more detail on how to implement TrustZone which is built into every Series 2 MCU from Silicon Labs.

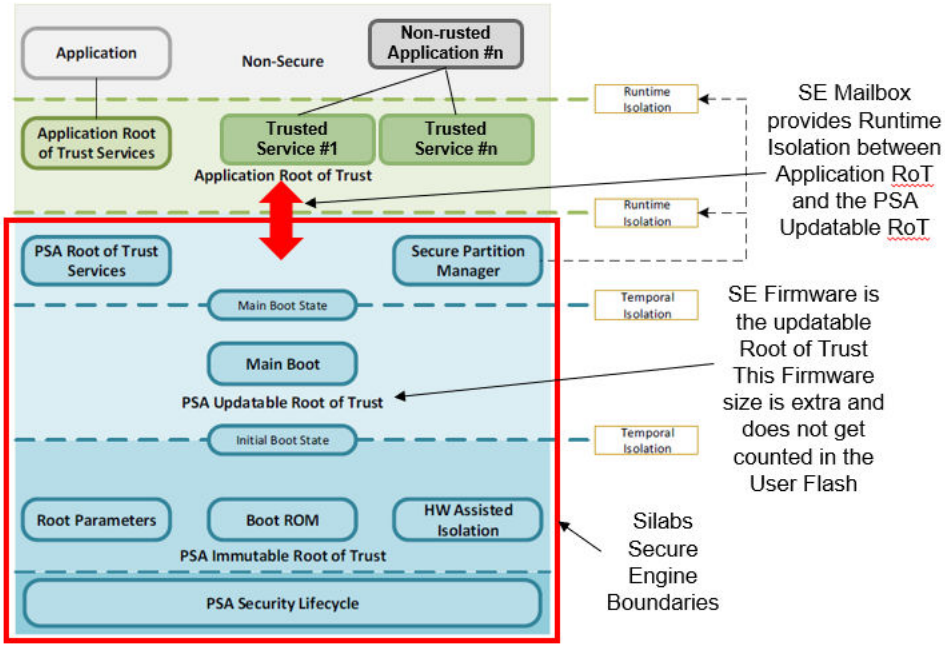


Figure 9.6. Silicon Labs Secure Vault™ High PSA Level 3 Implementation

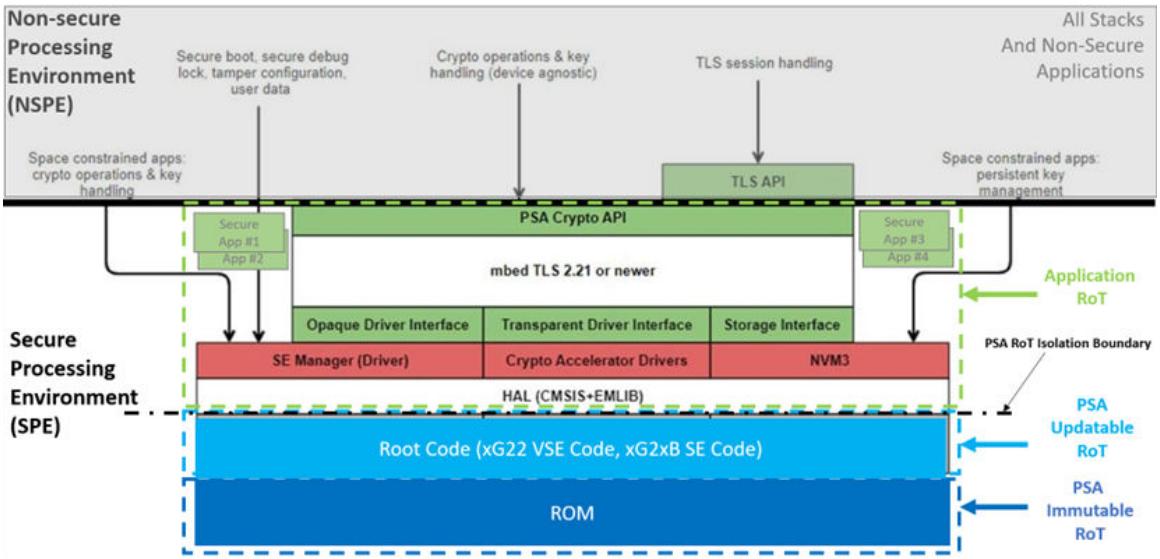


Figure 9.7. Silicon Labs Secure Vault™ High PSA Root of Trust Implementation

10. [AUM] – Authentication Mechanism (EN 18031 -1, -2, and -3)

Summary of Requirement:

For all required Access Control Mechanisms determined in [ACM], an authentication mechanism is required for all network and/or user interfaces that shall verify an “Entity’s” claim of authenticity based on one factor authentication of the following: knowledge (what you know), possession (what you have), or inherence (what you are i.e. biometrics).

Note: Refer to the EN 18031 standard for details.

10.1 Silicon Secure Identities Used to Authenticate the Secure Engine (SE)

In our physical world secure building analogy, the SE Mailbox is acting as mail slot in to and out of the Secure Engine (SE). We can send filled out pre-formatted request forms into and out of the secure room. But what if somehow the personnel carrying out the task in the secret room have been personally compromised by greed or blackmail. How do you verify the SE has not been compromised and is authentic.

All Silicon Labs Series 2 Secure Vault™ High HSE parts come from the factory with a Silicon Labs identity that can be used to perform a 3-factor authentication of the Silicon Labs MCU. The first part of the 3-factor authentication is to validate what the SE’s possession (what you have) by requesting the Batch and Device certificates which are stored in immutable One Time Programmable (OTP) memory. The Silicon Labs Root and Factory Certification are retrieved from the Silicon Labs website and once all the certificates are obtained, the certificate chain can be cryptographically validated from the Device to the Root certificate. The next step of the authentication process is to confirm knowledge (what you know) by asking the SE for a PSA Attestation Token and/or Security Configuration Token. Both tokens have specific information about the SE such as SE firmware version, boot seed, unique ID, tamper settings, security OTP configuration, public sign key, command key, etc. These pieces of information constitute what the SE knows and can be independently validated. The third authentication factor is to validate inheritance (what you are). The SE possesses a unique fingerprint which is the unique Device Private Key stored wrapped in OTP that corresponds to its Device Public Key that came with the Device Certificate. The tokens are signed by the SE with this Device Private Key so checking the signature of the tokens verifies “what the SE is” for the final authentication factor check.

Table 10.1. Secure Identities Reference Documentation

Reference	Title and Web Link
AN1268	Authenticating Silicon Labs Devices Using Device Certificates (Link)

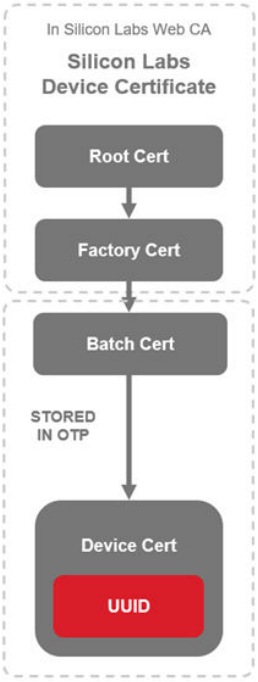


Figure 10.1. Silabs Secure Vault™ High Silicon Labs Identity Certificate Chain

10.2 Customized Secure Identities Used to Prevent Counterfeiting and Authenticate External "Entities"

With the Silicon Labs Custom Part Manufacturing Service (CPMS), the Silicon Labs Silicon Identity certificate chain can be modified to customer specifications. The customer will specify the fields in the Device and Factory certificates that they would like to modify and with what values. The customized Factory Cert can then be signed into the Customer's Root CA via Certificate Signing Request (CSR). Once all of this is complete, the Silicon Labs Identity has been transitioned into an identity of the Customers. The 3-factor authentication can be accomplished exactly as described above for the Silicon Labs Identity, but now it will authenticate not only the Secure Engine and its contents, but also that the device is a unique part manufactured for the Customer. This authentication, paired with the Secure Boot, Secure Debug, and Tamper Detection create a chip that is virtually impossible without complete re-engineering of the chip to duplicate… thus impossible to counterfeit.

Table 10.2. Learn more about Certificate Based Authentication and Pairing (CBAP)

Reference	Title and Web Link
http://www.silabs.com	Certificate Based Authentication and Pairing (Link)

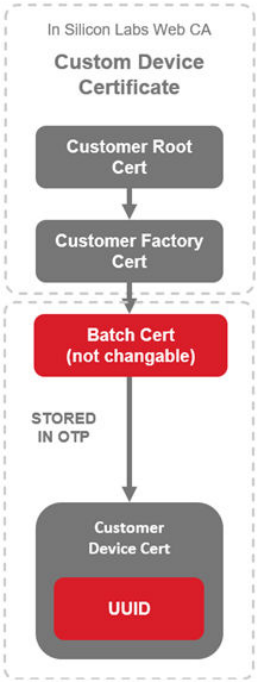


Figure 10.2. Customized Secure Vault™ High Silicon Labs Identity Certificate Chain

11. [SUM] – Secure Update Mechanism (EN 18031 -1, -2, and -3)

Summary of Requirement:

For software affecting security or network assets and is updatable and not an exception per the EN 18031 standard, must be proven to be updatable and must ensure integrity and authenticity of the update image. This update must be automatic, scheduled under human approval, or triggered under human approval if needed to prevent operational damage.

Note: Refer to the EN 18031 standard for details.

The security definitions of Integrity and Authenticity are:

- Integrity - protect data from unauthorized modification or destruction
- Authenticity - assurance that data genuinely originates from their claimed source

11.1 Secure Boot with Root of Trust Secure Loader (RTSL)

There are multiple ways allowed to accomplish this (refer to SUM-2 Secure Updates – Implementation Categories) The way that Silicon Labs recommends meeting this requirement is to cryptographically sign images of all updatable software and use our Secure Gecko Bootloader in combination with our Secure Boot w/ Root of Trust Loader (RTSL) as the security mechanism. Since the firmware of the Secure Vault ™ Engine is updatable, you will need to update that in addition to your application to meet the specification. The application and the Secure Engine firmware are updatable separately so that the memory required for staging updates can be minimized.

For all Secure Vault ™ High parts in Series 2, there is dual MCU Architecture where the Security Engine (SE) has its own One Time Programmable (OTP) memory as well as its own Flash and ROM. The Application MCU is separated with its own Flash (refer to the following figure).

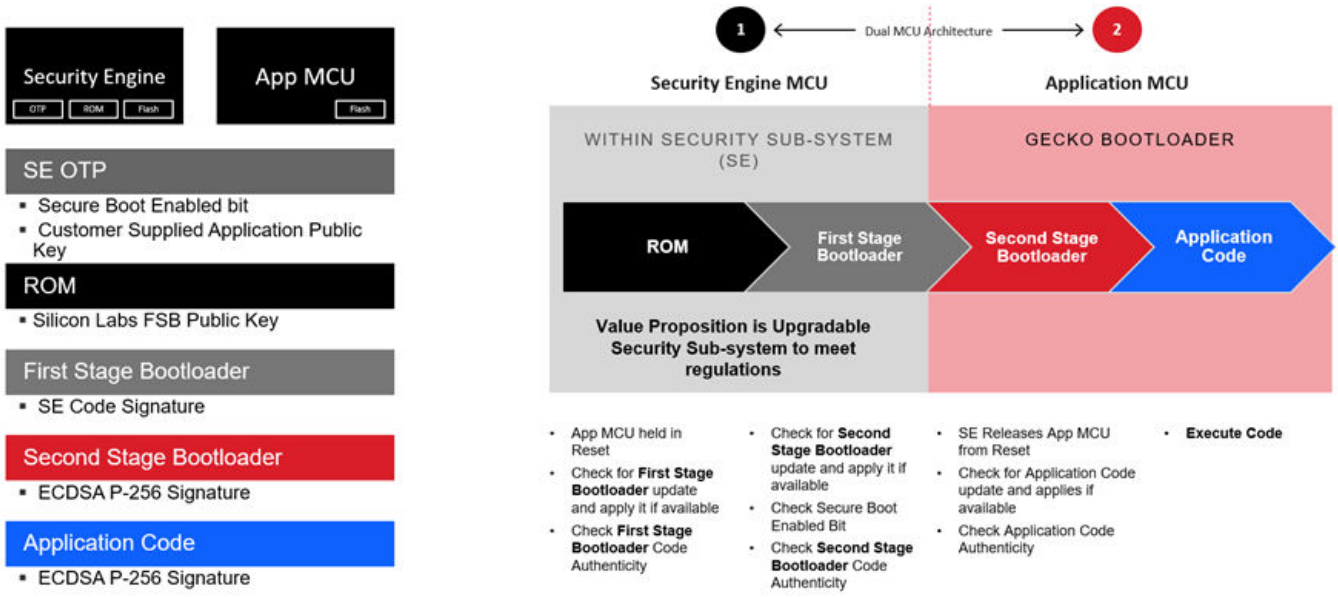
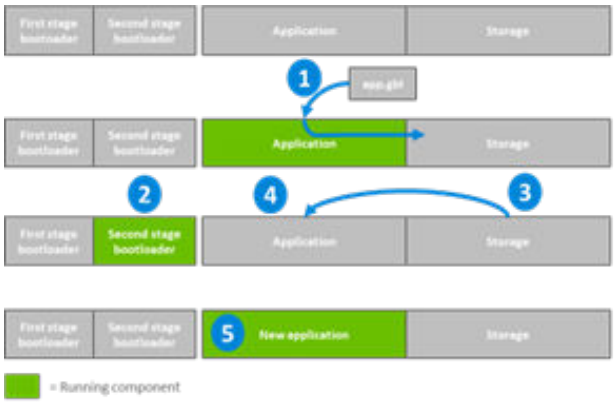


Figure 11.1. Series 2 Secure Loader Example

The first thing to recognize in a Series 2 Secure Vault High (HSE) with RTSL is that there are two separate microprocessors taking on very specific task during the boot process. The Security Engine (SE) MCU provides the hardware “Root of Trust” which is the immutable ROM boot code and then also runs the First Stage Bootloader (FSB) firmware within the Security Engine. Control will then be passed to the Gecko Bootloader (GBL) running in the Application MCU which will run the Second Stage Bootloader (SSB).

The boot process starts with the App MCU being held in reset and the Security Engine (SE) ROM code checking for a First Stage Bootloader (FSB) update and applying it if available. Then the ROM checks the signature of the FSB and if that checks out, the FSB firmware starts executing. The first thing the FSB does is check for an update of the Second Stage Bootloader (SSB) and apply it if available. Then, if the Secure Boot Enable bit is set, the FSB will verify the signature of the SSB and will release the App MCU from reset to start executing the SSB code. That SSB code is responsible for checking for an update of the application code, applying that update if present, and then checking the signature of the application code with the customer’s application public key which is called the Public Sign Key (PSK). The PSK is provided by the customer and should be generated and stored in an FIPS compliant Hardware Security Module (HSM). To enable RTSL the customer will need to program the PSK into the part at manufacture as well as program the Secure Boot Enable flag. Silicon Labs has a Custom Part Manufacturing Process (CPMS) that can program both of these items if desired (see Link for details)

We call this entire process “Secure Boot with Root of Trust and Secure Loader” or “Secure Boot with RTSL” for short. “Root of Trust” refers to the immutable ROM and “Secure Loader” refers to the First Stage Bootloader (FSB) that is part of the Hardware Secure Engine (HSE) firmware that is pre-loaded at the Silicon Labs factory (See the Figure below). This multi-staged and linked public key cryptography bootloader architecture is incredibly effective at resisting security attacks as all stages must be compromised to load malware into the silicon.



1. The existing application downloads the upgrade image onto the storage medium of the device (for example, the app.gbl file through OTA).
2. The device reboots into the second stage bootloader, and the bootloader enters firmware upgrade mode.
3. The secure loader in the second stage bootloader verifies the integrity and authenticity of the staged upgrade image in storage, prior to performing the upgrade.
4. The second stage bootloader applies the application upgrade from the upgrade image.
5. The device boots into the application. Application upgrade is complete.

Figure 11.2. Series 2 Secure Loader Example

On the surface, being able to update the SE firmware may seem inconvenient. However, over time security attack methods are becoming more and more sophisticated… algorithms that were secure today are not secure tomorrow. For an IoT device that is in the field for 10-20 years or even 2-3 years, being able to patch the SE firmware if an exploit is developed or an algorithm is broken becomes critical to ensuring your customers are protected as well as the brand value of your company.

For more details, please reference the following Application Notes:

Table 11.1. Secure Boot Reference Documentation

Reference	Title and Web link
UG103.6	Bootloader Fundamentals (Link)
UG489	Silicon Labs Gecko Bootloader User's Guide for GSDK 4.0 and Higher (Link)
AN1218	Series 2 Secure Boot with RTSL (Link)

12. [SSM] Secure Storage Mechanism (EN 18031 -1, -2, and -3)

Summary of Requirement:

Secure storage mechanisms shall be used to protect security and network assets that are stored persistently on the equipment. The integrity of each persistently stored security or network asset shall be protected and if that asset is a confidential asset, then its confidentiality (secrecy) shall also be protected.

Note: Refer to the EN 18031 standard for details.

12.1 Secure Vault High Secure Key Storage

All security schemes fall apart if the secret keys do not remain confidential (secret). Secure Vault High Series 2 parts all come with a very sophisticated and flexible secure key storage mechanism whose design using a Physically Unclonable Function (PUF) allows for securely storing a large amount of key material encrypted (or wrapped) which is only limited by the amount of flash (internal or external) available for such purpose. Since the PUF creates a unique seed key that creates a unique encryption key only when the part is powered up, a cheap flash read out of memory when the part is powered down is unable to obtain the encryption key. The seed key from the PUF is piped directly to the AES engine via a sea of gates in multiple layers and therefore that pipeline cannot be sniffed effectively to gain access to the seed key. Also, the AES engine holds the Root Key (RK) in its internal RAM which disappears when the part is powered down. All these mechanisms result in a key storage mechanism that would require re-engineering the chip to hack which is incredibly expensive and time consuming.

The figure below shows a high-level block diagram of Secure Vault High Key Management which is explained further below.

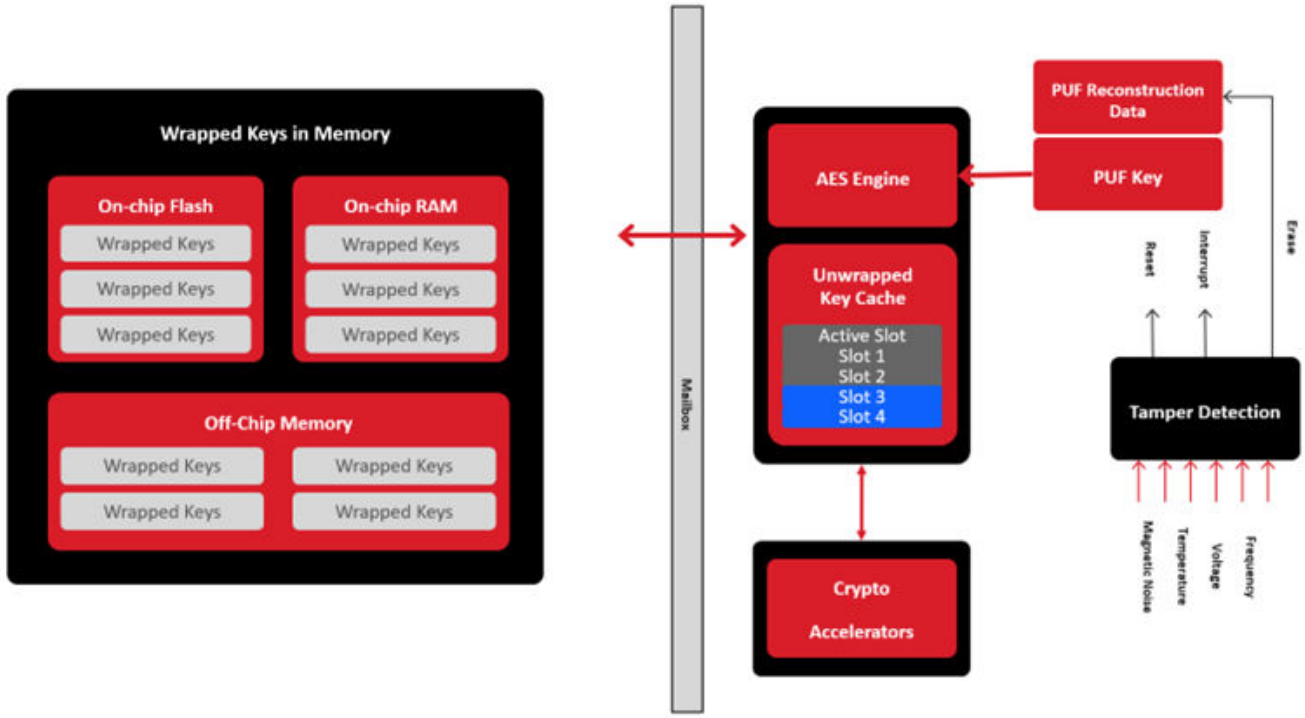


Figure 12.1. Secure Vault High Key Management

A common way to protect secret keys in other MCUs is to store them in protected memories. Protected memories are complex and take a lot of die area, so naturally, the number of protected key slots would need to be minimized. However, depending on the complexity of the device and its communications, several sets of asymmetric key pairs are likely to be needed on the device at any given time. Asymmetric keys tend to be large and as communications security becomes more complicated over time, the number of key pairs will increase… not decrease.

The other method to store key pairs when you are not actively using them, is to encrypt them, also called wrapping, in what are called 'key-blobs' which are normally stored in internal/external unprotected memories.

The problem with this strategy is that your whole security scheme now depends on a single secret key, the HSE Root Key (RK), used to encrypt and decrypt the key-blobs.

To address the challenge with the RK protection, Secure Vault generates the RK dynamically every time the silicon powers up. We do this with what is called a SRAM Physically Unclonable Function or PUF. A PUF creates a RK that only the chip knows, is never transmitted or stored in memories, and disappears when the chip is powered down.

So now that we have a very secure Root Key, we can use the RK as the private key, with AES 128 bit strength, in the Security Engine to securely wrap and un-wrap any number of key pairs and store them in On-chip Flash, On-chip RAM, or Off-chip Flash. The Security Engine supports generation of AES Symmetric keys up to 256 bits and ECC Asymmetric key pairs, up to 512 bits for the private key, which can then be exported and wrapped. There are five key slots in the Security Engines private RAM where the current "working" keys are temporarily stored. Once the keys are in these key slots they can be continuously used by the various crypto accelerators in the SE until other keys need to be unwrapped and brought into the key slots for use. This saves valuable time on the wrap and unwrap functions.

Our tamper detection system can trigger many different actions such as a chip reset, a code interrupt, and in the most extreme case, it can wipe the PUF reconstruction data. Erasing that data will prevent the PUF key from ever being reconstructed again. This means

that all the keys that are encrypted in external memories will never be able to be decrypted. Also decrypting the Public key, which is stored in OTP and used in our secure boot, cannot happen, which means that the chip will never be able to securely boot again. This effectively bricks the part… the ultimate weapon against hacking.

Table 12.1. Secure Key Storage Reference Documentation

Reference	Title and Web Link
AN1271	Secure Key Storage (Link)

To wrap an externally generated key:

1. After power-on, the device's unique root key is reconstructed with output from the Physically Unclonable Function (PUF).
2. A user key is generated and imported into device memory. In this example, the key is imported into RAM for easy deletion, and the added security that, if device power is removed, the key will be lost.
3. The user key is passed to HSE, where it is encrypted with the HSE's root key.
4. The wrapped key is passed back to the user application for storage in non-volatile memory (in this case, device flash).
5. The plain text key can now be deleted from the device. From this point forward, only the HSE will have access to the plaintext key.

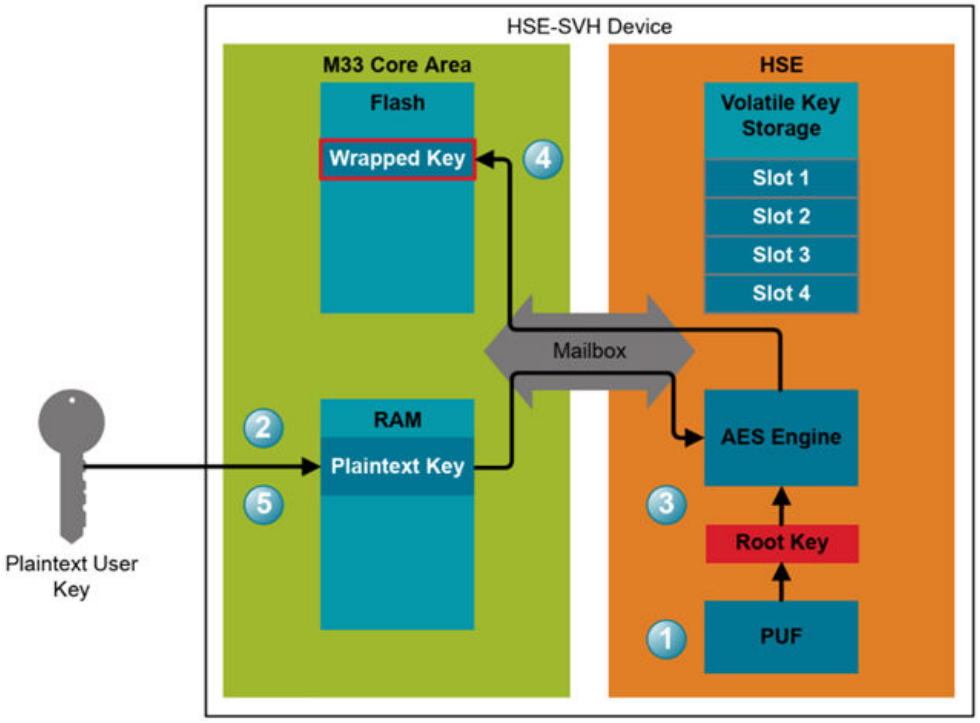


Figure 12.2. External Key Import, Wrapping, and Storage

To generate a new key internally in the SE and store it wrapped:

Instead of importing an external key, the HSE can generate a new key directly into one of its volatile key storage slots. This key can then be exported in wrapped form for secure persistent storage.

1. The user requests that the HSE generates a new key into one of its storage slots using the True Random Number Generator (TRNG).
2. The key is encrypted with the HSE's root key.
3. The wrapped key is passed back to the user application for non-volatile storage (flash, in this case).

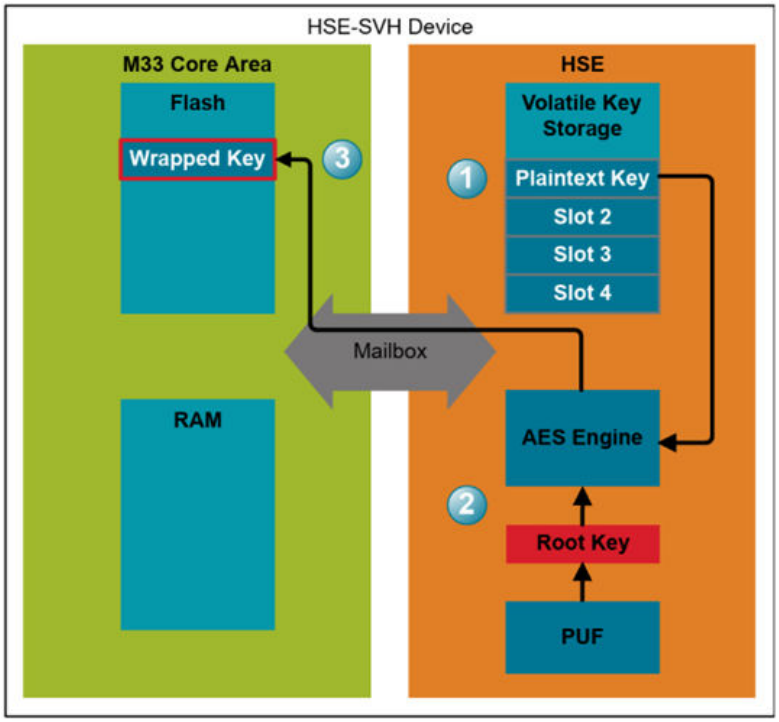


Figure 12.3. Internally Generated Key Wrapping and Storage

To import a wrapped key for use in the Hardware Secure Engine (HSE):

1. The wrapped key is passed to the HSE.
2. The wrapped key is decrypted ("unwrapped") with the HSE's root key.
3. The plaintext key is stored in a volatile key storage slot.

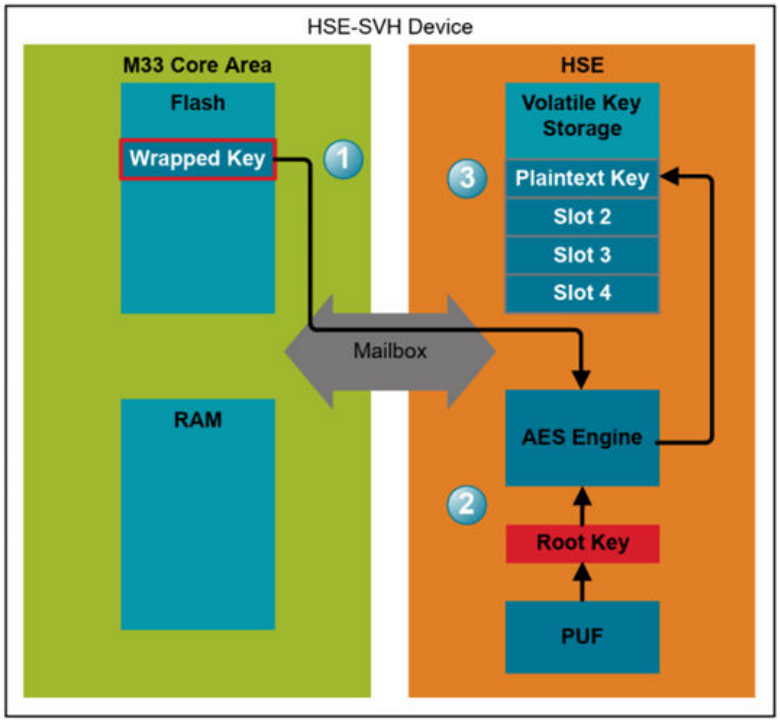


Figure 12.4. Wrapped Key Import

12.2 Using SE Keys to Store Binary Data with Integrity and Confidentiality

Symmetric cryptographic operations that provide both confidentiality and integrity are known as Authenticated Encryption with Associated Data (AEAD) operations. Using the PSA Crypto API and Silicon Labs SiSDK, the following symmetric algorithms achieve both confidentiality (encryption) and integrity (authentication):

- AES-GCM (Galois/Counter Mode)
- AES-CCM (Counter with CBC-MAC)
- CHACHA20-POLY1305

These AEAD algorithms encrypt the data (providing confidentiality) and generate an authentication tag (providing integrity and authenticity). The tag ensures that any modification to the ciphertext or associated data can be detected during decryption.

Table 12.2. Reference documentation on PSA Crypto APIs and Secure Key Storage

Reference	Title and Web link
AN1271	Secure Key Storage (Link)
Docs.silabs.com	PSA Crypto in the Simplicity SDK (Link)
Docs.silabs.com	PSA Crypto Extensions (Link)
AN1311	Integrated Crypto Functionality Using PSA Crypto Compared to Mbed TLS (Link)

To use the key for a cryptographic operation, the same steps are followed:

1. The user passes data to be processed (in this specific example, AES encrypted data) to the HSE.
2. The user requests that a cryptographic operation be performed on this data using one of the keys stored in the HSE volatile key storage slots. Alternatively, the wrapped key can be passed to the HSE directly for a singular cryptographic operation. In this case, the key will be unwrapped before being used but will not be stored for future operations.
3. The HSE performs the cryptographic operation.
4. The output of the cryptographic operation is passed back to the user for processing.

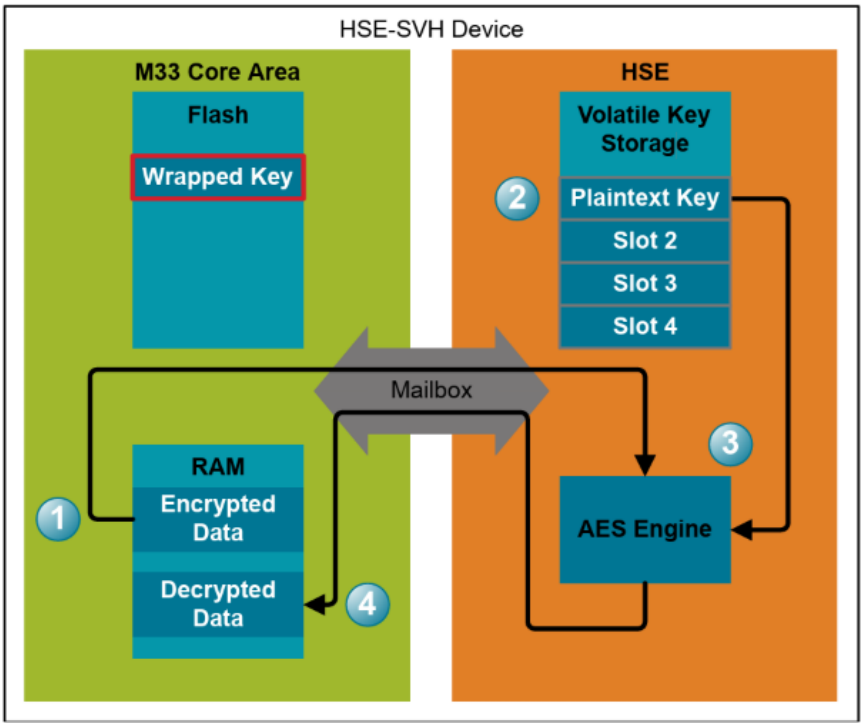


Figure 12.5. Wrapped Key Usage

13. [SCM] – Secure Communication Mechanism (EN 18031 -1, -2, and -3)

Summary of Requirement:

For each communication of security or network asset, a secure communication mechanism must be used. Best practice integrity and authenticity practices must be employed for any security or network asset that is communicated. If confidentiality of the asset is required, then best practices for maintaining confidentiality must be employed. Best practice anti-replay practices shall be employed for communicated assets.

Note: Refer to the EN 18031 standard for details.

13.1 Wireless Communication Protocol Security Provides a Secure Communication and Anti-replay Mechanisms

The communication protocols that are running on the Silicon Labs wireless SoCs have very extensive and sophisticated secure communication mechanisms that are best detailed by the standards for those protocols. For communication stacks running on Series 2 Secure Vault™ High, the persistent keys needed for the protocol are stored in the Secure Engine (SE) wrapped and non-exportable (see the “Secure Vault High Secure Key Storage” section for details). Below are references that are available from Silicon Labs describing the security of various protocols.

Table 13.1. Reference documentation on how Secure Vault works with wireless applications

Reference	Title and Web Link
AN1329	Using Silicon Labs Secure Vault Features with OpenThread (Link)
AN1302	Bluetooth Low Energy Application Security Design Considerations in SDK v3.x and Higher (Link)
INS13474	Z-Wave Security Whitepaper (Link)
AN1233	ZigBee Security (Link)
AN1396	Certificate-Based Bluetooth Authentication and Pairing (Link)

13.2 Encrypting Assets with Authenticated Encryption with Associated Data (AEAD) provides integrity and authenticity

Symmetric cryptographic operations that provide both confidentiality and integrity are known as **Authenticated Encryption with Associated Data (AEAD)** operations. Using the PSA Crypto API and Silicon Labs SiSDK, the following symmetric algorithms achieve both confidentiality (encryption) and integrity (authentication):

- AES-GCM (Galois/Counter Mode)
- AES-CCM (Counter with CBC-MAC)
- CHACHA20-POLY1305

These AEAD algorithms encrypt the data (providing confidentiality) and generate an authentication tag (providing integrity and authenticity). The tag ensures that any modification to the ciphertext or associated data can be detected during decryption.

Table 13.2. Reference documentation on PSA Crypto APIs and Secure Key Storage

Reference	Title and Web link
AN1271	Secure Key Storage (Link)
Docs.silabs.com	PSA Crypto in the Simplicity SDK (Link)
Docs.silabs.com	PSA Crypto Extensions (Link)
AN1311	Integrated Crypto Functionality Using PSA Crypto Compared to Mbed TLS (Link)

14. [LGM] – Logging Mechanism (EN 18031 -2 and -3 Only)

Summary of Requirement:

The equipment shall use logging mechanisms for internal activities (events) that are relevant to privacy assets and their protection. These logged events must be stored in persistent storage, contain a minimum number of events including the latest, and must contain a timestamp when a real time source is available or at least time related information if not.

Note: Refer to the EN 18031 standard for details.

To meet this requirement with Series 2 Secure Vault™ High with Hardware Security Engine (HSE) parts it is recommended to use the Tamper Detection feature (see the “Tamper Detection” section in this user guide) and log those tamper events in permanent storage. There is no hardware calendar mode in Series 2 MCUS. However, depending on the specific Series 2 part the time related sources that can be used are the Real Time Clock Capture (RTCC), the Backup Real Time Counter (BURTC), or the System Real Time Counter (SYSRTC). Please consult the specific reference manual for the exact part number you are using for details.

15. [DLM] – Deletion Mechanism (EN 18031 -2 Only)

Summary of Requirement:

The equipment shall provide a deletion mechanism, for the purpose of disposal or replacement of the equipment, that allows a user or authorized supervisory role to delete (or make permanently unrecoverable) their personal data and sensitive security parameters stored on the equipment.

Note: Refer to the EN 18031 standard for details.

To meet this requirement with Series 2 Secure Vault™ High with Hardware Security Engine (HSE) parts this function can be accomplished by triggering software that erases flash areas where personal and sensitive security parameters are stored. If the personal data or sensitive security parameters have been encrypted using a Secure Engine (SE) key, the SE can be commanded to delete the key via PSA Crypto which renders the data a bunch of useless 1's and 0's.

An extreme measure would be to make all the key material wrapped with the PUF permanently unrecoverable by using the Tamper Detection "Level 7" response (see the "Tamper Detection" section in this User Guide). A "Level 7" tamper response will destroy the PUF reconstruction data which will also permanently disable the PUF and therefore the key wrapping mechanism. If Secure Boot is also enabled, destroying the reconstruction data will also permanently "brick" the equipment as the public keys needed for Secure Boot are wrapped by the PUF and would per permanently unrecoverable.

16. [UNM] – User Notification Mechanism (EN 18031 -2 Only)

Summary of Requirement:

The equipment shall provide a user notification mechanism per use case for informing the user about changes to protection or privacy of personal information. The content of the notification shall include at a minimum the description of the change and how that change will affect the protection and privacy of the user's personal information.

Note: Refer to the EN 18031 standard for details.

This requirement is very specific to the end equipment use and will be met by application code written by the end equipment manufacturer running on the host M33 core of the Series 2 MCUs from Silicon Labs.

17. [RLM] – Resilience Mechanism (EN 18031 -1 Only)

Summary of Requirement:

The equipment shall use resilience mechanisms to mitigate the effects of Denial of Service (DoS) Attacks on the network interfaces that interoperate with other external, more global, untrusted/uncontrolled networks (equipment on trusted local networks are excluded). The equipment should enter a defined state during the DoS attack and return to defined operational state after the DoS attack. The intent is to ensure that equipment continues to function during and after a DoS attack. Some examples of mitigation are: network storm protection, network packet filtering mechanisms, network traffic rate limiting techniques, and strategies involving reservation of equipment internal resources to limit use of resources and protect against exhaustion.

Note: Refer to the EN 18031 standard for details.

This requirement is very specific to the end equipment use and will be met by application code written by the end equipment manufacturer running on the host M33 core of the Series 2 MCUs from Silicon Labs. The security feature for Series 2 Secure Vault™ High with HSE that might be applied here is the Secure Boot with RTSL (see the “Secure Boot with Root of Trust Secure Loader” section in this User Guide) which can be triggered by application forcing a Power-On Reset (POR) after a DoS attack to put the MCU back into a good known state.

18. [NMM] – Network Monitoring Mechanism (EN 18031 -1 Only)

Summary of Requirement:

If the equipment is network equipment as defined below, the equipment shall provide network monitoring mechanism(s) to detect unusual traffic patterns (i.e. datagram monitoring techniques) which could be related to Denial of Service (DoS) attacks in the network traffic it processes.

Note: Refer to the EN 18031 standard for details.

Network Equipment

Equipment that exchanges data between different networks used to permanently connect directly other devices to the internet.

This requirement is very specific to the end equipment which is likely to be a gateway or boarder router of some type that might use a Series 2 Silicon Labs MCU in a Network Co-Processor (NCP) or Radio Co-Processor (RCP) mode. In these types of devices, there is likely a Microprocessor (MPU) running Linux that would perform this task. Therefore, there is no security feature in a Series 2 MCU that is applicable to meet this requirement.

19. [TCM] – Traffic Control Mechanism (EN 18031 -1 Only)

Summary of Requirement:

If the equipment is network equipment as defined below, the equipment shall provide network traffic control mechanism(s) to protect against anomalous network traffic. Examples of implementation categories of these traffic control mechanisms are based on monitoring the IP datagrams for anomalous patterns and malicious traffic or on full physical or logical separation of traffic belonging to network domains.

Note: Refer to the EN 18031 standard for details.

Network Equipment

Equipment that exchanges data between different networks used to permanently connect directly other devices to the internet.

This requirement is very specific to the equipment which is likely to be a gateway or boarder router of some type that might use a Series 2 Silicon Labs MCU in a Network Co-Processor (NCP) or Radio Co-Processor (RCP) mode. In these types of devices, there is likely a Microprocessor (MPU) running Linux that would perform this task. Therefore, there is no security feature in a Series 2 MCU that is applicable to meet this requirement.

20. [CCK] – Confidential Cryptographic Keys (EN 18031 -1 Only)

Summary of Requirement:

1. Confidential Cryptographic Keys (CCKs) that are preinstalled or generated by the equipment shall support a minimum-security strength of 112 bits.
2. The generation of CCKs (preinstalled or generated by the equipment) shall adhere to best practice cryptography and must show evidence that they comply with those best practices.
3. Any pre-installed CCK must be proven practically to be unique per piece of equipment.

Note: Refer to the EN 18031 standard for details.

The following table lists the ECC Curves and AES Symmetric Key Size for the Series 2 Secure Vault™ High (SVH) with Hardware Security Engine (HSE). If these are used in the generation of keys except for P-192, the CCK strength will meet the minimum requirement of having a minimum security strength of 112 bits.

There are two Private keys on the Series 2 SVH HSE MCUs that are created by Silicon Labs during manufacture. One is the Host (CM33) Attestation Key and the other is the Secure Engine (SE) Attestation Key. Both of these keys are created by using the TRNG output directly with whitening, and both are 256 bit keys (used on the P-256 curve) which assures a bit strength of 256 bits.

Table 20.1. Key Strengths of Series 2 Secure Vault™ High Parts

ECC Curve Name	Field Size (bits)	Approx. Security Strength (bits)	Notes
NIST P-192 (SECP192R1)	192	96	Deprecated
NIST P-224 (SECP224R1)	224	112	Minimum NIST-approved
NIST P-256 (SECP256R1)	256	128	Widely used (TLS, FIPS)
NIST P-384 (SECP384R1)	384	192	Higher security
NIST P-521 (SECP521R1)	521	256	Maximum standardized
EdDSA (Curve25519)	255	~128	Efficient, modern default
EdDSA (Curve448)	448	~224	High-security alternative

Table 20.2. Symmetric Keys and their respective strength (bits)

Symmetric Key	Security Strength (bits)
AES-128	128
AES-192	192
AES-256	256

All Series 2 SVH HSE parts use a True Random Number Generator (TRNG) which meets the definition of “random number source” generation mechanism per EN 18031. Each major revision of the TRNG is tested per NIST test suites to comply with the NIST SP800-90(B) using the NIST Cryptographic Module Validation Program (CMVP)– Entropy Validation Submission Guidelines. This TRNG can then be used as a salt value for either SE or PSA Crypto Key Derivation functions.

Table 20.3. Reference documentation on PSA Crypto APIs, SE Manager, and Cryptographic Module Validation Program Entropy Validation

Reference	Title and Web Link
Docs.silabs.com	PSA Crypto in the Simplicity SDK (Link)
Docs.silabs.com	PSA Crypto Extensions (Link)
Docs.silabs.com	SE Manager Key Derivation (Link)

Reference	Title and Web Link
Docs.silabs.com	SE Manager Key Handling/Generation (Link)
AN1311	Integrated Crypto Functionality Using PSA Crypto Compared to Mbed TLS (Link)
NIST CMVP	Cryptographic Module Validation Program Entropy Validation (Link)

21. [GEC] – General Equipment Capabilities (EN 18031 -1, -2, and -3)

Summary of Requirement:

1. **Equipment shall not include "publicly known exploitable vulnerabilities" that if exploited, affect security and network assets EXCEPT for vulnerabilities that cannot be exploited due to specific conditions of the equipment, have been mitigated to an acceptable residual risk, or have been accepted on a risk basis.**

   Note: Refer to the EN 18031 standard for details.

   To assist in meeting the NO known vulnerabilities requirement, Silicon Labs is a Common Vulnerabilities and Exposures (CVE) Numbering Authority (CAN) with CVE.org which is a broadly known Vulnerability Reporting Agency backed by the U.S. Department of Homeland Security. The CVE.org database directly feeds the National Vulnerability Database (NVD) maintained by the U.S. National Institute of Standards and Technology (NIST). The NVD offers enhanced information, such as patch availability and Common Vulnerability Scoring System (CVSS) scores and is considered a better search tool. The CVSS scoring system was developed by FIRST.org and is an open framework for communicating the characteristics and severity of security vulnerabilities.

   Silicon Labs also has a public vulnerability reporting program to get advance notice of security vulnerabilities. Also, anyone with a Silicon Labs account can sign up to receive Security Advisory reports. You must opt into receiving the Security Advisories due to GDPR regulations. Silicon Labs has a dedicated Product Security Incident Response Team (PSIRT) to assess all reported vulnerabilities (internal or external), assign CVSS scores, assign number an log with cve.org, and issue Security Advisories. To encourage ethical hackers to find vulnerabilities with our products, Silicon Labs has partnered with HackerOne's to offer a Bug Bounty program.

Table 21.1. Security Vulnerability databases and Silicon Labs' Secure Vulnerability Management Processes

Reference	Title and Web Link
www.cve.org	CVE Vulnerability Search (Link)
nvd.nist.gov	NIST National Vulnerability Database Search (Link)
www.first.org	CVSS Scoring System (Link)
www.silabs.com/security	Security Vulnerability Reporting Page (Link)
www.silabs.com/security	How to sign up for Silicon Labs Security Advisories (Link)
www.silabs.com/security	Silicon Labs Security Vulnerability Disclosure Policy (Link)

2. In the factory default state, the equipment shall only expose network interfaces and/or network services that affect security/network assets, if they are "required" for equipment setup or operation.

   Note: Refer to the EN 18031 standard for details.

   This requirement is very specific to the end equipment use and will be met by application code written by the end equipment manufacturer running on the host M33 core of the Series 2 MCUs from Silicon Labs.

3. If there are other network interfaces and/or network services that are "optional" in the equipment factory default state that affect security/network assets, then an "authorized (protected according to [ACM] and [AUM] mechanisms), should have the option to enable/disable that optional network interface and/or network service.

   Note: Refer to the EN 18031 standard for details.

   This requirement is very specific to the end equipment use and will be met by application code written by the end equipment manufacturer running on the host M33 core of the Series 2 MCUs from Silicon Labs. Please refer to the [ACM] Access Control Mechanism and [AUM] Authentication Mechanism sections of this User Guide for any relevant Silicon Labs security features that might apply in meeting this requirement.

4. For each network interface and/or network service, that is delivered as part of the factory default state, it must be described in the user documentation.

   Note: Refer to the EN 18031 standard for details.

   This requirement is very specific to the end equipment as well as the documentation.

5. Equipment shall only expose “physical” external interfaces if they are necessary for intended functionality.

   Note: Refer to the EN 18031 standard for details.

   The primary interface that might be relevant for this requirement in a Series 2 Secure Vault™ High with HSE MCU is the debug port. It is recommended to always put the debug port in the “Secure Lock” or “Permanent Lock” state at the earliest possible moment during manufacture. Refer to Secure Debug section of this user guide for details on these two debug states.

6. The equipment shall “validate” input received via an “external” interface if the input has the potential to “impact” security/network assets.

   Note: Refer to the EN 18031 standard for details.

   This requirement is very specific to the end equipment use and will be met by application code written by the end equipment manufacturer running on the host M33 core of the Series 2 MCUs from Silicon Labs.

22. [CRY] – Cryptography (EN 18031 -1, -2, and -3)

Summary of Requirement:

The equipment shall use “best practice” for cryptography used for protection of security/network assets except where an exception was taken in other requirements.

Note: Refer to the EN 18031 standard for details.

Silicon Labs Series 2 MCUs offer NIST Federal Information Processing Standards (FIPS) approved and NIST recommended cryptographic algorithms that are validated via the NIST Cryptographic Algorithm Validation Program (CAVP) testing program. Also, Silicon Labs offers other cryptographic algorithms that are used and approved by various wireless protocol standards such as ChaCha20 which is used by Transport Layer Security (TLS 1.3). For a complete list of algorithms supported by your Series 2 Secure Vault™ High HSE MCU, refer to the Reference Manual for your part number.

Table 22.1. Understanding Cryptographic Algorithm Validation Program, list of Silicon Labs' certifications, and supporting documentation on relevant APIs

Reference	Title and Web Link
csrc.nist.gov	Cryptographic Algorithm Validation Program (Link)
csr.nist.gov	List of Silicon Labs CAVP Certifications (Link)
Docs.silabs.com	Security API Documentation (Link)
Docs.silabs.com	PSA Crypto in the Simplicity SDK (Link)
Docs.silabs.com	PSA Crypto Extensions (Link)
Docs.silabs.com	SE Manager Key Derivation (Link)
Docs.silabs.com	SE Manager Key Handling/Generation (Link)
AN1311	Integrated Crypto Functionality Using PSA Crypto Compared to Mbed TLS (Link)

23. Appendix

EN 18031 Mapping for Additional Devices

This document was originally written to address the mapping of existing Series 2 SVH features to the EN 18031 specification. This appendix adds additional reference mapping of the security features available on Series 2 SVM, Series 3, Series 1, SiWx917, and RS9116 to the security mechanisms defined in EN 18031.

Because the supported features differ across devices, some mechanisms may be fully implemented in hardware or platform services while others must be addressed through application firmware and final product design. This appendix is intended only as a high-level mapping; detailed technical guidance should be obtained from the documentation linked in each section. Refer to previous sections of this document for additional explanation on the requirement summary for each security mechanism.

23.1 Series 2 Secure Vault Mid (HSE and VSE) Mapping to EN 18031

The Series 2 Secure Vault™ Mid with Hardware Secure Engine (HSE) and Virtual Secure Engine (VSE) devices have many security features, services, and processes that are applicable in meeting the required security mechanisms. Please see table below for details:

Table 23.1. EN 18031 Requirement Mapping to Silicon Labs Series 2 SVM Security Features, Services, and Processes

Security Mechanism	Requirement Summary	Applicable Silabs Series 2 Secure Vault ™ Mid (HSE) Security Features/Services/Processes		Applicable Silabs Series 2 Secure Vault ™ Mid (VSE) Security Features/Services/Processes		-1	-2	-3
[ACM] Access Control	Access control of security/network assets	Applicable	Secure Debug (AN1190), Secure Engine (SE) Mailbox[1], Custom Identities w/ Custom Part Manufacturing Services (CPMS)	Applicable	Secure Debug (AN1190), Custom Identities w/ Custom Part Manufacturing Services (CPMS)	Applicable	Applicable	Applicable
[AUM] Authentication	Entity is what/who it claims to be	Applicable	Custom Identities w/ CPMS	Applicable	Custom Identities w/ CPMS	Applicable	Applicable	Applicable
[SUM] Secure Update	Patches can be installed securely	Applicable	Secure Boot with Root of Trust Secure Loader (RTSL) (AN1218), Secure Firmware Upgrades (UG489)	Applicable	Secure Boot with Root of Trust Secure Loader (RTSL) (AN1218), Secure Firmware Upgrades (UG489)	Applicable	Applicable	Applicable
[SSM] Secure Storage	Secure stored assets	Applicable	Cryptography (AN1311), TrustZone for Key Management (AN1374)	Applicable	Cryptography (AN1311), TrustZone for Key Management (AN1374)	Applicable	Applicable	Applicable
[SCM] Secure Communication	Securely communicate assets	Applicable	Cryptography (AN1311), Protocol Security	Applicable	Cryptography (AN1311), Protocol Security	Applicable	Applicable	Applicable
[LGM] Logging	Log events relevant to assets	None Applicable	Depends on final product design[1]	Not Applicable	Depends on final product design[1]	Not Applicable	Applicable	Applicable
[DLM] Deletion	Delete assets	None Applicable	Depends on final product design[1]	Not Applicable	Depends on final product design[1]	Not Applicable	Applicable	Not Applicable
[UNM] User Notification	Notify user of changes of assets	None Applicable	Depends on final product design[1]	Not Applicable	Depends on final product design[1]	Not Applicable	Applicable	Not Applicable

Security Mechanism	Requirement Summary	Applicable Silabs Series 2 Secure Vault ™ Mid (HSE) Security Features/Services/Processes		Applicable Silabs Series 2 Secure Vault ™ Mid (VSE) Security Features/Services/Processes		-1	-2	-3
[RLM] Resilience	Mitigate Denial of Service (DOS) attacks	Applicable	Secure Boot with Root of Trust Secure Loader (RTSL) (AN1218), Watchdog Timer	Applicable	Secure Boot with Root of Trust Secure Loader (RTSL) (AN1218), Watchdog Timer	Applicable	Not Applicable	Not Applicable
[NMM] Network Monitoring	Detect DOS and defend	None Applicable	Depends on final product design[1]	Not Applicable	Depends on final product design[1]	Applicable	Not Applicable	Not Applicable
[TCM] Traffic Control	Detect malicious comms traffic	None Applicable	Depends on final product design[1]	Not Applicable	Depends on final product design[1]	Applicable	Not Applicable	Not Applicable
[CCK] Cryptographic Keys	Guidance on key size, generation, and use	Applicable	TRNG, Cryptography (AN1311), PUF	Applicable	TRNG, Cryptography (AN1311), PUF (xG27 only)	Applicable	Not Applicable	Not Applicable
[GEC] General Equipment Capabilities	Up-to-date software and hardware with no known “exploitable” vulnerabilities, no unnecessary external interfaces	Applicable	Product Security Incident Reporting Process (PSIRP), Secure Debug (AN1190), Depends on final product design[1]	Applicable	Product Security Incident Reporting Process (PSIRP), Secure Debug (AN1190), Depends on final product design[1]	Applicable	Applicable	Applicable
[CRY] Cryptography	Shall use for Secure Update, Secure Storage, Secure Comms	Applicable	Cryptography (AN1311)	Applicable	Cryptography (AN1311)	Applicable	Applicable	Applicable

Note:

1. While no built-in security features exist to meet this requirement, application firmware can be written to address this requirement.

23.2 Series 3 (SixG301) Mapping to EN 18031

The Series 3 SixG301 Secure Vault™ High with Hardware Secure Engine (HSE) has many security features, services, and processes that are applicable in meeting the required security mechanisms. Please see table below for details:

Table 23.2. EN 18031 Requirement Mapping to Silicon Labs Series 3 (SixG301) Security Features, Services, and Processes

Security Mechanism	Requirement Summary	Applicable Silabs Series 3 (SixG301) Secure Vault ™ High (HSE) Security Features/Services/Processes		-1	-2	-3
[ACM] Access Control	Access control of security/network assets	Applicable	Secure Debug (AN1190), Secure Engine (SE) Mailbox[1], Secure Key Storage (AN1271), Authenticated Execute in Place (AXiP) (AN1509), Default Silicon Identities (AN1268), Custom Identities w/ Custom Part Manufacturing Services (CPMS)	Applicable	Applicable	Applicable
[AUM] Authentication	Entity is what/who it claims to be	Applicable	Custom Identities w/ CPMS	Applicable	Applicable	Applicable
[SUM] Secure Update	Patches can be installed securely	Applicable	Secure Boot with Root of Trust Secure Loader (RTSL) (AN1218), Secure Firmware Upgrades (UG489)	Applicable	Applicable	Applicable
[SSM] Secure Storage	Secure stored assets	Applicable	Secure Key Storage (AN1271), Cryptography (AN1311)	Applicable	Applicable	Applicable
[SCM] Secure Communication	Securely communicate assets	Applicable	Cryptography (AN1311), Protocol Security	Applicable	Applicable	Applicable
[LGM] Logging	Log events relevant to assets	Applicable	Tamper Detection (AN1247)	Not Applicable	Applicable	Applicable
[DLM] Deletion	Delete assets	Applicable	Tamper Detection (AN1247) - Deletion of secure keys and other assets	Not Applicable	Applicable	Not Applicable
[UNM] User Notification	Notify user of changes of assets	None Applicable	Depends on final product design	Not Applicable	Applicable	Not Applicable

Security Mechanism	Requirement Summary	Applicable Silabs Series 3 (SixG301) Secure Vault ™ High (HSE) Security Features/Services/Processes		-1	-2	-3
[RLM] Resilience	Mitigate Denial of Service (DOS) attacks	Applicable	Secure Boot with Root of Trust Secure Loader (RTSL) (AN1218), Watchdog Timer	Applicable	Not Applicable	Not Applicable
[NMM] Network Monitoring	Detect DOS and defend	None Applicable	Depends on final product design[2]	Applicable	Not Applicable	Not Applicable
[TCM] Traffic Control	Detect malicious comms traffic	None Applicable	Depends on final product design[2]	Applicable	Not Applicable	Not Applicable
[CCK] Cryptographic Keys	Guidance on key size, generation, and use	Applicable	TRNG, Cryptography (AN1311), PUF	Applicable	Not Applicable	Not Applicable
[GEC] General Equipment Capabilities	Up-to-date software and hardware with no known “exploitable” vulnerabilities, no unnecessary external interfaces	Applicable	Product Security Incident Reporting Process (PSIRP), Secure Debug (AN1190), Depends on final product design[2]	Applicable	Applicable	Applicable
[CRY] Cryptography	Shall use for Secure Update, Secure Storage, Secure Comms	Applicable	Cryptography (AN1311), AXiP/EXiP (AN1509)	Applicable	Applicable	Applicable

Note:

1. Refer to the device specific reference manuals for additional information.
2. While no built-in security features exist to meet this requirement, application firmware can be written to address this requirement.

23.3 SiWx917 Mapping to EN 18031

The Silicon Labs SiWx917 has many security features, services, and processes that are applicable in meeting the required security mechanisms. Please see table below for details:

Table 23.3. EN 18031 Requirement Mapping to Silicon Labs SiWx917 Security Features, Services, and Processes

Security Mechanism	Requirement Summary	Applicable Silicon Labs SiWx917 Security Features/Services/Processes		-1	-2	-3
[ACM] Access Control	Access control of security/network assets	Applicable	Debug Lock (AN1428), Encrypted Execute in Place (EXiP) (AN1443)	Applicable	Applicable	Applicable
[AUM] Authentication	Entity is what/who it claims to be	Applicable	PSA Attestation	Applicable	Applicable	Applicable
[SUM] Secure Update	Patches can be installed securely	Applicable	Secure Boot (AN1442), Secure Firmware Upgrades (AN1431, AN1435)	Applicable	Applicable	Applicable
[SSM] Secure Storage	Secure stored assets	Applicable	Key Storage, Cryptography[1]	Applicable	Applicable	Applicable
[SCM] Secure Communication	Securely communicate assets	Applicable	Cryptography[1] , Protocol Security	Applicable	Applicable	Applicable
[LGM] Logging	Log events relevant to assets	Not Applicable	Depends on final product design[2]	Not Applicable	Applicable	Applicable
[DLM] Deletion	Delete assets	Not Applicable	Depends on final product design[2]	Not Applicable	Applicable	Not Applicable
[UNM] User Notification	Notify user of changes of assets	Not Applicable	Depends on final product design[2]	Not Applicable	Applicable	Not Applicable
[RLM] Resilience	Mitigate Denial of Service (DOS) attacks	Applicable	Secure Boot (AN1442), Watchdog Timer	Applicable	Not Applicable	Not Applicable
[NMM] Network Monitoring	Detect DOS and defend	Not Applicable	Depends on final product design[2]	Applicable	Not Applicable	Not Applicable
[TCM] Traffic Control	Detect malicious comms traffic	Not Applicable	Depends on final product design[2]	Applicable	Not Applicable	Not Applicable
[CCK] Cryptographic Keys	Guidance on key size, generation, and use	Applicable	TRNG, PUF, Cryptography[1]	Applicable	Not Applicable	Not Applicable
[GEC] General Equipment Capabilities	Up-to-date software and hardware with no known “exploitable” vulnerabilities, no unnecessary external interfaces	Applicable	Product Security Incident Reporting Process (PSIRP), Debug Lock (AN1428), Depends on final product design[2]	Applicable	Applicable	Applicable

Security Mechanism	Requirement Summary	Applicable Silicon Labs SiWx917 Security Features/Services/Processes		-1	-2	-3
[CRY] Cryptography	Shall use for Secure Update, Secure Storage, Secure Comms	Applicable	Cryptography[1]	Applicable	Applicable	Applicable

Note:

1. Refer to the device specific data sheets and reference manuals for additional information.
2. While no built-in security features exist to meet this requirement, application firmware can be written to address this requirement.

23.4 Series 1 Mapping to EN 18031

While Series 1 devices have certain features and processes that may be applicable in meeting the required security mechanisms, many of the security mechanisms listed in EN 18031 will need to be addressed via application firmware and will depend on final product design. Please see table below for details. Refer to the linked references for additional technical details.

Table 23.4. EN 18031 Requirement Mapping to Silicon Labs Series 1 Security Features, Services, and Processes

Security Mechanism	Requirement Summary	Applicable Silicon Labs Series 1 Security Features/Services/Processes		-1	-2	-3
[ACM] Access Control	Access control of security/network assets	Applicable	Standard Debug Lock[1]	Applicable	Applicable	Applicable
[AUM] Authentication	Entity is what/who it claims to be	None Applicable	Depends on final product design[2]	Applicable	Applicable	Applicable
[SUM] Secure Update	Patches can be installed securely	Applicable	Secure Application Boot (UG103.6, UG489 Section 9)	Applicable	Applicable	Applicable
[SSM] Secure Storage	Secure stored assets	Applicable	Cryptography (AN0955)	Applicable	Applicable	Applicable
SCM] Secure Communication	Securely communicate assets	Applicable	Cryptography (AN0955), Protocol Security	Applicable	Applicable	Applicable
[LGM] Logging	Log events relevant to assets	None Applicable	Depends on final product design[2]	Not Applicable	Applicable	Applicable
[DLM] Deletion	Delete assets	None Applicable	Depends on final product design[2]	Not Applicable	Applicable	Not Applicable
[UNM] User Notification	Notify user of changes of assets	None Applicable	Depends on final product design[2]	Not Applicable	Applicable	Not Applicable
[RLM] Resilience	Mitigate Denial of Service (DOS) attacks	Applicable	Secure Application Boot (UG103.6, UG489 Section 9), Watchdog Timer	Applicable	Not Applicable	Not Applicable
[NMM] Network Monitoring	Detect DOS and defend	None Applicable	Depends on final product design[2]	Applicable	Not Applicable	Not Applicable
[TCM] Traffic Control	Detect malicious comms traffic	None Applicable	Depends on final product design[2]	Applicable	Not Applicable	Not Applicable
[CCK] Cryptographic Keys	Guidance on key size, generation, and use	Applicable	TRNG[1], Cryptography (AN0955)	Applicable	Not Applicable	Not Applicable
[GEC] General Equipment Capabilities	Up-to-date software and hardware with no known “exploitable” vulnerabilities, no unnecessary external interfaces	Applicable	Product Security Incident Reporting Process (PSIRP), Depends on final product design[2]	Applicable	Applicable	Applicable

Security Mechanism	Requirement Summary	Applicable Silicon Labs Series 1 Security Features/Services/Processes		-1	-2	-3
[CRY] Cryptography	Shall use for Secure Update, Secure Storage, Secure Comms	Applicable	Cryptography (AN0955)	Applicable	Applicable	Applicable

Note:

1. Refer to the device specific reference manual for additional details.
2. While no built-in security features exist to meet this requirement, application firmware can be written to address this requirement.

23.5 RS9116 Mapping to EN 18031

While RS9116 devices have certain features and processes that may be applicable in meeting the required security mechanisms, many of the security mechanisms listed in EN 18031 will need to be addressed via application firmware and will depend on final product design. Please see table below for details. Refer to the linked references for additional technical details.

Table 23.5. EN 18031 Requirement Mapping to Silicon Labs RS9116 Security Features, Services, and Processes

Security Mechanism	Requirement Summary	Applicable Silicon Labs RS9116 Security Features/Services/Processes		-1	-2	-3
[ACM] Access Control	Access control of security/network assets	None Applicable	Depends on final product design[1]	Applicable	Applicable	Applicable
[AUM] Authentication	Entity is what/who it claims to be	None Applicable	Depends on final product design[1]	Applicable	Applicable	Applicable
[SUM] Secure Update	Patches can be installed securely	None Applicable	Depends on final product design[1]	Applicable	Applicable	Applicable
[SSM] Secure Storage	Secure stored assets	Applicable	Cryptography	Applicable	Applicable	Applicable
SCM] Secure Communication	Securely communicate assets	Applicable	Cryptography, Protocol Security	Applicable	Applicable	Applicable
[LGM] Logging	Log events relevant to assets	None Applicable	Depends on final product design[1]	Not Applicable	Applicable	Applicable
[DLM] Deletion	Delete assets	None Applicable	Depends on final product design[1]	Not Applicable	Applicable	Not Applicable
[UNM] User Notification	Notify user of changes of assets	None Applicable	Depends on final product design[1]	Not Applicable	Applicable	Not Applicable
[RLM] Resilience	Mitigate Denial of Service (DOS) attacks	None Applicable	Depends on final product design[1], Watchdog Timer	Applicable	Not Applicable	Not Applicable
[NMM] Network Monitoring	Detect DOS and defend	None Applicable	Depends on final product design[1]	Applicable	Not Applicable	Not Applicable
[TCM] Traffic Control	Detect malicious comms traffic	None Applicable	Depends on final product design[1]	Applicable	Not Applicable	Not Applicable
[CCK] Cryptographic Keys	Guidance on key size, generation, and use	Applicable	TRNG, Cryptography	Applicable	Not Applicable	Not Applicable
[GEC] General Equipment Capabilities	Up-to-date software and hardware with no known “exploitable” vulnerabilities, no unnecessary external interfaces	Applicable	Product Security Incident Reporting Process (PSIRP), Depends on final product design[1]	Applicable	Applicable	Applicable

Security Mechanism	Requirement Summary	Applicable Silicon Labs RS9116 Security Features/Services/Processes		-1	-2	-3
[CRY] Cryptography	Shall use for Secure Update, Secure Storage, Secure Comms	Applicable	Cryptography	Applicable	Applicable	Applicable

Note:

1. While no built-in security features exist to meet this requirement, application firmware can be written to address this requirement.

24. Revision History

Revision 0.2

January, 2026

- Minor edits to Series 2 HSE Secure Vault High Mapping Table
- Minor typographical changes throughout the document
- Fixed Section headings for [GEC] and [CRY]
- Added Appendix and mappings for:
  - Series 2 Hardware Secure Engine - Secure Vault Mid
  - Series 2 Virtual Secure Engine - Secure Vault Mid
  - Series 3 Secure Vault (SixG301)
  - Series 1
  - SiWx917
  - RS9116

Revision 0.1

August, 2025

- Initial Release

Simplicity Studio

One-click access to MCU and wireless tools, documentation, software, source code libraries & more. Available for Windows, Mac and Linux!

IoT Portfolio
www.silabs.com/IoT

SW/HW
www.silabs.com/simplicity

Quality
www.silabs.com/quality

Support & Community
www.silabs.com/community

SILICON LABS

Silicon Laboratories Inc.
400 West Cesar Chavez
Austin, TX 78701
USA

www.silabs.com