Presentation Will Begin Shortly

4:00

SILICON LABS

CONNECTED INTELLIGENCE

Radio Equipment Directive, Silicon Labs' Strategy, and more!

Rohit Ravichandran

Product Manager, Security

August 2025

Agenda

- RED Legislative and EN18031-1/2/3 Requirements
- RED Timeline
- Why does RED Compliance matter?
- Manufacturer’s Responsibility
- RED Compliance Process
- How to assess the security needs for your assets?
- How does Series 2 Secure Vault High security address EN18031 requirements?
- Silabs RED Collateral
- Secure Vault: Recognized by Industry Leaders
- Questions and next steps

RED Legislative and EN18031-1/2/3 Requirements

2014 DIRECTIVE 53 – ARTICLE 3(3)

- (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**;

OCT 29, 2021 – SUPPLEMENT TO 2014 DIRECTIVE 53

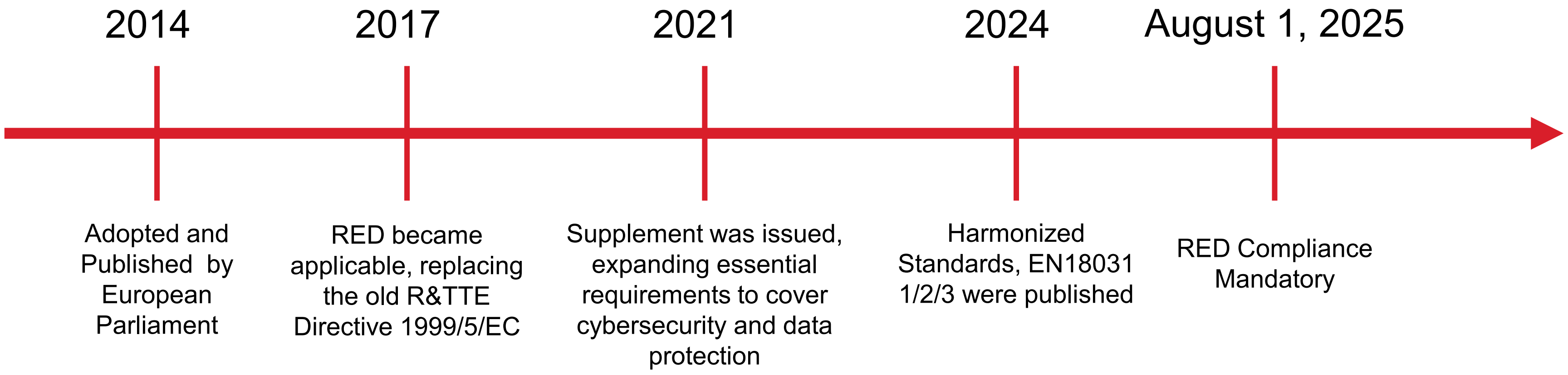
- Deadline set for **August 1st, 2025 – in effect for all new devices put on the market after this date, products placed on the market *before* this date can continue to be used until the end of their lifecycle**
- (d), (e), and (f) is the overarching legislative, while EN18031-1/2/3 are the “harmonized standards”
- In-Scope: Applies **only to** devices that can communicate over the internet or can be seen by the internet – Wi-Fi and Thread.
- **Exception**: childcare, toys, and wearables are in scope even if connected to a gateway *(i.e. Zigbee, Z-Wave, Proprietary)*

=>

HARMONIZED STANDARDS - EN 18031-1/2/3

- ETSI then published detailed requirements called “Harmonized Standards” for specific device types.
- **EN 18031-1:2024 -** Applies to **internet-connected radio equipment**
- **EN 18031-2:2024 -** Applies to equipment **that process personal data**
- **EN 18031-3:2024 -** Applies to equipment **enabling financial transactions**

RED Timeline



2014

Adopted and Published by European Parliament

2017

RED became applicable, replacing the old R&TTE Directive 1999/5/EC

2021

Supplement was issued, expanding essential requirements to cover cybersecurity and data protection

2024

Harmonized Standards, EN18031 1/2/3 were published

August 1, 2025

RED Compliance Mandatory

Why does RED Compliance matter?

- **It's Legally Mandatory**
  - From **August 1, 2025**, all new internet-connected radio equipment sold in the EU must comply with RED Articles 3(3)(d), (e), and (f).
  - Non-compliance means **products cannot legally be placed on the EU market**.
- **Avoids Market Access and Business Risks**
  - The EU market is huge - losing access can mean **millions in lost revenue**.
  - Non-compliance exposes manufacturers to **fines, liability claims, and reputational damage**.
- **Protects Consumers**
  - Compliance builds **trust with customers** (your device won't expose them to data theft or denial-of-service attacks).
- **Competitive Differentiator**
  - Demonstrates **security leadership** vs. competitors who scramble at the last minute.

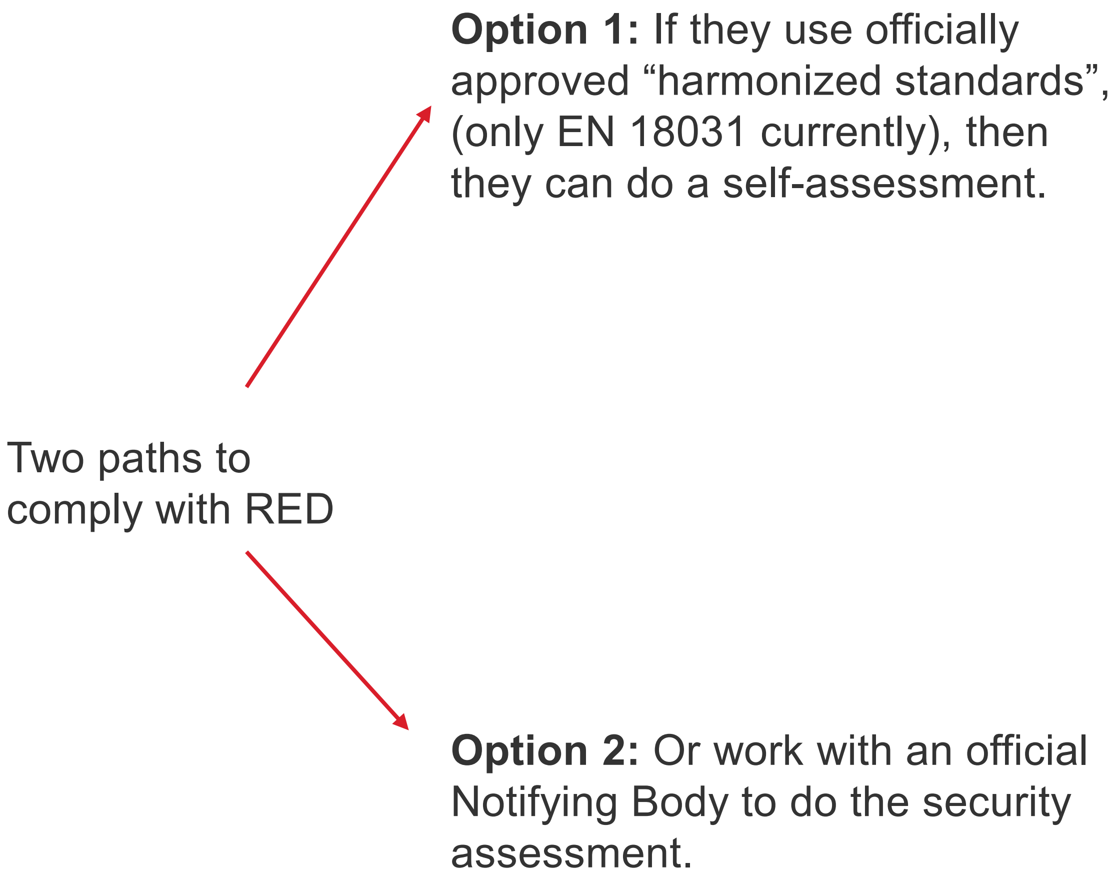
Image Credits: flaticon.com

Manufacturer’s Responsibility

- Final Responsibility Lies with the Manufacturer
- Mandatory Compliance from August 1, 2025
- Security by Design Required
- Risk Assessment & Documentation
- Updated EU Declaration & Quality Systems

Image Credits: flaticon.com

RED Compliance Process



Two paths to comply with RED

Option 1: If they use officially approved “harmonized standards”, (only EN 18031 currently), then they can do a self-assessment.

Option 2: Or work with an official Notifying Body to do the security assessment.

Three scenario **exceptions** that require a Notifying Body evaluation even if EN 18031 is followed:

1. If a product requires a password for access, but **if users can choose not to set a password**.
2. Standard EN 18031-2 outlines four **access control mechanisms for toys and childcare products,** some of which may **not be compatible with parental or guardian controls**.
3. Standard EN 18031-3 (section 6.3.2.4) describes four implementations for **secure update mechanisms**: digital signatures, secure communication, access control, and others. None of these methods alone is sufficient for handling **financial assets**.

How to assess the security needs for your assets?

- Identify What Needs Protection
- Conduct Threat Modeling & Risk Analysis
- Apply Appropriate Security Mechanisms
- Use a Decision Framework
- Ensure “Right-Sized” Security

Image Credits: flaticon.com

How does Series 2 Secure Vault High security address EN18031 requirements?

APPROVED REQUIREMENTS AS OF JANUARY 28, 2025

Security Mechanism	EN18031 Requirement	Silabs Security Features/Services/Processes	EN 18031		
			1	2	3
Access control	access control of security/network assets	Secure Vault API, Secure Debug Tokens, Non-Exportable Keys	✓	✓	✓
Authentication	entity is what/who it claims to be	Secure Identities (CPMS)	✓	✓	✓
Secure Update	patches can be installed securely	Gecko Bootloader	✓	✓	✓
Secure storage	secure stored assets	Secure Key Management, Cryptography	✓	✓	✓
Secure Communication	secure communicated assets	Cryptography	✓	✓	✓
Cryptographic Keys	guidance on key size, generation, and use	Cryptography	✓	✓	✓
General Capabilities	up-to-date software and hardware with no known “exploitable” vulnerabilities, no unnecessary external interfaces	Secure Debug Lock, PSIRT, SBOM, Secure SDLC Maturity Framework, SEMS	✓	✓	✓
Cryptography	shall use for Secure Update, Secure Storage, Secure Comms	Cryptography	✓	✓	✓
Resilience	mitigate Denial of Service (DOS) attacks	PSIRT, SSMF	✓		
Network Monitoring	detect DOS and defend	Tamper Detect	✓		
Traffic Control	detect malicious comms traffic	NA	✓		
User Notification	notify user of changes of assets	NA		✓	
Deletion	delete assets	Tamper Deletes PUF Key		✓	
Logging	Log events relevant to assets	Tamper		✓	✓

Silabs RED Collateral

Item	Description
User Guide for RED Assessment (Series 2)	In-depth analysis of what Silabs' interpretation of the RED requirements are, what security features are available on Silicon Labs' device to customers to help meet RED
RED Overview Power Point	What is RED, what are EN 18031 requirements and how Series 2 Secure Vault High Parts map to them
Blog	Lightweight read to understand RED, EN18031 requirements, and Silicon Labs' security offering
RED Web Page(s)	Web content referencing all other RED collateral
Security Regulations WP	Regulatory white-paper showcasing our commitment to staying ahead of the regulations

Secure Vault: Recognized by Industry Leaders

- **ARM PSA Level 4 iSE/SE**
  - First SoC to achieve PSA Level 4 iSE/SE certification
  - Assures resistance to advanced hardware and software attacks
- **ARM PSA Level 2 and 3**
  - First SoC to achieve Level 3 certification
  - Assures a proven hardware root of trust
- **SESIP Level 2 and 3**
  - First SoC to achieve a SESIP Level 3 certification
- **Independent Security Evaluation by Riscure**
  - Comprehensive analysis report from Riscure
  - Can be shared under NDA

Third Party Accreditation

Questions and next steps

Next Steps:

- Assess RED readiness
- Engage Silicon Labs for guidance
- Explore Secure Vault resources

Deadline: Aug 1, 2025 - RED compliance is mandatory. Secure Vault helps you get there.

SILICON LABS

CONNECTED INTELLIGENCE