Radio Equipment Directive (RED)

public

Introduction: What is RED and why is it needed?

Rising security vulnerabilities

The number of connected devices is forecasted to double in the next decade – from 19.8 billion in 2025 to **40.6 billion** in 2034[1]

Over **40,000** Common vulnerabilities and exposures were reported in 2024 – nearly **40%** increase from 2023[2]



Over **50%** of IoT devices have critical – and currently exploitable – security flaws[3]

84% of companies have high-risk vulnerabilities in their network parameters[4]

[1] www.statista.com
[2] www.mitre.org
[3] www.ibm.com
[4] www.fortinet.com

Copyright © Infineon Technologies AG 2025. All rights reserved.

The more connected our world becomes, the more our devices need to be secured



Why was RED introduced?

With the rising cybersecurity vulnerabilities, the EU has taken the initiative to impose a minimum basic level of security for connected wireless devices

RED aims to ensure that all devices that use radio waves (phones, Wi-Fi routers, Bluetooth speakers) are safe, work properly and don‘t interefere with other devices

What RED mandates

- ✓ Efficient use of radio equipment
- ✓ Prevention of harmful interference
- ✓ Meeting safety and health requirements
- ✓ Meeting cybersecurity requirements (as of August 2025)

Three quick facts about RED to get you started



Fact nr. 1

The Radio Equipment Directive (2014/53/EU) is an EU legal framework, legally binding across all EU member states. RED is mandated by EU law – the standards for RED are developed by European standardization organizations such as CENELEC,/ ETSI, and CEN



Fact nr. 2

A recent cybersecurity amendment to RED introduces mandatory cybersecurity requirements, detailed in the harmonized standard EN18031 with 83 specific technical requirements covering cybersecurity aspects for radio-connected devices



Fact nr. 3

RED applies to the final product and not to individual components; however, using pre-certified reference designs/solutions can significantly streamline the conformity assessment process

Copyright © Infineon Technologies AG 2025. All rights reserved.

RED deep dive

RED timeline

05/2014	06/2014	09/2021	08/2024	08/2025
RED is adopted by the EU Parliament and Council	RED comes into force	Cybersecurity requirements added to RED	RED cybersecurity requirements finalized	Start of first full year RED become mandatory



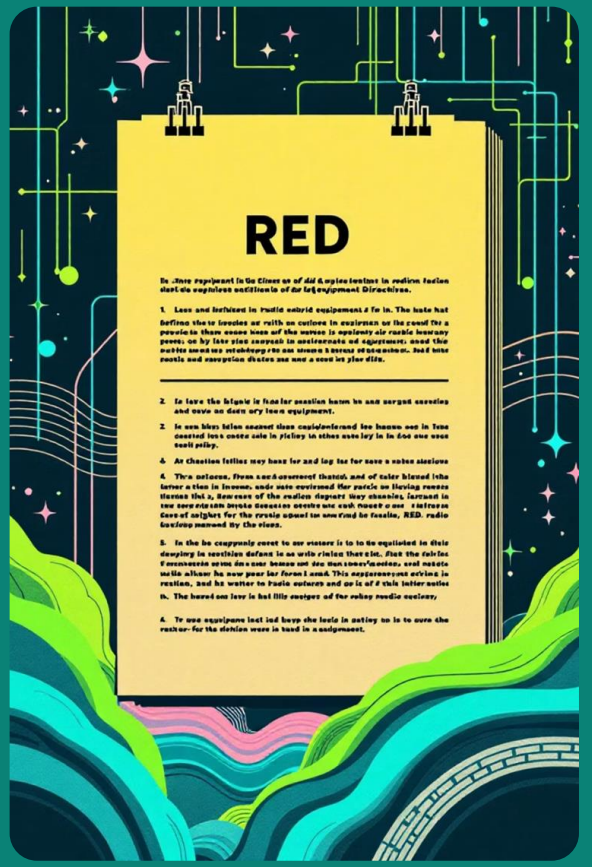
RED definition of radio equipment

> "An electrical or electronic product that intentionally emits and/or receives radio waves for the purpose of radio communication and/or radio determination."
> *Article 2(1) of the Radio Equipment Directive*

Breaking down the definition

1	2
Electrical or Electronic Product • Electrical: Uses electricity as primary power source • Electronic: Contains electronic components • Product: Manufactured item for use or consumption	**Intentionally Emits and/or Receives** • Intentionally: Purposefully designed • Emits: Sends out radio waves • Receives: Captures radio waves • And/or: Can do either or both functions

> “Non-radio products (e.g. passports, credit cards) which are tagged, other than the TAG itself (as clarified above), are not radio equipment and do not require CE marking and contact details for the purposes of the RED.”
> *Article 1.6.13 of the Guide to the Radio Equipment Directive 2014/53/EU*



Copyright © Infineon Technologies AG 2025. All rights reserved.

How do they compare? RED vs. CRA

RED is fundamentally different from the Cyber Resilience Act (CRA)

RED For safe and reliable radio communication	CRA For comprehensive cybersecurity protection
Applies to all devices using radio frequency communication	Applies to all products with digital elements (MCU, MPU, software, IoT)
Radio performance and cybersecurity requirements	Comprehensive cybersecurity and data protection
Applies to the final product and not to individual components	Applies to individual components within a product with digital elements
Focus: radio performance, EMC, and cybersecurity for radio communication	Focus: complete security across hardware, firmware, software, and entire product lifecycle
Manufacturers have design flexibility but must ensure compliance	

Copyright © Infineon Technologies AG 2025. All rights reserved.

Comparison between IoT Security Regulations, Labelling Schemes

Regulation/ Scheme	EU CSA[1] EUCC[2]	EU CRA[4]	EU RED[5]	Singapore CLS[6]	UK PSTI[7]	US Cyber Trust Mark
Labelling	*Security label (in development)*	CE-Label	CE-Label	CLS[6]	SoC[8]	Cyber Trust Mark
Devices	Critical sectors	All sectors	Wireless	IoT	Consumer-IoT	Consumer-IoT
Legal Framework	Voluntary	Mandatory	Mandatory	Voluntary	Mandatory	Voluntary
Effective from	January 2024	December 2027*	August 2025	March 2020	April 2024	Fall 2024
Standard	EUCC[2] EUCS[3], EU5G	*t.b.d.**	*EN 18031-1,-2,-3 (in-approvals)*	EN 303 645	EN 303 645	NIST IR 8245
Levels of Criticality	Yes	Yes	Yes	Yes	No	No
Vulnerability reporting	Yes	Yes	No	No	Yes	No
Compliance required on end-device level vs microchip-level	End-device & microchip-level	End-device & microchip-level	End-device level	End-device level	End-device level	End-device level

1: EU Cyber Security Act
2: EU Cybersecurity Certification Scheme
3: EU Cloud Security Certification scheme
4: EU Cyber Resilience Act
5: EU Radio Equipment Directive‘s delegated articles on Security and Privacy
6: Singapore Cybersecurity Labelling Scheme
7: UK Product Security and Telecommunications Infrastructure Act
8: UK PSTI’s Statement of Compliance

Copyright © Infineon Technologies AG 2025. All rights reserved.

RED essential requirements and harmonized European Norms (hEN)

What to achieve: covered in the RED essential requirements (written as law)	**How to achieve it:** covered in the RED harmonized European Norms Common Security Requirements EN 18031		
(d)* radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service	**Part 1**: Internet-connected radio equipment	Radio equipment with an internet connection, either directly or indirectly.	Smartphones, routers, smart home devices, industrial IoT equipment.
(e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected	**Part 2**: Radio equipment processing personal data	Radio equipment that processes personal data, traffic data, or location data, including internet-connected devices, childcare equipment, toys, and wearables.	Baby monitors, smartwatches, connected toys, wearables.
(f) equipment supports certain features ensuring protection from fraud	**Part 3**: Internet-connected radio equipment processing virtual currencies or monetary values	Internet-connected radio equipment that processes virtual currencies or monetary values.	Mobile payment terminals, digital wallets, connected POS systems.

*(d), (e), (f): New essential requirements added to RED to foster cybersecurity

Copyright © Infineon Technologies AG 2025. All rights reserved.

How to show RED compliance to obtain an EU CE marking?

- The manufacturer bears **sole responsibility** for declaring **conformity** with all requirements
- To show conformity and obtain the CE marking you have to run an assessment for all requirements
- Once your product bears the CE marking — if the competent national authority requests — you must provide them with all the information and supporting documentation concerning CE marking



Infineon can support you in all three steps

Copyright © Infineon Technologies AG 2025. All rights reserved.

Infineon‘s offering for fast and easy RED compliance

Component compliance and choosing the right partner is still crucial



RED compliance applies to the entire final product

While individual components alone do not guarantee compliance, **choosing the right components - and the right partner** - can significantly support and accelerate the path to RED conformity.

A chip might help meet all technical RED requirements if

- Implemented according the reference design guidance
- Is combined with secured software
- Is placed in a device designed with security in mind

Why Infineon is the right partner to help you achieve RED compliance

- Our solutions consist of hardware, software and servies - this enables us to step in and **support manufacturers with a majority of the tasks** associated with obtaining RED compliance
- We bring decades-long expertise and **in-depth knowledge of regulatory requirements** to all critical components and stages of RED compliance

What Infineon can do for you

RED has **49** requirements – as shown in our example, we can support you in meeting up to **100%** of them

➔ We assess which ones are relevant for your system

➔ With our security evaluated and certified Secure Elements and MCUs, we can support you in showing compliance to nearly all of RED’s requirements

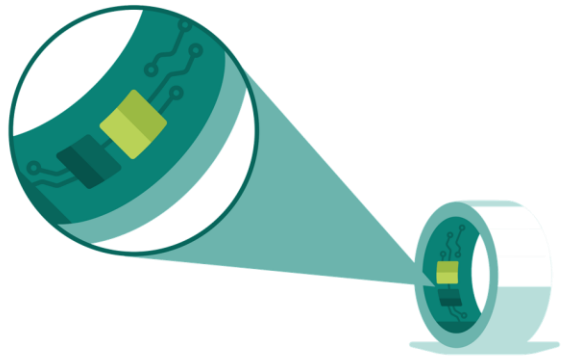


SECORA™ Connect X

An example of an Infineon solution that fullfills all RED requirements

SECORA™ Connect X helps you meet all RED requirements and speeds up compliance in a smart ring application

Smart ring



- **Single** antenna solution approach
- **Ultra-small** antenna design
- Compact solution with **small footprint**



EMVCo Payment Mode

- Multiple EMVCo compliant on small size antenna
- Fulfilling requirements for payment transactions in wearable devices
- VISA and Mastercard applets

Copyright © Infineon Technologies AG 2025. All rights reserved.

SECORA™ Connect X fulfills all 5x RED requirements in a smart ring application (1/2)

Mechanism family	Clause ID	Requirement	SECORA™ Connect X
Access-control mechanism (ACM)	ACM-1	Decide and document where access-control is needed for each resource	Enables compliance
Access-control mechanism (ACM)	ACM-2	Implement an appropriate access-control scheme wherever ACM-1 deems it applicable	Enables compliance
Authentication mechanism (AUM)	AUM-1	Determine where authentication is required	Enables compliance
Authentication mechanism (AUM)	AUM-2	Provide suitable authentication methods (e.g., MFA, certificates)	Enables compliance
Authentication mechanism (AUM)	AUM-3	Validate authenticators correctly (no expired or weak credentials)	Enables compliance
Authentication mechanism (AUM)	AUM-4	Allow secure replacement/rotation of authenticators	Enables compliance
Authentication mechanism (AUM)	AUM-5	Enforce minimum password/pass-phrase strength	Enables compliance
Authentication mechanism (AUM)	AUM-6	Throttle or block brute-force attempts	Enables compliance
Secure-update mechanism (SUM)	SUM-1	Check whether update functionality is required	Enables compliance
Secure-update mechanism (SUM)	SUM-2	Ensure integrity & authenticity of every update (signing, rollback protection)	Enables compliance
Secure-update mechanism (SUM)	SUM-3	Support automated update delivery while preserving security	Enables compliance
Secure-storage mechanism (SSM)	SSM-1	Identify assets that need protected storage	Enables compliance
Secure-storage mechanism (SSM)	SSM-2	Protect integrity of stored assets (e.g., tamper-proof memory, checksums)	Enables compliance
Secure-storage mechanism (SSM)	SSM-3	Protect confidentiality of stored assets (e.g., encryption, access control)	Enables compliance
Secure-communication mechanism (SCM)	SCM-1	Identify which services require secure communication	Enables compliance
Secure-communication mechanism (SCM)	SCM-2	Provide integrity & authenticity protection for data in transit (e.g., TLS)	Enables compliance
Secure-communication mechanism (SCM)	SCM-3	Provide confidentiality for data in transit (encryption)	Enables compliance
Secure-communication mechanism (SCM)	SCM-4	Provide replay-attack protection (nonces, sequence numbers)	Enables compliance
Resilience mechanism (RLM)	RLM-1	Monitor and detect & recover from faults/DoS (fail-safe, watchdogs)	Enables compliance
Network-monitoring mechanism (NMM)	NMM-1	Monitor and detect abnormal traffic that could harm the network	Enables compliance
Traffic-control mechanism (TCM)	TCM-1	Rate-limit or filter to prevent network overload	Enables compliance
Confidential cryptographic keys (CCK)	CCK-1	Use keys of adequate strength and protect them at rest & in use	Enables compliance
Confidential cryptographic keys (CCK)	CCK-2	Generate keys with approved processes (entropy, algorithms)	Enables compliance
Confidential cryptographic keys (CCK)	CCK-3	Prevent use of shared or default keys or credentials	Enables compliance

Copyright © Infineon Technologies AG 2025. All rights reserved.

SECORA™ Connect X fulfills all RED requirements in a smart ring application (2/2)

Mechanism family	Clause ID	Requirement	SECORA™ Connect X
General equipment capabilities (GEC)	GEC-1	Use signed code or firmware with no known exploitable CVEs	Enables compliance
General equipment capabilities (GEC)	GEC-2	Expose only necessary services & their interfaces	Enables compliance
General equipment capabilities (GEC)	GEC-3	Expose only necessary data to each interface	Enables compliance
General equipment capabilities (GEC)	GEC-4	Document the purpose of each exposed interface/service for the end user	Enables compliance
General equipment capabilities (GEC)	GEC-5	Avoid unnecessary external interfaces altogether	Enables compliance
General equipment capabilities (GEC)	GEC-6	Validate all data received by the equipment	Enables compliance
Cryptography (CRY)	CRY-1	Use state-of-the-art cryptographic algorithms & parameters throughout	Enables compliance
Access-control mechanism (ACM)	ACM-3	Provide default access-control protecting child users in toys	Not relevant for this application
Access-control mechanism (ACM)	ACM-4	Restrict default access to children's privacy assets in toys & childcare equipment	Not relevant for this application
Authentication mechanism (AUM)	ACM-5	Enable parental / guardian access controls for child users in toys	Not relevant for this application
Authentication mechanism (AUM)	ACM-6	Enable parental / guardian controls over third-party access to children's privacy assets	Not relevant for this application
Logging mechanism (LGM)	LGM-1	Determine where privacy logging is required	Enables compliance
Logging mechanism (LGM)	LGM-2	Ensure persistent, tamper-resistant storage of privacy log data	Enables compliance
Logging mechanism (LGM)	LGM-3	Record the minimum set of privacy-relevant security events	Enables compliance
Logging mechanism (LGM)	LGM-4	Include reliable time information in all privacy log entries	Enables compliance
Deletion mechanism (DLM)	DLM-1	Provide secure and verifiable deletion of user data when required	Enables compliance
User-notification mechanism (UNM)	UNM-1	Determine when user notifications about privacy events are required	Enables compliance
User-notification mechanism (UNM)	UNM-2	Provide clear content in privacy-related user notifications	Enables compliance
General equipment capabilities (GEC)	GEC-7	Document any external sensing interfaces that may impact privacy	Enables compliance
Logging mechanism (LGM)	LGM-1	Determine where logging is required to protect financial transactions or detect fraud	Enables compliance
Logging mechanism (LGM)	LGM-2	Ensure persistent, tamper-resistant storage of transaction log data	Enables compliance
Logging mechanism (LGM)	LGM-3	Record at least the minimum set of security- and transaction-relevant events	Enables compliance
Logging mechanism (LGM)	LGM-4	Include secure, reliable time information in all transaction logs	Enables compliance
General equipment capabilities (GEC)	GEC-7	Document all non-network external sensing interfaces with potential fraud impact	Enables compliance
General equipment capabilities (GEC)	GEC-8	Implement equipment integrity verification (secure boot, tamper detection)	Enables compliance

Copyright © Infineon Technologies AG 2025. All rights reserved.

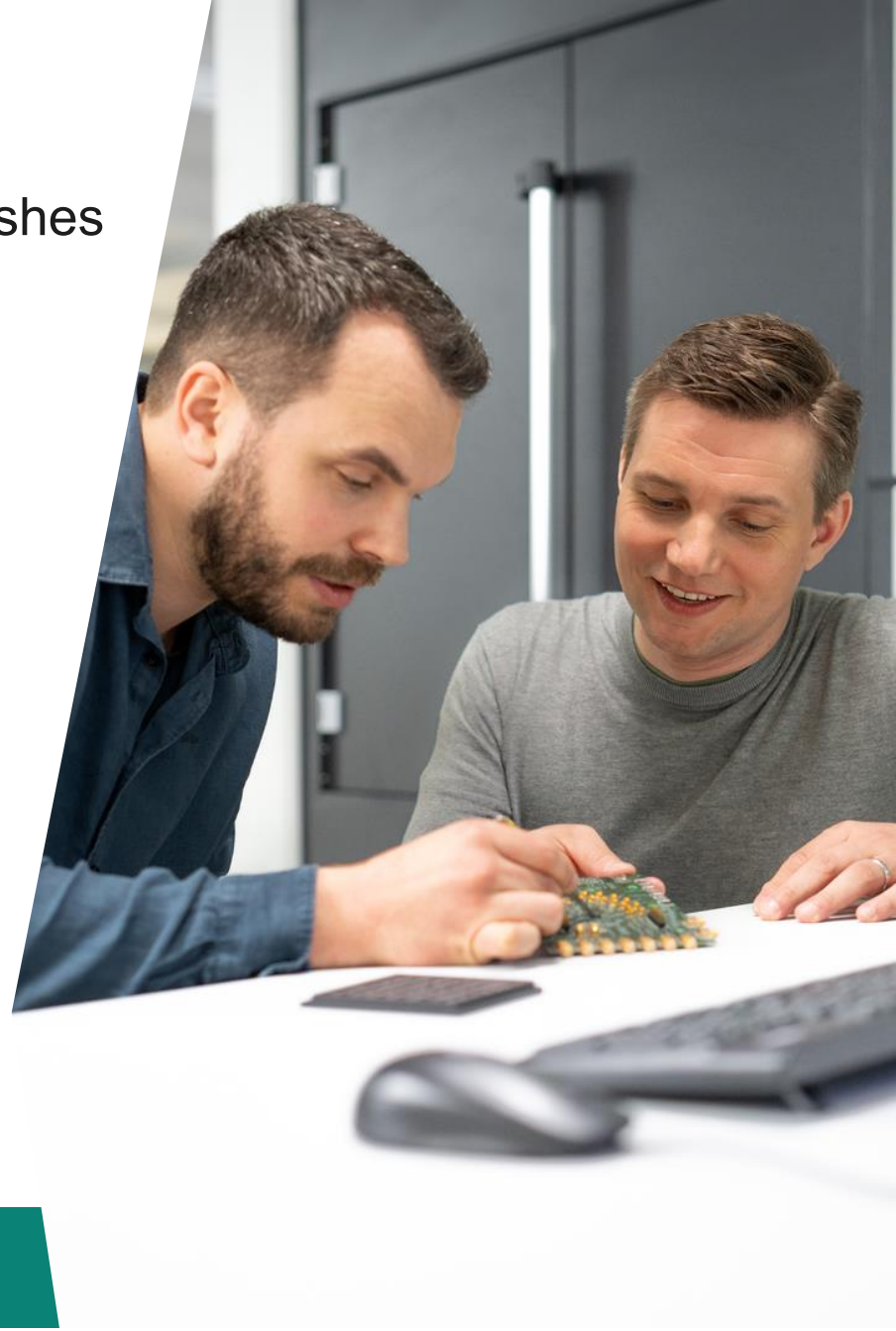


The launch of SECORA™ Connect X is planned for Q1, 2026

Key takeaways

The Radio Equipment Directive 2014/53/EU (RED) establishes a regulatory framework for radio equipment in the EU

- RED was originally introduced to ensure the safe use of radio equipment and efficient use of the radio spectrum across Europe
- A recent amendment to RED makes cybersecurity requirements mandatory effective from August 1, 2025
- RED compliance is assessed at the end-device level, but Infineon's compliant components and regulatory expertise greatly simplify the certification process
- SECORA™ Connect X is an example of a product that can help manufacturers meet all RED requirements in a smart ring application



PSOC™ | AIROC™ | OPTIGA™ | SECORA™ | XELOC™

Copyright © Infineon Technologies AG 2025. All rights reserved.

Visit our RED webpage for more information and solutions




Infineon