EU Compliance:

New Cybersecurity EN 18031-X:2024 Standards for Radio Equipment Directive (RED)

New regulatory developments for manufacturers of devices and systems that include radio or wireless enabled equipment (host devices) include newly ratified standards that address cybersecurity requirements that are mandatory starting August 1, 2025. The European Commission has officially listed the EN 18031-X:2024 series in the Official Journal (OJ) of the European Union under the Radio Equipment Directive (RED), 2014/53/EU. This applies to products that use WI-FI, Bluetooth, Zigbee, and other wireless technologies or protocols, including radio devices that do not connect to the internet.

Equipment that has access or is used with the Internet of Things (IoT) must meet the requirement that will include formal cybersecurity compliance on equipment. This includes household and similar appliances and other equipment that can be programmed or operated via internet commands from users' cell phones or other wireless devices, or associated applications that are involved with processing financial payments or access to virtual money or those items of monetary value.

While most equipment uses pre-approved wireless modules, and many wireless module manufacturers provide updated security protocols, it is the sole responsibility of the company placing the final products into the marketplace to ensure compliance for those end host products for these new cybersecurity requirements. Be aware that the security of the preapproved module is only a minor portion of the cybersecurity requirements for a product using that preapproved module. It is very important to determine the levels of security required for the equipment's intended usage when compared to the wireless modules. The use of independent evaluation and testing organizations can provide needed guidance and support with the detailed review and confirmation of compliance.

EN 18031-X and the Radio Equipment Directive (RED) Cybersecurity Requirements

Radio and wireless IoT integrated equipment placed into the EU market must meet the Radio Equipment Directive, including essential requirements related to safety, electromagnetic compatibility, and efficient spectrum use. The EU Commission introduced cybersecurity requirements in the Deregulated Regulation 2022/30, under Article 3(3):

- Article 3(3)(d): Protection against network harm and service degradation
- Article 3(3)(e): Safeguards for personal data and user privacy
- Article 3(3)(f): Measures to prevent fraud in radio equipment handling virtual currency

The EN 18031-X series of harmonized standards provide the specific requirements for manufacturers to demonstrate compliance with these new cybersecurity requirements.

- EN 18031-1:2024 covering article 3.3 (d) Ensures that radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service, and

unauthorized access

- EN 18031-2: 2024 covering article 3.3 (e) Safeguarding personal processing data, namely internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment using strengthened authentication, encryption, and other controls to prevent unauthorized access or usage.
- EN 18031-3: 2024 covering article 3.3 (f) Addresses risks specific to radio equipment processing virtual money or monetary value, with fraud protection, and prevention of payment system breaches.

Each of these three standards includes details on guidance, evaluation, security mechanisms, documentation, and testing processes and protocol. These standards have substantial overlapping in many areas but have specific requirements in the unique focus of each individual standard. A comparison of the 14 general categories is below:

Mechanisms (requirements)	EN 18031-1	EN 18031-2	EN 18031-3
ACM Access Control Mechanism	X	X	X
AUM Authentication Mechanism	X	X	X
SUM Secure Update Mechanism	X	X	X
SSM Secure Storage Mechanism	X	X	X
SCM Secure Communication Mechanism	X	X	X
RLM Resilience Mechanism	X		
NMM Networking Monitoring Mechanism	X		
TCM Traffic Control Mechanism	X		
LGM Logging Mechanism		X	X
DLM Deletion Mechanism		X	
UNM User Notification Mechanism		X	
CCK Confidential Cryptographic Keys	X	X	X
GEC General Equipment Capabilities	X	X	X
CRY Cryptography	X	X	X

These categories have additional detailed requirements for each section, and careful analysis must be given to address each applicable section and the unique requirements referenced. It may be that more than one standard would be applicable to show compliance.

Restrictions

Manufacturers can now use the EN 18031-X series to claim presumption of conformity with RED's cybersecurity requirements. However, this usage comes with certain restrictions, which must be carefully considered when implementing compliance strategies. Some of these restrictions relate to:

- Sections related to "rationale" and "guidance"
- Consideration and use of passwords
- Parental or guardian access control
- Transfer of monetary value

Action Items for Manufacturers

As the cybersecurity requirements of the Radio Equipment Directive are mandatory beginning August 2025, it is important for manufacturers to align their products with these new requirements. Key steps include:

1. Review the RED scope: Does your product fall under the scope of the cybersecurity requirements of Article 3(3) sections d, e, and f of the RED?

2. Review the new EN 18031-X Series: Understand how these standards apply to your products and any restrictions affecting their intended use. Multiple standards may apply.

3. Conduct a Risk Assessment Analysis: Assess your current cybersecurity measures against EN 18031-X requirements, including a review of a risk analysis, engaging independent third-party assistance if needed. Do not consider wireless module security alone to be sufficient.

4. Determine Compliance Path: Determining the best way to ensure compliance with the new requirements of the RED directive. A third-party analysis and approval often times equates to decreased time to market. In most cases a tailored test plan is developed, with documentation review, software analysis, and functional confirmation testing included.

5. Requirements for Market Readiness: Implement necessary changes in design, testing, and documentation to meet the August 2025 deadline. At a minimum, an updated technical file, updated users guide, and inclusion of the cybersecurity requirements of the RED Directive in the Manufacture's Declaration of Conformity will be required.

6. Establish On Going Cybersecurity Surveillance: Establish a go forward plan to monitor industry requirements and updates to cyber threats in the marketplace. Manufacturers are required to maintain a high level of cyber resilience, as long as products are in the marketplace.

Other Cybersecurity Considerations

As cybersecurity is a global threat, many counties are in the process of developing formal protection regulations. The United States has in process a program called the US Cyber Trust Mark, overseen by the FCC to address IoT accessed smart device protection. Canada

recently passed the Critical Cyber Systems Protection Act which aims to enhance cybersecurity protection. It can be expected that more formalized cybersecurity requirements will be developed on a global basis.

Summary

The publishing of the EN 18031-X series of harmonized standards in the Official Journal provides much-needed clarity for manufacturers navigating RED's cybersecurity requirements for EU compliance.

However, the accompanying restrictions highlight the need for careful evaluation and expert guidance. Independent third-party organizations can assist manufacturers in interpreting these requirements, conducting assessments, verify operating conditions, and ensuring their products meet all regulatory obligations for continued marketplace presence.

Cybersecurity regulatory updates can be found at: http://www.dlsemc.com/cybersecurity-testing.

Jack Black is the business development manager for D.L.S. Electronic Systems, Inc. and has over 30 years of experience in the field of compliance testing and standards development. Jack can be reached at jblack@dlsemc.com.

Corey Sweeney is President of D.L.S. Electronic Systems, Inc., a compliance testing laboratory located in Wheeling, IL. Corey can be reached at cs@dlsemc.com.

Marilyn Sweeney, CEO and one of the founding members of D.L.S., has published several industry related papers. Marilyn be reached at msweeney@dlsemc.com.