RED's Cybersecurity Requirements Update:

EN 18031-X:2024 Harmonized Standards and Related Thoughts

By Corey L. Sweeney, Jack Black, and Marilyn Sweeney

As a continuation of our article *Preparing for the EU's New RED Cybersecurity Requirements* from the June issue of *In Compliance* Magazine, this article will concentrate on the EN 18031-X series that was harmonized and published in the *Official Journal of the European Union* in January 2025, after our previous article was written.

Since our previous article covered the Radio Equipment Directive (Directive 2014/53/EU, known as the RED) plus other acts and directives referring to cybersecurity and why cybersecurity rules are necessary, we will not repeat them in this article.

Standards EN 18031-X:2024

(Authors' Note: To make compliance easier for products that meet some or all of the requirements for ETSI EN 303 645, each of the three EN 18031-X standards shows a map of which of its requirements match specific ETSI EN 303 645 provisions (requirements).)

The EN 18031-X series of standards was developed to provide manufacturers of radio equipment with a harmonized framework to meet the European Union's (EU's) cybersecurity requirements that became mandatory on August 1, 2025. Harmonized standards are a much easier way to go and are generally highly preferred. This series of standards combines the requirements for manufacturers and the requirements for testing laboratories into one standard, requiring less time to cross-reference documents when a better understanding of a requirement is needed.

The standard series is divided into three heavily overlapping standards, each of which has requirements consisting of an identifying code of three letters, a dash, and a number. For example, ACM-1 is the code for one of the requirements. EN 18031-1 has 31 requirements, EN 18031-2 has 40 requirements, and EN 18031-3 has 34 requirements.

Twenty-eight of the requirement codes are common to all three standards, making it appear that they are exactly the same. However, there are some differences in the text, and they do not necessarily all have the same section numbers, which can make the organization of the standards confusing. We will give examples of these differences later in this article.

To understand the organization of the standards better, it can help to know that they are divided into three parts to make it clear that they are covering 3(3)(d), 3(3)(e), and 3(3)(f) of the RED. More precisely:

- EN 18031–1 specifically addresses Article 3(3)(d), i.e., “radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service”;
- EN 18031–2 specifically addresses Article 3(3)(e), i.e., “radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected”;
- EN 18031–3 specifically addresses Article 3(3)(f), i.e., “radio equipment supports certain features ensuring protection from fraud”.

So, the question is not “Which of these three standards applies to your product?” but rather “How many of the three standards apply to your product?”

Complying

Risk Assessment

The answer to the above question will come from your product’s risk assessment. As the EN 18031-X standards themselves state in Section A.2 Rationale:

> *"Whether one or multiple standards need to be applied to a specific radio equipment is a consideration that is made through a product-relevant risk assessment by the economic operator in order to identify threats and assess risks on the need to fulfil the essential requirements of the Radio Equipment Directive."*

Instead of thinking of the three standards as being organized to help with testing or organized to help with implementation of the standard during development, think of them as organized to help perform the mandatory risk assessment that manufacturers are responsible for performing.

Early in the required risk assessment, manufacturers need to determine which essential requirements of RED, as well as requirements in other Directives, apply to their product. A good reference to the application of the risk assessment can be found in the EU “Blue Guide” on the implementation of EU product rules (2022/C 247/01):

> *"Essential requirements must be applied as a function of the hazard inherent to a given product. Therefore, manufacturers have to carry out a risk analysis to first identify all possible risks that the product may pose and determine the essential requirements relevant for the product."*

So, to be clear, your company's risk assessment for each product should include a cybersecurity portion, as well as other portions, such as EMC and Safety.

While you may already be familiar with the safety portion of your risk assessment, you may be less familiar with the cybersecurity portion, which is a bit different. To read an explanation of cybersecurity risk assessment in the context of the RED (as well as the Cyber Security Act, and the Cyber Resilience Act), download the free Technical Report ETSI TR 103 935 at:
https://www.etsi.org/deliver/etsi_tr/103900_103999/103935/01.01.01_60/tr_103935v010101p.pdf.

Since the EMC requirements have been active for much longer than the cybersecurity requirements, the guidance for the EMC portion of a risk assessment is more mature. Understanding risk assessment guidance in the context of something you already know can be potentially helpful. Guidance for the EMC portion of a risk assessment can be found in Technical Report ETSI TR 103 879. A free download can be obtained at:
https://www.etsi.org/deliver/etsi_tr/103800_103899/103879/01.01.01_60/tr_103879v010101p.pdf.

After you begin your risk assessment by deciding which essential requirements of RED and other directives apply to your product, you will need to try to apply harmonized standards to your product. For RED 3(3)(d), 3(3)(e), and 3(3)(f), that will be the harmonized EN 18031-X standards.

Once it has been determined which EN 18031-X standard(s) apply to your product, each of the applicable standards provides details of its own part of the cybersecurity risk assessment for its associated RED essential requirement. Details can be found in each standard, starting with Section A.2.3, which is called "Threat modelling and security risk assessment."

EN 18031-X uses "STRIDE," which is a threat model to identify and enumerate specific types of possible threats to determine what important parts of your product need to be addressed. Additional details about STRIDE can be found at https://owasp.org/www-community/Threat_Modeling_Process#stride. Information on putting STRIDE into context can be found in Technical Report ETSI TR 103 935, section 8.4.2 (see previously provided link) in a section named "STRIDE."

EN 18031-1 "Part 1: Internet connected radio equipment"

During the risk assessment, you will need to decide if EN 18031-1 applies to your product, which is simple for some products, but for other products, you'll need a definition of what counts as internet connected.

What follows is information that is currently available, in order of precedence:

- Directive 2014/53/EU 3(3)(d) basically states that the "goal" for EN 18031-1 is "radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service".

- Delegated regulation 2022/30 Article 1(1) says "The essential requirement set out in Article 3(3), point (d), of Directive 2014/53/EU shall apply to any radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment."

- The EN 18031-X standards themselves introduce the phrasing "Internet connected radio equipment."

Although this partially clarifies the situation, it still leaves a lot of questions open. For example, "In the case of a Bluetooth device connected to a smartphone, to which devices does it apply and to which does it not apply?" The answer is not spelled out in the EN 18031-1 standard nor in the RED, probably because there is no simple answer. It can depend on factors, such as the intended use (including with what app it is intended to be used).

Not all cases lead to a consensus. This is understandable given the complexity and how new the requirement is. As the industry gains experience with these issues, it would be reasonable to expect a convergence toward consensus. This means in your product's risk analysis you should probably add an "interpretation risk" for "internet connected" during the risk identification stage.

EN 18031-2 "Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment"

This is for "radio equipment processing personal data or traffic data or location data for either internet connected radio equipment, radio equipment designed or intended exclusively for childcare, toys, and wearable radio equipment."

To understand the intention of Part 2, several terms need to be defined.

- "Personal data" is defined as:

  "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;" [1]

- “Traffic data” is defined as:
  "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof" [2]

- “Location data” is defined as:
  "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;" [3]

EN 18031-3 "Part 3: Internet connected radio equipment processing virtual money or monetary value"

This is for "internet connected radio equipment. That equipment enables the holder or user to transfer money, monetary value or virtual currency."

Virtual currency is defined as:

"digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of a currency or money, but is accepted by natural or legal persons as a means of exchange, and which can be transferred, stored and traded electronically;" [4]

Requirements – Mechanisms

The EN 18031-X standards are made up of requirements that are grouped into categories called “mechanisms.” Each mechanism has a 3-letter code, for example, “General Equipment Capabilities” is “GEC.” The three-letter mechanism code becomes the first three letters of the five-character requirement code (e.g., GEC-1).

Table 1 shows which of the three standards has at least one requirement in each group (mechanism):

Mechanisms	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

Table 1: Mechanisms (requirement groups) included in each standard

Requirements That Are Similar But Not Exactly the Same in All Three Standards

Although Parts 1, 2, and 3 of the EN 18031-X series each have their own specific requirements, 28 of the requirement codes show up in all three documents. The sections documenting the requirement code in each standard have almost identical text with some minor changes that can potentially have large impacts.

To help you better understand these types of changes, some examples from requirement ACM-1 (Applicability of Access Control Mechanisms) are listed here:

- Wherever ACM-1 in EN 18031-1 mentions the word "network," EN 18031-2 mentions the word "privacy," and EN 18031-3 mentions the word "financial."

- ACM-1 in 18031-1:
  "Do the physical or logical measures in the targeted operational environment limit to authorized entities?"

  Whereas in ACM-1 in 18031-2 and 18031-3:
  "Do the physical or logical measures in the targeted environment ensure that its accessibility is limited to authorized entities?"

  - ACM-1 in 18031-1 and 18031-3:
    "The verdict FAIL for the assessment case is assigned if: ***a*** *path through the decision tree documented in E.Info.DT.ACM-1 ends with 'FAIL'…"*

    Whereas in ACM-1 in 18031-2:
    "The verdict FAIL for the assessment case is assigned if: ***all*** *path through the decision tree documented in E.Info.DT.ACM-1 ends with 'FAIL'…"*

  - ACM-1 in 18031-2 and 18032-3, but not in 18031-1:
    "If the equipment relies on the access control given by the intended operational environment, it is to be ensured that this access control is appropriate as described in ACM-2."

  - ACM-1 18031-2 but not in 18031-1 or 18032-3:
    "In general, full public accessibility to privacy assets cannot be considered as a reasonable intended equipment functionality, especially concerning children's privacy and childcare. However, specific scenarios involving public accessibility to privacy assets may be considered as intended equipment functionality if part of clearly advertised functionality or is communicated (to non-child users) via UNM."

  So be sure to check the requirements in each of the three standards even though they may appear to be the same.

Restrictions

When EN 18031-X was harmonized, restrictions were added, a full list of which can be found in OJ L, 2025/138 - 30/01/2025. [5] Here's an example of the importance of being aware of all restrictions that apply to these standards. In the Authentication category, AUM-5-1 *Requirement for factory default passwords* referenced in all three standards includes the line: "NOTE: The user can choose to not use any password."

However, in the Restrictions it says:

> *"Clauses 6.2.5.1 and 6.2.5.2 of harmonized standards EN 18031-1:2024, EN 18031-2:2024 and EN 18031-3:2024 deal with default passwords. Those clauses offer manufacturers the possibility to allow a user not to set or use any password. It is considered that, if this option is implemented, the relevant authentication risks will not be properly addressed and therefore conformity with the essential requirements set out in Article 3(3), first subparagraph points (d), (e) and (f), of Directive 2014/53/EU would not be ensured."*

Obtaining the EN 18031-X:2024 Standards

Although the ETSI EN 303 645 standard is available as a free download, there is not a clear path at this time for freely using downloaded copies of the harmonized EN 18031-X:2024 standards. Some progress has been made because of the "Malamud Case" so EN citizens may want to search on "Malamud Case" in order to see if their country's standards organization has made progress on making some form of free access available.

Otherwise, the EN 18031-X standards can be purchased. And yes, we realize the irony in how many people will end up lowering the security of their computers by installing "FileOpen" just to be able to download and read a security standard. ("FileOpen" appears to be a DRM binary without a reproducible build process or auditable source and requires other binaries without reproducible build process or auditable source preinstalled and prevents you from reading them from a secure system with access to the internet blocked.)

We are not providing a link to EN 18031-X:2024 as there is no single source for the standards since they are distributed through the standards organizations of the various EU countries.

A Word of Caution

Be aware that IEC/ISO 18031 is not the same as EN 18031-1, -2 and -3. While IEC/ISO 18031 is the same number and is also on the topic of cybersecurity, it is not the same type of standard, as it is specifically focused on random number generators. IEC/ISO 18031 is actually mentioned in the EN 18031-X series when discussing random number generation.

Conclusion

The world of cybersecurity is relatively new and rapidly changing. Meeting its regulations can feel complex and overwhelming, so you may want to contact your test lab for assistance. Cybersecurity updates can be found at http://www.dlsemc.com/cybersecurity-red.

References

[1] https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng , Article 4(1)

[2] https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng , Article 2(b)

[3] https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng , Article 2(c)

[4] https://eur-lex.europa.eu/eli/dir/2019/713/oj/eng , Article 2 (d)

[5] https://ec.europa.eu/docsroom/documents/64474/attachments/1/translations/en/renditions/native

About the Authors

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

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

Marilyn Sweeney *is CEO and one of founding members of D.L.S. Sweeney can be reached at msweeney@dlsemc.com.*

Published in InCompliance, September 2025