

EU RED Cybersecurity

Guidance for Short-Range modules

Application note

Abstract

This document helps integrators of u-blox radio modules to understand the RED cybersecurity requirements and navigate the legal framework surrounding it. The focus is primarily on the technical requirements of the EN 18031-1 standard and guidance regarding the split of responsibilities between the radio module manufacturer and the host product integrator. In addition to the technical guidance, the document also attempts to give helpful guidance on the surrounding legal terms, but with a careful approach as to not be understood as legal advice.

Document information

Title	EU RED Cybersecurity	
Subtitle	Guidance for Short-Range modules	
Document type	Application note	
Document number	UBXDOC-465451970-4598	
Revision and date	R03	12-Sep-2025
Disclosure sensitivity	C1-Public	

u-blox or third parties may hold intellectual property rights in the products, names, logos, and designs included in this document. Copying, reproduction, or modification of this document or any part thereof is only permitted with the express written permission of u-blox. Disclosure to third parties is permitted for clearly public documents only.

The information contained herein is provided “as is” and u-blox assumes no liability for its use. No warranty, either express or implied, is given, including but not limited to, with respect to the accuracy, correctness, reliability, and fitness for a particular purpose of the information. This document may be revised by u-blox at any time without notice. For the most recent documents, visit www.u-blox.com.

Copyright © u-blox AG.

Contents

Document information	2
1 Summary	4
2 Background.....	5
2.1 Regulation.....	5
2.1.1 Relation to the Cyber Resilience Act (CRA)	5
2.2 Standards	5
2.2.1 EN 18031 series	5
2.2.2 EN 303 645	6
2.3 Regulatory concepts	6
2.3.1 Applicability.....	6
2.3.2 Risk assessments.....	6
2.3.3 Declaration of Conformity (DoC)	6
2.3.4 Placing of products on the market.....	6
3 Module portfolio.....	7
4 Module integrator guidance.....	9
4.1 Regulatory guidance.....	9
4.2 EN 18031 guidance	9
4.2.1 Restrictions.....	9
4.2.2 Requirements	9
Appendix	18
A Terminology.....	18
B Common misconceptions	18
B.1 The cyber articles apply to all radio modules	18
B.2 Products already on the market	18
B.3 Integrator can only use modules with a DoC	18
B.4 Bluetooth applicability.....	19
Related documentation	20
Revision history	20
Contact.....	20

1 Summary

The RED cyber articles start to apply on 1-Aug-2025 and their applicability must be determined for every radio product placed on the EU market. Three standards with the designations EN 18031-1, EN 18031-2, and EN 18031-3 have been published and can be used for the purpose of self-assessment if certain criteria apply. This guide helps to ensure that the integrator of radio modules ends up with a product which fulfils the security objectives.

2 Background

2.1 Regulation

The regulation discussed here is the RED Delegated Regulation 2022/30^[1] which has jurisdiction within the EU common market. Through this act, a number of articles that were already present in the Radio Equipment Directive (RED) were activated, specifically 3.3 (d), (e), and (f) relating to cybersecurity.

Apart from the official name, plenty of shorter or more descriptive alternatives have been used to refer to the regulation and the articles, including:

- RED-DA,
- RED-cyber or REDCYBER,
- RED cyber articles,
- RED articles 3.3 (d), (e), and (f).

and a few other variations. At u-blox we have chosen to use REDCYBER to effectively communicate about it. This was inspired by the ETSI working group which early on worked on mapping EN 303 645 requirements to the RED cyber articles.

The activated articles denote essential requirements, and their applicability must be considered by anyone manufacturing radio equipment intended for the EU market. The articles are in force (i.e. accepted as law) and apply from 1-Aug-2025. The requirements can briefly be stated as:

- 3.3 (d): protect the network from harm,
- 3.3 (e): protect personal data and privacy, and
- 3.3 (f): protect against financial fraud.

2.1.1 Relation to the Cyber Resilience Act (CRA)

The REDCYBER regulation is in many ways a steppingstone towards the CRA which is a regulation with much broader applicability. When the CRA starts to fully apply on 11-Dec-2027 it is expected that REDCYBER will be subsumed into it, leaving just a single law which operates horizontally across the market for regulating the cybersecurity of products. Whereas REDCYBER applies to radio equipment, the CRA will in general apply to any product with digital elements, including pure software. There are however exceptions, e.g. medical devices which are regulated through other laws. The exact impact on radio modules is as of writing still being assessed by u-blox.

2.2 Standards

2.2.1 EN 18031 series

A series consisting of three standards corresponding to the respective cybersecurity articles and designated EN 18031-1, EN 18031-2 and EN 18031-3 respectively. They were developed by CEN/CENELEC specifically in response to the REDCYBER regulation. The standards take a formal approach rooted in the cybersecurity objectives of the regulation. Essential to the application of the standard is an understanding of the definitions for various asset classes (available in the Terms and definitions chapter). The standards can be bought from one of the national standardization bodies.

The standards have been harmonized and cited^[2] in the Official Journal of the EU (OJEU). They are thus possible to use for the purpose of self-assessment under a few preconditions. In particular note that the European Council harmonized the standards together with certain restrictions which must

be adhered to when utilizing them to achieve a presumption of conformity. There is further guidance for relevant restrictions in later chapters.

2.2.2 EN 303 645

An older standard developed by ETSI which is well-regarded and saw a lot of use in the interim period before EN 18031 was finalized. It does not offer presumption of conformity for self-assessment in the context of REDCYBER but is still a viable alternative at most test labs when certifying with a notified body.

2.3 Regulatory concepts

See also Common misconceptions in the appendix.

2.3.1 Applicability

For the purpose of this document applicability refers to the determination of whether any of the articles 3.3 (d), (e), and/or (f) apply to a particular product placed on the EU market. There are plenty of other cases when other types of applicability are relevant though, e.g. applicability of requirements, so it is important to always keep the context in mind. In chapter 3, the applicability when it comes to short-range radio modules is discussed. However, it is important for integrators to understand that they hold the full responsibility for their host products and that includes making a determination about applicability for it, irrespective of the radio module.

2.3.2 Risk assessments

Risk assessments are performed by manufacturers to capture risks related to their products being placed on the market. For the context here and especially when the applicability determination outcome is negative, it is important that the risk analysis is sound. One outcome of u-blox's risk assessment is this guidance document which ensures that market actors are aligned on their respective responsibilities so that only conformant host products are placed on the EU market.

2.3.3 Declaration of Conformity (DoC)


A document published by a manufacturer which declares which legal requirements and standards that a product conforms to, e.g. 3.3 (d) and EN 18031-1.

2.3.4 Placing of products on the market

To be legally allowed to place products on the EU market, they must fulfill the applicable requirements of applicable regulations. This includes the RED cybersecurity articles starting from 1-Aug-2025 if they are determined to apply. The exact definition of what “placing on the market” means is unfortunately often misunderstood. This concept is defined in the EU Blue Guide^[3] and applies equally to old as well as new products. The placement of a product refers to every individual unit and not to a type of product. Refer to the EU Blue Guide for more detailed information.

3 Module portfolio

u-blox categorizes its short-range radio modules into three major categories, namely 1) the wireless MCU or “Open CPU” modules, 2) the network processor modules with u-connectXpress software and 3) host-based modules. The REDCYBER regulations affect each of these modules in a different way. The exact impact of the REDCYBER requirements on these modules is described in detail in u-blox’s statement of RED DA on short-range radio products [6]. A summary of the impact of RED DA on our short-range module portfolio is included as a table below.

 This section talks only about how u-blox modules are affected by the new cybersecurity requirements. Module integrators must do their own analysis on their end-product design, independent of u-blox’s analysis, and make sure that they comply with the RED cybersecurity articles. See section 4.

Product	Category	Remark
ODIN-W26x NINA-W15x NORA-W36x	Stand-alone modules with u-connectXpress with multi-radio support	These modules are affected. All module-level activities around RED cybersecurity articles are completed. The DoCs are updated and published.
NINA-W13x	Stand-alone modules with u-connectXpress with support for Wi-Fi only	These modules are affected. All module-level activities around RED cybersecurity articles are completed. The DoCs are updated and published.
NINA-W10x NORA-W10x NORA-W30x NORA-W40x IRIS-W10x	Stand-alone open CPU modules with support for Wi-Fi and multi-radio	These modules are not affected by RED cybersecurity articles.
NINA-Bxx BMD-3xx NORA-Bxx ANNA-Bxx ALMA-B1x OBS421	Stand-alone modules with Bluetooth	These modules are not affected by RED cybersecurity articles.
LILY-Wxx EMMY-Wxx MAYA-Wxx	Host-based modules	The impact of RED cybersecurity articles on these modules is best analyzed on a system level.

JODY-Wxx		
RUBY-Wxx		

Summary of how the inclusion of cybersecurity articles in the RED DR affects u-blox Short Range
Radio module portfolio

4 Module integrator guidance

4.1 Regulatory guidance

Although there are multiple options available for achieving compliance with the REDCYBER regulation, the most common approach now that the standards have been harmonized is likely to use self-assessment. Using that approach the applicability of any of the cybersecurity articles must be determined by the manufacturer and the respective standard utilized for assessment. Note that the obligations under REDCYBER for a radio module manufacturer are independent from that of a host product manufacturer integrating such a module. Using a module with declared compliance to REDCYBER helps the assessment process of the host product, but it still has to go through its own conformity assessment.

4.2 EN 18031 guidance

The goal here is to make expectations and the division of responsibility when it comes to cybersecurity clear for the integrators of a u-blox radio module. The breakdown here covers the requirements in the EN 18031-1 standard which is the only one directly applicable to radio modules, as they do not directly deal with personal data and privacy assets (EN 18031-2) nor financial assets (EN 18031-3). Understanding how the requirements apply to a radio module helps to clarify which security properties are and aren't delivered as part of the module, and thus what an integrator must do to remain conformant with EN 18031-1 also for their host product. The guidance must only be interpreted in the context of the EN 18031-1 standard and the security objectives it aims to achieve. The markets targeted and the products in which u-blox radio modules are integrated might require the consideration of other security objectives not covered by EN 18031-1 and no guidance related to that is offered by this document.

4.2.1 Restrictions

When the EN 18031 standards were cited^[2], they were affixed with restrictions from the European Commission. The integrator of a radio module is advised to analyze these restrictions, and the exact wordings as published, but where we believe them to be relevant it will be noted in the following. Note that not all restrictions are deemed relevant for this document, so it does not exhaustively cover all of them.

One common restriction relates to the standards' sections named Rationale and Guidance which are restricted from usage for the purpose of achieving a presumption of conformity of a self-assessment. This means that it is not allowed to use what's written in those sections when arguing for conformity to the requirements. The arguments must be made strictly upon the normative sections (e.g. what's written under Requirement or Assessment Criteria).

4.2.2 Requirements

4.2.2.1 [ACM / AUM] Access Control and Authentication Mechanisms

Physical interfaces

When it comes to internal components in general, and radio modules specifically, there is typically no strict requirement to apply access control measures for the internal interfaces. The expectation is that such a component is fully enclosed and not directly accessible when integrated into the host product. Phrased differently, in the intended use the internal interfaces shall not be made available as an external interface. Intended use is a fundamental regulatory concept which shall be considered when analyzing the requirements.

If an integrator of such a component chooses to expose one of its internal interfaces, then compensatory controls may have to be added. This is the responsibility of the integrator.

Where possible it is of course always better to prevent access even through internal interfaces and u-blox in general provides guidance regarding this in the corresponding System Integration Manuals as necessary. In many cases, this achieves a stronger cybersecurity posture than what EN 18031-1 strictly requires and so again it is important to remember that the guidance here relates just on how to achieve conformance with that standard and does not indicate what is suitable for the specific product in its context.

Wireless interfaces

Wireless interfaces are in general not protected by enclosures, since radio signals permeate most materials. Thus even an internal antenna and the functions or services exposed through it must be considered external in the intended use. They must therefore have capabilities for access control.

As is hinted by the section title the access control and authentication mechanism can be treated as one and the same when it comes to the relevant wireless interfaces and functions available in the short-range radio modules, specifically for WLAN and Bluetooth. After a successful authentication they give full access to the corresponding functionality and there is no further fine-grained access control. This is why we here argue that at the level of the radio module, the access control mechanism and the authentication mechanism are the same. An integrator could build more fine-grained access control mechanisms on top of this.

Restrictions

The standards as published (cf. EN 18031-1:2024, AUM-5-2, “NOTE: The user can choose to not use any password.”) allowed a user to not set a password at all if the user so chooses. The European Commission did not consider this sufficiently secure and put a restriction against it. Empty passwords are thus not allowed.

4.2.2.2 [SUM] Secure update mechanism

Having the capability of updating the software of devices is fundamental to cybersecurity. All u-blox modules have the capability of receiving firmware updates through the host product over a physical interface. For the u-connectXpress family of modules u-blox publishes firmware updates online.

The module integrator must close the software update mechanism chain by delivering updates to the module through their host product. The modules will not attempt to download updates from the Internet themselves.

4.2.2.3 [SSM] Secure storage mechanism

From the perspective of the standard, this requirement refers to such assets stored within the module that are relevant for the networking functionality, for example:

- Wi-Fi credentials
- Bluetooth bonding security parameters
- Firmware update verification keys

Since the module is intended to be enclosed when integrated into the product, from an integrator's perspective, it is sufficient to not externally expose any of the module's internal physical interfaces to remain conformant. From the perspective of a radio module this is conformant through the DT.SSM-1.DN-1:YES branch (i.e. not applicable), considering the intended usage. Confidential parameters are however never extractable even over internal physical interfaces. Similarly, assets are neither extractable nor modifiable over any wireless interface to the module, so even reaching DT.SSM-1.DN-2 in the decision tree would deem radio modules conformant even outside of the intended usage.

4.2.2.4 [SCM] Secure communication mechanism

As the modules themselves do not communicate any assets (as defined in EN 18031), they are not themselves assessed against this requirement. However, modules do provide the communication mechanisms which can be utilized as SCMs. Thus we provide guidance for the respective wireless communication technologies which exist in our products. Note that u-blox cannot claim to be the final and only authoritative source regarding what constitutes a best practice and what can be justified in any specific context.

Under DT.SCM-2.DN-2 a deviation from the best practices can be allowed for interoperability reasons, e.g. to communicate with legacy equipment which only supports WPA or even WEP. Although those protocols may support some of the specific high-level requirements of SCM-2 to SCM-4, the suitability must be analyzed within the specific domain and context of the host product. Such arguments are primarily documented in CRY-1.

Note also that the standard requires integrity and authenticity for every SCM, but confidentiality and replay protection are conditioned on the necessity (e.g. for asset or use case). It can also be worthwhile to consider that additional cryptography can be layered on top of the base communications technologies. This would then give the possibility to strengthen any gaps, e.g. in a host processor, or simply argue that the radio module does not itself provide the SCM. A concrete example: Use the radio module's Wi-Fi to get network access, but then use TLS implemented in a host processor for the secure communication. The radio module does not serve as an SCM in that example, even if the Wi-Fi access itself has some means of protection. Another possible way to view it is as two independent mechanisms as part of a defense-in-depth setup.

WLAN

Note: WPA is a certification program managed by the Wi-Fi Alliance. However in common usage the term is typically used referring to the specific security mechanisms included within the specific certifications, e.g. WPA2 and WPA3. Similarly, Wi-Fi and WLAN are sometimes also used interchangeably.

To implement best practices for achieving integrity and authenticity (SCM-2), confidentiality (SCM-3), and replay protection (SCM-4) both WPA2 and WPA3 security modes are clearly suitable in u-blox's assessment. u-blox recommends following the guidance provided by its application note on Wi-Fi security^[4] to achieve a best practice configuration, e.g. to only utilize WPA3 if possible.

Refer to the following table for help with the conceptual assessment and filling out the E.Info fields.

Protocol	Application-specific protocol ⁽¹⁾ over WLAN using WPA2-Personal	Application-specific protocol ⁽¹⁾ over WLAN using WPA3-Personal	Application-specific protocol ⁽¹⁾ over WLAN using EAP-TLS	Application-specific protocol ⁽¹⁾ over WLAN using PEAP
Integrity/authenticity (IC.SCM-2)	ManufSecret or SecChanExchange ⁽²⁾	ManufSecret or SecChanExchange ⁽²⁾	PKI-based and/or ManufSecret or SecChanExchange ⁽²⁾	PKI-based and/or ManufSecret or SecChanExchange ⁽²⁾
Confidentiality (IC.SCM-3)	ChannelEnc	ChannelEnc	ChannelEnc	ChannelEnc
Replay protection (IC.SCM-4)	SeqNumb	SeqNumb	SeqNumb	SeqNumb

Authentication Capabilities⁽³⁾	4-way handshake (WPA2-Personal) Mutual authentication based on shared secret	SAE (WPA3-Personal) Mutual authentication based on shared secret Offline brute-force protection	EAP-TLS (WPA2/3-Enterprise) Custom PKI-based mutual authentication	PEAPv0/EAP-MSCHAPv2 (WPA2/3-Enterprise) Client authentication based on credentials Optional server authentication based on custom PKI
Implementation Details⁽⁴⁾	IEEE 802.11i	IEEE 802.11i IEEE 802.11s	IEEE 802.11i RFC 5216	IEEE 802.11i Kamath, 2002
CCK	Key derivation based on shared secret (SCM-2, password or PSK) resulting in AES key of either 128-bit or 192-bit used in AES-CCMP or AES-GCMP in a non-legacy configuration (SCM-3)	Key derivation based on shared secret (SCM-2, password or PSK) resulting in AES key of either 128-bit or 192-bit used in AES-CCMP or AES-GCMP in a non-legacy configuration (SCM-3)	Server authentication based on X.509 certificate (SCM-2) Confidentiality and integrity of data traffic depending on configuration and in a non-legacy configuration either AES-CCMP or AES-GCMP with 128-bit or 192-bit keys (SCM-3)	Server authentication based on X.509 certificate (SCM-2) Confidentiality and integrity of data traffic depending on configuration and in a non-legacy configuration either AES-CCMP or AES-GCMP with 128-bit or 192-bit keys (SCM-3)
Threat Protection (NOTE: The enumerated threats refer to the STRIDE model)	<p>Spoofing is protected against using authentication (<i>see: Authentication Capabilities</i>).</p> <p>Tampering is protected against using Authenticated Encryption (AE) cryptographic algorithms (<i>see: CCK</i>).</p> <p>Repudiation protection (non-repudiation) can in general not be achieved solely through the securing of a transport layer. Since SCM-4 refers to replay protection, our best advice is to mention that. (<i>see: IC.SCM-4</i>) Higher layer mechanisms may provide further non-repudiation.</p> <p>Information disclosure is protected against using encryption (<i>see: CCK</i>).</p> <p>Denial of service protection is primarily provided by the authentication mechanism which prevents the injection of frames intended for the malicious disruption of networks and devices. WPA3 (IEEE 802.11w) also mandates protected management frames (PMF).</p> <p>Elevation of privilege is not directly relevant at the transport layer further than what is</p>	(same as first column)	(same as first column)	(same as first column)

	protected against by the spoofing and tampering countermeasures.			
--	--	--	--	--

(1) All application-specific protocols are a concern of the integrator.

(2) Depends on host implementation and configuration.

(3) Capabilities can be used to fulfil security objectives (E.Info.SCM-1.SCM.SecObjectives).

The capabilities are also separately described in the E.Info.SCM-X.SCM.Capabilities fields.

(4) WPA specifications from the Wi-Fi Alliance are also useful as references.

Bluetooth

To implement best practices for achieving integrity and authenticity (SCM-2), confidentiality (SCM-3), and replay protection (SCM-4) the foremost recommendation is to utilize Secure Connections Only Mode together with a strong association model like OOB. This mode also prohibits the negotiation of less secure configurations to interoperate with less capable equipment, which otherwise is the typical mode of operation. In u-connectXpress products this mode is enabled using the +UBTST AT command with parameter security_type=2 (called FIPS mode) but isn't the default for reasons of interoperability.

Bluetooth has many other configurations and legacy modes available, and they are only recommended for backwards compatibility. The usage of legacy methods could be argued for reasons of interoperability (e.g. DT.SCM-2.DN-2). Note that even without using the Secure Connections Only Mode the most secure configuration supported by both devices will be negotiated. Further guidance can be found in u-blox's application note on Bluetooth security^[5].

Refer to the following table for help with the conceptual assessment and filling out the E.Info fields.

Configuration	Profile ⁽¹⁾ over BR/EDR Security Mode 4, Level 3 with E0/SAFER+ (128)	Profile ⁽¹⁾ over BR/EDR Security Mode 4, Level 3 with AES-CCM-128	Profile ⁽¹⁾ over BR/EDR Security Mode 4, Level 4 (Secure Connections Only Mode)	Profile ⁽¹⁾ over LE Security Mode 1, Level 4 (Secure Connections Only Mode)
Bluetooth Minimum Version	2.1	4.1	4.1	4.2
Integrity/authenticity (IC.SCM-2) category	Depends on the association model ⁽²⁾ used during pairing. Typically categorized as SecChanExchange or ManufSecret (OOB), SecChanExchange (NumericComparison or PasskeyEntry) or Generic (JustWorks).	Depends on the association model ⁽²⁾ used during pairing. Typically categorized as SecChanExchange or ManufSecret (OOB), SecChanExchange (NumericComparison or PasskeyEntry) or Generic (JustWorks).	Depends on the association model ⁽²⁾ used during pairing. Typically categorized as SecChanExchange or ManufSecret (OOB), SecChanExchange (NumericComparison or PasskeyEntry) or Generic (JustWorks).	Depends on the association model ⁽²⁾ used during pairing. Typically categorized as SecChanExchange or ManufSecret (OOB), SecChanExchange (NumericComparison or PasskeyEntry) or Generic (JustWorks).
Confidentiality (IC.SCM-3) category	ChannelEnc	ChannelEnc	ChannelEnc	ChannelEnc
Replay protection (IC.SCM-4) category	SeqNum	SeqNum	SeqNum	SeqNum
Authentication capabilities⁽³⁾	Data integrity based on CRC – not of cryptographic strength. Key agreement based on ECDH (P-192). Bonded authentication based on Link Key.	Data authenticity based on AES-CCM-128. Key agreement based on ECDH (P-192 or P-256). Bonded authentication based on Link Key.	Data authenticity based on AES-CCM-128. Key agreement based on ECDH (P-256). Bonded authentication based on Link Key.	Data authenticity based on AES-CCM-128. Key agreement based on ECDH (P-256).

Confidentiality capabilities⁽³⁾	E0/SAFER+ (128)	AES-CCM-128	AES-CCM-128	AES-CCM-128
Replay protection capabilities⁽³⁾	Repeating clock – not of cryptographic strength	AES-CCM-128 (36-bit packet counter in nonce)	AES-CCM-128 (36-bit packet counter in nonce)	AES-CCM-128 (39-bit packet counter in nonce)
Implementation Details	Bluetooth Core Specification v4.0 or earlier	Bluetooth Core Specification v4.1 or later RFC 3610	Bluetooth Core Specification v4.1 or later RFC 3610	Bluetooth Core Specification v4.2 or later RFC 3610
CCK	128-bit SAFER key	AES-128	AES-128	AES-128
Threat Protection (NOTE: The enumerated threats refer to the STRIDE model)	<p>Spoofing is protected against using authentication (see: Authentication Capabilities).</p> <p>Tampering is protected against with a mix of cryptographic and non-cryptographic methods (see: Authentication, Confidentiality, and Replay protection capabilities).</p> <p>Repudiation protection (non-repudiation) can in general not be achieved solely through the securing of a transport layer. Since SCM-4 refers to replay protection, our best advice is to mention that. (see: IC.SCM-4) Higher layer mechanisms may provide further non-repudiation.</p> <p>Information disclosure is protected against using encryption (see: Confidentiality capabilities).</p> <p>Denial of service protection is primarily provided by the authentication mechanism which prevents the injection of frames intended for the malicious disruption of networks and devices. Bluetooth's usage of channel hopping also helps against disruptions, even though it's not a security control.</p> <p>Elevation of privilege is not directly relevant at the transport layer further than what is protected against by the</p>	<p>Spoofing is protected against using authentication (see: Authentication Capabilities).</p> <p>Tampering is protected against using Authenticated Encryption (AE) cryptographic algorithm (see: Confidentiality and Replay protection capabilities).</p> <p>Repudiation protection (non-repudiation) can in general not be achieved solely through the securing of a transport layer. Since SCM-4 refers to replay protection, our best advice is to mention that. (see: IC.SCM-4) Higher layer mechanisms may provide further non-repudiation.</p> <p>Information disclosure is protected against using encryption (see: Confidentiality capabilities).</p> <p>Denial of service protection is primarily provided by the authentication mechanism which prevents the injection of frames intended for the malicious disruption of networks and devices. Bluetooth's usage of channel hopping also helps against disruptions, even though it's not a security control.</p> <p>Elevation of privilege is not directly relevant at the transport layer further than what is protected against by the spoofing and tampering countermeasures.</p>	<i>(same as second column)</i>	<i>(same as second column)</i>

	spoofing and tampering countermeasures.			
--	---	--	--	--

- (1) All application-specific protocols are a concern of the integrator.
(2) Depends on host implementation and configuration.
(3) Capabilities can be used to fulfil security objectives (E.Info.SCM-1.SCM.SecObjectives).
The capabilities are also separately described in the E.Info.SCM-X.SCM.Capabilities fields.

4.2.2.5 [RLM] Resilience mechanism

The standard is very vague on describing the exact type(s) of DoS attacks that are of concern, but in general every networking stack will manage its resources in a manner consistent with the goal of recovering from such attacks. For the stream of data which is output from the radio module and consumed by the host product the latter must ensure that resources are well managed so that at the end of a DoS attack the host product recovers. Techniques such as back pressure, limited buffer sizes, and load shedding may be of use.

4.2.2.6 [NMM] Network monitoring mechanism

The module is not a network equipment in and of itself but can be used to build devices which classify as such. Network monitoring mechanisms must be built by the integrator when building network equipment.

4.2.2.7 [TCM] Traffic control mechanism

The module is not a network equipment in and of itself but can be used to build devices which classify as such. Traffic control mechanisms must be built by the integrator when building network equipment.

4.2.2.8 [CCK] Confidential cryptographic keys

When integrating a radio module, you need to consider this requirement in the context of the control that you have over relevant confidential cryptographic keys, i.e. for the mechanisms as defined in the standard; ACM, AUM, SCM, SUM or SSM. Note that this requirement also only relates to confidential (secret) keys, which typically are those used for symmetric encryption, endpoint authentication, or signature creation. Signature verification keys, as a counterexample, are typically not confidential.

This requirement will be described as it applies to the various mechanisms.

Confidential keys for software updates (SUM)

For the software update mechanism (SUM), if the radio module manufacturer does not already offer for example a signature scheme based on a sufficiently strong cryptographic scheme, then an integrator may need to implement either a cryptographically protected communication mechanism or a signature mechanism for the delivery of authentic software updates. When utilizing a software signature scheme, then in the host product only the signature verification key would typically reside, which is not confidential. Such a key would not fall under this requirement. Similarly for a protected communication mechanism for fetching software updates, the remote endpoint would be authenticated based on public key material. The local endpoint (host product) would typically not have a need to authenticate itself.

Hence, for software updates, the CCK requirement is likely not relevant as there are no confidential keys in the host product in typical solutions. The appropriateness of algorithms and keys would be covered by what's written under SUM and CRY-1 requirements.

A software binary might be encrypted by a confidential key, but typically such encryption fulfils a security goal (protection of IP) which is outside of the scope of EN 18031-1 and is thus not covered by the CCK requirement.

Confidential keys for secure communication (SCM)

A confidential key in the context of an SCM would be used within a particular security mode (e.g. EAP-TLS for Wi-Fi, or Secure Connections for Bluetooth). Note that passwords are not considered cryptographic keys in the standards, but any other secret parameter would typically be.

CCK-1 (appropriate keys) can thus be fulfilled by selecting an appropriate security mode.

The requirements that relate to the key generation (CCK-2) or uniqueness (CCK-3) for keys injected into the radio module, e.g. private key for EAP-TLS, are the responsibility of the integrator. Keys not injected, e.g. bonding keys created during Bluetooth pairing, are the responsibility of the radio module firmware (e.g. u-connectXpress firmware) or host driver, depending on module type and technology.

Refer to the SCM section for help with understanding the cybersecurity capabilities of the different technologies in various configurations.

Confidential keys for authentication (AUM)

Within the context of a radio module this relates to the authentication that exists as part of an SCM. There are no other authentication mechanisms. The same advice from the previous section applies.

See also the argument relating to the conflation of ACM/AUM in the earlier section.

Confidential keys for secure storage (SSM)

The integrator of a radio module is not responsible for any confidential keys which may be used to implement a secure storage mechanism in the radio module, i.e. where the storage mechanism itself uses encryption or other cryptographic techniques. That storage mechanism in turn can be used to store other confidential parameters like private keys or passwords, as injected by the integrator. Storing such assets using the capabilities provided by u-connectXpress modules ensures conformity with EN 18031-1.

4.2.2.9 [GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities

This requirement must be interpreted in conjunction with the requirement for a software update mechanism (SUM). Since vulnerabilities can be discovered at any time, it is crucial that the software can be updated to patch them. Having such an update mechanism which functions in-field is a catch all solution which ensures that module firmware always can be patched. Update mechanisms which only exist earlier in the supply and production chain will limit the capabilities. For modules with u-connectXpress firmware u-blox publishes firmware updates online.

4.2.2.10 [GEC-2] Limit exposure of services via related network interfaces

This requirement shall be interpreted in the context of the wireless network interfaces and related services. None of them are enabled per default and hence this requirement is not directly applicable to u-blox radio modules. The module integrator has full control of which interfaces and services they enable in the host product.

4.2.2.11 [GEC-3] Configuration of optional services and the related exposed network interfaces

This requirement shall be interpreted in the context of the wireless network interfaces and related services. None of them are enabled per default (see GEC-2). Indeed however every service which can be enabled can also be disabled. This is fully in control of the module integrator and the requirement can thus be fulfilled by exposing sufficient control also in the host product.

4.2.2.12 [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces

NOTE: This requirement is not strictly required for conformity. See Annex ZA in the EN 18031-1 standard.

This requirement shall be interpreted in the context of the wireless network interfaces and related services. Similarly as for GEC-3 the module integrator is in full control of exposed services and the documentation for them. Refer to the product specific manuals for detailed information.

4.2.2.13 [GEC-5] No unnecessary external interfaces

This requirement shall primarily be interpreted in the context of the wireless network interface (i.e. antenna) and related network functions (e.g. Wi-Fi) in the intended usage. Such an interface becomes external only when enabled, since it's wireless and thus reaches through enclosures, regardless of the antenna being internal or external.

Internal physical interfaces are typically not expected to be externally exposed in the intended usage, but the integrator remains in full control of the design and can use product specific documentation and support services to assess the impact of exposing internal interfaces.

4.2.2.14 [GEC-6] Input validation

Whereas physical interfaces on a radio module are not available on the host product unless they've been explicitly made available by the integrator, a wireless interface is available as soon as it's been enabled. A wireless signal reaches through any enclosures and the input must thus be validated.

However, it is important to keep in mind what is and isn't validated at various points in a data communication path. The wireless input first reaches the wireless communications stack, but it can only parse the general structure of the frames and packets, e.g. headers and checksums. The application payload itself cannot be validated at this point and that responsibility could land for example on a host CPU.

4.2.2.15 [CRY-1] Best practice cryptography

Applicable to SCMs and corresponding AUMs for radio modules and thus indirectly analyzed, since the cryptography is mandated by the respective technology standards (e.g. IEEE 802-11i). The cryptographic algorithms and protocols used are decided by the technology standards in conjunction with the configuration.

It is important to note that the concept of a best practice often is subjective, although there are certain norms that have been evolved in various domains and it is important to make an application-specific analysis of the suitability of cryptographic methods. The standard (EN 18031-1) attempted to provide guidance in a dedicated section but note that the usage of this section was restricted during harmonization, meaning that it cannot be used normatively for the presumption of conformity. This leaves the adopters of the standard with very little authoritative guidance in the standard as to what constitutes a best practice.

Integrators of u-blox radio modules are encouraged to study the particular modules that they integrate and follow the best practices available, e.g. in our application notes on Wi-Fi and Bluetooth security, standards bodies (e.g. Wi-Fi alliance, BT-SIG, NIST) and expert bodies (e.g. SOG-IS, OWASP) if so deemed required.

For specific guidance related to the cryptographic methods used in SCM or AUM please see the respective sections. A deep dive into the specific underlying algorithms (e.g. AES) is not deemed necessary here as the options within each respective technology is mandated as well as limited by its standards. Choosing best practice methods within the respective technology translates to the best available option when using that technology. The standard also allows justifying the usage of non-best-practices for reasons of interoperability. A radio module can be seen as a toolbox from which a suitable best practice must be chosen.

Appendix

A Terminology

Term	Definition
CRA	Cyber Resilience Act
DoC	Declaration of Conformity
E.Info	An EN 18031 term referring to documentation about the device under test (DUT) – used to support the assessment.
Host product	The product into which a radio module is integrated.
Integrator	The one integrating a radio module into a host product.
Radio module	u-blox compact unit providing wireless communications technology. Not the same as the legislative definition of a radio module in the RED, radio equipment, or other similar terms. In this document u-blox exclusively discusses within the context of its own products.
RED	Radio Equipment Directive
RED-DA	RED Delegated Act
REDCYBER	Colloquial reference to the RED cyber articles 3.3 (d), (e), and (f) activated through the RED Delegated Act (RED-DA).

Table 1: Explanation of the abbreviations and terms used

B Common misconceptions

B.1 The cyber articles apply to all radio modules

There are a wide variety of radio modules and the determination of whether or not any of the cyber articles apply is a process owned by the module manufacturer and overseen by the market authorities. The arguments upon which such a determination rests are the regulatory texts and standards, but also opinions and statements shared in other forums like the REDCA, discussions with Notified Bodies, EU conferences, etc. Even if such statements perhaps cannot be directly referenced in e.g. a Risk Assessment, they shape the common understanding in the EU common market.

B.2 Products already on the market

There is a common misunderstanding around products already placed on the market. The misunderstanding stems from the meaning of the term ‘placing on the market’ itself. It must be understood and interpreted only as defined and used within the EU New Legislative Framework (NFL). Fully repeating what is stated there is out of scope of this document, but we want to highlight that both old and new products are generally in scope if they continue to be sold on the EU common market. Please refer to the EU Blue Guide^[3] for further information.

B.3 Integrator can only use modules with a DoC


There is no obligation for a host product manufacturer to only consider modules that have been certified or that have a DoC encompassing the cyber articles. The legal obligations for component and host product manufacturers are disconnected and each entity is solitarily responsible for ensuring a cybersecure end result. Where u-blox feasibly can contribute to the cybersecurity in the supply chain it will do so, either through direct assessment accordingly with EN 18031 or through the support of our customers.

B.4 Bluetooth applicability

This topic has been much debated and there are unfortunately a lot of different opinions out there. The scope of 3.3 (d) is very clear in that it applies to devices which operate protocols which are able to communicate themselves with the Internet. There is no consensus on the exact interpretation and every manufacturer must make its own determination. Note though that a device which is in scope due to other reasons might still need the Bluetooth functionality assessed against the standards, where applicable. Bluetooth as a technology cannot be dismissed for applicability as a whole.

Related documentation

- [1] [RED Delegated Regulation 2022/30 \(REDCYBER\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0030)
(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0030)
- [2] [Implementing Decision \(EU\) 2025/138 of 28 January 2025](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500138) (OJEU citation)
(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500138)
- [3] [The 'Blue Guide' on the implementation of EU product rules 2022](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC)
(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC)
- [4] [u-connectXpress Wi-Fi Security Application Note, UBX-20012830](https://content.u-blox.com/sites/default/files/u-connectXpress-Wi-Fi-Security_AppNote_UBX-20012830.pdf)
(https://content.u-blox.com/sites/default/files/u-connectXpress-Wi-Fi-Security_AppNote_UBX-20012830.pdf)
- [5] [u-connectXpress Bluetooth Security Application Note, UBX-16022676](https://content.u-blox.com/sites/default/files/u-connectXpress-BluetoothSecurity_AppNote_UBX-16022676.pdf)
(https://content.u-blox.com/sites/default/files/u-connectXpress-BluetoothSecurity_AppNote_UBX-16022676.pdf)
- [6] [u-blox RED DA statement on short-range radio products, UBXDOC-1905400739-29616](https://content.u-blox.com/sites/default/files/documents/u-blox_RED-DA-Statement_SHO_UBXDOC-1905400739-29616_C1.pdf)
(https://content.u-blox.com/sites/default/files/documents/u-blox_RED-DA-Statement_SHO_UBXDOC-1905400739-29616_C1.pdf)

 For product change notifications and regular updates of u-blox documentation, register on our website, www.u-blox.com.

Revision history

Revision	Date	Name	Comments
R01	09-Jun-2025	mfur	Initial release
R02	07-July-2025	hvig	Added table in section 3
R03	12-Sept-2025	hvig	Added Reference to SHO statement and removed duplicate information

Contact

u-blox AG

Address: Zürcherstrasse 68
8800 Thalwil
Switzerland

For further support and contact information, visit us at www.u-blox.com/support.