Willkommen

Radio Equipment Directive
Cybersecurity

Dietmar Frei , April.2024

AGENDA

Implementation of the RED requirements Art. 3.3

Risk assessment

- Working in groups

EN 18031-X

Security/Network Asset

- Working in groups

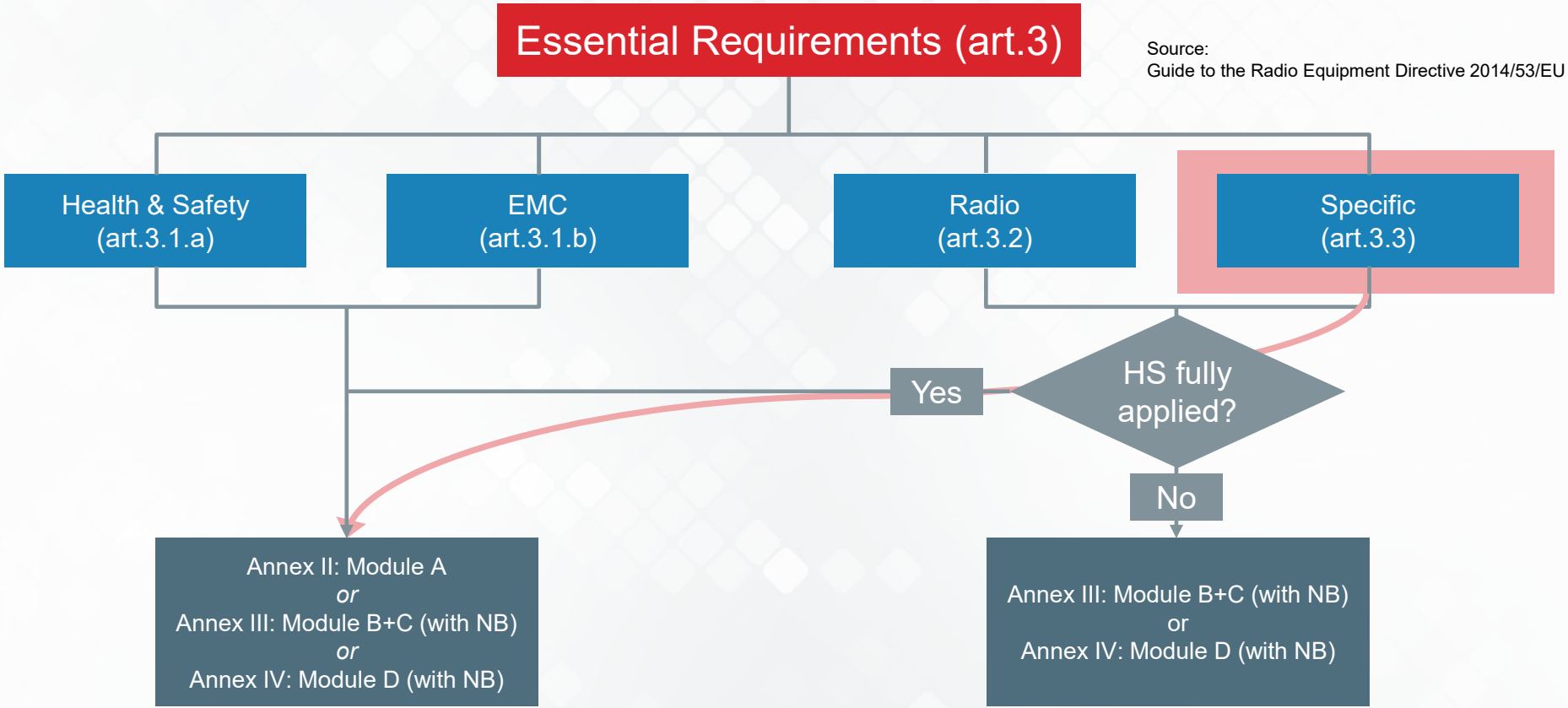
Applicability of access control mechanisms

- Working in groups

Appropriate access Access control mechanism

Summary

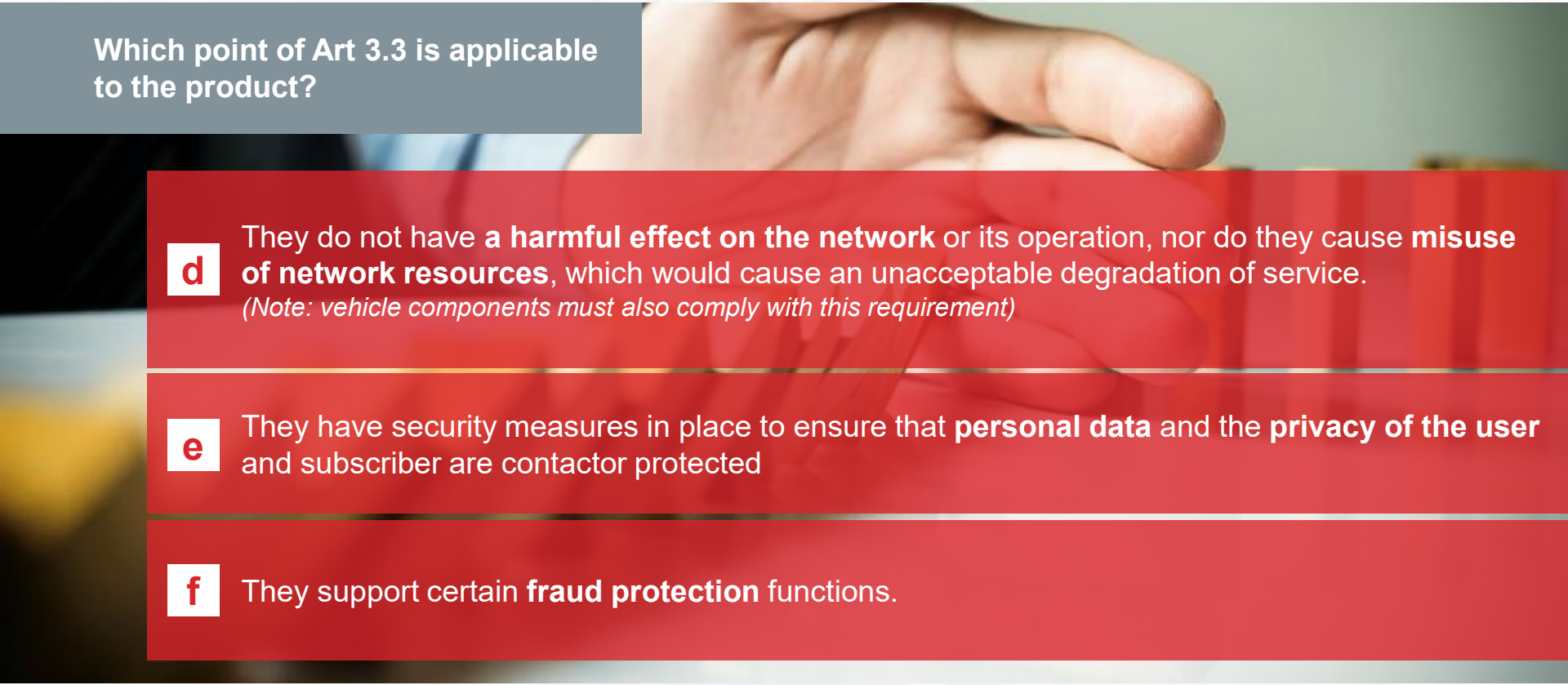
RED Essential requirements Conformity assessment in item 17



Source:
Guide to the Radio Equipment Directive 2014/53/EU

First step risk assessment

Which point of Art 3.3 is applicable to the product?

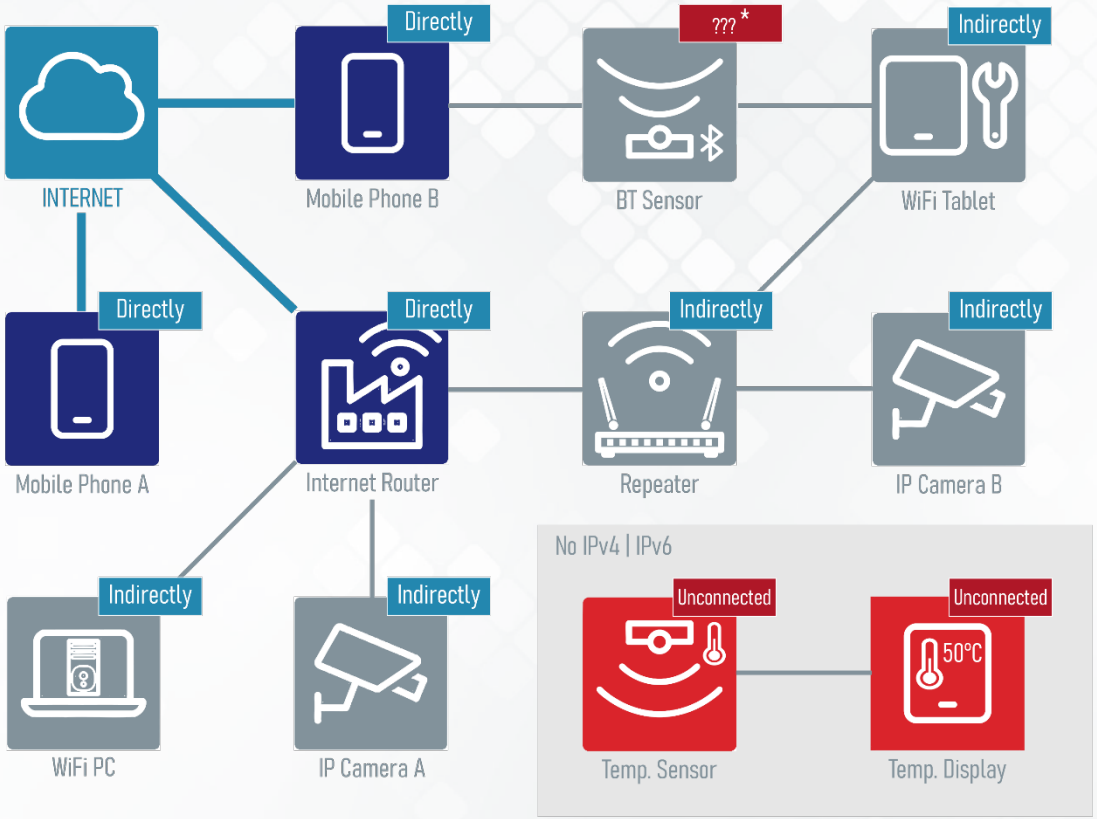


d They do not have **a harmful effect on the network** or its operation, nor do they cause **misuse of network resources**, which would cause an unacceptable degradation of service.
(Note: vehicle components must also comply with this requirement)

e They have security measures in place to ensure that **personal data** and the **privacy of the user** and subscriber are contactor protected

f They support certain **fraud protection** functions.

Directly or indirectly connected devices according to RED DA



*depends on BT Version / Implementation

Example 1
Fictitious product radiotelephony

Which point of Art 3.3 is applicable to the product?

d **Effects** on network / operation?
Misuse of network resources?

e **Personal data** available in the product ?

f Fraud regarding financial data?

Example 1
Fictitious product radiotelephony

Radiotelephone **without internet connection** and **personal data** is **not to be considered** according to RED Art. 3.3 d,e,f.

This assessment must be documented in the risk assessment.

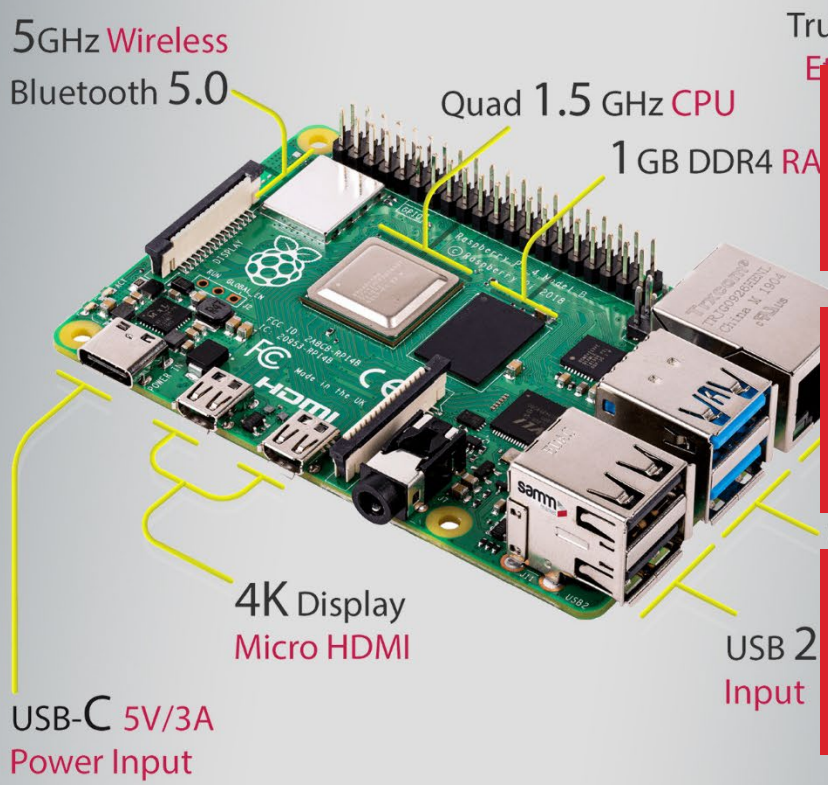
d **Effects** on network / operation?
Misuse of network resources?
No.

e **Personal data** available in the product ?
No.

f Fraud regarding financial data?
No.

→ Island solution

Example 2
Product Raspberry Pi

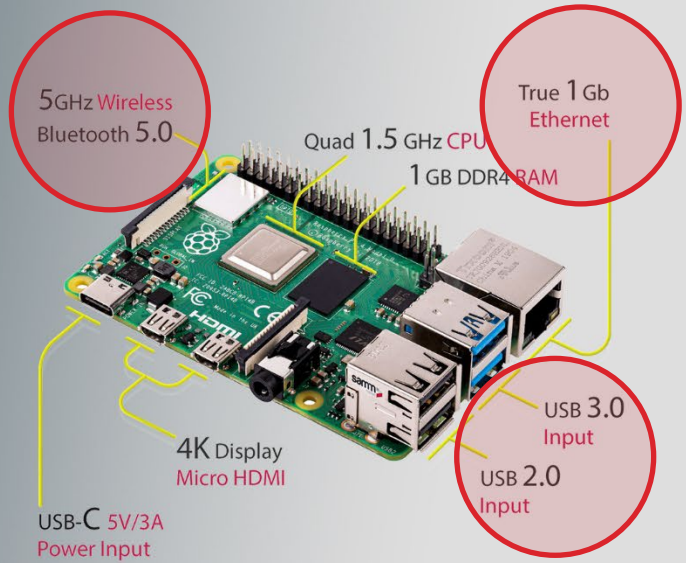


d **Effects** on network / operation?
Misuse of network resources?

e **Personal data** available in the product ?

f Fraud regarding financial data?

Example 2
Product Raspberry Pi



Family approval depends on the **model**.
Type requirement for family: RED Art. 3.1a, 3.1.b, 3.2, 3.3 identical

d **Effects** on network / operation? **Misuse** of network resources?

Possible impact on the grid.
RED Art. 3.3 d must be taken into account

e **Personal data** available in the product ?

RED Art. 3.3 e must be taken into account if the application permits the storage of **personal data**.

f Fraud regarding financial data?

RED Art. 3.3 f must be taken into account if the application allows the storage of **financial data**.

Example risk assessment:
Essential Requirements for RED ART. 3.3 d,e,f || Not applicable

Requirements	Specification/conditons	Compliance verfied by
(d) Radio equipment does not **harm the network** or its functioning nor misuses network resources, thereby causing an unacceptable degradation 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**	d) **Not applicable**: The DUT is only able to communicate via the following interfaces and protocols: 1. Bluetooth Low Energy 4.0: Using for first installations, updates and process data communication. The communication is done using protocols which does not exchange data with the internet either directly or of an intermediate equipment. The DUT is not capable itself to communicate over the internet. 2. profibus: Profibus is used to monitor and control the connected devices. The communication is done using protocols which does not exchange data with the internet either directly or of an intermediate equipment. The DUT is not capable itself to communicate over the internet. e) **Not applicable**: The DUT does not pose a risk to the user's privacy, as it does not store or process any personal data. f) **Not applicable**: The DUT cannot pose a risk of fraud because it does not store or process financial data.	

Example risk assessment:
Essential Requirements for RED Art 3.3 d,e,f || Applicable

Requirements	Specification/conditons	Compliance verfied by
(d) Radio equipment does not harm the network or its functioning nor misuses network resources, thereby causing an unacceptable degradation of service	**d) Applicable:** The DUT is communicated via the following interfaces and protocols: 1. WLAN 802.11b: Using for first installations, updates and process data communication. The communication is done via TCP/IP.	EN18031-1
e) Radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected	**e) Not applicable:** The DUT does not pose a risk to the user's privacy, as it does not store or process any personal data.	
(f) Radio equipment supports certain features ensuring protection from fraud	**f) Not applicable:** The DUT cannot pose a risk of fraud because it does not store or process financial data.	

Quintessence risk assessment

Island solution possible

Family approvals are depending on the model

RISK ASSESSMENT

Indirect connections to the network

Does the device speak "Internet table"?

AGENDA

Implementation of the RED requirements Art. 3.3

Risk assessment

- Working in groups

EN 18031-X

Security/Network Asset

- Working in groups

Applicability of access control mechanisms

- Working in groups

Appropriate access Access control mechanism

Summary

Standard EN 18031-X

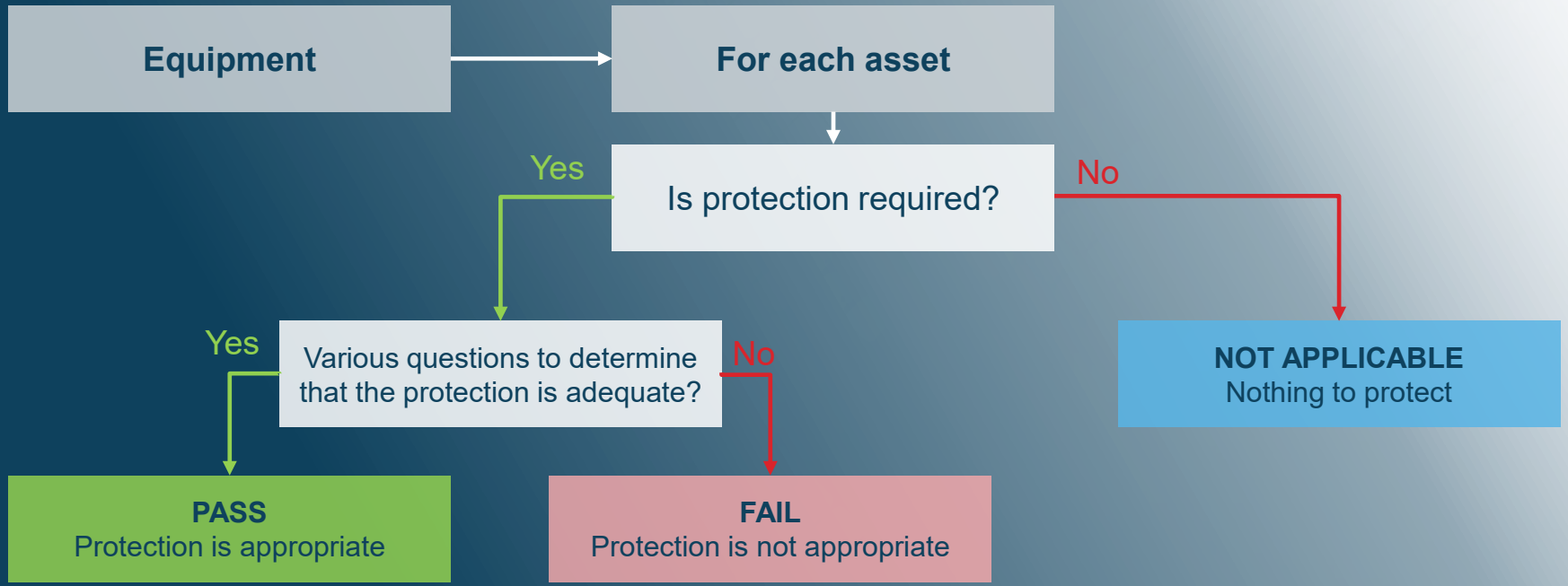
- To ensure that the requirements can be harmonized, assets have been introduced as the main targets to which the requirements are to be applied.

Essential requirements	EN 18031-1 RED 3.3 (d)	EN 18031-2 RED 3.3 (e)	EN 18031-3 RED 3.3 (f)
Security asset	☑	☑	☑
Network asset	☑	☒	☒
Privacy asset	☒	☑	☒
Financial asset	☒	☒	☑

Requirements of EN 18031-X

Abbreviation	Mechanism	EN 18031-1	EN 18031-2	EN 18031-3
ACM	Access control mechanism	☑	☑	☑
AUM	Mechanism for authentication	☑	☑	☑
SUM	Secure update mechanism	☑	☑	☑
SSM	Secure storage mechanism	☑	☑	☑
SCM	Mechanism for secure communication	☑	☑	☑
RLM	Fail-safe mechanism	☑	☒	☒
LGM	Mechanism for logging	☒	☑	☑
NMM	Network monitoring mechanism	☑	☒	☒
DLM	Mechanism for deleting data	☒	☑	☒
TCM	Traffic control mechanism	☑	☒	☒
UNM	Mechanism for notifying users	☒	☑	☒
CCK	Confidential cryptographic keys	☑	☑	☑
GEC	General equipment features	☑	☑	☑
CRY	Cryptography	☑	☑	☑

Decision Trees



Decision trees

Decision trees help to assess the requirements in terms of:

- Applicability and appropriateness

The decision trees are to be applied to each security/network asset

- (Username, Password, PIN, Network configuration, WLAN Access.)

Not included in the valuation:

- **Functional protocol tests**
- **Pen tests.**
- **multimedia** or **highly targeted/sophisticated attacks** and thus the invasive **analysis of hardware and software modules**.

The **test scenarios (TSOs)** are aimed at a **basic effort** in terms of **test depth** and **test scope** in accordance with **the basic security level.**