EN 18031 系列标准适用范围及检测服务

RED（Radio Equipment Directive）即无线电设备指令（2014/53/EU），是欧盟针对无线产品制定的强制性符合性指令，明确要求进入欧盟市场的无线产品需通过认证并加贴 CE 标志。RED DA 指令中的“DA”为 Directive Amendment（指令修订），重点聚焦网络安全领域，其中第 3.3 (d)(e)(f) 条作为核心条款，对无线产品网络安全设定最低标准，并自 2025 年 8 月 1 日起强制执行。该条款的实施，标志着未满足网络安全要求的无线产品将被禁止在欧盟境内销售或流通。

EN 18031 标准分为 EN 18031-1/2/3 三部分，分别对应 RED 指令中的要求。

法规	条款	对应标准
2022/30/EU	Article 3.3(d)网络安全	EN-18031-1
	Article 3.3(e)个人隐私	EN-18031-2
	Article 3.3(f)防止欺诈	EN-18031-3

一、EN 18031 标准体系解析

1. EN 18031-1

适用于任何能够通过互联网进行自我通信的无线电设备，无论它是直接通信还是通过其他设备(互联网连接的无线电设备)。

- 手机、平板电脑
- Wi-Fi 路由器和网关联网空调、
- 冰箱和其他家用电器
- 智能电视/电视盒和 3G/4G/5G 设备所有具有 Wi-Fi 通信功能的设备
- 车载联网组件
- 能源系统中的电源转换器

2. EN 18031-2

适用于处理个人数据、通信数据或直接定位数据的无线电设备，即互联网连接的无线电设备、儿童护理无线电

设备、玩具无线电设备和可穿戴无线电设备。

- 蓝牙连接手机、耳机或 Boombox
- 智能手表和其他可移动设备
- 智能传感器、空气净化器、吸尘器
- 婴儿监视器和 3G/4G/5G 设备
- 车载联网组件
- GPS 跟踪设备

3. EN 18031-3

适用于任何互联网连接的无线电设备，如果该设备使持有人或用户能够进行金钱、货币价值或虚拟货币的转移。

- POS 机、ATM 机
- 支持任何类型转账的设备

豁免范围：

1. 不适用 MDR 法规范围内的医疗器械设备。

2. 不适用 Regulation (EU)2018/1139、Regulation(EU) 2019/2144。

3. 不适用 Directive(EU)2019/520 法规范围内的航空或道路交通相关设备。

二、测试评估

EN18031 各子标准和安全需求对应表			
Requirement	EN18031-1	EN18031-2	EN18031-3
[ACM]Access control mechanism	√	√	√
[AUM]Authentication mechanism	√	√	√
[SUM] Secure update mechanism	√	√	√
[SSM]Secure storage mechanism	√	√	√
[SCM]Secure communication mechanism	√	√	√
[LGM] Logging mechanism	-	√	√
[DLM] Deletion mechanism	-	√	-
[UNM]User notificiation mechanism	-	√	-
[RLM]Resilience mechanism	√	-	-
[NMM] Network monitoring mechanism	√	-	-

[TCM]Traffic control mechanism	√	-	-
[CCK] Confidential cryptographic keys	√	√	√
[GEC]General equipment capabilities	√	√	√
[CRY] Cryptography	√	√	√

四类资产定义

保护资产不仅仅是保护设备存储和传输或以其他方式处理的特定数据，还包括保护设备使用的功能和这些功能的配置。

资产类型	数据&信息(配置)	配置(参数)	功能
安全资产	敏感安全参数	机密安全参数	安全功能
网络资产	敏感网络功能配置	机密网络功能配备	网络功能
隐私资产	个人信息	隐私功能配置	隐私功能
金融资产	金融数据	金融功能配置	金融功能

基本要求	3.3.d	3.3.e	3.3.f
安全资产	√	√	√
网络资产	√		
基本要求		√	
金融资产			√

安全评估：

概念评估: 对可访问的每个资产进行决策树判断

功能完整性评估: 从产品功能层面评估是否存在漏测资产

功能充分性评估:确认所有资产符合标准要求

三、自我声明

只要产品不触发以下限制条款，制造商可通过自声明证明合规：

1. 无默认密码漏洞

设备必须强制用户首次使用时设置密码（或生物识别等替代方案），不允许"无密码使用"模式。

示例：智能路由器要求用户首次联网必须修改默认密码 → 可自声明。

2. 不涉及高风险场景

非儿童设备：产品未涉及儿童隐私数据（如普通智能手环不收集儿童 GPS 数据）。

非金融设备：设备不处理支付、虚拟货币交易（如普通蓝牙音箱）。

3. 安全更新机制完善

固件更新需满足标准中的多重防护（如数字签名+防回滚），且不依赖单一措施。

示例：智能摄像头支持强制加密更新 → 可自声明。

四、标准实施的重要意义

1. 提升设备网络安全水平：通过严格规范访问控制、身份验证和安全更新等机制，有效提升无线产品网络安全性能，保护用户隐私与财产安全。

2. 推动产业升级：企业虽面临短期成本增加，但认证产品市场认可度更高，促使企业加大研发投入，推动行业安全标准提升，构建完善管理体系。

3. 确保欧盟市场合规准入：通过遵循标准进行产品研发与生产，制造商能够顺利通过欧盟市场准入审核，避免因合规问题导致的贸易壁垒和经济损失。

4. 规范市场秩序：统一行业评估准则，帮助认证机构客观认证，监管部门高效管理，减少恶性竞争，净化市场环境。

EN 18031 标准系列作为欧盟在无线电设备网络安全领域的重要举措，通过完善的标准体系、严格的技术要求和科学的评估机制，为全球无线电设备产业的网络安全发展树立了新的标杆。对于无线电设备制造商而言，积极遵循这一标准，不仅是满足市场准入的需要，更是提升产品竞争力、实现可持续发展的关键所在。随着标准的正式实施，全球无线电设备产业必将迎来网络安全防护水平的全面提升。