

欧盟网络安全法及其协调标准 EN 18031 解读

2025 年 1 月 30 日，欧盟委员会正式将 EN 18031 系列标准列入《欧盟官方公报》(OJ) 的《无线电设备指令》(RED) 协调标准清单，标志着该系列标准成为欧盟境内无线电设备网络安全合规的重要依据。新规将于 2025 年 8 月 1 日起强制实施，无疑对制造商立即采取行动提出了迫在眉睫的要求。

一、新规内容

EN 18031 系列标准分为 EN 18031-1、EN 18031-2、EN 18031-3 三个部分，分别对应 RED 指令第 3 (3) 条款的 (d)、(e)、(f) 要求，涵盖多种无线设备：

1. EN 18031-1: 互联网连接设备的安全基石

聚焦于互联网连接的无线电设备，包括能独立联网通信的智能手机、平板电脑、智能家居设备等，以及需借助网关、手机等中介设备间接联网的产品。此标准主要管制安全资产与网络资产，旨在确保设备连接互联网时，不会损害网络或其功能，避免滥用网络资源致使服务质量下降。

2. EN 18031-2: 数据处理设备的隐私堡垒

适用于处理数据的无线电设备，如互联网连接设备、儿童护理设备、玩具设备和可穿戴设备等。该标准着重关注隐私保护，要求设备建立起访问控制、数据加密等隐私保护机制，以此保障用户个人数据、交通数据或位置数据的安全。

3. EN 18031-3: 金融交易设备的安全盾牌

针对处理虚拟货币或货币价值的互联网连接无线电设备，像支持虚拟货币交易的支付终端、加密货币硬件钱包等。该标准要求设备具备防止欺诈的功能，例如采用日志记录、软件完整性验证等手段，保障金融交易安全。

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、之前做过 CE 认证的产品，还需要再重新做吗？

1. 需重新认证的情况

- 产品属于 RED 指令新增管控范围

例如：智能手机、智能家居设备、支付终端等需满足网络保护 (3.3d)、隐私保护 (3.3e) 和反欺诈 (3.3f) 要求，必须通过 EN 18031 测试并更新 CE-RED 证书。

- 原有 CE-RED 认证未覆盖网络安全条款

若证书未包含 2022 年补充的 RED-DA 要求（如设备默认密码防护、金融交易安全机制），需补充测试。

2. 无需重新认证的情况

- 产品不属于 RED 指令新增范围

例如：仅需符合 EMC（电磁兼容）或 LVD（低电压指令）的普通电器（如电风扇、灯具），若标准未更新且设计无变更，原证书继续有效。

- 认证仍在有效期内且标准未变更

CE 证书默认有效期为 5 年，若产品未改动且指令未更新，无需重复认证。

三、必须第三方认证且需要 NB 证书的情况：

1. 允许用户不设密码

示例：手机允许“无密码解锁”功能 → 需第三方认证。

2. 涉及儿童或隐私敏感设备

产品为儿童玩具、婴儿监视器或可穿戴设备，且未强制家长控制权限。

示例：儿童智能手表未内置远程禁用摄像头功能 → 需第三方认证。

3. 金融交易相关设备

涉及支付、虚拟货币存储（如 POS 机、硬件钱包），且仅依赖单一安全措施。

示例：加密货币硬件钱包仅用数字签名保护密钥 → 需第三方认证。

