

## TÜV南德解读欧盟无线电设备网络安全要求指南 (RED:2014/53/EU)

北京2025年2月24日 /美通社/ -- 在当今数字化时代，无线电设备在我们的生活和工作中扮演着愈发重要的角色。随着网络安全威胁的不断增加，保障无线电设备的网络安全已成为当务之急。欧盟无线电设备指令 (RED:2014/53/EU) 及其补充授权法规 (2022/30/EU) 要求：自 2025 年 8 月 1 日起，将强制实施 RED 指令 Article 3.3(d)、(e)、(f) 网络安全要求，这一举措旨在显著提升欧盟市场上无线电设备的网络安全防护能力，全方位保护用户数据与隐私，并有效防范金融欺诈风险。为助企业更好地理解无线电设备网络安全合规性要求，TÜV南德意志集团（以下简称“TÜV南德”）对其协调标准进行解读，确保无线电设备符合欧盟网络安全监管要求。

### 一、主要网络安全要求解读

1. Article 3.3(d) 网络安全保护：无线电设备的设计与运行应确保不对网络基础设施及其功能完整性造成任何损害，同时严格限制网络资源的非授权使用，以避免引发服务质量的显著下降或中断。
2. Article 3.3(e) 个人数据和隐私保护：在这个数据即资产的时代，个人数据和隐私的保护至关重要。无线电设备应集成先进的数据加密与访问控制机制，为用户及订阅者提供全面的个人数据保护方案。切实确保用户个人数据和隐私得到充分保护，防止数据泄露等安全事件的发生。
3. Article 3.3(f) 金融欺诈防范：为了保障用户的财产安全，无线电设备须配备完善的安全防护功能，有效识别并阻止潜在的欺诈活动，从而防范各类金融欺诈行为。无论是在移动支付还是其他涉及金融交易的场景中，设备都将成为防范欺诈的重要防线。

### 二、适用范围广泛

网络安全要求的适用范围：直接联网的无线电设备以及间接联网的无线电设备。无线通讯方式包括但不限于常见的 WIFI、蓝牙、ZigBee、4G/5G、LoRa 等多种技术。这也就意味着，几乎所有具备联网功能的无线电设备都需要符合网络安全要求，从我们日常使用的智能手机、智能手表，到工业领域的无线电通讯设备等，都在监管范围之内。



图示：直接联网的无线电设备



图示：间接联网的无线电设备

### 三、RED:2014/53/EU 协调标准解析

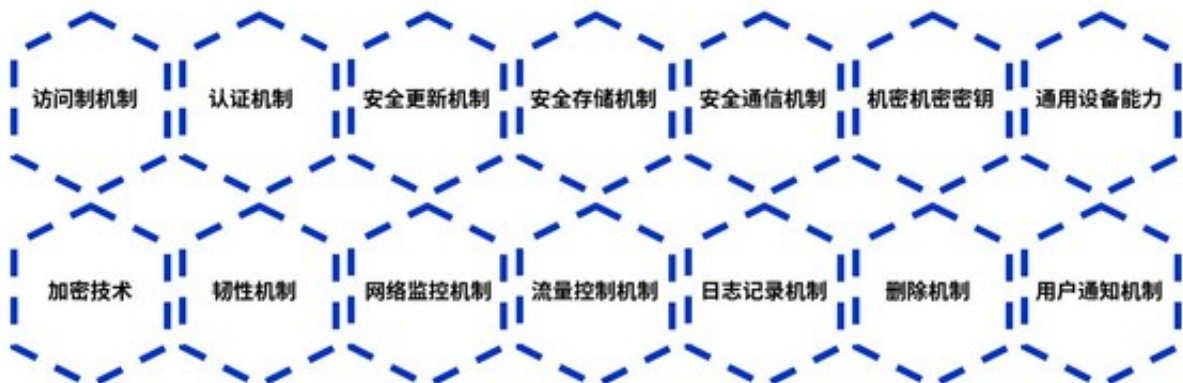
1. EN18031-1:2024标准对应Article 3.3(d)网络安全要求，适用于连接互联网的无线电设备。主要聚焦于无线电设备的

基本网络安全要求。其中包括对安全资产与风险、网络资产与风险的全面评估，以及对弹性机制、网络监控机制、认证机制等多个关键评估项目的考量，为设备的网络安全提供了基础保障。

2.EN18031-2:2024标准对应Article 3.3(e)网络安全要求，适用于处理数据隐私、流量或位置信息的无线电设备，包含儿童保育、儿童监护的无线电设备、可穿戴无线电设备等多种类型。主要聚焦于无线电设备的数据处理安全，特别针对上述设备的数据隐私与风险评估，以及访问控制机制、日志记录机制、删除机制、用户通知机制等评估项目，充分保护用户数据隐私安全。

3. EN18031-3:2024标准对应Article 3.3(f)网络安全要求，适用于处理金融价值转移的无线电设备。主要聚焦于连接互联网处理货币价值的无线电设备的网络安全，特别针对上述设备安全资产与风险、金融资产与风险的评估，以及事件追踪机制和软件可信性等评估项目，有力地保障金融交易相关设备的安全性。

| 标准编号           | 核心关注领域 | 关键技术指标                      | 典型应用场景           |
|----------------|--------|-----------------------------|------------------|
| EN18031-1:2024 | 基础网络安全 | 安全通讯机制<br>访问控制机制<br>加密算法合规性 | 智能家居<br>工业路由器    |
| EN18031-2:2024 | 数据隐私保护 | 日志记录机制<br>用户通知机制<br>地理位置模糊化 | 儿童智能手表<br>健康监测设备 |
| EN18031-3:2024 | 金融交易安全 | 网络监控机制<br>安全更新机制<br>交易追溯能力  | 移动支付终端<br>加密货币钱包 |



图示：EN18031系列标准的网络安全要求

TÜV南德作为全球知名的技术服务机构，在无线电通讯领域技术深厚，拥有丰富的项目经验，可依据欧盟无线电设备指令（RED）及 EN18031 等标准，全面测试各类联网无线电设备，涵盖基础安全、隐私保护、欺诈防范等，以发现潜在风险。TÜV南德遵循严格流程，对符合要求的产品评估认证并颁发证书，为产品进入欧盟市场提供权威资质，保障消费者预期。此外，TÜV南德还提供知识服务，协助企业解读法规标准、制定合规策略计划，并通过培训提升企业技术团队能力，确保产品全生命周期合规。

网络安全已成为数字经济稳健发展的基石，对企业而言，强化网络安全防护可降低运营风险，提升竞争力，拓展国际市场；从行业层面看，网络安全水平的提升可规范市场秩序，营造公平的竞争环境，激励企业加大研发创新投入，从而促进行业技术的迭代与升级。TÜV南德作为行业的重要参与者，将持续为企业赋能，构建可信赖的物联网生态系统，共同塑造安全互联的未来图景。

文中所列标准详情，可通过以下链接进行查询：

- 2014/53/EU     [EUR-Lex - 02014L0053-20241228 - EN - EUR-Lex](#)
- 2022/30/EU   [EUR-Lex - 02022R0030-20231027 - EN - EUR-Lex](#)
- EN 18031-1:2024   [CEN - CEN/CLC/JTC.13](#)
- EN 18031-2:2024   [CEN - CEN/CLC/JTC.13](#)
- EN 18031-3:2024   [CEN - CEN/CLC/JTC.13](#)

原文地址：<http://www.china-nengyuan.com/news/221223.html>