Electronic Design

By RACHEL MENDA-SHABAT,
Director of Certification, Winbond

Meeting EU's 2025 Radio Equipment Directive (RED) Cybersecurity Standards

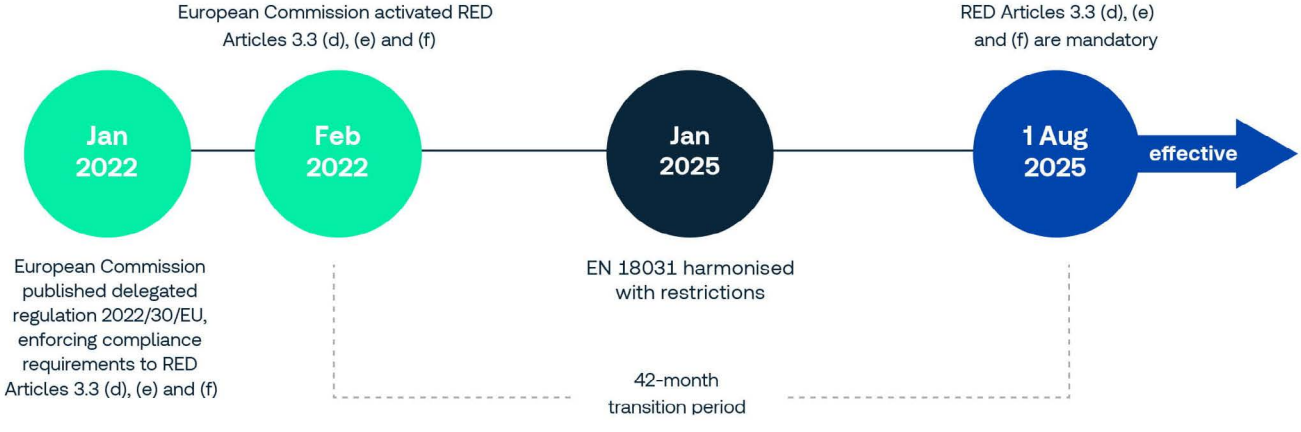
Trusted memory, which is at the core of complying with EU RED Cybersecurity requirements, plays a pivotal role in enabling secure boot, encrypted storage, and authenticated firmware updates.

As connected devices proliferate across IoT, automotive, and industrial markets, ensuring cybersecurity at the hardware level has become essential. The European Union's RED (Radio Equipment Directive) cybersecurity requirements mandate provides robust protections against data breaches, unauthorized access, and malicious firmware manipulation.

At the heart of these requirements lies the integrity of the device's firmware—a core component often stored and updated in flash memory. Secure flash memory plays a pivotal role in meeting RED compliance by enabling authenticated firmware updates, enforcing access controls, and ensuring resilience against tampering or rollback attacks. Without these protections rooted in memory security, connected devices remain vulnerable at their most fundamental layer.

The European Union's RED, particularly its Article 3.3, is at the forefront of ensuring that wireless devices sold within the EU market meet stringent cybersecurity requirements. The industry has a critical demand for secure data storage, resilient software updates, and robust access control mechanisms to address the RED regulations. This is specifically the case with the 2022/30/EU delegated regulation and the introduction of the EN 18031: 2024 common security requirements for radio equipment set of standards.

Secure flash memory solutions can be an answer to meeting these exacting standards, offering a robust, easy-to-inte-



The timeline to meet EU RED compliance ends in August 2025.

grate solution for manufacturers seeking to achieve compliance with RED cybersecurity requirements. The EN 18031 standards outline key requirements around providing essential features like secure storage, encrypted software updates, and resilience mechanisms.

Adopt or Face Potential Market Exclusion

The European Commission's Radio Equipment Directive (RED) 2014/53/EU establishes the legal framework for placing radio equipment on the EU market. As of January 2022, delegated regulation 2022/30/EU mandates compliance with Article 3.3, covering three critical areas: data protection, fraud prevention, and emergency services access. From August 2025, any non-compliant device will face potential market exclusion *(see figure)*.

The EN 18031: 2024 standards are crucial for ensuring compliance with these new security measures. This includes the protection of personal data, prevention of cyberattacks, and the capacity to securely update software—an essential factor in maintaining device security over time.

Key Security Enhancements Under EN 18031

The EN 18031 standards address several critical areas to ensure comprehensive security throughout the lifecycle of connected devices:

- **Access control:** Devices are required to have mechanisms in place to prevent unauthorized access to security and network assets. This includes the use of remote and local authentication to protect sensitive data.
- **Secure software updates:** A key requirement is the capability to deploy secure software updates that address vulnerabilities and maintain regulatory compliance. This includes ensuring that updates are encrypted, authenticated, and protected against rollback, with support for post-quantum cryptography (PQC), such as the Leighton-Micali Signature (LMS) scheme, which meets NSA CNSA 2.0 standards.
- **Secure storage and communication:** The standards emphasize the importance of robust cryptographic key management and secure storage for safeguarding sensitive data. Compliance requires secure storage systems that adhere to certifications like Common Criteria (CC) and SESIP.

Key Features Needed in Secure Flash Products to Meet Requirements

- **Post-quantum cryptography (PQC):** As cybersecurity evolves, so too must cryptographic techniques, ensuring support for PQC algorithms that protect devices from future quantum computing threats.
- **Secure over-the-air (OTA) updates:** Secure OTA firmware updates are a crucial feature for maintaining device security post-deployment.
- **Resilience mechanisms:** Meeting NIST SP 800-193 requirements for platform resilience ensures that systems can automatically recover from attacks or adverse conditions.
- **Automotive certifications:** Flash memory needs to be designed for high-speed data transfer with Octal SPI to meet automotive standards such as ISO 21434 and ISO 26262, to provide the protection needed for automotive cybersecurity applications.

As cybersecurity regulations change, it's important for manufacturers to future-proof their products. Secure flash memory solutions need to comply with current EN 18031 requirements. However, they must be designed to meet future mandates, such as ETSI EN 303 645, NIST IR 8259A, NIST IR 8425, IEC 62443 and CNSA 2.0, which becomes mandatory in 2025.

By incorporating secure memory solutions into their designs, manufacturers can ensure compliance with the EU's CE marking requirements and avoid penalties, market exclusion, or damage to their reputation. Providing a certified supply chain and security certifications (Common Criteria, SESIP Certified Secure Storage, FIPS 140-3) will offer further assurance of commitment to robust, secure product development.

The Future of Secure Flash

Secure flash memory like Winbond's W77Q and W77T families are tailored to meet the demands of the EN 18031 standards, providing manufacturers with a high-performance, drop-in replacement for existing SPI NOR flash solutions. These devices are particularly beneficial for IoT platforms, automotive systems, and industrial applications, where cybersecurity is paramount.

The secure flash devices offer manufacturers a simple path to compliance with the latest cybersecurity standards under the Radio Equipment Directive. Features like secure storage, authenticated software updates, cryptographic key management, and resilience mechanisms help manufacturers not only meet the EN 18031 requirements, but reduce cybersecurity risks and ensure long-term device integrity.

As the August 2025 deadline for mandatory compliance with RED cybersecurity regulations approaches, manufacturers must act now to secure their products and their place in the European market.

Rachel Menda-Shabat has over 20 years of experience in security product development and certification. She is the Director of Certification at Winbond, managing the security certification of Winbond products. She has led several certifications such as Common Criteria, FIPS 140-2, SESIP, PSA, EMVco, and more. Rachel is a member of Eurosmart and the chairwoman of 3S in SoC PP group, an active member of the JIL working group, ISCI-WG1, and involved in worldwide security groups, such as CCUF, GlobalPlatform, and ISO. She holds a Master's degree in Business Administration.