Secure Flash: A Practical Path to Cyber Resilience Act Compliance

In this deep dive, we explore a practical hardware foundation for secure boot, protected storage, authenticated updates, anti-rollback, recovery, and compliance evidence.

In this article, we'll expand on an All About Circuits news article by digging deeper into the details of Winbond's new conformance and integration Kit announced last week ahead of Electronica. We'll also examine in detail how Winbond's Secure Flash technology provides a practical way to ensure compliance with the Cyber Resilience Act (CRA).

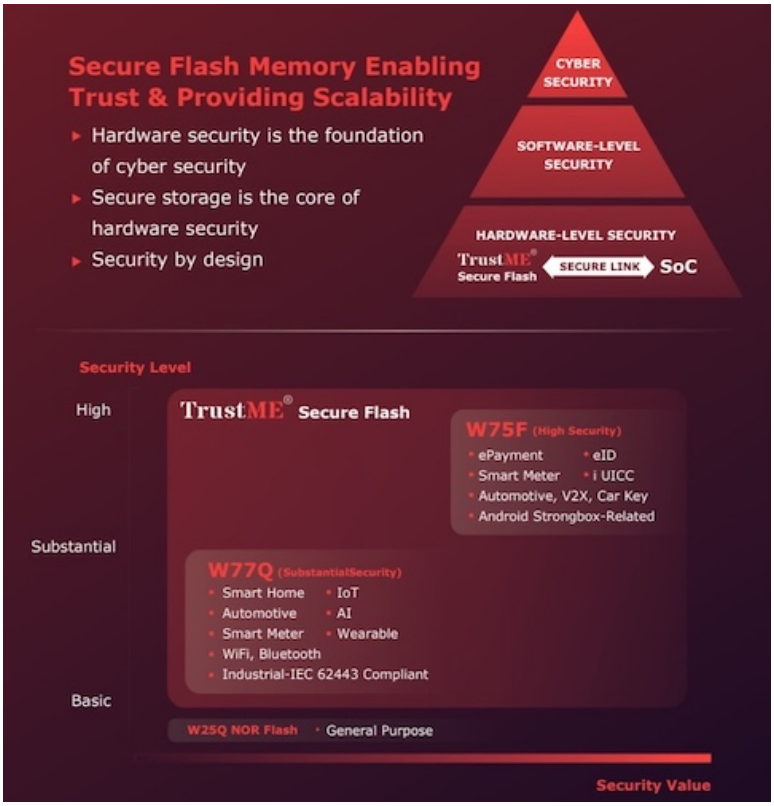
Kit for CRA Conformance and Integration

Last week Winbond announced its CRA Conformance and Integration Kit for its TrustME W77Q Secure Flash family. The package is designed to help manufacturers accelerate readiness for the European Union's Cyber Resilience Act (CRA) by providing hardware security, software, integration guidance, testing resources, reference designs, and security evidence in a unified package.

According to the company, the CRA introduces cybersecurity requirements across the lifecycle of products with digital elements, covering areas including secure design and development, production, vulnerability handling, software maintenance, and technical documentation. Winbond's CRA Conformance and Integration Kit helps customers translate these requirements into implementation and system-level verification activities.

TrustME W77Q Secure Flash has achieved SESIP Level 2 certification, providing independently assessed security evidence to support customers in evaluating the component's security and their own product-level compliance activities. Component-level certification does not by itself establish CRA conformity of the finished product.

For platforms already using external NOR Flash, W77Q can provide a practical migration path where package, voltage, interface, and system requirements align. While integration may require hardware and software changes, W77Q can strengthen external memory security without adding a separate security component or requiring a complete platform redesign.



Winbond's TrustME Secure Flash products meet a variety of key security certifications.

Introduction

The Cyber Resilience Act (CRA) is an EU regulation that establishes mandatory cybersecurity requirements for products with digital elements placed on the EU market. The regulation requires manufacturers to address cybersecurity risks throughout the product lifecycle, including secure design, development, production, and maintenance. The CRA also requires products to provide protection against unauthorized access, exploitation, and cyber threats, and to support secure handling of vulnerabilities and security updates.

The Regulation Creates a Product and Process Obligation

Regulation (EU) 2024/2847 applies broadly to hardware and software products with digital elements made available on the EU market. Annex I requires an appropriate level of cybersecurity based on risk and, where applicable, controls for secure defaults, security updates, unauthorized-access protection, confidentiality, integrity, availability, attack-surface reduction, exploitation mitigation, monitoring, and secure data removal. It separately defines vulnerability-handling duties, including a SBOM (Software Bill of Material), testing, remediation, coordinated disclosure, and secure update distribution[1].

The Regulation Timeline and Why It Matters

The regulation generally applies from 11 December 2027. Reporting obligations in Article 14 apply from 11 September 2026; provisions on notification of conformity assessment bodies apply from 11 June 2026.[1,2] Products already in the field can also become relevant where the regulation's transition rules or later substantial modifications apply. Product teams should therefore build reporting, evidence, and lifecycle operations now—not wait for the 2027 date.

Milestone	Engineering implication
11 June 2026	Provisions on notification of conformity assessment bodies apply.
11 September 2026	Article 14 reporting obligations apply; reporting procedures should already be operational.
11 December 2027	Main CRA provisions apply. Complete product assessment and evidence preparation before the relevant market placement.

Security Architecture

Begin with the assets and attacker paths: executable firmware, recovery code, update authorization, version state, credentials and configuration. Consider malicious network input, compromised application firmware, unauthorized SPI commands, flash-image replay, component replacement and physical access. Select physical-attack assumptions according to the product risk assessment.

Assign Enforcement to an Explicit Trust Boundary

Boundary	Design responsibility
OEM release service	Authorize software releases, protect signing keys and publish signed images and manifests.
Host MCU or SoC	Establish trusted startup; enforce execution policy; isolate update authority; protect plaintext in RAM and runtime services.
SPI interface and driver	Use the documented security protocol; authenticate protected operations; handle resets, timeouts and errors without bypassing policy.
W77Q subsystem	Enforce the enabled device security functions and protect designated persistent assets according to the provisioned policy.
Operations and verifier	Manage deployment, evidence appraisal, vulnerability response, key revocation and support-period commitments.

Example Logical Memory Allocation

The following layout is illustrative. Regions, sizes, alignment, permission granularity and atomicity must be derived from the selected device. Logical separation in software is not proof of independent hardware protection.

Asset	Recommended access policy
Boot policy and trust anchors	Write only through a controlled provisioning or authenticated key-transition process; protect against rollback.
Active firmware A	Normal execution reads; prevent unapproved modification while it is the trusted boot image.

Asset	Recommended access policy
Candidate firmware B	Permit authorized staging; do not execute until integrity, signature, target and version checks pass.
Recovery image	Separate update authority; authenticated content; explicit version and revocation policy.
Security metadata	Protect minimum version, key epoch, image-selection and commit state against tampering and replay.
Secrets and audit data	Separate identities and permissions; define confidential reads, controlled deletion and retention.

Account for Host Compromise

A compromised application that holds a valid Flash administrator credential may be able to issue authorized destructive commands. Keep release authority separate from routine access, restrict credential use to a trusted execution path where available, and bind update authorization to an approved image. Region protection is useful only if hostile code cannot freely change the policy or obtain its administrative authority.

Secure Boot and Recoverable Startup

Secure boot must connect a trusted decision to the bytes the processor actually executes. A valid hash stored beside an image is insufficient if an attacker can replace both. The expected digest, verification key or authenticated manifest needs a protected trust anchor.

Design Recovery as an Authenticated Operation

NIST SP 800-193 organizes firmware resilience around protection, detection and recovery. Applying those principles requires a trusted recovery source and a recovery path that can operate when the main firmware is damaged. Referencing the guideline is not itself a product certification.

Maintain a recovery image that is independently authenticated and governed by a documented update policy. A permanently frozen factory image can reintroduce vulnerabilities. If its version falls below the permitted security baseline, limit it to a restricted repair role or replace it using a separately authorized process; do not silently restore unrestricted operation with revoked firmware.

Prevent Recovery Loops and Unsafe Operation

Use bounded trial boots, an authenticated success condition and a persistent failure record. Define behavior when neither image is acceptable, when power repeatedly fails, and when network recovery is unavailable. For an actuator or industrial controller, the safe state must follow the system safety analysis; rebooting indefinitely may be unacceptable.

> **Acceptance evidence:** demonstrate that an invalid image never becomes executable; a damaged primary image reaches the approved recovery path; recovery respects version and key policy; and debug or alternative boot modes cannot bypass the production policy.

Authenticated Updates and Rollback Control

A signature establishes authorization and integrity. It does not by itself establish freshness: an old vulnerable image may still carry a valid signature. An update design therefore needs both authenticity checking and persistent version policy.

Use a Transaction That Survives Interruption

Download into a staging region. Validate the manifest before using any field as a trusted address or allocation size. Authenticate the image, check compatibility and version policy, and verify programmed content. Record a protected pending state before switching the boot selection. Trial boot with a bounded health check; commit only through the authorized confirmation path.

Order image commitment and minimum-version advancement so that interruption never permits an unauthorized downgrade or strands the device without an allowed boot or repair path. The chosen journal, redundant records or device transaction mechanism must have a defined result for every possible reset point. An ordinary rewritable version file cannot provide rollback resistance by itself.

Separate Two Meanings of Rollback

Operational rollback returns from an unsuccessful trial image to a previously working image. Security rollback reintroduces a version below the approved vulnerability baseline. A design can permit the first only when the fallback remains authorized. Update recovery content and policy coherently before advancing a baseline that would otherwise reject the only recovery image.

Control All Update Entry Points

Apply the same policy to OTA, local service ports, factory tools, recovery utilities and direct Flash access. Encrypted transport protects a connection; image authentication protects the artifact across caches, mirrors and offline handling. Neither replaces authorization of the release itself. Keep application writes out of boot policy and version metadata.

For multiple firmware components, authenticate a manifest that binds their compatible versions. Power interruption must not leave a combination that passes individual signature checks but violates a dependency or exposes an older privileged component.

Provisioning, Storage and Attestation

Provision a Controlled Production Identity

Define a lifecycle from manufacturing through provisioning, deployed operation, authorized service and retirement. Use separate authorities for production provisioning, software release, routine application access and recovery. Where supported, use per-device credentials or diversified keys to limit the effect of one compromised device. A shared fleet administrator secret creates a fleet-wide exposure.

Provision through an authenticated process, verify the resulting configuration, lock the intended production policy, and retain an audit record linking device identity to configuration revision. Keep secrets out of factory logs and build artifacts. Define how failed provisioning is detected and safely retried; irreversible locks require a verified pre-lock test.

Treat Storage Encryption and Channel Protection Separately

Access control restricts permitted commands; integrity protection detects modification; encryption protects confidentiality within its defined boundary. Document whether protection covers stored cells, SPI transfers, or both. Ordinary readable boot bytes must not be described as confidential merely because other regions use a secure channel.

A secure-channel design needs peer authentication, freshness, command binding and unambiguous failure handling. Verify which operations the selected device protects and which remain available through ordinary commands. Examine reset/session behavior and replay across power cycles. If a key is released to the host, host isolation and RAM handling become part of its security boundary.

Make Attestation Evidence Specific and Fresh

An illustrative attestation exchange uses a verifier-generated nonce and authenticated evidence binding that nonce to a device identity, relevant memory measurement, security version and configuration state. The verifier validates the credential chain or enrolled identity, matches the nonce, and appraises the result against an approved baseline. Include only fields the actual device and trusted software can reliably produce.

A fresh Flash measurement proves only what was measured and bound into the evidence. It does not establish that the host is currently executing those bytes, that RAM is uncompromised, or that unmeasured components are trustworthy. For supply-chain checks, bind the approved image and configuration to the intended product and custody process. If a stateful signing mechanism is used on-device, its signature budget and state recovery require explicit design.

Logging and Retirement

Record update acceptance, authentication failures, policy changes and recovery events in a bounded audit design. Protected storage can preserve records, but a compromised host may omit events unless capture is independently enforced. Define overflow, retention, export and time-source behavior. At retirement, remove credentials and sensitive data using the documented erase or key-destruction mechanism, including host copies, backups and service systems.

Winbond Secure Flash Eases the CRA Compliance

Winbond TrustME® Secure Flash can simplify that work by placing security enforcement next to the firmware and critical data it protects. The Secure Flash Memory device has full functional and pin-to-pin compatibility with standard Flash Memory devices, yet it offers substantial security well beyond ordinary Flash devices. It can help IoT device manufacturers to take an existing design and turn it into CRA compliant device without any PCB or design changes leading to faster time to market with minimal effort. In an appropriately designed system, the flash device can help authenticate stored code and data, secure boot, data confidentiality, constrain unauthorized access, establish replay-resistant state, support a protected recovery image (fail safe boot), PQC (Post Quantum Cryptography) compliant secure over the air (OTA) FW update and remote attestation. These capabilities reduce the amount of security logic that must be invented in application software and make it more secure and ready for the future.

Where Secure Flash Maps to CRA Outcomes

A Secure Flash feature supports a CRA claim only when it is enabled, correctly provisioned, integrated into the boot and update design, verified by testing, maintained through the support period, and described in the technical documentation. A disabled or unused feature is not a control.

The matrix below is an engineering traceability aid, not a declaration of conformity. Applicability depends on the product risk assessment and on the exact implementation.

CRA Outcome	Secure Flash Contributions	Evidence to Retain	Residual Product Duty
Secure by design and appropriate risk controls	A hardware-enforced storage trust boundary reduces dependence on mutable application code.	Threat model, architecture, security objectives, device configuration.	Risk assessment and rationale for control selection.
Protection from unauthorized access	Authenticated access and protected regions can restrict reads, writes, erases, and administrative operations.	Access-control tests, provisioning records, negative tests.	Identity, authorization, account and service controls across the full product.
Confidentiality and integrity	Cryptographic protection and authentication can safeguard stored code, secrets, and configuration.	Algorithm configuration, key ownership, integrity-failure tests.	End-to-end protection for data in RAM, transit, cloud, logs, and backups.
Security updates	Authenticates update content and can preserve trusted update metadata and version state.	Update protocol, signature verification, interrupted-update and rollback tests.	Operate update distribution, notification, support, remediation, and availability.
Availability and Recovery	Secure authenticated Fail-Safe Boot.	Recovery drill results, failure-injection tests, recovery-image governance.	System resilience, service continuity, DoS mitigations, user impact.

Build the Technical File as the Design Matures

The CRA requires manufacturers to demonstrate conformity. Secure Flash can make this easier when its security objectives, configuration, interfaces, tests, and assurance artifacts are incorporated into the product evidence package.

Recommended Evidence Set

Evidence Item	What to Capture	Why it matters
Architecture and data-flow description	Trust boundaries; boot chain; update chain; protected assets; recovery path; external interfaces.	Shows how the control design addresses the risk assessment.
Secure Flash configuration baseline	Part number; revision; enabled mechanisms; regions; permissions; lifecycle state; provisioning policy.	Makes the implemented control reproducible and auditable.
Verification package	Positive and negative tests; fault injection; rollback; interrupted update; recovery; unauthorized command tests.	Demonstrates that failure modes are secure and expected behavior is enforced.
Supplier assurance artifacts	Datasheets, security guidance, declarations, certification reports or public certificates, advisories, change notifications.	Supports component claims and supply-chain due diligence.
Operational procedures	Key management, signing, update release, vulnerability intake, incident escalation, reporting, end-of-life-support.	Connects the device control to lifecycle and vulnerability-handling duties.

Independent Assurance (Public Information)

Members of the TrustME3 family have obtained component-level security evaluations, including SESIP Level 2 with physical attacker resistance, Common Criteria Level 2, and FIPS 140-3 CMVP, etc. Such evidence can reduce duplicated analysis and strengthen supplier assurance. Always confirm that the certificate applies to the exact device, revision, configuration, and security functions used in the product.

Winbond Comprehensive CRA Integration Package

The Winbond CRA Integration Kit connects Secure Flash hardware capabilities to deployable host software, repeatable tests and customer compliance evidence. Its value is the complete integration path: choose a security architecture, configure and provision the device, integrate the software, verify enforcement, and retain the resulting evidence with each product release.

The eight package categories below come from the supplied material. The following subsections expand them into proposed technical content; they are not a statement that every interface, tool or platform is currently released. Winbond's public collateral includes software repositories, with additional confidential software and documentation available through its support and NDA process.

Package element	Technical content and acceptance check
Application notes	Map requirements to control, configuration, host assumption and test ID; distinguish native hardware enforcement from system software.
Hardware guidelines	Document voltage, footprint, pin functions, power ramp/reset, boot timing, SPI modes and security-specific wiring; validate a named board.
Low-level drivers	Provide versioned APIs, error semantics, concurrency rules, secure-channel lifecycle and integration examples; identify supported OS/RTOS and maintenance owner.
Sample code	Demonstrate boot/update/recovery and provisioning flows; remove development keys and unsafe debug defaults from production builds.

Package element	Technical content and acceptance check
Test suite	Automate positive and negative cases, power-interruption scenarios and evidence export; distinguish unit tests from product acceptance tests.
Conformance collateral	Provide certificate scope, security assumptions, risk/evidence templates, software inventory inputs and vulnerability contact information.
Conformity checklist	Track implemented controls, residual duties, open issues, evidence location and review owner; include the applicable assessment route.
Reference designs	Publish a reproducible board/software baseline, logical memory allocation, verified flows and measured resource/timing results.

Summary

CRA compliance must be engineered across the product lifecycle. W77Q provides hardware-enforced security building blocks for key CRA objectives. Secure Flash strengthens the existing external memory boundary without adding a separate security device. Drop-in replacement minimizes redesign effort resulting in fast time to market for existing products which will be CRA compliant.

References and Further Reading

1. European Union, Regulation (EU) 2024/2847 Cyber Resilience Act, Official Journal, 20 November 2024. See especially Articles 13, 14, 27, 32, 71 and Annexes I, II, VII and VIII.
2. European Commission, Cyber Resilience Act policy and implementation information, updated 7 September 2026.
3. GlobalPlatform, Winbond TrustME W77Q Secure Flash obtains SESIP Level 2 with physical attacker resistance certification.
4. Winbond Electronics, TrustME® Secure Flash Product information. Datasheets, Application Notes, Security Guidance and certificates, and ordering information.