digicert®

European Union Cyber Resilience Act

A Compliance Guide for Connected Devices

WHITE PAPER

A Compliance Guide for Connected Devices

The European Union (EU) Cyber Resilience Act (CRA) is reshaping how connected devices are designed, built, and maintained for the European market. As cyber threats grow and device ecosystems expand, the EU has established this regulation to ensure that security is no longer optional—it's a core requirement for market access.

Under the CRA, any product with digital elements (PDE)—from IoT devices and industrial controllers to smart appliances and embedded software—must meet strict cybersecurity obligations throughout its lifecycle. Failure to comply means products cannot be sold in the EU and manufacturers can be penalized of up to €15 million or 2.5% of their global revenue.

From Regulation to Reality

At its core, the CRA makes a simple promise: only secure products belong on the EU market.

Article 6 of the regulation lays out the foundation for compliance:

1. Products must meet the essential cybersecurity requirements in Annex I, Part I, provided they are properly installed, maintained, and updated.

2. Manufacturers must implement processes that meet Annex I, Part II obligations, including vulnerability management and secure lifecycle practices.

In other words, the CRA isn't just about how a device is built, it's about how it is supported and protected for its entire lifespan. This dual focus is what makes CRA compliance more than a one-time event; it's an ongoing commitment.

What the CRA Aims to Achieve

The EU's objectives with the CRA go beyond ticking regulatory boxes:

- Raising the baseline of cybersecurity for all connected products
- Protecting consumers and businesses from devices that introduce risk to their networks
- Creating a single, harmonized market standard to replace fragmented national regulations
- Empowering manufacturers to adopt security by design principles as a competitive advantage

For global OEMs, this means the path to EU market access is now tied directly to security maturity.

Who and What Falls Under the CRA

The CRA casts a broad net. It applies to any EU or non-EU manufacturer selling products with digital elements in Europe, including:

- IoT and embedded devices used in homes, healthcare, and industry
- Industrial control and automation equipment used in factories or critical infrastructure
- Consumer electronics like smart appliances, wearables, and security systems
- Software and firmware that runs on or ships with connected devices

CRA Regulatory Definition

Products with digital elements shall be made available on the market only where:

(a) they meet the essential cybersecurity requirements set out in Part I of Annex I, provided that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, the necessary security updates have been installed, and

(b) the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I.

Even a simple connected sensor or smart thermostat can fall under the CRA if it transmits or processes data in a networked environment.

What Compliance Requires

Complying with the CRA is not a onetime certification, it is a lifecycle commitment. Manufacturers must:

- Build security into products from the start, reducing attack surfaces and avoiding known vulnerabilities
- Maintain visibility and control over software components, including creating a Software Bill of Materials (SBOM)
- Actively manage vulnerabilities by detecting, reporting, and remediating issues quickly
- Provide secure updates—often over-the-air (OTA)—and keep records of update distribution and user notifications
- Document compliance to support CE marking and withstand audits

Some products—especially high-risk or critical devices—may also require third party conformity assessments before reaching the market.

A Ticking Clock for Manufacturers

The CRA is already law, and its compliance deadlines are approaching:

10 December 2024
– CRA enters into force

11 September 2026
– Vulnerability reporting obligations begin

11 December 2027
– Full compliance required for all products

This timeline means manufacturers must act now to ensure their product development and support processes align with CRA expectations.

The Stakes of Non-Compliance

The cost of falling short is high. Beyond reputational damage and lost market access, the CRA allows for penalties. Products found noncompliant can be pulled from the market, and OEMs may face mandatory remediation or redesign efforts.

Non-Compliance can lead to penalties of up to **€15 million** or **2.5%** of global annual revenue

How DigiCert Supports CRA Compliance

DigiCert Device Trust solutions provide the tools and frameworks manufacturers need to meet CRA requirements efficiently:

- **DigiCert Device Trust Manager** – Centralized, policy driven device identity management, certificate issuance and revocation, secure lifecycle management, and orchestrated OTA firmware and configuration updates
- **DigiCert TrustCore SDK** – Embedded cryptographic SDK, providing secure device identity provisioning, key storage, signing, and encryption for data at rest and in transit, with support for TPMs and secure elements
- **DigiCert TrustEdge** – Lightweight edge agent enabling secure device enrollment, mutual authentication, encrypted communications, and policy enforced OTA update and revocation workflows
- **DigiCert Software Trust Manager** – Secure code signing, SBOM generation, and signed release tracking to support vulnerability management workflows

Together, these solutions can help OEMs meet 17 of 22 CRA Annex I obligations, accelerating compliance and enabling CE marking for EU market access.

CRA Annex | Compliance Checklist for Connected Devices

The European Cyber Resilience Act establishes 22 Annex I requirements that manufacturers must meet to sell connected devices in the EU. These requirements are divided into two categories:

- **Part I:** Product design, development, and deployment
- **Part II:** Vulnerability management and lifecycle governance

Part I: Device Design, Production, and Deployment Requirements

Requirement (Number & Name)	Requirement Text	How DigiCert Helps OEMs to Comply
Part I1 (Secure by Design)	Products with digital elements shall be designed, developed, and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.	✓ TrustCore SDK and TrustEdge support secure design, allowing OEMs complete control over which SDK components are included in the device software, thereby reducing the device attack surface. Plus, support for TPMs, software, and hardware-based secure elements ensure keys are always protected.
Part I2(a) (No Known Exploitable Vulnerabilities	Products shall be made available on the market without known exploitable vulnerabilities.	✓ Software Trust Manager provides automated software validation and vulnerability scanning for your device software as part of your CI/CD process. It can also generate an SBOM as part of the process to show transparency in the software being used by the devices. ✓ Each TrustCore SDK and TrustEdge commit-and-release is automatically scanned for software vulnerabilities.
Part I2(b) (Secure Default Configuration)	Products shall be made available on the market with a secure-by-default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state.	✓ TrustCore SDK is modular, allowing OEMs to compile in only the features they need, thereby reducing the attack surface. ✓ By default, TrustEdge ships with no open inbound TCP/UDP service ports, avoiding the need to disable or firewall open ports. ✓ Both TrustCore SDK and TrustEdge support securing private keys in TPMs, secure elements, or using Physical Unclonable Functions (PUF). ✓ Both TrustCore SDK and TrustEdge support encryption of device data in transit, using TLS 1.3 and secure MQTT, and data at-rest using either AES, ML-DSA, or SLH-DSA. ✓ Both TrustCore SDK and TrustEdge are PQC-ready, supporting ML-KEM, ML-DSA, and SLH-DSA, protecting devices against the impending quantum threat.
Part I2(c) (Timely Security Updates)	Ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them.	✓ Device Trust Manager with TrustEdge enables secure over-the-air updates of binaries and configuration file updates over MQTTs. Updates can be packaged to include the ability to notify users, support opt-out, and postpone updates. ✓ Software Trust Manager can monitor SBOMs representing the software components installed on a device and notify development teams once a new CVE is discovered in a dependency, such as an open source software package.
Part I2(d) (Unauthorized Access Protection)	Ensure protection from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorized access.	✓ Device Trust Manager offers secure credential provisioning policies, ensuring each device has a strong, certificate-backed identity to avoid spoofing. Device access to certificate issuance, OTA updates, and policies are strictly controlled through the certificate-backed identity of the device, device group membership, and assignment of policies to the device group. ✓ Device Trust Manager user and API access are strictly controlled, using least-privileges, by a combination of role-based access control, API keys, two-factor authentication, client certificate authentication, and support for popular IDPs.

Requirement (Number & Name)	Requirement Text	How DigiCert Helps OEMs to Comply
Part I2(e) (Confidentiality of Data)	Protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms, and by using other technical means.	✓ By default, Device Trust Manager supports secure MQTT communication with devices over TLS 1.3 encryption. ✓ Both TrustCore SDK and TrustEdge support encryption of device data in transit, using TLS 1.3 and secure MQTT, and data-at-rest using AES, ML-DSA, or SLH-DSA.
Part I2(f) (Integrity of Data & Commands)	Protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs, and configuration against any manipulation or modification not authorized by the user, and report on corruptions.	✓ By default, Device Trust Manager supports secure MQTT communication with devices over TLS 1.3 encryption. It also supports deploying signed updates to devices. ✓ Both TrustCore SDK and TrustEdge support encryption of device data in transit, using TLS 1.3 and secure MQTT, and data-at-rest using AES, ML-DSA, or SLH-DSA.
Part I2(g) (Data Minimization)	Process only data, personal or other, that are adequate, relevant, and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimization).	✓ By default, TrustEdge does not send any personal data from the device to Device Trust Manager, nor does Device Trust Manager receive or store any personal data from devices. Only device metadata is sent by TrustEdge to Device Trust Manager (operating system, version, MAC address, and so on) to manage the device security and updates.
Part I2(h) (Availability of Essential Functions)	Protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks.	✓ Device Trust Manager allows administrators to temporarily disable devices while incidents are being investigated. This immediately severs communication between the device, Device Trust Manager, and any integrated cloud platforms. If the device is compromised, its certificate can be permanently revoked.
Part I2(i) (Minimize Negative Impact on Networks)	Minimize the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks.	✓ Device Trust Manager allows administrators to temporarily disable devices while incidents are being investigated. This immediately severs communication between the device, Device Trust Manager, and any integrated cloud platforms. If the device is compromised, its certificate can be permanently revoked.
Part I2(j) (Attack Surface Reduction)	Be designed, developed, and produced to limit attack surfaces, including external interfaces.	✓ TrustCore SDK is modular, allowing OEMs to compile in only the features they need, thereby reducing the attack service. ✓ By default, TrustEdge ships with no open inbound TCP/UDP service ports, avoiding the need to disable or firewall open ports.
Part I2(k) (Incident Impact Mitigation)	Be designed, developed, and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques.	✓ Device Trust Manager allows administrators to temporarily disable devices while incidents are being investigated. This immediately severs communication between the device, Device Trust Manager, and any integrated cloud platforms. If the device is compromised, its certificate can be permanently revoked.
Part I2(l) (Security Event Monitoring)	Provide security-related information by recording and monitoring relevant internal activity, including the access to or modification of data, services, or functions, with an opt-out mechanism for the user.	Coming soon from DigiCert.
Part I2(m) (Secure Data Deletion & Transfer)	Provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.	✓ Both TrustCore SDK and TrustEdge support encryption of device data in transit, using TLS 1.3 and secure MQTT, and data at-rest using AES, ML-DSA, or SLH-DSA. Also, OEMs can use TrustCore SDK and TrustEdge to decrypt at-rest data to securely transfer the data to another device over TLS 1.3.

Part II: Vulnerability Management & Lifecycle Governance

Requirement (Number & Name)	Requirement Text	How DigiCert Helps OEMs to Comply
Part II1 (SBOM & Component Tracking)	Identify and document vulnerabilities and components contained in products with digital elements, including drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products	✓ Software Trust Manager provides automated software validation and vulnerability scanning for device software as part of your CI/CD process. It can also generate an SBOM as part of the process to show transparency in the software being used by the devices.
Part II2 (Rapid Vulnerability Remediation)	In relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates.	✓ Device Trust Manager with TrustEdge enables secure over-the-air updates of binaries and configuration files over MQTTs. These can either be feature updates or security fixes. Updates can be quickly deployed to large groups of devices. Devices are immediately notified of the update.
Part II3 (Regular Security Testing)	Apply effective and regular tests and reviews of the security of the product with digital elements.	✕ This requirement falls on the manufacturer.
Part II4 (Public Vulnerability Disclosure)	Once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch.	✕ This requirement falls on the manufacturer.
Part II5 (Coordinated Vulnerability Disclosure Policy)	Put in place and enforce a policy on coordinated vulnerability disclosure.	✕ This requirement falls on the manufacturer.
Part II6 (Share Potential Vulnerability Information)	Take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements.	✕ This requirement falls on the manufacturer.
Part II7 (Secure Update Distribution)	Provide mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner.	✓ Device Trust Manager with TrustEdge enables secure over-the-air updates of binaries and configuration files over MQTTs. These can either be feature updates or security fixes. Updates can be quickly deployed to large groups of devices. Once connected, devices are immediately notified of the update.
Part II8 (Timely and Free Security Updates)	Ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.	✓ Device Trust Manager enables secure over-the-air updates of binaries and configuration files over MQTTs. These can either be feature updates or security fixes. Updates can be quickly deployed to large groups of devices. Once connected, devices are immediately notified of the update.

Industry Use Cases: Achieving CRA Compliance with DigiCert Device Trust Solutions

Manufacturers across multiple sectors face unique challenges in meeting the CRA's cybersecurity requirements. Below are two example use cases that demonstrate how DigiCert Device Trust solutions help organizations achieve and maintain compliance.

1. Industrial IoT (IIoT) Equipment Manufacturer

Scenario:

An industrial automation OEM builds PLCs and connected robotics for smart factories in Europe. These devices fall under CRA due to their digital components and exposure to network risk.

Challenges:

- Devices operate in unmonitored or semi-air-gapped environments
- Cyber incidents could halt factory operations or breach critical infrastructure networks
- CRA requires secure by design architecture and rapid remediation capability

How DigiCert Enables Compliance:

- TrustCore SDK provides a modular, embedded cryptographic framework with TPM/secure element support to reduce attack surfaces
- Device Trust Manager allows administrators to revoke or disable compromised devices to protect availability
- TrustEdge enables encrypted and authenticated device communications, ensuring integrity and compliance with CRA Annex I

Result:

- Meets CRA mandates for design security, integrity, and vulnerability mitigation
- Minimizes downtime risk and satisfies European industrial cybersecurity regulations

2. Consumer Smart Home Device Manufacturer

Scenario:

A company manufactures smart thermostats and security cameras for the EU market. The CRA applies because these products include digital elements, software updates, and network connectivity.

Challenges:

- Devices must ship without known exploitable vulnerabilities
- CRA requires default secure configurations and optout security updates
- Consumer privacy demands strict data minimization and protection

How DigiCert Enables Compliance:

- TrustEdge ensures devices launch with no open inbound ports and encrypted communications
- Software Trust Manager scans firmware for vulnerabilities and generates SBOMs for transparency
- Device Trust Manager enforces secure OTA updates and allows devices to be reset or securely wiped in the field

Result:

- CRA Annex I obligations for secure by default, vulnerability management, and data confidentiality are addressed
- Consumer trust and regulatory compliance enable smooth EU market entry

With DigiCert Device Trust solutions, OEMs across various industries and markets can confidently meet CRA compliance requirements and maintain secure, trusted device ecosystems throughout their lifecycle.

Ensure Your Devices Are Ready for CRA Compliance

The European Cyber Resilience Act fundamentally changes the way connected devices are designed, built, and maintained for the EU market. By December 11, 2027, all products with digital elements must meet the CRA's cybersecurity requirements or risk:

- Blocked market access in the EU
- Regulatory penalties up to €15 million or 2.5% of global turnover
- Brand and operational damage due to vulnerability exposure

Device Trust solutions give manufacturers the tools to confidently achieve and maintain compliance:

- **DigiCert Device Trust Manager** – Policy driven device identity, secure lifecycle management, and OTA update enforcement
- **DigiCert TrustCore SDK** – Embedded cryptography and secure device provisioning
- **DigiCert TrustEdge** – Lightweight agent for secure onboarding and communications
- **DigiCert Software Trust Manager** – SBOM generation, vulnerability scanning, and secure code distribution

Together, these solutions can help you meet 17 of 22 CRA Annex I obligations, reduce compliance complexity, and accelerate CE marking.

Want to review the complete European Union Cyber Resilience Act?

Visit: https://www.cyberresilienceact.eu to view the official regulation text.

Have questions about how DigiCert Device Trust solutions support compliance?

Contact us at device-trust@digicert.com or **scan the QR code** to connect with our team.

About DigiCert

DigiCert is the world's leading provider of digital trust, enabling individuals and businesses to engage online with the confidence that their footprint in the digital world is secure. DigiCert® ONE, the platform for digital trust, provides organizations with centralized visibility and control over a broad range of public and private trust needs, securing websites, enterprise access and communication, software, identity, content and devices. DigiCert pairs its award winning software with its industry leadership in standards, support and operations, and is the digital trust provider of choice for leading companies around the world. For more information, visit digicert.com or follow @digicert.