EU CYBER RESILIENCE ACT

Complying with CRA leveraging Digi ConnectCore Security Building Blocks

Agenda

1. Introduction to CRA
2. Timeline / Main Milestones
3. Product Categories & Conformity Assessment Procedures
4. Main CRA Pillars Overview
5. Digi Security Building Blocks
6. Complying with CRA leveraging Digi Security Building Blocks

Introduction to CRA (I)

EU Cyber Resilience Act (CRA) - Regulation (EU) 2024/2847

- The CRA fundamentally alters the landscape of product compliance in the EU
  - Integrating robust cybersecurity measures into the existing framework for CE marking
  - Mandatory for any **product or software** that contains digital elements
  - Manufacturers and retailers, both have responsibility
  - Throughout the entire product lifecycle
- **Twofold problem addressed**
  - Poor levels of cybersecurity in products or inadequate security updates
  - Inability of consumers and businesses to determine which products are secure or how to set them up to ensure they are protected
- **What will CRA guarantee?**
  - Harmonized rules when launching products or software with a digital component
  - Cybersecurity requirements framework governing the planning, design, development and maintenance of such products
  - Obligation to provide a duty of care throughout the entire product lifecycle

Introduction to CRA (II)

- **What does "the Regulation comes into force" mean?**
  - Software and Internet-connected products will carry the CE mark to indicate they comply with the new requirements
    - All products connected directly or indirectly to another device or network
    - Exclusions specified in Article 2, Scope
  - Consumers and businesses empowered to make informed decisions based on visible indicators (CE mark) of security compliance
  - Market surveillance authorities will enforce these regulations to ensure compliance across the EU market
- **What happens if products do not comply?**
  - No qualification for CE marking, no authorization for sale in the EU
  - Possible recall or withdrawal of products
  - Penalty payments (up to 2.5% of total annual turnover worldwide)
    - Further details in Article 64, Penalties

Introduction to CRA (III)

- Specified exclusions (Article 2, Scope)

PRODUCT TYPE	APPLICABLE EXISTING REGULATION
Medical devices	Regulation (EU) 2017/745
In vitro diagnostic medical devices	Regulation (EU) 2017/746
Motor vehicles and their trailers	Regulation (EU) 2019/2144
Civil aviation	Regulation (EU) 2018/1139
Marine equipment	Directive 2014/90/EU
Spare parts to replace identical components in products with digital elements and that are manufactured according to the same specifications as the components they are intended to replace	
Products with digital elements developed or modified exclusively for national security or defense purposes or products specifically designed to process classified information	

Timeline / Main Milestones (I)

- **14 December 2020** – Regulation was announced in the 2020 EU Cybersecurity Strategy
  - Complements the NIS2 Framework
- **15 September 2022** – Proposal for regulation published at EUR-Lex
- **1 December 2023** – Political agreement reached between the European Parliament and the Council on the Cyber Resilience Act
- **12 March 2024** – Parliament approved new cyber resilience standards
- **10 October 2024** – Council adopts new law on security requirements for digital products
- **23 October 2024** – Signature of the Regulation (EU) 2024/2847 by the European Parliament and the Council
- **20 November 2024** – Publication of the Regulation (EU) 2024/2847
  - To enter into force on the twentieth day following that of its publication in the Official Journal of the European Union
- **10 December 2024** – The Regulation came into force from this date
  - This Regulation shall be binding in its entirety and directly applicable in all Member States
- **11 June 2026** – Chapter IV (Articles 35 to 51, Notification of Conformity Assessment Bodies) shall apply from this date
- **11 September 2026** – Article 14 (Reporting Obligations of Manufacturers) shall apply from this date
  - Report actively exploited vulnerabilities to national authorities and ENISA
- **11 December 2027** – The Regulation will apply from this date
  - All products with digital elements must have CE marking indicating compliance with CRA

Timeline / Main Milestones (II) – RED & CRA

Radio Equipment Directive (RED)

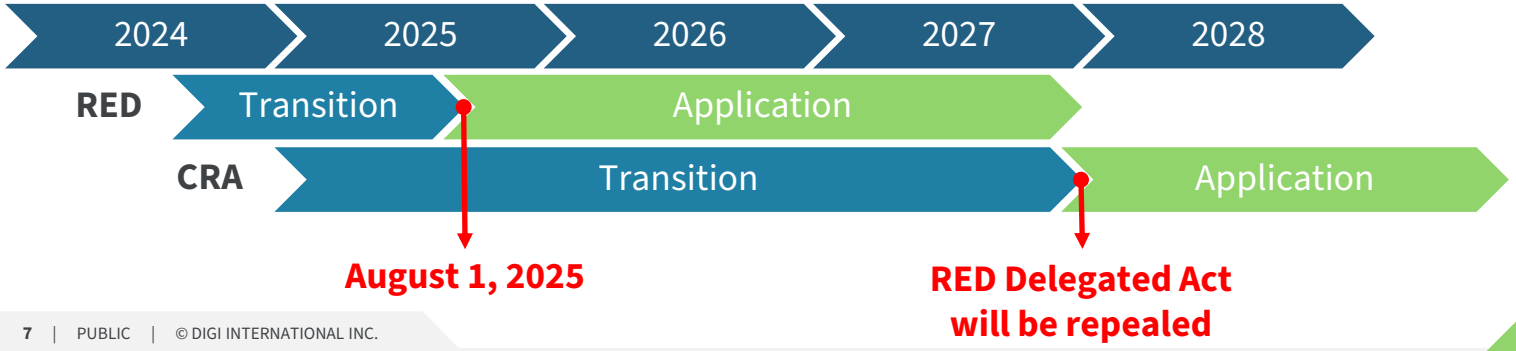
Essential requirements for radio equipment

- EMC, safety/health, privacy and fraud protection
- No known vulnerabilities at product launch
- Capability to update product software
- Conformity assessment with risk-based approach
- Hardware components: N/A
- IoT consumer and industrial devices: self-declaration
- Medical devices and auto: exemption

Cyber Resilience Act (CRA)

Ensures secure hardware and software products on the market

- Proactive and recurring vulnerability monitoring
- Capability to provide updates/patches for products
- Different levels of security according to categories defined in the Regulation
- Hardware components: third-party evaluation
- IoT consumer devices: self-declaration
- IoT industrial devices: third-party evaluation



Timeline / Main Milestones (III) – Manufacturers' obligations

Design & Development	Support period 5 years at least	Availability of security updates
Product risk assessment Product-related requirements Vulnerability handling requirements Technical documentation Conformity assessment CE marking, EU Declaration of Conformity	Compliance with vulnerability handling requirements	Security updates available 10 years after release

Reporting Obligations

Obligation to report actively exploited vulnerabilities and severe incidents to CSIRT and ENISA
for all products placed on the EU market before December 11, 2027
Early warning notification within 24h and vulnerability/incident notification within 72h

Product Categories & Conformity Assessment Procedures

Default products and open source	Important products Class I	Important products Class II	Critical products
Products not listed in other categories	• Boot managers • Physical and virtual network interfaces • Operating systems • **MCU/MPU/ASIC/FPGA w/ secure functionalities** • …	• Hypervisors • Firewalls, intrusion detection and prevention systems • **Tamper-resistant MCU/MPU**	• Hardware devices with security boxes • Smart meter gateways as per Directive (EU) 2019/944 • Smartcards including secure elements

Self-assessment (Module A)

Self-assessment only if against harmonized standard(s) (Module A)

Third-party – EU-type examination and internal production control (Module B+C) *(product assessment)*

Third-party – Full quality assurance (Module H) *(process assessment)*

Third-party – EUropean Cybersecurity Certification scheme EUCC *(product and process assessment)*

Main CRA Pillars Overview

Stricter Cybersecurity

Design, development, maintenance and EOL Proactive removal of vulnerabilities and recurring updates

Conformity Assessments

More detailed to ensure compliance with cybersecurity requirements

Transparency & Communication

Clear and up-to-date information on product security features and any relevant security issues

Early Vulnerability Notifications

Any actively exploited vulnerability discovered must be reported to authorities within 24 hours of its detection

Supervision & Audits

More intensive to ensure continued compliance with cybersecurity requirements

Product Classification

Different categories according to their level of risk (default, important and critical)

Digi Security Building Blocks

Digi ConnectCore provides

- **Digi TrustFence** to meet “secure by design” requirements
- **Digi ConnectCore Security Services** to address vulnerability management/disclosure requirements
- **Digi ConnectCore Cloud Services** to update devices without delay and to help monitoring

Complying with CRA leveraging Digi Security Building Blocks (I)

PART I	DESCRIPTION	DIGI TRUSTFENCE	DIGI CONNECTCORE SECURITY SERVICES	DIGI CONNECTCORE CLOUD SERVICES	DIGI EMBEDDED YOCTO
(1)	Products shall be designed, developed and produced ensuring an appropriate level of cybersecurity based on the risks	✓ TrustFence overall	✓ Security Services overall	✓ Cloud Services overall	✓ DEY overall
(2) (a)	Products shall be made available without known exploitable vulnerabilities	N/A	✓ Custom SBOM scans, meta-digi-security	✓ DRM Vulnerability Patch Policy	✓ Digi owned software maintenance
(2) (b)	Products shall be made available with a secure by default configuration	✓ TrustFence overall	N/A	N/A	✓ *Hardened DEY reference image**
(2) (c)	Products shall ensure that vulnerabilities can be addressed through security updates	✓ Secure software update	✓ meta-digi-security, consulting & support	✓ Secure remote OTA software updates	✓ Secure software update, dual boot configuration
(2) (d)	Products shall ensure protection from unauthorized access	✓ Secure console, secure JTAG	N/A	N/A	✓ SSH/TLS
(2) (e)	Products shall protect the confidentiality of stored, transmitted or otherwise processed data, personal or other	✓ Encrypted file system / files (hardware bound)	N/A	✓ File system access, TLS, certificate-based authentication & encryption	✓ Encryption, WPA3, FIPS 140-2/3**

*Roadmap (coming soon)

**Additional cost involved

Complying with CRA leveraging Digi Security Building Blocks (II)

PART I	DESCRIPTION	DIGI TRUSTFENCE	DIGI CONNECTCORE SECURITY SERVICES	DIGI CONNECTCORE CLOUD SERVICES	DIGI EMBEDDED YOCTO
(2) (f)	Products shall protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration	✓ Secure boot / authenticated file system	N/A	✓ File system access, TLS, certificate-based authentication & encryption	✓ TLS, read-only file system
(2) (g)	Products shall process only data, personal or other, that are adequate, relevant and limited to what is necessary	N/A	N/A	✓ Custom data streams	N/A
(2) (h)	Products shall protect the availability of essential and basic functions against denial-of-service attacks	N/A	N/A	N/A	✓ *Embedded systems security best practices**
(2) (i)	Products shall minimize the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks	N/A	N/A	N/A	✓ *Embedded systems security best practices**
(2) (j)	Products shall be designed, developed and produced to limit attack surfaces, including external interfaces	✓ Secure boot, secure console, secure JTAG, tamper detection	✓ meta-digi-security, consulting & support	N/A	N/A

*Roadmap (coming soon)

Complying with CRA leveraging Digi Security Building Blocks (III)

PART I	DESCRIPTION	DIGI TRUSTFENCE	DIGI CONNECTCORE SECURITY SERVICES	DIGI CONNECTCORE CLOUD SERVICES	DIGI EMBEDDED YOCTO
(2) (k)	Products shall be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques	✓ Tamper detection	N/A	✓ Templates	N/A
(2) (l)	Products shall provide security related information by recording and monitoring relevant internal activity	✓ Tamper detection	N/A	✓ *Security monitoring agent**	N/A
(2) (m)	Products shall 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	N/A	N/A	✓ File system access, DRM data/settings management	N/A

*Roadmap (coming soon)

Complying with CRA leveraging Digi Security Building Blocks (IV)

PART II	DESCRIPTION	DIGI TRUSTFENCE	DIGI CONNECTCORE SECURITY SERVICES	DIGI CONNECTCORE CLOUD SERVICES	DIGI EMBEDDED YOCTO
(1)	Manufacturers shall draw up a software bill of materials in a commonly used and machine-readable format	N/A	✓ Custom SBOM creation	N/A	✓ DEY SBOM
(2)	Manufacturers shall address and remediate vulnerabilities without delay	N/A	✓ meta-digi-security, consulting & support	✓ Secure remote OTA software updates, templates	✓ DEY regular releases
(3)	Manufacturers shall apply effective and regular tests and reviews of the security of the product	N/A	✓ Custom SBOM scans	✓ DRM Vulnerability Patch Policy	✓ DEY Patch Policy
(4)	Manufacturers shall share and publicly disclose information about fixed vulnerabilities	N/A	✓ Security Services overall	✓ Digi Security Center	✓ Digi Security Center
(5)	Manufacturers shall put in place and enforce a policy on coordinated vulnerability disclosure	N/A	N/A	✓ DRM Vulnerability Patch Policy, Digi Security Center	✓ DEY Patch Policy, Digi Embedded GitHub, Digi Security Center
(6)	Manufacturers shall facilitate the sharing of information about potential vulnerabilities including by providing a contact address for the reporting of the vulnerabilities discovered	N/A	N/A	✓ Digi security form	✓ Digi security form

Complying with CRA leveraging Digi Security Building Blocks (V)

PART II	DESCRIPTION	DIGI TRUSTFENCE	DIGI CONNECTCORE SECURITY SERVICES	DIGI CONNECTCORE CLOUD SERVICES	DIGI EMBEDDED YOCTO
(7)	Manufacturers shall provide for mechanisms to securely distribute updates to ensure that vulnerabilities are fixed or mitigated in a timely manner	✓ Secure software update	N/A	✓ Secure remote OTA software updates, templates, TLS, certificate-based authentication & encryption	N/A
(8)	Manufacturers shall ensure that, where security updates are available, they are disseminated without delay and, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken	N/A	N/A	✓ Secure remote OTA software updates, templates	✓ DEY Patch Policy, Digi Embedded GitHub

Any questions?

Many thanks!