Official Journal
of the European Union

EN
L series

2025/2392

1.12.2025

COMMISSION IMPLEMENTING REGULATION (EU) 2025/2392

of 28 November 2025

on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) ([1]), and in particular Article 7(4) thereof,

Whereas:

(1) Regulation (EU) 2024/2847 lays down rules on the cybersecurity of products with digital elements. In particular, Annex III to that Regulation sets out categories of important products with digital elements that, when placed on the market, are subject to conformity assessment procedures that are stricter than those applicable to other products with digital elements. Annex IV to Regulation (EU) 2024/2847 sets out categories of critical products with digital elements for which manufacturers could be required to obtain a European cybersecurity certificate under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council ([2]) or which would be subject to mandatory third-party conformity assessment, when placed on the market.

(2) Pursuant to Article 7(1) and Article 8(1) of Regulation (EU) 2024/2847, the core functionality of a product with digital elements determines whether that product with digital elements meets the technical description of a category of important or critical products with digital elements and therefore the applicable conformity assessment procedures.

(3) When developing a product with digital elements, and in order to achieve their desired set of functionalities, manufacturers typically integrate into their own products with digital elements other components which are also products with digital elements and that can meet the technical description of a category of important or critical products. Pursuant to Regulation (EU) 2024/2847, a product with digital elements is subject to the conformity assessment procedures applicable to important or critical products with digital elements, if that product as a whole is an important or critical product as set out in Annexes III and IV to that Regulation. For example, integrating an embedded browser as a component of a news app for use in smartphones does not in itself render the news app subject to the conformity assessment procedure applicable to products with digital elements that have the core functionality of 'standalone and embedded browsers'. Nonetheless, in accordance with Regulation (EU) 2024/2847, the manufacturer needs to ensure that the product with digital elements as a whole meets the essential cybersecurity requirements. Therefore, the manufacturer needs to evaluate the security of the whole product, considering, as appropriate, the security of the components or functionalities that are integrated into it. For example, in order for the manufacturer of a news app to demonstrate that its product with digital elements is in conformity with Regulation (EU) 2024/2847, that manufacturer is to demonstrate that the news app as a whole satisfies the applicable requirements, considering, as appropriate, the security of the embedded browser that is integrated into its app.

([1]) OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

([2]) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) The fact that a product with digital elements performs functions other than or additional to those detailed in the technical descriptions set out in this Regulation does not in itself mean that the product with digital elements does not have the core functionality of a product category set out in Annexes III and IV to Regulation (EU) 2024/2847. For example, products with digital elements that have the core functionality of 'operating systems' often include software that performs ancillary functions not included in the technical description of that product category, such as calculators or simple graphics editors. Products with digital elements often also incorporate components that have the functionality of another important or critical product with digital elements, such as an operating system integrating browser functionality, or a router integrating firewall functionality. This, however, does not in itself mean that such products with digital elements do not have the core functionality of 'operating systems' or 'routers, modems intended for the connection to the internet, and switches', respectively.

(5) On the other hand, a product with digital elements that has the ability to perform the functions of a product category set out in Annexes III and IV to Regulation (EU) 2024/2847 but whose core functionality itself is different from that of such product category is not to be considered to meet the technical description of that product category. For example, a security orchestration, automation and response (SOAR) software often has the ability to perform the functions of products with digital elements in the category of 'security information and event management (SIEM) systems', i.e. gather data, analyse it and present it as actionable information for security purposes. However, as its core functionality is not that of a SIEM, SOAR software are generally not to be considered to meet the technical description of 'security information and event management (SIEM) systems'. Similarly, a smartphone typically integrates components that perform the functions of several product categories set out in Annexes III and IV to Regulation (EU) 2024/2847, such as an operating system or an integrated password manager. However, as a smartphone's core functionality is not that of an operating system or of a password manager, it is generally not to be considered to meet the technical description of such product categories.

(6) Pursuant to Article 13(2) and (3) of Regulation (EU) 2024/2847, manufacturers of products with digital elements are to implement the essential cybersecurity requirements set out in Part I of Annex I to Regulation (EU) 2024/2847 in a way that is proportionate to the risks of the product with digital elements, based on the intended purpose and reasonably foreseeable use as well as the conditions of use of the product with digital elements, taking into account the length of time the product is expected to be in use. In accordance with Article 13(2) and (3) of that Regulation, and irrespective of whether the product with digital elements is considered to be an important or critical product with digital elements, manufacturers are to carry out a comprehensive cybersecurity risk assessment and indicate how the essential cybersecurity requirements are implemented as informed by the risk assessment, including their testing and assurance. Where the core functionality of their product with digital elements meets the technical description of an important or critical product with digital elements, manufacturers are to demonstrate conformity following the specific conformity assessment procedures established by Article 32(2), (3), (4) and (5) of Regulation (EU) 2024/2847.

(7) This Regulation includes examples of products with digital elements whose core functionality meets the technical description of certain important or critical products with digital elements. Such examples are provided for illustrative purposes only and are not an exhaustive list.

(8) In order to provide legal certainty to manufacturers, the categories of products with digital elements that are tamper-resistant microprocessors, tamper-resistant microcontrollers, and smartcards and similar devices, including secure elements, should be distinguished on the basis of the level of resistance against potential exploitability of flaws or weaknesses for which they have been designed. AVA_VAN level is an extensively used and standardised way to express such a level of resistance. AVA_VAN levels are set out in the publicly available Common Criteria and Common Evaluation Methodology standards, which underlie existing certification frameworks widely adopted on the market, such as Commission Implementing Regulation (EU) 2024/482 ([3]). Implementing Regulation

([3]) Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) (OJ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(EU) 2024/482 establishes a European cybersecurity certification scheme that can be used to certify a product at a specific assurance level. Drawing on global practices, Implementing Regulation (EU) 2024/482 foresees the possibility to issue certificates based on older versions of the standards until end of 2027. Hence, in the context of Regulation (EU) 2024/2847, it is appropriate to allow for AVA_VAN levels to be expressed by referring to either the latest version or older versions of those standards.

(9) The measures provided for in this Regulation are in accordance with the opinion of the Committee established by Article 62(1) of Regulation (EU) 2024/2847,

HAS ADOPTED THIS REGULATION:

Article 1

Definitions

For the purposes of this Regulation, the following definitions shall apply:

(1) 'Common Criteria' means the Common Criteria for Information Technology Security Evaluation as defined in Article 2(1) of Implementing Regulation (EU) 2024/482 or as set out in the standards referred to in Article 3(2), points (a) and (b), of that Implementing Regulation;

(2) 'Common Evaluation Methodology' means the Common Methodology for Information Technology Security Evaluation as defined in Article 2(2) of Implementing Regulation (EU) 2024/482 or as set out in the standards referred to in Article 3(2), points (c) and (d), of that Implementing Regulation.

Article 2

1. The technical description of the categories of products with digital elements under classes I and II listed in Annex III to Regulation (EU) 2024/2847 shall be as set out in Annex I to this Regulation.

2. The technical description of the categories of products with digital elements listed in Annex IV to Regulation (EU) 2024/2847 shall be as set out in the Annex II to this Regulation.

Article 3

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 28 November 2025.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX I

IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS

Class I

Category of product	Technical description
1. Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers	Identity management systems are products with digital elements that provide mechanisms for authentication or authorisation and that may also provide mechanisms for the lifecycle management of identity credentials of natural persons, legal persons, devices or systems, such as identity registration, provisioning, maintenance, deregistration. These systems include access management systems that control access of natural persons, legal persons, devices or systems to digital resources or physical locations. Privileged access management software is an access management system that controls and monitors access rights to IT or OT systems and sensitive information within an organisation, including systems enforcing differentiated access control policies for privileged users. This category includes but is not limited to authentication and access control readers, biometric readers, single sign-on software, federated identity management software, one-time password software, hardware authentication devices such as transaction authentication number (TAN) generators, authentication software and multi-factor authentication software.
2. Standalone and embedded browsers	Software products with digital elements that enable end users to access, render, and interact with web content and services hosted on servers that are connected to networks such as the Internet. They typically include a browser engine for interpreting and displaying content written in markup language (e.g. HTML), support for web protocols (e.g. HTTP, HTTPS), the ability to execute scripts and manage user inputs as well as storage of temporary or persistent data from websites (cookies). This category includes but is not limited to standalone applications that fulfil the functions of browsers, embedded browsers intended for integration into another system or application as well as browsers with AI agent integration.
3. Password managers	Products with digital elements that store passwords, locally on a device or on a remote server, including activities such as generation of passwords as well as password sharing and integration with local or third-party applications for usage of passwords. This category includes but is not limited to local password managers, password managers provided as browser extensions, enterprise password managers as well as hardware-based password managers.

Category of product	Technical description
4. Software that searches for, removes, or quarantines malicious software	Software products with digital elements, typically referred to as antivirus or antimalware, that detect or search for malicious software or code on devices, or remove or quarantine such software or code, in order to maintain the integrity, confidentiality, or availability of such devices. In the context of this category of products, malicious software means software containing malicious features or capabilities that can cause harm directly or indirectly to the user and/or the computer system, such as viruses, worms, ransomware, spyware and trojans. This category includes but is not limited to software that detects or searches for malicious software in real-time or manually, rootkit detection and rescue disks with the core functionality of searching, removing or quarantining malicious software.
5. Products with digital elements with the function of virtual private network (VPN)	Products with digital elements that establish an encrypted logical tunnel that is constructed from the system resources of a physical or virtual network. This category includes but is not limited to virtual private network clients, virtual private network servers and virtual private network gateways.
6. Network management systems	Products with digital elements that manage connected network elements, such as servers, routers, switches, workstations, printers or mobile devices, by monitoring them and controlling their network operations and configuration. This category includes but is not limited to end-to-end management systems and dedicated configuration management systems, such as controllers for software-defined networking.
7. Security information and event management (SIEM) systems	Products with digital elements that collect data from multiple sources, analyse and correlate that data and present it as actionable information for security-related purposes, such as threat and incident detection, forensic analysis or compliance purposes.
8. Boot managers	Software products with digital elements that manage the process of initial system startup after power on/restart by initialising hardware, loading or transferring control to the operating system environment or system resources, and selecting boot options. This category includes but is not limited to UEFI firmware, single-stage and multi-stage boot loaders.
9. Public key infrastructure and digital certificate issuance software	Products with digital elements used as part of a public key infrastructure (PKI) that manage the validation, creation, issuance, distribution, status publication, renewal or revocation of digital certificates, or the generation, storage, escrow, exchange, destruction or rotation of cryptographic keys associated with such digital certificates. This category includes but is not limited to key management systems, digital certificate management systems, online certificate status protocol responders and all-in-one PKI solutions.

Category of product	Technical description
10. Physical and virtual network interfaces	Physical network interfaces are products with digital elements that directly connect a device to a network via an application programming interface (API) provided by the interface drivers, typically operating at the data link layer, and that feature hardware adapters to transmission media with corresponding firmware, typically operating at the physical and data link layer. Virtual network interfaces are products with digital elements that directly or indirectly connect a device to a network via an API that emulates that of drivers of physical network interfaces, typically operating at the data link layer. This category includes but is not limited to wired and wireless network interface cards, controllers and adapters, such as for Wi-Fi, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee, or Fieldbus, as well as purely virtual standalone products, such as virtual network interface cards, container network interfaces and VPN interfaces.
11. Operating systems	Software products with digital elements that provide an abstract interface of the underlying hardware and control the execution of software, and that may provide services such as computing resource management and configuration, scheduling, input-output control, managing data, and providing an interface through which applications interact with system resources and peripherals. This category includes but is not limited to real-time operating systems, general-purpose and special-purpose operating systems.
12. Routers, modems intended for the connection to the internet, and switches	Routers are products with digital elements that establish and control the flow of data between different networks by selecting paths or routes using routing protocol mechanisms and algorithms, typically operating at the network layer. This category includes but is not limited to wired and wireless routers, virtual routers and routers with or without modems.
	Modems intended for the connection to the Internet are hardware products with digital elements that use digital modulation and demodulation techniques to convert analogue signals from and to digital signals for IP-based communication. This category includes but is not limited to fibre modems, Digital Subscriber Line (DSL) modems, cable (DOCSIS) modems, satellite modems and cellular modems.
	Switches are products with digital elements that provide connectivity between networked devices through packet forwarding mechanisms and that have a management plane, typically implemented at the data link or network layer. This category includes but is not limited to managed switches, smart switches, multilayer switches, virtual security switches, programmable switches for software-defined networking and bridges such as wireless access points.

Category of product	Technical description
13. Microprocessors with security-related functionalities	Products with digital elements that are integrated circuits that carry out central processing functions relying on external memory and peripherals, including microcode and other low-level firmware. They additionally provide security-related functionalities, such as encryption, authentication, secure key storage, random number generation, trusted execution environment, or other hardware-based protection mechanisms, that aim to secure other products, networks or services beyond the microprocessor itself, such as secure boot chain, virtualization or secure communication interfaces.
14. Microcontrollers with security-related functionalities	Products with digital elements that are integrated circuits that carry out central processing functions integrating memory allowing the microcontroller to be programmable and typically also other peripherals, including microcode and other low-level firmware. They additionally provide security-related functionalities, such as encryption, authentication, secure key storage, random number generation, trusted execution environment, or other hardware-based protection mechanisms, that aim to secure other products, networks or services beyond the microcontroller itself, such as secure boot chain, virtualization or secure communication interfaces.
15. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities	Application specific integrated circuits (ASIC) with security-related functionalities are products with digital elements that are integrated circuits, fully or partially custom-designed to perform a specific function or implement a specific application, including microcode and other low-level firmware. They additionally provide security-related functionalities, such as encryption, authentication, secure key storage, random number generation, trusted execution environment, or other hardware-based protection mechanisms, that aim to secure other products, networks or services beyond the ASIC itself, such as secure boot chain, virtualization or secure communication interfaces.
	Field-programmable gate arrays (FPGA) with security-related functionalities are products with digital elements that are integrated circuits characterized by a matrix of configurable logic blocks designed to be reprogrammable after manufacturing to perform a specific function or implement a specific application, including microcode and other low-level firmware. They additionally provide security-related functionalities, such as encryption, authentication, secure key storage, random number generation, trusted execution environment, or other hardware-based protection mechanisms, that aim to secure other products, networks or services beyond the FPGA itself, such as secure boot chain, virtualization or secure communication interfaces.
16. Smart home general purpose virtual assistants	Products with digital elements that communicate on the public Internet, whether directly or via other equipment, that process demands, tasks or questions based on natural language prompts, such as through audio or written input, and that, based on those demands, tasks or questions, provide access to other services or control the functions of connected devices in residential settings. This category includes but is not limited to smart speakers with an integrated virtual assistant, and standalone virtual assistants that meet this description.

Category of product	Technical description
17. Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems	Products with digital elements that protect the physical security of consumers in a residential setting and which can be controlled or managed remotely from other systems, as well as hardware and software that centrally control such products. This category includes but is not limited to smart door locking devices, baby monitoring systems, alarm systems and home security cameras.
18. Internet connected toys covered by Directive 2009/48/EC of the European Parliament and of the Council ([1]) that have social interactive features (e.g. speaking or filming) or that have location tracking features	Internet connected toys that have social interactive features are products with digital elements that are covered by Directive 2009/48/EC, that communicate on the public Internet, whether directly or via any other equipment, and that have embedded technologies that enable inbound and outbound communication, such as keyboard, microphone, speaker or camera.
	Internet connected toys that have location tracking features are products with digital elements that are covered by Directive 2009/48/EC, that communicate on the public Internet, whether directly or via any other equipment, and that have technologies that enable tracking or inferring of the geographical location of the toy or its user. Where the toy merely detects the proximity of the user or of other toys by using sensing technologies, the toy is not to be considered to have location tracking features.
19. Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 ([2]) or (EU) 2017/746 of the European Parliament and of the Council ([3]) do not apply, or personal wearable products that are intended for the use by and for children	Personal wearable products to be worn or placed on a human body that have a health monitoring purpose are products with digital elements that are worn on the body directly or via clothing or accessories and that can, regularly or continuously, sense and further process information, including body metrics, relevant to the user's health, excluding products that fall within the scope of Regulation (EU) 2017/745 or of Regulation (EU) 2017/746. This category includes but is not limited to fitness trackers, smartwatches, smart jewellery, smart clothing and sports apparel that meet this description.
	Personal wearable products that are intended for the use by and for children are products with digital elements which can be worn or placed on the body, directly or via clothing or accessories, of individuals under the age of 14. This category includes but is not limited to child safety wearables.

([1]) Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj).

Class II

Category of product	Technical description
1. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments	Hypervisors are software products with digital elements that abstract and/or allocate computing resources and enable the execution, management and orchestration of virtual machines that are logically separated from each other and/or from the physical hardware. Hypervisors may run directly on hardware (bare metal), on top of an operating system, or within another virtual machine (nested virtualisation). In the context of this category of products, a virtual machine is a software-defined logical separation of a computing environment, which includes a virtualised set of hardware resources (e.g. CPU, memory, storage, network interfaces) and typically hosts its own operating system. This category includes but is not limited to type 1 hypervisors (bare metal), type 2 hypervisors (hosted on an operating system) and hybrid hypervisors.
	Container runtime systems are software products with digital elements that manage the execution and lifecycle of containers running on a single host operating system as isolated processes, allocating resources and allowing the management and orchestration of individual containers. In the context of this category of products, a container is a software-based execution environment that encapsulates one or more software components and their dependencies in a single package, enabling it to run independently and consistently.
2. Firewalls, intrusion detection and prevention systems	Firewalls are products with digital elements that protect a connected network or system from unauthorized access by monitoring and restricting data communication traffic to and from that network. This category includes but is not limited to network firewalls and application firewalls such as web application firewalls or filters and anti-spam gateways.
	Intrusion detection systems are products with digital elements that monitor traffic once it has entered the network environment for suspicious activity and detect or identify that an intrusion has been attempted, is occurring, or has occurred on a connected network or system. This category includes but is not limited to network-based intrusion detection systems and host-based intrusion detection systems.
	Intrusion prevention systems are products with digital elements composed of an intrusion detection system that actively responds to an intrusion to a connected network or system. This category includes but is not limited to network-based intrusion prevention systems and host-based intrusion prevention systems.

Category of product	Technical description
3. Tamper-resistant microprocessors	Products with digital elements that are microprocessors with security-related functionalities referred to in Table 'Class I', point 13, of this Annex, including tamper evidence, resistance or response, and which additionally are designed to provide protection of AVA_VAN level 2 or 3, as set out in the Common Criteria and the Common Evaluation Methodology.
4. Tamper-resistant microcontrollers	Products with digital elements that are microcontrollers with security-related functionalities referred to in Table 'Class I', point 14, of this Annex, including tamper evidence, resistance or response, and which additionally are designed to provide protection of AVA_VAN level 2 or 3, as set out in the Common Criteria and the Common Evaluation Methodology.

ELI: http://data.europa.eu/eli/reg_impl/2025/2392/oj

ANNEX II

CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

Category of product	Technical description
1. Hardware Devices with Security Boxes	Hardware products with digital elements that securely store, process, or manage sensitive data or perform cryptographic operations, and that consist of multiple discrete components, incorporating a hardware physical envelope providing tamper evidence, resistance or response as countermeasures against physical attacks. This category includes but is not limited to physical payment terminals, hardware security modules that generate and manage cryptographic elements, and tachographs that meet the above description.
2. Smart meter gateways within smart metering systems as defined in Article 2(23) of Directive (EU) 2019/944 of the European Parliament and of the Council [1] and other devices for advanced security purposes, including for secure cryptoprocessing	Smart meter gateways are products with digital elements that control communication between components in or connected to smart metering systems as defined in Article 2(23) of Directive (EU) 2019/944, and authorised third parties, such as utility providers. Smart meter gateways collect, process and store meter or personal data, protect data and information flows by supporting specific cryptographic needs, such as encryption and decryption of data, incorporate firewalling functionalities and provide the means to control other devices. This category includes but is not limited to smart meter gateways related to smart metering systems measuring electricity as defined in Article 2(23) of Directive (EU) 2019/944. It may also include smart meter gateways used in other smart metering systems measuring consumption of other sources of energy such as gas or heat, provided that the gateway meets this description.
3. Smartcards or similar devices, including secure elements	Secure elements are microcontrollers or microprocessors with security-related functionalities, including tamper evidence, resistance or response. They typically store, process, or manage cryptographic operations or sensitive data, such as identity credentials or payment credentials. Secure elements are designed to provide protection of at least AVA_VAN.4, as set out in the Common Criteria or the Common Evaluation Methodology. They can be discrete silicon or can be integrated into systems on chip (SoC). Secure elements can incorporate an application environment or an operating system, and can include one or more applications. This category includes but is not limited to Trusted Platform Modules (TPMs) and embedded Universal Integrated Circuit Card (UICC).
	Smartcards or similar devices are secure elements integrated into a carrier material, such as plastic or wood, in the shape of a card, or secure elements integrated into carrier materials taking other shapes. This category includes but is not limited to identity and travel documents, qualified signature cards, replaceable UICCs, physical payment cards, physical access cards, digital tachograph cards or wrist bands with integrated payment secure elements.

[1] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).