EUROPEAN
COMMISSION

Brussels, XXX
[…](2025) XXX draft

ANNEXES 1 to 2

ANNEXES

to the

Commission Implementing Regulation

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

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 identity lifecycle management, such as identity provisioning, maintenance, authentication, authorisation and deprovisioning, and including associated metadata. Privileged access management hardware and software are products with digital elements that authenticate and authorise users or devices, granting or denying access to digital resources or to physical locations. This category includes but is not limited to products with digital elements that have the core functionality of either or both identity management and privileged access management; authentication and access control readers; biometric readers; single sign-on software; federated identity management software and multi-factor authentication software.
2. Standalone and embedded browsers	Standalone browsers are standalone applications that fulfil the functions of browsers.
	Embedded browsers are browsers that are intended for integration into another system or application.
	In the context of this category of products, browsers are software products with digital elements that enable end users to access and interact with web content hosted on servers that are connected to networks such as the Internet.

3. Password managers	Products with digital elements designed to store passwords, locally on a device or on a remote server, with a view to facilitate password management, 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, browser-based password managers, enterprise password managers as well as hardware-based password managers.
4. Software that searches for, removes, or quarantines malicious software	Software products with digital elements, typically referred to as antivirus or antimalware, that search for malicious software or code, or remove or quarantine such software or code to prevent or mitigate system infection or compromise. In the context of this category of products, malicious software means software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the user and/or the user's computer system, such as viruses, worms, ransomware, spyware and trojans. This category includes but is not limited to software that 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, as well as software matching the above definition that is used as a component in other products, such as firewalls.
5. Products with digital elements with the function of virtual private network (VPN)	Products with digital elements enabling access to a restricted-use logical computer network that is constructed from the system resources of a physical or virtual network, typically implemented at layer 3 of the OSI reference model, including cases where products are ultimately intended to provide access from a restricted-use logical computer network to the public internet. This category includes but is not limited to virtual private network clients, virtual private network servers, virtual private network gateways and virtual private network concentrators.
6. Network management systems	Products with digital elements that collect information about and allow the configuration of network elements, such as servers, routers, switches, workstations, printers or mobile devices.

	This category includes but is not limited to network management systems that can be deployed on premise or on cloud.
7. Security information and event management (SIEM) systems	Products with digital elements that provide the ability to gather data, at least from network components, analyse that data and present it as actionable information for security purposes.
8. Boot managers	Software products with digital elements that allow users to select boot options or load the operating system kernel or some of its elements and other system resources into the main memory of a device after it has been powered-up or restarted. This category includes but is not limited to single-stage and multi-stage boot loaders as well as boot managers allowing users to select boot options.
9. Public key infrastructure and digital certificate issuance software	Products with digital elements used as part of a public key cryptography scheme to manage asymmetric cryptographic keys and digital certificates, including their creation, issuance, distribution, validation, renewal, storage or revocation. This category includes but is not limited to key management systems, digital certificate management systems and online certificate status protocol responders.
10. Physical and virtual network interfaces	Products with digital elements that are any physical port (such as wired electrical or optical interfaces, or wireless radio or infrared interfaces) or virtual interface, which are also intended to enable Internet Protocol (IP) based communication between devices, including the relevant device drivers required to operate such ports or interfaces. This category includes but is not limited to wired and wireless network interfaces, such as Wi-Fi, Ethernet, Zigbee, optical fibre or Bluetooth interfaces as well as corresponding virtual adapters.
11. Operating systems	Software products with digital elements that control the execution of programs and that may provide services such as resource allocation, scheduling, input-output control, and data management. This category includes but is not limited to real-time operating systems, operating systems for

	servers, mainframes and mobile devices, network operating systems and general-purpose operating systems.
12. Routers, modems intended for the connection to the internet, and switches	Routers are products with digital elements that are used to establish and control the flow of data between different Internet Protocol (IP) based networks by selecting paths or routes based upon routing protocol mechanisms and algorithms. This category includes but is not limited to wired routers, wireless routers and routers with or without modems intended for the connection to the Internet.
	Modems are products with digital elements that use digital modulation and demodulation techniques to convert analogue signals from and to digital signals, intended for the connection to the Internet, typically via an internet service provider. This category includes but is not limited to fibre modems, Digital Subscriber Line modems, cable (DOCSIS) modems, satellite modems and cellular modems.
	Switches are products with digital elements that provide connectivity between networked devices by means of internal switching mechanisms, with the switching technology typically implemented at layer 2 or layer 3 of the OSI reference model. This category includes but is not limited to unmanaged switches, smart switches and managed switches.
13. Microprocessors with security-related functionalities	Products with digital elements consisting of a general-purpose central processing unit and relying on external memory and peripherals to carry out other functions beyond mathematical and logic processing, and which provide countermeasures against logical attacks, specifically through the support of additional hardware components.
14. Microcontrollers with security-related functionalities	Products with digital elements consisting of a general-purpose central processing unit, with sufficient memory allowing the microcontroller to be programmable and typically other peripherals on a single chip, and which provide countermeasures against logical attacks, specifically through the support of additional hardware components.

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 consisting of an integrated circuit, fully or partially custom-designed to perform a specific function or implement a specific application, and which provides countermeasures against logical attacks, specifically through the support of additional hardware components.
	Field-programmable gate arrays (FPGA) with security-related functionalities are products with digital elements consisting of an integrated circuit characterized by a matrix of configurable logic blocks designed to be reprogrammable after manufacturing to perform a specific function or implement a specific application, and which provides countermeasures against logical attacks, specifically through the support of additional hardware components.
16. Smart home general purpose virtual assistants	Internet-connected products with digital elements that process natural language prompts allowing users to interact with the assistant and control connected devices in residential settings. This category includes but is not limited to smart speakers and virtual assistant software that meet this definition.
17. Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems	Products with digital elements intended to protect the physical security, including safety, of consumers in a residential setting and which can be controlled and managed remotely from other systems, as well as hardware and software intended to centrally control such products. This category includes but is not limited to smart door locking devices, baby monitoring systems, alarm systems, home security cameras and smart smoke detectors.
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.	Products with digital elements that are covered by Directive 2009/48/EC, connected or intended to be connected to internet, and that have embedded technologies that enable inbound and outbound communication, such as keyboard, microphone, speaker or camera, or technologies

[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).

speaking or filming) or that have location tracking features	that enable tracking of the geographical location of the toy or its user, such as GPS or Bluetooth based functionalities. This category does not include toys that do not track the full geographical location but merely detect the proximity of the toy to its user or to other toys.
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 can be 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.
	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.

[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 mediate access to physical computing resources and enable the execution and management of virtualised workloads, by running directly on a host, on top of an operating system, or on a combination of the two. This category includes but is not limited to type 1 hypervisors, type 2 hypervisors and hybrid hypervisors.
	Container runtime systems are software products with digital elements that manage the lifecycle of containers running on a host operating system, allocating resources and providing isolation between each container and the rest of the system, through operating system level or application-level virtualisation. In the context of this category of products, a container is a software product that encapsulates one or more software components and its dependencies in a single package, enabling it to run independently and consistently. This category includes but is not limited to low-level container runtimes and high-level container runtimes.
2. Firewalls, intrusion detection and prevention systems	Firewalls are products with digital elements that monitor and control data communication traffic to and from a connected network or system.
	Intrusion detection systems are products with digital elements used to detect or identify that an intrusion has been attempted, is occurring, or has occurred on a connected network or system.
	Intrusion prevention systems are products with digital elements composed of an intrusion detection system that is designed to actively respond to an intrusion to a connected network or system, typically by blocking suspicious traffic.

3. Tamper-resistant microprocessors	Products with digital elements consisting of microprocessors with security-related functionalities, that provide countermeasures against physical attacks, including tamper evidence, resistance or response.
4. Tamper-resistant microcontrollers	Products with digital elements consisting of microcontrollers with security-related functionalities, that provide countermeasures against physical attacks, including tamper evidence, resistance or response.

ANNEX II

CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

Category of product	**Technical description**
1. Hardware Devices with Security Boxes	Hardware products with digital elements that incorporate a hardware physical envelope providing countermeasures against physical attacks, including tamper evidence, resistance or response, and that are designed to securely store, process, and manage sensitive data and cryptographic operations. This category includes but is not limited to payment terminals, hardware security modules, and tachographs that meet the above definition.
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[4] and other devices for advanced security purposes, including for secure cryptoprocessing	Products with digital elements that control communication between components in smart metering systems as defined in Article 2(23) of Directive (EU) 2019/944 and authorised third parties, such as utility providers, as well as other devices within the smart grid infrastructure, that collect, process and store meter data, and that also protect data and information flows by supporting specific cryptographic needs, such as encryption and decryption of data, and by firewalling between the wider network and the local network. 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 other smart metering systems measuring consumption of other sources of energy such as gas or heat.
3. Smartcards or similar devices, including secure	Secure elements are hardware components that incorporate a tamper-resistant microcontroller

[4] 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).

elements	or microprocessor and an application environment or operating system, and may include one or more applications, designed to securely store, process, and manage sensitive data and cryptographic operations. This category includes but is not limited to Trusted Platform Modules (TPMs) or embedded sim cards.
	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 replaceable sim cards, payment cards, physical access cards, digital tachograph cards or wrist bands with integrated secure elements.