Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
Eurosmart	Annex II	3. Smartcards or similar devices, including secure elements	te	**(1) Secure Element - Terminology Update – "Embedded UICC"** All references to "embedded SIM cards" should be replaced with "embedded UICCs", in accordance with ETSI TS 103 383 V12.8.0, which defines and standardizes this terminology. To eliminate ambiguity, we suggest the followings : • Replace all instances of SIM with UICC • Clarify that this category also includes chips containing an integrated Secure Element (iSE) or an integrated UICC (iUICC) **(2) Secure Element - Terminology Update – Integrated Secure Element (iSE)** An Integrated Secure Element (iSE) is a technology in which a single integrated circuit (IC) combines components that were previously discrete—for example, a modem, physical interface, and a Secure Element.The goal is to reduce physical size by consolidating functionality into a single chip, eliminating the need for a printed circuit board (PCB). In this configuration, the Secure Element is considered integrated, and referred to as an iSE. **(3) Secure Element - Clarification of "Application Environment"** The term "application environment" should be explicitly defined, as its current usage may be unclear. The application environment refers to the software and libraries:	A secure element is made of microcontroller (*1) (MCU) and/or microprocessor (MPU) (*1), , resistant to an attacker with moderate or high attack potential, with an application environment or operating system, which may include one or more applications. The combination of all these hardware and software elements must be resistant to an attacker with moderate or high attack potential. Secure elements are designed to securely store, process, and manage sensitive data and cryptographic operations while protecting against physical attacks through tamper evidence, resistance, or response mechanisms. Application environment designates softwares and librairies (1) loaded or executed within the tamper-resistant microcontroller or microprocessor and (2) offering basic services to interact with the hardware services provided with the tamper-resistant microcontroller or microprocessor. Application environment can include (1) cryptographic libraires, (2) loader, (3) firmware (low level software managing MCU/MPU init, boot and basic operations), (4) drivers and (5) hardware abstraction level." This category includes but is not limited to Trusted Platform Modules (TPMs), embedded UICC, chip containing an integrated secure elements or chip containing an integrated UICC". Embedded eUICCs are covered by GSMA scheme via SGP.06 and SGP.07 (*1)These products are resistant to attackers with moderate or high attack potential as defined in the documents: - "EUCC Scheme - State-of-the-art document - Application of attack potential to smart cards and similar devices, v1.2 , August 2024", with a rating at 31 and above. This document takes into consideration the evolution of the state of the art, studied in the "JHAS group" of the EUCC ISAC, based on the security risk assessment and the testing done accordingly - Table 4, Example definitions for the five levels of attack potential

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
				• Loaded or executed within the tamper-resistant microcontroller (MCU) or microprocessor (MPU), and • Providing basic services that interface with the hardware functionalities of the MCU/MPU. The application environment typically includes: • Cryptographic libraries • Loaders • Firmware **(4) Secure Element - Clarification of Secure Element Definition – Tamper Resistance Requirement** The proposed definition of secure element implies that any combination of a tamper-resistant MCU/MPU and an application environment or OS constitutes a secure element, regardless of the actual level of physical attack resistance. This interpretation is problematic. Secure elements must be based on hardware and software that offer a high level of physical tamper resistance. This is a fundamental requirement. A product lacking such hardware-level protection cannot be considered a secure element. Furthermore: • Other product characteristics (e.g., form factor) should not be highlighted unless they are directly related to the core security functionality.	(AP1-AP5), METHODOLOGY FOR SECTORAL CYBERSECURITY ASSESSMENTS, ENISA, EU Cybersecurity Certification Framework, SEPTEMBER 2021 - Table 1, Guidance on maximum timeframes for the vulnerability impact analysis, EUCC SCHEME GUIDELINES ON VULNERABILITY MANAGEMENT AND DISCLOSURE, ENISA, Version 1.1, January 2025 - Article 22, from EUCC regulation EU 2024/482 - Application of Attack Potential to Hardware Devices with Security Boxes, Joint Interpretation Library (JIL)

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
				• To prevent confusion with similarly shaped or named products lacking sufficient tamper resistance, an additional note should be included to scope the intended use cases based on applicability and security impact.	
Eurosmart	Annex II	3. Smartcards or similar devices, including secure elements	te	**(1) Smartcard -Clarification on when a Smartcard or Similar Device Must Be Considered Critical** Specify when a smartcard or similar device must be considered critical, and recall the definition of a product resistant to attackers with high attack potential (AVA_VAN.5). **(2) Smartcard - Core Security Functionality of Smartcard-Type Products** The core functionality of a product categorized as a smartcard, where the functionality is provided by the embedded secure element, is its high level of tamper resistance. Other product features, such as the form factor can or not bring additional security properties depending of its design and usage. **(3) Smartcard - Appropriateness of the given Use Cases** ETSI EUSR : The wrist bands used for fitness tracking would obviously fall within the definition of this category without additional uses case as payment Such products typically integrate a microcontroller or microprocessor provisioned with appropriate software to perform its functionalities. From there, a Security by desigh	Smartcards are secure elements integrated into a carrier material—such as plastic or wood—in the shape of a card, or secure elements embedded into carriers of other shapes. This category includes products whose core functionalities are resistant to attackers with high attack potential, as defined in the document "EUCC Scheme - State-of-the-Art Document - Application of Attack Potential to Smart Cards and Similar Devices," v1.2, August 2024, with a rating of 31 or above. This document reflects the evolution of the state of the art, as studied by JHAS within the EUCC ISAC, based on security risk assessments and corresponding testing. This category includes, but is not limited to, replaceable consumer UICCs, payment cards, physical access cards, digital tachograph cards, and wristbands with integrated payment secure elements. Products with digital elements with Smartcard form factor, integrated into a carrier material but with a security risk assessment focused on a low and moderate attack potential, are not part of this category. These should instead be considered as part of the class: "Microcontrollers with security-related functionalities," Class I.

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
				approach should determine the countermeasures to be implemented in such products, which may include hardware security features provided by the processing elements if the security sensitivity of the functionality and the nature of the intended operating environment justify such protection. However, if for the above reason or based on other practical and economic constraints, a manufacturer decides to use a tamper-resistant processing element to implement such wristband, the product would then fall into the definition of "smartcard" ("wrist bands with integrated secure element" being explicitly mentioned in their definition), ranked as "critical" and then subject to much higher scrutiny by the regulators. Such difference of treatment is not justified by a risk-based approach and may discourage adoption of hardware based security controls where they might be relevant. The consistency between all category definitions should be reviewed to eliminate potential overlaps and to ensure that the use of hardware implementing security countermeasure is encouraged as a security control for products that justify such measures. The inclusion of "wrist bands with integrated secure element" as a smart card form factor should be removed, so that a tamper resistant microcontroller/microprocessor or a secure element integrated in a wristband used for	

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
				fitness tracking could be treated as a component integrated in such products, rather than changing the category of the final product.	
Eurosmart	Annex II	1. Hardware Devices with Security Boxes	te	In order to avoid over-regulation, the technical description should be updated to explicitly exclude hardware devices with security boxes already covered under either: the EUDI regulation (such as QSCD used for Remote Server Signing); and tested as part of security testing under Chapter IV of DORA. These regulations already introduce significant overheads linked to cybersecurity for products sold into these markets and where the commission should take action to exclude these device from this regulation.	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. Hardware devices with security boxes already subject to threat based security testing under Regulations (EU) 910/2014 EU DI Regulation or Regulation (EU) 2022/2554, DORA are not included in this product category.
Eurosmart	Annex I, Class I	13. Microprocessors with security-related functionalities	te	New definition	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 resistance against logical attacks (such as attacks based on code execution, command exchanges, or spying communication allowing to extract exploitable information), through the support of hardware. They may include an application environment or Operating System. Examples of Products with Digital Elements with this configuration in this category include but are not limited to microprocessors with NFC, BLE, or WiFi functionality. Application environment designates softwares and libraries (1) loaded or executed within microcontroller or microprocessor and (2)

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
					offering basic services to interact with the hardware services provided with the microcontroller or microprocessor. Application environment can include (1) cryptographic libraries, (2) loader and (3) firmware.
Eurosmart	Annex I, Class I	14. Microcontrollers with security-related functionalities	te	New definition	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 resistance against logical attacks (such as attacks based on code execution, command exchanges, or spying communication allowing to extract exploitable information), through the support of hardware.They may include an application environment or Operating System. Examples of Products with Digital Elements with this configuration in this category include but are not limited to microprocessors with NFC, BLE, or WiFi functionality.
Eurosmart	Annex I, Class I	15. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities	te	New definition	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 provide resistance against logical attacks (such as attacks based on code execution, command exchanges, or spying communication allowing to extract exploitable information), through the support of hardware.
Eurosmart	Annex I, Class II	3. Tamper-resistant microprocessors	te	New definition	Products with digital elements consisting of microprocessor with security-related functionalities, that provide resistance against physical attacks. Tamper resistance has different levels depending on the complexity of the attacks which are resisted and is measured in terms of time, equipment, expertise, and knowledge needed to perform the attack. Products in this category provide resistance against attack level enhanced-basic*. They may include an application environment or Operating System. Examples of Products with Digital Elements include but are not limited to General purpose

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
					central processing unit containing a secure subsystem. **Note : enhanced basic as defined in the document "EUCC Scheme - State-of-the-art document - Application of attack potential to smart cards and similar devices, v1.2 , August 2024". Respectively, enhanced basic covers the attack range defined as AVA_VAN.3 , see as well EN 18037 Appendex D.*
Eurosmart	Annex I, Class II	4. Tamper-resistant microcontrollers	te	New definition	Products with digital elements consisting of microcontroller with security-related functionalities, that provide resistance against physical (such as attacks manipulating or interacting with the hardware to extract information, disrupting its operation, or modifying its behavior). Tamper resistance has different levels depending on the complexity of the attacks which are resisted and is measured in terms of time, equipment, expertise, knowledge needed to perform the attack. The resistance shall protect against attack level enhanced-basic *. They may include an application environment or Operating System. Examples of Products with Digital Elements include but are not limited to General purpose central processing unit containing a secure subsystem. **Note : enhanced basic as defined in the document "EUCC Scheme - State-of-the-art document - Application of attack potential to smart cards and similar devices, v1.2 , August 2024". Respectively, enhanced basic covers the attack range defined as AVA_VAN.3 , see as well EN 18037 Appendex D.*
Eurosmart	Main body	Recital 1	ge	Question about the last part of the sentence "…or which would be subject to strict conformity assessment procedures.": How to make apply a strict conformity assessment procedure for products relying on private schemes: EMVCo for banking products or GSMA eSA for eUICCs, PCI PTS	

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
				for payment terminals, PCI standards (SPoC, MPoC, CPoC, PTS, HSM). How to reuse the evaluation results to demonstrate their conformance against CRA's essential requirements ? A guide could be edited to clarify this aspect.	
Eurosmart	Main body	Recital 2	ge	The core functionality of a product is supposed to determine if a product fits into the description of a category. However, current definitions of categories do not describe core functionalities, fundamental features or capabilities. Furthermore, the primary purpose of a "final" product with digital elements must invitably refer to its role in its business vertical. Conversely, intermediate products may have different roles depending on their end use in different business verticals.It is important to remember here that an appropriate Risk Assessment is highly dependent on the product's role in its business vertical and on the criticality of that vertical. A guide could be edited to clarify this aspect	
Eurosmart	Main body		ge	Reading carefully the definition of product categories, it appears that in some cases, the same product could fall into two different product categories, each of different level. At least the following example has been identified: • A smartcard/SE containing an application and keys used as a CA (PKI component) to create digital certificates. In that case such PwDE falls into critical and important/class I category.	

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
				• A recital - or text in a recital - may be useful to clarify that in such cases, the highest classification applies.	
Eurosmart	Annex I, Class I	1. Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers	te	The wording used in this definition is unclear whci may lead to major ambiguity regarding the scope of PWDE covered by this definition. Therefore we suggest to: (1) Clarify the meaning of "identity" by refering to the meaning set in ISO/IEC 24760-1 => By doing so, it will be clear that "identity" does refer to any attribute relating to an entity. It will clear debate about the meaning of identity (unique identifier, set of attribute comprising the PID,...). it shall be noted that this definition applies to (1) a natural person, (2) a legal person or (3) an object. (2) Clarify the meaning of "identity management" by refering to ISO/IEC 24760-1 (3) Replace the wording "identity provisioning" which is very unclear by "identity registration" as defined in ISO/IEC 24760-1 (4) Replace the wording "deprovisioning" by "de registration" (5) Clarify the meaning of "maintenance" by refering to ISO/IEC 24760-1 (§10) (6) Clarify the meaning of "authentication" by refering to ISO/IEC 24760-1 (§9) (7) Clarify the meaning of "authorization" by refering to ISO/IEC 24760-1 (§9)	Change text as follows: "Identity management systems are products with digital elements that provide mechanisms for identity management, such as identity registration, maintenance, authentication, authorisation and deregistration, and including associated metadata. Identity, identity management, registration, maintenance, authentication, and authorization have the meaning as defined in ISO/IEC 24760-1. [...]"
Eurosmart	Annex I, Class I	1. Identity management systems and privileged	te	It is unclear whether software for payment tokenization platforms are included in the "Identity management systems and privileged access	Add the following clarification:"software for payment tokenization platforms, insofar they are covered by DORA when operated, are excluded from that category of product."

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
		access management software and hardware, including authentication and access control readers, including biometric readers		management software and hardware, including authentication and access control readers, including biometric readers" category. These PwDEs are not intended to consumer but exclusively to companies - such as banks - willing to set up and operate payment tokenization platforms.Once these PwDE are installed and operated, they are subject to DORA and thus subject to the corresponding obligations for cyberresilience, vulnerability handling and reporting which already ensures a high level of cyber resilience. However, in that case, these PwDEs would be subject to 2 conformity assessments, a third party assessment stemming from the CRA, and the assessment carried out by the operator of the PwDE - and its ex post audits by its supervision authority - as part of its obligations stemming from DORA. This double conformity assessment will result in a higher cost for the operator of the PwDE, more complexity for both the manufacturer and the operator of the PwDE, and a longer time to market. Therefore, to limit the conformity obligations - and the related costs and time to market - stemming from the CRA and DORA for the manufacturer and the operator of that PwDE, we suggest to exclude software for payment tokenization platforms from that product category.This approach will not impede the overall cyber resilience of PwDE, as it will still remain subject to a cybersecurity risk assessment, vulnerability handling and reporting	

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
				as per the CRA, and to an assessment by its operator and audits by supervision authority as per DORA. While streamlining the time to market and reducing cost, it will put the emphasize on the assessment of the PwDE configured to be operated.	
Eurosmart	Annex I, Class I	1. Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers	te	This category is very large and may cover various types of Products with Digital Element. In particular it includes Products with Digital Elements which are exclusively intended to, used by and sold to companies/operator and not to consumer/end user. Once these PwDEs are installed and operated, they may be subject to NISD2 (e.g. as part of " ICT-service management", “Public Administration entities”, “Digital Infrastructure/(non) Qualified trust service providers”) and thus subject to the corresponding obligations for cyberresilience and vulnerability handling (article 21 of NISD2) and reporting (article 23 of NISD2) which already ensures a high level of cyber resilience. However, in that case, these PwDEs would be subject to 2 conformity assessments, a third party assessment stemming from the CRA, and the assessment carried out by the operator of the PwDE - and its ex post audits by its supervision authority - as part of its obligations stemming from NISD2. This double conformity assessment will result in a higher cost for the operator of the PwDE, more complexity for both the manufacturer and the operator of the PwDE, and a longer time to market. Therefore, to limit the conformity obligations - and	Add the following clarification: "Product with Digital Elements which are covered by NISD2 when operated, are excluded from that category of product."

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
				the related costs and time to market - stemming from the CRA and NISD2 for the manufacturer and the operator of that PwDE, we suggest to exclude from that category of product, PwDE which are subject to NISD2 when operated. This approach will not impede the overall cyber resilience of PwDE, as it will still remain subject to a cybersecurity risk assessment, vulnerability handling and reporting as per the CRA, and to an assessment by its operator and audits by supervision authority as per NISD2. While streamlining the time to market and reducing cost, it will put the emphasize on the assessment of the PwDE configured to be operated.	
Eurosmart	Annex I, Class I	1. Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers	te	The first paragraph reads the following:"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."Yet, there are very specific categories of identity management systems which are designed to only allow identification and/or authentication of entities (e.g. persons) without supporting any access control or authorization, either directly - as these systems do not perform any authorization, or indirectly - as these systems do not support any privileged access management systems. Examples of these systems are (1) biometric systems which are used to identify or authenticate	Add the following clarification:"products with digital elements that provide mechanisms for identity lifecycle management, such as identity registration, maintenance, authentication, and deprovisioning, and including associated metadata, but which (1) do not implement authorisation and (2) are not intended to be used by any Privileged Access Control systems are not included in that product category."

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
				criminals to support police during investigation, (2) biometric systems used to identify or authenticate an individual in a crowd, of (3) biometric systems used to verify that the biometrics of an applicant requesting an identity document of digital identity has not already been registered under another identity (deduplication).These types of identity management systems are not intended to provide or allow any access to physical or digital resources, but only to allow identification and authentication to support administrative decision. These identification and authentication are aimed to obtain/gather information which is subsequently processed by an operator (e.g. police, public officer,...) to support an administrative decision. Such types of Identity management systems do not meet any of the criteria laid down in article 7.2 of the CRA to classify a PwDE as important, in particular the one in 7.2(a) regarding "securing authentication and access" and therefore should not be classified as "important".	
Eurosmart	Annex I, Class I	1. Identity management systems and privileged access management software and hardware, including authentication and access control readers, including	te	The second paragraph reads the following: "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." Physical access control systems comprise several functions which are (1) authentication, (2) authorization, and (3) granting/denying access. These functions may be achieved by several components (PwDE) integrated by a manufacturer.	We suggest to: -replace "granting and denying access" by "in order to grant or deny access" -add the following clarification "For physical access control, the system and hardware allowing the physical access (e.g. gate or door) are not included in that category of product."

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
		biometric readers		While the first two ones are likely to be achieved by software and/or hardware, in some settings the third one may be achieved by a device comprising a gate or a door which opens or not. When considering physical access control system, the wording "granting and denying access" raises ambiguity, as it could be understood as if the software and hardware controling the opening or not of the gate or door would be included in that category of product. It should not be the case as those do not implement privileged access management but implement the output of the privilege access management system. To clear this ambiguity, we suggest to: • replace "granting and denying access" by "in order to grant or deny access" • add the following clarification "For physical access control, the system and hardware allowing the physical access (e.g. gate or door) are not included in that category of product."	
Eurosmart	Annex I, Class I	1. Identity management systems and privileged access management software and hardware, including authentication and access control readers,	te	The case of products carrying out verification of correctness of executable code should be clarified. These products may be manifold, e.g (1) tools to verify that a compiled code abide by pre defined rules (tool for verification) or (2) Virtual Machine which verifies the consistency of the code being executed.These types of products should not be mixed with "Software that searches for, removes, or quarantines malicious software".In order to clear any ambiguity, the following clarification should be added:"Products with digital elements	Add the following clarification:"Products with digital elements carrying out verification of correctness of executeble code are not "Software that searches for, removes, or quarantines malicious software".

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
		including biometric readers		carrying out verification of correctness of executable code are not "Software that searches for, removes, or quarantines malicious software".	
Eurosmart	Annex I, Class I	6. Network management systems	te	This category is very large and may cover various types of Products with Digital Element. In particular it includes Products with Digital Elements which are exclusively intended to, used by and sold to companies/operator and not to consumer/end user. Once these PwDEs are installed and operated, they may be subject to NISD2 (e.g. as part of "Digital infrastructure/Providers of public electronic communications networks") and thus subject to the corresponding obligations for cyberresilience and vulnerability handling (article 21 of NISD2) and reporting (article 23 of NISD2) which already ensures a high level of cyber resilience. However, in that case, these PwDEs would be subject to 2 conformity assessments, a third party assessment stemming from the CRA, and the assessment carried out by the operator of the PwDE - and its ex post audits by its supervision authority - as part of its obligations stemming from NISD2. This double conformity assessment will result in a higher cost for the operator of the PwDE, more complexity for both the manufacturer and the operator of the PwDE, and a longer time to market. Therefore, to limit the conformity obligations - and the related costs and time to market - stemming from the CRA and NISD2 for the manufacturer and the operator of that PwDE, we suggest to exclude	Add the following clarification: "Network management systems which are covered by NISD2 when operated, are excluded from that category of product."

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
				from that category of product, PwDE which are subject to NISD2 when operated. This approach will not impede the overall cyber resilience of PwDE, as it will still remain subject to a cybersecurity risk assessment, vulnerability handling and reporting as per the CRA, and to an assessment by its operator and audits by supervision authority as per NISD2. While streamlining the time to market and reducing cost, it will put the emphasize on the assessment of the PwDE configured to be operated.	
Eurosmart	Annex I, Class I	9. Public key infrastructure and digital certificate issuance software	te	The text reads:"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, [...]"Usually creation and issuance of digital certificate includes HSM. It shall be made clear that HSM are excluded from this category as they fall under the critical category2/The text reads "digital certificates" which seems too restrictive. Such definition seems to exclude the case of the other items which can be created by a end entity of PKI using a “digital certificate” and the key it certifies, such as signed code, sealed data or encrypted message. Therefore we suggest talking of "digital certificates or signed or encrypted data created using digital certificates"3/The current definition covers the distribution and storage of "digital certificate", which is not a security operation as it is what PKI is made for, to ensure storage and distribution of “digital certificate” in an uncontrolled environment. In addition, these	1/Clarify that HSM are excluded from that category2/Replace "digital certificate" by "signed or encrypted data including digital certificates"3/Change the first paragraph as follows:"Products with digital elements used as part of a public key cryptography scheme to manage asymmetric cryptographic keys, including their creation, distribution, renewal, storage or revocation.Products with digital elements used as part of a public key cryptography scheme to manage digital certificates or signed or encrypted data created using digital certificates, including their creation, issuance, validation, renewal or revocation."

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
				operations could be achieved by a large diversity of tools, such as mail or file management tools. On the other hand, the distribution and storage of "asymmetric cryptographic keys" is critical, and PwDE supporting these features should be part of this product category? In addition the issuance or validation of “asymmetric cryptographic keys” is meaningless. Therefore the definition should be reviewed accordingly to separate the case of “asymmetric cryptographic keys” and “digital certificates’.	
Eurosmart	Annex I, Class I	10. Physical and virtual network interfaces	te	The definition is bound to IP protocol and network. Therefore if a PwDE implements another protocol, it would not fall into that definition. Therefore we suggest to extend this definition to any network protocol of the layer 3 of OSI model (see https://en.wikipedia.org/wiki/Network_layer).	Change definition as follows: "[...] which are also intended to enable communication between devices at the layer 3 of the OSI model, [...]."
Eurosmart	Annex I, Class I	11. Operating systems	te	The description provided for Operating System also applies to patch of Operating System. Thus this definition could create confusion as it could lead to consider that a patch belongs to that product categorie (and thus is PwDE) Yet, as per the CRA, the patch is not a PwDE, and is not subject to the CRA obligations. It is the PwDE modified by the patch which is subject to the obligations of the CRA. To avoid confusion, we suggest to: (1) clarify that a patch of operating system is excluded from that product categorie as it is not a PwDE but intended to modify an existing operating system (PwDE);	1/Add the following clarification : This category does not include patch of operating systems. 2/consider describing the difference between a PwDE and a patch in a guidance to be prepared;

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
				(2) consider describing the difference between a PwDE and a patch in a guidance to be prepared.	
Eurosmart	Annex I, Class I	11. Operating systems	te	The current definition seems to be very broad. As such, any Virtual Machine would fall into that definition, even if being executed over an Operating System. Therefore we suggest to refine that definition to product with digital element which may provide material ressource allocation.	Change the definition as follows: "[...] may provide services such as MATERIAL resource allocation, [...]"
Eurosmart	Annex I, Class I	12. Routers, modems intended for the connection to the internet, and switches	te	(1) The proposed definition of router seems too broad, as it is defined as establishing and controlling the flow of data between different Internet Protocol (IP) based networks. As such, any device triggering and controlling a flow of data but through which the data do not flow would qualify as "routers". This is the case for instance for an eSIM profile used to trigger and configure the access to a network of a mobile phone : thanks to the eSIM profile, the mobile phone connects to a first IP based network through the APN (via the mobile network), and then connects to another IP based network to reach the requested service. In that case such product would be considered as a router while it does not intervene in the flow of data. Therefore, to better target the right category of product, it should be clarified that these products do also transmit and receive the flow of data.	1/Change the definition of router as follows: "Routers are products with digital elements that are used to establish, control, TRANSMIT AND RECEIVE the flow of data between different Internet Protocol (IP) based networks [...]." 2/Extend the scope to any networks and remove any mention of Internet Protocol.

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
				(2) The definition is bound to IP protocol and network. Therefore if a PwDE implements another protocol, it would not fall into that definition. Therefore we suggest to extend this definition to any network protocol of the layer 3 of OSI model (see https://en.wikipedia.org/wiki/Network_layer).	
Eurosmart	Annex I, Class I	17. Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems	te	The functionality of sub-categorie "smart door locking devices" seems to overlap with the "Privileged access management software and hardware".	Add the following clarification : "in comparison "Smart Door locks", are Smart home products with security functionalities (17) , which can be controlled or managed remotely from respective "privileged access " systems".
Eurosmart	Annex I, Class II	1. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments	te	The definition of "container runtime systems" relies on the definition of "container" (provided in paragraph 2). Yet this second paragraph creates confusion, and it could be understood that "containers" are also part of this product category. If so it would mean that users of "container runtime systems", when generating "containers" would be subject to third party conformity assessment for their "containers". It would be very cumbersome for users and it is very likely that users will not be able to carry out that third party assessment as they do not have knowledge of the internal design of the "container runtime systems" and thus "containers". Therefore we suggest to explicit clarify that	After the second paragraph, add the following clarification: "containers as described above are excluded from this product category."

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Org.	Doc. type	Item number	Type of comment *	Comments	Proposed change
				"containers" are not included in that product category.	
Eurosmart	Annex I, Class II	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 and other devices for advanced security purposes, including for secure cryptoprocessing	te	It is unclear whether this description also includes Products with Digital Elements used by entities in charge of solely managing the smart metering system but not to collect the meter information.	

* **Type of comment:** **ge** = general **te** = technical **ed** = editorial