2025/2392

1.12.2025

REGOLAMENTO DI ESECUZIONE (UE) 2025/2392 DELLA COMMISSIONE

del 28 novembre 2025

relativo alla descrizione tecnica delle categorie di prodotti con elementi digitali importanti e critici a norma del regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza) ([1]), in particolare l'articolo 7, paragrafo 4,

considerando quanto segue:

(1) Il regolamento (UE) 2024/2847 stabilisce norme sulla cibersicurezza dei prodotti con elementi digitali. L'allegato III di tale regolamento stabilisce in particolare categorie di prodotti con elementi digitali importanti che, all'immissione sul mercato, sono soggetti a procedure di valutazione della conformità più rigorose di quelle applicabili ad altri prodotti con elementi digitali. L'allegato IV del regolamento (UE) 2024/2847 stabilisce categorie di prodotti con elementi digitali critici per i quali i fabbricanti potrebbero essere tenuti a ottenere un certificato europeo di cibersicurezza nell'ambito di un sistema europeo di certificazione della cibersicurezza a norma del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio ([2]) o che sarebbero soggetti a una valutazione obbligatoria della conformità da parte di terzi all'immissione sul mercato.

(2) A norma dell'articolo 7, paragrafo 1, e dell'articolo 8, paragrafo 1, del regolamento (UE) 2024/2847, la funzionalità principale di un prodotto con elementi digitali determina se tale prodotto con elementi digitali è conforme alla descrizione tecnica di una categoria di prodotti con elementi digitali importanti o critici e di conseguenza le procedure di valutazione della conformità applicabili.

(3) Al momento di sviluppare un prodotto con elementi digitali e al fine di ottenere l'insieme di funzionalità desiderate, generalmente i fabbricanti integrano nei propri prodotti con elementi digitali altri componenti che sono anch'essi prodotti con elementi digitali e sono in grado di conformarsi alla descrizione tecnica di una categoria di prodotti importanti o critici. A norma del regolamento (UE) 2024/2847, un prodotto con elementi digitali è soggetto alle procedure di valutazione della conformità applicabili ai prodotti con elementi digitali importanti o critici se tale prodotto nel suo complesso è un prodotto importante o critico di cui agli allegati III e IV di tale regolamento. Ad esempio, l'integrazione di un browser incorporato come componente di un'app di notizie da utilizzare negli smartphone non implica di per sé che tale app sia soggetta alla procedura di valutazione della conformità applicabile ai prodotti con elementi digitali la cui funzionalità principale è «browser autonomi e incorporati». Tuttavia, conformemente al regolamento (UE) 2024/2847, il fabbricante deve garantire che il prodotto con elementi digitali nel suo complesso sia conforme ai requisiti essenziali di cibersicurezza. Il fabbricante deve pertanto valutare la sicurezza dell'intero prodotto, se del caso tenendo conto della sicurezza dei componenti integrati o delle funzionalità integrate. Ad esempio, per dimostrare che il proprio prodotto con elementi digitali è conforme al regolamento (UE) 2024/2847, il fabbricante di un'app di notizie deve dimostrare che tale app nel suo complesso soddisfa i requisiti applicabili, se del caso tenendo conto della sicurezza del browser incorporato che è integrato nell'app.

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

([2]) Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») (GU L 151 del 7.6.2019, pag. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) Il fatto che un prodotto con elementi digitali svolga funzioni diverse o aggiuntive rispetto a quelle dettagliate nelle descrizioni tecniche di cui al presente regolamento non significa di per sé che il prodotto con elementi digitali non abbia la funzionalità principale di una categoria di prodotti di cui agli allegati III e IV del regolamento (UE) 2024/2847. Ad esempio, i prodotti con elementi digitali la cui funzionalità principale è «sistemi operativi» comprendono spesso un software che svolge funzioni ausiliarie non incluse nella descrizione tecnica di tale categoria di prodotti, come calcolatrici o semplici editor di grafica. I prodotti con elementi digitali spesso incorporano anche componenti che hanno la funzionalità di un altro prodotto con elementi digitali importante o critico, come un sistema operativo che integra la funzionalità browser o un router che integra la funzionalità firewall. Tuttavia ciò non significa di per sé che la funzionalità principale di tali prodotti con elementi digitali non sia rispettivamente «sistemi operativi» o «router, modem per la connessione a Internet e switch».

(5) D'altro canto, un prodotto con elementi digitali in grado di svolgere le funzioni di una categoria di prodotti di cui agli allegati III e IV del regolamento (UE) 2024/2847 ma la cui funzionalità principale è di per sé diversa da quella di tale categoria di prodotti non deve essere considerato conforme alla descrizione tecnica della categoria di prodotti in questione. Ad esempio, un software di orchestrazione, automazione e risposta della sicurezza (SOAR) è spesso in grado di svolgere le funzioni di prodotti con elementi digitali appartenenti alla categoria «sistemi di gestione delle informazioni e degli eventi di sicurezza (sistemi SIEM)», ovvero raccogliere dati, analizzarli e presentarli come informazioni utilizzabili a fini di sicurezza. Tuttavia, poiché la loro funzionalità principale non è quella di un SIEM, i software SOAR non sono generalmente da considerarsi conformi alla descrizione tecnica «sistemi di gestione delle informazioni e degli eventi di sicurezza (sistemi SIEM)». Analogamente, uno smartphone solitamente integra componenti che svolgono le funzioni di diverse categorie di prodotti di cui agli allegati III e IV del regolamento (UE) 2024/2847, come un sistema operativo o un sistema integrato di gestione delle password. Ciononostante, dato che la sua funzionalità principale non è quella di sistema operativo o di sistema di gestione delle password, uno smartphone non è generalmente da considerarsi conforme alla descrizione tecnica di tali categorie di prodotti.

(6) A norma dell'articolo 13, paragrafi 2 e 3, del regolamento (UE) 2024/2847, i fabbricanti di prodotti con elementi digitali sono tenuti ad attuare i requisiti essenziali di cibersicurezza di cui all'allegato I, parte I, del regolamento (UE) 2024/2847 in modo proporzionato ai rischi del prodotto con elementi digitali, in base alla finalità prevista e all'uso ragionevolmente prevedibile, nonché alle condizioni d'uso del prodotto con elementi digitali, tenendo conto della durata di utilizzo del prodotto prevista. Conformemente all'articolo 13, paragrafi 2 e 3, di tale regolamento, e indipendentemente dal fatto che il prodotto con elementi digitali sia considerato un prodotto con elementi digitali importante o critico, i fabbricanti devono effettuare una valutazione completa dei rischi di cibersicurezza e indicare le modalità di attuazione dei requisiti essenziali di cibersicurezza sulla base della valutazione dei rischi, comprese le relative prove e garanzie. Se la funzionalità principale del loro prodotto con elementi digitali è conforme alla descrizione tecnica di un prodotto con elementi digitali importante o critico, i fabbricanti sono tenuti a dimostrare la conformità secondo le specifiche procedure di valutazione della conformità di cui all'articolo 32, paragrafi 2, 3, 4 e 5, del regolamento (UE) 2024/2847.

(7) Il presente regolamento comprende esempi di prodotti con elementi digitali la cui funzionalità principale è conforme alla descrizione tecnica di determinati prodotti con elementi digitali importanti o critici. Tali esempi sono forniti solo a scopo illustrativo e non costituiscono un elenco esaustivo.

(8) Al fine di garantire la certezza del diritto per i fabbricanti, le categorie di prodotti con elementi digitali corrispondenti a microprocessori a prova di manomissione, microcontrollori a prova di manomissione e carte intelligenti e dispositivi analoghi, compresi gli elementi sicuri, dovrebbero essere distinte in base al livello di resistenza rispetto alla potenziale possibilità di sfruttare i difetti o i punti deboli per il quale sono state progettate. Il livello AVA_VAN è un modo ampiamente utilizzato e standardizzato per esprimere tale livello di resistenza. I livelli AVA_VAN sono stabiliti nelle norme dei criteri comuni e della metodologia comune di valutazione, pubblicamente disponibili, che sono alla base di quadri di certificazione esistenti ampiamente adottati sul mercato, ad esempio il regolamento di esecuzione (UE) 2024/482 della Commissione ([3]). Il regolamento di esecuzione (UE) 2024/482 istituisce un sistema

([3]) Regolamento di esecuzione (UE) 2024/482 della Commissione, del 31 gennaio 2024, recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC) (GU L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

europeo di certificazione della cibersicurezza che può essere utilizzato per certificare un prodotto per uno specifico livello di affidabilità. Ispirandosi a pratiche globali, il regolamento di esecuzione (UE) 2024/482 prevede la possibilità di rilasciare certificati basati su versioni precedenti delle norme fino alla fine del 2027. Nel contesto del regolamento (UE) 2024/2847 è pertanto opportuno consentire che i livelli AVA_VAN siano espressi facendo riferimento all'ultima versione di tali norme o, in alternativa, a loro versioni precedenti.

(9) Le misure di cui al presente regolamento sono conformi al parere del comitato istituito dall'articolo 62, paragrafo 1, del regolamento (UE) 2024/2847,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

1) «criteri comuni»: i criteri comuni per la valutazione della sicurezza delle tecnologie dell'informazione quali definiti all'articolo 2, punto 1), del regolamento di esecuzione (UE) 2024/482 o quali definiti nelle norme di cui all'articolo 3, paragrafo 2, lettere a) e b), del medesimo regolamento di esecuzione;

2) «metodologia comune di valutazione»: la metodologia comune per la valutazione della sicurezza delle tecnologie dell'informazione quale definita all'articolo 2, punto 2), del regolamento di esecuzione (UE) 2024/482 o quale definita nelle norme di cui all'articolo 3, paragrafo 2, lettere c) e d), del medesimo regolamento di esecuzione.

Articolo 2

1. La descrizione tecnica delle categorie di prodotti con elementi digitali delle classi I e II di cui all'allegato III del regolamento (UE) 2024/2847 figura nell'allegato I del presente regolamento.

2. La descrizione tecnica delle categorie di prodotti con elementi digitali di cui all'allegato IV del regolamento (UE) 2024/2847 figura nell'allegato II del presente regolamento.

Articolo 3

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 28 novembre 2025

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO I

PRODOTTI CON ELEMENTI DIGITALI IMPORTANTI

Classe I

Categoria di prodotti	Descrizione tecnica
1. Sistemi di gestione dell'identità e software e hardware per la gestione degli accessi privilegiati, compresi i lettori di autenticazione e controllo degli accessi, tra cui i lettori biometrici	I sistemi di gestione dell'identità sono prodotti con elementi digitali che forniscono meccanismi di autenticazione o autorizzazione e che possono anche fornire meccanismi per la gestione del ciclo di vita delle credenziali di identità di persone fisiche, persone giuridiche, dispositivi o sistemi, ad esempio per registrazione, fornitura, manutenzione e cancellazione dalla registrazione dell'identità. Tali sistemi comprendono sistemi di gestione degli accessi che controllano l'accesso di persone fisiche, persone giuridiche, dispositivi o sistemi a risorse digitali o a luoghi fisici. Il software per la gestione degli accessi privilegiati è un sistema di gestione degli accessi che controlla e monitora i diritti di accesso ai sistemi IT o OT e alle informazioni sensibili all'interno di un'organizzazione, compresi i sistemi che applicano politiche differenziate di controllo degli accessi per gli utenti privilegiati. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i lettori di autenticazione e controllo degli accessi, i lettori biometrici, i software SSO (*Single Sign-On*), i software di gestione dell'identità federata, i software per le password monouso (*One-Time Password*, OTP), i dispositivi di autenticazione hardware quali i generatori di numeri di autenticazione delle transazioni (*Transaction Authentication Number*, TAN), i software di autenticazione e i software di autenticazione a più fattori.
2. Browser autonomi e incorporati	Prodotti software con elementi digitali che consentono agli utenti finali di accedere a contenuti e servizi web ospitati su server collegati a reti quali Internet, interpretarli e visualizzarli e interagire con essi. Essi comprendono generalmente un motore di rendering del browser per l'interpretazione e la visualizzazione di contenuti scritti in linguaggio di markup (ad esempio HTML), il supporto per i protocolli web (ad esempio HTTP, HTTPS), la capacità di eseguire script e gestire gli input degli utenti, nonché di conservare dati temporanei o persistenti provenienti da siti web (cookie). Questa categoria comprende, a titolo esemplificativo ma non esaustivo, le applicazioni autonome (*standalone*) che svolgono le funzioni di browser, i browser destinati all'integrazione in un altro sistema o in un'altra applicazione, nonché i browser che integrano un agente di IA.
3. Sistemi di gestione delle password	Prodotti con elementi digitali che memorizzano password localmente su un dispositivo o su un server remoto e comprendono attività quali la generazione di password, la condivisione delle password e l'integrazione con applicazioni locali o di terzi per l'uso di password. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i sistemi locali di gestione delle password, i sistemi di gestione delle password forniti come estensioni del browser, i sistemi aziendali di gestione delle password e i sistemi di gestione delle password basati su hardware.

Categoria di prodotti	Descrizione tecnica
4. Software che cercano, rimuovono o mettono in quarantena i software maligni	Prodotti software con elementi digitali, generalmente denominati antivirus o antimalware, che rilevano o cercano software o codice maligno sui dispositivi, o rimuovono o mettono in quarantena tale software o codice, al fine di mantenere l'integrità, la riservatezza o la disponibilità di tali dispositivi. Nel contesto di questa categoria di prodotti, per software maligno si intende un software contenente caratteristiche o capacità dolose che possono causare danni diretti o indiretti all'utente e/o al sistema informatico, quali virus, worm, ransomware, spyware e trojan. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i software che rilevano o cercano software maligni in tempo reale o con avvio manuale della ricerca, il rilevamento di rootkit e i dischi di soccorso con la funzione principale di cercare, rimuovere o mettere in quarantena i software maligni.
5. Prodotti con elementi digitali con funzione di rete privata virtuale (VPN)	Prodotti con elementi digitali che creano un tunnel logico criptato costruito a partire dalle risorse di sistema di una rete fisica o virtuale. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i client di reti private virtuali, i server di reti private virtuali e i gateway di reti private virtuali.
6. Sistemi di gestione della rete	Prodotti con elementi digitali che gestiscono elementi di rete connessi, quali server, router, switch, workstation, stampanti o dispositivi mobili, monitorandoli e controllandone le operazioni in rete e la configurazione. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i sistemi di gestione end-to-end e i sistemi dedicati di gestione della configurazione, come i controllori (*controller*) per la creazione di reti definite da software.
7. Sistemi di gestione delle informazioni e degli eventi di sicurezza (sistemi SIEM)	Prodotti con elementi digitali che raccolgono dati da più fonti, analizzano e correlano tali dati e li presentano come informazioni utilizzabili a fini di sicurezza, ad esempio per il rilevamento di minacce e incidenti, l'analisi forense o la verifica della conformità.
8. Boot manager	Prodotti software con elementi digitali che gestiscono il processo di avviamento iniziale del sistema dopo l'accensione/il riavvio inizializzando l'hardware, caricando o trasferendo il controllo all'ambiente del sistema operativo o alle risorse di sistema e selezionando le opzioni di boot. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, il firmware UEFI, i boot loader monostadio e multistadio.
9. Infrastrutture a chiave pubblica e software per il rilascio di certificati digitali	Prodotti con elementi digitali utilizzati come parte di un'infrastruttura a chiave pubblica (*Public Key Infrastructure*, PKI) che gestisce la convalida, la creazione, il rilascio, la distribuzione, la pubblicazione dello stato, il rinnovo o la revoca di certificati digitali o la generazione, la conservazione, la garanzia, lo scambio, la distruzione o la rotazione di chiavi crittografiche associate a tali certificati digitali. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i sistemi di gestione delle chiavi, i sistemi di gestione dei certificati digitali, i responder del protocollo OCSP (*Online Certificate Status Protocol*) e le soluzioni PKI "all-in-one".

Categoria di prodotti	Descrizione tecnica
10. Interfacce di rete fisiche e virtuali	Le interfacce di rete fisiche sono prodotti con elementi digitali che collegano direttamente un dispositivo a una rete attraverso un'interfaccia per programmi applicativi (*Application Programming Interface*, API) fornita dai driver dell'interfaccia, i quali operano generalmente a livello di collegamento dati, e che comprendono adattatori hardware ai mezzi di trasmissione con i corrispondenti firmware, i quali operano generalmente a livello fisico e di collegamento dati. Le interfacce di rete virtuali sono prodotti con elementi digitali che collegano direttamente o indirettamente un dispositivo a una rete attraverso un'API che emula quella dei driver di interfacce di rete fisiche, i quali operano generalmente a livello di collegamento dati. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, schede di interfaccia di rete, controllori e adattatori con e senza fili, ad esempio per Wi-Fi, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee o Fieldbus, nonché prodotti autonomi (*standalone*) puramente virtuali, quali schede di interfaccia di rete virtuali, CNI (*Container Network Interface*) e interfacce VPN.
11. Sistemi operativi	Prodotti software con elementi digitali che forniscono un'interfaccia astratta dell'hardware sottostante, controllano l'esecuzione del software e possono fornire servizi quali la gestione e la configurazione delle risorse di calcolo, lo scheduling, il controllo input-output, la gestione dei dati e la fornitura di un'interfaccia che consente alle applicazioni di interagire con le risorse di sistema e le periferiche. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i sistemi operativi in tempo reale e i sistemi operativi generali o particolari.
12. Router, modem per la connessione a Internet e switch	I router sono prodotti con elementi digitali che stabiliscono e controllano il flusso di dati tra reti diverse selezionando percorsi (*path* o *route*) mediante l'uso di meccanismi e algoritmi di protocollo di instradamento (*routing protocol*), i quali operano generalmente a livello di rete. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i router con e senza fili, i router virtuali e i router con o senza modem.
	I modem per la connessione a Internet sono prodotti hardware con elementi digitali che utilizzano tecniche di modulazione e demodulazione digitali per convertire segnali analogici da e verso segnali digitali per la comunicazione basata su IP. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i modem in fibra ottica, i modem DSL (*Digital Subscriber Line*), i modem via cavo (DOCSIS), i modem satellitari e i modem cellulari.
	Gli switch sono prodotti con elementi digitali che forniscono connettività tra dispositivi collegati in rete attraverso meccanismi di inoltro di pacchetti e che hanno un piano di gestione, generalmente implementato a livello di collegamento dati o di rete. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, gli switch gestiti, gli switch intelligenti, gli switch multilivello, gli switch di sicurezza virtuali (*virtual security switch*), gli switch programmabili per le reti definite da software e i bridge quali gli access point senza fili.

Categoria di prodotti	Descrizione tecnica
13. Microprocessori con funzionalità legate alla sicurezza	Prodotti con elementi digitali costituiti da circuiti integrati che svolgono funzioni di elaborazione centrale basate su memoria esterna e periferiche, comprendenti microcodice e altri firmware di basso livello. Essi forniscono inoltre funzionalità legate alla sicurezza, quali cifratura, autenticazione, conservazione sicura delle chiavi, generazione casuale di numeri, ambiente di esecuzione affidabile o altri meccanismi di protezione basati su hardware, che mirano a proteggere altri prodotti, reti o servizi al di là del microprocessore stesso, come la catena di avvio protetto (*secure boot chain*), la virtualizzazione o le interfacce di comunicazione sicure.
14. Microcontrollori con funzionalità legate alla sicurezza	Prodotti con elementi digitali costituiti da circuiti integrati che svolgono funzioni di elaborazione centrale e integrano una memoria, che consente al microcontrollore di essere programmabile, e generalmente anche altre periferiche, comprendenti microcodice e altri firmware di basso livello. Essi forniscono inoltre funzionalità legate alla sicurezza, quali cifratura, autenticazione, conservazione sicura delle chiavi, generazione casuale di numeri, ambiente di esecuzione affidabile o altri meccanismi di protezione basati su hardware, che mirano a proteggere altri prodotti, reti o servizi al di là del microcontrollore stesso, come la catena di avvio protetto (*secure boot chain*), la virtualizzazione o le interfacce di comunicazione sicure.
15. Circuiti integrati per applicazioni specifiche (ASIC) e reti di porte programmabili dall'utilizzatore (FPGA) con funzionalità legate alla sicurezza	I circuiti integrati per applicazioni specifiche (*Application Specific Integrated Circuit*, ASIC) con funzionalità legate alla sicurezza sono prodotti con elementi digitali costituiti da circuiti integrati, progettati totalmente o parzialmente su misura per svolgere una funzione specifica o per implementare un'applicazione specifica, comprendenti microcodice e altro firmware di basso livello. Essi forniscono inoltre funzionalità legate alla sicurezza, quali cifratura, autenticazione, conservazione sicura delle chiavi, generazione casuale di numeri, ambiente di esecuzione affidabile o altri meccanismi di protezione basati su hardware, che mirano a proteggere altri prodotti, reti o servizi al di là degli ASIC stessi, come la catena di avvio protetto (*secure boot chain*), la virtualizzazione o le interfacce di comunicazione sicure.
	Le reti di porte programmabili dall'utilizzatore (*Field-Programmable Gate Array*, FPGA) con funzionalità legate alla sicurezza sono prodotti con elementi digitali costituiti da circuiti integrati caratterizzati da una matrice di blocchi logici configurabili progettati per poter essere riprogrammati dopo la fabbricazione al fine di svolgere una funzione specifica o implementare un'applicazione specifica, comprendenti microcodice e altro firmware di basso livello. Esse forniscono inoltre funzionalità legate alla sicurezza, quali cifratura, autenticazione, conservazione sicura delle chiavi, generazione casuale di numeri, ambiente di esecuzione affidabile o altri meccanismi di protezione basati su hardware, che mirano a proteggere altri prodotti, reti o servizi al di là delle FPGA stesse, come la catena di avvio protetto (*secure boot chain*), la virtualizzazione o le interfacce di comunicazione sicure.
16. Assistenti virtuali di uso generale per case intelligenti	Prodotti con elementi digitali che comunicano sulla rete Internet pubblica, direttamente o tramite altre apparecchiature, che elaborano richieste, compiti o domande basati su prompt in linguaggio naturale, ad esempio input scritti o audio, e che, sulla base di tali richieste, compiti o domande, forniscono accesso ad altri servizi o controllano le funzioni dei dispositivi connessi in contesti residenziali. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, gli altoparlanti intelligenti con un assistente virtuale integrato e gli assistenti virtuali *standalone* conformi a questa descrizione.

Categoria di prodotti	Descrizione tecnica
17. Prodotti per case intelligenti con funzionalità di sicurezza, tra cui serrature intelligenti, telecamere di sicurezza, sistemi di monitoraggio dei neonati e sistemi di allarme	Prodotti con elementi digitali che proteggono la sicurezza fisica dei consumatori in un contesto residenziale e che possono essere controllati o gestiti a distanza da altri sistemi, nonché l'hardware e il software che controllano a livello centrale tali prodotti. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, le serrature intelligenti, i sistemi di monitoraggio dei neonati, i sistemi di allarme e le telecamere di sicurezza domestica.
18. Giocattoli connessi a Internet disciplinati dalla direttiva 2009/48/CE del Parlamento europeo e del Consiglio ([1]) che presentano funzionalità sociali interattive (in grado ad esempio di parlare o filmare) o di geolocalizzazione	I giocattoli connessi a Internet che presentano funzionalità sociali interattive sono prodotti con elementi digitali disciplinati dalla direttiva 2009/48/CE, che comunicano sulla rete Internet pubblica, direttamente o tramite altre apparecchiature, e integrano tecnologie che consentono la comunicazione in entrata e in uscita, quali tastiera, microfono, altoparlante o telecamera.
	I giocattoli connessi a Internet che presentano funzionalità di geolocalizzazione sono prodotti con elementi digitali disciplinati dalla direttiva 2009/48/CE che comunicano sulla rete Internet pubblica, direttamente o tramite altre apparecchiature, e dispongono di tecnologie che consentono di tracciare o desumere la localizzazione geografica del giocattolo o del suo utilizzatore. Se rileva semplicemente la prossimità dell'utilizzatore o di altri giocattoli utilizzando tecnologie di rilevamento, il giocattolo non deve essere considerato dotato di funzionalità di geolocalizzazione.
19. Prodotti indossabili personali da indossare o collocare sul corpo umano a fini di monitoraggio della salute (come il tracciamento) e ai quali non si applica il regolamento (UE) 2017/745 ([2]) o il regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio ([3]), o prodotti indossabili personali destinati all'uso da parte dei bambini e per questi ultimi	I prodotti indossabili personali da indossare o collocare sul corpo umano a fini di monitoraggio della salute sono prodotti con elementi digitali che sono indossati sul corpo direttamente o tramite indumenti o accessori e che possono, periodicamente o continuativamente, rilevare e elaborare ulteriormente informazioni, comprese le metriche del corpo pertinenti per la salute dell'utente, esclusi i prodotti che rientrano nell'ambito di applicazione del regolamento (UE) 2017/745 o del regolamento (UE) 2017/746. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i tracciatori di attività (*fitness tracker*), gli smartwatch, i gioielli intelligenti, gli indumenti intelligenti e gli indumenti sportivi conformi a questa descrizione.
	I prodotti indossabili personali destinati all'uso da parte dei bambini e per questi ultimi sono prodotti con elementi digitali che possono essere indossati o collocati sul corpo, direttamente o tramite indumenti o accessori, di persone di età inferiore a 14 anni. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i dispositivi indossabili per la sicurezza dei bambini.

([1]) Direttiva 2009/48/CE del Parlamento europeo e del Consiglio, del 18 giugno 2009, sulla sicurezza dei giocattoli (GU L 170 del 30.6.2009, pag. 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio (GU L 117 del 5.5.2017, pag. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici *in vitro* e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione (GU L 117 del 5.5.2017, pag. 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj).

Classe II

Categoria di prodotti	Descrizione tecnica
1. Ipervisori e sistemi di runtime container che supportano l'esecuzione virtualizzata di sistemi operativi e ambienti simili	Gli ipervisori (*hypervisor*) sono prodotti software con elementi digitali che astraggono e/o assegnano risorse di calcolo e consentono l'esecuzione, la gestione e l'orchestrazione di macchine virtuali che sono separate logicamente l'una dall'altra e/o dall'hardware fisico. Gli ipervisori possono essere eseguiti direttamente sull'hardware (*bare metal*), su un sistema operativo o all'interno di un'altra macchina virtuale (*nested virtualisation*). Nel contesto di questa categoria di prodotti, una macchina virtuale è una separazione logica e definita da software di un ambiente informatico che comprende un insieme virtualizzato di risorse hardware (ad esempio CPU, memoria, archiviazione, interfacce di rete) e generalmente ospita il proprio sistema operativo. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, gli ipervisori di tipo 1 (*bare metal*), gli ipervisori di tipo 2 ospitati su un sistema operativo (*hosted*) e gli ipervisori ibridi.
	I sistemi di runtime container sono prodotti software con elementi digitali che gestiscono l'esecuzione e il ciclo di vita di container, i quali funzionano su un unico sistema operativo host come processi isolati, assegnando risorse e consentendo la gestione e l'orchestrazione dei singoli container. Nel contesto di questa categoria di prodotti, un container è un ambiente di esecuzione basato su software che racchiude in un unico pacchetto uno o più componenti software e le loro dipendenze, consentendogli di funzionare in modo indipendente e coerente.
2. Firewall, sistemi di rilevamento e prevenzione delle intrusioni	I firewall sono prodotti con elementi digitali che proteggono una rete o un sistema connessi dall'accesso non autorizzato, monitorando e limitando il traffico di comunicazione dei dati da e verso tale rete. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i firewall di rete e i firewall delle applicazioni, come i firewall o i filtri delle applicazioni web e i gateway antispam.
	I sistemi di rilevamento delle intrusioni sono prodotti con elementi digitali che monitorano il traffico in entrata nell'ambiente di rete alla ricerca di attività sospette e rilevano o individuano i tentativi di intrusione su una rete o un sistema connessi, le intrusioni in corso o quelle passate. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i sistemi di rilevamento delle intrusioni basati sulla rete e i sistemi di rilevamento delle intrusioni basati sull'host.
	I sistemi di prevenzione delle intrusioni sono prodotti con elementi digitali composti da un sistema di rilevamento delle intrusioni che risponde attivamente a un'intrusione in una rete o un sistema connessi. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i sistemi di prevenzione delle intrusioni basati sulla rete e i sistemi di prevenzione delle intrusioni basati sull'host.

Categoria di prodotti	Descrizione tecnica
3. Microprocessori a prova di manomissione	Prodotti con elementi digitali costituiti da microprocessori con funzionalità legate alla sicurezza di cui alla tabella "Classe I", punto 13, del presente allegato, che comprendono prove di manomissione, resistenza o risposta, e che sono inoltre progettati per fornire protezione di livello AVA_VAN 2 o 3, come stabilito nei criteri comuni e nella metodologia comune di valutazione.
4. Microcontrollori a prova di manomissione	Prodotti con elementi digitali costituiti da microcontrollori con funzionalità legate alla sicurezza di cui alla tabella "Classe I", punto 14, del presente allegato, che comprendono prove di manomissione, resistenza o risposta, e che sono inoltre progettati per fornire protezione di livello AVA_VAN 2 o 3, come stabilito nei criteri comuni e nella metodologia comune di valutazione.

ALLEGATO II

PRODOTTI CON ELEMENTI DIGITALI CRITICI

Categoria di prodotti	Descrizione tecnica
1. Dispositivi hardware con cassette di sicurezza	Prodotti hardware con elementi digitali che memorizzano, elaborano o gestiscono in modo sicuro dati sensibili o eseguono operazioni crittografiche e che sono costituiti da molteplici componenti discreti e comprendono un involucro fisico hardware che fornisce prove di manomissione, resistenza o risposta come contromisure contro gli attacchi fisici. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i terminali di pagamento fisici, i moduli di sicurezza hardware che generano e gestiscono elementi crittografici e i tachigrafi conformi alla descrizione di cui sopra.
2. Gateway per contatori intelligenti nell'ambito di sistemi di misurazione intelligenti quali definiti all'articolo 2, punto 23), della direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio ([1]), e altri dispositivi a fini di sicurezza avanzati, compreso il trattamento crittografico sicuro	I gateway per contatori intelligenti sono prodotti con elementi digitali che controllano la comunicazione tra componenti all'interno di sistemi di misurazione intelligenti o collegati ad essi, quali definiti all'articolo 2, punto 23), della direttiva (UE) 2019/944, e terzi autorizzati, quali i fornitori di servizi di pubblica utilità. I gateway per contatori intelligenti raccolgono, elaborano e conservano i dati personali o del contatore, proteggono i flussi di dati e informazioni supportando specifiche necessità crittografiche, ad esempio la crittazione e decrittazione dei dati, integrano funzionalità di firewall e forniscono i mezzi per controllare altri dispositivi. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i gateway per contatori intelligenti relativi ai sistemi di misurazione intelligenti che misurano l'energia elettrica quali definiti all'articolo 2, punto 23), della direttiva (UE) 2019/944. Essa può includere inoltre i gateway per contatori intelligenti utilizzati in altri sistemi di misurazione intelligenti che misurano il consumo di altre fonti di energia, come il gas o il calore, a condizione che il gateway sia conforme a questa descrizione.
3. Carte intelligenti o dispositivi analoghi, compresi gli elementi sicuri	Gli elementi sicuri sono microcontrollori o microprocessori con funzionalità legate alla sicurezza, che comprendono prove di manomissione, resistenza o risposta. Essi generalmente conservano, elaborano o gestiscono operazioni crittografiche o dati sensibili, quali credenziali di identità o credenziali di pagamento. Gli elementi sicuri sono progettati per fornire protezione almeno di livello AVA_VAN 4, come stabilito nei criteri comuni o nella metodologia comune di valutazione. Essi possono essere costituiti da componenti discreti di silicio o essere integrati in sistemi su chip (*Systems on Chip*, SoC). Gli elementi sicuri possono integrare un ambiente di applicazione o un sistema operativo e possono includere una o più applicazioni. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i *Trusted Platform Module* (TPM) e le schede a circuito integrato universale (*Universal Integrated Circuit Card*, UICC) incorporate.
	Le carte intelligenti o dispositivi analoghi sono elementi sicuri integrati in un materiale portante, come la plastica o il legno, in forma di carta, o elementi sicuri integrati in materiali portanti che assumono altre forme. Questa categoria comprende, a titolo esemplificativo ma non esaustivo, i documenti di identità e di viaggio, le carte per la firma elettronica qualificata, le UICC sostituibili, le carte di pagamento fisiche, le carte di accesso fisiche, le carte tachigrafiche digitali o i bracciali o gli orologi con elementi sicuri per il pagamento integrati.

([1]) Direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio, del 5 giugno 2019, relativa a norme comuni per il mercato interno dell'energia elettrica e che modifica la direttiva 2012/27/UE (GU L 158 del 14.6.2019, pag. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).