Uradni list
Evropske unije

SL
Serija L

2024/2981

4.12.2024

IZVEDBENA UREDBA KOMISIJE (EU) 2024/2981

z dne 28. novembra 2024

o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede certificiranja evropskih denarnic za digitalno identiteto

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES ([1]) ter zlasti člena 5c(6) Uredbe,

ob upoštevanju naslednjega:

(1) V skladu s členom 5c Uredbe (EU) št. 910/2014 se certificiranje evropskih denarnic za digitalno identiteto (v nadaljnjem besedilu: denarnice) izvaja v skladu z zahtevami glede funkcionalnosti, kibernetske varnosti in varstva podatkov, da se zagotovi visoka raven varnosti in zaupanja v denarnice. Te zahteve za certificiranje je treba uskladiti med državami članicami, da se prepreči razdrobljenost trga in vzpostavi trden okvir.

(2) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta ([2]) in, kadar je ustrezno, Direktiva 2002/58/ES Evropskega parlamenta in Sveta ([3]) se uporabljata za dejavnosti obdelave osebnih podatkov na podlagi te uredbe.

(3) Komisija redno ocenjuje nove tehnologije, prakse, standarde ali tehnične specifikacije. Za zagotovitev najvišje ravni harmonizacije med državami članicami za razvoj in certificiranje denarnic se tehnične specifikacije iz te uredbe opirajo na delo, opravljeno na podlagi Priporočila Komisije (EU) 2021/946 z dne 3. junija 2021 o skupnem unijskem naboru orodij za usklajen pristop k okviru za evropsko digitalno identiteto ([4]) ter zlasti arhitekturnega in referenčnega okvira, ki je del navedenega priporočila. V skladu z uvodno izjavo 75 Uredbe (EU) 2024/1183 Evropskega parlamenta in Sveta ([5]) bi morala Komisija pregledovati in po potrebi posodabljati to izvedbeno uredbo, da bi bila usklajena s svetovnim razvojem ter arhitekturnim in referenčnim okvirom ter sledila najboljšim praksam na notranjem trgu.

(4) Za potrditev skladnosti z zahtevami glede kibernetske varnosti, vključenimi v certifikacijski okvir, bi se moralo certificiranje rešitev denarnic nanašati na evropske certifikacijske sheme za kibernetsko varnost, vzpostavljene v skladu z Uredbo (EU) 2019/881 Evropskega parlamenta in Sveta ([6]), kadar so na voljo in kadar je to ustrezno. Če takih shem ni ali če delno zajemajo zahteve glede kibernetske varnosti, ta uredba določa splošne zahteve, ki se uporabljajo za nacionalne certifikacijske sheme ter zajemajo zahteve glede funkcionalnosti, kibernetske varnosti in varstva podatkov.

([1]) UL L 257, 28.8.2014, str. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).
([3]) Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).
([4]) UL L 210, 14.6.2021, str. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.
([5]) Uredba (EU) 2024/1183 Evropskega parlamenta in Sveta z dne 11. aprila 2024 o spremembi Uredbe (EU) št. 910/2014 v zvezi z vzpostavitvijo evropskega okvira za digitalno identiteto (UL L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).
([6]) Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(5) V skladu s členom 5a(11) Uredbe (EU) št. 910/2014 se denarnice certificirajo na visoki ravni zanesljivosti, kot je določeno v Uredbi (EU) št. 910/2014 in Izvedbeni uredbi Komisije (EU) 2015/1502 ([7]). Rešitev denarnice mora to raven zanesljivosti dosegati kot celota. V skladu s to uredbo se lahko nekatere komponente rešitve denarnice certificirajo na nižji ravni zanesljivosti, če je to ustrezno utemeljeno in ne vpliva na visoko raven zanesljivosti rešitve kot celote.

(6) Vse nacionalne certifikacijske sheme bi morale določiti lastnika sheme, ki bo odgovoren za razvoj in vzdrževanje certifikacijske sheme. Lastnik sheme je lahko organ za ugotavljanje skladnosti, vladni organ, panožno združenje, skupina organov za ugotavljanje skladnosti ali kateri koli ustrezen organ in se lahko razlikuje od organa, ki upravlja nacionalno certifikacijsko shemo.

(7) Predmet certificiranja bi moral vključevati komponente programske opreme rešitve denarnice, kot je instanca denarnice. Čeprav so varna kriptografska aplikacija denarnice, varna kriptografska naprava denarnice in platforme, na katerih se ti komponenti programske opreme izvajata, del operativnega okolja, bi morale biti vključene v predmet certificiranja le, če jih zagotavlja rešitev denarnice. V drugih primerih, zlasti kadar te naprave in platforme zagotavljajo končni uporabniki, bi morali ponudniki določiti predpostavke o operativnem okolju rešitve denarnice, vključno s temi napravami in platformami, ter izvesti ukrepe za potrditev, da se te predpostavke preverjajo v praksi. Da bi zagotovili zaščito kritičnih sredstev s strojno in sistemsko programsko opremo za upravljanje in zaščito kriptografskih ključev, ki jih ustvari, shrani ali obdela varna kriptografska naprava denarnice, mora ta naprava izpolnjevati visoke standarde certificiranja, kot se odražajo v mednarodnih standardih, kot so skupna merila (v nadaljnjem besedilu: EUCC), vzpostavljena z Izvedbeno uredbo Komisije (EU) 2024/482 ([8]), v oceni EAL4 in napredni metodološki analizi ranljivosti, npr. primerljivi z AVA_VAN.5. Te certifikacijske standarde bi bilo treba uporabiti najpozneje pri certificiranju skladnosti denarnic na podlagi evropske certifikacijske sheme za kibernetsko varnost, sprejete v skladu z Uredbo (EU) 2019/881.

(8) Popolnoma mobilne, varne in uporabniku prijazne denarnice podpira razpoložljivost standardiziranih in certificiranih rešitev, ki so zaščitene pred nedovoljenimi posegi, kot so vgrajeni varni elementi, zunanje naprave, kot so pametne kartice, ali vgrajene platforme SIM v mobilnih napravah. Pomembno je zagotoviti pravočasen dostop do vgrajenih varnostnih elementov za nacionalna sredstva elektronske identifikacije in denarnice ter usklajevati prizadevanja držav članic na tem področju. Skupina za sodelovanje na področju evropske digitalne identitete, ustanovljena v skladu s členom 46e(1) Uredbe (EU) št. 910/2014 (v nadaljnjem besedilu: skupina za sodelovanje), bi zato morala v ta namen ustanoviti namensko podskupino. Ta podskupina bi se morala po posvetovanju z zadevnimi deležniki dogovoriti o skupnem načrtu za dostop do vgrajenih varnostnih elementov, ki ga bo Komisija upoštevala pri poročilu o pregledu Uredbe (EU) št. 910/2014. Da bi olajšala uporabo denarnice na nacionalni ravni, bi morala Komisija v sodelovanju z državami članicami poleg tega pripraviti in stalno posodabljati priročnik za primere uporabe kot del arhitekturnega in referenčnega okvira.

(9) Predmet certificiranja nacionalnih certifikacijskih shem bi moral vključevati tudi postopke, ki se uporabljajo za zagotavljanje in upravljanje rešitve denarnice, tudi če se opredelitev ali izvedba teh postopkov odda v podizvajanje tretjim osebam. Informacije o zanesljivosti se lahko uporabijo kot dokaz, da postopki izpolnjujejo zahteve shem, če se za ugotavljanje zadostnosti informacij o zanesljivosti uporabi analiza odvisnosti. Informacije o zanesljivosti se pojavljajo v različnih oblikah, vključno s poročili in certifikati o skladnosti, ki so lahko zasebni, nacionalni, evropski ali mednarodni ter temeljijo na standardih ali tehničnih specifikacijah. Cilj analize odvisnosti je oceniti kakovost razpoložljivih informacij o zanesljivosti komponent denarnice.

([7]) Izvedbena uredba Komisije (EU) 2015/1502 z dne 8. septembra 2015 o določitvi minimalnih tehničnih specifikacij in postopkov za ravni zanesljivosti za sredstva elektronske identifikacije v skladu s členom 8(3) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu (UL L 235, 9.9.2015, str. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([8]) Izvedbena uredba Komisije (EU) 2024/482 z dne 31. januarja 2024 o določitvi pravil za uporabo Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta v zvezi s sprejetjem evropske certifikacijske sheme za kibernetsko varnost, ki temelji na skupnih merilih (UL L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg/2024/482/oj).

(10) Skupina za sodelovanje bi morala imeti možnost, da v skladu s postopki, vzpostavljenimi v ta namen, pripravi mnenja in priporočila o osnutkih nacionalnih shem certificiranja, ki so ji bili predloženi. Te nacionalne certifikacijske sheme bi morale biti specifične za arhitekturo denarnice, za vsako posamezno podprto arhitekturo pa bi morali obstajati posebni profili.

(11) Za zagotovitev skupnega razumevanja in usklajenega pristopa k oceni najbolj kritičnih tveganj, ki bi lahko vplivala na zagotavljanje in delovanje denarnic, bi bilo treba pripraviti register tveganj in groženj, ki bi jih bilo treba upoštevati pri oblikovanju rešitev denarnic neodvisno od njihove posebne arhitekture. Pri ugotavljanju, katera tveganja bi bilo treba vključiti v register, bi bilo treba upoštevati cilje kibernetske varnosti, opisane v Uredbi (EU) št. 910/2014, kot so zaupnost, celovitost in razpoložljivost rešitve denarnice ter zasebnost uporabnikov in podatkov. Ustrezno upoštevanje tveganj in groženj, vključenih v ta register tveganj, bi moralo biti del zahtev nacionalnih certifikacijskih shem. Da bi ohranili skladnost z nenehno spreminjajočim se okoljem groženj, bi bilo treba register tveganj voditi in redno posodabljati v sodelovanju s skupino za sodelovanje.

(12) Lastniki shem bi morali pri vzpostavljanju svojih certifikacijskih shem izvesti oceno tveganja, da bi precizirali in dopolnili tveganja in grožnje, navedene v registru, s tveganji in grožnjami, specifičnimi za arhitekturo ali izvajanje rešitve denarnice. V oceni tveganja bi bilo treba preučiti, kako je mogoče ustrezno obravnavati zadevna tveganja in grožnje. Ponudniki denarnic bi morali oceno tveganja sheme dopolniti z vsemi tveganji in grožnjami, značilnimi za njihovo izvajanje, ter predlagati ustrezne ukrepe za njihovo obravnavo, ki jih oceni certifikacijski organ.

(13) Da bi se dokazalo, da arhitektura rešitev denarnice izpolnjuje veljavne varnostne zahteve, bi morala vsaka shema ali profil, specifična za arhitekturo, vsebovati vsaj opis arhitekture rešitve denarnice, seznam varnostnih zahtev, ki se uporabljajo za to arhitekturo, načrt ocenjevanja za potrditev, da rešitev denarnice, ki temelji na tej arhitekturi, izpolnjuje navedene zahteve, in oceno tveganja. Nacionalne certifikacijske sheme bi morale od ponudnikov denarnic zahtevati, da dokažejo, kako zasnova rešitve denarnice, ki jo zagotavljajo, ustreza referenčni arhitekturi ter podrobno opisuje varnostni nadzor in načrte potrjevanja za določeno rešitev denarnice. Nacionalne certifikacijske sheme bi morale opredeliti tudi dejavnost ugotavljanja skladnosti, da se preveri, ali zasnova denarnice ustrezno odraža referenčno arhitekturo izbranega profila. Nacionalne certifikacijske sheme bi morale izpolnjevati zahteve iz člena 51 Uredbe (EU) 2019/881, razen točk (e) in (f), povezanih z beleženjem.

(14) Kar zadeva certificiranje proizvodov, bi bilo treba dovoliti uporabo certifikatov o skladnosti, izdanih v okviru evropske certifikacijske sheme za kibernetsko varnost, ki temelji na EUCC, in certifikatov o skladnosti, izdanih v okviru nacionalnih certifikacijskih shem v okviru sporazuma o vzajemnem priznavanju SOG-IS. Poleg tega bi bilo treba dovoliti uporabo drugih nacionalnih certifikacijskih shem za manj občutljive komponente proizvodov, kot so tiste, vzpostavljene v skladu s standardom CEN EN 17640 za metodologijo ocenjevanja kibernetske varnosti za določeno obdobje.

(15) Znak zaupanja za evropsko denarnico za digitalno identiteto (v nadaljnjem besedilu: znak zaupanja) bi bilo treba uporabljati kot jasno, preprosto in prepoznavno navedbo, da je bila denarnica zagotovljena v skladu z Uredbo (EU) št. 910/2014. Zato bi ga bilo treba obravnavati kot znak skladnosti za rešitev denarnice, certificirano v okviru nacionalnih certifikacijskih shem. Nacionalne certifikacijske sheme ne bi smele opredeljevati nobenih drugih znakov skladnosti.

(16) Za odvračanje od goljufij bi morale nacionalne certifikacijske sheme opredeliti ukrepe, ki jih je treba sprejeti, kadar se certificiranje na podlagi sheme uveljavlja na goljufiv način.

(17) Za zagotovitev učinkovitega upravljanja priglasitev ranljivosti bi morali ponudniki rešitev denarnic in sheme elektronske identifikacije, v okviru katere se te rešitve zagotavljajo, opredeliti in izvajati postopke za oceno resnosti in morebitnega vpliva ranljivosti. Nacionalne certifikacijske sheme bi morale določiti prag, nad katerim je treba ranljivosti priglasiti certifikacijskemu organu. Taka obveznost priglasitev ne bi smela vplivati na merila, ki jih določajo zakonodaja o varstvu podatkov in organi držav članic za varstvo podatkov, za obvestila o kršitvah varstva osebnih podatkov. Lahko bi se vzpostavile morebitne sinergije med obveznimi priglasitvami kršitev v zvezi z rešitvami denarnic ali njihovega ogrožanja in obvestilih o kršitvah varstva osebnih podatkov v skladu z Uredbo (EU) 2016/679. Ocena poročila o analizi učinka ranljivosti, ki jo opravi certifikacijski organ, ne bi smela posegati v oceno učinka v zvezi z varstvom podatkov, ki jo opravi organ za varstvo podatkov v skladu s členoma 35 in 36 Uredbe (EU) 2016/679.

(18) Ponudniki rešitev denarnic in sheme elektronske identifikacije, v okviru katere se te rešitve zagotavljajo, bi morali lastnika sheme obvestiti o vseh utemeljitvah izjem od ocene ranljivosti, potrebne za oceno varnih kriptografskih naprav denarnice in varnih kriptografskih aplikacij denarnice, kot je določeno v Prilogi IV.

(19) Preklic certifikata o skladnosti bi lahko imel resne posledice, kot je preklic vseh uvedenih enot denarnic. Zato bi morali certifikacijski organi o preklicu razmisliti le, če je verjetno, da bo nerešena ranljivost znatno vplivala na zanesljivost rešitve zadevne ali druge rešitve denarnice.

(20) Vzpostaviti bi bilo treba poseben postopek za posodobitev nacionalnih certifikacijskih shem za upravljanje prehoda med zaporednimi izdajami shem, zlasti v zvezi z ukrepi, ki jih mora imetnik certifikata sprejeti v zvezi s prihodnjimi ocenjevanji, vzdrževanjem, ponovnim certificiranjem in posebnimi ocenjevanji.

(21) Za lažjo preglednost bi morali ponudniki denarnic javno izmenjevati varnostne informacije o svoji rešitvi denarnice.

(22) Kadar nacionalne certifikacijske sheme temeljijo na informacijah o zanesljivosti iz drugih certifikacijskih shem ali virov, bi bilo treba izvesti analizo odvisnosti, da se preveri, ali je dokumentacija o zanesljivosti, na primer poročila o zanesljivosti in certifikati o skladnosti, na voljo in ustrezna za rešitve denarnice in shemo elektronske identifikacije, v okviru katere se te rešitve zagotavljajo. Podlaga za to analizo odvisnosti bi morala biti ocena tveganja rešitev denarnice in sheme elektronske identifikacije, v okviru katere se te rešitve zagotavljajo. V oceni bi bilo treba ugotoviti, ali je dokumentacija o zanesljivosti, ki je na voljo za določeno rešitev denarnice in shemo elektronske identifikacije, v okviru katere se ta rešitev zagotavlja, ustrezna za zagotavljanje zanesljivosti, ki ustreza ciljni ravni ocenjevanja. V okviru ocenjevanja bi bilo treba tudi posodobiti ali po potrebi v celoti ponovno izvesti analizo odvisnosti.

(23) Certifikacijski organi bi morali izdajati certifikate o skladnosti v nacionalnih certifikacijskih shemah skupaj z javno dostopnim poročilom o certificiranju iz člena 5d(2), točka (a), Uredbe (EU) št. 910/2014. Povezano poročilo o oceni certificiranja bi moralo biti dostopno skupini za sodelovanje.

(24) Nacionalne certifikacijske sheme bi morale določati letno nadzorno ocenjevanje, da se zagotovi učinkovito delovanje postopkov v zvezi z upravljanjem in vzdrževanjem denarnic, tj. kot je opredeljeno v politikah, ki jih določajo. Uredba (EU) št. 910/2014 zahteva dvoletno oceno ranljivosti, da se zagotovi, da rešitev denarnice še naprej ustrezno obravnava tveganja in grožnje za kibernetsko varnost, opredeljene v registru tveganj, vključno z morebitnim razvojem okolja groženj. Pojmi nadzornih ocenjevanj, ocenjevanj za ponovno certifikacijo in posebnih ocenjevanj bi morali biti v skladu s standardom EN ISO/IEC 17021-1:2015.

(25) Cikel certificiranja se konča s prenehanjem veljavnosti certifikata o skladnosti ali z izdajo novega certifikata o skladnosti po uspešnem ocenjevanju za ponovno certifikacijo. Ocenjevanje za ponovno certifikacijo bi moralo vključevati oceno vseh komponent predmeta certificiranja, vključno z oceno učinkovitosti in po potrebi oceno ranljivosti. Med ponovnim certificiranjem bi moralo biti mogoče ponovno uporabiti rezultate prejšnjih ocen nespremenjenih komponent.

(26) Ob sprejetju evropske certifikacijske sheme za kibernetsko varnost bi morale nacionalne certifikacijske sheme z enakim področjem uporabe po opredeljenem prehodnem obdobju iz člena 57(1) Uredbe (EU) 2019/881 prenehati izdajati certifikate.

(27) Nacionalne certifikacijske sheme bi se morale opirati na obstoječe okvire in po potrebi ponovno uporabiti dokaze, da se zagotovita harmonizacija in interoperabilnost. Države članice lahko sklenejo sporazume za čezmejno ponovno uporabo certifikacijskih shem ali njihovih delov. Evropska komisija in Agencija Evropske unije za kibernetsko varnost bi morali v sodelovanju s skupino za sodelovanje podpirati države članice pri razvoju in vzdrževanju nacionalnih certifikacijskih shem, da bi zagotovili izmenjavo znanj in dobri praks.

(28) V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta ([9]) je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 30. septembra 2024.

(29) Ukrepi iz te uredbe so v skladu z mnenjem odbora iz člena 48(1) Uredbe (EU) št. 910/2014 –

SPREJELA NASLEDNJO UREDBO:

POGLAVJE I

SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja in področje uporabe

Ta uredba določa referenčne standarde ter specifikacije in postopke za vzpostavitev trdnega okvira za certificiranje denarnic, ki ga je treba redno posodabljati, da bi bil skladen z razvojem tehnologije in standardov ter delom, opravljenim na podlagi Priporočila (EU) 2021/946 o skupnem unijskem naboru orodij za usklajen pristop k okviru za evropsko digitalno identiteto ter zlasti arhitekturnega in referenčnega okvira.

Člen 2

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „rešitev denarnice“ pomeni kombinacijo programske opreme, strojne opreme, storitev, nastavitev in konfiguracij, vključno z instancami denarnic, eno ali več varnimi kriptografskimi aplikacijami denarnic in eno ali več varnimi kriptografskimi napravami denarnic;

(2) „lastnik sheme“ pomeni organizacijo, ki je odgovorna za razvoj in vzdrževanje certifikacijske sheme;

(3) „predmet certificiranja“ pomeni proizvode, postopke in storitve ali njihovo kombinacijo, za katere veljajo določene zahteve;

(4) „varna kriptografska aplikacija denarnice“ pomeni aplikacijo, ki upravlja kritična sredstva tako, da je povezana s kriptografskimi in nekriptografskimi funkcijami, ki jih zagotavlja varna kriptografska naprava denarnice, in jih uporablja;

(5) „instanca denarnice“ pomeni aplikacijo, nameščeno in konfigurirano na napravi ali v okolju uporabnika denarnice, ki je del enote denarnice in ki jo uporabnik denarnice uporablja za interakcijo z enoto denarnice;

([9]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(6) „varna kriptografska naprava denarnice“ pomeni napravo, odporno proti nedovoljenim posegom, ki zagotavlja okolje, ki je povezano z varno kriptografsko aplikacijo denarnice in ga ta uporablja za zaščito kritičnih sredstev ter zagotavljanje kriptografskih funkcij za varno izvajanje kritičnih operacij;

(7) „register tveganj“ pomeni evidenco informacij o ugotovljenih tveganjih, pomembnih za postopek certificiranja;

(8) „ponudnik denarnice“ pomeni fizično ali pravno osebo, ki zagotavlja rešitve denarnice;

(9) „certifikacijski organ“ pomeni organ tretje strani za ugotavljanje skladnosti, ki upravlja sheme certificiranja;

(10) „enota denarnice“ pomeni edinstveno konfiguracijo rešitve denarnice, ki vključuje instance denarnice, varne kriptografske aplikacije denarnice in varne kriptografske naprave denarnice, ki jih ponudnik denarnice zagotavlja posameznemu uporabniku denarnice;

(11) „kritična sredstva“ pomenijo sredstva znotraj enote denarnice ali v zvezi z njo, ki so tako izjemno pomembna, da bi ogrožanje njihove razpoložljivosti, zaupnosti ali celovitosti resno ogrozilo zmožnost zanašanja na enoto denarnice;

(12) „uporabnik denarnice“ pomeni uporabnika, ki upravlja enoto denarnice;

(13) „incident“ pomeni incident, kot je opredeljen v členu 6, točka 6, Direktive (EU) 2022/2555 Evropskega parlamenta in Sveta ([10]);

(14) „vgrajena politika razkrivanja“ pomeni sklop pravil, ki jih ponudnik vključi v elektronsko potrdilo o atributih in v katerih so navedeni pogoji, ki jih mora izpolniti na denarnice zanašajoča se stranka za dostop do elektronskega potrdila o atributih.

POGLAVJE II

NACIONALNE CERTIFIKACIJSKE SHEME

Člen 3

Vzpostavitev nacionalnih certifikacijskih shem

1. Države članice določijo lastnika sheme za vsako nacionalno certifikacijsko shemo.

2. Predmet certificiranja, opredeljenega v nacionalnih certifikacijskih shemah, je zagotavljanje in delovanje rešitev denarnic in shem elektronske identifikacije, v okviru katerih se te rešitve zagotavljajo.

3. V skladu z Izvedbeno uredbo (EU) 2015/1502 predmet certificiranja v nacionalnih certifikacijskih shemah vključuje naslednje elemente:

(a) komponente programske opreme, vključno z nastavitvami in konfiguracijami rešitve denarnice in sheme elektronske identifikacije, v okviru katere se rešitve denarnice zagotavljajo;

(b) komponente strojne opreme in platforme, na katerih komponente programske opreme iz točke (b) delujejo ali se nanje zanašajo pri kritičnih operacijah, kadar jih neposredno ali posredno zagotavljata rešitev denarnice in shema elektronske identifikacije, v okviru katere se ta rešitev zagotavlja, in kadar morajo dosegati želeno raven zanesljivosti za te komponente programske opreme. Kadar ponudnik denarnice ne zagotavlja komponent strojne opreme in platform, nacionalne certifikacijske sheme oblikujejo predpostavke za oceno komponent strojne opreme in platform, na podlagi katerih se lahko zagotovi odpornost proti napadalcem z velikim potencialom za napad v skladu z Izvedbeno uredbo (EU) 2015/1502, in določijo dejavnosti ocenjevanja za potrditev teh predpostavk, kot je navedeno v Prilogi IV;

([10]) Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2) (UL L 333, 27.12.2022, str. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(c) postopke, ki podpirajo zagotavljanje in delovanje rešitve denarnice, vključno s postopkom za pristop uporabnikov iz člena 5a Uredbe (EU) št. 910/2014, in zajemajo vsaj prijavo, upravljanje sredstev elektronske identifikacije in organizacijo v skladu z oddelki 2.1, 2.2 in 2.4 Priloge I k Izvedbeni uredbi Komisije (EU) 2015/1502.

4. Nacionalne certifikacijske sheme vključujejo opis specifične arhitekture rešitev denarnice in sheme elektronske identifikacije, v okviru katere se te rešitve zagotavljajo. Kadar nacionalne certifikacijske sheme zajemajo več kot eno specifično arhitekturo, vključujejo profil za vsako specifično arhitekturo.

5. Nacionalne certifikacijske sheme za vsak profil določijo vsaj naslednje:

(a) specifično arhitekturo rešitve denarnice in sheme elektronske identifikacije, v okviru katere se ta rešitev zagotavlja;

(b) varnostne nadzore, povezane z ravnmi zanesljivosti iz člena 8 Uredbe (EU) št. 910/2014;

(c) načrt ocenjevanja, pripravljen v skladu z oddelkom 7.4.1 standarda EN ISO/IEC 17065:2012;

(d) varnostne zahteve, potrebne za obravnavanje tveganj in groženj za kibernetsko varnost, navedenih v registru tveganj iz Priloge I k tej uredbi, do zahtevane ravni zanesljivosti in, kadar je ustrezno, za doseganje ciljev iz člena 51 Uredbe (EU) 2019/881;

(e) razvrščanje nadzorov iz točke (b) tega odstavka po komponentah arhitekture;

(f) opis, kako varnostni nadzori, razvrščanje, varnostne zahteve in načrt ocenjevanja iz točk (b) do (c) ponudnikom rešitev denarnic in sheme elektronske identifikacije, v okviru katere se te rešitve zagotavljajo, omogočajo ustrezno obravnavo tveganj in groženj za kibernetsko varnost, opredeljenih v registru tveganj iz točke (d), do zahtevane ravni zanesljivosti na podlagi ocene tveganja, da bi se tveganja in grožnje iz registra tveganj precizirala in dopolnila s tistimi, ki so značilni za strukturo.

6. V načrtu ocenjevanja iz odstavka 5, točka (c), so navedene dejavnosti ocenjevanja, ki jih je treba vključiti v ocenjevanje rešitev denarnice in sheme elektronske identifikacije, v okviru katere se te rešitve zagotavljajo.

7. Pri dejavnosti ocenjevanja iz odstavka 6 se od ponudnikov rešitev denarnic in sheme elektronske identifikacije, v okviru katere se te rešitve zagotavljajo, zahteva, da zagotovijo informacije, ki izpolnjujejo zahteve iz Priloge II.

Člen 4

Splošne zahteve

1. Nacionalne certifikacijske sheme zajemajo funkcionalne zahteve ter zahteve glede kibernetske varnosti in varstva podatkov z uporabo naslednjih certifikacijskih shem, če so na voljo in je to ustrezno:

(a) evropskih certifikacijskih shem za kibernetsko varnost, vzpostavljenih v skladu z Uredbo (EU) 2019/881, vključno z EUCC;

(b) nacionalnih certifikacijskih shem za kibernetsko varnost, ki jih zajema EUCC, v skladu s členom 49 Izvedbene uredbe (EU) 2024/482.

2. Nacionalne certifikacijske sheme se lahko poleg tega sklicujejo na naslednje, če so na voljo in je to ustrezno:

(a) druge zadevne nacionalne certifikacijske sheme;

(b) mednarodne, evropske in nacionalne standarde;

(c) tehnične specifikacije, ki izpolnjujejo zahteve iz Priloge II k Uredbi (EU) št. 1025/2012 Evropskega parlamenta inm Sveta ([11]).

3. Nacionalne certifikacijske sheme:

(a) določajo elemente, navedene v oddelku 6.5 standarda EN ISO/IEC 17067:2013;

(b) se izvajajo kot shema tipa 6 v skladu z oddelkom 5.3.8 standarda EN ISO/IEC 17067:2013.

4. Nacionalne certifikacijske sheme izpolnjujejo naslednje zahteve:

(a) samo ponudniki iz člena 5a(2) Uredbe (EU) št. 910/2014 so upravičeni, da se jim izdajo potrdila v okviru nacionalnih certifikacijskih shem;

(b) kot znak skladnosti se uporablja samo znak zaupanja;

(c) ponudniki rešitev denarnic in sheme elektronske identifikacije, v okviru katere se te rešitve zagotavljajo, pri sklicevanju na shemo vključijo sklice na Uredbo (EU) št. 910/2014 in to uredbo;

(d) ponudniki rešitev denarnic in sheme elektronske identifikacije, v okviru katere se te rešitve zagotavljajo, dopolnijo oceno tveganja sheme iz člena 3, odstavek 5, točka (f), da bi opredelili tveganja in grožnje, specifične za njihovo izvajanje, ter predlagajo ustrezne ukrepe za obravnavo vseh zadevnih tveganj in groženj;

(e) odgovornosti in pravni ukrepi se določijo in vključujejo sklice na veljavno nacionalno zakonodajo, v kateri so opredeljene odgovornosti in morebitni pravni ukrepi, kadar se certificiranje v okviru sheme uporablja goljufivo.

5. Ocena iz odstavka 4, točka (d), se posreduje certifikacijskemu organu v ocenjevanje.

Člen 5

Obvladovanje incidentov in ranljivosti

1. Nacionalne certifikacijske sheme vsebujejo zahteve glede obvladovanja incidentov in ranljivosti v skladu z odstavki 2 do 9.

2. Imetnik certifikata o skladnosti rešitve denarnice in sheme elektronske identifikacije, v okviru katere se ta rešitev zagotavlja, brez nepotrebnega odlašanja uradno obvesti svoj certifikacijski organ o vsaki kršitvi ali ogrožanju rešitve denarnice ali sheme elektronske identifikacije, v okviru katere se ta rešitev zagotavlja, ki bi verjetno vplivala na skladnost z zahtevami nacionalnih certifikacijskih shem.

3. Imetnik certifikata o skladnosti vzpostavi, vzdržuje in vodi politiko in postopke za obvladovanje ranljivosti, pri čemer upošteva postopke, določene v obstoječih evropskih in mednarodnih standardih, vključno s standardom EN ISO/IEC 30111:2019.

4. Imetnik certifikata o skladnosti certifikacijskemu organu izdajatelju certifikata priglasi ranljivosti in spremembe, ki vplivajo na rešitev denarnice, in sicer na podlagi opredeljenih meril o vplivu teh ranljivosti in sprememb.

5. Imetnik certifikata o skladnosti pripravi poročilo o analizi učinka ranljivosti za vsako ranljivost, ki vpliva na komponente programske opreme rešitve denarnice. Poročilo vključuje naslednje informacije:

(a) posledice ranljivosti na certificirano rešitev denarnice;

(b) morebitna tveganja, povezana z bližino ali verjetnostjo napada;

([11]) Uredba (EU) št. 1025/2012 Evropskega parlamenta in Sveta z dne 25. oktobra 2012 o evropski standardizaciji, spremembi direktiv Sveta 89/686/EGS in 93/15/EGS ter direktiv 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES in 2009/105/ES Evropskega parlamenta in Sveta ter razveljavitvi Sklepa Sveta 87/95/EGS in Sklepa št. 1673/2006/ES Evropskega parlamenta in Sveta (UL L 316, 14.11.2012, str. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(c) ali je ranljivost mogoče odpraviti z razpoložljivimi sredstvi;

(d) če je ranljivost mogoče odpraviti z razpoložljivimi sredstvi, možne načine za odpravo ranljivosti.

6. Kadar se zahteva priglasitev iz odstavka 4, imetnik certifikata o skladnosti brez nepotrebnega odlašanja certifikacijskemu organu pošlje poročilo o analizi učinka ranljivosti iz odstavka 5.

7. Imetnik certifikata o skladnosti vzpostavi, vzdržuje in vodi politiko obvladovanja ranljivosti v skladu z zahtevami iz Priloge I k aktu o kibernetski odpornosti ([12]).

8. Nacionalne certifikacijske sheme določijo zahteve razkritja ranljivosti, ki se uporabljajo za certifikacijske organe.

9. Imetnik certifikata o skladnosti razkrije in registrira vsako javno znano in sanirano ranljivost v rešitvi denarnice ali v enem od spletnih repozitorijev iz Priloge V.

Člen 6

Vzdrževanje nacionalnih certifikacijskih shem

1. Nacionalne certifikacijske sheme vsebujejo postopek za redno pregledovanje njihovega delovanja. Cilj tega postopka je potrditi njihovo ustreznost in opredeliti vidike, ki jih je treba izboljšati, ob upoštevanju povratnih informacij deležnikov.

2. Nacionalne certifikacijske sheme vključujejo določbe v zvezi z njihovim vzdrževanjem. Ta postopek vključuje vsaj naslednje zahteve:

(a) pravila za upravljanje opredelitve in zahtev nacionalnih certifikacijskih shem;

(b) določitev rokov za izdajo certifikatov po sprejetju posodobljenih različic nacionalnih certifikacijskih shem, tako za nove kot za predhodno izdane certifikate o skladnosti;

(c) redni pregled nacionalnih certifikacijskih shem, da se zagotovi dosledna uporaba njihovih zahtev, pri čemer se upoštevajo vsaj naslednji vidiki:

— zahteve za pojasnilo, naslovljene na lastnika sheme, v zvezi z zahtevami nacionalne certifikacijske sheme;

— povratne informacije deležnikov in drugih zainteresiranih strani;

— odzivnost lastnika nacionalne certifikacijske sheme na zahteve po informacijah;

(d) pravila za spremljanje referenčnih dokumentov in postopki za razvoj referenčnih različic nacionalnih certifikacijskih shem, kar vključuje vsaj prehodna obdobja;

(e) postopek za zagotovitev, da so zajeta najnovejša tveganja in grožnje za kibernetsko varnost, kot so navedena v registru tveganj iz Priloge I k tej uredbi;

(f) postopek za upravljanje drugih sprememb v nacionalnih certifikacijskih shemah.

([12]) Uredba (EU) 2024/2847 Evropskega parlamenta in Sveta z dne 23. oktobra 2024 o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi uredb (EU) št. 168/2013 in (EU) 2019/1020 ter Direktive (EU) 2020/1828 (Akt o kibernetski odpornosti) (UL L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

3. Nacionalne certifikacijske sheme vsebujejo zahteve za izvajanje ocenjevanj trenutno certificiranih izdelkov v določenem obdobju po reviziji sheme ali po objavi novih specifikacij ali standardov ali njihovih novih različic, ki jih morajo izpolnjevati rešitve denarnice in shema elektronske identifikacije, v okviru katere se te rešitve zagotavljajo.

POGLAVJE III

ZAHTEVE V ZVEZI Z LASTNIKI SHEM

Člen 7

Splošne zahteve

1. Lastniki shem razvijejo in vzdržujejo nacionalne certifikacijske sheme ter urejajo njihovo delovanje.

2. Lastniki sheme lahko vse svoje naloge ali del njih oddajo v podizvajanje tretji osebi. Pri oddaji naročil podizvajalcem lastniki sistema s pogodbo določijo dolžnosti in odgovornosti vseh strank. Lastniki sheme so še naprej odgovorni za vse dejavnosti, oddane v podizvajanje, ki jih izvajajo njihovi podizvajalci.

3. Lastniki shem svoje dejavnosti spremljanja, kadar je ustrezno, izvajajo vsaj na podlagi naslednjih informacij:

(a) informacij, ki jih prejmejo od certifikacijskih organov, nacionalnih akreditacijskih organov in ustreznih organov za nadzor trga;

(b) informacij, ki izhajajo iz njihovih lastnih revizij in preiskav ali revizij in preiskav drugega organa;

(c) pritožb, prejetih v skladu s členom 15.

4. Lastniki shem obvestijo skupino za sodelovanje o revizijah nacionalnih certifikacijskih shem. S to priglasitvijo se skupini za sodelovanje zagotovijo ustrezne informacije za izdajo priporočil lastnikom shem in mnenj o posodobljenih nacionalnih certifikacijskih shemah.

POGLAVJE IV

ZAHTEVE V ZVEZI S PONUDNIKI REŠITEV DENARNIC IN SHEME ELEKTRONSKE IDENTIFIKACIJE, V OKVIRU KATERE SE TE REŠITVE ZAGOTAVLJAJO

Člen 8

Splošne zahteve

1. Nacionalne certifikacijske sheme vsebujejo zahteve glede kibernetske varnosti na podlagi ocene tveganja vsake posamezne podprte arhitekture. Namen teh zahtev glede kibernetske varnosti je obravnavati ugotovljena tveganja in grožnje za kibernetsko varnost, kot je določeno v registru tveganj iz Priloge I.

2. V skladu s členom 5a(23) Uredbe (EU) št. 910/2014 nacionalne certifikacijske sheme zahtevajo, da so rešitve denarnic in sheme elektronske identifikacije, v okviru katerih se te rešitve zagotavljajo, odporne proti napadalcem z velikim potencialom za napad in visoko raven zanesljivosti, kot je navedeno v Izvedbeni uredbi (EU) 2015/1502.

3. Nacionalne certifikacijske sheme določijo varnostna merila, ki vključujejo naslednje zahteve:

(a) Akt o kibernetski odpornosti, kadar je ustrezno, ali zahteve, ki izpolnjujejo varnostne cilje iz člena 51 Uredbe (EU) 2019/881;

(b) vzpostavitev in izvajanje politik in postopkov v zvezi z obvladovanjem tveganj, povezanih z delovanjem rešitve denarnice, vključno z opredelitvijo in oceno tveganj ter zmanjševanjem ugotovljenih tveganj;

(c) vzpostavitev in izvajanje politik in postopkov v zvezi z upravljanjem sprememb in upravljanjem ranljivosti v skladu s členom 5 te uredbe;

(d) vzpostavitev in izvajanje politik in postopkov upravljanja človeških virov, vključno z zahtevami glede strokovnega znanja, zanesljivosti, izkušenj, varnostnega usposabljanja in kvalifikacij osebja, ki sodeluje pri razvoju ali delovanju rešitve denarnice;

(e) zahteve v zvezi z operativnim okoljem rešitve denarnice, tudi v obliki predpostavk o varnosti naprav in platform, na katerih delujejo komponente programske opreme denarnice, vključno z varnimi kriptografskimi napravami denarnice, ter po potrebi zahteve za ugotavljanje skladnosti za potrditev, da so navedene predpostavke preverjene na zadevnih napravah in platformah;

(f) za vsako predpostavko, ki ni podprta s certifikatom o skladnosti ali drugimi sprejemljivimi informacijami o zanesljivosti, opis mehanizma, ki ga ponudnik denarnice uporablja za uveljavljanje predpostavke, ter utemeljitev, da mehanizem zadostuje za preverjanje predpostavke;

(g) vzpostavitev in izvajanje ukrepov za zagotovitev uporabe trenutno certificirane različice rešitve denarnice.

4. Nacionalne certifikacijske sheme vsebujejo funkcionalne zahteve v zvezi z mehanizmi posodabljanja za vsako komponento programske opreme rešitev denarnice in shemo elektronske identifikacije, v okviru katere se te rešitve zagotavljajo, za operacije iz Priloge III.

5. Nacionalne certifikacijske sheme zahtevajo, da prosilec za certificiranje certifikacijskemu organu zagotovi ali kako drugače da na voljo naslednje informacije in dokumentacijo:

(a) dokazila v zvezi z informacijami iz Priloge IV, točka 1, po potrebi vključno s podrobnostmi o rešitvi denarnice in njeni izvorni kodi, vključno z:

— *informacijami o arhitekturi:* opis bistvenih varnostnih lastnosti, vključno z zunanjimi odvisnostmi, vsake komponente rešitve denarnice (vključno s komponentami proizvoda, postopka in storitve);

— *nadzorom in ravnmi zanesljivosti:* za vsak varnostni nadzor rešitve denarnice opis nadzora in zahtevane ravni zanesljivosti na podlagi Priloge k Izvedbeni uredbi (EU) 2015/1502, ki določa številne tehnične specifikacije in postopke, ki se uporabljajo za različne nadzore, izvedene s sredstvi elektronske identifikacije;

— *razvrščanjem nadzora po komponentah arhitekture:* opis, kako se izvaja nadzor denarnice z uporabo različnih komponent rešitve denarnice, na podlagi utemeljitve, zakaj je potrebna določena raven zanesljivosti, in kako se izvaja nadzor z vsemi zahtevanimi varnostnimi vidiki na ustrezni ravni;

— *razlogi in utemeljitvami kritja tveganj:* utemeljitev:

  — razvrščanja nadzora po komponentah,

  — ustreznosti predlaganega načrta ocenjevanja, da ustrezno zajame ves nadzor,

  — obsega nadzora tveganj in groženj za kibernetsko varnost, opredeljenih v registru tveganj, dopolnjenega z nadzorom tveganj in groženj, značilnih za izvajanje, na ustrezni ravni zanesljivosti;

(b) informacije iz Priloge V;

(c) popoln seznam certifikatov o skladnosti in drugih informacij o zanesljivosti, ki se uporabljajo kot dokaz med dejavnostmi ocenjevanja;

(d) vse druge informacije, pomembne za dejavnosti ocenjevanja.

POGLAVJE V

ZAHTEVE V ZVEZI S CERTIFIKACIJSKIMI ORGANI

Člen 9

Splošne zahteve

1. Če certifikacijski organi izpolnjujejo zahteve iz nacionalnih certifikacijskih shem v skladu z odstavkom 2, jih nacionalni akreditacijski organi, imenovani v skladu z Uredbo (ES) št. 765/2008 Evropskega parlamenta in Sveta ([13]), akreditirajo v skladu s standardom EN ISO/IEC 17065:2012.

2. Za namene akreditacije morajo certifikacijski organi imeti vsa naslednja znanja:

(a) podrobno in tehnično znanje o zadevnih arhitekturah rešitve denarnice in sheme elektronske identifikacije, v okviru katere se ta rešitev zagotavlja, ter o grožnjah in tveganjih, pomembnih za te arhitekture;

(b) znanje o razpoložljivih varnostnih rešitvah in njihovih lastnostih v skladu s Prilogo k Izvedbeni uredbi (EU) 2015/1502;

(c) znanje o dejavnostih, ki se izvajajo na podlagi certifikatov o skladnosti komponent rešitve denarnice in sheme elektronske identifikacije, v okviru katere se ta rešitev zagotavlja, kot predmet certificiranja;

(d) podrobno znanje o veljavnih nacionalnih certifikacijskih shemah, vzpostavljenih v skladu s poglavjem II.

3. Certifikacijski organi svoje dejavnosti spremljanja izvajajo zlasti na podlagi naslednjih informacij:

(a) informacij nacionalnih akreditacijskih organov in ustreznih organov za nadzor trga;

(b) informacij, ki izhajajo iz njihovih lastnih revizij in preiskav ali revizij in preiskav drugega organa;

(c) pritožb, prejetih v skladu s členom 15.

Člen 10

Oddaja naročil podizvajalcem

Certifikacijski organi lahko dejavnosti ocenjevanja iz člena 13 oddajo v podizvajanje tretjim osebam. Kadar so dejavnosti ocenjevanja oddane podizvajalcem, nacionalne certifikacijske sheme določajo naslednje:

(1) vsi podizvajalci certifikacijskega organa, ki izvajajo dejavnosti ocenjevanja, izpolnjujejo zahteve harmoniziranih standardov, kot so EN ISO/IEC 17025:2017 za preskušanje, EN ISO/IEC 17020:2012 za inšpekcijske preglede, EN ISO/IEC 17021-1:2015 za revizijo in EN ISO/IEC 17029:2019 za potrjevanje in preverjanje, kot je ustrezno in primerno za dejavnosti, ki jih je treba izvesti;

(2) certifikacijski organi prevzamejo odgovornost za vse dejavnosti ocenjevanja, oddane v podizvajanje drugim organom, in dokažejo, da so med akreditacijo sprejeli ustrezne ukrepe, po potrebi tudi z zanašanjem na proizvajalčevo lastno akreditacijo;

(3) raven, do katere se od lastnikov sheme ali stranke, katere rešitev denarnice se certificira v okviru certifikacijske sheme, pridobi predhodno soglasje o potrebah podizvajanja.

([13]) Uredba (ES) št. 765/2008 Evropskega parlamenta in Sveta z dne 9. julija 2008 o določitvi zahtev za akreditacijo in nadzor trga v zvezi s trženjem proizvodov ter razveljavitvi Uredbe (EGS) št. 339/93 (UL L 218, 13.8.2008, str. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

Člen 11

Priglasitev nadzornemu organu

Certifikacijski organi obvestijo nadzorni organ iz člena 46a(1) Uredbe (EU) št. 910/2014 o izdaji, začasni razveljavitvi in preklicu certifikatov o skladnosti rešitev denarnice in sheme elektronske identifikacije, v okviru katere se te rešitve zagotavljajo.

Člen 12

Obvladovanje incidentov in ranljivosti

1. Certifikacijski organi brez nepotrebnega odlašanja začasno razveljavijo certifikat o skladnosti rešitev denarnice in sheme elektronske identifikacije, v okviru katere se te rešitve zagotavljajo, potem ko potrdijo, da priglašena kršitev varnosti ali ogrožanje vpliva na skladnost z zahtevami nacionalnih certifikacijskih shem ali skladnost rešitve denarnice ali sheme elektronske identifikacije, v okviru katere se ta rešitev zagotavlja.

2. Certifikacijski organi prekličejo certifikat o skladnosti, ki je bil začasno razveljavljen zaradi nepravočasno odpravljene kršitve varnosti ali ogrožanja.

3. Certifikacijski organi prekličejo certifikat o skladnosti, kadar ugotovljena ranljivost ni bila pravočasno odpravljena sorazmerno z njeno resnostjo in morebitnim učinkom v skladu s členom 5c(4) in členom 5e(2) Uredbe (EU) št. 910/2014.

POGLAVJE VI

DEJAVNOSTI UGOTAVLJANJA SKLADNOSTI

Člen 13

Dejavnosti vrednotenja

1. Nacionalne certifikacijske sheme vsebujejo metode in postopke, ki jih uporabljajo organi za ugotavljanje skladnosti pri izvajanju svojih dejavnosti ocenjevanja v skladu s standardom EN ISO/IEC 17065:2012 in zajemajo vsaj:

(a) metode in postopke za izvajanje dejavnosti ocenjevanja, vključno s tistimi, ki so povezane z varnimi kriptografskimi napravami denarnic, kot je določeno v Prilogi IV;

(b) revizijo izvajanja rešitve denarnice in sheme elektronske identifikacije, v okviru katere se ta rešitev zagotavlja, na podlagi registra tveganj iz Priloge I, po potrebi dopolnjenega s tveganji, specifičnimi za izvajanje;

(c) dejavnosti funkcionalnega preskušanja, ki temeljijo, kadar so na voljo in je to ustrezno, na preskusnih sklopih, opredeljenih v skladu s tehničnimi specifikacijami ali standardi;

(d) oceno obstoja in ustreznosti postopkov vzdrževanja, vključno vsaj z upravljanjem različic, posodobitev in ranljivosti;

(e) oceno operativne učinkovitosti postopkov vzdrževanja, vključno vsaj z upravljanjem različic, posodobitev in ranljivosti;

(f) analizo odvisnosti, ki jo zagotovi ponudnik denarnice, vključno z metodologijo za oceno sprejemljivosti informacij o zanesljivosti, ki vključuje elemente iz Priloge VI;

(g) oceno ranljivosti na ustrezni ravni, vključno s:

— pregledom zasnove rešitve denarnice in, kadar je ustrezno, njene izvorne kode;

— preskušanjem odpornosti rešitve denarnice proti napadalcem z velikim potencialom za napad za visoko raven zanesljivosti v skladu z oddelkom 2.2.1 Priloge k Izvedbeni uredbi (EU) 2015/1502;

(h) oceno razvoja okolja groženj in njegovega vpliva na kritje tveganj z rešitvijo denarnice, da se ugotovi, katere dejavnosti ocenjevanja so potrebne za različne komponente rešitve denarnice.

2. Nacionalne certifikacijske sheme vsebujejo oceno za ugotavljanje, ali se izvajanje rešitev denarnic in sheme elektronske identifikacije, v okviru katere se te rešitve zagotavljajo, ujema z arhitekturo iz člena 3, odstavek 5, točka (a), ter oceno za ugotavljanje, ali je načrt ocenjevanja, predlagan skupaj z izvajanjem, skladen z načrtom ocenjevanja iz člena 3, odstavek 5, točka (c).

3. Nacionalne certifikacijske sheme določajo pravila vzorčenja, da bi se izognili ponavljanju enakih dejavnosti ocenjevanja in osredotočili na dejavnosti, ki so specifične za določeno različico. Navedena pravila vzorčenja omogočajo, da se funkcionalni in varnostni preskusi izvajajo le na vzorcu različic ciljne komponente rešitve denarnice in sheme elektronske identifikacije, v okviru katere se ta rešitev zagotavlja, ter na vzorcu ciljnih naprav. Nacionalne certifikacijske sheme od vseh certifikacijskih organov zahtevajo, da utemeljijo uporabo vzorčenja.

4. Nacionalne certifikacijske sheme zahtevajo, da certifikacijski organ oceni varno kriptografsko aplikacijo denarnice na podlagi metod in postopkov iz Priloge IV.

Člen 14

Dejavnosti certificiranja

1. Nacionalne certifikacijske sheme določijo dejavnost potrjevanja za namen izdaje certifikata o skladnosti v skladu z oddelkom V(a) standarda EN ISO/IEC 17067:2013, preglednica 1, vključno z naslednjimi vidiki:

(a) vsebino certifikata o skladnosti, kot je določeno v Prilogi VII;

(b) kako je treba o rezultatih ocenjevanja poročati v javnem poročilu o certificiranju, vključno vsaj s povzetkom predhodnega načrta revizije in potrjevanja, kot je določeno v Prilogi VIII;

(c) vsebino rezultatov ocenjevanja, sporočenih v poročilu o oceni certificiranja, vključno z elementi iz Priloge VIII.

2. Poročilo o oceni certificiranja se lahko da na voljo skupini za sodelovanje in Komisiji.

Člen 15

Pritožbe

Nacionalne certifikacijske sheme vsebujejo postopke ali sklicevanja na veljavno nacionalno zakonodajo, ki opredeljujejo mehanizem za učinkovito vlaganje in obravnavanje pritožb v zvezi z njihovim izvajanjem certifikacijske sheme ali izdanega certifikata o skladnosti. Ti postopki vključujejo obveščanje pritožnika o poteku postopka in sprejeti odločitvi ter o pravici do učinkovitega pravnega sredstva. Nacionalne certifikacijske sheme zahtevajo, da se vse pritožbe, ki jih certifikacijski organ ni rešil ali jih ne more rešiti, pošljejo lastniku sheme v oceno in reševanje.

Člen 16

Nadzorne dejavnosti

1. Nacionalne certifikacijske sheme od certifikacijskih organov zahtevajo, da izvajajo nadzorne dejavnosti, ki vključujejo nadzorno ocenjevanje postopkov v kombinaciji z naključnimi preskusi ali inšpekcijskimi pregledi.

2. Nacionalne certifikacijske sheme od lastnikov shem zahtevajo, da spremljajo skladnost certifikacijskih organov z njihovimi obveznostmi v skladu z Uredbo (EU) št. 910/2014 in, kadar je ustrezno, v skladu z nacionalnimi certifikacijskimi shemami.

3. Nacionalne certifikacijske sheme od certifikacijskih organov zahtevajo, da spremljajo:

(a) skladnost imetnikov certifikata o skladnosti, izdanega v okviru nacionalnih certifikacijskih shem, z njihovimi obveznostmi glede certificiranja v skladu z Uredbo (EU) št. 910/2014 in nacionalnimi certifikacijskimi shemami;

(b) skladnost certificirane rešitve denarnice z zahtevami iz nacionalnih certifikacijskih shem.

Člen 17

Posledice neskladnosti

Nacionalne certifikacijske sheme določijo posledice za neskladnost certificirane rešitve denarnice in sheme elektronske identifikacije, v okviru katere se ta rešitev zagotavlja, z zahtevami iz te uredbe. Te posledice vključujejo:

(1) obveznost certifikacijskega organa, da o tem obvesti imetnika certifikata o skladnosti in od njega zahteva, da izvede popravne ukrepe;

(2) obveznost certifikacijskega organa, da o tem obvesti druge ustrezne organe za nadzor trga, kadar neskladnost zadeva ustrezno zakonodajo Unije;

(3) pogoje za izvedbo popravnih ukrepov s strani imetnika certifikata o skladnosti;

(4) pogoje za začasno razveljavitev certifikata o skladnosti s strani certifikacijskega organa in za njegovo ponovno vzpostavitev po odpravi neskladnosti;

(5) pogoje za preklic certifikata o skladnosti s strani certifikacijskega organa;

(6) posledice neizpolnjevanja zahtev nacionalne certifikacijske sheme s strani certifikacijskega organa.

POGLAVJE VII

ŽIVLJENJSKI CIKEL CERTIFICIRANJA

Člen 18

Življenjski cikel certificiranja

1. Veljavnost certifikatov o skladnosti, izdanih v okviru nacionalnih certifikacijskih shem, je odvisna od rednih dejavnosti ocenjevanja, ki jih certifikacijski organ izvaja v skladu z zahtevami iz Priloge IX.

2. Nacionalne certifikacijske sheme vsebujejo postopek za ponovno certificiranje rešitev denarnice in sheme elektronske identifikacije, v okviru katere se te rešitve zagotavljajo, na zahtevo imetnika certifikata o skladnosti pred iztekom veljavnosti prvotnega certifikata o skladnosti. Ta postopek ponovnega certificiranja vključuje celovito ocenjevanje rešitve denarnice in sheme elektronske identifikacije, v okviru katere se ta rešitev zagotavlja, vključno z oceno ranljivosti, v skladu z načeli iz Priloge IX.

3. Nacionalne certifikacijske sheme vključujejo postopek za upravljanje sprememb rešitve denarnice in sheme elektronske identifikacije, v okviru katere se ta rešitev zagotavlja. Ta postopek vključuje pravila za določanje, ali je treba spremembo vključiti v posebno ocenjevanje iz odstavka 4 ali v preverjanje operativne učinkovitosti postopkov vzdrževanja iz Priloge IV.

4. Nacionalne certifikacijske sheme vsebujejo postopek za posebna ocenjevanja v skladu s standardom EN ISO/IEC 17065:2012. Ta postopek za posebna ocenjevanja vključuje izbor dejavnosti, ki jih je treba izvesti za obravnavo specifičnega vprašanja, ki je sprožilo posebno ocenjevanje.

5. Nacionalne certifikacijske sheme določijo pravila v zvezi s preklicem certifikata o skladnosti.

POGLAVJE VIII

VODENJE EVIDENC IN VARSTVO INFORMACIJ

Člen 19

Hranjenje evidenc

1. Nacionalne certifikacijske sheme vsebujejo zahteve za certifikacijske organe v zvezi s sistemom evidentiranja vseh zadevnih informacij, pridobljenih v zvezi z dejavnostmi ugotavljanja skladnosti, ki jih izvajajo, vključno s podatki, ki jih izdajo in prejmejo ponudniki rešitev denarnic in shem elektronske identifikacije, v okviru katerih se te rešitve zagotavljajo. Evidence takih informacij se hranijo na varen način. Evidence se lahko hranijo v elektronski obliki in ostanejo dostopne tako dolgo, kot to zahteva pravo Unije ali nacionalno pravo, in vsaj pet let po preklicu ali izteku veljavnosti zadevnega certifikata o skladnosti.

2. Nacionalne certifikacijske sheme določajo, da mora imetnik certifikata o skladnosti naslednje informacije za namene te uredbe hraniti varno in vsaj pet let po preklicu ali izteku veljavnosti zadevnega certifikata o skladnosti:

(a) evidence informacij, zagotovljene certifikacijskemu organu ali njegovim morebitnim podizvajalcem med postopkom certificiranja;

(b) primerke komponent strojne opreme, ki so bile vključene v področje uporabe certifikacije rešitve denarnice.

3. Nacionalne certifikacijske sheme od imetnika potrdila o skladnosti zahtevajo, da na zahtevo zagotovi informacije iz odstavka 1 certifikacijskemu organu ali nadzornemu organu iz člena 46a(1) Uredbe (EU) št. 910/2014.

Člen 20

Varstvo informacij

V okviru nacionalnih certifikacijskih shem se od vseh oseb ali organizacij, ki jim je odobren dostop do informacij pri izvajanju dejavnosti v okviru nacionalne certifikacijske sheme, zahteva, da zagotovijo varnost in varstvo poslovnih skrivnosti in drugih zaupnih informacij, ohranijo pravice intelektualne lastnine ter sprejmejo potrebne in ustrezne tehnične in organizacijske ukrepe za zagotovitev te zaupnosti.

POGLAVJE IX

KONČNE DOLOČBE

Člen 21

Prehod na evropsko certifikacijsko shemo za kibernetsko varnost

Ta uredba se pregleda ob sprejetju prve evropske certifikacijske sheme za kibernetsko varnost za rešitve denarnic in sheme elektronske identifikacije, v okviru katerih se te rešitve zagotavljajo, da se upošteva prispevek take evropske certifikacijske sheme za kibernetsko varnost k splošnemu certificiranju rešitev denarnic in shem elektronske identifikacije, v okviru katerih se te rešitve zagotavljajo.

Člen 22

Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 28. novembra 2024

Za Komisijo
predsednica
Ursula VON DER LEYEN

PRILOGA I

REGISTER TVEGANJ ZA EVROPSKE DENARNICE ZA DIGITALNO IDENTITETO

Uvod

V registru tveganj so opisana glavna tveganja in grožnje za varnost in zasebnost denarnic, ki se ustrezno obravnavajo v vsaki arhitekturi in izvedbi denarnic. **Visoka tveganja** (oddelek I) so povezana z uporabo denarnic s strani uporabnikov in zanašajočih se strank ter z neposrednimi grožnjami, usmerjenimi v sredstva denarnic. Poleg tega je opredeljenih nekaj **sistemskih tveganj** (oddelek II) za denarnice, ki bi običajno izhajala iz kombinacije groženj, ki veljajo za celoten sistem denarnice.

Vrsta tveganja	ID tveganja	Naziv povezanega tveganja
Visoka tveganja za denarnice	R1	Ustvarjanje ali uporaba obstoječe elektronske identitete
	R2	Ustvarjanje ali uporaba lažne elektronske identitete
	R3	Ustvarjanje ali uporaba lažnih atributov
	R4	Kraja identitete
	R5	Kraja podatkov
	R6	Razkritje podatkov
	R7	Manipulacija s podatki
	R8	Izguba podatkov
	R9	Nedovoljena transakcija
	R10	Manipulacija s transakcijami
	R11	Zatajitev
	R12	Razkritje podatkov o transakcijah
	R13	Motnja storitve
	R14	Nadzor
Sistemska tveganja	SR1	Množični nadzor
	SR2	Škodovanje ugledu
	SR3	Pravna neskladnost

V registru so opredeljene tudi **tehnične grožnje** (oddelek III), usmerjene v izvajanje rešitve denarnice. Te grožnje so povezane z visokimi tveganji v smislu, da bi se lahko z vsako od njih sprožila številna visoka tveganja.

Vrsta grožnje	ID grožnje	Naziv povezane grožnje	Podkategorije groženj
Tehnična grožnja	TT1	Fizični napadi	1.1 *Kraja*
			1.2 *Uhajanje informacij*
			1.3 *Nedovoljeno poseganje*
	TT2	Napake in napačne konfiguracije	2.1 *Napake pri upravljanju informacijskega sistema*
			2.2 *Napake na ravni aplikacije ali uporabniške napake*
			2.3 *Napake razvojnega časa in napačne konfiguracije sistema*

Vrsta grožnje	ID grožnje	Naziv povezane grožnje	Podkategorije groženj
	TT3	Uporaba nezanesljivih virov	3.1 *Napačna uporaba ali konfiguracija komponent denarnice*
	TT4	Okvara in izpadi	4.1 *Okvara ali motnja v delovanju opreme, naprav ali sistemov*
			4.2 *Izguba sredstev*
			4.3 *Izguba podpornih storitev*
	TT5	Zlonamerna dejanja	5.1 *Prestrezanje informacij*
			5.2 *Ribarjenje in slepljenje*
			5.3 *Ponavljanje sporočil*
			5.4 *Napad s surovo silo*
			5.5 *Ranljivosti programske opreme*
			5.6 *Napadi na oskrbovalno verigo*
			5.7 *Zlonamerna programska oprema*
			5.8 *Napoved naključnega števila*

Nazadnje so v registru **navedene neposredne grožnje denarnicam**, pri čemer je vsaka povezana z (neizčrpno) izbiro tveganj (oddelek IV).

ODDELEK I:

Visoka tveganja za denarnice

R1. Ustvarjanje ali uporaba obstoječe elektronske identitete

Ustvarjanje ali uporaba obstoječe elektronske identitete pomeni ustvarjanje elektronske identitete v denarnici, ki obstaja v resničnem svetu in je dodeljena drugemu uporabniku. To tveganje v osnovi povzroča tveganje kraje identitete (R4) in nedovoljenih transakcij (R9).

R2. Ustvarjanje ali uporaba lažne elektronske identitete

Ustvarjanje ali uporaba lažne elektronske identitete pomeni ustvarjanje elektronske identitete v denarnici, ki ne obstaja v resničnem svetu.

R3. Ustvarjanje ali uporaba lažnih atributov

Ustvarjanje ali uporaba lažnih atributov pomeni ustvarjanje ali uporabo atributov, za katere ni mogoče potrditi, da jih je izdal določeni ponudnik, in ki jim ni mogoče zaupati.

R4. Kraja identitete

Kraja identitete pomeni nedovoljeno pridobitev enote denarnice ali izgubo avtentikacijskih dejavnikov, ki omogočajo lažno izdajanje za drugo osebo.

R5. Kraja podatkov

Kraja podatkov pomeni nedovoljeno pridobivanje podatkov. Kraja podatkov je povezana tudi z grožnjami, kot sta prestrezanje podatkov (nedovoljeno zajemanje podatkov v tranzitu) in dešifriranje podatkov (nedovoljeno dekodiranje šifriranih podatkov), ki lahko v nekaterih primerih privedejo do razkritja podatkov (R6).

R6. Razkritje podatkov

Razkritje podatkov pomeni nedovoljeno razkritje osebnih podatkov, vključno s posebnimi vrstami osebnih podatkov. Tveganje kršitve zasebnosti je zelo podobno, če se obravnava z vidika zasebnosti in ne z vidika varnosti.

R7. Manipulacija s podatki

Manipulacija s podatki pomeni nedovoljeno spreminjanje podatkov.

R8. Izguba podatkov

Izguba podatkov pomeni stanje, ko se podatki, shranjeni v denarnici, izgubijo zaradi napačne uporabe ali zlonamernega dejanja. To tveganje pogosto spremlja manipulacijo s podatki (R7) ali motnjo storitve (R13), kjer ni mogoče obnoviti podatkov ali dela podatkov.

R9. Nedovoljena transakcija

Nedovoljene transakcije pomenijo operativne dejavnosti, ki se izvajajo brez dovoljenja ali vednosti uporabnika denarnice. V številnih primerih lahko vodijo v krajo identitete (R4) ali razkritje podatkov (R6). Povezane so tudi z nedovoljenimi transakcijami, kot je napačna uporaba kriptografskih ključev.

R10. Manipulacija s transakcijami

Manipulacija s transakcijami pomeni nedovoljeno spreminjanje operacij v denarnici. Manipulacija s transakcijami je napad na celovitost in je povezana s kršitvijo celovitosti podatkov.

R11. Zatajitev

Zatajitev pomeni stanje, ko lahko deležnik zanika izvedbo dejanja ali sodelovanje v transakciji, drugi deležniki pa nimajo ustreznih dokazov, da bi mu nasprotovali.

R12. Razkritje podatkov o transakcijah

Razkritje podatkov o transakcijah pomeni razkritje informacij o transakciji med deležniki.

R13. Motnja storitve

Motnja storitve pomeni prekinitev ali poslabšanje normalnega delovanja denarnice. Posebna vrsta motnje storitve je zaklepanje uporabniškega dostopa, tj. nezmožnost uporabnika, da dostopa do svojega računa ali denarnice.

R14. Nadzor

Nadzor ali spremljanje pomeni nedovoljeno sledenje ali opazovanje dejavnosti, komunikacije ali podatkov uporabnika denarnice. Pogosto je povezan s sklepanjem, tj. izpeljevanjem občutljivih ali osebnih informacij iz na videz neškodljivih podatkov.

ODDELEK II:

Sistemska tveganja

Ta tveganja se ne uporabljajo na seznamu groženj, saj so običajno posledica več groženj, ki se ponavljajo na način, ki ogroža celoten sistem.

SR1. Množični nadzor

Množični nadzor pomeni sledenje ali opazovanje dejavnosti številnih uporabnikov prek komunikacije ali podatkov njihovih denarnic. Pogosto je povezan z nadzorom (R14) in sklepanjem na svetovni ravni, pri čemer se informacije o številnih uporabnikih kombinirajo, da se izpeljejo občutljivi ali osebni podatki o uporabnikih ali opredelijo statistični trendi, ki se lahko uporabijo za načrtovanje nadaljnjih napadov.

SR2. Škodovanje ugledu

Škodovanje ugledu pomeni škodo, povzročeno ugledu organizacije ali vladnega organa. Do njega lahko pride tudi zaradi drugih tveganj, kadar o kršitvi ali incidentu poročajo mediji in organizacijo prikažejo v neugodni luči. Škodovanje ugledu lahko povzroči dodatna tveganja, kot sta izguba zaupanja zaradi razumnih dvomov uporabnika in izguba ekosistema, ko se ekosistem v celoti zruši.

SR3. Pravna neskladnost

Pravna neskladnost pomeni stanje, v katerem ni mogoče upoštevati zadevnih zakonov, predpisov ali standardov. Ker sta, kar zadeva denarnice, varnost in zasebnost rešitve pravni zahtevi, bodo vse grožnje verjetno privedle do neke vrste pravne neskladnosti.

ODDELEK III:

Tehnične grožnje

Niso vse tehnične grožnje povezane s specifičnimi tveganji za denarnice, saj so mnoge od njih sredstva, ki bi jih bilo mogoče uporabiti za izvajanje napadov, ki ustrezajo več različnim tveganjem.

TT1. Fizični napadi

1.1 *Kraja*

Kraja pomeni krajo naprav, ki lahko spremenijo pravilno delovanje denarnice (če je naprava ukradena in enota denarnice ni ustrezno zaščitena). Prispeva lahko k številnim tveganjem, vključno s krajo identitete (R4), krajo podatkov (R5) in nedovoljenimi transakcijami (R9).

1.2 *Uhajanje informacij*

Uhajanje informacij pomeni nepooblaščen dostop, izpostavljenost informacijam ali njihovo posredovanje po fizičnem dostopu do denarnice. Prispeva lahko zlasti k razkritju podatkov (R6) in kraji podatkov (R5).

1.3 *Nedovoljeno poseganje*

Nedovoljeno poseganje pomeni kršitev celovitosti ene ali več komponent enote denarnice ali komponent, na katere se ta enota denarnice zanaša, npr. uporabniške naprave ali njenega operacijskega sistema. Prispeva lahko zlasti k manipulaciji s podatki (R7), izgubi podatkov (R8) in manipulaciji s transakcijami (R10). Nedovoljeno poseganje v komponente programske opreme lahko prispeva k številnim tveganjem.

TT2. Napake in napačne konfiguracije

2.1 *Napake pri upravljanju informacijskega sistema*

Napake pri upravljanju informacijskega sistema pomenijo uhajanje informacij, njihovo posredovanje ali škodo, ki jo povzroči napačna uporaba sredstev informacijske tehnologije s strani uporabnikov (nepoznavanje funkcij aplikacije) ali neustrezna konfiguracija ali upravljanje sredstev informacijske tehnologije.

2.2 *Napake na ravni aplikacije ali uporabniške napake*

Napake na ravni aplikacije ali uporabniške napake pomenijo motnje v delovanju aplikacije zaradi napake v sami aplikaciji ali napake enega od uporabnikov (uporabnikov denarnic in zanašajočih se strank).

2.3 *Napake razvojnega časa in napačne konfiguracije sistema*

Napake razvojnega časa in napačne konfiguracije sistema pomenijo motnje ali ranljivosti, ki jih povzročijo neustrezno razvita ali konfigurirana sredstva informacijske tehnologije ali poslovni procesi (neustrezne specifikacije izdelkov informacijske tehnologije, neustrezna uporabnost, nezanesljivi vmesniki, neustrezni politični in postopkovni tokovi, napake v zasnovi).

TT3. Uporaba nezanesljivih virov

Uporaba nezanesljivih virov pomeni dejavnost, ki privede do nenamerne škode zaradi slabo opredeljenih odnosov zaupanja, kot je zaupanje tretjemu ponudniku brez zadostne zanesljivosti.

3.1 *Napačna uporaba ali konfiguracija komponent denarnice*

Napačna uporaba ali konfiguracija komponent denarnice pomeni nenamerno škodo na komponentah denarnice zaradi napačne uporabe ali napačne konfiguracije s strani uporabnikov denarnic ali nezadostno usposobljenih razvijalcev ali zaradi neprilagoditve spremembam v okolju groženj, običajno zaradi uporabe ranljivih komponent tretjih strani ali izvajalnih platform.

TT4. Okvara in izpadi

4.1 *Okvara ali motnja v delovanju opreme, naprav ali sistemov*

Okvara ali motnja v delovanju opreme pomeni nenamerno škodo na sredstvih informacijske tehnologije zaradi okvare ali motnje v delovanju opreme, vključno z infrastrukturo ponudnika in uporabniškimi napravami.

4.2 *Izguba sredstev*

Izguba virov pomeni izpad ali motnjo zaradi nerazpoložljivosti takih virov, npr. vzdrževalnih delov.

4.3 *Izguba podpornih storitev*

Izguba podpornih storitev pomeni izpad ali motnjo zaradi nerazpoložljivosti podpornih storitev, potrebnih za pravilno delovanje sistema, vključno z omrežno povezljivostjo infrastrukture ponudnika in uporabniške naprave.

TT5. Zlonamerna dejanja

5.1 *Prestrezanje informacij*

Prestrezanje informacij pomeni zajetje neustrezno zavarovanih informacij pri prenosu, vključno z napadi moža v sredini.

5.2 *Ribarjenje in slepljenje*

Ribarjenje pomeni zajetje informacij, ki jih zagotovi uporabnik po zavajajoči interakciji in je pogosto povezano s slepljenjem zakonitih komunikacijskih sredstev in spletnih mest. Te grožnje so usmerjene v uporabnika in običajno prispevajo h kraji identitete (R4) in nedovoljenim transakcijam (R9), pogosto s krajo podatkov (R5) ali razkritjem podatkov (R6).

5.3 *Ponavljanje sporočil*

Ponavljanje sporočil pomeni ponovno uporabo predhodno prestreženih sporočil za izvajanje nedovoljenih transakcij, pogosto na ravni protokola. Ta tehnična grožnja prispeva predvsem k nedovoljenim transakcijam, ki lahko nato vodijo do drugih tveganj, odvisno od transakcije.

5.4 *Napad s surovo silo*

Napad s surovo silo pomeni kršitev varnosti, pogosto zaupnosti, z izvajanjem velikega števila interakcij, dokler odzivi ne zagotovijo koristnih informacij.

5.5 *Ranljivosti programske opreme*

Grožnja, povezana z ranljivostmi programske opreme, je kršitev varnosti z izkoriščanjem ranljivosti programske opreme v komponentah denarnice ali komponentah programske in strojne opreme, ki se uporabljajo pri izvajanju denarnice, vključno z objavljenimi in neobjavljenimi ranljivostmi (ranljivostmi ničtega dne).

5.6 *Napadi na oskrbovalno verigo*

Napad na oskrbovalno verigo pomeni kršitev varnosti z napadi na dobavitelja ponudnika denarnice ali uporabnike denarnice, da se omogočijo nadaljnji napadi na samo denarnico.

5.7 *Zlonamerna programska oprema*

Zlonamerna programska oprema pomeni kršitev varnosti z zlonamernimi aplikacijami, ki izvajajo neželena in nezakonita dejanja nad denarnico.

5.8 *Napoved naključnega števila*

Napoved naključnega števila pomeni omogočanje napadov s surovo silo z delnim ali popolnim napovedovanjem generiranih naključnih števil.

ODDELEK IV:

Grožnje denarnicam

V tem zadnjem oddelku je predstavljen izbor značilnih scenarijev groženj, specifičnih za denarnice, ki so razvrščeni glede na ključna povezana visoka tveganja, kot so navedena zgoraj. Ta seznam navaja grožnje, ki jih je treba zajeti, vendar ne predstavlja izčrpnega seznama groženj, ki so v veliki meri odvisne od arhitekture izbrane rešitve denarnice in razvoja okolja groženj. Poleg tega je lahko, kar zadeva oceno tveganja in predlagane ukrepe, ponudnik denarnice odgovoren le za komponente, ki spadajo na področje uporabe certificiranja (*).

ID *Identifikator*	Opis grožnje *Opis ugotovljene grožnje* (*)	Tveganje *Povezana tveganja*
TR1	Napadalec lahko psevdonime prekliče brez utemeljenega razloga.	Ustvarjanje ali uporaba lažne elektronske identitete (R2)
TR2	Napadalec lahko izda izmišljene elektronske identitete, ki ne obstajajo.	Ustvarjanje ali uporaba lažne elektronske identitete (R2)
TR3	Napadalec lahko začne izdajati nedovoljene identifikacijske podatke osebe.	Ustvarjanje ali uporaba lažne elektronske identitete (R2)
TR4	Napadalec lahko zavede administratorja, da na zanesljivi seznam ponudnikov identifikacijskih podatkov osebe vnese napačnega ponudnika.	Ustvarjanje ali uporaba lažne elektronske identitete (R2)
TR5	Napadalec lahko obide storitev za preverjanje identitete na daljavo.	Ustvarjanje ali uporaba obstoječe elektronske identitete (R1) / ustvarjanje ali uporaba lažne elektronske identitete (R2)
TR6	Napadalec lahko obide storitev fizičnega preverjanja identitete.	Ustvarjanje ali uporaba obstoječe elektronske identitete (R1) / ustvarjanje ali uporaba lažne elektronske identitete (R2)
TR7	Napadalec lahko obide storitve preverjanja identitete, povezane z uporabo (kvalificiranega) certifikata na daljavo.	Ustvarjanje ali uporaba obstoječe elektronske identitete (R1) / ustvarjanje ali uporaba lažne elektronske identitete (R2)
TR8	Napadalec lahko dobi dostop do denarnice, ki ni vezana na osebo.	Ustvarjanje ali uporaba obstoječe elektronske identitete (R1) / ustvarjanje ali uporaba lažne elektronske identitete (R2)
TR9	Napadalec lahko premaga tehnični in postopkovni nadzor, da bi ustvaril napačne identifikacijske podatke osebe.	Ustvarjanje ali uporaba obstoječe elektronske identitete (R1) / ustvarjanje ali uporaba lažne elektronske identitete (R2)
TR10	Napadalec lahko aktivira novo denarnico na neveljavni varni kriptografski napravi denarnice.	Ustvarjanje ali uporaba obstoječe elektronske identitete (R1) / ustvarjanje ali uporaba lažne elektronske identitete (R2)
TR11	Napadalec lahko obide storitev preverjanja identitete, povezano z uporabo obstoječih sredstev za elektronsko identifikacijo.	Ustvarjanje ali uporaba obstoječe elektronske identitete (R1) / kraja identitete (R4) / nedovoljena transakcija (R9)
TR12	Napadalec lahko zaobide preverjanje ponudnika identifikacijskih podatkov osebe, ali je denarnica pod nadzorom uporabnika, in doseže, da se identifikacijski podatki osebe izdajo ogroženi denarnici pod nadzorom napadalca.	Ustvarjanje ali uporaba obstoječe elektronske identitete (R1) / kraja identitete (R4) / nedovoljena transakcija (R9)

ID *Identifikator*	Opis grožnje *Opis ugotovljene grožnje (*)*	Tveganje *Povezana tveganja*
TR13	Napadalec lahko pridobi veljavne identifikacijske podatke osebe v neveljavni enoti denarnice.	Ustvarjanje ali uporaba obstoječe elektronske identitete (R1) / kraja identitete (R4) / nedovoljena transakcija (R9)
TR14	Ponudnik informacijskih podatkov osebe lahko izda izmišljeno identiteto, ki je povezana z obstoječo osebo.	Ustvarjanje ali uporaba obstoječe elektronske identitete (R1) / kraja identitete (R4) / nedovoljena transakcija (R9)
TR15	Napadalec lahko identifikacijske podatke osebe poveže z napačno denarnico, ker ponudnik identifikacijskih podatkov osebe teh ne more povezati s pravilno denarnico.	Ustvarjanje ali uporaba obstoječe elektronske identitete (R1) / kraja identitete (R4) / nedovoljena transakcija (R9)
TR16	Napadalec lahko zavede uporabnika, da odobri aktivacijo nove enote/instance denarnice pod napadalčevim nadzorom – tudi z naknadnim nadzorom potrdil.	Ustvarjanje ali uporaba obstoječe elektronske identitete (R1) / ustvarjanje ali uporaba lažne elektronske identitete (R2) / kraja identitete (R4) / nedovoljena transakcija (R9)
TR17	Napadalec lahko izda identifikacijske podatke osebe druge države za dostop do podatkov / digitalnih sredstev ciljanih državljanov.	Ustvarjanje ali uporaba obstoječe elektronske identitete (R1) / kraja identitete (R4) / nedovoljena transakcija (R9)
TR18	Napadalec lahko premaga tehnični in postopkovni nadzor, da bi ustvaril lažna (kvalificirana) elektronska potrdila o atributih.	Ustvarjanje ali uporaba lažnih atributov (R3)
TR19	Napadalec lahko predloži (kvalificirana) elektronska potrdila o atributih, ki mu niso veljavno izdana.	Ustvarjanje ali uporaba lažnih atributov (R3)
TR20	Napadalec lahko napade kriptografski povezovalni mehanizem denarnice med identifikacijskimi podatki osebe in (kvalificiranim) elektronskim potrdilom o atributih, ki se mu ne bi smeli izdati.	Ustvarjanje ali uporaba lažnih atributov (R3)
TR21	Napadalec lahko uporablja (kvalificirano) elektronsko potrdilo o atributih v denarnici, čeprav je fizična različica potrdila potekla ali je neveljavna.	Ustvarjanje ali uporaba lažnih atributov (R3)
TR22	Napadalec se lahko izogne ponudniku (kvalificiranega) elektronskega potrdila o atributih pri preverjanju, ali je denarnica pod nadzorom uporabnika, in doseže, da se (kvalificirano) elektronsko potrdilo o atributih izda ogroženi denarnici pod nadzorom napadalca.	Ustvarjanje ali uporaba lažnih atributov (R3)
TR23	Napadalec lahko ponaredi elektronska potrdila o atributih.	Ustvarjanje ali uporaba lažnih atributov (R3)
TR24	Napadalec lahko ponarejena elektronska potrdila o atributih vstavi v denarnico.	Ustvarjanje ali uporaba lažnih atributov (R3)
TR25	Denarnica lahko predstavi atribute zanašajoči se stranki brez odobritve uporabnika.	Razkritje podatkov (R6)
TR26	Identifikacijski podatki osebe, (kvalificirano) elektronsko potrdilo o atributih ali psevdonim se lahko predstavijo napačni zanašajoči se stranki.	Razkritje podatkov (R6)
TR27	Napadalec lahko sproži zlonamerno podaljšanje elektronskega potrdila o atributih.	Razkritje podatkov (R6)
TR28	Napadalec lahko zavede uporabnika, da napačno odobri zahtevek za elektronska potrdila o atributih (z ribarjenjem ali drugače).	Razkritje podatkov (R6)

ID *Identifikator*	Opis grožnje *Opis ugotovljene grožnje (*)*	Tveganje *Povezana tveganja*
TR29	Napadalec lahko razkrije atribute iz denarnice in identificira uporabnika denarnice, kjer identifikacija ni potrebna/ dovoljena.	Razkritje podatkov (R6)
TR30	Napadalec lahko premaga tehnični in postopkovni nadzor, da bi pridobil podatke.	Razkritje podatkov (R6)
TR31	Zahteva se lahko razkrije napadalcu.	Razkritje podatkov (R6)
TR32	Napadalec lahko pridobi informacije o vgrajeni politiki razkrivanja za atribute in predstavi atribute, ki so vključeni v trenutno zahtevo enot denarnic.	Razkritje podatkov (R6)
TR33	Napadalec lahko pridobi evidence ali njihove dele.	Razkritje podatkov (R6)
TR34	Napadalec lahko izve, ali je denarnica nameščena na isti napravi, kot jo sam uporablja, ali na drugi napravi ter pridobi informacije o njej.	Razkritje podatkov (R6)
TR35	Napadalec lahko pridobi faktor znanja, ki se uporablja za avtentikacijo uporabnika v varni kriptografski aplikaciji denarnice.	Razkritje podatkov (R6)
TR36	Elektronsko potrdilo o atributih o osebi, ki je predstavljena v več transakcijah z zanašajočo se stranko ali med različnimi zanašajočimi se strankami, nenamerno omogoča povezavo več transakcij z zadevno osebo.	Razkritje podatkov (R6)
TR37	Javni seznam preklicanih potrdil/zanašajočih se strank lahko vsebuje informacije o uporabnikovi uporabi potrdila (npr. lokacija, naslov IP itd.).	Razkritje podatkov (R6)
TR38	Ker ne morejo dokazati privolitve uporabnika za skupne atribute, lahko zanašajoče se stranke vplivajo na celovitost evidenc.	Razkritje podatkov (R6)
TR39	Napadalec lahko nezakonito sledi uporabnikom denarnice z uporabo edinstvenih/sledljivih identifikatorjev.	Razkritje podatkov (R6) / nadzor (R14)
TR40	Zanašajoča se stranka, ki jo sestavlja več enot/subjektov, od katerih ima vsak različen obseg tega, kar lahko zahteva/ obdeluje, lahko zahteva in obdeluje podatke, za katere nima zakonite podlage.	Razkritje podatkov (R6) / nedovoljena transakcija (R9)
TR41	Napadalec lahko zagotovi, da je preverjanje celovitosti in pristnosti identifikacijskih podatkov osebe, ki ga izvaja denarnica, vedno uspešno.	Manipulacija s podatki (R7)
TR42	Napadalec lahko zaobide preverjanja celovitosti in pristnosti zahtevanih atributov, ki jih izvaja denarnica, ali zagotovi, da so vedno uspešna.	Manipulacija s podatki (R7)
TR43	Napadalec lahko zaobide preverjanja vseh zahtevanih atributov istega uporabnika, ki jih izvaja denarnica, ali zagotovi, da so vedno uspešna.	Manipulacija s podatki (R7)
TR44	Napadalec lahko zaobide preverjanja, ki jih izvaja denarnica, o tem, ali so identifikacijski podatki osebe veljavni in jih je izdal zanesljiv ponudnik, ali zagotovi, da so vedno uspešna.	Manipulacija s podatki (R7)

ID *Identifikator*	Opis grožnje *Opis ugotovljene grožnje (*)*	Tveganje *Povezana tveganja*
TR45	Napadalec lahko zaobide preverjanja, ki jih izvaja denarnica, o tem, ali je kvalificirano elektronsko potrdilo o atributih veljavno in ga je izdal kvalificiran ponudnik storitev zaupanja, ali zagotovi, da so vedno uspešna.	Manipulacija s podatki (R7)
TR46	Napadalec lahko zaobide preverjanja, ki jih izvaja denarnica, o tem, ali je ponudnik identifikacijskih podatkov osebe preklical te podatke, ali zagotovi, da so vedno uspešna.	Manipulacija s podatki (R7)
TR47	Napadalec lahko zaobide preverjanja, ki jih izvaja denarnica, o tem, ali je ponudnik (kvalificiranega) elektronskega potrdila o atributih preklical to potrdilo, ali zagotovi, da so vedno uspešna.	Manipulacija s podatki (R7)
TR48	Napadalec lahko spremeni vsebino varnostnih kopij podatkov in podatkov za obnovo, ki bi morali biti izključno pod nadzorom uporabnika.	Manipulacija s podatki (R7) / izguba podatkov (R8)
TR49	Napadalec lahko spremeni zgodovino transakcij za določeno instanco denarnice iz evidenc dejavnosti.	Manipulacija s podatki (R7) / izguba podatkov (R8)
TR50	Napadalec lahko prisluškuje povezavi denarnice z zanašajočimi se strankami.	Kraja podatkov (R5) / razkritje podatkov (R6)
TR51	Napadalec lahko uporabnika prepriča, da z napadalcem ali tretjo osebo deli osebne podatke (tj. identifikacijske podatke osebe, elektronska potrdila o atributih, psevdonime, elektronske podpise, evidence in druge podatke), ki jih ni nameraval deliti.	Kraja podatkov (R5) / razkritje podatkov (R6)
TR52	Napadalec lahko prebere zgodovino transakcij za določeno instanco denarnice iz evidenc dejavnosti.	Kraja podatkov (R5) / razkritje podatkov (R6)
TR53	Napadalec lahko izvozi ali izlušči kriptografski ključ iz varne kriptografske naprave denarnice.	Kraja podatkov (R5) / razkritje podatkov (R6) / nedovoljena transakcija (R9)
TR54	Napadalec lahko prebere vsebino varnostnih kopij podatkov in podatkov za obnovo, ki bi morali biti izključno pod nadzorom uporabnika.	Kraja podatkov (R5) / razkritje podatkov (R6)
TR55	Napadalec lahko zaobide metodo avtentikacije uporabnika, da bi uporabil psevdonim, ki ga ustvari enota denarnice.	Kraja identitete (R4)
TR56	Napadalec lahko uporabnikom predlaga aplikacijo, ki posnema določeno zakonito denarnico.	Kraja identitete (R4)
TR57	Napadalec lahko izvozi podatke denarnice, vključno z identifikacijskimi podatki osebe, kvalificiranimi elektronskimi potrdili o atributih ali evidencami.	Kraja identitete (R4)
TR58	Napadalec lahko izvozi elemente kriptografske vezave.	Kraja identitete (R4)
TR59	Napadalec lahko prevzame identitete prek kriptografskih ključev denarnice.	Kraja identitete (R4)
TR60	Napadalec lahko na svoji osebni napravi ustvari dvojnik osebne denarnice drugega uporabnika in ga uporabi.	Kraja identitete (R4) / ustvarjanje ali uporaba obstoječe elektronske identitete (R1)

ID *Identifikator*	Opis grožnje *Opis ugotovljene grožnje (*)*	Tveganje *Povezana tveganja*
TR61	Organi druge države lahko od uporabnika zahtevajo, da prikaže in/ali deli vse podatke denarnice, kadar se nahaja v bližini, na primer pri prečkanju meje te države.	Kraja identitete (R4) / nadzor (R14)
TR62	Uporabniki po okvari uporabniške naprave ne morejo prenesti svojih evidenc transakcij, kar povzroči izgubo sledljivosti prejšnjih transakcij v novi denarnici.	Zatajitev (R11)
TR63	Uporabniki po okvari uporabniške naprave ne morejo obnoviti svojih evidenc transakcij, kar povzroči izgubo sledljivosti v novi denarnici.	Zatajitev (R11)
TR64	Zanašajoče se stranke imajo lahko težave pri dokazovanju privolitve za elektronske podpise na daljavo.	Zatajitev (R11)
TR65	Napadalec lahko med povezavo z zanašajočimi se strankami to povezavo preobremeni z zahtevami.	Motnja storitve (R13)
TR66	Napadalec lahko preobremeni storitev zagotavljanja statusa s povezavami z zanašajočimi se strankami.	Motnja storitve (R13)
TR67	Napadalec lahko predstavitev atributa prikaže kot sporno/zavrnjeno, čeprav ima navedeno veljavnost.	Motnja storitve (R13)
TR68	Napadalec lahko brez utemeljenega razloga prekliče identifikacijske podatke osebe.	Motnja storitve (R13)
TR69	Napadalec lahko brez privolitve uporabnika prekliče identifikacijske podatke osebe.	Motnja storitve (R13)
TR70	Napadalec lahko brez utemeljenega razloga prekliče (kvalificirano) elektronsko potrdilo o atributu.	Motnja storitve (R13)
TR71	Napadalec lahko brez privolitve uporabnika prekliče (kvalificirano) elektronsko potrdilo o atributu.	Motnja storitve (R13)
TR72	Napadalec lahko sproži več zahtev za identifikacijo, ne da bi bile prepoznane kot namerno opuščene zahteve.	Motnja storitve (R13)
TR73	Napadalec lahko pošlje več zahtevkov brez nadaljnjih transakcij.	Motnja storitve (R13)
TR74	Napadalec lahko zanašajoči se stranki omogoči, da zahteva identifikacijo brez ustrezne identifikacije (odgovora) in popolnega nadzora.	Motnja storitve (R13)
TR75	Napadalec lahko pošlje odgovor na zahtevo, ki je potekla, ali podobno stanje, ki povzroči motnjo storitve.	Motnja storitve (R13)
TR76	Zanašajoča se stranka lahko pošlje več neveljavnih zahtevkov.	Motnja storitve (R13)
TR77	Napadalec lahko ponudniku denarnice pošlje več neveljavnih zahtev.	Motnja storitve (R13)
TR78	Napadalec lahko povzroči, da država članica ne more preklicati nezanesljivega ponudnika identifikacijskih podatkov osebe z zanesljivega seznama zanesljivih ponudnikov identifikacijskih podatkov osebe.	Motnja storitve (R13)
TR79	Napadalec lahko prepreči začasno razveljavitev ali preklic denarnice.	Motnja storitve (R13)

ID *Identifikator*	Opis grožnje *Opis ugotovljene grožnje (*)*	Tveganje *Povezana tveganja*
TR80	Napadalec lahko blokira transakcije zanašajočih se strank, uporabnikov in/ali ponudnika identifikacijskih podatkov osebe.	Motnja storitve (R13)
TR81	Napadalec lahko onemogoči varno kriptografsko napravo denarnice ali dostop do nje.	Motnja storitve (R13)
TR82	Napadalec lahko povzroči, da ponudnik identifikacijskih podatkov osebe ne more preklicati ali začasno razveljaviti identifikacijskih podatkov osebe.	Motnja storitve (R13) / nedovoljena transakcija (R9)
TR83	Zanašajoča se stranka lahko izpelje podatke o identiteti uporabnika, ki so obširnejši od podatkov, deljenih z njo.	Nadzor (R14)
TR84	Skupina zanašajočih se strank ali ponudnikov identifikacijskih podatkov osebe, ki se tajno dogovarja, lahko izpelje podatke o identiteti uporabnika, ki so obširnejši od podatkov, ki so ji znani.	Nadzor (R14)
TR85	Napadalec lahko izsledi uporabnika in mu sledi z uporabo njegovih identifikacijskih podatkov osebe, kadar identifikacija uporabnika ni potrebna.	Nadzor (R14)
TR86	Napadalec lahko združi „ponarejeno“ predstavitev kombinacij (kvalificiranih) elektronskih potrdil o atributih.	Manipulacija s transakcijami (R10)
TR87	Napadalec lahko denarnico aktivira/prevzame na daljavo (npr. bančna aplikacija z vgrajeno zahtevo za avtentikacijo ali potrdilo) brez izrecne privolitve ali izključnega nadzora uporabnika v primerih, ko se uporabnik ne zaveda zanašajoče se stranke (npr. spi) ali je ne vidi.	Manipulacija s transakcijami (R10)
TR88	Napadalci lahko spremenijo metapodatke zahteve (ime storitve, uporabe itd.).	Manipulacija s transakcijami (R10)
TR89	Napadalci lahko spremenijo informacije odziva (stanje storitve, enkratno kriptografsko število itd.).	Manipulacija s transakcijami (R10)
TR90	Napadalci lahko spremenijo informacije o atributih zahteve (zahtevajo več, kot je nujno itd.).	Manipulacija s transakcijami (R10)
TR91	Zanašajoča se stranka lahko ponovi elemente iz prejšnje seje v drugi seji.	Manipulacija s transakcijami (R10)
TR92	Napadalec lahko nadomesti ali spremeni identifikacijske podatke osebe med njihovim prenosom od ponudnika identifikacijskih podatkov osebe do enote denarnice.	Manipulacija s transakcijami (R10)
TR93	Napadalec lahko nadomesti ali spremeni identifikacijske podatke osebe med njihovim prenosom od enote denarnice do spletne zanašajoče se stranke.	Manipulacija s transakcijami (R10)
TR94	Napadalec lahko nadomesti ali spremeni identifikacijske podatke osebe med njihovim prenosom od enote denarnice do nespletne zanašajoče se stranke.	Manipulacija s transakcijami (R10)
TR95	Napadalec lahko brez privolitve uporabnika izda identifikacijske podatke osebe.	Nedovoljena transakcija (R9)
TR96	Napadalec lahko uporablja preklicane ali neveljavne vgrajene politike razkrivanja, morda brez vednosti zanašajočih se strank.	Nedovoljena transakcija (R9)
TR97	Napadalec lahko pretenta denarnico, da potrdi napačne elektronske podpise.	Nedovoljena transakcija (R9)
TR98	Napadalec lahko uporablja denarnico zunaj uporabnikovega nadzora.	Nedovoljena transakcija (R9)

ID *Identifikator*	Opis grožnje *Opis ugotovljene grožnje* (*)	Tveganje *Povezana tveganja*
TR99	Napadalec lahko uporabnika prepriča, da avtenticira in odobri transakcije z napadalcem ali nepooblaščeno tretjo osebo.	Nedovoljena transakcija (R9)
TR100	Napadalec lahko zavede uporabnika v elektronski podpis, ne da bi mu predstavil vsebino ali po predstavitvi napačne vsebine.	Nedovoljena transakcija (R9)
TR101	Napadalec lahko zaobide nadzor dostopa do uporabniškega računa pri ponudniku denarnice.	Nedovoljena transakcija (R9)
TR102	Napadalec se lahko izdaja za zanašajoče se stranke med povezavo z zanašajočimi se strankami.	Nedovoljena transakcija (R9) / razkritje podatkov (R6)
TR103	Uporabnik povezave med zanašajočo se stranko in brskalnikom se lahko razlikuje od uporabnika povezave med zanašajočo se stranko in denarnico.	Nedovoljena transakcija (R9) / razkritje podatkov (R6) / kraja identitete (R4)
TR104	Napadalec lahko uporabnika prepriča, da brez razloga prekliče svojo denarnico.	Nedovoljena transakcija (R9) / motnja storitve (R13)
TR105	Napadalec lahko izvaja napade moža v sredini.	Nedovoljena transakcija (R9) / razkritje podatkov (R6) / nadzor (R14)
TR106	Napadalec lahko predloži neveljavne ali preklicane atribute iz denarnice, ki se ne povezuje redno z omrežjem.	Učinek na različna tveganja
TR107	Napadalec lahko ukrade informacije od uporabnika s slepljenjem denarnice.	Učinek na različna tveganja
TR108	Napadalec se lahko izdaja za uporabnika s ponavljanjem/posnemanjem zahteve za podatke (npr. avtentikacije), ki se zdi veljavna.	Učinek na različna tveganja
TR109	Napadalec lahko ponavlja vgrajeno politiko razkrivanja informacij uporabniku, da posnema odobreno zahtevo.	Učinek na različna tveganja
TR110	Napadalec lahko izkoristi pomanjkanje informacij uporabnikov denarnic ali nepotrebne zamude po kršitvi ali ogrožanju varnosti.	Učinek na različna tveganja
TR111	Napadalec lahko spremeni predhodno nameščeno zakonito instanco denarnice, da doda zlonamerne funkcije.	Učinek na različna tveganja
TR112	Napadalec lahko spremeni zakonito instanco denarnice in jo predlaga uporabnikom kot zakonito.	Učinek na različna tveganja
TR113	Napadalec lahko premaga mehanizem avtentikacije uporabnika, da bi se izognil avtentikaciji uporabnika denarnice.	Učinek na različna tveganja
TR114	Napadalec lahko med namestitvijo na uporabniško napravo v kodo denarnice vnese zlonamerno kodo ali stranska vrata.	Učinek na različna tveganja
TR115	Napadalec lahko med razvojem kode denarnice vanjo vnese zlonamerno kodo ali stranska vrata.	Učinek na različna tveganja
TR116	Napadalec lahko nedovoljeno posega v generiranje naključnih števil, da bi dovolj zmanjšal svojo entropijo in tako omogočil napade.	Učinek na različna tveganja

ID *Identifikator*	Opis grožnje *Opis ugotovljene grožnje (*)*	Tveganje *Povezana tveganja*
TR117	Napadalec lahko nedovoljeno posega v uporabniške naprave v oskrbovalni verigi, da vključi kodo ali konfiguracije, ki ne izpolnjujejo pogojev za uporabo denarnice.	Učinek na različna tveganja
TR118	Napadalec lahko aktivira enoto denarnice ob uporabi zaslepljene varne kriptografske naprave denarnice, ki je pod njegovim nadzorom.	Učinek na različna tveganja
TR119	Napadalec lahko prebere informacije, poslane varni kriptografski aplikaciji in/ali napravi denarnice.	Učinek na različna tveganja
TR120	Napadalec lahko varni kriptografski aplikaciji denarnice pošlje poljubne informacije.	Učinek na različna tveganja
TR121	Napadalec lahko ukrade informacije s prestrezanjem izmenjav med varno kriptografsko aplikacijo denarnice in varno kriptografsko napravo denarnice.	Učinek na različna tveganja
TR122	Napadalec lahko varni kriptografski napravi denarnice pošlje poljubne informacije.	Učinek na različna tveganja
TR123	Napadalec lahko pošlje informacije varni kriptografski napravi denarnice in pri tem zaobide varno kriptografsko aplikacijo denarnice.	Učinek na različna tveganja
TR124	Napadalec lahko z ribarjenjem zavede uporabnike v uporabo lažne denarnice in spletne aplikacije za upravljanje identifikacijskih podatkov osebe.	Učinek na različna tveganja
TR125	Napadalec lahko zamenja ključe denarnice z drugimi ključi, da bi ustvaril sporočila za uporabo v drugem napadu.	Učinek na različna tveganja
TR126	Napadalec lahko spremeni ali uniči ključe denarnice, zaradi česar so nekatere funkcije denarnice neuporabne.	Učinek na različna tveganja
TR127	Napadalec lahko uporabi zlonamerno programsko opremo za dostop do podatkov, shranjenih v denarnici.	Učinek na različna tveganja
TR128	Napadalec lahko dostopa do dokazov, ustvarjenih v denarnici.	Učinek na različna tveganja
TR129	Ponudniki denarnic lahko dostopajo do predmetov v denarnici.	Učinek na različna tveganja
TR130	Ponudniki denarnice lahko dostopajo do dokazov, ustvarjenih v denarnici.	Učinek na različna tveganja
TR131	Napadalec lahko ukrade odklenjeno denarnico.	Učinek na različna tveganja
TR132	Napadalec lahko manipulira s sistemom, da prepreči evidentiranje nekaterih dogodkov.	Učinek na različna tveganja
TR133	Napadalec lahko prestreza komunikacijo med instanco denarnice in varno kriptografsko aplikacijo denarnice ali ponavlja/posnema uporabnika (npr. z ugrabitvijo mehanizma avtentikacije).	Učinek na različna tveganja

PRILOGA II

MERILA ZA OCENJEVANJE SPREJEMLJIVOSTI INFORMACIJ O ZANESLJIVOSTI

Ime	Predmet	Točke, ki zahtevajo pozornost
EUCC	Proizvodi s področja IKT	O izdajatelju: brez (akreditirani certifikacijski organi). O področju uporabe: — preveriti profil zaščite in varnostni cilj; — preveriti raven zanesljivosti ocenjevanja in razširitev. O zanesljivosti: — preveriti omejitve v uporabniški dokumentaciji; — za sestavo je lahko potreben dostop do tehničnega poročila o oceni.
EUCS (če je na voljo)	Storitve v oblaku	O izdajatelju: brez (akreditirani certifikacijski organi). O področju uporabe: — preveriti opis storitve v oblaku; — preveriti raven ocenjevanja in profile razširitve. O zanesljivosti: — preveriti informacije o preglednosti in po potrebi informacije o sestavi.
Sheme, ki temeljijo na skupnih merilih in se uporabljajo v EU, vključno s shemami SOG-IS	Proizvodi s področja IKT	O izdajatelju: brez (države članice). O področju uporabe: — preveriti profil zaščite in varnostni cilj; — preveriti raven zanesljivosti ocenjevanja in razširitev. O zanesljivosti: — preveriti omejitve v uporabniški dokumentaciji; — za sestavo je lahko potreben dostop do tehničnega poročila o oceni.
EN 17640:2018 (FITCEM, vključno s CSPN, BSZ, LINCE in BSZA)	Proizvodi s področja IKT	O izdajatelju: — preveriti shemo in zahteve za certifikacijske organe. O področju uporabe: — preveriti opis proizvoda; — preveriti varnostne zahtevke; — preveriti raven zanesljivosti. O zanesljivosti: — preveriti izvedene dejavnosti in ugotovitve iz poročila.
Certifikacijske sheme naprav za ustvarjanje kvalificiranega podpisa v skladu s členom 30 Uredbe (EU) št. 910/2014	Naprave za ustvarjanje kvalificiranega podpisa	O izdajatelju: — preveriti shemo in zahteve za certifikacijske organe. O področju uporabe: — preveriti opis proizvoda; — preveriti varnostne zahtevke; — preveriti raven zanesljivosti. O zanesljivosti: — preveriti izvedene dejavnosti.

Ime	Predmet	Točke, ki zahtevajo pozornost
EN ISO/IEC 27001:2022	Sistem za upravljanje informacijske varnosti	O izdajatelju: brez (akreditirani certifikacijski organi). O področju uporabe: — preveriti opis sistema upravljanja; — preveriti izjavo o primernosti. O zanesljivosti: — preveriti izvedene dejavnosti.
SOC2	Organizacije	O izdajatelju: — preveriti status javnega računovodstva. O področju uporabe: — preveriti izjavo o upravljanju in opis nadzora; — preveriti izjavo o primernosti. O zanesljivosti: — preveriti ugotovitve iz poročila; — po potrebi preveriti medrevizijske izjave.
MDSCert (GSMA) (če je na voljo)	Mobilne naprave	O izdajatelju: — preveriti zahteve za certifikacijske organe. O področju uporabe: — preveriti raven varnosti; — preveriti zahteve sheme. O zanesljivosti: — preveriti dejavnosti in ugotovitve iz poročila.
Druge sheme	Katera koli komponenta	O shemi: — preveriti ustreznost in določbe sheme. O izdajatelju: — preveriti zahteve za certifikacijske organe. O področju uporabe: — preveriti zahteve sheme; — preveriti varnostni cilj ali podoben dokument, v katerem so opisane varnostne funkcionalne zahteve in zahteve za zagotavljanje varnosti; — preveriti opis proizvoda in izbrane varnostne funkcionalne zahteve. O zanesljivosti: — preveriti dejavnosti in ugotovitve iz poročila.

PRILOGA III

FUNKCIONALNE ZAHTEVE ZA REŠITVE DENARNIC

V skladu s členom 5a(4), (5), (8) in (14) Uredbe (EU) št. 910/2014 funkcionalna merila, ki jih morata izpolnjevati certificirana rešitev denarnice in shema elektronske identifikacije, v okviru katere se ta rešitev zagotavlja, vključujejo funkcionalne zahteve za operacije iz:

(1) Izvedbene uredbe Komisije (EU) 2024/2979 ([1]) o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede celovitosti in temeljnih funkcionalnosti;

(2) Izvedbene uredbe Komisije (EU) 2024/2982 ([2]) o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede protokolov in vmesnikov, ki jih mora podpirati okvir za evropsko digitalno identiteto;

(3) Izvedbene uredbe Komisije (EU) 2024/2977 ([3]) o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede identifikacijskih podatkov osebe in elektronskih potrdil o atributih, izdanih evropskim denarnicam za digitalno identiteto.

([1]) Izvedbena uredba Komisije (EU) 2024/2979 z dne 28. novembra 2024 o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede celovitosti in temeljnih funkcionalnosti (UL L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([2]) Izvedbena uredba Komisije (EU) 2024/2982 z dne 28. novembra 2024 o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede protokolov in vmesnikov, ki jih mora podpirati okvir za evropsko digitalno identiteto (UL L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([3]) Izvedbena uredba Komisije (EU) 2024/2977 z dne 28. novembra 2024 o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede identifikacijskih podatkov osebe in elektronskih potrdil o atributih, izdanih evropskim denarnicam za digitalno identiteto (UL L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

PRILOGA IV

METODE IN POSTOPKI ZA DEJAVNOSTI OCENJEVANJA

1. **Revizija izvajanja rešitve denarnice**

Dejavnost ugotavljanja skladnosti vključuje izbiro specifičnih dejavnosti ocenjevanja.

Nacionalne certifikacijske sheme določijo dejavnost ocenjevanja za oceno predloženih informacij, ki zajema vsaj naslednje:

(a) analizo predloženih informacij, s katero se potrdi, da so primerne za eno od arhitektur, določenih v nacionalnih certifikacijskih shemah;

(b) analizo zajemanja tveganj in groženj za kibernetsko varnost, opredeljenih v registru tveganj iz Priloge I, z opisanim varnostnim nadzorom.

Analizi iz točk (a) do (b) morata temeljiti na razlogih in utemeljitvah ponudnika denarnice.

2. **Dejavnosti ocenjevanja, povezane z varno kriptografsko napravo denarnice**

(1) Kritičnih operacij, vključno s kriptografskimi izračuni, ni treba v celoti izvajati v varnih kriptografskih napravah denarnic. Vendar mora del, ki se izvaja v njih, kadar deluje kot del rešitve denarnice, zagotavljati zaščito izvajanih kritičnih operacij pred napadi napadalcev z visokim potencialom za napad v skladu z Izvedbeno uredbo Komisije (EU) 2015/1502 ([1]).

(2) Varna kriptografska naprava denarnice ali njen del je lahko predmet certificiranja, če jo oz. ga zagotovi imetnik certifikata ali prosilec zahteve, ni pa predmet certificiranja, če je vgrajena oz. vgrajen v napravo, ki jo zagotovi končni uporabnik. Poleg tega se v nacionalnih certifikacijskih shemah določijo dejavnosti ocenjevanja za preverjanje ustreznosti varne kriptografske naprave denarnice v naslednjih dveh primerih:

(a) če je varna kriptografska aplikacija denarnice odvisna od določene varne kriptografske naprave denarnice (tj. če je aplikacijo treba oceniti kot sestavljeni proizvod na podlagi varne kriptografske naprave denarnice), je za oceno te aplikacije potreben dostop do dodatnih informacij, povezanih s certificiranjem varne kriptografske naprave denarnice, vključno zlasti s tehničnim poročilom o oceni;

(b) če arhitektura, zajeta v shemi, uporablja več varnih kriptografskih naprav denarnice ali če se nekatere operacije v zvezi s kritičnimi sredstvi izvajajo zunaj varne kriptografske naprave denarnice, nacionalne certifikacijske sheme vključujejo dejavnosti ocenjevanja za zagotovitev, da splošna rešitev zagotavlja pričakovano raven varnosti.

(3) Kot predpogoj za certificiranje v okviru nacionalnih certifikacijskih shem se varna kriptografska naprava denarnice oceni glede na zahteve glede visoke ravni zanesljivosti, kot so določene v Izvedbeni uredbi (EU) 2015/1502.

(a) Ko so izpolnjeni pogoji iz člena 3(3), točka (b), ocena varne kriptografske naprave denarnice ali njenega dela vključuje oceno ranljivosti iz standarda EN ISO/IEC 15408-3:2022 na ravni AVA_VAN.5, kot je določeno v Prilogi I k Izvedbeni uredbi Komisije (EU) 2024/482 ([2]), razen če je certifikacijskemu organu ustrezno utemeljeno, da varnostne značilnosti varne kriptografske aplikacije denarnice omogočajo uporabo nižje ravni ocenjevanja, hkrati pa ohranjajo visoko splošno raven zanesljivosti, kot je določena v Izvedbeni uredbi (EU) 2015/1502.

([1]) Izvedbena uredba Komisije (EU) 2015/1502 z dne 8. septembra 2015 o določitvi minimalnih tehničnih specifikacij in postopkov za ravni zanesljivosti za sredstva elektronske identifikacije v skladu s členom 8(3) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu (UL L 235, 9.9.2015, str. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([2]) Izvedbena uredba Komisije (EU) 2024/482 z dne 31. januarja 2024 o določitvi pravil za uporabo Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta v zvezi s sprejetjem evropske certifikacijske sheme za kibernetsko varnost, ki temelji na skupnih merilih (UL L, 2024/482, 7.2.2024, ELI http://data.europa.eu/eli/reg_impl/2024/482/oj).

(4) Poleg tega nacionalne certifikacijske sheme v dokumentaciji, povezani z vsako posebno arhitekturo, oblikujejo predpostavke za to oceno varne kriptografske naprave denarnice, na podlagi katerih se lahko zagotovi odpornost proti napadalcem z velikim potencialom za napad v skladu z Izvedbeno uredbo (EU) 2015/1502, ter opredelijo dejavnosti ocenjevanja za potrditev teh predpostavk in potrditev po izdaji certifikata, da so predpostavke še vedno preverjene. V nacionalnih shemah se od kandidatov za certifikacijo tudi zahteva, da precizirajo te predpostavke glede na njihovo specifično izvajanje in opišejo ukrepe, ki zagotavljajo, da se predpostavke preverjajo v celotnem življenjskem ciklu certificiranja.

(5) V vseh primerih nacionalne certifikacijske sheme vključujejo dejavnost ocenjevanja, da se preveri, ali so informacije o zanesljivosti, ki so na voljo za varne kriptografske naprave denarnice, primerne za rešitev denarnice, in sicer z analizo informacij o zanesljivosti, kot je varnostni cilj za certifikate EUCC, vključno z naslednjimi dejavnostmi:

(a) preverjanje, ali je obseg ocenjevanja primeren, kar na primer za certifikate EUCC pomeni preverjanje, ali varnostni cilj potrjuje skladnost z enim od profilov zaščite, priporočenih v EUCC;

(b) preverjanje, ali so predpostavke o operativnem okolju združljive z rešitvijo denarnice, kar na primer za certifikate EUCC pomeni, da je te predpostavke mogoče najti v varnostnem cilju;

(c) preverjanje, ali so priporočila iz navodil ali dokumentacije za uporabnike združljiva s pogoji, pod katerimi se varna kriptografska naprava denarnice uporablja v rešitvi denarnice;

(d) preverjanje, ali so predpostavke iz nacionalne certifikacijske sheme v zvezi z varnimi kriptografskimi napravami denarnice preverjene in zajete v informacijah o zanesljivosti.

(6) Kadar rezultati nekaterih preverjanj niso dokončni, nacionalne certifikacijske sheme od certifikacijskih organov zahtevajo, da določijo kompenzacijske zahteve za varno kriptografsko aplikacijo denarnice (WSCA) na podlagi varne kriptografske naprave denarnice, ki se morajo vključiti v oceno te aplikacije. Če to ni mogoče, se v nacionalnih certifikacijskih shemah šteje, da je varna kriptografska naprava denarnice neprimerna, kar pomeni, da se rešitvi denarnice ne izda potrdilo o skladnosti.

3. **Dejavnosti ocenjevanja, povezane z varno kriptografsko aplikacijo denarnice**

(1) Nacionalne certifikacijske sheme zahtevajo, da se varna kriptografska aplikacija denarnice kot del rešitve denarnice oceni v skladu z zahtevami najmanj visoke ravni zanesljivosti, kot je določeno v Izvedbeni uredbi (EU) 2015/1502.

(2) To ocenjevanje vključuje oceno ranljivosti iz standarda EN ISO/IEC 15408-3:2022 na ravni AVA_VAN.5, kot je določeno v Prilogi I k Izvedbeni uredbi (EU) 2024/482, razen če je certifikacijskemu organu ustrezno utemeljeno, da varnostne značilnosti varne kriptografske aplikacije denarnice omogočajo uporabo nižje ravni ocenjevanja, hkrati pa ohranjajo visoko splošno raven zanesljivosti, kot je določena v Izvedbeni uredbi (EU) 2015/1502.

(3) Kadar ponudnik denarnice ne zagotavlja varne kriptografske aplikacije denarnice, nacionalne certifikacijske sheme oblikujejo predpostavke za to oceno varne kriptografske aplikacije denarnice, na podlagi katerih se lahko zagotovi odpornost proti napadalcem z velikim potencialom za napad v skladu z Izvedbeno uredbo (EU) 2015/1502, ter opredelijo dejavnosti ocenjevanja za potrditev teh predpostavk in potrditev po izdaji certifikata, da so predpostavke še vedno preverjene. V nacionalnih shemah se od kandidatov za certifikacijo tudi zahteva, da precizirajo te predpostavke glede na njihovo specifično izvajanje in opišejo ukrepe, ki zagotavljajo, da se predpostavke preverjajo v celotnem življenjskem ciklu certificiranja.

(4) V vseh primerih nacionalne certifikacijske sheme vključujejo dejavnost ocenjevanja, da se preveri, ali so informacije o zanesljivosti, ki so na voljo za varne kriptografske aplikacije denarnice, primerne za rešitev denarnice, in sicer z analizo informacij o zanesljivosti, kot je varnostni cilj za certifikate EUCC, vključno z naslednjimi dejavnostmi:

(a) preverjanje, ali je obseg ocenjevanja primeren, kar na primer za certifikate EUCC pomeni preverjanje, ali varnostni cilj potrjuje skladnost z enim od profilov zaščite, priporočenih v EUCC;

(b) preverjanje, ali so predpostavke o operativnem okolju združljive z rešitvijo denarnice, kar na primer za certifikate EUCC pomeni, da je te predpostavke mogoče najti v varnostnem cilju;

(c) preverjanje, ali so priporočila iz navodil ali dokumentacije za uporabnike združljiva s pogoji, pod katerimi se varna kriptografska aplikacija denarnice uporablja v rešitvi denarnice;

(d) preverjanje, ali so predpostavke iz nacionalne certifikacijske sheme v zvezi z varnimi kriptografskimi aplikacijami denarnice preverjene in zajete v informacijah o zanesljivosti.

(5) Nacionalne certifikacijske sheme zahtevajo, da ocena varne kriptografske aplikacije denarnice zajema vse varnostne nadzore, ki jih izvaja ta aplikacija.

4. **Dejavnosti ocenjevanja, povezane z napravo končnega uporabnika**

Ker so v registru tveganj iz Priloge I k tej uredbi opredeljena tveganja, ki so neposredno povezana z varnostjo naprave končnega uporabnika, se v nacionalnih certifikacijskih shemah določijo varnostne zahteve za naprave končnih uporabnikov. Ker pa te naprave zagotovi končni uporabnik in ne ponudnik denarnice, te zahteve temeljijo na predpostavkah.

Za vsako predpostavko rešitev denarnice vključuje mehanizem, s katerim se za vsako enoto denarnice preveri, ali osnovna naprava končnega uporabnika izpolnjuje predpostavko. Taki mehanizmi se štejejo za varnostni nadzor in so zajeti v dejavnostih ocenjevanja, da se dokažeta njihova primernost in učinkovitost na ustrezni ravni zanesljivosti.

Dva primera sta navedena v nadaljevanju:

(a) naprava končnega uporabnika lahko vključuje certificirano varno kriptografsko napravo denarnice, kar je treba dokazati. Običajno se s kriptografskim mehanizmom preveri, ali je v certificirani varni kriptografski napravi denarnice prisotna kriptografska skrivnost, ki je na voljo samo v taki napravi. V tem primeru bi bilo treba to kriptografsko skrivnost obravnavati kot kritično sredstvo in vključiti v certificiranje varne kriptografske naprave in/ali aplikacije denarnice;

(b) tipična zahteva za naprave končnih uporabnikov bi bila, da morajo biti deležne varnostnih posodobitev. Ker je ta zahteva povezana z instanco denarnice, mora biti mehanizem za preverjanje razpoložljivosti varnostnih posodobitev zajet le v dejavnostih ocenjevanja na ravni zanesljivosti, primerni za instanco denarnice, zlasti ker bo verjetno vgrajen v instanco denarnice.

5. **Dejavnosti ocenjevanja, povezane z instanco denarnice**

(1) Pri ocenjevanju instance denarnice se upoštevata naslednja glavna izziva:

(a) instanca denarnice verjetno obstaja v nizu različic iste osnovne aplikacije, pri čemer je vsaka različica specializirana za določeno kategorijo naprav končnih uporabnikov;

(b) različne različice instance denarnice bodo verjetno potrebovale pogoste posodobitve, da bi lahko sledile razvoju osnovne varnostne platforme, na primer kadar se ugotovijo ranljivosti, ki zahtevajo spremembe aplikacij.

(2) Pri ocenjevanju instance denarnice se upoštevajo ti specifični izzivi. Ena od neposrednih posledic je, da okvir skupnih meril morda ne bo primeren v vseh primerih. Zato se po potrebi preučijo alternativne metodologije ocenjevanja. Nacionalne certifikacijske sheme preučijo možnost uporabe metodologije iz standarda EN 17640:2018:

(a) kot del sheme same;

(b) v okviru nacionalnih shem, ki temeljijo na metodologiji;

(c) v okviru nacionalnih shem, ki temeljijo na podobnih načelih, vendar so bile vzpostavljene pred razvojem metodologije iz standarda EN 17640:2018.

(3) Ker je lahko dodana vrednost izvedbe popolne namenske ocene vsake različice omejena, nacionalne certifikacijske sheme prav tako preučijo možnost določitve meril, ki omogočajo vzorčenje, da bi se izognili ponavljanju enakih dejavnosti ocenjevanja in se osredotočili na dejavnosti, ki so specifične za določeno različico. Nacionalne certifikacijske sheme od vseh certifikacijskih organov zahtevajo, da utemeljijo uporabo vzorčenja.

(4) Nacionalne certifikacijske sheme vključijo posodobitve instance denarnice v splošni postopek upravljanja sprememb, določen za rešitev denarnice. Določajo tudi pravila o postopkih, ki jih ponudnik denarnice izvaja za vsako posodobitev (npr. analiza učinka sprememb na varnostni nadzor), in o dejavnostih ocenjevanja, ki jih certifikacijski organ izvaja v zvezi s posodobitvami pod določenimi pogoji (npr. ocenjevanje operativne učinkovitosti spremenjenega varnostnega nadzora). Postopek upravljanja sprememb je eden od postopkov, katerih operativno učinkovitost je treba preveriti vsako leto v skladu s členom 18(3).

6. **Dejavnosti ocenjevanja, povezane s storitvami in postopki, ki se uporabljajo za zagotavljanje in delovanje rešitve denarnice**

(1) Za ocenjevanje storitev in postopkov, ki imajo vlogo pri zagotavljanju in delovanju rešitve denarnice in sheme elektronske identifikacije, v okviru katere se ta rešitev zagotavlja, ocenjevalna skupina zbere dokaze z izvajanjem dejavnosti ocenjevanja, ki lahko vključujejo revizije, inšpekcijske preglede, preverjanja in potrjevanja.

(2) Certifikacijski organ potrdi zadostnost in ustreznost dokazov, da se zagotovi zadostno jamstvo, da storitve in postopki izpolnjujejo zahteve za certificiranje, in sicer s potrditvijo:

(a) točnosti informacij, predstavljenih v opisu postopkov in storitev;

(b) ustreznosti zasnove in nadzora postopkov in storitev za izpolnjevanje meril za ocenjevanje;

(c) operativne učinkovitosti izvajanja tega nadzora v določenem obdobju pred ocenjevanjem.

(3) Točnost opisa in operativna učinkovitost izvajanja nadzora se lahko štejeta za cilja preverjanja v smislu standarda ISO/IEC 17000:2020 ustreznih trditev ponudnika denarnice (tj. potrditev poštenosti dogodkov, ki so se že zgodili, ali rezultatov, ki so že bili doseženi), medtem ko se lahko ustreznost zasnove in nadzora storitev in postopkov za izpolnjevanje meril za ocenjevanje šteje za cilj potrjevanja v smislu standarda ISO/IEC 17000:2020 ustrezne trditve ponudnika denarnice (tj. potrditev verjetnosti glede načrtovane prihodnje uporabe ali predvidenega izida).

(4) Glede na to, da rešitev denarnice ne sme delovati, preden je certificirana, operativne učinkovitosti ni mogoče potrditi na podlagi dejanskega delovanja rešitve. Zato se jo potrdi z dokazi, zbranimi med preskusi ali pilotnimi projekti.

(5) Nacionalne certifikacijske sheme že lahko obstajajo za specifične storitve in postopke, na primer za pristop uporabnikov. Uporabo takih shem, kadar je ustrezno, obravnavajo nacionalne certifikacijske sheme.

7. **Dejavnosti ocenjevanja, povezane s storitvami IKT, ki se uporabljajo za zagotavljanje in delovanje rešitve denarnice**

(1) Nekatere arhitekture denarnic se lahko opirajo na namenske storitve IKT, vključno s storitvami v oblaku za zagotavljanje in upravljanje rešitve denarnice, te storitve pa lahko gostijo občutljive podatke in operacije. V takem primeru nacionalne certifikacijske sheme določijo varnostne zahteve za te storitve IKT.

(2) Za storitve IKT, storitve v oblaku in druge vire informacij o zanesljivosti že obstajajo številne certifikacijske sheme, vključno s tistimi iz Priloge II. Nacionalne certifikacijske sheme se, kadar so na voljo in je to ustrezno, opirajo na te obstoječe mehanizme na enega od naslednjih načinov:

(a) določajo obvezno uporabo specifične sheme ali izbora shem z določitvijo pogojev, pod katerimi se na podlagi teh shem ocenijo storitve IKT ali storitve v oblaku;

(b) izbiro ocenjevanja prepustijo ponudniku denarnice in za analizo ustreznosti informacij o zanesljivosti, pridobljenih s temi ocenami, uporabijo analizo odvisnosti.

(3) V obeh primerih se v nacionalnih certifikacijskih shemah po potrebi določijo dodatne dejavnosti ocenjevanja, ki so potrebne za analizo ali dopolnitev informacij, pridobljenih s temi shemami.

PRILOGA V

SEZNAM JAVNO DOSTOPNIH INFORMACIJ O DENARNICAH

1. Informacije, ki se objavijo v skladu s členom 8(5), vključujejo vsaj naslednje:

   (a) kakršne koli omejitve uporabe rešitve denarnice;

   (b) smernice in priporočila ponudnika denarnice za pomoč končnim uporabnikom pri varni konfiguraciji, namestitvi, uvedbi, delovanju in vzdrževanju denarnic;

   (c) obdobje, v katerem bo končnim uporabnikom na voljo varnostna podpora, zlasti kar zadeva razpoložljivost posodobitev, povezanih s kibernetsko varnostjo;

   (d) kontaktne informacije proizvajalca ali ponudnika in sprejete metode za prejemanje informacij o šibkih točkah od končnih uporabnikov in raziskovalcev na področju varnosti;

   (e) sklice na spletne repozitorije, v katerih so navedene javno razkrite ranljivosti v zvezi z denarnicami, in vse morebitne zadevne nasvete za kibernetsko varnost.

2. Informacije iz odstavka 1 se dajo na voljo vsaki osebi, ki želi uporabiti rešitev denarnice, in sicer na javnem mestu ter na jasen, celovit in lahko dostopen način.

PRILOGA VI

METODOLOGIJA ZA OCENJEVANJE SPREJEMLJIVOSTI INFORMACIJ O ZANESLJIVOSTI

1. Ocenjevanje razpoložljivosti dokumentacije o zanesljivosti

Ocenjevalci navedejo dokumentacijo o zanesljivosti, ki je na voljo za vsako zadevno komponento rešitve denarnice in shemo elektronske identifikacije, na podlagi katere se zagotavljajo. Ocenjevalci nato ocenijo splošno ustreznost vsake dokumentacije o zanesljivosti za pregled odvisnosti.

V analizi se upoštevajo naslednji vidiki:

(1) o sami dokumentaciji o zanesljivosti:

(a) vrsta dokumentacije o zanesljivosti z vsemi zahtevanimi podrobnostmi

(primeri takih dokumentov so certifikati o skladnosti v skladu z EN ISO/IEC 27001:2022 ali tip 1 ali 2 poročila ISAE);

(b) obdobje, ki ga zajema, ali obdobje veljavnosti

(to obdobje se lahko dopolni z medrevizijsko izjavo (dokumentom, ki zajema obdobje med koncem poročevalnega obdobja sedanjega poročila ISAE in objavo novega poročila ISAE) ali podobno izjavo);

(c) veljavni okvir (npr. obstoječi standard);

(d) ali dokumentacija o zanesljivosti vključuje razvrstitev po zahtevah sheme.

(2) o strokovni usposobljenosti in nepristranskosti izdajatelja poročila o zanesljivosti:

(a) ime certifikacijskega organa in, če je na voljo, ime glavnega ocenjevalca;

(b) dokazila o usposobljenosti certifikacijskega organa in ocenjevalca (npr. akreditacija, osebna certifikacija itd.);

(c) dokazila o nepristranskosti certifikacijskega organa in ocenjevalca (npr. akreditacija itd.).

2. Ocenjevanje zanesljivosti v zvezi s posameznimi zahtevami

Ocenjevalci preverijo, ali je dokumentacija o zanesljivosti, ki je na voljo za rešitev denarnice in shemo elektronske identifikacije, v okviru katere se ta rešitev zagotavlja, ustrezna za ugotavljanje, ali rešitev denarnice izpolnjuje pričakovanja v zvezi s posameznimi zahtevami certifikacijske sheme.

Ta ocena se izvede za vsako zadevno komponento rešitve denarnice in sheme elektronske identifikacije, v okviru katere se ta rešitev zagotavlja, in sicer z oblikovanjem predpostavke o varnostnem nadzoru rešitve denarnice.

Ocenjevalna skupina za vsako tako predpostavko ugotovi, ali je zanesljivost iz razpoložljive dokumentacije o zanesljivosti ustrezna ali ne.

Ugotovitev, da je zanesljivost ustrezna, temelji na naslednjem:

(1) zahtevane informacije so na voljo v dokumentaciji o zanesljivosti in imajo pričakovano raven zanesljivosti;

(2) informacije, ki so na voljo v dokumentaciji o zanesljivosti, ne zajemajo celotnega obsega zahteve, vendar dodaten ali izravnalen nadzor (tj. notranji nadzor, ki zmanjšuje tveganje obstoječih ali morebitnih pomanjkljivosti pri nadzoru), uveden v rešitvi denarnici ali shemi elektronske identifikacije, v okviru katere se ta rešitev zagotavlja, ocenjevalcem omogoča ugotavljanje ustreznosti informacij;

(3) informacije, ki so na voljo v dokumentaciji o zanesljivosti, ne zagotavljajo pričakovane ravni zanesljivosti, vendar nadzor, ki se izvaja za ocenjevanje in spremljanje ponudnika denarnice, ocenjevalcem omogoča ugotavljanje ustreznosti informacij;

(4) če so v dokumentaciji o zanesljivosti navedene neskladnosti pri zasnovi ali izvajanju nadzora, uporabljenega za izpolnitev predpostavke, morajo biti popravni ukrepi, ki jih je ponudnik denarnice predlagal in izvedel ter so jih pregledali njegovi ocenjevalci, ustrezni za zagotovitev, da je predpostavka dejansko izpolnjena.

PRILOGA VII

VSEBINA CERTIFIKATA O SKLADNOSTI

1. Edinstveni identifikator, ki ga dodeli certifikacijski organ izdajatelj certifikata o skladnosti.

2. Informacije v zvezi s certificirano rešitvijo denarnice in shemo elektronske identifikacije, v okviru katere se ta rešitev zagotavlja, ter informacije o imetniku certifikata o skladnosti, vključno z naslednjim:
   (a) ime rešitve denarnice;
   (b) ime sheme elektronske identifikacije, v okviru katere se rešitev denarnice zagotavlja;
   (c) različica rešitve denarnice, ki je bila ocenjena;
   (d) ime, naslov in kontaktni podatki imetnika certifikata o skladnosti;
   (e) povezava na spletno mesto imetnika certifikata o skladnosti z informacijami, ki morajo biti javno dostopne.

3. Informacije v zvezi z ocenjevanjem in certificiranjem rešitve denarnice in sheme elektronske identifikacije, v okviru katere se ta rešitev zagotavlja, vključno z naslednjim:
   (a) ime, naslov in kontaktni podatki certifikacijskega organa izdajatelja certifikata o skladnosti;
   (b) kadar se razlikuje od certifikacijskega organa, ime organa za ugotavljanje skladnosti, ki je opravil ocenjevanje, skupaj z informacijami o njegovi akreditaciji;
   (c) ime lastnika sheme;
   (d) sklica na Uredbo (EU) št. 910/2014 in na to uredbo;
   (e) sklic na poročilo o certificiranju, povezano s certifikatom o skladnosti;
   (f) sklic na poročilo o oceni certificiranja, povezano s certifikatom o skladnosti;
   (g) sklic na standarde, uporabljene za ocenjevanje, vključno z njihovimi različicami;
   (h) datum izdaje certifikata o skladnosti;
   (i) datum veljavnosti certifikata o skladnosti.

PRILOGA VIII

VSEBINA JAVNEGA POROČILA O CERTIFICIRANJU IN POROČILA O OCENI CERTIFICIRANJA

1. Javno poročilo o certificiranju vsebuje vsaj:
   (a) povzetek;
   (b) identifikacijo rešitve denarnice in sheme elektronske identifikacije, v okviru katere se ta rešitev zagotavlja;
   (c) opis rešitve denarnice in sheme elektronske identifikacije, v okviru katere se ta rešitev zagotavlja;
   (d) varnostne informacije, ki morajo biti javno dostopne, kot je opisano v Prilogi V, ali sklic na te informacije;
   (e) povzetek predhodnega načrta revizije in potrjevanja;
   (f) povzetek pregleda in odločitve o certificiranju.

2. Poročilo o oceni certificiranja vsebuje vsaj:
   (a) opis zasnove rešitve denarnice, identifikacijskega sistema in pristopnega postopka skupaj z oceno tveganja in specifičnim načrtom potrjevanja;
   (b) opis, kako rešitev denarnice izpolnjuje zahteve glede visoke ravni zanesljivosti in kako to dokazujejo rezultati ocene certificiranja rešitve denarnice, izvedene v skladu s to uredbo;
   (c) opis rezultata ocene skladnosti rešitve denarnice in sheme elektronske identifikacije, v okviru katere so zagotovljene ustrezne enote denarnice, zlasti skladnosti z naslednjim:
      — zahtevami iz člena 5a(4), (5) in (8) Uredbe (EU) št. 910/2014;
      — zahtevo po logičnem ločevanju iz člena 5a(14) Uredbe (EU) št. 910/2014;
      — kadar je ustrezno, standardi in tehničnimi specifikacijami iz člena 5a(24) Uredbe (EU) št. 910/2014, pri čemer je opisano, kako so te zahteve povezane z ustreznimi normativnimi zahtevami, določenimi v nacionalnih certifikacijskih shemah;
   (d) povzetek rezultata izvedbe načrta potrjevanja, vključno z vsemi ugotovljenimi neskladnostmi.

PRILOGA IX

ČASOVNICA OBVEZNIH NADZORNIH OCENJEVANJ

1. Člen 18 določa zahteve za življenjski cikel certificiranja, zlasti za izvajanje rednih dejavnosti ocenjevanja. Te dejavnosti vključujejo najmanj naslednje:

   (a) celovito oceno predmeta ugotavljanja skladnosti pri začetnem ocenjevanju in vsakem ocenjevanju za ponovno certifikacijo, vključno s funkcijo posodabljanja katere koli komponente proizvoda;

   (b) oceno ranljivosti pri začetnem ocenjevanju in vsakem ocenjevanju za ponovno certifikacijo ter vsaj vsaki dve leti pri nadzornem ocenjevanju, pri čemer mora zajemati vsaj spremembe predmeta ugotavljanja skladnosti in spremembe v okolju groženj od zadnje ocene ranljivosti;

   (c) dodatne dejavnosti, kot je penetracijsko testiranje v primeru povečane stopnje tveganja ali pojava novih groženj;

   (d) vsaj letno oceno operativne učinkovitosti postopkov vzdrževanja pri nadzornem ocenjevanju in ocenjevanju za ponovno certifikacijo, pri čemer mora zajemati vsaj postopke preverjanja različic, posodabljanja in obvladovanja ranljivosti;

   (e) po uspešnem pregledu in odločitvi o certificiranju, izdajo certifikata o skladnosti po začetnem ocenjevanju in vsakem ocenjevanju za ponovno certifikacijo.

2. Referenčna časovnica je določena v preglednici 1 na podlagi štiriletnega cikla, pri čemer se:

   (a) leto 1 začne ob prvi izdaji certifikata o skladnosti;

   (b) vse dejavnosti ocenjevanja izvedejo v 12 mesecih od ocene v preteklem letu.

3. Časovnica iz preglednice 1 je priporočilo za zagotovitev pravočasne ponovne certifikacije in preprečitev motenj pri zagotavljanju rešitve denarnice. Možne so tudi druge časovnice, če veljavnost certifikata o skladnosti ni daljša od petih let, kot je določeno v členu 5c(4) Uredbe (EU) št. 910/2014.

4. Poleg rednih ocenjevanj se lahko na zahtevo certifikacijskega organa ali imetnika certifikata o skladnosti v primeru bistvene spremembe predmeta certificiranja ali okolja groženj izvede posebno ocenjevanje.

5. Vsako ocenjevanje, vključno z nadzornimi in posebnimi ocenjevanji, lahko privede do izdaje novega certifikata o skladnosti, zlasti v primeru bistvenih sprememb predmeta certificiranja, vendar z istim datumom poteka veljavnosti kot pri prvotnem certifikatu o skladnosti.

Preglednica 1

Celoten štiriletni ocenjevalni cikel

Čas	Vrsta ocenjevanja	Dejavnosti
Leto 0	Začetno	— Celovita ocena predmeta certificiranja, vključno z oceno ranljivosti; — vključno s funkcijo posodabljanja vsake komponente programske opreme; — ocena postopkov vzdrževanja, brez njihove operativne učinkovitosti; — izdaja certifikata o skladnosti in začetek štiriletnega cikla.
Leto 1	Nadzorno	— Ocena operativne učinkovitosti postopkov vzdrževanja; — vsaj preverjanje različice, posodabljanje in obvladovanje ranljivosti; — ocena sprememb, ki vplivajo na varnost proizvoda.

Čas	Vrsta ocenjevanja	Dejavnosti
Leto 2	Nadzorno	— Ocena ranljivosti za celotno rešitev; — ocena operativne učinkovitosti postopkov vzdrževanja; — vsaj preverjanje različice, posodabljanje in obvladovanje ranljivosti; — ocena sprememb, ki vplivajo na varnost proizvoda.
Leto 3	Nadzorno	— Ocena operativne učinkovitosti postopkov vzdrževanja; — vsaj preverjanje različice, posodabljanje in obvladovanje ranljivosti; — ocena sprememb, ki vplivajo na varnost proizvoda.
Leto 4	Ponovna certifikacija	(1) Celovita ocena predmeta certificiranja, vključno z oceno ranljivosti; (2) poenostavljena ocena nespremenjenih funkcij/postopkov; (3) vključno s funkcijo posodabljanja vsake komponente programske opreme; (4) ocena postopkov vzdrževanja, vključno z njihovo operativno učinkovitostjo; (5) izdaja novega certifikata o skladnosti.