REFERENČNA ŠTEVILKA: 2022-0941
ID KLASIFIKACIJE: 3.2.3

Okvir zaupanja

za švedsko e-identifikacijo

Različica 2022-10-04

1. Ozadje in namen

Cilj okvira zaupanja za švedsko e-identifikacijo je določiti skupne zahteve za izdajatelje elektronskih identitet, ki jih pregleda in odobri Švedska agencija za digitalno upravo (DIGG). Zahteve so razdeljene glede na različne razrede varstva oziroma ravni zanesljivosti, ki ustrezajo različnim stopnjam tehnične in operativne varnosti izdajatelja in različnim stopnjam preverjanja, ali je oseba, ki ji je izdan elektronski identifikacijski dokument, dejansko oseba, za katero se izdaja.

Zahteve tega okvira zaupanja se uporabljajo za ravni zanesljivosti 2 do 4, pri čemer raven 4 ustreza najvišji ravni varstva.

Skladnost se razlaga na naslednji način:

(a) če raven zanesljivosti ni določena, se zahteva izpolni na vseh ravneh in

(b) kadar je določena raven zanesljivosti, se skladnost zagotovi vsaj na ustrezni ravni.

Zahteve, določene za nižjo raven od ustrezne, se ne upoštevajo.

2. Organizacija in upravljanje

Splošne operativne zahteve

K2.1 Izdajatelji švedskih elektronskih identifikacij (eID), ki niso javni organi, morajo delovati kot registrirani pravni subjekti ter skleniti in vzdrževati zavarovanje, potrebno za poslovanje.

K2.2 Izdajatelji švedskih eID-jev morajo imeti vzpostavljeno podjetje, v celoti delovati v vseh delih, določenih v tem dokumentu, in biti dobro seznanjeni s pravnimi zahtevami, ki veljajo zanje kot izdajatelje švedskih eID-jev.

K2.3 Izdajatelji švedskih eID-jev morajo biti sposobni nositi tveganje odškodninske odgovornosti in imeti zadostna finančna sredstva za izvajanje svojih dejavnosti vsaj eno leto.

Informacijska varnost

K2.4 Izdajatelji švedskih eID-jev morajo za dele svojih dejavnosti, na katere vpliva okvir zaupanja, vzpostaviti sistem upravljanja informacijske varnosti (ISMS), ki temelji na standardu ISO/IEC 27001, kjer je ustrezno, ali enakovrednih načelih za upravljanje in nadzor dela na področju informacijske varnosti, vključno z naslednjim:

(a) Vsi za varnost pomembni upravni in tehnični postopki morajo biti dokumentirani in temeljiti na formalni podlagi, kjer so vloge, odgovornosti in pooblastila jasno opredeljeni.

(b) Izdajatelji švedskih eID-jev zagotovijo, da imajo vedno dovolj človeških virov za izpolnjevanje svojih obveznosti.

(c) Izdajatelji švedskih eID-jev vzpostavijo postopek obvladovanja tveganja, ki na ustrezen način, neprekinjeno ali vsaj vsakih 12 mesecev analizira grožnje in ranljivosti v poslovanju ter z uvedbo varnostnih ukrepov uravnoteži tveganja na sprejemljivo raven.

(d) Izdajatelji švedskih eID-jev vzpostavijo postopek obvladovanja incidentov, ki sistematično zagotavlja kakovost storitve, oblike nadaljnjega poročanja ter sprejetje ustreznih reaktivnih in preventivnih ukrepov za ublažitev ali preprečitev škode, ki je posledica takih dogodkov.

(e) Izdajatelji švedskih eID-jev pripravijo in redno preskušajo načrt neprekinjenega poslovanja, ki izpolnjuje zahteve podjetja glede dostopnosti z zmožnostjo ponovne vzpostavitve kritičnih procesov v primeru krize ali resnih incidentov.

(f) Izdajatelji švedskih eID-jev redno ocenjujejo delo na področju informacijske varnosti in v sistem upravljanja uvajajo ukrepe za izboljšanje.

K2.5 Obseg in zrelost sistema upravljanja:

Raven 4: Sistem upravljanja informacijske varnosti je skladen s standardom SS-ISO/IEC 27001:2017 ali enakovrednimi poznejšimi ali mednarodnimi različicami standarda in v okviru tega vključuje vse zahteve, ki veljajo za izdajatelje švedskih eID-jev.

Pogoji za podizvajanje

K2.6 Izdajatelj švedskih eID-jev, ki je izvajanje enega ali več za varnost pomembnih postopkov oddal v zunanje izvajanje drugi stranki, s pogodbo opredeli, za katere kritične postopke je odgovoren podizvajalec in katere zahteve se zanje uporabljajo, ter pojasni pogodbeno razmerje v izjavi izdajatelja.

Sledljivost, izbris in hramba dokumentov

K2.7 Izdajatelji švedskih eID-jev hranijo:

(a) dokumente o vlogah in dokumente v zvezi z izdajo, prejemom ali blokiranjem eID-jev;

(b) pogodbe, pravilnike in izjave izdajateljev in

(c) zgodovino obdelave in drugo dokumentacijo, ki je potrebna za dokazovanje skladnosti z zahtevami, ki veljajo za izdajatelje švedskih eID-jev, in ki omogoča nadaljnje spremljanje, ki dokazuje, da so postopki in kontrole, ki so pomembni za varnost, izvedeni in učinkoviti.

K2.8 Obdobje hrambe ne sme biti krajše od petih let, gradivo pa mora biti v celotnem obdobju mogoče pripraviti v berljivi obliki, razen če je zahteva za izbris potrebna z vidika zasebnosti in je podprta z zakonom ali drugim predpisom.

Pregled in spremljanje

K2.9 Izdajatelji švedskih eID-jev vzpostavijo funkcijo notranje revizije, ki redno pregleduje dejavnosti izdajanja. Notranji revizor je pri opravljanju svojih dolžnosti neodvisen na način, ki zagotavlja objektiven in nepristranski pregled, ter ima kompetence in izkušnje, potrebne za opravljanje svojih dolžnosti. Notranji revizor neodvisno načrtuje izvajanje revizije in to dokumentira v revizijskem načrtu za obdobje treh let. Revizijski elementi se izberejo na podlagi analize tveganja in pomembnosti ter temeljijo na opisih operacij, ki jih izdajatelj predloži Agenciji za digitalno upravo.

Ravni 3 in 4: Notranja revizija se izvaja na podlagi sprejetih revizijskih standardov.

3. Fizična, upravna in osebna varnost

K3.1 Osrednji deli operacije so fizično zaščiteni pred poškodbami zaradi okoljskih dogodkov, nepooblaščenega dostopa ali drugih zunanjih motenj. Nadzor dostopa se izvaja tako, da je dostop do občutljivih območij omejen na pooblaščeno osebje, da so nosilci podatkov varno shranjeni in odstranjeni ter da se dostop do teh zaščitenih območij stalno spremlja.

K3.2 Preden oseba prevzame katero koli vlogo, opredeljeno v skladu s K2.4(a), ki je posebnega pomena za varnost, izdajatelj švedskih eID-jev opravi preverjanje preteklosti, da se zagotovi, da se oseba lahko šteje za zanesljivo ter da ima kvalifikacije in usposobljenost, potrebne za varno in zanesljivo opravljanje nalog, ki izhajajo iz vloge.

K3.3 Izdajatelji imajo vzpostavljene postopke za zagotovitev, da ima dostop do podatkov, zbranih in hranjenih v skladu s K2.7, samo posebej pooblaščeno osebje.

K3.4 **Ravni 3 in 4:** Izdajatelji v celotni verigi postopka izdaje zagotovijo, da se delitev nalog uporablja tako, da nobena oseba ne more pridobiti eID-ja v imenu druge osebe.

4. Tehnična varnost

K4.1 Izdajatelji švedskih eID-jev zagotovijo, da vzpostavljeni tehnični nadzori zadostujejo za doseganje ravni zaščite, ki se šteje za potrebno glede na naravo, obseg in druge okoliščine poslovanja, ter da ti nadzori delujejo in so učinkoviti.

K4.2 Elektronska komunikacijska sredstva, ki se uporabljajo pri prenosu občutljivih podatkov, morajo biti zaščitena pred prestrezanjem, manipulacijo in ponovnim predvajanjem.

K4.3 Občutljivo gradivo šifrirnih ključev, ki se uporablja za izdajo eID-jev, identifikacijo imetnikov in izdajo potrdil o identiteti, se zaščiti tako, da:

(a) je dostop logično in fizično omejen na vloge in aplikacije, ki so nujno potrebne;

(b) gradivo ključev ni nikoli shranjeno v navadnem besedilu na trajnih nosilcih podatkov;

(c) je gradivo ključev zaščiteno z uporabo kriptografskega modula strojne opreme z aktivnimi varnostnimi mehanizmi, ki preprečujejo fizične in logične poskuse ogrožanja gradiva ključev;

(d) so varnostni mehanizmi za zaščito gradiva ključev pregledni ter temeljijo na priznanih in uveljavljenih standardih; in

(e) **ravni 3 in 4:** aktivacijski podatki za zaščito gradiva ključev se upravljajo z večosebnim nadzorom.

K4.4 Izdajatelji morajo imeti vzpostavljene dokumentirane postopke za zagotovitev, da se lahko zahtevana raven zaščite v ustreznem okolju IT ohrani skozi čas in v povezavi s spremembami, vključno z rednimi ocenami ranljivosti ter ustrezno pripravljenostjo za obvladovanje spreminjajočih se ravni tveganja in incidentov, ki se zgodijo.

5. Vloga, identifikacija in registracija

Informacije o pogojih

K5.1 Izdajatelji švedskih eID-jev morajo povezanim uporabnikom, ponudnikom e-storitev in drugim, ki se lahko zanesejo na storitev izdajatelja, zagotoviti informacije o pogodbah, pogojih in določilih ter s tem povezane informacije in morebitne omejitve uporabe storitve.

K5.2 Izdajatelj švedskih eID-jev se jasno sklicuje na pogoje in oblikuje postopke tako, da so pogoji vlagatelju zagotovljeni v postopku izdaje.

K5.3 Izdajatelji švedskih eID-jev predložijo izjavo izdajatelja, ki vključuje:

(a) identiteto in kontaktne podatke izdajatelja;

(b) kratke opise storitev in rešitev, ki jih zagotavlja izdajatelj, vključno z uporabljenimi metodami za vlogo, izdajo in blokiranje;

(c) pogoje, povezane z opravljeno storitvijo, vključno z obveznostmi uporabnika, da zaščiti svojo elektronsko identiteto, obveznostmi in odgovornostmi izdajatelja, vsemi danimi jamstvi in obljubljeno razpoložljivostjo;

(d) informacije o obdelavi osebnih podatkov in načinu, kako se izvaja; in

(e) postopke za spreminjanje določil ali drugih pogojev zagotovljene storitve, vključno z ukrepi, ki jih je treba sprejeti za nadzorovano ukinitev storitve.

K5.4 **Ravni 3 in 4:** Izdajatelji švedskih eID-jev na zahtevo Agencije za digitalno upravo (DIGG) ali druge pogodbenice, ki se zanaša na storitve, ki jih zagotavlja izdajatelj, zagotovijo informacije o lastništvu in upravljanju podjetja.

K5.5 Izdajatelj švedskih eID-jev, ki preneha opravljati svoje dejavnosti, upošteva vnaprej določen načrt za prenehanje opravljanja storitve. Načrt vključuje obveščanje vseh uporabnikov storitve in DIGG. Izdajatelj hrani arhivirano gradivo tudi po prenehanju v skladu s K2.7 in K2.8.

Vloga

K5.6 Švedski eID se lahko izda le na zahtevo vlagatelja ali v drugem enakovrednem postopku sprejemanja in šele potem, ko je bil vlagatelj seznanjen s pogoji, pod katerimi se izda, in odgovornostjo, ki mu bo naložena.

Izdaja eID-ja, ki nadomešča ali dopolnjuje prej izdan veljaven ali pred kratkim blokiran eID istega izdajatelja, pa se lahko izvede brez predhodne oddaje vloge.

K5.7 Vloga za švedski eID mora biti povezana z osebno identifikacijsko številko ali koordinacijsko številko ter informacijami, ki jih izdajatelj sicer potrebuje za zagotovitev takega eID-ja.

Ugotavljanje identitete vlagatelja

K5.8 Izdajatelji švedskih eID-jev morajo preveriti, ali so informacije, povezane z vlogo, popolne in ustrezajo informacijam, registriranim v uradnem registru.

K5.9 Kadar so informacije, ki jih je treba preveriti v uradnem registru, označene kot zaupne („zaščitena identiteta“), se lahko potrebni pregledi izvedejo na drug enakovreden način.

K5.10 Identifikacija vlagatelja med osebnim obiskom:

Izdajatelji švedskih eID-jev lahko identiteto vlagatelja preverijo med osebnim obiskom na enak način kot pri izdaji standardnega osebnega dokumenta.

K5.11 Identifikacija vlagatelja na daljavo v obstoječem razmerju:

Raven 3: Izdajatelji švedskih eID-jev, ki so vlagatelja že identificirali v razmerju, ki vključuje gospodarsko ali pravno pomembne transakcije, in kjer je vlagatelja mogoče identificirati na daljavo z drugimi zanesljivimi sredstvi, ki ustrezajo zahtevam za raven 3 znaka kakovosti za švedske eID-je, lahko to metodo uporabijo za ugotavljanje identitete vlagatelja.

Raven 4: Ni ustrezno.

K5.12 Identifikacija prek švedskega eID-ja:

Izdajatelj švedskih eID-jev lahko vlagatelja identificira na daljavo z obstoječim veljavnim švedskim eID-jem, ki ima vsaj enako raven zanesljivosti kot tisti, ki bo izdan, če lahko tako identifikacijo brez pogodbenih ovir uporabi kot podlago za izdajo novega eID-ja.

Raven 4: Obdobje veljavnosti novoizdanega eID-ja je omejeno tako, da ne presega obdobja veljavnosti obstoječega eID-ja.

K5.13 Identifikacija vlagatelja na daljavo:

Raven 2: Izdajatelji švedskih eID-jev lahko uporabijo zanesljive slikovne posnetke veljavnega standardnega osebnega dokumenta in podobo obraza vlagatelja kot podlago za ugotavljanje vlagateljeve identitete na daljavo, če primerjava ne vzbuja dvomov o vlagateljevi resnični identiteti.

Raven 3: Izdajatelji švedskih eID-jev lahko z varnim odčitavanjem veljavnega standardnega osebnega dokumenta, ki vsebuje elektronsko shranjene biometrične podatke, na podlagi teh podatkov na daljavo ugotovijo identiteto vlagatelja, če je mogoče ustrezne biometrične podatke osebe, ki jo je treba identificirati, zbrati na dovolj varen način, da se lahko izvede primerjava z enako zanesljivostjo kot v primeru osebnega obiska, in če primerjava ne vzbuja dvomov o resnični identiteti vlagatelja.

Raven 4: Ni ustrezno.

Registracija

K5.14 Izdajatelji švedskih eID-jev morajo ob upoštevanju veljavnih pravil o varstvu osebnih podatkov voditi register povezanih uporabnikov in dodeljenih elektronskih identifikacijskih dokumentov ter ga posodabljati.

6. Izdajanje in blokiranje eID-ja

Zasnova tehničnih sredstev

K6.1 Tehnična sredstva:

Ravni 2 in 3: Tehnična sredstva za elektronsko identifikacijo prek eID-ja z znakom kakovosti za švedski eID morajo biti zasnovana v skladu z načelom dveh faktorjev, pri čemer en del sestavljajo elektronsko shranjene informacije, ki jih ima uporabnik, drugi del pa tisto, kar uporabnik uporabi za aktivacijo eID-ja.

Raven 4: Tehnična sredstva za elektronsko identifikacijo prek eID-ja z znakom kakovosti za švedski eID morajo biti zasnovana v skladu z načelom dveh faktorjev, pri čemer en del sestavlja osebni varnostni modul, ki ga mora imeti uporabnik, drugi del pa tisto, kar uporabnik uporabi za aktivacijo varnostnega modula.

K6.2 Aktivacijski mehanizem in osebna koda morata biti zasnovana tako, da je malo verjetno, da bi tretje osebe prebile zaščito, tudi z mehanskimi sredstvi.

Ravni 3 in 4: Zaščita vključuje mehanizme za preprečevanje kopiranja in manipulacije elektronskega identifikacijskega dokumenta.

K6.3 Uporabniki eID-ja z znakom kakovosti za švedski eID lahko v obdobju veljavnosti eID-ja na lastno pobudo brezplačno in brez znatnih nevšečnosti spremenijo ali zahtevajo novo osebno kodo ter s smernicami ali samodejno pripravo prejmejo pomoč za ohranitev zahtev iz oddelka K6.2.

Če je eID zasnovan tako, da osebne kode ni mogoče spremeniti, bi moral imeti uporabnik namesto tega pod enakimi pogoji možnost, da takoj pridobi novi eID z novo osebno kodo, ki s postopkom blokiranja nadomesti prejšnjega.

K6.4 Izdajatelji švedskih eID-jev morajo zagotoviti, da podatki, registrirani za elektronsko identifikacijo imetnikov, enolično predstavljajo vlagatelja in se dodelijo zadevni osebi ob izdaji dokumenta eID.

K6.5 Obdobje veljavnosti izdanih eID-jev je omejeno ob upoštevanju varnostnih lastnosti dokumenta eID in tveganj zlorabe. Najdaljše obdobje veljavnosti eID-ja je pet let.

Izdaja dokumenta eID

K6.6 Izdaja na daljavo:

Raven 2: Izdajatelj švedskih eID-jev zagotovi dokument eID na način, ki potrjuje kontaktne podatke, shranjene v uradnem registru, ali take informacije, evidentirane v povezavi z elektronskim postopkom v skladu s K5.13, raven 2.

Raven 3: Izdajatelj švedskih eID-jev, ki zagotavlja eID po elektronskem postopku, ki je v skladu s K5.11, raven 3, K5.12, raven 3, ali K5.13, raven 3, mora ob novi izdaji ločeno in neodvisno od določbe v smislu varnosti zagotoviti, da je uporabnik obveščen, da je tak dokument eID bil izročen, ali z drugimi ukrepi zagotoviti enakovredno stopnjo nadzora, da je oseba opozorjena na tveganje kraje identitete v zvezi z izdajo.

Raven 4: Izdajatelj švedskih eID-jev, ki zagotavlja eID po elektronskem postopku v skladu s K5.12, raven 4, ob novi izdaji ločeno in neodvisno od določbe v zvezi z varnostjo zagotovi, da je uporabnik obveščen, da je bil tak dokument eID izročen.

K6.7 Izdaja med osebnim obiskom:

Izdajatelj švedskih eID-jev med osebnim obiskom in po preverjanju identitete v skladu s K5.10 predloži elektronski identifikacijski dokument proti podpisanemu potrdilu o prejemu ter zagotovi tudi del, ki ga uporabnik uporabi za aktiviranje eID-ja ločeno in neodvisno od predložitve dokumenta eID v smislu varnosti, na podlagi kontaktnih podatkov, shranjenih v uradnem registru, ali drugih informacij, ki so enako verodostojne.

Storitev blokiranja

K6.8 Izdajatelji švedskih eID-jev zagotovijo storitev blokiranja, ki je uporabniku enostavno dostopna, da lahko blokira svoj eID.

K6.9 Izdajatelji švedskih eID-jev nemudoma in varno obdelajo in izvedejo zahteve za blokiranje ter sprejmejo ukrepe za preprečevanje sistematične zlorabe storitve blokiranja ali drugih namernih dejanj, ki povzročajo vsesplošno blokiranje elektronskih identifikacijskih dokumentov, s čimer se zagotovi, da so eID-ji uporabnikov na voljo, kadar je to potrebno.

7. Preverjanje elektronskih identitet imetnikov

K7.1 Izdajatelji švedskih eID-jev zagotovijo, da se pri preverjanju identitete imetnika opravi zanesljivo preverjanje verodostojnosti in veljavnosti dokumenta eID.

K7.2 Izdajatelji švedskih eID-jev zagotovijo, da se pri preverjanju elektronskih identitet imetnikov izvajajo tehnični varnostni ukrepi, tako da ni verjetno, da bi tretje osebe z ugibanjem, prisluškovanjem, ponavljanjem ali manipulacijo postopka lahko prebile zaščitne mehanizme.

8. Izdaja potrdil o identiteti

Izdajatelji švedskih eID-jev, ki zagotavljajo storitev izdajanja potrdil o identiteti odvisnim e-storitvam, morajo prav tako izpolnjevati določbe tega oddelka.

K8.1 Izdajatelji švedskih eID-jev zagotovijo, da je storitev izdajanja potrdil o identiteti lahko dostopna in da se pred izdajo potrdil o identiteti opravi zanesljiva identifikacija v skladu z določbami oddelka 7.

Raven 4: Potrdila vključujejo sklic na gradivo šifrirnih ključev, za katerega izdajatelj potrdi, da je v izključni lasti imetnika.

K8.2 Predložena potrdila o identiteti so veljavna le toliko časa, kolikor je potrebno, da se uporabniku omogoči dostop do zahtevane e--storitve, in so zaščitena tako, da lahko informacije prebere le predvideni prejemnik in da prejemniki potrdil lahko preverijo pristnost potrdil.

K8.3 Izdajatelji švedskih eID-jev ob upoštevanju tveganja zlorabe storitve certificiranja omejijo obdobje, v katerem se lahko določenemu imetniku izda več zaporednih potrdil o identiteti, preden se imetnik ponovno identificira v skladu z določbami oddelka 7.