

Okvir povjerenja

za švedsku elektroničku identifikaciju

Verzija od 04. listopada 2022.

1. Kontekst i svrha

Okvirom povjerenja za švedsku elektroničku identifikaciju (eID) nastoje se uspostaviti zajednički zahtjevi za izdavatelje elektroničkih osobnih iskaznica koje je preispitala i odobrila Švedska agencija za digitalnu upravu (DIGG). Zahtjevi su podijeljeni na različite razine zaštite, nazivaju se i razine osiguranja, koje odgovaraju različitim stupnjevima tehničke i operativne sigurnosti izdavatelja i različitim stupnjevima provjere je li osoba kojoj je izdan elektronički identifikacijski dokument doista ona za koju se tvrdi da jest.

Zahtjevi ovog okvira povjerenja primjenjuju se na razine osiguranja od 2. do 4., pri čemu 4. razina odgovara najvišoj razini zaštite.

Usklađenost se tumači na sljedeći način:

- (a) ako razina osiguranja nije definirana, zahtjev mora biti ispunjen na svim razinama, i
- (b) ako razina osiguranja je definirana, usklađenost se osigurava barem na relevantnoj razini.

Zahtjevi utvrđeni za nižu razinu od relevantne ne uzimaju se u obzir.

2. Organizacija i upravljanje

Opći operativni zahtjevi

- K2.1 Izdavatelji švedskih eID-ova koji nisu javna tijela djeluju kao registrirani pravni subjekti te sklapaju i održavaju osiguranje potrebno za poslovanje.
- K2.2 Izdavatelji švedskih eID-ova moraju imati uhodano poslovanje, biti potpuno operativni u svim dijelovima navedenima u ovom dokumentu i dobro upoznati s pravnim zahtjevima koji se na njih primjenjuju kao izdavatelje švedskih eID-ova.
- K2.3 Izdavatelji švedskih eID-ova moraju biti sposobni snositi rizik od odgovornosti za štetu i posjedovati dostatna financijska sredstva za obavljanje svojeg poslovanja najmanje godinu dana.

Informacijska sigurnost

K2.4 Izdavatelji švedskih eID-ova dužni su uspostaviti sustav upravljanja informacijskom sigurnošću (ISMS) za dijelove svojih aktivnosti na koje utječe okvir povjerenja, koji se, ako je primjenjivo, temelji na normi ISO/IEC 27001 ili jednakovrijednim načelima za upravljanje i kontrolu rada u području informacijske sigurnosti, uključujući sljedeće:

- (a) Svi administrativni i tehnički postupci koji su ključni za sigurnost moraju biti dokumentirani i temeljiti se na formalnim osnovama, gdje su jasno definirane uloge, odgovornosti i ovlasti.
- (b) Izdavatelji švedskih eID-ova osiguravaju da u svakom trenutku imaju dovoljno ljudskih resursa za ispunjavanje svojih obveza.
- (c) Izdavatelji švedskih eID-ova uspostavljaju postupak upravljanja rizikom kojim se na odgovarajući način, kontinuirano ili najmanje svakih 12 mjeseci, analiziraju prijetnje i ranjivosti u poslovanju te kojim se uvođenjem sigurnosnih mjera rizici uravnotežuju na prihvatljive razine.
- (d) Izdavatelji švedskih eID-ova uspostavljaju postupak upravljanja incidentima za sustavno osiguravanje kvaliteta usluge, zahtjeve za daljnje izvješćivanje i poduzimanje odgovarajućih reaktivnih i preventivnih mjera za ublažavanje ili sprečavanje štete koja proizlazi iz takvih događaja.
- (e) Izdavatelji švedskih eID-ova uspostavljaju i redovito ispituju plan kontinuiteta koji ispunjava zahtjeve za pristupačnost poslovanja kroz sposobnost ponovne uspostave kritičnih procesa u slučaju krize ili ozbiljnih incidenata.
- (f) Izdavatelji švedskih eID-ova redovito ocjenjuju rad na informacijskoj sigurnosti i uvode mjere poboljšanja u sustav upravljanja.

K2.5 Područje primjene i zrelost sustava upravljanja:

4. razina: Sustav upravljanja informacijskom sigurnošću mora biti u skladu s normom SS-ISO/IEC 27001:2017 ili jednakovrijednim naknadnim ili međunarodnim verzijama norme te u okviru tog područja primjene uključivati sve zahtjeve nametnute izdavateljima švedskih eID-ova.

Uvjeti podugovaranja

- K2.6 Izdavalatelj švedskih eID-ova koji je eksternalizirao provedbu jednog ili više postupaka ključnih za sigurnost drugoj strani ugovorom definira za koje je ključne postupke odgovoran podugovaratelj i koji se zahtjevi na njih primjenjuju te pojašnjava ugovorni odnos u izjavi izdavalatelja.

Sljedivost, brisanje i pohrana dokumenata

- K2.7 Izdavalatiji švedskih eID-ova pohranjuju:
- (a) dokumente povezane sa zahtjevom i dokumente koji se odnose na izdavanje, primanje ili blokiranje eID-ova;
 - (b) ugovore, dokumente o politikama i izjave izdavalatelja; i
 - (c) povijest obrade i drugu sličnu dokumentaciju koja je potrebna za dokazivanje usklađenosti sa zahtjevima uvedenima za izdavalatelje švedskih eID-ova i koja omogućuje daljnje postupanje kojim se dokazuje da su uspostavljeni i učinkoviti sigurnosno-kritični procesi i kontrole.
- K2.8 Razdoblje pohrane ne smije biti kraće od pet godina, a materijal se mora moći proizvesti u čitljivom obliku tijekom cijelog tog razdoblja, osim ako je zahtjev za brisanjem potreban sa stajališta privatnosti i poduprt je zakonom ili drugim propisom.

Revizija i daljnje praćenje

- K2.9 Izdavatelji švedskih eID-ova uspostavljaju funkciju unutarnje revizije kojom se periodično preispituju aktivnosti izdavanja. Unutarnji revizor neovisan je u obavljanju svojih dužnosti na način kojim se osigurava objektivna i nepristrana revizija te ima stručno znanje i iskustvo koji su potrebni za obavljanje svojih dužnosti. Unutarnji revizor neovisno planira provedbu revizije i dokumentira je u planu revizije koji obuhvaća razdoblje od tri godine. Elementi revizije odabiru se na temelju analize rizika i značajnosti te se temelje na opisima operacija koje izdavatelj dostavlja Agenciji za digitalnu upravu.

3. i 4. razina: Unutarnja revizija provodi se na temelju prihvaćenih revizijskih standarda.

3. Fizička, administrativna i osobna sigurnost

- K3.1 Središnji dijelovi operacije fizički su zaštićeni od štete koja je posljedica okolišnih događaja, neovlaštenog pristupa ili drugih vanjskih smetnji. Kontrola pristupa primjenjuje se tako da je pristup osjetljivim područjima ograničen na ovlašteno osoblje, da se mediji-nositelji podataka sigurno pohranjuju i odlažu te da se pristup tim zaštićenim područjima stalno nadzire.
- K3.2 Prije nego što osoba preuzme bilo koju od uloga utvrđenih u skladu s K2.4. točkom (a) i koje su od posebne važnosti za sigurnost, izdavatelj švedskih eID-ova provodi provjere podobnosti kako bi osigurao da se osoba može smatrati pouzdanom te da ima kvalifikacije i osposobljavanje potrebne za sigurno i zaštićeno obavljanje zadaća koje proizlaze iz te uloge.
- K3.3 Izdavatelji uspostavljaju postupke kojima se osigurava da samo posebno ovlašteno osoblje ima pristup podacima koji se prikupljaju i zadržavaju u skladu s K2.7.
- K3.4 **3. i 4. razina:** Izdavatelji osiguravaju da se u cijelom lancu postupka izdavanja razdvajanje dužnosti primjenjuje tako da nijedna osoba ne može dobiti eID u ime druge osobe.

4. Tehnička sigurnost

- K4.1 Izdavatelji švedskih eID-ova osiguravaju da su uspostavljene tehničke kontrole dostatne za postizanje razine zaštite koja se smatra potrebnom s obzirom na prirodu, opseg i druge okolnosti poslovanja i da te kontrole funkcioniraju i da su učinkovite.
- K4.2 Elektronička sredstva komunikacije koja se upotrebljavaju za prijenos osjetljivih podataka moraju biti zaštićena od presretanja, manipulacije i ponavljanja.

K4.3 Osjetljivi kriptografski ključevi koji se upotrebljavaju za izdavanje eID-ova, identifikaciju nositelja i izdavanje potvrda o identitetu zaštićeni su na sljedeći način:

- (a) pristup je logički i fizički ograničen na uloge i primjene koje su strogo nužne;
- (b) kriptografski ključevi nikad se ne pohranjuju u običnom tekstu na trajnim medijima za pohranu;
- (c) kriptografski ključevi zaštićeni su upotrebom kriptografskog hardverskog modula s aktivnim sigurnosnim mehanizmima koji suzbijaju fizičke i logičke pokušaje ugrožavanja kriptografskih ključeva;
- (d) sigurnosni mehanizmi za zaštitu kriptografskih ključeva transparentni su i temelje se na priznatim i dobro utvrđenim standardima; i
- (e) **3. i 4. razina:** aktivacijskim podacima za zaštitu kriptografskih ključeva upravlja se putem kontrole više osoba.

K4.4 Izdavatelji moraju imati uspostavljene dokumentirane postupke kako bi osigurali da se potrebna razina zaštite u relevantnom IT okruženju može održati tijekom vremena i u slučaju promjena, uključujući redovite procjene ranjivosti i odgovarajuću pripravnost za zadovoljavanje promjenjivih razina rizika i incidenata koji se dogode.

5. Prijava, identifikacija i registracija

Informacije o uvjetima

- K5.1 Izdavalci švedskih eID-ova pružaju informacije o ugovorima, uvjetima i odredbama, kao i povezane informacije i sva ograničenja upotrebe usluge povezanim korisnicima, pružateljima e-usluga i drugima koji se mogu oslanjati na uslugu izdavalca.
- K5.2 Izdavalac švedskih eID-ova jasno upućuje na uvjete i oblikuje postupke tako da se uvjeti dostave podnositelju zahtjeva u postupku izdavanja.
- K5.3 Izdavalci švedskih eID-ova dostavljaju izjavu izdavalca koja uključuje:
- (a) identitet i podatke za kontakt izdavalca;
 - (b) kratki opisi usluga i rješenja koje pruža izdavalac, uključujući metode korištene za primjenu, izdavanje i blokiranje;
 - (c) uvjete povezane s pruženom uslugom, uključujući obveze korisnika da zaštiti svoj elektronički ID, obveze i odgovornosti izdavalca, sva jamstva koja su dana i obećanu dostupnost;
 - (d) informacije o obradi osobnih podataka i načinu na koji se provodi; i
 - (e) mehanizme za izmjenu uvjeta ili drugih uvjeta pružene usluge, uključujući korake koje treba poduzeti kako bi se usluga prekinula na kontrolirani način.
- K5.4 **3. i 4. razina:** Izdavalci švedskih eID-ova na zahtjev Agencije za digitalnu upravu (DIGG) ili druge ugovorne strane koja se oslanja na usluge koje pruža izdavalac, dostavljaju informacije o obliku vlasništva poduzeća i kako se njime upravlja.
- K5.5 Izdavalac švedskih eID-ova koji prestane s radom slijedi unaprijed utvrđeni plan za prekidanje usluge. Plan uključuje obavješćivanje svih korisnika usluge i DIGG-a. Izdavalac nadalje drži arhivirani materijal dostupnim u skladu s K2.7 i K2.8 nakon prekida.

Primjena

- K5.6 Švedski eID može se izdati samo na zahtjev podnositelja zahtjeva ili u okviru drugog jednakovrijednog postupka prihvatanja i tek nakon što je podnositelj zahtjeva upoznat s uvjetima pod kojima se izdaje i odgovornošću koja će mu biti dodijeljena.

Međutim, izdavanje eID-a kojim se zamjenjuje ili dopunjuje valjani ili nedavno blokirani dokument elektroničke identifikacije koji je prethodno izdao isti izdavalac može se obaviti bez prethodnog postupka podnošenja zahtjeva.

- K5.7 Zahtjev za švedski eID povezan je s osobnim identifikacijskim brojem ili jedinstvenim brojem, kao i s informacijama koje su izdavatelju inače potrebne za pružanje takvog eID-a.

Utvrđivanje identiteta podnositelja zahtjeva

K5.8 Izdavatelji švedskih eID-ova moraju provjeriti jesu li informacije povezane sa zahtjevom potpune i odgovaraju li informacijama upisanim u službeni registar.

K5.9 Ako su podaci koje treba provjeriti u službenom registru označeni kao povjerljivi („zaštićeni identitet”), potrebne provjere mogu se provesti drugim jednakovrijednim sredstvima.

K5.10 Identifikacija podnositelja zahtjeva tijekom osobnog posjeta:

Izdavatelji švedskih eID-ova mogu provjeriti identitet podnositelja zahtjeva tijekom osobnog posjeta, na isti način kao i pri izdavanju standardne identifikacijske isprave.

K5.11 Daljinska identifikacija podnositelja zahtjeva u postojećem odnosu:

3. razina: Izdavatelji švedskih eID-ova koji su već identificirali podnositelja zahtjeva u odnosu koji uključuje gospodarski ili pravno značajne transakcije, i gdje se podnositelj zahtjeva može identificirati na daljinu drugim pouzdanim sredstvima koja odgovaraju zahtjevima 3. razine švedske oznake kvalitete eID-a, mogu upotrijebiti ovu metodu za utvrđivanje identiteta podnositelja zahtjeva.

4. razina: Nije primjenjivo.

K5.12 Identifikacija putem švedskog eID-a:

Izdavatelj švedskih eID-ova može na daljinu identificirati podnositelja zahtjeva pomoću postojećeg valjanog švedskog eID-a koji je najmanje iste razine sigurnosti kao onaj koji se treba izdati, ako može, bez ugovornih prepreka, koristiti takvu identifikaciju kao osnovu za izdavanje novog eID-a.

4. razina: Razdoblje valjanosti novoizdanog eID-a ograničeno je na razdoblje koje ne prelazi razdoblje valjanosti postojećeg eID-a.

K5.13 Daljinska identifikacija podnositelja zahtjeva:

2. razina: Izdavatelji švedskih eID-ova mogu koristiti pouzdane snimke valjane standardne identifikacijske isprave i slike lica podnositelja zahtjeva kao osnovu za daljinsko utvrđivanje identiteta podnositelja zahtjeva ako usporedba ne izaziva sumnje u pogledu pravog identiteta podnositelja zahtjeva.

3. razina: Izdavatelji švedskih elektroničkih osobnih iskaznica mogu, sigurnim čitanjem važeće standardne identifikacijske isprave koja sadržava elektronički pohranjene biometrijske podatke, na daljinu utvrditi identitet podnositelja zahtjeva na temelju tih podataka ako se odgovarajući biometrijski podaci osobe koju treba identificirati mogu prikupiti na dovoljno siguran način kako bi se usporedba mogla

provesti s jednakom pouzdanošću kao u slučaju osobnog posjeta i ako usporedba ne dovodi u pitanje stvarni identitet podnositelja zahtjeva.

4. razina: Nije primjenjivo.

Registracija

K5.14 Izdavatelji švedskih eID-ova, uzimajući u obzir primjenjive propise o zaštiti osobnih podataka, vode registar povezanih korisnika i dodijeljenih elektroničkih identifikacijskih dokumenata te ažuriraju taj registar.

6. Izdavanje i blokiranje eID-a

Izrada tehničkih sredstava

K6.1 Tehnička sredstva:

2. i 3. razina: Tehnička sredstva za elektroničku identifikaciju putem eID-a sa švedskom oznakom kvalitete eID-a izrađuju se na načelu dvaju faktora, pri čemu jedan dio čine elektronički pohranjene informacije koje korisnik treba posjedovati, a drugi dio ono što korisnik treba koristiti za aktivaciju eID-a.

4. razina: Tehnička sredstva za elektroničku identifikaciju putem eID-a sa švedskom oznakom kvalitete izrađuju se na načelu dvaju faktora, pri čemu jedan dio čini osobni sigurnosni modul koji korisnik mora posjedovati, a drugi dio ono što korisnik mora koristiti za aktivaciju sigurnosnog modula.

K6.2 Aktivacijski mehanizam i osobni kôd izrađeni su na način da je malo vjerojatno da će treće strane onesposobiti zaštitu, čak ni mehaničkim sredstvima.

3. i 4. razina: Zaštita uključuje mehanizme za sprečavanje kopiranja i manipulacije elektroničkim identifikacijskim dokumentom.

K6.3 Korisnici eID-a sa švedskom oznakom kvalitete eID-a mogu, na vlastitu inicijativu, tijekom razdoblja valjanosti eID-a, besplatno i bez znatnih neugodnosti razmijeniti ili zatražiti novi osobni kôd te im se, s pomoću smjernica ili automatske izrade, može pomoći da zadrže zahtjeve iz K6.2.

Ako je eID osmišljen tako da se osobni kôd ne može razmijeniti, korisnik bi umjesto toga trebao, pod istim uvjetima, odmah moći dobiti novi eID s novim osobnim kôdom koji zamjenjuje prethodni putem postupka blokiranja.

K6.4 Izdavatelji švedskih eID-ova osiguravaju da podaci registrirani za elektroničku identifikaciju nositelja na jedinstven način predstavljaju podnositelja zahtjeva i pripisuju se predmetnoj osobi pri izdavanju eID dokumenta.

K6.5 Razdoblje valjanosti izdanih eID-a ograničeno je uzimajući u obzir sigurnosne značajke eID dokumenta i rizike od zlouporabe. Najdulje razdoblje valjanosti eID-a je pet godina.

Pružanje eID dokumenta

K6.6 Pružanje na daljinu:

2. razina: Izdavalatelj švedskih eID-a dostavlja e-ID dokument na način kojim se potvrđuju podaci za kontakt koji se vode u službenom registru ili podaci zabilježeni u vezi s elektroničkim postupkom u skladu s K5.13. za 2. razinu.

3. razina: Izdavalatelj švedskih eID-ova koji pruža eID elektroničkim postupkom koji je u skladu s K5.11. za 3. razinu, K5.12. za 3. razinu ili K5.13. za 3. razinu dužan je, pri novom izdavanju, odvojeno i neovisno o pružanju u pogledu sigurnosti, osigurati da je korisnik obaviješten o tome da je takav e-ID dokument uručen, ili drugim mjerama osigurati jednakovrijedan stupanj kontrole da je osoba upozorena na rizik od krađe identiteta u vezi s pružanjem.

4. razina: Izdavalatelj švedskih eID-ova koji pruža eID putem elektroničkog postupka u skladu s K5.12. za 4. razinu, pri novom izdavanju, odvojeno i neovisno o pružanju u smislu sigurnosti, osigurava da je korisnik obaviješten da je takav eID dokument predan.

K6.7 Pružanje tijekom osobnog posjeta:

Izdavalatelj švedskih eID-ova tijekom osobnog posjeta i nakon provjere identiteta u skladu s K5.10. dostavlja elektronički identifikacijski dokument uz potpisanu potvrdu o primitku te dodatno dostavlja dio koji korisnik upotrebljava za aktivaciju eID-a zasebno i neovisno o pružanju eID dokumenta u smislu sigurnosti, na temelju podataka za kontakt koji se čuvaju u službenom registru ili drugih informacija jednake vjerodostojnosti.

Usluga blokiranja

- K6.8 Izdavalci švedskih eID-ova trebaju pružiti uslugu blokiranja s dobrom dostupnošću kako bi korisnik mogao blokirati svoj eID.
- K6.9 Izdavalci švedskih eID-ova odmah i na siguran način obrađuju i izvršavaju zahtjeve za blokiranje te poduzimaju mjere za sprečavanje sustavne zlorabe usluge blokiranja ili drugih namjernih radnji koje mogu uzrokovati širenje blokiranja elektroničkih identifikacijskih dokumenata, osiguravajući da su eID-ovi korisnika dostupni kada je to potrebno

7. Provjera elektroničkih identiteta nositelja

- K7.1 Izdavalci švedskih eID-ova osiguravaju da se pri provjeri identiteta nositelja provode pouzdane provjere autentičnosti i valjanosti eID dokumenta.
- K7.2 Izdavalci švedskih eID-ova osiguravaju provedbu tehničkih sigurnosnih kontrola pri provjeri elektroničkih identiteta nositelja, tako da je malo vjerojatno da bi treće strane, nagađanjem, prisluškivanjem, ponovnim prikazivanjem ili manipuliranjem postupkom, mogle zaobići zaštitne mehanizme.

8. Izdavanje potvrda o identitetu

Izdavalci švedskih eID-ova koji pružaju uslugu izdavanja potvrda o identitetu za pouzdajuće e-usluge također moraju poštovati odredbe ovog odjeljka.

- K8.1 Izdavalci švedskih eID-ova osiguravaju da je usluga izdavanja potvrda o identitetu dobro dostupna i da izdavanju potvrda o identitetu prethodi pouzdana identifikacija u skladu s odredbama odjeljka 7.

4. razina: Potvrde uključuju referencu na kriptografske ključeve koje je izdavalac potvrdio kao isključivo u posjedu nositelja.

- K8.2 Podnesene potvrde o identitetu valjane su samo onoliko dugo koliko je potrebno kako bi se korisniku omogućio pristup traženoj e-usluzi, te su zaštićene tako da informacije može pročitati samo predviđeni primatelj i da primatelj potvrda mogu provjeriti vjerodostojnost potvrda.
- K8.3 Uzimajući u obzir rizike zlorabe usluge certificiranja, izdavalci švedskih eID-ova ograničavaju razdoblje unutar kojeg se određenom nositelju može izdati nekoliko uzastopnih potvrda o identitetu prije ponovne identifikacije nositelja u skladu s odredbama odjeljka 7.