DOKUMENTA NUMURS: 2022-0941
KLASIFIKĀCIJAS ID: 3.2.3.

Uzticamības satvars

Zviedrijas e-identifikācijai

Izdots piektdienā, 2022.10.04.

1. Pamatinformācija un mērķis

Zviedrijas e-identifikācijas uzticamības satvara mērķis ir noteikt kopīgas prasības elektronisko ID izdevējiem, ko pārskata un apstiprina Zviedrijas Digitālās pārvaldības aģentūra (DIGG). Prasības ir iedalītas dažādās aizsardzības klasēs — garantijas līmeņos —, kas atbilst dažādām izdevēja tehniskās un darbības drošības pakāpēm un dažādām verifikācijas pakāpēm, lai pārliecinātos, ka persona, kurai tiek izsniegts elektroniskās identifikācijas dokuments, patiešām ir tā, par ko tā uzdodas.

Šī uzticamības satvara prasības attiecas uz 2.–4. uzticamības līmeni, un 4. līmenis atbilst augstākajam aizsardzības līmenim.

Atbilstība tiek interpretēta šādi:

(a) ja apliecinājuma līmenis nav noteikts, prasība jāizpilda visos līmeņos, un

(b) ja ir noteikts apliecinājuma līmenis, atbilstība jānodrošina vismaz attiecīgajā līmenī.

Prasības, kas noteiktas zemākam līmenim nekā attiecīgais, neņem vērā.

2. Organizācija un pārvaldība

Vispārējās darbības prasības

K2.1 Zviedrijas eID izdevēji, kas nav publiskas struktūras, darbojas kā reģistrētas juridiskas personas un iegādājas un uztur uzņēmējdarbībai nepieciešamo apdrošināšanu.

K2.2 Zviedrijas eID izdevējiem jābūt iedibinātiem uzņēmumiem, tiem jābūt pilnībā spējīgiem darboties visās šajā dokumentā norādītajās daļās un labi jāpārzina juridiskās prasības, kas tiem noteiktas kā Zviedrijas eID izdevējiem.

K2.3 Zviedrijas eID izdevējiem jābūt spējīgiem uzņemties atbildību par zaudējumiem un jābūt pietiekamiem finanšu resursiem, lai vismaz vienu gadu veiktu savu darbību.

Informācijas drošība

K2.4 Zviedrijas eID izdevējiem attiecībā uz tām savu darbību daļām, uz kurām attiecas uzticamības satvars, ir jābūt izveidotai informācijas drošības pārvaldības sistēmai (ISMS), kuras pamatā attiecīgā gadījumā ir ISO/IEC 27001 vai līdzvērtīgi informācijas drošības darba pārvaldības un kontroles principi, tostarp šādi:

(a) Visi drošībai būtiskie administratīvie un tehniskie procesi ir jādokumentē, un to pamatā jābūt oficiālam pamatam, kurā ir skaidri noteiktas lomas, pienākumi un pilnvaras.

(b) Zviedrijas eID izdevējiem jānodrošina, ka tiem vienmēr ir pietiekami cilvēkresursi, lai pildītu savus pienākumus.

(c) Zviedrijas eID izdevējiem ir jāizveido riska pārvaldības process, kas piemērotā veidā, pastāvīgi vai vismaz reizi 12 mēnešos analizē apdraudējumus un ievainojamības uzņēmējdarbībā un kas, ieviešot drošības pasākumus, līdzsvaro riskus līdz pieņemamam līmenim.

(d) Zviedrijas eID izdevēji izveido incidentu pārvaldības procesu, kas sistemātiski nodrošina pakalpojuma kvalitāti, turpmākas ziņošanas formas un to, ka tiek veikti atbilstoši reaģējoši un preventīvi pasākumi, lai mazinātu vai novērstu šādu notikumu radīto kaitējumu.

(e) Zviedrijas eID izdevējiem ir jāizstrādā un regulāri jātestē darbības nepārtrauktības plāns, kas atbilst uzņēmuma piekļūstamības prasībām, nodrošinot spēju krīzes vai nopietnu incidentu gadījumā atjaunot kritiski svarīgus procesus.

(f) Zviedrijas eID izdevēji regulāri izvērtē darbu informācijas drošības jomā un ievieš uzlabošanas pasākumus pārvaldības sistēmā.

K2.5 Pārvaldības sistēmas darbības joma un termiņš:

4. līmenis: Informācijas drošības pārvaldības sistēmai jāatbilst standartam SS-ISO/IEC 27001:2017 vai līdzvērtīgām turpmākajām vai starptautiskajām versijām, un tās darbības jomā jāietver visas prasības, kas noteiktas Zviedrijas eID izdevējiem.

Apakšuzņēmumu nolīgšanas nosacījumi

K2.6 Zviedrijas eID izdevējs, kas viena vai vairāku drošībai būtisku procesu izpildi ir ārpakalpojuma veidā uzticējis citai pusei, līgumā nosaka, par kuriem kritiskiem procesiem ir atbildīgs apakšuzņēmējs un kādas prasības uz to attiecas, un izdevēja deklarācijā precizē līgumattiecības.

Dokumentu izsekojamība, dzēšana un glabāšana

K2.7 Zviedrijas eID izsniedzēji glabā:

(a) pieteikuma dokumentus un dokumentus, kas saistīti ar eID izsniegšanu, saņemšanu vai bloķēšanu;

(b) līgumus, politikas dokumentus un izdevēja deklarācijas, un

(c) apstrādes vēsturi un citu tādu dokumentāciju, kas vajadzīga, lai pierādītu atbilstību Zviedrijas eID izdevējiem noteiktajām prasībām, un kas ļauj veikt turpmākus pasākumus, kas apliecina, ka drošībai kritiskie procesi un kontroles ir ieviesti un efektīvi.

K2.8 Glabāšanas laiks nav mazāks par pieciem gadiem, un materiālu ir iespējams sagatavot salasāmā veidā visā šajā laikā, ja vien no privātuma viedokļa nav nepieciešama dzēšana un to atbalsta tiesību akti vai citi noteikumi.

Pārskatīšana un turpmākie pasākumi

K2.9 Zviedrijas eID izdevēji izveido iekšējās revīzijas funkciju, kas periodiski pārskata izsniegšanas darbības. Iekšējais revidents, pildot savus pienākumus, ir neatkarīgs tādā veidā, kas nodrošina objektīvu un neitrālu pārskatīšanu, un viņam ir kompetence un pieredze, kas nepieciešama pienākumu veikšanai. Iekšējais revidents neatkarīgi plāno revīzijas veikšanu un dokumentē to revīzijas plānā, kas ietver trīs gadu laikposmu. Revīzijas elementus atlasa, pamatojoties uz riska un būtiskuma analīzi, un to pamatā ir darbību apraksti, ko izdevējs ir iesniedzis Digitālās pārvaldības aģentūrai.

3. un 4. līmenis: Iekšējo revīziju veic, pamatojoties uz atzītiem revīzijas standartiem.

3. Fiziskā, administratīvā un uz personu orientētā drošība

K3.1 Darbības centrālās daļas ir fiziski aizsargātas pret kaitējumu, ko rada vides notikumi, neatļauta piekļuve vai citi ārēji traucējumi. Piekļuves kontroli piemēro tā, lai piekļuve jutīgām zonām būtu atļauta tikai pilnvarotam personālam, informācijas nesēji tiktu droši uzglabāti un iznīcināti, un piekļuve šīm aizsargājamām zonām tiktu pastāvīgi uzraudzīta.

K3.2 Pirms persona uzņemas kādu no funkcijām, kas noteiktas saskaņā ar K2.4. punkta a) apakšpunktu un kas ir īpaši svarīgas drošībai, Zviedrijas eID izdevējam ir jāveic iepriekšējās darbības pārbaudes, lai nodrošinātu, ka personu var uzskatīt par uzticamu un ka personai ir kvalifikācija un izieta apmācība, kas nepieciešama, lai droši un neapdraudēti veiktu uzdevumus, kas izriet no šīs funkcijas.

K3.3 Izdevējiem ir jāievieš procedūras, lai nodrošinātu, ka tikai īpaši pilnvarotiem darbiniekiem ir piekļuve datiem, kas vākti un saglabāti saskaņā ar K2.7. punktu.

K3.4 **3. un 4. līmenis:** Izdevēji visā izdošanas procesa ķēdē nodrošina, ka pienākumu nodalīšana tiek piemērota tā, lai neviena persona nevarētu iegūt eID citas personas vārdā.

4. Tehniskā drošība

K4.1 Zviedrijas eID izdevējiem jānodrošina, ka ieviestās tehniskās kontroles ir pietiekamas, lai sasniegtu aizsardzības līmeni, kas tiek uzskatīts par nepieciešamu, ņemot vērā uzņēmējdarbības veidu, darbības jomu un citus apstākļus, un ka šīs kontroles darbojas un ir efektīvas.

K4.2 Elektroniskie saziņas līdzekļi, ko izmanto sensitīvu datu pārraidīšanai, ir aizsargāti pret pārtveršanu, manipulācijām un atkārtošanu.

K4.3 Sensitīvus kriptogrāfijas atslēgu materiālus, ko izmanto eID izdošanai, turētāju identificēšanai un identitātes sertifikātu izdošanai, aizsargā tā:

(a) lai piekļuve ir loģiski un fiziski ierobežota attiecībā uz lomām un lietojumprogrammām, kas ir stingri nepieciešamas;

(b) lai atslēgu materiāls nekad netiktu glabāts vienkāršā tekstā pastāvīgā datu nesējā;

(c) lai atslēgu materiāls ir aizsargāts, izmantojot kriptogrāfijas aparatūras moduli ar aktīviem drošības mehānismiem, kas novērš gan fiziskus, gan loģiskus mēģinājumus kompromitēt atslēgu materiālu;

(d) lai drošības mehānismi atslēgu materiāla aizsardzībai ir pārredzami un balstīti uz atzītiem un vispāratzītiem standartiem, un

(e) **3. un 4. līmenis:** lai aktivizēšanas dati atslēgu materiāla aizsardzībai tiek pārvaldīti, izmantojot vairāku personu kontroli.

K4.4 Izdevējiem ir jābūt ieviestām dokumentētām procedūrām, lai nodrošinātu, ka vajadzīgo aizsardzības līmeni attiecīgajā IT vidē var saglabāt laika gaitā un saistībā ar izmaiņām, tostarp regulāri veicot neaizsargātības novērtējumus, un pienācīgi sagatavoties mainīgajiem riska līmeņiem un notiekošajiem incidentiem.

5. Pieteikums, identifikācija un reģistrācija

Informācija par nosacījumiem

K5.1 Zviedrijas eID izdevēji sniedz informāciju saistītajiem lietotājiem, e-pakalpojumu sniedzējiem un citām personām, kuras var paļauties uz izdevēja pakalpojumu, par līgumiem, noteikumiem un nosacījumiem, kā arī saistīto informāciju un informāciju par jebkādiem pakalpojuma izmantošanas ierobežojumiem.

K5.2 Zviedrijas eID izdevējam skaidri jāatsaucas uz noteikumiem un jāizstrādā procedūras tā, lai noteikumi tiktu sniegti pieteikuma iesniedzējam izdošanas procesā.

K5.3 Zviedrijas eID izdevēji iesniedz izdevēja deklarāciju, kurā iekļauj:

(a) izdevēja identitāti un kontaktinformāciju;

(b) īsus aprakstus par izdevēja sniegtajiem pakalpojumiem un risinājumiem, tostarp par piemērotajām pieteikumu iesniegšanas, dokumentu izdošanas un bloķēšanas metodēm;

(c) nosacījumus, kas saistīti ar sniegto pakalpojumu, tostarp lietotāja pienākumus aizsargāt savu elektronisko identifikatoru, izdevēja pienākumus un atbildību, visas sniegtās un solītās pieejamības garantijas;

(d) informāciju par personas datu apstrādi un tās veikšanas veidu, un

(e) pasākumus, lai grozītu sniegtā pakalpojuma noteikumus vai citus nosacījumus, tostarp pasākumus, kas jāveic, lai pārtrauktu pakalpojumu kontrolētā veidā.

K5.4 **3. un 4. līmenis:** Zviedrijas eID izdevēji pēc Digitālās pārvaldības aģentūras (DIGG) vai citas līgumslēdzējas puses, kas paļaujas uz izdevēja sniegtajiem pakalpojumiem, pieprasījuma sniedz informāciju par to, kā uzņēmums tiek pārvaldīts un kam tas pieder.

K5.5 Zviedrijas eID izdevējs, kas pārtrauc savu darbību, ievēro iepriekš noteiktu plānu pakalpojuma pārtraukšanai. Plānā jāiekļauj visu pakalpojuma lietotāju un DIGG informēšanu. Izdevējs pēc darbības pārtraukšanas nodrošina arhivētā materiāla pieejamību saskaņā ar K2.7. un K2.8. punktu.

Pieteikuma iesniegšana

K5.6 Zviedrijas eID var izdot tikai pēc pieteikuma iesniedzēja pieprasījuma vai, izmantojot citu līdzvērtīgu pieņemšanas procedūru, un tikai pēc tam, kad pieteikuma iesniedzējs ir informēts par nosacījumiem, saskaņā ar kuriem tā tiek izdota, un par atbildību, kas viņam tiks uzlikta.

Tomēr eID, kas aizstāj vai papildina derīgu vai nesen bloķētu eID dokumentu, kuru iepriekš izdevis tas pats izdevējs, var izdot bez iepriekšējas pieteikšanās procedūras.

K5.7 Zviedrijas eID pieteikumam jābūt saistītam ar personas kodu vai koordinācijas numuru, kā arī ar informāciju, kas izdevējam citādi ir nepieciešama šāda eID izsniegšanai.

Pieteikuma iesniedzēja identitātes noteikšana

K5.8 Zviedrijas eID izdevējiem ir jāpārbauda, vai ar pieteikumu saistītā informācija ir pilnīga un atbilst informācijai, kas reģistrēta oficiālā reģistrā.

K5.9 Ja oficiālajā reģistrā pārbaudāmā informācija ir atzīmēta kā konfidenciāla ("aizsargāta identitāte"), vajadzīgās pārbaudes var veikt ar citiem līdzvērtīgiem līdzekļiem.

K5.10 Pieteikuma iesniedzēja identifikācija klātienes apmeklējuma laikā:

Zviedrijas eID izdevēji var pārbaudīt pieteikuma iesniedzēja identitāti klātienes apmeklējuma laikā tādā pašā veidā, kā izsniedzot standarta personu apliecinošu dokumentu.

K5.11 Pieteikuma iesniedzēja attālināta identifikācija pašreizējāsattiecībās:

3. līmenis: Zviedrijas eID izdevēji, kuri jau ir identificējuši pieteikuma iesniedzēju attiecībās, kas ietver ekonomiski vai juridiski nozīmīgus darījumus, un ja pieteikuma iesniedzēju var identificēt attālināti, izmantojot citus uzticamus līdzekļus, kas ir līdzvērtīgi Zviedrijas eID kvalitātes zīmes 3. līmeņa prasībām, var izmantot šo metodi, lai noteiktu pieteikuma iesniedzēja identitāti.

4. līmenis: Nepiemēro.

K5.12 Identifikācija, izmantojot Zviedrijas eID:

Zviedrijas eID izdevējs var attālināti identificēt pieteikuma iesniedzēju, izmantojot derīgu Zviedrijas eID, kam ir vismaz tāds pats uzticamības līmenis kā izsniedzamajai eID, ja tas bez līgumiskiem šķēršļiem var izmantot šādu identifikāciju kā pamatu jaunas eID izdošanai.

4. līmenis: Jaunizdotās eID derīguma termiņš nepārsniedz esošās eID derīguma termiņu.

K5.13 Pieteikuma iesniedzēja attālināta identifikācija:

2. līmenis: Zviedrijas eID izdevēji var izmantot ticamus derīga standarta personu apliecinoša dokumenta attēlu ierakstus un pieteikuma iesniedzēja sejas attēlu kā pamatu pieteikuma iesniedzēja identitātes attālinātai noteikšanai, ja salīdzinājums nerada šaubas par pieteikuma iesniedzēja patieso identitāti.

3. līmenis: Zviedrijas eID izdevēji, droši nolasot derīgu standarta identitātes dokumentu, kurā ir elektroniski uzglabāti biometriskie dati, var attālināti noteikt pieteikuma iesniedzēja identitāti, pamatojoties uz šiem datiem, ja attiecīgos identificējamās personas biometriskos datus var savākt pietiekami drošā veidā, lai varētu veikt salīdzināšanu ar līdzvērtīgu uzticamību kā klātienes apmeklējuma

gadījumā, un ja salīdzinājums nerada šaubas par pieteikuma iesniedzēja patieso identitāti.

4. līmenis: Nepiemēro.

Reģistrācija

K5.14 Zviedrijas eID izdevēji, ņemot vērā piemērojamos noteikumus par personas datu aizsardzību, uztur savienoto lietotāju un piešķirto elektroniskās identifikācijas dokumentu reģistru un regulāri atjaunina šo reģistru.

6. eID izdošana un bloķēšana

Tehnisko līdzekļu projektēšana

K6.1 Tehniskie līdzekļi:

2. un 3. līmenis: Tehniskos līdzekļus elektroniskai identifikācijai, izmantojot eID ar Zviedrijas eID kvalitātes zīmi, izstrādā saskaņā ar divfaktoru principu, saskaņā ar kuru vienu daļu veido elektroniski uzglabāta informācija, kas ir lietotāja rīcībā, bet otru daļu veido informācija, ko lietotājs izmanto, lai aktivizētu eID.

4. līmenis: Tehniskos līdzekļus elektroniskai identifikācijai, izmantojot eID ar Zviedrijas eID kvalitātes zīmi, izstrādā saskaņā ar divfaktoru principu, saskaņā ar kuru vienu daļu veido lietotāja rīcībā esošs personīgās drošības modulis, bet otru daļu veido tas, ko lietotājs izmantos, lai aktivizētu drošības moduli.

K6.2 Aktivizēšanas mehānisms un personalizētais kods ir konstruēti tā, ka ir maz ticams, ka trešās personas varētu pārkāpt aizsardzību, pat ar mehāniskiem līdzekļiem.

3. un 4. līmenis: Aizsardzība ietver mehānismus, lai novērstu elektroniskā identifikācijas dokumenta kopēšanu un manipulācijas ar to.

K6.3 eID lietotājiem ar Zviedrijas eID kvalitātes zīmi eID derīguma termiņa laikā pēc savas iniciatīvas bez maksas un bez ievērojamām neērtībām jābūt iespējai apmainīt vai pieprasīt jaunu personas kodu, un, izmantojot norādījumus vai automātisku sagatavošanu, viņiem jāpalīdz saglabāt K6.2. punkta prasības.

Ja eID ir izstrādāta tā, ka tā nevar apmainīties ar personalizētu kodu, lietotājam tā vietā ar tādiem pašiem nosacījumiem būtu nekavējoties jāspēj iegūt jaunu eID ar jaunu personalizētu kodu, kas aizstāj iepriekšējo kodu, izmantojot bloķēšanas procedūru.

K6.4 Zviedrijas eID izdevējiem jānodrošina, ka dati, kas reģistrēti turētāju elektroniskajai identifikācijai, unikāli pārstāv pieteikuma iesniedzēju un, izsniedzot eID dokumentu, tiek attiecināti uz attiecīgo personu.

K6.5 Izsniegto eID derīguma termiņu ierobežo, ņemot vērā eID dokumenta drošības elementus un ļaunprātīgas izmantošanas riskus. eID maksimālais derīguma termiņš ir pieci gadi.

Elektroniskās identifikācijas dokumenta nodrošināšana

K6.6 Neklātienes noteikums:

2. līmenis: Zviedrijas eID izdevējs nodrošina e-ID dokumentu tādā veidā, kas apstiprina oficiālajā reģistrā glabāto kontaktinformāciju vai šādu informāciju, kas reģistrēta saistībā ar elektronisko procedūru saskaņā ar K5.13 2. līmeni.

3. līmenis: Zviedrijas eID izdevējs, kas nodrošina eID, izmantojot elektronisku procedūru, kura atbilst K5.11 3. līmenim, K5.12 3. līmenim vai K5.13 3. līmenim, no jauna izdodot, atsevišķi un neatkarīgi no noteikuma par drošību nodrošina, ka lietotājs ir informēts, ka šāds e-ID dokuments ir nodots, vai ar citiem pasākumiem nodrošina līdzvērtīgu kontroles pakāpi, ka persona tiek brīdināta par identitātes zādzības risku saistībā ar noteikumu.

4. līmenis: Zviedrijas eID izdevējs, kas nodrošina eID, izmantojot elektronisku procedūru, kura atbilst K5.12 4. līmenim, no jauna izdodot, atsevišķi un neatkarīgi no drošības noteikuma nodrošina, ka lietotājs ir informēts par to, ka šāds eID dokuments ir nodots.

K6.7 Piedāvājums klātienes apmeklējuma laikā:

Zviedrijas eID izdevējs klātienes apmeklējuma laikā un pēc identitātes pārbaudes saskaņā ar K5.10. punktu izsniedz elektroniskās identifikācijas dokumentu apmaiņā pret parakstītu saņemšanas dokumentu un papildus nodrošina daļu, ko lietotājs izmanto, lai aktivizētu eID atsevišķi un neatkarīgi no eID dokumenta nodrošināšanas drošības ziņā, pamatojoties uz oficiālā reģistrā glabāto kontaktinformāciju vai citu līdzvērtīgas ticamības informāciju.

Bloķēšanas pakalpojums

K6.8 Zviedrijas eID izdevējiem ir jānodrošina bloķēšanas pakalpojums ar labu piekļūstamību, lai lietotājs varētu bloķēt savu eID.

K6.9 Zviedrijas eID izdevējiem nekavējoties un droši jāapstrādā un jāizpilda bloķēšanas pieprasījumi, kā arī jāveic pasākumi, lai novērstu bloķēšanas pakalpojuma sistemātisku ļaunprātīgu izmantošanu vai citas tīšas darbības, kas noved pie elektroniskās identifikācijas dokumentu plašas bloķēšanas, nodrošinot, ka lietotāju eID ir pieejamas, kad tās vajadzīgas

7. Turētāju elektronisko identitāšu verifikācija

K7.1 Zviedrijas eID izdevējiem ir jānodrošina, ka, pārbaudot turētāja identitāti, tiek veiktas uzticamas eID dokumenta autentiskuma un derīguma pārbaudes.

K7.2 Zviedrijas eID izdevējiem jānodrošina, ka, pārbaudot turētāju elektroniskās identitātes, ir ieviestas tehniskās drošības kontroles, lai būtu maz ticams, ka trešās personas, uzminot, noklausoties, atkārtojot vai manipulējot ar procesu, varētu pārkāpt aizsardzības mehānismus.

8. Identitātes apliecību izdošana

Zviedrijas eID izdevēji, kas sniedz pakalpojumu identitātes sertifikātu izdošanai uzticamajiem e-pakalpojumiem, ievēro arī šā panta noteikumus.

K8.1 Zviedrijas eID izdevējiem jānodrošina, ka identitātes sertifikātu izdošanas pakalpojumam ir laba pieejamība un ka pirms identitātes sertifikātu izdošanas tiek veikta uzticama identifikācija saskaņā ar 7. panta noteikumiem.

4. līmenis: Sertifikātos iekļauj atsauci uz kriptogrāfisko atslēgu materiālu, ko izdevējs verificējis kā tādu, kas ir vienīgi turētāja rīcībā.

K8.2 Iesniegtie identitātes sertifikāti ir derīgi tikai tik ilgi, cik nepieciešams, lai lietotājs varētu piekļūt pieprasītajam e-pakalpojumam, un tie ir aizsargāti tā, lai informāciju varētu izlasīt tikai paredzētais saņēmējs un lai sertifikātu saņēmēji varētu pārbaudīt sertifikātu autentiskumu.

K8.3 Zviedrijas eID izdevējiem, ņemot vērā sertifikācijas pakalpojuma ļaunprātīgas izmantošanas riskus, ir jāierobežo laikposms, kurā konkrētam turētājam var izdot vairākus secīgus identitātes sertifikātus, pirms turētājs tiek atkārtoti identificēts saskaņā ar 7. panta noteikumiem.