BYLOS NUMERIS: 2022-0941
KLASIFIKAVIMO ID: 3.2.3

Pasitikėjimo sistema

Švedijos el. identifikavimas

2022 m. spalio 4 d. redakcija

1. Bendroji informacija ir tikslas

Švedijos el. identifikavimo patikimumo užtikrinimo sistema siekiama nustatyti bendruosius reikalavimus elektroninių identifikatorių išdavėjams, kuriuos peržiūrėjo ir patvirtino Švedijos skaitmeninės valdžios agentūra (DIGG). Reikalavimai suskirstyti į skirtingus apsaugos lygius, vadinamus saugumo užtikrinimo lygiais, atitinkančius skirtingus išdavėjo techninio ir operacinio saugumo lygius ir skirtingus tikrinimo, ar asmuo, kuriam išduodamas elektroninio identifikavimo dokumentas, iš tikrųjų yra tas, kas jis teigia esąs, laipsnius.

Šios patikimumo sistemos reikalavimai taikomi 2-4 užtikrinimo lygiams, o 4 lygis atitinka aukščiausią apsaugos lygį.

Atitiktis aiškinama taip:

(a) jei užtikrinimo lygis nenurodytas, reikalavimas turi būti įvykdytas visais lygiais ir

(b) jei nustatytas saugumo užtikrinimo lygis, užtikrinama, kad būtų laikomasi bent atitinkamo lygio.

Neatsižvelgiama į reikalavimus, nustatytus žemesniam nei atitinkamas lygis.

2. Organizavimas ir valdymas

Bendrieji eksploataciniai reikalavimai

K2.1 Švedijos elektroninio identifikavimo priemonių išdavėjai, kurie nėra viešieji subjektai, turi veikti kaip registruoti juridiniai asmenys ir sudaryti bei palaikyti verslui reikalingą draudimą.

K2.2 Švedijos elektroninio identifikavimo priemonių išdavėjai turi turėti įsteigtą įmonę, visapusiškai veikti visose šiame dokumente nurodytose srityse ir gerai išmanyti teisinius reikalavimus, kurie jiems taikomi kaip Švedijos elektroninio identifikavimo priemonių išdavėjams.

K2.3 Švedijos elektroninio identifikavimo priemonių išdavėjai turi būti pajėgūs prisiimti atsakomybę už riziką dėl žalos ir turėti pakankamai finansinių išteklių savo veiklai vykdyti bent vienerius metus.

informacijos saugumas –

K2.4 Švedijos elektroninio identifikavimo priemonių išdavėjai savo veiklos dalims, kurioms taikoma patikimumo užtikrinimo sistema, turi būti įdiegę informacijos saugumo valdymo sistemą (ISVS), kuri, kai taikytina, grindžiama ISO/IEC 27001 arba lygiaverčiais informacijos saugumo valdymo ir kontrolės principais, įskaitant šiuos reikalavimus:

(a) visi saugai svarbūs administraciniai ir techniniai procesai turi būti įforminti dokumentais ir pagrįsti oficialiu pagrindu, kuriame aiškiai apibrėžtos funkcijos, atsakomybė ir įgaliojimai.

(b) Švedijos elektroninio identifikavimo priemonių išdavėjai užtikrina, kad jie visada turėtų pakankamai žmogiškųjų išteklių savo įsipareigojimams vykdyti.

(c) Švedijos elektroninio identifikavimo priemonių išdavėjai nustato rizikos valdymo procesą, per kurį tinkamu būdu, nuolat arba bent kas 12 mėnesių, analizuojamos grėsmės ir verslo pažeidžiamumas ir kuris, įvedus saugumo priemones, subalansuoja riziką iki priimtino lygio.

(d) Švedijos elektroninio identifikavimo priemonių išdavėjai nustato incidentų valdymo procesą, kuriuo sistemingai užtikrinama paslaugos kokybė, tolesnio pranešimo formos ir tai, kad būtų imamasi tinkamų atsakomųjų ir prevencinių priemonių siekiant sumažinti tokių įvykių daromą žalą arba užkirsti jai kelią.

(e) Švedijos elektroninio identifikavimo priemonių išdavėjai parengia ir reguliariai tikrina veiklos tęstinumo planą, kuris atitinka prieinamumo reikalavimus ir leidžia atkurti kritinius procesus krizės ar rimtų incidentų atveju.

(f) Švedijos elektroninio identifikavimo priemonių išdavėjai reguliariai vertina informacijos saugumo darbą ir įdiegia valdymo sistemos tobulinimo priemones.

K2.5 Valdymo sistemos taikymo sritis ir brandumas:

4 lygis: Informacijos saugumo valdymo sistema turi atitikti standartą SS-ISO/IEC 27001:2017 arba lygiavertes vėlesnes ar tarptautines standarto versijas, ir į jos taikymo sritį turi būti įtraukti visi Švedijos elektroninio identifikavimo priemonių išdavėjams nustatyti reikalavimai.

Subrangos sąlygos

K2.6 Švedijos elektroninio identifikavimo priemonių išdavėjas, kuris perdavė vieno ar daugiau saugumui svarbių procesų vykdymą kitai šaliai, sutartimi apibrėžia, už kuriuos svarbiausius procesus atsako subrangovas ir kokie reikalavimai jiems taikomi, taip pat paaiškina sutartinius santykius išdavėjo deklaracijoje.

Dokumentų atsekamumas, panaikinimas ir saugojimas

K2.7 Švedijos elektroninio identifikavimo priemonių išdavėjai saugo:

(a) prašymų dokumentus ir dokumentus, susijusius su elektroninio identifikavimo priemonės išdavimu, gavimu ar blokavimu;

(b) sutartis, politikos dokumentus ir išdavėjo deklaracijas; ir

(c) tvarkymo istoriją ir kitus dokumentus, kurių reikia siekiant įrodyti, kad laikomasi Švedijos elektroninio identifikavimo priemonių išavėjams nustatytų reikalavimų, ir kurie suteikia galimybę imtis tolesnių veiksmų, kuriais įrodoma, kad yra įdiegti ir veiksmingi saugumui itin svarbūs procesai ir kontrolės priemonės.

K2.8 Saugojimo laikotarpis turi būti ne trumpesnis kaip penkeri metai, o medžiagą turi būti įmanoma pateikti įskaitoma forma per visą šį laikotarpį, išskyrus atvejus, kai panaikinimo reikalavimas yra būtinas privatumo požiūriu ir yra pagrįstas įstatymais ar kitais teisės aktais.

Peržiūra ir tolesni veiksmai

K2.9 Švedijos elektroninio identifikavimo priemonių išdavėjai turi nustatyti vidaus audito funkciją, kuri periodiškai peržiūri išdavimo veiklą. Vidaus auditorius savo pareigas atlieka nepriklausomai, užtikrindamas objektyvią ir nešališką peržiūrą, ir turi savo pareigoms atlikti reikalingą kompetenciją ir patirtį. Vidaus auditorius savarankiškai planuoja audito atlikimą ir tai dokumentuoja audito plane, apimančiame trejų metų laikotarpį. Audito elementai atrenkami remiantis rizikos ir reikšmingumo analize ir Išdavėjo Skaitmeninės valdžios agentūrai pateiktais operacijų aprašais.

3 ir 4 lygiai: Vidaus auditas atliekamas remiantis pripažintais audito standartais.

3. Fizinis, administracinis ir į asmenį orientuotas saugumas

K3.1 Centrinės operacijos dalys turi būti fiziškai apsaugotos nuo žalos, kurią sukelia aplinkos įvykiai, neteisėta prieiga ar kiti išoriniai trikdžiai. Patekimo kontrolė taikoma taip, kad patekti į jautrias zonas galėtų tik įgalioti darbuotojai, kad būtų saugiai laikomos ir šalinamos informaciją pernešančios laikmenos ir kad patekimas į šias saugomas zonas būtų nuolat stebimas.

K3.2 Prieš asmeniui prisiimant bet kurį iš vaidmenų, nustatytų pagal K2.4 skirsnio a punktą ir kurie yra ypač svarbūs saugumui, Švedijos elektroninio identifikavimo priemonių išdavėjas turi atlikti asmens patikrinimą, kad įsitikintų, jog asmuo gali būti laikomas patikimu ir kad jis turi reikiamą kvalifikaciją ir išsilavinimą, kad galėtų saugiai ir patikimai atlikti susijusias užduotis pagal patikėtą vaidmenį.

K3.3 Išdavėjai nustato procedūras, kuriomis užtikrinama, kad prieigą prie pagal K2.7 surinktų ir saugomų duomenų turėtų tik specialiai įgalioti darbuotojai.

K3.4 **3 ir 4 lygiai:** Išdavėjai visoje išdavimo proceso grandinėje užtikrina, kad pareigos būtų atskirtos taip, kad nė vienas asmuo negalėtų gauti elektroninio identifikavimo priemonės kito asmens vardu.

4. Techninis saugumas

K4.1 Švedijos elektroninio identifikavimo priemonių išdavėjai užtikrina, kad taikomos techninės kontrolės priemonės būtų pakankamos, kad būtų pasiektas apsaugos lygis, laikomas būtinu atsižvelgiant į verslo pobūdį, aprėptį ir kitas aplinkybes, ir kad šios kontrolės priemonės veiktų ir būtų veiksmingos.

K4.2 Perduodant neskelbtinus duomenis naudojamos elektroninės ryšio priemonės turi būti apsaugotos nuo perėmimo, manipuliavimo ir pakartotinio perdavimo.

K4.3 Jautri kriptografinė raktų medžiaga, naudojama elektroninio identifikavimo priemonėms išduoti, turėtojams identifikuoti ir tapatybės pažymėjimams išduoti, turi būti apsaugota taip, kad:

(a) būtų ribojama prieiga, logiškai ir fiziškai, tik prie tų funkcijų ir taikomųjų programų, kurios yra griežtai būtinos;

(b) raktų medžiaga niekada nebūtų saugoma paprastu tekstu nuolatinėse laikmenose;

(c) raktų medžiaga būtų apsaugota naudojant kriptografinės aparatinės įrangos modulį su aktyviais apsaugos mechanizmais, kurie neutralizuoja fizinius ir loginius bandymus pakenkti raktų medžiagai;

(d) raktų medžiagos apsaugos saugumo mechanizmai būtų skaidrūs ir pagrįsti pripažintais ir nusistovėjusiais standartais; ir

(e) **3 ir 4 lygiai:** aktyvinimo duomenys, skirti raktų medžiagos apsaugai, valdomi naudojant kelių asmenų kontrolę.

K4.4 Išdavėjai privalo turėti dokumentuotas procedūras, kuriomis užtikrinama, kad reikiamas apsaugos lygis atitinkamoje IT aplinkoje galėtų būti išlaikytas laikui bėgant ir atsižvelgiant į pokyčius, įskaitant reguliarius pažeidžiamumo vertinimus, ir tinkamą pasirengimą reaguoti į kintančius rizikos lygius ir įvykusius incidentus.

5. Paraiška, identifikavimas ir registravimas

Informacija apie sąlygas

K5.1 Švedijos elektroninio identifikavimo priemonių išdavėjai teikia informaciją apie sutartis, nuostatas ir sąlygas, taip pat susijusią informaciją ir bet kokius naudojimosi paslauga apribojimus susietiesiems naudotojams, elektroninių paslaugų teikėjams ir kitiems asmenims, kurie gali pasikliauti išdavėjo paslauga.

K5.2 Švedijos elektroninio identifikavimo priemonių išdavėjas aiškiai nurodo sąlygas ir parengia procedūras taip, kad per išdavimo procesą sąlygos būtų pateiktos pareiškėjui.

K5.3 Švedijos elektroninio identifikavimo priemonių išdavėjai pateikia išdavėjo deklaraciją, kurioje nurodoma:

(a) išdavėjo tapatybė ir kontaktiniai duomenys;

(b) trumpi išdavėjo teikiamų paslaugų ir sprendimų aprašai, įskaitant taikomus taikymo, išleidimo ir blokavimo metodus;

(c) sąlygos, susijusios su teikiama paslauga, įskaitant naudotojo pareigas apsaugoti savo elektroninį tapatybės dokumentą, išdavėjo pareigas ir atsakomybę, visas suteiktas garantijas ir žadamą prieinamumą;

(d) informacija apie asmens duomenų tvarkymą ir jo vykdymo būdą; ir

(e) susitarimai dėl teikiamos paslaugos sąlygų ar kitų sąlygų pakeitimo, įskaitant veiksmus, kurių reikia imtis siekiant kontroliuojamu būdu nutraukti paslaugos teikimą.

K5.4 **3 ir 4 lygiai:** Švedijos elektroninio identifikavimo priemonių išdavėjai Skaitmeninės valdžios agentūros (DIGG) arba kitos susitariančiosios šalies, kuri remiasi išdavėjo teikiamomis paslaugomis, prašymu pateikia informaciją apie tai, kaip įmonė yra valdoma ir kam ji priklauso.

K5.5 Švedijos elektroninio identifikavimo priemonių išdavėjas, kuris nutraukia savo veiklą, laikosi iš anksto nustatyto paslaugos nutraukimo plano. Plane turi būti numatyta informuoti visus paslaugos naudotojus ir DIGG. Nutraukęs veiklą, išdavėjas toliau saugo archyvuotą medžiagą, prieinamą pagal K2.7 ir K2.8.

Taikymo sritis

K5.6 Švedijos elektroninio identifikavimo priemonė gali būti išduodama tik prašytojo prašymu arba taikant kitą lygiavertę priėmimo procedūrą ir tik po to, kai prašytojui pranešama apie jos išdavimo sąlygas ir atsakomybę, kuri jam bus nustatyta.

Nepaisant to, elektroninio identifikavimo priemonė, kuria pakeičiamas arba papildomas galiojantis arba neseniai užblokuotas to paties išdavėjo anksčiau išduotas elektroninio identifikavimo dokumentas, gali būti išduodama be jokios išankstinės paraiškos teikimo procedūros.

K5.7 Paraiška dėl Švedijos elektroninio identifikavimo priemonės turi būti susieta su asmens tapatybės numeriu arba koordinavimo numeriu, taip pat su informacija, kuri kitu atveju reikalinga, kad išdavėjas galėtų suteikti tokią elektroninio identifikavimo priemonę.

Pareiškėjo tapatybės nustatymas

K5.8 Švedijos elektroninio identifikavimo priemonių išdavėjai turi patikrinti, ar su paraiška susijusi informacija yra išsami ir atitinka oficialiame registre užregistruotą informaciją.

K5.9 Jei oficialiame registre tikrintina informacija pažymėta kaip konfidenciali („saugoma tapatybė“), būtinus patikrinimus galima atlikti kitomis lygiavertėmis priemonėmis.

K5.10 Prašytojo tapatybės nustatymas per tiesioginį vizitą:

Švedijos elektroninio identifikavimo priemonių išdavėjai gali patikrinti pareiškėjo tapatybę per tiesioginį vizitą taip pat, kaip išduodami standartinį tapatybės dokumentą.

K5.11 Prašytojo nuotolinis identifikavimas esamuosesantykiuose:

3 lygis: Švedijos elektroninio identifikavimo priemonių išdavėjai, kurie jau identifikavo pareiškėją ekonomiškai ar teisiškai svarbiuose sandoriuose ir kai pareiškėją galima identifikuoti nuotoliniu būdu kitomis patikimomis priemonėmis, lygiavertėmis Švedijos elektroninio identifikavimo kokybės ženklo 3 lygio reikalavimams, gali naudoti šį metodą pareiškėjo tapatybei nustatyti.

4 lygis: Netaikoma.

K5.12 Tapatybės nustatymas naudojant Švedijos elektroninio identifikavimo priemonę:

Švedijos elektroninio identifikavimo priemonių išdavėjas gali nuotoliniu būdu nustatyti pareiškėjo tapatybę naudodamas galiojančią Švedijos elektroninio identifikavimo priemonę, kurios saugumo užtikrinimo lygis yra bent toks pat kaip išduodamos elektroninio identifikavimo priemonės, jeigu jis gali be sutartinių kliūčių naudoti tokią identifikavimo priemonę naujai elektroninio identifikavimo priemonei išduoti.

4 lygis: Naujai išduotos elektroninio identifikavimo priemonės galiojimo laikotarpis turi būti ne ilgesnis nei esamos elektroninio identifikavimo priemonės galiojimo laikotarpis.

K5.13 Prašytojo nuotolinis identifikavimas:

2 lygis: Švedijos elektroninio identifikavimo priemonių išdavėjai gali naudoti patikimus galiojančio standartinio asmens tapatybės dokumento vaizdo įrašus ir pareiškėjo veido atvaizdą kaip pagrindą pareiškėjo tapatybei nuotoliniu būdu nustatyti, jei atlikus palyginimą nekyla abejonių dėl pareiškėjo tikrosios tapatybės.

3 lygis: Švedijos elektroninio identifikavimo priemonių išdavėjai, saugiai nuskaitydami galiojantį standartinį tapatybės dokumentą, kuriame yra elektroniniu

būdu saugomų biometrinių duomenų, remdamiesi tais duomenimis gali nuotoliniu būdu nustatyti prašytojo tapatybę, jei atitinkamus asmens, kurio tapatybė turi būti nustatyta, biometrinius duomenis galima surinkti pakankamai saugiai, kad palyginimą būtų galima atlikti taip pat patikimai, kaip ir tiesioginio apsilankymo atveju, ir jei palyginus duomenis nekyla abejonių dėl prašytojo tikrosios tapatybės.

4 lygis: Netaikoma.

Registracija

K5.14 Švedijos elektroninio identifikavimo priemonių išdavėjai, atsižvelgdami į taikytinas asmens duomenų apsaugos taisykles, tvarko susietųjų naudotojų ir paskirtų elektroninio identifikavimo dokumentų registrą ir jį atnaujina.

6. Elektroninio identifikavimo priemonių išdavimas ir blokavimas

Techninių priemonių projektavimas

K6.1 Techninės priemonės:

2 ir 3 lygiai: Elektroninio identifikavimo naudojant elektroninio identifikavimo priemones su Švedijos eID kokybės ženklu techninės priemonės projektuojamos laikantis dviejų veiksnių principo, pagal kurį vieną dalį sudaro elektroniniu būdu saugoma informacija, kurią turi turėti naudotojas, o kitą dalį sudaro tai, ką naudotojas turi naudoti, kad aktyvuotų elektroninio identifikavimo priemonę.

4 lygis: Elektroninio identifikavimo naudojant elektroninio identifikavimo priemonę su Švedijos eID kokybės ženklu techninės priemonės projektuojamos laikantis dviejų veiksnių principo, pagal kurį vieną dalį sudaro asmeninis saugumo modulis, kurį turi turėti naudotojas, o kitą dalį sudaro tai, ką naudotojas turi naudoti saugumo moduliui aktyvuoti.

K6.2 Aktyvavimo mechanizmas ir suasmenintas kodas turi būti suprojektuoti taip, kad trečiosioms šalims būtų mažai tikėtina pažeisti apsaugą net mechaninėmis priemonėmis.

3 ir 4 lygiai: Apsauga apima mechanizmus, kuriais užkertamas kelias siekiant kopijuoti ir manipuliuoti elektroninio identifikavimo dokumentu.

K6.3 Švedijos elektroninio identifikavimo kokybės ženklu pažymėtos elektroninio identifikavimo priemonės naudotojai turi turėti galimybę savo iniciatyva elektroninio identifikavimo priemonės galiojimo laikotarpiu nemokamai ir nepatirdami didelių nepatogumų pasikeisti arba prašyti naujo asmens kodo ir, naudodamiesi gairėmis arba automatiniu pateikimu, jiems turi būti padedama laikytis K6.2 punkto reikalavimų.

Jei elektroninio identifikavimo priemonė sukurta taip, kad negalima keistis suasmenintu kodu, naudotojas tokiomis pačiomis sąlygomis turėtų turėti galimybę nedelsdamas gauti naują elektroninio identifikavimo priemonę su nauju suasmenintu kodu, kuriuo būtų pakeistas ankstesnis kodas, taikant blokavimo procedūrą.

K6.4 Švedijos elektroninio identifikavimo priemonės išdavėjai turi užtikrinti, kad elektroniniam identifikavimui užregistruoti turėtojų duomenys unikaliai atspindėtų pareiškėją ir būtų priskirti atitinkamam asmeniui išduodant elektroninio identifikavimo priemonės dokumentą.

K6.5 Išduotų elektroninio identifikavimo priemonių galiojimo laikotarpis ribojamas atsižvelgiant į elektroninio identifikavimo dokumento saugumo ypatybes ir netinkamo naudojimo riziką. Ilgiausias elektroninio identifikavimo priemonės galiojimo laikotarpis yra penkeri metai.

Elektroninio identifikavimo dokumento pateikimas

K6.6 Nuotolinis teikimas:

2 lygis: Švedijos elektroninio identifikavimo priemonių išdavėjas pateikia elektroninio- identifikavimo dokumentą, kuriuo patvirtinami oficialiame registre saugomi kontaktiniai duomenys arba tokia informacija, užregistruota atliekant elektroninę procedūrą pagal K5.13 2 lygį.

3 lygis: Švedijos elektroninio identifikavimo priemonių išdavėjas, kuris elektroninio identifikavimo priemonę suteikia taikydamas elektroninę procedūrą, atitinkančią K5.11 3 lygio, K5.12 3 lygio arba K5.13 3 lygio reikalavimus, naujai išduodamas atskirai ir nepriklausomai nuo nuostatos dėl saugumo užtikrina, kad naudotojas būtų informuotas, jog toks elektroninio- identifikavimo dokumentas buvo perduotas, arba kitomis priemonėmis užtikrina lygiavertę kontrolę, kad asmuo būtų įspėtas apie tapatybės vagystės riziką, susijusią su šia nuostata.

4 lygis: Švedijos elektroninio identifikavimo priemonių, suteikiančių elektroninio identifikavimo priemonę taikant elektroninę procedūrą, atitinkančią K5.12 4 lygį, išdavėjas, naujai išduodamas, atskirai ir nepriklausomai nuo nuostatos dėl saugumo, užtikrina, kad naudotojas būtų informuotas apie tokio elektroninio identifikavimo dokumento perdavimą.

K6.7 Per tiesioginį vizitą teikiama:

Švedijos elektroninio identifikavimo priemonių išdavėjas per tiesioginį vizitą ir po tapatybės patikrinimo pagal K5.10 pateikia elektroninio identifikavimo dokumentą su pasirašytu gavimu ir papildomai pateikia dalį, kurią naudotojas naudoja elektroninio identifikavimo priemonei aktyvuoti atskirai ir nepriklausomai nuo elektroninio identifikavimo dokumento pateikimo saugumo požiūriu, remdamasis oficialiame registre saugomais kontaktiniais duomenimis arba kita lygiaverčio patikimumo informacija.

Blokavimo paslauga

K6.8 Švedijos elektroninio identifikavimo priemonių išdavėjai turi teikti blokavimo paslaugą, kuri būtų gerai prieinama naudotojui, kad jis galėtų blokuoti savo elektroninio identifikavimo priemonę.

K6.9 Švedijos elektroninio identifikavimo priemonių išdavėjai nedelsdami ir saugiai tvarko ir vykdo blokavimo prašymus ir imasi priemonių, kad užkirstų kelią sistemingam netinkamam blokavimo paslaugos naudojimui ar kitiems tyčiniams veiksmams, dėl kurių plačiai blokuojami elektroninio identifikavimo dokumentai, užtikrinant, kad prireikus būtų galima naudotis naudotojų elektroninio identifikavimo priemonėmis

7. Turėtojų elektroninės tapatybės tikrinimas

K7.1 Švedijos elektroninio identifikavimo priemonių išdavėjai užtikrina, kad tikrinant turėtojo tapatybę būtų atliekami patikimi elektroninio identifikavimo dokumento autentiškumo ir galiojimo patikrinimai.

K7.2 Švedijos elektroninio identifikavimo priemonių išdavėjai užtikrina, kad tikrinant turėtojų elektronines tapatybes būtų įgyvendintos techninės saugumo kontrolės priemonės, siekiant sumažinti tikimybę, jog trečiosios šalys, atspėdamos, pasiklausydamos, pakartodamos ar manipuliuodamos procesu, galėtų pažeisti apsaugos mechanizmus.

8. Tapatybės sertifikatų išdavimas

Švedijos elektroninio identifikavimo priemonių išdavėjai, teikiantys tapatybės sertifikatų išdavimo paslaugą pasitikimui elektroninėmis paslaugomis, taip pat laikosi šio skirsnio nuostatų.

K8.1 Švedijos elektroninio identifikavimo priemonių išdavėjai užtikrina, kad tapatybės sertifikatų išdavimo paslauga būtų tinkamai prieinama ir kad prieš išduodant tapatybės sertifikatus būtų atliekamas patikimas tapatybės nustatymas pagal 7 skirsnio nuostatas.

4 lygis: Sertifikatuose pateikiama nuoroda į kriptografinę raktų medžiagą, kurią, kaip patikrino išdavėjas, turi tik turėtojas.

K8.2 Pateikti tapatybės sertifikatai galioja tik tiek laiko, kiek būtina, kad naudotojas galėtų prieiti prie prašomos elektroninės -paslaugos, ir yra apsaugoti taip, kad informaciją galėtų perskaityti tik numatytas gavėjas ir kad sertifikatų gavėjai galėtų patikrinti sertifikatų autentiškumą.

K8.3 Švedijos elektroninio identifikavimo priemonių išdavėjai, atsižvelgdami į piktnaudžiavimo sertifikavimo paslauga riziką, apriboja laikotarpį, per kurį konkrečiam turėtojui gali būti išduoti keli vienas po kito einantys tapatybės sertifikatai, kol pagal 7 skirsnio nuostatas iš naujo nustatoma turėtojo tapatybė.