ČÍSLO SPISU: 2022-0941
ID KLASIFIKÁCIE: 3.2.3

Rámec dôvery

pre švédsku elektronickú identifikáciu

Verzia z 04. októbra 2022

1. Súvislosti a účel

Cieľom rámca dôvery pre švédsku elektronickú identifikáciu je stanoviť spoločné požiadavky na vydavateľov elektronických identifikácií, ktoré preskúma a schváli Švédska agentúra pre digitálnu správu (DIGG). Požiadavky sú rozdelené do rôznych úrovní ochrany – známych ako úrovne zabezpečenia –, ktoré zodpovedajú rôznym stupňom technickej a prevádzkovej bezpečnosti na strane vydavateľa a rôznym stupňom overenia, že osoba, ktorej je elektronický identifikačný dokument vydaný, je skutočne osobou, za ktorú sa vydáva.

Požiadavky tohto rámca dôvery sa vzťahujú na úrovne zabezpečenia 2 až 4, pričom úroveň 4 zodpovedá najvyššej úrovni ochrany.

Súlad sa vykladá takto:

(a) ak úroveň zabezpečenia nie je špecifikovaná, požiadavka musí byť splnená na všetkých úrovniach a

(b) ak je úroveň zabezpečenia stanovená, súlad sa zabezpečí aspoň na príslušnej úrovni.

Požiadavky stanovené pre nižšiu úroveň, ako je príslušná úroveň, sa neberú do úvahy.

2. Organizácia a riadenie

Celkové prevádzkové požiadavky

K2.1 Vydavatelia švédskych elektronických identifikácií, ktorí nie sú verejnými orgánmi, musia pôsobiť ako registrované právnické osoby a musia uzatvoriť a udržiavať poistenie potrebné na podnikanie.

K2.2 Vydavatelia švédskych elektronických identifikácií musia mať etablovanú podnikateľskú činnosť, musia byť plne funkční vo všetkých častiach uvedených v tomto dokumente a musia byť dobre oboznámení s právnymi požiadavkami, ktoré sa na nich ako na vydavateľov švédskych elektronických identifikácií kladú.

K2.3 Vydavatelia švédskych elektronických identifikácií musia byť schopní niesť riziko zodpovednosti za škody a musia mať dostatočné finančné zdroje na vykonávanie svojich činností aspoň jeden rok.

Informačná bezpečnosť

K2.4 Vydavatelia švédskych elektronických identifikácií musia mať zavedený systém riadenia informačnej bezpečnosti (ISMS) pre tie časti svojich činností, na ktoré sa vzťahuje rámec dôvery, ktorý je v prípade potreby založený na norme ISO/IEC 27001 alebo rovnocenných zásadách riadenia a kontroly práce v oblasti informačnej bezpečnosti, vrátane tohto:

(a) Všetky administratívne a technické procesy kritické z hľadiska bezpečnosti musia byť zdokumentované a založené na formálnom základe, v ktorom sú jasne vymedzené úlohy, zodpovednosti a právomoci.

(b) Vydavatelia švédskych elektronických identifikácií zabezpečia, aby mali vždy dostatok ľudských zdrojov na plnenie svojich povinností.

(c) Vydavatelia švédskych elektronických identifikácií zavedú proces riadenia rizík, ktorým sa primeraným spôsobom priebežne alebo aspoň každých 12 mesiacov analyzujú hrozby a zraniteľné miesta v podniku a ktorým sa zavedením bezpečnostných opatrení vyvažuje riziko na prijateľnú úroveň.

(d) Vydavatelia švédskych elektronických identifikácií zavedú proces riadenia incidentov, ktorým sa systematicky zabezpečí kvalita služby, formy následného nahlasovania a prijatie vhodných reaktívnych a preventívnych opatrení na zmiernenie škôd alebo predchádzanie škodám vyplývajúcim z takýchto udalostí.

(e) Vydavatelia švédskych elektronických identifikácií musia vypracovať a pravidelne testovať plán na zabezpečenie kontinuity, ktorý spĺňa požiadavky podniku na prístupnosť prostredníctvom schopnosti obnoviť kritické procesy v prípade krízy alebo závažných incidentov.

(f) Vydavatelia švédskych elektronických identifikácií pravidelne vyhodnocujú prácu v oblasti informačnej bezpečnosti a zavádzajú opatrenia na zlepšenie systému riadenia.

K2.5 Rozsah a vyspelosť systému riadenia:

Úroveň 4: Systém riadenia informačnej bezpečnosti musí byť v súlade s normou SS-ISO/IEC 27001:2017 alebo rovnocennými následnými alebo medzinárodnými verziami normy a v rámci rozsahu tejto normy musí zahŕňať všetky požiadavky uložené vydavateľom švédskych elektronických identifikácií.

Podmienky pre subdodávateľov

K2.6 Vydavateľ švédskych elektronických identifikácií, ktorý externe zadal vykonávanie jedného alebo viacerých procesov kritických z hľadiska bezpečnosti inej strane, zmluvne vymedzí, za ktoré kritické procesy je subdodávateľ zodpovedný a ktoré požiadavky sa na ne vzťahujú, a objasní zmluvný vzťah vo vyhlásení vydavateľa.

Vysledovateľnosť, vymazanie a uchovávanie dokumentov

K2.7 Vydavatelia švédskych elektronických identifikácií musia uchovávať:

(a) dokumenty súvisiace so žiadosťou a dokumenty týkajúce sa vydávania, prijímania alebo blokovania elektronických identifikácií;

(b) zmluvy, dokumenty o politike a vyhlásenia vydavateľa a

(c) históriu spracovania a inú dokumentáciu, ktorá sa vyžaduje na preukázanie súladu s požiadavkami uloženými na vydavateľov švédskych elektronických identifikácií a ktorá umožňuje následné opatrenia, ktorými sa preukazuje zavedenie a účinnosť procesov a kontrol kritických z hľadiska bezpečnosti.

K2.8 Obdobie uchovávania nesmie byť kratšie ako päť rokov a materiál musí byť možné vyhotoviť v čitateľnej forme počas celého tohto obdobia, pokiaľ nie je požiadavka na vymazanie potrebná z hľadiska ochrany súkromia a nie je podporená zákonom alebo iným predpisom.

Preskúmanie a následné opatrenia

K2.9 Vydavatelia švédskych elektronických identifikácií zriadia funkciu vnútorného auditu, ktorou sa pravidelne preskúmavajú činnosti vydávania. Vnútorný audítor musí byť pri výkone svojich povinností nezávislý spôsobom, ktorým sa zabezpečuje objektívne a nestranné preskúmanie, a musí mať odbornú spôsobilosť a skúsenosti potrebné na výkon svojich povinností. Vnútorný audítor musí nezávisle naplánovať vykonávanie auditu a zdokumentovať to v pláne auditu na obdobie troch rokov. Prvky auditu sa vyberajú na základe analýzy rizík a významnosti a vychádzajú z opisov operácií, ktoré vydavateľ predložil Agentúre pre digitálnu správu.

Úrovne 3 a 4: Vnútorný audit sa vykonáva na základe uznávaných audítorských štandardov.

3. Fyzická, administratívna a personálna bezpečnosť

K3.1 Centrálne časti prevádzky musia byť fyzicky chránené pred poškodením v dôsledku environmentálnych udalostí, neoprávneného prístupu alebo iných vonkajších narušení. Kontrola prístupu sa uplatňuje tak, aby sa prístup do citlivých oblastí obmedzil na oprávnený personál, aby sa médiá prenášajúce informácie bezpečne uchovávali a likvidovali a aby sa prístup do týchto chránených oblastí neustále monitoroval.

K3.2 Skôr ako osoba prevezme ktorúkoľvek z úloh určených v súlade s bodom K2.4 písm. a), ktoré majú osobitný význam pre bezpečnosť, vydavateľ švédskych elektronických identifikácií vykoná previerku osoby s cieľom zabezpečiť, aby sa osoba mohla považovať za spoľahlivú a aby mala kvalifikáciu a odbornú prípravu potrebnú na bezpečné a spoľahlivé vykonávanie úloh vyplývajúcich z tejto úlohy.

K3.3 Vydavatelia musia mať zavedené postupy na zabezpečenie toho, aby k údajom zhromaždeným a uchovávaným v súlade s bodom K2.7 mali prístup len osobitne oprávnení zamestnanci.

K3.4 **Úrovne 3 a 4:** Vydavatelia zabezpečia, aby sa v celom reťazci procesu vydávania uplatňovalo oddelenie povinností tak, aby žiadna osoba nebola schopná získať elektronickú identifikáciu v mene inej osoby.

4. Technická bezpečnosť

K4.1 Vydavatelia švédskej elektronickej identifikácie zabezpečia, aby zavedené technické kontroly boli dostatočné na dosiahnutie úrovne ochrany, ktorá sa považuje za potrebnú vzhľadom na povahu, rozsah a iné okolnosti podnikania, a aby tieto kontroly fungovali a boli účinné.

K4.2 Elektronické komunikačné prostriedky používané pri prenose citlivých údajov musia byť chránené pred odpočúvaním, manipuláciou a opakovaným prehrávaním.

K4.3 Citlivý kryptografický kľúčový materiál používaný na vydávanie elektronických identifikácií, identifikáciu držiteľov a vydávanie certifikátov identity musí byť chránený tak, aby:

(a) bol prístup logicky a fyzicky obmedzený na úlohy a aplikácie, ktoré sú striktne nevyhnutné;

(b) kľúčový materiál nikdy nebol uložený ako obyčajný text na trvalých pamäťových médiách;

(c) bol kľúčový materiál chránený použitím kryptografického hardvérového modulu s aktívnymi bezpečnostnými mechanizmami, ktoré bránia fyzickým aj logickým pokusom o ohrozenie kľúčového materiálu;

(d) boli bezpečnostné mechanizmy na ochranu kľúčového materiálu transparentné a založené na uznávaných a zavedených normách a

(e) **Úrovne 3 a 4:** aktivačné údaje na ochranu kľúčového materiálu sa spravovali prostredníctvom kontroly viacerých osôb.

K4.4 Vydavatelia musia mať zavedené zdokumentované postupy na zabezpečenie zachovania požadovanej úrovne ochrany v príslušnom IT prostredí v priebehu času a v súvislosti so zmenami vrátane pravidelných posúdení zraniteľnosti a primeranej pripravenosti na zvládnutie meniacich sa úrovní rizika a incidentov, ktoré sa vyskytnú.

5. Žiadosť, identifikácia a registrácia

Informácie o podmienkach

K5.1 Vydavatelia švédskych elektronických identifikácií poskytujú informácie o zmluvách, podmienkach, ako aj súvisiace informácie a akékoľvek obmedzenia používania služby pripojeným používateľom, poskytovateľom elektronických služieb a iným osobám, ktoré sa môžu spoliehať na službu vydavateľa.

K5.2 Vydavateľ švédskych elektronických identifikácií musí jasne uviesť podmienky a navrhnúť postupy tak, aby sa podmienky poskytli žiadateľovi v procese vydávania.

K5.3 Vydavatelia švédskych elektronických identifikácií musia poskytnúť vyhlásenie vydavateľa, ktoré obsahuje:

(a) identitu a kontaktné údaje vydavateľa;

(b) stručný opis služieb a riešení poskytovaných vydavateľom vrátane uplatnených metód na uplatňovanie, vydávanie a blokovanie;

(c) podmienky spojené s poskytovanou službou vrátane povinností používateľa chrániť svoju elektronickú identifikáciu, povinností a zodpovedností vydavateľa, všetkých poskytnutých záruk a sľúbenej dostupnosti;

(d) informácie o spracúvaní osobných údajov a spôsobe, akým sa vykonáva a

(e) opatrenia na zmenu podmienok alebo iných podmienok poskytovanej služby vrátane krokov, ktoré sa majú prijať na ukončenie služby kontrolovaným spôsobom.

K5.4 **Úrovne 3 a 4:** Vydavatelia švédskej elektronickej identifikácie poskytnú na žiadosť Agentúry pre digitálnu správu (DIGG) alebo inej zmluvnej strany, ktorá využíva služby poskytované vydavateľom, informácie o tom, ako je podnik vlastnený a riadený.

K5.5 Vydavateľ švédskych elektronických identifikácií, ktorý ukončí svoju činnosť, sa musí riadiť vopred stanoveným plánom na ukončenie služby. Plán zahŕňa informovanie všetkých používateľov služby a DIGG. Vydavateľ po ukončení musí ďalej uchovávať archivovaný materiál dostupný v súlade s K2.7 a K2.8.

Uplatňovanie

K5.6 Švédska elektronická identifikácia sa môže vydať len na žiadosť žiadateľa alebo prostredníctvom iného rovnocenného postupu prijatia a len po tom, ako bol žiadateľ oboznámený s podmienkami, za ktorých sa vydáva, a so zodpovednosťou, ktorá mu bude uložená.

Vydanie elektronickej identifikácie, ktorá nahrádza alebo dopĺňa platný alebo nedávno zablokovaný doklad o elektronickej identifikácii, ktorý predtým vydal ten istý vydavateľ, sa však môže uskutočniť bez akéhokoľvek predchádzajúceho postupu podávania žiadosti.

K5.7 Žiadosť o švédsku elektronickú identifikáciu musí byť spojená s osobným identifikačným číslom alebo koordinačným číslom, ako aj s informáciami, ktoré sú inak potrebné na to, aby vydavateľ poskytol takúto elektronickú identifikáciu.

Určenie identity žiadateľa

K5.8 Vydavatelia švédskych elektronických identifikácií musia overiť, či sú informácie súvisiace so žiadosťou úplné a či zodpovedajú informáciám zaregistrovaným v úradnom registri.

K5.9 Ak sú informácie, ktoré sa majú skontrolovať v úradnom registri, označené ako dôverné („chránená identita“), potrebné kontroly sa môžu vykonať inými rovnocennými prostriedkami.

K5.10 Identifikácia žiadateľa počas osobnej návštevy:

Vydavatelia švédskych elektronických identifikácií môžu overiť identitu žiadateľa počas osobnej návštevy rovnakým spôsobom ako pri vydávaní štandardného identifikačného dokumentu.

K5.11 Diaľková identifikácia žiadateľa v existujúcom vzťahu:

Úroveň 3: Vydavatelia švédskych elektronických identifikácií, ktorí už identifikovali žiadateľa vo vzťahu zahŕňajúcom ekonomicky alebo právne významné transakcie, a ak možno žiadateľa identifikovať na diaľku inými spoľahlivými prostriedkami rovnocennými s požiadavkami švédskej značky kvality elektronických identifikácií úrovne 3, môžu túto metódu použiť na zistenie identity žiadateľa.

Úroveň 4: Neuplatňuje sa.

K5.12 Identifikácia prostredníctvom švédskej elektronickej identifikácie:

Vydavateľ švédskych elektronických identifikácií môže identifikovať žiadateľa na diaľku prostredníctvom existujúcej platnej švédskej elektronickej identifikácie aspoň na rovnakej úrovni zabezpečenia, ako je tá, ktorá sa má vydať, ak môže bez zmluvných prekážok použiť takúto identifikáciu ako základ na vydanie novej elektronickej identifikácie.

Úroveň 4: Obdobie platnosti novovydanej elektronickej identifikácie je obmedzené tak, aby nepresahovalo obdobie platnosti existujúcej elektronickej identifikácie.

K5.13 Diaľková identifikácia žiadateľa:

Úroveň 2: Vydavatelia švédskych elektronických identifikácií môžu používať spoľahlivé obrazové záznamy platného štandardného identifikačného dokumentu a podobu tváre žiadateľa ako základ na zistenie identity žiadateľa na diaľku, ak porovnanie nevyvoláva pochybnosti o skutočnej identite žiadateľa.

Úroveň 3: Vydavatelia švédskych elektronických identifikácií môžu prostredníctvom zabezpečeného čítania platného štandardného identifikačného

dokumentu obsahujúceho elektronicky uchovávané biometrické údaje zistiť identitu žiadateľa na diaľku na základe týchto údajov, ak zodpovedajúce biometrické údaje osoby, ktorá sa má identifikovať, možno získať dostatočne bezpečným spôsobom, aby sa porovnanie mohlo vykonať s rovnakou spoľahlivosťou ako v prípade osobnej návštevy, a ak porovnanie nevyvoláva pochybnosti o skutočnej identite žiadateľa.

Úroveň 4: Neuplatňuje sa.

Registrácia

K5.14 Vydavatelia švédskych elektronických identifikácií vedú register pripojených používateľov a pridelených dokumentov elektronickej identifikácie a tento register aktualizujú, pričom zohľadňujú platné pravidlá ochrany osobných údajov.

6. Vydávanie a blokovanie elektronických identifikácií

Návrh technických prostriedkov

K6.1 Technické prostriedky:

Úrovne 2 a 3: Technické prostriedky elektronickej identifikácie prostredníctvom elektronickej identifikácie so švédskou značkou kvality elektronických identifikácií sa navrhujú podľa dvojfaktorovej zásady, pričom jedna časť pozostáva z elektronicky uchovávaných informácií, ktoré musí mať používateľ, a druhá časť pozostáva z toho, čo musí používateľ použiť na aktiváciu elektronickej identifikácie.

Úroveň 4: Technické prostriedky elektronickej identifikácie prostredníctvom elektronickej identifikácie so švédskou značkou kvality elektronických identifikácií sa navrhujú podľa dvojfaktorovej zásady, pričom jedna časť pozostáva z osobného bezpečnostného modulu, ktorý musí mať používateľ, a druhá časť pozostáva z toho, čo musí používateľ použiť na aktiváciu bezpečnostného modulu.

K6.2 Aktivačný mechanizmus a personalizovaný kód musia byť navrhnuté tak, aby bolo nepravdepodobné, že by tretie strany mohli porušiť ochranu, a to aj mechanickými prostriedkami.

Úrovne 3 a 4: Ochrana zahŕňa mechanizmy na zabránenie kopírovaniu a manipulácii s elektronickým identifikačným dokumentom.

K6.3 Používatelia elektronickej identifikácie so švédskou značkou kvality elektronických identifikácií si môžu z vlastnej iniciatívy, v rámci obdobia platnosti elektronickej identifikácie, bezplatne a bez závažných ťažkostí vymeniť alebo požiadať o nový personalizovaný kód a prostredníctvom usmernenia alebo automatickej tvorby sa im pomôže zachovať požiadavky úrovne K6.2.

Ak je elektronická identifikácia navrhnutá tak, že nie je možné vymeniť personalizovaný kód, používateľ by mal mať namiesto toho za rovnakých podmienok možnosť okamžite získať novú elektronickú identifikáciu s novým personalizovaným kódom, ktorý nahradí predchádzajúci prostredníctvom postupu blokovania.

K6.4 Vydavatelia švédskych elektronických identifikácií zabezpečia, aby údaje zaregistrované na účely elektronickej identifikácie držiteľov jednoznačne zastupovali žiadateľa a boli priradené dotknutej osobe pri vydávaní dokladu o elektronickej identifikácii.

K6.5 Obdobie platnosti vydaných elektronických identifikácií je obmedzené s prihliadnutím na bezpečnostné prvky dokladu o elektronickej identifikácii a riziká zneužitia. Maximálne obdobie platnosti elektronickej identifikácie je päť rokov.

Poskytnutie dokladu o elektronickej identifikácii

K6.6 Diaľkové poskytovanie:

Úroveň 2: Vydavateľ švédskych elektronických identifikácií poskytne doklad o elektronickej identifikácii spôsobom, ktorým sa potvrdzujú kontaktné údaje uchovávané v úradnom registri alebo takéto informácie zaznamenané v súvislosti s elektronickým postupom podľa úrovne 2 K5.13.

Úroveň 3: Vydavateľ švédskych elektronických identifikácií, ktorý poskytuje elektronickú identifikáciu prostredníctvom elektronického postupu, ktorý je v súlade s úrovňou 3 K5.11, úrovňou 3 K5.12 alebo úrovňou 3 K5.13, zabezpečí, aby bol používateľ pri novom vydaní, oddelene a nezávisle od poskytovania z hľadiska bezpečnosti, informovaný o tom, že takýto doklad o elektronickej identifikácii bol odovzdaný, alebo inými opatreniami zabezpečí rovnocenný stupeň kontroly, aby bola osoba upozornená na riziko krádeže totožnosti v súvislosti s poskytovaním.

Úroveň 4: Vydavateľ švédskych elektronických identifikácií, ktorý poskytuje elektronickú identifikáciu prostredníctvom elektronického postupu v súlade s úrovňou 4 K5.12, musí pri novom vydaní, oddelene a nezávisle od poskytovania z hľadiska bezpečnosti, zabezpečiť, aby bol používateľ informovaný o tom, že takýto doklad o elektronickej identifikácii bol odovzdaný.

K6.7 Poskytnutie počas osobnej návštevy:

Vydavateľ švédskych elektronických identifikácií poskytne počas osobnej návštevy a po kontrole identity v súlade s úrovňou K5.10 doklad o elektronickej identifikácii oproti podpísanému potvrdeniu a ďalej poskytne časť, ktorú používateľ použije na aktiváciu elektronickej identifikácie samostatne a nezávisle od poskytnutia dokladu o elektronickej identifikácii z hľadiska bezpečnosti, na základe kontaktných údajov uchovávaných v úradnom registri alebo iných informácií rovnocennej dôveryhodnosti.

Služba blokovania

K6.8 Vydavatelia švédskych elektronických identifikácií poskytujú službu blokovania s dobrou dostupnosťou pre používateľa, aby mohol zablokovať svoju elektronickú identifikáciu.

K6.9 Vydavatelia švédskych elektronických identifikácií bezodkladne a bezpečne spracujú a vykonajú žiadosti o blokovanie a prijmú opatrenia na zabránenie systematickému zneužívaniu služby blokovania alebo iným úmyselným činnostiam, ktoré vedú k rozsiahlemu blokovaniu dokladov o elektronickej identifikácii, čím sa zabezpečí, že elektronické identifikácie používateľov budú v prípade potreby k dispozícii

7. Overovanie elektronickej identity držiteľov

K7.1 Vydavatelia švédskych elektronických identifikácií zabezpečia, aby sa pri overovaní identity držiteľa vykonávali spoľahlivé kontroly pravosti a platnosti dokladu o elektronickej identifikácii.

K7.2 Vydavatelia švédskych elektronických identifikácií zabezpečia, aby sa pri overovaní elektronickej identity držiteľov vykonali technické bezpečnostné kontroly, aby bolo nepravdepodobné, že by tretie strany mohli prostredníctvom hádania, odpočúvania, prehrávania alebo manipulácie s procesom porušiť ochranné mechanizmy.

8. Vydávanie certifikátov identity

Vydavatelia švédskych elektronických identifikácií, ktorí poskytujú službu vydávania certifikátov identity spoliehajúcim sa elektronickým službám, musia takisto dodržiavať ustanovenia tohto oddielu.

K8.1 Vydavatelia švédskych elektronických identifikácií zabezpečia, aby služba vydávania certifikátov identity bola dobre prístupná a aby vydávaniu certifikátov identity predchádzala spoľahlivá identifikácia v súlade s ustanoveniami oddielu 7.

Úroveň 4: Certifikáty musia obsahovať odkaz na kryptografický kľúč, pri ktorom vydavateľ overil, že je vo výlučnom vlastníctve držiteľa.

K8.2 Predložené certifikáty identity sú platné len tak dlho, ako je potrebné na to, aby sa používateľovi umožnil prístup k požadovanej elektronickej službe, a musia byť chránené tak, aby informácie mohol čítať len zamýšľaný príjemca a aby príjemcovia certifikátov mohli overiť pravosť týchto certifikátov.

K8.3 Vydavatelia švédskych elektronických identifikácií, s prihliadnutím na riziká zneužitia certifikačnej služby, obmedzia lehotu, v rámci ktorej možno konkrétnemu držiteľovi vydať niekoľko po sebe nasledujúcich certifikátov identity pred opätovnou identifikáciou držiteľa v súlade s ustanoveniami oddielu 7.