ČÍSLO SPISU: 2022-0941
IDENTIFIKAČNÍ ČÍSLO
KLASIFIKACE: 3.2.3

Rámec pro důvěryhodnost

pro švédskou elektronickou identifikaci

Verze ze dne 4. října 2022

1. Souvislosti a účel

Cílem rámce pro důvěryhodnost švédské elektronické identifikace je stanovit společné požadavky na vydavatele elektronických identifikátorů, které přezkoumává a schvaluje Švédská agentura pro digitální správu (DIGG). Požadavky jsou rozděleny do různých tříd ochrany – úrovní důvěryhodnosti – odpovídajících různým stupňům technické a provozní bezpečnosti vydavatele a různým stupňům ověření, že osoba, které je elektronický doklad totožnosti vydán, je tím, za koho se vydává.

Požadavky tohoto rámce pro důvěryhodnost se vztahují na úrovně důvěryhodnosti 2 až 4, přičemž úroveň 4 odpovídá nejvyšší úrovni ochrany.

Soulad se vykládá takto:

(a) není-li úroveň důvěryhodnosti stanovena, musí být požadavek splněn na všech úrovních a

(b) je-li stanovena úroveň důvěryhodnosti, musí být soulad zajištěn alespoň na příslušné úrovni.

Požadavky stanovené pro nižší úroveň, než je relevantní, se neberou v úvahu.

2. Organizace a řízení

Celkové provozní požadavky

K2.1 Vydavatelé švédských elektronických průkazů totožnosti, kteří nejsou veřejnými orgány, musí působit jako registrované právnické osoby a uzavírat a udržovat pojištění požadované pro podnikání.

K2.2 Vydavatelé švédských elektronických průkazů totožnosti musí mít zavedenou činnost, být plně funkční ve všech částech uvedených v tomto dokumentu a být dobře obeznámeni s právními požadavky, které jsou na ně kladeny jako na vydavatele švédských elektronických průkazů totožnosti.

K2.3 Vydavatelé švédských elektronických průkazů totožnosti musí být schopni nést riziko odpovědnosti za škody a mít dostatečné finanční zdroje k provádění svých operací po dobu nejméně jednoho roku.

Bezpečnost informací

K2.4 Vydavatelé švédských elektronických průkazů totožnosti musí mít zaveden systém řízení bezpečnosti informací (ISMS) pro části svých činností, na něž se vztahuje rámec pro důvěryhodnost, který je případně založen na normě ISO/IEC 27001 nebo rovnocenných zásadách pro řízení a kontrolu práce v oblasti bezpečnosti informací, včetně níže uvedeného:

(a) Všechny administrativní a technické procesy, které mají zásadní význam pro bezpečnost, musí být zdokumentovány a založeny na formálním základě, v němž jsou jasně definovány úlohy, odpovědnosti a pravomoci.

(b) Vydavatelé švédských elektronických průkazů totožnosti zajistí, aby měli vždy k dispozici dostatečné lidské zdroje pro plnění svých povinností.

(c) Vydavatelé švédských elektronických průkazů totožnosti zavedou proces řízení rizik, který vhodným způsobem průběžně nebo alespoň každých 12 měsíců analyzuje hrozby a zranitelná místa v podniku a který zavedením bezpečnostních opatření vyvažuje rizika na přijatelnou úroveň.

(d) Vydavatelé švédských elektronických průkazů totožnosti zavedou proces řízení incidentů, který systematicky zajišťuje kvalitu služby, formy dalšího hlášení a přijetí vhodných reaktivních a preventivních opatření ke zmírnění nebo prevenci škod způsobených těmito událostmi.

(e) Vydavatelé švédských elektronických průkazů totožnosti vypracují a pravidelně testují plán kontinuity, který splňuje požadavky podniku na přístupnost prostřednictvím schopnosti obnovit kritické procesy v případě krize nebo závažných incidentů.

(f) Vydavatelé švédských elektronických průkazů totožnosti pravidelně vyhodnocují činnost v oblasti bezpečnosti informací a zavádějí opatření ke zlepšení v systému řízení.

K2.5 Oblast působnosti a vyspělost systému řízení:

Úroveň 4: Systém řízení bezpečnosti informací musí být v souladu s normou SS-ISO/IEC 27001:2017 nebo rovnocennými pozdějšími nebo mezinárodními verzemi normy a v rámci toho musí zahrnovat všechny požadavky kladené na vydavatele švédských elektronických průkazů totožnosti.

Podmínky pro subdodavatele

K2.6 Vydavatel švédských elektronických průkazů totožnosti, který zadal provádění jednoho nebo více procesů kritických z hlediska bezpečnosti jiné straně, musí smluvně vymezit, za které kritické procesy je subdodavatel odpovědný a které požadavky se na ně vztahují, a objasnit smluvní vztah v prohlášení vydavatele.

Sledovatelnost, vymazávání a uchovávání dokumentů

K2.7 Vydavatelé švédských elektronických průkazů totožnosti uchovávají:

(a) dokumenty týkající se žádosti a dokumenty týkající se vydávání, přijímání nebo blokování elektronických průkazů totožnosti;

(b) smlouvy, smluvní dokumenty a prohlášení vydavatele; a

(c) historii zpracování a další podobnou dokumentaci, která je nezbytná k prokázání souladu s požadavky kladenými na vydavatele švédských elektronických průkazů totožnosti a která umožňuje následnou kontrolu, jež prokazuje, že procesy a kontroly důležité z hlediska bezpečnosti jsou zavedeny a účinné.

K2.8 Doba uchovávání nesmí být kratší než pět let a materiál musí být po celou tuto dobu k dispozici v čitelné podobě, pokud neexistuje požadavek na vymazání z důvodu ochrany soukromí a není podložen zákonem nebo nařízením.

Přezkum a následná opatření

K2.9 Vydavatelé švédských elektronických průkazů totožnosti zřídí funkci interního auditu, která pravidelně přezkoumává činnosti vydávání. Interní auditor musí být při výkonu svých povinností nezávislý tak, aby byl zajištěn objektivní a nestranný audit, a musí mít pro výkon svých povinností potřebnou odbornou způsobilost a zkušenosti. Interní auditor nezávisle naplánuje provedení auditu a zdokumentuje to v plánu auditu na období tří let. Prvky auditu musí být vybrány na základě analýzy rizik a významnosti a musí vycházet z popisu operací, který vydavatel poskytl Agentuře pro digitální správu.

Úrovně 3 a 4: Interní audit se provádí na základě uznávaných auditorských standardů.

3. Fyzická, administrativní a osobní bezpečnost

K3.1 Klíčové prvky provozu musí být fyzicky chráněny před poškozením v důsledku vlivu prostředí, neoprávněného přístupu nebo jiných vnějších zásahů. Řízení přístupu se provádí tak, aby přístup do citlivých oblastí byl vyhrazen pouze oprávněným pracovníkům, nosiče informací byly bezpečně uloženy a likvidovány a přístup do těchto chráněných oblastí byl nepřetržitě monitorován.

K3.2 Předtím, než osoba převezme některou z rolí identifikovaných v souladu s K2.4 písm. a), které mají zvláštní význam pro bezpečnost, musí vydavatel švédských elektronických průkazů totožnosti provést ověření spolehlivosti, aby zajistil, že danou osobu lze považovat za spolehlivou a že má kvalifikaci a odbornou přípravu potřebnou k bezpečnému a zabezpečenému plnění úkolů vyplývajících z dané role.

K3.3 Vydavatelé musí mít zavedeny postupy, které zajistí, aby k údajům shromážděným a uchovávaným v souladu s K2.7 měli přístup pouze konkrétně pověření pracovníci.

K3.4 **Úrovně 3 a 4:** Vydavatelé v průběhu celého postupu vydávání zajistí, aby se oddělení povinností uplatňovalo tak, že žádná jednotlivá osoba nemůže získat elektronickou průkaz totožnosti jménem jiné osoby.

4. Technická bezpečnost

K4.1 Vydavatelé švédských elektronických průkazů totožnosti musí zajistit, aby zavedené technické kontroly byly dostatečné k dosažení úrovně ochrany považované za nezbytnou s ohledem na povahu, rozsah a další okolnosti činnosti a aby tyto kontroly byly funkční a účinné.

K4.2 Elektronické komunikační kanály používané při přenosu citlivých údajů musí být chráněny proti neoprávněnému přístupu, manipulaci a opakovanému přenosu.

K4.3 Citlivý materiál kryptografických klíčů používaný k vydávání elektronických průkazů totožnosti, identifikaci držitelů a vydávání osvědčení totožnosti musí být chráněn tak, aby:

(a) přístup byl logicky a fyzicky omezen na ty role a aplikace, které to nezbytně vyžadují;

(b) klíčovací materiál nebyl nikdy uložen v prostém textu na trvalém paměťovém médiu;

(c) klíčovací materiál byl chráněn použitím kryptografického hardwarového modulu s aktivními bezpečnostními mechanismy, které působí proti fyzickým i logickým pokusům o ohrožení klíčovacího materiálu;

(d) bezpečnostní mechanismy na ochranu klíčovacího materiálu byly transparentní a založené na uznávaných a zavedených normách; a

(e) **Úrovně 3 a 4:** aktivační údaje pro ochranu klíčovacího materiálu jsou spravovány prostřednictvím kontroly více osob.

K4.4 Vydavatelé musí mít zavedeny zdokumentované postupy, které zajistí, že požadovaná úroveň ochrany v příslušném prostředí IT může být udržována v průběhu času a v souvislosti se změnami, včetně pravidelných analýz zranitelností a odpovídající připravenosti na měnící se úroveň rizika a nastalé incidenty.

5. Žádost, identifikace a registrace

Informace o podmínkách

K5.1 Vydavatelé švédských elektronických průkazů totožnosti poskytují připojeným uživatelům, poskytovatelům elektronických služeb a dalším osobám, které se mohou spoléhat na službu certifikační autority, informace o dohodách, podmínkách a souvisejících informacích a o případných omezeních používání služby.

K5.2 Vydavatel švédských elektronických průkazů totožnosti musí jasně odkazovat na podmínky a navrhnout postupy tak, aby byly podmínky poskytnuty žadateli v procesu vydávání.

K5.3 Vydavatelé švédských elektronických průkazů totožnosti poskytují prohlášení vydavatele, které obsahuje:

(a) totožnost a kontaktní údaje vydavatele;

(b) stručný popis služeb a řešení poskytovaných vydavatelem, včetně použitých metod pro uplatňování, vydávání a blokování;

(c) podmínky spojené s poskytovanou službou, včetně povinností uživatele chránit svou elektronickou identifikaci, povinností a odpovědnosti vydavatele, veškerých poskytnutých záruk a přislíbené dostupnosti;

(d) informace o zpracování osobních údajů a způsobu, jakým je prováděno a

(e) postupy při změně podmínek nebo jiných podmínek poskytované služby, včetně kroků, které je třeba podniknout k řízenému ukončení služby.

K5.4 **Úrovně 3 a 4:** Vydavatelé švédských elektronických průkazů totožnosti poskytují na žádost Agentury pro digitální správu (DIGG) nebo jiné smluvní strany, která se spoléhá na služby poskytované vydavatelem, informace o tom, jak je podnik vlastněn a řízen.

K5.5 Vydavatel švédských elektronických průkazů totožnosti, který ukončí svou činnost, se řídí předem stanoveným plánem pro ukončení služby. Plán zahrnuje informování všech uživatelů služby a DIGG. Vydavatel dále uchovává archivovaný materiál k dispozici v souladu s K2.7 a K2.8 po ukončení.

Použití

K5.6 Švédský elektronický průkaz totožnosti může být vydán pouze na žádost žadatele nebo prostřednictvím jiného rovnocenného přijímacího řízení a pouze poté, co byl žadatel informován o podmínkách, za nichž je vydána, a o odpovědnosti, která na něj bude kladena.

Vydání elektronického průkazu totožnosti, který nahrazuje nebo doplňuje platný nebo nedávno zablokovaný doklad elektronického průkazu totožnosti dříve vydaný stejným vydavatelem, však může proběhnout bez jakéhokoli předchozího postupu pro podání žádosti.

K5.7 Žádost o švédský elektronický průkaz totožnosti musí být spojena s osobním identifikačním číslem nebo koordinačním číslem, jakož i s informacemi, které jsou jinak nezbytné k tomu, aby vydavatel mohl takový elektronický průkaz poskytnout.

Určení totožnosti žadatele

K5.8 Vydavatelé švédských elektronických průkazů totožnosti musí ověřit, zda jsou informace spojené s žádostí úplné a odpovídají informacím zapsaným v úředním rejstříku.

K5.9 Pokud jsou informace, které mají být v úředním rejstříku zkontrolovány, označeny jako důvěrné (tzv. „chráněná identita“), mohou být nezbytné kontroly provedeny jinými rovnocennými prostředky.

K5.10 Identifikace žadatele při osobní návštěvě:

Vydavatelé švédských elektronických průkazů totožnosti mohou při osobní návštěvě ověřit totožnost žadatele stejným způsobem jako při vydávání standardního dokladu totožnosti.

K5.11 Vzdálená identifikace žadatele ve stávajícímvztahu:

Úroveň 3: Vydavatelé švédských elektronických průkazů totožnosti, kteří již identifikovali žadatele ve vztahu zahrnujícím finančně nebo právně významné jednání a pokud lze žadatele identifikovat na dálku jiným spolehlivým způsobem, který odpovídá požadavkům na švédskou značku kvality elektronického průkazu totožnosti úrovně 3, mohou tento způsob použít ke zjištění totožnosti žadatele.

Úroveň 4: Nehodí se.

K5.12 Identifikace prostřednictvím švédského elektronického průkazu totožnost:

Vydavatel švédských elektronických průkazů totožnosti může žadatele identifikovat na dálku prostřednictvím stávajícího platného švédského elektronické průkazu totožnosti, která má přinejmenším stejnou úroveň záruky jako ta, která má být vydána, pokud může tuto identifikaci bez smluvních překážek použít jako základ pro vydání nového elektronického průkazu totožnosti.

Úroveň 4: Doba platnosti nově vydaný elektronický průkaz totožnosti je omezena tak, aby nepřesahovala dobu platnosti stávajícího elektronického průkazu totožnosti.

K5.13 Vzdálená identifikace žadatele:

Úroveň 2: Vydavatelé švédských elektronických průkazů totožnosti mohou použít spolehlivé obrazové záznamy platného standardního dokladu totožnosti a zobrazení obličeje žadatele jako základ pro zjištění totožnosti žadatele na dálku, pokud srovnání nevyvolává pochybnosti o skutečné totožnosti žadatele.

Úroveň 3: Vydavatelé švédských elektronických průkazů totožnosti mohou prostřednictvím bezpečného čtení platného standardního dokladu totožnosti

obsahujícího elektronicky uchovávané biometrické údaje na dálku zjistit totožnost žadatele na základě těchto údajů, pokud lze odpovídající biometrické údaje osoby, která má být identifikována, získat dostatečně bezpečným způsobem, aby bylo možné provést srovnání s rovnocennou spolehlivostí jako v případě osobní návštěvy, a pokud toto porovnání nevyvolává pochybnosti o skutečné totožnosti žadatele.

Úroveň 4: Nehodí se.

Registrace

K5.14 Vydavatelé švédských elektronických průkazů totožnosti vedou s ohledem na platná pravidla ochrany osobních údajů registr připojených uživatelů a vydaných elektronických identifikačních dokladů a tento rejstřík aktualizuje.

6. Vydávání a blokování elektronických průkazů totožnosti

Návrh technických prostředků

K6.1 Technické prostředky:

Úrovně 2 a 3: Technické prostředky pro elektronickou identifikaci prostřednictvím elektronického průkazu totožnosti se švédskou značkou kvality elektronického průkazu totožnosti jsou navrženy podle dvoufaktorového principu, přičemž jedna část se skládá z elektronicky uložených informací, které uživatel uchovává, a druhá část se skládá z toho, co uživatel použije k aktivaci elektronického průkazu totožnosti.

Úroveň 4: Technické prostředky pro elektronickou identifikaci prostřednictvím elektronického průkazu totožnosti se švédskou značkou kvality elektronického průkazu totožnosti musí být navrženy podle dvoufaktorového principu, přičemž jedna část se skládá z osobního bezpečnostního modulu, který musí uživatel vlastnit, a druhá část z toho, co uživatel použije k aktivaci bezpečnostního modulu.

K6.2 Aktivační mechanismus a personalizovaný kód musí být navrženy tak, aby bylo nepravděpodobné, že třetí strany poruší ochranu, a to i mechanickými prostředky.

Úrovně 3 a 4: Ochrana zahrnuje mechanismy zabraňující kopírování a manipulaci s elektronickým průkazem totožnosti.

K6.3 Uživatelé elektronického průkazu totožnosti se švédskou značkou kvality elektronického průkazu totožnosti musí mít možnost z vlastního podnětu, v době platnosti elektronického průkazu totožnosti, bezplatně a bez značných obtíží si vyměnit nebo požádat o nový osobní kód a prostřednictvím pokynů nebo automatické výroby jim musí být poskytnuta pomoc při udržování požadavků K6.2.

Pokud je elektronický průkaz totožnosti navržen tak, že personalizovaný kód nelze vyměňovat, měl by mít uživatel místo toho za stejných podmínek možnost okamžitě získat nový elektronický průkaz totožnosti s novým personalizovaným kódem, který nahrazuje předchozí kód prostřednictvím blokovacího postupu.

K6.4 Vydavatelé švédských elektronických průkazů totožnosti zajišťují, aby údaje registrované pro elektronickou identifikaci držitelů jednoznačně reprezentovaly žadatele a byly přiřazeny dotyčné osobě při vydávání dokladu elektronického průkazu totožnosti.

K6.5 Doba platnosti vydaných elektronických průkazů totožnosti je omezena s ohledem na bezpečnostní prvky dokladu elektronického průkazu totožnosti a rizika zneužití. Maximální doba platnosti elektronického průkazu totožnosti je pět let.

Poskytnutí dokladu elektronického průkazu totožnosti

K6.6 Vzdálené poskytnutí:

Úroveň 2: Vydavatel švédských elektronických průkazů totožnosti poskytuje doklad elektronického průkazu totožnosti (e-ID) způsobem, který potvrzuje kontaktní údaje vedené v úředním rejstříku nebo takové informace zaznamenané v souvislosti s elektronickým postupem podle K5.13 úrovně 2.

Úroveň 3: Vydavatel švédských elektronických průkazů totožnosti, který poskytuje elektronický průkaz totožnosti prostřednictvím elektronického postupu, který je v souladu s K5.11 úrovně 3, K5.12 úrovně 3 nebo K5.13 úrovně 3, zajistí, aby byl uživatel při novém vydání samostatně a nezávisle na ustanovení z hlediska bezpečnosti informován o tom, že takový doklad elektronického průkazu totožnosti (e-ID) byl předán, nebo byla jinými opatřeními zajištěna rovnocenná míra kontroly, že je daná osoba upozorněna na riziko krádeže totožnosti v souvislosti s poskytnutím.

Úroveň 4: Vydavatel švédských elektronických průkazů totožnosti, který poskytuje elektronický průkaz totožnosti prostřednictvím elektronického postupu v souladu s K5.12 úrovně 4, zajišťuje, aby byl uživatel v případě nového vydání samostatně a nezávisle na ustanovení týkajícím se bezpečnosti informován o tom, že tento doklad elektronického průkazu totožnosti byl předán.

K6.7 Předání při osobní návštěvě:

Vydavatel švédských elektronických průkazů totožnosti poskytne během osobní návštěvy a po kontrole totožnosti v souladu s K5.10 elektronický průkaz totožnosti proti podepsanému potvrzení o přijetí a dále poskytne část, kterou uživatel použije k aktivaci elektronické identifikace samostatně a nezávisle na poskytnutí dokladu elektronického průkazu totožnosti z hlediska bezpečnosti, a to na základě kontaktních údajů vedených v úředním rejstříku nebo jiných informací rovnocenné důvěryhodnosti.

Služba blokování

K6.8 Vydavatelé švédských elektronických průkazů totožnosti poskytnou službu blokování s dobrou přístupností, aby uživatel mohl jejich elektronický průkaz totožnosti zablokovat.

K6.9 Vydavatelé švédských elektronických průkazů totožnosti neprodleně a bezpečně vyřizují a provádějí žádosti o blokování a přijímají opatření, aby zabránili systematickému zneužívání služby blokování nebo jiným úmyslným činnostem, které vedou k rozsáhlému zablokování elektronických průkazů totožnosti, a zajišťují dostupnost elektronických průkazů totožnosti uživatelů v případě potřeby.

7. Ověřování držitelů elektronických identit

K7.1 Vydavatelé švédských elektronických průkazů totožnosti zajistí, aby při ověřování totožnosti držitele byly prováděny spolehlivé kontroly pravosti a platnosti dokladu elektronického průkazu totožnosti.

K7.2 Vydavatelé švédských elektronických průkazů totožnosti zajistí, aby byly při ověřování elektronických identit držitelů zavedeny technické bezpečnostní kontroly, takže je nepravděpodobné, že by třetí strany mohly prostřednictvím hádání, odposlechu, opakovaného přehrávání nebo manipulace s procesem porušit ochranné mechanismy.

8. Vydávání osvědčení totožnosti

Vydavatelé švédských elektronických průkazů totožnosti, kteří poskytují službu vydávání osvědčení totožnosti spoléhajícím se elektronickým službám, musí rovněž dodržovat ustanovení této části.

K8.1 Vydavatelé švédských elektronických průkazů totožnosti zajišťují, aby služba vydávání průkazů totožnosti byla dobře přístupná a aby vydání průkazů totožnosti předcházela spolehlivá identifikace v souladu s ustanoveními oddílu 7.

Úroveň 4: Certifikáty obsahují odkaz na kryptografický klíčovací materiál, u něhož vydavatel ověřil, že je ve výhradním držení držitele.

K8.2 Předložené osvědčení totožnosti jsou platné pouze po dobu nezbytnou k umožnění přístupu uživatele k požadované e-službě a jsou chráněny tak, aby informace mohly být čteny pouze zamýšleným příjemcem a aby pravost osvědčení mohla být ověřena příjemci těchto osvědčení.

K8.3 Vydavatelé švédských elektronických průkazů totožnosti omezují s ohledem na rizika zneužití certifikační služby dobu, během níž může být vydáno několik po sobě jdoucích certifikátů totožnosti určitému držiteli, než bude držitel znovu identifikován v souladu s ustanoveními oddílu 7.