MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dokument konkretizující minimální požadavky na kvalifikované systémy elektronické identifikace a na prostředky pro elektronickou identifikaci v rámci nich vydávané a používané [DKP IDP]

Historie dokumentu:

Verze	*Vytvořeno*	*Autor*	*Poznámka*	*Status*
1	12/2017	FB	první draft	Návrh
2	1/2018	OHA	připomínky	Návrh
2.1	3/2018	FB,OHA	Vypořádání připomínek	Návrh
3	5/2018	OEG,OHA, externí subjekty	Vypořádání připomínek od externích subjektů (RELSIE spol. s r.o., Elektrotechnický zkušební ústav, s.p., ADUCID s.r.o., Česká spořitelna, a.s. a MONET+, a.s.).	Ke zveřejnění

Obsah

1. Účel dokumentu

Dokument byl vypracován Ministerstvem vnitra pro účely vysvětlení a bližší konkretizace požadavků CIR 2015/1502[1], na které odkazuje zákon č. 250/2017 Sb., o elektronické identifikaci (dále jen zákon o elektronické identifikaci) v souvislosti s požadavky na kvalifikované systémy elektronické identifikace (dále jen „kvalifikovaný systém“) a na prostředky pro elektronickou identifikaci (dále jen „eID prostředky“) v rámci nich vydávané a používané. Jedná se o výklad Ministerstva vnitra, který bere v potaz rovněž nezávazný dokument *Guidance for the application of the levels of assurance which support the eIDAS Regulation*[2] vypracovaný členskými státy v rámci eIDAS expert group (pracovní skupina pod vedením EK[3]).

Dokument je primárně určen pro žadatele o získání akreditace pro správu kvalifikovaného systému, dále pro kvalifikované správce (viz § 4 a § 5 zákona o elektronické identifikaci) a v neposlední řadě pro pověřené osoby posuzující splnění požadavků kladených zákonem o elektronické identifikaci na kvalifikované systémy a eID prostředky (viz § 11 zákona o elektronické identifikaci). Vzhledem k tomu, že se materiál vyslovuje k dynamickým oblastem, kde technický vývoj neustále pokračuje, předpokládá se průběžná aktualizace tohoto dokumentu.

Kvalifikovaný správce musí samozřejmě kromě zákona o elektronické identifikaci dodržovat v souvislosti se svojí činností i další relevantní právní předpisy, jako je například nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Z něj mimo jiné vyplývá, že osobní údaje, které jsou svou povahou obzvláště citlivé z hlediska základních práv a svobod (např. biometrické údaje),

[1] CIR 2015/1502 - Prováděcí nařízení komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu. Dostupné na: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002

[2] Guidance for the application of the levels of assurance which support the eIDAS Regulation. Dostupné na: https://www.google.cz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwjOyduYqIjVAhUGOxQKHR1dCKoQFgg0MAI&url=https%3A%2F%2Fec.europa.eu%2Fcefdigital%2Fwiki%2Fdownload%2Fattachments%2F40044784%2FGuidance%2520on%2520Levels%2520of%2520Assurance.docx%3Fversion%3D1%26modificationDate%3D1488295895839%26api%3Dv2&usg=AFQjCNGidAS04-eAY_OR13N-TXaRPAhOkQ

[3] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3032

zasluhují zvláštní ochranu, jelikož by při jejich zpracování mohla vzniknout závažná rizika v rámci zásahu do těchto práv.

Základní východiska a jejich důsledky:

- **Přístup k elektronickým službám ČR je umožněn osobám, které vlastní prostředek pro elektronickou identifikaci vydaný správcem kvalifikovaného systému v rámci kvalifikovaného systému (dle §3 zákona o elektronické identifikaci) nebo prostředek vydaný oznámeným systémem v rámci nařízení eIDAS. Pro úplnost je vhodné uvést, že pro obstarání výstupů z informačních systémů veřejné správy je možné využít prostředek pro elektronickou identifikaci umožňující přístup se zaručenou identitou ve smyslu §2 písm. x) zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.**
- **Občanský průkaz s identifikačním certifikátem občanského průkazu vydaný Českou republikou je prostředek elektronické identifikace s vysokou úrovní záruky, jehož životní cyklus je řízen zákonem č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů.**

A tedy:

- Kvalifikovaný správce může vydat eID prostředek pouze osobě, která je vedena v registru obyvatel a je buď držitelem identifikačního dokladu (jehož číslo je vedené v registru obyvatel dle §18 odst. 1 písm. g) zákona 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů) nebo je držitelem prostředku pro elektronickou identifikaci vysoké úrovně záruky (osoby vedené v registru obyvatel dle §17 písm. e) zák. č. 111/2009 Sb.)
    - Pro osoby, občany ČR, mladší 15-ti let (starší mají dle zákona č. 328/1999 Sb. občanský průkaz povinně) je nutnou podmínkou pro vydání **jakéhokoli** eID prostředku to, že vlastní identifikační doklad uvedený v registru obyvatel (občanský průkaz nebo pas).
    - Pro osoby uvedené v registru obyvatel, které nejsou občany ČR, platí bez ohledu na věk to, že musí být držitelem identifikačního dokladu uvedeného v registru obyvatel.
- Pokud požaduje osoba, která není státním občanem České republiky nebo cizincem uvedeným v registru obyvatel, vydání eID prostředku dle zákona o elektronické identifikaci, pak musí být nejdříve zavedena do registru obyvatel – EJFO – evidence jiných fyzických osob – subjekt, který osobu do registru obyvatel zavádí, zodpovídá za to, že provedl prokázání totožnosti a ověření údajů o této osobě. Tento proces zatím není implementován.

Zákon o elektronické identifikaci ve svém § 3 stanovuje za jakých podmínek je systém elektronické identifikace považován za kvalifikovaný systém:

§ 3 Kvalifikovaný systém

(1) Kvalifikovaným systémem je systém elektronické identifikace,

a) který spravuje kvalifikovaný správce systému elektronické identifikace (dále jen „kvalifikovaný správce“),

b) který splňuje technické specifikace, normy a postupy alespoň pro jednu z úrovní záruky stanovených přímo použitelným předpisem Evropské unie upravujícím minimální technické specifikace, normy a postupy pro úrovně záruky prostředků pro elektronickou identifikaci (dále jen „příslušný předpis Evropské unie“),

c) který umožňuje poskytnutí služby národního bodu pro identifikaci a autentizaci (dále jen „národní bod“),

d) v jehož rámci jsou osobní identifikační údaje jedinečně identifikující osobu v okamžiku vydání prostředku pro elektronickou identifikaci spojeny s danou osobou v souladu s technickými specifikacemi, normami a postupy pro příslušnou úroveň záruky stanovenými příslušným předpisem Evropské unie a

e) v jehož rámci je vydáván a používán pouze prostředek pro elektronickou identifikaci, který je spojen s osobou, kterou identifikuje, v souladu s technickými specifikacemi, normami a postupy pro příslušnou úroveň záruky stanovenými příslušným předpisem Evropské unie.

(2) Kvalifikovaným systémem je dále systém elektronické identifikace oznámený podle přímo použitelného předpisu Evropské unie upravujícího elektronickou identifikaci1), v jehož rámci je vydáván a používán pouze prostředek pro elektronickou identifikaci s úrovní záruky alespoň značnou.

Jak již bylo řečeno v úvodu dokumentu, cílem tohoto materiálu je rozvést požadavky dle §3 odst. 1 písm. b) zákona o elektronické identifikaci kladených na kvalifikované systémy (a na eID prostředky v rámci nich vydávané a používané).

Nařízení Evropského Parlamentu a RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení

směrnice 1999/93/ES[4] (dále jen nařízení eIDAS) definuje ve čl. 8 celkem tři úrovně záruky eID prostředků vydávaných v rámci systému elektronické identifikace:

a) nízká úroveň záruky označuje v souvislosti se systémem elektronické identifikace prostředek pro elektronickou identifikaci, který nabízí omezenou míru spolehlivosti u deklarované nebo uváděné totožnosti určité osoby a je charakterizován pomocí souvisejících technických specifikací, norem a postupů, včetně technických kontrol, jejichž účelem je snížit riziko zneužití nebo změny totožnosti;

b) značná úroveň záruky označuje v souvislosti se systémem elektronické identifikace prostředek pro elektronickou identifikaci, který nabízí značnou míru spolehlivosti u deklarované nebo uváděné totožnosti určité osoby a je charakterizován pomocí souvisejících technických specifikací, norem a postupů, včetně technických kontrol, jejichž účelem je značně snížit riziko zneužití nebo změny totožnosti;

c) vysoká úroveň záruky označuje v souvislosti se systémem elektronické identifikace prostředek pro elektronickou identifikaci, který nabízí vyšší míru spolehlivosti u deklarované nebo uváděné totožnosti určité osoby než prostředek pro elektronickou identifikaci se značnou úrovní záruky a je charakterizován pomocí souvisejících technických specifikací, norem a postupů, včetně technických kontrol, jejichž účelem je předejít zneužití nebo změně totožnosti.

CIR 2015/1502 pak následně blíže stanovuje minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci (nízká, značná a vysoká úroveň). Úroveň záruky eID prostředků se určí s ohledem na splnění specifikací a postupů stanovených v příloze CIR 2015/1502.

[4] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

2. Definice a požadavky CIR 2015/1502.

Úvodní články CIR 2015/1502

Článek 1

1.Nízká, značná a vysoká úroveň záruky prostředků pro elektronickou identifikaci vydaných v rámci oznámeného systému elektronické identifikace se určí s ohledem na specifikace a postupy stanovené v příloze.

2.Specifikace a postupy stanovené v této příloze se použijí k upřesnění úrovně záruky prostředků pro elektronickou identifikaci vydaných v rámci oznámeného systému elektronické identifikace určením spolehlivosti a kvality těchto prvků:

a) přihlášení, jak je stanoveno v oddíle 2.1 přílohy tohoto nařízení v souladu s čl. 8 odst. 3 písm. a) nařízení (EU) č. 910/2014;

b) správy prostředků pro elektronickou identifikaci, jak je stanoveno v oddíle 2.2 přílohy tohoto nařízení podle čl. 8 odst. 3 písm. b) a f) nařízení (EU) č. 910/2014;

c) autentizace, jak je stanoveno v oddíle 2.3 přílohy tohoto nařízení v souladu s čl. 8 odst. 3 písm. c) nařízení (EU) č. 910/2014;

d) řízení a organizace, jak je stanoveno v oddíle 2.4 přílohy tohoto nařízení v souladu s čl. 8 odst. 3 písm. d) a e) nařízení (EU) č. 910/2014.

3.Pokud prostředek pro elektronickou identifikaci vydaný v rámci oznámeného systému elektronické identifikace splňuje požadavek uvedený ve vyšší úrovni záruky, má se za to, že splňuje odpovídající požadavek nižší úrovně záruky.

4.Není-li v příslušné části přílohy uvedeno jinak, musí být k dosažení požadované úrovně záruky splněny všechny prvky uvedené v příloze pro konkrétní úroveň záruky prostředků pro elektronickou identifikaci vydaných v rámci oznámeného systému elektronické identifikace.

Výsledná úroveň záruky eID prostředků je dána podle nejnižší dosažené úrovně záruky v jednotlivých oblastech (tj. pravidlo – „řetěz je tak silný jako jeho nejslabší část“).

Článek 2

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v Úředním věstníku Evropské unie.

CIR 2015/1502 bylo zveřejněno v Úředním věstníku EU dne 9. září 2015, vstoupilo v platnost 29. září 2015.

Definice CIR 2015/1502

V příloze CIR 2015/1502 jsou uvedeny definice, které se následně používají v souvislosti s technickými specifikacemi a postupy pro nízkou, značnou a vysokou úroveň záruky eID prostředků.

1) „spolehlivým zdrojem" se rozumí jakýkoli zdroj bez ohledu na svou formu, u něhož se lze spolehnout na to, že poskytuje přesné údaje, informace a/nebo důkazy, které lze použít k prokázání totožnosti;

Spolehlivým zdrojem může být jakýkoli zdroj, který je na národní úrovni důvěryhodný a poskytuje validní data. Spolehlivými zdroji mohou být:

- základní registry,
- výstup z informačního systému veřejné správy, rejstříku nebo seznamu spravovaným orgánem veřejné moci pro údaje, které nejsou vedeny v základních registrech,
- občanské průkazy, cestovní pasy, řidičské průkazy, zbrojní průkazy a případné další doklady vydávané dle zákona, kde je zákonem stanoveno, že jimi lze prokazovat údaje uvedené na dokumentu a zároveň obsahují minimálně fotografii pro ověření oprávnění držet tento doklad

Informace o totožnosti osoby musí být poskytovány tak, aby byla zajištěna pravost dat (např. elektronická pečeť na výpisu z ISVS, doklady totožnosti opatřené ochrannými prvky,…).

Veřejný rejstřík pravých dokladů totožnosti a cestovních dokladů je k dispozici na adrese: http://www.consilium.europa.eu/prado/cs/prado-start-page.html (Databáze PRADO). V rejstříku PRADO je možné vyhledat informace o typech vydávaných dokladů totožnosti a cestovních dokladech včetně informací o ochranných prvcích. Vyhledávání podle vydávající země: http://www.consilium.europa.eu/prado/cs/search-by-document-country.html.

2) „faktorem autentizace" se rozumí faktor, který je prokazatelně spojen s osobou a spadá do některé z těchto kategorií:

a) „faktorem autentizace na základě vlastnictví“ se rozumí faktor autentizace, kdy osoba musí prokázat, že jej má ve svém vlastnictví;

b) „faktorem autentizace na základě znalostí“ se rozumí faktor autentizace, kdy osoba musí prokázat jeho znalost;

c) „inherentním faktorem autentizace“ se rozumí faktor autentizace, který vychází z fyzické vlastnosti fyzické osoby a u něhož musí osoba prokázat, že danou fyzickou vlastnost má;

Faktor autentizace na základě vlastnictví – např. čipová karta obsahující soukromý klíč k autentizačnímu certifikátu, mobilní telefon (resp. SIM karta) na kterou se posílají OTP hesla (One-Time-Password), RSA tokeny či karty obsahující vytištěná jednorázová hesla. Kvalifikovaný správce musí zajistit dostatečnou ochranu před možností reprodukce eID prostředku založeného na tomto faktoru.

Faktor autentizace na základě znalostí – hesla, PINy,… V případě použití eID prostředku založeného na faktoru autentizace na základě znalostí, musí být definována politika pro tvorbu a použití hesel či PINů obsahující taková pravidla, která vedou ke snížení možnosti uhádnutí hesla.

Inherentní faktor autentizace – např. otisk prstů, otisk dlaně, geometrie tváře, sken oční duhovky,.. V případě použití eID prostředku založeného na tomto fakturu, musí být přijata opatření ke snížení rizika možného podvržení či duplikace (např. umělý otisk prstu).

Pro stanovení dostatečně bezpečných parametrů jednotlivých faktorů autentizace může sloužit dokument vydaný organizací NIST (National Institute of Standards and Technology) NIST Special Publication 800 - 63B „Digital Identity Guidelines - Authentication and Lifecycle Management“ dostupný na adrese: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf. Relevantními kapitolami jsou v tomto ohledu zejména kapitoly 5 a 10.

V případě, kdy eID prostředek kombinuje alespoň 2 prvky z různých kategorií faktorů autentizace, pak se jedná o multi - faktorový eID prostředek. Použití multi - faktorového prostředku je vyžadováno pro úroveň značnou a vysokou.

3) „dynamickou autentizací“ se rozumí elektronický proces, který s využitím kryptografie nebo jiných metod vytváří na požádání elektronický důkaz, že osoba disponuje identifikačními údaji nebo je má

ve svém vlastnictví a který se mění při každé autentizaci mezi osobou a systémem ověřujícím její totožnost;

Dynamická autentizace může být implementována prostřednictvím autentizačního faktoru (např. jednorázové hesla) nebo může být zajištěna mechanismem autentizace (implementace dynamické autentizace pomocí použití challenge-response protokolu, např. SSL/TLS).

4) „systémem řízení bezpečnosti informací" se rozumí soubor procesů a postupů určených ke zmírňování rizik týkajících se bezpečnosti informací na přijatelné úrovně.

2.1. Kapitola „Přihlášení" přílohy CIR 2015/1502

2.1.1. Žádost a registrace

Úroveň záruky	***Potřebné prvky***
Nízká	*1.Zajistit, aby byl žadatel obeznámen s podmínkami používání prostředků pro elektronickou identifikaci.* Žadatel musí mít možnost se seznámit s podmínkami používání eID prostředků (podmínky v elektronické či listinné podobě). Žadatel potvrzuje před vydáním prostředku či jeho aktivním používáním, že se s těmito podmínkami seznámil. *2.Zajistit, aby byl žadatel obeznámen s doporučenými bezpečnostními opatřeními spojenými s používáním prostředků pro elektronickou identifikaci.* Doporučená bezpečnostní opatření mohou být součástí podmínek používání eID prostředků nebo mohou být dostupná v jiném dokumentu umístěném např. na webu kvalifikovaného správce. Kvalifikovaný správce musí dbát na to, aby žadatel o eID prostředek či následný uživatel (po vydání prostředku) měl snadný přístup k bezpečnostním doporučením. *3. Shromáždit příslušné údaje o totožnosti nezbytné pro prokazování a ověřování totožnosti.* Kvalifikovaný správce musí získat patřičné údaje a dokumenty od žadatele, které se použijí pro fázi ověřování totožnosti. S ohledem na povinnost vést evidenci vydaných eID prostředků stanovenou v § 22 zákona o elektronické identifikaci, musí shromáždit takové údaje o žadateli, aby splnil zákonné požadavky.
Značná	*Stejné jako při nízké úrovni.*

Vysoká	*Stejné jako při nízké úrovni.*

2.1.2. Prokazování a ověřování totožnosti (fyzická osoba)

Úroveň záruky	***Potřebné prvky***
Nízká	*1.Lze předpokládat, že osoba vlastní důkaz deklarované totožnosti uznaný členským státem, ve kterém se žádost o prostředek pro elektronickou identifikaci podává.* Vlastnictví důkazu deklarované totožnosti lze prokázat předložením osobního identifikačního dokladu v rámci registrace, který je pro danou osobu ověřitelný vůči základnímu registru obyvatel prostřednictvím národního bodu. V případě, že registrační proces umožňuje některé kroky, či celou žádost realizovat elektronicky, musí být prokázáno, že předkládající osoba je oprávněným držitelem dokladu. Pro účely získání eID prostředků úrovně záruky nízká může být užito video identity proofingu za podmínky, že další kroky v procesu vydání, doručení, aktivace eID prostředku umožní potvrdit předpoklad správnosti deklarované totožnosti osoby (tj. osoba je oprávněným držitelem dokladu). Například žádost o vydání prostředku vyplnit elektronicky a poté se dostavit osobně za účelem ověření údajů. Nebo registrační formulář odeslat prostřednictvím datové schránky žádající fyzické osoby s uvedením druhu a čísla elektronicky čitelného dokladu ověřitelného v registru obyvatel prostřednictvím národního bodu. *2.Lze předpokládat, že tento důkaz je pravý nebo podle spolehlivého zdroje existuje, a důkaz se jeví být platným.* Osobní identifikační doklad nebyl na první pohled pozměněn či zfalšován a je platný (tj. doklad se předkládá v době platnosti dokladu). V případě žádosti o vydání eID prostředku elektronicky musí být nejpozději v okamžiku předání nebo před jeho prvním použitím v rámci kvalifikovaného systému elektronické identifikace ověřena platnost osobního identifikačního dokladu dotazem do registru obyvatel prostřednictvím národního bodu. Pokud žadatel dokládá při registraci např. výpis z ISVS ověřit, zda byl výpis korektně opatřen elektronickou pečetí. Pro účely získání eID prostředků úrovně záruky nízká může být užito video identity

	proofingu za podmínky, že další kroky v procesu vydání, doručení, aktivace eID prostředku umožní potvrdit předpoklad pravosti dokladu deklarované totožnosti. *3. Spolehlivému zdroji je známo, že deklarovaná identita existuje, a lze předpokládat, že osoba deklarující identitu je jedna a tatáž.* Předložením osobního identifikačního dokladu je splněna podmínka, že spolehlivému zdroji je známo, že identita existuje. Porovnáním fotografie uvedené na dokladu a podoby žadatele lze s jistou mírou rozhodnout, zda se jedná o stejnou osobu. V případě elektronické žádosti, pokud byla žádost o vydání eID prostředku odeslána z datové schránky fyzické osoby, považuje se to za důkaz, že osoba deklarující identitu je jedna a tatáž. Před vydáním nebo prvním použitím eID prostředku v rámci kvalifikovaného systému má kvalifikovaný správce povinnost dle zákona o elektronické identifikaci ověřit totožnost držitele eID prostředku prostřednictvím národního bodu. Tímto se docílí splnění požadavku, že deklarovaná identita existuje v registru obyvatel. Pro účely získání eID prostředků úrovně záruky nízká může být užito video identity proofingu za podmínky, že další kroky v procesu vydání, doručení, aktivace eID prostředku umožní potvrdit předpoklad, že osoba pro potvrzení svojí identity používá doklad totožnosti vydaný pro svojí osobu.
Značná	*Nízká úroveň a navíc musí být splněna jedna z alternativ uvedených v bodech 1 až 4:* *1. Bylo ověřeno, že osoba vlastní důkaz deklarované totožnosti uznaný členským státem, ve kterém se žádost o prostředek pro elektronickou identifikaci podává,* *a* *důkaz se zkontroluje, aby se zjistilo, zda je pravý, nebo je podle spolehlivého zdroje známo, že důkaz existuje a vztahuje se ke skutečné osobě,* V případě fyzického prokazování a ověřování totožnosti musí být ověřena pravost dokladu (ochranné prvky viz Veřejný rejstřík pravých dokladů totožnosti a cestovních dokladů - PRADO: http://www.consilium.europa.eu/prado/cs/prado-start-page.html). V případě dokladu vydaného Českou republikou musí být jeho platnost a pravost (ověření údajů na dokladu) ověřena vůči základnímu registru obyvatel. Fyzickou kontrolou osobního identifikačního dokladu je provedena kontrola, že je doklad pravý (nejsou porušeny ochranné prvky). V případě žádosti o vydání nehmotného eID prostředku kompletně elektronickou cestou s využitím datových schránek, musí být osobní identifikační doklad ověřen v základním registru obyvatel (oprávněným držitelem je osoba, z jejíž datové schránky byla žádost

	odeslána). Pozn. Kompletní elektronickou cestou se má na mysli proces, kdy žadatel v žádném kroku není ve fyzickém kontaktu s kvalifikovaným správcem či se subjektem, který provedl prvotní ztotožnění osoby a zároveň se nepoužívá pro vydání nového eID prostředku jiný (stávající) eID prostředek patřící osobě. *a* *byly podniknuty kroky s cílem minimalizovat riziko, že totožnost osoby není deklarovanou totožností, přičemž bylo zohledněno například riziko ztráty, odcizení, zrušení důkazu nebo pozastavení či vypršení jeho platnosti;* Kontrolou vůči osobnímu dokladu opatřeného fotografií před předáním eID prostředku lze rozhodnout, zda se doklad váže k osobě, která má převzít vydaný eID prostředek. V případě realizace žádosti o vydání nehmotného eID prostředku kompletně elektronickou cestou s využitím datových schránek, musí žadatel uvést číslo osobního identifikačního dokladu. Kvalifikovaný správce pak musí v každém případě ověřit platnost dokladu a správnost uvedených údajů ověřením v základním registru obyvatel prostřednictvím národního bodu. Opatření má za cíl snížit riziko možného zneužití přihlašovacích údajů do datové schránky fyzické osoby. *nebo* *2. během procesu registrace se předloží doklad totožnosti v členském státě, kde byl doklad vydán, a doklad se zjevně vztahuje k osobě, která jej předložila,* Žadatel předloží identifikační doklad vydaný Českou republikou. Porovnáním fotografie lze určit, zda se dokument vztahuje k osobě, která jej předložila. Příjemce registrace ověří platnost dokladu vůči základnímu registru obyvatel prostřednictvím národního bodu. Fyzickou kontrolou identifikačního dokladu je provedena kontrola, že je doklad pravý (nejsou porušeny ochranné prvky). Veřejný rejstřík pravých dokladů totožnosti a cestovních dokladů online je k dispozici na adrese: http://www.consilium.europa.eu/prado/cs/prado-start-page.html (Databáze PRADO). V rejstříku PRADO je možné vyhledat informace o typech vydávaných dokladů totožnosti a cestovních dokladech včetně informací o ochranných prvcích. Vyhledávání podle vydávající země: http://www.consilium.europa.eu/prado/cs/search-by-document-country.html. *a* *byly podniknuty kroky s cílem minimalizovat riziko, že totožnost osoby není deklarovanou totožností, přičemž bylo zohledněno například riziko ztráty, odcizení, zrušení dokladů*

	nebo pozastavení či vypršení jejich platnosti; Kvalifikovaný správce musí ověřit platnost předloženého identifikačního dokladu vůči registru obyvatel prostřednictvím národního bodu a může požadovat sekundární osobní doklad žadatele pro rozhodnutí, zda osoba je oprávněným držitelem osobního identifikačního dokladu (např. při pochybnostech porovnáním fotografie). *nebo* *3. pokud postupy, které předtím používal veřejný či soukromý subjekt v témže členském státě za jiným účelem než vydávání prostředků pro elektronickou identifikaci, zajišťují záruky rovnocenné s postupy stanovenými v oddíle 2.1.2 pro značnou úroveň záruky, nemusí subjekt odpovědný za registraci opakovat tyto dřívější postupy za předpokladu, že takovou rovnocennou záruku potvrdí subjekt posuzování shody uvedený v čl. 2 odst. 13 nařízení Evropského parlamentu a Rady (ES) č. 765/2008 [(1)] nebo rovnocenný subjekt;* Rovnocenným subjektem se má na mysli Ministerstvo vnitra České republiky jako dohledový orgán dle zákona o elektronické identifikaci. *nebo* *4. pokud jsou prostředky pro elektronickou identifikaci vydány na základě platných oznámených prostředků pro elektronickou identifikaci, které mají značnou nebo vysokou úroveň záruky, a je přitom přihlédnuto k rizikům změny osobních identifikačních údajů, není nutno postupy prokazování a ověřování totožnosti opakovat. Pokud prostředek pro elektronickou identifikaci sloužící jako základ nebyl oznámen, musí značnou nebo vysokou úroveň záruky potvrdit subjekt posuzování shody uvedený v čl. 2 odst. 13 nařízení (ES) č. 765/2008 nebo rovnocenný subjekt.* Prokázat a ověřit totožnost žadatele je možné realizovat rovněž prostřednictvím již vydaných eID prostředků (případy, kdy žadatel již disponuje platným eID prostředkem a chce si na dálku požádat o vydání jiného eID prostředku). Může být akceptován jak oznámený eID prostředek s úrovní záruky značná a vysoká, tak i „vnitrostátní“ eID prostředek s úrovní záruky značná a vysoká, který byl vydán na základě zákona o elektronické identifikaci a nebyl oznámen EK v souladu s čl. 9 nařízení eIDAS. V případě, kdy se jedná o obnovu či výměnu (tj. žadatel pouze vyměňuje „starý“ prostředek od stejného kvalifikovaného správce za „nový“ nebo se prodlužuje platnost stávajícího eID prostředku), uplatní se požadavky uvedené v kapitole „2.2.4. Obnovení a výměna“.
Vysoká	*Musí být splněny požadavky bodu 1, nebo bodu 2:* *1. Značná úroveň a navíc musí být splněna jedna z alternativ uvedených v písmenech a) až c):*

a)Pokud bylo ověřeno, že osoba vlastní důkaz totožnosti opatřený fotografií nebo biometrickými údaji uznaný členským státem, ve kterém se žádost o prostředky pro elektronickou identifikaci podává, a že důkaz označuje deklarovanou totožnost, důkaz se zkontroluje, aby se zjistilo, zda je podle spolehlivého zdroje platný,

Každý předložený identifikační doklad vydaný Českou republikou, kvalifikovaný správce ověří v základním registru obyvatel prostřednictvím národního bodu z hlediska platnosti a příslušnosti osobě.

a

na základě srovnání jedné nebo více fyzických vlastností osoby s údaji ze spolehlivého zdroje se zjistí, zda se totožnost žadatele shoduje s deklarovanou totožností;

Porovnat, zda se podoba žadatele shoduje s fotografiemi uvedenými na identifikačních dokladech nebo zda osoba zadala správný bezpečnostní osobní kód. Porovnání fyzické podoby musí být učiněno při prezenční kontrole totožnosti (Video identity proofing nepovažuje Ministerstvo vnitra za dostatečně bezpečné a průkazné[5] pro účely vydání eID prostředku s úrovní záruky vysoká).

Z důvodu snížení rizika možného zneužití totožnosti, je nutné pro vydání eID prostředku s nejvyšší úrovní záruky provést jedno z následujících dodatečných ověření totožnosti, nebo provést ověření totožnosti na ekvivalentní úrovni:

- ověřit bezpečnostní osobní kód (dle §8a zákona 328/1999 o občanských průkazech) v případě prezenční kontroly totožnosti
- předložit další doklad ověřitelný v základním registru obyvatel v případě prezenční kontroly totožnosti
- předložit doklad totožnosti vydávaný jiným státem uznávaný Českou republikou, ze kterého je patrno, že doklad patří stejnému žadateli (např. shodné jméno a příjmení a datum narození, rodné číslo, fotka, adresa trvalého pobytu,…)
- předložit doklady vydaný Českou republikou s fotografií žadatele a kde se osobní údaje shodují s primárním osobním identifikačním dokladem
- využít informace o žadateli, které má kvalifikovaný správce k dispozici (biometrická fotografie žadatele, aktuálně vedené osobní údaje,…).

Nebo

[5] Při video-proofingu není možné důvěryhodně zkontrolovat, zda nejsou porušeny ochranné prvky dokladů.

b) pokud postupy, které předtím používal veřejný či soukromý subjekt v témže členském státě za jiným účelem než vydávání prostředků pro elektronickou identifikaci, zajišťují záruky rovnocenné s postupy stanovenými v oddíle 2.1.2 pro vysokou úroveň záruky, nemusí subjekt odpovědný za registraci opakovat tyto dřívější postupy za předpokladu, že takovou rovnocennou záruku potvrdí subjekt posuzování shody uvedený v čl. 2 odst. 13 nařízení Evropského parlamentu a Rady (ES) č. 765/2008 nebo rovnocenný subjekt,

Rovnocenným subjektem se má na mysli Ministerstvo vnitra České republiky jako dohledový orgán dle zákona o elektronické identifikaci.

a

jsou podniknuty kroky s cílem prokázat, že výsledky předchozích postupů zůstávají v platnosti;

Před vydáním nebo prvním použitím eID prostředku v rámci kvalifikovaného systému eID prostředku má kvalifikovaný správce povinnost, dle zákona o elektronické identifikaci, ověřit totožnost držitele eID prostředku prostřednictvím národního bodu vůči základnímu registru obyvatel. Tímto se docílí splnění požadavku, že deklarovaná identita existuje a nedošlo např. ke změně jména osoby.

Nebo

c) pokud jsou prostředky pro elektronickou identifikaci vydány na základě platného oznámeného prostředku pro elektronickou identifikaci, který má značnou nebo vysokou úroveň záruky, a je přitom přihlédnuto k rizikům změny osobních identifikačních údajů, není nutno opakovat postupy prokazování a ověřování totožnosti. Pokud prostředek pro elektronickou identifikaci sloužící jako základ nebyl oznámen, musí vysokou úroveň záruky potvrdit subjekt posuzování shody uvedený v čl. 2 odst. 13 nařízení (ES) č. 765/2008 nebo rovnocenný subjekt,

a

Rovnocenným subjektem se má na mysli Ministerstvo vnitra České republiky jako dohledový orgán dle zákona o elektronické identifikaci.

jsou podniknuty kroky s cílem prokázat, že výsledky předchozího postupu vydávání oznámeného prostředku pro elektronickou identifikaci zůstávají v platnosti.

Prokázat a ověřit totožnost žadatele je možné realizovat rovněž prostřednictvím již vydaných eID prostředků (případy, kdy žadatel již disponuje platným eID prostředkem a chce si na dálku požádat o jiný eID prostředek). Může být akceptován jak eID prostředek oznámený EK v souladu s čl. 9 nařízení eIDAS s úrovní záruky vysoká, tak i eID prostředek s úrovní záruky vysoká, který byl vydán na základě zákona o elektronické identifikaci a nebyl oznámen EK v souladu s čl. 9 nařízení eIDAS.

V případě, kdy se jedná o obnovu či výměnu (tj. žadatel pouze vyměňuje „starý“ prostředek od stejného kvalifikovaného správce za „nový“ nebo se prodlužuje platnost

	stávajícího eID prostředku), uplatní se požadavky uvedené v kapitole „2.2.4. Obnovení a výměna“. Před vydáním nebo prvním použitím eID prostředku v rámci kvalifikovaného systému má kvalifikovaný správce povinnost, dle zákona o elektronické identifikaci, ověřit totožnost držitele eID prostředku prostřednictvím národního bodu vůči základnímu registru obyvatel. Tímto se docílí splnění požadavku, že deklarovaná identita existuje a nedošlo např. ke změně jména osoby. *NEBO* *2.Pokud žadatel nepředloží žádný uznaný důkaz totožnosti opatřený fotografií nebo biometrickými údaji, uplatní se naprosto stejné postupy, jaké se pro získání takového uznaného důkazu totožnosti opatřeného fotografií nebo biometrickými údaji používají na vnitrostátní úrovni v členském státě subjektu odpovědného za registraci.* Uplatní se při žádosti o vydání občanského průkazu umožňujícího elektronickou identifikaci dle zákona č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů.

2.2. Kapitola „Správa prostředků pro elektronickou identifikaci“ přílohy CIR 2015/1502

2.2.1. Vlastnosti a forma prostředků pro elektronickou identifikaci.

Úroveň záruky	***Potřebné prvky***
Nízká	*1.Prostředek pro elektronickou identifikaci využívá alespoň jednoho faktoru autentizace.* eID prostředek musí využívat alespoň jednoho faktoru autentizace (faktor autentizace na základě vlastnictví nebo faktor autentizace na základě znalostí nebo inherentní faktor autentizace). *2.Prostředek pro elektronickou identifikaci je navržen tak, aby vydavatel mohl přijmout přiměřené kroky k ověření toho, zda se používá pouze pod kontrolou nebo v rámci vlastnictví osoby, které patří.* Požadavek souvisí s procesem vydání, doručení a aktivace eID prostředku. Tj. jakým způsobem je eID prostředek předán uživateli, viz kapitola 2.2.2. Vydání, doručení

	a aktivace.
Značná	*1. Prostředek pro elektronickou identifikaci využívá alespoň dvou faktorů autentizace z odlišných kategorií.* Požadavek využití alespoň dvou faktorů autentizace z odlišných kategorií zvyšuje bezpečnost eID prostředku (a procesu autentizace). Příkladem může být čipová karta či token, u které je nutné znát PIN k odemčení karty či tokenu. *2. Prostředek pro elektronickou identifikaci je navržen tak, aby bylo možno předpokládat, že se používá pouze pod kontrolou nebo v rámci vlastnictví osoby, které patří.* Díky požadavku alespoň dvou faktorů autentizace z odlišných kategorií je dosaženo toho, že v případě zcizení např. čipové karty nemůže útočník eID prostředek použít, neboť nezná heslo či nedisponuje fyzickou vlastností (např. otiskem prstu), kterým by kartu mohl odemknout.
Vysoká	*Značná úroveň a navíc:* *1. Prostředek pro elektronickou identifikaci chrání proti vyhotovování duplikátů a neoprávněné manipulaci i proti útočníkům s vysokým potenciálem útoku.* Ochrana proti vyhotovování duplikátů a neoprávněné manipulaci se týká celého eID prostředku, nikoli jen jednotlivých autentizačních faktorů, které eID prostředek využívá. Např. v případě použití čipových karet a kryptografických klíčů na ní uložených, karta (a obslužný SW na kartě) musí chránit soukromé klíče tak, aby se nemohly z karty exportovat. Vhodnou formou prokázání těchto vlastností je např. certifikace dle Common Criteria. *2. Prostředek pro elektronickou identifikaci je navržen tak, aby jej mohla osoba, které patří, spolehlivě chránit před zneužitím třetí osobou.* V případě čipové karty vyžadovat vždy zadání PIN k odblokování. Dále např. politika pro vytváření hesel (délka hesla, platnost) v případě použití statických hesel, důraz na používání bezpečných kryptografických algoritmů. Stanovení maximálního počtu neúspěšných pokusů, …

2.2.2. Vydání, doručení a aktivace.

Úroveň záruky	*Potřebné prvky*
Nízká	*Po vydání je prostředek pro elektronickou identifikaci doručen prostřednictvím mechanismu, na základě kterého lze předpokládat, že prostředek dostane pouze určená osoba.* Pokud eID prostředek využívá pouze jediného faktoru autentizace, aktivační link (nebo např. OTP heslo potřebné k aktivaci prostředku) musí být poslán na e-mail/telefon/adresu, který byl v předchozích krocích ověřen, že je pod kontrolou dotyčné osoby. Možné jsou samozřejmě i další formy důvěryhodnější formy doručení – např. osobní předání, doručení prostřednictvím doporučené pošty do vlastních rukou.
Značná	*Po vydání je prostředek pro elektronickou identifikaci doručen prostřednictvím mechanismu, na základě kterého lze předpokládat, že je prostředek předán pouze do vlastnictví osoby, které patří.* Možné metody doručení zahrnují osobní předání, doručení prostřednictvím doporučené pošty do vlastních rukou. Je možné využít i další metody, přičemž ale jednotlivé faktory autentizace eID prostředku musejí být doručeny žadateli nezávisle na sobě – tj. využití různých doručovacích kanálů (např. fyzické poslání eID prostředku poštou na adresu osoby a aktivační link či heslo na ověřený telefon). V případě fyzického předávání eID prostředku osoba musí předložit osobní doklad totožnosti, který je uveden v žádosti a byla tedy ověřena jeho platnost vůči základnímu registru obyvatel prostřednictvím národního bodu nejpozději před prvním použitím v rámci kvalifikovaného systému. Požadavek stejného dokladu je stanoven z toho důvodu, aby osoba předávající prostředek nemusela disponovat prostředky pro ověření jiného dokladu totožnosti v registru obyvatel. Pokud proces registrace probíhá čistě v elektronické podobě, je nutné použít pro doručení jednoho faktoru autentizace, či aktivačního linku nebo OTP hesla potřebného k aktivaci prostředku, datové schránky.
Vysoká	*V procesu aktivace se ověří, že byl prostředek pro elektronickou identifikaci předán pouze do vlastnictví osoby, které patří.* Je povinně vyžadován proces aktivace. Tj. samotné důvěryhodné předání prostředku není pro tuto úroveň dostatečné. Aktivační proces obecně vyžaduje interakci žadatele. Cílem aktivačního procesu je kromě potvrzení toho, že eID prostředek byl doručen správnému žadateli, také výslovný krok žadatele pro potvrzení vlastnictví prostředku. Teprve poté může být eID prostředek používán. Aktivační proces musí zajistit, že pouze oprávněný

	žadatel může aktivovat eID prostředek a dále že aktivační proces je chráněn před náhodnými ztrátami a hrozbami ze strany insiderů (osob z okruhu zaměstnanců či dodavatelů kvalifikovaného správce). Kompletní proces registrace a aktivace eID prostředku nesmí spočívat v rukou pouze jedné osoby tak, aby byla snížena možnost selhání jedné osoby. Pokud jsou použity aktivační kódy, musí být stanovena jejich dočasná platnost. Pod doručením eID prostředku si lze například představit i personalizaci stažené mobilní aplikace (například zadáním PINu, hesla či jiných údajů do stažené aplikace), tím dojde k doručení eID prostředku. Tj. doručení eID prostředku nemusí nutně znamenat pouze fyzické doručení. Aktivační proces se skládá z dílčích kroků, z nich jeden může být právě doručení aktivačního kódu. Tzn. aktivační proces nezahrnuje pouze samotný úkon aktivace eID prostředku. Jako příklady splnění podmínky lze uvést: • vydání eID prostředku na registračním místě a doručení aktivačního kódu běžnou poštou na ověřenou adresu žadatele. • doručení eID prostředku, o který bylo požádáno prostřednictvím on-line procesu, běžnou poštou a vyzvednutí aktivačního kódu u důvěryhodného subjektu oproti prokázání totožnosti. • fyzické doručení eID prostředků důvěryhodným kurýrem a předání prostředku po ověření totožnosti žadatele. Aktivační kód odesílán samostatně prostřednictvím jiného doručovacího kanálu (např. poštou na ověřenou adresu uživatele). • vydání nehmotného eID prostředku na základě vzdáleného ověření identity na úrovni vysoká a předání aktivačního kódu s ověřením totožnosti příjemce (např. poštou na ověřenou adresu nebo prostřednictvím datových schránek)

2.2.3. Pozastavení, zrušení a reaktivace.

Úroveň záruky	***Potřebné prvky***
Nízká	*1.Prostředek pro elektronickou identifikaci je možné včas a účinným způsobem pozastavit a/nebo zrušit.* Existence služby pozastavení nebo zneplatnění eID prostředku, která je veřejně dostupná např. po telefonu, webu, e-mailem apod. Prostředek musí být pozastaven nebo zneplatněn co nejdříve ze strany kvalifikovaného správce (po ověření pravosti žádosti o pozastavení nebo zneplatnění). Povinnost zneplatnit eID prostředek je stanovena rovněž zákonem o elektronické identifikaci (viz § 16 odst. 1 písm. h)).

	2.Existují opatření přijatá s cílem zabránit neoprávněnému pozastavení, zrušení a/nebo reaktivaci. Před pozastavením či zneplatněním eID prostředku musí kvalifikovaný správce ověřit pravost žádosti o pozastavení či zneplatnění eID prostředku. V rámci definice služby musí být stanoveno, kdo všechno může žádat o pozastavení nebo zneplatnění eID prostředku. *3.Reaktivaci je možné provést, pouze pokud budou nadále splněny stejné požadavky na záruku, které byly stanoveny před pozastavením nebo zrušením.* V případě žádosti o opětovnou aktivaci pozastaveného eID prostředku, je nutné ověřit pravost žádosti o reaktivaci se stejnou úrovní záruky jako je vydání prostředku.
Značná	*Stejné jako při nízké úrovni.*
Vysoká	*Stejné jako při nízké úrovni.*

2.2.4. Obnovení a výměna.

Úroveň záruky	***Potřebné prvky***
Nízká	*S přihlédnutím k rizikům změny osobních identifikačních údajů musí obnova nebo výměna splňovat stejné požadavky na záruku jako původní prokazování a ověřování totožnosti nebo vycházet z platného prostředku pro elektronickou identifikaci se stejnou nebo vyšší úrovní záruky.* V případě, kdy bude žádáno o obnovu či výměnu eID prostředku, musí být použit platný eID prostředek se stejnou nebo vyšší úrovní záruky. V opačném případě musí uživatel podstoupit registrační proces znovu. Současně při vydání eID prostředku kvalifikovaný správce ověří aktuálnost údajů dotazem do základních registrů prostřednictvím národního bodu.
Značná	*Stejné jako při nízké úrovni.*
Vysoká	*Nízká úroveň a navíc:* *Pokud obnovení nebo výměna probíhá na základě platného prostředku pro elektronickou identifikaci, ověří se údaje o totožnosti podle spolehlivého zdroje.* Díky tomu, že kvalifikovaný správce má povinnost aktualizovat údaje v evidenci vydaných eID prostředků na základě upozornění správce národního bodu pro identifikaci a autentizaci o změně údajů (viz §16 odst. 1 písm. e)), bude zajištěno, že kvalifikovaný správce bude mít k dispozici vždy aktuální údaje o totožnosti uživatele.

2.3. Kapitola „Autentizace“ přílohy CIR 2015/1502

Tento oddíl se zaměřuje na hrozby související s používáním mechanismu autentizace a obsahuje požadavky pro každou úroveň záruky. Kontroly se v tomto oddíle považují za přiměřené rizikům na dané úrovni.

2.3.1. Mechanismus autentizace.

Mechanismus autentizace sám o sobě nemůže úplně zabránit všem útokům, může ale poskytnout ochranu vůči útokům určité úrovně. Standardní způsob určení odolnosti různých mechanismů autentizace spočívá v zařazení do skupin a to podle odolnosti mechanismu proti útokům s určitým potenciálem útoku.

V rámci jednotlivých úrovní záruky jsou použity termíny „zvýšený základní“, „mírný“ a „vysoký“ potenciál pro označování různých potenciálů útoků. Tato terminologie vychází z normy ISO / IEC 15408 "Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT " a normy ISO / IEC 18045 "Informační technologie - Bezpečnostní techniky - Metodika hodnocení IT bezpečnosti". Text standardů je také volně k dispozici na adrese www.commoncriteriaportal.org/cc (Common Criteria části 1-3 odpovídají normě ISO / IEC 15408 a CEM [Common Methodology for Information Technology Security Evaluation] odpovídá normě ISO / IEC 18045).

Norma ISO / IEC 15408-1 definuje "potenciál útoku jako míru úsilí vynaloženého na útočení z hlediska odbornosti, zdrojů a motivace útočníka".

Příloha B. 4 normy ISO / IEC 18045 / CEM obsahuje pokyny pro výpočet potenciálu útoku potřebného k využití dané slabiny mechanismu autentizace.

Aby bylo možné splnit požadavky stanovené v prováděcím aktu, mělo by být provedeno určité posouzení odolnosti mechanismu autentizace proti potenciálním útokům (např. penetrační testy). Hodnocení by mělo vzít v úvahu příslušné hrozby. Například norma ISO 29115 uvádí následující hrozby: hádání, offline analýza, reprodukce, phishing, odposlouchávání, replay útok, krádež relace, man-in-the-middle, krádež přihlašovacích údajů, spoofing a masquerading.

Při posuzování odolnosti mechanismu autentizace proti útokům je třeba vzít v úvahu celý mechanismus autentizace včetně rizik vyplývajících z ověření vlastnictví eID prostředků.

Například:

• Pro vysokou úroveň záruky je nutné nejen, aby čipová karta chránila kryptografický klíč proti manipulaci s vysokým potenciálem útoku, ale také, aby použitý kryptografický protokol poskytoval dostatečnou ochranu mechanismu ověření vlastnictví klíče proti manipulaci komunikace/opakování s vysokým potenciálem útoku.

• Pro token s OTP heslem, kdy se generované jednorázové heslo předává prostřednictvím zabezpečeného kanálu (např. TLS), je odolnost tohoto faktoru autentizace založeného na vlastnictví omezena nejen silou tokenu, ale také mírou bezpečnosti daného zabezpečeného kanálu.

• Mechanismus pro prokázání vlastnictví generátoru jednorázového hesla založeného na čase je založeno na předání tohoto hesla kvalifikovanému správci. Síla tohoto mechanismu je omezena mimo jiné délkou jednorázového hesla, omezenou časovou platností hesla a bezpečností přenosu.

Při posuzování rizika by měly být vzaty rovněž v úvahu přiměřené předpoklady týkající se úrovně bezpečnosti použitých prvků, které nejsou pod správou kvalifikovaného správce (např. prostředí uživatele, prohlížeč, chytrý telefon atd.). Tyto prvky lze obvykle provozovat v různých konfiguracích s různými bezpečnostními nastaveními. Jako příklad lze uvést, že hodnocení rizik může předpokládat, že uživatel (držitel eID prostředku) provozuje na svém počítači firewall a antivir. Naproti tomu, v současné době by nebylo rozumné předpokládat, že prohlížeč uživatele je konfigurován tak, aby používal pouze zabezpečené šifrovací sady TLS - nicméně toto může být vynuceno mechanismem autentizace.

V rámci hodnocení rizik mohou být předpokládána přiměřená nastavení pro prvky, které nejsou součástí systému ověřování.

Úroveň záruky	*Potřebné prvky*
Nízká	*1. Vydání osobních identifikačních údajů předchází spolehlivé ověření prostředku pro elektronickou identifikaci a jeho platnosti.* *2. Pokud jsou osobní identifikační údaje uloženy jako součást mechanismu autentizace, jsou tyto informace zabezpečeny proti ztrátě a vyzrazení, včetně offline analýzy.* Pro uložená osobní data musí být zavedena kontrola přístupu. Měla by být zavedena opatření na ochranu osobních identifikačních údajů, například šifrování a hašování v souladu s osvědčenou praxí, jako např. doporučení od agentury ENISA nebo národní kryptografické „katalogy“. Veškerý přístup k osobním identifikačním údajům musí být auditován. *3. Mechanismus autentizace provádí bezpečnostní kontroly k ověření prostředku pro elektronickou identifikaci, takže je velmi nepravděpodobné, že by činnosti jako hádání, odposlech, reprodukce nebo manipulace komunikace ze strany útočníka se zvýšeným základním potenciálem útoku mohly mechanismy autentizace narušit.* Všechny nezbytné kroky vedoucí k ověření eID prostředku musí být jasně popsány, implementovány a testovány. Kvalifikovaný správce zavedením politiky hesel stanovuje minimální bezpečností požadavky na kvalitu hesla. V případě, kdy uživatel bude chtít zvolit heslo, které neodpovídá stanovené politice, takové heslo odmítnout.
Značná	*Nízká úroveň a navíc:* *1. Vydání osobních identifikačních údajů předchází spolehlivé ověření prostředku pro elektronickou identifikaci a jeho platnosti prostřednictvím dynamické autentizace.* V praxi to znamená, že eID prostředky by měly využívat buď jednorázový kód, nebo jednorázový challenge-response, aby se zajistilo splnění požadavku na dynamickou autentizaci. Jednorázový kód nebo výzva (challenge) by se měly vytvářet způsobem, který neumožní jeho manipulaci a opakované neoprávněné použití výzvy. Při použití náhodných čísel v challenge-response protokolu, je třeba dbát na zajištění "kvality" těchto náhodných čísel (například dodržením osvědčených postupů pro bezpečné generátory pseudonáhodných čísel). *2. Mechanismus autentizace provádí bezpečnostní kontroly k ověření prostředku pro elektronickou identifikaci, takže je velmi nepravděpodobné, že by činnosti jako hádání, odposlech, reprodukce nebo manipulace komunikace ze strany útočníka*

	s mírným potenciálem útoku mohly mechanismy autentizace narušit.
Vysoká	*Značná úroveň a navíc:* *Mechanismus autentizace provádí bezpečnostní kontroly k ověření prostředku pro elektronickou identifikaci, takže je velmi nepravděpodobné, že by činnosti jako hádání, odposlech, opakování nebo manipulace komunikace ze strany útočníka s vysokým potenciálem útoku mohly mechanismy autentizace narušit.* V případě použití kryptografie v rámci mechanismu autentizace musí být vybrány dostatečně silné kryptografické protokoly a bezpečné délky klíčů. Důležitou metodou pro zajištění dostatečné odolnosti kryptografických protokolů jsou kryptografické analýzy, jako například důkazy o kryptografické bezpečnosti daných algoritmů. Je třeba zajistit používání bezpečných protokolů a případně zavést příslušná opatření, pokud se ukáže, že na použitý protokol byly nalezeny nové metody útoků, které ovlivňují bezpečnost těchto protokolů. V případě, kdy mechanismus autentizace používá řešení založené na kryptografii, je nutno vzít v úvahu nejen kryptografické primitivy, ale i protokoly a prostředí, zejména správu klíčů. Typickým mechanismem správy klíčů je využití infrastruktury veřejného klíče (PKI). Provozní bezpečnost CA přímo ovlivňuje bezpečnost autentizačního mechanismu. Je-li použito několik CA pro vydávání certifikátů pro určité části systému elektronické identifikace, musí být vzata v úvahu celková bezpečnost všech důvěryhodných certifikačních autorit. Obecně, v souladu s osvědčenou praxí, pokud infrastruktura systému elektronické identifikace je založena na využití PKI, pak pro vysokou úroveň by mělo být uživateli doporučeno používat odpovídající bezpečnostní mechanismy.

2.4. Kapitola „Řízení a organizace“ přílohy CIR 2015/1502

Všichni účastníci, kteří poskytují služby související s elektronickou identifikací v přeshraničním kontextu (dále jen „poskytovatelé“), musí mít zavedeny dokumentované postupy řízení bezpečnosti informací, politiky, přístupy k řízení rizik a další uznané kontroly, aby správním orgánům příslušným pro systémy elektronické identifikace v jednotlivých členských státech poskytli záruku, že se používají účinné postupy. Všechny požadavky/prvky v oddíle 2.4 se považují za přiměřené rizikům na dané úrovni.

Vyjádření „Všichni účastníci“ zahrnuje subjekty zapojené v procesu elektronické identifikace, včetně kvalifikovaného správce a případné ověřovací služby provozované členským státem (pokud existuje), nikoli však autoritativní zdroje.

Obecnou zásadou v řízení rizik je, že je na organizaci, aby si zvolila, kterou úroveň rizika považuje za přijatelnou. Tato obecné zásada je pozměněna požadavky uvedenými v této kapitole, jelikož organizace by měla mít zavedeny opatření, které odpovídají rizikům pro danou úroveň záruky.

Většina požadavků této kapitoly je splněna, pokud:

- je zaveden a auditován systém managementu bezpečnosti informací podle normy ČSN ISO / IEC 27001: 2013 nebo
- poskytovatelé, kteří poskytují provozní služby, jsou kvalifikovaní poskytovatelé služeb vytvářejících důvěru podle nařízení eIDAS.

Výše uvedené nevylučuje použití další standardů, např. aby byly použity vhodné vnitrostátní systémy a požadavky, které splňují požadavky uvedené v kapitole. V případě systému řízení bezpečnosti informací podle normy ČSN ISO / IEC 27001: 2013 jsou všechny požadavky uvedené v oddílech 2.4.4 - 2.4.6 kapitoly „Řízení a organizace“ přílohy CIR 2015/1502 zahrnuty do příslušných opatření z této normy.

2.4.1. Obecná ustanovení.

Úroveň záruky	***Potřebné prvky***
Nízká	*1. Poskytovateli provozních služeb, na které se vztahuje toto nařízení, jsou orgány veřejné správy nebo právnické osoby uznané jako takové podle vnitrostátního práva členského státu, které mají zavedenou organizační strukturu a jsou plně provozuschopné ve všech úsecích relevantních pro poskytování služeb.* *2. Poskytovatelé dodržují všechny právní požadavky, které se na ně vztahují v souvislosti s provozem a poskytováním služby, včetně druhů informací, které je možno požadovat, způsobů ověřování totožnosti a upřesnění, jaké informace mohou být uchovávány a jak dlouho.* *3. Poskytovatelé jsou s to prokázat svou schopnost převzít riziko odpovědnosti*

	za škodu, jakož i dostatek finančních prostředků pro nepřetržitý provoz a poskytování služeb. Na základě zákona o elektronické identifikaci musí být žadatel o akreditaci pojištěn pro případ odpovědnosti za škodu způsobenou při správě kvalifikovaného systému (viz § 9 zákona). Povinnost pojištění se netýká státních orgánů, u kterých se předpokládá, že disponují dostatečnými finančními prostředky k pokrytí případných škod. 4. *Poskytovatelé nesou odpovědnost za plnění veškerých závazků zadaných externím subjektům a za dodržování politiky systému, jako by tyto povinnosti plnili sami.* 5. *Systémy elektronické identifikace, které nebyly zřízeny podle vnitrostátního práva, musí mít zavedeny účinný plán ukončení činnosti. Tento plán musí zahrnovat řádné ukončení služby nebo pokračování jiným poskytovatelem, způsob, jakým jsou informovány příslušné orgány a koneční uživatelé, a podrobnosti, jak mají být chráněny, uchovávány a ničeny záznamy v souladu s politikou systému.* Povinnost mít stanoven plán ukončení činností vyplývá přímo z § 15 zákona o elektronické identifikace a platí jak pro státní orgány, tak i pro akreditované osoby. V plánu ukončení činnosti uvede kvalifikovaný správce postupy při ukončení vydávání a používání prostředků pro elektronickou identifikaci a poskytnutí služby autentizace, včetně způsobu, jakým jsou správce národního bodu a držitelé prostředků pro elektronickou identifikaci informováni o ukončení činnosti kvalifikovaného správce. Plán musí počítat s předvídatelnými okolnostmi, které mohou vést k ukončení činnosti (např. zánik právnické osoby, nedostatek finančních zdrojů, rozhodnutí o ukončení služeb,…).
Značná	*Stejné jako při nízké úrovni.*
Vysoká	*Stejné jako při nízké úrovni.*

2.4.2. Zveřejněná oznámení a informace pro uživatele.

Úroveň záruky	***Potřebné prvky***
Nízká	*1. Existuje zveřejněná definice služby, která zahrnuje všechny platné podmínky a poplatky, včetně veškerých omezení jejího používání. Definice služby zahrnuje politiku ochrany osobních údajů.*

	Informace jsou uvedeny ve veřejně přístupných dokumentech (nejčastěji zveřejněny prostřednictvím webu kvalifikovaného správce) nebo např. také v zákonech. *2.Je nutno zavést vhodnou politiku a postupy, které zajistí, aby byli uživatelé služby včas a spolehlivým způsobem informováni o veškerých změnách definice služeb a platných podmínek a politiky ochrany osobních údajů u dané služby.* Povinnost informovat uživatele o veškerých změnách v definici služby a platných podmínek může být splněno nejen notifikací uživatelů (emailem, zobrazením upozornění v jeho uživatelském profilu, apod.), ale také patřičným upozorněním na změny na internetových stránkách kvalifikovaného správce. *3.Je nutno zavést vhodné politiky a postupy, které zajistí úplné a správné odpovědi na žádosti o informace.*
Značná	*Stejné jako při nízké úrovni.*
Vysoká	*Stejné jako při nízké úrovni.*

2.4.3. Řízení bezpečnosti informací.

Úroveň záruky	**Potřebné prvky**
Nízká	Existuje účinný systém řízení bezpečnosti informací pro řízení a kontrolu rizik v oblasti bezpečnosti informací. Řízení rizik informační bezpečnosti je relevantní pro všechny část eID systému. V rámci systému řízení bezpečnosti informací musí být brány v potaz rizika pro všechny části systému.
Značná	Nízká úroveň a navíc: Systém řízení bezpečnosti informací dodržuje osvědčené normy nebo zásady řízení a kontroly rizik v oblasti bezpečnosti informací. Norma ČSN ISO / IEC 27001: 2013 je známým a osvědčeným standardem pro řízení rizik bezpečnosti informací. Viz také část 2.4.7 pro zajištění souladu s požadavky.
Vysoká	Stejné jako při značné úrovni.

2.4.4. Vedení záznamů.

Úroveň záruky	**Potřebné prvky**
Nízká	1.Zaznamenávání a uchovávání příslušných informací prostřednictvím účinného systému správy záznamů při zohlednění platných právních předpisů a osvědčených postupů

	v souvislosti s ochranou údajů a uchováváním údajů. Kvalifikovaný správce má povinnost dle §22 zákona o elektronické identifikaci uchovávat po dobu 15 let údaje související s evidencí vydaných eID prostředků. Použitý systém pro správu a uchování záznamů musí zajistit integritu a důvěrnost záznamů po celou dobu jejich uchování. V rámci systému řízení bezpečnosti informací implementovaného podle normy ČSN ISO / IEC 27001: 2013 je tento požadavek zahrnut jako součást opatření - A.12 "Bezpečnost provozu" v kombinaci s A.18 "Soulad s požadavky" (zejména požadavek A.12.4 zaznamenávání formou logů a monitorování). 2. Uchovávání, pokud to povolují vnitrostátní právní předpisy nebo jiná vnitrostátní správní opatření, a ochrana záznamů po dobu potřebnou pro účely auditu, vyšetřování případů narušení bezpečnosti a ukládání dat a jejich následné bezpečné zničení. Po uplynutí zákonem stanovené lhůty 15 let, musí být údaje související s evidencí vydaných eID prostředků bezpečně zničeny. V rámci systému řízení bezpečnosti informací implementovaného podle normy ČSN ISO / IEC 27001: 2013 je tento požadavek zahrnut jako součást opatření - A.18 "Soulad s požadavky" (viz požadavek A.18.1.3).
Značná	Stejné jako při nízké úrovni.
Vysoká	Stejné jako při nízké úrovni.

2.4.5. Zařízení a personál.

V následující tabulce jsou uvedeny požadavky týkající se zařízení a personálu a případně subdodavatelů, kteří vykonávají úkoly v oblasti působnosti tohoto nařízení. Shoda s každým z požadavků musí být úměrná úrovni rizika spojeného s poskytovanou úrovní záruky.

Úroveň záruky	***Potřebné prvky***
Nízká	*1. Existují postupy, které zajistí, aby zaměstnanci a subdodavatelé měli dostatečnou odbornou přípravu a dostatečné kvalifikace a zkušenosti v dovednostech nutných k výkonu úkolů, které plní.* V případě, kdy zaměstnanci/dodavatelé plní úkoly vyžadující zvláštní znalosti/ dovednosti, musí být zaveden program vzdělávání a školení, který zajistí patřičné znalosti a dovednosti zaměstnanců/subdodavatelů v průběhu času včetně prokázání, že zaměstnanec/dodavatel disponuje potřebnými znalostmi/ dovednostmi. Mezi povinnosti kvalifikovaného správce patří rovněž dle §16 zákona o elektronické identifikaci zajistit, aby řídící činnosti při správě kvalifikovaného systému vykonávaly fyzické osoby, které získaly vysokoškolské vzdělání v rámci akreditovaného bakalářského nebo magisterského studijního programu a mají praxi v oblasti informačních technologií v délce nejméně 3 let, nebo fyzické osoby, které získaly středoškolské vzdělání a mají praxi

	v oblasti informačních technologií v délce nejméně 5 let. Kvalifikovaný správce musí dále zajistit, aby fyzické osoby, které vykonávají řídící činnosti při správě kvalifikovaného systému, a fyzické osoby, které ověřují totožnost držitele, byly bezúhonné. Dobrá praxe pro zaměstnance, kteří kontrolují pravost fyzických dokumentů (např. ověřují totožnost fyzických osob -tj. provádí kontrolu identifikačních dokladů): • jsou si vědomi nebezpečí krádeže a zneužití cizí identity, • mají patřičné znalosti a schopnosti odhalit případné anomálie v dokumentech jako jsou pravopisné chyby, odlišná písma, chybějící stránky a nesrovnalosti v rozvržení a zarovnání dokumentu. • jsou schopni odhalit poškozené či záměrně upravené dokumenty. • jsou pravidelně školeni jak provádět kontrolu identifikačních dokladů včetně kontroly jejich bezpečnostních prvků. V rámci systému řízení bezpečnosti informací implementovaného podle normy ČSN ISO / IEC 27001: 2013 je tento požadavek pokryt jako součást opatření - A.7 "Bezpečnost lidských zdrojů" (viz zejména A.7.2.2). *2.Zaměstnanci a subdodavatelé jsou v dostatečném počtu potřebném k adekvátnímu provozu služby a zajištění přiměřených zdrojů v souladu s jejími politikami a postupy.* V rámci systému řízení bezpečnosti informací implementovaného podle normy ČSN ISO / IEC 27001: 2013 je tento požadavek pokryt jako součást opatření - A.12 "Bezpečnost provozu" (viz bod A.12.1.2 "Řízení kapacit"), který se rovněž zabývá kapacitou lidských zdrojů. *3.Zařízení používaná pro poskytování služby jsou nepřetržitě monitorována a chráněna proti škodám způsobeným ekologickými událostmi, neoprávněným přístupem a jinými faktory, které mohou ovlivnit bezpečnost služby.* Kriticky důležité služby, např. služba pro zneplatnění eID prostředků, musí být odolná vůči výpadkům a přerušením. Tyto služby musí být dostatečně chráněny proti přírodním událostem, jako jsou požáry, povodně, bouře a zemětřesení apod. Mezi povinnosti kvalifikovaného správce patří dle zákona o elektronické identifikaci bez zbytečného odkladu zneplatnit eID prostředek držitele, o kterém se prokazatelně dozvěděl, že zemřel, nebo byl prohlášen za mrtvého, a dále také zneplatnit eID prostředek na základě žádosti držitele, nebo na základě ohlášení držitele o zneužití nebo hrozícím nebezpečí zneužití prostředku pro elektronickou identifikaci. Tzn. tyto požadavky vyžadují, aby služba pro zneplatnění eID prostředku byla dostatečně robustní a odolná proti možným výpadkům. Pokud je to vhodné a možné, zařízení používané pro zajištění služeb elektronické identifikace, by mělo být fyzicky zabezpečeno pomocí umístění do vhodných prostor opatřených zámky, řízením přístupu a fyzického sledování (např. CCTV). Tyto služby může zajišťovat např. správce objektu, není tedy nutné, aby kvalifikovaný správce tyto funkce

	nutně vykonával sám. Musí být zaveden proces sledování neoprávněného přístupu a případného upozornění, pokud dojde k detekci neoprávněného přístupu/události. V rámci systému řízení bezpečnosti informací implementovaného podle normy ČSN ISO / IEC 27001: 2013 je tento požadavek pokryt jako součást opatření - A.11 "Fyzická bezpečnost a bezpečnost prostředí" a A.9 "Řízení přístupu". Monitorovací mechanismy by měly být také považovány za součást opatření - A.12 "Bezpečnost provozu". *4.Zařízení používaná pro poskytování služby zajišťují, že přístup do prostor, v nichž se uchovávají nebo zpracovávají osobní, kryptografické nebo jiné citlivé informace, mají pouze oprávnění zaměstnanci nebo subdodavatelé.* V rámci systému řízení bezpečnosti informací implementovaného podle normy ČSN ISO / IEC 27001: 2013 je tento požadavek pokryt jako součást opatření - A.9 "Řízení přístupu", jehož cílem je zejména omezit přístup k informacím a zařízením na zpracování informací, A.10 "Kryptografie" a A.18.1.5 "Regulace kryptografických opatření".
Značná	*Stejné jako při nízké úrovni.*
Vysoká	*Stejné jako při nízké úrovni.*

2.4.6. Technické kontroly.

Úroveň záruky	***Potřebné prvky***
Nízká	*1.Existují přiměřené technické kontroly za účelem řízení rizik ohrožujících bezpečnost služeb a na ochranu důvěrnosti, integrity a dostupnosti zpracovávaných informací.* Je důležité oddělit posouzení požadavků na ochranu důvěrnosti a integrity. Zatímco ochrana integrity (nebo pravosti) je v zásadě určena úrovní záruky, důvěrnost osobních údajů musí rovněž vzít v úvahu druh údajů a možné právní požadavky na jejich ochranu. Musí být zajištěna ochrana osobních údajů, musí být proto zavedeny kontroly založené na posouzení míry rizika podle zvoleného systému řízení bezpečnosti informací. Měly by být vzaty v potaz ochrana před hackingem, zneužitím a nesprávným použitím údajů, opatření proti DoS a DDoS útokům. Zajištění důvěrnosti a integrity přenášených osobních údajů při přeshraničním elektronické identifikaci se řídí CIR 2015/1501[6].

[6] PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2015/1501 ze dne 8. září 2015 o rámci interoperability podle čl. 12 odst. 8 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu

	V rámci systému řízení bezpečnosti informací implementovaného podle normy ČSN ISO / IEC 27001: 2013 je tento požadavek pokryt jako součást opatření - A.10 "Kryptografie", A.12 "Bezpečnost provozu" (vztahující se k dostupnosti) A.17 "Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací" a A.18.1.5 "Regulace kryptografických opatření".
	2. Kanály elektronické komunikace používané pro výměnu citlivých nebo osobních informací jsou chráněny proti odposlechu, manipulaci a opakování dat („replay“).
	Je třeba mít na vědomí, že mezi různými subjekty, které jsou zapojeni v poskytování služeb elektronické identifikace, mohou existovat komunikační kanály, např. mezi vlastníkem eID prostředku a službou nebo např. mezi municipalitou a výrobcem eID prostředku. Jednou z možností ochrany komunikačních kanálů je respektování technických příruček/pokynů vydaných příslušným kompetentním orgánem, který poskytuje doporučení stran kryptografických a bezpečnostních opatření. To se obvykle dosahuje použitím vhodných kryptografických protokolů obsahující prvky ověření. Požadavky na komunikační kanály mezi eIDAS uzly jsou uvedeny v technických specifikacích pro rámec interoperability[7]. V rámci systému řízení bezpečnosti informací implementovaného podle normy ČSN ISO / IEC 27001: 2013 je tento požadavek pokryt jako součást opatření - A.10 "Kryptografie", A.13 "Bezpečnost komunikací" a A.18.1.5 "Regulace kryptografických opatření", které mohou rovněž obsahovat odkazy na výše uvedené technické příručky/pokyny.
	3. Pokud se pro vydávání prostředků pro elektronickou identifikaci a autentizaci používají citlivé kryptografické materiály, je přístup k nim omezen pouze na úlohy a aplikace, které přístup bezpodmínečně vyžadují. Musí se zajistit, aby takový materiál nebyl nikdy trvale uchováván jako jednoduchý text.
	V rámci systému řízení bezpečnosti informací implementovaného podle normy ČSN ISO / IEC 27001: 2013 je tento požadavek pokryt jako součást opatření - A.9 "Řízení přístupu" a A.10 "Kryptografie".
	4. Existují postupy k zajištění toho, aby se trvale udržovala bezpečnost a bylo možno reagovat na změny úrovní rizik, incidenty a případy narušení bezpečnosti.
	V rámci systému řízení bezpečnosti informací implementovaného podle normy ČSN ISO / IEC 27001: 2013 je tento požadavek pokryt jako součást opatření - A.14 "Akvizice, vývoj a údržba systémů" a A.16 "Řízení incidentů bezpečnosti informací".
	5. Všechny nosiče obsahující osobní, kryptografické nebo jiné citlivé informace se uchovávají, přepravují a likvidují bezpečným a chráněným způsobem.

[7] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Profile

	V rámci systému řízení bezpečnosti informací implementovaného podle normy ČSN ISO / IEC 27001: 2013 je tento požadavek pokryt jako součást opatření - A.8 "Řízení aktiv".
Značná	*Stejné jako při nízké úrovni a navíc:* *Citlivý kryptografický materiál, který se používá pro vydávání prostředků pro elektronickou identifikaci a autentizaci, je chráněn před neoprávněnou manipulací.* Pod termín „citlivý kryptografický materiál“ se má na mysli kryptografický materiál používaný k vydávání eID prostředků, k autentizaci uživatelů a vydávání assertion (je-li použito). Ochrana těchto typů kryptografických klíčů má zásadní význam pro bezpečnost eID systému. Mechanismy ochrany proti neoprávněné manipulaci jsou zamýšleny jako ochrana proti jakýmkoli pokusům o vyzrazení, neoprávněné manipulaci nebo zneužití kryptografického materiálu během jeho celého životního cyklu. Toho lze dosáhnout zavedením fyzických a logických bezpečnostních opatření pro ochranu těchto klíčů. Je běžnou praxí, že výše zmíněné bezpečnostní opatření jsou implementovány jako součást hardware security modulů (HSM). Bezpečnostní certifikace HSM modulů může posloužit jako důkaz bezpečnosti a kvality HSM modulů. Příkladem je certifikace v rámci dohody Criteria Recognition Arrangement (CCRA) nebo v rámci dohody Senior Officials Group Information Systems Security Mutual Recognition Agreement (SOGIS-MRA) nebo certifikace dle amerického FIPS-140. Moduly musí pocházet od důvěryhodného dodavatele a musí být nasazeny tak, aby byla zajištěna kvalitní správa modulů, od výroby až po nasazení HSM modulů. V rámci systému řízení bezpečnosti informací implementovaného podle normy ČSN ISO / IEC 27001: 2013 je tento požadavek pokryt jako součást opatření - A.10 "Kryptografie" a A.11 "Fyzická bezpečnost a bezpečnost prostředí".
Vysoká	*Stejné jako při značné úrovni.*

2.4.7. Dodržování a audit.

Úroveň záruky	***Potřebné prvky***
Nízká	*Existují pravidelné interní audity, jejichž rozsah zahrnuje všechny úseky týkající se poskytování služeb, aby se zajistilo dodržování příslušné politiky.* Audity zohledňují míru rizika spojeného se systémem / částmi systému. Z toho vyplývá, že rozsah a důkladnost auditu může být pro různé úrovně záruky odlišná. Požadavek na interní audit může být rovněž splněn auditem provedeným externím subjektem. V případě nízké úrovně záruky se nevyžaduje nezávislý audit (k pojmu nezávislý audit viz níže). Standardní postup pro audity systému řízení bezpečnosti informací zahrnuje kompletní audit všech části systému každé tři roky včetně každoročních dohledových auditů. V rámci systému řízení bezpečnosti informací implementovaného podle normy ČSN ISO /

	IEC 27001: 2013 je tento požadavek pokryt jako součást opatření - A.18 "Soulad s požadavky" (viz A.18.2 "Přezkoumání bezpečnosti informací"). Doporučujeme provádět audity v intervalu jednou za 12 – 24 měsíců pro úroveň nízká.
Značná	*Existují pravidelné nezávislé interní nebo externí audity, jejichž rozsah zahrnuje všechny úseky týkající se poskytování služeb, aby se zajistilo dodržování příslušné politiky.* Audit, který je prováděn interně podle vlastních norem organizace a kde je výsledek předáván především vedení vlastní organizace, je všeobecně nazýván interním auditem. Interní audit musí být prováděn objektivně a nezávisle, a může být základem pro vlastní prohlášení organizace o souladu s požadavky. Audit musí být proveden nezávisle, aby se zabránilo předpojatosti a konfliktu zájmů (tj. auditoři se nesmí podílet na činnosti systému nebo chodu části organizace, kterou auditují). Externí audity (prováděny třetími stranami) jsou audity prováděné nezávislými auditními organizacemi, jako jsou například dohledové orgány nebo certifikační orgány. Cílem je posoudit organizaci, která je auditována, na soulad s určitými požadavky a množinou zásad a kritérií a učinit prohlášení, zda je tvrzení vedení k těmto principům správně uvedeno. K provedení externích auditu jsou obvykle využity existující standardy pro provádění auditů, jako např. standard ISO / IEC 27007. Norma ISO 19011: 2011 poskytuje pokyny pro audity systémů řízení, včetně principů interního a externího auditu, jakož i pokyny pro hodnocení kompetencí osob zapojených do procesu auditu. Doporučujeme provádět audity v intervalu jednou za 12 – 24 měsíců pro úroveň značná.
Vysoká	*1.Existují pravidelné nezávislé externí audity, jejichž rozsah zahrnuje všechny úseky týkající se poskytování služeb, aby se zajistilo dodržování příslušné politiky.* Tento požadavek lze splnit auditem / certifikací provedenou podle normy ISO / IEC 27007. Doporučujeme provádět audity v intervalu jednou za 12 měsíců pro úroveň vysoká. *2.Spravuje-li systém přímo orgán veřejné správy, probíhá audit v souladu s vnitrostátními právními předpisy.*

3. Zkratky

[1] DKP IDP - Dokument konkretizující požadavky na kvalifikované systémy elektronické identifikace spravované kvalifikovanými správci a na prostředky pro elektronickou identifikaci v rámci nich vydávané a používané.

[2] Zákon o elektronické identifikaci – Zákon č. 250/2017 Sb., o elektronické identifikaci.

[3] Kvalifikovaný systém – kvalifikovaný systém elektronické identifikace ve smyslu § 3 odst. 1 zákona.

[4] eID prostředek - prostředek pro elektronickou identifikaci dle čl. 3 odst. 2 nařízení eIDAS.

[5] Nařízení eIDAS - nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES).

[6] CIR 2015/1502 - Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.

[7] CIR 2015/1501 - Prováděcí nařízení Komise (EU) 2015/1501 ze dne 8. září 2015 o rámci interoperability podle čl. 12 odst. 8 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu

[7] Databáze PRADO - Veřejný rejstřík pravých dokladů totožnosti a cestovních dokladů online

[8] NIST - National Institute of Standards and Technology

4. Zdroje

[1] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[2] PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002.

[3] Guidance for the application of the levels of assurance which support the eIDAS Regulation, https://www.google.cz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwjOyduYqIjVAhUGOxQKHR1dCKoQFgg0MAI&url=https%3A%2F%2Fec.europa.eu%2Fcefdigital%2Fwiki%2Fdownload%2Fattachments%2F40044784%2FGuidance%2520on%2520Levels%2520of%2520Assurance.docx%3Fversion%3D1%26modificationDate%3D1488295895839%26api%3Dv2&usg=AFQjCNGidAS04-eAY_OR13N-TXaRPAhOkQ

[4] Rejstřík PRADO, http://www.consilium.europa.eu/prado/cs/prado-start-page.html

[5] NIST Special Publication 800 - 63B „Digital Identity Guidelines - Authentication and Lifecycle Management“, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.