

Vládní návrh

ZÁKON

ze dne 2017

o elektronické identifikaci

Parlament se usnesl na tomto zákoně České republiky:

§ 1

Předmět úpravy

Tento zákon upravuje v návaznosti na přímo použitelný předpis Evropské unie upravující elektronickou identifikaci¹⁾

- a) využití elektronické identifikace,
- b) působnost Ministerstva vnitra (dále jen „ministerstvo“) a Správy základních registrů na úseku elektronické identifikace a
- c) přestupky na úseku elektronické identifikace.

CELEX 32014R0910

§ 2

Prokázání totožnosti s využitím elektronické identifikace

Vyžaduje-li právní předpis nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace (dále jen „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 úroveň záruky prostředků pro elektronickou identifikaci²⁾ (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

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.

²⁾ Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úroveň 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.

- 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.

CELEX 32014R0910

§ 4

Kvalifikovaný správce

Kvalifikovaným správcem může být pouze

- a) státní orgán, nebo
- b) osoba, které byla udělena akreditace pro správu kvalifikovaného systému (dále jen „akreditovaná osoba“).

Akreditace

§ 5

(1) Ministerstvo rozhodne o udělení akreditace pro správu kvalifikovaného systému (dále jen „akreditace“) na základě písemné žádosti.

(2) Podmínkou pro udělení akreditace je

- a) skutečnost, že žadatelem o akreditaci vydávaný prostředek pro elektronickou identifikaci a žadatelem o akreditaci spravovaný systém elektronické identifikace splňují technické specifikace, normy a postupy stanovené příslušným předpisem Evropské unie,
- b) bezúhonnost žadatele o akreditaci,
- c) pojištění odpovědnosti za škodu způsobenou při správě kvalifikovaného systému,
- d) zpracování plánu ukončení činnosti,
- e) skutečnost, že systém elektronické identifikace žadatele o akreditaci umožňuje poskytnutí služby národního bodu, a
- f) skutečnost, že žadatel o akreditaci je způsobilý pro správu kvalifikovaného systému z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob.

(3) Žadatel o akreditaci k žádosti o akreditaci přikládá

- a) smlouvu o uzavření pojištění odpovědnosti za škodu způsobenou při správě kvalifikovaného systému,
- b) doklad o bezúhonnosti, neprokazuje-li se bezúhonnost výpisem z evidence Rejstříku trestů,
- c) potvrzení, že žadatelem o akreditaci vydávaný prostředek pro elektronickou identifikaci a žadatelem o akreditaci spravovaný systém elektronické identifikace splňují technické specifikace, normy a postupy stanovené příslušným předpisem Evropské unie, a
- d) plán ukončení činnosti.

(4) Ministerstvo si vyžádá vyjádření správce národního bodu, zda systém elektronické identifikace žadatele o akreditaci umožňuje poskytnutí služby národního bodu.

(5) Ministerstvo je oprávněno při zjišťování skutečnosti podle odstavce 2 písm. f) požádat o informace Policii České republiky, zpravodajskou službu nebo jiný orgán.

(6) Ministerstvo rozhodne o žádosti o udělení akreditace do 3 měsíců ode dne jejího podání. Splňuje-li žadatel o akreditaci podmínky pro udělení akreditace, ministerstvo udělí akreditaci. V opačném případě ministerstvo žádost zamítne.

(7) Akreditovaná osoba je povinna bez zbytečného odkladu písemně oznámit ministerstvu, že přestala splňovat některou z podmínek pro udělení akreditace.
CELEX 32014R0910

§ 6

(1) Ministerstvo rozhodne o změně akreditace na základě písemné žádosti akreditované osoby o rozšíření správy kvalifikovaného systému o vydávání a používání dalšího prostředku pro elektronickou identifikaci.

(2) Akreditovaná osoba je povinna v žádosti podle odstavce 1 doložit splnění podmínky podle § 5 odst. 2 písm. a) ve vztahu k dalšímu prostředku pro elektronickou identifikaci.

(3) Ministerstvo rozhodne o žádosti podle odstavce 1 do 3 měsíců ode dne jejího podání. Splňuje-li akreditovaná osoba ve vztahu k dalšímu prostředku pro elektronickou identifikaci podmínku podle § 5 odst. 2 písm. a), ministerstvo změní akreditaci. V opačném případě ministerstvo žádost zamítne.

§ 7

(1) Přestane-li akreditovaná osoba splňovat některou z podmínek pro udělení akreditace, ministerstvo ji písemně upozorní na možnost odnětí akreditace a zároveň ji vyzve, aby bez zbytečného odkladu zjedнала nápravu. Nejedná-li akreditovaná osoba ani na základě upozornění ministerstva nápravu, ministerstvo jí akreditaci odejme.

(2) Ministerstvo odejme akreditaci, jestliže o to akreditovaná osoba písemně požádala.

§ 8

Akreditace zaniká smrtí nebo zánikem akreditované osoby.

§ 9

Pojištění odpovědnosti za škodu

(1) Žadatel o akreditaci musí být pojištěn pro případ odpovědnosti za škodu způsobenou při správě kvalifikovaného systému tak, aby výše pojistné částky byla úměrná možným škodám, které lze v rozumné míře předpokládat.

(2) Akreditovaná osoba je povinna nahradit škodu způsobenou při správě kvalifikovaného systému bez ohledu na sjednaný limit pojistného plnění.

§ 10
Bezúhonnost

(1) Za bezúhonnou se pro účely tohoto zákona považuje osoba, která nebyla pravomocně odsouzena pro

- a) úmyslný trestný čin, nebo
- b) trestný čin proti pořádku ve věcech veřejných z nedbalosti.

(2) Za bezúhonnou se pro účely tohoto zákona považuje též osoba, na kterou se hledí, jako by nebyla odsouzena.

(3) Bezúhonnost fyzických osob se prokazuje

- a) výpisem z evidence Rejstříku trestů,
- b) výpisem z evidence Rejstříku trestů s přílohou obsahující informace, které jsou zapsané v evidenci trestů členského státu Evropské unie, jehož je osoba státním příslušníkem, nebo členského státu Evropské unie posledního pobytu, je-li osoba státním příslušníkem jiného členského státu Evropské unie nebo měla-li nebo má bydliště v jiném členském státě Evropské unie,
- c) výpisem z evidence trestů nebo rovnocenným dokladem vydaným státem, jehož je osoba státním příslušníkem, nebo nevydává-li tento stát výpis z evidence trestů nebo rovnocenný doklad, čestným prohlášením o bezúhonnosti učiněným před notářem nebo jiným příslušným orgánem státu, jehož je osoba státním příslušníkem,
- d) výpisem z evidence trestů nebo rovnocenným dokladem vydaným státem posledního pobytu, trvajícího déle než 3 měsíce ve 2 po sobě následujících letech, nebo nevydává-li tento stát výpis z evidence trestů nebo rovnocenný doklad, čestným prohlášením o bezúhonnosti učiněným před notářem nebo jiným příslušným orgánem státu pobytu.

(4) Bezúhonnost právnických osob se prokazuje

- a) výpisem z evidence Rejstříku trestů,
- b) výpisem z evidence Rejstříku trestů s přílohou obsahující informace, které jsou zapsané v evidenci trestů členského státu Evropské unie, na jehož území má osoba sídlo, má-li sídlo v jiném členském státě Evropské unie,
- c) výpisem z evidence trestů nebo rovnocenným dokladem vydaným státem, na jehož území má osoba sídlo, nebo nevydává-li tento stát výpis z evidence trestů nebo rovnocenný doklad, čestným prohlášením o bezúhonnosti učiněným před notářem nebo jiným příslušným orgánem státu, na jehož území má osoba sídlo,
- d) výpisem z evidence trestů nebo rovnocenným dokladem vydaným státem, na jehož území osoba v posledních 2 po sobě následujících letech podnikala, nebo nevydává-li tento stát výpis z evidence trestů nebo rovnocenný doklad, čestným prohlášením o bezúhonnosti učiněným před notářem nebo jiným příslušným orgánem státu, na jehož území osoba podnikala.

(5) Doklad o bezúhonnosti podle odstavce 3 písm. b) až d) a odstavce 4 písm. b) až d) nesmí být starší 3 měsíců.

(6) Ministerstvo si vyžádá výpis z evidence Rejstříku trestů za účelem zjištění bezúhonnosti podle zákona o Rejstříku trestů. Žádost o vydání výpisu z evidence Rejstříku trestů a výpis z evidence Rejstříku trestů se předává v elektronické podobě, a to způsobem umožňujícím dálkový přístup.

Posuzování prostředku pro elektronickou identifikaci a systému elektronické identifikace

§ 11

(1) Prostředek pro elektronickou identifikaci a systém elektronické identifikace posuzuje osoba, která k tomu byla pověřena ministerstvem (dále jen „pověřená osoba“).

(2) Ministerstvo pověří posuzováním prostředku pro elektronickou identifikaci a systému elektronické identifikace na základě žádosti osobu pověřenou k provádění atestací podle zákona o informačních systémech veřejné správy. Pověření k posuzování prostředku pro elektronickou identifikaci a systému elektronické identifikace (dále jen „pověření“) nelze převést na jinou osobu.

§ 12

(1) Přestane-li pověřená osoba plnit povinnosti stanovené tímto zákonem, ministerstvo ji písemně upozorní na možnost odnětí pověření a zároveň ji vyzve, aby bez zbytečného odkladu zjednala nápravu. Nejednala-li pověřená osoba ani na základě upozornění ministerstva nápravu, ministerstvo jí pověření odejme.

(2) Ministerstvo odejme pověření, jestliže o to pověřená osoba písemně požádala.

(3) Pověření zaniká, jestliže pověřená osoba pozbyla pověření k provádění atestací podle zákona o informačních systémech veřejné správy.

§ 13

(1) Pověřená osoba posuzuje, zda prostředek pro elektronickou identifikaci a systém elektronické identifikace splňuje technické specifikace, normy a postupy stanovené příslušným předpisem Evropské unie. Ustanovení § 6d odst. 3 a § 6e zákona o informačních systémech veřejné správy se při posuzování prostředku pro elektronickou identifikaci a systému elektronické identifikace použijí obdobně.

(2) Splňuje-li prostředek pro elektronickou identifikaci a systém elektronické identifikace technické specifikace, normy a postupy stanovené příslušným předpisem Evropské unie, pověřená osoba písemně potvrdí tuto skutečnost žadateli o posouzení do 3 měsíců ode dne podání žádosti o posouzení.

(3) Potvrzení podle odstavce 2 obsahuje stanovenou úroveň záruky prostředku pro elektronickou identifikaci podle příslušného předpisu Evropské unie.

(4) Nesplňuje-li prostředek pro elektronickou identifikaci a systém elektronické identifikace technické specifikace, normy a postupy stanovené příslušným předpisem Evropské unie, pověřená osoba písemně vyrozumí o této skutečnosti žadatele o posouzení do 3 měsíců ode dne podání žádosti o posouzení a sdělí mu důvody nesplnění požadavků.

§ 14

Není-li posuzováním prostředku pro elektronickou identifikaci a systému elektronické identifikace pověřena žádná osoba, posuzuje prostředek pro elektronickou identifikaci a systém elektronické identifikace ministerstvo. Ustanovení § 13 se na posuzování prostředku pro elektronickou identifikaci a systému elektronické identifikace ministerstvem použije obdobně.

§ 15

Plán ukončení činnosti

Státní orgán nebo žadatel o akreditaci v plánu ukončení činnosti uvede 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 (dále jen „držitel“) informováni o ukončení činnosti kvalifikovaného správce.

§ 16

Povinnosti kvalifikovaného správce

(1) Kvalifikovaný správce

- a) zajistí dostupnost jím spravovaného kvalifikovaného systému pro spoléhající se stranu způsobem umožňujícím dálkový přístup prostřednictvím národního bodu a pro národní bod způsobem umožňujícím dálkový přístup,
- b) vede evidenci jím vydaných prostředků pro elektronickou identifikaci,
- c) před prvním použitím prostředku pro elektronickou identifikaci v rámci kvalifikovaného systému ověří totožnost držitele prostřednictvím národního bodu,
- d) zapíše identifikátor jím vydaného prostředku pro elektronickou identifikaci a úroveň záruky tohoto prostředku do národního bodu,
- e) aktualizuje údaje v evidenci vydaných prostředků pro elektronickou identifikaci na základě upozornění správce národního bodu na změny údajů,
- f) po ukončení své činnosti předá evidenci vydaných prostředků pro elektronickou identifikaci ministerstvu,
- g) bez zbytečného odkladu zneplatní prostředek pro elektronickou identifikaci držitele, o kterém se prokazatelně dozvěděl, že zemřel, nebo byl prohlášen za mrtvého,
- h) bez zbytečného odkladu zneplatní prostředek pro elektronickou identifikaci na základě žádosti držitele, nebo na základě ohlášení držitele o zneužití nebo hrozícím nebezpečí zneužití prostředku pro elektronickou identifikaci,
- i) při ukončení své činnosti zneplatní jím vydané prostředky pro elektronickou identifikaci,
- j) oznámí správci národního bodu zneplatnění prostředku pro elektronickou identifikaci podle písmen g) až i),
- k) vede a aktualizuje plán ukončení činnosti a
- l) při ukončení své činnosti postupuje podle plánu ukončení činnosti.

(2) Kvalifikovaný správce zajistí, aby řídicí 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.

(3) Kvalifikovaný správce zajistí, aby fyzické osoby, které vykonávají řídicí činnosti při správě kvalifikovaného systému, a fyzické osoby, které ověřují totožnost držitele, byly bezúhonné.

CELEX32014R0910

§ 17

Povinnosti držitele

Držitel

- a) ověří správnost údajů zapsaných v prostředku pro elektronickou identifikaci při převzetí tohoto prostředku,
- b) zachází s prostředkem pro elektronickou identifikaci s náležitou péčí tak, aby minimalizoval možnost jeho zneužití,
- c) bez zbytečného odkladu ohlásí kvalifikovanému správci zneužití nebo hrozící nebezpečí zneužití prostředku pro elektronickou identifikaci.

§ 18

Povinnosti kvalifikovaného poskytovatele

(1) Ten, kdo umožňuje prokázání totožnosti, které vyžaduje právní předpis nebo výkon působnosti, s využitím elektronické identifikace (dále jen „kvalifikovaný poskytovatel“), vyrozumí o této skutečnosti správce národního bodu, a to bez zbytečného odkladu poté, co nastala. Kvalifikovaný poskytovatel ve vyrozumění uvede on-line službu nebo jinou činnost, při nichž prokázání totožnosti s využitím elektronické identifikace umožňuje, a úroveň záruky prostředku pro elektronickou identifikaci, kterou při prokázání totožnosti s využitím elektronické identifikace požaduje.

(2) Ten, kdo přestal umožňovat prokázání totožnosti způsobem podle odstavce 1, vyrozumí o této skutečnosti bez zbytečného odkladu správce národního bodu.

(3) Vyrozumění podle odstavců 1 nebo 2 se činí prostřednictvím elektronické aplikace spravované správcem národního bodu.

§ 19

Působnost na úseku elektronické identifikace

(1) Ministerstvo

- a) plní úkoly podle čl. 9 a 10 přímo použitelného předpisu Evropské unie upravujícího elektronickou identifikaci¹⁾,
- b) plní úkoly jednotného kontaktního místa podle přímo použitelného předpisu Evropské unie upravujícího procesní opatření pro spolupráci mezi členskými státy v oblasti elektronické identifikace³⁾,
- c) kontroluje kvalifikované správce, kvalifikované poskytovatele a pověřené osoby,
- d) vede evidenci udělených akreditací a jejich změn a zveřejňuje ji na svých internetových stránkách a

³⁾ Prováděcí rozhodnutí Komise (EU) 2015/296 ze dne 24. února 2015, kterým se stanoví procesní opatření pro spolupráci mezi členskými státy v oblasti elektronické identifikace podle čl. 12 odst. 7 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.

- e) uchovává údaje vedené v evidenci vydaných prostředků pro elektronickou identifikaci kvalifikovaného správce, který ukončil činnost, a tyto údaje zpřístupní tomu, kdo osvědčí právní zájem na jejich zpřístupnění, nebo stanoví-li to zákon.

(2) Správa základních registrů

- a) se vyjadřuje, zda systém elektronické identifikace žadatele o akreditaci umožňuje poskytnutí služby národního bodu,
b) na základě vyrozumění kvalifikovaného poskytovatele umožní poskytnutí služby národního bodu a
c) upozorňuje kvalifikovaného správce na změny údajů v evidenci vydaných prostředků pro elektronickou identifikaci.

CELEX 32014R0910

CELEX 32015D0296

Národní bod

§ 20

(1) Národní bod je informační systém veřejné správy podporující proces elektronické identifikace a autentizace prostřednictvím kvalifikovaného systému.

(2) Správcem národního bodu je Správa základních registrů.

(3) Samostatná součást národního bodu plní úlohu uzlu podle přímo použitelného předpisu Evropské unie upravujícího rámec interoperability⁴⁾.

(4) Správce národního bodu zajistí, aby národní bod splňoval požadavky stanovené přímo použitelným předpisem Evropské unie upravujícím rámec interoperability⁴⁾.

CELEX 32015R1501

§ 21

(1) V národním bodu se vede

- a) identifikátor prostředku pro elektronickou identifikaci a údaj o úrovni záruky tohoto prostředku,
b) agendový identifikátor držitele pro agendu autentizace,
c) identifikátor držitele v rámci kvalifikovaného systému a
d) identifikátor držitele v rámci on-line služby nebo jiné činnosti splňující požadavky stanovené přímo použitelným předpisem Evropské unie upravujícím rámec interoperability⁴⁾.

(2) V národním bodu se jako provozní údaj vede alespoň

- a) datum prvotního zápisu údaje do národního bodu,
b) datum poslední změny údaje vedeného v národním bodu a
c) záznam o využití údaje z národního bodu.

(3) V národním bodu se dále mohou vést údaje, které poskytne držitel.

⁴⁾ 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.

(4) Údaje podle odstavců 1 a 2 zapisuje do národního bodu správce národního bodu. Údaje podle odstavce 3 zapisuje do národního bodu držitel.

(5) Údaje podle odstavců 1 a 2 se v národním bodu uchovávají po dobu 15 let od skončení platnosti prostředku pro elektronickou identifikaci. Údaje podle odstavce 3 se v národním bodu uchovávají po dobu platnosti prostředku pro elektronickou identifikaci, nevymaže-li je dříve držitel.

(6) Údaje, které se vedou v uzlu podle čl. 9 odst. 3 přímo použitelného předpisu Evropské unie upravujícího rámec interoperability⁴⁾, se uchovávají po dobu 15 let od jejich prvotního zápisu.

CELEX 32015R1501

§ 22

Evidence vydaných prostředků pro elektronickou identifikaci

(1) V evidenci vydaných prostředků pro elektronickou identifikaci se vede

- a) jméno, popřípadě jména, a příjmení držitele,
- b) adresa místa trvalého pobytu držitele, popřípadě adresa místa bydliště mimo území České republiky, pokud držitel nemá trvalý pobyt na území České republiky,
- c) datum narození držitele,
- d) identifikátor prostředku pro elektronickou identifikaci,
- e) identifikátor držitele v rámci kvalifikovaného systému,
- f) údaj o způsobu ověření totožnosti žadatele o vydání prostředku pro elektronickou identifikaci a byla-li totožnost ověřena průkazem totožnosti, rovněž číslo a druh průkazu totožnosti,
- g) datum a čas vydání prostředku pro elektronickou identifikaci a datum a čas jeho zneplatnění,
- h) doba platnosti prostředku pro elektronickou identifikaci a
- i) datum a čas přijetí žádosti o zneplatnění prostředku pro elektronickou identifikaci nebo oznámení držitele o zneužití nebo hrozícím nebezpečí zneužití prostředku pro elektronickou identifikaci.

(2) Údaje podle odstavce 1 se v evidenci vydaných prostředků pro elektronickou identifikaci uchovávají po dobu 15 let od skončení platnosti prostředku pro elektronickou identifikaci.

(3) Kvalifikovaný správce zpřístupní údaje podle odstavce 1 tomu, kdo osvědčí právní zájem na jejich zpřístupnění, nebo stanoví-li to zákon.

§ 23

Seznam kvalifikovaných správců a kvalifikovaných poskytovatelů

(1) Správa základních registrů vede seznam kvalifikovaných správců usazených v České republice spolu s jimi vydanými prostředky pro elektronickou identifikaci a seznam kvalifikovaných poskytovatelů usazených v České republice spolu s on-line službami nebo jinými činnostmi, při nichž umožňují prokázání totožnosti s využitím elektronické identifikace.

(2) Správa základních registrů zveřejňuje seznam podle odstavce 1 na svých internetových stránkách.

§ 24

Využívání údajů z informačních systémů veřejné správy na úseku elektronické identifikace

(1) Správa základních registrů využívá při výkonu působnosti podle tohoto zákona ze základního registru obyvatel údaje v rozsahu

- a) příjmení,
- b) jméno, popřípadě jména,
- c) adresa místa pobytu,
- d) datum, místo a okres narození; u fyzické osoby, která se narodila v cizině, datum, místo a stát, kde se narodila,
- e) datum, místo a okres úmrtí; jde-li o úmrtí mimo území České republiky, datum úmrtí, místo a stát, na jehož území k úmrtí došlo; je-li vydáno rozhodnutí soudu o prohlášení za mrtvého, den, který je v rozhodnutí uveden jako den smrti nebo den, který fyzická osoba nepřežila, a datum nabytí právní moci tohoto rozhodnutí a
- f) státní občanství, popřípadě více státních občanství.

(2) Správa základních registrů využívá při výkonu působnosti podle tohoto zákona z informačního systému evidence obyvatel údaje v rozsahu

- a) jméno, popřípadě jména, příjmení, rodné příjmení,
- b) datum, místo a okres narození; u občana, který se narodil v cizině, datum, místo a stát, kde se narodil,
- c) pohlaví,
- d) státní občanství, popřípadě více státních občanství,
- e) adresa místa trvalého pobytu, případně též adresa, na kterou mají být doručovány písemnosti podle jiného právního předpisu, a
- f) datum, místo a okres úmrtí; jde-li o úmrtí mimo území České republiky, datum úmrtí, místo a stát, na jehož území k úmrtí došlo; je-li vydáno rozhodnutí soudu o prohlášení za mrtvého, den, který je v rozhodnutí uveden jako den smrti nebo den, který fyzická osoba nepřežila, a datum nabytí právní moci tohoto rozhodnutí.

(3) Správa základních registrů využívá při výkonu působnosti podle tohoto zákona z informačního systému cizinců údaje v rozsahu

- a) jméno, popřípadě jména, a příjmení,
- b) datum narození,
- c) druh a adresa místa pobytu a
- d) datum, místo a okres úmrtí; jde-li o úmrtí mimo území České republiky, datum úmrtí, místo a stát, na jehož území k úmrtí došlo; je-li vydáno rozhodnutí soudu o prohlášení za mrtvého, den, který je v rozhodnutí uveden jako den smrti nebo den, který fyzická osoba nepřežila, a datum nabytí právní moci tohoto rozhodnutí.

(4) Správa základních registrů využívá při výkonu působnosti podle tohoto zákona ze základního registru agend, orgánů veřejné moci, soukromoprávních uživatelů údajů a některých práv a povinností údaje v rozsahu

- a) název orgánu veřejné moci, který údaje o rozhodnutích nebo jiných úkonech orgánů veřejné moci, včetně veřejnoprávních smluv a opatření obecné povahy (dále jen „rozhodnutí“) vydal, a identifikátor tohoto orgánu veřejné moci,

- b) číslo a název právního předpisu a označení jeho ustanovení, podle kterého bylo rozhodnutí vydáno,
- c) jméno, popřípadě jména, příjmení, adresa místa pobytu, datum narození fyzické osoby ve formě referenční vazby na referenční údaj v základním registru obyvatel nebo obchodní firma nebo název, adresa sídla právnické osoby ve formě referenční vazby na referenční údaj v základním registru právnických osob, podnikajících fyzických osob a orgánů veřejné moci, kterým právo nebo povinnost vznikly,
- d) název a kód agendy, při jejímž výkonu bylo rozhodnutí vydáno,
- e) vymezení práva nebo povinnosti subjektů podle písmene c), kterých se rozhodnutí týká,
- f) údaj, který je rozhodnutím přidělen orgánem veřejné moci, který rozhodnutí vydal, na základě zaevidování rozhodnutí v evidenci dokumentů, a
- g) datum nabytí právní moci, vykonatelnosti nebo jiných právních účinků rozhodnutí.

(5) Údaje, které jsou vedeny jako referenční údaje v základním registru obyvatel, se využijí z informačního systému evidence obyvatel a informačního systému cizinců, pouze pokud jsou ve tvaru předcházejícím současný stav.

(6) Z údajů podle odstavců 1 až 4 lze v konkrétním případě využít vždy jen takové údaje, které jsou nezbytné ke splnění daného úkolu.

Přestupky na úseku elektronické identifikace

§ 25

(1) Akreditovaná osoba se dopustí přestupku tím, že

- a) nezajistí dostupnost jí spravovaného kvalifikovaného systému podle § 16 odst. 1 písm. a),
- b) nevede evidenci jí vydaných prostředků pro elektronickou identifikaci podle § 16 odst. 1 písm. b),
- c) neověří totožnost držitele prostřednictvím národního bodu podle § 16 odst. 1 písm. c),
- d) nezapíše identifikátor vydaného prostředku pro elektronickou identifikaci a úroveň záruky tohoto prostředku do národního bodu podle § 16 odst. 1 písm. d),
- e) neaktualizuje údaje v evidenci vydaných prostředků pro elektronickou identifikaci podle § 16 odst. 1 písm. e),
- f) nepředá ministerstvu evidenci vydaných prostředků pro elektronickou identifikaci podle § 16 odst. 1 písm. f),
- g) nezneplatní prostředek pro elektronickou identifikaci podle § 16 odst. 1 písm. g) až i),
- h) neoznámí zneplatnění prostředku pro elektronickou identifikaci podle § 16 odst. 1 písm. j),
- i) v rozporu s § 16 odst. 1 písm. k) nevede nebo neaktualizuje plán ukončení činnosti,
- j) nepostupuje podle plánu ukončení činnosti podle § 16 odst. 1 písm. l),
- k) nezajistí, aby řídicí činnosti při správě kvalifikovaného systému vykonávaly fyzické osoby splňující předpoklady podle § 16 odst. 2, nebo
- l) v rozporu s § 16 odst. 3 nezajistí, aby řídicí činnosti při správě kvalifikovaného systému a ověření totožnosti prováděly bezúhonné fyzické osoby.

(2) Za přestupek lze uložit pokutu do

- a) 1 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. k) nebo l), nebo
- b) 2 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. a) až j).

§ 26

Přestupky podle tohoto zákona projednává ministerstvo.

§ 27

Přechodná ustanovení

(1) Ten, kdo umožňoval prokázání totožnosti, které vyžaduje právní předpis nebo výkon působnosti, s využitím elektronické identifikace přede dnem nabytí účinnosti tohoto zákona a umožňuje toto prokázání totožnosti i ode dne nabytí účinnosti tohoto zákona, vyrozumí o této skutečnosti správce národního bodu do 6 měsíců ode dne nabytí účinnosti tohoto zákona. Ustanovení § 18 odst. 3 se použije obdobně.

(2) Po dobu 2 let ode dne nabytí účinnosti tohoto zákona lze umožnit prokázání totožnosti, které vyžaduje právní předpis nebo výkon působnosti, s využitím elektronické identifikace, při kterém se nepoužije kvalifikovaný systém.

§ 28

Účinnost

Tento zákon nabývá účinnosti dnem 1. července 2018.

DŮVODOVÁ ZPRÁVA

A. OBECNÁ ČÁST

1. Zhodnocení platného právního stavu, včetně zhodnocení současného stavu ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen

V českém právním řádu není v současné době upraven obecný institut elektronické identifikace. Jsou toliko upraveny dílčí postupy, kdy a jakým způsobem se lze vzdáleně identifikovat vůči jednotlivým službám veřejného sektoru. K tomu je využívána samostatná identifikace upravená zvláštními právními předpisy ad hoc (např. zákon č. 187/2006 Sb., o nemocenském pojištění) anebo ověřená identita prostřednictvím informačního systému datových schránek (např. zákon č. 235/2004 Sb., o dani z přidané hodnoty). Tato úprava však není provázána s pravidly elektronické identifikace obsaženými v 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 (dále též „nařízení eIDAS“). Nadto jde o úpravu partikulární týkající se v zásadě jednoho typu elektronické identifikace a obvykle jedné veřejnoprávní agendy.

Co se týče prostředků pro elektronickou identifikaci, které jsou vydávány a občany dnes běžně používány v soukromém sektoru, neexistuje vnitrostátní právní úprava, která by umožnila jejich využití pro účely vzdáleného přístupu k on-line službám nebo jiným činnostem ve smyslu předkládaného návrhu zákona o elektronické identifikaci. Problematika, jež je upravena návrhem zákona o elektronické identifikaci, který je mj. adaptačním právním předpisem k části nařízení eIDAS, která se týká elektronické identifikace, je částečně upravena právě v tomto nařízení a jeho prováděcích aktech, a to zejména z pohledu přeshraničního uznávání prostředků pro elektronickou identifikaci. Těmito prováděcími akty jsou:

- rozhodnutí Komise (EU) 2015/296 ze dne 24. února 2015, kterým se stanoví procesní opatření pro spolupráci mezi členskými státy v oblasti elektronické identifikace podle čl. 12 odst. 7 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu,
- 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,
- nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úroveň 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,
- rozhodnutí Komise (EU) 2015/1984 ze dne 3. listopadu 2015, kterým se stanoví okolnosti, formáty a postupy pro oznamování podle čl. 9 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.

Po zhodnocení současného platného právního stavu v oblasti elektronické identifikace je tedy nezbytné přijmout takovou právní úpravu, která by umožnila fyzickým osobám při přístupu k příslušným on-line službám nebo jiným činnostem použití systémů elektronické

identifikace zaručujících bezpečnou a důvěryhodnou elektronickou identifikaci fyzických osob. Takové řešení je rovněž plně v souladu s cíli Strategie rozvoje ICT služeb veřejné správy schválené usnesením vlády ze dne 2. listopadu 2015 č. 889. S postupující elektronizací společnosti je třeba, aby veřejný sektor tento trend reflektoval a nabízel možnost pro fyzické osoby, potažmo občany, aby s ním mohli komunikovat na dálku a plně elektronicky. Pro celou řadu on-line služeb nebo jiných činností je nezbytné, aby fyzická osoba, která hodlá službu využít, byla identifikována. Identifikace člověka je nezbytná i pro ryze informační služby, kdy fyzická osoba například žádá „pouze“ o výpis z informačních systémů veřejné správy. Komerční i akademická sféra již používá model federované identity, kdy se lze pomocí jednoho prostředku pro elektronickou identifikaci přihlásit k víceru služeb. Veřejný sektor by měl tento technologický pokrok rovněž následovat, neboť jeho cílem je efektivní poskytování využitelných veřejných služeb. Občanovi tento model přinese, kromě jiného, více pohodlí při využívání on-line služeb nebo jiných činností bez toho, aby bylo nutné se ke každé službě přihlašovat jiným prostředkem pro elektronickou identifikaci.

Stávající právní úprava nepřipouští diskriminační přístup, neboť zaručuje stejná práva a povinnosti bez diskriminace založené na jakémkoli důvodu, jako je pohlaví, rasa, barva pleti, jazyk, náboženství, politické nebo jiné smýšlení, národnostní nebo sociální původ, příslušnost k národnostní menšině, majetek, rod nebo jiné postavení.

2. Odůvodnění hlavních principů navrhované právní úpravy, včetně dopadů navrhovaného řešení ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen

Navrhovaný zákon usiluje o podstatně větší penetraci prostředků pro elektronickou identifikaci mezi občany České republiky, což je klíčový předpoklad pro to, aby mohlo dojít k dalšímu rozvoji on-line služeb nebo jiných činností především veřejného sektoru (návrh zákona ovšem dopadá také na soukromoprávní poskytovatele on-line služeb nebo jiných činností, které k ověření totožnosti zmocňuje konkrétní právní předpis). Bez dostatečného počtu uživatelů nikdy nebude možné dosáhnout plošného využívání těchto služeb.

V rámci specifického cíle 3.1. „Dobudování funkčního rámce eGovernmentu“ Strategického rámce rozvoje veřejné správy České republiky pro období 2014–2020 je stanoveno klíčové opatření dobudování architektury eGovernmentu. Splnění specifického cíle má být, kromě jiného, dosaženo za pomoci realizace plošně využitelného, jednotného, státem garantovaného a v rámci Evropské unie interoperabilního systému elektronické identifikace, autentizace a autorizace pro klíčové agendové a provozní informační systémy spravované orgány veřejné moci podle principů, které předpokládá nařízení eIDAS.

Nařízení eIDAS je nutné chápat jako další krok, který má vést k vytvoření jednotného digitálního trhu. Stanovuje povinnost za určitých podmínek uznávat prostředky pro elektronickou identifikaci pro přístup k on-line službám nebo jiným činnostem poskytovaných subjekty nejen veřejného sektoru, které byly vydány v rámci oznámeného systému elektronické identifikace. Aby mohlo být výše uvedené vzájemné uznávání elektronické identifikace technicky realizovatelné, je nutné zajistit interoperabilitu oznámených systémů elektronické identifikace, a to za pomoci tzv. uzlů [čl. 2 odst. 1 prováděcího nařízení Komise (EU) 2015/1501]. Z tohoto důvodu je navrhováno, že uzel bude samostatnou součástí národního bodu pro identifikaci a autentizaci.

Ustanovení nařízení eIDAS o využívání systémů elektronické identifikace budou aplikovatelná od září roku 2018, a proto je nezbytné přijmout i související vnitrostátní právní úpravu regulující tuto problematiku.

Návrh zákona o elektronické identifikaci je navrhován jako obecný právní předpis pro prokazování totožnosti elektronickými prostředky, jiné zákony pak mohou pro konkrétní služby veřejného sektoru zvolit odlišnou právní úpravu a využívat jiná řešení.

Navrhovaný zákon přináší obecný způsob prokazování totožnosti elektronickými prostředky. Oproti současnému stavu dojde k zakotvení jednotného obecného způsobu prokazování totožnosti a státního informačního systému garantujícího „zprostředkování“ důvěryhodné elektronické identifikace vůči základním registrům (upraveny v zákonu č. 111/2009 Sb., o základních registrech). Tento informační systém bude využitelný pro služby veřejného i soukromého sektoru.

Stanoví se akreditační mechanismus těch nestátních subjektů, které budou žádat o to, aby se staly kvalifikovaným správcem systému elektronické identifikace, tedy subjektem, který bude poskytovat služby ověřené elektronické identifikace (tj. bude potvrzovat „elektronickou“ identitu). Je navrhováno, aby prostředek pro elektronickou identifikaci a systém elektronické identifikace byly posuzovány osobou, která k tomu bude Ministerstvem vnitra pověřena. V návrhu zákona jsou taktéž stanoveny povinnosti, které musí dodržovat kvalifikovaný správce systému elektronické identifikace, držitel prostředku pro elektronickou identifikaci (např. občanského průkazu s kontaktním elektronickým čipem) a konečně kvalifikovaný poskytovatel, tj. ten, který v rámci jím poskytované on-line služby nebo jiné činnosti umožňuje elektronické identifikování adresáta služby (např. správce databáze poskytující klientovi údaje obsažené v této databázi). Mimo jiné je žádoucí, aby byla vedena evidence vydaných prostředků pro elektronickou identifikaci a seznam kvalifikovaných správců systémů elektronické identifikace a kvalifikovaných poskytovatelů. Je nezbytné upravit informační systém, který zprostředkovává služby elektronické identifikace a autentizace a který tvoří základ pro poskytování této služby. V souladu s nařízením eIDAS se navrhuje tento informační systém nazvat národním bodem pro identifikaci a autentizaci. Tento národní bod pro identifikaci a autentizaci bude mít oprávnění využívat některé údaje ze základních registrů a agendových informačních systémů. V neposlední řadě je potřeba, aby právní úprava obsahovala přestupky na úseku elektronické identifikace.

Primárními cíli návrhu zákona jsou:

- stanovení obecného právního rámce pro prokazování totožnosti s využitím elektronické identifikace,
- stanovení podmínek, za kterých bude systém elektronické identifikace považován za kvalifikovaný systém elektronické identifikace,
- nastavení akreditačního schématu nestátních subjektů, které budou chtít poskytovat službu prokazování totožnosti kvalifikovaným systémem elektronické identifikace,
- nastavení pravidel pro přístup k poskytování služby kvalifikovaného systému elektronické identifikace,

- nastavení pravidel pro posuzování prostředku pro elektronickou identifikaci a systému elektronické identifikace,
- stanovení povinností kvalifikovaného správce systému elektronické identifikace, držitele prostředku pro elektronickou identifikaci a toho, kdo umožňuje prokázání totožnosti, které vyžaduje právní předpis nebo výkon působnosti, s využitím elektronické identifikace (tzv. kvalifikovaný poskytovatel),
- zakotvení národního bodu pro identifikaci a autentizaci.

Návrh zákona nemá negativní dopady do zákazu diskriminace a do vztahu rovnosti mužů a žen.

Návrh zákona o elektronické identifikaci, který zavádí obecné principy institutu elektronické identifikace, se bude týkat všech fyzických osob, které budou používat prostředky pro elektronickou identifikaci, a osob, které budou poskytovat služby kvalifikovaného systému elektronické identifikace a budou zahrnuty do federace poskytovatelů těchto služeb buď ex lege (v případě státních poskytovatelů) nebo po podstoupení procesu akreditace (v případě nestátních poskytovatelů). Poslední kategorií dotčených subjektů budou kvalifikovaní poskytovatelé.

Elektronická identifikace se dotkne rovněž Správy základních registrů, která bude správcem národního bodu pro identifikaci a autentizaci, tedy informačního systému veřejné správy podporujícího proces elektronické identifikace a autentizace prostřednictvím kvalifikovaného systému elektronické identifikace.

Dalším dotčeným subjektem bude osoba, která bude posuzovat prostředek pro elektronickou identifikaci a systém elektronické identifikace. Tímto subjektem bude osoba pověřená k provádění atestací podle zákona o informačních systémech veřejné správy. Pověření bude vydávat Ministerstvo vnitra.

Ministerstvo vnitra bude ostatně vykonávat celou řadu dalších úkolů, a to jak v oblasti tuzemské, tak na úrovni evropské [členství v síti pro spolupráci (Cooperation Network na základě rozhodnutí Komise (EU) 2015/296, orgán zodpovědný za oznámený systém elektronické identifikace].

3. Vysvětlení nezbytnosti navrhované právní úpravy v jejím celku

S ohledem na povinnost vzájemného uznávání prostředků pro elektronickou identifikaci za podmínek stanovených čl. 6 nařízení eIDAS by neprovedení adaptace národního právního řádu na část nařízení upravující oblast elektronické identifikace mohlo být Evropskou komisí považováno za nesplnění povinnosti vyplývající České republice z primárního práva Evropské unie (Smlouva o Evropské unii a Smlouva o fungování Evropské unie), přičemž by Evropská komise na základě čl. 258 Smlouvy o fungování Evropské unie mohla předložit tuto záležitost Soudnímu dvoru Evropské unie. Zákon o elektronické identifikaci v tomto ohledu zakotvuje informační systém pro identifikaci a autentizaci (národní bod pro identifikaci a autentizaci), jehož samostatná součást plní úlohu uzlu podle nařízení eIDAS, resp. 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.

Neprovedení legislativního zásahu v oblasti elektronické identifikace v národním právním řádu by znamenalo zachování nežádoucího stavu spočívajícího v neexistenci zákonného zakotvení způsobu prokázání totožnosti. Nadále by se tak dílčí právní úprava omezila na úpravu „specializovaných“ způsobů prokázání totožnosti. Neexistoval by národní bod pro identifikaci a autentizaci a provedení ztotožnění konkrétní fyzické osoby oproti základním registrům by bylo nadále plně ponecháno na jednotlivých orgánech veřejné moci, které poskytují on-line službu nebo jinou činnost. Nikoli obecně využitelným v rámci elektronické identifikace by zůstal veřejnoprávní prostředek pro elektronickou identifikaci – občanský průkaz se strojově čitelnými údaji a s kontaktním elektronickým čipem obsahujícím identifikační certifikát. Prostředky pro elektronickou identifikaci, které jsou naopak (již dnes) vydávány subjekty soukromého práva, by nebylo možno pro přístup k on-line službám nebo jiným činnostem veřejného sektoru využít vůbec.

V případě, kdy by nebyl realizován plošně využitelný, jednotný, státem garantovaný a v rámci EU interoperabilní systém elektronické identifikace a autentizace, se kterým se počítá v rámci specifického cíle 3.1. „Dobudování funkčního rámce eGovernmentu“ Strategického rámce rozvoje veřejné správy České republiky pro období 2014–2020, hrozí, že nedojde k očekávaným úsporám v souvislosti se zavedením státem garantované elektronické identifikace a autentizace a rovněž nedojde k rozvoji on-line služeb nebo jiných činností veřejného sektoru.

Nepominutelným rizikem zůstává i fakt, aby Česká republika nebyla jediným členským státem EU, který by neoznámil systém elektronické identifikace, čímž by mohla utrpět mezinárodní prestiž České republiky. V případě nevybudování svého národního systému elektronické identifikace může těžko Česká republika pomýšlet na umístění v předních příčkách hodnocení, která se zaobírají porovnáváním a hodnocením služeb eGovernmentu. Např. nedílnou součástí indexu DESI (The Digital Economy and Society Index) je právě hodnocení úrovně digitalizace veřejných služeb.

4. Zhodnocení souladu navrhované právní úpravy s ústavním pořádkem České republiky, mezinárodními smlouvami, jimiž je Česká republika vázána, a s předpisy Evropské unie, judikaturou soudních orgánů Evropské unie nebo obecnými právními zásadami práva Evropské unie

Navrhovaná právní úprava je v souladu s ústavním pořádkem České republiky.

Co se týče právních předpisů nejvyšší právní síly, je kromě obecných ustanovení ústavního zákona č. 1/1993 Sb., Ústava České republiky, a usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, relevantní též ustanovení čl. 7 Listiny. Návrh zákona je s těmito i dalšími ustanoveními v souladu.

Problematika elektronické identifikace není upravena žádnou mezinárodní úmluvou. Pokud jde o Úmluvu o ochraně lidských práv a základních svobod, pak je návrh zákona v souladu s požadavkem čl. 8, je tedy dodržováno právo na respektování soukromého života, neboť osobní údaje budou zpracovávány výhradně na základě zákona nebo se souhlasem subjektu údajů.

Podmínka zákonnosti je naplněna tím, že zásah je v případě předkládaného návrhu zákona stanoven právním předpisem, který odpovídá podstatným vnitrostátním požadavkům z hlediska ústavnosti, je dostupný (zákon bude vyhlášen ve Sbírce zákonů) a předvídatelný. Navrhovaná sankční ustanovení jsou slučitelná s čl. 7 Úmluvy, tj. se zásadou uložení trestu jen na základě zákona. V tomto článku se odráží princip legality a požadavky na jasnou a předvídatelnou úpravu správního trestání, zejména z hlediska předvídatelnosti hrozících postihů.

Navrhovaná právní úprava je plně v souladu s předpisy Evropské unie, judikaturou Soudního dvora Evropské unie a obecnými právními zásadami práva Evropské unie.

Návrhu zákona se dotýkají následující předpisy Evropské unie:

- 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,
- prováděcí rozhodnutí Komise (EU) 2015/296 ze dne 24. února 2015, kterým se stanoví procesní opatření pro spolupráci mezi členskými státy v oblasti elektronické identifikace,
- prováděcí nařízení Komise (EU) 2015/1501 ze dne 8. září 2015 o rámci interoperability,
- prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úroveň záruky prostředků pro elektronickou identifikaci,
- prováděcí rozhodnutí Komise (EU) 2015/1984 ze dne 3. listopadu 2015, kterým se stanoví okolnosti, formáty a postupy pro oznamování,
- směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů [s účinností od 25. května 2018 nahrazena nařízením 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].

Cílem navrhované právní úpravy je provedení adaptace národního právního řádu na nařízení eIDAS. Zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, byla započata adaptace na nařízení eIDAS, a to na část nařízení eIDAS týkající se služeb vytvářejících důvěru pro elektronické transakce. Zákonem o elektronické identifikaci bude tato adaptace dokončena.

5. Předpokládaný hospodářský a finanční dopad na státní rozpočet, ostatní veřejné rozpočty, na podnikatelské prostředí České republiky a sociální dopady

Celkové náklady na veřejné rozpočty při odhadu 25 veřejnoprávních poskytovatelů on-line služeb nebo jiných činností činí 140,1 milionů Kč investičních nákladů a 58,5 milionů Kč ročních nákladů včetně odhadovaných nákladů orgánů veřejné moci. Pro výkon agendy Ministerstva vnitra na činnost spojenou s udělováním akreditace pro správu kvalifikovaného systému elektronické identifikace, vydáváním rozhodnutí o udělení akreditace a práci dohledového orgánu nad evidencí všech změn akreditovaných osob, včetně procesu odejmutí akreditace při nesplnění zákonných podmínek, jsou plánovány roční rozpočtové náklady cca 2,8 milionů Kč za rok, počínaje rokem 2018. Jednorázové náklady na vybudování národního bodu pro identifikaci a autentizaci budou čerpány v roce schválení zákona a v roce

následujícím. Provozní náklady budou čerpány každý rok od roku následujícího po schválení zákona.

Návrh zákona může mít příznivý dopad na podnikatelské subjekty zejména v sektorech, jako je bankovníctví, telekomunikace, pojišťovnictví a podobně, kdy vzdálenou identifikaci poskytovanou národním bodem pro identifikaci a autentizaci budou moci využít též soukromoprávní kvalifikovaní správci systémů elektronické identifikace, kteří budou akreditováni na základě zákona, případně na ně napojené soukromoprávní subjekty k identifikaci svých klientů. V současné době je v legislativním procesu vládní návrh zákona, kterým se mění zákon č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů, a další související zákony, (sněmovní tisk 928), který zavádí tzv. „elektronický občanský průkaz s čipem“ jako jediný typ občanského průkazu pro všechny občany. Každý občan bude tedy moci využívat jako státem garantovaný prostředek pro elektronickou identifikaci občanský průkaz se strojově čitelnými údaji a s kontaktním elektronickým čipem obsahujícím identifikační certifikát.

6. Zhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů

Návrh zákona o elektronické identifikaci jako takový nepřináší nové administrativní povinnosti pro občana. Z návrhu textace zákona není možné dovozovat, že občan je vystavován novým povinností, jejichž nesplnění by bylo sankcionováno. Právě naopak. Návrh zákona si klade za cíl zjednodušit některé agendy veřejného sektoru, a ulehčit tak administrativní náklady občana při výkonu jeho povinností. V žádném případě není návrhem zákona zasahováno do práv a svobod fyzických osob.

Vzhledem k tomu, že návrh zákona upravuje oblast elektronických komunikací a informačních a komunikačních technologií, je nezbytné odhalit jeho dopady do soukromí občana. V rámci využívání služby elektronické identifikace budou samozřejmě zpracovávány osobní údaje.

Soukromé chování člověka v obecné rovině nebude sledováno, avšak je třeba si uvědomit, že informační systém pro elektronickou identifikaci a autentizaci bude uchovávat informace o poskytnutí elektronické identifikace, tedy o zpracování osobních údajů za účelem přidělení elektronické totožnosti, což je ale zcela nezbytné pro účely disponování informacemi o tom, kdy a kdo využil služby elektronické identifikace. Tato informace nebude veřejně dostupná. Bude využitelná pro případné soudní, správní či trestní řízení. Stejně tak budou některé služby veřejného sektoru uchovávat údaje o tom, kdy, kým a jak byly využity. Vzhledem k tomu, že meritorně se bude jednat zejména o činění podání vůči orgánům veřejné moci, je nezbytné, aby byla zaznamenána informace o učinění podání v rozsahu dostatečném pro identifikování podatele. Není to nic neobvyklého a již dnes poskytovatelé služeb nikoliv v elektronické podobě uchovávají po stanovenou dobu údaje o přístupech k těmto službám. Oblast samotného výkonu poskytování on-line služeb nebo jiných činností je ale záležitostí, kterou tento návrh zákona neřeší.

Národní bod pro identifikaci a autentizaci, tj. informační systém veřejné správy podporující proces elektronické identifikace a autentizace prostřednictvím kvalifikovaného systému elektronické identifikace, bude zpracovávat osobní údaje. Zpracování osobních údajů bude realizováno na základě využívání údajů ze základních registrů a agendových informačních systémů. Rozsah a účel zpracování je uveden přímo v návrhu zákona

o elektronické identifikaci. Informační systém bude moci využívat pouze ty osobní údaje, ke kterým bude mít ze zákona přístup, a pouze za účelem plnění své funkce, tedy ověření elektronické identity předané poskytovatelem služby pro elektronickou identifikaci, tedy kroku nezbytnému pro autentizaci uživatele, a doplnění osobních údajů vedených v základních registrech a agendových informačních systémech tak, aby bylo zaručeno, že elektronická identifikace poskytovaná v aktuálním čase odpovídá elektronické identitě zapsané v základním registru obyvatel. V návrhu zákona je explicitně uvedeno, že osobní údaje lze použít jen v případě, který je nezbytný ke splnění daného úkolu. Využívání údajů ze základních registrů a agendových informačních systémů bude podléhat pravidlům služby informačního systému základních registrů, jenž zaznamenává poskytování údajů a tyto záznamy uchovává. Subjekt údajů může požádat o záznam o využívání údajů v základním registru, který se vydává v podobě ověřeného výstupu z informačního systému veřejné správy.

V rámci agendy poskytování elektronické identifikace bude národní bod pro identifikaci a autentizaci využívat osobní údaje na žádost subjektu údajů, nikoliv z moci úřední. Fyzická osoba bude seznámena s tím, jaké osobní údaje jsou jí pro účely elektronické identifikace k přístupu k on-line službě nebo jiné činnosti poskytnuty, a rozhodne se, zda chce tyto své osobní údaje a v jakém rozsahu použít v rámci přihlášení se k této službě veřejného či soukromého sektoru; poskytovatel této služby tyto osobní údaje zpracuje pouze v případě, že subjekt údajů vysloví souhlas s tím, že poskytovateli za účelem k přihlášení k on-line službě nebo jiné činnosti předat. Tento poskytovatel služby tak bude osobní údaje zpracovávat na základě dobrovolného rozhodnutí a souhlasu subjektu údajů. Poskytovatel služby bude oprávněn tyto osobní údaje využívat pouze k tomu účelu, ke kterému mu byly poskytnuty. To znamená, že proti vydaným osobním údajům, tedy elektronickému prokázání totožnosti, poskytne nějakou subjektu údajů požadovanou službu, která vyžaduje ztotožnění uživatele. Paralelu je možné hledat v rámci využití možnosti podání prostřednictvím kontaktního místa veřejné správy, kde je fyzická osoba ztotožněna a svým jménem za účasti asistence úředníka přistupuje k žádané službě, která jeho osobní údaje zpracovává. Zpracování osobních údajů poskytovatelem služby nebude stanoveno v návrhu tohoto zákona, neboť takové zpracování spadá do působnosti příslušných agendových zákonů upravujících jednotlivé služby, potažmo do obsahu smluvního ujednání. Pro služby veřejného sektoru je subsidiárně přípustné využití ustanovení správního řádu o vedení spisu. V listinné podobě se ve spise taktéž zpracovávají osobní údaje. Otázka odpovědnosti poskytovatele on-line služby nebo jiné činnosti za zpracování osobních údajů vyplývá z obecných právních předpisů na ochranu osobních údajů. Návrh zákona navíc tuto část komunikace subjektu údajů a poskytovatele on-line služby nebo jiné činnosti řeší toliko obecně. Konkretizace tohoto vztahu může být upravena zvláštním zákonem nebo vyplývat ze smluvního ujednání.

Požadavek zákonné formy zpracování osobních údajů je v případě elektronické identifikace zachován, neboť veškeré zpracování osobních údajů, které spadá do působnosti tohoto návrhu zákona, je v návrhu stanoveno. Účelem zpracování osobních údajů je poskytnutí služby elektronické identifikace. Jeho obsahem je pak využívání osobních údajů ze základních registrů a agendových informačních systémů informačním systémem pro účely provedení elektronické identifikace. Toto zpracování osobních údajů je realizováno na žádost subjektu údajů. Subjekt údajů si pak vybírá, jak s poskytnutými osobními údaji o své osobě dál naloží, tedy typicky zda je poskytne subjektu provozujícímu on-line službu nebo jinou činnost či nikoliv. Pokud se rozhodne své osobní údaje poskytnout, vejde s poskytovatelem on-line služby nebo jiné činnosti v právní vztah, v rámci kterého je poskytovatel on-line služby nebo jiné činnosti oprávněn osobní údaje zpracovávat toliko v souladu s právními

předpisy upravujícími ochranu osobních údajů. Zpracování osobních údajů poskytovatelem on-line služby nebo jiné činnosti není předmětem návrhu tohoto zákona. Rozsah osobních údajů, které mohou být poskytnuty národnímu bodu pro identifikaci a autentizaci základními registry či agendovými informačními systémy, je stanoven v návrhu tohoto zákona. Třetí osobě, tedy poskytovateli on-line služby nebo jiné činnosti, je pak subjekt údajů poskytuje po svém uvážení. Nutno podotknout, že pokud se bude jednat o veřejnoprávní subjekt, pak bude jeho agenda, ke které je takto přístupováno, popsána v agendovém zákoně s tím, že pro účely výkonu této agendy bude tento subjekt pravděpodobně sám oprávněn využívat osobní údaje ze základního registru nebo agendového informačního systému.

Navrhovaný zákon je v souladu se zákonem č. 89/2012 Sb., občanský zákoník, neboť soukromí člověka je chráněno tím, že osobní údaje jsou zpracovávány v míře nezbytně nutné a na základě zákona, případně na žádost subjektu údajů. Cílem zpracovávání osobních údajů je poskytnutí on-line služby nebo jiné činnosti. Osobní údaje jsou využívány za účelem elektronického potvrzení totožnosti osoby, které má být poskytnuta on-line služba nebo jiná činnost. Subjekt údajů není do takového zpracování osobních údajů nikterak nucen, neboť je na jeho rozhodnutí, zda k využití on-line služby nebo jiné činnosti přistoupí či nikoliv. Není nezbytné poměřovat kolizi základních práv, neboť ty v tomto případě v kolizi nejsou. Ve světle této argumentace ob stojí i tvrzení, podle kterého je návrh zákona v souladu s Listinou základních práv a svobod, Úmluvou o ochraně lidských práv a základních svobod a ustanovením čl. 8 odst. 1 Listiny základních práv Evropské unie a čl. 16 odst. 1 Smlouvy o fungování Evropské unie.

Navrhovaná právní úprava je v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Ve smyslu tohoto zákona bude zpracování osobních údajů probíhat ve dvou právních režimech. Jednak se bude jednat o zpracování osobních údajů na základě zákona, kdy takové zpracování osobních údajů bude provádět národní bod pro identifikaci a autentizaci, který bude osobní údaje zpracovávat tak, že je bude využívat ze základních registrů nebo agendových informačních systémů a předávat je subjektu údajů. Právní oporou pro aplikaci takového procesu je mimo jiné ustanovení § 5 odst. 5 zákona č. 111/2009 Sb., o základních registrech, podle kterého jsou fyzické osobě po ověření její totožnosti poskytnuty referenční údaje, které jsou o ní vedeny. S využitím tohoto postupu je počítáno rovněž při ověřování totožnosti subjektem vydávajícím prostředky pro elektronickou identifikaci. Návrh zákona taktéž vyhovuje požadavkům Směrnice EU o ochraně osobních údajů a Směrnici EU o soukromí a elektronických komunikacích, neboť návrhem zákona jsou kladeny podmínky na poskytovatele prostředku pro elektronickou identifikaci, které se týkají bezpečnosti a mazání provozních údajů po stanoveném čase. Vzhledem k tomu, že budou využívány osobní údaje vedené v základních registrech, bude se subjekt údajů moci dozvědět o tom, jaké osobní údaje, kdy, kým a proč byly zpracovány, což již nyní umožňuje služba informačního systému základních registrů.

Na základě nařízení eIDAS je předpokládáno, že tuzemský systém elektronické identifikace bude v budoucnu napojen na systémy elektronické identifikace jiných členských států. V takovém případě bude moci dojít k situaci, kdy osobní údaje budou předávány zahraničnímu poskytovateli on-line služby nebo jiné činnosti. Vzhledem k tomu, že se tak bude dít výlučně do jiného členského státu, má tento princip oporu v zákoně o ochraně osobních údajů. Opět je nezbytně podotknout, že se tak bude dít pouze se souhlasem subjektu údajů.

Zvláštní pozornost byla věnována souladu navrhované právní úpravy s nařízením Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. Ve vztahu k tomuto nařízení lze konstatovat, že osobní údaje budou v rámci služeb elektronické identifikace zpracovávány korektně a zákonným a transparentním způsobem. Osobní údaje nebudou shromažďovány a budou zpracovávány tak, aby byla zajištěna jejich ochrana a integrita. Pro zpracování ve smyslu poskytnutí osobních údajů poskytovateli on-line služby nebo jiné činnosti bude vyžadován výslovný souhlas subjektu údajů. Povinnost doložit tento souhlas bude na poskytovateli on-line služby nebo jiné činnosti, což je oblast, kterou tento zákon věcně a obsahově neupravuje. Národní bod pro identifikaci a autentizaci bude osobní údaje zpracovávat na základě zákona. Citlivé osobní údaje neboli zvláštní kategorie osobních údajů nebude v rámci systému elektronické identifikace zpracovávána. Národní bod pro identifikaci a autentizaci bude subjektu údajů předávat informace ve smyslu čl. 14 odst. 1 nařízení. Vzhledem k nastavení systému a jeho použití budou osobní údaje de facto zpracovávány na základě žádosti subjektu údajů o přístup k osobním údajům ve smyslu čl. 15 nařízení. Zpracování osobních údajů v národním bodu pro identifikaci a autentizaci je realizováno s využitím služby informačního systému základních registrů, který zaručuje bezpečnost takového zpracování. Osobní údaje nebudou předávány do třetích zemí, neboť systém elektronické identifikace bude fungovat v rámci Evropské unie.

Navrhovaná právní úprava neobsahuje žádná ustanovení, která by narušovala právo na rovné zacházení a vedla k diskriminaci. Z hlediska principů rovnosti mužů a žen je návrh zákona neutrální, neboť navrhovaná právní úprava nemá bezprostřední, ani sekundární dopady na rovnost mužů a žen a nevede k diskriminaci jednoho z pohlaví, neboť nijak nerozlišuje, ani nezvýhodňuje jedno z pohlaví a nestanoví pro něj odlišné podmínky.

7. Zhodnocení korupčních rizik

Předkládaný návrh zákona představuje další krok k elektronizaci veřejného sektoru a rovněž ke zvýšení důvěryhodnosti elektronických transakcí prováděných prostřednictvím on-line služeb nebo jiných činností vyžadujících elektronickou identifikaci. Návrh zákona stanovuje práva a povinnosti jak pro subjekty z veřejného sektoru, tak i pro subjekty ze soukromého sektoru v případě, kdy se chtějí stát kvalifikovaným správcem systému elektronické identifikace. Pokud se konkrétní subjekt pro tento krok rozhodne, pak návrh zákona stanovuje specifická práva a povinnosti. Je nezbytné stanovit požadovanou úroveň bezpečnosti, aby byla zajištěna bezpečnost celého systému (tzv. federace správců systémů elektronické identifikace a poskytovatelů on-line služeb nebo jiných činností) a bylo možné se spoléhat na elektronickou identifikaci a autentizaci prováděnou v jeho rámci. Z tohoto pohledu proto návrh zákona nezakládá korupční rizika, neboť podstata navrhované právní úpravy je takového charakteru, který by neměl mít na korupci jako takovou negativní vliv. Vzhledem k obsahu právní úpravy tak nebyla shledána žádná rizika, která by mohla vést ke korupčnímu jednání.

V rámci posuzování korupčních rizik jsou dále hodnocena tato kritéria:

a. Přiměřenost

Předmětný návrh je svým rozsahem přiměřený množině vztahů, které má upravovat. Z důvodu zajištění důvěry je nutné zákonným předpisem stanovit podmínky, jimiž se řídí poskytování elektronické identifikace a procesy autentizace osoby. Bez stanovení těchto podmínek by vše bylo založeno na „dobrém slově“. Takovýto

stav je nežádoucí z několika pohledů. Nejvýznamnějším z těchto faktorů je zřejmě odpovědnost za případné způsobené škody chybnou nebo záměrně chybnou elektronickou identifikací a autentizací. Návrh předpisu stanovuje nové kompetence pro orgány veřejné správy, které jsou nezbytné k zajištění řádného fungování celé federace. Ministerstvo vnitra, jakožto orgán dohledu nad federací spravovanou prostřednictvím národního bodu pro identifikaci a autentizaci, bude pověřeno vykonáváním dohledu nad členy federace, zejména nad kvalifikovanými správci systémů elektronické identifikace. Vzhledem k dobrovolnosti rozhodnutí pro soukromý sektor začlenit se do federace spravované prostřednictvím národního bodu pro identifikaci a autentizaci nezakládají se pro soukromý sektor nové povinnosti, pokud se subjekt nechce z jakéhokoliv důvodu zapojit do federace. V případě zapojení do federace, náklady na přizpůsobení s vysokou pravděpodobností subjektům vzniknou, nicméně tomuto se nelze vyhnout. Zaváděním nových služeb vesměs vždy vzniknou náklady. Toto platí jak pro veřejný, tak i pro soukromý sektor.

b. Jednoznačnost

Jednoznačné právní úpravě dotčené oblasti napomáhá stanovení povinností pro kvalifikované poskytovatele a kvalifikované správce systémů elektronické identifikace. Úprava rovněž navazuje na nařízení eIDAS, které stanovuje, za jakých podmínek mají členské státy uznávat prostředky pro elektronickou identifikaci vydávané v rámci oznámených systémů elektronické identifikace. Inspirací pro stanovení procesu akreditace se stal dnes již zrušený zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve kterém bylo Ministerstvo vnitra zmocněno k udělování akreditace poskytovatelům certifikačních služeb. Akreditace napomáhala k vybudování společné úrovně bezpečnosti a právní jistoty.

c. Standardnost

Akreditace a stanovení podmínek má zajistit, aby procesy související s elektronickou identifikací a autentizací probíhaly na základě stejných principů a ctily základní požadavky. Dalším nástrojem pro zajištění standardnosti je dohled nad celým systémem, přičemž orgán dohledu má podle návrhu právní úpravy kompetenci kontrolovat kvalifikované správce systémů elektronické identifikace. Při návrhu zákona byla rovněž věnována pozornost zákonům upravujícím podobnou materii v jiných členských státech.

d. Kontrolovatelnost rozhodnutí

Vzhledem k tomu, že rozhodovací proces o akreditaci kvalifikovaných správců systémů elektronické identifikace nestátní povahy a povolení přístupu k autentizaci přes národní bod pro identifikaci a autentizaci bude prováděno na základě specifikovaných požadavků, nehrozí zde případ nejednotnosti v rozhodování. Informace o osobách, kterým byla udělena akreditace pro správu kvalifikovaného systému elektronické identifikace, budou zveřejněny na internetových stránkách Ministerstva vnitra. Kdokoliv se tedy bude moci přesvědčit, kterým osobám byla udělena akreditace pro správu kvalifikovaného systému elektronické identifikace. Toto opatření rovněž zajistí supervizi ze strany veřejnosti.

e. Odpovědnost

Stanovení odpovědnosti při přeshraniční autentizaci je normováno přímo v nařízení eIDAS, kde je určeno, která strana je za co odpovědná. Jedná se konkrétně o čl. 11

nařízení eIDAS ve spojení s preambulí č. 18 zmíněného nařízení. Režim odpovědnosti kvalifikovaných správců systémů elektronické identifikace se bude obecně řídit principy stanovenými zákonem č. 89/2012 Sb., občanský zákoník. V navrhovaném zákoně je dostatečně určena odpovědnost jednotlivých subjektů, ať už Ministerstva vnitra jako orgánu dohledu a orgánu, který rozhoduje o udělování akreditace pro správu kvalifikovaného systému elektronické identifikace, tak Správy základních registrů jako správce národního bodu pro identifikaci a autentizaci a rovněž kvalifikovaných správců systémů elektronické identifikace, kteří jsou začleněni do federace spravované Správou základních registrů jakožto správcem národního bodu pro identifikaci a autentizaci.

f. **Opravné prostředky**

Obecně pro rozhodování o udělování akreditace pro správu kvalifikovaného systému elektronické identifikace se použije jako procesní předpis zákon č. 500/2004 Sb., správní řád. Ministerstvo vnitra projednává v prvním stupni přestupky kvalifikovaných správců systémů elektronické identifikace nestátní povahy. Proti rozhodnutí Ministerstva vnitra je možné se odvolat v souladu se správním řádem. Na přestupky spáchané právníky a fyzickými osobami se budou vztahovat pravidla stanovená v zákoně č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich.

g. **Transparentnost**

Navrhovaná právní úprava nemá vliv na dostupnost informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Informace o poskytovaných službách v rámci federace budou průběžně zveřejňovány na internetových stránkách Ministerstva vnitra. Cílem celého řešení je poskytnout fyzickým a právníkům osobám nové služby, proto je nanejvýš žádoucí, aby veřejnost byla informována i o podmínkách těchto služeb a rovněž bezpečnostních doporučení, které by měly být dodržovány.

8. Zhodnocení dopadů na bezpečnost nebo obranu státu

Dopady navrhované úpravy na bezpečnost a obranu státu jsou rozebrány v závěrečné zprávě z hodnocení dopadů regulace (RIA).

B. ZVLÁŠTNÍ ČÁST

Obecně

Návrh zákona upravuje zejména využití elektronické identifikace, působnost Ministerstva vnitra a Správy základních registrů na úseku elektronické identifikace a přestupky na úseku elektronické identifikace.

Návrh zákona neřeší a ani do jeho působnosti nespadá používání elektronické identifikace v rámci soukromého práva mimo povinnosti k prokázání totožnosti stanovené zákonem.

Elektronickou identifikací se podle návrhu zákona rozumí možnost prokázání totožnosti s využitím elektronických prostředků. Jako prostředek pro elektronickou identifikaci si lze představit například certifikát, který bude uložen v paměťovém zařízení, třeba na flash disku. K elektronické identifikaci bude sloužit i občanský průkaz s kontaktním elektronickým čipem, ve kterém bude nahrán identifikační certifikát. Výhodou využívání elektronické identifikace je úspora času a peněz, dostupnost, rychlost, předvídatelnost, a to, že jedním prostředkem pro elektronickou identifikaci se bude možné přihlásit k více on-line službám nebo jiným činnostem. Využitelnost se nabízí zejména u služeb, které z povahy věci mohou být činěny na dálku a nevyžadují prezenční účast na úřadě.

Podle návrhu zákona, stanoví-li právní předpis povinnost k prokázání totožnosti nebo je prokázání totožnosti vyžadováno v rámci výkonu působnosti (tzn. veřejné moci), lze umožnit elektronické prokázání totožnosti. Aby bylo zaručeno, že elektronická identifikace pro účely plnění právních povinností bude probíhat toliko skrze důvěryhodný systém napojený na základní registry, je k takovému prokázání totožnosti elektronicky možné využít pouze kvalifikovaný systém elektronické identifikace. Kvalifikovaný systém elektronické identifikace je systém, který slouží *pro vydávání prostředků pro elektronickou identifikaci a k zajištění procesu samotné elektronické identifikace* jako takové. Aby bylo možné považovat systém elektronické identifikace za kvalifikovaný, bude muset splňovat zákonné požadavky. Vždy bude muset být provozován kvalifikovaným správcem systému elektronické identifikace. Kvalifikovaným systémem elektronické identifikace bude podle návrhu zákona i systém zahraniční, který bude oznámen podle pravidel stanovených nařízením eIDAS.

Kvalifikovaným správcem systému elektronické identifikace může být podle návrhu zákona jednak státní orgán, jednak osoba, které byla udělena akreditace pro správu kvalifikovaného systému elektronické identifikace, tj. akreditovaná osoba. Bude-li státní orgán zamýšlet vydávat prostředky pro elektronickou identifikaci a zajišťovat proces prokazování totožnosti na dálku, bude ze zákona při splnění jeho podmínek kvalifikovaným správcem systému elektronické identifikace. Ostatní subjekty, tedy soukromoprávní entity, ale i kraje nebo obce, budou muset projít procesem akreditace, aby získaly status kvalifikovaného správce systému elektronické identifikace. V rámci akreditace bude muset žadatel o akreditaci mimo jiné prokázat, že splňuje požadavky stanovené zákonem, bude muset být pojištěn pro případ odpovědnosti za škodu a být bezúhonný. Každý kvalifikovaný správce systému elektronické identifikace bude muset dodržovat povinnosti stanovené návrhem zákona a samozřejmě stanovené jinými právními předpisy. Mimo jiné podle návrhu zákona povede evidenci jím vydaných prostředků pro elektronickou identifikaci.

O udělení akreditace bude rozhodovat Ministerstvo vnitra. Prostředek pro elektronickou identifikaci a systém elektronické identifikace však nebude v rámci procesu akreditace primárně posuzovat Ministerstvo vnitra, ale jím pověřená osoba. Touto osobou může být na základě žádosti osoba pověřená k provádění atestací dle zákona o informačních systémech veřejné správy. Pouze pokud by neexistovala žádná pověřená osoba, pak by posuzovat prostředek pro elektronickou identifikaci a systém elektronické identifikace posuzovalo přímo Ministerstvo vnitra.

Kvalifikovaným poskytovatelem je podle návrhu zákona míněn ten, kdo umožňuje prokázání totožnosti, které vyžaduje právní předpis nebo výkon působnosti, s využitím elektronické identifikace, a to při poskytování on-line služby nebo realizace jiných svých úkolů (činností). Takovou on-line službu nebo jinou činnost může představovat například agenda úřadu, který se rozhodl nebo kterému zákon stanoví, že podání žádosti bude moci probíhat i elektronicky. Příkladem takového kvalifikovaného poskytovatele může být Ministerstvo vnitra při samoobslužném poskytování výpisů z jím spravovaných databází.

Elektronické prokazování totožnosti bude realizováno s přístupem a ověřením osobních údajů zejména v základním registru obyvatel a informačním systému evidence obyvatel. Tento přístup a ověřování bude zajišťovat informační systém veřejné správy národní bod pro identifikaci a autentizaci. Správcem tohoto systému bude Správa základních registrů.

Proces přihlášení se k on-line službě nebo jiné činnosti a využití on-line služby nebo jiné činnosti si lze představit následovně. Osoba si vybere on-line službu nebo jinou činnost, kterou chce využít. Poskytovatel této služby automatizovaně přesměruje započatou komunikaci na národní bod pro identifikaci a autentizaci, přičemž musí být zřejmé, jakou úroveň záruky prostředku pro elektronickou identifikaci kvalifikovaný poskytovatel při prokázání totožnosti s využitím elektronické identifikace požaduje. Národní bod pro identifikaci a autentizaci osobě, která má v úmyslu službu využít, zobrazí prostředky pro elektronickou identifikaci, kterými se lze ke službě identifikovat (tyto musí odpovídat příslušné úrovni záruky, kterou požaduje kvalifikovaný poskytovatel). Osoba si vybere prostředek pro elektronickou identifikaci, který má k dispozici. Národní bod pro identifikaci a autentizaci pak komunikaci automatizovaně přesměruje ke kvalifikovanému správci systému elektronické identifikace, pod jehož kvalifikovaný systém elektronické identifikace příslušný prostředek pro elektronickou identifikaci spadá. Úkolem kvalifikovaného správce systému elektronické identifikace je identifikovat a rovněž autentizovat osobu, jejímž cílem je službu využít. V případě, že je tato osoba úspěšně identifikována a autentizována, pokračuje komunikace zpět k národnímu bodu pro identifikaci a autentizaci. Ten provede další ověření totožnosti osoby s využitím údajů ze základního registru obyvatel a následně doplní údaje ze svého datového fondu, které jsou pro poskytnutí služby nezbytné a které automatizovaně získá z relevantních informačních systémů veřejné správy. Kompletní údaje o osobě, která chce službu využít, po jejím odsouhlasení předá poskytovateli služby, tedy kvalifikovanému poskytovateli. Kvalifikovaný poskytovatel na základě obdržených údajů autorizuje identifikovanou a autentizovanou osobu a umožní jí práci se službou.

Návrh zákona stanoví i některé povinnosti pro držitele prostředku pro elektronickou identifikaci. Ten bude muset ověřovat správnost údajů při převzetí prostředku pro elektronickou identifikaci, zacházet s prostředkem pro elektronickou identifikaci s náležitou péčí tak, aby minimalizoval jeho zneužití a hlásit jeho zneužití.

S návrhem zákona o elektronické identifikaci je současně předkládán návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o elektronické identifikaci, který reflektuje změny vyvolané návrhem zákona o elektronické identifikaci a nařízením eIDAS.

K § 1

V zájmu snazší orientace adresáta zákona paragraf deklaruje obsah zákona.

Součástí zákona o elektronické identifikaci není ustanovení, které by definovalo pojmy spjaté s problematikou elektronické identifikace. Je tomu tak především z důvodu, že většinu těchto pojmů definuje přímo nařízení eIDAS, přičemž principy evropského práva neumožňují duplikovat definice obsažené v přímo použitelných právních předpisech Evropské unie ve vnitrostátních právních předpisech. Klíčové pojmy, které z uvedeného nařízení vycházejí a s nimiž pracuje také zákon o elektronické identifikaci, jsou především:

- elektronická identifikace jakožto postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu;
- prostředek pro elektronickou identifikaci jakožto hmotná či nehmotná jednotka obsahující osobní identifikační údaje, která se používá k autentizaci pro účely on-line služby; příkladem takového prostředku je občanský průkaz s kontaktním elektronickým čipem;
- osobní identifikační údaje jakožto soubor údajů umožňujících určit totožnost fyzické či právnické osoby nebo fyzické osoby zastupující právnickou osobu;
- systém elektronické identifikace jakožto systém pro elektronickou identifikaci, na jehož základě jsou fyzickým či právnickým osobám nebo fyzickým osobám zastupujícím právnické osoby vydávány prostředky pro elektronickou identifikaci;
- autentizace jakožto elektronický postup, který umožňuje potvrdit elektronickou identifikaci fyzické či právnické osoby nebo původ a integritu dat v elektronické podobě;
- spoléhající se strana jakožto fyzická nebo právnická osoba, která se spoléhá na elektronickou identifikaci nebo službu vytvářející důvěru (pro účely zákona o elektronické identifikaci je relevantní část definice vztahující se k elektronické identifikaci).

Zákon o elektronické identifikaci dále zavádí pojmy, které nařízení eIDAS nezná, které jsou však s elektronickou identifikací spjaty. Tyto pojmy jsou vždy vysvětleny v rámci odůvodnění příslušného ustanovení.

Zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce byla započata adaptace na nařízení eIDAS. Zákonem o elektronické identifikaci bude tato adaptace dokončena.

K § 2

Jedná se o klíčové ustanovení zákona o elektronické identifikaci, které zakotvuje obecné pravidlo vztahující se k prokazování totožnosti s využitím elektronické identifikace. Pojem elektronická identifikace definuje nařízení eIDAS ve svém čl. 3 odst. 1 jako postup

používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu.

Obecné pravidlo, které tvoří podstatu daného ustanovení, může být modifikováno zvláštními zákony například v tom smyslu, že tyto zákony možnost prokázání totožnosti s využitím elektronické identifikace zcela vyloučí, nebo naopak omezí způsoby prokázání totožnosti na ty s využitím elektronické identifikace. Zvláštní právní předpisy mohou upravovat také vlastní způsoby prokazování totožnosti na dálku. Příkladem je zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, nebo zákon č. 187/2006 Sb., o nemocenském pojištění.

Zákon o elektronické identifikaci představuje právní základ pro prokazování totožnosti s využitím elektronické identifikace, pakliže právní předpis, nebo výkon působnosti vyžaduje prokázání totožnosti. Ustanovení má dopad jak do právních vztahů regulovaných právem veřejným, tak i právních vztahů řídicích se pouze principy práva soukromého. Formulace „vyžaduje-li právní předpis“ se vztahuje k oběma oblastem, formulace „vyžaduje-li výkon působnosti“ toliko k veřejnoprávní sféře. V soukromoprávních vztazích jsou dotčené subjekty podřízeny režimu § 2 pouze v případě, kdy je prokázání totožnosti, eventuálně její vyžadování stanoveno právním předpisem *jako povinnost, nikoliv jako možnost, respektive oprávnění*. V těchto vztazích tak § 2 nedopadá například na osoby ověřující totožnost osob vstupujících do budovy na základě obecného oprávnění vlastníka budovy. Příkladem právního předpisu vyžadujícího prokázání totožnosti v oblasti soukromoprávních vztahů je zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, jehož § 7 stanoví povinnost identifikace. V oblasti veřejnoprávních vztahů budou režimu § 2 podléhat nejenom situace, kdy právní předpis stanoví povinnost prokázat totožnost (vyžadovat prokázání totožnosti), nýbrž i situace, kdy tak budou vyžadovat okolnosti naplnování působnosti (tedy uplatňování veřejné moci), pochopitelně v mezích pravomoci konkrétního vykonavatele působnosti. Pojem „působnost“ navrhovaný zákonem pojímá v tomtéž smyslu jako Ústava České republiky, tj. výkonem působnosti se rozumí výkon veřejné moci. Ve stejném smyslu pojímá výkon působnosti také správní řád, který je zdrojem pravidel regulujících výkon převážné části působnosti v oblasti veřejné správy, a konečně i druhý právní předpis adaptující nařízení eIDAS, zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. Terminologická jednotnost obou adaptačních zákonů je v případě tohoto pojmu klíčová, jakákoliv nuance v jednom zákonu může mít negativní vliv na interpretaci druhého zákona.

Prokázání totožnosti s využitím elektronické identifikace je podmíněno dvěma skutečnostmi. V první řadě je zapotřebí, aby bylo prokázání totožnosti s využitím elektronické identifikace umožněno ze strany subjektu oprávněného k ověření totožnosti. To znamená, že umožnění prokázání totožnosti s využitím elektronické identifikace je zcela v kompetenci subjektu, který totožnost ověřuje, není tedy odvislé od vůle zákonodárce (ledaže by jiný zákon stanovil jinak). Další podmínkou či spíše povinností je umožnění prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace. Kvalifikovaný systém elektronické identifikace má dvě činnostní dimenze. Tou první je služba vydávání prostředků pro elektronickou identifikaci, druhou pak vlastní služba provozování postupu autentizace.

Prokázání totožnosti s využitím elektronické identifikace je imanentní to, že není vyžadována fyzická přítomnost osoby, která prokazuje svoji totožnost, neboť tato je nahrazena vzdáleným ztotožněním, které probíhá prostřednictvím kvalifikovaného systému

elektronické identifikace. Tento systém umožňuje, aby byly na dálku činěny úkony, jež jsou běžně spojeny s osobním ztotožněním určité osoby. Jako konkrétní příklad si lze představit situaci, kdy se osoba, která je držitelem prostředku pro elektronickou identifikaci, přihlásí k určité elektronické aplikaci, přičemž v případě, že se tato osoba identifikuje a následně je autentizována (tj. její totožnost je potvrzena), mohou jí být prostřednictvím této elektronické aplikace poskytnuty služby, které příslušná elektronická aplikace nabízí. Zpravidla se bude jednat o poskytnutí aktuálních údajů vedených o dané osobě v příslušné agendě, například ve formě výpisu. Lze předeslat, že v současné době se jako pilotní oblast pro umožnění prokázání totožnosti s využitím elektronické identifikace jeví oblast sociální.

V souvislosti s elektronickou identifikací je třeba uvést, že zákonem o elektronické identifikaci není obecná identifikace fyzické osoby ve smyslu § 3019 zákona č. 89/2012 Sb., občanský zákoník, dotčena.

Pro úplnost je uveden přehled právních předpisů s jednotlivými ustanoveními, v nichž se objevuje povinnost prokázat/ověřit/zjistit totožnost (v přehledu nejsou zahrnuty právní předpisy, které k prokázání/ověření/zjištění totožnosti požadují konkrétní doklad):

- zákon č. 141/1961 Sb., trestní řád – § 91 odst. 1, § 101 odst. 1, § 111 odst. 2 a 3, § 114 odst. 3 a § 205 odst. 1;
- zákon č. 99/1963 Sb., občanský soudní řád – § 50c odst. 2, § 126 odst. 2, § 329 odst. 1 a § 336h odst. 5;
- zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon) – § 31 odst. 10;
- zákon č. 553/1991 Sb., o obecní policii – § 12 odst. 2;
- zákon č. 114/1992 Sb., o ochraně přírody a krajiny – § 5a odst. 3, § 54 odst. 2, § 77 odst. 1 písm. l), § 77a odst. 4 písm. q), § 80 odst. 1 a § 81 odst. 7 písm. a);
- zákon č. 555/1992 Sb., o Vězeňské službě a justiční strážní České republiky – § 13 odst. 1a 2 a § 22 odst. 1;
- zákon č. 182/1993 Sb., o Ústavním soudu – § 103 odst. 1;
- zákon č. 111/1994 Sb., o silniční dopravě – § 18a odst. 2 písm. d);
- zákon č. 266/1994 Sb., o dráhách – § 37 odst. 5 písm. d);
- zákon č. 289/1995 Sb., o lesích a o změně a doplnění některých zákonů – § 39 odst. 2;
- zákon č. 140/1996 Sb., o zpřístupnění svazků vzniklých činnostmi bývalé Státní bezpečnosti – § 8 odst. 3;
- zákon č. 13/1997 Sb., o pozemních komunikacích – § 40 odst. 8;
- zákon č. 49/1997 Sb., o civilním letectví a o změně a doplnění zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů – § 85g odst. 1;
- zákon č. 26/2000 Sb., o veřejných dražbách – § 23 odst. 2 a § 47 odst. 2;
- zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel) – § 8 odst. 5;
- zákon č. 242/2000 Sb., o ekologickém zemědělství a o změně zákona č. 368/1992 Sb., o správních poplatcích, ve znění pozdějších předpisů – § 30 odst. 2;
- zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů – § 19 odst. 3;
- zákon č. 301/2000 Sb., o matrikách, jménu a příjmení a o změně některých souvisejících zákonů – § 14 odst. 5;
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů – § 9b odst. 3;

- zákon č. 56/2001 Sb., o podmínkách provozu vozidel na pozemních komunikacích a o změně zákona č. 168/1999 Sb., o pojištění odpovědnosti za škodu způsobenou provozem vozidla a o změně některých souvisejících zákonů (zákon o pojištění odpovědnosti z provozu vozidla), ve znění zákona č. 307/1999 Sb. – § 8 odst. 3;
- zákon č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením a o změně zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů – § 10 písm. a);
- zákon č. 440/2003 Sb., o nakládání se surovými diamanty, o podmínkách jejich dovozu, vývozu a tranzitu a o změně některých zákonů – § 27 odst. 5;
- zákon č. 100/2004 Sb., o ochraně druhů volně žijících živočichů a planě rostoucích rostlin regulováním obchodu s nimi a dalších opatřeních k ochraně těchto druhů a o změně některých zákonů (zákon o obchodování s ohroženými druhy) – § 25 odst. 4 písm. b) a § 30 odst. 1;
- zákon č. 99/2004 Sb., o rybníkářství, výkonu rybářského práva, rybářské strážní, ochraně mořských rybolovných zdrojů a o změně některých zákonů (zákon o rybářství) – § 16 písm. b) bod 1;
- zákon č. 190/2004 Sb., o dluhopisech – § 24a odst. 2;
- zákon č. 561/2004 Sb., o předškolním, školním, středním, vyšším odborném a jiném vzdělávání (školský zákon) – § 60g odst. 2;
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti – § 104 odst. 2;
- zákon č. 187/2006 Sb., o nemocenském pojištění – § 64 odst. 1 písm. b) a d);
- zákon č. 378/2007 Sb., o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech) – § 101 odst. 2 písm. c);
- zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu – § 8 odst. 2 a 6 a § 11 odst. 8;
- zákon č. 273/2008 Sb., o Policii České republiky – § 36 odst. 3, § 48 odst. 4 písm. b) a § 63 odst. 2;
- zákon č. 111/2009 Sb., o základních registrech – § 5 odst. 5 a § 58 odst. 8;
- zákon č. 280/2009 Sb., daňový řád – § 23 odst. 1, § 43 odst. 2 a § 194 odst. 4;
- zákon č. 284/2009 Sb., o platebním styku – § 124j odst. 5;
- zákon č. 136/2011 Sb., o oběhu bankovek a mincí a o změně zákona č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů – § 11 odst. 2 a § 12 odst. 2 písm. b) a odst. 4;
- zákon č. 341/2011 Sb., o Generální inspekci bezpečnostních sborů a o změně souvisejících zákonů – § 32 odst. 2;
- zákon č. 17/2012 Sb., o Celní správě České republiky – § 29 odst. 2 a § 49 odst. 2;
- zákon č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) – § 167 odst. 2 a § 398 odst. 2;
- zákon č. 255/2012 Sb., o kontrole (kontrolní řád) – § 8;
- zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních – § 58 odst. 5;
- zákon č. 256/2013 Sb., o katastru nemovitostí (katastrální zákon) – § 52 odst. 3 a 4;
- zákon č. 300/2013 Sb., o Vojenské policii a o změně některých zákonů (zákon o Vojenské policii) – § 27 odst. 2 a 3;
- zákon č. 320/2015 Sb., o Hasičském záchranném sboru České republiky a o změně některých zákonů (zákon o hasičském záchranném sboru) – § 33 odst. 2;
- zákon č. 186/2016 Sb., o hazardních hrách – § 29 odst. 3, § 44 odst. 3, § 46, § 71 odst. 3 a § 76 odst. 3;

- zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce – § 17 odst. 4 písm. a).

K § 3

K odstavci 1

Pojem kvalifikovaný systém elektronické identifikace vychází z pojmu systém elektronické identifikace, který nařízení eIDAS definuje v čl. 3 odst. 4 jako systém pro elektronickou identifikaci, na jehož základě jsou fyzickým či právnickým osobám nebo fyzickým osobám zastupujícím právnické osoby vydávány prostředky pro elektronickou identifikaci. Ve smyslu nařízení eIDAS je tedy systém elektronické identifikace úzce spojen s prostředkem pro elektronickou identifikaci definovaným v čl. 3 odst. 2, tedy hmotnou či nehmotnou jednotkou obsahující identifikační údaje, která se používá k autentizaci pro účely on-line služby. Systém elektronické identifikace je však nutno chápat v pojetí širším, zahrnujícím rovněž proces autentizace. Autentizace představuje elektronický postup, který umožňuje potvrdit elektronickou identifikaci fyzické či právnické osoby nebo původ a integritu dat v elektronické podobě (vizte čl. 3 odst. 5 nařízení eIDAS). Z definice prostředku pro elektronickou identifikaci plyne, že tento se používá právě k autentizaci konkrétní osoby. Systém elektronické identifikace tedy zajišťuje poskytování dvou do jisté míry samostatných služeb, z nichž první spočívá ve vydávání prostředků pro elektronickou identifikaci, obsahem druhé je potom vlastní umožnění procesu autentizace. Aby systém elektronické identifikace nabyl přívlastku „kvalifikovaný“, musí splňovat podmínky stanovené zákonem o elektronické identifikaci.

První z podmínek spočívá v požadavku na osobu, která má daný systém elektronické identifikace spravovat. Touto osobou může být pouze kvalifikovaný správce systému elektronické identifikace, jenž je samostatně upraven v rámci § 4.

Další podmínka má vztah k čl. 8 nařízení eIDAS, v němž jsou definovány úrovně záruky systémů elektronické identifikace. Nařízení eIDAS rozlišuje úroveň nízkou, značnou a vysokou, přičemž uvedené úrovně záruky musí splňovat tato příslušná kritéria:

- 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**;
- 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**;
- 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**.

Výše uvedené úrovně záruky systémů elektronické identifikace podrobněji specifikuje 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 eIDAS.

Dále se vyžaduje, aby kvalifikovaný systém elektronické identifikace umožňoval poskytnutí služby národního bodu pro identifikaci a autentizaci. Národní bod pro identifikaci a autentizaci je informačním systémem veřejné správy a službou informačního systému veřejné správy se obecně rozumí, jak vyplývá z § 2 písm. g) zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, činnost informačního systému uspokojující dané požadavky oprávněného subjektu spojená s funkcí informačního systému. V případě národního bodu pro identifikaci a autentizaci bude službou poskytování, respektive zprostředkování dat. Kvalifikovaný systém elektronické identifikace by měl být tedy nastaven způsobem, aby byl s to takovou službu využívat (musí být s národním bodem pro identifikaci a autentizaci kompatibilní).

Poslední dva požadavky souvisí s čl. 7 písm. d) nařízení eIDAS a čl. 7 písm. e) nařízení eIDAS a s již zmiňovaným prováděcím nařízením Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci.

K odstavci 2

Za kvalifikovaný systém elektronické identifikace je považován také systém elektronické identifikace, který byl oznámen v souladu s čl. 9 nařízení eIDAS a v jehož rámci je vydáván a používán pouze prostředek pro elektronickou identifikaci s úrovní záruky alespoň značnou. Značnou úroveň záruky prostředku pro elektronickou identifikaci charakterizuje prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, podle něhož prostředek pro elektronickou identifikaci se značnou úrovní záruky využívá alespoň dvou faktorů autentizace z odlišných kategorií a je navržen tak, aby jej mohla osoba, které patří, spolehlivě chránit před zneužitím třetí osobou.

Důvodem zahrnutí je fakt, že podle čl. 6 nařízení eIDAS mají členské státy takový systém, respektive v jeho rámci provedenou elektronickou identifikaci a autentizaci uznávat.

K § 4

V příslušném ustanovení je zakotvena funkce tzv. kvalifikovaného správce systému elektronické identifikace, jehož činnost spočívá ve správě kvalifikovaného systému elektronické identifikace. Zákon o elektronické identifikaci vymezuje dva okruhy kvalifikovaných správců systémů elektronické identifikace, přičemž rozlišuje mezi kvalifikovanými správci státními a kvalifikovanými správci nestátními. Státním kvalifikovaným správcem systému elektronické identifikace může být státní orgán plnící povinnosti uvedené v § 16. Tímto kvalifikovaným správcem systému elektronické identifikace tak bude například Ministerstvo vnitra, které se pro účely elektronické identifikace považuje za vydavatele občanského průkazu se strojově čitelnými údaji a s kontaktním elektronickým čipem jakožto prostředku pro elektronickou identifikaci. Nestátním kvalifikovaným správcem systému elektronické identifikace se rozumí osoba, které byla udělena akreditace pro správu kvalifikovaného systému elektronické identifikace, tedy osoba, která splnila podmínky akreditace a zároveň plní povinnosti uvedené v § 16. Na nestátního kvalifikovaného správce systému elektronické identifikace jsou

z pochopitelných důvodů kladeny jiné požadavky než na státního kvalifikovaného správce systému elektronické identifikace, neboť jde o subjekt podléhající odlišným principům než státní orgány. Konstrukce vychází z čl. 7 písm. a) nařízení eIDAS, které vždy předpokládá ingerenci státu při využívání elektronické identifikace, a čl. 11 odst. 1 téhož právního předpisu zakládajícího odpovědnost státu na úseku elektronické identifikace.

Státním orgánem, který může být kvalifikovaným správcem systému elektronické identifikace, se rozumí zákonem nebo na základě zákona (např. rozhodnutím) zřízená či ustavená organizační jednotka státu, jejímž prostřednictvím a v rozsahu jí svěřených kompetencí stát jedná. Za takovou jednotku lze považovat organizační složky státu či jejich soubory a entity obdobného postavení jako organizační složky státu (např. Kancelář Poslanecké sněmovny či Kancelář Senátu), státní sbory (např. Policie České republiky), s ohledem na jejich postavení některé právnické osoby (např. Česká národní banka), sbory fyzických osob (např. vláda) a jednotlivé fyzické osoby (např. prezident republiky či veřejný ochránce práv).

Obdobně jako nařízení eIDAS chápe zákon o elektronické identifikaci osobu kvalifikovaného správce systému elektronické identifikace ve dvojitě smyslu. Jednak jako stranu vydávající prostředky pro elektronickou identifikaci, jednak jako stranu provozující samotný postup autentizace, tj. potvrzování totožnosti. Obě tyto služby tvoří kostru kvalifikovaného systému elektronické identifikace, jehož správa náleží kvalifikovanému správci systému elektronické identifikace.

Jde-li o první ze zmíněných služeb, tedy vydávání prostředku pro elektronickou identifikaci, tato služba je nutně spojena s prvotním ztotožněním žadatele o vydání prostředku pro elektronickou identifikaci. Kvalifikovaný správce systému elektronické identifikace využívá při ztotožnění žadatele o vydání prostředku pro elektronickou identifikaci služeb národního bodu pro identifikaci a autentizaci.

K § 5

Ustanovení upravuje proces udělení akreditace pro správu kvalifikovaného systému elektronické identifikace. Nezbytným předpokladem k zahájení procesu akreditace je zaslání písemné žádosti Ministerstvu vnitra (řízení o udělení akreditace tedy bude řízením o žádosti ve smyslu zákona č. 500/2004 Sb., správní řád, přičemž požadavek písemné formy žádosti vylučuje ústní žádost zaznamenanou v protokolu). Žádost musí předně obsahovat obecné náležitosti, které jsou stanoveny v § 37 zákona č. 500/2004 Sb., tzn. identifikační údaje žadatele o akreditaci, označení správního orgánu (kterým je v tomto případě Ministerstvo vnitra) a podpis žadatele o akreditaci.

Podmínky pro udělení akreditace jsou obsaženy v odstavci 2 a jsou jimi: prostředek pro elektronickou identifikaci a systém elektronické identifikace žadatele o akreditaci, které splňují technické specifikace, normy a postupy stanovené prováděcím nařízením Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úroveň záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení eIDAS, bezúhonnost žadatele o akreditaci, pojištění odpovědnosti za škodu způsobenou při správě kvalifikovaného systému elektronické identifikace, plán ukončení činnosti, skutečnost, že systém elektronické identifikace žadatele o akreditaci umožňuje poskytnutí služby národního bodu pro identifikaci a autentizaci a skutečnost, že žadatel o akreditaci je způsobilý pro správu kvalifikovaného systému elektronické identifikace

z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob. Cílem těchto požadavků je zajištění věcně správného a zákonného výkonu akreditované činnosti. Takový výkon mohou zajistit pouze osoby disponující určitými vlastnostmi.

K žádosti o akreditaci musí být připojeny dokumenty, které dokládají splnění výše uvedených požadavků kladených na akreditovanou osobu. Jedná se o odbornou dokumentaci vyžadovanou ke správnému výkonu činnosti kvalifikovaného správce systému elektronické identifikace [posouzení souladu jím používaného prostředku pro elektronickou identifikaci a jím spravovaného systému elektronické identifikace s požadavky prováděcího nařízení Komise (EU) 2015/1502 ze dne 8. září 2015], smlouvu o uzavřeném pojištění odpovědnosti za škodu způsobenou při správě kvalifikovaného systému elektronické identifikace, doklad o bezúhonnosti, neprokazuje-li se bezúhonnost výpisem z evidence Rejstříku trestů (výpis si Ministerstvo vnitra vyžádá podle § 10 odst. 6) a plán ukončení činnosti coby dokument upravující postup kvalifikovaného správce systému elektronické identifikace při ukončení jeho činnosti.

Odstavec 4 se váže k jedné z podmínek pro udělení akreditace, konkrétně k podmínce spočívající ve skutečnosti, že systém elektronické identifikace žadatele o akreditaci umožňuje poskytnutí služby národního bodu pro identifikaci a autentizaci [vizte § 5 odst. 2 písm. e)]. Za účelem zjištění, zda systém elektronické identifikace žadatele o akreditaci splňuje tuto podmínku, je Ministerstvo vnitra oprávněno vyžádat si vyjádření správce národního bodu pro identifikaci a autentizaci, tedy Správy základních registrů. Správci národního bodu pro identifikaci a autentizaci je tato kompetence založena v § 19 odst. 2 písm. a). Žadatel o akreditaci tedy uvedenou podmínku pro udělení akreditace nikterak nedokládá, obstarání potřebného vyjádření správce národního bodu pro identifikaci a autentizaci si zabezpečuje Ministerstvo vnitra samo (žadatel však musí poskytnout součinnost Správě základních registrů při samotném posuzování splnění podmínky).

Odstavec 5 navazuje na další z podmínek pro udělení akreditace, konkrétně na podmínku spočívající ve skutečnosti, že žadatel o akreditaci je způsobilý pro správu kvalifikovaného systému elektronické identifikace z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob. S ohledem na důsledky spojené s potvrzením totožnosti osoby je smysl této podmínky zřejmý, tedy zajistit, aby kvalifikovanými správci systémů elektronické identifikace byly pouze důvěryhodné subjekty. Ministerstvo vnitra je při zjišťování této skutečnosti oprávněno požádat o informace Policii České republiky, zpravodajskou službu nebo jiný orgán.

Odstavec 6 ustanovení upravuje lhůtu k vydání rozhodnutí o udělení akreditace. Odchylku od obecné právní úpravy v zákoně č. 500/2004 Sb. vyžaduje složitost projednávané materie. Činnost vykonávaná akreditovanou osobou je náročná na odborné posouzení, a proto není možné rozhodnout ve lhůtě stanovené obecně pro jakákoli správní řízení (tzn. bezodkladně, popřípadě do 30 dnů).

Povinností akreditované osoby je pak oznámit Ministerstvu vnitra, že přestala splňovat některou z podmínek pro udělení akreditace, neboť tato skutečnost má klíčový vliv na trvání akreditace.

K § 6

Ustanovení § 6 stanoví podmínky pro změnu akreditace, která je možná na základě písemné žádosti akreditované osoby o rozšíření správy kvalifikovaného systému elektronické identifikace o vydávání a používání dalšího prostředku pro elektronickou identifikaci.

Pro posouzení změny akreditace spočívající v rozšíření správy kvalifikovaného systému elektronické identifikace o další prostředek pro elektronickou identifikaci musí akreditovaná osoba doložit splnění podmínky podle § 5 odst. 2 písm. a). Další prostředek pro elektronickou identifikaci a systém elektronické identifikace tedy musí být v souladu s prováděcím nařízením Komise (EU) 2015/1502.

O změně akreditace spočívající v rozšíření správy kvalifikovaného systému elektronické identifikace o další prostředek pro elektronickou identifikaci rozhodne Ministerstvo vnitra do 3 měsíců ode dne podání žádosti. I zde je tedy odchylka od obecné úpravy v zákoně č. 500/2004 Sb., neboť složitost projednávané materie vyžaduje delší lhůtu pro rozhodnutí. Pokud akreditovaná osoba splní požadavek stanovený v odstavci 2, Ministerstvo vnitra změní akreditaci. Nesplní-li akreditovaná osoba zákonem stanovený požadavek, Ministerstvo vnitra její žádost zamítne. Zamítnutí pochopitelně nebude mít vliv na poskytování služeb v rámci původního rozsahu akreditace, pouze nebude možné využívat další prostředek pro elektronickou identifikaci.

K § 7 a 8

Zákon v § 7 a 8 stanoví, v jakých případech akreditace zaniká a v jakých případech ji Ministerstvo vnitra může akreditované osobě odejmout. Vedle vlastní písemné žádosti akreditované osoby (nikdo nemůže být nucen vykonávat proti své vůli činnost akreditované osoby) může Ministerstvo vnitra akreditaci odejmout v případech, kdy akreditovaná osoba přestala splňovat některou z podmínek pro udělení akreditace stanovených v § 5 odst. 2 a ani po písemném upozornění Ministerstva vnitra nezjedнала bez zbytečného odkladu nápravu tohoto stavu. Vytvoření prostoru pro nápravu je činěno z toho důvodu, že případné odejmutí akreditace zasáhne nejenom samotnou akreditovanou osobu, ale zejména držitele jí vydaných prostředků pro elektronickou identifikaci a konečně i kvalifikované poskytovatele, tedy ovlivní velké množství právních vztahů. Odejmutí akreditace bude reakcí na notifikaci ze strany akreditované osoby nebo na zjištění z vlastní kontrolní činnosti. Akreditace pak přirozeně zaniká se zánikem akreditované osoby nebo její smrtí, neboť je svázána s „osobními“ poměry akreditované osoby. V tomto smyslu se úprava v zásadě neliší od úpravy jiných akreditací.

K § 9

Akreditované osoby, respektive žadatelé o akreditaci musí mít uzavřené pojištění pro případ odpovědnosti za škodu způsobenou při správě kvalifikovaného systému elektronické identifikace. Bez předložení smlouvy o uzavřeném pojištění není možné s ohledem na možný rozsah a povahu škod, které by mohly při činnosti kvalifikovaného správce systému elektronické identifikace vzniknout, tuto činnost vykonávat.

Uzavření pojištění je povinné pouze pro akreditované osoby, tedy nikoli pro ty kvalifikované správce systému elektronické identifikace, kteří jsou státními orgány. Je nepravděpodobné, že by státní orgány nebyly schopny dostát svým závazkům a uhradit

vzniklou škodu. Pojištění těchto subjektů by bylo ekonomicky nevýhodné a ze stávající praxe nejsou známy případy, kdy by i mnohem závažnější činnosti vykonávané státním orgánem byly pojišťovány.

Povinné pojištění akreditovaných osob představuje tzv. bezpečnostní „pojistku“ pro případy, kdy v souvislosti se správou kvalifikovaného systému elektronické identifikace vznikne škoda zainteresovaným stranám (například kvalifikovaným poskytovatelům, držitelům prostředků pro elektronickou identifikaci, státu). Význam nutnosti existence pojištění akreditovaných osob je možné spatřovat nejvíce v těch případech, kdy kvalifikovaný správce systému elektronické identifikace nestátní povahy, tedy akreditovaná osoba, ukončil činnost a nedisponuje dostatečnými finančními prostředky, které by pokryly jím způsobené případné škody. Pro akreditované osoby spočívá výhoda pojištění v tom, že nemusí udržovat vysoké finanční prostředky pro krytí případných škod. Další výhodou pojištění akreditovaných osob je fakt, že v případě, kdy akreditovaná osoba při správě kvalifikovaného systému elektronické identifikace způsobí škodu, nemusí mít tato událost nutně vliv na její činnost tak, jak by tomu bylo v případě, kdy by musela tuto škodu hradit z vlastního rozpočtu. Rovněž dle prováděcího nařízení Komise (EU) 2015/1502 musí poskytovatelé, kteří poskytují služby související s elektronickou identifikací v přeshraničním kontextu, prokázat svou schopnost převzít riziko odpovědnosti za škodu (vizte bod 2.4.1 přílohy uvedeného nařízení). V oblasti poskytování kvalifikovaných služeb vytvářejících důvěru je zavedenou praxí, že kvalifikovaní poskytovatelé mají uzavřeno pojištění pro případ krytí způsobených škod.

Koncepce povinného pojištění byla zvolena tak, že výše pojistné částky musí být úměrná možným škodám, které lze v rozumné míře předpokládat. Výše pojistné částky by tak měla zohledňovat rozsah činnosti kvalifikovaného správce systému elektronické identifikace například v tom smyslu, kolik prostředků pro elektronickou identifikaci je vydáváno a používáno v rámci jím spravovaného kvalifikovaného systému elektronické identifikace. Důležitým hlediskem bude rovněž počet osob, kterým byl vydán prostředek pro elektronickou identifikaci, tj. počet držitelů prostředků pro elektronickou identifikaci vydaných v rámci kvalifikovaného systému elektronické identifikace příslušného kvalifikovaného správce systému elektronické identifikace.

Akreditovaná osoba je povinna nahradit škodu způsobenou při správě kvalifikovaného systému elektronické identifikace bez ohledu na sjednaný limit pojistného plnění. Účelem této úpravy je zabránit situacím, kdy by v důsledku nedostatečného pojištění odpovědnosti za škodu, nebyla akreditovaná osoba nucena nahradit škodu, kterou by sjednané pojištění nepokrylo. Akreditované osoby by tak vždy měly přihlídnout k rozsahu jimi vykonávané činnosti a pro tuto činnost se adekvátně pojistit.

Nařízení eIDAS v čl. 11 upravuje odpovědnost členského státu za škodu, kterou úmyslně nebo z nedbalosti způsobí kterékoliv fyzické nebo právnické osobě tím, že nezajistí dostupnost on-line autentizace pro osoby usazené na území jiného členského státu směřující k potvrzení osobních identifikačních údajů obdržných v elektronické podobě [čl. 7 písm. f) nařízení eIDAS], eventuálně tím, že nezajistí soulad osobních identifikačních údajů jednoznačně identifikujících danou osobu v rámci určitého systému s technickými specifikacemi, normami a postupy pro příslušnou úroveň záruky [čl. 7 písm. d) nařízení eIDAS]. Nařízení eIDAS stanovuje okruh odpovědných subjektů, pokud však jde o pravidla odpovědnosti za škodu, odkazuje v plném rozsahu na vnitrostátní pravidla odpovědnosti za škodu včetně pravidel týkajících se zejména vymezení škody, úmyslu, nedbalosti a souvisejících pravidel (čl. 11 ve spojení s bodem 18 recitálu nařízení eIDAS).

Odpovědnost členského státu za škodu způsobenou úmyslně i z nedbalosti fyzickým nebo právnickým osobám vzniká pouze v případě, že poruší povinnosti uvedené v čl. 11 odst. 1 nařízení eIDAS. Pokud oznámený systém elektronické identifikace přestane splňovat stanovené podmínky, členský stát musí takovou rozhodnou skutečnost bez zbytečného odkladu oznámit Komisi Evropské unie, která ji následně promítne do seznamu systémů elektronické identifikace v Úředním věstníku Evropské unie. Ve své podstatě se tak jedná o garanci přeshraničního fungování systému. Posouzení nepředvídatelnosti krátkodobého výpadku může podléhat individuálním okolnostem, přičemž je nezbytné vzít ohled zejména na plnění oznamovací povinnosti členského státu vůči Komisi Evropské unie a na další okolnosti, například zda k výpadku došlo zaviněním členského státu. V této pozici, kdy členský stát vystupuje jako garant určitého systému, odpovídá za škodu způsobenou nesplněním povinností podle čl. 7 písm. d) a f) nařízení eIDAS podle ustanovení o mimosmluvní odpovědnosti (§ 2910 občanského zákoníku).

K § 10

Bezúhonnost představuje primárně jednu z podmínek pro to, aby se z žadatele o akreditaci stala akreditovaná osoba, tedy kvalifikovaný správce systému elektronické identifikace nestátní povahy. Požadavek bezúhonnosti se však vztahuje rovněž na fyzické osoby, které vykonávají řídicí činnosti při správě kvalifikovaného systému elektronické identifikace, a fyzické osoby, které ověřují totožnost držitele prostředku pro elektronickou identifikaci (vizte § 16 odst. 3), tedy osoby vykonávající činnosti nejen pro kvalifikovaného správce systému elektronické identifikace nestátní povahy, ale také osoby vykonávající činnosti pro kvalifikovaného správce systému elektronické identifikace státní povahy. Lze mít za to, že osoba pravomocně odsouzená pro spáchání úmyslného trestného činu nebo trestného činu proti pořádku ve věcech veřejných z nedbalosti je náchylnější k opakování potenciálně riskantního jednání. Ve svém důsledku to znamená, že tato osoba není dostatečně způsobilá pro to, aby se stala kvalifikovaným správcem systému elektronické identifikace, neboť pro výkon činnosti kvalifikovaného správce systému elektronické identifikace se vyžaduje určitá míra serióznosti, případně tato osoba není způsobilá pro to, aby pro kvalifikovaného správce systému elektronické identifikace vykonávala některou z činností uvedenou v § 16 odst. 3.

Zákon o elektronické identifikaci se v případě úpravy trestných činů proti pořádku ve věcech veřejných z nedbalosti inspiroval zákonem č. 234/2014 Sb., o státní službě. Tato množina trestných činů byla zvolena z důvodu, že stejný požadavek, který v případě zákona č. 234/2014 Sb. směřuje vůči státním zaměstnancům, by měl být uplatněn vůči osobám, které vykonávají činnost pro kvalifikovaného správce systému elektronické identifikace, neboť kvalifikovanými správci systémů elektronické identifikace budou rovněž státní orgány.

Zákon o elektronické identifikaci upravuje jak bezúhonnost fyzických osob, tak bezúhonnost právnických osob (užitím neutrálního výrazu „osoba“). Zákon dále upravuje problematiku prokazování bezúhonnosti, a to rutinním způsobem obdobným jiným právním úpravám. Ministerstvo vnitra bude na základě výpisu z Rejstříku trestů posuzovat tuto záležitost věcně, a to v rámci probíhajícího správního řízení o udělení akreditace pro správu kvalifikovaného systému elektronické identifikace.

Způsoby prokazování bezúhonnosti osob se odvíjejí od skutečnosti, v jakém postavení se daná osoba nachází. Bude-li například fyzická osoba občanem České republiky s tím, že v minulosti pobývala na území státu déle než 3 měsíce ve 2 po sobě následujících letech,

bude předkládat jak výpis z evidence Rejstříku trestů (respektive tento výpis si vyžádá samo Ministerstvo vnitra), tak výpis z evidence trestů nebo rovnocenný doklad vydaný státem posledního pobytu, případně čestné prohlášení o bezúhonnosti.

K § 11 až 14

Volba osob pověřených k provádění atestací podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, jako subjektů, z jejichž okruhu se mohou etablovat osoby pověřené k posuzování systémů elektronické identifikace (zákon pro ně zavádí legislativní zkratku „pověřená osoba“), byla učiněna s ohledem na fakt, že systémy elektronické identifikace a informační systémy veřejné správy jsou budovány na základě obdobných principů.

Osoby pověřené k provádění atestací podle zákona č. 365/2000 Sb. musí splňovat přísné podmínky akreditace podle téhož zákona a jsou pod dohledem akreditující osoby, což je dostatečnou zárukou pro to, aby tyto subjekty posuzovaly prostředky pro elektronickou identifikaci a systémy elektronické identifikace, a to aniž by musela být ověřována odbornost těchto subjektů. Posuzováním prostředku pro elektronickou identifikaci a systému elektronické identifikace je tzv. pověřená osoba pověřena Ministerstvem vnitra na základě své žádosti.

Výkon kontroly nad plněním povinností pověřených osob vyplývajících z tohoto zákona je svěřen Ministerstvu vnitra. Při posuzování prostředku pro elektronickou identifikaci a systému elektronické identifikace se pověřené osoby budou řídit příslušnými ustanoveními prováděcího nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úroveň záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení eIDAS, a zákona č. 365/2000 Sb.

Pověření k posuzování prostředku pro elektronickou identifikaci a systému elektronické identifikace je nepřevoditelné.

Pro případ, že by se v rámci kontroly zjistily v činnosti pověřené osoby nedostatky, se zakládá pravomoc Ministerstva vnitra pověřením k posuzování prostředku pro elektronickou identifikaci a systému elektronické identifikace odejmout. Ministerstvo vnitra je povinno, dříve než o odejmutí rozhodne, pověřenou osobu na možnost odejmutí pověřením upozornit s uvedením důvodů, pro které by bylo možné v konkrétním případě pověřením odejmout, a zároveň pověřenou osobu vyzvat, aby bez zbytečného odkladu zjednala nápravu. Oprávněná osoba může nadto kdykoliv požádat Ministerstvo vnitra o odejmutí pověřením k posuzování prostředku pro elektronickou identifikaci a systému elektronické identifikace a Ministerstvo vnitra je povinno této žádosti vyhovět.

V případě kladného posouzení prostředku pro elektronickou identifikaci a systému elektronické identifikace vydá pověřená osoba ve lhůtě 3 měsíců potvrzení o souladu prostředku pro elektronickou identifikaci a systému elektronické identifikace s nařízením Komise (EU) 2015/1502. Pokud prostředek pro elektronickou identifikaci a systém elektronické identifikace nebude splňovat požadavky pro ně stanovené, pověřená osoba sdělí do 3 měsíců od podání žádosti žadateli důvody nesplnění požadavků.

Pokud by žádná z osob, které provádějí atestace podle zákona o informačních systémech veřejné správy, neměla zájem o posuzování prostředku pro elektronickou

identifikaci a systému elektronické identifikace, bude posuzování provádět samo Ministerstvo vnitra. Tato situace by však v reálu nastat neměla.

K § 15

Ustanovení upravuje základní požadavky na plán ukončení činnosti, který je jednou z podmínek pro udělení akreditace podle § 5. Plán ukončení činnosti ovšem zpracovává nejenom žadatel o akreditaci (potenciální kvalifikovaný správce systému elektronické identifikace nestátní povahy), ale i státní orgán coby kvalifikovaný správce systému elektronické identifikace státní povahy. Povinnosti kvalifikovaného správce systému elektronické identifikace, které jsou s plánem ukončení činnosti spojeny, jsou vymezeny v následujícím § 16 odst. 1 písm. k) a l).

K § 16

Navrhovaný § 16 upravuje povinnosti kvalifikovaného správce systému elektronické identifikace shodně pro všechny typy kvalifikovaných správců systémů elektronické identifikace, tedy jak pro státní orgány, tak pro kvalifikované správce systémů elektronické identifikace, kteří museli projít procesem akreditace, pro něž zákon zavádí legislativní zkratku „akreditovaná osoba“. Tyto základní povinnosti kvalifikovaných správců systémů elektronické identifikace jsou podmínkou pro věcně správný výkon jejich činnosti (tj. správy kvalifikovaného systému elektronické identifikace).

Povinnost zajistit dostupnost jím spravovaného kvalifikovaného systému elektronické identifikace pro spoléhající se stranu způsobem umožňujícím dálkový přístup prostřednictvím národního bodu pro identifikaci a autentizaci a pro národní bod pro identifikaci a autentizaci způsobem umožňujícím dálkový přístup je promítnutím povinnosti, kterou na oznámený systém elektronické identifikace klade nařízení eIDAS v čl. 7 písm. f).

Povinnost vést evidenci vydaných prostředků pro elektronickou identifikaci souvisí s požadavky kladenými na důvěryhodnost a bezpečnost činnosti kvalifikovaného správce systému elektronické identifikace a ochranu osobních údajů osob, kterým jsou vydávány prostředky pro elektronickou identifikaci.

Kvalifikovaný správce systému elektronické identifikace je dále povinen ztotožnit držitele prostředku pro elektronickou identifikaci před tím, než tento prostředek poprvé použije, vůči národnímu bodu pro identifikaci a autentizaci. Národní bod pro identifikaci a autentizaci (respektive Správa základních registrů) obdržené údaje o držiteli prostředku pro elektronickou identifikaci porovná s údaji vedenými o držiteli v základním registru obyvatel, a to na základě § 5 odst. 5 zákona č. 111/2009 Sb., o základních registrech, který fyzické osobě umožňuje poskytnout údaje, které jsou o ní vedeny v základních registrech, jiné fyzické nebo právnické osobě. Podmínkou tedy bude, aby držitel prostředku pro elektronickou identifikaci vyslovil s poskytnutím údajů souhlas.

Kvalifikovaný správce systému elektronické identifikace zapisuje identifikátor prostředku pro elektronickou identifikaci, který vydal, a rovněž úroveň záruky tohoto prostředku (nízká, značná, vysoká) do národního bodu pro identifikaci a autentizaci. V národním bodu pro identifikaci a autentizaci se tento údaj vedle podle § 21 odst. 1 písm. a).

Kvalifikovaný správce systému elektronické identifikace je povinen vést v evidenci vydaných prostředků pro elektronickou identifikaci aktuální údaje, a to na základě oznámení o změnách od správce národního bodu pro identifikaci a autentizaci. Správce národního bodu pro identifikaci a autentizaci získává informace o změnách údajů ze základních registrů.

Z důvodu zachování důkazů pro případné trestní či správní řízení je nezbytné, aby evidence vydaných prostředků pro elektronickou identifikaci, kterou vede kvalifikovaný správce systému elektronické identifikace, respektive údaje v ní obsažené byly dostupné i v případě, že kvalifikovaný správce systému elektronické identifikace ukončí svou činnost. Navrhuje se proto, aby v takovém případě kvalifikovaný správce systému elektronické identifikace předal tuto evidenci Ministerstvu vnitra. Údaje v ní však nebudou obecně veřejné, nýbrž budou zpřístupněny pouze tomu, kdo osvědčí právní zájem na jejich zpřístupnění (ten se předpokládá v případě orgánů veřejné moci), nebo stanoví-li to zákon.

Ke zneplatnění prostředku pro elektronickou identifikaci může kvalifikovaný správce systému elektronické identifikace přistoupit na základě žádosti držitele prostředku pro elektronickou identifikaci (z jakéhokoliv důvodu i bez udání důvodu), na základě oznámení držitele prostředku pro elektronickou identifikaci o zneužití nebo hrozcím nebezpečí zneužití prostředku pro elektronickou identifikaci nebo v případě, že se na základě notifikace od správce národního bodu pro identifikaci a autentizaci (či jiným prokazatelným způsobem) dozví, že držitel prostředku pro elektronickou identifikaci zemřel nebo byl prohlášen za mrtvého. Kvalifikovaný správce systému elektronické identifikace je rovněž povinen zneplatnit jím vydané prostředky pro elektronickou identifikaci tehdy, rozhodne-li se ukončit svou činnost.

S výše uvedenou povinností spočívající v zneplatnění prostředku pro elektronickou identifikaci souvisí také další povinnost kvalifikovaného správce systému elektronické identifikace, a to oznámit tuto skutečnost správci národního bodu pro identifikaci a autentizaci.

Kvalifikovaný správce systému elektronické identifikace je povinen vést a aktualizovat plán ukončení činnosti. Podle tohoto plánu ukončení činnosti je kvalifikovaný správce systému elektronické identifikace povinen postupovat, rozhodne-li se činnost kvalifikovaného správce systému elektronické identifikace ukončit.

Kvalifikovaný správce systému elektronické identifikace je konečně povinen zajistit, aby řídicí činnosti při správě kvalifikovaného systému elektronické identifikace byly vykonávány pouze pracovníky s určitými kvalifikačními předpoklady, kterými se v tomto případě rozumí absolvování odpovídajícího vzdělání a získání dostatečné praxe v oboru. Další podmínkou je, že fyzické osoby, které vykonávají řídicí činnosti při správě kvalifikovaného systému elektronické identifikace, a rovněž fyzické osoby, které ověřují totožnost držitele prostředku pro elektronickou identifikaci, musí být bezúhonné. Co se rozumí bezúhonností a jak se prokazuje, je stanoveno v § 10.

K § 17

S držením prostředku pro elektronickou identifikaci vznikají jeho držitelům určité povinnosti, jejichž primárním účelem je zabránit zneužití prostředku pro elektronickou identifikaci, jehož důsledkem by mohlo být zneužití tzv. zaručené elektronické identity.

První ze tří povinností spočívá v ověření správnosti údajů, které jsou zapisovány v prostředku pro elektronickou identifikaci. K tomuto ověření má dojít již při převzetí prostředku pro elektronickou identifikaci, čímž má být zamezeno pozdějším nesrovnalostem, které by mohly vyvstat například v důsledku chybně nahlášených identifikačních údajů.

Druhá povinnost klade důraz na řádné zacházení s prostředkem pro elektronickou identifikaci, pro které je typické jeho zabezpečení na veřejnosti. Tímto se má předejít případnému odcizení prostředku pro elektronickou identifikaci a jeho následnému zneužití.

Třetí povinnost navazuje na povinnost předešlou, neboť reaguje na situaci, kdy zneužití či hrozící nebezpečí zneužití prostředku pro elektronickou identifikaci již reálně nastane. Tuto skutečnost je držitel povinen bez zbytečného odkladu ohlásit kvalifikovanému správci systému elektronické identifikace, jehož povinností je v takové situaci prostředek pro elektronickou identifikaci zneplatnit, a to na základě povinnosti uložené mu § 16 odst. 1 písm. h).

K § 18

Ustanovení upravuje povinnosti toho, kdo umožňuje prokázání totožnosti, které vyžaduje právní předpis nebo výkon působnosti, s využitím elektronické identifikace, tedy „kvalifikovaného poskytovatele“. Zákon o elektronické identifikaci nevymezuje, kdo je považován za kvalifikovaného poskytovatele. Obecně jím může být subjekt či jiné právní uspořádání, tedy jak osoba fyzická nebo právnická, tak například organizační složka státu.

Prokázání totožnosti s využitím elektronické identifikace, se umožňuje v rámci on-line služby nebo jiné činnosti. On-line služba obecně je termínem užívaným nařízením eIDAS, byť jím nedefinovaným (skutečnost, že je nařízením eIDAS užívána, eliminuje možnost jejího definování vnitrostátním předpisem). Z nařízení eIDAS lze nicméně dovodit, že jde o jakoukoliv službu (veřejnoprávní či soukromoprávní), která je poskytována s využitím elektronických nástrojů (výpočetní techniky, internetu apod.).

Zákon o elektronické identifikaci neukládá žádným subjektům nebo jiným právním uspořádáním povinnost poskytovat on-line službu nebo jinou činnost, která umožní prokázání totožnosti s využitím elektronické identifikace. Poskytování on-line služby nebo jiné činnosti, která umožní prokázání totožnosti s využitím elektronické identifikace, je výsledkem rozhodnutí samotného subjektu nebo jiného právního uspořádání – samozřejmě za splnění dalších, především technických podmínek. Atributem on-line služby nebo jiné činnosti, která umožní prokázání totožnosti s využitím elektronické identifikace, je zajištění bezpečného a spolehlivého přihlášení s využitím zaručené elektronické identity. Úroveň bezpečnosti poskytované on-line služby nebo jiné činnosti stanovuje kvalifikovaný poskytovatel tím, že ve vyznění adresovaném správci národního bodu pro identifikaci a autentizaci uvede úroveň záruky prostředku pro elektronickou identifikaci, kterou při prokázání totožnosti s využitím elektronické identifikace požaduje. Přihlášení osoby k on-line službě nebo jiné činnosti v sobě nutně zahrnuje proces identifikace a autentizace této osoby. Tento proces však není v rukách kvalifikovaného poskytovatele, nýbrž je svěřen do portfolia kvalifikovaného správce systému elektronické identifikace a národního bodu pro identifikaci a autentizaci, na jehož služby musí být kvalifikovaný poskytovatel napojen.

Proces přihlášení se k on-line službě nebo jiné činnosti a využití on-line služby nebo jiné činnosti si lze představit následovně. Osoba si vybere on-line službu nebo jinou činnost,

kerou chce využít. Poskytovatel této služby automatizovaně přesměruje započatou komunikaci na národní bod pro identifikaci a autentizaci, přičemž musí být zřejmé, jakou úroveň záruky prostředku pro elektronickou identifikaci kvalifikovaný poskytovatel při prokázání totožnosti s využitím elektronické identifikace požaduje. Národní bod pro identifikaci a autentizaci osobě, která má v úmyslu službu využít, zobrazí prostředky pro elektronickou identifikaci, kterými se lze ke službě identifikovat (tyto musí odpovídat příslušné úrovni záruky, kterou požaduje kvalifikovaný poskytovatel). Osoba si vybere prostředek pro elektronickou identifikaci, který má k dispozici. Národní bod pro identifikaci a autentizaci pak komunikaci automatizovaně přesměruje ke kvalifikovanému správci systému elektronické identifikace, pod jehož kvalifikovaný systém elektronické identifikace příslušný prostředek pro elektronickou identifikaci spadá. Úkolem kvalifikovaného správce systému elektronické identifikace je identifikovat a rovněž autentizovat osobu, jejímž cílem je službu využít. V případě, že je tato osoba úspěšně identifikována a autentizována, pokračuje komunikace zpět k národnímu bodu pro identifikaci a autentizaci. Ten provede další ověření totožnosti osoby s využitím údajů ze základního registru obyvatel a následně doplní údaje ze svého datového fondu, které jsou pro poskytnutí služby nezbytné a které automatizovaně získá z relevantních informačních systémů veřejné správy. Kompletní údaje o osobě, která chce službu využít, po jejím odsouhlasení předá poskytovateli služby, tedy kvalifikovanému poskytovateli. Kvalifikovaný poskytovatel na základě obdržených údajů autorizuje identifikovanou a autentizovanou osobu a umožní jí práci se službou.

Kvalifikovaný poskytovatel představuje spoléhající se stranu ve smyslu čl. 3 odst. 6 nařízení eIDAS, neboť spoléhá na výsledek procesu autentizace vzešlý ze strany národního bodu pro identifikaci a autentizaci.

K § 19

K odstavci 1

Vymezuje se působnost Ministerstva vnitra na úseku elektronické identifikace.

V působnosti Ministerstva vnitra je v první řadě plnění úkolů podle čl. 9 a 10 nařízení eIDAS, mezi které patří zejména oznamování systémů elektronické identifikace, případně činění požadavků na vyškrtnutí systému elektronické identifikace, který oznámil.

Ministerstvo vnitra rovněž plní úkoly jednotného kontaktního místa. Dle prováděcího rozhodnutí Komise (EU) 2015/296 ze dne 24. února 2015, kterým se stanoví procesní opatření pro spolupráci mezi členskými státy v oblasti elektronické identifikace podle čl. 12 odst. 7 nařízení eIDAS, mají jednotná kontaktní místa sloužit k umožnění účinné spolupráce a zjednodušení správních postupů. Prostřednictvím jednotného kontaktního místa může členský stát kontaktovat příslušné orgány a subjekty jiného členského státu, pokud se jedná např. o výměnu informací, zkušeností a osvědčených postupů v oblasti elektronické identifikace či při žádosti o informace týkající se interoperability a bezpečnosti systémů elektronické identifikace. Informativní seznam jednotných kontaktních míst je uveden na stránkách

<https://ec.europa.eu/cefdigital/wiki/display/EIDCOOPNET/Points+of+single+contact>.

Dále jsou Ministerstvu vnitra uloženy funkce povahy především kontrolní a evidenční. V případě kontrolní funkce bude Ministerstvo vnitra postupovat v souladu se zákonem č. 255/2012 Sb., o kontrole (kontrolní řád). Jde-li o funkci evidenční, Ministerstvo vnitra vede evidenci udělených akreditací, kterou dle potřeby průběžně aktualizuje, přičemž tato evidence

je veřejně dostupná na internetových stránkách Ministerstva vnitra. Dále je Ministerstvu vnitra s ohledem na povinnost stanovenou kvalifikovanému správci systému elektronické identifikace § 16 odst. 1 písm. f), svěřeno uchovávání údajů vedených v evidenci vydaných prostředků pro elektronickou identifikaci kvalifikovaného správce systému elektronické identifikace, který ukončil svou činnost. Účelem této kompetence je zajištění důkazů o vydaných prostředcích pro elektronickou identifikaci pro případné soudní, trestní či správní řízení. Údaje z této evidence zpřístupní Ministerstvo vnitra tomu, kdo na jejich zpřístupnění osvědčí právní zájem, nebo stanoví-li to zákon.

K odstavci 2

Působnost Správy základních registrů na úseku elektronické identifikace se dotýká tří oblastí. V první řadě oblasti akreditace, která je upravena v § 5, kdy se Správa základních registrů na žádost Ministerstva vnitra vyjadřuje, zda systém elektronické identifikace žadatele o akreditaci umožňuje poskytnutí služby národního bodu pro identifikaci a autentizaci. Druhá kompetence Správy základních registrů má vztah ke kvalifikovaným poskytovatelům. Kvalifikovaní poskytovatelé Správu základních registrů vyrozumívají o poskytování on-line služby nebo jiné činnosti, při nichž se umožňuje prokázání totožnosti s využitím elektronické identifikace podle § 2. Na základě tohoto vyrozumění jim Správa základních registrů umožní poskytnutí služby národního bodu pro identifikaci a autentizaci (informační systémy kvalifikovaných poskytovatelů pochopitelně musí být kompatibilní s národním bodem pro identifikaci a autentizaci, kvalifikovaní poskytovatelé tak budou vázáni příslušnými částmi provozní dokumentace národního bodu pro identifikaci a autentizaci, zejména uživatelskou příručkou). Třetí kompetence Správy základních registrů spočívá v upozornění kvalifikovaného správce systému elektronické identifikace na změny údajů v evidenci vydaných prostředků pro elektronickou identifikaci. Povinností kvalifikovaného správce systému elektronické identifikace je totiž aktualizovat údaje v evidenci vydaných prostředků pro elektronickou identifikaci podle § 16 odst. 1 písm. e).

K § 20

K odstavcům 1 a 2

Národní bod pro identifikaci a autentizaci je stěžejním institutem zákona o elektronické identifikaci. Jedná se o informační systém veřejné správy, tudíž se na něj použije definice uvedená v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, podle které se informačním systémem veřejné správy rozumí funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy. Tak jako ostatní informační systémy veřejné správy zahrnuje i tento informační systém data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a dále nástroje umožňující výkon informačních činností.

Národní bod pro identifikaci a autentizaci je klíčovým nástrojem pro umožnění ověřování elektronické identity a předávání ověřených informací o uživateli potřebných pro využívání služeb poskytovaných na dálku. Národní bod pro identifikaci a autentizaci předává požadavek na ověření identity klienta obdrženy od kvalifikovaného poskytovatele klientem zvolenému kvalifikovanému správci systému elektronické identifikace. Tento na základě klientem předloženého prostředku pro elektronickou identifikaci provede identifikaci klienta, na kterou vzápětí navazuje autentizace prováděná dle vlastních pravidel kvalifikovaného správce systému elektronické identifikace. Výsledek identifikace je předán národnímu bodu pro identifikaci a autentizaci, který jej doplní o údaje ze základních registrů,

případně o údaje dobrovolně vedené u národního bodu pro identifikaci a autentizaci klientem. Národní bod pro identifikaci a autentizaci předá tento výsledek kvalifikovanému poskytovateli, který na něj spoléhá.

Správce národního bodu pro identifikaci a autentizaci je Správa základních registrů, která poskytuje služby národního bodu pro identifikaci a autentizaci a za národní bod pro identifikaci a autentizaci odpovídá.

Národní bod pro identifikaci a autentizaci představuje nástupce informačního systému pro autentizaci držitelů občanských průkazů upraveného v zákonu č. 328/1999 Sb., o občanských průkazech, který plnil tutéž úlohu, avšak toliko ve vztahu k jedinému prostředku pro elektronickou identifikaci, občanskému průkazu se strojově čitelnými údaji a s kontaktním elektronickým čipem. Z hlediska programového a technického vybavení je národní bod pro identifikaci a autentizaci původním informačním systémem pro autentizaci držitelů občanských průkazů, jehož funkcionality jsou upraveny tak, aby mohl plnit stejnou úlohu, avšak vůči více typům prostředků pro elektronickou identifikaci.

K odstavci 3

Uzel je definován prováděcím nařízením Komise (EU) 2015/1501 ze dne 8. září 2015 o rámci interoperability jako místo připojení, které je součástí architektury interoperability elektronické identifikace a je zapojeno do přeshraniční autentizace osob a které je schopno rozeznat a zpracovávat přenosy údajů nebo je předávat na jiné uzly tím, že umožňuje propojení vnitrostátní infrastruktury elektronické identifikace jednoho členského státu s vnitrostátními infrastrukturami elektronické identifikace ostatních členských států.

Koncepce, která je zvolena v zákoně o elektronické identifikaci, tedy že uzel je samostatnou součástí národního bodu pro identifikaci a autentizaci, je reakcí na čl. 6 odst. 2 uvedeného prováděcího aktu, v němž je stanoveno, že uzly neuchovávají žádné osobní údaje s výjimkou údajů v prováděcím aktu výslovně uvedených. S ohledem na tuto skutečnost je pojetí zákona o elektronické identifikaci takové, že uzel je samostatnou součástí národního bodu pro identifikaci a autentizaci, v níž nejsou uchovávány žádné osobní údaje.

K odstavci 4

Jedná se o požadavky vyplývající z čl. 5 až 10 nařízení Komise (EU) 2015/1501 ze dne 8. září 2015 o rámci interoperability.

K § 21

K odstavci 1

V národním bodu pro identifikaci a autentizaci budou vedeny především bezvýznamové identifikátory držitele prostředku pro elektronickou identifikaci a údaje týkající se tohoto prostředku.

K odstavci 2

V národním bodu pro identifikaci a autentizaci jsou vedeny také údaje provozního typu, a to za účelem dohledání historických transakcí s údaji vedenými v národním bodu pro identifikaci a autentizaci, jejichž potřeba náhledu by se mohla v budoucnu vyskytnout. V odstavci se stanoví minimální penzum provozních údajů, jejichž vedení je správce národního bodu pro identifikaci a autentizaci povinen zajistit. Vedení dalších provozních

údajů je na jeho úvaze, pochopitelně při respektování jiných právních předpisů, zejména právní úpravy ochrany osobních údajů.

K odstavci 3

Držitel prostředku pro elektronickou identifikaci je oprávněn na základě vlastního rozhodnutí poskytnout národnímu bodu pro identifikaci a autentizaci údaje, které se týkají jeho osoby. Zpravidla se bude jednat o údaje typu telefonní číslo pro veřejnou mobilní telefonní síť či adresu elektronické pošty. Tyto údaje zapíše do národního bodu pro identifikaci a autentizaci samotný držitel, a to prostřednictvím příslušného přístupového rozhraní.

K odstavci 4

V odstavci jsou vymezeny subjekty (správce národního bodu pro identifikaci a autentizaci a držitel prostředku pro elektronickou identifikaci), kterým přísluší do národního bodu pro identifikaci a autentizaci zapisovat určitý druh údajů (být editory údajů).

K odstavci 5 a 6

V odstavci 5 se stanoví doba uchovávání údajů vedených v národním bodu pro identifikaci a autentizaci. Doba 15 let vychází z úpravy obsažené v zákoně o občanských průkazech, neboť stěžejním prostředkem pro elektronickou identifikaci bude právě občanský průkaz se strojově čitelnými údaji a s kontaktním elektronickým čipem.

V odstavci 6 se stanoví doba uchovávání údajů vedených v uzlu podle čl. 9 odst. 3 prováděcího nařízení Komise (EU) 2015/1501 ze dne 8. září 2015. Údaje vedené v uzlu se uchovávají po dobu 15 let od jejich prvotního zápisu.

K § 22

Vedení evidence vydaných prostředků pro elektronickou identifikaci je povinností každého kvalifikovaného správce systému elektronické identifikace. Tato povinnost vyplývá z navrhovaného § 16 odst. 1 písm. b).

Z důvodu zajištění právní jistoty správy kvalifikovaného systému elektronické identifikace musí být vedena důvěryhodná evidence, která bude obsahovat dostatečné informace o vydaných prostředcích pro elektronickou identifikaci tak, aby bylo možné pro případné soudní, trestní a správní řízení poskytnout pro tyto účely dostatek věrohodných informací. Evidence není veřejná, což však nebrání orgánům veřejné moci nadaným příslušnou pravomocí k přístupu k jejímu obsahu (orgánům činným v trestním řízení pro potřeby trestního řízení, Ministerstvu vnitra při kontrole podle tohoto zákona apod.).

Evidence musí obsahovat nejen informace o osobě, které byl prostředek pro elektronickou identifikaci vydán, ale rovněž technické informace vztahující se k prostředku pro elektronickou identifikaci.

Při stanovení lhůty 15 let pro uchovávání údajů v evidenci vydaných prostředků pro elektronickou identifikaci předkladatel vycházel z obecné zásady nařízení eIDAS, podle které by se na poskytovatele služeb elektronické identifikace měla vztahovat obdobná pravidla jako pravidla stanovená pro poskytovatele služeb vytvářejících důvěru. Předkladatel tedy vychází zejména z čl. 5 nařízení eIDAS a § 3 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. Lhůta uchovávání údajů 15 let odpovídá

potřebám poskytnutí důkazů v trestním a správním řízení a zajištění kontinuity služby. Obdobná lhůta (20 let) byla taktéž stanovena ve zrušeném zákoně o elektronickém podpisu.

K § 23

K odstavci 1

Pro potřeby všeobecného přehledu o kvalifikovaných správcích systémů elektronické identifikace a kvalifikovaných poskytovatelích usazených v České republice o těchto subjektech a jimi poskytovaných službách povede Správa základních registrů seznam. V případě služeb kvalifikovaných správců systémů elektronické identifikace se jedná o používané prostředky pro elektronickou identifikaci, v případě služeb kvalifikovaných poskytovatelů o poskytované on-line služby nebo jiné činnosti. Na rozdíl od evidence vydaných prostředků pro elektronickou identifikaci (vizte § 22), která se vztahuje vždy ke konkrétnímu kvalifikovanému správci systému elektronické identifikace a jím vydávaným prostředkům pro elektronickou identifikaci, je tento seznam komplexním přehledem prostředků pro elektronickou identifikaci používaných na území České republiky. Seznam kvalifikovaných správců systémů elektronické identifikace a kvalifikovaných poskytovatelů bude Správou základních registrů průběžně aktualizován, ať už v pozitivním smyslu, například v podobě rozšíření o nové kvalifikované správce systémů elektronické identifikace či nové kvalifikované poskytovatele, či ve smyslu negativním, kdy bude stávající seznam kvalifikovaných správců systémů elektronické identifikace a kvalifikovaných poskytovatelů zúžen, například v důsledku ukončení činnosti některého z nich.

K odstavci 2

Seznam kvalifikovaných správců systémů elektronické identifikace a kvalifikovaných poskytovatelů bude k dispozici na internetových stránkách Správy základních registrů. Tato forma uveřejnění garantuje jednoduché a bezproblémové vyhledání kvalifikovaných správců systémů elektronické identifikace a kvalifikovaných poskytovatelů působících na území České republiky a jimi poskytovaných služeb v podobě používaných prostředků pro elektronickou identifikaci a poskytovaných on-line služeb nebo jiných činností. Přístup k seznamu kvalifikovaných správců systémů elektronické identifikace a kvalifikovaných poskytovatelů není ničím podmíněn, tudíž je přístupný široké veřejnosti.

K § 24

Údaje, které Správa základních registrů využívá při výkonu působnosti na úseku elektronické identifikace, musí být získány z důvěryhodných zdrojů, u kterých je zaručena jejich pravost a aktuálnost. Z tohoto důvodu by měl být primárním zdrojem těchto informací základní registr obyvatel, informační systém evidence obyvatel, informační systém cizinců a základní registr agend, orgánů veřejné moci, soukromoprávních uživatelů údajů a některých práv a povinností. Správa základních registrů bude moci údaje z uvedených informačních systémů veřejné správy využívat pro veškerou působnost založenou jí zákonem o elektronické identifikaci.

K § 25

Zákon o elektronické identifikaci obsahuje výčet přestupků, kterých se dopustí akreditovaná osoba, jestliže poruší některou z povinností vyplývajících pro ni z § 16.

Výše pokut byla stanovena na základě potenciálně způsobené škody. Navrhované výše pokut je možné považovat za přiměřeně přísné a odrazující. Většinu spáchaných přestupků bude možné postihnout až do výše 2 milionů Kč, což lze považovat vzhledem k závažnosti jednání za dostatečné. Při konkrétním stanovení výše pokuty bude správní orgán samozřejmě přihlížet k majetkovým a osobním poměrům delikventa. Pro delikventa, kvalifikovaného správce systému elektronické identifikace nestátní povahy, bude přiměřená maximální sankce ve výši 2 miliony Kč, neboť tato pokuta jistě zasáhne do jeho majetkové sféry, ale zároveň pro jeho podnikání nebude mít likvidační charakter.

K § 26

Uvedené ustanovení vymezuje kompetenci Ministerstva vnitra projednávat přestupky spáchané na úseku elektronické identifikace.

K § 27

K odstavci 1

Subjekty, které umožňovaly prokázání totožnosti, které vyžaduje právní předpis nebo výkon působnosti, s využitím elektronické identifikace již před nabytím účinnosti zákona o elektronické identifikaci, přičemž uvedené prokázání totožnosti umožňují i po nabytí účinnosti tohoto zákona, jsou povinny vyrozumět o této skutečnosti správce národního bodu pro identifikaci a autentizaci do 6 měsíců ode dne nabytí účinnosti tohoto zákona. Na základě tohoto vyrozumění bude těmto subjektům umožněno využívat služeb národního bodu pro identifikaci a autentizaci pro účely jejich on-line služby nebo jiné činnosti a současně relevantní správní úřady i veřejnost nabudou povědomí i o těchto kvalifikovaných poskytovatelích.

K odstavci 2

Důvodem pro stanovení 2letého přechodného období je skutečnost, že v současné době již existují potenciální kvalifikovaní správci systémů elektronické identifikace, kteří disponují vlastním systémem elektronické identifikace a jimi používanými prostředky pro elektronickou identifikaci, které však nelze označit za kvalifikovaný systém elektronické identifikace ve smyslu § 3. Přizpůsobení se kvalifikovanému systému elektronické identifikace proto vyžaduje určité časové období. Těmto subjektům je tak ze zákona poskytnuto 2leté období, v němž mohou nadále používat vlastní systém i prostředky. Předpokládá se však, že do 2 let ode dne nabytí účinnosti zákona o elektronické identifikaci přejdou na kvalifikovaný systém elektronické identifikace a budou využívat služeb národního bodu pro identifikaci a autentizaci.

K § 28

Nabytí účinnosti zákona o elektronické identifikaci se navrhuje dnem 1. července 2018. Účinnost zákona tak bude předcházet účinnosti ustanovení nařízení eIDAS upravujících problematiku elektronické identifikace (účinná od 28. září 2018), což vytvoří prostor pro právní vznik vnitrostátních kvalifikovaných systémů elektronické identifikace a ověření funkčnosti národního bodu pro identifikaci a autentizaci. Navrhovaná účinnost by měla rovněž korespondovat s účinností novely zákona č. 328/1999 Sb., o občanských průkazech, (sněmovní tisk 928), která zavádí tzv. „elektronický občanský průkaz s čipem“ coby jediný typ občanského průkazu pro všechny občany. Občanský průkaz se strojově čitelnými údaji

a s kontaktním elektronickým čipem by měl představovat jeden ze stěžejních prostředků pro elektronickou identifikaci.

V Praze dne 8. března 2017

Předseda vlády:
Mgr. Bohuslav Sobotka v.r.

Ministr vnitra:
v zastoupení
Ministryně práce a sociálních věcí:
Mgr. Michaela Marksová v.r.