VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2015/1502

z 8. septembra 2015,

ktorým sa stanovujú minimálne technické špecifikácie a postupy pre úrovne zabezpečenia prostriedkov elektronickej identifikácie podľa článku 8 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES ([1]), a najmä na jeho článok 8 ods. 3,

keďže:

(1) V článku 8 nariadenia (EÚ) č. 910/2014 sa stanovuje, že schéma elektronickej identifikácie oznámená podľa článku 9 ods. 1 musí obsahovať špecifikácie úrovní zabezpečenia „nízka“, „pokročilá“ a „vysoká“ pre prostriedky elektronickej identifikácie vydávané v rámci danej schémy.

(2) Určenie minimálnych technických špecifikácií, noriem a postupov je nevyhnutné na zaistenie jednotného chápania podrobných vlastností úrovní zabezpečenia a na zaistenie interoperability pri mapovaní vnútroštátnych úrovní zabezpečenia oznámených schém elektronickej identifikácie na úrovne zabezpečenia podľa článku 8, ako sa uvádza v článku 12 ods. 4 písm. b) nariadenia (EÚ) č. 910/2014.

(3) Pri príprave špecifikácií a postupov stanovených v tomto vykonávacom akte bola ako zásadná medzinárodná norma v oblasti úrovní zabezpečenia prostriedkov elektronickej identifikácie zohľadnená medzinárodná norma ISO/IEC 29115. Obsah nariadenia (EÚ) č. 910/2014 sa však od tejto medzinárodnej normy líši, a to najmä pokiaľ ide o požiadavky na preukazovanie a overovanie totožnosti, ako aj o spôsob, akým sa zohľadňujú rozdiely medzi dojednaniami v oblasti totožnosti v jednotlivých členských štátoch a existujúcimi nástrojmi na rovnaký účel v EÚ. Preto by sa v prílohe nemalo odkazovať na konkrétny obsah normy ISO/IEC 29115, hoci z tejto medzinárodnej normy vychádza.

(4) Toto nariadenie bolo vypracované na základe prístupu založeného na výsledkoch, keďže bol najvhodnejší, čo sa odráža aj vo vymedzeniach použitých na špecifikovanie termínov a pojmov. Berie sa v nich do úvahy cieľ nariadenia (EÚ) č. 910/2014 v súvislosti s úrovňami zabezpečenia prostriedkov elektronickej identifikácie. Preto by sa pri stanovovaní špecifikácií a postupov stanovených v tomto vykonávacom akte mal v najvyššej možnej miere zohľadniť rozsiahly pilotný projekt STORK vrátane špecifikácií, ktoré boli v jeho rámci vyvinuté, ako aj vymedzenia a pojmy uvedené v norme ISO/IEC 29115.

(5) Spoľahlivé zdroje môžu mať v závislosti od kontextu, v ktorom treba overiť nejaký aspekt dôkazu totožnosti, mnoho podôb, ako sú okrem iného registre, doklady a orgány. V rôznych členských štátoch sa môžu spoľahlivé zdroje líšiť, a to dokonca v podobnom kontexte.

(6) V požiadavkách na preukazovanie a overovanie totožnosti by sa mali zohľadňovať rozdielne systémy a postupy a zároveň zaistiť dostatočne vysoký stupeň zabezpečenia s cieľom vytvoriť potrebnú dôveru. Preto by sa akceptovanie postupov, ktoré sa predtým používali na iné účely, než je vydávanie prostriedkov elektronickej identifikácie, malo podmieniť potvrdením toho, že tieto postupy spĺňajú požiadavky stanovené pre príslušnú úroveň zabezpečenia.

([1]) Ú. v. EÚ L 257, 28.8.2014, s. 73.

(7) Obvykle sa využívajú určité faktory autentifikácie, ako napríklad spoločné tajomstvá, fyzické zariadenia a fyzické vlastnosti. Na zvýšenie bezpečnosti procesu autentifikácie by sa však malo podnecovať používanie väčšieho počtu faktorov autentifikácie, a najmä z rôznych kategórií faktorov.

(8) Toto nariadenie by nemalo mať vplyv na práva právnických osôb na zastúpenie. V prílohe by sa však mali stanovovať požiadavky na prepojenie medzi prostriedkami elektronickej identifikácie fyzických a právnických osôb.

(9) Mal by sa uznať význam systémov riadenia informačnej bezpečnosti a služieb, ako aj význam používania uznávaných metodík a uplatňovania zásad zakotvených v normách, ako sú normy súboru ISO/IEC 27000 a súboru ISO/IEC 20000.

(10) Do úvahy by sa mali brať aj osvedčené postupy týkajúce sa úrovní zabezpečenia v jednotlivých členských štátoch.

(11) Dôležitým nástrojom na overovanie súladu produktov s bezpečnostnými požiadavkami tohto vykonávacieho aktu je bezpečnostná certifikácia IT založená na medzinárodných normách.

(12) Výbor uvedený v článku 48 nariadenia (EÚ) č. 910/2014 nevydal stanovisko v termíne stanovenom jeho predsedom,

PRIJALA TOTO NARIADENIE:

Článok 1

1. Úrovne zabezpečenia „nízka“, „pokročilá“ a „vysoká“ pre prostriedky elektronickej identifikácie vydané v rámci oznámenej schémy elektronickej identifikácie sa určujú vzhľadom na špecifikácie a postupy stanovené v prílohe.

2. Na špecifikovanie úrovne zabezpečenia prostriedkov elektronickej identifikácie vydaných v rámci oznámenej schémy elektronickej identifikácie sa použijú špecifikácie a postupy stanovené v prílohe tak, že sa určí spoľahlivosť a kvalita týchto prvkov:

a) prihlásenie, ako sa stanovuje v oddiele 2.1 prílohy k tomuto nariadeniu podľa článku 8 ods. 3 písm. a) nariadenia (EÚ) č. 910/2014;

b) riadenie prostriedkov elektronickej identifikácie, ako sa stanovuje v oddiele 2.2 prílohy k tomuto nariadeniu podľa článku 8 ods. 3 písm. b) a f) nariadenia (EÚ) č. 910/2014;

c) autentifikácia, ako sa stanovuje v oddiele 2.3 prílohy k tomuto nariadeniu podľa článku 8 ods. 3 písm. c) nariadenia (EÚ) č. 910/2014;

d) riadenie a organizácia, ako sa stanovuje v oddiele 2.4 prílohy k tomuto nariadeniu podľa článku 8 ods. 3 písm. d) a e) nariadenia (EÚ) č. 910/2014.

3. Ak prostriedky elektronickej identifikácie vydané v rámci oznámenej schémy elektronickej identifikácie spĺňajú nejakú požiadavku uvedenú pre vyššiu úroveň zabezpečenia, potom sa predpokladá, že spĺňajú aj zodpovedajúcu požiadavku nižšej úrovne zabezpečenia.

4. Pokiaľ nie je v príslušnej časti prílohy uvedené inak, musia byť na dosiahnutie údajnej úrovne zabezpečenia splnené všetky prvky uvedené v prílohe pre konkrétnu úroveň zabezpečenia prostriedkov elektronickej identifikácie vydaných v rámci oznámenej schémy elektronickej identifikácie.

Článok 2

Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 8. septembra 2015

Za Komisiu

predseda

Jean-Claude JUNCKER

PRÍLOHA

Technické špecifikácie a postupy pre úrovne zabezpečenia „nízka“, „pokročilá“ a „vysoká“ pre prostriedky elektronickej identifikácie vydané v rámci oznámenej schémy elektronickej identifikácie

1. Platné vymedzenie pojmov

Na účely tejto prílohy sa uplatňuje toto vymedzenie pojmov:

1. „spoľahlivý zdroj“ je akýkoľvek zdroj bez ohľadu na svoju podobu, pri ktorom sa dá spoľahnúť na to, že poskytuje presné údaje, informácie a/alebo dôkazy, ktoré sa môžu použiť na preukázanie totožnosti;

2. „faktor autentifikácie“ je faktor, pri ktorom sa potvrdilo, že je spojený s osobou, a ktorý patrí do niektorej z týchto kategórií:

   a) „faktor autentifikácie na základe držby“ je faktor autentifikácie, ktorého držbu je osoba povinná preukázať;

   b) „faktor autentifikácie na základe poznania“ je faktor autentifikácie, ktorého poznanie je osoba povinná preukázať;

   c) „inherentný faktor autentifikácie“ je faktor autentifikácie, ktorý je založený na fyzickej vlastnosti fyzickej osoby, pričom osoba je povinná preukázať, že má túto fyzickú vlastnosť;

3. „dynamická autentifikácia“ je elektronický proces využívajúci kryptografiu alebo iné techniky na poskytnutie prostriedkov, ktoré na požiadanie vytvoria elektronický dôkaz o tom, že osoba má kontrolu nad identifikačnými údajmi alebo ich má v držbe, pričom tento proces sa pri každej autentifikácii medzi osobou a systémom, ktorý overuje jej totožnosť, mení;

4. „systém riadenia informačnej bezpečnosti“ je súbor procesov a postupov určených na zmiernenie rizík súvisiacich s informačnou bezpečnosťou na prijateľné úrovne.

2. Technické špecifikácie a postupy

Prvky technických špecifikácií a postupov uvedené v tejto prílohe sa používajú na stanovenie spôsobu, akým sa požiadavky a kritériá uvedené v článku 8 nariadenia (EÚ) č. 910/2014 uplatňujú na prostriedky elektronickej identifikácie vydané v rámci schémy elektronickej identifikácie.

2.1. *Registrácia*

2.1.1. Žiadosť a prihlásenie

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Zabezpečenie toho, aby žiadateľ poznal podmienky týkajúce sa používania prostriedkov elektronickej identifikácie. 2. Zabezpečenie toho, aby žiadateľ poznal odporúčané bezpečnostné opatrenia týkajúce sa prostriedkov elektronickej identifikácie. 3. Zhromaždenie relevantných údajov o totožnosti požadovaných na preukázanie a overenie totožnosti.
Pokročilá	Rovnaké ako pri úrovni „nízka“.
Vysoká	Rovnaké ako pri úrovni „nízka“.

2.1.2. Preukazovanie a overovanie totožnosti (fyzická osoba)

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Možno predpokladať, že daná osoba má v držbe dôkaz označujúci údajnú totožnosť, uznaný členským štátom, v ktorom sa žiadosť o prostriedok elektronickej identifikácie podáva. 2. Možno predpokladať, že dôkaz je pravý alebo že podľa spoľahlivého zdroja existuje, a podľa všetkého je platný. 3. Spoľahlivému zdroju je známe, že údajná totožnosť existuje, a možno predpokladať, že osoba hlásiaca sa k nejakej totožnosti, je jedna a tá istá.
Pokročilá	Úroveň „nízka“ a zároveň musí byť splnená jedna z alternatív uvedených v bodoch 1 až 4: 1. Bolo overené, že osoba má v držbe dôkaz označujúci údajnú totožnosť, uznaný členským štátom, v ktorom sa žiadosť o prostriedok elektronickej identifikácie podáva, a dôkaz je skontrolovaný, aby sa zistilo, či je pravý, alebo je podľa spoľahlivého zdroja známe, že existuje a viaže sa na skutočnú osobu, a boli podniknuté kroky na minimalizáciu rizika, že totožnosť danej osoby nie je údajná totožnosť, pričom sa bralo do úvahy napríklad riziko, že dôkaz sa stratil, bol odcudzený, jeho platnosť bola pozastavená alebo zrušená alebo uplynula, alebo 2. sa predloží doklad totožnosti počas procesu registrácie v členskom štáte, v ktorom sa doklad vydal, a tento doklad sa zjavne viaže na osobu, ktorá ho predkladá, a podnikli sa kroky na minimalizáciu rizika, že totožnosť danej osoby nie je údajná totožnosť, pričom sa bralo do úvahy napríklad riziko, že doklady sa stratili, boli odcudzené, bola pozastavená alebo zrušená ich platnosť alebo ich platnosť uplynula, alebo 3. ak postupy, ktoré v minulosti použil verejný alebo súkromný subjekt v tom istom členskom štáte na iné účely, než je vydanie prostriedku elektronickej identifikácie, poskytujú zabezpečenie rovnocenné s postupmi stanovenými v oddiele 2.1.2 pre úroveň zabezpečenia „pokročilá“, potom subjekt zodpovedný za registráciu nemusí opakovať už tieto použité postupy za predpokladu, že takéto rovnocenné zabezpečenie potvrdí orgán posudzovania zhody uvedený v článku 2 bode 13 nariadenia Európskeho parlamentu a Rady (ES) č. 765/2008 ([1]) alebo rovnocenný orgán, alebo 4. ak sa prostriedky elektronickej identifikácie vydávajú na základe platného oznámeného prostriedku elektronickej identifikácie s úrovňou zabezpečenia „pokročilá“ alebo „vysoká“, pričom sa berú do úvahy riziká zmeny osobných identifikačných údajov, nie je potrebné opakovať procesy preukazovania a overovania totožnosti. Ak prostriedok elektronickej identifikácie slúžiaci ako základ nebol oznámený, musí úroveň zabezpečenia „pokročilá“ alebo „vysoká“ potvrdiť orgán posudzovania zhody uvedený v článku 2 bode 13 nariadenia (ES) č. 765/2008 alebo rovnocenný orgán.

Úroveň zabezpečenia	Potrebné prvky
Vysoká	Musia byť splnené požiadavky uvedené v bode 1 alebo v bode 2: 1. Úroveň „pokročilá“ a zároveň musí byť splnená jedna z alternatív uvedených v písmenách a) až c): a) Ak bolo overené, že daná osoba má v držbe fotografický alebo biometrický identifikačný dôkaz uznaný členským štátom, v ktorom sa žiadosť o prostriedok elektronickej identifikácie podáva, a tento dôkaz označuje údajnú totožnosť, dôkaz je skontrolovaný, aby sa zistilo, či je podľa spoľahlivého zdroja platný, a prostredníctvom porovnania jednej alebo viacerých fyzických vlastností danej osoby so spoľahlivým zdrojom sa identifikuje, že žiadateľ má údajnú totožnosť, alebo b) ak postupy, ktoré v minulosti použil verejný alebo súkromný subjekt v tom istom členskom štáte na iné účely, než je vydanie prostriedku elektronickej identifikácie, poskytujú zabezpečenie rovnocenné s postupmi uvedenými v oddiele 2.1.2 pre úroveň zabezpečenia „vysoká“, potom subjekt zodpovedný za registráciu nemusí opakovať tieto predchádzajúce postupy za predpokladu, že je takéto rovnocenné zabezpečenie potvrdené orgánom posudzovania zhody uvedeným v článku 2 bode 13 nariadenia (ES) č. 765/2008 alebo rovnocenným orgánom, a sú prijaté kroky na preukázanie toho, že výsledky predchádzajúcich postupov sú naďalej platné, alebo c) ak sa prostriedky elektronickej identifikácie vydávajú na základe platných oznámených prostriedkov elektronickej identifikácie s úrovňou zabezpečenia „vysoká“, pričom sa berú do úvahy riziká zmeny osobných identifikačných údajov, nie je potrebné opakovať procesy preukazovania a overovania totožnosti. Ak prostriedok elektronickej identifikácie slúžiaci ako základ nebol oznámený, musí úroveň zabezpečenia „vysoká“ potvrdiť orgán posudzovania zhody uvedený v článku 2 bode 13 nariadenia (ES) č. 765/2008 alebo rovnocenný orgán, a sú prijaté kroky na preukázanie toho, že výsledky predchádzajúceho postupu vydávania oznámených prostriedkov elektronickej identifikácie naďalej platia, alebo 2. ak žiadateľ nepredloží žiadny uznaný fotografický alebo biometrický identifikačný dôkaz, uplatnia sa rovnaké postupy, aké sa na získanie takéhoto uznaného fotografického alebo biometrického identifikačného dôkazu používajú na vnútroštátnej úrovni v členskom štáte subjektu zodpovedného za registráciu.

([1]) Nariadenie Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93 (Ú. v. EÚ L 218, 13.8.2008, s. 30).

2.1.3. Preukazovanie a overovanie totožnosti (právnická osoba)

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Údajná totožnosť právnickej osoby je preukázaná na základe dôkazu uznaného členským štátom, v ktorom sa žiadosť o prostriedok elektronickej identifikácie podáva.

Úroveň zabezpečenia	Potrebné prvky
	2. Dôkaz je podľa všetkého platný a možno predpokladať, že je pravý alebo že podľa spoľahlivého zdroja existuje, ak je zahrnutie právnickej osoby do spoľahlivého zdroja dobrovoľné a upravuje ho dohoda medzi právnickou osobou a spoľahlivým zdrojom. 3. Spoľahlivému zdroju nie je známe, že by právnická osoba mala postavenie, ktoré by jej bránilo konať ako daná právnická osoba.
Pokročilá	Úroveň „nízka“ a zároveň musí byť splnená jedna z alternatív uvedených v bodoch 1 až 3: 1. Údajná totožnosť právnickej osoby je preukázaná na základe dôkazu uznaného členským štátom, v ktorom sa žiadosť o prostriedok elektronickej identifikácie podáva, a to vrátane názvu, právnej formy a (prípadne) registračného čísla právnickej osoby, a dôkaz je skontrolovaný, aby sa zistilo, či je pravý, alebo či je podľa spoľahlivého zdroja známe, že existuje, ak sa pre pôsobenie právnickej osoby v jej odvetví vyžaduje, aby bola zahrnutá do spoľahlivého zdroja, a boli podniknuté kroky na minimalizáciu rizika, že totožnosť právnickej osoby nie je údajná totožnosť, pričom sa bralo do úvahy napríklad riziko, že doklady sa stratili, boli odcudzené, bola pozastavená alebo zrušená ich platnosť alebo ich platnosť uplynula, alebo 2. ak postupy, ktoré v minulosti použil verejný alebo súkromný subjekt v tom istom členskom štáte na iné účely, než je vydanie prostriedku elektronickej identifikácie, poskytujú zabezpečenie rovnocenné s postupmi uvedenými v oddiele 2.1.3 pre úroveň zabezpečenia „pokročilá“, potom subjekt zodpovedný za registráciu nemusí opakovať tieto predchádzajúce postupy za predpokladu, že je takéto rovnocenné zabezpečenie potvrdené orgánom posudzovania zhody uvedeným v článku 2 bode 13 nariadenia (ES) č. 765/2008 alebo rovnocenným orgánom, alebo 3. ak sa prostriedky elektronickej identifikácie vydávajú na základe platných oznámených prostriedkov elektronickej identifikácie s úrovňou zabezpečenia „pokročilá“ alebo „vysoká“, nie je potrebné opakovať procesy preukazovania a overovania totožnosti. Ak prostriedok elektronickej identifikácie slúžiaci ako základ nebol oznámený, musí úroveň zabezpečenia „pokročilá“ alebo „vysoká“ potvrdiť orgán posudzovania zhody uvedený v článku 2 bode 13 nariadenia (ES) č. 765/2008 alebo rovnocenný orgán.
Vysoká	Úroveň „pokročilá“ a zároveň musí byť splnená jedna z alternatív uvedených v bodoch 1 až 3: 1. Údajná totožnosť právnickej osoby je preukázaná na základe dôkazu uznaného členským štátom, v ktorom sa žiadosť o prostriedok elektronickej identifikácie podáva, a to vrátane názvu právnickej osoby, jej právnej formy a najmenej jedného jedinečného identifikátora používaného na vnútroštátnej úrovni a označujúceho danú právnickú osobu, a dôkaz je skontrolovaný, aby sa zistilo, či je podľa spoľahlivého zdroja platný, alebo

Úroveň zabezpečenia	Potrebné prvky
	2. ak postupy, ktoré v minulosti použil verejný alebo súkromný subjekt v tom istom členskom štáte na iné účely, než je vydanie prostriedku elektronickej identifikácie, poskytujú zabezpečenie rovnocenné s postupmi uvedenými v oddiele 2.1.3 pre úroveň zabezpečenia „vysoká“, potom subjekt zodpovedný za registráciu nemusí opakovať tieto predchádzajúce postupy za predpokladu, že je takéto rovnocenné zabezpečenie potvrdené orgánom posudzovania zhody uvedeným v článku 2 bode 13 nariadenia (ES) č. 765/2008 alebo rovnocenným orgánom, a sú prijaté kroky na preukázanie toho, že výsledky tohto predchádzajúceho postupu sú naďalej platné, alebo 3. ak sa prostriedky elektronickej identifikácie vydávajú na základe platných oznámených prostriedkov elektronickej identifikácie s úrovňou zabezpečenia „vysoká“, nie je potrebné opakovať procesy preukazovania a overovania totožnosti. Ak prostriedok elektronickej identifikácie slúžiaci ako základ nebol oznámený, musí úroveň zabezpečenia „vysoká“ potvrdiť orgán posudzovania zhody uvedený v článku 2 bode 13 nariadenia (ES) č. 765/2008 alebo rovnocenný orgán, a sú prijaté kroky na preukázanie toho, že výsledky predchádzajúceho postupu vydávania oznámených prostriedkov elektronickej identifikácie naďalej platia.

2.1.4. Prepojenie medzi prostriedkami elektronickej identifikácie fyzických a právnických osôb

V príslušných prípadoch platia pre prepojenie medzi prostriedkom elektronickej identifikácie fyzickej osoby a prostriedkom elektronickej identifikácie právnickej osoby (ďalej len „prepojenie“) tieto podmienky:

1. Musí byť možné pozastaviť a/alebo zrušiť prepojenie. Životný cyklus prepojenia (napr. aktivácia, pozastavenie, obnovenie, zrušenie) sa spravuje podľa postupov uznaných na vnútroštátnej úrovni.

2. Fyzická osoba, ktorej prostriedok elektronickej identifikácie je prepojený s prostriedkom elektronickej identifikácie právnickej osoby, môže poveriť uplatňovaním tohto prepojenia inú fyzickú osobu na základe postupov uznaných na vnútroštátnej úrovni. Zodpovednosť však naďalej nesie poverujúca fyzická osoba.

3. Prepojenie sa realizuje takto:

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Je overené, že preukázanie totožnosti fyzickej osoby konajúcej v mene právnickej osoby bolo vykonané na úrovni „nízka“ alebo na vyššej úrovni. 2. Prepojenie bolo vytvorené na základe postupov uznaných na vnútroštátnej úrovni. 3. Spoľahlivému zdroju nie je známe, že by fyzická osoba mala postavenie, ktoré by jej bránilo konať v mene danej právnickej osoby.
Pokročilá	Bod 3 úrovne „nízka“ a zároveň: 1. Je overené, že preukázanie totožnosti fyzickej osoby konajúcej v mene právnickej osoby bolo vykonané na úrovni „pokročilá“ alebo „vysoká“.

Úroveň zabezpečenia	Potrebné prvky
	2. Prepojenie bolo vytvorené na základe postupov uznaných na vnútroštátnej úrovni, ktorých výsledkom bola registrácia prepojenia v spoľahlivom zdroji. 3. Prepojenie bolo overené na základe informácií zo spoľahlivého zdroja.
Vysoká	Bod 3 úrovne „nízka“ a bod 2 úrovne „pokročilá“ a zároveň: 1. Je overené, že preukázanie totožnosti fyzickej osoby konajúcej v mene právnickej osoby bolo vykonané na úrovni „vysoká“. 2. Prepojenie bolo overené na základe jedinečného identifikátora označujúceho právnickú osobu používaného na vnútroštátnej úrovni a na základe informácií zo spoľahlivého zdroja, ktoré jedinečným spôsobom vystihujú fyzickú osobu.

2.2. *Riadenie prostriedkov elektronickej identifikácie*

2.2.1. Vlastnosti a uspôsobenie prostriedkov elektronickej identifikácie

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Prostriedok elektronickej identifikácie využíva najmenej jeden faktor autentifikácie. 2. Prostriedok elektronickej identifikácie je uspôsobený tak, aby vydavateľ mohol prijať primerané kroky na kontrolu toho, či sa používa iba pod kontrolou alebo v držbe osoby, ktorej patrí.
Pokročilá	1. Prostriedok elektronickej identifikácie využíva najmenej dva faktory autentifikácie z rôznych kategórií. 2. Prostriedok elektronickej identifikácie je uspôsobený tak, aby bolo možné predpokladať, že sa používa iba pod kontrolou alebo v držbe osoby, ktorej patrí.
Vysoká	Úroveň „pokročilá“ a zároveň: 1. Prostriedok elektronickej identifikácie chráni proti vyhotovovaniu duplikátov a manipulácii, ako aj proti útočníkom s vysokým útočným potenciálom. 2. Prostriedok elektronickej identifikácie je uspôsobený tak, aby ho osoba, ktorej patrí, mohla spoľahlivo chrániť pred použitím inými osobami.

2.2.2. Vydanie, doručenie a aktivácia

Úroveň zabezpečenia	Potrebné prvky
Nízka	Po vydaní sa prostriedok elektronickej identifikácie doručí prostredníctvom mechanizmu, na základe ktorého sa dá predpokladať, že ho dostane iba určená osoba.
Pokročilá	Po vydaní sa prostriedok elektronickej identifikácie doručí prostredníctvom mechanizmu, na základe ktorého sa dá predpokladať, že bude doručený iba do držby osoby, ktorej patrí.
Vysoká	V procese aktivácie sa overí, že prostriedok elektronickej identifikácie bol doručený iba do držby osoby, ktorej patrí.

2.2.3. Pozastavenie, zrušenie a obnovenie aktivácie

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Prostriedok elektronickej identifikácie je možné pozastaviť a/alebo zrušiť včas a účinným spôsobom. 2. Existujú opatrenia na zabránenie neoprávnenému pozastaveniu, zrušeniu a/alebo obnoveniu aktivácie. 3. K obnoveniu aktivácie dôjde len vtedy, ak sú naďalej splnené rovnaké požiadavky na zabezpečenie ako požiadavky stanovené pred pozastavením alebo zrušením.
Pokročilá	Rovnaké ako pri úrovni „nízka“.
Vysoká	Rovnaké ako pri úrovni „nízka“.

2.2.4. Obnovenie a výmena

Úroveň zabezpečenia	Potrebné prvky
Nízka	Ak sa vezmú do úvahy riziká zmeny osobných identifikačných údajov, obnovenie alebo výmena musia spĺňať rovnaké požiadavky na zabezpečenie ako pôvodné preukázanie a overenie identity alebo sa zakladajú na platnom prostriedku elektronickej identifikácie rovnakej alebo vyššej úrovne zabezpečenia.
Pokročilá	Rovnaké ako pri úrovni „nízka“.
Vysoká	Úroveň „nízka“ a zároveň: Ak sa obnovenie alebo výmena zakladajú na platnom prostriedku elektronickej identifikácie, identifikačné údaje sa overujú podľa spoľahlivého zdroja.

2.3. *Autentifikácia*

Tento oddiel sa zameriava na hrozby spojené s používaním mechanizmu autentifikácie a uvádzajú sa v ňom požiadavky na každú úroveň zabezpečenia. Kontroly sa v tomto oddiele chápu ako kontroly úmerné rizikám na danej úrovni.

2.3.1. Mechanizmus autentifikácie

V nasledujúcej tabuľke sa uvádzajú požiadavky podľa jednotlivých úrovní zabezpečenia, pokiaľ ide o mechanizmus autentifikácie, prostredníctvom ktorého fyzická alebo právnická osoba používa prostriedok elektronickej identifikácie na potvrdenie svojej totožnosti spoliehajúcej sa strane.

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Uvoľneniu osobných identifikačných údajov predchádza spoľahlivé overenie prostriedku elektronickej identifikácie a jeho platnosti. 2. Ak sú osobné identifikačné údaje uložené ako súčasť mechanizmu autentifikácie, tieto informácie sú zabezpečené proti strate a proti vyzradeniu vrátane offline analýzy. 3. V mechanizme autentifikácie sú implementované bezpečnostné kontroly na overenie prostriedku elektronickej identifikácie, takže je veľmi nepravdepodobné, že by činnosti, ako je hádanie, odpočúvanie, reprodukcia alebo manipulácia komunikácie útočníkom s rozšíreným základným útočným potenciálom, mohli rozvrátiť mechanizmus autentifikácie.

Úroveň zabezpečenia	Potrebné prvky
Pokročilá	Úroveň „nízka“ a zároveň: 1. Uvoľneniu osobných identifikačných údajov predchádza spoľahlivé overenie prostriedku elektronickej identifikácie a jeho platnosti prostredníctvom dynamickej autentifikácie. 2. V mechanizme autentifikácie sú implementované bezpečnostné kontroly na overenie prostriedku elektronickej identifikácie, takže je veľmi nepravdepodobné, že by činnosti, ako je hádanie, odpočúvanie, reprodukcia alebo manipulácia komunikácie útočníkom so stredným útočným potenciálom, mohli rozvrátiť mechanizmus autentifikácie.
Vysoká	Úroveň „pokročilá“ a zároveň: V mechanizme autentifikácie sú implementované bezpečnostné kontroly na overenie prostriedku elektronickej identifikácie, takže je veľmi nepravdepodobné, že by činnosti, ako je hádanie, odpočúvanie, reprodukcia alebo manipulácia komunikácie útočníkom s vysokým útočným potenciálom, mohli rozvrátiť mechanizmus autentifikácie.

2.4. *Riadenie a organizácia*

Všetci účastníci, ktorí poskytujú služby súvisiace s elektronickou identifikáciou v cezhraničnom kontexte (ďalej len „poskytovatelia“), musia mať zavedené zdokumentované postupy a politiky riadenia informačnej bezpečnosti, prístupy k riadeniu rizík a iné uznané kontroly, aby príslušným riadiacim orgánom pre schémy elektronickej identifikácie v jednotlivých členských štátoch poskytli záruku, že sa zaviedli účinné postupy. V celom oddiele 2.4 sa všetky požiadavky/prvky chápu ako úmerné rizikám na danej úrovni.

2.4.1. Všeobecné ustanovenia

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Poskytovatelia dodávajúci prevádzkové služby, na ktoré sa vzťahuje toto nariadenie, sú orgány verejnej správy alebo právnické osoby uznané ako také vnútroštátnym právom členského štátu, majú zavedenú organizáciu a sú plne prevádzkyschopné na všetkých úsekoch, ktoré sú relevantné pre poskytovanie týchto služieb. 2. Poskytovatelia spĺňajú všetky právne požiadavky, ktoré sa na nich vzťahujú v súvislosti s prevádzkou a dodávaním služby, vrátane druhov informácií, ktoré možno požadovať, spôsobu vykonávania preukazovania totožnosti, informácií, ktoré sa môžu uchovávať, a času, počas ktorého sa môžu uchovávať. 3. Poskytovatelia dokážu preukázať svoju schopnosť prevziať riziko zodpovednosti za škodu, ako aj to, že majú dostatočné finančné zdroje na pokračovanie činnosti a poskytovanie služieb. 4. Poskytovatelia sú zodpovední za plnenie všetkých záväzkov zadaných externým subjektom a za ich súlad s politikou schémy tak, ako keby tieto úlohy vykonali samotní poskytovatelia. 5. Schémy elektronickej identifikácie, ktoré neboli zriadené na základe vnútroštátneho práva, majú zavedený účinný plán ukončenia činnosti. Takýto plán musí zahŕňať riadne prerušenie služby alebo pokračovanie iným poskytovateľom, spôsob, akým sa informujú príslušné orgány a koncoví používatelia, ako aj podrobnosti o tom, akým spôsobom sa v súlade s politikou schémy majú chrániť, uchovávať a ničiť záznamy.
Pokročilá	Rovnaké ako pri úrovni „nízka“.
Vysoká	Rovnaké ako pri úrovni „nízka“.

2.4.2. Uverejnené oznámenia a informácie pre používateľov

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Existencia zverejneného vymedzenia služby, ktoré zahŕňa všetky platné podmienky a poplatky vrátane všetkých obmedzení jej používania. Vymedzenie služby musí obsahovať politiku ochrany osobných údajov. 2. Musí sa zaviesť vhodná politika a postupy, aby sa zabezpečilo, že používatelia služby budú včas a spoľahlivo informovaní o všetkých zmenách vymedzenia služby a akýchkoľvek platných podmienok a politiky ochrany osobných údajov pre uvedenú službu. 3. Musia sa zaviesť vhodné politiky a postupy na zabezpečenie úplných a správnych odpovedí na žiadosti o informácie.
Pokročilá	Rovnaké ako pri úrovni „nízka“.
Vysoká	Rovnaké ako pri úrovni „nízka“.

2.4.3. Riadenie informačnej bezpečnosti

Úroveň zabezpečenia	Potrebné prvky
Nízka	Existuje účinný systém riadenia informačnej bezpečnosti na riadenie a kontrolu rizík v oblasti informačnej bezpečnosti.
Pokročilá	Úroveň „nízka“ a zároveň: Systém riadenia informačnej bezpečnosti dodržiava osvedčené normy alebo zásady riadenia a kontroly rizík v oblasti informačnej bezpečnosti.
Vysoká	Rovnaké ako pri úrovni „pokročilá“.

2.4.4. Vedenie záznamov

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Zaznamenávanie a uchovávanie relevantných informácií pomocou účinného systému riadenia záznamov pri zohľadnení platných právnych predpisov a osvedčených postupov v oblasti ochrany a uchovávania údajov. 2. Pokiaľ to povoľujú vnútroštátne právne predpisy alebo iné vnútroštátne správne úpravy, uchovávanie a ochrana záznamov, kým sa vyžadujú na účely auditu a vyšetrovania porušení bezpečnosti a uchovávania údajov, a ich následné bezpečné zničenie.
Pokročilá	Rovnaké ako pri úrovni „nízka“.
Vysoká	Rovnaké ako pri úrovni „nízka“.

2.4.5. Zariadenia a personál

V nasledujúcej tabuľke sa uvádzajú požiadavky na zariadenia a personál a prípadne na subdodávateľov, ktorí vykonávajú úlohy, na ktoré sa vzťahuje toto nariadenie. Súlad s každou z požiadaviek musí byť úmerný úrovni rizika spojeného s poskytovanou úrovňou zabezpečenia.

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Existencia postupov, ktoré zabezpečujú, aby personál a subdodávatelia boli dostatočne vyškolení, kvalifikovaní a skúsení, pokiaľ ide o zručnosti potrebné na vykonávanie úloh, ktoré plnia. 2. Existencia dostatočného počtu zamestnancov a subdodávateľov na primeranú prevádzku služby a zaistenie jej zdrojov v súlade s jej politikami a postupmi. 3. Zariadenia používané na poskytovanie služby sa nepretržite monitorujú vzhľadom na škody spôsobené environmentálnymi udalosťami, neoprávnený prístup a iné faktory, ktoré môžu mať vplyv na bezpečnosť služby, a sú pred nimi chránené. 4. Zariadenia používané na poskytovanie služby zabezpečujú, aby bol prístup do priestorov, v ktorých sa uchovávajú alebo spracúvajú osobné, kryptografické alebo iné citlivé informácie, obmedzený na oprávnených zamestnancov alebo subdodávateľov.
Pokročilá	Rovnaké ako pri úrovni „nízka“.
Vysoká	Rovnaké ako pri úrovni „nízka“.

2.4.6. Technické kontroly

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Existencia primeraných technických kontrol na riadenie rizík ohrozujúcich bezpečnosť služieb a na ochranu dôvernosti, integrity a dostupnosti spracúvaných informácií. 2. Elektronické komunikačné kanály používané na výmenu osobných alebo citlivých informácií sú chránené proti odpočúvaniu, manipulácii a reprodukcii. 3. Ak sa na vydávanie prostriedkov elektronickej identifikácie a autentifikáciu používa citlivý kryptografický materiál, prístup k nemu je obmedzený na úlohy a aplikácie, ktoré si ho bezpodmienečne vyžadujú. Musí sa zabezpečiť, aby sa takýto materiál nikdy trvalo neuchovával ako jednoduchý text. 4. Existujú postupy na zabezpečenie toho, aby sa stále udržiavala bezpečnosť a aby existovala schopnosť reagovať na zmeny úrovní rizika, incidenty a narušenia bezpečnosti. 5. Všetky nosiče obsahujúce osobné, kryptografické alebo iné citlivé informácie sa uchovávajú, prepravujú a odstraňujú bezpečným a zabezpečeným spôsobom.
Pokročilá	Rovnaké ako pri úrovni „nízka“ a zároveň: Ak sa na vydávanie prostriedkov elektronickej identifikácie a na autentifikáciu používa citlivý kryptografický materiál, je chránený pred manipuláciou.
Vysoká	Rovnaké ako pri úrovni „pokročilá“.

2.4.7. Súlad a audit

Úroveň zabezpečenia	Potrebné prvky
Nízka	Existencia pravidelných vnútorných auditov zameraných na pokrytie všetkých úsekov týkajúcich sa dodávania poskytovaných služieb na zabezpečenie súladu s príslušnou politikou.

Úroveň zabezpečenia	Potrebné prvky
Pokročilá	Existencia pravidelných nezávislých vnútorných alebo vonkajších auditov zameraných na pokrytie všetkých úsekov týkajúcich sa dodávania poskytovaných služieb na zabezpečenie súladu s príslušnou politikou.
Vysoká	1. Existencia pravidelných nezávislých vonkajších auditov zameraných na pokrytie všetkých úsekov týkajúcich sa dodávania poskytovaných služieb na zabezpečenie súladu s príslušnou politikou. 2. Ak schému riadi priamo orgán verejnej správy, audit sa uskutočňuje v súlade s vnútroštátnymi právnymi predpismi.