PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2015/1502

ze dne 8. září 2015,

kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na 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 ([1]), a zejména na čl. 8 odst. 3 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Článek 8 nařízení (EU) č. 910/2014 stanoví, že systém elektronické identifikace oznámený podle čl. 9 odst. 1 musí uvádět nízkou, značnou nebo vysokou úroveň záruky pro prostředky pro elektronickou identifikaci vydávané v rámci tohoto systému.

(2) Je nezbytné stanovit minimální technické specifikace, normy a postupy, aby bylo dosaženo obecné shody ohledně podrobností týkajících se úrovní záruky a byla zajištěna interoperabilita při mapování vnitrostátních úrovní záruky oznámených systémů elektronické identifikace podle úrovní záruky uvedených v článku 8, jak stanoví čl. 12 odst. 4 písm. b) nařízení (EU) č. 910/2014.

(3) Při stanovování specifikací a postupů v tomto prováděcím aktu byla jako základní mezinárodní norma dostupná v oblasti úrovní záruky prostředků pro elektronickou identifikaci zohledněna mezinárodní norma ISO/IEC 29115. Obsah nařízení (EU) č. 910/2014 se však od uvedené mezinárodní normy liší, zejména pokud jde o požadavky na prokazování a ověřování totožnosti a o způsob, jakým se zohledňují rozdíly mezi opatřeními členských států v oblasti totožnosti a stávajícími nástroji v Evropské unii v téže oblasti. Příloha by proto neměla odkazovat na žádný konkrétní obsah mezinárodní normy ISO/IEC 29115, přestože z této normy vychází.

(4) Toto nařízení bylo vypracováno na základě přístupu orientovaného na výsledky, protože tento přístup byl nejvhodnější, což je rovněž patrné v definicích použitých k upřesnění pojmů a konceptů. Berou v úvahu cíl nařízení (EU) č. 910/2014, pokud jde o úrovně záruky prostředků pro elektronickou identifikaci. Proto by se při stanovování specifikací a postupů v tomto prováděcím aktu měl co nejvíce zohlednit rozsáhlý pilotní projekt STORK, včetně specifikací vypracovaných v jeho rámci, a definice a koncepty z ISO/IEC 29115.

(5) V závislosti na kontextu, v němž je třeba ověřit nějaký aspekt prokázání totožnosti, mohou mít spolehlivé zdroje různou podobu, např. registrů, dokumentů, subjektů aj. Spolehlivé zdroje se mohou v různých členských státech navzdory podobnému kontextu lišit.

(6) Požadavky na prokazování a ověřování totožnosti by měly zohlednit různé systémy a postupy a současně zajistit dostatečně vysokou úroveň záruky, aby byla vytvořena nezbytná důvěra. Postupy, které se předtím používaly pro jiné účely než vydávání prostředků pro elektronickou identifikaci, by proto měly být přijaty za podmínky, že tyto postupy splňují požadavky stanovené pro příslušnou úroveň záruky.

([1]) Úř. věst. L 257, 28.8.2014, s. 73.

(7) Obvykle se používají určité faktory autentizace, jako jsou sdílená tajemství, fyzické prostředky a fyzické vlastnosti. Za účelem zvýšení bezpečnosti procesu autentizace by se však mělo podpořit používání většího počtu faktorů autentizace, zejména z různých kategorií faktorů.

(8) Tímto nařízením by neměla být dotčena práva právnických osob na zastoupení. V příloze by však měly být stanoveny požadavky na propojení mezi prostředky pro elektronickou identifikaci fyzických a právnických osob.

(9) Měl by být uznán význam systémů řízení informační bezpečnosti a služeb, jakož i význam používání uznaných metod a uplatňování zásad obsažených v normách, jako je řada ISO/IEC 27000 a ISO/IEC 20000.

(10) Dále by se měly zohlednit osvědčené postupy v členských státech týkající se úrovní záruky.

(11) Důležitým nástrojem pro ověřování souladu produktů s bezpečnostními požadavky tohoto prováděcího aktu je certifikace bezpečnosti IT systémů založená na mezinárodních normách.

(12) Výbor uvedený v článku 48 nařízení (EU) č. 910/2014 nezaujal stanovisko ve lhůtě stanovené předsedou,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

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

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

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

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

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

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

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

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

Článek 2

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

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 8. září 2015.

Za Komisi
předseda
Jean-Claude JUNCKER

PŘÍLOHA

Technické specifikace a postupy pro nízkou, značnou a vysokou úroveň záruky prostředků pro elektronickou identifikaci vydaných v rámci oznámeného systému elektronické identifikace

1. **Použitelné definice**

Pro účely této přílohy se použijí tyto definice:

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

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

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

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

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

3) „dynamickou autentizací“ se rozumí elektronický proces, který s využitím kryptografie nebo jiných metod vytváří na požádání elektronický důkaz, že osoba disponuje identifikačními údaji nebo je má ve svém vlastnictví a který se mění při každé autentizaci mezi osobou a systémem ověřujícím její totožnost;

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

2. **Technické specifikace a postupy**

Prvky technických specifikací a postupů uvedené v této příloze se použijí k určení způsobu, jak se požadavky a kritéria článku 8 nařízení (EU) č. 910/2014 uplatňují na prostředky pro elektronickou identifikaci vydané v rámci systému elektronické identifikace.

2.1. *Přihlášení*

2.1.1. Žádost a registrace

Úroveň záruky	Potřebné prvky
Nízká	1. Zajistit, aby byl žadatel obeznámen s podmínkami používání prostředků pro elektronickou identifikaci. 2. Zajistit, aby byl žadatel obeznámen s doporučenými bezpečnostními opatřeními spojenými s používáním prostředků pro elektronickou identifikaci. 3. Shromáždit příslušné údaje o totožnosti nezbytné pro prokazování a ověřování totožnosti.
Značná	Stejné jako při nízké úrovni.
Vysoká	Stejné jako při nízké úrovni.

2.1.2. Prokazování a ověřování totožnosti (fyzická osoba)

Úroveň záruky	Potřebné prvky
Nízká	1. Lze předpokládat, že osoba vlastní důkaz deklarované totožnosti uznaný členským státem, ve kterém se žádost o prostředek pro elektronickou identifikaci podává. 2. Lze předpokládat, že tento důkaz je pravý nebo podle spolehlivého zdroje existuje, a důkaz se jeví být platným. 3. Spolehlivému zdroji je známo, že deklarovaná identita existuje, a lze předpokládat, že osoba deklarující identitu je jedna a tatáž.
Značná	Nízká úroveň a navíc musí být splněna jedna z alternativ uvedených v bodech 1 až 4: 1. Bylo ověřeno, že osoba vlastní důkaz deklarované totožnosti uznaný členským státem, ve kterém se žádost o prostředek pro elektronickou identifikaci podává, a důkaz se zkontroluje, aby se zjistilo, zda je pravý, nebo je podle spolehlivého zdroje známo, že důkaz existuje a vztahuje se ke skutečné osobě, a byly podniknuty kroky s cílem minimalizovat riziko, že totožnost osoby není deklarovanou totožností, přičemž bylo zohledněno například riziko ztráty, odcizení, zrušení důkazu nebo pozastavení či vypršení jeho platnosti; nebo 2. během procesu registrace se předloží doklad totožnosti v členském státě, kde byl doklad vydán, a doklad se zjevně vztahuje k osobě, která jej předložila, a byly podniknuty kroky s cílem minimalizovat riziko, že totožnost osoby není deklarovanou totožností, přičemž bylo zohledněno například riziko ztráty, odcizení, zrušení dokladů nebo pozastavení či vypršení jejich platnosti; nebo 3. pokud postupy, které předtím používal veřejný či soukromý subjekt v témže členském státě za jiným účelem než vydávání prostředků pro elektronickou identifikaci, zajišťují záruky rovnocenné s postupy stanovenými v oddíle 2.1.2 pro značnou úroveň záruky, nemusí subjekt odpovědný za registraci opakovat tyto dřívější postupy za předpokladu, že takovou rovnocennou záruku potvrdí subjekt posuzování shody uvedený v čl. 2 odst. 13 nařízení Evropského parlamentu a Rady (ES) č. 765/2008 [1] nebo rovnocenný subjekt; nebo 4. pokud jsou prostředky pro elektronickou identifikaci vydány na základě platných oznámených prostředků pro elektronickou identifikaci, které mají značnou nebo vysokou úroveň záruky, a je přitom přihlédnuto k rizikům změny osobních identifikačních údajů, není nutno postupy prokazování a ověřování totožnosti opakovat. Pokud prostředek pro elektronickou identifikaci sloužící jako základ nebyl oznámen, musí značnou nebo vysokou úroveň záruky potvrdit subjekt posuzování shody uvedený v čl. 2 odst. 13 nařízení (ES) č. 765/2008 nebo rovnocenný subjekt.

Úroveň záruky	Potřebné prvky
Vysoká	Musí být splněny požadavky bodu 1, nebo bodu 2: 1. Značná úroveň a navíc musí být splněna jedna z alternativ uvedených v písmenech a) až c): a) Pokud bylo ověřeno, že osoba vlastní důkaz totožnosti opatřený fotografií nebo biometrickými údaji uznaný členským státem, ve kterém se žádost o prostředky pro elektronickou identifikaci podává, a že důkaz označuje deklarovanou totožnost, důkaz se zkontroluje, aby se zjistilo, zda je podle spolehlivého zdroje platný, a na základě srovnání jedné nebo více fyzických vlastností osoby s údaji ze spolehlivého zdroje se zjistí, zda se totožnost žadatele shoduje s deklarovanou totožností; nebo b) pokud postupy, které předtím používal veřejný či soukromý subjekt v témže členském státě za jiným účelem než vydávání prostředků pro elektronickou identifikaci, zajišťují záruky rovnocenné s postupy stanovenými v oddíle 2.1.2 pro vysokou úroveň záruky, nemusí subjekt odpovědný za registraci opakovat tyto dřívější postupy za předpokladu, že takovou rovnocennou záruku potvrdí subjekt posuzování shody uvedený v čl. 2 odst. 13 nařízení Evropského parlamentu a Rady (ES) č. 765/2008 nebo rovnocenný subjekt, a jsou podniknuty kroky s cílem prokázat, že výsledky předchozích postupů zůstávají v platnosti; nebo c. pokud jsou prostředky pro elektronickou identifikaci vydány na základě platného oznámeného prostředku pro elektronickou identifikaci, který má značnou nebo vysokou úroveň záruky, a je přitom přihlédnuto k rizikům změny osobních identifikačních údajů, není nutno opakovat postupy prokazování a ověřování totožnosti. Pokud prostředek pro elektronickou identifikaci sloužící jako základ nebyl oznámen, musí vysokou úroveň záruky potvrdit subjekt posuzování shody uvedený v čl. 2 odst. 13 nařízení (ES) č. 765/2008 nebo rovnocenný subjekt, a jsou podniknuty kroky s cílem prokázat, že výsledky předchozího postupu vydávání oznámeného prostředku pro elektronickou identifikaci zůstávají v platnosti. NEBO 2. Pokud žadatel nepředloží žádný uznaný důkaz totožnosti opatřený fotografií nebo biometrickými údaji, uplatní se naprosto stejné postupy, jaké se pro získání takového uznaného důkazu totožnosti opatřeného fotografií nebo biometrickými údaji používají na vnitrostátní úrovni v členském státě subjektu odpovědného za registraci.

([1]) Nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93 (Úř. věst. L 218, 13.8.2008, s. 30).

2.1.3. Prokazování a ověřování totožnosti (právnická osoba)

Úroveň záruky	Potřebné prvky
Nízká	1. Deklarovaná totožnost právnické osoby se prokáže na základě důkazu uznaného členským státem, ve kterém se žádost o prostředek pro elektronickou identifikaci podává.

Úroveň záruky	Potřebné prvky
	2. Důkaz se jeví být platným a lze předpokládat, že je pravý nebo že podle spolehlivého zdroje existuje, pokud je zahrnutí právnické osoby do spolehlivého zdroje dobrovolné a je upraveno dohodou mezi právnickou osobou a spolehlivým zdrojem. 3. Spolehlivému zdroji není známo, že by právnická osoba byla v situaci, která by jí bránila jednat jako právnická osoba.
Značná	Nízká úroveň a navíc musí být splněna jedna z alternativ uvedených v bodech 1 až 3: 1. Deklarovaná totožnost právnické osoby se prokáže na základě důkazu uznaného členským státem, ve kterém se žádost o prostředek pro elektronickou identifikaci podává, a to včetně názvu právnické osoby, její právní formy a (případně) registračního čísla, a důkaz se zkontroluje, aby se zjistilo, zda je pravý nebo zda je podle spolehlivého zdroje známo, že existuje, pokud se pro působení právnické osoby v jejím odvětví vyžaduje, aby byla zahrnuta do spolehlivého zdroje, a byly podniknuty kroky s cílem minimalizovat riziko, že totožnost právnické osoby není deklarovanou totožností, přičemž bylo zohledněno například riziko ztráty, odcizení, zrušení dokladů nebo pozastavení či vypršení jejich platnosti; nebo 2. pokud postupy, které předtím používal veřejný či soukromý subjekt v témže členském státě za jiným účelem než vydávání prostředků pro elektronickou identifikaci, zajišťují záruky rovnocenné s postupy stanovenými v oddíle 2.1.3 pro značnou úroveň záruky, nemusí subjekt odpovědný za registraci opakovat tyto dřívější postupy za předpokladu, že takovou rovnocennou záruku potvrdí subjekt posuzování shody uvedený v čl. 2 odst. 13 nařízení (ES) č. 765/2008 nebo rovnocenný subjekt; nebo 3. pokud jsou prostředky pro elektronickou identifikaci vydány na základě platného oznámeného prostředku pro elektronickou identifikaci, který má značnou nebo vysokou úroveň záruky, není nutno opakovat postupy prokazování a ověřování totožnosti. Pokud prostředek pro elektronickou identifikaci sloužící jako základ nebyl oznámen, musí značnou nebo vysokou úroveň záruky potvrdit subjekt posuzování shody uvedený v čl. 2 odst. 13 nařízení (ES) č. 765/2008 nebo rovnocenný subjekt.
Vysoká	Značná úroveň a navíc musí být splněna jedna z alternativ uvedených v bodech 1 až 3: 1. Deklarovaná totožnost právnické osoby se prokáže na základě důkazu uznaného členským státem, ve kterém se žádost o prostředek pro elektronickou identifikaci podává, a to včetně názvu právnické osoby, její právní formy a alespoň jednoho jedinečného identifikátoru označujícího danou právnickou osobu, který je používán na vnitrostátní úrovni, a důkaz se zkontroluje, aby se zjistilo, zda je podle spolehlivého zdroje platný; nebo

Úroveň záruky	Potřebné prvky
	2. pokud postupy, které předtím používal veřejný či soukromý subjekt v témže členském státě za jiným účelem než vydávání prostředků pro elektronickou identifikaci, zajišťují záruky rovnocenné s postupy stanovenými v oddíle 2.1.3 pro vysokou úroveň záruky, nemusí subjekt odpovědný za registraci opakovat tyto dřívější postupy za předpokladu, že takovou rovnocennou záruku potvrdí subjekt posuzování shody uvedený v čl. 2 odst. 13 nařízení (ES) č. 765/2008 nebo rovnocenný subjekt, a jsou podniknuty kroky s cílem prokázat, že výsledky tohoto předchozího postupu zůstávají v platnosti; nebo 3. pokud jsou prostředky pro elektronickou identifikaci vydány na základě platného oznámeného prostředku pro elektronickou identifikaci, který má vysokou úroveň záruky, není nutno opakovat postupy prokazování a ověřování totožnosti. Pokud prostředek pro elektronickou identifikaci sloužící jako základ nebyl oznámen, musí vysokou úroveň záruky potvrdit subjekt posuzování shody uvedený v čl. 2 odst. 13 nařízení (ES) č. 765/2008 nebo rovnocenný subjekt, a jsou podniknuty kroky s cílem prokázat, že výsledky předchozího postupu vydávání oznámeného prostředku pro elektronickou identifikaci zůstávají v platnosti.

2.1.4. Propojení mezi prostředky pro elektronickou identifikaci fyzických a právnických osob

V příslušných případech platí pro propojení mezi prostředky pro elektronickou identifikaci fyzické osoby a prostředky pro elektronickou identifikaci právnické osoby (dále jen „propojení“) tyto podmínky:

1) Propojení musí být možné pozastavit a/nebo zrušit. Životní cyklus propojení (např. aktivace, pozastavení, obnovení, zrušení) je spravován podle vnitrostátně uznávaných postupů.

2) Fyzická osoba, jejíž prostředek pro elektronickou identifikaci je propojen s prostředkem pro elektronickou identifikaci právnické osoby, může pověřit vykonáváním propojení jinou fyzickou osobu na základě vnitrostátně uznávaných postupů. Odpovědnost však nadále nese pověřující fyzická osoba.

3) Propojení se provádí následujícím způsobem:

Úroveň záruky	Potřebné prvky
Nízká	1. Je ověřeno, že byla prokázána totožnost fyzické osoby, která jedná jménem právnické osoby, na nízké nebo vyšší úrovni. 2. Propojení bylo stanoveno na základě vnitrostátně uznávaných postupů. 3. Spolehlivému zdroji není známo, že by fyzická osoba byla v situaci, která by jí bránila jednat jménem právnické osoby.
Značná	Bod 3 nízké úrovně a navíc: 1. Je ověřeno, že byla prokázána totožnost fyzické osoby, která jedná jménem právnické osoby, na značné nebo vysoké úrovni.

Úroveň záruky	Potřebné prvky
	2. Propojení bylo stanoveno na základě vnitrostátně uznávaných postupů, jejichž výsledkem byla registrace propojení ve spolehlivém zdroji. 3. Propojení bylo ověřeno na základě informací ze spolehlivého zdroje.
Vysoká	Bod 3 nízké úrovně a bod 2 značné úrovně a navíc: 1. Je ověřeno, že byla prokázána totožnost fyzické osoby, která jedná jménem právnické osoby, na vysoké úrovni. 2. Propojení bylo ověřeno na základě jedinečného identifikátoru označujícího právnickou osobu, který je používán na vnitrostátní úrovni, a na základě informací ze spolehlivého zdroje, které fyzickou osobu jednoznačně označují.

2.2. *Správa prostředků pro elektronickou identifikaci*

2.2.1. Vlastnosti a forma prostředků pro elektronickou identifikaci

Úroveň záruky	Potřebné prvky
Nízká	1. Prostředek pro elektronickou identifikaci využívá alespoň jednoho faktoru autentizace. 2. Prostředek pro elektronickou identifikaci je navržen tak, aby vydavatel mohl přijmout přiměřené kroky k ověření toho, zda se používá pouze pod kontrolou nebo v rámci vlastnictví osoby, které patří.
Značná	1. Prostředek pro elektronickou identifikaci využívá alespoň dvou faktorů autentizace z odlišných kategorií. 2. Prostředek pro elektronickou identifikaci je navržen tak, aby bylo možno předpokládat, že se používá pouze pod kontrolou nebo v rámci vlastnictví osoby, které patří.
Vysoká	Značná úroveň a navíc: 1. Prostředek pro elektronickou identifikaci chrání proti vyhotovování duplikátů a neoprávněné manipulaci i proti útočníkům s vysokým potenciálem útoku. 2. Prostředek pro elektronickou identifikaci je navržen tak, aby jej mohla osoba, které patří, spolehlivě chránit před zneužitím třetí osobou.

2.2.2. Vydání, doručení a aktivace

Úroveň záruky	Potřebné prvky
Nízká	Po vydání je prostředek pro elektronickou identifikaci doručen prostřednictvím mechanismu, na základě kterého lze předpokládat, že prostředek dostane pouze určená osoba.
Značná	Po vydání je prostředek pro elektronickou identifikaci doručen prostřednictvím mechanismu, na základě kterého lze předpokládat, že je prostředek předán pouze do vlastnictví osoby, které patří.
Vysoká	V procesu aktivace se ověří, že byl prostředek pro elektronickou identifikaci předán pouze do vlastnictví osoby, které patří.

2.2.3. Pozastavení, zrušení a reaktivace

Úroveň záruky	Potřebné prvky
Nízká	1. Prostředek pro elektronickou identifikaci je možné včas a účinným způsobem pozastavit a/nebo zrušit. 2. Existují opatření přijatá s cílem zabránit neoprávněnému pozastavení, zrušení a/nebo reaktivaci. 3. Reaktivaci je možné provést, pouze pokud budou nadále splněny stejné požadavky na záruku, které byly stanoveny před pozastavením nebo zrušením.
Značná	Stejné jako při nízké úrovni.
Vysoká	Stejné jako při nízké úrovni.

2.2.4. Obnovení a výměna

Úroveň záruky	Potřebné prvky
Nízká	S přihlédnutím k rizikům změny osobních identifikačních údajů musí obnova nebo výměna splňovat stejné požadavky na záruku jako původní prokazování a ověřování totožnosti nebo vycházet z platného prostředku pro elektronickou identifikaci se stejnou nebo vyšší úrovní záruky.
Značná	Stejné jako při nízké úrovni.
Vysoká	Nízká úroveň a navíc: Pokud obnovení nebo výměna probíhá na základě platného prostředku pro elektronickou identifikaci, ověří se údaje o totožnosti podle spolehlivého zdroje.

2.3. *Autentizace*

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

2.3.1. Mechanismus autentizace

V následující tabulce jsou pro každou úroveň záruky stanoveny požadavky na mechanismus autentizace, jehož prostřednictvím fyzická nebo právnická osoba používá prostředek pro elektronickou identifikaci k potvrzení své totožnosti spoléhající se straně.

Úroveň záruky	Potřebné prvky
Nízká	1. Vydání osobních identifikačních údajů předchází spolehlivé ověření prostředku pro elektronickou identifikaci a jeho platnosti. 2. Pokud jsou osobní identifikační údaje uloženy jako součást mechanismu autentizace, jsou tyto informace zabezpečeny proti ztrátě a vyzrazení, včetně offline analýzy. 3. Mechanismus autentizace provádí bezpečnostní kontroly k ověření prostředku pro elektronickou identifikaci, takže je velmi nepravděpodobné, že by činnosti jako hádání, odposlech, reprodukce nebo manipulace komunikace ze strany útočníka se zvýšeným základním potenciálem útoku mohly mechanismy autentizace narušit.

Úroveň záruky	Potřebné prvky
Značná	Nízká úroveň a navíc: 1. Vydání osobních identifikačních údajů předchází spolehlivé ověření prostředku pro elektronickou identifikaci a jeho platnosti prostřednictvím dynamické autentizace. 2. Mechanismus autentizace provádí bezpečnostní kontroly k ověření prostředku pro elektronickou identifikaci, takže je velmi nepravděpodobné, že by činnosti jako hádání, odposlech, reprodukce nebo manipulace komunikace ze strany útočníka s mírným potenciálem útoku mohly mechanismy autentizace narušit.
Vysoká	Značná úroveň a navíc: Mechanismus autentizace provádí bezpečnostní kontroly k ověření prostředku pro elektronickou identifikaci, takže je velmi nepravděpodobné, že by činnosti jako hádání, odposlech, opakování nebo manipulace komunikace ze strany útočníka s vysokým potenciálem útoku mohly mechanismy autentizace narušit.

2.4. *Řízení a organizace*

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

2.4.1. Obecná ustanovení

Úroveň záruky	Potřebné prvky
Nízká	1. Poskytovateli provozních služeb, na které se vztahuje toto nařízení, jsou orgány veřejné správy nebo právnické osoby uznané jako takové podle vnitrostátního práva členského státu, které mají zavedenou organizační strukturu a jsou plně provozuschopné ve všech úsecích relevantních pro poskytování služeb. 2. Poskytovatelé dodržují všechny právní požadavky, které se na ně vztahují v souvislosti s provozem a poskytováním služby, včetně druhů informací, které je možno požadovat, způsobů ověřování totožnosti a upřesnění, jaké informace mohou být uchovávány a jak dlouho. 3. Poskytovatelé jsou s to prokázat svou schopnost převzít riziko odpovědnosti za škodu, jakož i dostatek finančních prostředků pro nepřetržitý provoz a poskytování služeb. 4. Poskytovatelé nesou odpovědnost za plnění veškerých závazků zadaných externím subjektům a za dodržování politiky systému, jako by tyto povinnosti plnili sami. 5. Systémy elektronické identifikace, které nebyly zřízeny podle vnitrostátního práva, musí mít zavedeny účinný plán ukončení činnosti. Tento plán musí zahrnovat řádné ukončení služby nebo pokračování jiným poskytovatelem, způsob, jakým jsou informovány příslušné orgány a koneční uživatelé, a podrobnosti, jak mají být chráněny, uchovávány a ničeny záznamy v souladu s politikou systému.
Značná	Stejné jako při nízké úrovni.
Vysoká	Stejné jako při nízké úrovni.

2.4.2. Zveřejněná oznámení a informace pro uživatele

Úroveň záruky	Potřebné prvky
Nízká	1. Existuje zveřejněná definice služby, která zahrnuje všechny platné podmínky a poplatky, včetně veškerých omezení jejího používání. Definice služby zahrnuje politiku ochrany osobních údajů. 2. Je nutno zavést vhodnou politiku a postupy, které zajistí, aby byli uživatelé služby včas a spolehlivým způsobem informováni o veškerých změnách definice služeb a platných podmínek a politiky ochrany osobních údajů u dané služby. 3. Je nutno zavést vhodné politiky a postupy, které zajistí úplné a správné odpovědi na žádosti o informace.
Značná	Stejné jako při nízké úrovni.
Vysoká	Stejné jako při nízké úrovni.

2.4.3. Řízení bezpečnosti informací

Úroveň záruky	Potřebné prvky
Nízká	Existuje účinný systém řízení bezpečnosti informací pro řízení a kontrolu rizik v oblasti bezpečnosti informací.
Značná	Nízká úroveň a navíc: Systém řízení bezpečnosti informací dodržuje osvědčené normy nebo zásady řízení a kontroly rizik v oblasti bezpečnosti informací.
Vysoká	Stejné jako při značné úrovni.

2.4.4. Vedení záznamů

Úroveň záruky	Potřebné prvky
Nízká	1. Zaznamenávání a uchovávání příslušných informací prostřednictvím účinného systému správy záznamů při zohlednění platných právních předpisů a osvědčených postupů v souvislosti s ochranou údajů a uchováváním údajů. 2. Uchovávání, pokud to povolují vnitrostátní právní předpisy nebo jiná vnitrostátní správní opatření, a ochrana záznamů po dobu potřebnou pro účely auditu, vyšetřování případů narušení bezpečnosti a ukládání dat a jejich následné bezpečné zničení.
Značná	Stejné jako při nízké úrovni.
Vysoká	Stejné jako při nízké úrovni.

2.4.5. Zařízení a personál

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

Úroveň záruky	Potřebné prvky
Nízká	1. Existují postupy, které zajistí, aby zaměstnanci a subdodavatelé měli dostatečnou odbornou přípravu a dostatečné kvalifikace a zkušenosti v dovednostech nutných k výkonu úkolů, které plní. 2. Zaměstnanci a subdodavatelé jsou v dostatečném počtu potřebném k adekvátnímu provozu služby a zajištění přiměřených zdrojů v souladu s jejími politikami a postupy. 3. Zařízení používaná pro poskytování služby jsou nepřetržitě monitorována a chráněna proti škodám způsobeným ekologickými událostmi, neoprávněným přístupem a jinými faktory, které mohou ovlivnit bezpečnost služby. 4. Zařízení používaná pro poskytování služby zajišťují, že přístup do prostor, v nichž se uchovávají nebo zpracovávají osobní, kryptografické nebo jiné citlivé informace, mají pouze oprávnění zaměstnanci nebo subdodavatelé.
Značná	Stejné jako při nízké úrovni.
Vysoká	Stejné jako při nízké úrovni.

2.4.6. Technické kontroly

Úroveň záruky	Potřebné prvky
Nízká	1. Existují přiměřené technické kontroly za účelem řízení rizik ohrožujících bezpečnost služeb a na ochranu důvěrnosti, integrity a dostupnosti zpracovávaných informací. 2. Kanály elektronické komunikace používané pro výměnu citlivých nebo osobních informací jsou chráněny proti odposlechu, manipulaci a opakování dat („replay“). 3. Pokud se pro vydávání prostředků pro elektronickou identifikaci a autentizaci používají citlivé kryptografické materiály, je přístup k nim omezen pouze na úlohy a aplikace, které přístup bezpodmínečně vyžadují. Musí se zajistit, aby takový materiál nebyl nikdy trvale uchováván jako jednoduchý text. 4. Existují postupy k zajištění toho, aby se trvale udržovala bezpečnost a bylo možno reagovat na změny úrovní rizik, incidenty a případy narušení bezpečnosti. 5. Všechny nosiče obsahující osobní, kryptografické nebo jiné citlivé informace se uchovávají, přepravují a likvidují bezpečným a chráněným způsobem.
Značná	Stejné jako při nízké úrovni a navíc: Citlivý kryptografický materiál, který se používá pro vydávání prostředků pro elektronickou identifikaci a autentizaci, je chráněn před neoprávněnou manipulací.
Vysoká	Stejné jako při značné úrovni.

2.4.7. Dodržování a audit

Úroveň záruky	Potřebné prvky
Nízká	Existují pravidelné interní audity, jejichž rozsah zahrnuje všechny úseky týkající se poskytování služeb, aby se zajistilo dodržování příslušné politiky.

Úroveň záruky	Potřebné prvky
Značná	Existují pravidelné nezávislé interní nebo externí audity, jejichž rozsah zahrnuje všechny úseky týkající se poskytování služeb, aby se zajistilo dodržování příslušné politiky.
Vysoká	1. Existují pravidelné nezávislé externí audity, jejichž rozsah zahrnuje všechny úseky týkající se poskytování služeb, aby se zajistilo dodržování příslušné politiky. 2. Spravuje-li systém přímo orgán veřejné správy, probíhá audit v souladu s vnitrostátními právními předpisy.