

Úrovne autentifikácie elektronických služieb verejnej správy

Úrovne autentifikácie elektronizácie služieb verejnej správy sa získavajú na základe úrovne registračnej fázy a úrovne autentifikačnej fázy.

1. Registračná fáza

1.1 Úroveň registračnej fázy sa získava na základe úrovne kvality identifikačnej registrácie, úrovne kvality doručovania prihlasovacích údajov a úrovne garancií štátu pre registračnú autoritu.

1.2 Kvalita identifikačnej registrácie sa skladá z fyzickej prítomnosti identifikovanej osoby, kvality preukazovania identity pri identifikačnej registrácii a overovania preukazovania identity pri identifikačnej registrácii.

1.2.1 Fyzická prítomnosť identifikovanej osoby má tieto varianty:

- a) fyzická prítomnosť identifikovanej osoby sa počas identifikačnej registrácie nevyžaduje,
- b) fyzická prítomnosť identifikovanej osoby sa počas identifikačnej registrácie vyžaduje najmenej raz; pri obnovení registrácie už fyzickú prítomnosť identifikovanej osoby nie je potrebné vyžadovať,
- c) fyzická prítomnosť identifikovanej osoby sa vyžaduje pri preberaní certifikátu najmenej raz; pri opakovanom preberaní certifikátu sa už fyzická prítomnosť identifikovanej osoby nemusí vyžadovať.

1.2.2 Kvalita preukazovania identity pri identifikačnej registrácii má tieto varianty:

- a) registračné údaje sa počas identifikačnej registrácie poskytujú jednorazovo, pričom môžu byť známe aj inej osobe a nemusia viesť k jednoznačnej identifikácii osoby, napríklad meno, priezvisko, e-mailová adresa alebo rok narodenia,
- b) registračné údaje sa počas identifikačnej registrácie poskytujú viacnásobne, pričom môžu byť známe aj inej osobe a vedú k jednoznačnej identifikácii osoby, napríklad meno, priezvisko, e-mailová adresa alebo rok narodenia,
- c) registračné údaje poskytnuté počas identifikačnej registrácie sú známe len registrovanej osobe, pričom sú overiteľné podľa určeného registra a vedú k jednoznačnej identifikácii osoby, napríklad rodné číslo, číslo občianskeho preukazu alebo číslo cestovného pasu.

1.2.3 Overovanie preukazovania identity pri identifikačnej registrácii má tieto varianty:

- a) pravdivosť poskytnutých registračných údajov sa overuje najviac overením funkčnosti poskytnutej e-mailovej adresy alebo obdobného elektronického konta, ak sú poskytnuté,
- b) registračné údaje sa overujú na základe porovnania s určenou dôveryhodnou databázou alebo registrom, napríklad orgánom verejnej moci, bankou, poisťovňou a podobne,

- c) registračné údaje sú podpísané elektronickým podpisom podľa osobitného predpisu,⁵²⁾
- d) overovanie vyžaduje vyhlásenie zamestnávateľa na základe zmluvy medzi ním a osobou vydávajúcou autentifikačný nástroj, ktorej obsahom je skutočnosť, že zamestnávateľ počas zamestnaneckého vzťahu s identifikovanou osobou overil listinnú formu dokladu totožnosti, obsahujúcu najmenej fotografiu identifikovanej osoby, napríklad občiansky preukaz, cestovný pas, vodičský preukaz,
- e) overovanie vyžaduje preukázanie fotokópie alebo skenu preukazu totožnosti, obsahujúcich najmenej fotografiu a podpis identifikovanej osoby, napríklad občiansky preukaz, cestovný pas, vodičský preukaz, pričom platnosť tohto preukazu totožnosti sa overuje prostredníctvom evidencie odcudzených a stratených dokladov,
- f) overovanie vyžaduje preukázanie fotokópie alebo skenu preukazu totožnosti obsahujúcich najmenej fotografiu a podpis identifikovanej osoby, napríklad občiansky preukaz, cestovný pas, vodičský preukaz, pričom je vykonaná úspešná finančná transakcia, a to prostredníctvom bankového účtu, pri ktorom je na jeho zriadenie potrebné preukázanie obdobného platného preukazu totožnosti, ktorý sa týkal tej istej identifikovanej osoby,
- g) overovanie vyžaduje preukázanie preukazu totožnosti obsahujúceho najmenej fotografiu a podpis identifikovanej osoby, napríklad občiansky preukaz, cestovný pas, vodičský preukaz,
- h) registračné údaje sú podpísané elektronickým podpisom, overeným pred ukončením identifikačnej registrácie certifikačnou autoritou.

1.3 Kvalita doručovania prihlasovacích údajov má tieto varianty:

1.3.1 prihlasovacie údaje sa doručujú bez akejkoľvek formy overovania,

1.3.2 prihlasovacie údaje sa identifikovanej osobe doručujú s nízkou úrovňou overovania jej identity pri ich preberaní, a to napríklad

- a) meno a heslo sa doručujú dvomi nezávislými poštovými zásielkami alebo správami, pričom aspoň jedna sa zasiela v listinnej podobe na adresu vedenú v určenom registri alebo databáze,
- b) prihlasovacie údaje sa priamo sťahujú prostredníctvom odkazu, ktorý je identifikovanej osobe doručený na určenú e-mailovú adresu; platnosť uvedeného odkazu po adekvátnej dobe expiruje, obvykle po 24 hodinách,

1.3.3 prihlasovacie údaje sa identifikovanej osobe doručujú so strednou úrovňou overovania jej identity pri ich preberaní, a to napríklad

- a) doručujú sa na adresu overenú v príslušnom určenom registri alebo databáze, v ktorom je táto adresa evidovaná, a ktorý má najmenej úroveň doporučenej pošty,
- b) je možné ich získať stiahnutím prostredníctvom internetu na základe žiadosti podpísanej kvalifikovaným podpisom, overeným certifikačnou autoritou,

⁵²⁾ Čl. 3 ods. 10 nariadenia 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 (Ú. v. EÚ L 257, 28. 8. 2014).

- c) je možné ich získať prostredníctvom internetu po použití hesla, ktoré registrovaná osoba dostala do vlastných rúk počas identifikačnej registrácie, ktorej kvalita je najmenej úrovne 3 podľa tabuľky č. 1,
- 1.3.4 prihlasovacie údaje sa identifikovanej osobe doručujú s vysokou úrovňou overovania jej identity pri ich preberaní, a to napríklad
- a) prihlasovacie údaje sa osobne preberajú po overení identity identifikovanej osoby,
 - b) prihlasovacie údaje sa identifikovanej osobe zasielajú, ale aktivujú sa až po overení jej identity na základe fyzickej prítomnosti.
- 1.4** Garancie štátu pre registračnú autoritu identifikácie majú tieto varianty:
- 1.4.1 registračnej autority identifikácie sa netýka žiadny relevantný mechanizmus garancií zo strany štátu, najmä dohľad, schvaľovanie alebo akreditácia,
- 1.4.2 činnosť registračnej autority identifikácie v tejto oblasti podlieha súhlasu príslušného orgánu verejnej moci,
- 1.4.3 činnosť registračnej autority identifikácie v tejto oblasti je vykonávaná orgánom verejnej moci alebo na základe akreditácie alebo dohľadu orgánu verejnej moci,
- 1.4.4 činnosť registračnej autority identifikácie v tejto oblasti spĺňa požiadavky na činnosť registračnej autority, ktorá koná v mene kvalifikovaného poskytovateľa dôveryhodnej služby podľa osobitného predpisu.⁵³⁾

2. Autentifikačná fáza

2.1 Úroveň autentifikačnej fázy sa získava na základe úrovne typov a robustnosti preukazovania identity a úrovne bezpečnosti autentifikačného mechanizmu.

2.2 Typy a robustnosť preukazovania identity má tieto varianty:

- 2.2.1 používa sa autentifikačný nástroj typu heslo alebo token založený na PIN-e, ktorý môže byť zvolený identifikovanou osobou alebo je automaticky generovaný, pričom tento nespĺňa obvyklé pravidlá pre vytváranie silných hesiel alebo PIN-ov, napríklad nemá dostatočnú dĺžku, adekvátny pomer znakov a podobne, a preto je zraniteľný uhádnutím alebo slovníkovými útokmi,
- 2.2.2 používa sa autentifikačný nástroj typu heslo alebo token založený na PIN-e, ktorý môže byť zvolený identifikovanou osobou alebo je automaticky generovaný, pričom tento spĺňa obvyklé pravidlá pre vytváranie silných hesiel alebo PIN-ov, napríklad má dostatočnú dĺžku, adekvátny pomer znakov a podobne, a preto nie je zraniteľný uhádnutím alebo slovníkovými útokmi,
- 2.2.3 používajú sa jednorazové heslá alebo certifikáty uložené na ľubovoľnom úložisku, ktorými sú kryptografické kľúče, obvykle uložené v súboroch na pevnom disku, USB alebo podobnom dátovom nosiči, pričom autentifikácia sa vykonáva preukázaním vlastníctva a držby takéhoto kľúča, nakoľko prístup ku kľúču je založený na hesle známom len používateľovi,
- 2.2.4 používajú sa kvalifikované certifikáty, uložené na ľubovoľnom úložisku a primerane spĺňajúce požiadavky podľa osobitného predpisu,⁵⁴⁾

⁵³⁾ Čl. 24 nariadenia (EÚ) č. 910/2014.

⁵⁴⁾ Čl. 28 nariadenia (EÚ) č. 910/2014.

- 2.2.5 používajú sa certifikáty uložené na chránenom úložisku, ktorými sú chránené kryptografické kľúče, obvykle uložené v čípe smart kariet alebo obdobných médií, pričom autentifikácia sa vykonáva preukázaním vlastníctva takéhoto média a držby príslušného kľúča,
- 2.2.6 používajú sa kvalifikované certifikáty uložené na chránenom úložisku spĺňajúce požiadavky podľa osobitného predpisu.⁵⁴⁾

2.3 Bezpečnosť autentifikačného mechanizmu má tieto varianty:

- 2.3.1 autentifikačný mechanizmus neposkytuje žiadnu alebo poskytuje nízku úroveň ochrany pred útokmi uhádnutím, odpočúvaním siete, únosom relácie, typu odpovedí a muž v strede; nízkou úrovňou ochrany sa rozumie, že ani jedna úroveň nie je poskytovaná primerane,
- 2.3.2 bezpečný autentifikačný mechanizmus poskytuje určitú úroveň ochrany pred útokmi uhádnutím, odpočúvaním siete, únosom relácie, typu odpovedí a muž v strede, čím sa rozumie primeraná ochrana aspoň pred jedným typom útoku,
- 2.3.3 bezpečný autentifikačný mechanizmus poskytuje ochranu pred väčšinou útokov, ktorými sú uhádnutie, odpočúvanie siete, únos relácie, útok typu odpovedí a muž v strede,
- 2.3.4 uznávaný bezpečný autentifikačný mechanizmus poskytuje ochranu pred všetkými útokmi, ktorými sú uhádnutie, odpočúvanie siete, únos relácie, útok typu odpovedí a muž v strede, a to najmenej na úrovni Evaluation Assurance Level 4 (EAL4+) podľa technickej normy.⁵⁵⁾

3. Mechanizmus výpočtu úrovne registračnej fázy, úrovne autentifikačnej fázy a úrovne autentifikácie elektronických služieb verejnej správy

3.1 Kvalita identifikačnej registrácie sa rozdeľuje na štyri úrovne podľa tabuľky č. 1.

Tabuľka č. 1

Požiadavky	Kvalita identifikačnej registrácie			
	Úroveň 1	Úroveň 2	Úroveň 3	Úroveň 4
<ul style="list-style-type: none"> Fyzická prítomnosť podľa bodu 1.2.1 písm. a). Identifikačná registrácia je on-line. Kvalita preukazovania identity podľa bodu 1.2.2 písm. a) až c). Overovanie preukazovania identity podľa bodu 1.2.3 písm. a) až h). 	X			
<ul style="list-style-type: none"> Fyzická prítomnosť podľa bodu 1.2.1 písm. a). Kvalita preukazovania identity podľa bodu 1.2.2 písm. b) alebo písm. c). 		X		

⁵⁵⁾ ISO/IES 15408 Informačné technológie. Bezpečnostné techniky. Kritériá na hodnotenie bezpečnosti IT.

<ul style="list-style-type: none"> • Overovanie preukazovania identity podľa bodu 1.2.3 písm. b). 				
<ul style="list-style-type: none"> • Fyzická prítomnosť podľa bodu 1.2.1 písm. b). • Kvalita preukazovania identity podľa bodu 1.2.2 písm. b) alebo písm. c). • Overovanie preukazovania identity podľa bodu 1.2.3 písm. c) až h). 			X	
<ul style="list-style-type: none"> • Fyzická prítomnosť podľa bodu 1.2.1 písm. a). Identifikačná registrácia je on-line. • Kvalita preukazovania identity podľa bodu 1.2.2 písm. c). • Overovanie preukazovania identity podľa bodu 1.2.3 písm. d) až h). 			X	
<ul style="list-style-type: none"> • Fyzická prítomnosť podľa bodu 1.2.1 písm. b) alebo písm. c). • Kvalita preukazovania identity podľa bodu 1.2.2 písm. c). • Overovanie preukazovania identity podľa bodu 1.2.3 písm. g) alebo písm. h). 				X

3.2 Kvalita doručovania prihlasovacích údajov sa rozdeľuje na štyri úrovne podľa tabuľky č. 2.

Tabuľka č. 2

Požiadavky	Kvalita doručovania prihlasovacích údajov			
	Úroveň 1	Úroveň 2	Úroveň 3	Úroveň 4
Kvalita doručovania prihlasovacích údajov podľa bodu 1.3.1.	X			
Kvalita doručovania prihlasovacích údajov podľa bodu 1.3.2.		X		
Kvalita doručovania prihlasovacích údajov podľa bodu 1.3.3.			X	
Kvalita doručovania prihlasovacích údajov podľa bodu 1.3.4.				X

3.3 Garancie štátu pre registračnú autoritu sa rozdeľujú na štyri úrovne podľa tabuľky č. 3.

Tabuľka č. 3

Požiadavky	Garancie štátu pre registračnú autoritu			
	Úroveň 1	Úroveň 2	Úroveň 3	Úroveň 4
Garancie štátu pre registračnú autoritu podľa bodu 1.4.1.	X			
Garancie štátu pre registračnú autoritu podľa bodu 1.4.2.		X		
Garancie štátu pre registračnú autoritu podľa bodu 1.4.3.			X	
Garancie štátu pre registračnú autoritu podľa bodu 1.4.4.				X

3.4 Registračná fáza sa rozdeľuje na štyri úrovne podľa tabuľky č. 4, pričom úroveň registračnej fázy nemôže byť vyššia ako najnižšia úroveň jednej z jej častí.

Tabuľka č. 4

Požiadavky	Registračná fáza			
	Úroveň 1	Úroveň 2	Úroveň 3	Úroveň 4
Kvalita identifikačnej registrácie podľa bodu 3.1	1	2	3	4
Kvalita doručovania prihlasovacích údajov podľa bodu 3.2	1	2	3	4
Garancie štátu pre registračnú autoritu podľa bodu 3.3	1	2	3	4

3.5 Typy a robustnosť preukazovania identity sa rozdeľuje na štyri úrovne podľa tabuľky č. 5.

Tabuľka č. 5

Požiadavky	Typy a robustnosť preukazovania identity			
	Úroveň 1	Úroveň 2	Úroveň 3	Úroveň 4
Typy a robustnosť preukazovania identity podľa bodu 2.2.1.	X			

Typy a robustnosť preukazovania identity podľa bodu 2.2.2.		X		
Typy a robustnosť preukazovania identity podľa bodov 2.2.3 až 2.2.5.			X	
Typy a robustnosť preukazovania identity podľa bodu 2.2.6.				X

3.6 Bezpečnosť autentifikačného mechanizmu sa rozdeľuje na štyri úrovne podľa tabuľky č. 6.

Tabuľka č. 6

Požiadavky	Bezpečnosť autentifikačného mechanizmu			
	Úroveň 1	Úroveň 2	Úroveň 3	Úroveň 4
Bezpečnosť autentifikačného mechanizmu podľa bodu 2.3.1.	X			
Bezpečnosť autentifikačného mechanizmu podľa bodu 2.3.2.		X		
Bezpečnosť autentifikačného mechanizmu podľa bodu 2.3.3.			X	
Bezpečnosť autentifikačného mechanizmu podľa bodu 2.3.4.				X

3.7 Autentifikačná fáza sa rozdeľuje na štyri úrovne podľa tabuľky č. 7.

Tabuľka č. 7

Požiadavky	Autentifikačná fáza			
	Úroveň 1	Úroveň 2	Úroveň 3	Úroveň 4
Typy a robustnosť preukazovania identity podľa bodu 3.5.	1	2	3	4
Bezpečnosť autentifikačného mechanizmu podľa bodu 3.6.	1 až 3	1 až 3	1 až 3	4

3.8 Autentifikácia elektronických služieb verejnej správy sa rozdeľuje na štyri úrovne podľa tabuľky č. 8, pričom úroveň autentifikácie elektronických služieb verejnej správy nemôže byť vyššia ako najnižšia úroveň jednej z jej častí.

Tabuľka č. 8

		Úrovne autentifikačnej fázy			
		1	2	3	4
Úrovne registračnej fázy	1	Úroveň 1	Úroveň 1	Úroveň 1	Úroveň 1
	2	Úroveň 1	Úroveň 2	Úroveň 2	Úroveň 2
	3	Úroveň 1	Úroveň 2	Úroveň 3	Úroveň 3
	4	Úroveň 1	Úroveň 2	Úroveň 3	Úroveň 4