

Zdôvodnenie zníženia vyžadovanej úrovne zabezpečenia na prihlasovanie

1.1 Úrovně zabezpečenia stanovené európskou legislatívou eIDAS

V súlade s Nariadením 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 (ďalej len „Nariadenie eIDAS“) by mali úrovne zabezpečenia *„charakterizovať stupeň dôveryhodnosti prostriedkov elektronickej identifikácie pri určovaní totožnosti osoby, čím by poskytovali záruku, že osoba hlásiaca sa k nejakej totožnosti, je naozaj osobou, ku ktorej bola totožnosť priradená. Úroveň zabezpečenia závisí od stupňa dôveryhodnosti, ktorý poskytuje daný prostriedok elektronickej identifikácie, pokiaľ ide o údajnú alebo uvádzanú totožnosť osoby, pričom sa zohľadňujú používané procesy (napríklad preukazovanie totožnosti a overovanie a autentifikácia), riadiace činnosti (napríklad subjekt vydávajúci prostriedky elektronickej identifikácie a postup ich vydávania) a technické kontroly“*.¹

Nariadenie eIDAS obsahuje špecifikácie **troch úrovní** zabezpečenia: „**vysoká**“, „**pokročilá**“ a „**nízka**“. Pre každú z predmetných úrovní stanovuje Nariadenie eIDAS kritériá, ktoré musia byť splnené na dosiahnutie konkrétnej úrovne.

Každý členský štát vrátane Slovenskej republiky má za splnenia ostatných podmienok stanovených Nariadením eIDAS **povinnosť uznávať úroveň zabezpečenia prostriedkov elektronickej identifikácie „pokročilá“ a „vysoká“**. Táto povinnosť vyplýva z Nariadenia eIDAS a je priamo aplikovateľná a záväzná. Minimálne technické špecifikácie, normy a postupy, na základe ktorých sa stanovujú úrovne zabezpečenia, sú uvedené vo vykonávacom predpise Európskej komisie². V súlade s týmto vykonávacím predpisom sa pri určovaní úrovni zabezpečenia berie do úvahy spoľahlivosť a kvalita prihlásenia, riadenie prostriedkov elektronickej identifikácie, autentifikácia, riadenie a organizácia.

1.2 Úrovně zabezpečenia stanovené vnútroštátnou právnou úpravou v Slovenskej republike

V podmienkach Slovenskej republiky sú úrovne zabezpečenia stanovené vyhláškou Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. zo 16. marca 2020 o štandardoch pre informačné technológie verejnej správy (ďalej len „Vyhláška o štandardoch“), konkrétne jeho prílohou č. 4, ktorá stanovuje **štyri úrovne** autentifikácie elektronických služieb verejnej správy: „**Úroveň 1**“, „**Úroveň 2**“, „**Úroveň 3**“ a „**Úroveň 4**“.³

¹ Bod 16 úvodných ustanovení Nariadenia eIDAS.

² 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.

³ Je potrebné podotknúť, že Nariadenie eIDAS nekladie požiadavku zrušenia národných schém úrovní zabezpečenia.

1.3 Povinnosť vzájomného uznávania prostriedkov elektronickej identifikácie

Podľa čl. 6 ods. 1 písm. b) a c) Nariadenia eIDAS, „keď sa podľa vnútroštátneho práva alebo administratívnej praxe na prístup k službe, ktorú poskytuje subjekt verejného sektora online v jednom členskom štáte, vyžaduje elektronická identifikácia pomocou prostriedkov elektronickej identifikácie a autentifikácia, prostriedky elektronickej identifikácie vydané v inom členskom štáte sa v prvom členskom štáte uznávajú na účely cezhraničnej autentifikácie pre danú službu online, ak sú splnené tieto podmienky: úroveň zabezpečenia prostriedkov elektronickej identifikácie zodpovedá úrovni zabezpečenia, ktorá je rovnaká alebo vyššia ako úroveň zabezpečenia, ktorú vyžaduje príslušný subjekt verejného sektora na prístup k danej službe online v prvom členskom štáte, za predpokladu, že úroveň zabezpečenia daných prostriedkov elektronickej identifikácie zodpovedá úrovni zabezpečenia „pokročilá“ alebo „vysoká“ a zároveň „príslušný subjekt verejného sektora používa vo vzťahu k prístupu k danej službe online úroveň zabezpečenia „pokročilá“ alebo „vysoká“.

Vyžadovaná úroveň autentifikácie vo vzťahu k prístupu k elektronickým službám Ústredného portálu verejnej správy (ďalej len „ÚPVS“) je vedená v centrálnom metainformačnom systéme verejnej správy Slovenskej republiky (MetaIS), a to v súlade s úrovňami autentifikácie elektronických služieb verejnej správy v zmysle Výnosu Vyhlášky o štandardoch. Každý „vlastník“ príslušnej elektronickej služby je povinný určiť úroveň zabezpečenia prístupu k danej službe.

1.4 Aktuálny stav

V zmysle zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (zákon o e-Governmente) (ďalej len „zákon č. 305/2013 Z. z.“), platí pre orgány verejnej moci povinnosť používať určené spoločné moduly, medzi ktoré patrí aj autentifikačný modul. „Autentifikačný modul na základe identifikátora osoby a autentifikátora podľa § 21 ods. 1 zabezpečuje autentifikáciu osoby podľa § 19 ods. 4 na účely elektronickej komunikácie, využitie elektronickej identity osoby pre všetky prístupové miesta na účely elektronickej komunikácie a prenos informácie o overenej identite.“

V súlade s § 21 predmetného zákona, autentifikátorom je:

„a) úradný autentifikátor, ktorým sú občiansky preukaz s elektronickým čipom a bezpečnostný osobný kód podľa osobitného predpisu, alebo doklad o pobyte s elektronickým čipom a bezpečnostný osobný kód podľa osobitného predpisu,

b) alternatívny autentifikátor, ktorý ustanoví všeobecne záväzný právny predpis,

c) autentifikačný certifikát, ak ide o autentifikáciu pri prístupe k informačnému systému alebo pri elektronickej komunikácii, ktoré súvisia s výkonom verejnej moci, alebo na účely prístupu do elektronickej schránky alebo disponovania s elektronickou schránkou, a to automatizovaným spôsobom, s použitím technického prostriedku alebo programového prostriedku alebo

d) prostriedok elektronickej identifikácie vydaný v rámci schémy elektronickej identifikácie, ktorý je uvedený v zozname podľa osobitného predpisu, ak sú splnené podmienky podľa osobitného predpisu.“

Úradný autentifikátor podľa písmena a) v súčasnosti dosahuje úroveň zabezpečenia „vysoká“.

Alternatívny autentifikátor podľa písmena b) dosahuje podľa dostupných informácií úroveň zabezpečenia „vysoká“.

Autentifikačný modul pre tieto autentifikátory (úradný autentifikátor a alternatívny autentifikátor) vždy uvádza vo vydanom SAML Assertion úroveň QAA Level 4 (pozri tabuľka č. 1). Týmto autentifikátormi je možné sa prihlásiť len s použitím používateľského rozhrania portálov s využitím WebSSO.

Autentifikačný certifikát podľa písmena c) v súčasnosti dosahuje úroveň zabezpečenia nižšej ako „vysoká“, a to „pokročilá“. Autentifikačný modul na úspešnú autentifikáciu autentifikačným certifikátom vo vydanom SAML vždy uvádza úroveň QAA Level 3. Od roku 2013 sú autentifikačné certifikáty v autentifikačnom module akceptované na autentifikáciu a sú používané niekoľkými stovkami informačných systémov tretích strán integrovaných na moduly ÚPVS. Na autentifikáciu autentifikačným certifikátom sa v súčasnosti vyžaduje vytvorený VPN tunel na prístup do prostredia spoločných modulov, a to po podpise dohody o integračnom zámere, ktorú uzatvára každý integrujúci sa subjekt s Národnou agentúrou pre sieťové a elektronické služby. S využitím autentifikačných certifikátov sa počíta aj s prístupom k službám prostredníctvom mobilných aplikácií, kde sa predpokladá použitie dvojfaktorovej autentifikácie.

Prostriedky elektronickej identifikácie podľa písmena d) dosahujú úrovne zabezpečenia „nízka“, „pokročilá“, „vysoká“, v závislosti od jednotlivých **notifikovaných schém elektronickej identifikácie jednotlivých členských štátov Európskej únie**. Národný uzol eIDAS Slovenskej republiky v súčasnosti umožňuje prihlásenie týmito prostriedkami len v prípade úrovne zabezpečenia „pokročilá“ alebo „vysoká“. Služby verejného sektora dostupné použitím autentifikácie s autentifikačným certifikátom sú v zmysle Nariadenia eIDAS „služby online“, rovnako ako služby dostupné použitím autentifikácie s inými autentifikátormi. Pre všetky služby online poskytované subjektmi verejného sektora v zmysle Nariadenia eIDAS platí povinnosť uznávať všetky notifikované prostriedky elektronickej identifikácie dosahujúce úroveň zabezpečenia stanovenú príslušným vlastníkom elektronickej služby ako minimálnu na prístup k danej službe. Služby dostupné použitím autentifikačného certifikátu umožňujú používať technický alebo programový prostriedok na automatizovaný prístup. Elektronické služby, ktoré sú dostupné prostredníctvom používateľského rozhrania a autentifikácie úradným autentifikátorom, majú byť zároveň dostupné aj prostredníctvom autentifikácie autentifikačným certifikátom, a to vzhľadom na skutočnosť, že v zmysle zákona č. 305/2013 Z. z. sa elektronické podanie tvorené údajmi vyplnenými podľa elektronického formulára považuje za podané odoslaním do elektronickej schránky orgánu verejnej moci. Údaje vyplnené podľa elektronického formulára je možné odosielať z integrovaných systémov do elektronických schránok orgánov verejnej moci vo forme elektronických úradných správ prostredníctvom univerzálneho integračného rozhrania ÚPVS „UIR“, dostupného cez autentifikáciu autentifikačným certifikátom.

Z hľadiska Nariadenia eIDAS je podľa vyššie uvedeného pri prístupe k elektronickým službám v súčasnosti uznávaná aj úroveň „pokročilá“. V prípade autentifikácie prostredníctvom ÚPVS (t. j. prostredníctvom používateľského rozhrania) však nie je úroveň „pokročilá“ akceptovaná.

Tabuľka 1: Hodnoty QAA Level vo vydanom potvrdení o autentifikácii z autentifikačného modulu - IAM ÚPVS (v SAML tokene)

HODNOTA QAA LEVEL V SAML	TEXTOVÁ REPREZENTÁCIA	ÚROVEŇ
4	Prihlásenie eID kartou alebo zahraničným prostriedkom elektronickej identifikácie podľa Nariadenia EP a Rady 910/2014 (eIDAS) s úrovňou zabezpečenia (Level of Assurance) „vysoká“ (high)	Vysoká
3	Prihlásenie pomocou autentifikačného certifikátu alebo zahraničným prostriedkom elektronickej identifikácie podľa Nariadenia EP a Rady 910/2014 (eIDAS) s úrovňou zabezpečenia (Level of Assurance) „pokročilá“ (substantial)	Pokročilá
2	Prihlásenie prihlasovacím menom a dodatočne overenie GRID kartou	Nízka
1	Prihlásenie prihlasovacím menom alebo cez sociálnu sieť	Nízka

1.5 Zníženie minimálnej úrovne zabezpečenia prístupu k elektronickým službám ÚPVS

Elektronické podania sa v používateľskom prostredí ústredného portálu verejnej správy vyplňajú prostredníctvom konštruktora správy na ÚPVS, pričom nastavenie minimálnej vyžadovanej úrovne zabezpečenia je v súčasnosti možné výlučne globálne pre všetky elektronické podania (s triedou správ EGOV_APPLICATION) a nie je pri dnešnom technickom riešení možné nastaviť pre rôzne elektronické podania odlišnú minimálnu úroveň zabezpečenia. Na vyplňanie podaní na ÚPVS je aktuálne vyžadovaná úroveň „vysoká“, čím sa znemožňuje elektronické podanie držiteľom prostriedkov elektronickej identifikácie s úrovňou zabezpečenia „pokročilá“.

Služba všeobecného podania (formulár „všeobecná agenda“) má podľa MetaIS určenú úroveň č. 3, ktorá je ekvivalentná úrovni „pokročilá“. V skutočnosti sa však v konštruktore správy na ÚPVS v súčasnosti vyžaduje úroveň „vysoká“, vzhľadom na nastavenú úroveň zabezpečenia pre triedu správ EGOV_APPLICATION.

V súčasnosti platí povinnosť uznávania prostriedkov elektronickej identifikácie s úrovňou zabezpečenia „pokročilá“ z nasledujúcich štátov Európskej únie, ktoré svoje prostriedky notifikovali v zmysle Nariadenia eIDAS:

- Taliansko - od septembra 2019,
- Holandsko - od septembra 2020 (posun termínu zo strany Holandska na 2. polrok 2021),
- Lotyšsko - od decembra 2020,
- Dánsko – najneskôr od apríla 2021.

V súčasnosti platí povinnosť uznávania prostriedkov elektronickej identifikácie s úrovňou zabezpečenia „vysoká“ z nasledujúcich štátov EÚ:

- Nemecko – od septembra 2018,
- Estónsko – od októbra 2019,
- Chorvátsko – od októbra 2019,
- Luxembursko – od októbra 2019,
- Španielsko – od októbra 2019,
- Belgicko – od decembra 2019,

- Portugalsko – od februára 2020,
- Česká republika – od septembra 2020,
- Taliansko – od septembra 2020,
- Holandsko – od septembra 2020,
- Lotyšsko – od decembra 2020,
- Litva – najneskôr od augusta 2021.

Vzhľadom na vyššie uvedené je potrebné realizovať zníženie vyžadovanej minimálnej úrovne zabezpečenia prostriedkov elektronickej identifikácie pre elektronické služby poskytované cez grafické používateľské rozhranie na ÚPVS a podania vyplňané v konštruktoch správ na ÚPVS (používané pre elektronické podania rôznych orgánov verejnej moci) z úrovne číslo 4 na úroveň číslo 3.