(Návrh)

**Legislatívny zámer zmien v autorizácii**

**elektronickej úradnej komunikácie**

Obsah

[1. Sledované ciele 3](#_Toc33427716)

[2. Platná právna úprava a dôvody jej zmeny 5](#_Toc33427717)

[2.1. Platná právna úprava 5](#_Toc33427718)

[2.2. Dôvody zmeny právnej úpravy 8](#_Toc33427719)

[3. Obsah zmien právnej úpravy 9](#_Toc33427720)

[3.1. Zákon č. 305/2013 Z.z. 9](#_Toc33427721)

[3.1.1. Legislatívny prístup 9](#_Toc33427722)

[3.1.2. Kritériá pre spôsoby autorizácie 9](#_Toc33427723)

[3.1.3. Posudzovanie splnenia kritérií 11](#_Toc33427724)

[3.1.4. Používanie jednotlivých spôsobov autorizácie 12](#_Toc33427725)

[3.1.5. Spôsoby autorizácie priamo zo zákona 13](#_Toc33427726)

[3.2. Vykonávací predpis k zákonu č. 305/2013 Z.z. 14](#_Toc33427727)

[3.3. Štandardy podľa zákona č. 95/2019 Z.z. 14](#_Toc33427728)

[3.4. Účinnosť 15](#_Toc33427729)

# **Sledované ciele**

Autorizácia elektronických podaní je základným nástrojom na využívanie elektronickej úradnej komunikácie, keďže predstavuje vyjadrenie súhlasu s obsahom úkonu, napr. podania a jeho podaním príslušnému orgánu verejnej moci. Inými slovami, ide o nevyhnutný, častokrát prvý krok na to, aby bolo možné využívať elektronickú službu štátu.

Na rozdiel od listinného spôsobu komunikácie, ktorý napriek rozmanitosti spôsobov listinného doručovania je vo svojej podstate stále rovnaký a viazaný na fyzický a v podstate vždy papierový nosič informácie, v elektronickej úradnej komunikácii je ťažké, ak nie nemožné pomenovať uzatvorenú skupinu spôsobov, akými sa bude vykonávať. Oblasť spôsobov autorizácie v kyberpriestore je jedna z najviac sa rozvíjajúcich v súčasnosti, a preto týchto spôsobov bude do budúcnosti pribúdať, či už ide o mobilné spôsoby komunikácie, používanie aplikácií tretích strán alebo automatizovanú komunikáciu system-system.

Platí tiež, že v oblasti elektronickej komunikácie v súkromno-právnych vzťahoch je elektronické prejavovanie vôle s obsahom a vykonaním právneho úkonu bežné a je realizované rôznymi spôsobmi, s rôznymi úrovňami záruk, pokiaľ ide o identitu konajúceho,  ochranu obsahu právneho úkonu, ako aj zabezpečenie nepopierateľnosti vykonania právneho úkonu. Ide pritom o právne úkony v rozmanitých vzťahoch, od potvrdzovania doručenia zásielok, cez komunikáciu s dodávateľmi služieb až po prevody finančných prostriedkov. Nie vždy, resp. v málo prípadoch sa pri týchto úkonoch využívajú „inštitucionalizované“ (t.j. legislatívne definované a štandardizované) riešenia pokročilých, či kvalifikovaných elektronických podpisov, práve naopak, škála používaných nástrojov je pomerne pestrá a z právneho hľadiska nepožívajúca fikciu zachovania písomnej formy právneho úkonu, ale opierajúca sa o „vyvrátiteľnú domnienku“ zachytenia obsahu úkonu a identifikácie konajúceho.

To, čo pri dnešnom využívaní prejavu vôle elektronickými prostriedkami prevláda je dostupnosť a jednoduchosť zvoleného nástroja a vyhodnotenie rizika jeho zneužitia, ako aj vyhodnotenie poskytovaných záruk vo väzbe na charakter a dôležitosť úkonu, ktorý sa týmto spôsobom vykonáva, resp. s ktorého obsahom a vykonaním sa vyjadruje súhlas.

Pre elektronickú úradnú komunikáciu je naopak typický konzervatívny prístup k autorizácii, ktorý sa prejavuje najmä v taxatívnom vymenovaní prípustných spôsobov autorizácie a tiež priradenie jednotlivých týchto spôsobov taxatívne vymenovaným spôsobom autorizácie v listinnom prostredí - k vlastnoručnému podpisu alebo k vlastnoručnému podpisu, ktorý je úradne osvedčený. Inými slovami, množina nástrojov na autorizáciu v elektronickej úradnej komunikácii je v súčasnom stave typicky uzavretá a neposkytuje priestor pre rozlišovanie medzi jednotlivými nástrojmi z pohľadu dôležitosti samotného úkonu.

Základnými cieľmi, ktoré sa zmenou právnej úpravy sledujú, sú

* otvorenie možnosti autorizácie elektronických podaní do budúcnosti novým, najmä mobilným spôsobom autorizácie, čo primárne znamená, že v rámci štátu (v jeho vnútornom priestore) bude upravený spôsob na vytvorenie flexibilného prostredia pre využívanie inovatívnych spôsobov autorizácie v úradnej elektronickej komunikácii (pričom z pohľadu interoperability si štát zachová konzervatívny prístup),
* postaviť úrovne autorizácie na poskytovaných bezpečnostných zárukách a neviazať ich na jednu konkrétnu technológiu, napr. elektronický podpis, resp. kvalifikovaný elektronický podpis,
* získať nástroje na autorizáciu, ktoré sú v ideálnom prípade nezávislé od použitého spôsobu, platformy, z ktorej prebieha elektronická úradná komunikácia,
* dať možnosť rozlišovať pri autorizácii aj z pohľadu dôležitosti daného úkonu a
* vytvoriť priestor pre využívanie princípu dostupnosti a jednoduchosti nástrojov na autorizáciu.

# **Platná právna úprava a dôvody jej zmeny**

# **Platná právna úprava**

Zákon č. 305/2013 Z.z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov (ďalej len „zákon č. 305/2013 Z.z.“) definuje autorizáciu v § 3 písm. o) ako „*vyjadrenie súhlasu s obsahom právneho úkonu a s vykonaním tohto právneho úkonu*”.

Jednotlivé spôsoby autorizácie ustanovuje § 23 ods. 1 zákona č. 305/2013 Z.z., pričom základným delením medzi týmito spôsobmi je delenie z pohľadu subjektu, ktorý autorizáciu vykonáva, a to na (i) autorizáciu elektronického podania alebo elektronického úradného dokumentu orgánom verejnej moci pri výkone verejnej moci a (ii) autorizáciu elektronického podania osobou, ktorá nie je orgánom verejnej moci.

Podľa § 26 ods. 4 zákona č. 305/2013 Z.z., ak je niektorá z obsahových náležitostí elektronického úradného dokumentu viazaná na listinnú podobu, považuje sa táto náležitosť za splnenú autorizovaním elektronického úradného dokumentu. Podľa § 23 ods. 1 zákona č. 305/2013 Z.z. orgány verejnej moci autorizujú elektronické podanie alebo elektronický úradný dokument dvomi možnými spôsobmi, a to (i) kvalifikovaným elektronickým podpisom vyhotoveným s použitím mandátneho certifikátu alebo (ii) kvalifikovanou elektronickou pečaťou, pričom v oboch prípadoch pripájajú kvalifikovanú elektronickú časovú pečiatku.

Mandátnym certifikátom je kvalifikovaný certifikát pre elektronický podpis vydaný fyzickej osobe oprávnenej zo zákona alebo na základe zákona konať za inú osobu alebo orgán verejnej moci alebo v ich mene, alebo fyzickej osobe, ktorá vykonáva činnosť podľa osobitného predpisu, alebo vykonáva funkciu podľa osobitného predpisu. Inými slovami, mandátny certifikát slúži na vyhotovenie kvalifikovaného elektronického podpisu a zároveň na preukázanie, že podpisujúci buď koná za alebo v mene orgánu verejnej moci, sám je orgánom verejnej moci (napr. notár, exekútor) alebo zastáva funkciu v orgáne verejnej moci (napr. sudca, prokurátor).

Z uvedeného vyplýva, že ak sa vyhotovuje elektronický úradný dokument, ktorého obsahové náležitosti sú z povahy veci viazané na listinnú podobu (typicky ide najmä o odtlačok pečiatky alebo o vlastnoručný podpis), môže orgán verejnej moci „nahradiť“ tieto obsahové náležitosti autorizáciou - kvalifikovaným elektronickým podpisom s použitím mandátneho certifikátu, ako aj kvalifikovanou elektronickou pečaťou.

Voľbu medzi použitím kvalifikovaného elektronického podpisu s mandátnym certifikátom a kvalifikovanej elektronickej pečate následne ovplyvňujú najmä ustanovenia osobitných zákonov, upravujúce náležitosti úradného dokumentu. Pre voľbu spôsobu autorizácie je podstatným najmä to, na akú osobu je (v tomto prípade) spôsob vyjadrenia vôle orgánu verejnej moci podľa osobitných predpisov viazaný. Voľba medzi podpisom a pečaťou je regulovaná pravidlom podľa § 23 ods. 3 zákona č. 305/2013 Z.z., podľa ktorého výlučne kvalifikovaný elektronický podpis sa používa vždy v prípadoch, kedy ide o autorizáciu, pri ktorej zákon vyžaduje prejav vôle konkrétnej osoby alebo osoby v konkrétnom postavení. V ostatných prípadoch má orgán verejnej moci na výber, či použije kvalifikovaný elektronický podpis alebo kvalifikovanú elektronickú pečať.

 Kvalifikovaný elektronický podpis, rovnako ako kvalifikovaná elektronická časová pečiatka sú regulované 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“) a sú štandardizované na úrovni vykonávacích rozhodnutí Komisie (EÚ), najmä vykonávacím rozhodnutím Komisie (EÚ) 2015/1506 z 8. septembra 2015.

Kvalifikovaná elektronická pečať je z hľadiska náležitostí regulovaná rovnako vyššie uvedenými právnymi predpismi na úrovni EÚ, pričom jej použitie na účely autorizácie (ako kvázi ekvivalentu kvalifikovaného elektronického podpisu) je upravené len na národnej úrovni, vo vzťahu k elektronickej úradnej komunikácii práve § 23 ods. 1 zákona č. 305/2013 Z.z.

Osoby, ktoré nie sú orgánom verejnej moci, majú autorizáciu upravenú odlišne. V prvom rade pre ne neplatí pravidlo § 23 ods. 3 zákona č. 305/2013 Z.z. o voľbe medzi kvalifikovaným elektronickým podpisom a kvalifikovanou elektronickou pečaťou vo väzbe na osobu, ktorá elektronické podanie autorizuje. Následne zákon č. 305/2013 Z.z. rozdeľuje spôsoby autorizácie podľa „váhy podpisu“ na tie, ktoré predstavujú „elektronickú alternatívu“ k úradne osvedčenému podpisu a tie, ktoré buď predstavujú alternatívu k vlastnoručnému podpisu alebo sú použiteľné vždy, ak ide o elektronické podanie a osobitný predpis neustanovuje inak.

Inými slovami, vo vzťahu k osobám, ktoré nie sú orgánom verejnej moci je autorizácia upravená ako elektronický ekvivalent pre prípady, kedy osobitný predpis ustanovuje použitie vlastnoručného podpisu (či už osvedčeného alebo nie) a tiež ako *lex generalis* pre všetky prípady, kedy sa podľa osobitného predpisu umožňuje podanie elektronického podania.

Elektronickým ekvivalentom úradne osvedčeného vlastnoručného podpisu je podľa § 23 ods. 1 písm. b) zákona č. 305/2013 Z.z. kvalifikovaný elektronický podpis, ktorého kvalifikovaný certifikát obsahuje minimálny súbor osobných identifikačných údajov reprezentujúcich jedinečným spôsobom fyzickú osobu podľa osobitného predpisu, a ktorý zahrnul do autorizácie aj kvalifikovanú elektronickú časovú pečiatku, ktorá určuje dátum a čas, po ktorom nastala autorizácia. Inými slovami musí byť použitý kvalifikovaný elektronický podpis, certifikát použitý na jeho vytvorenie musí obsahovať jedinečné identifikačné znaky a kvalifikovaná elektronická časová pečiatka musí byť zahrnutá do autorizácie. Kvalifikovanú elektronickú pečať nie je na tento účel možné použiť.

Vlastnoručný podpis, ktorý nevyžaduje úradné osvedčenie, má na účel elektronického podania ustanovené štyri možnosti autorizácie – (i) kvalifikovaný elektronický podpis, (ii) kvalifikovaná elektronická pečať (napr. ak autorizuje právnická osoba), (ii) tzv. podpis klikom a (iv) uznaný spôsob autorizácie. Tieto spôsoby je rovnako možné použiť tam, kde osobitný predpis ustanovuje možnosť elektronického podania a neustanovuje iný, resp. jeden konkrétny spôsob jeho autorizácie.

Z uvedeného vyplýva, že súčasný legislatívny priestor pre zavedenie rôznych, v zákone konkrétne nepomenovaných spôsobov vyjadrenia vôle na úrovni vlastnoručného podpisu, je daný v zákone č. 305/2013 Z.z. ustanovením o (i) tzv. „podpise klikom“ podľa § 23 ods. 1 písm. a) druhého bodu alebo (ii) uznanom spôsobe autorizácie podľa § 23 ods. 1 písm. a) tretieho bodu a ods. 2, keďže tak kvalifikovaný elektronický podpis, ako aj kvalifikovaná elektronická pečať sú konkrétne pomenovanými spôsobmi autorizácie, reprezentujúcimi konkrétne a štandardizované riešenie, hoc aj voľne dostupné od rôznych poskytovateľov kvalifikovaných dôveryhodných služieb.

Uznaný spôsob autorizácie môže ustanoviť vykonávací predpis a zákon č. 305/2013 Z.z. ustanovuje len jeho všeobecné náležitosti – teda, že zabezpečuje (i) spoľahlivú identifikáciu osoby, ktorá autorizáciu vykonala, (ii) spoľahlivé zachytenie obsahu právneho úkonu, ktorý autorizovala, ako aj (iii) zhodu medzi autorizovaným právnym úkonom a právnym úkonom, ktorý osoba autorizovala.

Vykonávací predpis, ustanovujúci uznané spôsoby autorizácie dnes nie je vydaný.

Pokiaľ ide o tzv. podpis klikom, ustanovenie § 23 ods. 1 písm. a) druhého bodu zákona č. 305/2013 Z.z. upravuje všeobecné podmienky, ktoré musí spĺňať – (i) vyhotovuje sa s použitím na to určenej funkcie informačného systému prístupového miesta, (ii) vyžaduje úspešnú autentifikáciu osoby ktorá autorizáciu vykonáva, zodpovedajúcej najmenej úrovni zabezpečenia „pokročilá“ podľa nariadenia eIDAS, (iii) musí byť zabezpečené uvedenie podpisujúcej osoby ako odosielateľa elektronickej správy s autorizovaným dokumentom, (iv) musí byť zabezpečená nemennosť obsahu autorizovaného dokumentu do momentu uloženia v elektronickej schránke adresáta, a (v) musí byť zabezpečené spojenie autorizovaného dokumentu s identifikátorom osoby odosielateľa a zachovanie väzby medzi nimi. Tzv. podpis klikom je možné použiť vždy, ak to osobitný predpis nezakazuje.

Z hľadiska podmienky vyhotovovania prostredníctvom určenej funkcie prístupového miesta platí, že samotný tzv. podpis klikom musí byť vytváraný v podmienkach prístupového miesta. Inými slovami, má byť implementovaný v rámci prístupového miesta. Ide z povahy veci primárne o tri prístupové miesta – ústredný portál verejnej správy (ďalej len „ÚPVS“), špecializovaný portál a integrované obslužné miesto (ďalej len „IOM“) – keďže funkcie ústredného kontaktného centra nie sú zamerané na elektronickú komunikáciu smerom k orgánu verejnej moci (aj keď nie je vylúčené jeho použitie napr. pri autorizácii nahlasovaného technického problému).

Ustanovením tejto podmienky sa sledujú dva hlavné ciele – (i) odbremeniť užívateľa služby od potreby vynakladania osobitných nákladov ma obstaranie si a udržiavanie spôsobu autorizácie a (ii) zveriť vytvorenie a kontrolu nad spôsobom autorizácie „do rúk štátu“ s tým, aby nebola potrebná žiadna ďalšia regulácia konkrétnych technických podrobností s tým spojených (ako by to bolo v prípade „otvorenia“ Podpisu klikom pre akéhokoľvek poskytovateľa). Svojim spôsobom teda išlo primárne o snahu vybudovať centralizovaný komponent na podpisovanie najmä na ÚPVS a v druhom rade dať túto možnosť aj pre konkrétne agendové systémy.

Podmienka autentifikácie najmenej na úrovni „pokročilá“ odkazuje na podmienky, vymedzené čl. 8 ods. 2 písm. c) a súvisiacimi článkami nariadenia eIDAS. Z hľadiska zákona č. 305/2013 Z.z. je dôležité, že úspešná autentifikácia je podmienkou autorizácie v zmysle, že musí byť „viazaná“ k autorizácii. Inými slovami, musí ísť o autentifikáciu, ktorej jediným dôvodom je s tým spojená autorizácia konkrétneho elektronického podania. Z tohto pohľadu je teda podmienka splnená, ak po tom, ako užívateľ zvolí dokument, ktorý chce autorizovať, musí absolvovať úspešnú autentifikáciu, ktorej bezprostredným „následkom“ je autorizácia dokumentu.

Uvedenie autorizujúcej osoby ako odosielateľa elektronickej správy súvisí s podmienkou zviazania identity odosielateľa s autorizovaným dokumentom a vytvorením väzby medzi nimi. Dôvod je zrejmý, ide o deklarovanie identity autorizujúcej osoby vo vzťahu k autorizovanému dokumentu. Ďalšou podmienkou, ktorá z týchto náležitostí vyplýva je, že takýto spôsob autorizácie nie je možné využiť v prípadoch, kedy je autorizujúca osoba odlišná od odosielateľa správy – alebo presnejšie povedané od osoby, ktorá je ako odosielateľ správy uvedená.

Zákon nepredpisuje konkrétne technologické riešenie na vytvorenie väzby medzi dokumentom a informáciou o identite toho, kto ho autorizoval. Dôležité je len to, že takáto väzba bude existovať a bude „nepochybná“ a určujúca identitu autorizujúcej osoby.

Poslednou podmienkou je zabezpečenie nemennosti obsahu autorizovaného dokumentu, pričom zákon túto podmienku vyžaduje splniť minimálne do doby uloženia v elektronickej schránke adresáta. Napriek tomu, že sa v náležitostiach tzv. podpisu klikom uvádza elektronická schránka adresáta je potrebné upozorniť na to, že tzv. podpis klikom je autorizáciou a teda separátnym, oddeleným úkonom od doručovania. Inými slovami, nejde o jeden a ten istý úkon, rovnako ako nejde o úkony podmienené. Alebo ešte inak, tzv. podpis klikom môže spĺňať zákonné náležitosti aj v prípade ak k odoslaniu autorizovaného dokumentu nikdy nedôjde, alebo ak s ním bude naložené iným spôsobom, ako doručením do elektronickej schránky adresáta. Ide totiž o podmienku, ktorá je kladená na „kvalitu“ tzv. podpisu klikom a nie o podmienku alebo náležitosť jeho použitia.

Zákon nepredpisuje konkrétne technologické riešenie tzv. podpisu klikom, z čoho vyplýva, že podstatným pre posúdenie splnenia náležitostí tzv. podpisu klikom je posúdenie splnenia podmienok podľa § 23 ods. 1 písm. a) druhého bodu zákona č. 305/2013 Z.z.. Z technologického hľadiska je teda možností realizácie niekoľko, vrátane využitia už existujúcich a štandardizovaných riešení, akými sú aj elektronické podpisy podľa nariadenia eIDAS – zákon tomuto žiadnym spôsobom nebráni.

Dôvod, pre ktorý sa venuje taký priestor tzv. podpisu klikom je ten, že ide de facto o jediné dnes v zákone upravené riešenie, ktoré je použiteľné na autorizáciu a zároveň je technologicky neutrálne v zmysle, že je na jeho vytvorenie možné použiť rôzne a viaceré postupy a nástroje a neodkazuje na konkrétne, resp. konkrétnym spôsobom štandardizované riešenie. Je teda možné konštatovať, že spĺňa cieľ priniesť flexibilitu a inovatívnosť pre riešenia a spôsoby autorizácie, ktoré má štát pod kontrolou a zároveň dodržuje konzervatívny prístup pre interoperabilitu a pre riešenia, ktoré štát pod kontrolou nemá.

# **Dôvody zmeny právnej úpravy**

Dôvod zmeny existujúcej právnej úpravy spočíva v snahe dosiahnuť ciele, popísané v prvej časti tohto dokumentu. Ak sa má dosiahnuť otvorenosť spôsobov autorizácie do budúcnosti a umožniť väčší priestor pre voľbu jednotlivých spôsobov autorizácie vo väzbe na dôležitosť úkonu, potom dnešný spôsob úpravy autorizácie musí byť nahradený novým, keďže ide o zmenu vo filozofii právnej úpravy.

Zmenou právnej úpravy, popísanou v tretej časti tohto dokumentu dôjde k vytvoreniu priestoru na zapojenie tak existujúcich, ako aj budúcich nástrojov autorizácie do elektronických služieb e-Governmentu a dôjde k rozšíreniu možnosti využitia nástrojov, ktoré sa dnes používajú v súkromnoprávnych vzťahoch a na ktoré sú ich používatelia zvyknutí. Zároveň, keďže právna úprava nebude popisovať konkrétne technické riešenia, nebude potrebná žiadna jej úprava na to, aby sa (aj nové) nástroje autorizácie v budúcnosti do elektronických služieb zapojili.

# **Obsah zmien právnej úpravy**

# **Zákon č. 305/2013 Z.z.**

# Legislatívny prístup

Z hľadiska spôsobu úpravy sa navrhuje ustanoviť v zákone č. 305/2013 Z.z. (i) kritériá, ktoré sa budú pri spôsoboch autorizácie posudzovať, (ii) príslušný orgán a spôsob, akým sa splnenie kritérií bude posudzovať, (iii) pravidlá pre publikáciu a používanie jednotlivých spôsobov autorizácie, (iv) spôsoby autorizácie, ktoré sú zo zákona zaradené do jednotlivých kategórií a (v) splnomocňovacie ustanovenie pre úpravu podrobností.

Z hľadiska podrobností sa predpokladá vydanie vykonávacieho právneho predpisu k zákonu č. 305/2013 Z.z. a premietnutie nového prístupu k autorizácii aj do štandardov pre informačné technológie verejnej správy podľa zákona č. 95/2019 Z.z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 95/2019 Z.z.“).

# Kritériá pre spôsoby autorizácie

Spôsob autorizácie predstavuje kombináciu technických, procedurálnych a organizačných opatrení (v ľubovoľnej kombinácii), prostredníctvom ktorých je vlastná autorizácia vykonávaná.

Jednotlivé spôsoby autorizácie a z toho vyplývajúce úrovne autorizácie sa navrhuje posudzovať z hľadiska splnenia štyroch kritérií, ktorými sú (i) nespochybniteľnosť úkonu, (ii) identifikácia konajúceho, (iii) integrita úkonu a (iv) čas vykonania úkonu.

Nižšie uvádzame ku každému z týchto kritérií príklad ich posúdenia vo väzbe na prostriedky autorizácie podľa nariadenia eIDAS, pričom samozrejme nepôjde o výlučný spôsob posudzovania.

Kritériá podľa nariadenia eIDAS sa budú aplikovať na prostriedky autorizácie týmto nariadením regulované – teda elektronické podpisy, elektronické pečate a elektronické časové pečiatky. Tento postup je potrebný okrem iného aj na zabezpečenie plnenia záväzkov Slovenskej republiky vo vzťahu k interoperabilite (aj) prostriedkov autorizácie, ktoré nariadenie eIDAS reguluje.

Iné spôsoby autorizácie budú posudzované na základe autonómnych kritérií, ustanovených zákonom č. 305/2013 Z.z., resp. v podrobnostiach vykonávacím predpisom k nemu a budú vychádzať zo všeobecne akceptovaných štandardov a uznaných technických noriem v tejto oblasti. Formulovanie autonómnych kritérií je nevyhnutné najmä z dôvodu, že spôsobom autorizácie nemusí byť prostriedok regulovaný nariadením eIDAS a môže ísť o spôsoby, ktoré formálnu reguláciu právnym predpisom nemajú, resp. majú vo vzťahu k vymedzenej oblasti úkonov (napr. finančné služby), napriek tomu sú však na trhu používané a sú všeobecne akceptované a spôsobilé dosiahnuť (aj) najvyššie úrovne autorizácie.

Nespochybniteľnosťou úkonu sa rozumie stav, kedy spôsob autorizácie (použité nástroje) umožňujú vo vysokej miere dôverovať tomu, že autorizáciu konkrétneho úkonu bolo možné vykonať len pod kontrolou osoby, ktorá je identifikovaná ako autorizujúca osoba a len vo vzťahu k úkonu, ktorý bol autorizovaný. To je možné dosiahnuť napríklad tým, že

* osoba má pod svojou výlučnou kontrolou údaje alebo prostriedky, ktorými sa autorizácia vykonáva, tieto sú dôverne chránené pred inými osobami a sú jedinečné pre osobu, ktorá autorizáciu vykonala alebo
* bola použitá kombinovaná metóda založená na „vysokej pravdepodobnosti, že osoba má pod svojou kontrolou údaje alebo prostriedky” a súčasne na tom, že „sa dá overiť, že úkon inicializuje naozaj daná osoba”.

Pri splnení tohto kritéria bude daný spôsob autorizácie osobe, ktorá ho použila, zaručovať to, že autorizácia úkonu nebude spochybniteľná bez toho, aby sa nepreukázalo, že v konkrétnom prípade bola kontrola tejto osoby nad autorizáciou zmarená alebo obmedzená.

Možné hodnoty tohto kritéria budú (i) áno – danú vlastnosť spôsob autorizácie zabezpečuje alebo (ii) nie – danú vlastnosť spôsob autorizácie nezabezpečuje, resp. nezabezpečuje spôsobom, ktorému je možné vo vysokej miere dôverovať.

Ak pôjde o spôsob autorizácie

* podľa nariadenia eIDAS, bude toto kritérium splnené napr. ak osoba údaje na vykonanie autorizácie uchováva na kvalifikovanom zariadení na vyhotovovanie kvalifikovaného elektronického podpisu podľa nariadenia eIDAS a toto zariadenie používa na vykonanie autorizácie,
* regulovaný z hľadiska podmienok nespochybniteľnosti úkonu v inom právnom predpise, použijú sa kritériá podľa tohto právneho predpisu,
* neregulovaný z hľadiska nespochybniteľnosti úkonu žiadnym predpisom, použijú sa autonómne kritériá ustanovené zákonom č. 305/2013 Z.z., resp. v podrobnostiach vykonávacím predpisom k nemu.

Identifikáciou konajúceho je stav, kedy na základe údajov o identite, ktoré z autorizovaného úkonu vyplývajú, je stotožnenie s osobou deklarovanej identity nespochybniteľné (vysoká úroveň), do vysokej miery nespochybniteľné (pokročilá úroveň), alebo do istej miery nespochybniteľné (nízka úroveň). Toto kritérium bude hovoriť o tom, v akej miere (i) bola vykonaná identifikácia osoby pri zriadení, vzniku či registrácii osoby k danému spôsobu autorizácie, ako aj o tom, (ii) v akej miere je možné spoľahnúť sa na to, že údaje o identite tejto osoby, ktoré z autorizovaného úkonu vyplývajú, neboli zmenené.

Ak pôjde o spôsob autorizácie

* podľa nariadenia eIDAS, budú jednotlivé úrovne považované za splnené pri splnení podmienok, kladených na úroveň vysoká, pokročilá a nízka podľa čl. 8 nariadenia eIDAS. Z tohto pohľadu potom úroveň vysoká bude splnená pri použití kvalifikovaného elektronického podpisu alebo zdokonaleného elektronického podpisu založeného na kvalifikovanom certifikáte, úroveň pokročilá pri použití zdokonaleného elektronického podpisu založeného na certifikáte, ktorý nie je kvalifikovaný a úroveň nízka pri použití elektronického podpisu, ktorý spĺňa iba požiadavky článku 3 bod 10 nariadenia eIDAS,
* regulovaný z hľadiska podmienok identifikácie konajúceho v inom právnom predpise, použijú sa kritériá podľa tohto právneho predpisu,
* neregulovaný z hľadiska podmienok identifikácie konajúceho žiadnym predpisom, použijú sa autonómne kritériá ustanovené zákonom č. 305/2013 Z.z., resp. v podrobnostiach vykonávacím predpisom k nemu.

Zabezpečením integrity úkonu sa bude rozumieť stav, kedy je zabezpečené, že obsah právneho úkonu po autorizácii nie je možné meniť bez toho, aby sa dalo zistiť, že k zmene došlo alebo mohlo dôjsť. Posudzuje sa teda skutočnosť, či je autorizácia prepojená s obsahom autorizovaného úkonu (elektronickým dokumentom) takým spôsobom, že každú dodatočnú zmenu obsahu úkonu po vykonaní autorizácie možno zistiť.

Možné hodnoty tohto kritéria budú (i) áno – danú vlastnosť spôsob autorizácie zabezpečuje alebo (ii) nie – danú vlastnosť spôsob autorizácie nezabezpečuje, resp. nezabezpečuje spôsobom, ktorému je možné vo vysokej miere dôverovať.

Ak pôjde o spôsob autorizácie

* podľa nariadenia eIDAS, bude toto kritérium splnené napr. ak sa použije zdokonalený elektronický podpis, kde vlastná technológia PKI umožňuje priamo identifikovať zmenu podpísaného obsahu,
* regulovaný z hľadiska podmienok zabezpečenia integrity v inom právnom predpise, použijú sa kritériá podľa tohto právneho predpisu,
* neregulovaný z hľadiska podmienok zabezpečenia integrity žiadnym predpisom, použijú sa autonómne kritériá ustanovené zákonom č. 305/2013 Z.z., resp. v podrobnostiach vykonávacím predpisom k nemu.

Časom vykonania úkonu je známy čas, kedy bol úkon autorizovaný, resp. čas, pred ktorým určite bola autorizácia úkonu vykonaná a tento čas je známy z dôveryhodného zdroja, ktorý je založený na presnom zdroji času, prepojenom s koordinovaným svetovým časom.

Možné hodnoty tohto kritéria budú (i) áno – danú vlastnosť spôsob autorizácie zabezpečuje alebo (ii) nie – danú vlastnosť spôsob autorizácie nezabezpečuje, resp. nezabezpečuje spôsobom, ktorému je možné vo vysokej miere dôverovať.

Ak pôjde o spôsob autorizácie

* podľa nariadenia eIDAS, bude toto kritérium splnené napr. ak pôjde o použitie kvalifikovanej elektronickej časovej pečiatky,
* regulovaný z hľadiska zabezpečenia uvedenia času vykonania úkonu v inom právnom predpise, použijú sa kritériá podľa tohto právneho predpisu,
* neregulovaný z hľadiska zabezpečenia uvedenia času vykonania úkonu žiadnym predpisom, použijú sa autonómne kritériá ustanovené zákonom č. 305/2013 Z.z., resp. v podrobnostiach vykonávacím predpisom k nemu.

Podľa splnenia jednotlivých kritérií bude spôsobu autorizácie priradená úroveň autorizácie nasledovne:

|  |  |
| --- | --- |
|  | Podmienky na dosiahnutie úrovne v závislosti od splnenia kritérií |
| Názov úrovne | Nespochybniteľnosť úkonu | Identifikácia konajúceho | Integrita úkonu | Čas vykonania úkonu |
| Osvedčená | Áno | Vysoká | Áno | Áno |
| Kvalifikovaná | Áno | Vysoká | Áno | Nie |
| Dôveryhodná | Nie | Vysoká | Áno | Nie |
| Pokročilá | Nie | Pokročilá | Áno | Nie |
| Nízka | Nie | Nízka | Áno | Nie |

# Posudzovanie splnenia kritérií

Posúdenie, či spôsob autorizácie spĺňa kritériá vo vyššie uvedených štyroch oblastiach bude zabezpečovať Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu (ďalej len „Úrad“), keďže ide o ústredný orgán štátnej správy v oblasti informatizácie a ústredný orgán pre podsektor informačných systémov verejnej správy v oblasti kybernetickej bezpečnosti, pričom splnenie kritérií spôsobov autorizácie bude posudzované v zásadnej miere z pohľadu ich bezpečnosti a dopadov na informačné technológie verejnej správy.

Posudzovanie sa bude vykonávať na žiadosť osoby, ktorá spôsob autorizácie prevádzkuje, resp. poskytuje alebo na žiadosť orgánu verejnej moci, ktorý ho má záujem používať. Obsahom, resp. prílohou žiadosti bude aj podrobný popis spôsobu autorizácie, jeho bezpečnostných charakteristík a spôsob naplnenia bezpečnostných záruk pre autorizáciu a jeho navrhovaného začlenenia a spôsobu používania v procesoch e-Governmentu.

Predmetom posudzovania bude splnenie podmienok, ustanovených pre jednotlivé kritériá v zákone č. 305/2013 Z.z. (a v podrobnostiach vo vykonávacom predpise), ako aj splnenia podmienok, súvisiacich s autorizáciou a v podrobnostiach ustanovených v štandardoch podľa zákona č. 95/2019 Z.z. Posudzovať sa bude aj praktický dopad zavedenia spôsobu autorizácie do procesov e-Governmentu. Inými slovami, bude sa skúmať v prvom rade splnenie kritérií kladených na samotný spôsob autorizácie, ako aj jeho súlad s podmienkami, ktoré sa na autorizáciu v procesoch elektronického výkonu verejnej moci kladú a tiež to, aké konkrétne opatrenia na strane orgánov verejnej moci by si vyžiadalo jeho zavedenie do praxe.

Pri posudzovaní každého spôsobu autorizácie je splnenie podmienok ustanovených pre jednotlivé kritériá len jednou z podmienok potrebných na to, aby bol takýto spôsob na účely autorizácie použiteľný - ide o posúdenie, ktoré sa týka spôsobu samotného. Rovnako dôležité však bude posúdenie toho, aké dopady by implementácia takéhoto spôsobu do praxe vyvolala – či už potreba implementácie na strane prístupového miesta vo vzťahu k vykonávaniu autorizácie alebo potreba implementácie zmien na strane elektronických podateľní vo vzťahu k prijímaniu a ďalšiemu spracovaniu autorizovaných dokumentov.

Z uvedených dôvodov nebude existovať právny nárok na zavedenie spôsobu autorizácie do procesov e-Governmentu, pričom dôvodom na nezavedenie bude môcť byť práve potenciálny dopad na strane informačných systémov orgánov verejnej moci, ktorý bude musieť byť odôvodnený.

Proces posudzovania bude upravený podobne, ako pri zápise do evidencie vládnych cloudových služieb podľa § 10a zákona č. 305/2013 Z.z. a na tento proces sa nebude vzťahovať Správny poriadok.

Výsledkom posúdenia bude záver Úradu o zaradení spôsobu autorizácie do jednej z vyššie uvedených skupín a o možnosti jeho použitia na účely autorizácie podľa zákona č. 305/2013 Z.z. bude zápis do evidencie spôsobov autorizácie.

Predpokladá sa vytvorenie centrálnej evidencie spôsobov autorizácie, ktorú bude v elektronickej podobe viesť Úrad a ktorej obsahom budú jednotlivé spôsoby autorizácie, spolu s popisom všetkých skutočností, potrebných na ich používanie.

# Používanie jednotlivých spôsobov autorizácie

Úprava používania spôsobov autorizácie bude postavená na troch základných princípoch.

Prvým z nich princíp výberu, ktorý bude náležať vždy orgánu verejnej moci. Z úrovní autorizácie podľa vyššie uvedenej tabuľky si bude orgán verejnej moci môcť zvoliť úroveň autorizácie, ktorá pre jednotlivé elektronické konania pred ním (teda pre „jeho elektronické služby“) bude použiteľná. Táto voľba sa prakticky vykoná podobne, ako sa dnes vykonáva voľba úrovne autentifikácie – teda priradením príznaku pre každú služby v evidencii elektronických služieb.

Vychádza sa z toho, že orgán verejnej moci, ktorý konanie vykonáva a má danú oblasť, agendu v kompetencii vie pre každé konanie, resp. úkon v ňom posúdiť takpovediac mieru dôvery, ktorú nevyhnutne potrebuje mať vo vzťahu k použitej úrovni autorizácie. Zákon nebude predpisovať orgánom verejnej moci kritériá, ktoré pri výbere majú zohľadniť – to bude na posúdení každého jedného orgánu.

Ďalším bude pravidlo použiteľnosti všetkých spôsobov autorizácie, zapísaných pre zvolenú úroveň v evidencii spôsobov autorizácie a všetky spôsoby autorizácie, zapísané v evidencii pre všetky vyššie úrovne autorizácie. Inými slovami, ak si orgán verejnej moci pre konkrétnu službu určí úroveň autorizácie „pokročilá“, budú môcť byť elektronické podania v danej službe autorizované všetkými zapísanými spôsobmi autorizácie pre úrovne pokročilá, dôveryhodná, kvalifikovaná a osvedčená.

Posledným princípom je rešpektovanie konaní, ktoré nemajú osobitnú úpravu pre elektronické podania, resp. majú explicitnú úpravu spôsobu autorizácie.

Keďže náležitosti podaní pre mnohé konania sú dnes ešte stále ustanovené vo väzbe na listinnú podobu a teda označené len ako „vlastnoručný podpis“ a nie všeobecným pojmom „autorizácia“, je potrebné zákonom ustanoviť, ktoré úrovne autorizácie budú zodpovedať vlastnoručnému podpisu. Uvedené bude zároveň znamenať, že v takýchto prípadoch orgán verejnej moci nebude môcť zvoliť nižšiu úroveň, než najnižšiu z tých, ktoré zodpovedajú úrovni vlastnoručného podpisu. Navrhuje sa túto minimálnu úroveň ustanoviť na úroveň „Dôveryhodná“.

Obdobná situácia je v niektorých prípadoch, kedy osobitný predpis výslovne pomenúva spôsob autorizácie. Zákon č. 305/2013 Z.z. v dnešnej úprave § 23 ods. 1 písm. a) umožňuje použitie spôsobu autorizácie, ustanoveného osobitným predpisom. Vychádza to z princípu všeobecnosti úpravy zákona č. 305/2013 Z.z. a (v tomto prípade) prednosti úpravy osobitných prepisov, ako úpravy špeciálnej. Tento princíp po prijatí novej právnej úpravy stratí na všeobecnej úrovni zmysel, avšak pre tie typy konaní, kde osobitný predpis (špeciálna úprava) striktne ustanovuje použitie napríklad kvalifikovaného elektronického podpisu bude ustanovené pravidlo, že túto podmienku autorizácie je možné splniť aj iným spôsobom tej istej úrovne, alebo vyššej úrovne autorizácie.

# Spôsoby autorizácie priamo zo zákona

Vzhľadom na to, že dnes najčastejšie používané spôsoby autorizácie bude potrebné a vhodné zachovať a tiež vzhľadom na to, že ide o štandardizované riešenia, v súlade s nariadením eIDAS, ktorých poskytovanie je regulované ako kvalifikovaná dôveryhodná služba, budú tieto prostriedky priamo zo zákona zaradené do konkrétnych kategórií a následne publikované v evidencii spôsobov autorizácie.

Pôjde o (i) kvalifikovaný elektronický podpis, (ii) kvalifikovanú elektronickú pečať a (iii) kvalifikovanú elektronickú časovú pečiatku, s nimi používanú.

Rovnaký princíp, teda zápis spôsobu autorizácie do evidencie priamo zo zákona, bude uplatnený pre všetky spôsoby autorizácie podľa zákona č. 305/2013 Z.z., používané podľa právnych predpisov, účinných ku dňu prijatie navrhovaných zmien a budú zaradené do príslušnej úrovne autorizácie. Tento proces bude prebiehať na základe žiadosti toho subjektu ktorý daný spôsob autorizácie prevádzkuje.

# **Vykonávací predpis k zákonu č. 305/2013 Z.z.**

Obsahom vykonávacieho predpisu budú podrobnosti o (i) podmienkach kladených na splnenie jednotlivých kritérií spôsobu autorizácie a (ii) o žiadosti na posúdenie spôsobu autorizácie, vrátane podrobností o spôsobe opisu spôsobu a jeho použitia.

Na účely posúdenia nespochybniteľnosti úkonu sa vyhodnocuje miera kontroly osoby identifikovanej ako autorizujúcej nad spôsobom, ktorým sa autorizácia vykonáva, resp. spôsob preukázania vôle osoby identifikovanej ako autorizujúcej vykonať autorizáciou konkrétneho obsahu. Prostriedky a postupy, ktoré zabezpečia preukázateľnosť vôle autorizujúcej osoby vykonať autorizáciu konkrétneho obsahu sú spôsobilé preukázať bezpečnostnú garanciu nespochybniteľnosti.

Pokiaľ ide o identifikáciu konajúcej osoby, splnenie podmienok pre jednotlivé úrovne bude posudzované vo vzťahu k spôsobu, akým je spôsob autorizácie spojený s identitou osoby, ktorá ním vyjadruje svoju vôľu a do akej miery je takto deklarovaná identita dôveryhodná, najmä z hľadiska jedinečnosti a ochrany pred zneužitím.

Podmienky pre úrovne vysoká, pokročilá a nízka budú považované za splnené v prvom rade vždy vtedy, ak bude identita osoby určená s použitím prostriedku, ktorý spĺňa náležitosti úrovne zabezpečenia pre príslušnú úroveň podľa čl. 8 ods. 2 nariadenia eIDAS. Dôvodom je príprava na budúce zladenie úrovní autentifikácie ustanovených slovenským právnym poriadkom pre informačné technológie verejnej správy s úpravou tej istej oblasti v nariadení eIDAS.

Okrem toho bude dosiahnutie jednotlivých úrovní identifikácie osoby možné aj bez väzby na splnenie všetkých podmienok podľa nariadenia eIDAS, avšak len v špecifických prípadoch, najmä ak pôjde o identifikáciu osoby spôsobom, ktorý je výlučne pod kontrolou orgánu verejnej moci.

Integrita úkonu je jediným kritériom, ktoré musí byť splnené pre každú úroveň autorizácie a jej posúdenie. Posudzovanie garancie zabezpečenia integrity spočíva v preukázaní identifikácie každej zmeny obsahu autorizovaného úkonu po jeho autorizácii.

Kritérium uvedenia času bude viazané na získanie informácie o čase z dôveryhodného zdroja. Musí byť preukázané, že uvedenie času v autorizovanom úkone je spojené s vlastným úkonom, uvedená čas je presný a jeho poskytovanie a začlenenie do autorizácie je dôveryhodné.

# **Štandardy podľa zákona č. 95/2019 Z.z.**

Podľa dnešného právneho stavu je štandardom vlastností elektronických služieb aj ich rozdelenie podľa úrovní autentifikácie a ich označenie príslušnou úrovňou autentifikácie [§ 47 písm. d) a e) výnosu č. 55/2014 Z.z. v znení neskorších predpisov]. Rovnako tak je štandardom aj zaregistrovanie elektronickej služby v centrálnom metainformačnom systéme [§ 47 písm. h) výnosu č. 55/2014 Z.z. v znení neskorších predpisov].

V nadväznosti na zmeny v právnej úprave budú doplnené aj uvedené štandardy vlastností elektronických služieb o rozdelenie podľa úrovní autorizácie a označenie príslušnou úrovňou. Týmto spôsobom sa zabezpečí previazanie úrovne autorizácie a elektronickej služby rovnakým spôsobom, ako je to dnes zabezpečené vo vzťahu k autentifikácii.

# **Účinnosť**

Účinnosť zmien sa predpokladá koncom roka 2020.