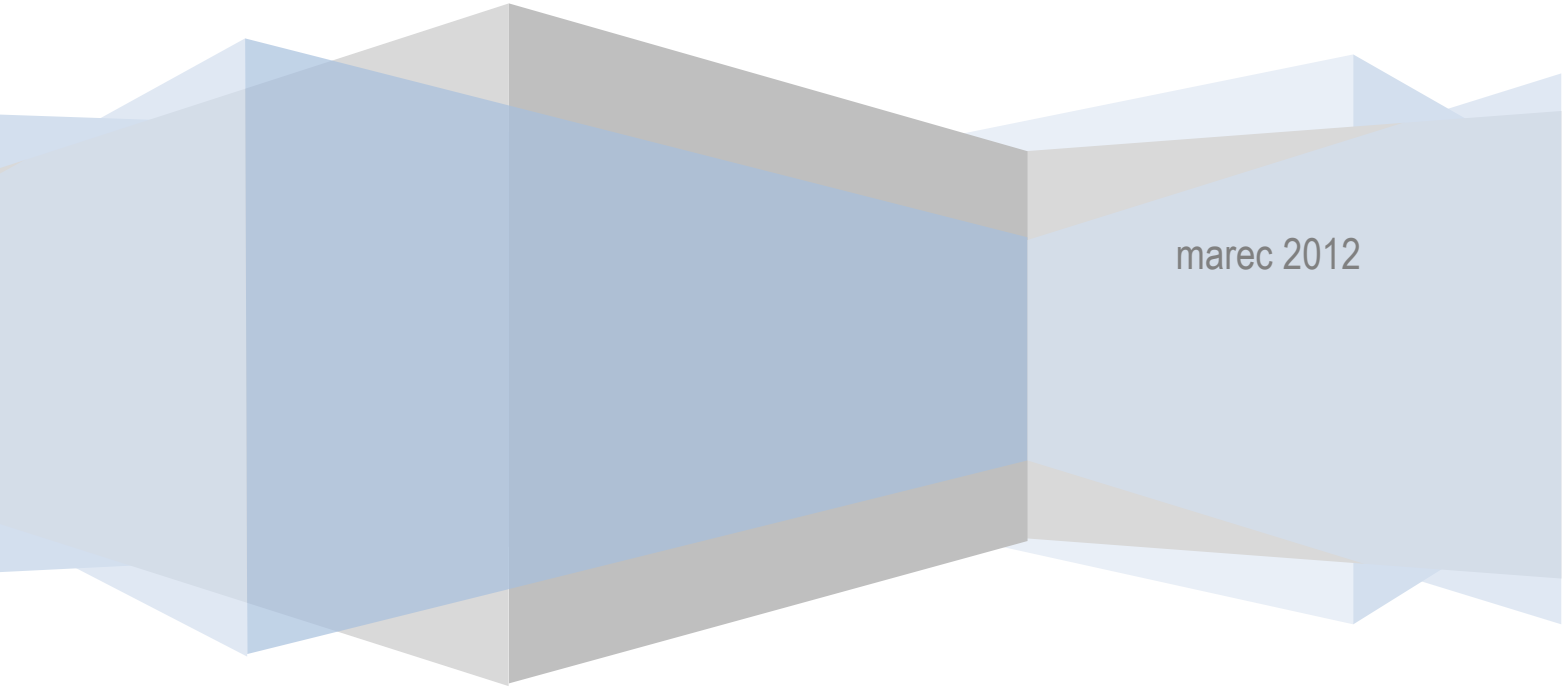
MF SR, Sekcia informatizácie spoločnosti

Návrh strategického smerovania eID pre SR

Analýza vývoja a trendov v oblasti elektronickej identity a návrh strategického smerovania pre SR v oblasti elektronickej autentifikácie.

pracovná verzia 3.0



marec 2012

Obsah

Úvod

Zmeny v spoločnosti vyvolané vývojom technológií sú bezprecedentné. Rozsah používania internetu a elektronických prostriedkov v bežnom živote človeka je z roka na rok väčší. Využívanie internetu a kybernetického priestoru pre najbežnejšie činnosti človeka ako je komunikácia, zábava, nakupovanie, učenie sa či práca tvorí stále významnejšiu časť života. Digitálny svet neprináša len výhody, ale sú s ním spojené aj značné riziká. Tak ako stúpa hodnota informácie, stúpa aj miera rizika spojeného so zneužitím informácií a elektronických prostriedkov. Jedným z najvýznamnejších faktorov napomáhajúcich rozvoju elektronického prostredia je dôvera. Kľúčom k dôvere sú nielen samotné dôveryhodné a bezpečné technológie ale aj identita účastníka.

Dôveryhodná elektronická identita predstavuje kľúč k rozvinutiu potenciálu digitálneho priestoru. Zároveň je aj podmienkou pre realizáciu mnohých, doteraz neuskutočňovaných transakcií, spôsobov komunikácie, či práce. Tak ako je v hmatateľnom svete dôveryhodnosť účastníka komunikácie, či zmluvnej strany postavená na jeho identite, tak je tomu aj v elektronickom svete. Vo fyzickom svete je identita overiteľná pohľadom na človeka, prípadne potvrdením identity prostredníctvom dokladov. V elektronickom svete je paralela s fyzickým svetom dôležitá. Obdobne ako vo fyzickom svete, je potrebné vedieť identifikovať protistranu a mať dôveru v jej rozpoznanie. Dôležitosť vyplýva z jednoduchého faktu, a to uvedomenia si, že aktivita v elektronickom svete má svoj dopad v reálnom svete. Elektronický prevod peňazí zníži reálny zostatok na účte. Nákup v elektronickom svete vedie k vyskladneniu fyzického tovaru.

Elektronická identita, t.j. identita fyzického človeka v kybernetickom priestore je jeho prenesením do digitálneho sveta s reálnymi dopadmi. Preto, aby toto prenesenie malo svoju váhu a zmysel, je potrebné definovať princípy, prostredníctvom ktorých bude elektronická identita rovnoprávnym obrazom fyzického človeka v kyberpriestore.

Riešenie elektronickej identity má široký dopad na spoločnosť a prináša so sebou celý rad výhod. Verejná správa bude profitovať zo zvýšenej dôveryhodnosti pri zabezpečení elektronickej komunikácie, zo zjednodušenia administratívnych procesov. To všetko za výraznej úspory finančných prostriedkov, ktoré by boli inak vynakladané na vývoj a prevádzku vlastných riešení jednotlivých rezortov. Prínosy pre občanov sú rovnako významné, zahŕňajú zjednodušenie vzájomnej interakcie s verejnou správou, úsporu času, zvýšenú mieru ochrany súkromia a bezpečnosti.

Neexistuje všeobecný model elektronickej identity, ktorý by sa dal aplikovať nezávisle od národného kontextu. Prístupy k vytvoreniu a riadeniu elektronickej identity sú do veľkej miery závislé od kultúrneho a historického vývoja danej krajiny a nedajú sa jednoducho kopírovať. Taktiež nie je realistické snažiť sa pokryť národnou stratégiou eID všetky oblasti a všetky výzvy v rovnakej miere komplexnosti a s rovnakou prioritou. Je potrebné hľadať rovnováhu medzi krátkodobými cieľmi s maximálnym dopadom a širšími prioritami v národnom aj EÚ kontexte.

Existencia národného poňatia elektronickej identity umožní zapojenie sa do cezhraničného riešenia eID čo prinesie celý rad dodatočných výhod. Cezhraničné riešenie eID umožní nové spôsoby interakcie občanov, podnikateľov a verejnej správy v dôveryhodnom a bezpečnom prostredí, podstatným spôsobom zvýši počet dostupných elektronických služieb pre občanov a podnikateľov a prispeje k rozvoju jednotného trhu a vzniku nových biznis modelov. Dosiahnutie cezhraničnej interoperability v oblasti elektronickej identity je ambiciózny cieľ blízkej budúcnosti a na ceste k nemu leží mnoho prekážok v technologickej, politickej, právnej, ekonomickej , koncepčnej aj organizačnej oblasti. V súčasnosti rozbehnuté aktivity na politickej úrovni v rámci plnenia cieľov iniciatívy Digitálna agenda pre Európu a technologickej úrovni (STORK[7]) jasne indikujú potrebu urýchlene sa zaoberať národným riešením elektronickej identity.

Cieľom tohto dokumentu je priblížiť riešenie elektronickej identity z pohľadu stratégií, odporúčaní a platnej či pripravovanej legislatívy Európskej komisie a medzinárodných inštitúcií. Zároveň bude analyzovaná východisková situácia v oblasti elektronickej identity v Slovenskej republike a navrhnuté strategické smerovanie v oblasti elektronickej autentifikácie pre Ministerstvo financií SR tak, aby bolo kompatibilné s riešeniami, ktoré sú pripravované na úrovni EÚ.

Stratégia eID v kontexte EÚ

Politiky podporujúce stratégiu eID

Bezpečná online správa elektronických identít a spoľahlivá autentifikácia sú základom väčšiny národných stratégií v oblasti eID. Analýza riešení národných stratégií[1] krajín Európskej únie a OECD potvrdila, že každá krajina vyvíja vlastnú stratégiu a implementačnú politiku, ktorá reflektuje národný štýl, kultúru a zaužívaný postup pri tradičnej - papierovej forme správy identít. Všetky krajiny automatizujú a migrujú existujúce procesy riadenia identít a neuvažujú nad cestou vytvárania či zavádzania úplne nových procesov vhodnejších digitálny svet. Neexistuje žiadny všeobecný model elektronickej identity, ktorý by sa dal aplikovať nezávisle od národného kontextu. Z analýzy riešení národných eID stratégií však výrazne vystupuje do popredia niekoľko kľúčových trendov, ktoré sa všeobecne dajú zaradiť k politikám podporujúcim eID. Niektoré z nich sú v súčasnosti aktívne rozvíjané a niektoré patria viac k nastupujúcim trendom s predpokladanou realizáciou v dlhodobejšom horizonte.

Registračná politika

Registráciou sa vytvára puto viažuce osobu a jej elektronickú identitu. Zvolená registračná politika vychádza z historického vývoja a je do veľkej miery ovplyvnená spôsobom registrácie používaným pri offline interakcii občanov s verejnou správou. Taktiež odráža mieru autonómnosti jednotlivých úrovní verejnej správy. Najčastejším prípadom je centralizovaná registračná politika vo všeobecnosti založená na tradícii registra obyvateľov a jednotného identifikátora osoby. V krajinách, kde sa tieto z historického kontextu nevyvinuli, sa uplatňuje model podporujúci podstatne väčšiu autonómnosť jednotlivých zložiek verejnej správy, ktoré majú často vlastné registračné politiky. Tieto sú následne koordinované pomocou federatívnych dohôd umožňujúcich interoperabilitu prostriedkov elektronickej identifikácie (credentials). Zavedenie jednotného prihlásenia, pri ktorom zadá používateľ do systému svoju totožnosť iba raz a tým získa prístup k ďalším službám a aplikáciám bez nutnosti opätovnej identifikácie tzv. single sign-on využíva na svojich národných eGovernment portáloch väčšina krajín OECD (napr. Rakúsko, Holandsko, Kanada, Dánsko). Naopak výnimkou sú krajiny ako USA alebo Nemecko, ktoré nezvažujú zavedenie single sign-on riešenia z dôvodu možného zneužitia, resp. nedostatočnej ochrany súkromia (osobné údaje z elektronickej autentifikácie nemôžu byť automaticky zasielané tretím stranám).

Politika získania a používania prostriedkov elektronickej identifikácie.

Získavanie prostriedkov elektronickej identifikácie môže byť buď povinné alebo založené na dobrovoľnej báze, pričom tieto môžu byť rôzneho charakteru a technologickej vyspelosti. Typickým je kombinácia diskrétnych informácií, napríklad kombinácia mena a hesla, alebo autentifikačných predmetov na dôveryhodnom nosiči, napríklad na čipovej karte. Práve umiestnenie prostriedkov pre autentifikáciu na čipovú kartu vydávanú namiesto papierovej identifikačnej karty je jednou z najrozvíjanejších metód. Krajiny, ktoré majú historicky danú tradíciu povinných papierových identifikačných kariet všeobecne migrujú týmto smerom aj svoju online politiku. Používanie elektronických identifikačných kariet býva v tomto prípade taktiež povinné, čo významným spôsobom uľahčuje a urýchľuje ich penetráciu a využívanie v elektronických službách. V iných krajinách, kde je získanie identifikačných kariet, prípadne iných prostriedkov elektronickej identifikácie dobrovoľné, vlády rôznymi spôsobmi podporujú alebo si vyžadujú ich použitie občanmi alebo poskytovateľmi služieb. Napriek tomu rozšírenie elektronických identifikačných kariet býva pomalé.

So zvyšujúcim sa počtom on-line služieb sa úmerne zvyšuje aj počet eID systémov a rastie ich zložitosť. Koncoví používatelia tak musia vytvárať a spravovať veľký počet prostriedkov elektronickej identifikácie. Za účelom zjednodušenia prístupu sa väčšina krajín zameriava na znižovanie počtu digitálnych kľúčov a prostriedkov elektronickej identifikácie pre používateľov pri interakciách s vládou. Výzvou je tiež dostupnosť „rozšíreného“ autentifikačného nástroja tzv. tokenu ako reprezentanta potvrdenej identity, t.j. overenej s využitím prostriedkov elektronickej identifikácie. V súčasnosti, kedy sa vyžaduje dvojfázová autentifikácia, musí mať používateľ token pre každý prostriedok elektronickej identifikácie (napr. kreditnú kartu pre každý účet, cestovný pas, vodičský preukaz či preukaz poistenca). Táto situácia nastáva z dôvodu nedostatku interoperability medzi schémami elektronickej identity a je nekomfortná pre užívateľov a neefektívna pre trhy. Budúcnosťou by mohla byť dostupnosť „rozšíreného“ tokenu, ktorý by konsolidoval existujúce tokeny alebo čítačky/PIN technológie a navyše

[1] National Strategies and Policies for Digital Identity Management in OECD Countries (DSTI/ICCP/REG(2010)3/final), The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies (JRC Scientific and Technical Reports, 2010), Towards a Trusted and Sustainable European Federated eID system (EC study, 2011)

ponúkal užívateľom dodatočné funkcionality. Je vysoko pravdepodobné, že najmä finančné inštitúcie budú chcieť skresať počet vydávaných kariet s cieľom znížiť finančné náklady. Na technickej úrovni existujú inovatívne riešenia: napr. EMV[2] schéma, ktorá je schopná pracovať s viacerými účtami na jednom tokene alebo EMUE[3] prístup, ktorý integruje čítačky kariet s kartami tak, že čítačka PINu je integrovaná do karty, ktorá môže obsahovať desať rôznych prostriedkov elektronickej identifikácie.

Primárne sú eID riešenia s využitím prostriedkov elektronickej identifikácie zamerané na využívanie v elektronických službách verejnej správy. Zatiaľ, čo niektoré krajiny len plánujú využitie prostriedkov elektronickej identifikácie aj pre súkromný sektor, veľa ďalších už nasadzuje univerzálny prístup prostriedkov elektronickej identifikácie pre oba, verejný aj súkromný kontext. Dobrým príkladom je Rakúsko, kde je „karta občana" vyvinutá a ponúkaná súkromnými aj verejnými subjektmi pre transakcie vo verejnom aj súkromnom sektore. Iným príkladom univerzálneho verejno /privátneho prístupu je portugalská stratégia kde je single sign on služba rozšírená aj na služby súkromného sektora[4]. V dlhodobom horizonte sa predpokladá, že vlády budú akceptovať privátne komerčné prostriedky elektronickej identifikácie, ale tiež že národné prostriedky elektronickej identifikácie budú využívané aj pre online služby súkromného sektora.

Politika interoperability

Národná interoperabilita v rámci verejného sektora býva riešená prostredníctvom národného autentifikačného rámca, alebo národného rámca interoperability. Krajiny uznávajú kľúčovú úlohu technických noriem a štandardov najmä s ohľadom na bezpečnostné aspekty, a podporujú hlavne tie najviac rozšírené. Úroveň interoperability, ktorú môžu národné politiky stanoviť, je ovplyvnená najmä samotnou registračnou politikou. Napríklad v krajine s decentralizovanou registračnou politikou (ako Kanada) je interoperabilita podporovaná v rámci dohôd federácie. Spoločné ciele sú popísané nezávisle od možných technických riešení a organizácie sú autonómne v tom, akými technickými prostriedkami stanovený ciel dosiahnu. V krajinách s centralizovanou registračnou politikou je možné stanoviť prísnejšie pravidlá. Napríklad rakúska vláda vyvíja a poskytuje open source softvérové moduly k zjednodušeniu vývoja služieb kompatibilných s národnou občianskou kartou. Krajiny, ktoré podporujú využívanie PKI všeobecne podporujú PKI interoperabilitu pomocou vytvorenia právneho rámca, kontrolných mechanizmov a štandardov. Zatiaľ len málo krajín vo svojich eID stratégiách sústreďuje svoj záujem na konkrétne riešenia v oblasti cezhraničnej interoperability elektronických služieb (viď. kapitola Cezhraničná interoperabilita elektronickej identity).

Bezpečnostná politika

Bezpečnostná politika týkajúca sa špecificky elektronickej identity väčšinou vychádza z širšieho kontextu národnej politiky informačnej bezpečnosti a nebýva riešená samostatne. V mnohých prípadoch sa bezpečnosť elektronickej identity umelo zveličuje, čím sa opodstatňujú veľké počiatočné náklady na implementáciu národného riešenia eID, ktoré ako také nemá perspektívu finančnej návratnosti. Nebezpečenstvo tohto prístupu spočíva v pridaní nadbytočných bezpečnostných prvkov, ktoré nakoniec prispejú k obmedzenej miere rozšírenia eID riešenia a tiež interoperability.

V otázke bezpečnosti väčšina krajín OECD implementuje politiku založenú na využívaní PKI (infraštruktúry verejného kľúča) a legislatívny rámec pre elektronický podpis. Krajiny, ktoré historicky nepoužívajú národnú kartu identity (občiansky preukaz) vyvíjajú alternatívne postupy pre zavedenie prostriedkov elektronickej identifikácie. Príkladom je Švédsko, ktoré má dlhú tradíciu v offline overovaní totožnosti pomocou bankových prostriedkov elektronickej identifikácie a preto ich digitálna správa elektronickej identity iba jednoducho rozširuje túto zásadu. Banky vybrané prostredníctvom verejných obstarávaní poskytujú PKI certifikáty občanom.

Politika ochrany súkromia

Hlavným nástrojom na ochranu súkromia je aplikácia existujúceho právneho rámca. V rámci Európskej únie je problematika ochrany súkromia a ochrany osobných údajov riešená vo viacerých právne záväzných aktoch (viď. kapitola „Odporúčania, nariadenia a záväzky na úrovni EÚ ovplyvňujúce rámec eID"), ktoré členské štáty prevzali do svojej legislatívy. Významná je úloha úradov na ochranu osobných údajov, ako sprievodcov pri zavádzaní eID.

---

[2] www.emvco.com

3 http://www.emue.com/site/home.htm

[4] Ide o proces, v ktorom užívateľ zadá, alebo uvedie do systému svoju totožnosť iba raz a tým získa prístup k službám bez toho, aby bolo nutné identifikovať sa každému zdroju a používať niekoľko rôznych prístupových hesiel.

Niektoré krajiny používajú pri zavádzaní eID systémov v elektronickej verejnej správe tzv. posúdenie dopadu na ochranu súkromia (Privacy Impact Assessments). Väčšina krajín sa tiež prikláňa k poskytovaniu minimálneho množstva údajov potrebných pre identifikáciu entity. Krajiny s centralizovanou registračnou politikou založenou na tradícii registra obyvateľov, jednotného identifikátora osoby a väčšinou aj identifikačných kariet čelia špecifickým výzvam. Napríklad ochranu pred použitím identifikátora na účely nepovoleného spárovania identity voči rôznym registrom riešia najčastejšie zavedením sektorovo orientovaných identifikátorov osoby. Často je ochrana riešená technickými opatreniami (tzv. prístup „privacy by design"), ktoré zvyšujú dôveru a akceptáciu eID riešenia. Mnohé krajiny zaviedli, prípadne zvažujú zavedenie notifikácie o narušení osobných údajov, ako spôsob k zvýšeniu povedomia o ochrane súkromia a osobných údajov.

Politika spolupráce so súkromným sektorom

Trh s eID produktmi a službami je veľmi dynamický, existujúce a novo vznikajúce technológie poskytujú priestor na vytváranie nových aplikácií a partnerstiev. Nastáva posun v dôraze od základnej eID technológie k službám s vysokou pridanou hodnotou napr. marketingové databázy, online platby. Banky a mobilní operátori, môžu zohrať dôležitú úlohu ako poskytovatelia online služieb ktoré využívajú dôveryhodné eID. Ak raz začnú využívať existujúce dôveryhodné eID, môžu sa sústrediť na hlavný predmet svojej činnosti a poskytovať služby s vyššou pridanou hodnotou pre svojich zákazníkov. Je dôležité, aby verejný sektor umožnil ľahké, rýchle pripojenie komerčných poskytovateľov elektronických služieb k eID infraštruktúre. V krátkodobom horizonte sa predpokladá, že technológie eID sa všeobecne budú vyvíjať smerom k praktickejšiemu využitiu a to pomocou ich komercializácie. Narastajúcim trendom je využitie zjednotených eID technológií (napr. SUN/Oracle s Liberty Alliance) v medzi podnikových aplikáciách. Ako dôvera v technológie rastie, sú konkurenční poskytovatelia tradične viac ochotní spoliehať sa na vzájomne na svoje prostriedky elektronickej identifikácie.

Využitie alternatívnych autentifikačných kanálov, napr. mobilných technológií, môže pomôcť v podpore eID interoperability, bezpečnosti a k výhodnosti z pohľadu užívateľa. Rozšírenie využitia interoperabilných digitálnych certifikátov je závislé na úzkej spolupráci štandardizačných orgánov z oblasti telekomunikácií a mobilných operátorov. Krajiny ako Belgicko a Estónsko, ktoré do svojich národných eID schém zakomponovali prenositeľnosť (portability) identity, v súčasnej dobe profitujú zo zabudovaných certifikátov v mobilných zariadeniach. Nasledujúcim štádiom bude plná integrácia certifikátu do SIM karty. Týmto sa umožní vysoká úroveň autentifikácie mobilného zariadenia, a tým aj jeho vlastníka, vhodná pre aplikácie v oblasti elektronického bankovníctva, elektronického hlasovania, elektronického zdravotníctva a iných služieb. Naviac, prenositeľné prostriedky elektronickej identifikácie na mobilných tokenoch redukujú riziko krádeže identity (nie je tu centralizované úložisko osobných údajov vzťahujúcich sa k identite). V dlhodobom horizonte bude trh s eID riešeniami pravdepodobne najviac ovplyvnený virtualizáciou služieb a cloud computing, pričom virtualizácia dátových centier, infraštruktúry, procesov je vnímaná ako úvodné štádium pre prechod na cloud computing. Tento trend okrem predpokladaných pozitív v úsporách nákladov prinesie ďalšie nároky na zabezpečenie bezpečnosti a integrity údajov, prípadne nové postupy riadenia a licenčné modely.

Cezhraničná interoperabilita elektronickej identity

Dostupnosť cezhraničného riešenia elektronickej identity zatiaľ existuje ako vízia, ktorá umožní občanom bezpečne pristupovať a využívať služby nezávisle na čase a mieste či krajine kde sa nachádzajú. Taktiež by mala vytvoriť podmienky pre spustenie nových komerčne využiteľných elektronických služieb, ktoré podporia jednotný európsky trh.

Na scéne existuje mnoho rôznych organizácií ponúkajúcich riešenia online služieb, ktoré využívajú určitú formu elektronickej identity na identifikovanie koncového používateľa. Či už sa jedná o verejnú správu s národnými riešeniami eID, ktorá poskytuje elektronické služby pre občanov aj podnikateľov, alebo sa jedná o rôznorodé riešenia súkromného sektora využívajúce elektronickú identitu (najčastejšie banky a obchodníci ponúkajúci tovar online). Naviac, v krajinách existujú rôzne spôsoby, akými sú k eID riešeniam priradené úrovne zabezpečenia (assurance levels). Len čo sa však zameriame na cezhraničné využitie elektronických služieb, ktoré sú založené na elektronickej identite, narazíme na veľké problémy. Väčšina týchto služieb cezhranične nefunguje vôbec, prípadne vyžaduje prekonať rôzne administratívne či technické prekážky. Používateľ naviac čelí riziku ohrozenia súkromia a identity, nakoľko nie je jasná úroveň dôveryhodnosti a spoľahlivosti autentifikačného riešenia ani úroveň zabezpečenia ochrany užívateľovho súkromia. Na úrovni EÚ zatiaľ chýba štandardizovaný interoperabilný rámec eID, ktorý by ponúkol riešenie dôveryhodného online prístupu k elektronickým službám tak pre verejnú

správu, ako aj pre komerčný sektor. Aktivity na úrovni EÚ však už v tejto oblasti prebiehajú. Jedná sa najmä o prvé základné legislatívne riešenia (napr. Smernica o elektronickom podpise, Smernica o službách) a tiež o ďalšie aktivity, v súčasnosti zatiaľ najmä na úrovni konzultácií, štúdií, akčných plánov, s cieľom pripraviť primeraný legislatívny rámec umožňujúci federatívny európsky rámec eID. Viac o aktivitách na úrovni EÚ sa nachádza v kapitole Odporúčania, nariadenia a záväzky na úrovni EÚ ovplyvňujúce rámec eID.

V súčasnosti môžeme sledovať tendenciu pristupovať k interoperabilite elektronickej identity z pohľadu autentifikačného mechanizmu[5]. Interoperabilita v tomto význame zahŕňa hlavne možnosť používať autentifikačný systém jednej krajiny na prístup k aplikácii v inej krajine. Autentifikácia v tomto prípade znamená overenie elektronickej identity používateľa, ktorá je tvorená súborom informácii o entite a identifikátorom, ktorý jednoznačne reprezentuje tento set informácii.

V krajinách existujú rôzne spôsoby, akými sú k eID riešeniam priradené úrovne zabezpečenia. Niektoré krajiny majú štyri úrovne zabezpečenia a iné len dve, pričom úrovne sú stanovené rôznym spôsobom. Sú krajiny ktoré preferujú klasifikáciu úrovní zabezpečenia založenú na spôsobe autentifikácie (elektronickými kartami s využitím PKI, softwarovými certifikátmi, menom/heslom) iné sledujú prítomnosť či absenciu určitého kroku v procese autentifikácie. Výsledkom je realita, kedy napríklad tretej úrovni zabezpečenia zodpovedá v jednej krajine autentifikácia softvérovým certifikátom doručeným cez internet bez fyzického overenia identity (bez nutnosti osobnej návštevy príslušnej autority) a v inej krajine tejto úrovni zodpovedá kombinácia mena/hesla zaslaná na oficiálnu poštovú adresu.

Aj keď tieto úrovne navzájom nekorešpondujú, je reálne stanoviť referenčný rámec autentifikácie voči ktorému môžu byť jednotlivé autentifikačné riešenia posúdené. Krajiny si musia byť vedomé akú úroveň má autentifikačné riešenie inej krajiny a musia mu dôverovať. Táto dôvera je založená na úrovni zabezpečenia prislúchajúcej autentifikačnému riešeniu, ktoré musí spĺňať spoločne stanovené bezpečnostné kritériá. Interoperabilita je založená na zhode v stanovení úrovní zabezpečenia. Každá úroveň zabezpečenia popisuje úroveň, do akej si môže byť poskytovateľ elektronickej služby istý, že informácie o identite, sprístupnené poskytovateľom identity, naozaj reprezentujú entitu na ktorú sa tieto informácie viažu.

Pre definovanie referenčných úrovní zabezpečenia autentifikačného mechanizmu existuje niekoľko prístupov[6] založených napríklad na dôležitosti transakcie, na vážnosti dôsledkov zneužitia prostriedkov elektronickej identifikácie alebo na pravdepodobnosti následkov spôsobených nesprávnou autentifikáciou. Vzhľadom na rôzne úrovne a druhy rizík ktoré sa spájajú s elektronickými transakciami, ako najvhodnejší sa javí viacúrovňový autentifikačný mechanizmus, kde je úroveň priradená miere/stupňu istoty o identite entity.

Cezhraničná interoperabilita bola overená teoreticky a do určitej úrovne aj prakticky v projekte STORK[7], ktorý je zameraný na interoperabilné riešenie elektronickej identity. Interoperabilná platforma bola stanovená tak, aby rešpektovala národné riešenia, požiadavku škálovateľnosti, princípy dôvery a bezpečnosti a ochrany súkromia. Dôraz bol kladený na dosiahnutie technickej interoperability. Identifikované prekážky interoperability v legislatívnej oblasti (jedná sa napríklad o národnú legislatívu v oblasti identifikátorov entity, legislatívny základ pre cezhraničnú autentifikáciu) budú do určitej miery riešené v pripravovanej legislatíve na úrovni EÚ. Z pohľadu národných riešení eID je dôležité, že riešenie neobsahuje návrh jednotného riešenia autentifikácie, spoločného a záväzného pre všetky krajiny, ale v rámci neho boli vyvinuté a otestované na pilotných riešeniach spoločné špecifikácie pre vzájomné uznávanie národných elektronických identít. Základom pre definovanie viacúrovňovej autentifikačnej schémy v projekte STORK bol návrh IDABC „Návrh viacúrovňového autentifikačného mechanizmu a mapovanie existujúcich autentifikačných mechanizmov“, ktorý bol následne upravený aby viac zodpovedal praktickým požiadavkám a doplňal úrovne zabezpečenia prislúchajúce jednotlivým národným autentifikačným riešeniam. Význam tohto projektu spočíva nielen v jeho širokom akceptovaní členskými štátmi (v projekte je zapojených až 19 štátov), ale najmä v tom, že výsledky projektu Európska komisia prezentuje ako základ pre následný proces tvorby legislatívy a štandardov.

[5] Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms, IDABC, December 2007, pilotný projekt STORK

[6] Napríklad „IDABC Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms“, alebo „Liberty Alliance assurance framework document“

[7] Projekt STORK, podporovaný z Rámcového programu pre konkurencieschopnosť a inovácie, program podpory politiky informačných a komunikačných technológií (CIP ICT PSP)

Odporúčania, nariadenia a záväzky na úrovni EÚ ovplyvňujúce rámec eID

Až do nedávnej doby, bola v európskych predpisoch úloha elektronickej identifikácie a autentifikácie ako celku, riešená nesúrodým spôsobom. Prvé systematické kroky sa objavili v **akčnom pláne pre elektronickú verejnú správu**[8], ktorý bol prijatý Európskou komisiou v roku 2006, a v súvisiacej **cestovnej mape pre paneurópsky rámec eID do roku 2010**[9]. V týchto dokumentoch je prijatie spoločnej viacúrovňovej autentifikačnej politiky vnímané ako jeden zo základných stavebných blokov pre vytvorenie paneurópskeho rámca pre interoperabilitu v oblasti eID. Dôvodom je najmä rôznorodosť autentifikačných riešení v jednotlivých krajinách, kde ich dôveryhodnosť a úrovne zabezpečenia závisia od požiadaviek špecifických aplikácií a zvolenej národnej politiky eID.

Hlavným regulačným rámcom zatiaľ ostáva **Smernica 1999/93/ES** Európskeho parlamentu a Rady z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy (ďalej ako „Smernica o elektronickom podpise"). Od jej prijatia v roku 1999, vzniklo niekoľko právnych nástrojov, ktoré sa okrajovo týkali konceptu elektronickej identity, identifikácia a autentifikácia však neboli nikde priamo riešené.

Jednou z oblastí, ktorá sa týka elektronickej identity, je oblasť ochrany súkromia a osobných údajov. V rámci Európskej únie problematika ochrany súkromia a ochrany osobných údajov vychádza z článku 6 odsek 2 **Zmluvy o Európskej únii,** podľa ktorého sa Únia zaväzuje rešpektovať ochranu základných ľudských práv a slobôd, garantovaných **Chartou základných práv Európskej únie**. Podľa článku 8 Charty, má každý právo na ochranu osobných údajov, ktoré sa ho týkajú a členské štáty EÚ majú zabezpečiť, aby tieto údaje boli riadne spracované na určené účely na základe súhlasu dotknutej osoby. Charta zároveň garantuje právo osoby na prístup k zhromaždeným údajom, ktoré sa jej týkajú, a právo na ich opravu. Problematiku ochrany osobných údajov v oblasti automatizovaného spracovania dát upravuje **Dohovor Rady Európy o ochrane jednotlivca pri automatizovanom spracovaní osobných údajov**, ktorý ukladá zmluvným stranám vytvoriť potrebné bezpečnostné opatrenia na ochranu osobných údajov v automatizovaných súboroch údajov pre náhodným alebo nepovoleným zničením alebo náhodnou stratou, ako aj pred nepovoleným prístupom, zmenami alebo šírením. Významným prameňom v oblasti ochrany osobných údajov v rámci EÚ je **smernica Európskeho parlamentu a Rady č. 95/46/EHS** zo dňa 24. 10. 1995 o ochrane fyzických osôb pre spracovaní osobných údajov a o voľnom pohybe týchto údajov. Táto smernica vychádza zo zásady ochrany súkromia v súvislosti so spracovaním osobných údajov a ukladá členským štátom konkrétne požiadavky na spracovanie, zhromažďovanie, udržiavanie osobných údajov. Zameriava sa tiež na bezpečnosť ich spracovania, kedy členské štáty musia zabezpečiť zavedenie príslušných technických a organizačných opatrení na ochranu osobných údajov pred náhodným alebo nezákonným poškodením, alebo náhodnou stratou, zmenou, neoprávneným prezradením alebo sprístupnením.

Prijatie oznámenia Európskej komisie v roku 2010 o **Digitálnej agende pre Európu**[10] a následne **Európskeho akčného plánu pre elektronickú verejnú správu na roky 2011-2015**[11]**,** znamenali upriamenie pozornosti na služby elektronickej identifikácie a autentifikácie. Digitálna agenda pre Európu potvrdzuje, že technológie elektronickej identity a autentifikačné služby sú podstatou pre transakcie na internete, tak pre verejný ako aj pre súkromný sektor. Zároveň umiestňuje elektronickú identitu a do širšieho kontextu bezpečnosti a dôvery a spolu s autentifikačnými mechanizmami sú považované za mechanizmy, ktoré môžu prispieť k budovaniu životaschopných riešení pre tieto problémy. Akčný plán identifikuje elektronický podpis, eID a interoperabilitu ako jasné predpoklady k zlepšeniu podmienok pre rozvoj cezhraničných služieb elektronickej verejnej správy poskytovaných občanom a firmám. Zameriava sa na cezhraničné služby mobility pre občanov a podniky. Pre služby, ktoré umožnia občanom a firmám bývať, študovať a podnikať kdekoľvek v EÚ sú technológie elektronickej totožnosti a autentifikačné mechanizmy významné z hľadiska bezpečnosti elektronických transakcií.

Nutnosť cezhraničnej a interoperabilnej elektronickej identity, ktorá je základným prvkom pre dosiahnutie slobody pohybu tovaru, služieb a kapitálu je podoprená **Smernicou EP a Rady č. 2006/123/ES** o službách na vnútornom trhu, ktorá okrem iného žiada umožniť realizovať všetky postupy a formálne náležitosti vzťahujúce sa na prístup k činnostiam v oblasti služieb a ich vykonávanie na diaľku a elektronickými prostriedkami. Táto smernica požaduje od členských štátov, aby vytvorili prostredie pre poskytovanie cezhraničných služieb pre podnikateľov

[8] i2010 eGovernment Action Plan - Accelerating eGovernment in Europe for the Benefit of All - COM(2006)173 final

[9] A roadmap for eID for the Implementation of the eGovernment Action Plan, A Roadmap for a pan-European eIDM Framework by 2010

[10] KOM/2010/0245 v konečnom znení

[11] KOM/2010/0743 v konečnom znení

prostredníctvom jednotných kontaktných miest. Ukázala sa ako hlavnou hnacou silou diskusie pre zavedenie celoeurópskej infraštruktúry eID pre podnikateľov.

Súčasne platná Smernica o elektronických podpisoch je stredobodom pozornosti od roku 1998, ale postupne s omnoho heterogénnejšou a komplexnejšou situáciou na trhu s identifikačnými a autentifikačnými mechanizmami trpí viacerými nedostatkami. Smernica je nejasná a nejednoznačná v niektorých dôležitých právnych bodoch (najmä pre oblasť použitia elektronického podpisu u právnických osôb, verejnej správy). K jej nedostatkom patria aj problémy s definovaním rámca spoľahlivosti, ako aj technologicky prekonané a nekompletné štandardy. Smernica zahŕňa napríklad veľmi podrobné pravidlá pre certifikačné autority, ale nerieši ďalšie kategórie elektronickej identifikácie a autentifikácie alebo poskytovateľov dôveryhodných služieb. Požiadavky na reguláciu aj iných oblastí sú však prinajmenšom rovnako akútne ako požiadavky certifikačných autorít. Existuje napríklad potreba regulácie poskytovateľov archívnych služieb alebo registrovaných poštových služieb.

K 28. decembru 2009 padla prvá prekážka v cezhraničnom uznávaní kvalifikovaných certifikátov, Európska komisia vydala **Rozhodnutie č. 2009/767/ES**, ktorým sa ustanovujú opatrenia na uľahčenie postupov elektronickými spôsobmi prostredníctvom „miest jednotného kontaktu“ podľa Smernice č. 2006/123/ES o službách na vnútornom trhu. Dôsledkom tohto Rozhodnutia by Slovensko, okrem slovenských kvalifikovaných certifikátov, malo uznávať aj kvalifikované certifikáty z EÚ. Členským štátom bola zároveň uložená povinnosť zriadiť a udržovať zoznam dôveryhodných certifikačných služieb.

S cieľom vyriešiť vyššie uvedené problémy a najmä poskytnúť právny rámec pre cezhraničné uznávanie a interoperabilitu elektronických autentifikačných systémov sa Európska komisia, v rámci implementácie Digitálnej agendy pre Európu (konkrétne kľúčová akcia č. 3), zaviazala navrhnúť **revíziu Smernice 1999/93/ES** o elektronickom podpise. Digitálna agenda pre Európu ďalej obsahuje súvisiace záväzky (konkrétne kľúčová akcia č. 16), predložiť do roku 2012 **návrh rozhodnutia** Európskeho parlamentu a Rady **o zaistení vzájomného uznávania elektronickej identifikácie a elektronickej autentifikácie** v celej EÚ založeného na online „autentifikačných službách“ poskytovaných vo všetkých členských štátoch. K nedávnym aktivitám Európskej komisie smerujúcim k tvorbe vyššie spomenutých legislatívnych návrhov patrí najmä snaha získať spätnú väzbu a zozbierať od všetkých zainteresovaných subjektov námety, ako by mala byť pripravovaná legislatíva navrhnutá tak, aby spĺňala výzvy digitálneho jednotného trhu, aby bola otvorená a nie viazaná na dopredu určené technické riešenia. Za týmto účelom bola od 18.2.2011 do 15.4.2011 Európskou komisiou zorganizovaná online verejná konzultácia, kde bola identifikovaná potreba zlepšiť dôveru v elektronický podpis a mieru jeho použitia, pokryť legislatívou nové scenáre napr. podpisovanie mobilom a tiež bola zdôraznená potreba štandardizácie a technologickej neutrality. Výsledky verejnej konzultácie naznačujú, že za nízkym rozšírením používania elektronického podpisu stojí limitované množstvo ponúkaných elektronických služieb naviazaných na používanie elektronického podpisu, nedostatok technických riešení priateľských k užívateľovi a problémy s cezhraničnou interoperabilitou. Až 65 % respondentov vyjadrilo potrebu jednotnej EÚ legislatívy v oblasti eID, 66 % požadovalo zvýšiť bezpečnosť zaručeného elektronického podpisu, 82 % bolo za riešenie eID aj v oblasti mobilných zariadení. Ďalším krokom pri príprave návrhu legislatívy je zadanie vypracovania štúdie o elektronickej identifikácii, autentifikácii a podpisovej politike (ďalej ako „štúdia IAS), ktoré bude trvať 18 mesiacov, cca, do októbra 2012. Analýza dopadu pre navrhnuté možnosti úpravy legislatívy bude zverejnená Európskou komisiou na jar 2012, kedy by mal byť pripravený legislatívny návrh. Nasledovať bude vypracovanie implementačných aktov a racionalizácia štandardov.

Jedným z najnovších pripravovaných konkrétnych nástrojov na finančnú podporu projektov na zlepšenie prístupu k cezhraničným online službám aj prostredníctvom autentifikácie je **Integrovaný nástroj Spájame Európu na podporu dokončovania prioritných energetických, dopravných a digitálnych infraštruktúr** (ďalej ako „CEF“), schválený Európskou komisiou v rámci viacročného finančného rámca pre roky 2014 až 2020[12] „Rozpočet stratégie Európa 2020“. V rámci CEF vydali Európsky parlament a Rada **návrh nariadenia o usmerneniach pre transeurópske telekomunikačné siete**[13], ktorého cieľom je pripraviť sériu usmernení na identifikáciu projektov spoločného záujmu pre oblasť zavádzania širokopásmových sietí a infraštruktúr digitálnych služieb. Medzi projekty spoločného záujmu v oblasti infraštruktúr digitálnych služieb patrí aj cezhraničné poskytovanie služieb elektronickej verejnej správy založených na interoperabilnej identifikácii a autentifikácii, kde

[12] KOM(2011) 500/I v konečnom znení a KOM(2011) 500/II v konečnom znení (Prehľady politík)

[13] KOM(2011) 657 v konečnom znení

sa počíta so zavedením sady spojených a zabezpečených autentifikačných serverov a protokolov, ktorá zabezpečí interoperabilitu rôznych typov autentifikačných, identifikačných a autorizačných systémov, ktoré existujú v Európe. Táto platforma bude pozostávať zo základnej vrstvy pre všetky digitálne služby, pre ktoré bude potrebná elektronická identifikácia a autentifikácia, napríklad elektronické obstarávanie, online zdravotnícke služby, elektronickú výmenu informácií v oblasti súdnictva, transeurópsku online registráciu spoločností, služby elektronickej verejnej správy pre podniky, vrátane komunikácie medzi obchodnými registrami týkajúcej sa cezhraničných fúzií a zahraničných pobočiek.

Riešenie eID v SR

Slovensko – základné prvky eID

Jedným z prvých návrhov ako riešiť riadenie elektronickej identity na národnej úrovni bol návrh systému založeného na elektronických identifikačných kartách ako povinných dokladoch o elektronickej identite vydávaných s úmyslom umožniť prístup k službám elektronickej verejnej správy. V roku 2006 Ministerstvo financií SR predstavilo „Štúdiu uskutočniteľnosti elektronických identifikačných kariet vydávaných pre používanie v elektronických službách verejnej správy“, ktorá bola súčasťou Stratégie konkurencieschopnosti Slovenskej Republiky do roku 2010 – Akčného plánu. Štúdia nebola zavedená do praxe. Ďalším krokom v tejto oblasti bolo prijatie Stratégie informatizácie verejnej správy[14] a následne Národnej koncepcie informatizácie verejnej správy (ďalej ako „NKIVS“). V NKIVS boli stanovené najdôležitejšie základné komponenty architektúry integrovaných informačných systémov verejnej správy (ďalej ako „ISVS”), ktoré by mali byť používané pri elektronickej forme výkonu správy.

Komponenty architektúry s dosahom na oblasť elektronickej identity podľa NKIVS sú najmä:

- Elektronická identifikačná karta,
- Základné identifikátory,
- Základné registre, najmä register obyvateľov a register právnických osôb
- Spoločné moduly ÚPVS, najmä modul Správy identít a riadenia prístupových práv (ďalej ako „modul IAM”)

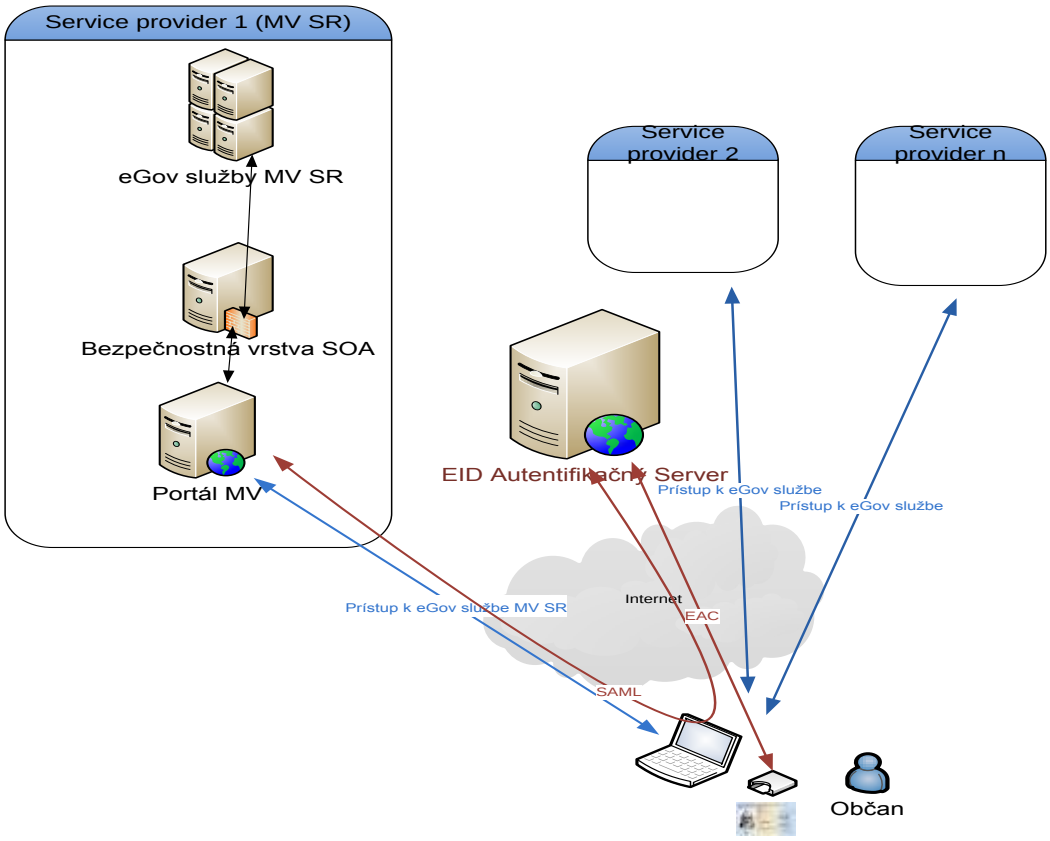
Elektronická identifikačná karta

V súlade s NKIVS bola Ministerstvom financií SR realizovaná štúdia uskutočniteľnosti vydávania elektronického preukazu totožnosti ako nástroja elektronickej identifikácie, rovnako ako prostriedku autentifikácie v rámci elektronickej komunikácie. Následný projekt, ktorý bude implementovať elektronický preukaz totožnosti financovaný zo štrukturálnych fondov – OPIS je v štádiu implementácie, s očakávaným zavedením elektronickej identifikačnej karty koncom roku 2012. Odporúčaným riešením je vydávať eID kartu, ktorá bude obsahovať elektronický čip, jednoznačnú bezvýznamovú identifikáciu fyzických osôb a bude slúžiť pre účely identifikácie a autentifikácie. Čip eID karty by mal poskytovať voliteľnú funkčnosť generovania zaručeného elektronického podpisu. Tento nástroj je navrhnutý na jasné určenie a autentifikáciu fyzických osôb.

Oproti pôvodnému konceptu navrhnutému v štúdii uskutočniteľnosti sa momentálne pri realizácii eID karty uvažuje o zmene v spôsobe autentifikácie. Namiesto použitia certifikátu X.509 (štandard pre systémy založené na verejnom kľúči a PKI infraštruktúre) sa navrhuje použitie EAC online autentifikácie. Ide o nový spôsob autentifikácie, v ktorom po odsúhlasení prístupu k čipu občanom zadaním svojho prístupového PIN, dôjde medzi serverom a čipom preukazu k vytvoreniu zabezpečeného dôveryhodného kanála, cez ktorý server vyčíta identitu občana alebo len jej časť. Teda v prípade služieb s autentifikáciou prostredníctvom EAC online autentifikácie občan použije ako autentifikačný token novú eID kartu s čipom. Pre účely autentifikácie nie je nutné aby na eID kartu bol dodatočne zapísaný autentifikačný certifikát vydávaný akreditovanou certifikačnou autoritou. Pri prístupe cez EAC sa využívajú tzv. CV (Card Verifiable) terminálové certifikáty. Občan teda spolu s novou eID kartou získava aj možnosť autentifikovať sa pomocou svojho elektronického občianskeho preukazu eID pri prístupe k elektronickým službám verejnej správy ale aj ku službám komerčných poskytovateľov služieb (elektronický obchod, banka, ...). Za účelom zabezpečenia prístupu poskytovateľov služieb k funkciám dokladu je nutné

[14] schválená uznesením vlády SR č. 131/2008 dňa 27. februára 2008

implementovať špecifický systém - eID autentifikačný systém (eID AS), prostredníctvom ktorého budú môcť systémy poskytovateľov služieb využívať plnú funkcionalitu nového dokladu. eID AS bude v tomto procese vystupovať ako poskytovateľ identity. Systém eID AS dokáže po súhlase občana zadaním PIN cez zabezpečený šifrovaný kanál pristúpiť ku vzdialenej eID karte a prečítať z nej občanovu identitu. Pred zadaním PIN je občanovi zobrazená informácia o poskytovateľovi služby, o účele autentifikácie a o údajoch, ktoré majú byť z čipu prečítané. Občan má možnosť modifikovať zoznam čítaných údajov a svoj súhlas s ich prečítaním vyjadruje zadaním prístupového PIN. Proces žiadosti, overenia identity a doručenie tokenu pre autentifikáciu je rovnaký, respektíve je zabezpečený procesmi žiadosti, overenia identity a doručenia eID karty. Samotný proces autentifikácie s použitím eID karty (EAC online autentifikácia) je znázornený na nasledujúcom obrázku.



Identifikátory identity

V súčasnosti je jednotným identifikátorom fyzickej osoby tradične používané osobné identifikačné číslo, tzv. rodné číslo. Rodné číslo sa používa ako primárny identifikátor, ktorý jednoznačne identifikuje fyzické osoby. Podľa zákona č 301/1995 Z.z. o rodnom čísle, Slovenská republika využíva rodné číslo ako všeobecný a jednotný identifikátor osoby v informačných systémoch. Celá rada informačných systémov, vrátane komerčných, používa rodné číslo ako identifikátor, rovnako ako kľúčové kritérium pre vyhľadávanie v informačných systémoch. Rodné číslo je zapísané v centrálnej evidencii obyvateľov, v gescii Ministerstva vnútra SR. Rodné číslo je pridelené každej osobe narodenej na území Slovenskej republiky na Matrike ihneď po narodení. Ministerstvo vnútra SR prostredníctvom Matriky priradí rodné číslo občanovi narodenému na území Slovenskej republiky s trvalým pobytom na Slovensku, občanovi Slovenskej republiky narodenému v cudzine, cudzincovi s trvalým alebo dlhodobým pobytom na území Slovenska, utečencom s bydliskom na Slovensku a osobám bez trvalého pobytu Slovensku, ktoré o to požiadali. Dokument formálne zavádzajúci rodné číslo, je rodný list alebo občiansky preukaz, cestovný doklad (cestovný pas), povolenie na pobyt alebo potvrdenie o rodnom čísle.

Mnoho slovenských zákonov je výslovne spätých s rodným číslom. Rodné číslo však nie je použiteľné pre budúce informačné systémy verejnej správy, pretože je z neho možné odvodiť osobné údaje o osobe, ako je dátum narodenia, pohlavie, miesto narodenia a pod. Taktiež jeho rozšírenosť prináša nebezpečenstvo previazania rôznych databáz prostredníctvom rodného čísla. Vyskytuje sa tiež chybovosť pri prideľovaní rodného čísla a z nej vyplývajúca možnosť výskytu duplikátu rodného čísla (rovnaké rodné číslo pre dve alebo viac osôb). Tieto faktory spôsobili nevyhnutnosť nahradiť starý systém tvorby rodného čísla novým identifikátorom, ktorý bude poskytovať lepšiu ochranu pred rizikami vyplývajúcimi z elektronického spracovania údajov. Zavedenie nového identifikátora má byť výsledkom realizácie národného projektu financovaného z OPIS.

Iné dôležité identifikátory používané na území Slovenskej republiky pre právnické osoby sú identifikačné číslo organizácie IČO, daňové identifikačné číslo, číslo platcu dane z pridanej hodnoty, identifikátory z informačných systémov Sociálnej poisťovne a zdravotných poisťovní.

Register obyvateľov

Riešenie identity úzko súvisí s vybudovaním registra fyzických osôb. Register fyzických osôb by mal, v súvislosti s plánovaným ukončením projektu financovaného z OPIS k 31.10.2012, nahradiť doteraz používaný register obyvateľov. V súčasnosti je na Slovensku hlavným tradične používaným zdrojom identity register obyvateľov. Register obyvateľov, spravovaný Ministerstvom vnútra SR, obsahuje súbor informácií o občanoch Slovenskej republiky, na základe ktorých je možné identifikovať osobu, zistiť jej bydlisko a jej vzťahy k ostatným osobám. Tento register je v súčasnosti používaný ako zdroj platných informácií o občanoch Slovenskej republiky pre potreby orgánov štátnej správy, územnej samosprávy. Register obyvateľov súčasnej dobe nie je voľne prístupný. V osobitných prípadoch majú verejné orgány prístup k registru, sú schopné prehľadávať register obyvateľstva a využívať dáta v ňom uchovávané. Register obsahuje informácie o identite fyzických osôb, vrátane osobných údajov (meno, priezvisko, akademický titul, rodné priezvisko, rodné číslo, dátum narodenia, miesto narodenia, okres narodenia, krajina narodenia, pohlavie, rodinný stav, štátne občianstvo, dátum a miesto úmrtia), informácie o trvalom alebo prechodnom bydlisku (názov okresu, názov obce, názov časti obce, názov ulice, číslo orientačné, registračné číslo), informácie o vzťahu k iným fyzickým osobám (osobné údaje manžela alebo manželky, osobné údaje otca a matky, osobné údaje dieťaťa) a administratívne údaje o fyzickej osobe (číslo a séria občianskeho preukazu, číslo a typ cestovného dokladu, ak je vydaný, informácie o rozhodnutí súdu týkajúce sa schopnosti k právnym úkonom, informácie o rozhodnutí súdu týkajúce sa rozvodu manželstva, informácie o rozhodnutí súdu v súvislosti s oznámením, že manželstvo je neplatné, údaje o rozhodnutí súdu v súvislosti s oznámením, že občan je mŕtvy, informácie o zákaze pobytu, informácie o udelení slovenského štátneho občianstva).

Spoločné moduly ÚPVS, najmä modul Správy identít a riadenia prístupových práv (ďalej ako „modul IAM")

Cieľová architektúra integrovaného ISVS predpokladá využívanie spoločných modulov ÚPVS, ktoré majú byť používané ISVS pri elektronickej forme výkonu správy. K spoločným modulom patrí podľa NKIVS aj modul správy identít a riadenia prístupových práv, ktorý by mal vytvoriť prostredie pre centrálnu správu životného cyklu identít, správu autentifikačných údajov, poskytovanie informácií o oprávneniach a jednotný prístup pre webové služby a autentifikačný server. Prostredníctvom modulu IAM mala byť zabezpečená aj centrálna identifikácia a autentifikácia občana elektronickou identifikačnou kartou.

Vybudovanie modulu IAM malo byť realizované v rámci projektu OPIS – Elektronické služby spoločných modulov ÚPVS a prístupových komponentov. Tento projekt bol v roku 2010 pozastavený, čo prinieslo problémy projektom naviazaným na spoločnú funkcionalitu. Jedným z navrhovaných riešení je vybudovanie centrálneho prístupového komponentu pre účely identifikácie a autentifikácie na Ministerstve vnútra SR (eID autentifikačný systém).

Slovensko – aktuálny stav autentifikačných riešení

V podmienkach Slovenskej republiky doteraz neexistuje všeobecne platný systém autentifikácie s definovanými úrovňami zabezpečenia. Vo verejnom sektore existuje veľké množstvo elektronických služieb, ktoré majú autentifikačný systém nastavený špecificky v rôznej kvalite a s rôznou úrovňou zabezpečenia, podľa uváženia príslušnej organizácie. Toto samozrejme do veľkej miery ovplyvňuje interoperabilitu služieb z pohľadu využitia elektronickej identity a neúmerne komplikuje prípadnú cezhraničnú interoperabilitu.

Elektronické služby využívajúce autentifikáciu by sme mohli zhruba rozdeliť do nasledovných úrovní zabezpečenia (pre podrobnejší popis viď. príloha):

1. Služby nevyžadujúce žiadnu autentifikáciu, napríklad online prístup k základným údajom katastra nehnuteľností, vrátane možnosti vytvárať rôzne zostavy a sledovať status katastrálneho konania. Ďalšie služby katastra nehnuteľností, dostupné len pre oprávnené osoby, však už vyžadujú autentifikáciu na úrovni č. 3.
2. Služby s autentifikáciou prostredníctvom mena a hesla používateľa, napr. niektoré služby ústredného portálu verejnej správy. Prístup k určitým službám ÚPVS je poskytovaný akejkoľvek registrovanej entite, pričom registrácia pozostáva z vyplnenia a zaslania online formulára. Platný emailový účet slúži potom k aktivácii vytvoreného konta prostredníctvom hypertextového odkazu doručeného e-mailom. Ďalšie služby dostupné prostredníctvom ÚPVS, napríklad prístup k elektronickým službám Obchodného registra, však už vyžadujú autentifikáciu na úrovni č. 4 až 5.
3. Do tretej úrovne môžeme zaradiť služby s autentifikáciou s použitím softvérových certifikátov, prípadne služby s autentifikáciou prostredníctvom mena a hesla podobne ako v druhej úrovni, avšak s podstatne dôveryhodnejšou formou registrácie. Sú to napríklad elektronické služby verejného obstarávania prevádzkované Úradom pre verejné obstarávanie, ktoré podporujú zatiaľ tri fázy verejného obstarávania – vyhlásenie verejného obstarávania (eNotification), predkladanie ponúk (eTendering) a vyhodnocovanie ponúk (eAwarding).
4. Služby s autentifikáciou prostredníctvom kvalifikovaného certifikátu – so zaručeným elektronickým podpisom a s potrebou registračného a autorizačného procesu u poskytovateľa služby, napr. online elektronické služby poskytované Daňovou správou SR. Pre používanie týchto služieb, používateľ potrebuje kvalifikovaný certifikát – zaručený elektronický podpis vydávaný akreditovanou certifikačnou autoritou. Pre registráciu používateľa je potrebná osobná návšteva žiadateľa o registráciu v kancelárii certifikačnej autority. V procese registrácie je identita používateľa potvrdená dvomi dokumentmi (napr. občianskym preukazom, vodičským preukazom). Vo všeobecnosti, pred prvým použitím služby je nevyhnutná dodatočná registrácia a autorizácia u poskytovateľa služby prostredníctvom osobnej návštevy.
5. Služby s autentifikáciou prostredníctvom kvalifikovaného certifikátu – so zaručeným elektronickým podpisom a s potrebou registrácie u poskytovateľa služby. Od predchádzajúcej úrovne sa líši tým, že pred získaním prístupu ku službe nie je potrebná osobná návšteva u poskytovateľa služby. Príkladom takýchto elektronických služieb sú napríklad elektronické služby colnej správy. Pre používanie týchto služieb, používateľ (osoba zastupujúca subjekt v elektronickej komunikácii s colnou správou, ktorá má oprávnenie podpísať za daný subjekt elektronický dokument) musí vlastniť prostriedky na vytvorenie zaručeného elektronického podpisu, a to kvalifikovaný certifikát, čipovú kartu certifikovanú Národným bezpečnostným úradom SR a čítačku čipovej karty, ktoré sú vydávané akreditovanou certifikačnou autoritou. Podmienkou využívania elektronických služieb colnej správy je podpísanie dohody o používaní zaručeného elektronického podpisu pri využívaní vybraných elektronických služieb colnej správy medzi používateľom elektronických služieb a colnou správou.

Slovensko – návrh strategického smerovania v oblasti elektronickej autentifikácie

Či už bude autentifikácia riešená prostredníctvom vybudovania modulu IAM v rámci projektu OPIS – Elektronické služby spoločných modulov ÚPVS a prístupových komponentov, alebo bude podporené riešenie vybudovania centrálneho prístupového komponentu pre účely identifikácie a autentifikácie na Ministerstve vnútra SR (eID AS), úlohou Ministerstva financií SR, ako subjektu zodpovedného za prípravu, koordináciu a spracovávanie návrhov všeobecne záväzných právnych predpisov upravujúcich proces informatizácie spoločnosti, ostáva navrhnúť a legislatívne ukotviť národný viacstupňový autentifikačný rámec. Národný viacstupňový autentifikačný rámec bude definovať úrovne autentifikácie pre elektronické služby verejnej správy, pričom povinné osoby budú povinné určiť úroveň autentifikácie pre každú nimi poskytovanú elektronickú službu, zabezpečiť dodržanie podmienok a postupov pre určenú úroveň a poskytnúť informáciu o určenej úrovni do centrálneho metainformačného systému verejnej správy. Národný viacstupňový autentifikačný rámec by mal byť navrhnutý tak, aby zohľadňoval

princípy cezhraničnej komunikácie a perspektívne uľahčoval porovnávanie jednotlivých úrovní voči rôznym medzinárodným eID riešeniam, čím vytvorí predpoklady pre cezhraničné sprístupnenie elektronických služieb verejnej správy, tak, ako sú v súčasnosti plánované a pripravované na úrovni legislatívnych zámerov a pilotných projektov EÚ.

Aby bolo možné určiť úroveň zabezpečenia autentifikačného mechanizmu je potrebné zmerať kvalitu rôznych autentifikačných procedúr, čo umožní prehlásiť, že určitá elektronická služba má rovnakú (lepšiu alebo horšiu) úroveň zabezpečenia autentifikačného mechanizmu ako iná služba. Pri známej úrovni zabezpečenia autentifikačného mechanizmu elektronickej služby, je možné predpokladať väčšiu ochotu poskytovateľa služby sprístupniť službu cezhranične za podmienky dodržania rovnakej úrovne zabezpečenia autentifikačného riešenia.

Keďže každá krajina Európskej únie implementuje vlastné riešenie elektronickej identity, navrhla EÚ vo svojej štúdii[5] viacúrovňový autentifikačný mechanizmus vrátane návrhu mapovania existujúcich autentifikačných mechanizmov. Tento návrh zahŕňa aj spoločné špecifikácie pre vytvorenie interoperability medzi autentifikačnými riešeniami v už využívaných alebo zatiaľ len plánovaných aplikáciách bez toho, aby ovplyvnila jednotlivé existujúce národné infraštruktúry. Rozsah pôsobnosti návrhu je obmedzený na autentifikáciu fyzických a právnických osôb prostredníctvom prostriedkov elektronickej identifikácie. Hoci je primárne zameraný na overovanie identity v oblasti elektronickej verejnej správy, je zároveň použiteľný aj v kontexte súkromného sektora. Tento návrh bol ďalej rozpracovaný v rámci projektu STORK[7], kde si zúčastnené krajiny navrhnutý viacúrovňový autentifikačný mechanizmus prispôsobili tak, aby viac zodpovedal praktickým potrebám poskytovateľov elektronických služieb. Návrh národného viacstupňového autentifikačného rámca by mal vychádzať, prípadne sa čo najviac približovať týmto riešeniam.

Popis viacúrovňového autentifikačného mechanizmu podľa IDABC[5]

Úrovne zabezpečenia autentifikačného mechanizmu, ktoré tvoria súčasť spoločných špecifikácií pre interoperabilný manažment elektronickej identity, umožnia posúdiť úroveň zabezpečenia /bezpečnosti autentifikačných riešení a zároveň ich klasifikovať do abstraktných úrovní. Taktiež definované úrovne zabezpečenia autentifikačného mechanizmu umožnia zvoliť si špecifickú úroveň bezpečnosti, ktorú budú (krajiny/poskytovatelia elektronických služieb) vyžadovať na účely autentifikácie v elektronických službách.

Mechanizmus je postavený na troch základných premisách:

1) stanovenie bezpečnostných požiadaviek definujúcich úrovne zabezpečenia autentifikačného mechanizmu (AAL). Kritériá hodnotenia rizík v kombinácii s možnými škodami v prípade incidentov berú do úvahy organizačné a technické aspekty autentifikačného procesu. Sú užitočné pre vlastníkov aplikácií/služieb pri stanovení vhodnej bezpečnostnej úrovne.

   Odporúčané sú nasledovné úrovne zabezpečenia autentifikačného mechanizmu:

Úroveň 1	minimálne zabezpečenie
Úroveň 2	nízke zabezpečenie
Úroveň 3	významné zabezpečenie
Úroveň 4	vysoké zabezpečenie

2) stanovenie registračných požiadaviek pre vydávanie prostriedkov elektronickej identifikácie v jednotlivých stanovených úrovniach, ktoré zahŕňa tak preukázanie identity ako aj doručenie prostriedkov elektronickej identifikácie. Registračný mechanizmus uplatňujúci sa pri vydávaní prostriedkov elektronickej identifikácie má zásadný vplyv na posudzovanie spoľahlivosti autentifikačných mechanizmov.

   Posudzované sú:
   - vyžadovaná dokumentácia pred vydaním tokenu/prostriedkov elektronickej identifikácie, včítane spôsobu osobného dostavenia, alebo registráciou na diaľku a overenia špecifických atribútov popísaných v predkladaných dokumentoch
   - proces vydávania, t.j. osobné vydanie klientovi, alebo elektronicky alebo prostredníctvom pošty na trvalé bydlisko
   - kvalita vydávajúceho orgánu;

- uchovávanie registračných informácií

3) definovanie autentifikačných požiadaviek pre použitie prostriedkov elektronickej identifikácie v jednotlivých stanovených úrovniach. Overovanie identity sa zvyčajne dosiahne prostredníctvom jedného alebo viacerých spôsobov:
   - autentifikácia znalosťou (niečo čo viete) - napr. heslo, PIN
   - autentifikácia vlastníctvom (niečo čo máte) - napr. smart karty, hardware token, občiansky preukaz
   - autentifikácia charakteristikou (niečo čo ste) - využitie biometriky - unikátnych vlastností klienta

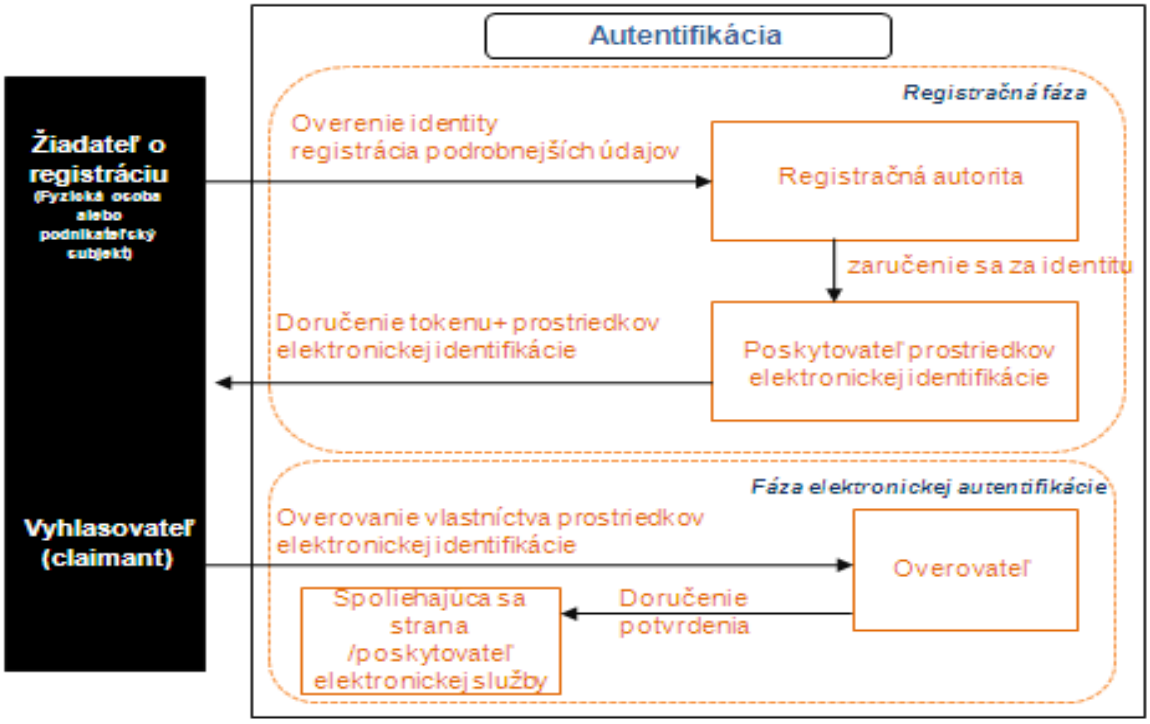
Popis procesného modelu autentifikácie

Autentifikácia entity vyžaduje dve hlavné fázy (viď. obrázok nižšie):

Registračná fáza - je proces v ktorom užívateľ získava token / prostriedok elektronickej identifikácie (napríklad užívateľské meno alebo digitálny certifikát) pre následnú autentifikáciu. Registrácia vo všeobecnosti pozostáva z:

- overenia identity, počas ktorej je overená reálna (real world) identita vyhlasovateľa
- registrácie podrobnejších údajov o vyhlasovateľovi a doručenie tokenu
- doručenie prostriedku elektronickej identifikácie

Fáza elektronickej autentifikácie – sa nazýva tiež dôkaz o držbe, a počas tejto fázy sa overuje elektronická identita vyhlasovateľa. Autorizácia je stanovenie čo je identita oprávnená robiť, alebo aké má prístupové privilégiá. V žiadnom prípade sa nesmie zamieňať s autentifikáciou.



Hlavní účastníci procesu autentifikácie

Pri popise hlavných účastníkov procesu autentifikácie, a tiež celkovo pri popise autentifikačného riešenia, narážame na problém zjednotenia odbornej terminológie v oblasti eID a autentifikácie, jej záväznosť pre oblasť informatizácie a informačnej bezpečnosti a pre tvorbu legislatívnych a koncepčných materiálov. Navrhnutý preklad pojmov z oblasti eID použitý v tomto dokumente sa môže zmeniť. V budúcnosti bude potrebné zjednotiť terminológiu napr. prostredníctvom aktualizácie Metodického pokynu na použitie odborných výrazov pre oblasť informatizácie spoločnosti, ktorý vydáva Ministerstvo financií Slovenskej republiky v záujme zabezpečenia jednotného postupu pri výklade pojmov v oblasti informatizácie na základe svojej pôsobnosti vyplývajúcej zo

zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení neskorších zákonov v znení zákona č. 678/2006 Z. z.

Žiadateľ o registráciu (subscriber) / vyhlasovateľ (claimant)
Entita vyhlasujúca identitu sa nazýva vyhlasovateľ. Predtým, ako osoba môže vyhlásiť identitu, musí preukázať že táto identita je reálna /existuje a že je oprávnená túto identitu používať. Z tohto dôvodu vyhlasovateľ (v autentifikačnom protokole) musí byť žiadateľom o registráciu u poskytovateľa prostriedkov elektronickej identifikácie. Nakoľko token a/alebo prostriedky elektronickej identifikácie slúžia na autentifikáciu identity žiadateľa o registráciu, žiadateľ o registráciu má povinnosť udržiavať nad ním výlučnú kontrolu.

Registračná autorita
Registračná autorita je zodpovedná za overenie identity žiadateľa o registráciu, zvyčajne prostredníctvom predloženej papierovej formy prostriedkov identifikácie a záznamov v databázach. Registračná autorita sa zaručí za identitu žiadateľa o registráciu poskytovateľovi prostriedkov elektronickej identifikácie. V podmienkach Slovenskej republiky je registračná autorita pre oblasť zaručeného elektronického podpisu definovaná v Zákone č. 215/2002 Z. z. o elektronickom podpise ako poskytovateľ certifikačných služieb, ktorý v mene certifikačnej autority vykonáva vybrané certifikačné činnosti a sprostredkúva služby certifikačnej autority držiteľom certifikátov a žiadateľom o vydanie certifikátu, najmä prijíma žiadosti o vydanie certifikátu, kontroluje súlad údajov v žiadosti o vydanie certifikátu s údajmi v predloženom preukaze totožnosti žiadateľa o vydanie certifikátu, odosiela žiadosti o vydanie certifikátu certifikačnej autorite, odovzdáva certifikáty žiadateľom o vydanie certifikátu. Registračná autorita bude tiež definovaná v pripravovanom návrhu zákona o informačnej bezpečnosti, kde registračnou autoritou identifikácie by mal byť poskytovateľ identifikačnej registrácie, výsledkom ktorej je priradenie určitej identity entite v určenom kontexte.

Poskytovateľ prostriedkov elektronickej identifikácie (**credentials)**
Poskytovateľ prostriedkov elektronickej identifikácie registruje alebo dáva žiadateľovi o registráciu token, ktorý bude používať v procese autentifikácie a podľa potreby vydáva prostriedky elektronickej identifikácie na zviazanie tokenu s identitou, alebo na zviazanie identity s iným atribútom. Žiadateľovi o registráciu môže byť poskytnutý prostriedok elektronickej identifikácie k tokenu v čase registrácie, alebo prostriedok elektronickej identifikácie môže byť generovaný neskôr v prípade potreby. Medzi registračnou autoritou a poskytovateľom prostriedkov elektronickej identifikácie je vždy vzťah. V najjednoduchšom, a snáď aj najrozšírenejšom, prípade registračná autorita a poskytovateľ prostriedkov elektronickej identifikácie sú dve oddelené funkcie jednej organizácie. Registračná autorita však môže byť časť organizácie, ktorá registruje žiadateľov o registráciu s využitím jedného alebo viacerých nezávislých poskytovateľov prostriedkov elektronickej identifikácie. Z tohto dôvodu poskytovateľ prostriedkov elektronickej identifikácie môže mať integrovanú registračnú autoritu prípadne môže mať vzťah s viacerými nezávislými registračnými autoritami pričom tiež registračná autorita môže mať vzťah s viacerými poskytovateľmi prostriedkov elektronickej identifikácie. Podľa terminológie STORK je to poskytovateľ identity (identity provider).

Overovateľ
V každej autentifikovanej online transakcii, musí overovateľ overiť, že vyhlasovateľ vlastní a má kontrolu nad tokenom a/alebo prostriedkom elektronickej identifikácie, ktorý potvrdzuje jeho identitu. Vyhlasovateľ autentifikuje svoju identitu pred overovateľom použitím tokenu a/alebo prostriedkov elektronickej identifikácie a autentifikačným protokolom. Toto sa nazýva preukázanie držby. Overovateľ a poskytovateľ prostriedkov elektronickej identifikácie môže byť tá istá organizácia. Overovateľ a poskytovateľ elektronickej služby môže byť tá istá organizácia. Taktiež môžu byť poskytovateľ prostriedkov elektronickej identifikácie , overovateľ a poskytovateľ elektronickej služby tri rôzne organizácie. V prípade, že sú overovateľ a poskytovateľ elektronickej služby rôzne organizácie, overovateľ musí postúpiť výsledok autentifikačného protokolu poskytovateľovi elektronickej služby. Elektronický objekt vytvorený overovateľom za účelom postúpenia výsledku autentifikačného protokolu sa nazýva potvrdenie (assertion).

Spoliehajúca sa strana - poskytovateľ elektronickej služby
Spoliehajúca sa strana - poskytovateľ elektronickej služby sa pri založení identity alebo atribútu žiadateľa o registráciu na účely transakcie spolieha na výsledky online autentifikácie. Overovateľ a poskytovateľ elektronickej služby môžu byť tou istou, alebo rôznymi organizáciami. Ak sú rôznymi organizáciami, poskytovateľ služby obdrží

od overovateľa potvrdenie (Elektronický objekt vytvorený overovateľom za účelom postúpenia výsledku autentifikačného protokolu).

Procesy v oblasti autentifikácie

Overenie identity

Overenie identity je proces, ktorým sa zabezpečí aby identita skutočne zodpovedala reálnej entite a mala správne priradené atribúty (tieto môžu byť veľmi limitované, napr. iba meno). Zvýšenie úrovne zabezpečenia vyžaduje zvýšené úsilie na zloženie identity žiadateľov o registráciu. Entita zodpovedná za overenie identity žiadateľa o registráciu je registračná autorita.

Doručenie tokenu a prostriedkov elektronickej identifikácie

Poskytovateľ prostriedkov elektronickej identifikácie registruje alebo dáva žiadateľovi o registráciu token, ktorý bude používať v procese autentifikácie (v autentifikačnom protokole) a podľa potreby vydáva prostriedky elektronickej identifikácie na zviazanie tokenu s identitou, alebo na zviazanie identity s iným užitočným atribútom.

Dôkaz o držbe (overovanie vlastníctva prostriedkov elektronickej identifikácie)

Keď vyhlasovateľ overovateľovi úspešne demonštruje držbu a kontrolu nad /ovládanie tokenu a/alebo prostriedkov elektronickej identifikácie v online autentifikácii prostredníctvom autentifikačného protokolu, overovateľ môže založiť/zriadiť identitu žiadateľa o registráciu. Overovateľ môže poskytovateľovi elektronickej služby odovzdať potvrdenie o identite, alebo poskytnúť atribút vyhlasovateľa. Poskytovateľ elektronickej služby môže využiť autentifikovanú identitu a ďalšie faktory na riadenie prístupu ku službe alebo na rozhodnutia týkajúce sa autorizácie.

Doručenie potvrdenia

V prípade ak sú oddelenými organizáciami, poskytovateľ služby prijíma potvrdenie od overovateľa. Poskytovateľ služby je zodpovedný si overiť, že prijaté potvrdenie pochádza od overovateľa, ktorému poskytovateľ služby dôveruje. Tam, kde sa z potvrdení dá vyrozumieť čas vytvorenia alebo atribúty spojené s vyhlasovateľom, je poskytovateľ elektronickej služby tiež zodpovedný za overenie týchto informácií.

Stanovenie úrovní zabezpečenia autentifikačných riešení

Štyri úrovne zabezpečenia autentifikačného mechanizmu (AAL), podľa viacúrovňového autentifikačného mechanizmu IDABC[5], sú determinované vzájomnou súvzťažnosťou rizika, škôd, vplyvu škody a pravdepodobnosťou. Riziko je definované ako pravdepodobnosť poškodenia alebo straty a môže byť rozšírené o ich dopad. Pri určovaní AAL boli identifikované možné riziká zneužitia autentifikačnej metódy a možné škody vzniknuté týmto zneužitím.

Riziko	Škoda	Pravdepodobnosť	Miera závažnosti vplyvu
Riziko 1: Fiktívna identita v reálnom svete	Strata integrity	Takmer istá	Zanedbateľná
Riziko 2: Nepravdivé údaje	Strata dostupnosti	Pravdepodobná	Nízka
Riziko 3: Krádež prístupového tokenu	Strata dôveryhodnosti	Stredná	Stredná
Riziko 4: Krádež identity v reálnom svete	Riziko pre personálnu bezpečnosť	Nepravdepodobná	Vysoká
Riziko 5: Odchytenie alebo prezradenie tajných autentifikačných informácií	Finančná strata	Výnimočná	Veľmi vysoká
Riziko 6: Používanie tajných autentifikačných informácií v nedôveryhodnom termináli			
Riziko 7: Neautorizované			

použitie prístupového tokenu
Riziko 8: Použitie nedôveryhodných prostriedkov elektronickej identifikácie
Riziko 9: Použitie prostriedkov elektronickej identifikácie po významnej zmene skutočností
Riziko 10: Použitie prostriedkov elektronickej identifikácie pre nezamýšľané dôvody
Riziko 11: Stiahnutie prostriedkov elektronickej identifikácie bez udania dôvodu
Riziko 12: Podvodné použitie prostriedkov elektronickej identifikácie
Riziko 13: Hackerský útok
Riziko 14: Rozptýlené ukladanie informácií

Miera rizika je určená vzťahom medzi pravdepodobnosťou, že udalosť nastane a vplyvom možných škôd. Najväčšie riziká pre aplikácie, sú tie, ktoré majú extrémny vplyv a je takmer isté, že nastanú. Naopak výnimočnú udalosť so zanedbateľným vplyvom je možné považovať za banálnu. AAL sa stanoví maticou vyššie spomínaných faktorov pomocou referenčnej matice.

Referenčná matica

		VPLYV ŠKODY				
	PRAVDEPODOBNOSŤ	Veľmi vysoká	vysoká	stredná	nízka	zanedbateľná
Riziko	Takmer isté	-	-	Úroveň 4	Úroveň 3	Úroveň 3
	Pravdepodobné	-	Úroveň 4	Úroveň 3	Úroveň 3	Úroveň 2
	Stredné	Úroveň 4	Úroveň 3	Úroveň 3	Úroveň 2	Úroveň 2
	Nepravdepodobné	Úroveň 3	Úroveň 3	Úroveň 2	Úroveň 2	Úroveň 1
	Výnimočné	Úroveň 3	Úroveň 2	Úroveň 2	Úroveň 1	Úroveň 1

Sumarizáciou troch základných stavebných blokov je možné určiť požiadavky a možnosti pre každú zo štyroch úrovní autentifikácie.

Pre úroveň 1:

Registračná fáza	
Proces overovania identity, registrácia používateľa, doručovanie prostriedkov elektronickej identifikácie	Popis: škody, ktoré môžu vzniknúť zneužitím identity v reálnom svete by mali zanedbateľný alebo nízky vplyv.
	Požiadavky: Registračnou autoritou je akýkoľvek subjekt, ktorého metódy autentifikácie sú akceptované v eGovernment službách. Nie je žiadna požiadavka na preukázanie totožnosti alebo udržiavanie záznamov o registráciách. Žiadateľom určená e-mailová adresa musí byť jednoznačná a platná.
	Doručenie: Nie je špecifická požiadavka na doručenie prostriedkov elektronickej identifikácie.
Doba uchovávania registračných dát	Žiadna.
Fáza elektronickej autentifikácie	

Autentifikačný protokol pre dôkaz o držbe/overovanie vlastníctva prostriedkov elektronickej identifikácie	Vo väčšine overovanie vlastníctva prostriedkov elektronickej identifikácie postačuje prostredníctvom hesla typu výzva - odpoveď, avšak po posúdení miery rizika môže byť aj: overovanie vlastníctva prostredníctvom hesla posielaného tunelom, overovanie vlastníctva prostriedkov elektronickej identifikácie prostredníctvom jednorazového (alebo silného) hesla, overovanie vlastníctva prostredníctvom symetrického kľúča, overovanie vlastníctva prostredníctvom privátneho kľúča.
Typ tokenu	Všetky typy tokenu sú prijateľné, najčastejšie sú preferované heslo a PIN tokeny.

Pre úroveň 2:

Registračná fáza	
Proces overovania identity, registrácia používateľa, doručovanie tokenov a prostriedkov elektronickej identifikácie	Popis: škody, ktoré môžu vzniknúť zneužitím identity v reálnom svete by mali stredný vplyv. V mnohých prípadoch je možné na úrovni 2 registráciu vykonať on-line a okamžite.
	Požiadavky: Token / prostriedky elektronickej identifikácie musia byť vydané orgánom, ktorý je pod štátnym dohľadom. Nie je nutný osobný kontakt, registrácia môže prebiehať online na základe údajov predložených žiadateľom, ktoré umožnia jeho jednoznačnú identifikáciu. Predložené údaje musia prejsť základným overením buď krížovým overením atribútov z úradných zdrojov alebo z dôveryhodnej databázy ako banka, poisťovňa alebo zaslaním prostriedkov elektronickej identifikácie na adresu trvalého pobytu alebo implicitne napr. zaslaním prostriedkov elektronickej identifikácie na trvalý pobyt žiadateľa, alebo osobným vyzdvihnutím tokenu žiadateľom počas, ktorého musia byť predložené údaje validované s úradnými dokumentmi potvrdzujúcimi identitu.
	Doručenie: Token / prostriedky elektronickej identifikácie musia byť zaslané dvoma oddelenými korešpondenciami, aspoň jedna z nich musí byť fyzickou poštou (nie e-mail) na oficiálnu adresu žiadateľa, ako je uvedené v úradnej databáze identít, v ktorej bola fyzická adresa zapísaná. Alebo: Token / prostriedky elektronickej identifikácie je možné stiahnuť priamo žiadateľom pomocou odkazu na webovú stránku, ktorý bol zaslaný na žiadateľom určenú e-mailovú adresu, v tomto prípade nesmie byť odkaz platný dlhšie ako 24 hodín.
Doba uchovávania registračných dát	Odporúčaná doba je 5 rokov po uplynutí doba platnosti alebo zrušení prostriedkov elektronickej identifikácie.
Fáza elektronickej autentifikácie	
Autentifikačný protokol pre dôkaz o držbe/ overovanie vlastníctva prostriedkov elektronickej identifikácie	Vo väčšine prípadov overovanie vlastníctva pomocou hesla posielaného tunelom, overovanie vlastníctva prostredníctvom jednorazového (alebo silného) hesla, avšak po posúdení miery rizika môže byť aj overovanie vlastníctva prostredníctvom symetrického kľúča, overovanie vlastníctva prostredníctvom privátneho kľúča.
Typ tokenu	Všetky typy tokenu sú prijateľné, okrem prípadu používateľom vybraného hesla. Na minimálnej úrovni sa odporúča náhodne generované heslo alebo PIN, a najlepšie je použiť autentifikačný nástroj na vytváranie jednorazových hesiel.

Pre úroveň 3:

Registračná fáza	
Proces overovania identity, registrácia používateľa, doručovanie tokenov a prostriedkov elektronickej identifikácie	Popis: škody, ktoré môžu vzniknúť zneužitím identity v reálnom svete by mali vysoký vplyv.
	Požiadavky: Token / prostriedky elektronickej identifikácie musia byť vydané orgánom, ktorý je pod štátnym dohľadom. Vyžadovaný je osobný kontakt, počas registrácie žiadateľ predloží oficiálny identifikačný doklad ako napr. občiansky preukaz, cestovný pas alebo vodičské oprávnenie alebo poskytne aspoň dve potvrdenia od neutrálnych a dôveryhodných zdrojov ako sú banky, poisťovne.. Alebo alternatívne nemusí prísť k osobnému kontaktu, registrácia prebehne online na základe údajov predložených žiadateľom, ktoré umožnia jeho jednoznačnú identifikáciu a ktoré sú podpísané zaručeným elektronickým podpisom, ktorý registračná autorita validuje. Alebo alternatívne: nemusí prísť k osobnému kontaktu, registrácia prebehne online na základe údajov predložených žiadateľom, ktoré umožnia jeho jednoznačnú identifikáciu a aspoň jeden z predložených údajov musí byť známy len používateľovi (napr. číslo OP, číslo cestovného pasu..), predložené údaje musia byť overené krížovo s oficiálnym zdrojom identít.
	Doručenie: Minimálne token / prostriedky elektronickej identifikácie musia byť zaslané doporučenou poštou na adresu, po predchádzajúcej validácii žiadateľovej adresy s oficiálnou databázou identít, v ktorej bola fyzická adresa registrovaná.
Doba uchovávania registračných dát	Odporúčaná doba je 7 rokov po uplynutí doba platnosti alebo zrušení prostriedkov elektronickej identifikácie.
Fáza elektronickej autentifikácie	
Autentifikačný protokol pre dôkaz o držbe/overovanie vlastníctva prostriedkov elektronickej identifikácie	Overovanie vlastníctva prostredníctvom jednorazového (alebo silného) hesla, avšak po posúdení miery rizika môže byť aj overovanie vlastníctva prostredníctvom symetrického kľúča, overovanie vlastníctva prostredníctvom privátneho kľúča.
Typ tokenu	Minimálne je vyžadované použitie softvérového kryptografického autentifikačného nástroja alebo autentifikačného nástroja na vytváranie jednorazových hesiel.

Pre úroveň 4:

Registračná fáza	
Proces overovania identity, registrácia používateľa, doručovanie tokenov a prostriedkov elektronickej identifikácie	Popis: škody, ktoré môžu vzniknúť zneužitím identity v reálnom svete by mali veľmi vysoký vplyv. Táto úroveň vyžaduje buď priame alebo nepriame osobné overovanie identity prostredníctvom oficiálnych identifikačných dokladov.
	Požiadavky: Token / prostriedky elektronickej identifikácie musia byť vydané orgánom, ktorý je pod štátnym dohľadom. Registračná autorita musí zabezpečiť aby žiadateľova informácia o identite bola verifikovaná a skontrolovaná v súlade so štátnou registračnou politikou. Vyžaduje sa osobný kontakt, počas registrácie žiadateľ predloží oficiálny identifikačný doklad ako napr. občiansky preukaz, cestovný pas alebo vodičské oprávnenie, ktorý obsahuje

	fotografiu a podpis, a ktorý registračná autorita overila pred vydaním tokenu/ prostriedkov elektronickej identifikácie. Alebo alternatívne nemusí prísť k osobnému kontaktu, registrácia prebehne online na základe údajov predložených žiadateľom, ktoré umožnia jeho jednoznačnú identifikáciu a ktoré sú podpísané využitím zaručeného elektronického podpisu a ktoré registračná autorita validuje. Úroveň 4 vyžaduje aby bol token/ prostriedok elektronickej identifikácie doručený osobne, preto nie je možné aby bola dosiahnutá úroveň 4 bez osobnej identifikácie.
	Doručenie: Token / prostriedok elektronickej identifikácie musí byť odovzdaný žiadateľovi osobne po validácii jeho identity pomocou úradného dokladu totožnosti.
Doba uchovávania registračných dát	Odporúčaná doba je 10 rokov po uplynutí doba platnosti alebo zrušení prostriedku elektronickej identifikácie.
Fáza elektronickej autentifikácie	
Autentifikačný protokol pre dôkaz o držbe overovanie vlastníctva prostriedkov elektronickej identifikácie	Overovanie vlastníctva prostredníctvom symetrického kľúča, overovanie vlastníctva prostredníctvom privátneho kľúča.
Typ tokenu	Len hardvérový kryptografický autentifikačný nástroj.

Záver

Problematika eID je široká a na národnej úrovni doposiaľ nedostatočne riešená. Základné komponenty architektúry integrovaných informačných systémov verejnej správy s dosahom na oblasť elektronickej identity sa centrálne riešia prostredníctvom národných projektov financovaných z OPIS, tak, ako boli zadefinované v NKIVS a následných štúdiách uskutočniteľnosti. Z hľadiska rozvoja potenciálu elektronických služieb verejnej správy by bolo žiaduce zakomponovať do návrhu tých komponentov eID, ktorých stav riešenia to ešte umožňuje, niektoré z identifikovaných kľúčových trendov, prináležiacich k politikám podporujúcim eID. Národné riešenie elektronickej identity by tiež malo priniesť možnosť väčšej miery spolupráce verejného a súkromného sektora. Z pohľadu kompetencií MF SR v oblasti informatizácie spoločnosti je potrebné zadefinovať viacúrovňový mechanizmus autentifikácie elektronických služieb, zakotviť ho v legislatíve a podrobne ho rozpracovať do úrovne štandardov ISVS a metodického pokynu. Návrh národného viacstupňového autentifikačného rámca by mal vychádzať, prípadne sa čo najviac približovať riešeniam ktoré dosiahli medzinárodný konsenzus na úrovni EÚ.

Príloha

Procesný model najčastejšie používaných autentifikačných riešení

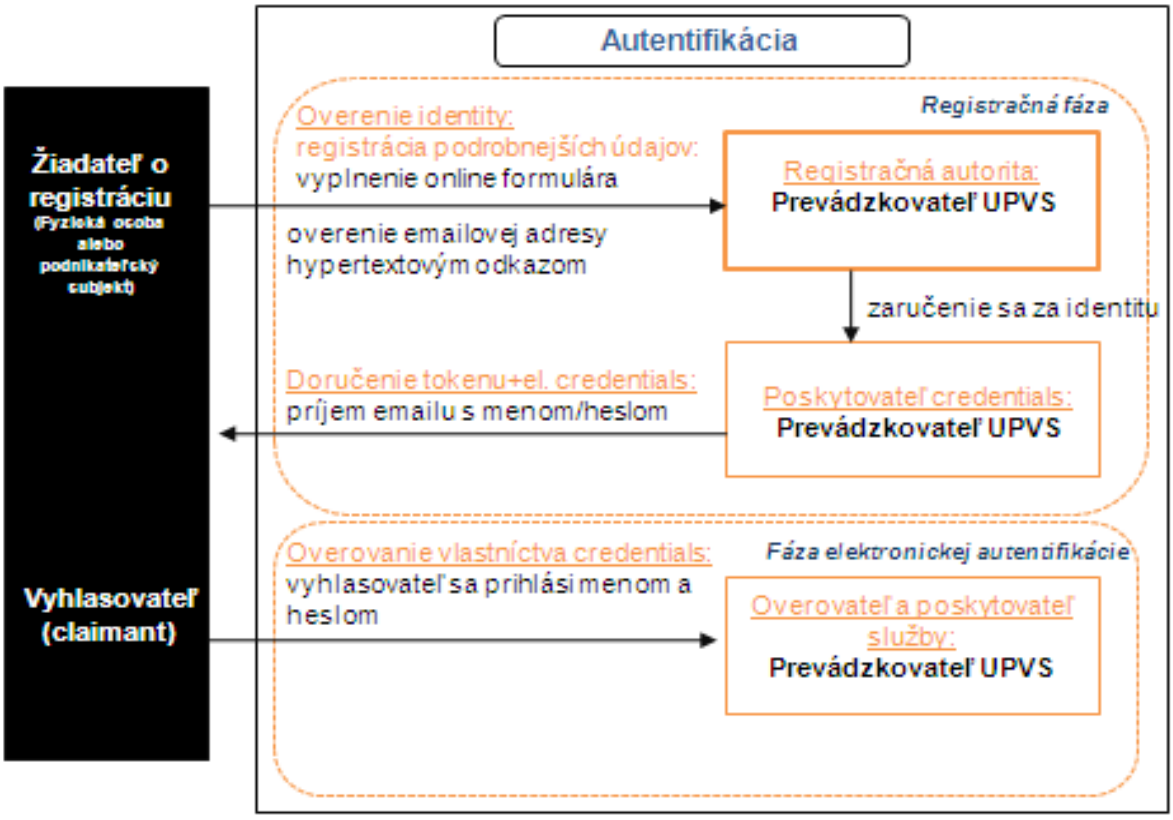
Elektronické služby verejnej správy v Slovenskej republike využívajúce autentifikáciu by sme mohli zhruba rozdeliť do niekoľkých úrovní zabezpečenia. Tieto úrovne zabezpečenia autentifikačného mechanizmu sú však len indikatívne, nie sú nikde stanovené a jedná sa skôr o najčastejšie používané riešenia zoskupené podľa príbuzných znakov. Ide o úrovne zabezpečenia uvedené v kapitole Slovensko – aktuálny stav autentifikačných riešení, pričom popísané autentifikačné riešenie je v tejto prílohe podrobnejšie popísané a pre názornosť je zobrazené v procesnom modeli. Všeobecný procesný model je popísaný v kapitole Slovensko – návrh strategického smerovania v oblasti elektronickej autentifikácie (popis procesného modelu autentifikácie).

Prvá úroveň:

Elektronické služby verejnej správy nevyžadujúce žiadnu autentifikáciu, napríklad online prístup k základným údajom katastra nehnuteľností, vrátane možnosti vytvárať rôzne zostavy a sledovať status katastrálneho konania.

Druhá úroveň:

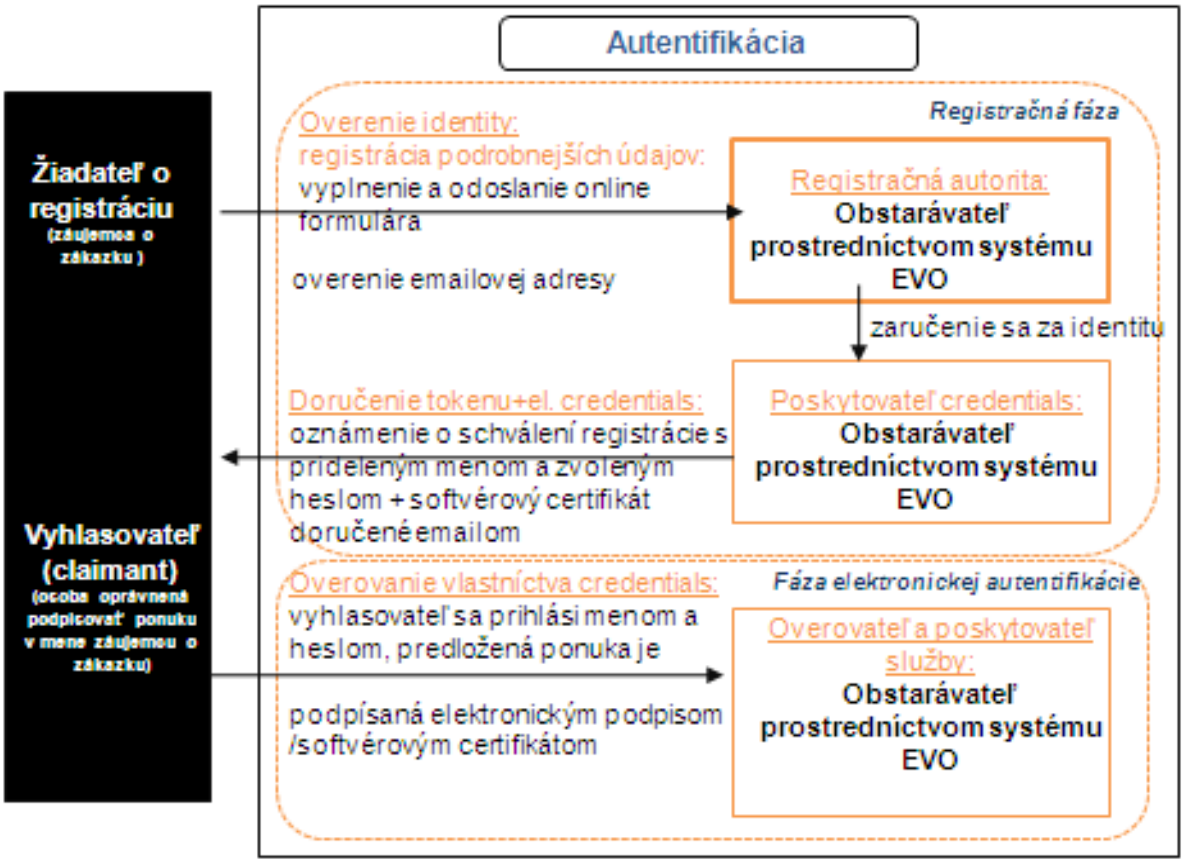
Služby s autentifikáciou prostredníctvom mena a hesla používateľa, napr. niektoré služby ústredného portálu verejnej správy. Prístup k určitým službám ÚPVS je poskytovaný akejkoľvek registrovanej entite, pričom registrácia pozostáva z vyplnenia a zaslania online formulára. Platný emailový účet slúži potom k aktivácii vytvoreného konta prostredníctvom hypertextového odkazu doručeného e-mailom. Ďalšie služby dostupné prostredníctvom ÚPVS, napríklad prístup k elektronickým službám Obchodného registra, však už vyžadujú autentifikáciu na úrovni č. 4 až 5.



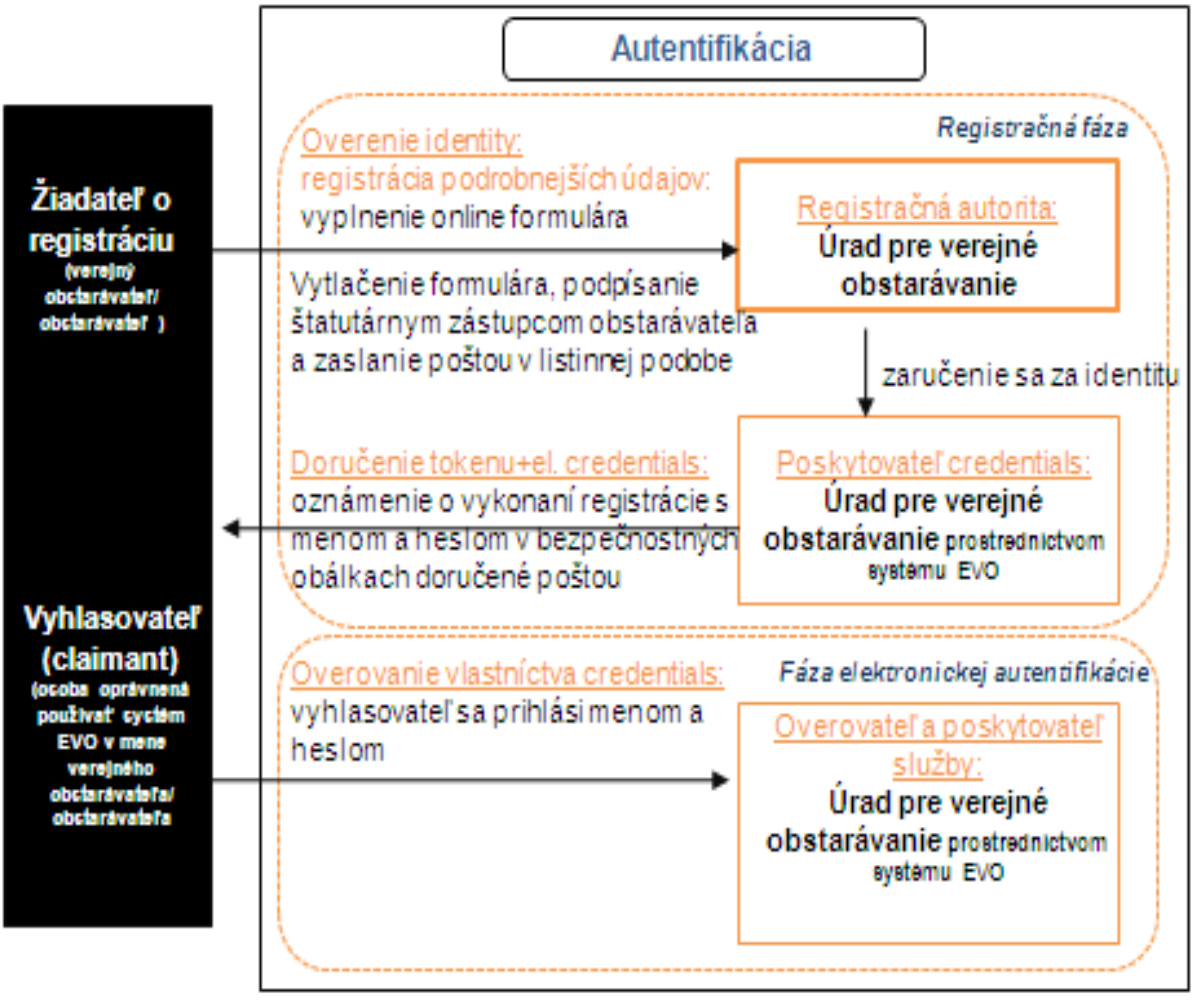
Tretia úroveň:

Do tretej úrovne môžeme zaradiť služby s autentifikáciou s použitím softvérových certifikátov, prípadne služby s autentifikáciou prostredníctvom mena a hesla podobne ako v druhej úrovni, avšak s podstatne dôveryhodnejšou formou registrácie. Sú to napríklad elektronické služby verejného obstarávania (ďalej ako „EVO“) prevádzkované Úradom pre verejné obstarávanie (ďalej ako „ÚVO“), ktoré podporujú zatiaľ tri fázy verejného obstarávania – vyhlásenie verejného obstarávania (eNotification), predkladanie ponúk (eTendering) a vyhodnocovanie ponúk (eAwarding).

Príkladom elektronickej služby kde je použitá autentifikácia prostredníctvom softvérového certifikátu je predkladanie ponúk záujemcami o zákazku prostredníctvom EVO. Záujemca o zákazku má možnosť prihlásiť sa do verejnej súťaže. Po vybratí zákazky, o ktorú sa chce uchádzať, sa musí registrovať vyplnením online registračného formulára prostredníctvom systému EVO, vrátane zadania emailovej adresy a zvolenia si hesla. Užívateľské meno mu je pridelené systémom EVO v čase registrácie, pričom je pre každú zákazku jedinečné a nedá sa použiť na prihlásenie do inej zákazky. Vo formulári je tiež označená osoba, ktorá žiada o registráciu a je oprávnená podpisovať ponuku v mene spoločnosti/záujemcu. Táto osoba obdrží súbor s elektronickým podpisom (softvérový certifikát) a len táto osoba môže podpisovať ponuku a predkladať v systéme EVO platné dokumenty tvoriace ponuku. Po odoslaní žiadosti o registráciu cez systém EVO nasleduje schválenie registrácie verejným obstarávateľom/obstarávateľom. Potvrdenie o registrácii obdrží žiadateľ o registráciu, pričom osoba oprávnená podpisovať ponuku v mene spoločnosti/záujemcu obdrží aj softvérový certifikát elektronickou poštou na zadanú e-mailovú adresu. Na prihlásenie sa do zvolenej zákazky použije registrovaný záujemca pridelené užívateľské meno a heslo zvolené pri registrácii. Predkladanie ponuky ukončí vytvorením sprievodného listu so zoznamom priložených dokumentov, ktorý sa po podpísaní elektronickým podpisom/softvérovým certifikátom odošle prostredníctvom systému EVO obstarávateľovi.



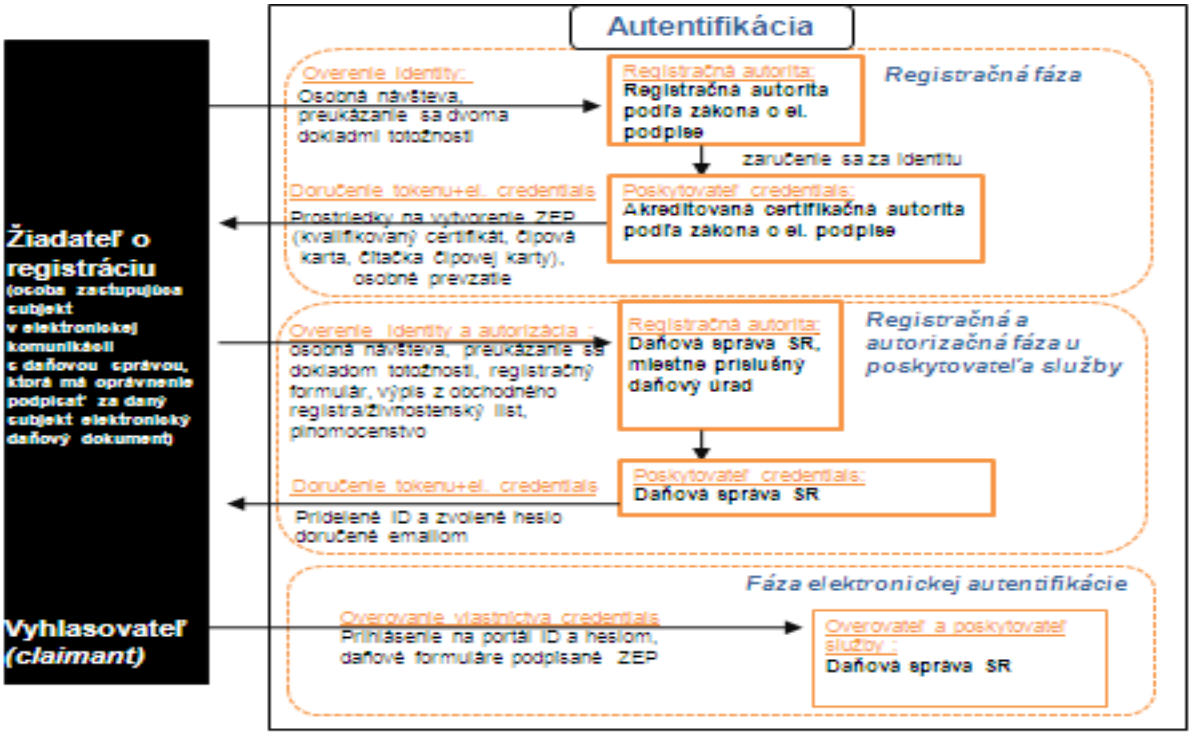
Príkladom elektronickej služby kde je použitá autentifikácia prostredníctvom mena a hesla podobne ako v druhej úrovni, avšak s podstatne dôveryhodnejšou formou registrácie je používanie systému EVO pre verejných obstarávateľov a obstarávateľov (ďalej len „obstarávateľov“). Pred prvým použitím systému musí byť obstarávateľ registrovaný, pričom pre registráciu musí obstarávateľ vyplniť registračný formulár dostupný na internetových stránkach. Registračný formulár je rozdelený do dvoch častí. Prvá časť obsahuje informácie o obstarávateľovi, vyžadovaný je aj zoznam osôb oprávnených používať systém EVO v mene obstarávateľa. Pre registráciu je vyžadovaná identifikácia rozsahu prístupových práv a rozsahu práce pre užívateľa. Druhá časť obsahuje osobné identifikačné údaje o všetkých osobách, ktoré sú definované v prvej časti registračného formulára. Vyplnený formulár musí byť vytlačený, pričom prvá časť je podpísaná štatutárnym zástupcom obstarávateľa, druhá časť je podpísaná osobou (prípadne osobami), ktoré budú oprávnené používať systém EVO v mene obstarávateľa. Následne sa formulár výlučne v listinnej podobe zašle poštou do kancelárie ÚVO. Registrácia je schvaľovaná ÚVO. Po úspešnom zaregistrovaní organizácie do systému EVO zašle ÚVO obstarávateľovi oznámenie o vykonaní registrácie. Prílohu oznámenia tvoria bezpečnostné obálky obsahujúce autentifikačné údaje (užívateľské meno a prístupové heslo) pre každého z oprávnených zamestnancov. EVO používa pri komunikácii s oprávnenými osobami zabezpečený https protokol.



Štvrtá úroveň:

Služby s autentifikáciou prostredníctvom kvalifikovaného certifikátu – so zaručeným elektronickým podpisom a s potrebou registračného a autorizačného procesu u poskytovateľa služby, napr. jedna z online elektronických služieb poskytovaných Daňovou správou SR. Pre používanie tejto služby, používateľ (osoba zastupujúca subjekt v elektronickej komunikácii s daňovou správou, ktorá má oprávnenie podpísať za daný subjekt elektronický daňový dokument) musí vlastniť prostriedky na vytvorenie zaručeného elektronického podpisu, a to kvalifikovaný certifikát, čipovú kartu certifikovanú Národným bezpečnostným úradom SR a čítačku čipovej karty, ktoré sú vydávané akreditovanou certifikačnou autoritou. Pre registráciu používateľa (za účelom získania zaručeného elektronického podpisu) je potrebná osobná návšteva žiadateľa o registráciu v kancelárii registračnej autority. V procese registrácie je identita používateľa potvrdená dvomi dokladmi totožnosti. Primárnym dokladom totožnosti je občiansky preukaz alebo cestovný pas, prípadne povolenie na trvalý pobyt pre občana tretích krajín, ktorý chce mať v kvalifikovanom certifikáte uvedené rodné číslo v zmysle platnej legislatívy. Sekundárnym dokladom totožnosti je napríklad vodičský preukaz, zbrojný preukaz, služobný preukaz, preukaz poistenca zdravotného poistenia, prípadne cestovný pas ak nebol predložený ako primárny doklad. Kvalifikovaný certifikát, čipová karta a čítačka sú dodávané vždy pri osobnej návšteve registračnej autority.

Vo všeobecnosti, pred prvým použitím služby, je nevyhnutná registrácia a autorizácia u poskytovateľa služby. Pri registrácii uvedie používateľ svoje základné identifikačné údaje (napr. meno, priezvisko, adresa, rodné číslo/číslo pasu), kontaktné údaje (napr. telefónne číslo, fax, e-mailová adresa) a autentifikačné údaje (heslo, osobný identifikačný kód, kontrolná otázka a odpovede v prípade požiadavky na generovanie nového hesla). Výsledkom registrácie je pridelenie ID používateľa, ktoré sa použije ako prihlasovací údaj na vstup do autorizovanej zóny portálu. Používateľovi je automaticky generovaný Registračný formulár používateľa vo formáte PDF. Tento dokument je odoslaný spolu s potvrdením o realizovanej registrácii na e-mailovú adresu používateľa, ktorú uviedol pri vypĺňaní registračného formulára. Autorizácia predstavuje proces overenia oprávnenia registrovaného používateľa konať v mene daňového subjektu alebo za daňový subjekt pred správcom dane pri využívaní Autorizovaných elektronických služieb. Pri autorizácii používateľa na miestne príslušnom daňovom úrade je potrebné predložiť osobný identifikačný doklad (občiansky preukaz, pas), registračný formulár, živnostenský list, výpis z obchodného registra alebo iného obdobného registra, plnomocenstvo na využívanie Autorizovaných elektronických služieb v prípade, ak si daňový subjekt zvolí zástupcu. Po vytvorení konta na portáli Daňového riaditeľstva SR, sa používateľ prihlási na portál cez ID pridelené v procese registrácie a zvolené heslo.



Piata úroveň:

Služby s autentifikáciou prostredníctvom kvalifikovaného certifikátu – so zaručeným elektronickým podpisom obsahujúcim jednotný identifikátor (v súčasnosti rodné číslo) a s potrebou registrácie u poskytovateľa služby. Od predchádzajúcej úrovne sa líši tým, že pred získaním prístupu ku službe nie je potrebná osobná návšteva u poskytovateľa služby. Príkladom takýchto elektronických služieb sú napríklad elektronické služby colnej správy. Pre používanie týchto služieb, používateľ (osoba zastupujúca subjekt v elektronickej komunikácii s colnou správou, ktorá má oprávnenie podpísať za daný subjekt elektronický dokument) musí vlastniť prostriedky na vytvorenie zaručeného elektronického podpisu, a to kvalifikovaný certifikát, čipovú kartu certifikovanú Národným bezpečnostným úradom SR a čítačku čipovej karty, ktoré sú vydávané akreditovanou certifikačnou autoritou. Pre registráciu používateľa (za účelom získania zaručeného elektronického podpisu) je potrebná osobná návšteva žiadateľa o registráciu v kancelárii registračnej autority. V procese registrácie je identita používateľa potvrdená dvomi dokladmi totožnosti. Primárnym dokladom totožnosti je občiansky preukaz alebo cestovný pas, prípadne povolenie na trvalý pobyt pre občana tretích krajín, ktorý chce mať v kvalifikovanom certifikáte uvedené rodné číslo v zmysle platnej legislatívy. Sekundárnym dokladom totožnosti je napríklad vodičský preukaz, zbrojný preukaz, služobný preukaz, preukaz poistenca zdravotného poistenia, prípadne cestovný pas ak nebol predložený ako primárny doklad. Kvalifikovaný certifikát, čipová karta a čítačka sú dodávané vždy pri osobnej návšteve registračnej autority.

Podmienkou využívania elektronických služieb colnej správy je podpísanie dohody o používaní zaručeného elektronického podpisu pri využívaní vybraných elektronických služieb colnej správy medzi používateľom elektronických služieb a colnou správou. Návrh dohody v dvoch rovnopisoch, vrátane prílohy „Technické parametre elektronickej komunikácie“, ako aj originál alebo overený výpis z obchodného registra alebo overenú fotokópiu živnostenského listu je potrebné doručiť na Colné riaditeľstvo SR. Vyššie uvedené dokumenty musí podpísať štatutárny zástupca navrhovateľa, pričom sa nevyžaduje overenie tohto podpisu. Doručenie sa môže uskutočniť podaním vyššie uvedených dokumentov na ktorejkoľvek pobočke colného úradu, osobným doručením do podateľne Colného riaditeľstva SR, alebo zaslaním poštou na adresu Colného riaditeľstva SR. Colné riaditeľstvo SR doručí späť navrhovateľovi platnú dohodu. V nej je uvedené „evidenčné číslo“, ktoré slúži pre identifikáciu subjektu pri elektronickej komunikácii. Pre prihlásenie na komunikáciu a získanie prístupu na portál prostredníctvom mena a hesla je potrebné zaslať na Colné riaditeľstvo SR požiadavku na pridelenie prihlasovacieho mena a hesla na príslušnom tlačive. Pridelené meno a heslo je doručené emailom.