Ministerstvo zdravotnictví České republiky
Palackého nám. č 4, 128 01 Praha 2, IČ: 00024341

Národní strategie elektronického zdravotnictví

Analýza cílové architektury registrů ve zdravotnictví včetně řešení elektronické identity a dalších dopadů nařízení eIDAS

Příloha 2

Analýza a návrh řešení dopadů nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce

Dokument	Analýza cílové architektury registrů ve zdravotnictví včetně řešení elektronické identity a dalších dopadů nařízení eIDAS, Příloha č. 2
Status	Draft k dalšímu využití
Distribuce	Ke zveřejnění

Verze	Datum	Zpracoval	Za správnost	Schválil
1.0	31. 7. 2016	Odbor informatiky MZ ČR	Útvar hlavního architekta elektronizace zdravotnictví	Ředitel odboru informatiky

Obsah

Seznam tabulek

Seznam obrázků

Slovník pojmů

Pojem	Definice, vysvětlení
AS-IS (stav)	Popis současného stavu.
Autentizace	Elektronický postup, který umožňuje potvrdit elektronickou identifikaci fyzické či právnické osoby nebo původ a integritu dat v elektronické podobě (č. 3 odst. 5 nařízení eIDAS).
Autentizace internetových stránek	Návštěvník určitých internetových stránek se pomocí prostředků poskytnutých certifikačními službami pro autentizaci internetových stránek může ujistit, že tyto stránky reprezentují skutečný a legitimní subjekt (důvod 67 nařízení eIDAS).
Autorizace	Přidělení přístupových práv uživateli po jeho úspěšné autentizaci. Prokázání oprávnění (již dříve autentizovaného uživatele).
Certifikát (pro elektronický podpis)	Elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických podpisů s určitou fyzickou osobou a potvrzuje alespoň jméno nebo pseudonym této osoby (čl. 3 odst. 14 nařízení eIDAS).
Certifikát pro autentizaci internetových stránek	Potvrzení, které umožňuje autentizovat internetové stránky a spojuje je s fyzickou nebo právnickou osobou, jíž je certifikát vydán (čl. 3 odst. 38 nařízení eIDAS).
Certifikát pro elektronickou pečeť	Elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických pečetí s určitou právnickou osobou a potvrzuje název této osoby (čl. 3 odst. 29 nařízení eIDAS).
CzechPOINT	Kontaktní místo veřejné správy, poskytující občanům zejména ověřené údaje vedené v centrálních registrech. (Tzv. Český Podací Ověřovací a Informační Národní Terminál, součást eGovernmentu.)
Data pro vytváření elektronických podpisů a pečetí	Soukromý klíč ve správě podepisující / pečetící osoby nebo kvalifikovaného poskytovatele služeb.
Důvěryhodné seznamy	Seznamy, které udávají stav kvalifikace poskytovatele služeb v době dohledu (důvod 46 nařízení eIDAS). Seznamy obsahují informace týkající se kvalifikovaných poskytovatelů služeb vytvářejících důvěru v působnosti členského státu spolu s informacemi o jimi poskytovaných kvalifikovaných službách vytvářejících důvěru.
Elektronická identifikace	Postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu (čl. 3 odst. 1 nařízení eIDAS).
Elektronická pečeť	Data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu (čl. 3 odst. 25 nařízení eIDAS). Obdoba elektronického podpisu u právnických osob. Slouží jako důkaz toho, že elektronický dokument vydala určitá právnická osoba.
Elektronická značka	Údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které splňují požadavky zákona č. 227/200 Sb. o elektronickém podpisu.

Pojem	Definice, vysvětlení
Elektronické časové razítko	Data v elektronické podobě, která spojují jiná data v elektronické podobě s určitým okamžikem a prokazují, že tato jiná data existovala v daném okamžiku (čl. 3 odst. 33 nařízení eIDAS).
Elektronický dokument	Jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka (čl. 3 odst. 35 nařízení eIDAS).
Elektronický podpis	Data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena, a která podepisující osoba používá k podepsání (čl. 3 odst. 10 nařízení eIDAS).
Kvalifikovaná elektronická pečeť	Zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť (čl. 3 odst. 27 nařízení eIDAS).
Kvalifikovaná služba elektronického doporučeného doručování	Služba elektronického doporučeného doručování, která splňuje požadavky stanovené v článku 44 nařízení eIDAS (čl. 3 odst. 37 nařízení eIDAS).
Kvalifikovaná služba vytvářející důvěru	Služba vytvářející důvěru, která splňuje použitelné požadavky stanovené v nařízení eIDAS. Splňuje požadavky a povinnosti, které zajistí vysokou úroveň bezpečnosti používaných nebo poskytovaných služeb a produktů (důvod 28 nařízení eIDAS).
Kvalifikované elektronické časové razítko	Elektronické časové razítko, které splňuje požadavky stanovené v článku 42 nařízení eIDAS (čl. 3 odst. 34 nařízení eIDAS).
Kvalifikované uchovávání kvalifikovaných elektronických podpisů	Kvalifikovanou službu uchovávání kvalifikovaných elektronických podpisů může poskytovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru, který používá postupy a technologie, jež jsou s to zajistit důvěryhodnost kvalifikovaného elektronického podpisu i po uplynutí doby technické platnosti.
Kvalifikovaný certifikát pro elektronický podpis	Certifikát pro elektronický podpis, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze I nařízení eIDAS (čl. 3 odst. 15 nařízení eIDAS).
Kvalifikovaný certifikát pro autentizaci internetových stránek	Certifikát pro autentizaci internetových stránek, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze IV nařízení eIDAS (čl. 3 odst. 39 nařízení eIDAS).
Kvalifikovaný certifikát pro elektronickou pečeť	Certifikát pro elektronickou pečeť, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze III nařízení eIDAS (čl. 3 odst. 30 nařízení eIDAS).
Kvalifikovaný elektronický podpis	Zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy (čl. 3 odst. 12 nařízení eIDAS). Má rovnocenný právní účinek jako podpis vlastnoruční.

Pojem	Definice, vysvětlení
Kvalifikovaný poskytovatel služeb vytvářejících důvěru	Poskytovatel služeb vytvářejících důvěru, který poskytuje jednu či více kvalifikovaných služeb vytvářejících důvěru a kterému orgán dohledu udělil status kvalifikovaného poskytovatele (čl. 3 odst. 20 nařízení eIDAS).
Kvalifikovaný prostředek pro vytváření elektronických pečetí	Prostředek pro vytváření elektronických pečetí, který přiměřeně splňuje požadavky stanovené v příloze II nařízení eIDAS (čl. 3 odst. 32 nařízení eIDAS).
Kvalifikovaný prostředek pro vytváření elektronických podpisů	Prostředek pro vytváření elektronických podpisů, který splňuje požadavky stanovené v příloze II nařízení eIDAS (čl. 3 odst. 23 nařízení eIDAS). Jde o zařízení, na němž je vytvářen kvalifikovaný elektronický podpis.
Nařízení eIDAS	Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, včetně návazných právních předpisů.
Návrh adaptačního zákona	Návrh zákona o službách vytvářejících důvěru pro elektronické transakce a o změně některých zákonů.
Nekvalifikovaný poskytovatel služeb vytvářejících důvěru	Poskytovatel služeb vytvářejících důvěru, kterému nebyl udělen status kvalifikovaného poskytovatele.
Orgán dohledu	Subjekt, který vykonává činnosti v oblasti dohledu podle nařízení eIDAS (důvod 30 nařízení eIDAS).
Osobní identifikační údaje	Soubor údajů umožňujících určit totožnost fyzické či právnické osoby nebo fyzické osoby zastupující právnickou osobu (čl. 3 odst. 3 nařízení eIDAS).
Oznámený systém elektronické identifikace	Systém pro elektronickou identifikaci, (na jehož základě jsou fyzickým či právnickým osobám nebo fyzickým osobám zastupujícím právnické osoby vydávány prostředky pro elektronickou identifikaci), který je uvedený na seznamu zveřejněném Komisí podle článku 9 nařízení eIDAS.
Poskytovatel služeb vytvářejících důvěru	Fyzická nebo právnická osoba, která poskytuje jednu či více služeb vytvářejících důvěru buď jako kvalifikovaný, nebo jako nekvalifikovaný poskytovatel služeb vytvářejících důvěru (čl. 3 odst. 19 nařízení eIDAS).
Posuzování shody	Posuzování, zda kvalifikovaní poskytovatelé služeb vytvářejících důvěru a jimi poskytované služby splňují požadavky stanovené v nařízení eIDAS.
Prostředek pro elektronickou identifikaci	Hmotná či nehmotná jednotka obsahující osobní identifikační údaje, která se používá k autentizaci pro účely on-line služby (čl. 3 odst. 2 nařízení eIDAS).
Prostředek pro vytváření elektronických pečetí	Konfigurované programové vybavení nebo technické zařízení, které se používá k vytváření elektronických pečetí (čl. 3 odst. 31 nařízení eIDAS).

Pojem	Definice, vysvětlení
Prostředek pro vytváření elektronických podpisů	Konfigurované programové vybavení nebo technické zařízení, které se používá k vytváření elektronických podpisů (čl. 3 odst. 22 nařízení eIDAS).
Služba elektronického doporučeného doručování	Služba, která umožňuje přenášet data mezi třetími osobami elektronickými prostředky a poskytuje důkazy týkající se nakládání s přenášenými daty, včetně dokladu o odeslání a přijetí dat, a která chrání přenášená data před rizikem ztráty, odcizení, poškození nebo neoprávněných změn (čl. 3 odst. 36 nařízení eIDAS).
Služba vytvářející důvěru	Elektronická služba, která je zpravidla poskytována za úplatu a spočívá: (čl. 3 odst. 16 nařízení eIDAS.) a) ve vytváření, ověřování shody a ověřování platnosti elektronických podpisů, elektronických pečetí nebo elektronických časových razítek, služeb elektronického doporučeného doručování a certifikátů souvisejících s těmito službami nebo b) ve vytváření, ověřování shody a ověřování platnosti certifikátů pro autentizaci internetových stránek nebo c) v uchovávání elektronických podpisů, pečetí nebo certifikátů souvisejících s těmito službami.
Subjekt odpovědný za vedení důvěryhodných seznamů	Subjekt odpovědný za zřízení, udržování a zveřejnění vnitrostátních důvěryhodných seznamů. Subjekty určují členské státy EU a informace o nich sdělují Komisi EU.
Subjekt posuzování shody	Subjekt vymezený v čl. 2 bodě 13 nařízení (ES) č. 765/2008, který je v souladu s uvedeným nařízením akreditován jako způsobilý provádět posuzování shody kvalifikovaného poskytovatele služeb vytvářejících důvěru a jím poskytovaných kvalifikovaných služeb vytvářejících důvěru (čl. 3 odst. 18 nařízení eIDAS).
Systém elektronické identifikace	Systém, na jehož základě jsou fyzickým či právnickým osobám nebo fyzickým osobám zastupujícím právnické osoby vydávány prostředky pro elektronickou identifikaci (čl. 3 odst. 4 nařízení eIDAS).
TO-BE (stav)	Popis budoucího (cílového) stavu.
Úroveň záruky prostředků pro elektronickou identifikaci	Oznámený systém elektronické identifikace musí uvádět nízkou, značnou nebo vysokou úroveň záruky pro prostředky pro elektronickou identifikaci vydávané v rámci tohoto systému. Nízká, značná a vysoká úroveň záruky vyjadřuje míru jistoty, že prostředek vlastní a používá osoba, pro niž byl vydán. Minimální technické specifikace a postupy pro úrovně záruky jsou stanoveny v prováděcím nařízení komise EU 2015/1502.
Zaručená elektronická pečeť	Elektronická pečeť, která splňuje požadavky stanovené v článku 36 nařízení eIDAS (čl. 3 odst. 26 nařízení eIDAS).
Zaručený elektronický podpis	Elektronický podpis, který splňuje požadavky stanovené v článku 26 nařízení eIDAS (čl. 3 odst. 11 nařízení eIDAS).
Značka důvěry EU	Označení, které označuje kvalifikované služby vytvářející důvěru poskytované kvalifikovanými poskytovateli služeb vytvářejících důvěru a jasně odlišuje tyto služby od ostatních služeb vytvářejících důvěru (čl. 23 nařízení eIDAS).

Seznam zkratek

Zkratka	Význam
AAA	Subsystém pro správu uživatelů a přístupů
AIS	Agendový informační systém
API	Aplikační programovací rozhraní (Application Programming Interface)
APV	Aplikační a programové vybavení
B2B	Koncept týkající se obchodních vztahů a vzájemné komunikace mezi dvěma společnostmi (Business to Business)
CA	Certifikační autorita
CA/B	Fórum pro certifikační orgány a vyhledávače (https://cabforum.org/)
CMS	Centrální místo služeb
CRL	Seznam revokovaných certifikátů (Certificate Revocation List)
ČR	Česká republika
DB	Databáze
DMS	Systém pro správu dokumentů (Document Management System)
DMZ	Síť vložená mezi chráněnou a vnější síť za účelem zajištění dalšího stupně zabezpečení (Demilitarized Zone). Do této sítě se umisťují zařízení (servery), která mají komunikovat s vnějšími účastníky anebo zařízení se zvýšenou ochranou.
DNS	Hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace (Domain Name System). Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě.
DOC	Formát dokumentů firmy Microsoft
DS	Datová schránka
DZ	Datová zpráva
eID	Elektronická identita
eIDAS	Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (Electronic Identification and Trust Services)
ENISA	Agentura Evropské unie pro bezpečnost sítí a informací
eOP	Elektronický občanský průkaz
EPDZ	Elektronická podatelna datových zpráv
ES	Evropské společenství

Zkratka	Význam
ESB	Sběrnice služeb pro implementaci služeb servisně orientované architektury (Enterprise Service Bus)
ESI	Pracovní skupina v rámci ETSI
ESS	Elektronická spisová služba
ETSI	Evropský ústav pro telekomunikační normy
EU	Evropská unie
FO	Fyzická osoba
G2G	Komunikace typu B2B mezi úřady veřejné správy
HW	Technické vybavení počítače (hardware)
HTML	Název značkovacího jazyka používaného pro tvorbu webových stránek, které jsou propojeny hypertextovými odkazy (HyperText Markup Language)
HTTP	Internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML (Hypertext Transfer Protocol)
HTTPS	Nadstavba síťového protokolu HTTP, která umožňuje zabezpečit spojení mezi webovým prohlížečem a webovým serverem před odposloucháváním, podvržením dat a umožňuje též ověřit identitu protistrany (Hypertext Transfer Protocol Secure)
IČO	Identifikační číslo organizace
ID	Identifikátor
IP	Číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP (internetový protokol).
IS	Informační systém
ISDS	Informační systém datových schránek
ISZR	Informační systém základních registrů
IT	Informační technologie
MV	Ministerstvo vnitra
NIA	Národní identitní autorita ČR
OTP	Jednorázové heslo (One Time Password)
OVM	Orgán veřejné moci
PDF	Formát dokumentů firmy Adobe (Portable Document Format)
PEPS	Národní autentizační brány (Pan-European Proxy Services)
PIN	Číselná kombinace, která uživateli umožňuje autentizovat se do systému nebo zařízení (Personal Identification Number)
PO	Právnická osoba
PVS	Portál veřejné správy

Zkratka	Význam
RČ	Rodné číslo
RPP	Registr práv a povinností
SMS	Textová zpráva
SOAP	Protokol pro výměnu zpráv založených na XML (Simple Object Access Protocol)
SQL	Standardizovaný strukturovaný dotazovací jazyk, který je používán pro práci s daty v relačních databázích (Structured Query Language)
SSIP	Systém pro správu identit a pověření
SSL (protokol)	Protokol, resp. vrstva vložená mezi vrstvu transportní a aplikační, která poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran (Secure Socket Layer)
STORK, STORK II	Projekty, jejichž cílem bylo prakticky vyzkoušet možnosti přeshraničního uznávání elektronických identit
SW	Programové vybavení (software)
TLS (protokol)	Kryptografické protokoly, poskytující možnost zabezpečené komunikace na Internetu pro služby jako WWW, elektronická pošta, internetový fax a další datové přenosy (Transport Layer Security)
TSL	Důvěryhodné seznamy, seznamy kvalifikovaných poskytovatelů služeb poskytujících důvěru (Trusted Services Lists)
URL	Uniform Resource Locator (jednotná adresa zdroje) je řetězec znaků s definovanou strukturou, který slouží k přesné specifikaci umístění zdrojů informací (ve smyslu dokument nebo služba) na Internetu
USB	Univerzální sériová sběrnice, moderní způsob připojení periferií k počítači (Universal Serial Bus)
VPZS	Veřejnoprávní zdravotnický subjekt
VS	Veřejná správa
WS	Webová služba
XML	Obecný značkovací jazyk, který byl vyvinut a standardizován konsorciem W3C (Extensible Markup Language)

1 Rekapitulace zadání

Předkládaný dokument je součástí analýzy a návrhu cílové architektury registrů ve zdravotnictví a návrhu konceptu sdílených služeb elektronického zdravotnictví. **Jedná se o průběžnou verzi dokumentu, která je určená pro připomínkování členy projektového týmu MZČR EA. Tato verze není určena pro distribuci mimo tento projektový tým.**

Jedna z hlavních sdílených služeb ve zdravotnictví je služba identifikace, autentizace a autorizace subjektů ve zdravotnictví zejména pracovníků ve zdravotnictví a pacientů. Návrh cílového řešení musí vycházet z nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále jen „nařízení eIDAS“), které dne 1. července 2016 nabývá účinnosti.

Nařízení eIDAS stanovuje novou právní úpravu dvou oblastí, které jsou nezbytné k posílení jednotného digitálního trhu a přeshraničních digitálních služeb. První oblast obsahuje právní úpravu uznávání elektronické identifikace fyzických a právnických osob napříč unijními státy s vysokou mírou bezpečnosti a interoperability. Druhou oblast tvoří právní úprava služeb vytvářejících důvěru, která nahradí stávající vnitrostátní právní předpisy k elektronickému podpisu.

Cílem dokumentu je analyzovat a navrhnout řešení dopadů nařízení eIDAS a z něj vyplývajícího vnitrostátního adaptačního zákona na služby v resortu zdravotnictví, zejména na identifikaci a autentizaci zdravotních profesionálů a pacientů, ePreskripci, výměnu zdravotní dokumentace a na základní informační infrastrukturu.

Pro analýzu dopadů nařízení eIDAS na organizace resortu zdravotnictví je nezbytné zdůraznit skutečnost, že povinnosti nařízení se vztahují primárně na subjekty veřejného práva. Pro účely této analýzy proto definujeme pojem **veřejnoprávní zdravotnický subjekt** (dále též „**VPZS**“), kterým jsou chápany především Ministerstvo zdravotnictví a jím zřizované organizace a zdravotní pojišťovny.

2 Popis současného stavu a identifikace problémových oblastí

2.1 Úvod

Řešení autorizace, autentizace, řízení oprávnění, souhlasů a přístupů je ve zdravotnických informačních systémech implementováno s ohledem na místní podmínky: neexistence centrálního autentizačního mechanismu pro zdravotnické pracovníky či pro pacienty dává prostor pro lokální řešení tam, kde pro provozování konkrétní aplikace je takový mechanismus zapotřebí, ať je to přístup k některým databázím Národního zdravotnického informačního systému či přístup k informačním systémům či jiným aplikacím provozovaným jednotlivými zdravotnickými zařízeními.

2.2 Východiska

2.2.1 Strategický rámec

Mezi nejvýznamnější iniciativy v oblasti budování jednotného digitálního trhu patří Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále též „nařízení eIDAS“), jakožto jedno z klíčových opatření Aktu o jednotném trhu a má za cíl zvýšit důvěryhodnost elektronických transakcí v rámci vnitřního trhu EU. Komise zde navazuje na úkoly vytyčené v Digitální agendě pro Evropu, jako jsou řešení technologie elektronické totožnosti, zajištění interoperability na základě norem a otevřených vývojových platforem, vytváření digitální důvěry.

Národní strategie elektronického zdravotnictví (2015, soustava cílů a opatření) se identifikací, autentizací a autorizací poskytovatelů zdravotních služeb i pacientů zabývá ve svém strategickém cíli 4 Správa elektronického zdravotnictví, konkrétně ve specifickém cíli 4.1 Rozvoj infrastruktury pro sdílení a poskytování zdravotních služeb, a to zejména v následujících opatřeních:

- opatření 4.1.5 Autorizace, autentizace a řízení oprávnění poskytovatelů
- opatření 4.1.7 Snadná a přesná identifikace pacienta a získávání pacientských údajů

Požadavek na zasazení systému elektronického zdravotnictví do kontextu vzájemného uznávání eID a dalších důvěryhodných služeb v návaznosti na Digitální agendu EU byl vznesen i v Národní koncepci elektronického zdravotnictví 2013.

Strategie rozvoje ICT služeb veřejné správy a její opatření na zefektivnění ITC služeb ve svém strategickém cíli C7 Od izolovaných identitních systémů k jednotným identitním systémům uživatelů služeb veřejné správy a úředníků veřejné správy stanovuje úkol navrhnout a implementovat jednotnou identifikaci a autentizaci občanů ČR vůči VS.

2.2.2 Právní rámec

2.2.2.1 Evropské právo – nařízení eIDAS a jeho prováděcí akty

V evropském měřítku je nejzásadnějším právním předpisem, řešícím oblast elektronické identifikace a autentizace (a služeb vytvářejících důvěru pro elektronické transakce), Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (tzv. „nařízení eIDAS“).

Nařízení eIDAS je doplněno dalšími prováděcími akty, jako jsou prováděcí nařízení a prováděcí rozhodnutí Komise (EU).

2.2.2.2 Vnitrostátní právní předpisy

2.2.2.2.1 Stávající právní úprava

Nařízení eIDAS nahrazuje směrnici 1999/93/ES, jejíž implementací do českého národního práva je zákon č. 227/2000 Sb. o elektronickém podpisu, který upravuje podmínky pro vytvoření jednotného digitálního trhu EU usnadněním přeshraničního využívání on-line služeb a zvláštní pozornost věnuje usnadnění bezpečné elektronické identifikace a autentizace.

Zákon č. 227/200 Sb. bude zrušen nabytím účinnosti návrhu adaptačního zákona, stejně jako budou zrušeny i vyhláška č. 378/2006 Sb. o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb) a vyhláška č. 212/2012 Sb., o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka (vyhláška o ověřování platnosti zaručeného elektronického podpisu).

2.2.2.2.2 Budoucí právní úprava

Nařízení eIDAS a návazné prováděcí akty Komise jsou dle zásad Evropského práva nadřazené vnitrostátnímu právu, s přímými účinky a okamžitě použitelné. Vnitrostátní právní předpisy tak mohou upravovat pouze ty právní skutečnosti, u kterých je v Nařízení eIDAS výslovně předepsána anebo umožněna vnitrostátní dispozice, nebo které nejsou v rozporu s kogentními ustanoveními nařízení.

V legislativním procesu jsou v souvislosti s nařízením eIDAS a oblastí služeb vytvářejících důvěru dva návrhy zákonů.

Návrhem adaptace nařízení eIDAS do vnitrostátního práva ČR je návrh zákona o službách vytvářejících důvěru pro elektronické transakce (dále též „adaptační zákon“), který je v současné době ve fázi projednávání Poslaneckou sněmovnou. Dostupný je on-line jako sněmovní tisk 763 na URL adrese http://www.psp.cz/sqw/historie.sqw?o=7&T=763.

Druhým návrh navazuje na návrh adaptačního zákona a tvoří soubor změn stávajících zákonů. Má dopad i na klíčový zákon č. 372/2011 Sb. o zdravotních službách, konkrétně v ustanovení o převodu listinné zdravotnické dokumentace do elektronické podoby, která

musí být doplněna doložkou potvrzující převedení podepsanou uznávaným elektronickým podpisem osoby, která převod provedla. Návrh změn zákonů je dostupný on-line jako sněmovní tisk 764 na URL adrese http://www.psp.cz/sqw/historie.sqw?o=7&t=764.

V navrhovaném adaptačním zákoně je upraveno pouze to, co nařízení eIDAS výslovně nechává na úpravu vnitrostátním právním řádem. Neřeší veškeré oblasti nařízení eIDAS, ale pouze ty jeho části, které budou aplikovatelné od 1. července 2016, tzn. problematiku služeb vytvářejících důvěru.

Na způsoby identifikace, autentizace a autorizace zdravotnických pracovníků a pacientů má tedy návrh zákona vliv pouze v tom případě, jsou-li k těmto procesům využívány zaručené elektronické podpisy a digitální certifikáty.

V přímé souvislosti s návrhem adaptačního zákona jsou navrhovány změny celé řady zákonů, které využívají ustanovení dosud platného zákona č. 227/2000 Sb., o elektronickém podpisu. Proto druhým právním předpisem, připravovaným v souvislosti s nařízením eIDAS a navazujícím na adaptační zákon, je Vládní návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů. Tento zákon přinese řadu změn v jiných zákonech, jedná se však převážně pouze o terminologické změny.

2.2.2.3 Návaznost na resort zdravotnictví a zdravotnickou legislativu

V resortu zdravotnictví se problematiky elektronické identifikace a autentizace dotýká zejména zákon č. 372/2011 Sb. o zdravotních službách a podmínkách jejich poskytování, a to převážně v oblastech zdravotnické dokumentace (vedené v elektronické formě), NZIS a vedení zdravotnických a dalších registrů.

Jak vyplývá ze studie Posouzení realizovatelnosti vybraných oblastí Národní strategie elektronického zdravotnictví[1], z hlediska sdílení informací o zdravotní péči je významné zejména to, že zápis do zdravotnické dokumentace vedené v elektronické podobě musí být opatřen identifikátorem záznamu (viz § 54 odst. 3 písm. b) zákona č. 372/2011 Sb.) a informační systém, ve kterém je vedena zdravotnická dokumentace v elektronické podobě, má dle zákona evidovat seznam identifikátorů záznamů v elektronické dokumentaci pacientů vedené poskytovatelem a umožňuje jeho poskytování dálkovým přístupem (viz § 55 písm. b) zákona č. 372/2011 Sb.). Formát identifikátoru záznamu a podmínky kladené na formát identifikátoru záznamu mají být stanoveny prováděcím právním předpisem, avšak stávající vyhláška č. 98/2012 Sb. o zdravotnické dokumentaci takovou úpravu neobsahuje.

V případě zdravotnické dokumentace vedené v elektronické podobě a použití elektronických prostředků při jednání do ní zaznamenávaných (typicky udělování souhlasu s poskytováním zdravotních služeb), u nichž zákon o zdravotních službách v některých případech vyžaduje, aby projev pacienta měl písemnou formu projevu (viz §34 odst. 2 zákona č. 372/2011 Sb.), je nutné vycházet z obecných ustanovení v zákoně č. 89/2012 Sb. občanský zákoník.

[1] Grant Thornton Advisory s.r.o.: Posouzení realizovatelnosti vybraných oblastí Národní strategie elektronického zdravotnictví, Fáze I. – výstupní analýza posuzující realizovatelnost vybraných oblastí (prefinální verze). Praha, 2016.

Konkrétně ustanovení § 561 a §562 občanského zákoníku stanoví, že písemná forma právního jednání je zachována i tehdy, je-li toto jednání učiněno elektronickými či jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby. K platnosti tohoto právního jednání se vyžaduje podpis jednajícího, avšak občanský zákoník dále výslovně nestanoví náležitosti tohoto podpisu pro případ jednání elektronickými prostředky. Stejně tak ani Zákon o zdravotních službách ani Vyhláška o zdravotnické dokumentaci ve své současné podobě neřeší otázku, jakým způsobem bude jednání učiněné vůči poskytovateli zdravotních služeb elektronickými prostředky následně zaznamenáno do elektronické zdravotnické dokumentace konkrétního pacienta (viz výše zmiňovaná studie Posouzení realizovatelnosti vybraných oblastí Národní strategie elektronického zdravotnictví).

Otázky identifikace, autentizace a autorizace se dotýkají také vyhlášky č. 54/2008 Sb. o způsobu předepisování léčivých přípravků, údajích uváděných na lékařském předpisu a o pravidlech používání lékařských předpisů a zákona č. 70/2013 Sb., kterým se mění zákon č. 378/2007 Sb., o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech), ve znění pozdějších předpisů, (který zavádí povinný elektronický recept) a další právní předpisy.

2.2.3 Metodický rámec

Návrh cílové architektury je v souladu s NAP VS ČR a v souladu s předběžnou verzí metodiky EA Ministerstva zdravotnictví ČR. Detailní popis metodiky EA se nachází v dokumentu Metodický rámec Enterprise architektury pro resort zdravotnictví.

Diagramy prezentované v tomto dokumentu jsou vytvořeny v notaci jazyka ArchiMate. Modelovací jazyk ArchiMate umožňuje jednotnou reprezentaci diagramů popisujících enterprise architekturu. Nabízí integrovaný architektonický přístup pro popis a vizualizaci jednotlivých architektonických domén (procesní, aplikační, technologická atd.) a jejich základních vztahů a závislostí.

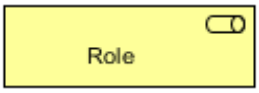
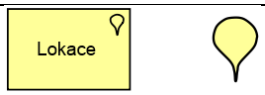
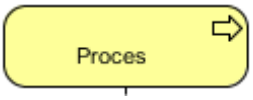
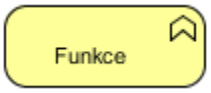
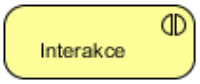
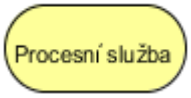
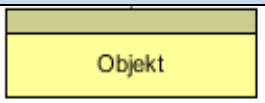
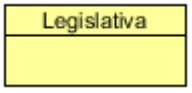
ArchiMate definuje tři základní domény (znázorněné různými barvami):

- **Byznys (procesní) doména** (znázorněná žlutou barvou) zachycuje účastníky, jejich role a užívané byznys služby, které jsou realizovány procesy. V pohledu na byznys (procesní) doménu jsou zachyceny stěžejní prvky cílové architektury na úrovni EA.
- **Aplikační doména** (znázorněná modrou barvou) podporuje byznys (procesní) doménu pomocí aplikačních služeb, které jsou realizovány aplikačními komponentami (aplikacemi a infomačními systémy).
- **Technologická a infrastrukturní doména** (znázorněné zelenou barvou) podporuje aplikační doménu pomocí technologických služeb nezbytných pro běh aplikací, které jsou realizovány výpočetní technikou a systémovým software.

V níže uvedených tabulkách se nachází výčet vybraných elementů jednotlivých domén architektury.

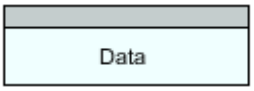
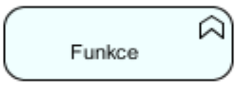
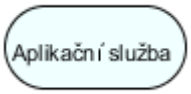
2.2.3.1 Výčet vybraných elementů byznys (procesní) domény

Tabulka 1 Seznam a popis vybraných elementů byznys domény

Pojem	Popis	Symbol
Elementy aktivní struktury		
Účastník, aktér/ Business Actor	Účastník je definován jako organizační jednotka schopna vykonávat aktivitu přiřazenou k jedné nebo více byznys rolím.	
Role / Business Role	Zodpovědnost za vykonávání specifického chování, ke které může být přiřazen účastník procesu.	
Rozhraní/ Business Interface	Přístupový bod, kde je procesní služba dostupná okolnímu prostředí.	
Lokalita,místo/ Location	Místo v prostoru, kde se nacházejí aktéři nebo kde je vykonáváno chování	
Elementy chování		
Proces/ Business Process	Element chování, který sdružuje skupiny chování na základě pořadí činností. Je určen k produkování sady produktů nebo byznys služeb.	
Funkce/ Business Function	Element chování, který seskupuje chování podle vybraná sady kritérií (typicky požadovaných dovedností, znalostí, zdrojů.	
Interakce/ Business Interaction	Element chování, který popisuje chování spolupráce.	
(Byznys) služba/ Business Service	Byznys služba je definována jako služba, která naplňuje potřeby zákazníka (interního nebo externího vůči poskytující organizaci).	
Elementy pasivní struktury		
Objekt/ Business Object	Pasivní element, který má relevanci z předmětného pohledu.	
Kontrakt/ Contract	Formální nebo neformální specifikace dohody, která specifikuje práva a povinnosti spojené s produktem.	

2.2.3.2 Výčet vybraných elementů aplikační domény

Tabulka 2 Seznam a popis vybraných elementů aplikační domény

Pojem	Popis	Symbol
Komponenta aplikace/ Application Component	Modulární, nasaditelná a nahraditelná část softwarového systému, zapouzdřující své chování a data, které poskytuje skrz sadu rozhraní.	
Rozhraní aplikace/ Application Interface	Přístupový bod, ve kterém je služba aplikace dostupná pro využití uživatelem nebo jinou komponentou aplikace	
Datový objekt/ Data Object	Pasivní element vhodný k automatickému zpracování.	
Funkce aplikace/ Application Function	Element chování, který seskupuje automatizované chování, které může být prováděno kteroukoliv aplikační komponentou.	
Služba aplikace/ Application Service	Služba, která poskytuje automatizované chování	

2.3 Přehled stávajících řešení

2.3.1 eGovernment ČR

Systém základních registrů (MV) i národní zdravotnický informační systém jsou v ČR funkční, nicméně z řady důvodů spolu nejsou propojeny. Základem českého e-Governmentu je systém 4 základních registrů (Registr osob, Registr obyvatel, Registr práv a povinností, Registr územní identifikace, adres a nemovitostí) provozovaných příslušnými centrálními úřady, a propojený v Informačním systému základních registrů; podrobnosti jsou uvedeny v kapitole věnované opatření 4.1.2. Pro komunikaci se státní správou je pak určen systém datových schránek a navazující infrastruktura (CzechPOINT, KIVS).

Identifikace občana ČR, pacienta i pojištěnce je prováděna přes rodné číslo, vydávané v kompetenci MV ČR. Toto číslo není bezvýznamové, lze z něj vyčíst datum narození a pohlaví. Je vydáváno i cizincům zdržujícím se delší dobu na území ČR. Další země, které používá tento formát univerzálního identifikátoru je Slovenská Republika. Zákon o veřejném zdravotním pojištění umožňuje oddělit číslo pojištěnce od rodného čísla, stejně tak v řadě nemocničních informačních systémů (např. UNIS) je odděleno číslo pacienta, číslo pojištěnce a rodné číslo.

Rozvoj nástrojů eGovernmentu je aktuálně zakotven ve Strategickém rámci rozvoje veřejné správy ČR pro období 2014-2020, v rámci strategického cíle 3 - Zvýšení dostupnosti a transparentnosti veřejné správy prostřednictvím nástrojů eGovernmentu. Klíčové technologie pro infrastrukturu eHealth (např. autorizace, autentizace pacientů a zdravotníků) nejsou centrálně implementovány.

2.3.2 Přehled řešení autentizace v resortu zdravotnictví

Na základě provedeného průzkumu organizací resortu zdravotnictví ČR, produktů (informačních systémů) vytvářených a dodávaných pro zdravotnictví[2] a interview se zástupci organizací v rámci pracovní skupiny Registry e eID byly identifikovány následující způsoby ověřování identity uživatelů pro přístupy do informačních systémů v resortu zdravotnictví:

1. Pomocí identifikačních údajů (jméno a heslo)
2. OTP – přihlášení jednorázovým heslem, které uživatel obdrží na vyžádání buď formou SMS na předem zaregistrované telefonní číslo nebo formou e-mailu na zaregistrovanou e-mailovou adresu (s možností volby separátního kanálu nebo bez možnosti volby)
3. Pomocí elektronického podpisu (na základě ověření digitálního certifikátu pro elektronický podpis), přičemž seznam uznávaných certifikátů (dle vydávajících certifikačních autorit) se pro jednotlivé IS může lišit
4. Pomocí identifikačních předmětů

Výše uvedené způsoby autentizace uživatelů mohou být v praxi navzájem kombinovány a lze říci, že ve značné části případů kombinovány jsou. Nejběžněji se vyskytují kombinace identifikační údaje + OTP a identifikační údaje + digitální certifikát pro elektronický podpis.

Některé systémy (IS zdravotních pojišťoven) umožňují uživateli volbu způsobu autentizace, a to buď identifikačními údaji + OTP anebo digitálním certifikátem pro elektronický podpis, ovšem s tím omezením, že některé úkony je možné provádět pouze po autentizaci prostřednictvím certifikátu.

Na druhou stranu, autentizace prostřednictvím identifikačních údajů + OTP dává uživateli širší možnosti přístupu k systému z různých zařízení, neboť autentizace digitálním certifikátem je vázána na zařízení, do něhož je certifikát nainstalován. Uživateli je také umožněno využívat střídavě oba způsoby autentizace, (pokud se pro oba zaregistruje - povolený způsob autentizace je součástí konfigurace účtu uživatele), dle jeho potřeby.

U žádného z prověřovaných IS nebyla zjištěna autentizace uživatelů pomocí identifikačních předmětů (čipová karta nebo token), s výjimkou autentizace pracoviště prostřednictvím VPN routeru s přístupovým certifikátem, který poskytuje SÚKL pro autentizaci do systému eRecept.

Autentizace se zpravidla zaměřuje pouze na uživatele, který se do systému přihlašují, ale vyskytuje se i způsob dvojí autentizace v rámci jednoho přihlášení do systému:

1. autentizace pracoviště
2. autentizace uživatele

Následující tabulka zobrazuje využívání jednotlivých způsobů autentizace informačními systémy (či skupinami systémů). Jedná se o generalizovaný přehled nejobvyklejších forem, vyjímečné odlišnosti proto nemusí být v tabulce zachyceny.

[2] V rámci průzkumu byly studovány webové stránky všech organizací spadajících do přímé působnosti Ministerstva zdravotnictví ČR, orgánů ochrany veřejného zdraví, vybraných poskytovatelů zdravotních služeb, zdravotních pojišťoven a vybraných významných dodavatelů SW do resortu zdravotnictví. Doplňkovými zdroji informací byly studie Soutěž o návrh „Hospodárné a funkční elektronické zdravotnictví“ (Microsoft, 2012) a Posouzení realizovatelnosti vybraných oblastí Národní strategie elektronického zdravotnictví, Fáze I. – výstupní analýza posuzující realizovatelnost vybraných oblastí (prefinální verze) (Grant Thornton Advisory s.r.o., 2016).

Tabulka 3 Souhrn současného stavu způsobu autentizace

Způsob autentizace	Informační systém (skupina systémů)				
	IS zdravotních pojišťoven	**IS zdravotních pojišťoven (B2B)**	**Centrální IS MZ ČR (registry)**	**eRecept**	**Objednávkové a rezervační IS**
Způsob ověřování identity uživatelů					
Pomocí identifikačních údajů	X		X	X	
OTP - jednorázové heslo pro přihlášení	X		X		
Pomocí certifikátu pro el. podpis	X	X		X	
Pomocí identifikačních předmětů					
Bez autentizace					X
Způsob ověřování identity pracoviště					
Pomocí identifikačních údajů				X	
OTP - jednorázové heslo pro přihlášení					
Pomocí certifikátu pro el. podpis					
Pomocí identifikačních předmětů				X	
Bez autentizace					

2.4 Současný stav autentizace subjektů ve zdravotnictví ČR

2.4.1 Subjekty ve zdravotnictví

V resortu zdravotnictví byly identifikovány následující subjekty, pro které je nutná autentizace:

- Klient zdravotních služeb (KZS)
  - pacient, pojištěnec, občan
- Zdravotnický pracovník (ZP)
  - lékař (dle zákona č. 95/2004 Sb.), nelékař (dle zákona č. 96/2004 Sb.)
- Poskytovatel zdravotních služeb (PZS)
  - právnická osoba, podnikající fyzická osoba, poskytovatel – IČZ – IČP
- Systémy a zařízení s vlastní autentizací
  - počítač, terminál, či jiné zařízení (autentizace typicky certifikátem)
- Veřejnoprávní subjekty a jejich pověřené osoby
- Soukromoprávní subjekty a jejich pověřené osoby

2.4.2 Existující služby autentizace

Tabulka 4 Současný stav možností autentizace subjektů ve zdravotnictví

Služba autentizace	Klient zdrav. sl.	Zdravot. Pracovník	Poskyt. zdrav. sl.	Systémy a zařízení	Pov.osoba veř. subj.	Pov.ososba soukr. subj.
AS PVS (ISDS)	Ano	Ne	Ne	Ne	Ne	Ne
JIP/KAAS	Ne	Ne	Ne	Ne	Ano	Ne
Portály ZP	Ano *	Ne	Ano	Ne	Ano	Ano
eREG	Ne	Ano	Ano	Ano	Ano	Ano
SÚKL	Ne	Ano	Ne	Ano	Ne	Ne
NIS FN	Ne	Ano	Ne	Ne	Ne	Ne

* jen registrovaní klienti

2.5 Současný stav využívání elektronického podpisu ve zdravotnictví ČR

2.5.1 Subjekty ve zdravotnictví

V resortu zdravotnictví byly identifikovány následující subjekty, které využívají uznávané elektronické podpisy založené na kvalifikovaných certifikátech vydaných kvalifikovaným poskytovatelem certifikačních služeb (pojmy dle stávajícího zákona č. 227/2000 Sb.):

- Ministerstvo zdravotnictví ČR a jím zřizované organizace
  - Elektronická spisová služba (ESS)
  - Příjem elektronických podání
  - Vytváření elektronických podání
  - Zdravotnické registry (eREG)
  - Státní ústav pro kontrolu léčiv (SÚKL)
    - Systém elektronické preskripce (eRecept)
  - Všeobecná fakultní nemocnice v Praze (VFN)
    - Elektronická zdravotnická dokumentace (EZD)
- Zdravotní pojišťovny
  - Elektronická spisová služba (ESS)
  - Příjem elektronických podání
  - Vytváření elektronických podání
  - Internetový portál ZP (VZP Point, e-Komunikace ZP MV, Portál ZP)
- Soukromoprávní poskytovatelé zdravotních služeb (dobrovolné využití el. podpisu)
  - Elektronická spisová služba (ESS)
  - Příjem elektronických podání
  - Vytváření elektronických podání

2.5.2 Existující systémy využívající elektronický podpis

Tabulka 5 Současný stav využívání elektronického podpisu ve zdravotnictví

Systém	Ověřování uznávaných el. podpisů/značek	Vytváření uznávaných el. podpisů/značek	Opatřování kvalifikovanými časovými razítky
ESS – Elektronická spisová služba	Ano	Ano	Ano
Příjem elektronického podání	Ano	Ne	Ne
Vytvoření elektronického podání	Ne	Ano	Ne
eREG	Ano	Ne	Ne
eRecept	Ano	Ano	Ne
EZD VFN	Ano	Ano	Ne
Internetový portál ZP	Ano	Ne	Ne

2.6 Motivace pro vytvoření pohledů na současný stav

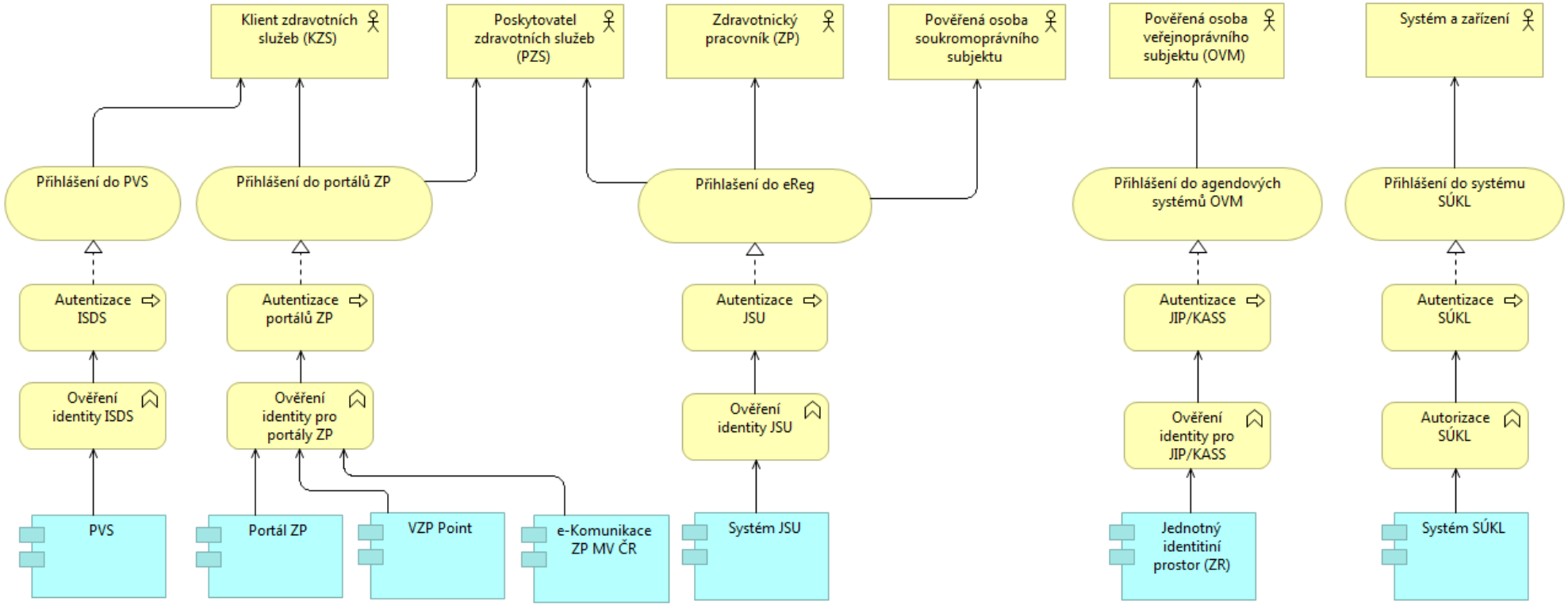
V následujících kapitolách jsou popsány následující pohledy na současný (AS-IS) stav enterprise architektury tématu:

- Business doména – diagram slouží pro zobrazení současného stavu služeb pro autentizaci včetně podpůrných funkcí a jejich využívání subjekty ve zdravotnictví.
- Aplikační doména – diagram slouží pro zobrazení
    - současného stavu aplikačních komponent systémů, které poskytují autentizační služby subjektům ve zdravotnictví;
    - současného stavu aplikačních komponent systémů, jež jsou subjekty ve zdravotnictví využívány k práci a elektronickými dokumenty opatřenými uznávanými elektronickými podpisy.

2.7 Pohledy na současný stav

2.7.1 Business doména

Diagram znázorňuje pohled na byznys (procesní) doménu současného stavu autentizačních služeb v resortu zdravotnictví. Procesní diagram AS-IS stavu autentizačních služeb v resortu zdravotnictví má za cíl zachytit klíčové aktéry, funkce a poskytované byznys služby.



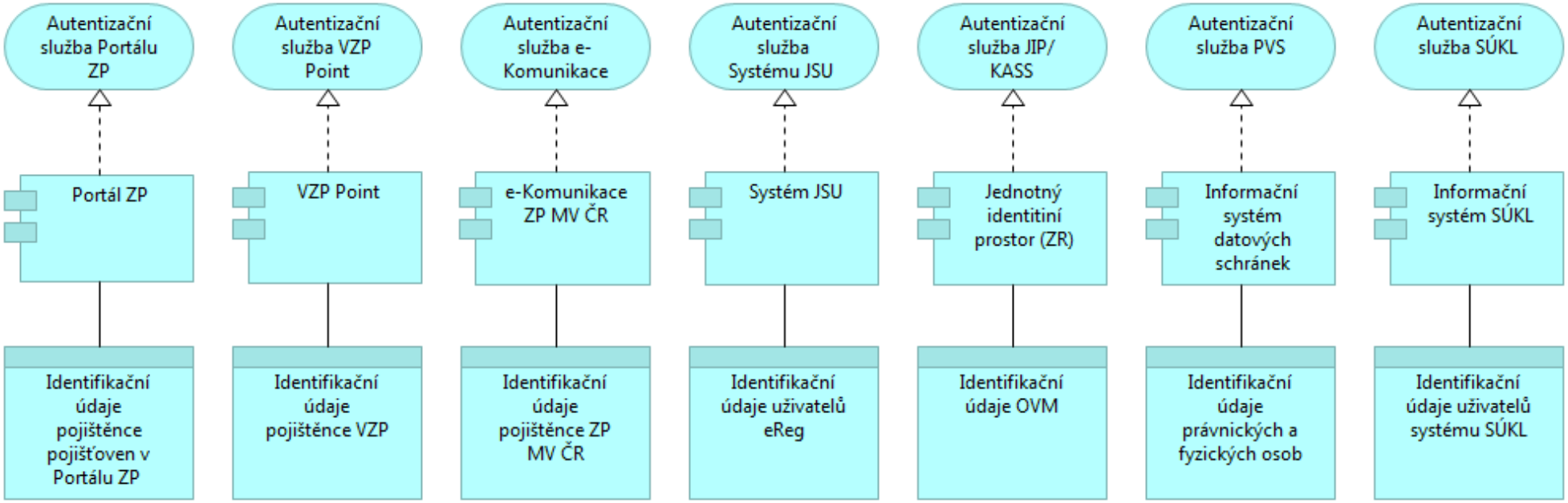
Obrázek 1 Procesní diagram AS-IS stavu identifikace a autentizace

Hlavními byznys objekty v diagramu jsou služby přihlášení do informačních systémů, které mohou využívat subjekty ve zdravotnictví.

2.7.2 Aplikační doména

2.7.2.1 AS-IS stav identifikace a autentizace

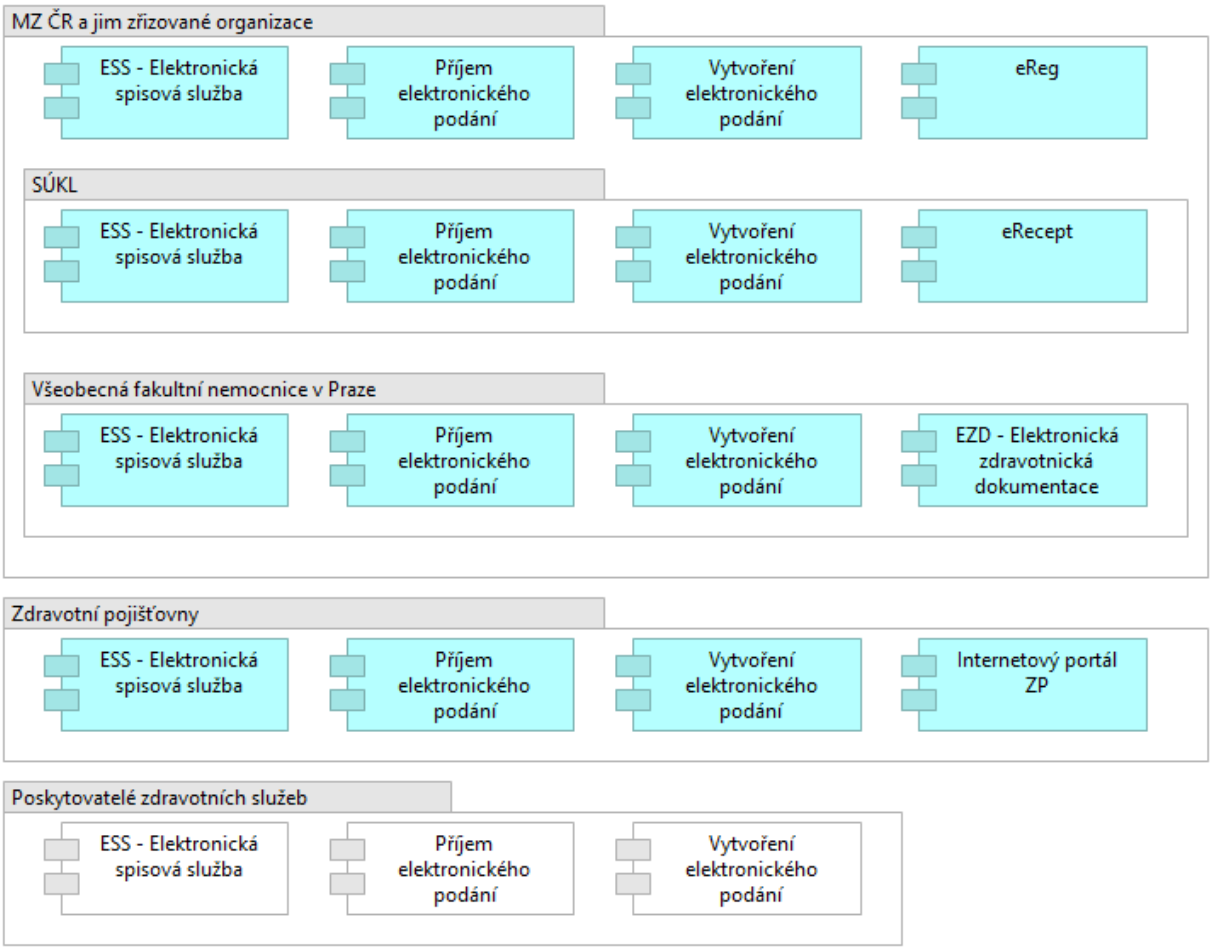
Diagram znázorňuje pohled na aplikační doménu současného stavu autentizačních služeb v resortu zdravotnictví. Aplikační diagram AS-IS stavu autentizačních služeb v resortu zdravotnictví má za cíl zachytit aplikační komponenty (systémy s autentizací) a datové objekty (identifikace subjektů).



Obrázek 2 Aplikační diagram AS-IS stavu identifikace a autentizace

2.7.2.2 AS-IS stav využívání uznávaného elektronického podpisu

Diagram znázorňuje pohled na aplikační doménu současného stavu využívání uznávaného elektronického podpisu v resortu zdravotnictví. Aplikační diagram AS-IS stavu má za cíl zachytit subjekty ve zdravotnictví a jimi používané aplikační komponenty, které pracují s uznávanými elektronickými podpisy.



Obrázek 3 Aplikační diagram AS-IS stavu využívání elektronického podpisu

Pozn.: modře vybarvené aplikační komponenty jsou provozovány veřejnoprávními subjekty, na které se vztahuje povinnost používat uznávané elektronické podpisy dle zákona č. 227/2000 Sb. a vztahuje se na ně budoucí povinnost z nařízení eIDAS používat kvalifikované elektronické podpisy. Bíle vybarvené aplikační komponenty jsou provozovány soukromoprávními subjekty, které se dobrovolně rozhodli akceptovat elektronické dokumenty opatřené uznávanými elektronickými podpisy a rovněž budoucí používání kvalifikovaných elektronických podpisů pro ně nebude povinná.

2.8 Identifikace problémových oblastí

Tabulka 6 Identifikace problémových oblastí

Problematická oblast	**Zdůvodnění výběru**
Jak bude zajištěna kooperace mezi registry (i vzhledem k ZOOÚ)?	Soustava cílů tak, jak je popsána, může být interpretována tak, že vyžaduje vznik dodatečných registrů pro identifikaci všech subjektů zdravotní péče. V tomto případě se může jednat o legislativní změny.
Jak budou řešeny odpovědnosti za autorizaci, autentizaci a řízení oprávnění?	Soustava cílů tak, jak je popsána, vyžaduje faktický i legislativní souběh více způsobů autentizace dle role uživatele a případu použití. Tato problematika je komplexní z hlediska odpovědností, ale řešitelná. Vyžaduje však, aby již při přípravě varianty byly diskutovány kompetence alespoň na základní úrovni.
Bude vytvářena kopie některých registrů nebo navýšena kapacita připojení ke stávajícím?	Budou-li registry používány pro provozní identifikaci, zvýší se počet přístupů v rozsahu několika řádů. Jedná se o zcela konkrétní otázku na rozmezí technologie a politiky.
Jak budou uvedené činnosti probíhat pro pacienty EU?	Doplněno plošně jako test kompatibility s EU projekty a legislativou.
Jak bude přihlašován lékař?	Modelový příklad; souhrnná otázka na správu identit lékařů. Termín „přihlášení“ je zde použit jako příklad životní situace zahrnující autentizaci a povolení přístupu.
Jak budou přihlašováni ostatní zdravotničtí profesionálové?	Na základě konzultace s nelékaři doplněna otázka ostatních zdravotnických profesionálů a jejich správy identit.
Kdo bude technicky zajišťovat vedení registrů, autorizaci, autentizaci a oprávnění.	Tyto otázky byly doplněny na společné schůzce GTA-MZČR.
Dočasné řešení před eIDAS.	
Postoj k biometrii a implantovatelným identifikátorům.	

3 Popis mezinárodní praxe a srovnatelných výsledků v ostatních zemích EU

Podle studie *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services* z roku 2014, jsou v 15 ze sledovaných zemí pro autentizaci zdravotnických pracovníků využívány systémy založené na elektronickém podpisu či na elektronických kartách (smart card). Jiný specifický přístup pro zdravotnické profesionály je používán v 6 zemích. Kypr například využívá uživatelské jméno a heslo, v Belgii existují pro přístup k elektronickému zdravotnímu záznamu striktní pravidla, kde se kontroluje také to, jestli je zdravotnický profesionál registrovaný. Následně musí také poskytnout evidenci ohledně terapeutického vztahu s pacientem. V Polsku se uživatelé identifikují kvalifikovaným certifikátem, nebo důvěryhodným profilem „trusted profile“, poskytovaným Elektronickou Platformou Veřejných Administrativních Služeb (Electronic Platformo of Public Administration Service). V Portugalsku je přístup řízen prostřednictvím lokálních aplikací poskytovatelů zdravotních služeb, na základě jejich interních pravidel. Ve zbylých 8 zemích neexistují systémy řízeného přístupu zdravotnických profesionálů. Pravidla pro autentizaci zdravotnických pracovníků většinou vycházejí z praxe a nejsou ukotvena v zákoně.

V 16 zemích jsou úrovně přístupu k zdravotnickému záznamu odlišeny podle specifické autorizace zdravotnických pracovníků. Zavedení úrovní přístupu se v rámci krajin liší. V některých (Rakousko, Maďarsko) jsou typy přístupu odlišené na základě typů poskytovatelů zdravotních služeb, v jiných (Francie, Slovensko, Luxembursko) se liší přístup obvodního lékaře od ostatních zdravotnických pracovníků. Ve Švédsku a Anglii jsou různá data přístupna různým poskytovatelům zdravotních služeb. V Bulharsku je povolen pouze jeden typ přístupu a není umožněné schovat žádná data. V Estonsku je přístup povolen všem poskytovatelům zdravotních služeb, definovaných estonským zákonem. Další možnost je udělení pravomoci rozhodování o přístupech samotnému pacientovi, nad touto možností se uvažuje například v Chorvatsku. V 6 zemích jsou některé kategorie zdravotníků z přístupu k elektronickému zdravotnímu záznamu výslovně vyloučeny. Například v Rakousku se jedná o zaměstnavatele, konzultanty personálního oddělení nebo pojišťovny.

V rámci krajin Evropské unie se také liší systém identifikace pacientů pro účely eHealth. Ve 14 zemích je využívána ID karta; ve 13 zemích je to pak číslo zdravotního pojištění. Některé krajiny, byly převzaté opatření, které zajišťují důvěrnost dat. Například ve Francii je každému uživateli národní zdravotní péče uděleno automaticky generované číslo (INS), které je přístupné v zdravotnické kartě. Specifický identifikační kód pro eHealth není zaveden v žádné ze sledovaných zemí, pouze v Skotsku, kde byla vytvořena databáze demografických a klinických údajů (Community Health Index), které slouží pro jednoznačnou identifikaci.

Následující tabulka shrnuje vybrané ukazatele pro jednotlivé sledované krajiny Evropské unie.

Tabulka 7 Stav identifikace, autentizace a autorizace v Evropské unii

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Pravidla autentizace pro zdravotnické pracovníky																													
Systém neexistuje					X				X						X			X	X		X	X				X			
E-podpis/ e-karta	X		X			X	X			X	X	X	X	X			X			X					X		X	X	X
Jiný přístup (hesla apod.)		X		X				X								X							X	X					
Odlišení úrovní autorizace zdravotnických pracovníků																													
Odlišné kategorie přístupu	X			X			X			X	X	X	X			X		X	X	X		X					X	X	X
Výslovné zákazy přístupu	X	X										X				X					X	X							
Způsob identifikace																													
Specifické eHealth číslo																													
ID průkaz		X	X	X			X	X			X						X		X	X	X	X	X				X	X	
Číslo zdravotního pojištění	X					X			X	X		X	X	X	X	X		X							X	X				X

Z vyjmenovaných prvků infrastruktury se dá nepřímo sledovat existence registru zdravotnických profesionálů: pravidla pro jejich identifikaci a autentizaci dávají představu o tom, že v 15 ze sledovaných zemí, ve kterých jsou zdravotníci identifikováni elektronicky, existuje nějaká forma registru zdravotnických profesionálů pro potřeby aplikací eHealth (Česká republika je uvedena mezi zeměmi, kde pravidla identifikace / autentizace zdravotnických profesionálů neexistují).

4 Posouzení ekonomických, organizačních, časových, technologických a legislativních aspektů řešení

Výsledky posouzení ekonomických, organizačních, časových, technologických a legislativních aspektů řešení uvádí následující tabulka.

Tabulka 8 Analýza ekonomických, organizačních, technologických a právních aspektů

Hledisko	**Výsledky analýzy**
Ekonomické aspekty navržených opatření	V rámci této skupiny opatření se počítá s investičními náklady na centrální část systému (výše pak specifická dle navržených variant).
Organizační aspekty navržených opatření	Činnosti uváděné v Národní strategii mohou být řešeny: 1. pověřením stávajících institucí v gesci MZ 2. zřízením nových institucí
Časové aspekty navržených opatření	Nejpomalejší součástí procesu bude implementace požadovaných legislativních změn, kterou lze urychlit kvalitní přípravou.
Technologické aspekty navržených opatření	Systémy pro identifikaci, autentizaci, autorizaci a řízení přístupů a oprávnění navrhované v rámci této skupiny opatření jsou klíčové pro celou budovanou koncepci elektronického zdravotnictví. Koncepční příprava technologie musí být postavena na silných základech.
Legislativní aspekty navržených opatření	Dílčí funkcionality mohou být zpočátku budovány v rámci stávajících předpisů, v dlouhodobém měřítku je však navrhovaná opatření bez ohledu na způsob realizace vyžadují legislativní změny s ohledem na vytvoření kompetencí příslušných subjektů v oblasti státní správy a s ohledem na omezené možnosti využití souhlasů se zpracováním osobních údajů v oblasti zdravotních služeb. Legislativní změny vyžadují plný legislativní proces.

5 Prognóza budoucího vývoje bez realizace navrženého řešení

Pokud nebudou realizovány navrhované změny resortních elektronických služeb, dojde s vysokou pravděpodobností k situaci, kterou lze charakterizovat takto:

- Zdravotnictví je velmi konzervativní obor, budou přetrvávat stávající technologická řešení a tlak na jejich změnu bude minimální. Dojde k zavedení požadavků nařízení eIDAS zejména pro eGovernment, digitální podpisy občanů bude možné použít i v rámci jejich role jako příjemce zdravotního a sociálního pojištění.
- Bez realizace navrženého řešení lze předpokládat absenci stimulace pro vznik centrálně řízené infrastruktury. Legislativně bude dále podporován vznik a integrace registrů, postup však bude systematicky zpomalován nesouhlasem odborné veřejnosti. Budou postupně implementovány povinné požadavky eIDAS, nevznikne však propojení do oblasti e-Health.
- Jednotlivá zdravotnická zařízení (nebo jejich skupiny) budou pro zasílání a sdílení elektronických dokumentů používat vlastní dodavatelská řešení. Nelze vyloučit, že systémem akvizic a fúzí společností vyvíjejících zdravotnický software dojde de facto ke standardizaci nezávislé na MZ ČR.
- Vzhledem k nedostatku lepších nástrojů očekáváme zvýšení zájmu zdravotnických zařízení o technologie datových schránek a systémů provozovaných soukromoprávními subjekty, jako např. lékařský email eZpráva. Takový vývoj lze očekávat minimálně do doby, než bude implementován systém kompatibilní s nařízením eIDAS.

6 Analýza požadavků na řešení

6.1 Právní akty eIDAS a jejich kontext

Právní akty eIDAS tvoří následující předpisy:

- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 (eIDAS),
- Prováděcí akty – prováděcí nařízení a prováděcí rozhodnutí Komise (EU),
- Vnitrostátní právní předpisy členských států EU.

6.1.1 Nařízení eIDAS a prováděcí akty

Nařízení eIDAS a návazné prováděcí akty Komise jsou dle zásad Evropského práva nadřazená vnitrostátnímu právu, s přímými účinky a okamžitě použitelná. Vnitrostátní právní předpisy tak mohou upravovat právní skutečnosti, u kterých je v nařízení eIDAS výslovně předepsána anebo umožněna vnitrostátní dispozice, nebo které nejsou v rozporu s kogentními ustanoveními nařízení.

Nařízení eIDAS nahrazuje směrnici 1999/93/ES, jejíž implementací do českého národního práva je zákon č. 227/2000 Sb. o elektronickém podpisu, upravuje podmínky pro vytvoření jednotného digitálního trhu EU usnadněním přeshraničního využívání on-line služeb a zvláštní pozornost věnuje usnadnění bezpečné elektronické identifikace a autentizace. K tomu Nařízení eIDAS zavádí dvě základní oblasti elektronických nástrojů:

1. **Systémy elektronické identifikace a autentizace** – přihlašování osob k on-line službám
2. **Služby vytvářející důvěru** – poskytují důkazy autenticity elektronických dokumentů založené na zaručeném elektronickém podpisu

Z hlediska dopadů eIDAS jsou relevantní následující prováděcí akty:

- Prováděcí nařízení Komise (EU) 2015/1501 ze dne 8. září 2015 o rámci interoperability podle čl. 12 odst. 8 nařízení eIDAS
- Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení eIDAS
- Prováděcí rozhodnutí Komise (EU) 2015/1505 ze dne 8. září 2015, kterým se stanoví technické specifikace a formáty důvěryhodných seznamů podle čl. 22 odst. 5 nařízení eIDAS
- Prováděcí rozhodnutí Komise (EU) 2015/1506 ze dne 8. září 2015, kterým se stanoví specifikace pro formáty zaručených elektronických podpisů a zaručených pečetí uznávaných subjekty veřejného sektoru podle čl. 27 odst. 5 a čl. 37 odst. 5 nařízení eIDAS

6.1.2 Návrh vnitrostátní adaptace eIDAS

V současnosti se v Poslanecké sněmovně projednává návrh adaptace eIDAS do vnitrostátního práva ČR, návrh zákona o službách vytvářejících důvěru pro elektronické transakce a o změně některých zákonů, dostupný on-line na URL adrese http://www.psp.cz/sqw/historie.sqw?o=7&T=763 (dále též „adaptační zákon“).

V přímé souvislosti s návrhem adaptačního zákona jsou navrhovány změny celé řady zákonů, které využívají ustanovení dosud platného zákona č. 227/2000 Sb., o elektronickém podpisu, dostupné on-line na URL adrese http://www.psp.cz/sqw/historie.sqw?o=7&t=764.

Návrh adaptačního zákona upravuje pro vnitrostátní právo ČR:

- Povinnosti při podepisování a pečetění elektronických dokumentů.
- Oprávnění k zápisu dat a kvalifikovaného certifikátu na občanský průkaz.
- MV ČR jako orgán dohledu nad poskytovateli služeb vytvářejících důvěru.
- Přestupky, správní delikty a pokuty pro kvalifikované poskytovatele služeb vytvářejících důvěru.

6.1.3 Vysvětlení hlavních pojmů zaváděných nařízením eIDAS

Pro analýzu dopadů nařízení eIDAS na organizace resortu zdravotnictví je nezbytné zdůraznit skutečnost, že povinnosti nařízení se vztahují primárně na subjekty veřejného práva. Pro účely této analýzy proto definujeme pojem **veřejnoprávní zdravotnický subjekt** (dále též „**VPZS**“), kterým jsou chápany především Ministerstvo zdravotnictví a jím zřizované organizace a zdravotní pojišťovny.

Po nabytí účinnosti nařízení eIDAS budou všechny VPZS v závislosti na rozsahu poskytovaných elektronických služeb od 1. 7. 2016 v právním postavení:

- Poskytovatele on-line služby poskytované subjektem veřejného sektoru.

  „On-line službou“ je veřejně dostupný informační systém poskytující služby fyzickým a právnickým osobám, který uznává prostředky pro elektronickou identifikaci osob.

  „Subjektem veřejného sektoru“ je orgán státní a veřejné moci, veřejnoprávní subjekt dle směrnice 2014/24/EU, nebo soukromý subjekt pověřený těmito orgány poskytovat veřejné služby.

- Spoléhající se strany.

  „Spoléhající se stranou“ je fyzická nebo právnická osoba, včetně subjektu veřejného sektoru, které se spoléhá na elektronickou identifikaci nebo službu vytvářející důvěru.

- Provozovatele uzavřených systémů.

  Uzavřený systém – jeho používání vyplývá z vnitrostátního práva nebo z dohod mezi určeným okruhem účastníků a nevztahují se na něj ustanovení nařízení č. 910/2014.

Po nabytí účinnosti vnitrostátního adaptačního zákona č. X/2016 (dosud v návrhu), o službách vytvářejících důvěru pro elektronické transakce, bude VPZS v právním postavení:

- Veřejnoprávní podepisující.

  „Veřejnoprávním podepisujícím“ je stát, územní samosprávný celek, právnická osoba zřízená zákonem nebo právnická osoba zřízená nebo založená státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem.

6.1.4 Důvody vzniku a obsah nařízení eIDAS

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES je známé pod zkratkou eIDAS.

V publikovaném Nařízení eIDAS Evropský parlament a Rada Evropské unie uvádí 77 důvodů vzniku tohoto nařízení, níže jsou vyzdvihnuty některé vybrané důvody:

- Zvýšení důvěryhodnosti elektronických transakcí na vnitřním trhu.
- Původní směrnice 1999/93/ES upravovala elektronické podpisy, aniž by poskytovala ucelený rámec pro bezpečné, důvěryhodné a snadno použitelné elektronické transakce.
- Podporuje a rozvíjí požadavky Jednotného digitálního trhu, je jedním z jeho nástrojů.
- Směrnice Evropského parlamentu a Rady 2006/123/ES vyžaduje, aby členské státy vytvořily jednotná kontaktní místa, jejichž on-line služby používají elektronickou identifikaci, autentizaci a podpis.
- Stanovit odpovědnosti pro všechny poskytovatele služeb vytvářejících důvěru.
- Je vhodné zajistit dlouhodobé uchovávání informací, dlouhodobou platnost elektronických podpisů a elektronických pečetí, ověření dokumentů a dat bez ohledu na budoucí technologické změny.
- Elektronickému dokumentu nesmějí být upírány právní účinky na základě skutečnosti, že má elektronickou podobu.

Obsah Nařízení eIDAS tvoří šest kapitol, kterými jsou:

1. Obecná ustanovení (kapitola I)
2. **Elektronická identifikace (kapitola II)**
3. **Služby vytvářející důvěru (kapitola III)**, v rámci nichž jsou upraveny:
   - elektronické podpisy,
   - elektronické pečetě,
   - elektronická časová razítka,
   - služba elektronického doporučeného doručování,
   - autentizace internetových stránek
4. **Elektronické dokumenty (kapitola IV)**
5. Přenesení pravomoci a prováděcí ustanovení (kapitola V)
6. Závěrečná ustanovení (kapitola VI)

6.2 Elektronická identifikace a autentizace

Nařízení eIDAS dává prostor jednotlivým členským státům na vytvoření vlastních systémů elektronické identifikace, či na využití těch stávajících. Vše za předpokladu, že splní určitou, definovanou „kvalitu“ služby, včetně splnění požadavků na definované úrovně záruky prostředků pro elektronickou identifikaci.

Úrovně záruky prostředků pro elektronickou identifikaci a autentizaci jsou v Nařízení eIDAS označovány jako:

Nízká – účelem je snížit riziko zneužití, nebo změny totožnosti

Značná – zde je již nutné vhodnými prostředky značně snížit riziko zneužití, či změnu totožnosti

Vysoká – účelem je předejít zneužití nebo změně totožnosti.

Podrobněji je tato oblast specifikována v prováděcím nařízení komise (EU) 2015/1502, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci. Jsou definovány požadavky pro různé oblasti nakládání s prostředkem a prokazování identity. Například registrace, prokazování a ověřování totožnosti fyzické, resp. právnické osoby, správa prostředků pro elektronickou identifikaci, autentizace a další.

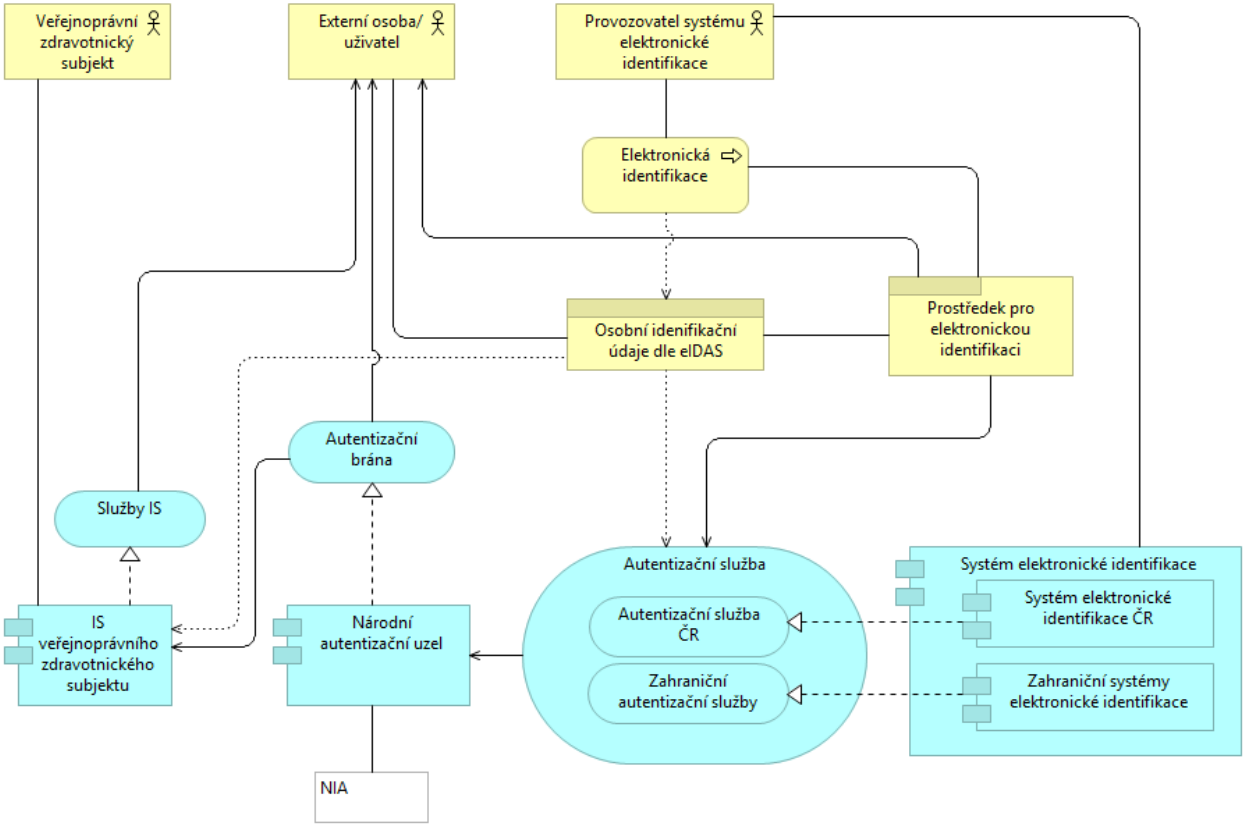
Systém elektronické identifikace členského státu, který má být uznán v rámci EU, musí být členským státem notifikován a oznámen Evropské komisi. Komise pak dále zveřejňuje seznam těchto oznámených systémů.

6.2.1 Vysvětlení hlavních pojmů elektronické identifikace

Nařízení eIDAS v souvislosti s elektronickou identifikací a autentizací zavádí do právního řádu následující pojmy:

- Elektronická identifikace – postup používání údajů, které jedinečně identifikují fyzickou nebo právnickou osobu.
- Osobní identifikační údaje – soubor identifikačních údajů dle přílohy prováděcího nařízení EU 2015/1501 pro fyzické a právnické osoby – údaje právnické osoby nejsou spojeny s fyzickou osobou.
- Prostředek pro elektronickou identifikaci – hmotný či nehmotný prostředek k identifikaci a autentizaci tj. údaje a předměty.
- Systém elektronické identifikace – vydává a spravuje prostředky elektronické identifikace, systémy elektronické identifikace zveřejňuje Komise na seznamu.
- Úroveň záruky prostředků pro elektronickou identifikaci – nízká, značná a vysoká úroveň splnění požadavků prováděcího nařízení EU 2015/1502. Vyjadřuje míru jistoty, že prostředek vlastní a používá osoba, pro niž byl vydán.

Pojmy elektronické identifikace a autentizace dle eIDAS zasazené do kontextu informačních systémů VPZS znázorňuje následující diagram.



Obrázek 4: Systém elektronické identifikace dle nařízení eIDAS

6.2.2 Systémy elektronické identifikace

Pokud se podle vnitrostátního práva nebo správní praxe pro přístup ke službě poskytované on-line subjektem veřejného sektoru v určitém členském státě vyžaduje elektronická identifikace s použitím prostředku pro elektronickou identifikaci a autentizaci, je pro účely přeshraniční autentizace pro danou on-line službu uznán v tomto členském státě prostředek pro elektronickou identifikaci vydaný v jiném členském státě, pokud jsou splněny tyto podmínky:

a) daný prostředek pro elektronickou identifikaci je vydán v rámci systému elektronické identifikace, který je uveden na seznamu zveřejněném Komisí,
b) úroveň záruky daného prostředku pro elektronickou identifikaci odpovídá stejné úrovni záruky, jako je úroveň záruky požadovaná příslušným subjektem veřejného sektoru v daném členském státě pro přístup k dané on-line službě, nebo vyšší úrovni, pokud úroveň záruky daného prostředku pro elektronickou identifikaci odpovídá značné nebo vysoké úrovni záruky,
c) příslušný subjekt veřejného sektoru používá v souvislosti s přístupem k dané on-line službě značnou nebo vysokou úroveň záruky.

K tomuto procesu uznání dojde do 12 měsíců od uveřejnění na seznamu zveřejněném Komisí.

Zde se dají očekávat komplikace v postupném zavádění jednotlivých systémů elektronické identifikace a jejich zveřejnění na seznamu Komise a dále pak v uznání ostatními členskými

státy. Další lhůtou definovanou pro uveřejnění systémů elektronické identifikace je povinnost poskytnutí popisu daného systému ostatním členským státům nejméně 6 měsíců před vlastním oznámením.

Garantem systému pro elektronickou identifikaci je oznamující členský stát, neboť dle článku 7 nařízení eIDAS platí:

Systém elektronické identifikace je způsobilý pro oznámení, pokud prostředky pro elektronickou identifikaci v rámci daného systému elektronické identifikace:

i) vydává oznamující členský stát;
ii) jsou vydávány z pověření oznamujícího členského státu; nebo
iii) jsou vydávány nezávisle na oznamujícím členském státu a tento členský stát je uznává

Provázání jednotlivých systémů elektronické identifikace členských států je pak realizováno prostřednictvím napojení na národní uzly. Tato problematika je blíže specifikována v prováděcím nařízení komise (EU) 2015/1501 o rámci interoperability. Při stanovování tohoto prováděcího rozhodnutí byl zohledněn pilotní projekt STORK a STORK II včetně specifikací vytvořených v tomto projektu.

Funkce a součásti těchto eIDAS uzlů jsou definovány a popsány v dokumentu Nástroje pro propojení Evropy vytvořeného nařízením Evropského parlamentu a Rady (EU) č. 1316/2013.

Mezi základní požadavky nařízení eIDAS na systém elektronické identifikace patří:

- zajištění požadovaných úrovní záruky,
- garance procesů prokazování a ověřování totožnosti,
- garance procesů pro vydávání prostředků pro elektronickou identifikaci,
- splnění technických a bezpečnostních požadavků,
- zajištění souladu s rámcem interoperability,
- poskytování minimálního souboru údajů fyzické nebo právnické osoby.

6.2.3 Prostředky pro elektronickou identifikaci

Následující tabulka přibližuje charakteristiky bezpečnostních funkcí, které souvisejí s přihlašováním uživatelů k on-line službám a s jejich využíváním, a uvádí příklady souvisejících údajů a předmětů. Pole, která jsou vyznačena modrou barvou, tvoří „prostředky pro elektronickou identifikaci“ fyzických a právnických osob dle nařízení eIDAS.

Tabulka 9 Prostředky pro elektronickou identifikaci dle nařízení eIDAS

Bezpečnostní funkce	Údaje	Předměty

Identifikace
Jednoznačné rozlišení osoby (uživatele systému)
	• Jedinečný identifikátor
	• Údaje specifikující osobu
	  • RČ, jméno, adresa
	  • IČO, název, sídlo
		Předmět pro zjištění identity
		• Průkazy vydávané státem
		• Identifikační karty s fotografií

Autentizace Ověření identity osoby pro přihlášení k systému	Tajný údaj pro ověření identity v systému • Heslo • PIN	Předmět pro ověření identity v systému • OTP – jednorázové kódy • Kryptografický token
Autorizace Udělení práva osoby použít funkci systému	Data pověření k funkcím systému • Registr práv uživatelů • Typy uživatelů a akcí	Prokázání odpovědnosti a vůle k provedení akce • SMS – zasílání OTP • Elektronický podpis

6.2.4 Minimální soubor osobních identifikačních údajů

Tyto minimální identifikační údaje definuje prováděcí rozhodnutí Komise 2015/1501 ve své příloze nazvané:

Požadavky týkající se minimálního souboru osobních identifikačních údajů jedinečně identifikujících fyzickou nebo právnickou osobu podle článku 11

6.2.4.1 Minimální soubor údajů pro fyzické osoby

Minimální soubor údajů pro fyzické osoby musí obsahovat všechny tyto povinné atributy:

a) současné (současná) příjmení;
b) současné jméno (současná jména);
c) datum narození;
d) jedinečný identifikátor vytvořený odesílajícím členským státem v souladu s technickými specifikacemi pro účely přeshraniční identifikace a pokud možno následně neměnný.

Minimální soubor údajů pro fyzické osoby může obsahovat jeden nebo více těchto dalších atributů:

a) jméno (jména) a příjmení při narození;
b) místo narození;
c) současnou adresu;
d) pohlaví.

6.2.4.2 Minimální soubor údajů pro právnické osoby

Minimální soubor údajů pro právnické osoby musí obsahovat všechny tyto povinné atributy:

a) současný oficiální název;
b) jedinečný identifikátor vytvořený odesílajícím členským státem v souladu s technickými specifikacemi pro účely přeshraniční identifikace a pokud možno následně neměnný.

Minimální soubor údajů pro právnické osoby může obsahovat jeden nebo více těchto dalších atributů:

a) současnou adresu;
b) identifikační číslo pro účely DPH;
c) daňové registrační číslo;
d) identifikační kód uvedený v čl. 3 odst. 1 směrnice Evropského parlamentu a Rady 2009/101/ES;
e) identifikační kód právnické osoby uvedený v prováděcím nařízení Komise (EU) č. 1247/2012;
f) registrační a identifikační číslo hospodářských subjektů (EORI) uvedené v prováděcím nařízení Komise (EU) č. 1352/2013;
g) číslo pro účely spotřebních daní stanovené v čl. 2 bodu 12 nařízení Rady (ES) č. 389/2012.

6.3 Služby vytvářející důvěru

Elektronické on-line služby mohou být úspěšné pouze v případě, že jim zákazníci důvěřují. Tato důvěra je klíčová z hlediska jejich ekonomického rozvoje, ale také z hlediska rozvoje společnosti a jednotného digitálního trhu.

Cílem eIDAS je vytvořit takové prostředí, ve kterém budou služby vytvářející důvěru poskytovat posílení jistoty a podněcovat využívání elektronických on-line služeb. Služby vytvářející důvěru mohou být nekvalifikované – status „služba vytvářející důvěru“ nebo kvalifikované – status „kvalifikovaná služba vytvářející důvěru“.

Služby vytvářející důvěru jsou definovány jako elektronické služby, které jsou zpravidla poskytovány za úplatu a spočívají:

a) ve vytváření a ověřování platnosti elektronických podpisů, elektronických pečetí nebo elektronických časových razítek, služeb elektronického doporučeného doručování a certifikátů souvisejících s těmito službami nebo
b) ve vytváření a ověřování platnosti certifikátů souvisejících s těmito službami;
c) v uchovávání elektronických podpisů, pečetí nebo certifikátů souvisejících s těmito službami.

Kvalifikovaná služba vytvářející důvěru je taková služba, která splňuje požadavky stanovené v nařízení eIDAS.

Na poskytovatele služeb vytvářejících důvěru jsou kladeny bezpečnostní požadavky, mezi které patří zajišťování takové úrovně bezpečnosti, která je přiměřená míře rizika.

Kvalifikovanou službu vytvářející důvěru může poskytovat pouze kvalifikovaný poskytovatel služby vytvářející důvěru.

Pro služby vytvářející důvěru obecně platí, že poskytovatelé služeb vytvářejících důvěru odpovídají za škodu, kterou úmyslně nebo z nedbalosti způsobí fyzické nebo právnické osobě nesplněním povinností vyplývajících z nařízení eIDAS. Zároveň však platí, že se mohou z této odpovědnosti vyvinit, pokud předem a řádně seznámí své zákazníky s omezeními jimi poskytované služby a tato omezení jsou rozpoznatelná i pro třetí osoby.

Pro zajištění souladu s požadavky kladenými na kvalifikované poskytovatele služby by měl být v každém členském státě ustanoven orgán dohledu.

Orgán dohledu může být po dohodě usazen i v jiném členském státě. Musí mu být uděleny odpovídající pravomoci a zdroje pro plnění zejména následujících cílů:

- vykonávání dohledu nad kvalifikovanými poskytovateli služeb vytvářejících důvěru preventivně tak, aby tito splňovali požadavky na ně kladené,
- vykonávání následného dohledu nad poskytovateli služeb vytvářejících důvěru s přijetím opravných prostředků v případě podezření na neplnění požadavků,
- podávání průběžných zpráv Komisi,
- předkládání zprávy Komisi do 31. března každého roku,
- udělování / odebírání statusu kvalifikovaného poskytovatele služeb.

Kvalifikovaní poskytovatelé služeb vytvářejících důvěru jsou povinni podrobit se na vlastní náklady auditu, a to alespoň jednou za 24 měsíců. Orgán dohledu však může audit provést kdykoli za účelem potvrzení, že jak sami kvalifikovaní poskytovatelé, tak i jimi poskytované kvalifikované služby vytvářející důvěru, splňují požadavky stanovené tímto Nařízením.

Pro jasnou identifikaci kvalifikovaných poskytovatelů byla Evropskou komisí vytvořena a přijata oficiální značka důvěry EU pro kvalifikované služby vytvářející důvěru.

Tato značka byla specifikována v prováděcím nařízení Komise (EU) 2015/806.

Obrázek 5: Značka důvěry EU pro kvalifikované služby vytvářející důvěru

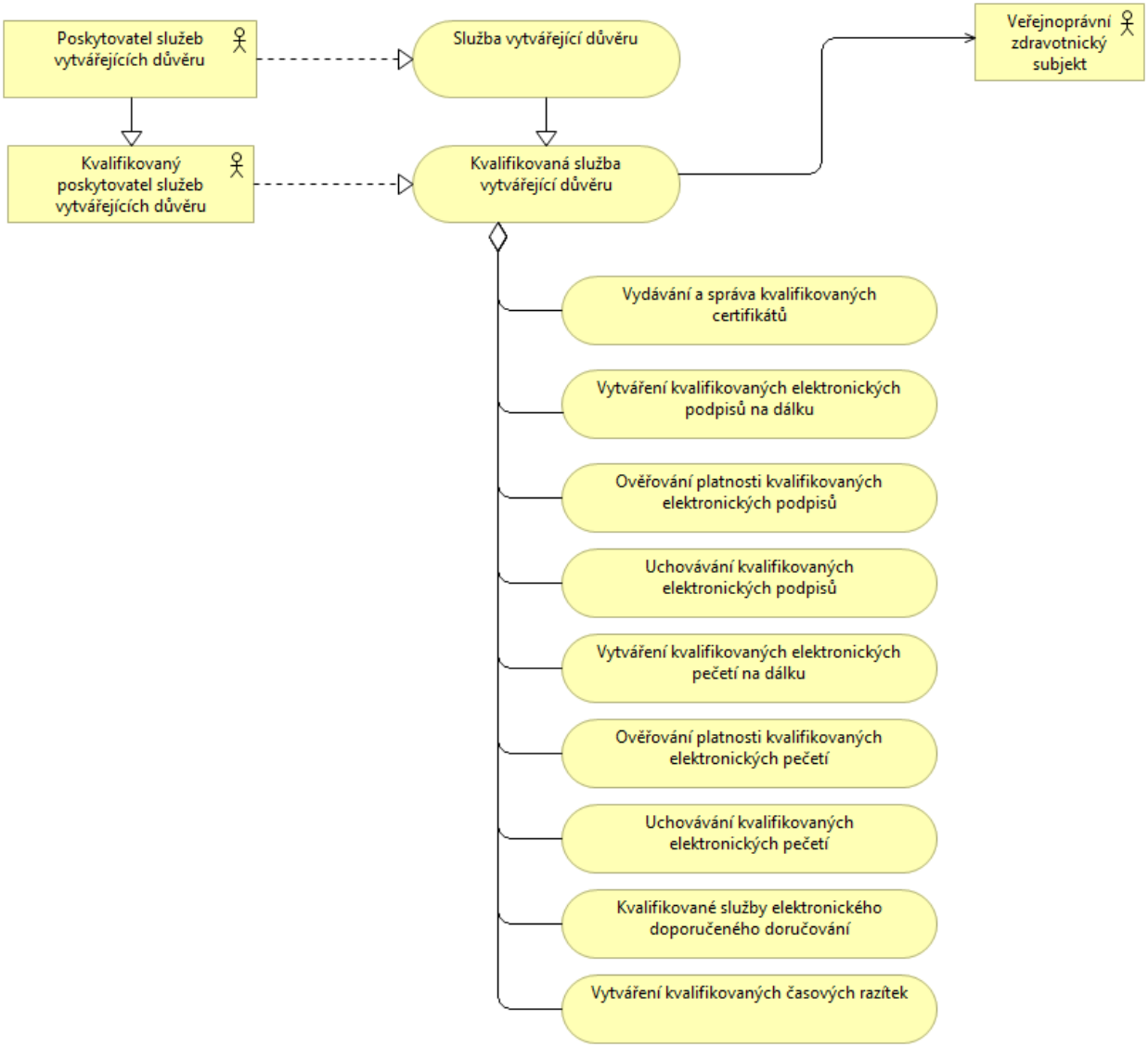
6.3.1 Vysvětlení hlavních pojmů služeb vytvářejících důvěru

Nařízení eIDAS v souvislosti se službami vytvářejícími důvěru zavádí do právního řádu pojmy, jejichž význam volně přibližujeme:

- Zaručený elektronický podpis/pečeť – vytvořen na principu asymetrického šifrování, certifikát identifikuje podepisující osobu.
- Kvalifikovaný elektronický podpis/pečeť – vytvořen kvalifikovaným prostředkem a je založen na kvalifikovaném certifikátu.

- Data pro vytváření elektronických podpisů/pečetí – soukromý klíč ve správě podepisující/pečetící osoby nebo kvalifikovaného poskytovatele služeb.
- Kvalifikovaný certifikát pro elektronický podpis/pečeť – vydán kvalifikovaným poskytovatelem a splňuje požadavky dle přílohy I/III eIDAS.
- Kvalifikovaný prostředek pro vytváření elektronických podpisů/pečetí – certifikovaný SW nebo HW, certifikační orgán určí členský stát, certifikované prostředky zvěřejňuje Komise na seznamu.
- Kvalifikovaný poskytovatel služeb vytvářejících důvěru – poskytuje alespoň jednu kvalifikovanou službu a orgán dohledu (MV ČR) mu udělil status „kvalifikovaný“.

Přehled kvalifikovaných služeb vytvářejících důvěru, tzn. těch služeb, k jejichž poskytování budou dle nařízení eIDAS oprávněni výlučně kvalifikovaní poskytovatelé, a na něž se bude VPZS spoléhat, znázorňuje následující diagram.



Obrázek 6: Služby vytvářející důvěru dle nařízení eIDAS

6.3.2 Přehled hlavních změn účinných od 1. 7. 2016

V souladu s ustanovením čl. 52 odst. 2 je nařízení eIDAS pro služby vytvářející důvěru účinné od 1. 7. 2016. Vzhledem k blízkosti termínu účinnosti Nařízení stanovuje čl. 51 přechodná opatření a návrh adaptačního zákona přináší změkčení právní úpravy a v § 13 přechodná ustanovení. Na tomto místě je uveden přehled hlavních změn, definice vyznačené kurzívou jsou dle zákona č. 227/2000 Sb., podtržené dle nařízení eIDAS.

- *Směrnice 1999/93/ES* (vnitrostátní implementace) → Nařízení EU 910/2014 (eIDAS)
- *Uznávaný elektronický podpis* → Kvalifikovaný elektronický podpis
- *Uznávaná elektronická značka*→ Kvalifikovaná elektronická pečeť
    - *Označující osoba* – fyzická nebo právnická osoba nebo organizační složka státu
    - Pečetící osoba – jen právnická osoba (včetně subjektu veřejného sektoru)
- *Kvalifikované časové razítko* → Kvalifikované elektronické časové razítko
- *Kvalifikovaný poskytovatel certifikačních služeb* → Kvalifikovaný poskytovatel služeb vytvářejících důvěru
- Komerční certifikát pro HTTPS web server → Kvalifikovaný certifikát pro autentizaci internetových stránek

6.3.3 Přehled zcela nových služeb vytvářejících důvěru

Nařízení eIDAS umožňuje kvalifikovaným poskytovatelům zavést a provozovat zcela nové, v praxi dosud neexistující služby:

- Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů – ověřování elektronických podpisů a pečetí na dálku u kvalifikovaného poskytovatele
- Kvalifikovaná služba uchovávání elektronických podpisů – zajistí důvěryhodnost kvalifikovaných elektronických podpisů a pečetí i po uplynutí doby technické platnosti
- Služba správy dat pro vytváření kvalifikovaných elektronických podpisů a vytváření kvalifikovaných elektronických podpisů jménem podepisující osoby – správa soukromých klíčů podepisujících osob a vytváření kvalifikovaných elektronických podpisů a pečetí na dálku u kvalifikovaných poskytovatelů
- Kvalifikovaná služba elektronického doporučeného doručování – odesílání a přijímání je zabezpečeno zaručeným podpisem či pečetí a časovým razítkem

6.3.4 Elektronický podpis

Nařízení eIDAS definuje pro elektronický podpis následující:

- **elektronický podpis** - data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena, a která podepisující osoba používá k podepsání;
- **zaručený elektronický podpis** - elektronický podpis, který splňuje tyto požadavky:
    - je jednoznačně spojen s podepisující osobou;
    - umožňuje identifikaci podepisující osoby;
    - je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou;

- je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat;

- **kvalifikovaný elektronický podpis** - zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy.

Z hlediska použitelnosti ve veřejných službách jsou důležité definice zaručeného a kvalifikovaného elektronického podpisu.

Elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy.

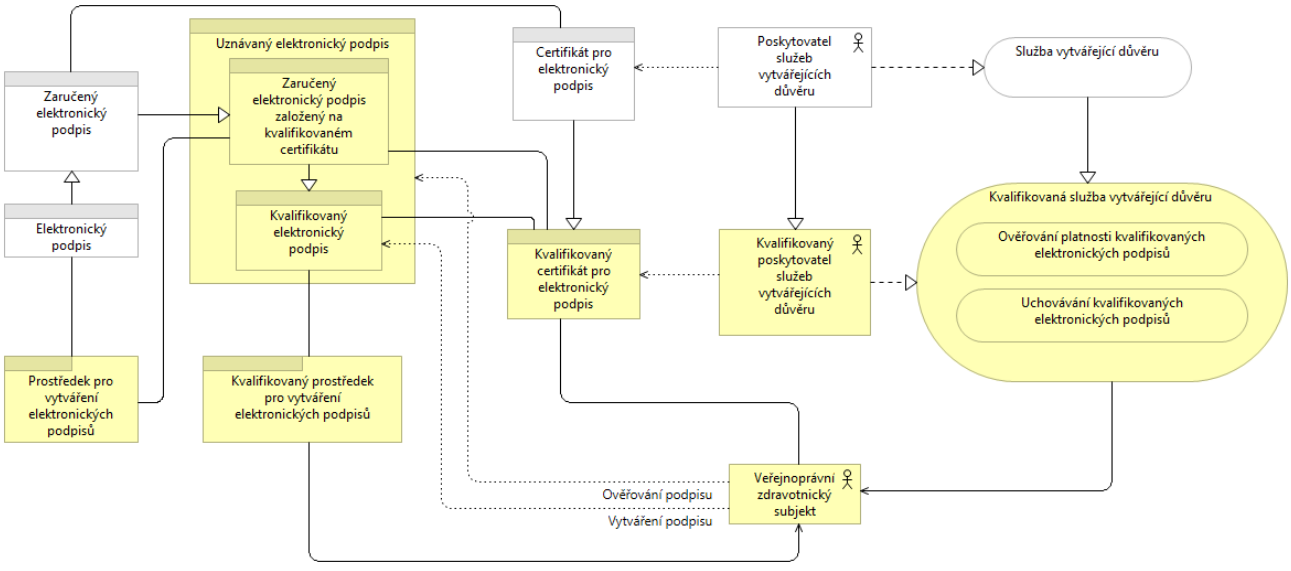
Kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu.

Kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě se uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech.

Této problematice se věnuje prováděcí rozhodnutí Komise (EU) 2015/1506, kterým se stanoví specifikace pro formáty zaručených elektronických podpisů a zaručených pečetí uznávaných subjekty veřejného sektoru.

Toto prováděcí rozhodnutí pak pracuje s termínem „zaručený elektronický podpis založený na kvalifikovaném certifikátu“. Tedy kombinace stávajícího stavu, kdy nejsou poptávány kvalifikované prostředky pro vytváření podpisu.

Jednotlivé typy elektronických podpisů, prostředky pro jejich vytváření, certifikáty pro jejich ověřování, související kvalifikované služby vytvářející důvěru a vzájemné vazby mezi nimi znázorňuje následující diagram.



Obrázek 7: Elektronické podpisy dle nařízení eIDAS

6.3.5 Kvalifikované certifikáty pro elektronický podpis

Kvalifikované certifikáty pro elektronické podpisy obsahují:

a) označení, alespoň ve formě vhodné pro automatické zpracování, že se certifikát vydává jako kvalifikovaný certifikát pro elektronický podpis;
b) soubor dat jednoznačně identifikujících kvalifikovaného poskytovatele služeb vytvářejících důvěru, který vydává kvalifikované certifikáty, včetně alespoň členského státu, v němž je poskytovatel usazen, a
   – v případě právnické osoby: název a případné registrační číslo uvedené v úředních záznamech,
   – v případě fyzické osoby: jméno osoby;
c) alespoň jméno podepisující osoby nebo pseudonym; je-li použit pseudonym, musí být tato skutečnost jasně vyznačena;
d) data pro ověřování platnosti elektronických podpisů, která odpovídají datům pro vytváření elektronických podpisů;
e) označení začátku a konce doby platnosti certifikátu;
f) identifikační číslo certifikátu, které musí být jedinečné pro daného kvalifikovaného poskytovatele služeb vytvářejících důvěru;
g) zaručený elektronický podpis nebo zaručenou elektronickou pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru, který certifikát vydává;
h) údaj o místu, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle písmene g);
i) údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu;
j) pokud jsou data pro vytváření elektronických podpisů spojená s daty pro ověřování platnosti elektronických podpisů obsažena v kvalifikovaném prostředku pro vytváření elektronických podpisů, příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování.

6.3.6 Elektronická pečeť

Podle nařízení eIDAS se elektronickou pečetí rozumí data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu.

Podobně jako pro elektronický podpis (identifikaci fyzické osoby), definuje nařízení eIDAS i úrovně pečetě:

- **elektronická pečeť** - data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu;
- **zaručená elektronická pečeť** - elektronická pečeť, která splňuje tyto požadavky:
  - je jednoznačně spojena s pečetící osobou;
  - umožňuje identifikaci pečetící osoby;
  - je vytvořena pomocí dat pro vytváření elektronických pečetí, která může pečetící osoba s vysokou úrovní důvěry použít k vytváření elektronické pečeti pod svou kontrolou;
  - je k datům, ke kterým se vztahuje, připojena takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat;

- **kvalifikovaná elektronická pečeť** - zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť;

Pečetící osobou je právnická osoba, která vytváří elektronickou pečeť.

Elektronické pečeti nesmějí být upírány právní účinky a nesmí být odmítána jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické pečetě.

U kvalifikované elektronické pečeti platí domněnka integrity dat a správnosti původu těch dat, s nimiž je kvalifikovaná elektronická pečeť spojena.

Kvalifikovaná elektronická pečeť založená na kvalifikovaném certifikátu vydaném v jednom členském státě se uznává jako kvalifikovaná elektronická pečeť ve všech ostatních členských státech.

6.3.7 Kvalifikované certifikáty pro elektronické pečetě

Kvalifikované certifikáty pro elektronické pečetě obsahují:

a) označení, alespoň ve formě vhodné pro automatické zpracování, že se certifikát vydává jako kvalifikovaný certifikát pro elektronickou pečeť;
b) soubor dat jednoznačně identifikujících kvalifikovaného poskytovatele služeb vytvářejících důvěru, který vydává kvalifikované certifikáty, včetně alespoň členského státu, v němž je poskytovatel usazen, a
   – v případě právnické osoby: název a případné registrační číslo uvedené v úředních záznamech,
   – v případě fyzické osoby: jméno osoby;
c) alespoň jméno pečetící osoby a případné registrační číslo uvedené v úředních záznamech;
d) data pro ověřování platnosti elektronických pečetí, která odpovídají datům pro vytváření elektronických pečetí;
e) označení začátku a konce doby platnosti certifikátu;
f) identifikační číslo certifikátu, které musí být jedinečné pro daného kvalifikovaného poskytovatele služeb vytvářejících důvěru;
g) zaručený elektronický podpis nebo zaručenou elektronickou pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru, který certifikát vydává;
h) údaj o místu, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle písmene g);
i) údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu;
j) pokud jsou data pro vytváření elektronických pečetí spojená s daty pro ověřování platnosti elektronických pečetí obsažena v kvalifikovaném prostředku pro vytváření elektronických pečetí, příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování.

6.3.8 Formáty zaručených elektronických podpisů a zaručených pečetí

Nařízení eIDAS ukládá členským státům povinnost vyžadovat zaručený elektronický podpis nebo pečeť.

Za účelem vymezení specifických formátů a referenčních metod byla stanovena řada formátů elektronických podpisů prováděcím rozhodnutím 2014/148 (EU). Na toto rozhodnutí pak navazuje prováděcí rozhodnutí Komise (EU) 2015/1506, kterým se stanoví specifikace pro formáty zaručených elektronických podpisů a zaručených pečetí uznávaných subjekty veřejného sektoru podle Nařízení eIDAS.

Jedná se o technické specifikace ETSI pro zaručené elektronické podpisy pro jednotlivé typy dokumentů, PDF dokumenty – PAdES, XML dokumenty – XAdES, obecná binární data – CAdES, a kontejnery s přidruženým podpisem – ASiC.

Seznam technických specifikací pro zaručené elektronické podpisy a pečetě ve formátech XML, CMS nebo PDF a kontejner s přidruženým podpisem:

- Výchozí profil XAdES: ETSI TS 103171 v.2.1.1
- Výchozí profil CAdES: ETSI TS 103173 v.2.2.1
- Výchozí profil PAdES: ETSI TS 103172 v.2.2.2
- Výchozí profil ASiC: ETSI TS 103174 v.2.2.1

6.3.9 Elektronická časová razítka

Elektronickému časovému razítku nesmějí být upírány právní účinky a nesmí být odmítáno jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické časové razítko.

U kvalifikovaného elektronického časového razítka platí domněnka správnosti data a času, které udává, a integrity dat, s nimiž jsou toto datum a tento čas spojeny.

Kvalifikované elektronické časové razítko vydané v jednom členském státě se uznává jako kvalifikované elektronické časové razítko ve všech členských státech.

Kvalifikované elektronické časové razítko může poskytovat pouze kvalifikovaný poskytovatel služby vytvářející důvěru.

Elektronický podpis, pečeť a časové razítko jsou prostředky pro vytváření elektronických dokumentů tak, aby byl jasně definován projev vůle podepisující osoby včetně jejího ztotožnění a dále pak ukotven okamžik podepsání.

6.3.10 Ověřování elektronických podpisů, pečetí a časových razítek

Typickým příkladem služby vytvářející důvěru je služba zajišťující ověření podpisových certifikátů použitých pro vytvoření elektronického podpisu, pečeti nebo razítka.

Nařízení eIDAS specifikuje obecný postup pro ověření platnosti podpisu, pečeti či razítka následujícími body:

- certifikát, na němž je podpis založen, byl v okamžiku podpisu kvalifikovaným certifikátem pro elektronický podpis;
- kvalifikovaný certifikát byl vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a v okamžiku podpisu byl platný;

- data pro ověřování platnosti podpisu odpovídají datům poskytnutým spoléhající se straně;
- spoléhající se straně je řádně poskytnut jedinečný soubor dat identifikujících podepisující osobu v certifikátu;
- pokud byl v okamžiku podpisu použit pseudonym, je jeho použití jednoznačně sděleno spoléhající se straně;
- elektronický podpis byl vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů;
- nebyla ohrožena integrita podepsaných dat;
- v okamžiku podpisu byly splněny požadavky na úroveň zaručený elektronický podpis.

Dále definuje požadavek na předložení výsledku postupu ověření. Systém použitý k ověření platnosti kvalifikovaného elektronického podpisu musí poskytovat spoléhající se straně řádný výsledek postupu ověření platnosti a umožňovat jí zjistit jakékoli problémy týkající se bezpečnosti.

Pro kvalifikovanou službu vytvářející důvěru pro ověřování elektronických podpisů, pečetí a razítek navíc definuje, že takový systém smí provozovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru a musí splňovat požadavky na poskytnutí výsledku ověření oběma spoléhajícím stranám automatizovaným způsobem, který je spolehlivý, účinný a je opatřen zaručeným elektronickým podpisem nebo zaručenou elektronickou pečetí poskytovatele kvalifikované služby ověřování platnosti.

Dále pak nařízení eIDAS definuje v části týkající se požadavků na kvalifikované poskytovatele služeb vytvářejících důvěru dobu, ve které je nutné uveřejnit zneplatnění certifikátu:

„Jestliže se kvalifikovaný poskytovatel služeb vytvářejících důvěru vydávající kvalifikované certifikáty rozhodne určitý certifikát zneplatnit, zaeviduje toto zneplatnění ve své databázi certifikátů a zneplatnění certifikátu včas a v každém případě do 24 hodin od obdržení žádosti zveřejní. Zneplatnění nabývá účinku okamžitě po zveřejnění.“

Očekáváme upřesnění této formulace v novém zákonu o službách vytvářejících důvěru, neboť z této formulace se dá dedukovat, že po zneplatnění certifikátu je možné s ním dále podepisovat a takto vytvořené podpisy budou platné až 24 hodin od zneplatnění. Je zde jistý tlak na kvalifikované poskytovatele služeb vytvářející důvěru (certifikační autority), aby informace o zneplatněných certifikátech zveřejňovali okamžitě. Ale tento tlak není dán legislativou a nařízení eIDAS trochu nešťastně definuje pouze okamžik nabytí účinku zneplatnění.

6.3.11 Uchování elektronických podpisů

Kvalifikovanou službu uchovávání kvalifikovaných elektronických podpisů může poskytovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru, který používá postupy a technologie, jež jsou s to zajistit důvěryhodnost kvalifikovaného elektronického podpisu i po uplynutí doby technické platnosti.

Toto je prozatím veškerá formulace v rámci nařízení eIDAS týkající se dlouhodobého uchovávání elektronických podpisů. V kontextu specifikací technických norem ETSI pro

formáty zaručených elektronických podpisů a pečetí lze předpokládat, že Komise (EU) prostřednictvím prováděcích aktů určí čísla referenčních norem, které budou navazovat na existující specifikace ETSI.

6.3.12 Elektronické doporučené doručování

Nařízení eIDAS definuje elektronické doporučené doručování jako službu, která umožňuje přenášet data mezi třetími osobami elektronickými prostředky a poskytuje důkazy týkající se nakládání s přenášenými daty, včetně dokladu o odeslání a přijetí dat, a která chrání přenášená data před rizikem ztráty, odcizení, poškození nebo neoprávněných změn.

Dále pak definuje kvalifikovanou službu doporučeného doručování, která musí splnit následující:

- je poskytována jedním či více kvalifikovanými poskytovateli služeb vytvářejících důvěru;
- s vysokou úrovní spolehlivosti zajišťuje identifikaci odesílatele;
- zajišťuje identifikaci příjemce před doručením dat;
- odesílání a přijímání dat je zabezpečeno prostřednictvím zaručeného elektronického podpisu nebo zaručené elektronické pečeti kvalifikovaného poskytovatele služeb vytvářejících důvěru tak, aby byla vyloučena možnost nezjistitelné změny dat;
- odesílatel a příjemce dat jsou jednoznačně vyrozuměni o případných změnách dat potřebných za účelem odeslání nebo přijetí dat;
- datum a čas odeslání, přijetí a případná změna dat jsou označeny prostřednictvím kvalifikovaného elektronického časového razítka.

6.4 Návrh adaptačního zákona eIDAS

Adaptaci eIDAS do vnitrostátního práva ČR tvoří návrh zákona o službách vytvářejících důvěru pro elektronické transakce a o změně některých zákonů, dostupný on-line na URL adrese http://www.psp.cz/sqw/historie.sqw?o=7&T=763.

Na návrh adaptačního zákona navazuje návrh souboru změn stávajících zákonů, dostupný on-line na URL adrese http://www.psp.cz/sqw/historie.sqw?o=7&t=764. Soubor změn souvisejících s návrhem adaptačního zákona obsahuje i návrhy změn zákonů relevantních pro resort zdravotnictví:

- Zákon č. 551/1991 Sb., o Všeobecné zdravotní pojišťovně České republiky
- Zákon č. 280/1992 Sb., o resortních, oborových, podnikových a dalších zdravotních pojišťovnách
- Zákon č. 258/2000 Sb., o ochraně veřejného zdraví
- Zákon č. 372/2011 Sb., o zdravotních službách
- Zákon č. 373/2011 Sb., o specifických zdravotních službách

Následující kapitoly obsahují popis základních změn, které návrh adaptačního zákona obsahuje.

6.4.1 Oblast elektronické identifikace a autentizace

Návrh adaptace eIDAS do vnitrostátního práva ČR se týká výlučně úpravy podrobností využívání a poskytování služeb vytvářejících důvěru, do oblasti elektronické identifikace a autentizace nijak nezasahuje.

6.4.2 Oblast služeb vytvářejících důvěru

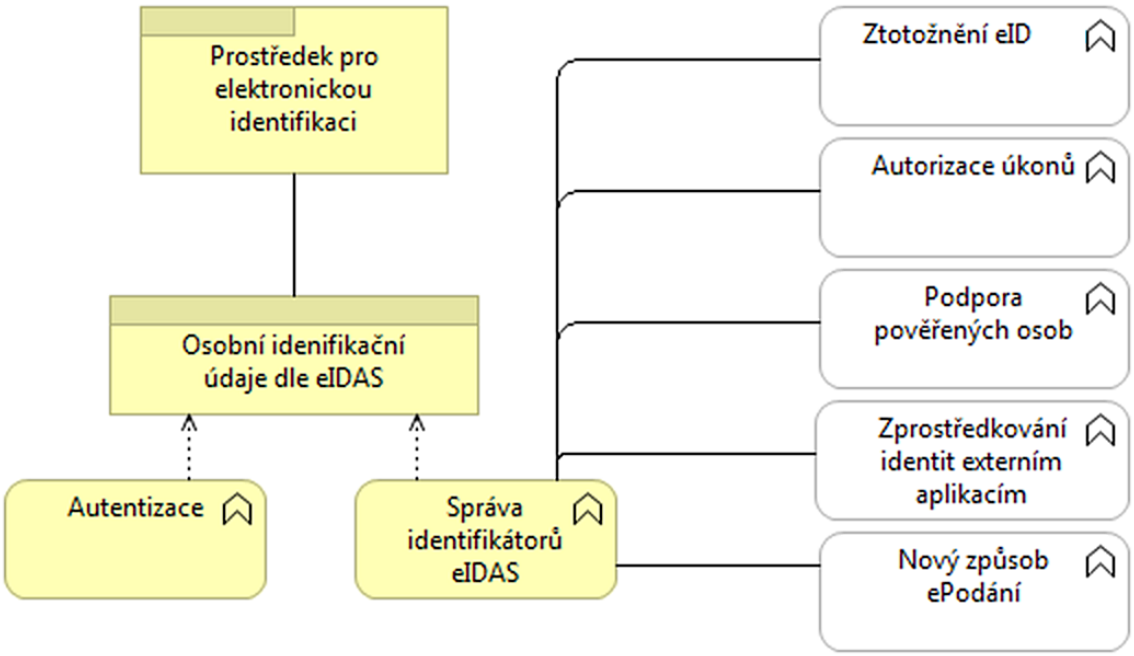
Návrh adaptace eIDAS do vnitrostátního práva ČR obsahuje v oblasti služeb vytvářejících důvěru následující skutečnosti:

- Zavádí ve vnitrostátním právu nový význam pojmu uznávaný elektronický podpis. Fakticky budou uznávány 2 formy elektronických podpisů:
  - zaručený elektronický podpis = založený na kvalifikovaném certifikátu;
  - kvalifikovaný elektronický podpis = zaručený elektronický podpis vytvořený kvalifikovaným prostředkem pro vytváření elektronických podpisů.
- Zavádí nový pojem uznávaná elektronická pečeť, která nahradí stávající uznávanou elektronickou značku. Rozdíl oproti stávající uznávané elektronické značce spočívá v tom, že pečetící osobou bude moci být pouze právnická osoba. Analogicky k uznávanému elektronickému podpisu adaptační zákon rovněž rozlišuje 2 formy elektronických pečetí:
  - zaručená elektronická pečeť = založená na kvalifikovaném certifikátu;
  - kvalifikovaná elektronická pečeť = zaručená elektronická pečeť vytvořená kvalifikovaným prostředkem pro vytváření elektronických podpisů.
- Fyzické a právnické osoby mohou vůči orgánům státní správy a veřejné moci činit úkony oběma typy elektronických podpisů/pečetí.
- Orgány státní správy a veřejné moci (jako tzv. veřejnoprávní podepisující) mohou činit úkony pouze kvalifikovanými elektronickými podpisy/pečetěmi s odkladem této povinnosti do 2 let od nabytí účinnosti adaptačního zákona;
  - mohou přechodně 2 roky činit úkony i zaručeným elektronickým podpisem/značkou.
- Ruší zákon č. 227/2000 Sb. o elektronickém podpisu včetně prováděcích vyhlášek:
  - č. 212/2012 Sb. o ověřování platnosti zaručeného elektronického podpisu;
  - č. 378/2006 Sb. o postupech kvalifikovaných poskytovatelů certifikačních služeb.

6.5 Přehled druhů dopadů

6.5.1 Dopady elektronické identifikace

Nařízení eIDAS a související právní normy předepisují podmínky pro systémy elektronické identifikace a podmínky pro jejich využívání ve službách veřejného sektoru. Přímé i odvozené důsledky těchto předpisů ilustruje následující obrázek. Žluté komponenty označují přímé dopady, bílé komponenty pak odvozené dopady elektronické identifikace.



Obrázek 8: Dopady nařízení eIDAS na elektronickou identifikaci

Přímým důsledkem eIDAS je pro účely autentizace nutnost přeshraničního uznávání prostředků pro elektronickou identifikaci. Bude tedy nutné rozšířit informační systémy VPZS o evidenci a správu prostředků pro elektronickou identifikaci dle eIDAS a s nimi spojených identifikačních údajů. eIDAS předepisuje minimální soubor identifikačních údajů pro fyzické i právnické osoby včetně jedinečných identifikátorů. Protože každá osoba může mít více prostředků pro elektronickou identifikaci a tedy i více identifikačních údajů, bude třeba řešit také správu identifikátorů eIDAS.

Nepřímým důsledkem přeshraničního uznávání prostředků pro elektronickou identifikaci bude nutnost rozšíření stávajících systémů takovým způsobem, aby uživatelé autentizovaní prostřednictvím autentizačních služeb systému elektronické identifikace měli přístup ke stejným službám IIS jako uživatelé autentizovaní prostřednictvím jiných služeb.

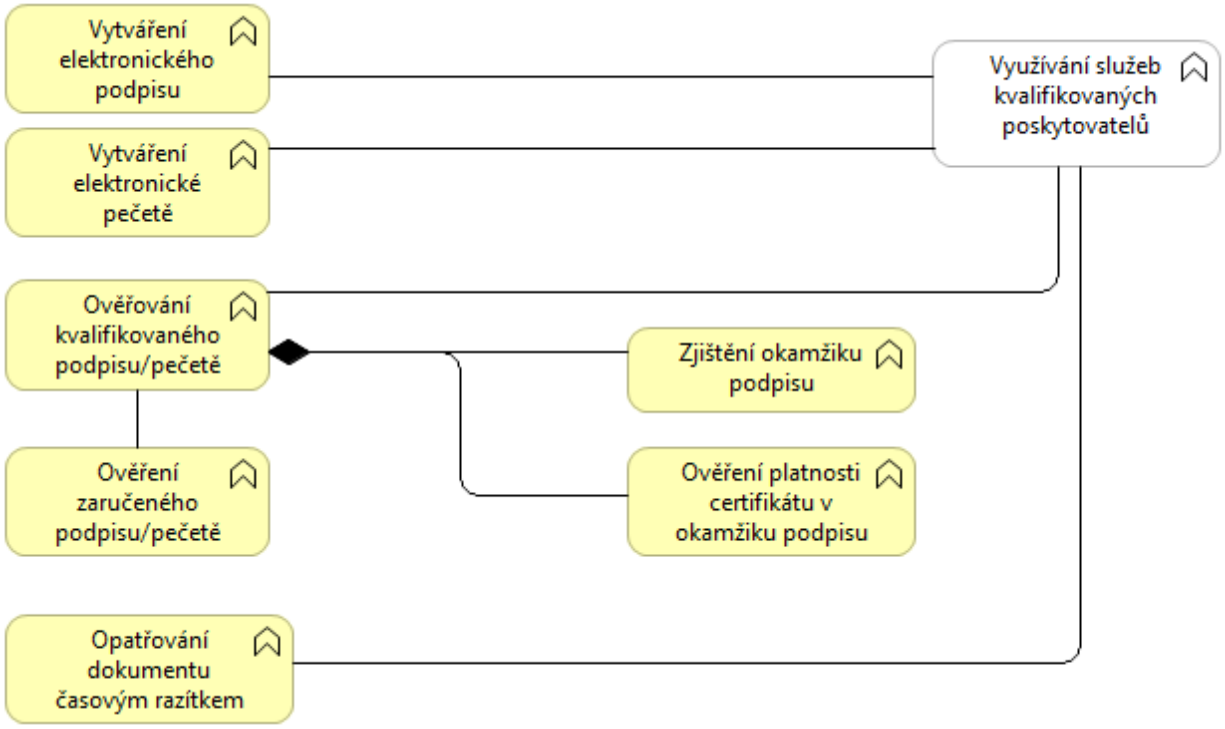
Těmito nepřímými dopady jsou zejména:

- Ztotožnění eID: Kvůli novým možnostem přihlašování bude třeba upravit a rozšířit způsob, jak ztotožnit elektronickou identitu s osobou v IS VPZS.
- Zprostředkování identit externím aplikacím: Způsob zprostředkování identit externím aplikacím musí umožňovat zprostředkování i těch identit, které jsou uznávané v rámci přeshraničního uznávání autentizačních služeb.
- Nový způsob e-Podání: Možnost učinit elektronické podání bez nutnosti využít datovou schránku či použití kvalifikovaného certifikátu musí být v souladu s nutností přeshraničního uznávání autentizačních služeb.
- Podpora pověřených osob: Podpora pověření a oprávnění při využívání on-line služeb VPZS musí být v souladu s nutností přeshraničního uznávání autentizačních služeb.
- Autorizace úkonů: Autorizace úkonů při využívání on-line služeb VPZS musí být v souladu s nutností přeshraničního uznávání autentizačních služeb.

6.5.2 Dopady služeb vytvářejících důvěru

Služby vytvářející důvěru nahrazují ustanovení směrnice 1999/93/ES a vnitrostátního práva k elektronickému podpisu. Současně přinášejí zcela nové kvalifikované služby, které mají odstranit překážky pro výkon práv občanů jednotného digitálního trhu. K provozování a poskytování kvalifikovaných služeb eIDAS opravňuje výlučně kvalifikované poskytovatele.

Přímé i odvozené důsledky těchto předpisů ilustruje následující obrázek. Žluté komponenty označují přímé dopady, bílé komponenty pak odvozené dopady kvalifikovaných služeb vytvářejících důvěru.



Obrázek 9: Dopady využívání služeb vytvářejících důvěru dle nařízení eIDAS

Přímými dopady eIDAS a souvisejících právních norem jsou změny v oblastech:

- Vytváření elektronického podpisu: Návrh adaptačního zákona předepisuje pro subjekty veřejného sektoru povinnost používat výhradně kvalifikované podpisy, bude tedy nutné zajistit vytváření elektronického podpisu prostřednictvím kvalifikovaného prostředku.
- Vytváření elektronické pečetě: Návrh adaptačního zákona předepisuje pro subjekty veřejného sektoru povinnost používat kvalifikované elektronické pečetě, bude tedy nutné zajistit vytváření elektronické pečetě prostřednictvím kvalifikovaného prostředku.
- Ověřování zaručeného podpisu/pečetě, ověřování kvalifikovaného podpisu/pečetě: eIDAS požaduje ověřování platnosti certifikátu, na kterém je podpis založen, k okamžiku podpisu. Bude tedy třeba zajistit, že proces ověřování uznávaných elektronických podpisů odpovídá novým požadavkům. Prováděcí nařízení specifikující technické požadavky na ověřování podpisů a pečetí nejsou v současnosti k dispozici.

- Opatřování dokumentu časovým razítkem: Návrh adaptačního zákona předepisuje pro subjekty veřejného sektoru povinnost používat kvalifikovaná časová razítka a bude tedy nutné zajistit vytváření časových razítek prostřednictvím kvalifikované služby.

Nařízení eIDAS umožňuje kvalifikovaným poskytovatelům zavést a provozovat zcela nové, v praxi dosud neexistující služby:

- Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů – ověřování elektronických podpisů a pečetí na dálku u kvalifikovaného poskytovatele
- Kvalifikovaná služba uchovávání elektronických podpisů – zajistí důvěryhodnost kvalifikovaných elektronických podpisů/pečetí i po uplynutí doby technické platnosti
- Služba správy dat pro vytváření kvalifikovaných elektronických podpisů a vytváření kvalifikovaných elektronických podpisů jménem podepisující osoby – správa soukromých klíčů podepisujících osob a vytváření kvalifikovaných elektronických podpisů/pečetí na dálku u kvalifikovaných poskytovatelů
- Kvalifikovaná služba elektronického doporučeného doručování – odesílání a přijímání zabezpečeno zaručeným podpisem/pečetí a časovým razítkem

Dá se předpokládat nepřímý dopad na aplikační služby, protože s rozšířením těchto služeb bude ze strany veřejnosti očekáváno jejich využívání orgány veřejné moci.

6.5.3 Dopady služeb elektronického doručeného doručování

Nařízení eIDAS stanoví nová pravidla pro kvalifikované služby elektronického doporučené doručování. Tato pravidla mohou mít vliv na změny současného systému Datových schránek a těmto změnám bude třeba se přizpůsobit.

6.5.4 Dopady autentizace webových stránek

Nařízení eIDAS stanoví požadavky na kvalifikované certifikáty pro autentizaci internetových stránek. Webové stránky VPZS tedy budou muset používat certifikáty, které tyto požadavky splňují.

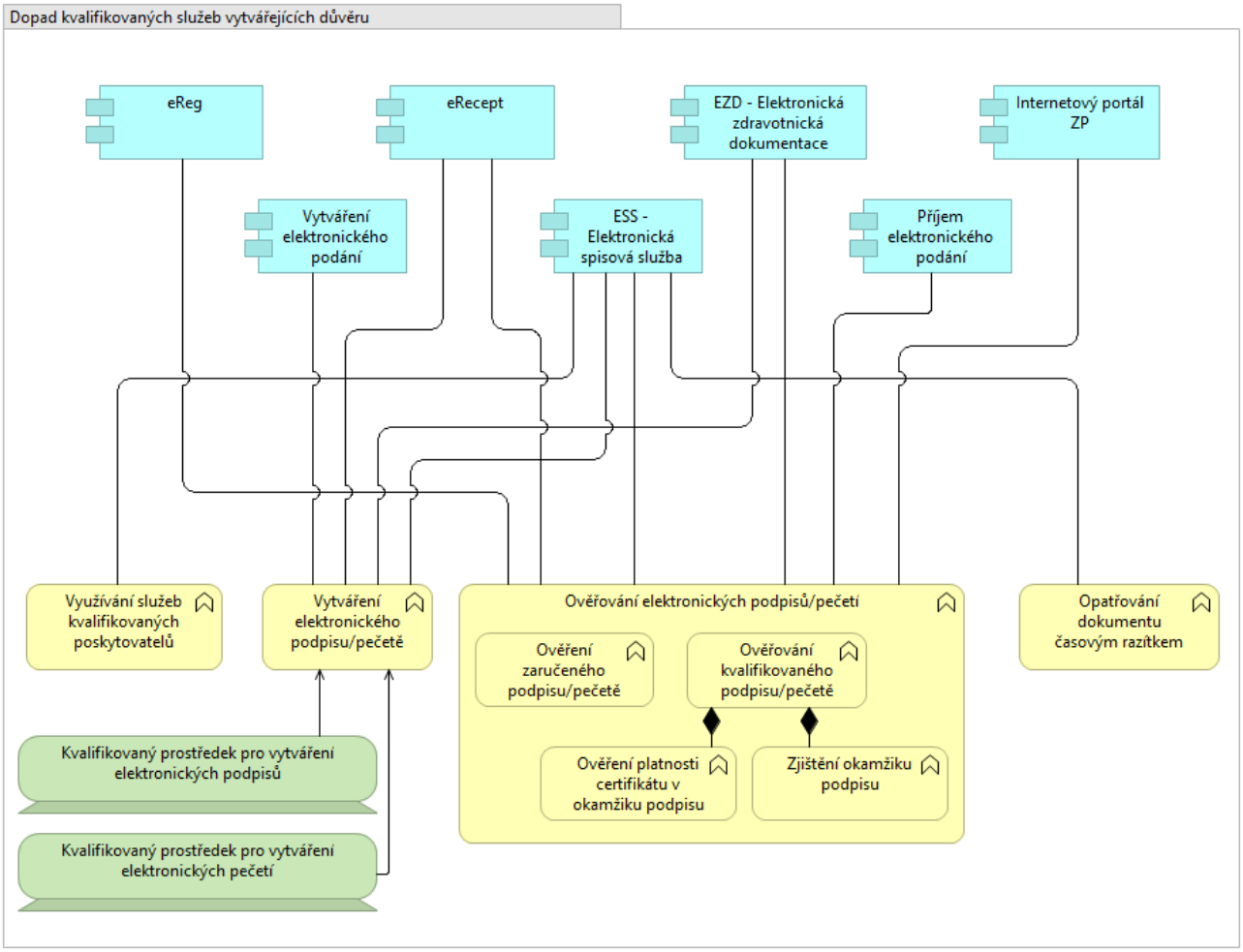
6.5.5 Dopady při komunikaci s externími systémy

Vzhledem ke skutečnosti, že komunikace IS VPZS mohou probíhat oddělenými kanály mimo veřejně dostupné služby, je nutné, aby každý VPZS posoudil právní stav a určil, zda se u jím provozovaných systémů jedná dle eIDAS o tzv. uzavřený systém, nebo o tzv. veřejnou on-line službu. Podle zjištěného právního stavu připadají do úvahy dvě varianty dopadů:

a) **uzavřený systém** – požadavky eIDAS se na elektronické podpisy/pečetě nevztahují;
b) **veřejná on-line služba** – bude třeba přejít na kvalifikované podpisy/pečetě a bude nutné zajistit podepisování kvalifikovaným prostředkem.

6.6 Dopady eIDAS na systémy VPZS využívající uznávané elektronické podpisy

Přehled dopadů v oblasti využívání elektronických podpisů a pečetí včetně vazeb na konkrétní systémy VPZS zobrazuje následující obrázek. Modře podbarvené komponenty diagramu představují systémy VPZS, zelené prvky jsou kvalifikované prostředky pro vytváření elektronických podpisů a pečetí.



Obrázek 10:Dopady na využívání elektronických podpisů dle nařízení eIDAS

7 Návrh cílového stavu ve dvou variantách

7.1 Detailní popis řešení

V následujících kapitolách je popsán cílový stav architektury řešení dopadů nařízení eIDAS.

7.1.1 Odpovědnost VPZS vyplývající z nařízení eIDAS

Ustanovení nařízení eIDAS a adaptačního zákona kladou na VPZS odpovědnost:

- Zajistit ověřování kvalifikovaných elektronických podpisů a pečetí v souladu s požadavky čl. 32 nařízení č. 910/2014.
- Zajistit ověřování zaručených elektronických podpisů a pečetí v souladu s požadavky vnitrostátního adaptačního zákona.
- Zajistit vytváření kvalifikovaných elektronických podpisů a pečetí kvalifikovaným prostředkem pro vytváření elektronických podpisů v souladu s požadavky čl. 29 nařízení č. 910/2014.
- Uznávat prostředky pro elektronickou identifikaci fyzických a právnických osob, které byly vydány v souladu s nařízením č. 910/2014 v jiných členských státech.
- Odpovídat za škodu, kterou úmyslně nebo z nedbalosti způsobí kterékoli fyzické nebo právnické osobě nezajištěním správného fungování autentizace v přeshraniční transakci.

7.1.2 Hlavní povinnosti VPZS vyplývající z nařízení eIDAS;

V rámci předchozích kapitoly analýzy byly identifikovány systémy resortu zdravotnictví, na které má nařízení eIDAS přímý dopad.

Povinnosti vyplývající z nařízení č. 910/2014 lze rozdělit na tři základní oblasti a jim odpovídající požadavky na úpravy v informačních systémech VPZS:

1. **Ověřování elektronických podpisů a pečetí**
   Požadavek: Zavést nový způsob ověřování kvalifikovaných elektronických podpisů a pečetí.
2. **Vytváření kvalifikovaných elektronických podpisů a pečetí**
   Požadavek: Zavést kvalifikované prostředky pro vytváření kvalifikovaných elektronických podpisů a pečetí.
3. **Uznávání prostředků pro elektronickou identifikaci (dále též „eID“)**
   Požadavek: Realizovat systém pro uznávání prostředků pro elektronickou identifikaci.

7.1.3 Návrh variant řešení nových povinností VPZS

7.1.3.1 Ověřování elektronických podpisů a pečetí od 1. 7. 2016

Zavedení nového postupu a metody ověřování kvalifikovaných elektronických podpisů a pečetí a uznávaných elektronických podpisů a pečetí.

Podle nařízení eIDAS bude od 1. 7. 2016 povinností VPZS:

- Ověřovat kvalifikované elektronické podpisy a pečetě novým postupem v souladu s požadavky čl. 32 nařízení č. 910/2014.
- Uznávat kvalifikované elektronické podpisy a pečetě osob, kterým byl vydán kvalifikovaný certifikát v jiném členském státě EU.

K tomu byly identifikovány 2 alternativy ověřování kvalifikovaných elektronických podpisů a pečetí (dále též „QEP“):

Varianta A: QEP se budou ověřovat prostředky systémů VPZS, které jejich dodavatelé upraví dle požadavků nařízení č. 910/2014. V tomto případě dodavatelé smluvně převezmou závazek odpovědnosti za soulad s nařízením č. 910/2014 a povinností uhradit náhradu vzniklé škody.

Varianta B: QEP se budou ověřovat s využitím služby kvalifikovaného poskytovatele služeb vytvářejících důvěru, v systémech VPZS bude zaveden modul (knihovna) pro ověřování dodaný kvalifikovaným poskytovatelem. V tomto případě bude právní odpovědnost za soulad s nařízením č. 910/2014 přenesena na kvalifikovaného poskytovatele služeb vytvářejících důvěru.

Obě výše uvedené varianty musí zahrnovat i funkcionalitu ověření uznávaného elektronického podpisu a pečeti.

Termín pro nasazení změn v ověřování kvalifikovaného elektronického podpisu a kvalifikované pečetě v produkci je do 30. 6. 2016, nařízení eIDAS pro tento požadavek je účinné od 1. 7. 2016.

7.1.3.2 Vytváření kvalifikovaných elektronických podpisů a pečetí

Podle nařízení eIDAS bude nejpozději do 2 let od nabytí účinnosti vnitrostátního zákona o službách vytvářejících důvěru povinností VPZS:

- Vytvářet pouze kvalifikované elektronické podpisy a pečetě. Přechodně bude po 1. 7. 2016 moci po dobu 2 let používat stávající zaručené elektronické podpisy a pečetě.
- K vytváření kvalifikovaných elektronických podpisů a pečetí používat pouze kvalifikované prostředky pro vytváření elektronických podpisů certifikované dle standardu CEN CWA 14169.

K tomu byly identifikovány 2 alternativy vytváření kvalifikovaných elektronických podpisů a pečetí kvalifikovanými prostředky pro vytváření elektronických podpisů (dále též „QESCD“):

Varianta A: VPZS nakoupí QESCD a ty budou integrovány do systémů VPZS, které k tomu jejich dodavatelé upraví dle požadavků VPZS.

Varianta B: Bude využito ustanovení odst. 3. přílohy II nařízení č. 910/2014, kdy data podepisujících osob pro vytváření elektronického podpisu a QESCD spravuje kvalifikovaný poskytovatel služeb vytvářejících důvěru. Jednalo by se tedy o vytváření na dálku, kdy by v systémech VPZS byl zaveden modul (knihovna) pro komunikaci se systémem kvalifikovaného poskytovatele.

Namísto uznávaných elektronických podpisů a uznávaných elektronických značek při jejich vytváření musí VPZS přejít k používání kvalifikovaných elektronických podpisů a kvalifikovaných elektronických pečetí. Zároveň je potřeba zavést kvalifikované prostředky pro vytváření elektronických podpisů (obdoba současných prostředků pro bezpečné vytváření elektronických podpisů), což jsou certifikované HW nástroje.

Termín pro zavedení je v souladu s přechodným obdobím účinnosti adaptačního zákona 2 roky, reálně však do vypršení platnosti jednotlivých certifikátů stávajících elektronických podpisů a značek, protože je možné, že certifikační autority budou po 1. 7. 2016 vydávat nové certifikáty pouze podle nových pravidel stanovených nařízením eIDAS.

7.1.3.3 Uznávání prostředků pro elektronickou identifikaci

Zavedení systému pro uznávání prostředků pro elektronickou identifikaci fyzických a právnických osob, které jsou spojeny se systémy elektronické identifikace zveřejněnými v úředním věstníku EU.

Podle nařízení eIDAS bude nejpozději od 18. 9. 2018 v souvislosti s veřejně dostupnými informačními systémy povinností VPZS:

- Uznávat prostředky pro elektronickou identifikaci fyzických a právnických osob, které byly vydány v souladu s nařízením č. 910/2014 v jiných členských státech (dobrovolné uznávání od 18. 9. 2016).

Uznávání prostředků pro elektronickou identifikaci dle nařízení eIDAS se primárně týká klientů zdravotních služeb (pacientů / pojištěnců / občanů), ale může být volitelně využito i zdravotnickými pracovníky.

K tomu byly identifikovány 2 alternativy uznávání prostředků pro elektronickou identifikaci:

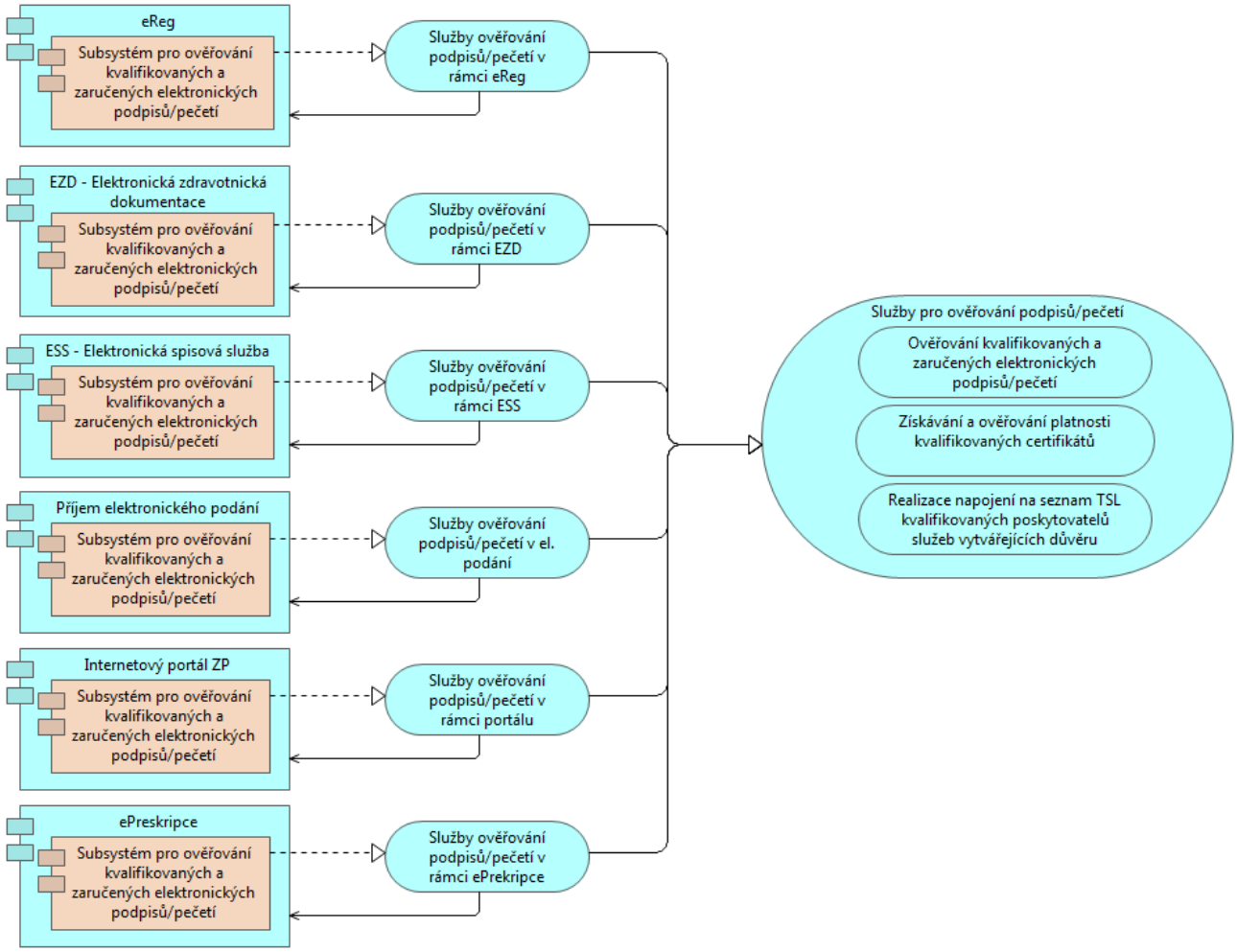
Varianta A: VPZS se pro identifikaci a autentizaci klientů zdravotních služeb budou spoléhat na systém Národní identitní autorita (NIA), který připravuje a bude provozovat MV ČR jako tzv. národní uzel eIDAS. NIA bude propojena s registrem obyvatel (ROB) a bude poskytovat o osobě i další údaje než požaduje nařízení eIDAS. Tato varianta podporuje maximální využití prostředků dostupných v rámci eGovernmentu – strategie „eGov first“.

Varianta B: MZ ČR vybuduje nový identitní prostor pro správu klientů zdravotních služeb, který bude zajišťovat registraci, ztotožnění a správu identifikačních údajů osoby vlastníka prostředků pro elektronickou identifikaci, případně umožní i použití jiných prostředků pro autentizaci než požadovaných nařízením eIDAS. Tato varianta podporuje resortní odpovědnost za existenci základního registru pacientů – strategie řízení oddělených identit, vhodným příkladem je stav v Rakousku.

Termín pro implementaci služeb souvisejících s elektronickou identifikací a autentizací je 18. 9. 2018. Vzhledem k náročnosti implementace je navrženo zahájit výše uvedené úpravy již nyní v postupných krocích.

7.1.4 Varianta A

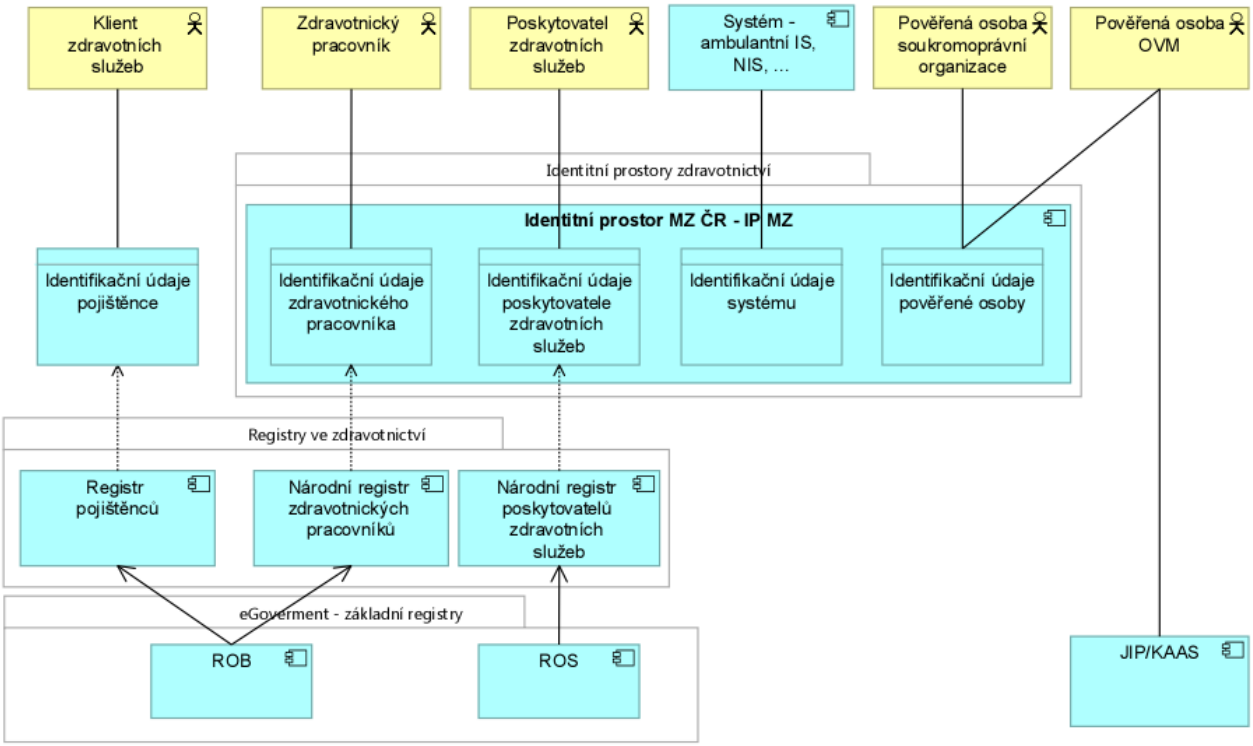
7.1.4.1 Ověřování elektronických podpisů



Obrázek 11 – Varianta A ověřování kvalifikovaných elektronických podpisů

Oranžově podbarvené komponenty představují subsystémy jednotlivých systémů VPZS, které budou upraveny dle požadavků nařízení eIDAS. Modře podbarvené jsou služby těchto subsystémů – ověřování kvalifikovaných a zaručených elektronických podpisů/pečetí, získávání a ověřování platnosti kvalifikovaných certifikátů, realizace napojení na seznam TSL kvalifikovaných poskytovatelů služeb vytvářejících důvěru. Bíle podbarvené komponenty představují systémy VPZS, které budou tyto služby využívat.

7.1.4.2 Identitní prostory



Obrázek 12 – Varianta A správy subjektů v identitních prostorech

Základním prvkem architektury se vztahem na identifikaci a autentizaci jsou identitní prostory. Diagram zobrazuje vazbu mezi subjekty a identitními prostory.

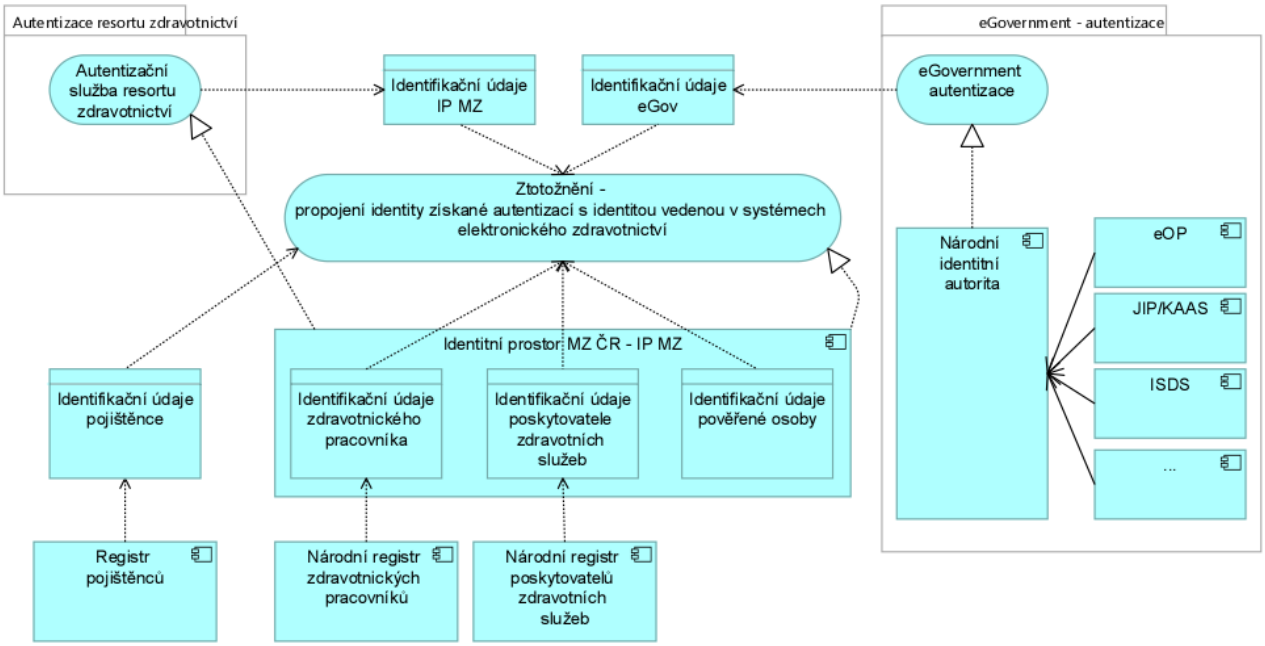
Subjekty, pro které bude třeba ve zdravotnictví řešit identifikaci a autentizaci, jsou:

- Klient zdravotních služeb
- Zdravotnický pracovník
- Poskytovatel zdravotních služeb
- Pověřená osoba soukromoprávní organizace
- Pověřená osoba OVM
- Systém – např. NIS, ambulatní IS atd.

Autoritativní identifikační údaje pro klienty zdravotních služeb zastřešuje Národní identitní autorita (NIA), která Zdrojovým systémem NIA pro autoritativní identifikační údaje je základní registr obyvatel (ROB).

Autoritativní identifikační údaje pro ostatní subjekty zastřešuje aplikační komponenta Identitní prostor MZ ČR (IP MZ). Zdrojovými systémy pro autoritativní identifikační údaje pro některé subjekty jsou registry ve zdravotnictví – Registr pojištěnců, Národní registr zdravotnických profesionálů a Národní registr poskytovatelů zdravotních služeb. Zdrojem referenčních údajů pro tyto registry jsou ROS a ROB. Tím je zajištěno, že identita všech hlavních subjektů ve zdravotnictví je ztotožněna se základními registry.

7.1.4.3 Vazby autentizačních služeb



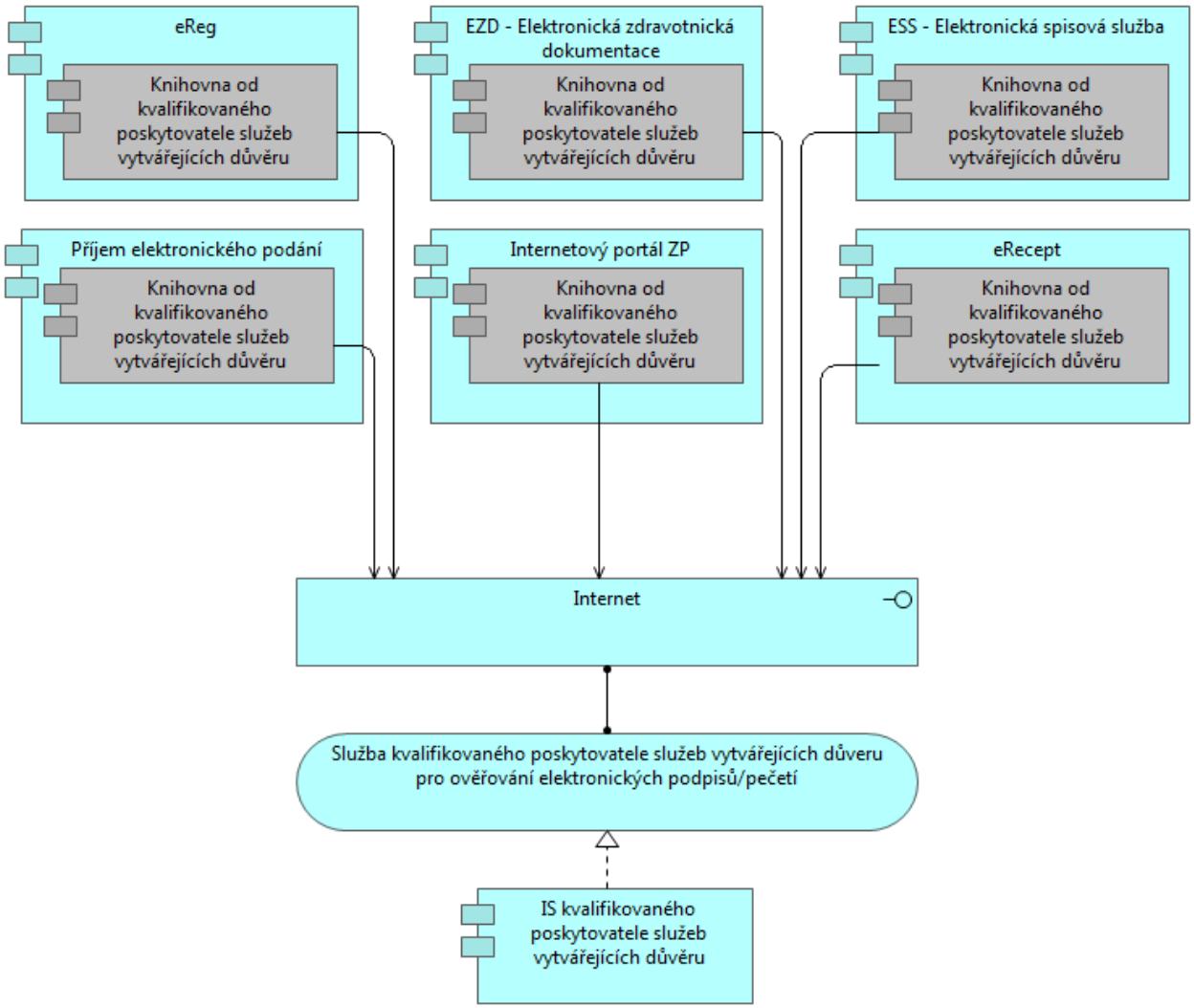
Obrázek 13 – Varianta A autentizačních služeb

Diagram zachycuje dvě autentizační služby, které budou sloužit k přihlašování ke službám elektronického zdravotnictví. První je eGovernment autentizace, kterou bude realizovat Národní identitní autoria (NIA). NIA bude slouži pro autentizaci různými autentizačními prostředky – eOP, ISDS, JIP/KAAS, zahraničním prostředkem dle nařízení eIDAS a dalšími.

Klienti zdravotních služeb budou moci využívat výlučně autentizační služby NIA. Pro ostatní subjekty, které nebudou využívat autentizační služby NIA, realizuje Identitní prostor MZ ČR alternativu ve formě autentizační služby resortu zdravotnictví. IP MZ také realizuje službu Ztotožnění, která zajistí propojení identifikačních dat získaných od autentizačních služeb s autoritativními identifikačními údaji.

7.1.5 Varianta B

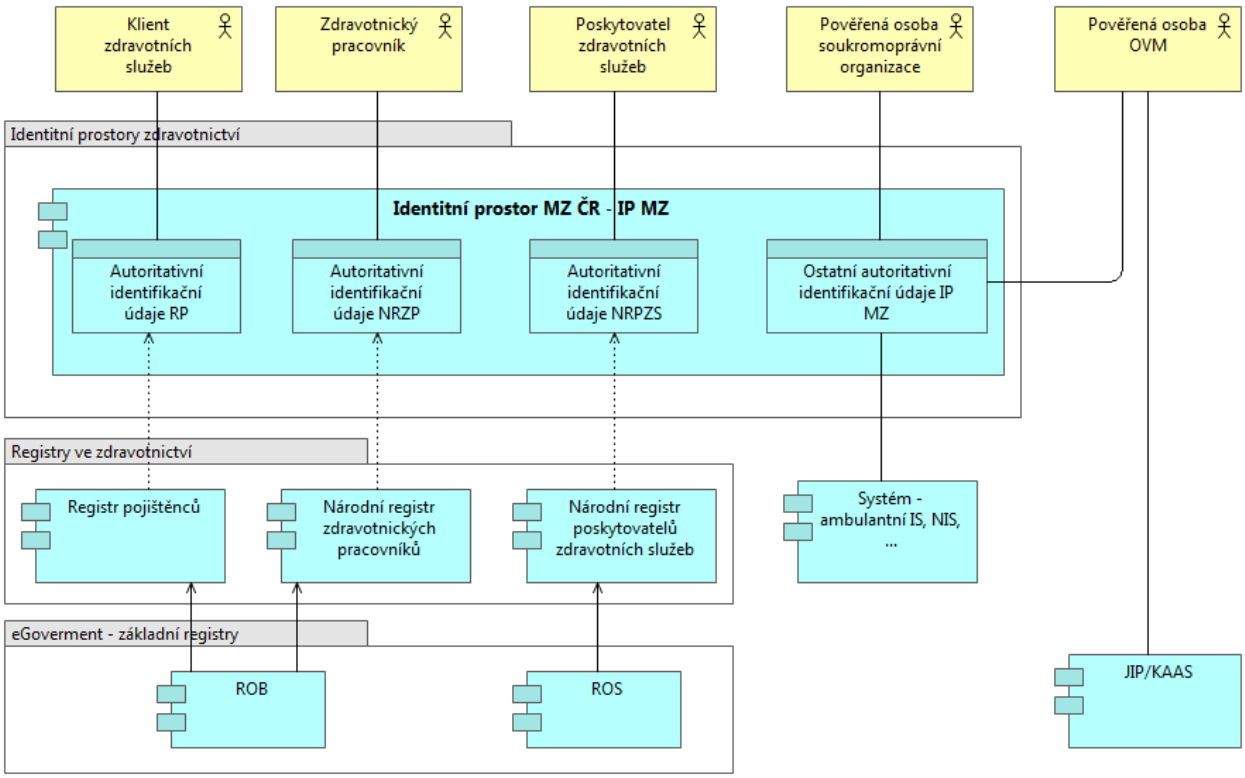
7.1.5.1 Ověřování elektronických podpisů



Obrázek 14 – Varianta B ověřování kvalifikovaných elektronických podpisů

Šedě podbarvené jsou knihovny, které budou nasazeny v systémech VPZS, a kterých úkolem bude zpracovávat ověřované dokumenty a volat službu pro ověření. Služba pro ověřování elektronických podpisů bude vystavená v Internetu. Bíle podbarvené komponenty představují systémy VPZS, které budou tuto službu využívat.

7.1.5.2 Identitní prostory



Obrázek 15 – Varianta B správy subjektů a v identitních prostorech

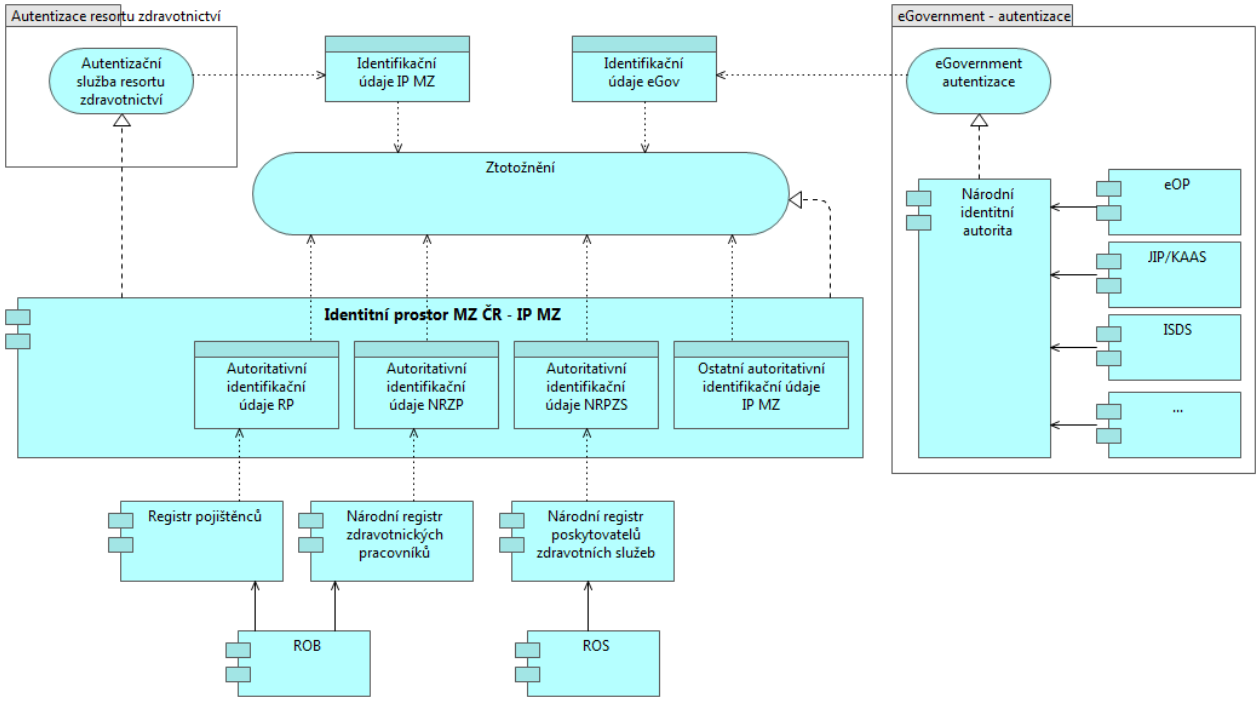
Základním prvkem architektury se vztahem na identifikaci a autentizaci jsou identitní prostory. Diagram zobrazuje vazbu mezi subjekty a identitními prostory.

Subjekty, pro které bude třeba ve zdravotnictví řešit identifikaci autentizaci, jsou:

- Klient zdravotních služeb
- Zdravotnický pracovník
- Poskytovatel zdravotních služeb
- Pověřená osoba soukromoprávní organizace
- Pověřená osoba OVM
- Systém – např. NIS, ambulatní IS atd.

Autoritativní identifikační údaje pro všechny tyto subjekty zastřešuje aplikační komponenta Identitní prostor MZ ČR (IP MZ). Zdrojovými systémy pro autoritativní identifikační údaje pro některé subjekty jsou registry ve zdravotnictví – Registr pojištěnců, Národní registr zdravotnických profesionálů a Národní registr poskytovatelů zdravotních služeb. Zdrojem referenčních údajů pro tyto registry jsou ROS a ROB. Tím je zajištěno, že identita všech hlavních subjektů ve zdravotnictví je ztotožněna se základními registry.

7.1.5.3 Vazby autentizačních služeb



Obrázek 16 – Varianta B autentizačních služeb

Diagram zachycuje dvě autentizační služby, které budou sloužit k přihlašování ke službám elektronického zdravotnictví. První je eGovernment autentizace, kterou bude realizovat Národní identitní autoria (NIA). NIA bude slouži pro autentizaci různými autentizačními prostředky – eOP, ISDS, JIP/KAAS, zahraničním prostředkem dle nařízení eIDAS a dalšími.

Pro všechny subjekty včetně klientů zdravotních služeb, které nebudou využívat autentizační služby NIA, realizuje Identitní prostor MZ ČR alternativu ve formě autentizační služby resortu zdravotnictví. IP MZ také realizuje službu Ztotožnění, která zajistí propojení identifikačních dat získaných od autentizačních služeb s autoritativními identifikačními údaji.

7.2 Vztah varianty k požadavkům na řešení

7.2.1 Ověřování elektronických podpisů a pečetí

Varianta A i B odráží reálné možnosti ověřování elektronických podpisů v systémech VPZS. Pokud by nařízení eIDAS nezavedlo nový typ služby ověřování elektronických podpisů „na dálku“ u kvalifikovaného poskytovatele, pak by tato varianta nebyla možná.

7.2.2 Vytváření kvalifikovaných elektronických podpisů a pečetí

Varianta A i B odráží reálné možnosti vytváření kvalifikovaných elektronických podpisů v systémech VPZS. Pokud by nařízení eIDAS nezavedlo nový typ služby vytváření elektronických podpisů „na dálku“ u kvalifikovaného poskytovatele, pak by tato varianta nebyla možná.

7.2.3 Uznávání prostředků pro elektronickou identifikaci

Varianty A a B odrážejí protikladné strategie pro identifikaci a autentizaci klientů zdravotních služeb. Zatímco varianta A odpovídá strategii „eGov first“, která podporuje sdílené využívání prostředků pro občanský život, varianta B odpovídá strategii řízení oddělených identit, která podporuje oddělení prostředky pro zdravotní služby od jiných typů právních vztahů.

7.3 Kvalifikovaný odhad nákladů pro dosažení navržené varianty cílového stavu včetně hodnocení udržitelnosti projektu

Zpracování kvalifikovaného odhadu nákladů se předpokládá až po diskusi otázek spojených s realizovatelností jednotlivých variant na úrovni pracovních skupin MZ ČR.

7.4 Vyjádření přínosů pro účastníky – cílové skupiny, zejména pro občany, pacienty, poskytovatele zdravotních služeb, plátce a regulátory

Zásadním přínosem je vytvoření společných infrastrukturních bezpečnostních služeb pro aplikační služby elektronického zdravotnictví. Využívání jednotných technologií pro realizaci základních funkcí, jakými identifikace, autentizace, autorizace a elektronické podepisování bezpochyby jsou, významně stimuluje vznik centrálně řízené infrastruktury elektronického zdravotnictví.

Využití prostředků a kvalifikovaných služeb, které přináší nařízení eIDAS, zjednodušuje všem uživatelům budovaných systémů elektronického zdravotnictví možnosti jejich využívání. Příznivý dopad v nárůstu uživatelů bezpochyby pozitivně ovlivní prestiž systémů elektronického zdravotnictví, což bude pozitivně působit na jeho používání laickou i odbornou veřejností.

7.5 Analýza rizik navržené varianty

Požadavky eIDAS přinášejí podstatná rozšíření možností komunikace občanů a firem s orgány státní správy a veřejné moci (dle eIDAS subjekty veřejné moci). Především zcela nové právní instituty v oblasti elektronické identifikace fyzických a právnických rozšíří způsoby přihlašování k on-line službám poskytovaných subjekty veřejného sektoru. S těmito rozšířeními eIDAS jsou spojena bezpečnostní rizika, která bude nezbytné průběžně identifikovat, vyhodnocovat a ošetřovat je dostatečně účinnými opatřeními.

Byly identifikovány následující skupiny rizik:

- Zvolení nedostatečné úrovně záruky prostředků pro elektronickou identifikaci ze strany spoléhající se strany (VPZS)
- Zneužití prostředků pro elektronickou identifikaci neoprávněnou osobou (krádeže identity)
- Neočekávané technické a právní dopady využívání více eIDAS identifikátorů jednou osobou
- Nesprávné ztotožnění eIDAS identifikátoru osoby s identifikátorem v systému VPZS
- Rizika spojená s odpovědností za škodu a jejím vymáhání při škodě způsobené projevem předchozích rizik, tj. při využívání autentizačních služeb dle eIDAS

- Neočekáváné technické a právní dopady spojené s používáním pseudonymů, které eIDAS umožňuje využívat v souladu s vnitrostátním právem (§ 79 občanského zákoníku)
- Nedodržení postupu pro ověření platnosti kvalifikovaných elektronických podpisů/pečetí
- Nemožnost určení okamžiku vzniku kvalifikovaného elektronického podpisu/pečeti
- Nemožnost ověření platnosti kvalifikovaného certifikátu k okamžiku vzniku podpisu
- Návrhem adaptace zachované používání zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu ve vnitrostátním právu a současném zrušení vyhlášky č. 212/2012 Sb. o ověřování platnosti zaručeného elektronického podpisu
- Rizika spojená s odpovědností za škodu a jejím vymáhání při škodě způsobené upřením právních účinků elektronického dokumentu, elektronického podpisu, elektronické pečeti, časového razítka nebo dat odeslaných a přijatých prostřednictvím služby elektronického doporučeného doručování.
- Zneužití prostředků pro elektronickou identifikaci neoprávněnou osobou (krádeže identity) při využívání služeb vytváření a ověřování kvalifikovaných elektronických podpisů/značek na dálku u kvalifikovaných poskytovatelů.
- Neoprávněné nakládání s osobními údaji a citlivými údaji při využívání služeb vytváření a ověřování kvalifikovaných elektronických podpisů/značek na dálku u kvalifikovaných poskytovatelů.
- Rizika spojená s odpovědností za škodu a jejím vymáhání při škodě způsobené zneužitím služeb kvalifikovaných poskytovatelů vytvářejících důvěru neoprávněnou osobou.

7.6 Rámcový harmonogram řešení podle navržené varianty

Rámcový harmonogram řešení s hlavními milníky uvádí následující tabulka.

Tabulka 10 Rámcový harmonogram řešení dopadů nařízení eIDAS

Rok	Milník dle nařízení/ Dílčí realizační milník	Oblast	Úkoly
2016	**1. 7. 2016**	Ověřování elektronických podpisů a pečetí	Příprava na ověřování kvalifikovaných elektronických podpisů a pečetí: • vytvoření modulu pro ověřování • integrace APV s modulem pro ověřování
2016	31. 12. 2016	Uznávání prostředků pro elektronickou identifikaci	Vytvoření prototypu systému k uznávání prostředků pro elektronickou identifikaci: • prototyp registrace, ztotožnění, autentizace • integrace na prototyp NIA/eOP

2017	30. 6. 2017	Vytváření kvalifikovaných elektronických podpisů a pečetí	Příprava pilotu na vytváření kvalifikovaných elektronických podpisů a pečetí: • výběr kvalifikovaných prostředků (certifikovaných dle CWA 14169) • vytvoření modulu pro vytváření • integrace pilotního APV s modulem pro vytváření
2017	31. 12. 2017	Vytváření kvalifikovaných elektronických podpisů a pečetí	Dokončení přechodu na vytváření kvalifikovaných elektronických podpisů a pečetí • integrace všech dotčených APV s modulem pro vytváření
2017	31. 12. 2017	Uznávání elektronické identifikace	Pilotní provoz systému k uznávání prostředků pro elektronickou identifikaci: • zahájení produkce (registrace a uznávání eID, ztotožnění eID, autentizace, oprávnění a souhlasy) • integrace systému NIA
2018	**1. 7. 2018**	Vytváření kvalifikovaných elektronických podpisů a pečetí	Vytváření pouze kvalifikovaných elektronických podpisů a pečetí: • přesné datum bude určeno 2 roky od nabytí účinnosti vnitrostátního zákona o službách vytvářejících důvěru
2017	**18. 9. 2018**	Uznávání elektronické identifikace	Povinné přeshraniční uznávání prostředků pro elektronickou identifikaci: • týká se systémů zveřejněných ve věstníku před 12 a více měsíci • u později zveřejněných eID systémů je 12 měsíců na realizaci

8 Porovnání výhod a nevýhod navržených variant a doporučení vhodné varianty řešení

8.1.1 Ověřování elektronických podpisů a pečetí

8.1.1.1 Varianta A

Varianta navrhuje řešit ověřování elektronických podpisů nadále stejným způsobem jako dosud, tj. prostředky systémů, ve kterých k ověřování elektronických podpisů dochází.

Výhody varianty:

- minimální náklady na úpravy systému, pokud VPZS smluvně zavázal dodavatele systému k provádění úpravám v souladu s požadavky platných právních předpisů;
- nevyžaduje úpravy v provozním technologickém prostředí systému.

Nevýhody varianty:

- VPZS nese právní rizika spojená s nedodržením požadavků čl. 32 nařízení eIDAS na postup ověřování kvalifikovaných elektronických podpisů;
- je nutno s prováděním úprav systému i v budoucnu z důvodu změn právních předpisů a technických norem.

8.1.1.2 Varianta B

Varianta navrhuje řešit ověřování elektronických podpisů s využitím kvalifikované služby poskytované kvalifikovaným poskytovatelem služeb vytvářejících důvěru.

Výhody varianty:

- právní rizika spojená s nedodržením požadavků čl. 32 nařízení eIDAS a případné sankce jdou k tíži kvalifikovaného poskytovatele služeb vytvářejících důvěru;
- VPZS získá jednotný způsob ověřování elektronických podpisů ve více systémech.

Nevýhody varianty:

- do systému se integruje komponenta (knihovna), kterou vyvíjí třetí a strana a mohou vzniknout technické komplikace jako např. nekompatibilita verzí knihoven;
- vyšší provozní náklady při velkých objemech ověřovaných elektronických podpisů.

8.1.1.3 Doporučení vhodné varianty

Doporučujeme provést výběr vhodné varianty samostatně každým VPZS podle jeho specifických technických a právních podmínek.

8.1.2 Vytváření kvalifikovaných elektronických podpisů a pečetí

8.1.2.1 Varianta A

Varianta navrhuje řešit vytváření kvalifikovaných elektronických podpisů s využitím kvalifikovaného prostředku pro vytváření elektronických podpisů.

Výhody varianty:

- způsob vytváření elektronických podpisů zachovává dosavadní paradigma odpovědnosti podepisující osoby za ochranu dat pro vytváření elektronického podpisu (tzv. soukromého klíče);
- nevyžaduje připojení k internetu nebo jinou interakci s okolím.

Nevýhody varianty:

- technické obtíže při vytváření na chytrých zařízeních, jako tablety a mobilní telefony, ke kterým nelze snadno připojit kvalifikovaný prostředek pro vytváření elektronického podpisu (HW zařízení zpravidla s USB rozhraním).

8.1.2.2 Varianta B

Varianta navrhuje řešit vytváření elektronických podpisů s využitím kvalifikované služby poskytované kvalifikovaným poskytovatelem služeb vytvářejících důvěru.

Výhody varianty:

- podepisující osoba přenáší riziko ochrany dat pro vytváření kvalifikovaného elektronického podpisu na třetí stranu – kvalifikovaného poskytovatele;
- nevyžaduje úpravy zařízení (počítače), se kterým pracuje podepisující osoba;
- nezávislosti podepisující osoby na konkrétním uživatelském zařízení (počítači).

Nevýhody varianty:

- zvýšené nároky na ochranu důvěrnosti údajů, protože kvalifikovaný poskytovatel musí mít k dispozici elektronický dokument, jehož elektronický podpis je vytvářen;
- vyšší provozní náklady při velkých objemech vytvářených elektronických podpisů.

8.1.2.3 Doporučení vhodné varianty

Doporučujeme realizovat variantu A z důvodu, že varianta B je v současnosti právně upravená možnost, ale fakticky ji zatím žádný kvalifikovaný poskytovatel služeb vytvářejících důvěru neposkytuje ani nenabízí.

8.1.3 Uznávání prostředků pro elektronickou identifikaci

8.1.3.1 Varianta A

Varianta navrhuje řešit identifikaci a autentizaci klientů zdravotních služeb výhradně prostředky, které bude podporovat Národní identitní autorita (NIA).

Výhody varianty:

- resort nemusí investovat do technologických řešení a organizování provozu;
- resort přenáší rizika spojená s krádežemi identit uživatelů na třetí stranu – MV ČR;
- resort podporuje zájem rozvoje služeb eGovernmentu.

Nevýhody varianty:

- nástroje určené k právním úkonům v občanském životě (např. elektronický OP) budou používány pro principálně odlišný způsob užití – pro přístup k citlivým údajům o zdravotním stavu a prováděných zdravotnických úkonech;

- vysoké nároky na technickou způsobilost a funkční gramotnost, které jsou nezbytné pro správné použití nástrojů (např. elektronického OP) a minimalizaci rizika zneužití.

8.1.3.2 Varianta B

Varianta navrhuje řešit identifikaci a autentizaci klientů zdravotních služeb systémy a prostředky vybudovanými výhradně pro účely spojené se zdravotními službami.

Výhody varianty:

- oddělení prostředků pro identifikaci a autentizace klientů zdravotních služeb od jiných existujících prostředků z důvodů:
    - důrazu na zájem ochrany soukromí,
    - minimalizace rizik spojených s kompromitací prostředku (kompromitace víceúčelového/centralizovaného prostředku násobně zvyšuje možné dopady).

Nevýhody varianty:

- vybudování technologicky a organizačně komplexního systému;
- není zcela zřejmé, v čí správě by takový systém měl být, zda MZ ČR, nebo VZP.

8.1.3.3 Doporučení vhodné varianty

Doporučujeme realizovat variantu A. Považujeme ovšem za nezbytné dodat, že nikoliv proto, že by byla jednoznačně lepší, ale z pragmatického důvodu, že systém NIA budovaný MV ČR bude k dispozici mnohem dříve než případné vlastní resortní řešení.

Vzor citace dle ČSN ISO 690:2011

MINISTERSTVO ZDRAVOTNICTVÍ ČESKÉ REPUBLIKY. *Příloha 2. Analýza a návrh řešení dopadů nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce*. Verze 1.00. Praha, 2016. Licencováno pod CC BY 4.0, licenční podmínky dostupné z: http://creativecommons.org/licenses/by/4.0/.