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

MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Národní strategie elektronického zdravotnictví

Enterprise Architektura resortu Ministerstva zdravotnictví ČR

Architektonická vize

Cílová architektura tématu T04 – Řešení autentizace a autorizace zdravotnických pracovníků a pacientů v resortu zdravotnictví, zřizování přístupů, řízení souhlasů a přístupu k informacím, identifikace pacienta

Dokument	Cílová architektura tématu T04 – Řešení autentizace a autorizace zdravotnických pracovníků a pacientů v resortu zdravotnictví, zřizování přístupů, řízení souhlasů a přístupu k informacím, identifikace pacienta
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

Seznam zkratek a pojmů

Tabulka 1 Seznam zkratek a pojmů

Pojem, zkratka	Definice, vysvětlení
AS-IS (stav)	Popis současného stavu
AS PVS	Autentizační služba portálu veřejné správy
Autentizace	Elektronický postup, který umožňuje potvrdit elektronickou identifikaci fyzické či právnické osoby nebo původ a integritu dat v elektronické podobě (čl. 3 odst. 5 nařízení eIDAS)

Pojem, zkratka	Definice, vysvětlení
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)
CALLIOPE	Projekt CALLIOPE je společným konceptem Evropské unie pro budování interoperabilních národních systémů elektronického zdravotnictví
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)
ČR	Česká republika
EA	Enterprise Architecture (česky: Podniková architektura)
EHR	Elektronický zdravotní záznam
eID	Technologie elektronické totožnosti
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)
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)
eOP	Elektronický občanský průkaz
eREG	Registry resortu zdravotnictví
EU	Evropská unie
FN	Fakultní nemocnice
GAP analýza	Rozdílová analýza
GSM	Globální Systém pro Mobilní komunikaci
HW	Hardware
ICT, ITC	Informační a komunikační technologie

Pojem, zkratka	Definice, vysvětlení
IČP	Identifikační číslo pracoviště
IČZ	Identifikační číslo zařízení
IDRR	Informační a datové rozhraní resortu
IP MZ	Identitiní prostor MZ ČR
IS	Informační systém
ISDS	Informační systém datových schránk
JIP/KAAS	Jednotný identitní prostor / Katalog autentizačních a autorizačních služeb
MZ	Ministerstvo zdravotnictví
NAP VS ČR	Národní akční plán veřejné správy ČR
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
NIA	Národní identitní autorita ČR (projekt MV ČR a SZR)
NIS	Nemocniční IS
NRZP	Národní registr zdravotnických pracovníků
NRPZS	Národní registr poskytovatelů zdravotních služeb
NZIS	Národní zdravotnický informační systém
Osobní identifikační údaje	Soubor údajů umožňujících určit totožnost fyzické či právnické osoby nebo fyzické osoby zastupující právnickou osobu (čl. 3 odst. 3 nařízení eIDAS)
OTP	One-Time Password, jednorázové heslo
OVM	Orgán veřejné moci
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
PHR	Osobní zdravotní záznam
PKI	Public Key Infrastructure, infrastruktura veřejných klíčů
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)
ROB	Registr obyvatel

Pojem, zkratka	Definice, vysvětlení
ROS	Registr osob
SIDP	Soukromoprávní poskytoval prostředku pro identifikaci
SIM	Subscriber Identity Module
Služba vytvářející důvěru	Elektronická služba, která je zpravidla poskytována za úplatu a spočívá: 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. (čl. 3 odst. 16 nařízení eIDAS.)
SÚKL	Státní ústav pro kontrolu léčiv
SW	Software
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 prostředků pro elektronickou identifikaci jsou stanoveny v prováděcím nařízení komise EU 2015/1502.
VPN	Virtual Private Network, virtuální privátní síť
VS	Veřejná správa
VZP	Všeobecná zdravotní pojišťovna
Zaručený elektronický podpis	Elektronický podpis, který splňuje požadavky stanovené v článku 26 nařízení eIDAS (čl. 3 odst. 11 nařízení eIDAS).
ZD	Zdravotnická dokumentace

1 Úvod

Tento dokument je dílčí výstup v rámci realizace fáze architektonické vize projektu „Zpracování koncepce a vize Enterprise architektury elektronického zdravotnictví“ pro téma T04, jeho předmětem je řešení:

- řešení autentizace a autorizace zdravotnických pracovníků a pacientů v resortu zdravotnictví.
- identifikace a autentizace pacientů
- identifikace a autentizace zdravotnických profesionálů
- autorizace zdravotnických profesionálů ke službám elektronického zdravotnictví
- správa mandátů pro autorizaci při zastupování jinou osobou
- správa souhlasů pro autorizaci přístupu k informacím

Cílem dokumentu je navrhnout cílovou architekturu průřezových služeb pro identifikaci, autentizaci a autorizaci subjektů, jež budou využívat elektronické služby v resortu zdravotnictví.

Dokument je strukturován do následujících kapitol:

1. Úvod – stanovuje cíl dokumentu
2. Východiska – přehled strategických, právních a dalších požadavků
3. Metodický rámec – popis metodiky modelování enterprise architektury
4. Analýza současného stavu – popis existujících systémů identifikace a autentizace
5. Návrh cílové architektury – stanovení architektonických principů a modelů
6. GAP analýza – popis kroků k dosažení cílového stavu
7. Otevřené body – registr otevřených otázek a problémů

2 Východiska

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 (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 pro Evropu 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 Právní rámec

2.2.1 Právní předpisy vymezující elektronickou identifikaci

Právním předpisem nejvyšší úrovně, který vymezuje oblast elektronické identifikace a autentizace, je 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“). Nařízení eIDAS je doplněno dalšími prováděcími akty, pro oblast elektronické identifikace a autentizace jsou to především prováděcí nařízení Komise (EU) č. 2015/1501 a 2015/1502.

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.

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

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, tj. problematiku služeb vytvářejících důvěru (týká se oblasti využívání elektronických podpisů).

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.

2.2.2 Právní předpisy resortu zdravotnictví

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. 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

[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.

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.

2.3 Přehled požadavků z katalogu požadavků

Zdrojem požadavků pro cílový stav architektury tématu T04 Řešení autentizace a autorizace zdravotnických pracovníků a pacientů v resortu zdravotnictví, zřizování přístupů, řízení souhlasů a přístupu k informacím, identifikace pacienta jsou požadavky uvedené v dokumentu MZd EA Katalog požadavků, který je výstupem předběžné fáze projektu Zpracování koncepce a vize Enterprise architektury elektronického zdravotnictví.

Dokument MZd EA Katalog požadavků obsahuje identifikované požadavky ze strategií a dalších závazných dokumentů. Těmi jsou především právní akty spojené s nařízením eIDAS.

Tabulka 2 Seznam požadavků vztahujících se k předmětu zadání z Katalogu požadavků

ID	Název požadavku	Detailní popis požadavku	Zdroj požadavku	Podrobné určení zdroje
219	Zajistit autentizaci uživatelů systému	Zajištění jednoduché, cenově přijatelné, ale spolehlivé a robustní metody autentizace uživatelů systému.	Národní strategie elektronického zdravotnictví (2015, soustava cílů a opatření)	Strategický cíl 4, specifický cíl 4.1 Rozvoj infrastruktury pro sdílení a poskytování zdravotních služeb
231	Zabezpečit jednoznačnou a spolehlivou identifikaci všech subjektů	Je nutné zabezpečit jednoznačnou a spolehlivou identifikaci všech subjektů a bezpečné a transparentní řízení přístupu k datům a službám elektronického zdravotnictví, tzv. autentizaci a autorizaci a realizovat s nimi spojený systémy správy identit a oprávnění.	Národní strategie elektronického zdravotnictví (2015, soustava cílů a opatření)	Strategický cíl 4, specifický cíl 4.1, opatření 4.1.5 Autorizace, autentizace a řízení oprávnění poskytovatelů
232	Navázat systém identifikace na „základní registry“ elektronického zdravotnictví	Systém identifikace bude navázán na „základní registry“ elektronického zdravotnictví, zejména na Národní registr poskytovatelů zdravotních služeb (NRPZS), Národní registr zdravotnických pracovníků a Centrální registr pojištěnců. V těchto registrech budou uloženy garantované informace o každém poskytovateli zdravotních služeb a o dalších subjektech elektronického zdravotnictví. Identita subjektů bude zároveň ověřována proti základním registrům veřejné správy.	Národní strategie elektronického zdravotnictví (2015, soustava cílů a opatření)	Strategický cíl 4, specifický cíl 4.1, opatření 4.1.5 Autorizace, autentizace a řízení oprávnění poskytovatelů
233	Určit rozsah oprávnění fyzických osob ke konkrétním aplikacím, jejich funkcím a informacím v nich obsažených pomocí autorizace	Autorizace určí rozsah oprávnění fyzických osob ke konkrétním aplikacím, jejich funkcím a informacím v nich obsažených, v souladu s bezpečností politikou systému elektronického zdravotnictví a v souladu se svobodnou volbou pacienta.	Národní strategie elektronického zdravotnictví (2015, soustava cílů a opatření)	Strategický cíl 4, specifický cíl 4.1, opatření 4.1.5 Autorizace, autentizace a řízení oprávnění poskytovatelů

ID	Název požadavku	Detailní popis požadavku	Zdroj požadavku	Podrobné určení zdroje
244	Zajistit jednoznačnou a důvěryhodnou identifikaci pacientů	Jednoznačná a důvěryhodná identifikace pacientů - předpokládá se, že řešení identifikace osob pro potřeby eGovernmentu bude použitelné i v oblasti zdravotnictví. Bude zapotřebí analyzovat řešení identifikace občanů z pohledu všech možných skupin občanů (děti, občané EU, cizinci) a všech možných scénářů primární i sekundární identifikace (pacienti bez možnosti identifikace, přeshraniční péče). To může vést k tomu, že pro potřeby zdravotnictví bude nutné doplnit identifikaci pro eGovernment o řadu dalších scénářů a odpovídajících technických řešení.	Národní strategie elektronického zdravotnictví (2015, soustava cílů a opatření)	Strategický cíl 4, specifický cíl 4.1, opatření 4.1.7 Snadná a přesná identifikace pacienta a získávání pacientských údajů
295	Zajištění interoperability na základě norem a otevřených vývojových platforem	Technologie elektronické totožnosti (eID) a autentizační služby jsou pro transakce na internetu v soukromém i veřejném sektoru zásadní. V dnešní době je nejběžnějším způsobem autentizace používání hesel. U mnohých aplikací může být tato praxe postačující, ale stále více jsou zapotřebí bezpečnější řešení. Jelikož se bude nabízet řada řešení, mělo by odvětví za podpory politických opatření – zejména služeb elektronické veřejné správy – zajistit interoperabilitu na základě norem a otevřených vývojových platforem.	Digitální agenda pro Evropu	
302	Technologie elektronické totožnosti (eID)	Technologie elektronické totožnosti (eID)	Digitální agenda pro Evropu	
339	Vytváření digitální důvěry	Vytváření digitální důvěry Uživatelé musí být schopni nalézt jednoduchá, kodifikovaná vysvětlení svých práv a povinností, stanovených transparentním a pochopitelným způsobem, např. prostřednictvím on-line platforem, které vychází z prototypu příručky eYou Guide.	Digitální agenda pro Evropu	
371	Zasazení systému elektronického zdravotnictví do kontextu vzájemného uznávání eID a dalších důvěryhodných služeb v		Národní koncepce elektronického zdravotnictví 2013	

ID	Název požadavku	Detailní popis požadavku	Zdroj požadavku	Podrobné určení zdroje
	návaznosti na Digitální agendu EU			
548	Od izolovaných identitních systémů k jednotným identitním systémům uživatelů služeb veřejné správy a úředníků veřejné správy		Strategie rozvoje ICT služeb veřejné správy a její opatření na zefektivnění ITC služeb	kap. 3. Strategické cíle a navrhovaná opatření pro jejich dosažení - C7)
654	Řešit správu identifikátorů eIDAS, protože každá osoba může mít více prostředků pro elektronickou identifikaci a tedy i více 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.	Nařízení eIDAS	
655	Rozšířit resortní IS o evidenci a správu prostředků pro elektronickou identifikaci dle eIDAS a s nimi spojených identifikačních údajů.	Z důvodu nutnosti přeshraničního uznávání prostředků pro elektronickou identifikaci pro účely autentizace bude nutné rozšířit IS rezortu 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.	Nařízení eIDAS	
656	Nutnost rozšíření stávajících systémů takovým způsobem, aby uživatelé autentizovaní prostřednictvím autentizačních služeb systému elektronické identifikace měli přístup ke stejným službám IS jako uživatelé autentizovaní prostřednictvím jiných služeb.	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.	Nařízení eIDAS	
657	Ztotožnění eID vůči vlastnímu systému identifikace osob	Kvůli novým možnostem přihlašování bude třeba upravit a rozšířit způsob, jak ztotožnit elektronickou identitu s osobou ve vlastním systému identifikace osob.	Nařízení eIDAS	
658	Způsob zprostředkování identit		Nařízení eIDAS	

ID	Název požadavku	Detailní popis požadavku	Zdroj požadavku	Podrobné určení zdroje
	externím aplikacím musí umožňovat zprostředkování i těch identit, které jsou uznávané v rámci přeshraničního uznávání autentizačních služeb.			
659	Možnost učinit elektronické podání bez nutnosti využít datovou schránku či použití kvalifikovaného certifikátu musí být v souladu s nutností přeshraničního uznávání autentizačních služeb.		Nařízení eIDAS	
660	Podpora pověřených osob: Případná podpora pověření a oprávnění při využívání resortních on-line služeb musí být v souladu s nutností přeshraničního uznávání autentizačních služeb.		Nařízení eIDAS	
661	Autorizace úkonů při využívání on-line služeb resortních IS musí být v souladu s nutností přeshraničního uznávání autentizačních služeb.		Nařízení eIDAS	
670	Analyzovat požadavky na úrovně záruky prostředků elektronické identifikace dle prováděcího nařízení EU 2015/1502 a stanovit úroveň záruky, kterou bude resort MZd uznávat.		Nařízení eIDAS	
671	Vybudovat autentizační modul (moduly) resortních IS napojený na národní autentizační uzel.		Nařízení eIDAS	

ID	Název požadavku	Detailní popis požadavku	Zdroj požadavku	Podrobné určení zdroje
672	Rozšířit autentizační modul (moduly) resortních IS o nové systémy elektronické identifikace fyzických osob, a to do 12 měsíců po zveřejnění těchto systémů v seznamu oznámených systémů elektronické identifikace v rámci EU.	Uznávání systému elektronické identifikace je od 18. 9. 2016 dobrovolné, od 18. 9. 2018 povinné.	Nařízení eIDAS	
673	Rozšířit autentizační modul a registrační modul o autentizaci právnických osob dle eIDAS.		Nařízení eIDAS	
674	Vybudovat modul registru eIDAS identifikátorů v resortních IS, který zajistí registraci a ztotožnění eIDAS identifikátorů osoby s identifikátorem osoby ve vlastním systému identifikace osob.		Nařízení eIDAS	

2.4 Rámec bezpečnosti kyberprostoru

2.4.1 Obecné zákonitosti

Kybernetický prostor se výrazně liší od reálného prostoru. To se týká jak identity, tak hrozeb a rizik. Kybernetický prostor je založen na digitálním principu, pracuje pouze s diskrétní informací. Má globální charakter a síťovou topologii.

Z pohledu identity to znamená, že nelze rozpoznat originál od kopie. Nelze spolehlivě rozpoznat skutečnou vzdálenost (na Internetu jsou všichni „sousedi“). Nelze spoléhat na vynutitelnost práva (drtivá většina lidí v Internetu je mimo dosah právního systému ČR – v ČR je méně jak 1% uživatelů Internetu).

V reálném světě je nemožné vytvářet dokonalou kopii člověka, je možné použít více dalších informací ke zvýšení spolehlivosti identifikace, lze pracovat se vzdáleností a s vynutitelností práva.

V kybernetickém prostoru lze ověřit deklarovanou identitu jen pomocí autentizace a k tomu se používá tajná informace (tajemství). Taková informace by však neměla existovat nikde jinde na světě, aby autentizace mohla být prokazatelná. To je možné jen při použití asymetrické kryptografie, se kterou však člověk bez patřičného výpočetního vybavení nemůže pracovat.

Potřeby využití identity v reálném světě a v kybernetickém prostoru se také výrazně liší.

V kybernetickém světě počítače na základě autentizace rozhodují podle předem daných algoritmů a pravidel okamžitě o přístupu k daným aktivům (autorizace). Při tom nepracují s reálnou identitou, používají kybernetickou identitu a autorizační pravidla.

Reálnou identitu potřebují lidé, kteří autorizační pravidla pro počítače připravují. Proto (a ještě z dalších důvodů) je správné oddělit reálnou identitu od kybernetické identity (autentizace, autentizačního prostředku) a zacházet s každou z nich správným způsobem.

Celková kvalita systému elektronické identity (eID ekosystém) je hodnocena podle více kritérií a výsledná hodnota je dána nejhorším výsledkem jednotlivého kritéria (Authentication Assurance Level, Quality Authentication Assurance, Assurance Level).

Bezpečnost v kybernetickém prostoru je limitována bezpečností autentizace. Pokud cílový systém nerozliší správně uživatele od útočníka, nemůže správně aplikovat žádné další bezpečnostní opatření (autorizaci a řízení přístupu, šifrování, el. podpis,…).

Z toho vyplývá, že bezpečnost celého ICT systému nemůže být lepší, než nejslabší část autentizace.

2.4.2 Kritéria eID ekosystému

2.4.2.1 Síla autentizace

Pojmem síla autentizace se hodnotí způsob ověření kybernetické identity v kybernetickém prostoru. Hodnotí se odolnost autentizace proti různým druhům útoků. Jako příklad lze uvést odposlech komunikace, možnost opakovaného použití zjištěných informací, sociální útoky (např. phishing), MITM (man-in-the-middle), útok na jiný subjekt (při sdíleném tajemství).

V současné době je za kvalitní považována dynamická autentizace, zejména pokud používá asymetrickou kryptografii.

Upozornění

Nejvíce rozšířený způsob autentizace, tj. loginname/password má velmi malou až nepoužitelnou sílu autentizace.

Existuje řada technologií mylně vydávaných za autentizační technologie, (protože se v autentizačních systémech používají). Jedná se např. o PKI a tzv. federativní eID.

PKI vytváří pouze autentizační prostředky používající asymetrickou kryptografii (soukromý a veřejný klíč), které mohou být použity k různým účelům (autentizace, podpis, šifrování). Vlastní autentizace není součástí PKI.

Standardy federativní eID nezahrnují provedení autentizace. Jejich předmětem je přenos výsledku autentizace mezi subjekty.

2.4.2.2 Uživatelská jednoduchost

Uživatelská jednoduchost je kritickým faktorem celého eID ekosystému. Už mnohokrát se ověřilo, že uživatelsky komplikovaná autentizace buď nefunguje, nebo chování uživatelů výrazně degraduje celkovou bezpečnost. Buď se uživatelé vyhýbají používání složitého systému (jako v případě plošného nasazení čipových karet v řadě států – využití 3-7%), nebo si uživatelé pomáhají rizikovým chováním (např. opakované používání stejného hesla, poznamenávání hesel na papírku nalepeném na monitoru).

V topologicky komplikovaném prostředí, jako je prostředí zdravotnictví, uživatelé vnímají celkovou složitost. To vede k požadavku „user centric“ řešení, kde s počtem partnerů neroste složitost pro uživatele (analogie se „single-sign-on“).

Upozornění

Opakované použití „provider centric“ řešení (jako jsou např. klasické OTP generátory, specializované certifikáty vydávané poskytovatelem) by vedly v prostředí zdravotnictví k neakceptovatelné uživatelské zkušenosti.

2.4.2.3 Náklady

Do celkových nákladů eID ekosystému spadají nejen náklady na pořízení a provoz potřebného HW a SW, ale také náklady na obslužné systémy potřebné k zajištění kompletního životního cyklu eID. Tam patří typicky náklady na obnovu kryptomateriálu (např. opakované vydávání certifikátu po vypršení platnosti), řešení mimořádných situací (krádež, kompromitace, zapomenutí), a to včetně zotavení z takové situace a druhotných nákladů vyvolaných nedostupností služeb. Tyto náklady často výrazně převyšují náklady na HW a SW.

2.4.2.4 Ochrana soukromí

Moderní koncepty eID ekosystému zahrnují ochranu soukromí jako kritérium kvality. Nejedná se „jen“ o ochranu soukromí (základní lidské právo) zahrnující vyloučení nechtěného zveřejňování ověřených osobních údajů, které je součástí autentizace (jako v případě PKI certifikátů), ale také o významný bezpečnostní prvek potřebný v případě zotavení eID z mimořádné situace.

Upozornění

Nelze chránit žádné údaje, dokud není provedena autentizace (a autorizace). Tedy nelze ochránit osobní údaje, které jsou součástí autentizace (pokud data samotná nemají vestavěný systém řízení přístupu – včetně autentizace). To platí i pro stabilní či dlouhodobě používané identifikátory, (které může útočník velmi pravděpodobně propojit s osobními údaji z jiných zdrojů).

2.4.2.5 Dostupnost služby

Dostupnost služby je standardní část ICT bezpečnosti (+ důvěrnost, integrita a případně neodmítnutelnost). Funkčnost služby v kybernetickém prostoru je podmíněna funkčností autentizace. Tedy dostupnost cílové služby nemůže být lepší než dostupnost autentizace.

Z tohoto pohledu je překvapivé, že řešení dostupnosti autentizace nebývá standardní součástí eID ekosystému, nebo řešení dostupnosti přináší významná bezpečnostní rizika. Např. součástí PKI je pouze podpora zneplatnění certifikátu (CRL + organizační opatření v certifikační politice), obnova zapomenutých hesel je známou a útočníky oblíbenou slabinou, nové vydání a doručení rozbitého či ztraceného OTP generátoru nebo čipové karty není rychlá, jednoduchá ani levná záležitost.

Upozornění

Chybějící podpora dostupnosti autentizace samotnou autentizační technologií vyžaduje dodatečná organizační opatření v této oblasti bezpečnosti cílových systémů, která mohou výrazně ovlivnit celkové paramenty dostupnosti služby a také celkové náklady.

2.4.2.6 Dlouhodobá udržitelnost

Ze střednědobého a dlouhodobého hlediska je jisté, že stávající kryptografické metody a algoritmy nebude bezpečné v budoucnosti používat (stejně jako není bezpečné dnes používat metody a algoritmy, které byly bezpečné v minulosti). Kromě rizik kompromitace je zde trvalý růst dostupného výpočetního výkonu.

Budoucí přechod eID ekosystému na nové kryptografické metody a algoritmy může být vynucen jak neočekávanou krizovou událostí (např. objevenou slabinou), tak může být vynucen modernizací.

Takový přechod může být logisticky mnohem náročnější než zavedení nového eID ekosystému „na zelené louce“. Bude vyžadována dostupnost cílových služeb s minimálními výpadky v průběhu celého přechodu a při zachování bezpečnosti. Vážným problémem může být synchronizace okamžiku přechodu mezi všemi subjekty, pokud původní eID ekosystém nebude s takovou možností počítat. Velmi pravděpodobně nebude akceptovatelné v takovém případě opakovat postupy ověření identity, zejména v případě nutnosti osobního kontaktu.

V případě neočekávané krizové události bude podstatný i čas reakce a celková doba zotavení celého eID ekosystému.

Upozornění

Existují na první pohled neočekávané logistické limity zejména v případě neočekávané krizové situace. Např. kapacita pracovišť vydávajících autentizační prostředky osobně

v případě, že zotavení z takové krizové situace vyžaduje nové vydání a doručení autentizačního prostředku. Např. v případě nutnosti nově vydat všechny elektronické občanské průkazy by doba vydávání byla cca 1 rok, pokud by se kapacita příslušných úřadů zvýšila na desetinásobek běžné kapacity.

2.4.2.7 Ochrana cílových aktiv

Přístup k cílovým aktivům v kybernetickém prostoru je vždy pomocí prostředků elektronické komunikace, která by měla být chráněna (datový kanál). K ochraně cílových aktiv nestačí odlišit uživatele od útočníka kdekoli. Podstatné je, kdo používá datový kanál, kterým přistupuje k cílovým aktivům.

Existují dvě základní architektury autentizace z pohledu vazby na datový kanál. Vestavěná autentizace a externí autentizace.

Vestavěná autentizace přímo autentizuje příslušný datový kanál. Jedná se o autentizaci přímo vestavěnou do příslušného komunikačního protokolu. Tato architektura se výborně vypořádává s požadavkem ochrany datového kanálu. Přináší však problém uživatelské jednoduchosti ve složitějším prostředí – není „user centric“. Jde o nejstarší řešení autentizace.

Alternativou je externí autentizace, tedy univerzální autentizační služba mimo cílový datový kanál (např. Kerberos). Externí autentizace má šanci vyřešit uživatelskou jednoduchost, ale přináší problém provázání výsledků autentizace s ochranou datového kanálu.

Existují také architektury sdílených autentizačních prostředků využívaných vestavěnou autentizací. Příkladem může být PKI všeobecně uznávané autority nebo vícenásobný kryptomateriál. Sdílený autentizační prostředek však ochranu datového kanálu neřeší. To je úloha pro autentizaci.

Upozornění

Federativní systémy dle všeobecně známých standardů izolují autentizaci uživatele od ochrany datového kanálu k cílovým aktivům. Jedinou výjimkou je „holder-of-key“ profil SAML, který by měl vyřešit část tohoto problému. Proto nelze tyto technologie (kromě „holder-of-key“) používat pro nejvyšší úroveň záruky.

2.4.2.8 Podpora ověření identity (identity proofing)

Bezpečnost ověření skutečné identity v reálném světě a její provázání s autentizací (s kybernetickou identitou, s autentizačním prostředkem) je limitujícím faktorem správného stanovení přístupových práv. Správně stanovená přístupová práva jsou nutnou podmínkou správného řízení přístupu po rozpoznání uživatele (po autentizaci).

Proto je ověření identity (identity proofing, ověřování totožnosti) a bezpečné provázání kybernetické identity s reálnou identitou (vydávání, doručování a aktivace elektronických prostředků) součástí klasifikace eID ekosystému.

Technologické vlastnosti eID ekosystému mohou podporovat, nebo naopak komplikovat postupy provázání ověřené reálné identity s kybernetickou identitou (autentizačními prostředky). Mohou být ve svých důsledcích výrazným nákladem nebo značným bezpečnostním rizikem, nebo mohou přinést úspory a lepší uživatelský efekt.

Upozornění

Často používaný postup Ověření identity → výroba či spárování autentizačního prostředku → doručení uživateli → aktivace není jediným akceptovatelným postupem. Přináší řadu bezpečnostních a logistických úskalí a nákladů.

Protože propojení kybernetické identity (autentizačního prostředku) s ověřenou reálnou identitou je potřeba k řízení přístupových práv (ne k vlastní autentizaci), je možné s výhodou použít i jiné postupy, které mohou být efektivnější, uživatelsky vstřícnější a bezpečnější.

2.4.3 Současné trendy

Dominantním současným trendem ICT je rychlý růst obliby mobilních (chytrých) zařízení, které si uživatelé sami kupují a chtějí je všude používat. Tato zařízení přinášejí novou úroveň uživatelského komfortu a nové funkčnosti. Lze očekávat, že používání takových zařízení (chytré telefony, tablety, chytré hodinky,…) bude dominantní způsob používání ICT v blízké budoucnosti.

Tento trend přináší nové výzvy (problémy) pro eID a zároveň přináší nové možnosti pro řešení eID.

2.4.3.1 Nové výzvy

Z pohledu klasických technologií eID může být chytré mobilní zařízení výrazná komplikace nebo i bloker. Uveďme příklady:

- Standardní logistika eID (tj. ověření osobních údajů → personifikace prostředku eID → doručení správné osobě → aktivace) přestává fungovat. Uživatel si sám vybírá a kupuje své zařízení, které je výrazně dražší, než klasické prostředky eID. Další zařízení nechce používat.
- Klasické prostředky eID nespolupracují s chytrými mobilními zařízeními, nebo je spolupráce uživatelsky příliš komplikovaná a přináší nová bezpečnostní rizika. Kontaktní čipovou kartu nelze přímo zastrčit ani do chytrého telefonu, ani do tabletu, ani do chytrých hodinek. Přídavná čtečka je uživatelsky příliš komplikovaná (třetí věc) a nebezpečná (problematická ochrana přístupu škodlivého kódu k funkcionalitě eID). Řada chytrých mobilních zařízení neumožňuje spolupráci s bezdrátovými čipovými kartami.
- Většina mobilních zařízení obsahuje SIM kartu, která má funkčnost bezpečného elementu. Tedy existuje teoretická možnost využít přímo tento HW. Tato možnost existuje již od vzniku GSM a o této možnosti odborná veřejnost diskutuje mnoho let. Zatím se nepodařilo ve větším měřítku vyřešit základní problém SIM, a tím je její vlastnictví (poskytovatelem telekomunikačních služeb). Existují úspěšná využití SIM pro eID ve skandinávských zemích, které využívají výjimečné situace, tj. existence certifikační autority široce uznávané v tomto regionu a dohod mezi telekomunikačními poskytovateli na tomto trhu.
- Rozmach chytrých zařízení přinesl změnu v této oblasti. Kromě komplikací s různými formáty SIM se otvírá diskuse o ukončení používání SIM. Je jen otázkou času, kdy používání SIM skončí. Z hlediska současných možností chytrých zařízení je používání SIM jen zbytečným nákladem jak pro výrobce zařízení, tak pro telekomunikační operátory.

2.4.3.2 Nové možnosti

Z pohledu klasických technologií eID přináší chytré mobilní zařízení také nové možnosti. Uveďme příklady:

- Padá bariéra chybějícího napájení, malého výpočetního výkonu, chybějící klávesnice a obrazovky v porovnání s klasickými čipovými kartami. Přibývají možnosti on-line výkonné komunikace. To umožňuje likvidovat bezpečnostní rizika a přinést lepší uživatelskou zkušenost.
- Standardní distribuční kanál mobilních aplikací je další významnou systémovou vlastností. Umožňuje výrazně rychleji fixovat chyby, inovovat řešení a téměř okamžitě je distribuovat obrovskému množství uživatelů. Něco takového klasické eID technologie založené na zabezpečených HW prostředcích neumožňují. Každý update je logisticky komplikovaná a velmi drahá záležitost.
- Otvírá se cesta nové logistiky eID. Prostředky eID mohou mít formu SW aplikace bez identity. Identita může vzniknout až po instalaci na konkrétním zařízení. To výrazně zlevňuje zajištění prostředků eID a zvyšuje uživatelské pohodlí a likviduje bezpečnostní rizika distribuce klasických personifikovaných eID prostředků.
- Přináší to i nové možnosti ověření identity. Už není nutné odrazovat uživatele komplikovanými procedurami před prvním použitím eID vyplývajícím z klasické logistiky. Uživatel může používat ihned své mobilní zařízení bez ověření jeho identity k takovým účelům, kde ověření není třeba. Ověření může proběhnout později či postupně.
- Výpočetní výkon a komunikační schopnosti chytrých mobilních zařízení umožňují nové přístupy k řešení bezpečnosti eID. Lze využívat výrazně náročnější kryptografii a lze využívat dynamickou ochranu.

2.4.3.3 Shrnutí

Současné trendy rostoucí obliby chytrých mobilních zařízení přinášejí do oblasti eID nové výzvy, které výrazně komplikují, až znemožňují, použití klasických prostředků eID s vyšší úrovní bezpečnosti. Zároveň tyto trendy otvírají nové možnosti, které mohou využívat jen nově vznikající technologie eID.

Je nezbytné zmínit, že musí existovat možnost zakázat chytré mobilní zařízení, pokud nebude splňovat minimální bezpečnostní požadavky. Např. při publikovaném prolomení ochrany konkrétního typu chytrého mobilního zařízení se bude moci pro ověřování identity uživatele používat až po instalaci opravy.

2.4.4 Doporučení

Pro hodnocení kvality eID ekosystému je rozumné použít multikriteriální klasifikaci podle moderních mezinárodně uznávaných principů založených na hodnocení nejslabšího článku.

Při výběru respektovat trend používání chytrých mobilních zařízení kupovaných uživateli a do výběru zahrnout nové technologie eID určené pro chytrá mobilní zařízení.

2.5 Další východiska

- Milieu Ltd – time.lex: 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. (Brusel, 2014)

3 Metodický rámec

3.1 Metodika EA

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.

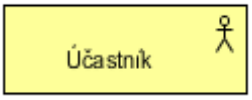
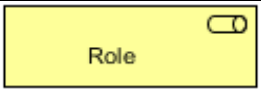
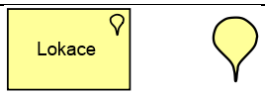
ArchiMate definuje tři základní domény (znázorněné různými barvami):

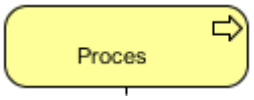
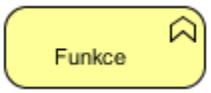
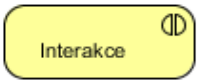
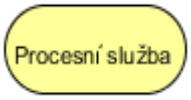
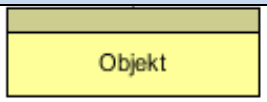
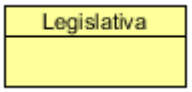
- **Byznys (procesní) doména** (znázorněná žlutou barvou) zachycuje účastníky, jejich role a užívané byznys služby, které jsou realizovány procesy. V pohledu na byznys (procesní) doménu jsou zachyceny stěžejní prvky cílové architektury na úrovni EA.
- **Aplikační doména** (znázorněná modrou barvou) podporuje 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.

3.1.1 Výčet vybraných elementů byznys (procesní) domény

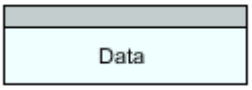
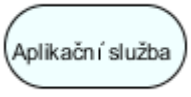
Tabulka 3 Seznam a popis vybraných elementů byznys domény

Pojem	Popis	Symbol
Elementy aktivní struktury		
Účastník, aktér/ Business Actor	Účastník je definován jako organizační jednotka schopná 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.	

Pojem	Popis	Symbol
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 vybrané 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.	

3.1.2 Výčet vybraných elementů aplikační domény

Tabulka 4 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.	

4 Popis současného stavu

4.1 Shrnutí současného stavu 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.

[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 Microsoft: Soutěž o návrh „Hospodárné a funkční elektronické zdravotnictví“ (2012) a 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).

Autentizace se zpravidla zaměřuje pouze na uživatele, kteří 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, výjimečné odlišnosti proto nemusí být v tabulce zachyceny.

Tabulka 5 Souhrn současného stavu způsobů 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					

4.2 Stav prostředku pro identifikaci a autentizaci v 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[3] jsou v 15 ze sledovaných zemí pro autentizaci zdravotnických pracovníků využívány systémy založené na

[3] Milieu Ltd – time.lex: 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. (Brusel, 2014)

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 z 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, Lucembursko) 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 umožněno uchovávat 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 zemí 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 země zavedly opatření, která zajišťují důvěrnost dat. Například ve Francii je každému uživateli národní zdravotní péče uděleno automaticky generované číslo, které je přístupné v zdravotnické kartě. Specifický identifikační kód pro eHealth není zaveden v žádné ze sledovaných zemí kromě Skotska, kde byla vytvořena databáze demografických a klinických údajů (Community Health Index), které slouží pro jednoznačnou identifikaci.

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

Tabulka 6 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).

4.3 Současný stav autentizace subjektů ve zdravotnictví ČR

4.3.1 Subjekty ve zdravotnictví

V resortu zdravotnictví byly identifikovány následující typy subjektů, 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
  - jiné zařízení (autentizace typicky certifikátem)
- Veřejnoprávní subjekty a jejich pověřené osoby
- Soukromoprávní subjekty a jejich pověřené osoby

4.3.2 Existující služby autentizace

Tabulka 7 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. osoba 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

4.4 Motivace pro vytvoření pohledů na současný stav

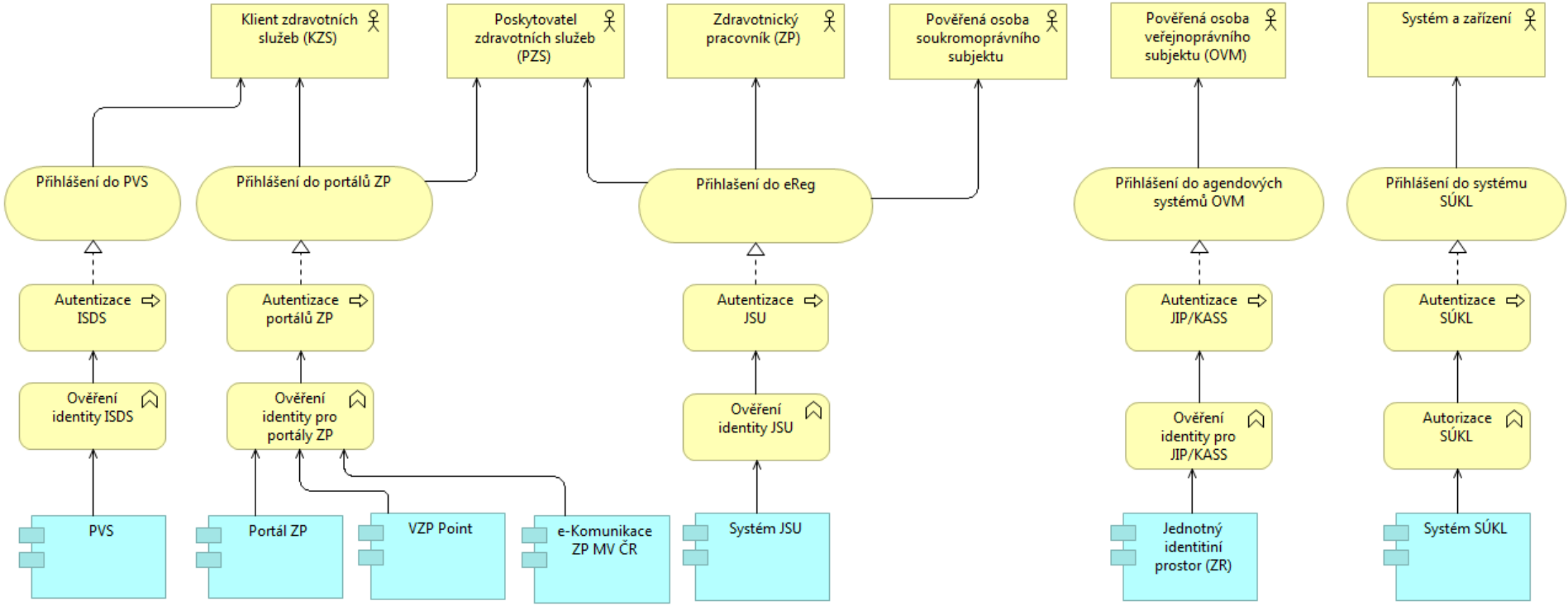
V následujících kapitolách jsou popsány následující pohledy na současný (AS-IS) stav enterprise architektury tématu:

- 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.

4.5 Pohledy na současný stav

4.5.1 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.

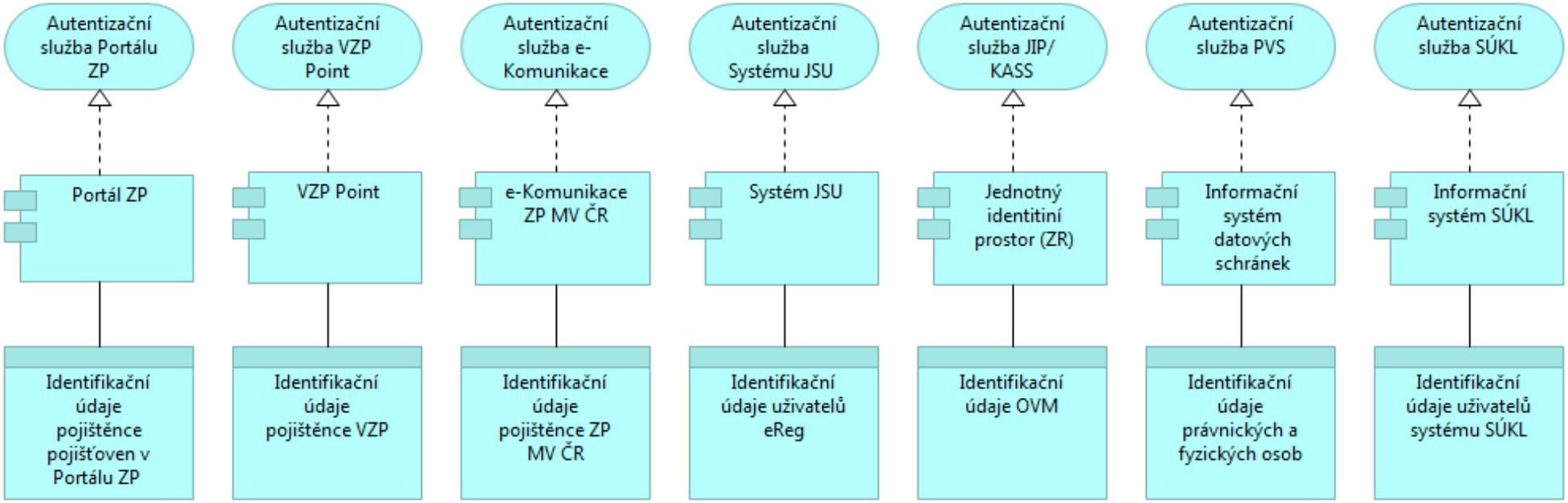


Obrázek 1 Procesní diagram AS-IS stavu identifikace a autentizace

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

4.5.2 Aplikační doména

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

4.6 Katalogy prvků současného stavu

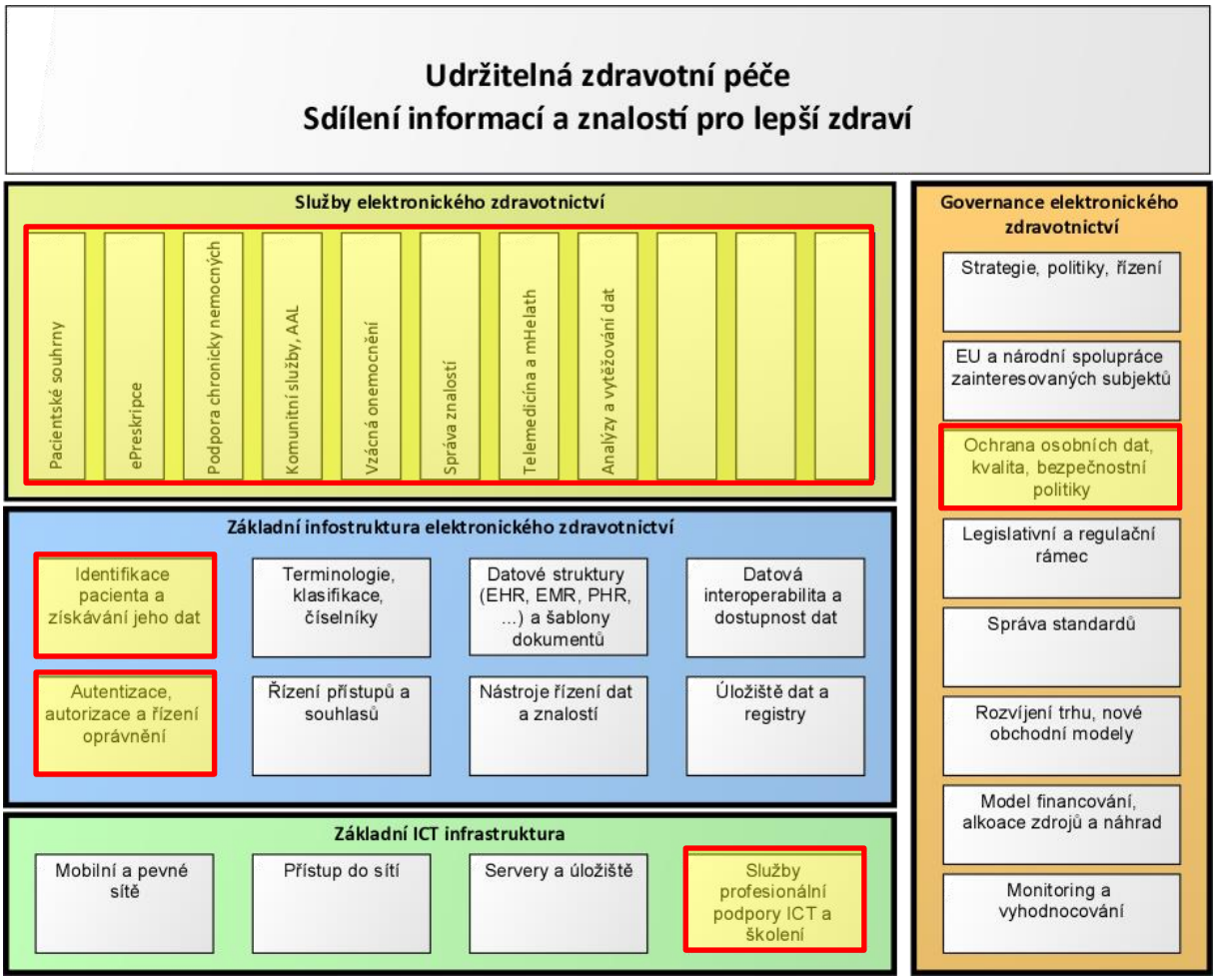
Katalogy prvků současného stavu byznys a aplikační domény jsou uvedeny v souboru MZCR_EA_T04_Katalog_prvku.xlsx v Příloze 1 tohoto dokumentu.

5 Návrh cílové architektury

5.1 Zasazení tématu do architektonického rámce elektronického zdravotnictví

Pro zasazení popisovaného tématu do architektonického rámce elektronického zdravotnictví byl zvolen společný koncept Evropské unie tak, jak je definován v projektu CALLIOPE pro budování interoperabilních národních systémů elektronického zdravotnictví. Níže uvedený diagram včetně textu je převzatý z výstupních dokumentů projektu CALLIOPE.

Pozn.: V diagramu jsou zvýrazněny oblasti, do kterých popisované téma zasahuje.



Obrázek 3 Model EU CALLIOPE pro interoperabilní elektronické zdravotnictví

Základní vrstva ICT infrastruktury zahrnuje národní infrastrukturu elektronických komunikací založenou na mobilních a pevných sítích, přístup k ICT sítím a službám zahrnujících i bezpečnostní služby, potřebné výpočetní zdroje a datová úložiště, profesionální technickou podporu a vzdělávání v oblasti ICT. Tato infrastruktura by měla být orientovaná na budoucí potřeby a měla by řešit potřeby na národní úrovni i potřeby vyplývající z přeshraniční spolupráce.

Základní vrstva infastruktury obsahuje všechny datové struktury, kodifikace, terminologie a ontologie, standardy datové interoperability a přístupu k datům, uložené informace a údaje, jakož i pravidla a dohody pro sběr a správu těchto dat a nástrojů pro jejich využívání. Dále obsahuje podpůrné služby jako je identifikace pacienta, autentizace, autorizace, řízení oprávnění, řízení souhlasů a dalších podpůrných služeb.

Vrstva služeb elektronického zdravotnictví obsahuje všechny komponenty, které přímo přispívají ke kvalitní péči a lepší přístupnosti a snižování nákladů, jako jsou pacientské informace, ePreskripce, řízení léčby chronických onemocnění, domácí sledování, telekonzultace, teleradiologie a další. Tyto služby obvykle odrážejí národní priority.

Oblast **governance elektronického zdravotnictví** zastřešuje jednotlivé vrstvy elektronického zdravotnictví. Jedná se o soubor činností, procesů, aktivit a politik, které mají na základě národních a EU strategii zajistit řízený elektronického zdravotnictví.

5.1.1 Zasazení tématu do celkového rámce elektronického zdravotnictví

Téma Řešení autentizace a autorizace zdravotnických pracovníků a pacientů v resortu zdravotnictví, zřizování přístupů, řízení souhlasů a přístupu k informacím, identifikace pacienta zasahuje do těchto oblastí:

- Služby elektronického zdravotnictví
  - Všechny služby vyžadující neanonymní přístup uživatelů
- Základní infastruktura elektronického zdravotnictví
  - Oblast Identifikace pacienta a získávání jeho dat
  - Oblast Autentizace, autorizace a řízení oprávnění
- Základní ICT infrastruktura
  - Oblast Služby profesionální podpory ICT a školení (zajištění způsobilosti uživatelů používat prostředky pro elektronickou identifikaci a autentizaci)
- Governance elektronického zdravotnictví
  - Vydání anebo novelizace veřejnoprávních předpisů vymezujících používání prostředků pro elektronickou identifikaci a autentizaci v resortu MZ ČR
  - Vydání pro uživatele závazných provozních pravidel a podmínek používání prostředků pro elektronickou identifikaci a autentizaci

5.1.2 Využívání sdílených služeb elektronického zdravotnictví

Identifikace, autentizace a autorizace uživatelů služeb je základním stavebním kamenem pro elektronické zdravotnictví. Identifikační údaje a autentizační a autorizační služby musí využívat veškeré navazující systémy v rámci elektronického zdravotnictví.

Téma Řešení autentizace a autorizace zdravotnických pracovníků a pacientů v resortu zdravotnictví, zřizování přístupů, řízení souhlasů a přístupu k informacím, identifikace pacienta realizuje následující centrální služby elektronického zdravotnictví:

- Služby autentizace
  - Autentizace klienta zdravotních služeb
  - Autentizace zdravotnického pracovníka
  - Autentizace pověřené osoby
  - Autentizace systému

- Služby autorizace
    - Kontrola oprávnění zdravotnického subjektu na služby
    - Kontrola mandátů
    - Evidence mandátů

5.2 Hlavní požadavky na cílový stav

5.2.1 Cílový stav tématu

V cílovém stavu tématu Autentizace a autorizace zdravotnických pracovníků a pacientů v resortu zdravotnictví je nezbytné zajistit následující průřezové funkce:

1. Identifikace
    - Jednoznačné rozlišení osoby
2. Autentizace
    - Ověření identity osoby pro přihlášení k systému
3. Autorizace
    - Udělení práva osoby použít funkci systému
4. Autentizace v urgentních situacích
    - Přístup k základním zdravotním údajům uložených na elektronickém průkaze zdravotního pojištění nebo spojených s číslem průkazu zdravotního pojištění
    - Přístup k zdravotním údajům pacienta v elektronické zdravotní dokumentaci

5.2.2 Cílový stav souvisejících témat

S tématem Autentizace a autorizace zdravotnických pracovníků a pacientů v resortu zdravotnictví úzce souvisí téma Sdílení a výměna dat mezi poskytovateli zdravotních služeb – eŽádanka, sdílení zdravotní péče. V rámci tématu je nezbytné zajistit následující funkce:

1. Zaručený elektronický podpis
    - Autenticita, integrita, nepopiratelnost,
    - Časové ukotvení (s využitím časového razítka)
2. Šifrování zpráv mezi osobami
    - Utajení obsahu zprávy
    - Zajištění, že zprávu dokáže přečíst pouze adresát

5.3 Architektonické principy

Cílový návrh architektury tématu Řešení autentizace a autorizace zdravotnických pracovníků a pacientů v resortu zdravotnictví, zřizování přístupů, řízení souhlasů a přístupu k informacím, identifikace pacienta je v souladu s architektonickými principy resortu zdravotnictví uvedenými v dokumentu MZd_EA_Architektonické_principy_v1.xlsx. Kromě nich aplikuje cílový návrh i architektonické principy stanovené v následujících podkapitolách.

5.3.1 Principy identifikace a autentizace

Principy identifikace a autentizace stanovují zásady využívání prostředků pro autentizaci uživatelů k systémům poskytujícím služby elektronického zdravotnictví.

Tabulka 8 Architektonické principy identifikace a autentizace

Princip	Vysvětlení
Využití existujících prostředků	Pokud subjekt již má vyhovující prostředek pro autentizaci, neměl by být nucen používat jiný
Uznávání eGov prostředků	Je nezbytné akceptovat prostředky zavedené veřejnoprávními předpisy v rámci eGovernmentu
Zvládání urgentních situací	Přístup k základním informacím z autorizovaných systémů bez autentizace uživatele
Uživatelská volba prostředků	Klient zdravotních služeb má možnost využívat vyhovující prostředek dle svého rozhodnutí
Autonomie vůle v soukromém právu	Zdravotnický pracovník má možnost využívat jiný vyhovující prostředek než jako soukromá osoba
Dostatečná úroveň záruky a důvěryhodnosti	Prostředek pro autentizaci, jeho vydávání a správa splňují stanovené podmínky

5.3.2 Principy autorizace

Principy autorizace stanovují zásady řízení přístupu uživatelů k systémům poskytujícím služby elektronického zdravotnictví.

Tabulka 9 Architektonické principy autorizace

Princip	Vysvětlení
Úplný přístup k údajům	Systémy nesmí bránit uživatelům využívat služby a údaje, které ovlivňují kvalitu zdravotních služeb
Auditovatelnost aktivit uživatelů	Systémy zaznamenávají aktivity uživatelů se službami a údaji, záznamy zpřístupňují vlastníkům údajů
Registrace využívajících systémů k agendám	IS využívající elektronické služby jsou registrovány k jedné nebo více zdravotnickým agendám
Příslušnost sdílených služeb k agendám	Každá elektronická služba poskytujícího IS je přiřazena k jedné nebo více zdravotnickým agendám
Řízení přístupu dle příslušnosti k agendám	Přístup k elektronickým službám je řízen příslušností volajícího IS ke zdravotnické agendě na úrovni referenčního rozhraní resortu MZ ČR
Jednotný katalog zdravotnických profesí	MZ ČR vede jednotný katalog profesí zdravotnických pracovníků pro účely identifikace role pracovníka
Důvěryhodnost správy profesí ve využívajících systémech	IS využívající elektronické služby předává identifikační údaje osob ztotožněné s identitním prostorem MZ ČR a profese ztotožněné s jednotným katalogem profesí

Důvěra poskytujícího systému v předané údaje	IS poskytující elektronickou službu důvěřuje údajům předaným IS využívajícím elektronickou službu
Odpovědnost využívajícího a poskytujícího systému za řízení přístupu	IS poskytující elektronickou službu odpovídá za stanovení podmínek a provádění řízení přístupu na základě údajů předaných IS využívajícím elektronickou službu

5.3.3 Principy mandátů

Principy mandátů stanovují zásady oprávnění zastupovat určitého uživatele (mandanta) jiným uživatelem (mandatářem) v systémech poskytujících služby elektronického zdravotnictví.

Tabulka 10 Architektonické principy mandátů

Princip	Vysvětlení
Centrální správa mandátů	Registr mandátů je veden centrálně na úrovni resortu MZ ČR
Odpovědnost ověřování mandátů	IS poskytující elektronické služby ověřují mandáty výhradně v registru mandátů

5.4 Motivace pro vytvoření pohledů na cílový stav enterprise architektury tématu

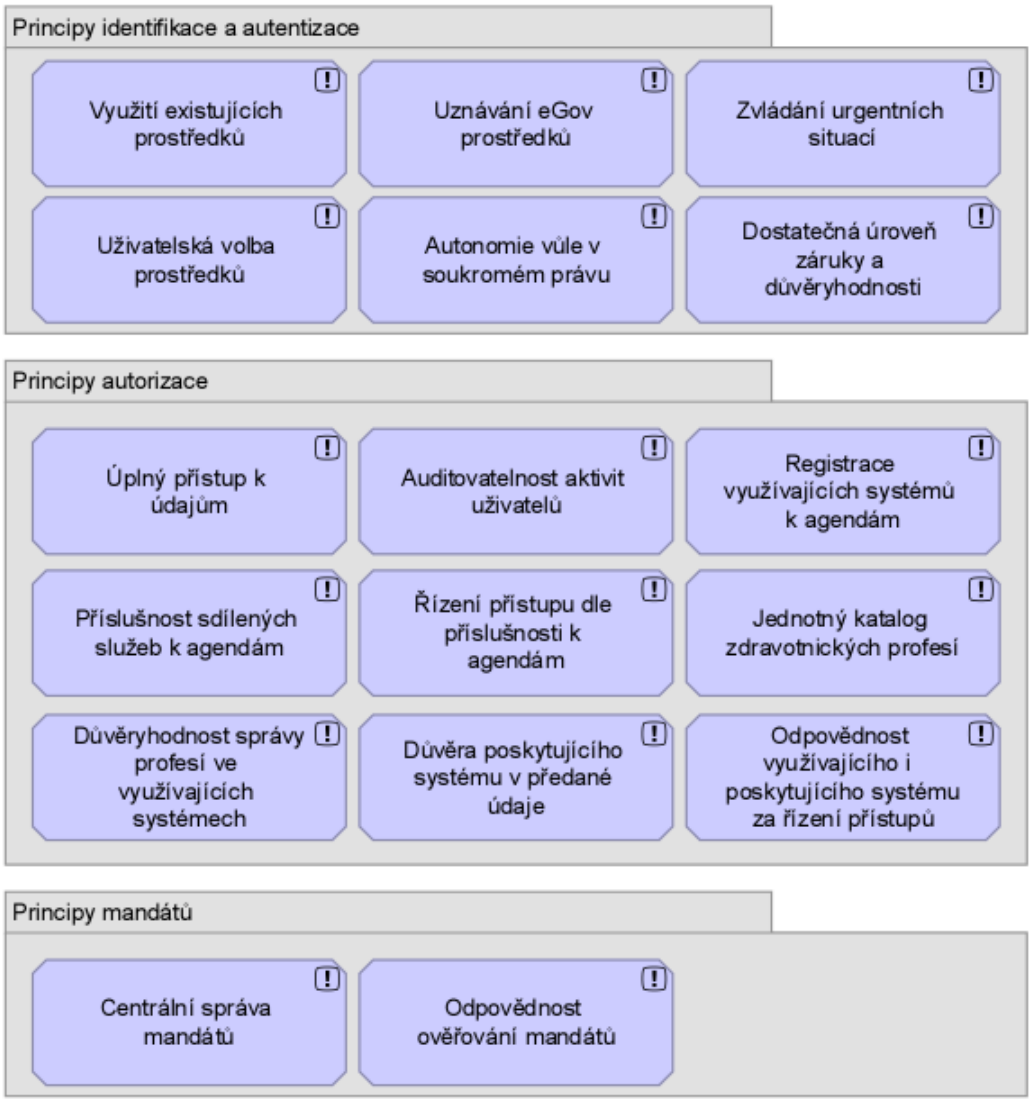
V následujících kapitolách jsou popsány tyto pohledy na cílový stav enterprise architektury tématu:

- Architektonické principy – souhrn závazných zásad pro řešení identifikace, autentizace a autorizace subjektů elektronického zdravotnictví.
- Identitní prostory – diagram slouží pro zobrazení základních subjektů v rámci elektronického zdravotnictví, zdroje identifikačních údajů těchto subjektů a vztah identifikačních údajů k referenčním údajům v základních registrech eGovernementu.
- Vazby autentizačních služeb – diagram slouží pro zobrazení aplikačních komponent se vztahem k autentizaci a jejich vzájemných vazeb.
- Autorizace – diagram slouží pro zobrazení aplikačních komponent realizujících služby pro autorizaci v elektronickém zdravotnictví a způsobu, jak jsou tyto služby publikovány a využívány.
- Uplatnění principů autorizace – diagram slouží pro zobrazení vazeb architektonických principů a aplikačních komponent odpovědných za realizaci autorizačních služeb a funkcí v elektronickém zdravotnictví.

5.5 Pohledy na cílový stav enterprise architektury tématu

5.5.1 Motivační doména

5.5.1.1 Architektonické principy



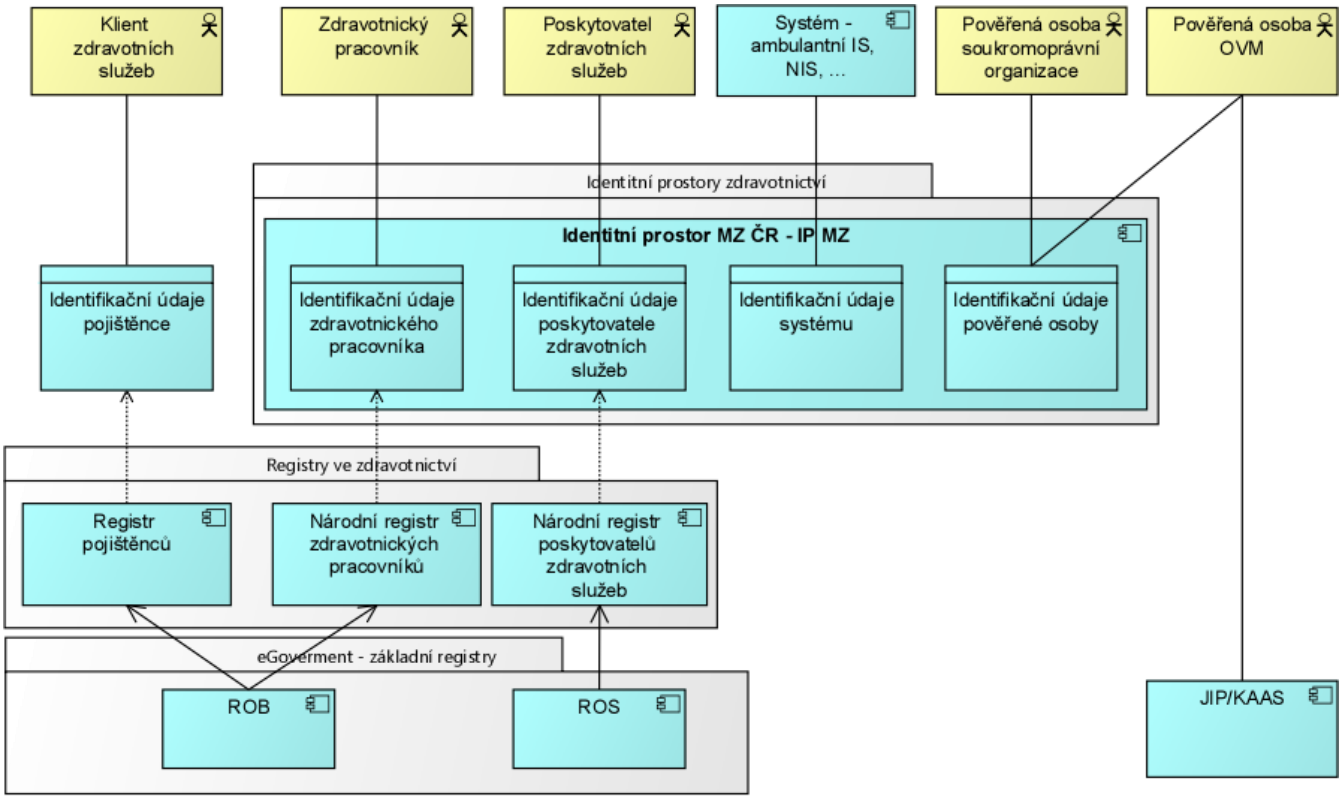
Obrázek 4 Principy identifikace, autentizace, autorizace a mandátů

Přítomnost motivační domény, která obsahuje model architektonických principů, je dána skutečností, že identifikace, autentizace a autorizace tvoří průřezové funkce, které budou společné pro všechny služby elektronického zdravotnictví. Z toho důvodu je správná definice jejich vlastností zásadní pro celkovou bezpečnost a spolehlivost komplexu systémů, jež jsou předmětem řešení všech ostatních témat.

Definice architektonických principů je obsažena v kapitole 5.3 výše.

5.5.2 Business doména

5.5.2.1 Identitní prostory



Obrázek 5 Vazba subjektů na identitní prostory

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

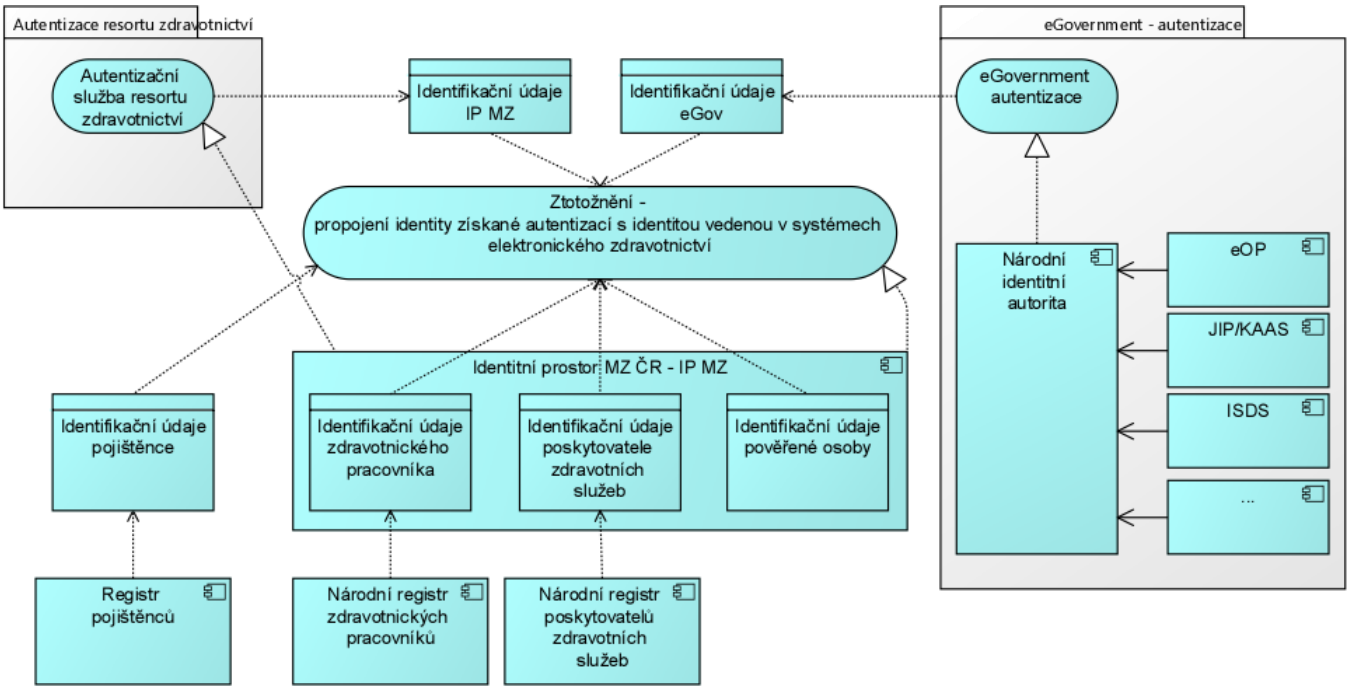
Subjekty, pro které bude třeba ve zdravotnictví řešit autentizaci a identifikaci, jsou:

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

5.5.3 Aplikační doména

5.5.3.1 Vazby autentizačních služeb

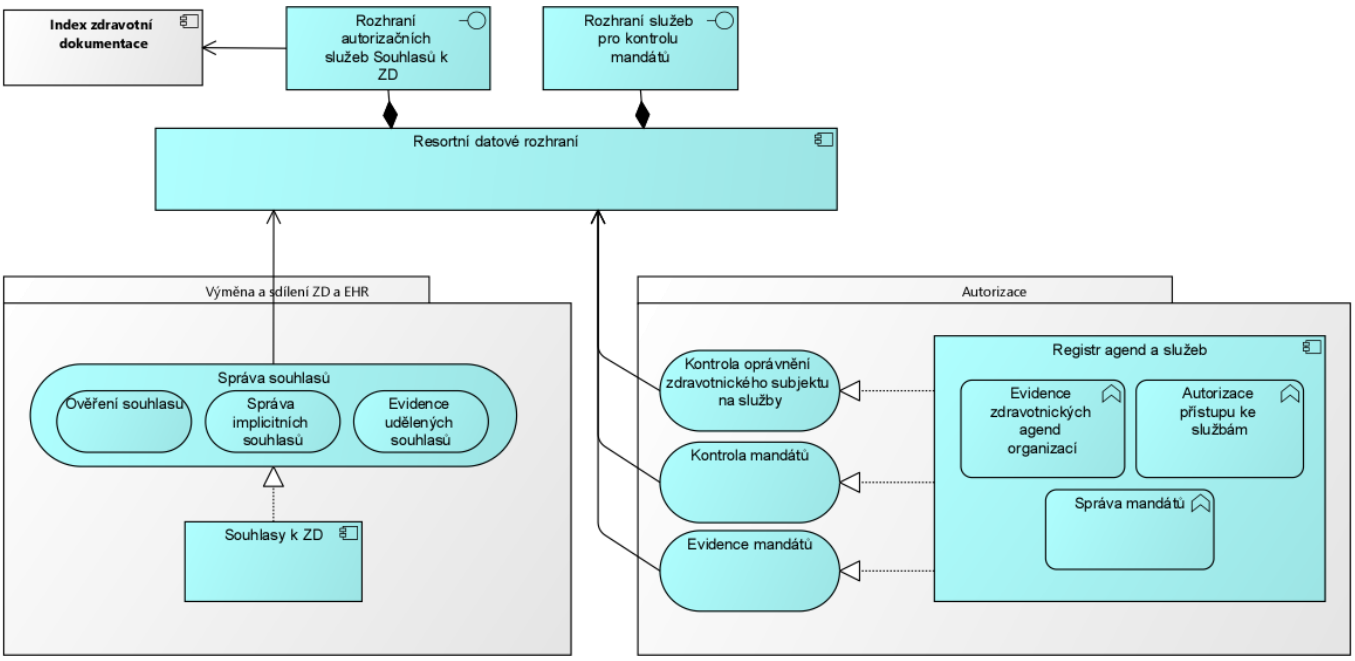


Obrázek 6 Cílový stav autentizačních služeb

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

Je nezbytné zmínit, že zavádění eOP v rámci eGovernmentu si vyžádá několik let a může být doprovázeno různými problémy. Je pro nutné uvažovat i o alternativním řešení v rámci Informačního a datového rozhraní resortu (IDRR). V takovém případě je třeba uzavřít memorandum s MV ČR do doby než bude obyvatelstvo v dostatečném rozsahu pokryto eOP (cca rok 2022).

5.5.3.2 Autorizace



Obrázek 7 Cílový stav autorizace

Pro elektronické služby ve zdravotnictví je třeba rozlišovat dva druhy autorizace:

- Autorizace na úrovni systémů a rolí
- Souhlasy v rámci sdílení zdravotní dokumentace, EHR a PHR

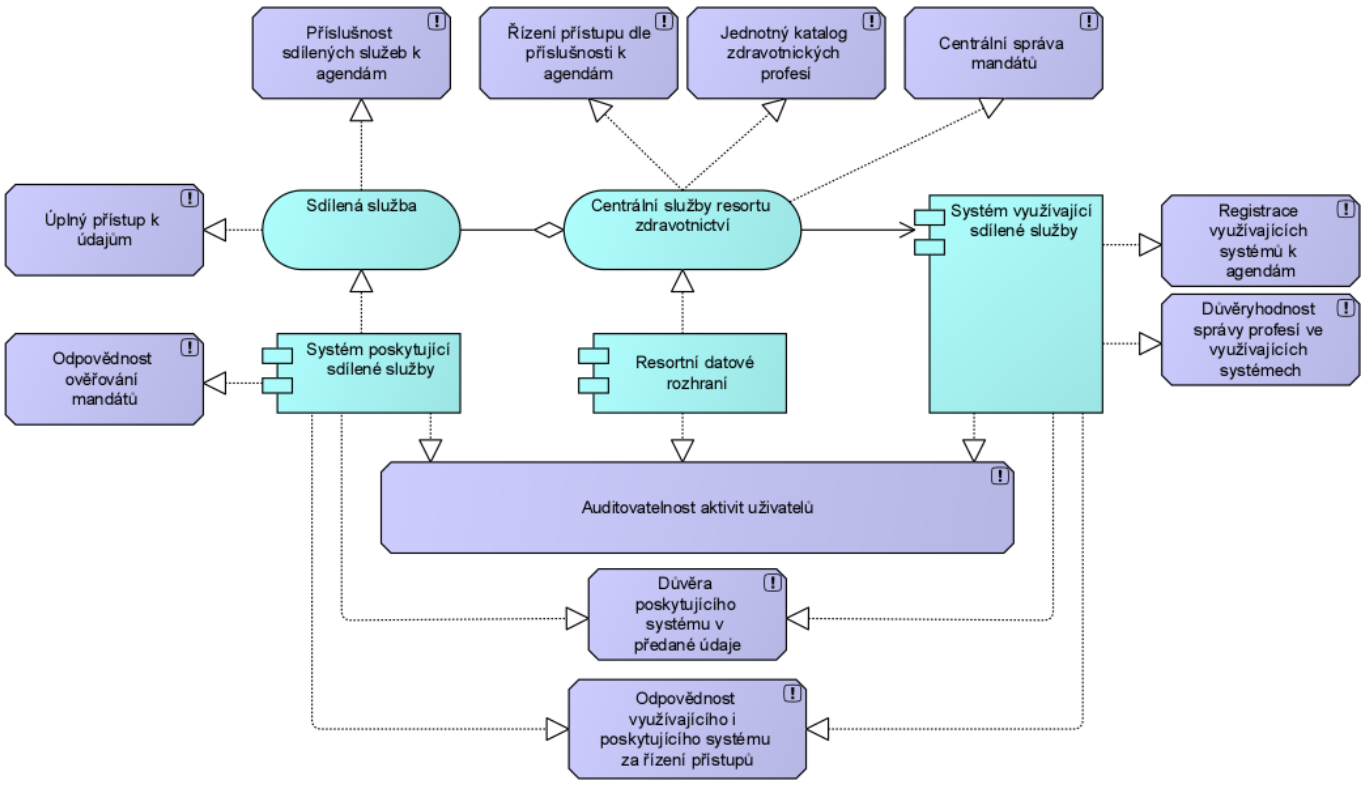
Služby pro autorizaci na úrovni systémů a rolí bude zajišťovat komponenta Registr agend a služeb a její subkomponenta Registr mandátů.

Registr agend a služeb slouží zejména k evidenci zdravotnických agend organizací a elektronických služeb přiřazených k těmto agendám. Na základě této evidence je následně řízena autorizace přístupu konkrétních IS ke konkrétním elektronickým službám. Službu Kontrola oprávnění zdravotnického subjektu na služby využívá zejména Informační a datové rozhraní resortu (IDRR), které na základě výsledků služby umožňuje nebo blokuje přístup k elektronickým službám, které jsou přes IDRR vystaveny.

Součástí Registru agend a služeb je také Mandátní registr, jehož úlohou je správa mandátů, tj. správa pověření osob vůči jiným osobám. Služby pro kontrolu mandátů jsou publikovány na Resortním datovém rozhraní.

Evidence souhlasů v rámci sdílení zdravotní dokumentace, EHR, PHR a také přístupu k indexu zdravotní dokumentace náleží komponentě Souhlasy k ZR. Komponenta realizuje služby pro ověřování souhlasů, správu implicitních souhlasů a evidence udělených souhlasů. Služby jsou publikovány prostřednictvím Resortního datového rozhraní.

5.5.3.3 Uplatnění principů autorizace



Obrázek 8 Odpovědnosti za uplatnění principů autorizace

Klíčovým faktorem pro řádnou a funkční autorizaci přístupu uživatelů ke sdíleným službám elektronického zdravotnictví je prosazení odpovědnosti tvůrců a provozovatelů informačních systémů za uplatňování stanovených principů.

Odpovědnosti za uplatnění principů autorizace jsou rozděleny do tří oblastí:

1. Odpovědnost resortního datového rozhraní, které prostřednictvím centrálních služeb resortu zdravotnictví zprostředkovává systémům využívajícím sdílené služby přístup k systémům poskytujícím sdílené služby. Za prosazení principů autorizace odpovídá MZ ČR.
2. Odpovědnost systémů poskytujících sdílené služby za způsob realizace řízení přístupu ke službám a datům, především na základě údajů o zdravotnické profesi přistupujícího uživatele. Za prosazení principů autorizace odpovídá správce systému poskytujícího sdílené služby.
3. Odpovědnost systémů využívajících sdílené služby za řádnou správu uživatelů a přiřazení zdravotnické profese uživatele v roli spojené se službou, která volá službu poskytujícího systému. Za prosazení principů autorizace odpovídá správce systému využívajícího sdílené služby.

Nástrojem kontroly řádného prosazení principů autorizace budou pravidelně prováděné bezpečnostní audity všech informačních systémů využívajících a poskytujících sdílené služby elektronického zdravotnictví. Závazek podstoupit bezpečnostní audit a realizovat opatření k nápravě nálezů bude součástí smluvních podmínek připojení informačního systému k resortnímu datovému rozhraní.

5.6 Katalogy prvků cílového stavu

Katalogy prvků cílového stavu byznys a aplikační domény jsou uvedeny v souboru MZCR_EA_T04_Katalog_prvku.xlsx v Příloze 1 tohoto dokumentu.

5.7 Shrnutí navrhované architektury

5.7.1 Prostředky pro autentizaci klientů zdravotních služeb

Pro klienty zdravotních služeb budou k dispozici prostředky pro autentizaci zařazené do systému Národní identitní autorita (NIA), kterou bude provozovat MV ČR. Předpokládá se možnost využití následujících prostředků:

- NIA/eOP (elektronický občanský průkaz)
  - přihlášení pomocí eOP ČR prostřednictvím Národní identitní autority
- NIA/ISDS (informační systém datových schránek)
  - přihlášení pomocí autentizačních údajů ISDS prostřednictvím NIA
- NIA/SIDP (eID prostředky poskytované soukromoprávními subjekty, např. mojeID)
  - přihlášení pomocí služby soukromoprávního poskytovatele identifikačních a autentizačních služeb (např. mojeID) prostřednictvím NIA
- NIA/eIDAS (prostředky zveřejněné na seznamu Komise EU)
  - přihlášení pomocí zahraničního prostředku elektronické identifikace v souladu s eIDAS zprostředkované pomocí NIA

5.7.2 Strategická doporučení

Strategie v oblasti autentizace, identifikace, autorizace:

1. Využívání služeb eGovernmentu (eGov first)
2. Vytvoření identitního prostoru MZ ČR (IP MZ ČR) pro osoby ve zdravotnictví, který bude propojen na systémy základních registrů
3. Zajištění správy pověření (mandátů) pro segment zdravotnictví

5.7.3 Doporučení pro autentizaci subjektů ve zdravotnictví

- Klient (pacient, pojištěnec, občan)
  - eGov first – může využít eGov služby
  - MZ ČR nebude budovat systémy pro autentizaci klientů (pacient, pojištěnec, občan). Motivuje k využívání eGov služeb.
- Zdravotnický pracovník
  - eGov first – může využít eGov služby
  - MZ ČR nabídne alternativu (IP MZ ČR)
- Pověřené osoby veřejnoprávních subjektů (OVM)
  - eGov first – může využít eGov služby
  - MZ ČR nabídne alternativu (IP MZ ČR)
- Pověřené osoby soukromoprávních subjektů
  - eGov first – může využít eGov služby
  - MZ ČR nabídne alternativu (IP MZ ČR)

6 GAP analýza

Pro dosažení cílového stavu je nutné:

- Realizovat napojení na Národní identitní autoritu ČR (NIA)
- Realizovat propojení Registru pojištěnců VZP (RP) s Registrem obyvatel (ROB) a provést ztotožnění identit v RP s ROB
- Realizovat Identitní prostor MZ ČR (IP MZ)
- Realizovat Autentizační službu resortu zdravotnictví
- Realizovat Národní registr zdravotnických pracovníků (NRZP)
- Realizovat propojení Národního registru poskytovatelů zdravotních služeb (NRPZS) s Registrem osob (ROS) a provést ztotožnění identit v NRPZS s ROS
- Realizovat Centrální službu resortu zdravotnictví s funkcionalitou řízení přístupu ke sdíleným službám dle příslušnosti k agendám elektronického zdravotnictví
- Realizovat Jednotný katalog zdravotnických profesí
- Realizovat Centrální správu mandátů a souhlasů
- Zavést procesy provozní podpory a školení uživatelů pro zajištění jejich způsobilosti k používání prostředků pro elektronickou identifikaci a autentizaci
- Stanovit právní a technické podmínky pro používání zaručených elektronických podpisů elektronických dokumentů a jejich důvěryhodného úložiště s využitím časových razítek
- Stanovit právní a technické podmínky pro odesílání a příjem šifrovaných dat mezi zdravotnickými profesionály
- Stanovit právní a technické podmínky spojené s autorizací v informačních systémech využívajících sdílené služby elektronického zdravotnictví
- Stanovit právní a technické podmínky spojené s autorizací v informačních systémech poskytujících sdílené služby elektronického zdravotnictví
- Vydat anebo novelizovat veřejnoprávní předpisy vymezující používání prostředků pro elektronickou identifikaci a autentizaci v resortu zdravotnictví
- Vydat pro uživatele závazná provozní pravidla a podmínky používání prostředků pro elektronickou identifikaci a autentizaci v resortu zdravotnictví

7 Otevřené body

Tabulka 11 Seznam otevřených bodů

ID bodu	Název bodu	Popis otevřeného bodu
B01	Elektronický průkaz zdravotního pojištění	Elektronický průkaz zdravotního pojištění je vhodnou alternativou pro identifikaci i případnou autentizaci klientů zdravotních služeb a jako nosič základních údajů o zdravotním stavu (emergency data set). Záměry MZ ČR v oblasti standardizace a zavedení elektronického průkazu zdravotního pojištění v ČR nejsou k dispozici.

Příloha 1 – Katalog prvků

Příloha je uvedena v samostatném souboru MZCR_EA_T04_Katalog_prvku.xlsx.

Web strategie: http://www.nsez.cz

Vzor citace dle ČSN ISO 690:2011

MINISTERSTVO ZDRAVOTNICTVÍ ČESKÉ REPUBLIKY. *Cílová architektura tématu T04 – Řešení autentizace a autorizace zdravotnických pracovníků a pacientů v resortu zdravotnictví, zřizování přístupů, řízení souhlasů a přístupu k informacím, identifikace pacienta.* Verze 1.00. Praha, 2016. Licencováno pod CC BY 4.0, licenční podmínky dostupné z: http://creativecommons.org/licenses/by/4.0/.