eHealth

nová dimenzia v starostlivosti o Vaše zdravie

eSO1 eHealth služby občanom

Európsky fond regionálneho rozvoja
„Tvoríme vedomostnú spoločnosť"

Projekt je spolufinancovaný Európskou úniou

MINISTERSTVO FINANCIÍ Slovenskej republiky
Sprostredkovateľský orgán OPIS

MINISTERSTVO ZDRAVOTNÍCTVA Slovenskej republiky

Riadiaci orgán OPIS

Európska únia

OPIS

NÁRODNÉ CENTRUM ZDRAVOTNÍCKYCH INFORMÁCIÍ

eHealth elektronické zdravotníctvo

eSO1 eHealth služby občanom

LYNX

Bezpečnosť eHealth a eSO1

ITAPA, október 2011

RNDr. Michal Danilák
tím eSO1

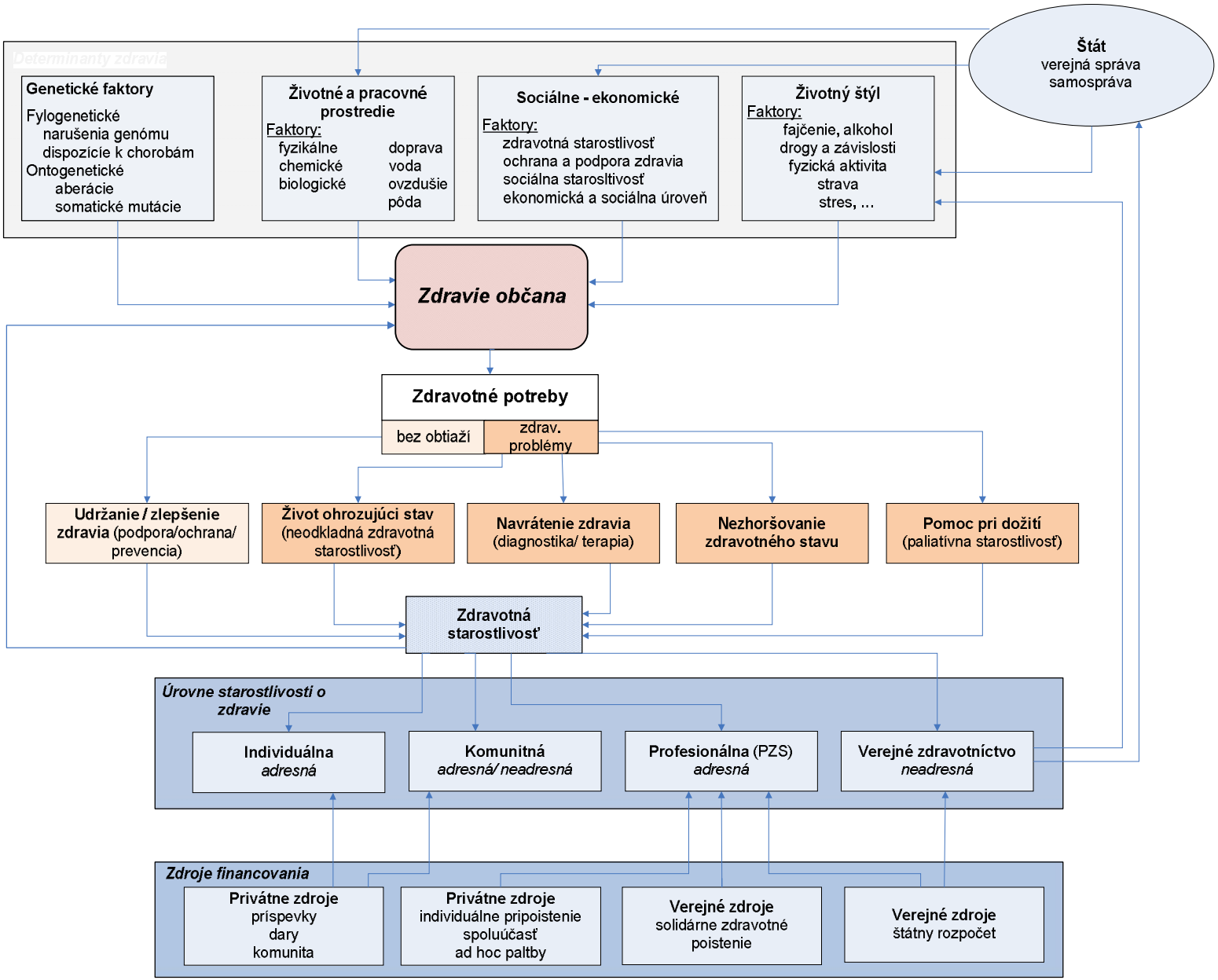
Čo je eHealth a čo je predmetom jeho bezpečnosti?

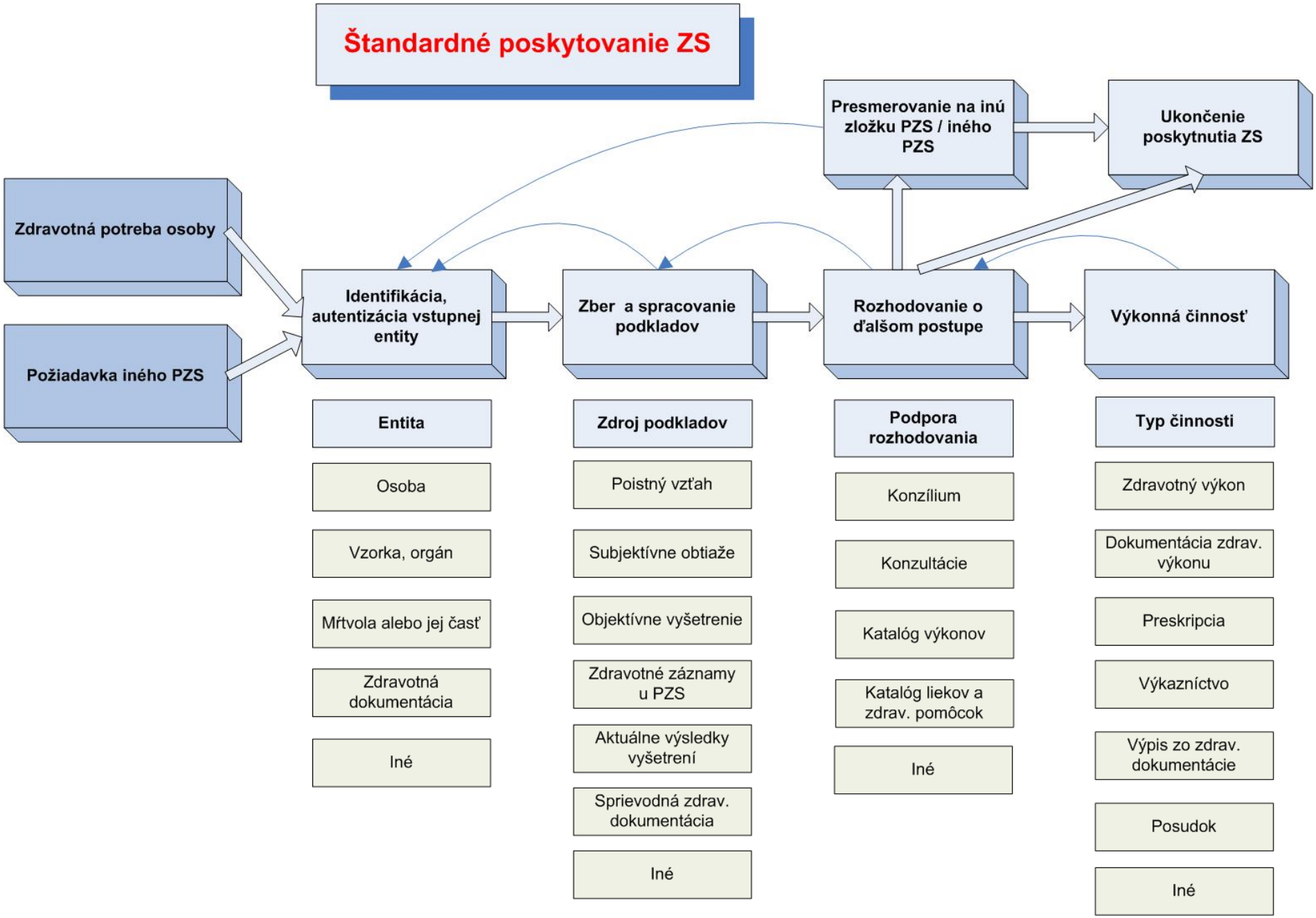
Poslaním zdravotníctva je významne prispievať k zvyšovaniu kvality života občanov prostredníctvom znižovania úmrtnosti, chorobnosti, trvalých a dočasných následkov chorôb a úrazov; poskytovaním zdravotnej starostlivosti, pôsobením verejného zdravotníctva, podporou individuálnej a komunitnej starostlivosti o zdravie.

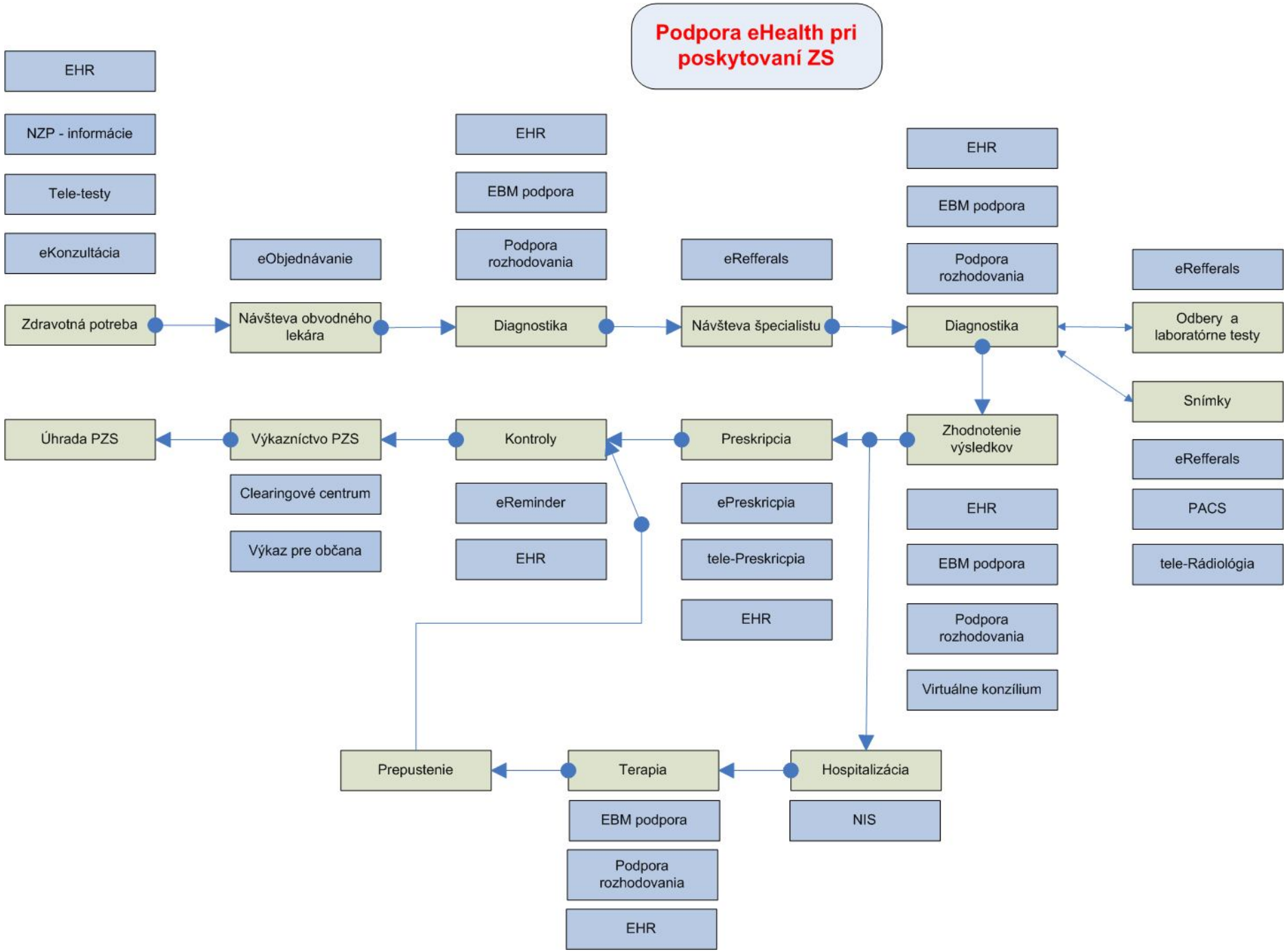
Poslaním elektronického zdravotníctva (eHealth) je podpora poslania zdravotníctva prostredníctvom informačných a komunikačných technológií.

Bezpečnosť elektronického zdravotníctva je vymedzená nielen poslaním eHealth, ale aj poslaním a významom zdravotníctva, zdravia a práv občanov.

Model starostlivosti o zdravie




Štandardné poskytovanie ZS
Zdravotná potreba osoby
Požiadavka iného PZS
Identifikácia, autentizácia vstupnej entity
Zber a spracovanie podkladov
Rozhodovanie o ďalšom postupe
Výkonná činnosť
Presmerovanie na inú zložku PZS / iného PZS
Ukončenie poskytnutia ZS
Entita
Osoba
Vzorka, orgán
Mŕtvola alebo jej časť
Zdravotná dokumentácia
Iné
Zdroj podkladov
Poistný vzťah
Subjektívne obtiaže
Objektívne vyšetrenie
Zdravotné záznamy u PZS
Aktuálne výsledky vyšetrení
Sprievodná zdrav. dokumentácia
Iné
Podpora rozhodovania
Konzílium
Konzultácie
Katalóg výkonov
Katalóg liekov a zdrav. pomôcok
Iné
Typ činnosti
Zdravotný výkon
Dokumentácia zdrav. výkonu
Preskripcia
Výkazníctvo
Výpis zo zdrav. dokumentácie
Posudok
Iné


Podpora eHealth pri poskytovaní ZS
EHR
NZP - informácie
Tele-testy
eKonzultácia
Zdravotná potreba
eObjednávanie
Návšteva obvodného lekára
EHR
EBM podpora
Podpora rozhodovania
Diagnostika
eRefferals
Návšteva špecialistu
EHR
EBM podpora
Podpora rozhodovania
Diagnostika
eRefferals
Odbery a laboratórne testy
Snímky
eRefferals
PACS
tele-Rádiológia
Zhodnotenie výsledkov
EHR
EBM podpora
Podpora rozhodovania
Virtuálne konzílium
Preskripcia
ePreskripcia
tele-Preskripcia
EHR
Kontroly
eReminder
EHR
Výkazníctvo PZS
Clearingové centrum
Výkaz pre občana
Úhrada PZS
Prepustenie
Terapia
EBM podpora
Podpora rozhodovania
EHR
Hospitalizácia
NIS

eHealth je zložitý, jeho bezpečnosť tiež ...

	Nár. legislatíva	Legislatíva EÚ	Národné normy	Medzinár. normy	Architekt. rámec	Certif. / akr. / HTA	Sieťová vrstva HIN	Podpora HIN	Dátové úložiská HIN	PKI infraštruktúra	Registre	Infraštruktúra EHR	Infraštruktúra EDS	NZP	Switch Point	El. preukaz PZS	El. preuk. poist.	Infr. ePreskripcie	Infr. el. výkaznictva	Integr. Middleware	Ambulantné IS	Lekárenské IS	Laboratórne IS	PACS	NIS	NTS	IZS	IS záchranky	Obj. / Refferals	ePreskripcia	IS verejného zdrav.	Monitoring ZS	Integrácia do NZP	Call centr. eHealth	Telemedicína	EBM	IT podpora DRG	EÚ mobilita	eLearning	IT nové med. obl.	Výskum a vývoj	Využitie tokenu	Integrácia s eGov.
Národná legislatíva		sZ	P	mZ	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Legislatíva EÚ	P			P																																						
Národné normy a dátové štandardy	sZ	Z		sZ	P		P		P	P	P	P	P			P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Medzinárodné normy a štandardy	P	sZ																																								
Architektonický rámec	Z	mZ	sZ	Z			P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	Z
Certifikácia / akreditácia / HTA	sZ	mZ	Z	mZ	Z					P	P					P	P	P	P		P	P	P	P																		
Sieťová vrstva HIN	mZ	mZ	Z	mZ	sZ			P	P	P	P	P	P	P	P			P	P	P	P	P	P	P	P	P	P	P	P	P	P		P	P			P	P	P	P		Z
Podpora HIN	mZ	mZ	mZ	Z	sZ		sZ		P	P	P	P	P	P	P			P	P	P	P	P	P	P	P	P	P	P	P		P	P		P	P			P	P	P		
Dátové úložiská v rámci HIN	mZ	mZ	Z	mZ	sZ	P	sZ	mZ		Z	P	P	P	P	P	P	P	P	P	P				P	P	P			P	P	P	P		P	P			P		P	P		Z
PKI infraštruktúra v rámci HIN	sZ	mZ	sZ	Z	Z	P	mZ	mZ	P			P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P		P	P				P			P		P	P	sZ	sZ
Registre	sZ	mZ	sZ	mZ	mZ				sZ				P	P	P	P	P	P	P		P	P	P	P	P	P	P		P	P			P	P			Z		P		Z	Z
Infraštruktúra pre EHR	mZ	mZ	Z	Z	sZ		sZ	Z	Z	sZ	Z		Z	Z		Z	Z	mZ	mZ	P	P	P	P	P	P	P	P			P		P	P		P		P		P	P	Z	Z
Infraštruktúra pre EDS	mZ	mZ	Z	Z	sZ		Z	Z	sZ	Z	Z	sZ		Z		Z	sZ			P						P	Z	Z		Z		P		P			P		P	P	Z	Z
Národný zdravotný portál	mZ	mZ	mZ	mZ	Z		Z	Z	Z	Z	mZ	mZ	mZ		P	P	P	Z	Z	Z	P	P	P	P	P	P	P	P	Z	Z	Z		Z	mZ	mZ	P	P	P	P	P	Z	Z
Switch Point	mZ	sZ	mZ	mZ	mZ		Z	mZ					mZ							Z					P		P											sZ					
Elektronický preukaz PZS (HPI)	Z	mZ	Z	mZ	sZ					sZ	Z							P	P		P	P	P		P					P												sZ	sZ
Elektronický preukaz poistenca	Z	Z	Z	Z	Z					sZ	Z		P								P	P			P	P	P	P														sZ	sZ
Infraštruktúra pre ePreskripciu	mZ	mZ	mZ	Z	sZ		Z	Z	sZ	Z	sZ	Z		sZ		sZ	Z			Z	P	P			P					P		P	Z				P				Z	Z
Infraštruktúra pre el. clearing	mZ	mZ	mZ		sZ		Z	Z	mZ	Z	Z	mZ		sZ		sZ		mZ		Z	P	P	P		P								Z								Z	Z
Integračný middleware	Z		mZ	mZ	Z		mZ		mZ	Z	Z	Z	Z	mZ	Z	sZ	Z	Z	Z		sZ	sZ	sZ	Z	sZ	Z	mZ	mZ	mZ	sZ	mZ	sZ	sZ	mZ	mZ	P	P	Z		mZ	P	mZ	sZ
Samostatné ambulantné IS	Z	mZ	mZ	mZ	P	Z	mZ		mZ	mZ	mZ	Z	mZ	P	Z	Z	Z	mZ	Z	mZ		mZ	mZ	mZ	mZ				Z	Z	P	P	P	P	P	P	P		P		mZ	mZ
Samostatné lekárenské IS	Z	mZ	mZ	mZ	P	Z	mZ		mZ	mZ	mZ	Z	mZ	P	Z	Z	Z	mZ	Z	mZ	mZ				mZ				P		P	P	P	P		P		P			mZ	mZ
Samostatné laboratórne IS	Z	mZ	mZ	mZ	P	Z	mZ		mZ	mZ	mZ	Z	mZ	P	mZ	mZ			Z	mZ	P				P				Z		P	P	P	P	P	P	P		P		mZ	
Rádiodiagnostické IS / PACS	Z	mZ	mZ	Z	P	Z	Z		sZ	mZ	mZ	Z		P	Z	mZ				mZ	P				P				Z		P	P	P		Z		P		P			mZ
Nemocničné IS	Z	mZ	mZ	mZ	P	Z	Z		Z	mZ	mZ	Z	Z	P	Z	sZ	Z	Z	mZ	Z	P	P	P	P		mZ	P	P	P	Z	P	Z	P	P	Z			P		P	P	mZ	
IS národnej transfúznej služby	Z	mZ	mZ	mZ	Z		mZ		Z		sZ	mZ	mZ	mZ		Z	Z			mZ	P				P			sZ	P		P	P	P									Z	
IS pre Integrovaný záchr. systém	Z	Z	mZ	Z	mZ		mZ				mZ	Z	sZ	mZ		mZ	Z			mZ					Z	P		Z			P	P			Z			P		P		mZ	Z
IS pre záchranné služby	Z	mZ	mZ	mZ	mZ		mZ				Z		sZ				Z			mZ					sZ	Z	sZ				P	P			mZ								mZ	mZ
Objednávanie / eRefferals	Z		mZ	mZ	Z	Z	sZ	Z	Z		mZ			sZ	mZ	mZ	Z			mZ	sZ		sZ	sZ	sZ						P	P		mZ		P	P		P		mZ	mZ
ePreskripcia	sZ	mZ	Z	Z	Z	Z	sZ	mZ	Z	Z	Z	mZ		sZ	mZ	sZ	mZ	sZ		mZ	sZ	sZ	sZ		sZ				P		P	P	Z	P	P	P	P	P				sZ	mZ
Informatizácia verejného zdrav.	mZ	mZ		mZ	mZ		Z		mZ		mZ			Z	mZ					mZ	Z	mZ	mZ	mZ	Z	mZ	mZ		mZ	Z		sZ	Z				mZ					sZ
Monitoring / hodnotenie poskyt. ZS	Z	mZ	mZ	mZ	mZ		sZ		Z		mZ			mZ	mZ	Z	Z	mZ	mZ	Z	Z	Z	Z		sZ	Z	Z	Z	mZ	Z	P		Z	mZ	Z			P	P			mZ
Integrácia aplikácií do NZP	mZ			mZ	sZ		mZ		Z	Z	Z			sZ	mZ	Z	Z	mZ	mZ	Z	P	P	P	P	Z	Z	Z	mZ	P	Z		P		mZ			P		P		Z	Z
Call centrum pre eHealth	mZ		mZ	mZ	Z		Z		mZ		Z			mZ	P					mZ	Z	Z	mZ		Z	P			Z		P	mZ	mZ		mZ			Z		mZ			Z
Telemedicínske aplikácie	Z	mZ	mZ	Z	Z	Z	sZ	mZ	Z	mZ	Z	Z		Z	mZ	Z	mZ			mZ	Z				Z		Z	Z	Z		P	mZ	Z		P	P	P		P	P	mZ	Z
Evidence based medicine support	mZ		mZ	Z	mZ						mZ			Z						mZ	Z				Z					sZ		P	Z		P				mZ	Z	mZ		
IT podpora DRG	mZ		mZ	mZ	mZ						mZ			Z						mZ	Z	Z	Z	Z	Z		Z	Z	Z	Z	P	P	mZ		P	Z				Z	Z		mZ
EÚ mobilita poistenca / pacienta	mZ	sZ	Z	sZ	mZ		mZ		Z		sZ		mZ	mZ	Z	mZ	Z	mZ	Z	Z	Z	Z	Z	Z	Z		Z	P	P	Z		P	P	P			P		P		Z	mZ
eLearning v eHealth				mZ	mZ		mZ							Z						mZ	mZ	mZ	mZ	mZ	mZ				Z	Z	Z		P	P	P			P	P			mZ
IT v nových oblastiach medicíny	Z	mZ	mZ	Z	Z	Z	Z		sZ	Z	Z		mZ	Z				mZ		mZ	P	P	P	P	P			P		P	P		P	P					Z	mZ	mZ
Výskum a vývoj v oblasti eHealth	Z	Z	Z	Z	Z	mZ			mZ	mZ	mZ	mZ	mZ	mZ			mZ	mZ	mZ		P	P	P	P	P	P	P	P	P	P	P		P	P	P	P	P	P		P	
Viacnásobné využitie tokenu	sZ	mZ	Z	mZ	sZ		mZ			sZ			sZ	sZ		Z	sZ	mZ	Z							Z	Z	Z	mZ	Z			Z		Z		Z		Z			P
Integrácia s eGovernmentom	sZ		Z	mZ	Z		Z	mZ	P	Z	Z	mZ	mZ		mZ		Z	mZ	mZ	mZ						mZ	mZ	mZ	mZ	mZ	Z	mZ	Z	Z			mZ	mZ		mZ	Z		
	sZ		Z		sZ		mZ			Z	mZ	Z	Z	Z		mZ	sZ	Z			mZ	mZ		mZ	Z	Z	Z	mZ	sZ	sZ	mZ	sZ		Z	mZ		Z		mZ		sZ	
	mZ		Z	mZ	mZ		mZ	mZ	mZ		mZ																		mZ	mZ												Z

sZ - silne závisí od
Z - závisí od
mZ - v menšej miere závisí od
P - dostáva podnety a požiadavky od

Význam bezpečnosti v eHealth / eSO1

- Otázka týkajúca bezpečnosti eHealth či v rámci projektu eSO1 je jednou z najčastejších.
- Väčšina obáv občanov znie: ***čo ak sa niekto neoprávnený dostane k mojim záznamom?***
- Zdravotné záznamy sú omnoho citlivejšie vnímané ako akékoľvek iné údaje, ktoré sú v súčastnosti centralizovane zbierané (je to osobitná kategória osobných údajov podľa zákona č. 428/2002 Z. z.)
- Akékoľvek ohrozenie zdravotných záznamov je vnímané vysoko emotívne, keďže ich zneužitie predstavuje útok do intímnej sféry občanov, s možným dopadom na ich spoločenské postavenie.
- Je tu ale ešte jedna podstatná otázka: ***čo ak lekár nemá potrebné informácie pre správne poskytnutie zdravotnej starostlivosti?***

Protichodnosť požiadaviek zdravotník / občan

Očakávania zdravotníkov (vysoká úroveň dostupnosti):

Správne informácie v správny čas na správnom mieste pre každého zdravotníka.

Predstavy mnohých občanov (vysoká úroveň dôvernosti):

Nikomu nič neposkytnúť, aby nedošlo k úniku mojich osobných údajov, alebo aspoň absolútne dokonalé zabezpečenie.

Otázka:

Čo je vyššou prioritou pre onkologického pacienta?

Vymedzenie bezpečnosti eHealth / eSO1

Každá oblasť bezpečnosti je vymedzená:

- Chránenými aktívami
- Hrozbami pre aktíva
- Rizikami vyplývajúcimi z daných hrozieb
  - Riziká sú podmienené dopadmi hrozieb, zraniteľnosťami a možnosťami realizácie hrozieb
- Protiopatreniami na zníženie rizík
  - Znížením možností nastania hrozby
  - Znížením dopadov v prípade nastania hrozby

Aktíva v eHealth

Non-IT aktíva

- **Zdravie občanov** (vysoká úroveň dostupnosti)
- Zdroje občanov (čas, financie)
- Zdroje poskytovateľov ZS (čas zdravotníkov, energie, priestory, lieky, prístroje, financie)
- Zdroje ZP (financie)

IT aktíva

- **Zdravotné záznamy občanov** (vysoká úroveň dôvernosti)
- eHealth služby
- IS podporujúce eHealth služby
- Infraštruktúra pre IS eHealth, ...

Základné atribúty IT bezpečnosti

Najčastejšia otázka, týkajúca sa prístupu neoprávnenej osoby k zdravotným záznamom občana, sa týka len jedného z troch základných atribútov bezpečnosti. Aj ďalšie sú podstatné.

Základné atribúty, ktoré musia byť presadené pri tvorbe bezpečnostného riešenia pre eHealth systém sú:

- **Dôvernosť**: dáta v rámci informačného systému nie sú dostupné, odovzdávané alebo prezradzované neoprávneným subjektom.
- **Dostupnosť**: potrebné dáta sú prístupné v prijateľnom časovom intervale a použiteľné požadovaným spôsobom.
- **Integrita**: dáta v rámci informačného systému nie je možné zmeniť neautorizovaným spôsobom.

Plus atribúty ako neodmietnuteľnosť, auditovateľnosť, spoľahlivosť.

Narušenie atribútov bezpečnosti v eHealth

- Narušenie akéhokoľvek atribútu bezpečnosti, čo i len v malom meradle, môže mať ďalekosiahlé následky.
- **Jeden bezpečnostný incident môže znehodnotiť celé riešenie.**

- **Narušenie dôvernosti**, napr.: časť zdravotných záznamov občana bola sprístupnená neautorizovaným osobám alebo zverejnená, môže byť verenosťou interpretované ako: zdravotné záznamy občanov budú zvrejnené na internete.

- **Narušenie dostupnosti**, napr.: výpadok internetu u lekára v ambulancii, môže byť verejnosťou interpretované ako: informačné systémy zlyhajú v kritických okamihoch a budú umierať pacienti.

- **Narušenie integrity**, napr.: v zdravotnom zázname pribudli neznámym spôsobom údaje, môže byť verejnosťou interpretované ako: elektronické dáta môže ktokoľvek akokoľvek zmeniť a sú teda úplne nespoľahlivé

Zdroje požiadaviek na bezpečnosť

- Legislatívne požiadavky vyplývajúce zo zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov.
- Štandardy pre verejnú správu v oblasti bezpečnosti.
- Požiadavky na bezpečnosť uvedené v Štúdiách uskutočniteľnosti programu eHealth a projektu eSO1, zohľadnené aj v ponuke konzorcia
- Architektúra eGovernmentu
- Požiadavky vyplývajúce z Best practices riešení bezpečnosti eHealth iných krajín EÚ.

Bezpečnosť v procese vývoja riešenia

- Pri návrhu riešenia bezpečnosti budú zohľadňované všetky požadované atribúty bezpečnosti.
- Dodržiavanie bezpečnosti bude vynucované od počiatočných fáz vývoja riešenia po všetkých subjektoch.
- Ak budú splnené všetky požiadavky na funkcionalitu riešenia a budú na výber varianty riešenia, rozhodujúce slovo pri výbere varianty má doména Bezpečnosť.
- Ak nastane konflikt návrhu riešenia, ktoré ako jediné spĺňa definovanú funkcionalitu, a bezpečnosti, bude tento konflikt riešený na základe analýzy rizík a rozhodnutia Riadiaceho výboru projektu.

Smerovanie bezpečnostných opatrení

Bezpečnostné opatrenia a mechanizmy sú smerované do oblasti prevencie, detekcie a eliminácie narušení.

Prevencia – antimalware ochrana, hardening počítačov, bezpečná konfigurácia sieťových prvkov, ochranu pred únikom informácií, prvky aplikačnej bezpečnosti.

Detekcia – bezpečnostný monitoring všetkých komponentov informačného systému eSO1 v rámci Bezpečnostného dohľadového centra, anti-malware SW, IDS.

Eliminácia – pripravené plány na obnovu informačného systému eSO1 po narušení.

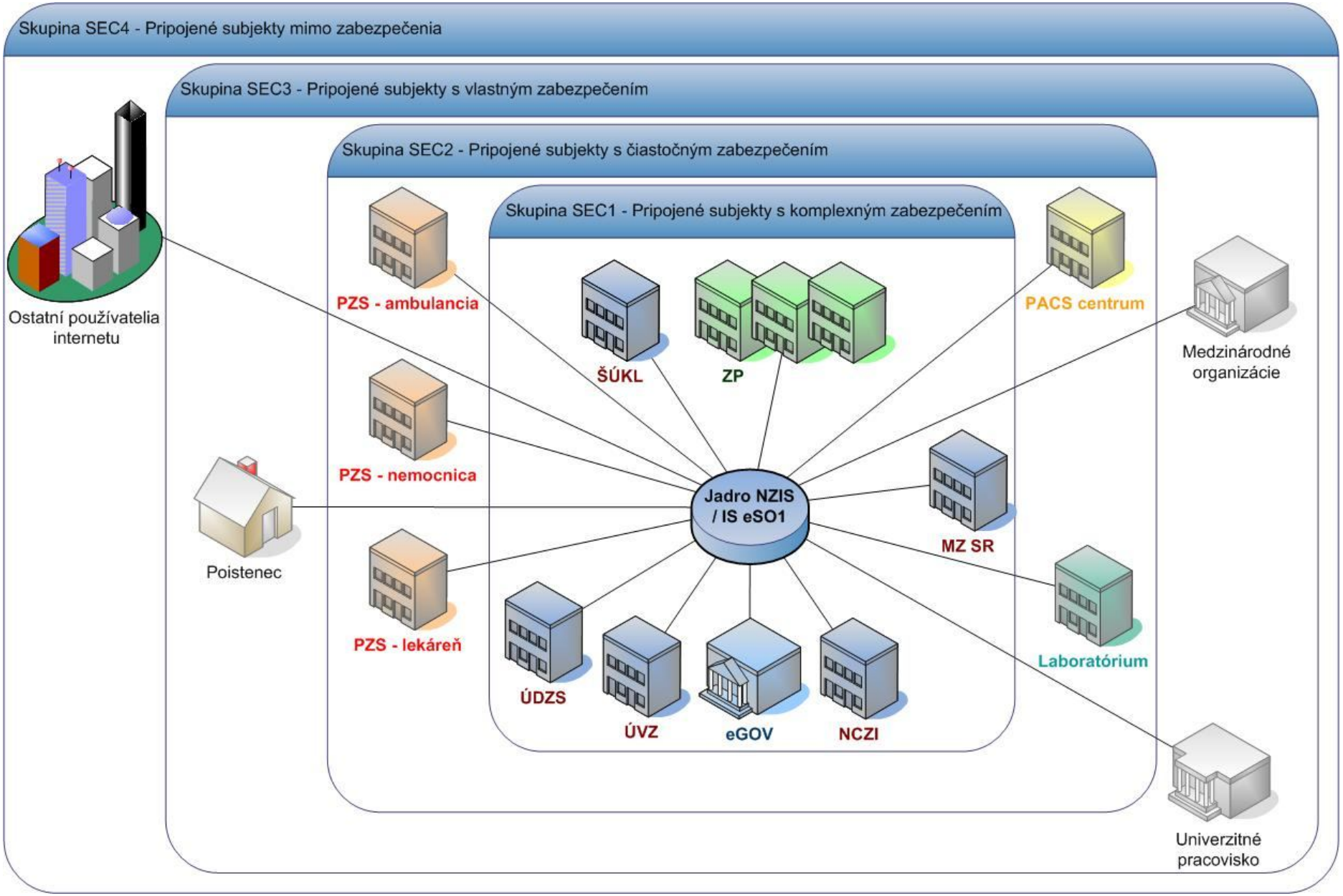
Úroveň zabezpečenia zapojených subjektov

Okrem zabezpečenia samotného informačného systému eSO1 budú zabezpečené aj subjekty, ktoré sa do neho pripájať a budú s ním v interakcii.

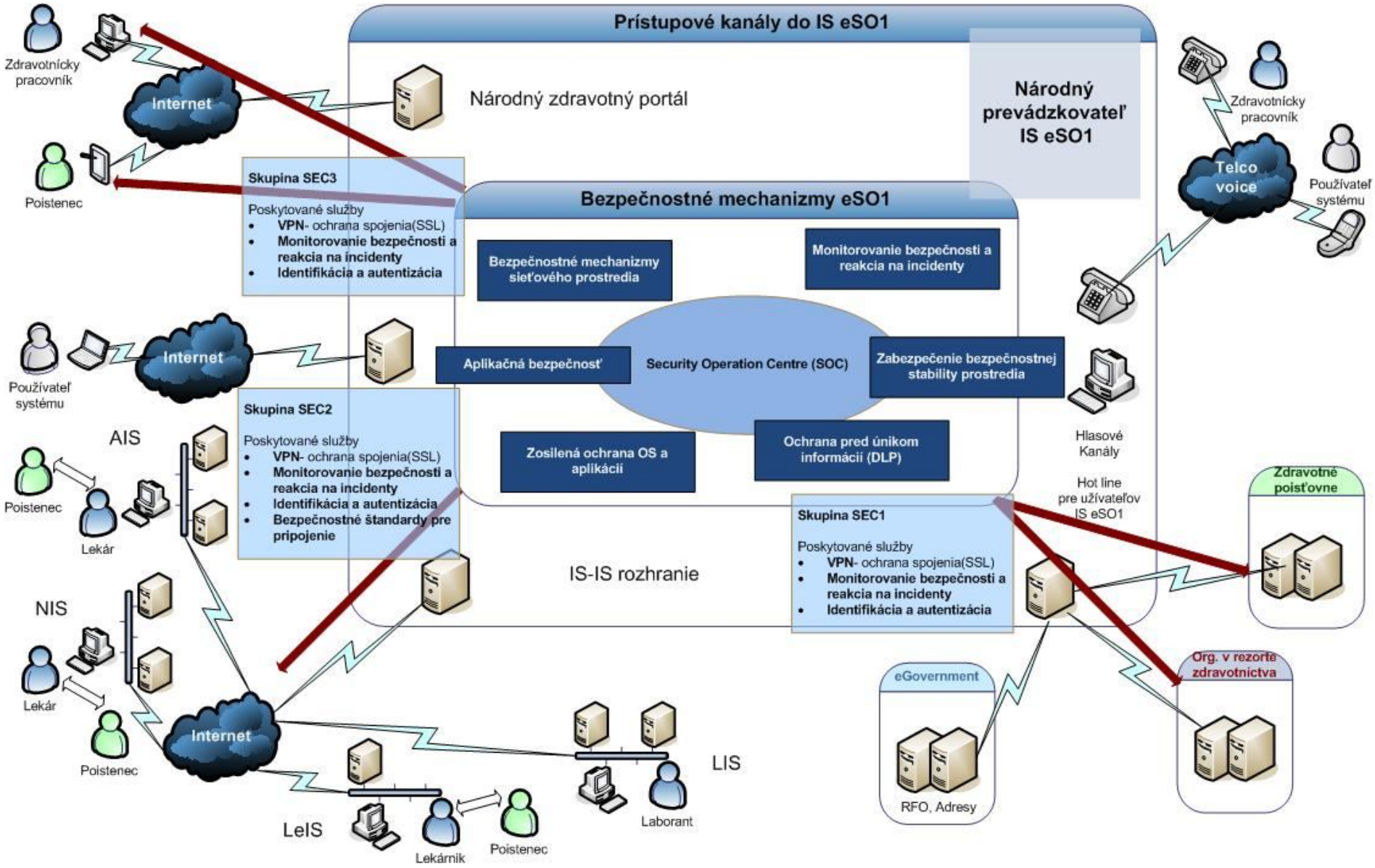
Podľa úrovne zabezpečenia subjekty rozdeľujeme do štyroch skupín:

- Skupina SEC1 – do tejto skupiny patria organizácie rezortu zdravotníctva (MZ SR, NCZI, ÚDZS, ŠÚKL, ÚVZ), zdravotné poisťovne a subjekty eGovernmentu, ich bezpečnosť bude riešená aj v rámci eSO1 a samostatnými bezpečnostnými projektami.
- Skupina SEC2 – do tejto skupiny patria ambulancie, nemocnice, lekárne, laboratória a PACS centrá, ich bezpečnosť bude riešená aj v rámci eSO1 a budú vydané záväzné štandardy pre lokálne informačné systémy týchto subjektov.
- Skupina SEC3 – do tejto skupiny patria všetky subjekty, ktorým budú vytvorené a sprístupnené účty cez NZP, či už sa jedná o samotných poistencov alebo vzdelávacie organizácie či medzinárodné organizácie, subjekty z tejto skupiny budú v rámci projektu eSO1 čiastočne zabezpečené.
- Skupina SEC4 – do tejto skupiny patria všetci ostatní používatelia internetu, ktorí budú IS eSO1 používať len anonymne.

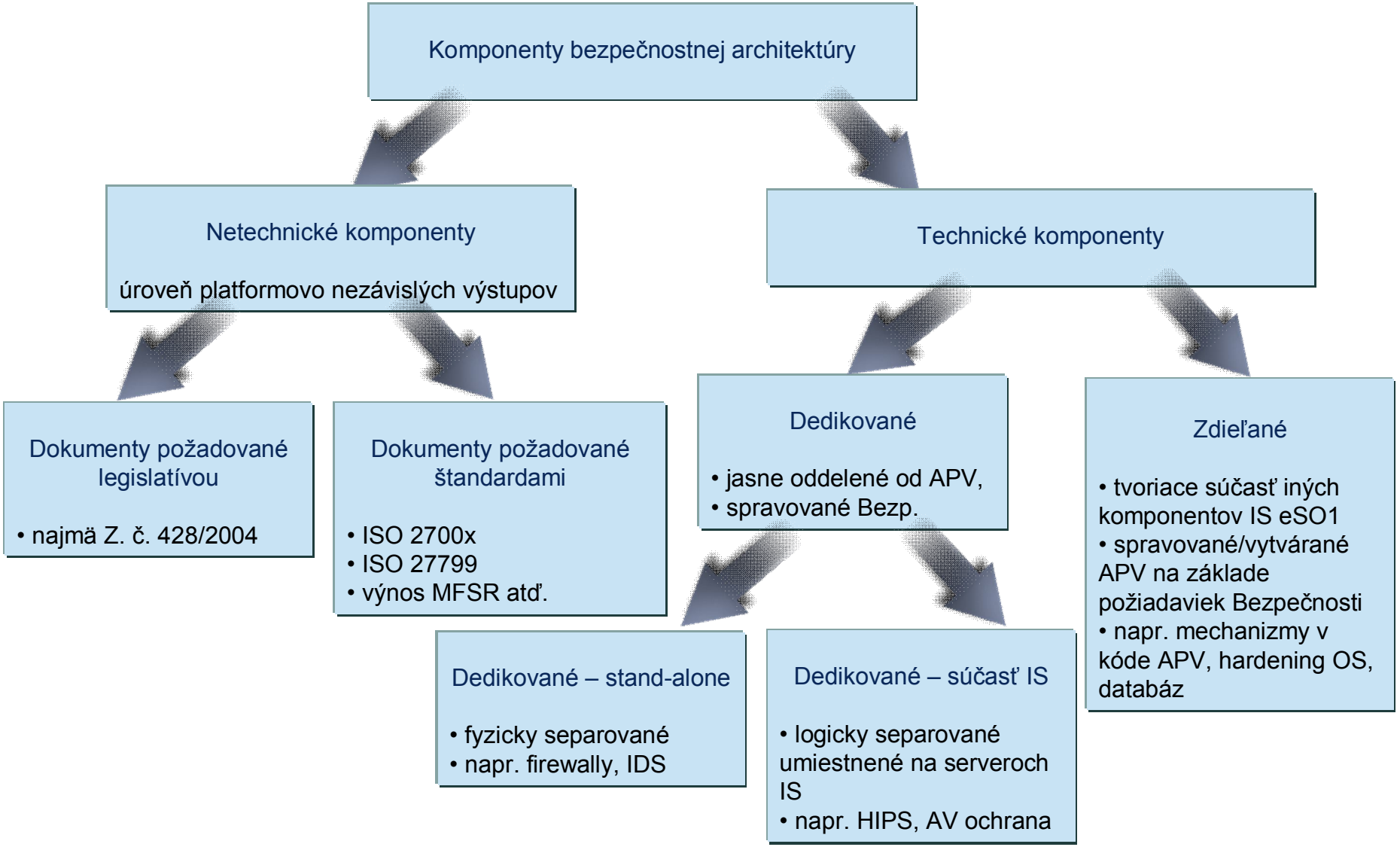
Skupiny subjektov podľa zabezpečenia



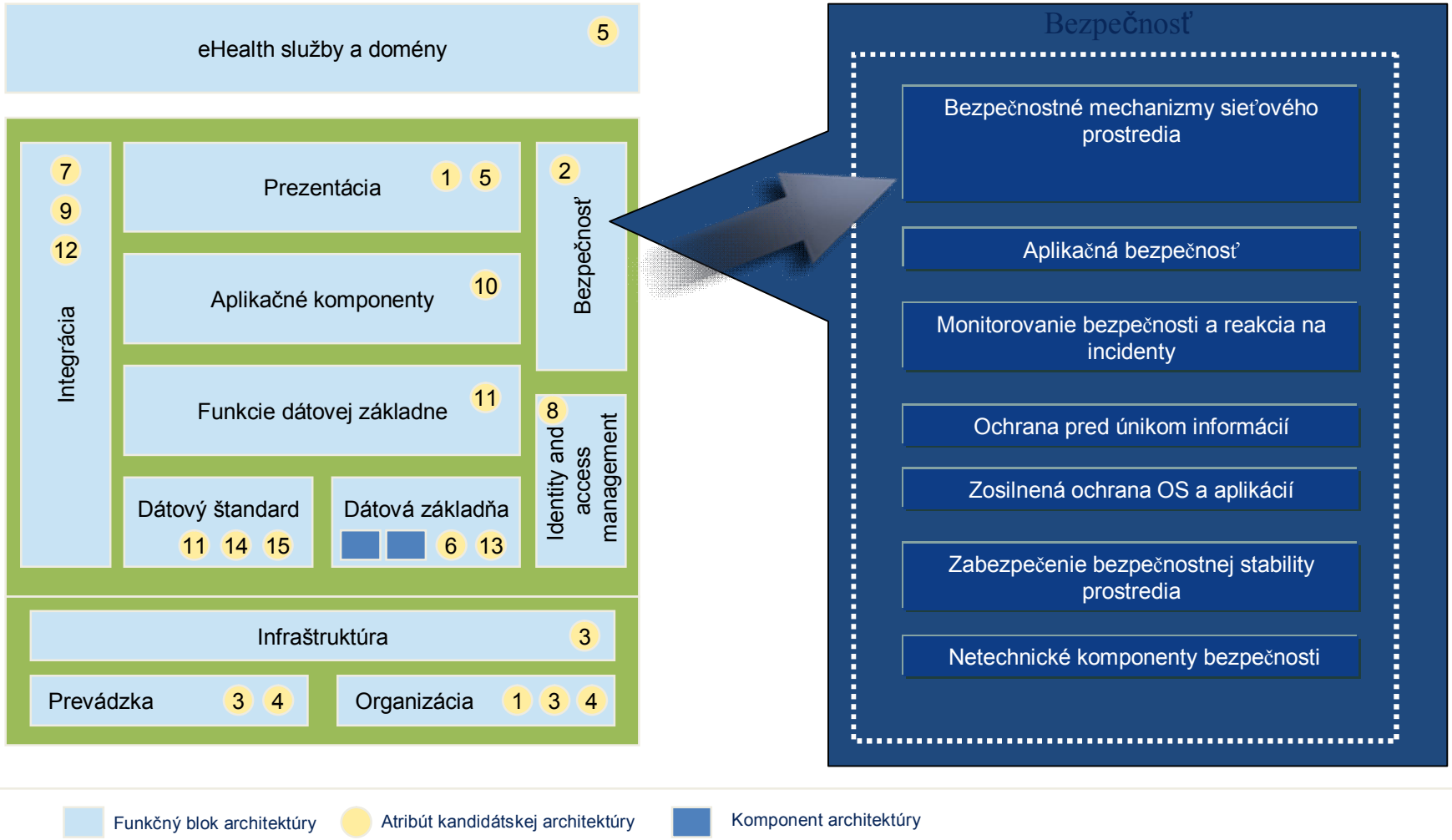
Ochrana subjektov v rámci eSO1



Základné typy komponentov bezpečnosti



Bezpečnosť – vybrané oblasti riešenia



Bezpečnosť- vybrané oblasti riešenia

Zabezpečenie bezpečnostnej stability prostredia

- Predstavuje riešenie v dvoch základných rovinách:
  - Statická –udržanie konfiguračnej stability -nezávislé automatizované mechanizmy pre enforcement a audit zmien
  - Dynamická- udržanie úrovne bezpečnosti vzhľadom na meniace sa vonkajšie hrozby

Sieťová bezpečnosť

- Vytvorenie bezpečnostných zón na úrovni siete mechanizmami, ktoré sú úplne nezávislé od aplikácií
- Dôraz bude kladený na:
  - maximálnu granularitu
  - hĺbkovú aplikačnú inšpekciu
- Vytvorenie šifrovaných komunikačných kanálov

Aplikačná bezpečnosť

- Implementácia bezpečnostných prvkov do vyvíjaného softvéru od ranných štádií
- Vytvorenie architektúry APV s dôrazom na bezpečnostné aspekty

Bezpečnosť- vybrané oblasti riešenia

Zosilnená ochrana OS a COTS aplikácií

- Použitie renomovaných štandardov (DISA, NIST,NSA) pre zvýšenie bezpečnosti
- Použitie host-based dedikovaných bezpečnostných prvkov

Monitorovanie bezpečnosti

- Zabezpečenie bezpečnostného monitorovania eSO1 pomocou SIEM
- CIRT capability

Ochrana pred únikom informácií

- Implementácia špecializovaných mechanizmov priamo do APV komponentov
- Implementácia dedikovaných nezávislých bezpečnostných mechanizmov

Netechnické komponenty bezpečnosti

Cieľ

- Splniť legislatívne požiadavky a implementovať systém riadenia informačnej bezpečnosti

Rozsah činností

- Vytvorenie platformovo nezávislých výstupov (riadiace dokumenty IB, nadväzné dokumenty), vrátane výstupov požadovaných legislatívou najmä Zákonom o ochrane osobných údajov (bezpečnostný projekt, zámer...).
- Vytvorenie šablón pre ostatné domény pre platformovo závislé výstupy.
- Spracovanie analýzy rizík a jej priebežná aktualizácia.
- Kontrola dodržiavania definovaných pravidiel bezpečnosti.

Ďakujem za pozornosť