

eHealth

nová dimenzia v starostlivosti o Vaše zdravie



Európsky fond regionálneho rozvoja
„Tvoríme vedomostnú spoločnosť“

Projekt je spolufinancovaný Európskou úniou



Bezpečnosť eHealth a eSO1

ITAPA, október 2011

RNDr. Michal Danilák
tím eSO1

Čo je eHealth a čo je predmetom jeho bezpečnosti?

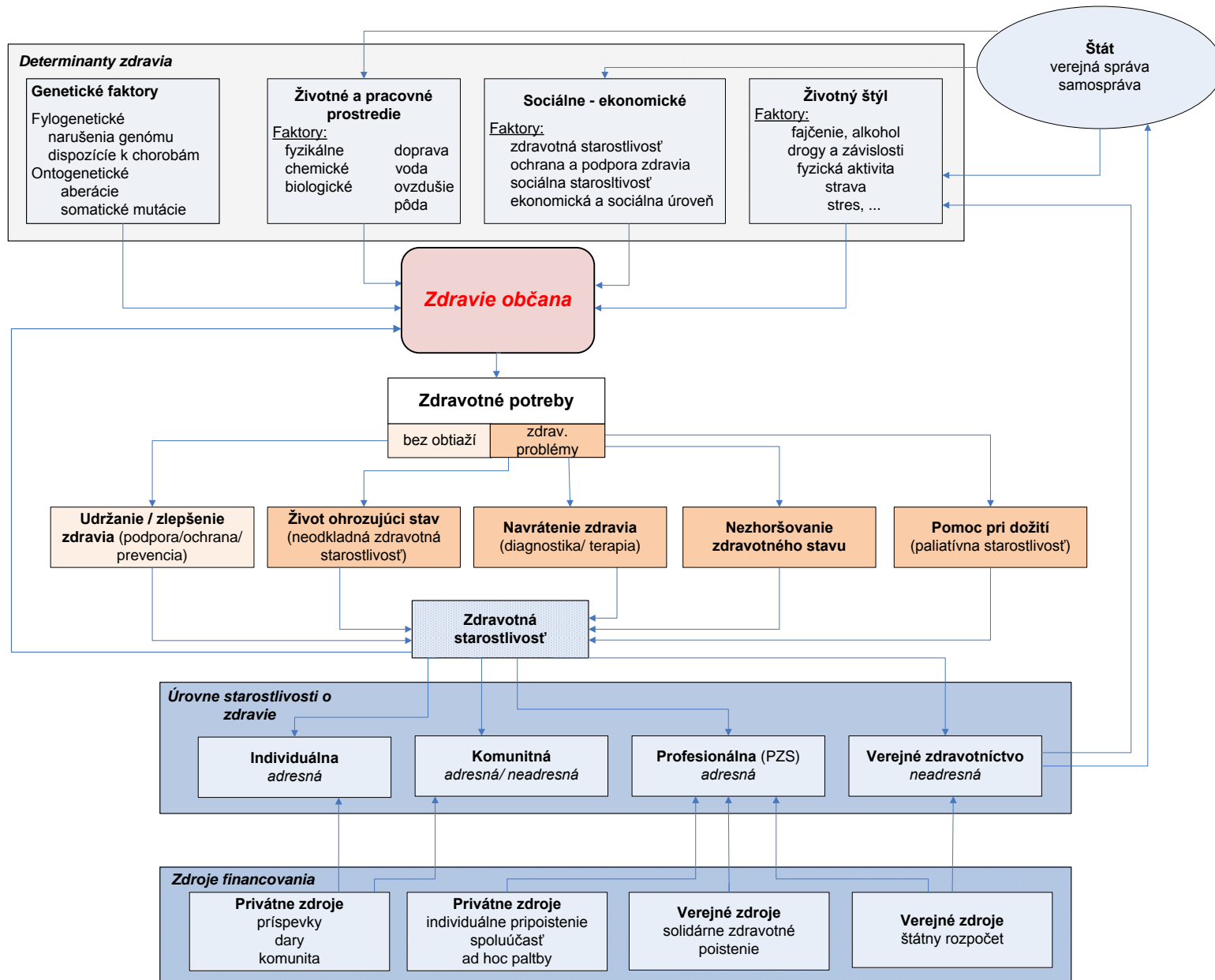


Poslaním zdravotníctva je významne prispievať k zvyšovaniu kvality života občanov prostredníctvom znižovania úmrtnosti, chorobnosti, trvalých a dočasných následkov chorôb a úrazov; poskytovaním zdravotnej starostlivosti, pôsobením verejného zdravotníctva, podporou individuálnej a komunitnej starostlivosti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

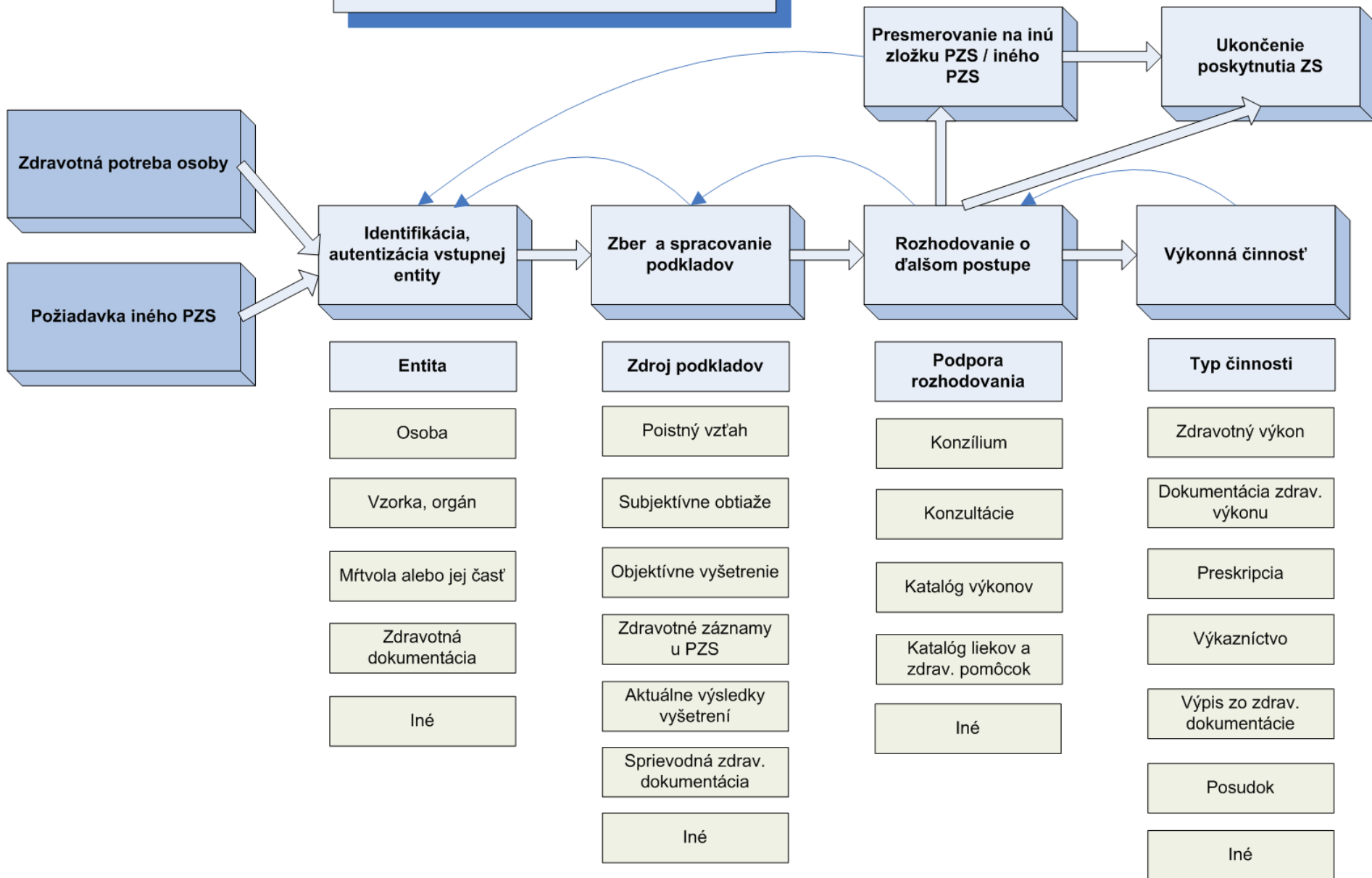
Poslaním elektronického zdravotníctva (eHealth) je podpora poslania zdravotníctva prostredníctvom informačných a komunikačných technológií.

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

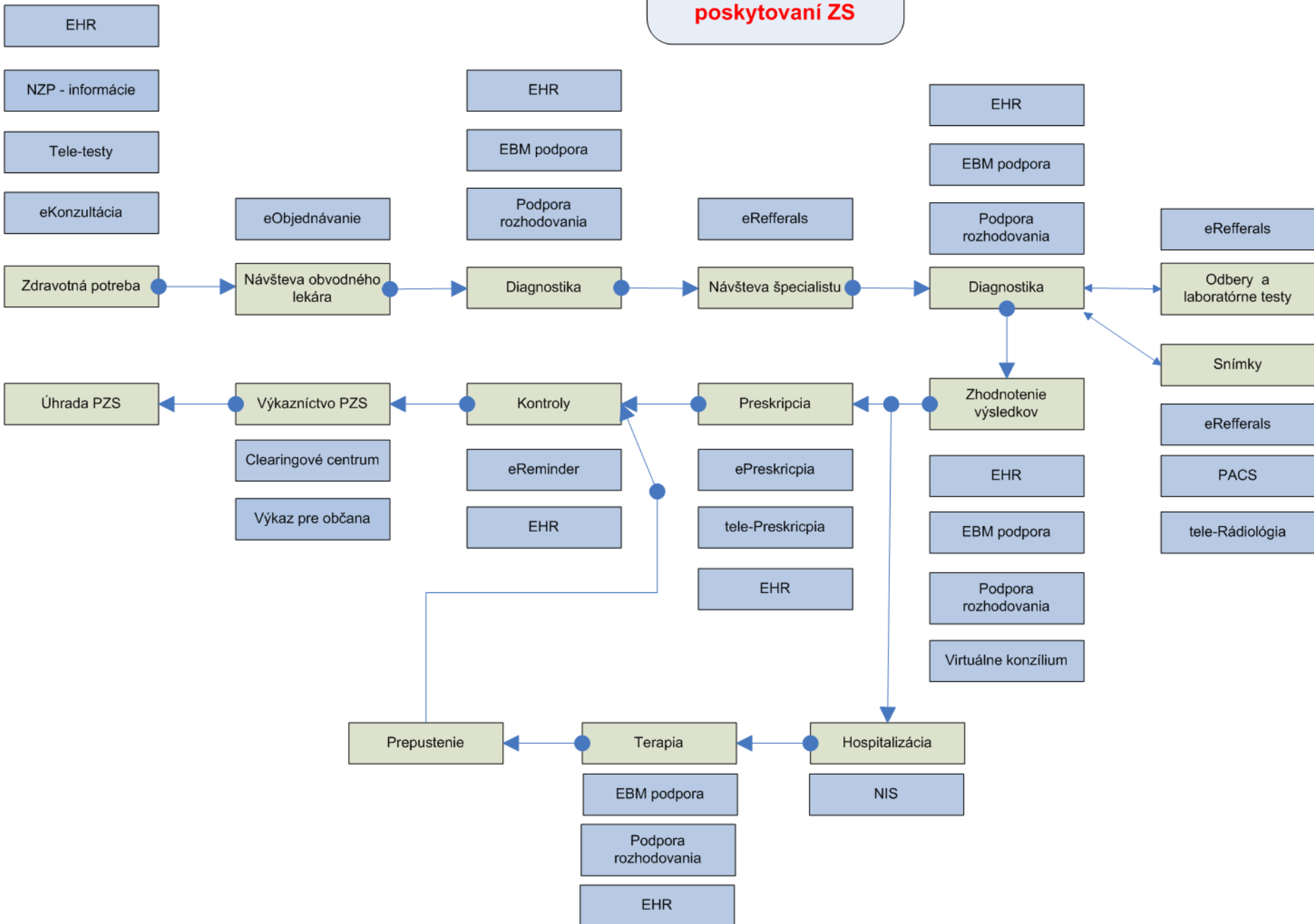
Model starostlivosti o zdravie



Štandardné poskytovanie ZS



Podpora eHealth pri poskytovaní ZS



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 súčasnosti 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):

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

Otázka:

Čo je vyššou prioritou pre onkologického pacienta?

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

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, ...

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:

- **Dôvernost'**: dáta v rámci informačného systému nie sú dostupné, odovzdávané alebo prezradzované neoprávneným subjektom.
- **Dostupnost'**: 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 verejnosťou interpretované ako: zdravotné záznamy občanov budú zverejnené na internete.
- **Narušenie dostupnosti**, napr.: výpadok internetu u lekára v ambulancii, môže byť verejnosťou interpretované ako: informačné systémy zlyhávajú 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

- 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 počiatkových fáz vývoja riešenia po všetkých subjektoch.
- Ak budú splnené všetky požiadavky na funkcionality 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 funkcionality, 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 pripájajú 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, ŠUKL, 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.

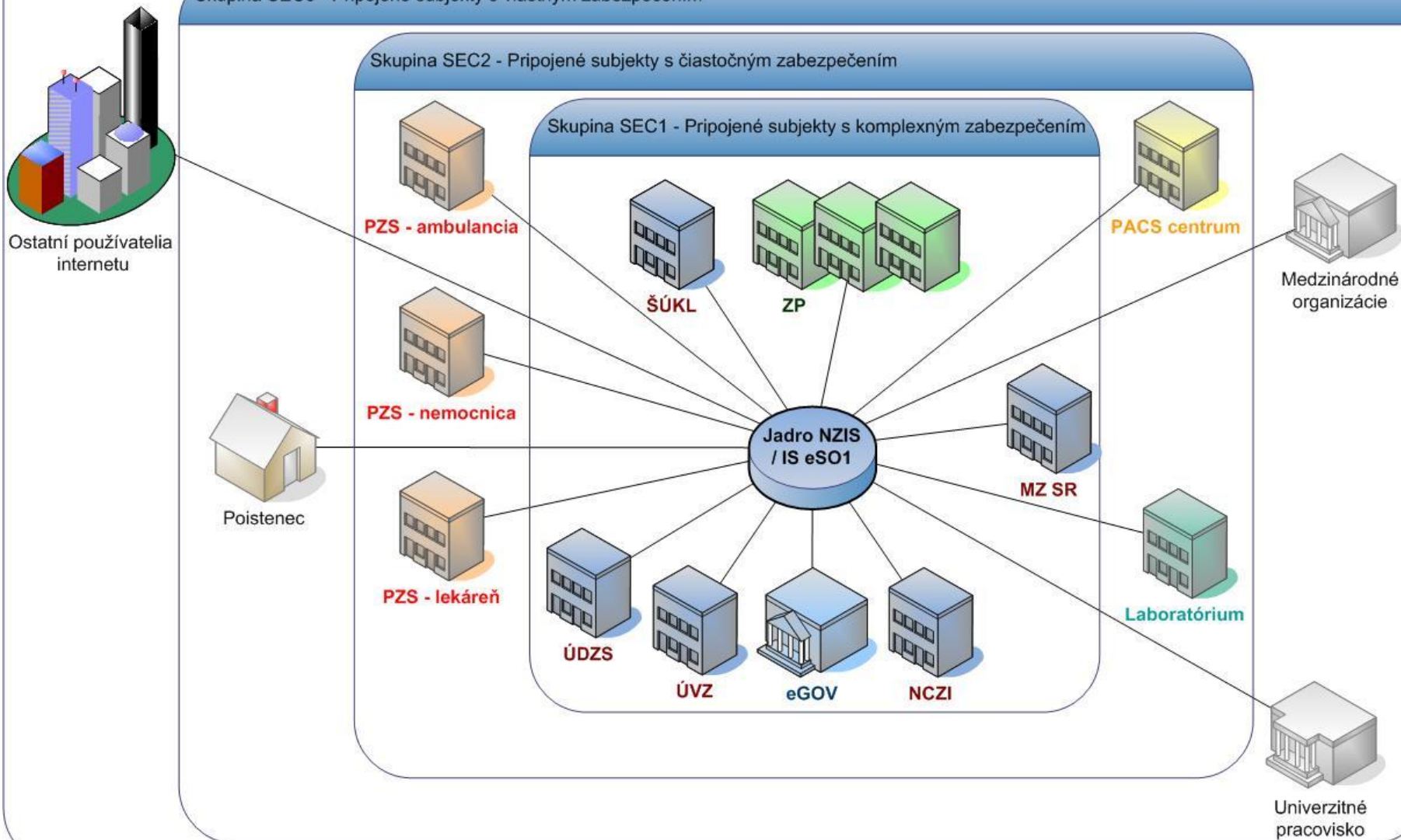
Skupiny subjektov podľa zabezpečenia

Skupina SEC4 - Pripojené subjekty mimo zabezpečenia

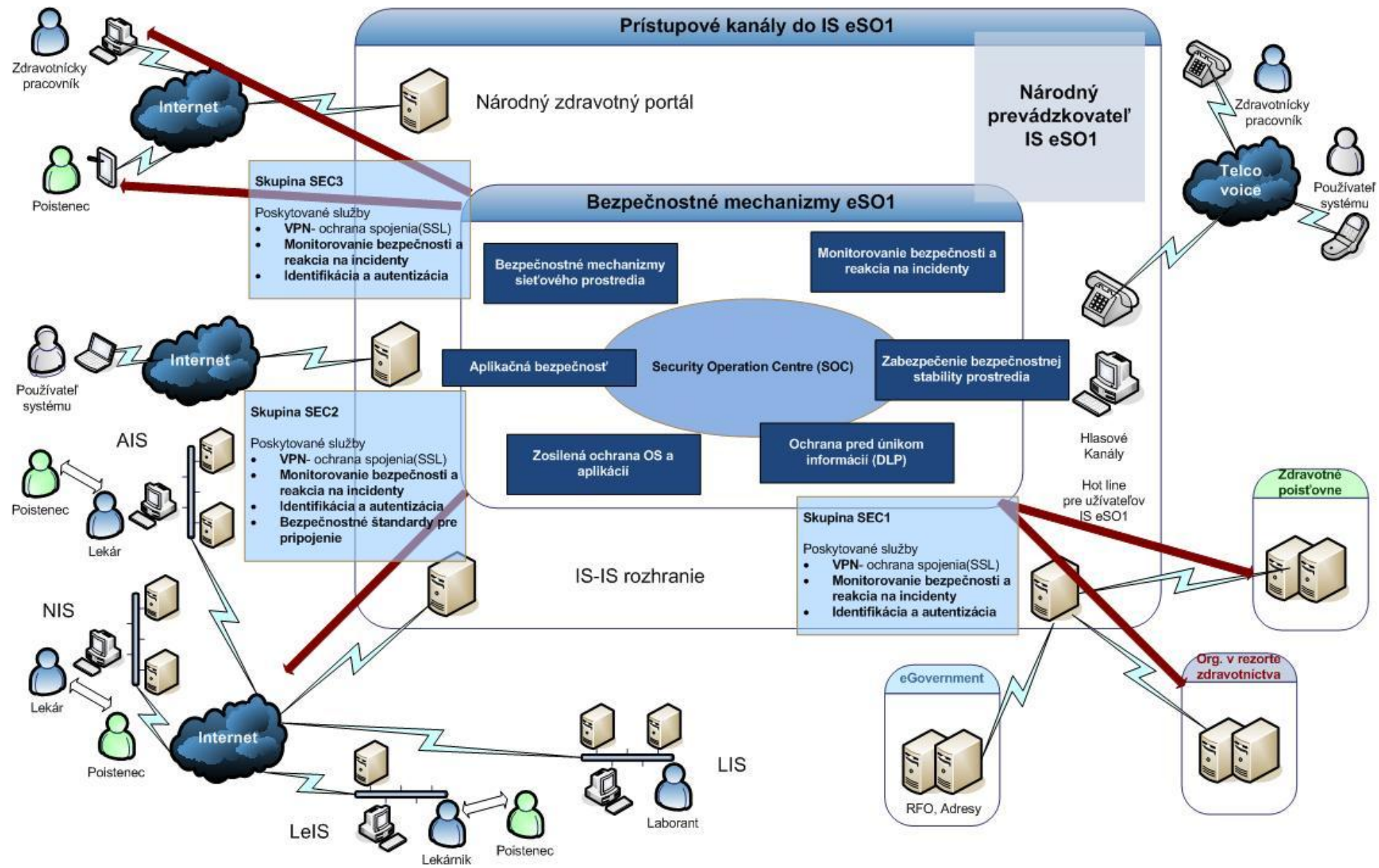
Skupina SEC3 - Pripojené subjekty s vlastným zabezpečením

Skupina SEC2 - Pripojené subjekty s čiastočným zabezpečením

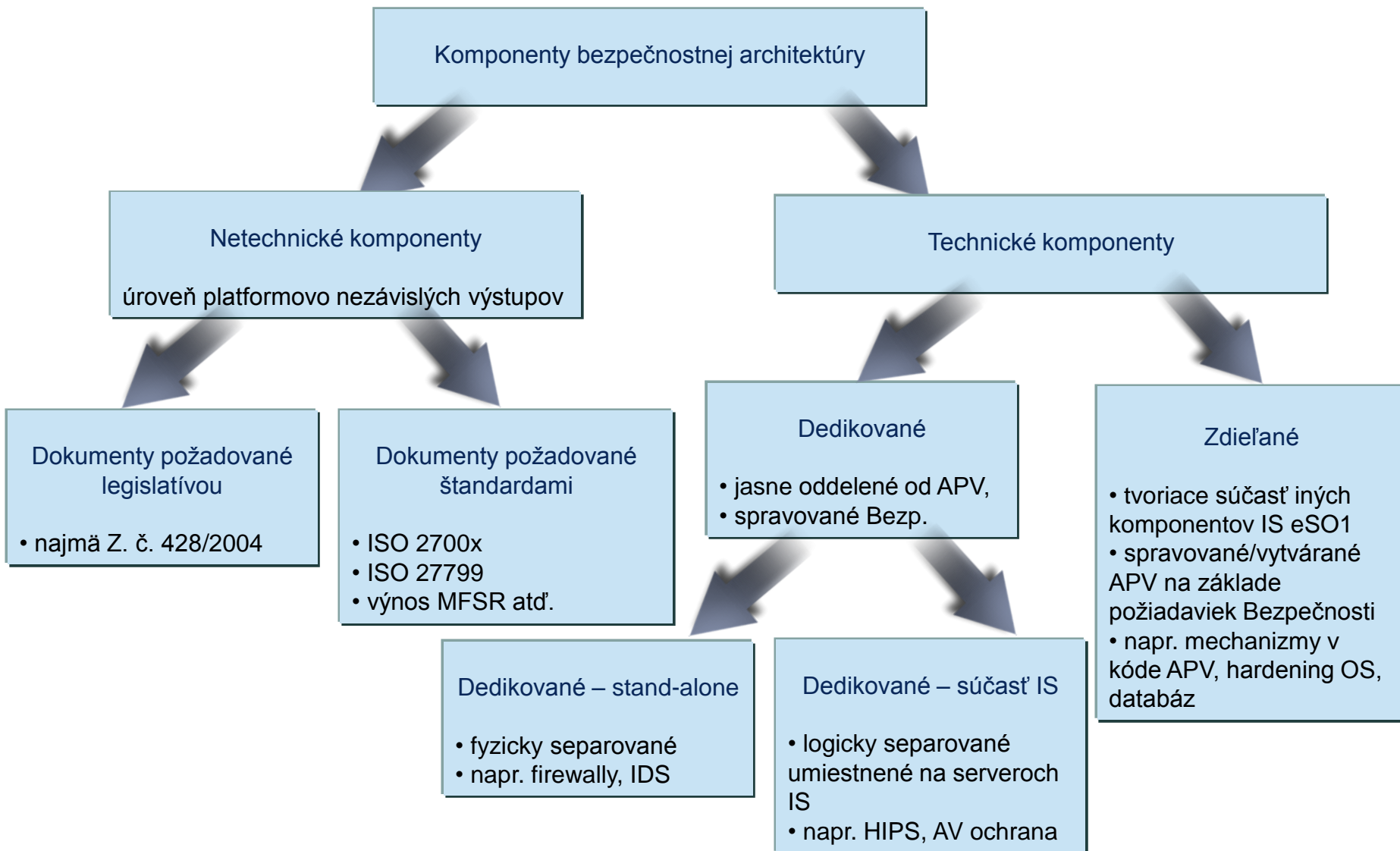
Skupina SEC1 - Pripojené subjekty s komplexným zabezpečením



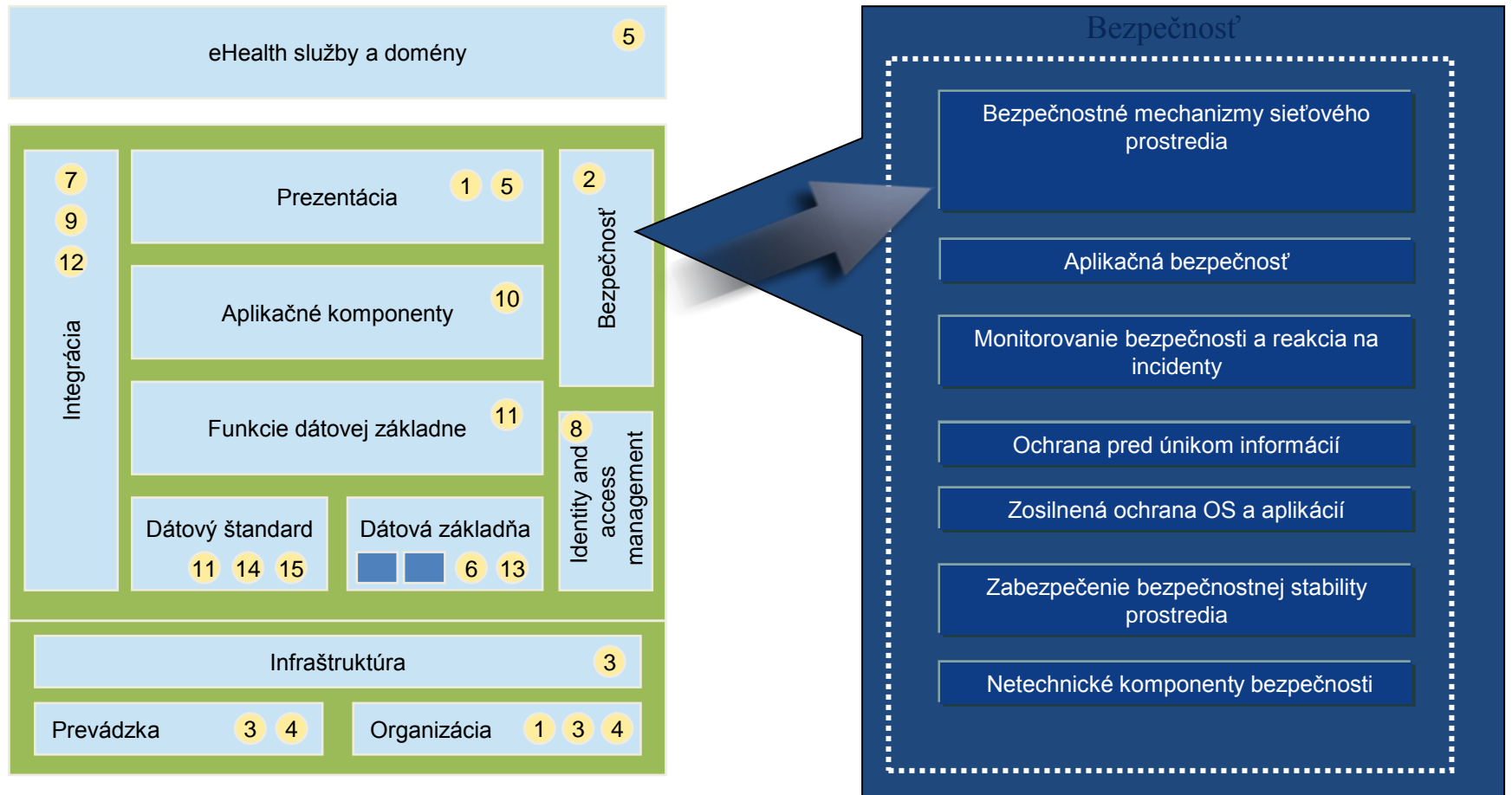
Ochrana subjektov v rámci eSO1



Základné typy komponentov bezpečnosti



Bezpečnosť – vybrané oblasti riešenia



■ Funkčný blok architektúry

● Atribút kandidátskej architektúry

■ Komponent architektúry

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, nadväznú 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