Sdílené služby eGOV ČR 2016 a CMS 2.0

Ondřej Felix

MV ČR

Telč 2016

Proč sdílené služby eGOV

- Proč pro efektivní výkon veřejné správy potřebujeme bezpečné, transparentní a logicky centralizované aplikační služby
- Proč pro provoz logicky centralizovaných aplikací potřebujeme služby privátního cloudu
- Proč pro bezpečný provoz privátního sloudu VS potřebujeme bezpečnou sdílenou privátní komunikační infrastrukturu

Protože jinak si to bude každý zabezpečovat po svém a budeme plýtvat prostředky

Čtyřvrstvá architektura sdílených služeb eGOV

- Služby veřejné správy – např. Zápis do živnostenského rejstříku
- Služby aplikací – např. služby ISZR pro čtenářské AISy
- Služby platforem – např. služby bezpečnostního dohledu
- Služby komunikační infrastruktury a datových center - např. služba vytvoření přístupové VPN z přípojek KIVS

Sdílení služeb v kontextu veřejné správy ČR – poskytovatel služby službu poskytuje v rámci své zákonné kompetence, ostatní službu využívají v rámci svých zákonných kompetencí

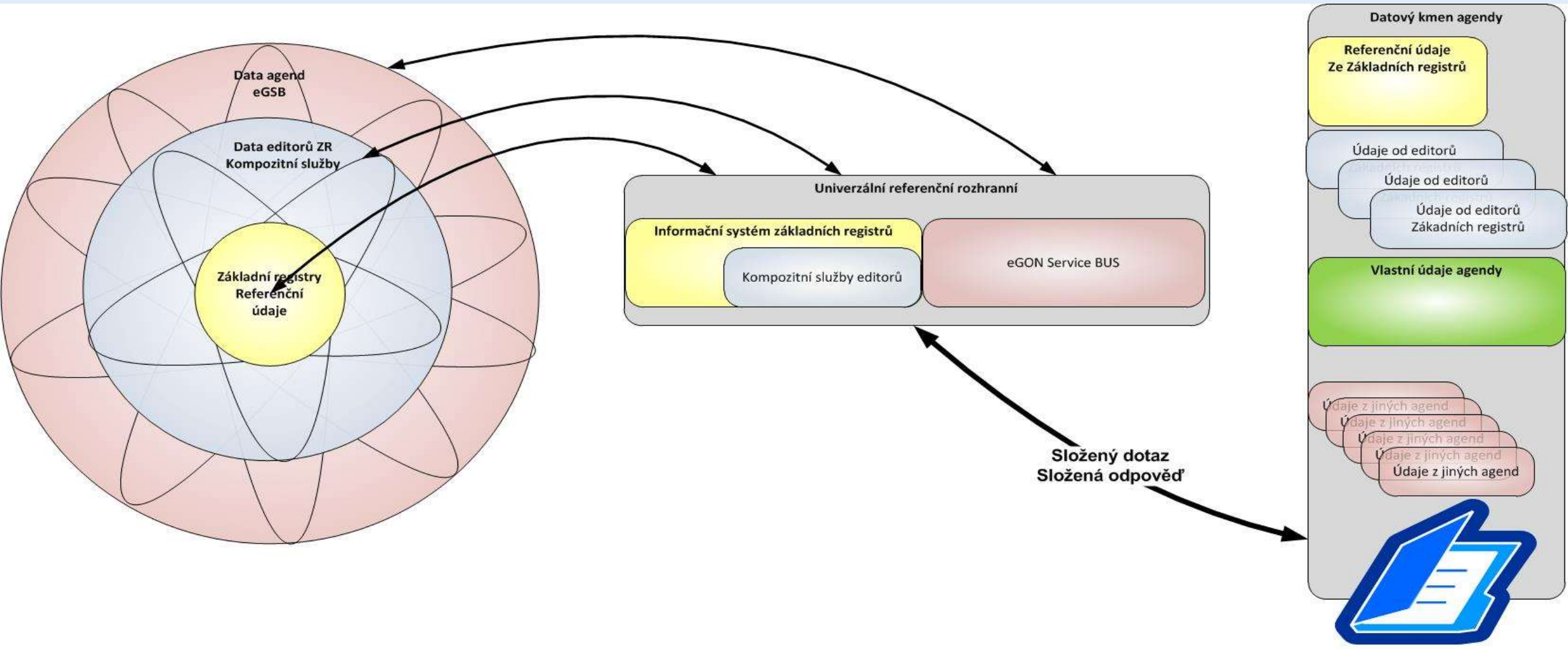
Principy sdílení údajů mezi AIS

- Využívání referenčních údajů ze Základních registrů
- Využívání nereferenčních údajů editorů ZR
- Využívání nereferenčních údajů z dalších autoritativních zdrojů
- Sdílení údajů zdrojové Agendy s ostatními Agendami na základě zákonné kompetence
- Poskytování údajů subjektu údajů – právo subjektu údajů na informace o sobě
- Údaje se sdílí publikací služby v propojeném datovém fondu
- Veřejné údaje se sdílí s využitím konceptu open dat

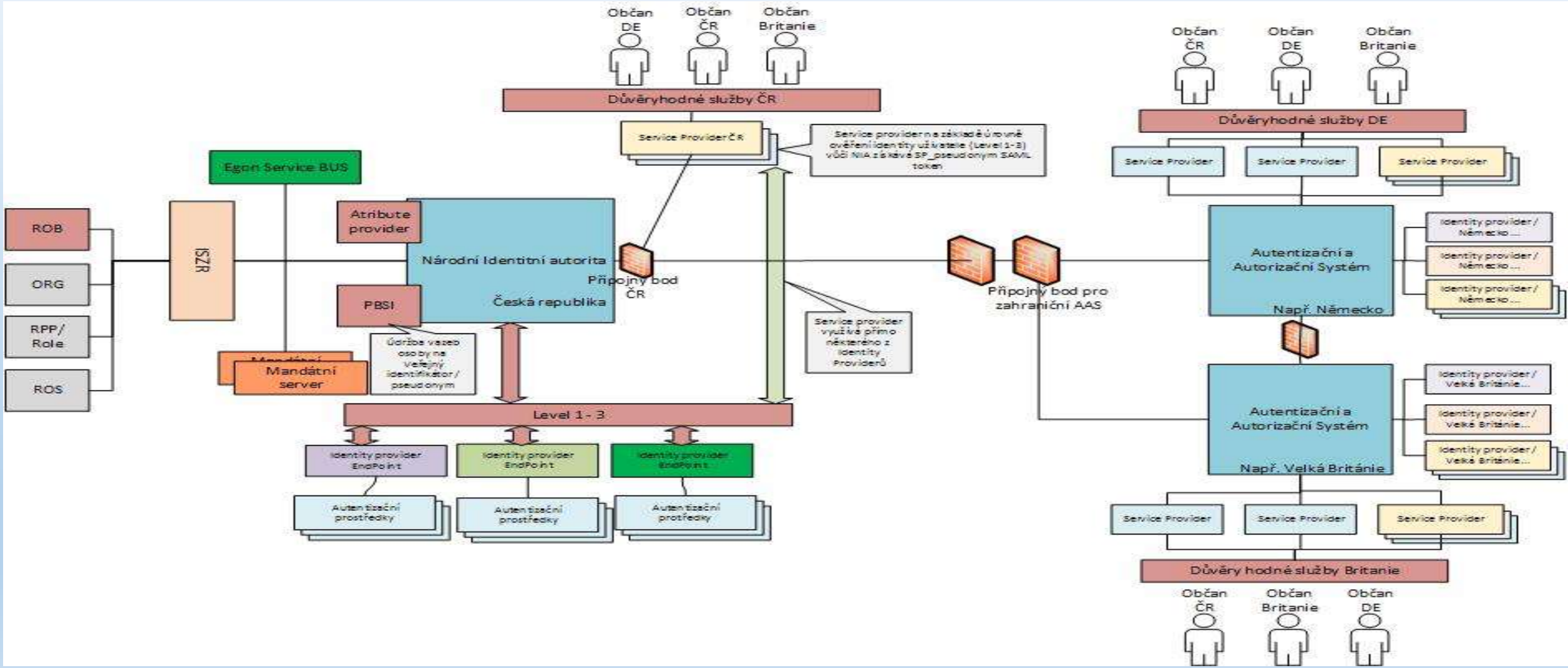
Služby Propojeného datového fondu

- Základní registry přes služby ISZR referenční údaje poskytují, AISy využívají podle zákonných zmocnění
- Služby editorů základních registrů přes ISZR nereferenční údaje poskytují, AISY využívají podle zákonných zmocnění
- Služby autoritativních zdrojů údajů přes EGSB nereferenční údaje poskytují, AISy využívají podle zákonných zmocnění
- Propojený datový fond poskytuje údaje Portálu občana a NIA, občané a firmy využívají podle svých práv na svoje údaje

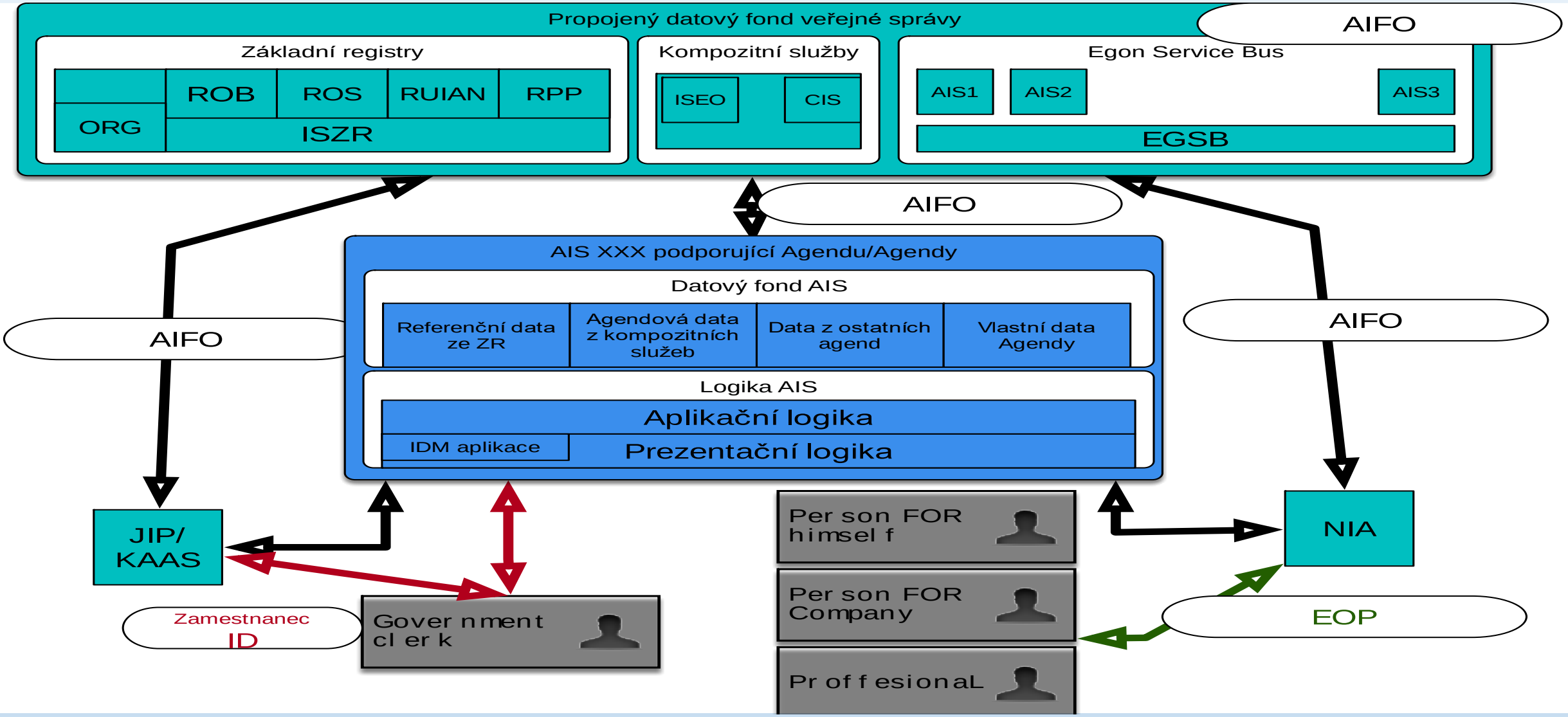
Služby Propojeného datového fondu



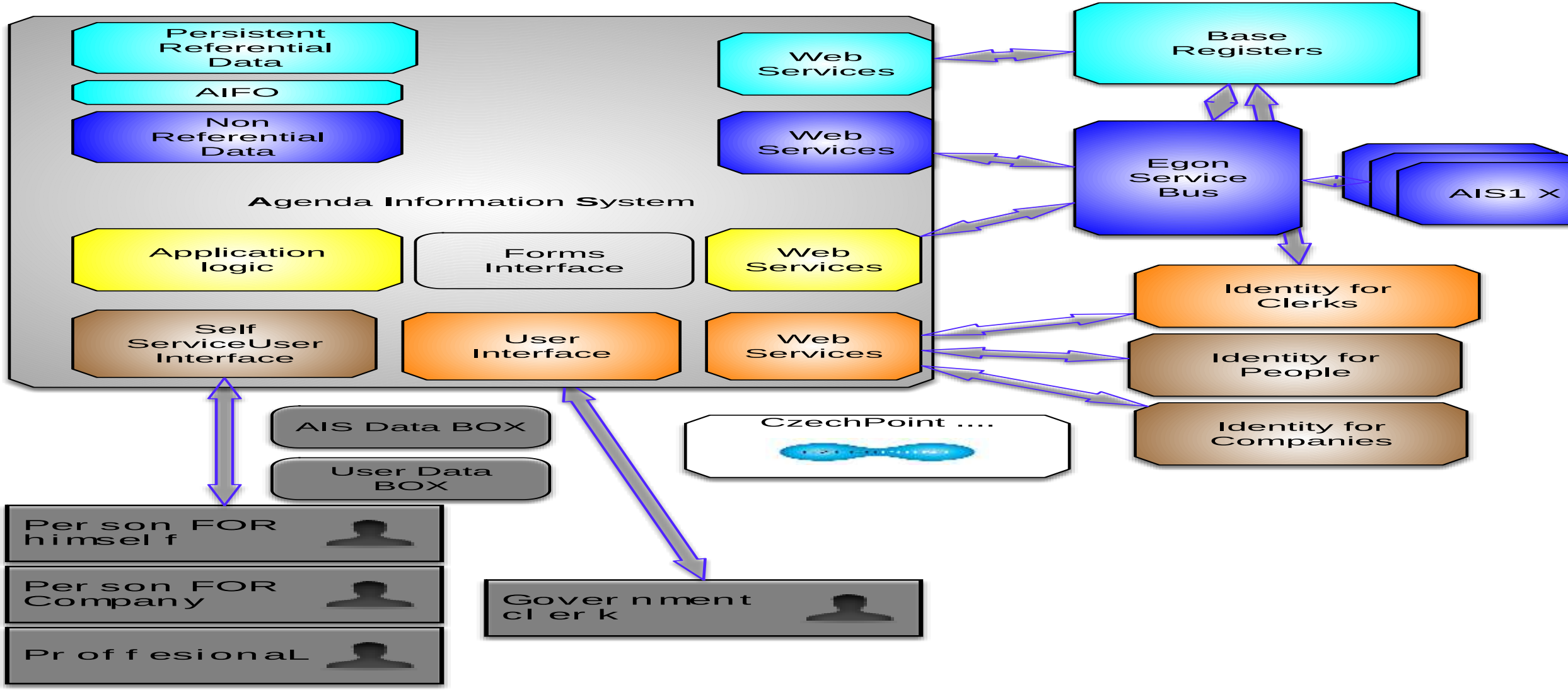
Služby Propojeného datového fondu pro služby NIA



Služby PPDF, NIA, JIP/KAAS pro AISy



AIS využívající sdílené služby



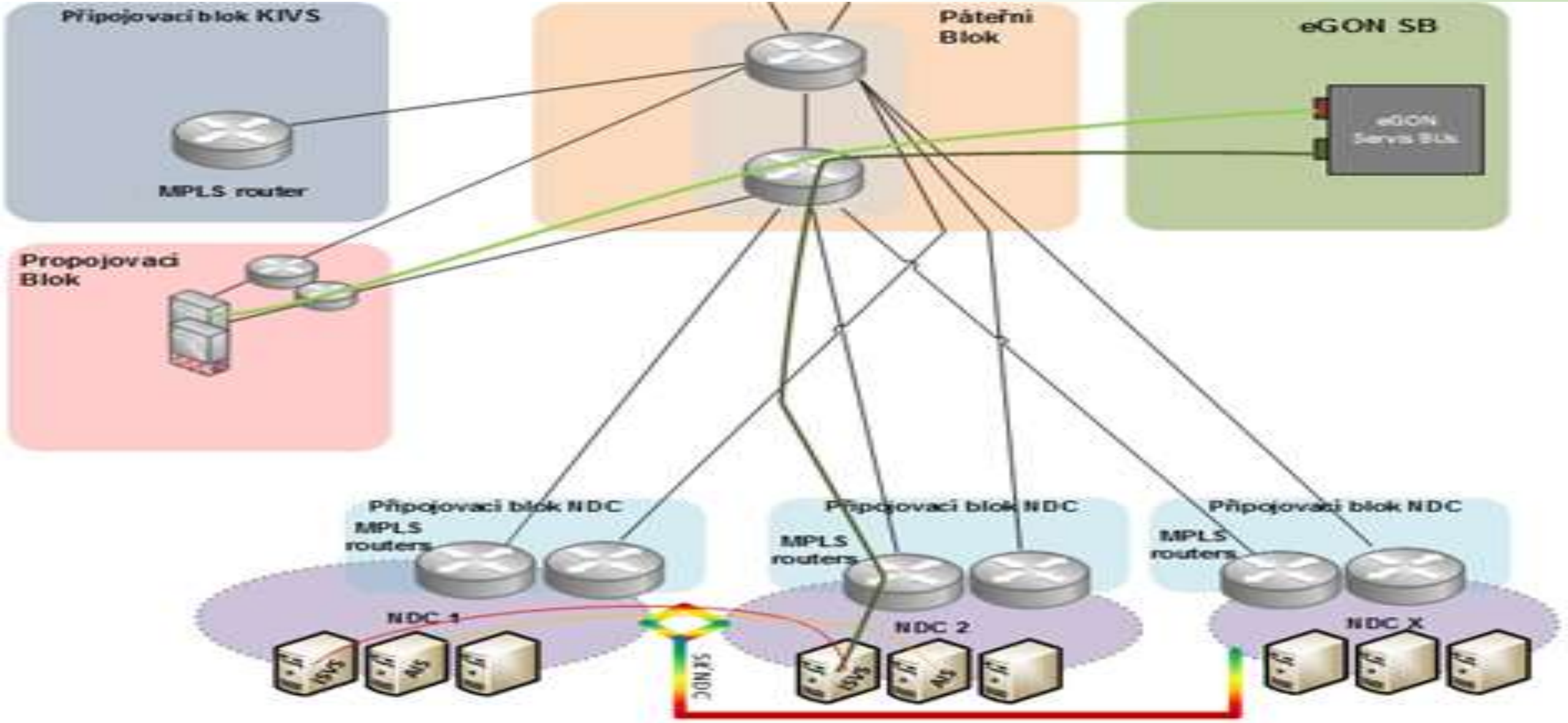
Komunikační Infrastruktura Veřejné Správy

- Služba bezpečného (vyhrazeného) komunikačního kanálu z lokality A do lokality B s parametry definovanými příslušným SLA
- Z jednotlivých přípojek vzniká privátní síť veřejné správy jako bezpečný komunikačního základ privátního cloudu veřejné správy
- Služby bezpečné přípojky si zajišťuje prostřednictvím dynamického nákupního systému ve správě MV koncové OVM
- Pro bezpečné přípojky si na portálu CMS 2.0 objednává koncové OVM jejich využití

Služby centrálního místa služeb KIVS v. 2 (opakování matka moudrosti)

- Čtyři prostředí (Internet, sTESTA, KIVS, eGON služby)
- Krajské konektory a páteř republikou
- Připojení regionálních sítí
- Definice služeb podle eTOM

Základní architektura CMS 2.0



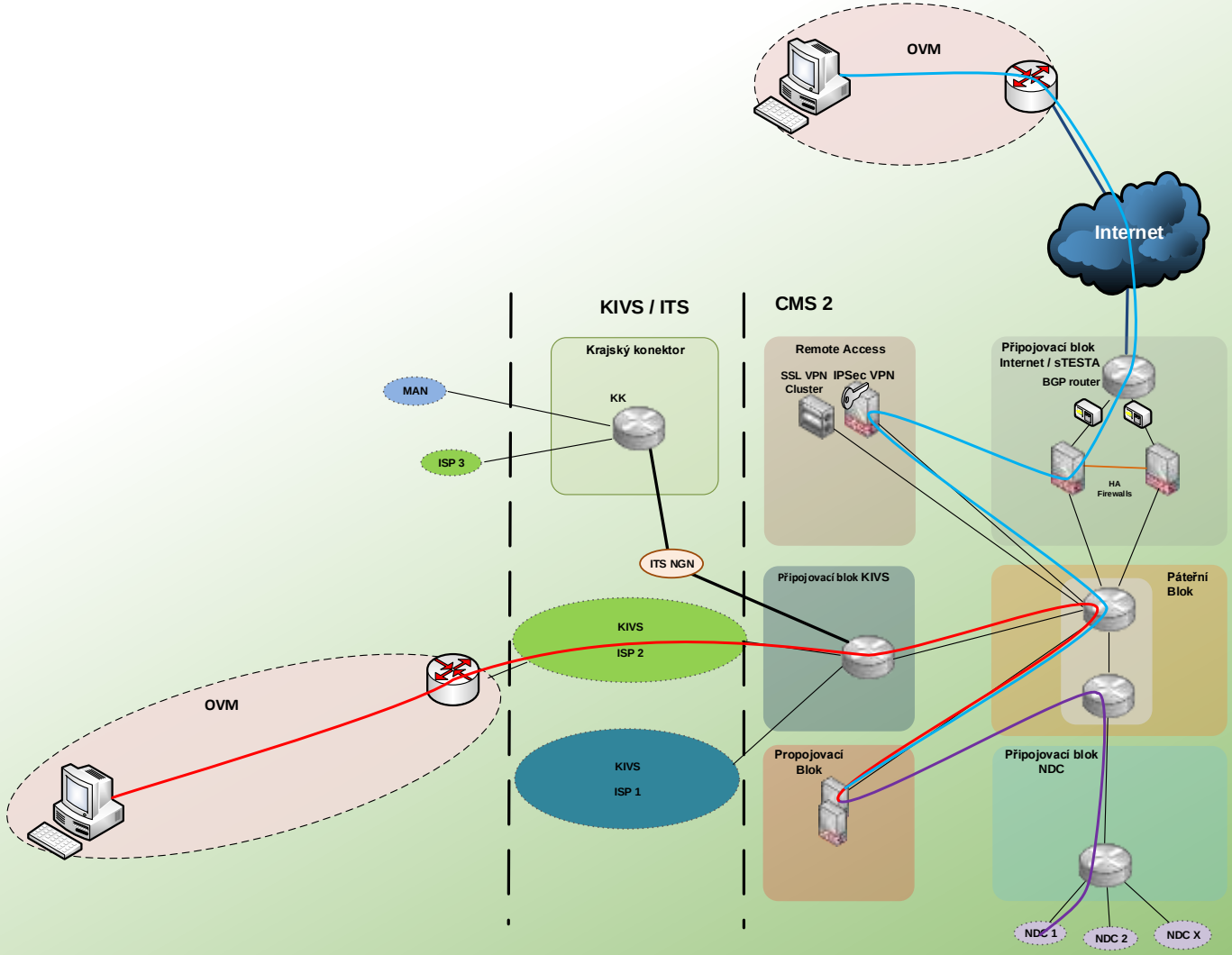
Správa služeb OVM v CMS 2.0

- OVM vysloví souhlas s podmínkami používání CMS
  - OVM zašle správci CMS žádost datovou schránkou
  - Správce CMS povolí v JIP přístup uživatelů z OVM k Portálu a Provisioningu CMS
  - Správce CMS vrátí schválení do datové schránky OVM
- Správa dalších služeb přes Portál CMS
  - Portál autentizuje uživatele OVM vůči JIP
  - Portál a Provisioning autorizují požadavky uživatele vůči JIP

Připojení OVM k CMS 2.0

- Připojení OVM k CMS, lze připojit:
  - lokalitu OVM: přípojkou KIVS nebo IPSec VPN přes Internet
  - skupinu uživatelů OVM: s využitím IPSec VPN nebo SSL VPN přes Internet
- Připojení OVM do Internetu
  - Zabezpečené: inspekce provozu
  - Přímé (nezabezpečené)

Propojení KIVS VPN a IPSec VPN OVM



Prostředí Internet

- Přístup uživatelů z Internetu k aplikačním službám publikovaným z CMS do Internetu
- Připojení lokality OVM k CMS přes Internet s využitím VPN
- Připojení uživatelů OVM k CMS přes Internet s využitím VPN
- Připojení lokality OVM do Internetu přes CMS

Služba CMS „Publikace aplikační služby“

- Definuje správce služby
- Odkud publikovat: KIVS (lokalita), NDC
- Co publikovat: aplikace, služba, IP adresy, port TCP/UDP
- Kam publikovat: KIVS, Internet, eGSB, Extranet
- Pro koho publikovat: veřejná služba, pro kategorii OVM (např. ORP), pro OVM ze seznamu, OVM musí požádat správce služby o přístup
- Podmínky: load balancing, omezení podle IP adres

Služba CMS „Přístup k aplikační službě“

- Přístup ke službě publikované aplikací jiného OVM
- Pravidla pro přístup definuje správce služby
- Správce klientské aplikace rozhodne, zda požádá o přístup
- Odkud lze požadovat přístup: KIVS, Internet, Extranet, eGSB, IPSec/SSL VPN

Služba CMS „Umístění aplikace OVM do NDC“

- Požadavek na umístění instancí aplikace do jednoho nebo více NDC
- Požadavky na konektivitu mezi instancemi
- Žádost o připojení aplikace k CMS
- Kontakty na provozovatele NDC
- Aplikace musí splňovat požadavky na aplikace poskytující centrální eGON služby

Další služby CMS 2.0

- Elektronická pošta
  - Příjem a odesílání zpráv
  - Nezahrnuje poštovní schránky
- Služby Certifikační autority
  - Neveřejná autorita
  - Certifikáty pouze pro připojení IPSec a SSL VPN k CMS
- Služby STESTA
  - Propojení mezi aplikacemi OVM a aplikacemi v síti STESTA

Přístup OVM portálem k vlastním údajům v CMS

- Seznam služeb, historie služeb
- Přístup k záznamům o provozu: plnění SLA, vybrané logy
- Přístup k účtovacím informacím
- Přístup pouze k vlastním záznamům OVM
- Maximálně 12 měsíců zpět
- Možnost vyhledávání v záznamech
- Možnost exportu dat

Prostředí centrálních eGon služeb

- Správcem prostředí je MV
- Publikace klíčových aplikačních služeb pro potřeby státní správy ČR
- Aplikace musí být umístěny v NDC
- Zpřístupnění aplikačních služeb do různých prostředí
- NDC jsou propojena sítí NDC
- MV definuje požadavky na aplikace, služby, NDC a síť NDC

Komunikační prostředí EU

- Vzájemná komunikace aplikací na základě dvoustranných dohod OVM ČR a subjektů EU
- CMS poskytuje momentálně konektivitu pouze do sítě STESTA
- Správce CMS2 je autorizován ze strany správce sítě STESTA pro propojování subjektů ČR do STESTA

Prostředí KIVS

- Možnost přímé komunikace mezi lokalitami jednoho OVM
- Publikace aplikačních služeb pro (jiné) OVM přes CMS
- Přístup k aplikačním službám nabízeným aplikacemi OVM přes CMS

Katalog služeb CMS 2.0

Kód služby	Název služby
CMS2-01-1	Akceptace provozních podmínek CMS
CMS2-02-1	Zveřejnění aplikace do sítě Internet
CMS2-02-2	Zveřejnění aplikace do sítě CMS
CMS2-02-3	Zveřejnění aplikace do sítě sTESTA
CMS2-02-4	Zveřejnění aplikace do Extranetu
CMS2-03-1	Přístup k aplikaci v síti CMS
CMS2-03-2	Přístup k aplikaci v síti sTESTA
CMS2-03-3	Přístup k aplikaci v síti Internet
CMS2-03-4	Přístup k aplikaci v Extranetu
CMS2-03-5	Čtenář eGON Service Bus
CMS2-04-1	Fyzické připojení infrastruktury v NDC k síti CMS
CMS2-04-2	Dedikované propojení infrastruktury umístěné ve více NDC

Katalog služeb CMS 2.0

Kód služby	Název služby
CMS2-05-1	Odchozí provoz elektronické pošty
CMS2-05-2	Příchozí provoz elektronické pošty
CMS2-06-1	DNS hosting - Veřejná registrovaná doména
CMS2-06-2	DNS hosting - Veřejná doména CMS
CMS2-06-3	DNS hosting - Neveřejná doména
CMS2-07-1	Služby sTESTA
CMS2-08-1	Přístup do CMS přes KIVS
CMS2-08-2	Přístup do CMS přes IPsec
CMS2-08-3	Přístup do CMS přes SSL
CMS2-08-4	Přístup do CMS z NDC
CMS2-09-1	Přímý přístup do Internetu
CMS2-09-2	Bezpečný přístup do Internetu
CMS2-10-1	Přístup k záznamům o provozu
CMS2-11-1	Přístup k účtovacím informacím
CMS2-12-1	Propojovací bod subjektu
CMS2-12-2	Propojovací bod pro extranet

Současný stav CMS 2.0

- Technologie a systémy nainstalovány ve dvou DC v režimu Active - StandBy
- Realizováno propojení s krajskými konektory
- Propojení do CZ NIC realizováno
- Síťová infrastruktura v provozu
- Service desk v provozu
- Probíhá ověřování formulářů uživatelského portálu
- V CMS 2.0 jsou publikovány a dostupné centrální aplikační služby z CMS 1.0
- Zahájeno pilotní ověřování na NMNM ve spolupráci s krajem Vysočina

Dotazy a odpovědi ?