

Národný projekt: Elektronická identifikačná karta

Technologické aspekty riešenia projektu

Hewlett Packard Enterprise
RNDr. Milan Ďurana











Rozsah projektu

1. Rozšírenie Personalizačného systému NPC MV SR
2. Rozšírenie centrálnych systémov IDC a ECU
3. Rozšírenie riešenia Jednotných pracovísk PZP
4. eGovernment služby
5. Zabezpečenia centralizovaného riadenia prístupu k eGovernment službám (IAM)
6. Mobilné pracoviská na zber žiadostí pre vydávane eID
7. Technické riešenie Centrálnej tlače pre hromadnú tlač dokumentov v pôsobnosti MV SR

Grafický dizajn eID



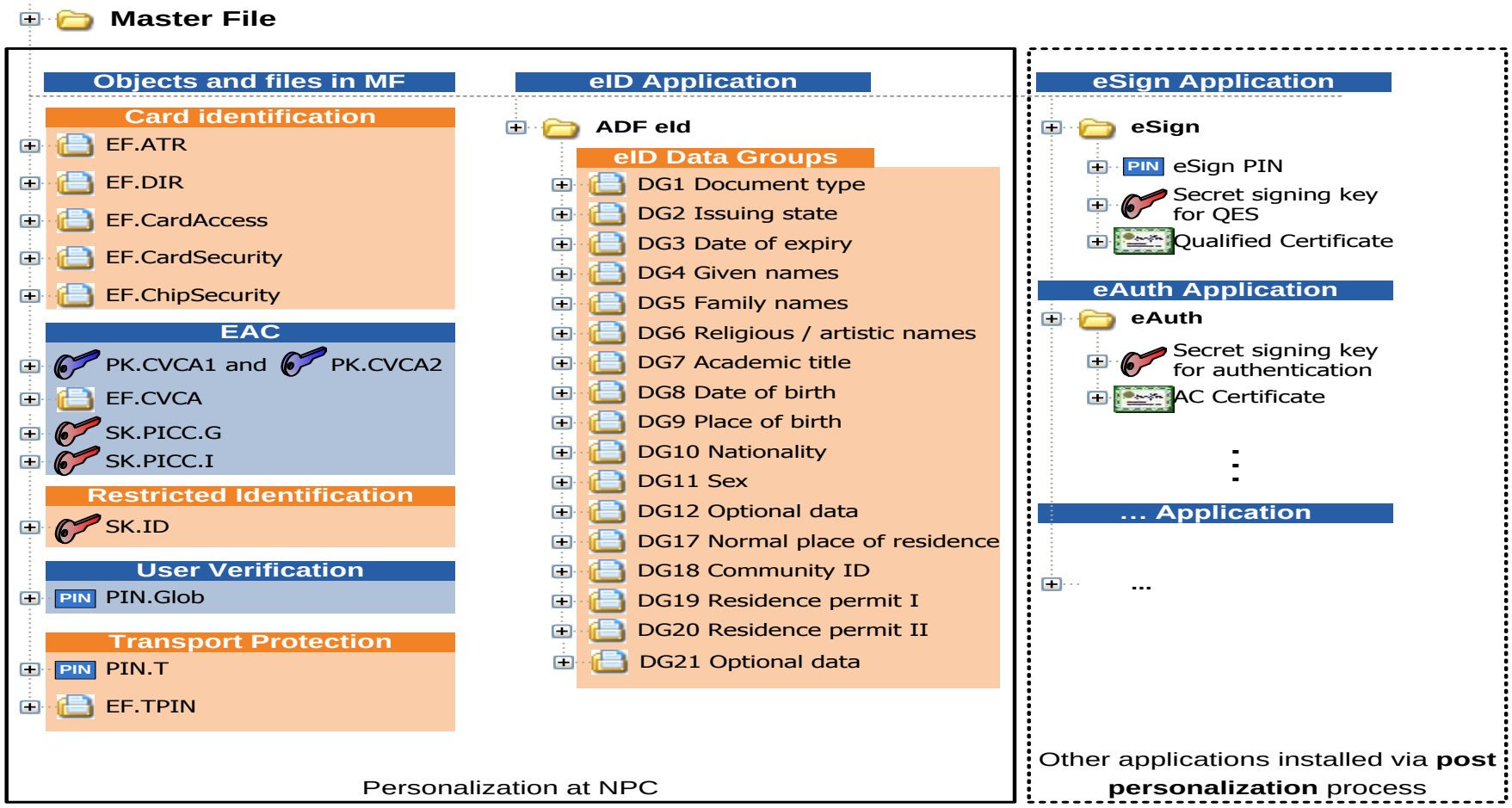


- **Jadrom eID je kontaktný čip s kapacitou pamäte 96 kB**
  - Čip Infineon SLE78CFX3000P s flash pamäťou
  - OS Atos CardOS verzie 5.0
- **Údaje v pamäti čipu sú uchované v zašifrovanej podobe**

Súlad riešenia eID s normami

- **CEN/TS 15480-1**, Identification card systems – European Citizen Card – Part 1: Physical, electrical and transport protocol characteristics
- **CEN/TS 15480-2**, Identification card systems – European Citizen Card – Part 2: Logical data structures and card services
- **BSI TR-03110**, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)Version 2.03

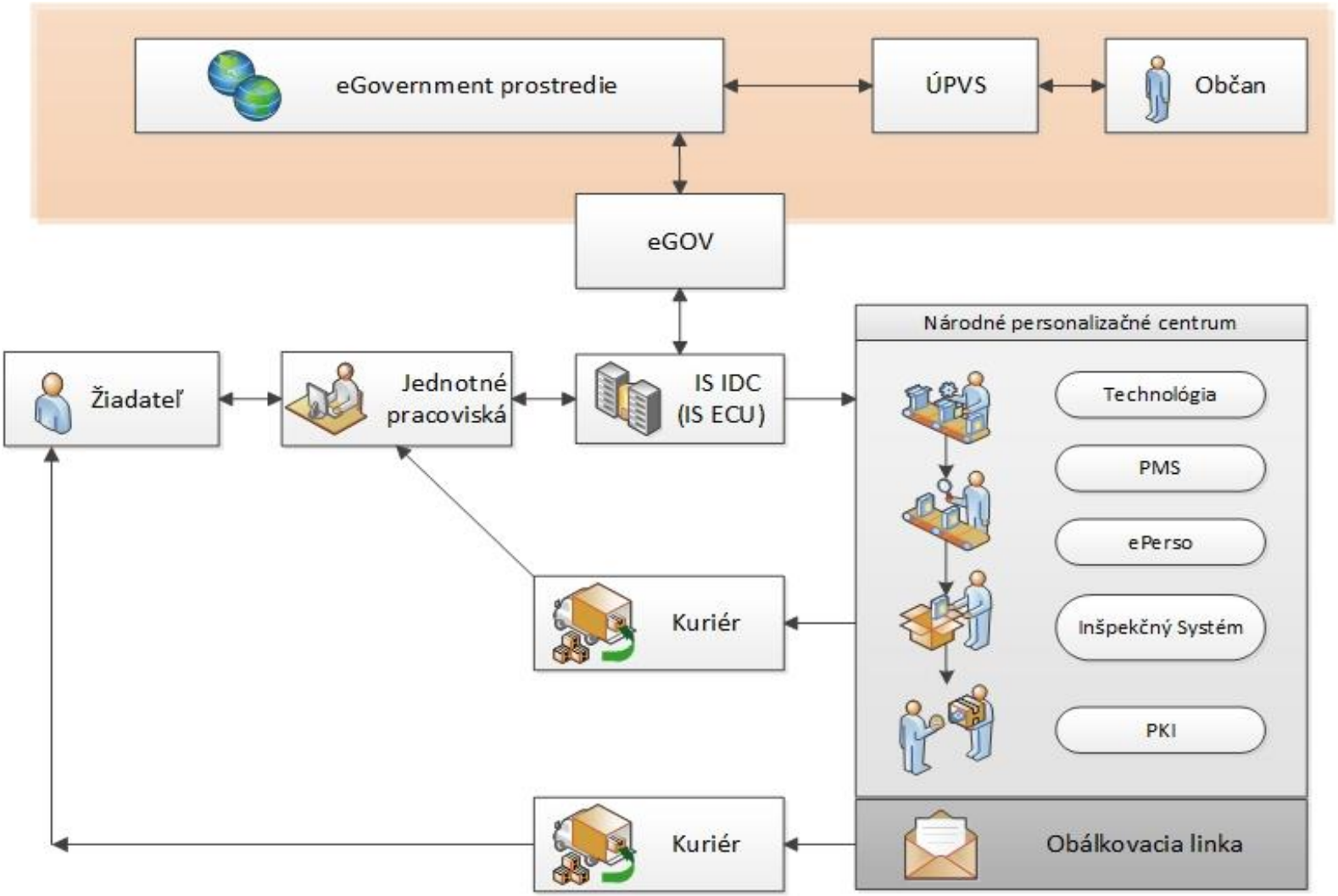
Údajová štruktúra pre eID kartu



Bezpečnostné prvky riešenia eID (odporúčania ENISA, STORK)

- **Selective Disclosure (EU data protection, Directive 95/46/EC)**
  - Doklad nemôže sprístupniť väčší rozsah údajov ako je schválený držiteľom karty
- **Riadenie prístupu k údajom o držiteľovi**
  - BOK (6 čísiel) držiteľa karty
  - Terminálový certifikát definuje oprávnenia na prístup k údajom
  - Vzájomná autentifikácia
- **Bezpečná komunikácia s eID k poskytovateľovi služby**
  - Silne kryptovaný komunikačný kanál pre údaje čítané z karty
- **Koncept (eID) podporuje obmedzenú identifikáciu**
  - pseudonym, sektorovo špecifický identifikátor pri transakciách v komerčnom sektore

Proces vydávania eID dokladu



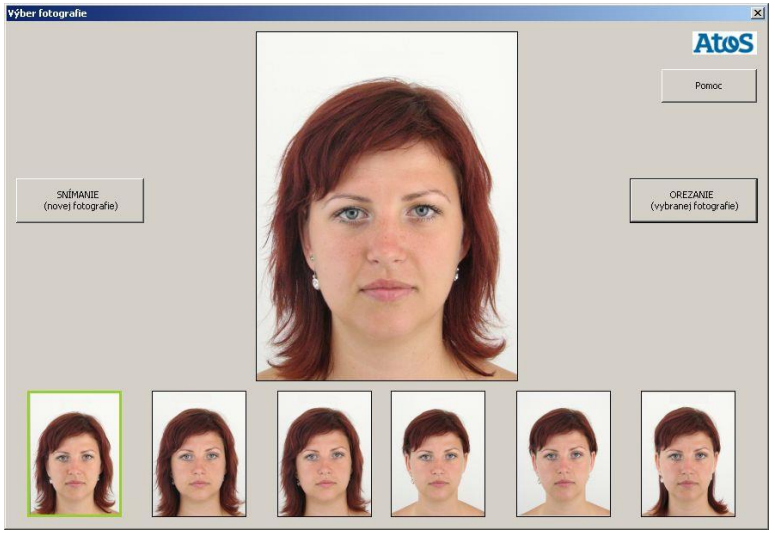
Zmeny v aplikačnom vybavení JP

- APV Jednotných pracovísk prispôsobené pre príjem žiadostí o eID a ich vydávanie
- Klientsky komponent pre bezpečné zadávanie PINu (pinReader)
- Jednotný inšpekčný systém zabezpečujúci riadenie oprávnení na kontrolu, overenie funkčnosti a postpersonalizáciu dokladov eID a eDoPP
- Klientsky komponent pre prečítanie obsahu čipu eID karty a pre zmenu/odblokovanie PINu (eIDDisplay)
- APV Kioskov upravené pre čítanie a zobrazovanie obsahu čipu eID karty a pre zmenu PINu

Zmeny v aplikačnom vybavení JP – fotografie a odtlačky

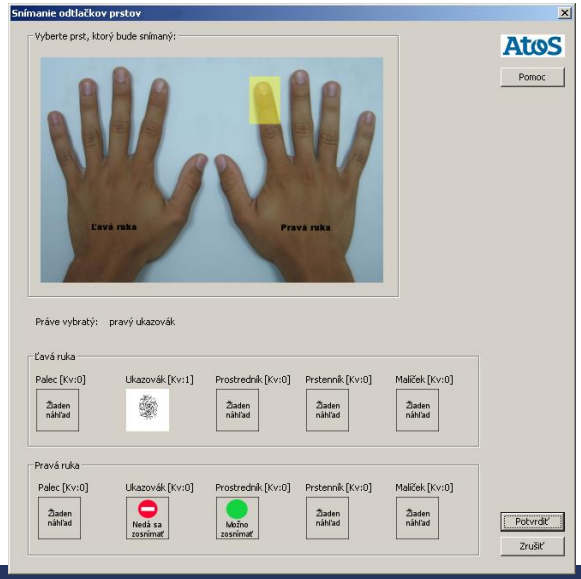
Fotografia

- Sekvenčné snímanie fotografie
- Galéria fotografií

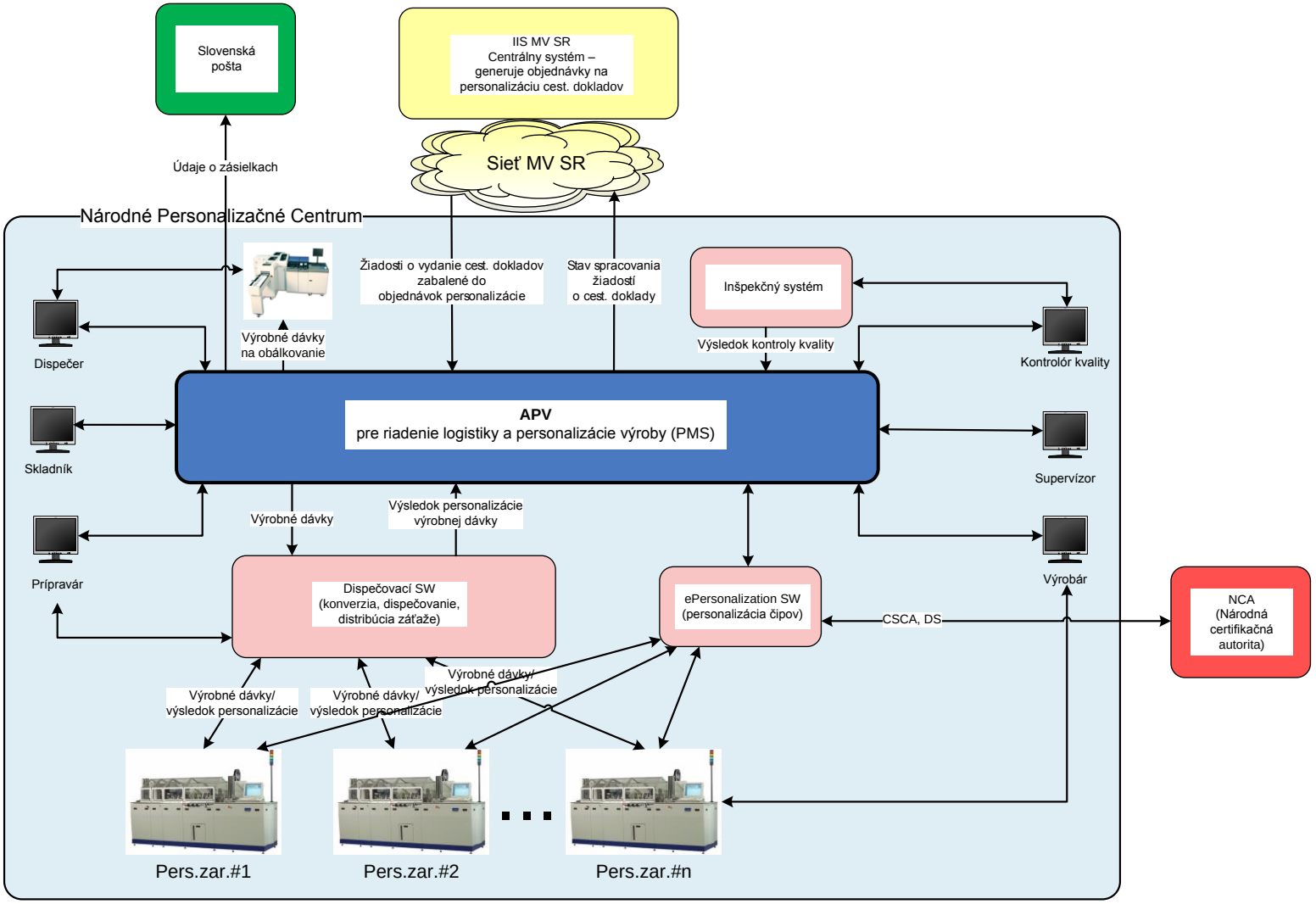


Odtlačky

- Možnosť zmeny výberu prstov bez straty zosnímaných údajov
- Viacnásobné snímanie s ponechaním vyššej kvality

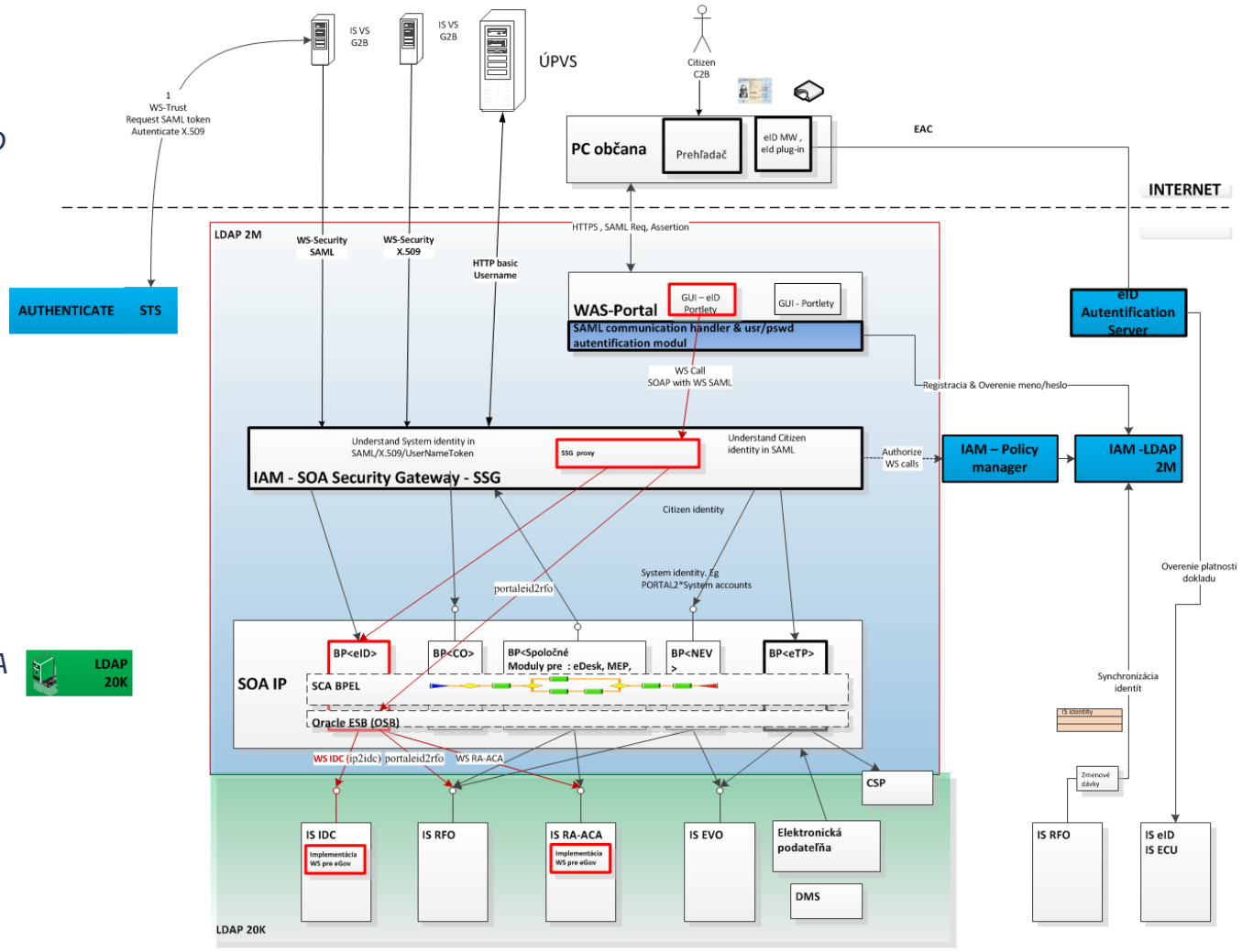


Logická schéma Personalizačného systému NPC

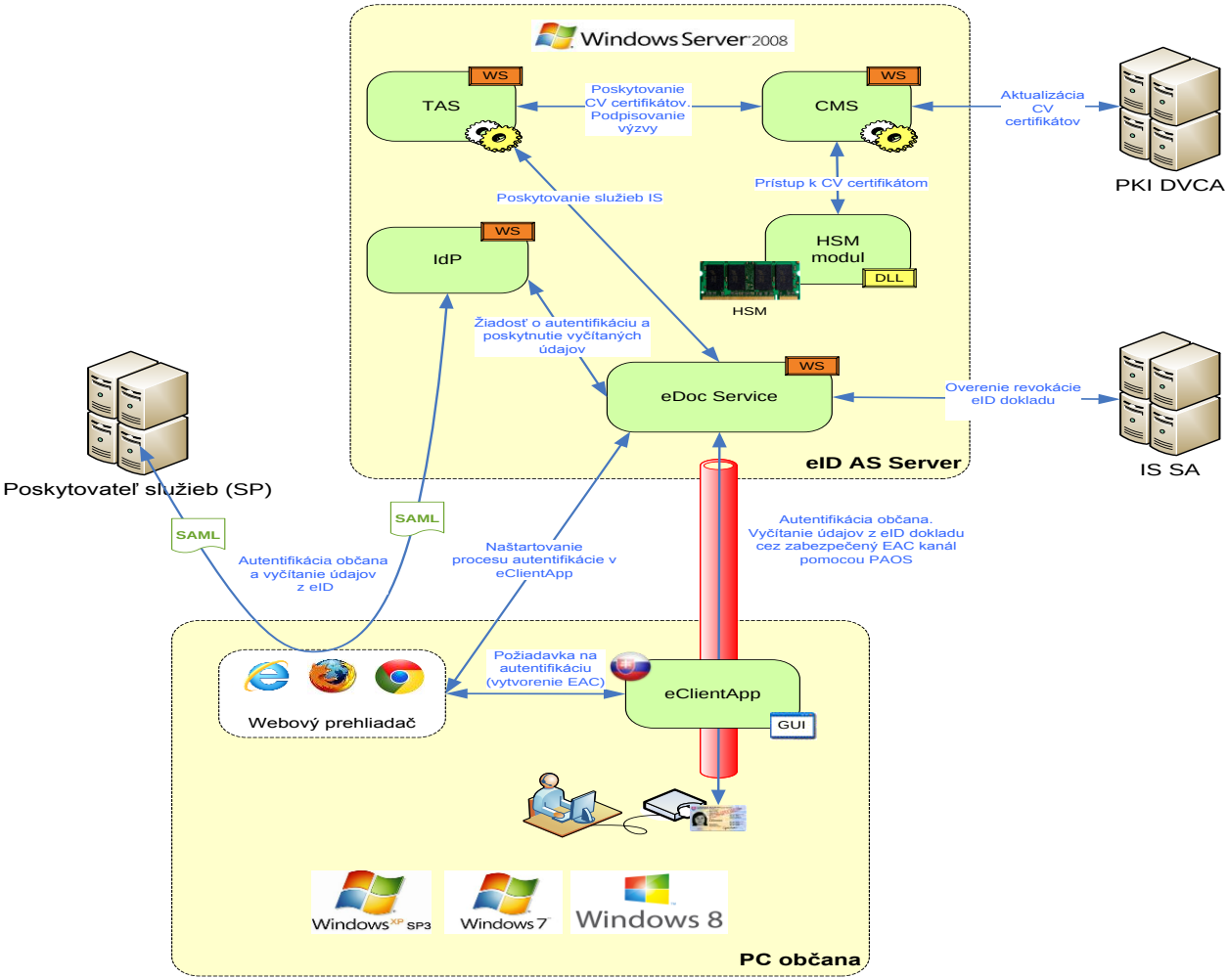


Logická schéma eGovernment prostredia MV SR

- Portál - *IBM Web Sphere Portal*
- eID AS – *IdP, SAML CH, eID klient*
- IAM – *SSG, LDAP*
- SOA IP - *SCA-BPEL, OSB*
- Spoločné moduly – *integrácia na eDesk, MEP, Podpora pre Logovanie, Fault handling*
- Centrálne komponenty - *EKR/DMS, CESP*
- Backendové systémy - *RFO, IDC, CO, EVO, RA-ACA ...)*
- SW komponenty pre implementáciu eGov služby



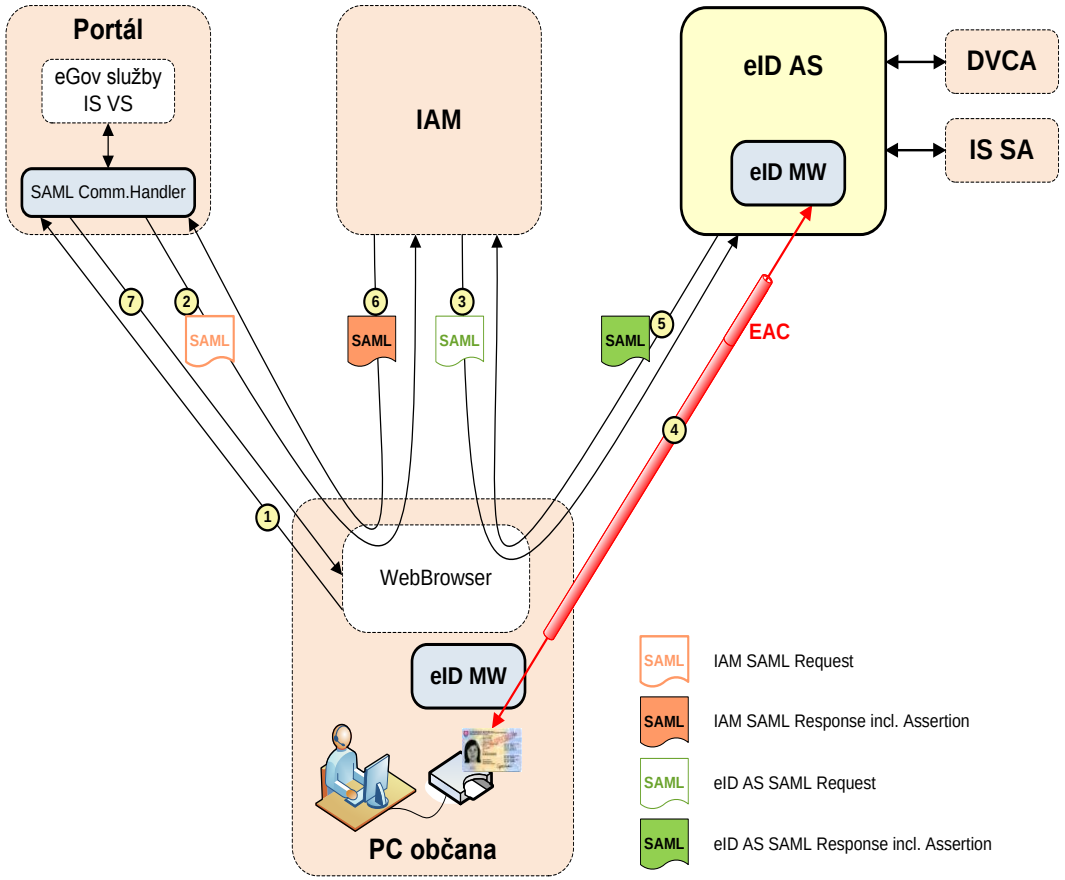
eID Autentifikačný server – Funkčná architektúra



eID AS – podporované platformy

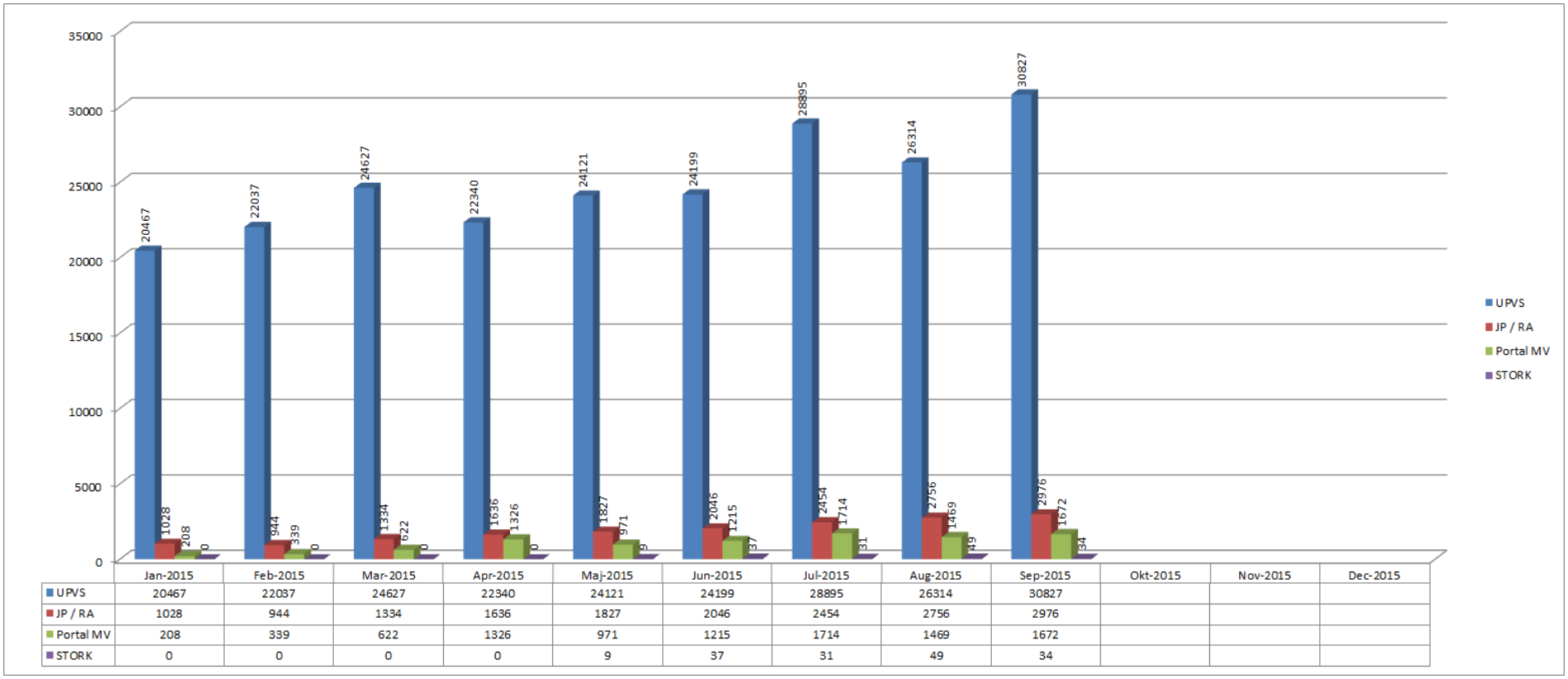
- **Operačný systém Windows**
  - W XP SP3, Vista, W7 (32 bit / 64 bit), W8 (32 bit / 64 bit)
  - Prehliadače: IE verzia 7-11, Chrome v 28-45, Firefox v 23-41, Opera 15-32
- **Operačný systém MAC OS X**
  - OS X Mountain Lion (v 10.8), OS X Mavericks (v 10.9), OS X Yosemite (v 10.10.2, 10.10.3)
  - Prehliadače: Safari v 6 – 8, Chrome v 28-45, Firefox v 23-41
- **Operačný systém LINUX**
  - Ubuntu LTS v 12.04 a 14.04 (32 bit / 64 bit), Mint LTS v 13 a 17 (32 bit / 64 bit), Debian 7 (32 bit / 64 bit)
  - Prehliadače: Chrome v 28-45, Firefox v 23-41, IceWeasel v 24 - 38

Proces identifikácie a autentifikácie k elektronickým službám



1. Občan prostredníctvom svojho internetového prehliadača žiada na portáli o prístup eGov službe.
2. Poskytovateľ služby vygeneruje SAML Authentication Request pre IAM.
3. IAM vygeneruje SAML Authentication Request pre eID AS.
4. eID AS vykoná autentifikáciu občana prostredníctvom eID karty
5. eID AS vystaví SAML Assertion obsahujúce atribúty identity občana vyčítané z eID karty a odošle SAML Response IAM
6. IAM vystaví SAML Assertion obsahujúce atribúty identity občana vyčítané zo SAML Assertion prijatého z eID AS ako aj ďalšie údaje, získané z iných autoritatívnych zdrojov.
7. SP po overení SAML Assertion povolí občanovi prístup k požadovanej elektronickej službe.

Štatistika používania eID pri autentifikácii



	Jan-2015	Feb-2015	Mar-2015	Apr-2015	Maj-2015	Jun-2015	Jul-2015	Aug-2015	Sep-2015	Okt-2015	Nov-2015	Dec-2015
UPVS	20467	22037	24627	22340	24121	24199	28895	26314	30827			
JP / RA	1028	944	1334	1636	1827	2046	2454	2756	2976			
Portal MV	208	339	622	1326	971	1215	1714	1469	1672			
STORK	0	0	0	0	9	37	31	49	34			

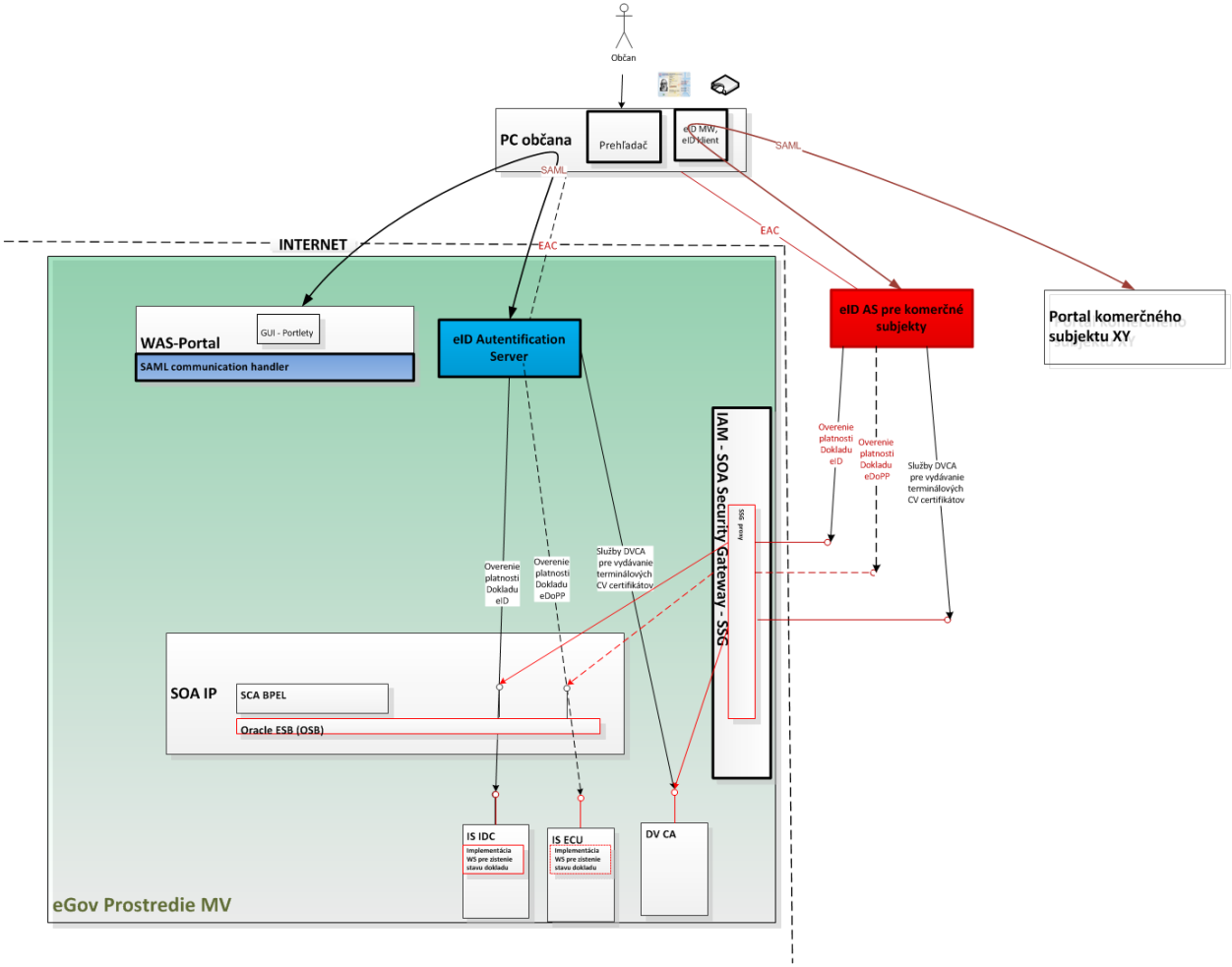
Využitie eID AD v komerčnom sektore - alternatíva A

Vybudovanie separátnej inštancie eID AS pre komerčné subjekty

MV bude poskytovať iba (G2B):

- Službu overovania stavu dokladu (stratený,..) v agende IDC, prípadne ECU
- Periodické čítanie DV CA certifikátov

- Služby DVCA pre vydávanie terminálových CV certifikátov



Využitie eID AD v komerčnom sektore - alternatíva B

eID AS MV SR bude poskytovať služby IdP (Identity Providera) aj komerčným subjektom

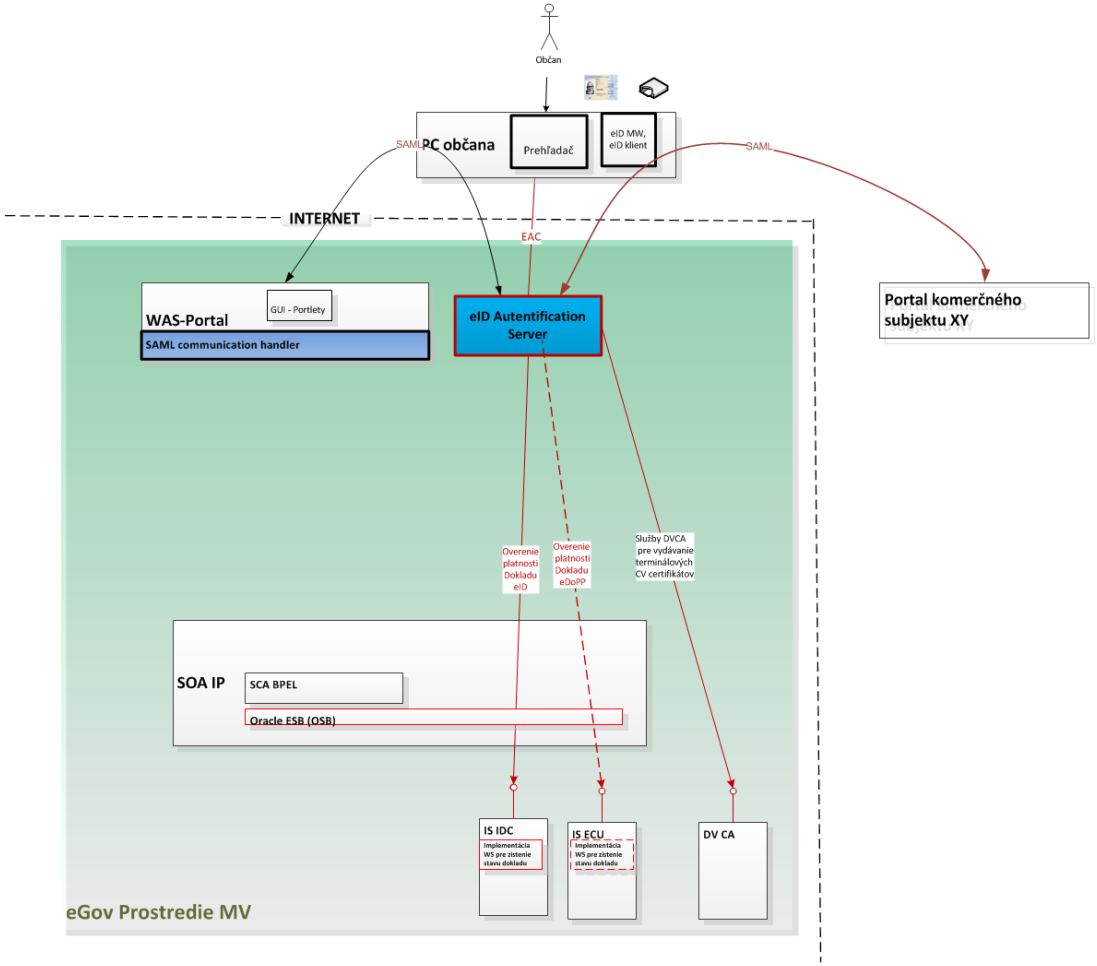
Na eID AS budú zaregistrovaní ako SP (Service Provider) :

- Portál MV
- RA MV
- ÚPVS
- Komerčný subjekt X
- Komerčný subjekt Y

- Overovanie stavu dokladu v IDC, prípadne ECU (priepustnosť OSB, agend IDC, ECU)
- Služby DVCA pre vydávanie terminálových CV certifikátov(iba malá záťaž : cca 1x za 2 týždne pre jedného SP)

=> Nárast záťaže :

- Priepustnosť eID AS MV (dimenzovanie HW)



Ďakujem za pozornosť !

milan.durana@hpe.com