SPRÁVA ZÁKLADNÍCH REGISTRŮ

JE UŽ eIDENTITA ZA DVEŘMI?

Michal Pešek

Správa základních registrů

31. května 2018

Státní identitní systém(y) – PROČ?

- 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
- zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce a související změnový zákon č. 298/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce….
- Zákon 250/2017 Sb. O elektronické identifikaci rozšiřuje odpovědnosti SZR o povinnost poskytování a uznávání identit v prostředí EU
- Novela zákona o občanských průkazech zavádí identifikační certifikát na občanský průkaz a stvrzuje tak jeho „elektronickou část“
- STÁT MÁ POVINNOST A ZÁJEM POSKYTNOUT OBČANŮM DŮVĚRYHODNÉ SLUŽBY NA NEJVYŠŠÍ ÚROVNI DŮVERYHODNOSTI A TO I V PŘESHRANIČNÍM STYKU

Státní identitní systém (y) – JAK?

- **Elektronický občanský průkaz (eOP)** - Občan může při převzetí občanského průkazu nebo kdykoli poté u kteréhokoliv obecního úřadu obce s rozšířenou působností zadat identifikační osobní kód (IOK) pro účely aktivace identifikačního certifikátu – stovky tisíc klientů ročně
- **ISDS** - je momentálně jediným identitním prostorem, který uznává stát při komunikaci s občanem. Proces vzniku identity v rámci ISDS je spojen se zřízením datové schránky – stovky tisíc klientů již nyní
- **NIA** jako národní bod pro identifikaci a autorizaci, OTP (one-time-password), dnes využití pro SUKL

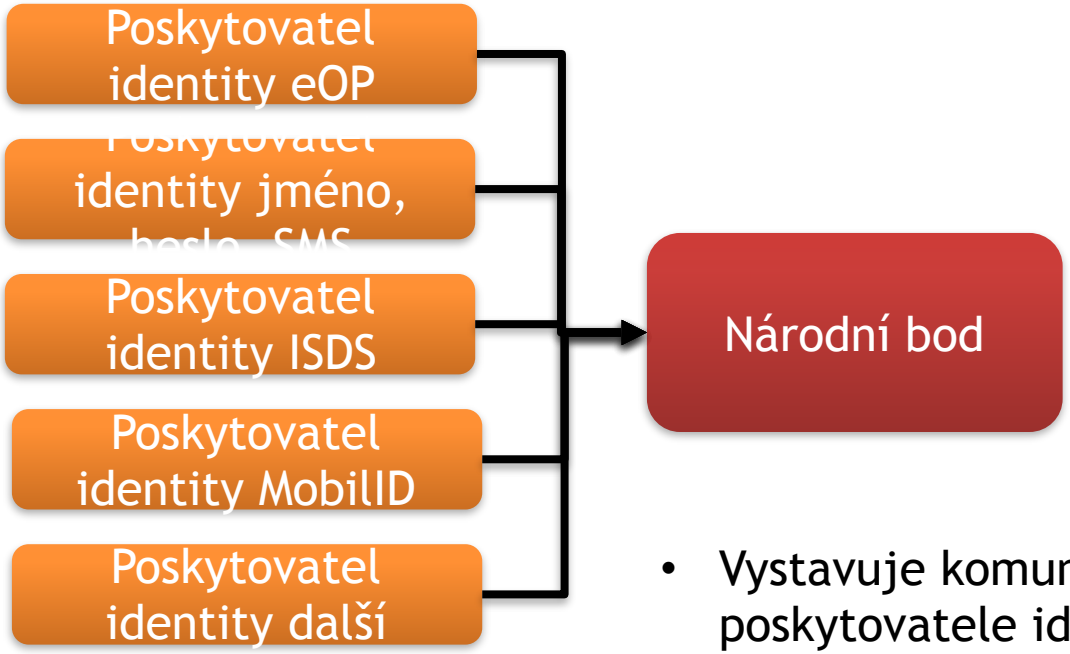
Státní identitní systém (y) – KDE?

- PORTÁL OBČANA – nový portál veřejné správy jako centrální místo služeb státu pro občany v oblasti elektronické komunikace
- SLUŽBY STÁTU, KRAJŮ, MĚST A OBCÍ pro občana
  - poskytnutí identity systému pro státní organizace
  - poskytovány formou dlaždic
  - přístup zvoleným IDP podle úrovně důvěry
- Služby MV, ČSSZ, GFŘ, MZ – SÚKL, KRAJ Vysočina, portály nemocnic, ČUZK,

PORTÁL NÁRODNÍHO BODU

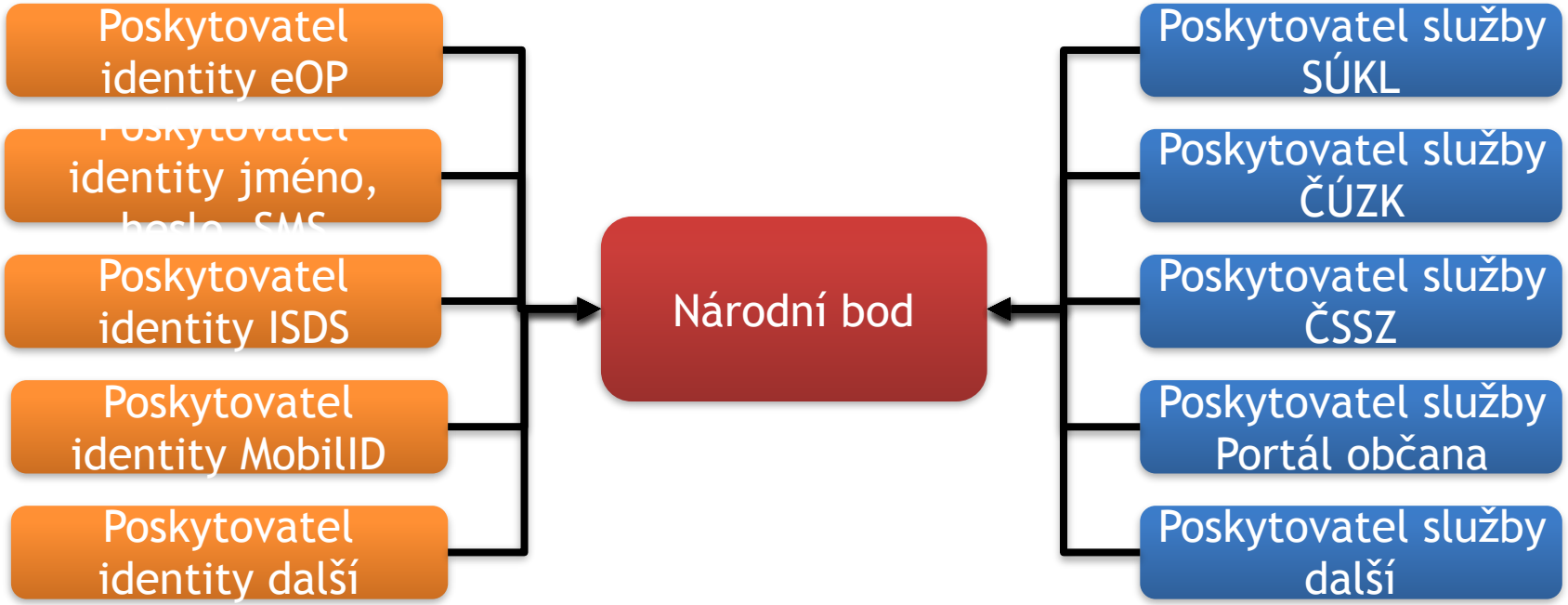
identita.cz

Zdroj: MONET+



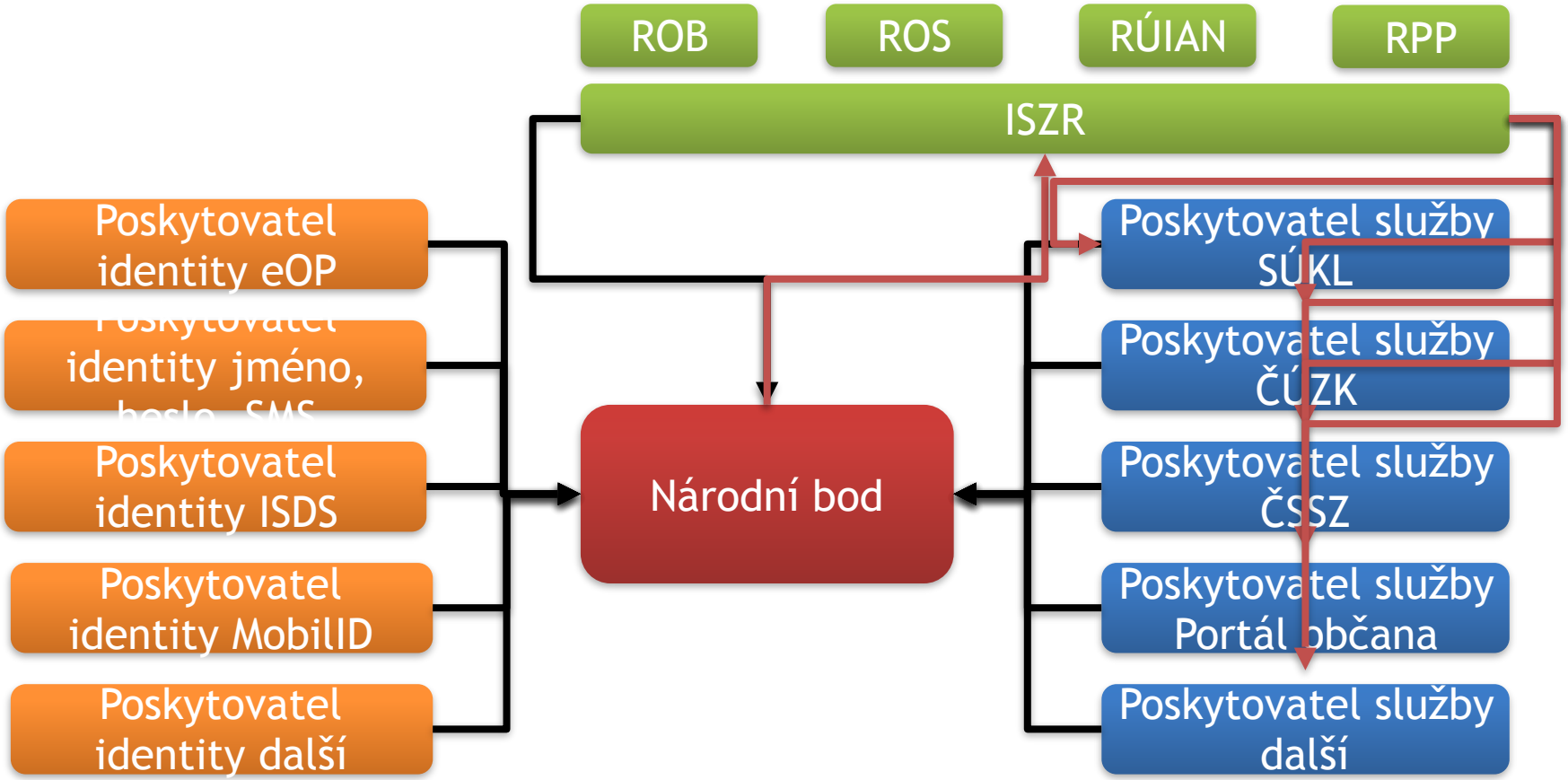
- Vystavuje komunikační rozhraní pro poskytovatele identit
- Vystavuje služby potřebné při fungování poskytovatele identit
  - Ztotožnění subjektu
  - Notifikace při změně dat
  - Služby evidence národního bodu
- Zprostředkovává předání žádosti o provedení autentizace od poskytovatele služby

identita.cz



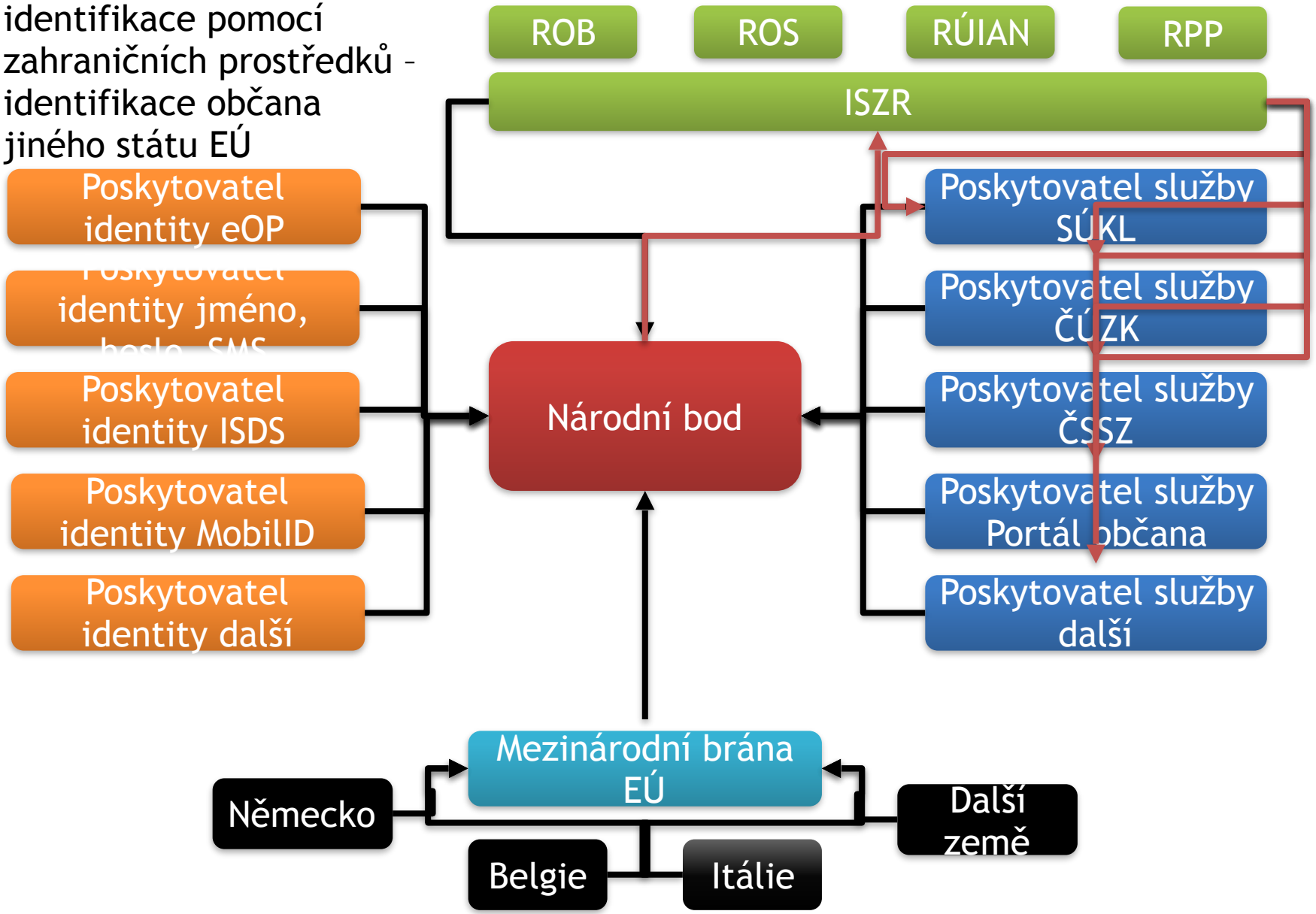
- Zajišťuje federaci identit od jejich poskytovatelů k jejich konzumentům
- Jednotí komunikační protokol pro jednotlivé poskytovatele služeb – poskytovatel si jen volí požadovanou úroveň.
- Udržuje vztahy důvěry mezi poskytovatelem služby a sám sebou

identita.cz

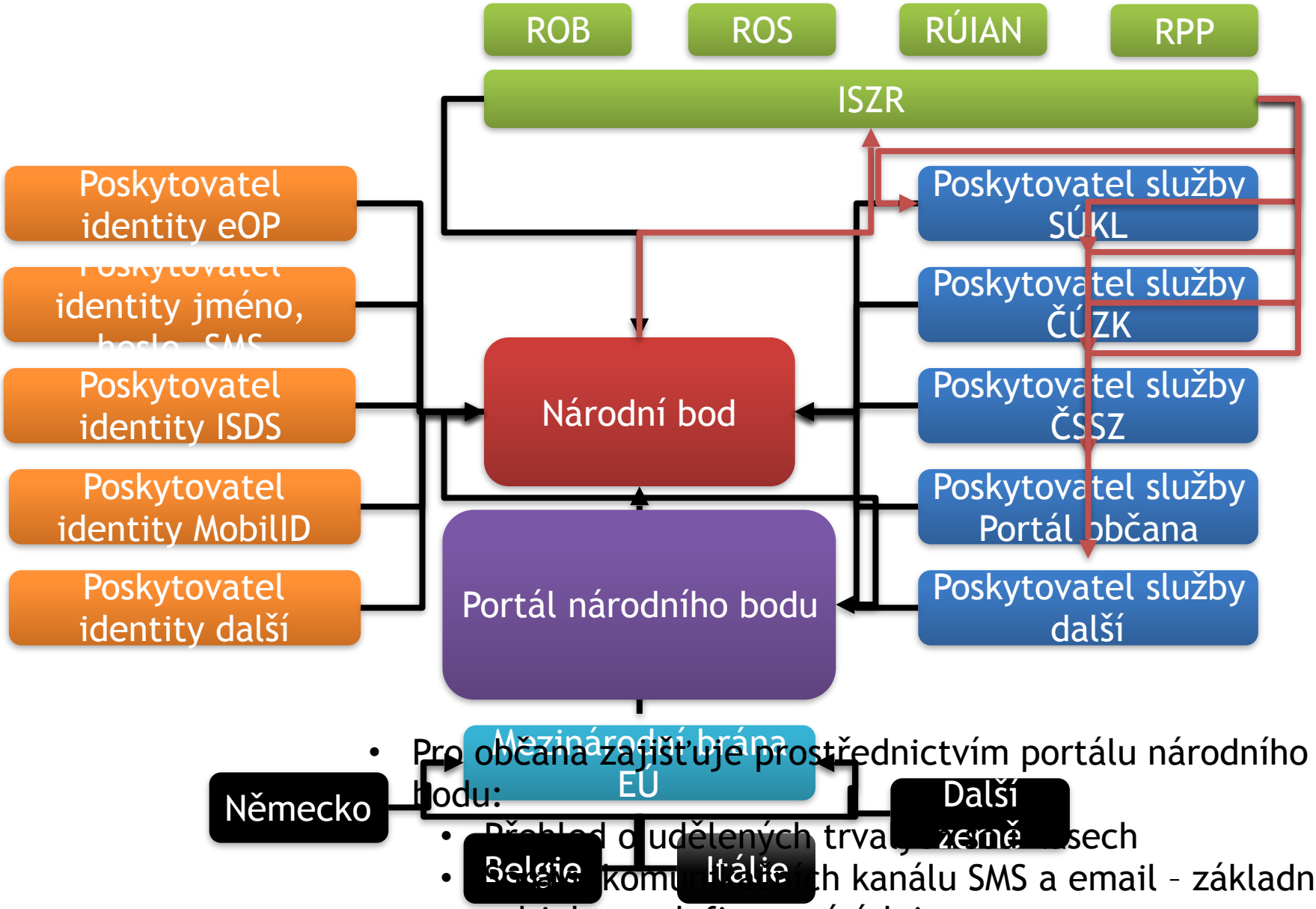


- Provádí kontrolu subjektu vůči referenčním datům – kontrola úmrtí
- U českých identit zajišťuje načtení referenčních osobních dat a jejich výdej
- Zajišťuje službu pro ISZR pro umožnění překladu směrového identifikátoru na AIFO agendy poskytovatele služby – pouze pro OVM

- Zajišťuje zprostředkování identifikace pomocí zahraničních prostředků – identifikace občana jiného státu EÚ



identita.cz



- Pro občana zajišťuje prostřednictvím portálu národního bodu:
  - Přehled o udělených trvalých souhlasech
  - Komunikaci prostřednictvím kanálu SMS a email – základní subjektem definované údaje
  - Správu identifikačních prostředků
  - A postupně další funkcionality

identita.cz

ELEKTRONICKÉ FUNKCE NOVÉ EOP

identita.cz

Zdroj: MONET+

Nová verze eOP: prostředek pro elektronizaci občana vůči státní správě

- Reakce na Nařízení Evropského parlamentu a rady č.910/2014 (eIDAS)
  - Elektronická identifikace a služby vytvářející důvěru
- ČR dává občanům **prostředek pro elektronickou identifikaci** a uložení (+použití) **certifikátů pro elektronický podpis**
- Novela Zákona o občanských průkazech, č.328/1999 Sb.
  - Účinnost k 1.7.2018
- Zákon o elektronické identifikaci, č.250/2017 Sb.

- Nová verze eOP bude v sobě sdružovat:
  - **Prostředek elektronickou identifikaci s úrovní záruky „vysoká“** (=nejvyšší)
  - **Kvalifikovaný prostředek pro vytváření elektronických podpisů**
- SZR je (ze zákona) správcem národního bodu pro elektronickou identifikaci
  - Kvalifikovaný systém elektronické identifikace

identita.cz

Zdroj: MONET+

Nové funkce eOP (podle zákona)

- **Prostředek elektronickou identifikaci s úrovní záruky „vysoká“**

- Bezpečné přihlašování na webové stránky
- Uznávané napříč státy EU
- Nejvyšší míra důvěry → čerpání citlivých služeb

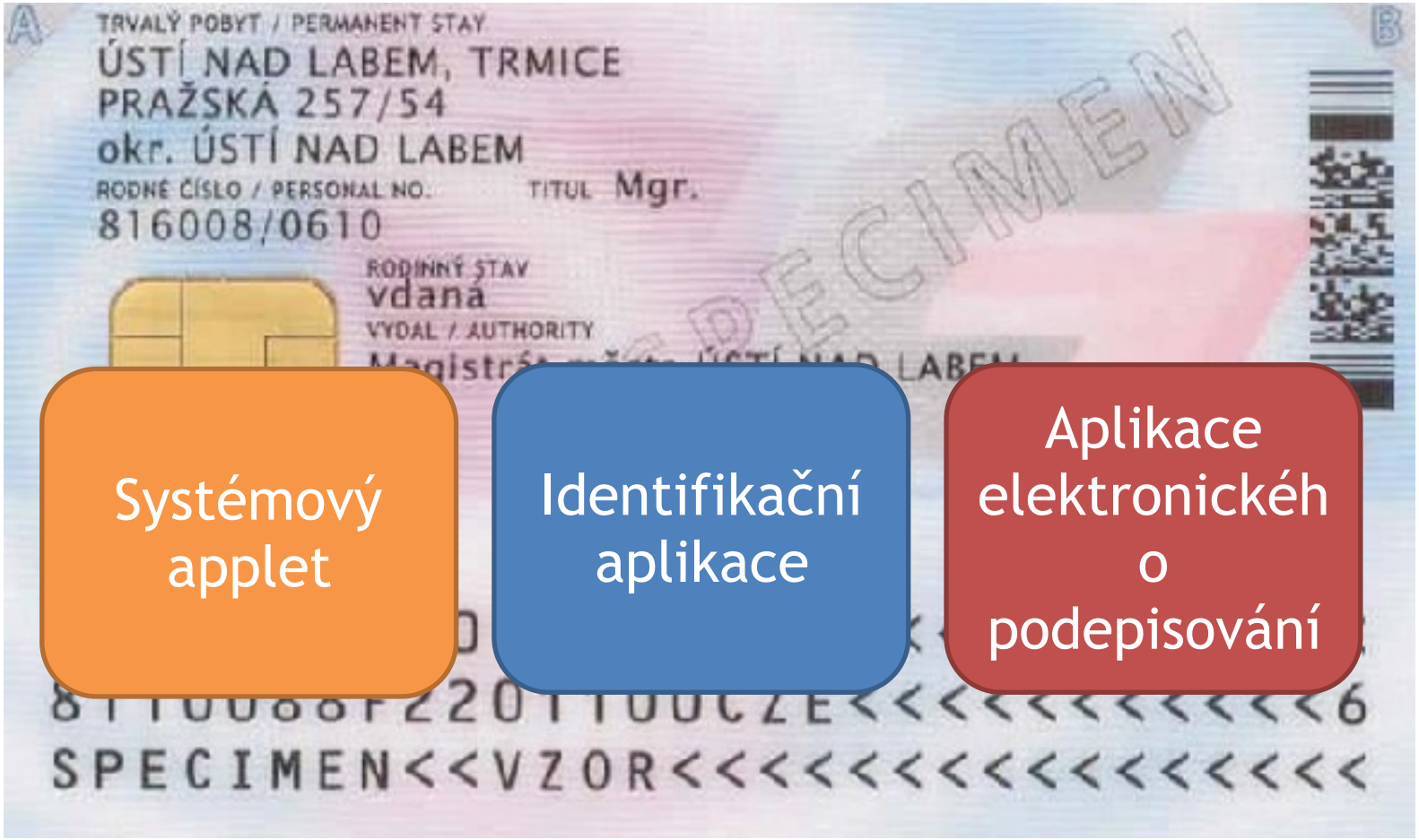
- **Kvalifikovaný prostředek pro vytváření elektronických podpisů**

- Kvalifikované certifikáty uznávané v rámci EU
- (možnost uložení i dalších certifikátů)
- Nejvyšší úroveň důvěry

identita.cz

Zdroj: MONET+

Aplikace v čipu nového OP

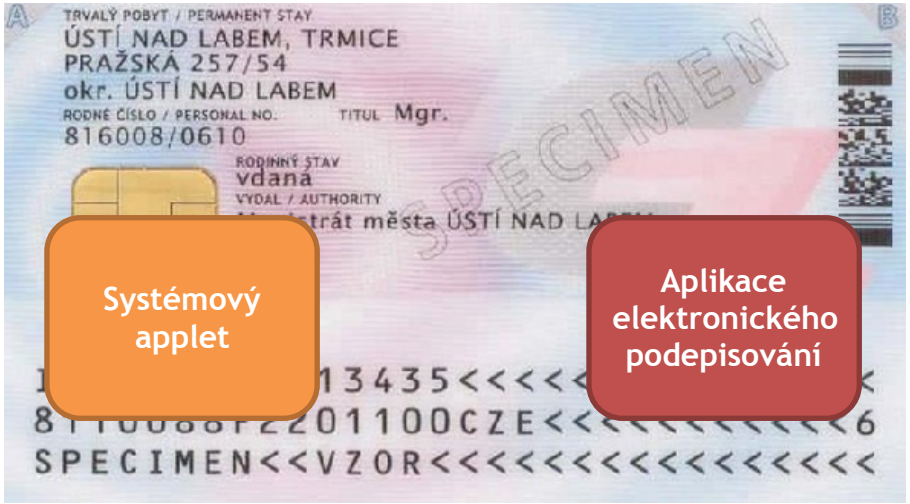


identita.cz

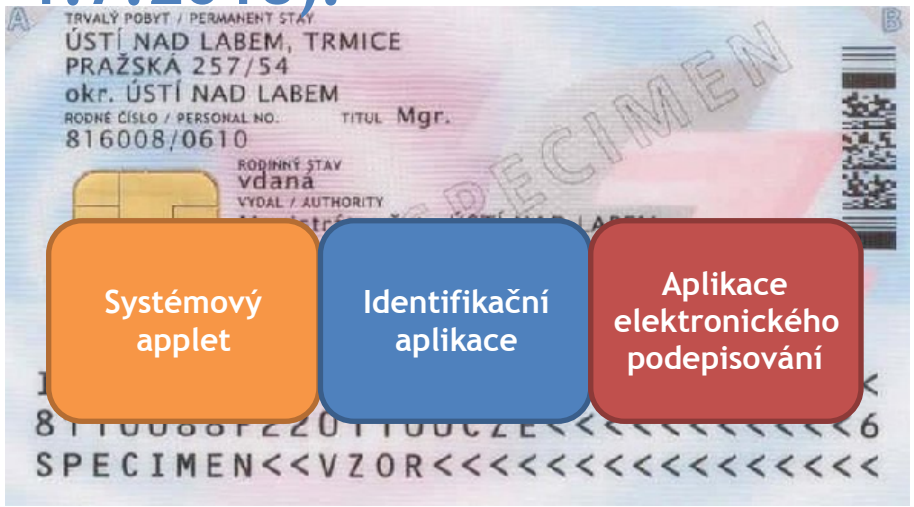
Zdroj: MONET+

Porovnání předchozí a nové verze eOP

Stávající verze eOP:



Nová verze eOP (od 1.7.2018):



Hlavní změny:

- **Přibyla el.identifikace**
- **Jiné PINové objekty**

identita.cz

Zdroj: MONET+

Aplikace v čipu nového eOP

- Systémový applet
  - Výdej a distribuce eOP
  - (bez praktického použití občanem)
- Identifikační aplikace
  - Identifikace občana na internetu
- Aplikace elektronického podepisování
  - Práce s certifikáty (a klíči)
  - Elektronické podepisování
  - Přihlašování certifikátem apod…

identita.cz

Zdroj: MONET+

Systémový applet

- Podpora vydávání OP občanům
- Využívá se na úřadech Obcí s rozšířenou působností
- Technologické využití, kontrola funkčnosti čipů
- Podpora evidencí OP
- Bez aplikačního využití občanem
- Pracovníci podpory se s funkcí systémového appletu nesetkají

identita.cz

Zdroj: MONET+

Identifikační aplikace

- Nově zavedená funkce
- Identifikace (přihlašování) na internetu
- Předpokládá se, že bude nejvíce využívanou funkcí eOP
  - (pokud stát připraví pro občany užitečné služby na internetu)
- V čipu je uložen identifikační certifikát občana
  - Z výroby, nelze měnit

- Typický scénář:
  - Uživatel se chce identifikovat vůči internetovým stránkám
  - Spustí proces identifikace z webových stránek
  - Připojí čtečku
  - Vloží do čtečky eOP
  - Zadá hodnotu IOK (schválení operace)
  - Čip eOP zajistí identifikaci (přihlášení) na webové stránky
  - Webové stránky po přihlášení vědí, kdo s nimi komunikuje

identita.cz

Zdroj: MONET+

Aplikace elektronického podepisování

- Vylepšení dosavadní funkce
- Uložení elektronických certifikátů v čipu
  - Ke každému certifikátu je v čipu kryptografický klíč
- Možnost využívat certifikáty v aplikacích třetích stran
  - Elektronické podepisování
  - Přihlašování (certifikátem), např. přes webový prohlížeč
- Podpora *získání* certifikátu do čipu eOP
- Do čipu lze ukládat různé certifikáty
  - Ve správě uživatele
  - Při předání držiteli nejsou uloženy žádné certifikáty

- Typický scénář:
  - Aplikace (např. Adobe Reader) chce podepsat dokument
  - Aplikace zavolá kryptografickou funkci operačního systému
  - Operační systém osloví ovladač karty (=eOP), vyzve ke vložení čtečky a karty
  - Uživatel zadá PIN (schválení podpisu)
  - Čip karty podepíše dokument (klíčem, uloženým v čipu)
  - Podepsaný dokument nese informaci o autorovi (schvalovateli)

Zdroj: MONET+

Podpora aplikací v čipu eOP

- Pouze nepřímá
  - Nelze upgradovat aktualizace v čipu, ani hledat v nich chyby
  - Neexistuje žádný žurnál aplikace v čipu, v němž lze hledat záznamy
- Aplikace v čipu jsou dostupné prostřednictvím aplikací v PC anebo v mobilním telefonu
  - Ale bez aplikací v čipu by nefungovaly aplikace eOP v PC ani v mobilním telefonu
- Předpokládá se, že jsou aplikace v čipu správně zapsány a funkční
- Aplikace v čipu spravují PINové objekty
  - PINové objekty budou zřejmě častým zdrojem dotazů a problémů
  - Pro každou z aplikací jsou určeny jiné PINové objekty
  - Pokud se zablokují některé PINové objekty, pak příslušná aplikace nefunguje
- Rozlišovat verze eOP!
  - Např. podle data vydání
  - Na starší verzi eOP nejsou dostupné některé funkce

Zdroj: MONET+

PINOVÉ OBJEKTY ANEB NEBOJME SE EOP

identita.cz

Zdroj: MONET+

PINové objekty občana

IOK

PUK

PIN

DOK

QPIN

BOK

identita.cz

Zdroj: MONET+

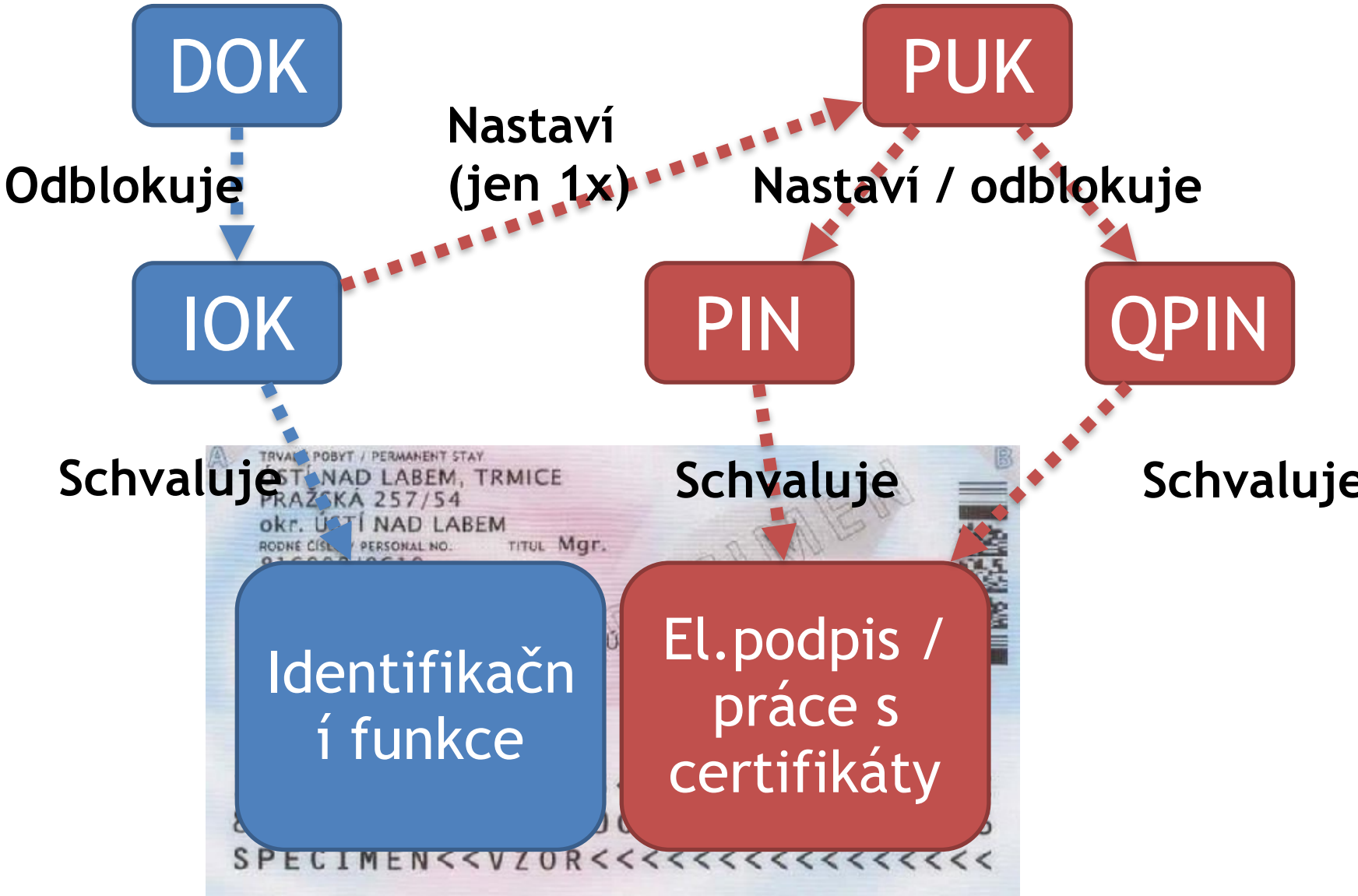
PINové objekty

Zkratka	Název	Aplikace eOP	Délka	Poč. pokusů
DOK	Deblokační osobní kód	Identifikace	4-10	10x
IOK	Identifikační osobní kód	Identifikace	4-10	3x
PUK	PIN Unblocking Key	El.podpis	8-15	5x
PIN	Personal Identification Number	El.podpis	5-15	3x
QPIN	PIN pro práci s kvalifikovanými certifikáty	El.podpis	5-15	3x
BOK	Bezpečnostní osobní kód	není spojen s eOP	4-10	3x

identita.cz

Zdroj: MONET+

Účel a hierarchie PINových objektů



Nastavení / odblokování PINových objektů

Zkratka	Prvotní nastavení	Autorizace nastavení	Odblokování	Autorizace odblokování
DOK	Na ORP (spolu s IOK)	Systém správy eOP	Na ORP (spolu s IOK)	Systém správy eOP
IOK	Na ORP (spolu s DOK)	Systém správy eOP	Na ORP (spolu s DOK), resp. doma	Systém správy eOP, resp. DOK
PUK	Doma (pouze 1x)	IOK	**NELZE**	N/A
PIN	Doma	PUK	Doma	PUK
QPIN	Doma	PUK	Doma	PUK

identita.cz

Zdroj: MONET+

DOK - Deblokační osobní kód

- Pro odblokování hodnoty IOK
- Nastavuje se na ORP (např. při převzetí eOP, anebo kdykoli potom)
  - Společně s IOK
- Zablokovaný DOK lze odblokovat na ORP
  - Nastavuje se i nový IOK
  - Lze i opakovaně
- DOK lze změnit na uživatelském PC (po zadání platné hodnoty DOK)

Zdroj: MONET+

IOK - Identifikační osobní kód

- Pro schvalování (autorizaci) identifikační operace
  - A vyčtení identifikačního certifikátu
- Nastavuje se na ORP (např. při převzetí eOP, anebo kdykoli potom)
  - Společně s DOK
- Zablokovaný IOK lze odblokovat:
  - na ORP (společně s DOK)
  - na PC uživatele (autorizace pomocí DOK)
  - Lze i opakovaně
- IOK lze změnit na uživatelském PC (po zadání platné hodnoty IOK)
- Pomocí IOK se autorizuje prvotní nastavení PUK

Zdroj: MONET+

PUK - PIN Unblocking Key

- Pro odblokování hodnot PIN a QPIN
- Nastavuje se na uživatelském PC, autorizace pomocí IOK
  - Nastavení lze provést právě 1x
- **Zablokovaný PUK nelze odblokovat!**
  - PIN a QPIN lze používat i po zablokování PUK
  - Pokud se PIN či QPIN zablokují (nebo nejsou nastaveny), nelze bez PUK provozovat
- PUK lze změnit na uživatelském PC (po zadání platné hodnoty PUK)

Zdroj: MONET+

PIN - Personal Identification Number

- Pro schvalování (autorizaci) operací s klíči a certifikáty
  - Vytváření klíčů
  - Zápis dat do čipu (zápis certifikátu, …)
  - Operace s ne-kvalifikovanými klíči
- Nastavuje se na PC uživatele; autorizace pomocí PUK
- Zablokovaný PIN lze odblokovat:
  - na PC uživatele (autorizace pomocí PUK)
  - Lze i opakovaně
- PIN lze změnit na uživatelském PC (po zadání platné hodnoty PIN)

Zdroj: MONET+

QPIN - PIN pro práci s kvalifikovanými certifikáty

- Pro schvalování (autorizaci) operací s klíči kvalifikovaných certifikátů
  - Kvalifikovaný podpis
- Nastavuje se na PC uživatele; autorizace pomocí PUK
- Zablokovaný QPIN lze odblokovat:
  - na PC uživatele (autorizace pomocí PUK)
  - Lze i opakovaně
- QPIN lze změnit na uživatelském PC (po zadání platné hodnoty QPIN)

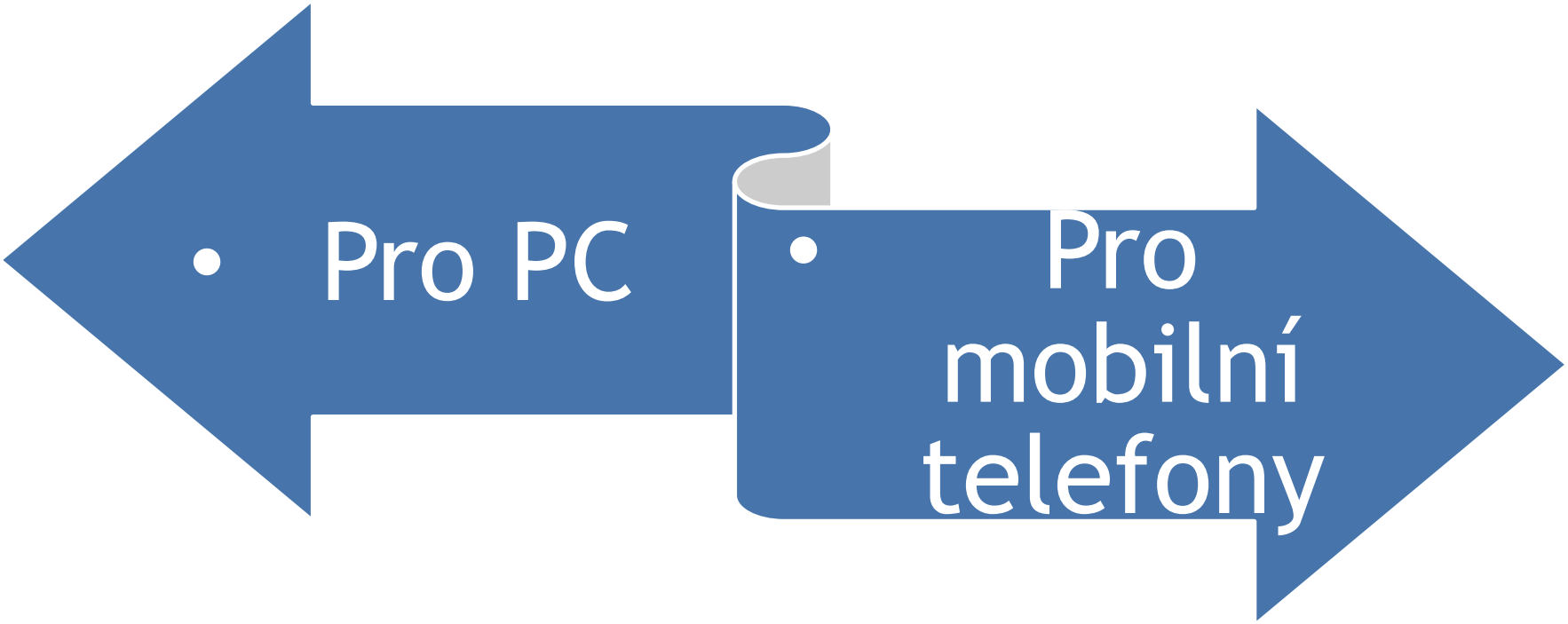
Zdroj: MONET+

KLIENTSKÉ APLIKACE PRO PODPORU EOP

identita.cz

Zdroj: MONET+

Klientské aplikace



identita.cz

Zdroj: MONET+

Klientské aplikace pro podporu eOP

Název	Účel	PC	Mobilní telefon
eObčanka	Elektronická identifikace	Ano	Ano
Správce karty	Správa dat podpisové aplikace + PINových objektů	Ano	Ne
Ovladače karty	El. Podpis, přihlašování, dešifrování v aplikacích 3.stran	Ano	Ne
Správa kvalifikovaných certifikátů	Získání kvalifikovaného certifikátu	Ano	Ne
Podpisové SDK	Elektronický podpis na mobilním telefonu	Ne	Ano

Vazba klientských aplikací a aplikací v čipu

eObčanka (PC)

eObčanka (mobilní)

Správa kvalifik. certifikátů (PC)

Podpisové SDK (mobilní)

Identifikační funkce

El.podpis / práce s certifikáty

Ovladače karty (PC)

Správce karty (PC)

Podporované platformy

PC

07/2018

10/2018

10/2018

Mobilní

identita.cz

Zdroj: MONET+

Instalace aplikací

PC

- Stažení z webu podpory eOP
- Grafický instalační průvodce
  - Resp. obvyklý instalátor pro daný OS
- Práva správce operačního systému
- Všechny aplikace se instalují jedním instalátorem
  - Instaluje se i příslušný framework
  - ~ 80 MB

Mobilní telefon

- Stažení z aplikačního store
- Obvyklý způsob instalace mobilní aplikace
- Pouze eObčanka
  - Mobilní SDK není určeno k instalaci koncovým uživatelům

identita.cz

Zdroj: MONET+

Žurnál a diagnostika

PC

- Aplikace generují žurnál
  - Důležité informace o prováděné činnosti
  - Nezbytné pro odhalení problému
- eObčanka a Správce karty generují také diagnostiku prostředí
- eObčanka a Správa kval.certifikátů umí poslat soubor se žurnálem, resp. diagnostikou na podporu

Mobilní telefon

- Standardní crash report
  - Dostupné přes web platformy
- Statistika havárií atd…

identita.cz

Zdroj: MONET+

Čtečka čipových karet

- Pro komunikaci s kontaktním čipem je čtečka nezbytná
  - Připojení konektorů čtečky k čipu
  - Propojení čipu se zařízením a aplikacemi
- Volba čtečky + zprovoznění je na uživateli
  - Nejednotnost použitých čteček
  - Nelze připravit příručky pro zprovoznění
  - Asi největší zdroj problémů
  - Hledání řešení bez možnosti vyzkoušet na konkrét
- Čtečky mají standardizované rozhraní
  - PC konektor = USB
  - Připojení k mobilnímu telefonu přes Bluetooth
  - Komunikační standard PC/SC (podporováno na PC)
- Ne všichni výrobci čteček důsledně dodržují standardy
  - Ne všechny čtečky jsou stejně kvalitní
- Oficiálně nejsou čtečky předmětem podpory
  - Ale bez funkční čtečky nefungují aplikace

identita.cz

Zdroj: MONET+

eObčanka – identifikace pomocí eOP

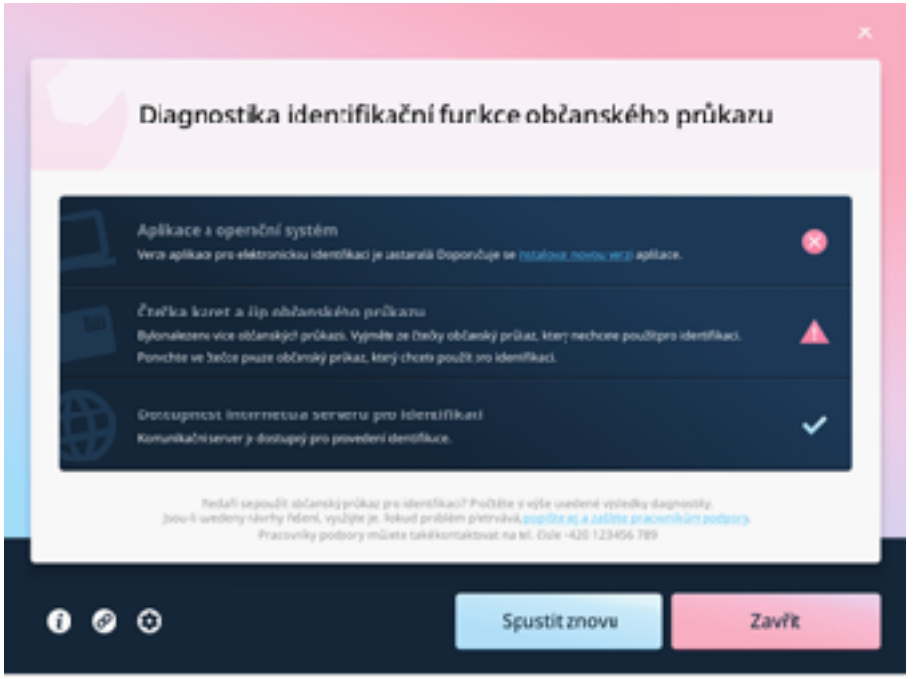
- Uživatel se chce přihlásit na webové stránky
- Webové stránky přesměrují na Národní bod a pak na stránku pro přihlášení pomocí eOP
- Spustí se aplikace eObčanka
- Vyzve uživatele k připojení čtečky + vložení eOP
- Uživatel schválí přihlášení zadáním IOK
- Čip eOP komunikuje se serverem (prostřednictvím eObčanka)
  - Kryptograficky zabezpečená komunikace, autentizace
  - Z čipu se vyčte identifikační certifikát
- Na základě kryptogramů a identifikačního certifikátu server důvěřuje připojenému klientovi
- Předá webovým stránkám informace o přihlášeném uživateli

identita.cz

Zdroj: MONET+

eOběanka p

- Kromě identifikace také diagnostický mód
  - Uživatel může vygenerovat diagnostiku
  - Po manuálním spuštění
  - Detekce problémů
  - Jednoduché návrhy řešení
- Možnost odeslat problém na podporu
  - Přiložit žurnál i diagnostiku
- Nejen pro identifikaci, ale také pro detekci a řešení problémů



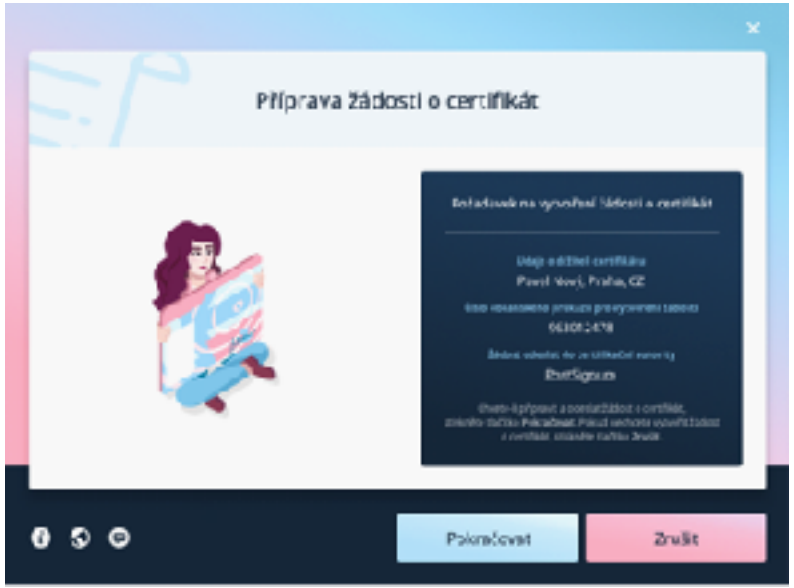
Správce karty – správa dat v čipu

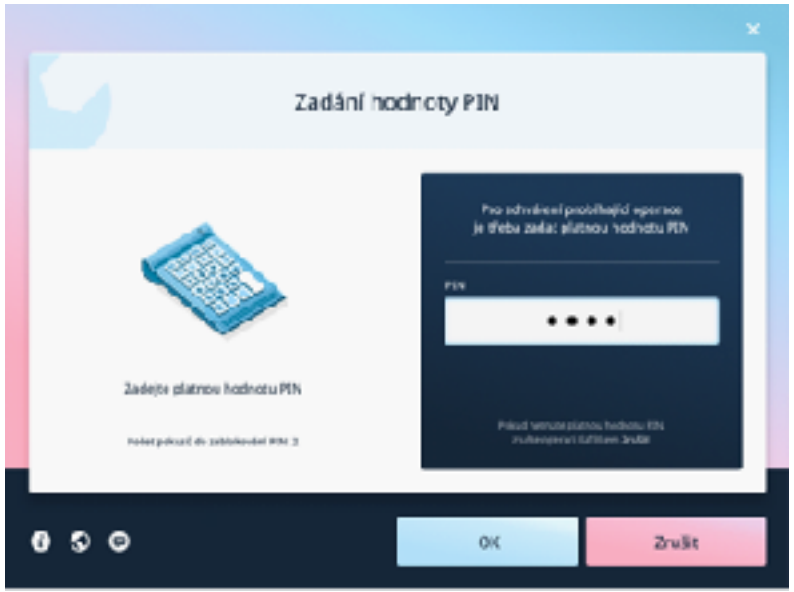
- Načtení a zobrazení obsahu čipu
  - Hierarchická struktura dat + podrobnosti
  - Certifikáty a klíče k certifikátům
- Správa PINových objektů
  - Nastavení / změna / odblokování
- Smazání certifikátu + klíče
- Import certifikátu + klíče
- Test klíče

- Návrhy problémových stavů
- Diagnostika karty + prostředí
  - Použít pro řešení problémů

Správa kvalifikovaných certifikátů

- Umožní uživateli získat kvalifikovaný certifikát
  - Průvodce vydáním certifikátu
- Komunikace s CA
  - Zatím není stanoveno, jaká CA
- Pokud nemá uživatel nastavené PINové hodnoty, snaží se navést uživatele k nastavení
- Generuje žurnál a jednoduchou diagnostiku
- Návrhy řešení problémů
- Možnost odeslat problém na podporu





Očekávané problémy

- Potíže s připojením čtečky, ovladače čtečky
  - Zprovoznění bluetooth čtečky na mobilním telefonu
  - Snaha o použití nesprávného typu čtečky (čtečka paměťových karet, …)
- Záměna se starší verzí eOP
- Potíže s instalací aplikací
  - Nesprávný instalační balíček
  - Absence páv správce
- Zablokování / zapomenutí PINových objektů
  - Použití nesprávného PINového objektu
- Nenastavené PINové objekty
- Neschopnost získat certifikát

- …obecně spíše problémy se zprovozněním, než nefunkčnost aplikací

Zdroj: MONET+

identita.cz

SPRÁVA ZÁKLADNÍCH REGISTRŮ

K čemu bude elektronická identita:

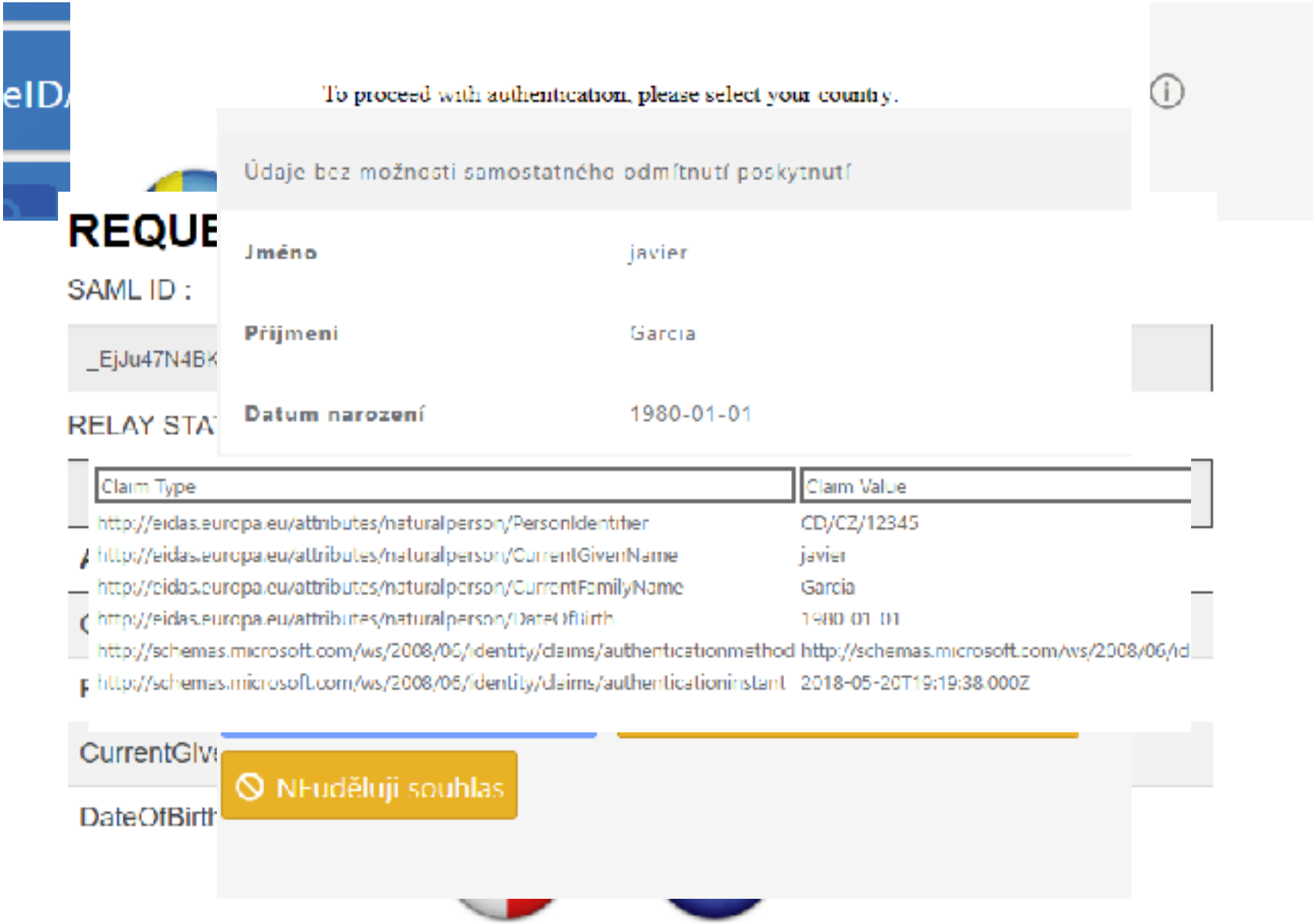
- všechna **podání** do VS (kromě anonymních) se musí činit **jménem žadatele** (**subjektu údajů**)
- pokud je podání činěno vzdáleně, je třeba mít **spolehlivou** vzdálenou el. **identifikaci**
- protože tento úkon se neustále **opakuje**, je vhodné, aby vzdálená identifikace byla **univerzální sdílenou službou**, **poskytující** spolehlivou **autentizaci** jako **subdodávku** pro další volající služby
- pro občany ČR a cizince s trvalým pobytem je identita reprezentována záznamem **v ROB**
- k jedné identitě může být **více ID prostředků**, pomocí kterých se identita prokazuje

SPRÁVA ZÁKLADNÍCH REGISTRŮ

Co přináší národní bod občanům?

- **svobodu** při výběru identitního prostředku
- **kontrolu** nad přístupem k jeho identifikačním údajům:
  - bude moci zabránit výdeji svých identitních údajů při každé identifikaci
  - každou vlastní identifikaci bude vidět na ročním výpisu z ROB včetně subjektu, kde byla činěna

NÁRODNÍ BOD – přeshraniční uznávání eID, testování


To proceed with authentication, please select your country.
Údaje bez možnosti samostatného odmítnutí poskytnutí
Jméno
javier
Příjmení
Garcia
Datum narození
1980-01-01
Claim Type
Claim Value
http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier
CD/CZ/12345
http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName
javier
http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName
Garcia
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod
http://schemas.microsoft.com/ws/2008/06/id
2018-05-20T19:19:38.000Z
Nesouhlasím
Nudělují souhlas

Věříte?

Věřte!

- https://tnia.eidentita.cz/sep3/public/
- https://twww.eidentita.cz/vtmap

SPRÁVA ZÁKLADNÍCH REGISTRŮ

DĚKUJI ZA POZORNOST