ADUCID

JEDNODUŠE A PŘITOM BEZPEČNĚ ON-LINE

Chytrá identita v chytrém telefonu

Libor Neumann

7. září 2016 | ADUCID s.r.o.

ANECT

Co podstatného se stalo?

Eroze hesel

Login-name/password – nejrozšířenější identita v Internetu (přes 90% služeb)
Bezpečnost trvale klesá – více jak 95% hesel není silných

Entity, které autentizují uživatele MUSÍ nabízet autentizační mechanizmus, který rozšiřuje nebo je alternativou k heslům.

The IDentity Ecosystem Stearing Group (IDESG)
PPP projekt pod NSTIC, USA

Chytrá zařízení

Boom používání mobilních chytrých zařízení
Nové možnosti a nové výzvy
BYOD (Bring Your Own Device)

Chytré mobilní zařízení je nosičem identity v kybernetickém prostoru

- Dostatečný výpočetní výkon
- Kvalitní periferie
  - ✓ dotykový displej,
  - ✓ komunikace,
  - ✓ fotoaparát,
  - ✓ NFC,
  - ✓ čtečka otisku prstu,
  - ✓ GPS
  - ✓ a další
- Stále v pohotovosti v ruce uživatele

Různé použití identity na mobilním zařízení

Mobilní app

mGovernment - nový fenomén eGovernmentu
Identita pro mobilní app

Přínosy:

- Snížení nákladů
- Výkonnost
- Modernizace veřejného sektoru
- Pohodlí a flexibilita
- Lepší služby pro občany
- Možnost komunikovat s velkým počtem lidí

Webové rozhraní

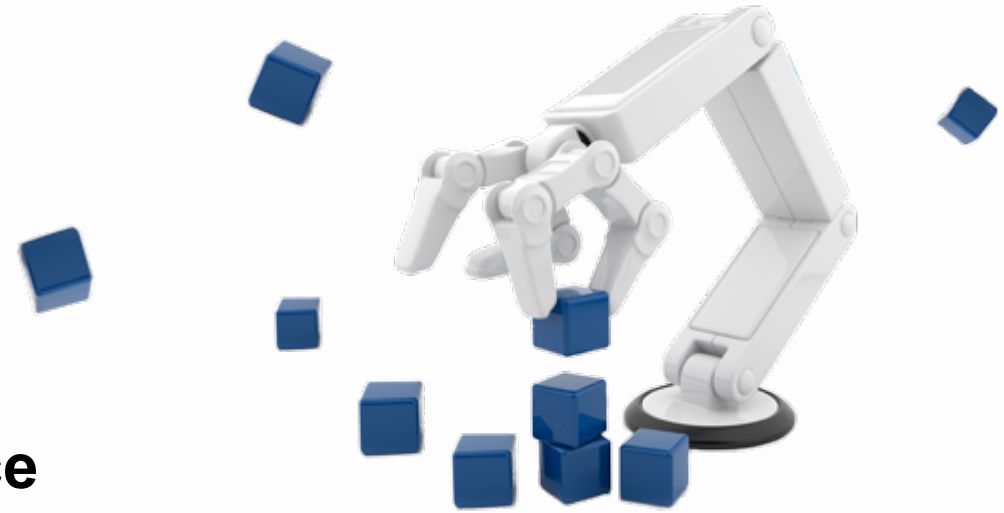
Identita na mobilním zařízení
Klasická webová aplikace + QR kód

Maximální automatizace ➡ jednoduché užití

Chytrý telefon je výkonný počítač !!!

Automaticky spravované identifikátory

- Uživatel nic nezadává
- Správce nemusí řešit konflikty
- Vestavěná ochrana soukromí



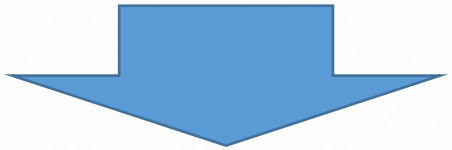
Automaticky spravované kryptografické klíče

- Uživatel se stará jen o své zařízení
- Bezpečnost řídí bezpečnostní správce

Logistika

BYOD
Občan má svůj chytrý telefon, pečuje o něj, běžně a rád ho používá

CzechPoint
Stačí jediná návštěva – ověření identity a registrace chytrého telefonu



Rychlý náběh elektronické identity
Penetrace chytrých telefonů v ČR je vyšší než 60%

Když se něco zhatí …

Nouzové stavy

Ztráta, porucha elektronické identity

- Výpadek cílových služeb pro občana
- Šance pro útočníka

Replika

Více zařízení jednoho uživatele

- Automatická detekce útoku
- Samoobsluha
- Bez výpadku cílových služeb

Osobní faktor – nový design druhého faktoru

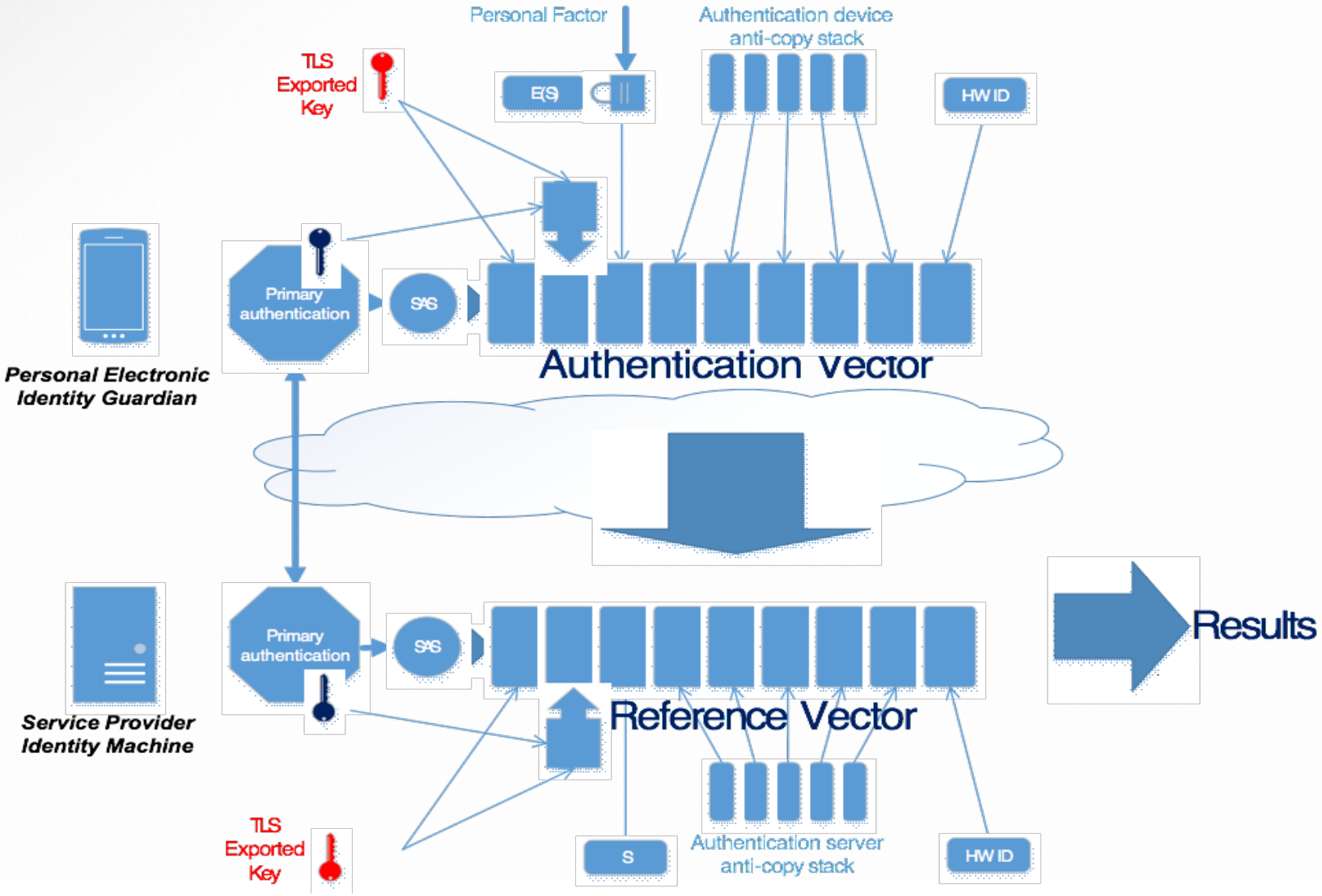
Prokazuje že nosič elektronické identity je ve správných rukách

Jediný faktor (pro všechny poskytovatele služeb i všechny repliky)
Adaptivní použití řízené poskytovatelem služby

Vysoká bezpečnost
- Tajná vrstva
- Náhodné rozložení na dotykové klávesnici
- Duální ověření – osobní faktor není nikde uložen

Dobrá zapamatovatelnost
- Historka z obrázků nebo číslice

Co se skrývá pod kapotou



ADUCID ANECT

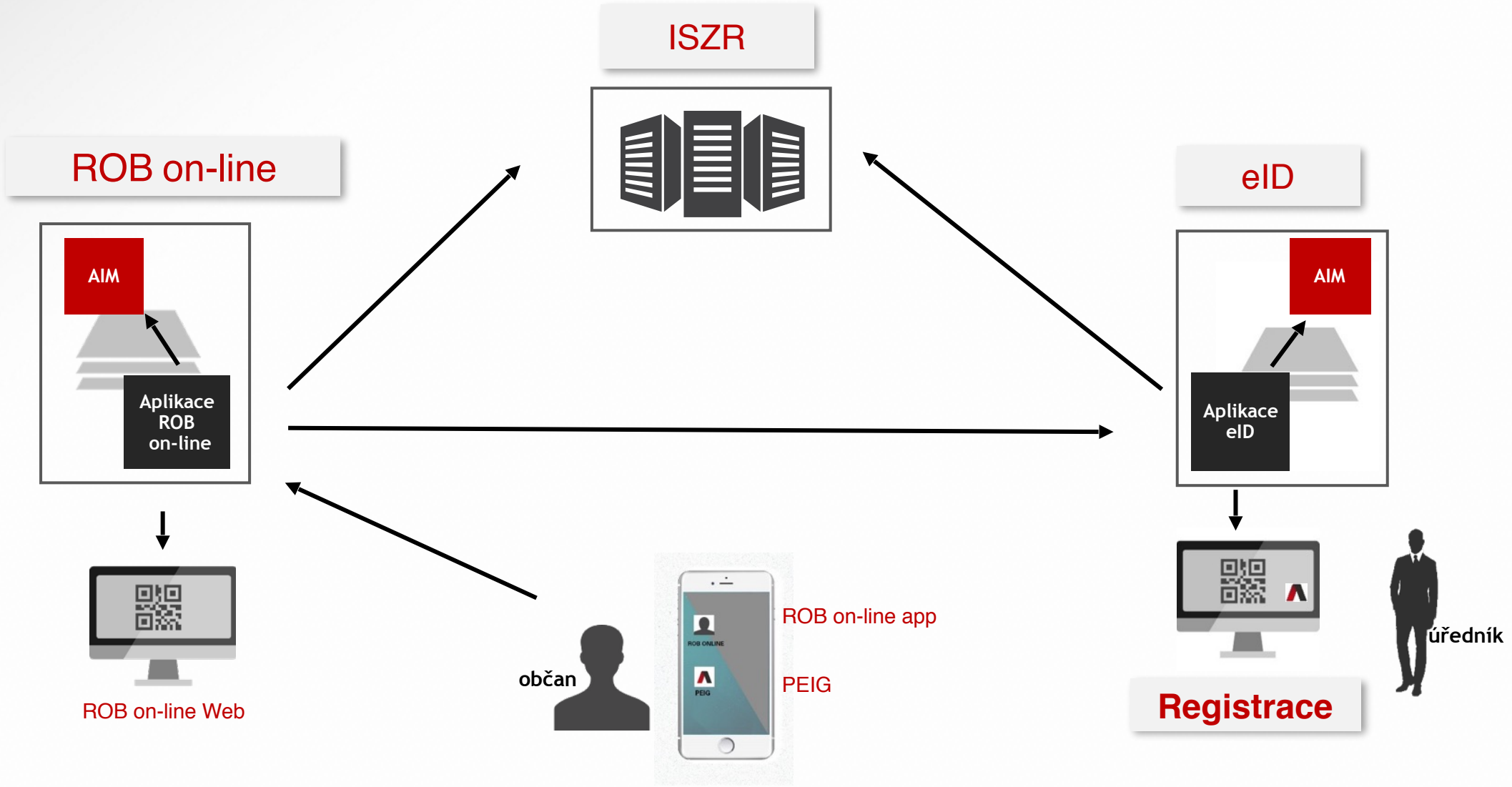
Děkuji za pozornost

Otázky…


ADUCID
JEDNODUŠE A PŘITOM BEZPEČNĚ ON-LINE

Backup slides …

Způsob implementace …



Funkční schéma ADUCID

- External authentication service

- Fully automated identifiers management
- Fully automated life-cycle of cyber-identities
- Mutual authentication using asymmetric cryptography
- Universal Cryptographic Protocol
- Independent cryptographic layer
- Built-in security management
- Integrated data channel binding with binding control