EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

Libor Neumann, ANECT a.s.

ALUCID a řízení bezpečnosti informačních systémů

Ministerstvo průmyslu a obchodu

OPPI

Agenda

- Celkový kontext
- Výsledky analýz současného stavu a trendů
- Základní principy
- Vrstvový model
- Ověření fyzické identity
- Systémová řešení
- Praktická ukázka

Kontext v rámci ISMS

- IAM (Identity and Access Management) je limitujícím faktorem celkové bezpečnosti – bez odlišení oprávněného uživatele od útočníka nelze aplikovat bezpečnostní opatření
- Omezování možností používat opatření fyzické bezpečnosti (lokální přístup -> vzdálený přístup)
- potřeba nahradit klasická opatření fyzické bezpečnosti ICT technologickými opatřeními –> vzdálená autentizace a autorizace

Kontext v rámci ISMS

- **Nové trendy**
  - Vzdálený přístup k interním systémům
  - ICT jako služba (hosting, cloud computing)
  - Rozšiřující se počet služeb ICT používaných jedním uživatelem
  - Personifikace služeb
  - Schopnosti koncového uživatele nelze vylepšit

- **Důsledky**
  - Autentizace a autorizace je limitujícím faktorem současné informační bezpečnosti
  - Koncový uživatel je limitujícím faktorem autentizace a autorizace

Analýza I – proč nová technologie?

- **Hledání vhodného produktu pro naše zákazníky**
- **Rok 2007 – systematická analýza v celoevropském kontextu**
- **6 kritérií:**
  - Orientace na uživatele (User Centricity)
  - Technologická neutralita
  - Škálovatelná úroveň bezpečnosti (včetně vysoké bezpečnosti)
  - Ochrana proti síťovým útokům
  - Ochrana soukromí
  - Podpora e-governmentu
- **Výsledek – žádná technologie nevyhovuje ve všech kritériích**

Analýza I – výsledky analýzy

	User-centric	Techno-logy neutrality	Scalable level of security, including high security	Network attacks protection	Privacy protect-tion	e govern-ment support
Login/password	No	Partially	No	No	No	No
One-time password	No	No	No scalability. High level of security.	Yes	Partially	No
Certificate	No	Yes	No scalability. High level of security.	Yes	Partially	Partially
Biometrics	Theoretic ally, yes	No	Currently no scalability. Middle level of security.	Currently unsolved	No	No
Federative ID	No	Yes	No scalability. High level of security.	Yes	Partially	No
Identity management	Local only	No	Yes	Yes	No	Local only
State-issued identity	No	No	No scalability. High level of security.	Yes	Partially	Yes

Analýza II – současné limity

- **Analýzy trendů a limitů při hromadném nasazování**
- **Principielní limity v oblasti vzdálené autentizace (komunikace člověk – počítač).**
  - Počítač pracuje při autentizaci s tajemstvím (secret).
  - V ICT není možné rozpoznat originál a kopii informace (ve skutečnosti se při vzdálené komunikaci přenáší kopie)
  - Lidské schopnosti práce s tajemstvím jsou limitovány
  - Stále platí Moorův zákon (růst výkonu ICT v čase)
  - Roste výkon a dostupnost ICT prostředků použitelných útočníky

Analýza II – faktory

- **Co jsem – biometrie**
  - Uživatelsky centristický
  - Spolehlivost klesá s růstem počtu osob
  - Neobsahuje tajemství – biometrické informace nelze chránit u zdroje
  - Neexistuje přijatelné zotavení při kompromitaci
- **Co znám – hesla, PIN,…**
  - Nejrozšířenější způsob
  - Potřeba pamatovat velké množství informace (více a komplikovanějších hesel měnících se v čase)
  - Entropie už dnes nevyhovuje
  - Kompromitace používáním – neschopnost člověka dělat kryptografické operace
- **Co mám – tokeny, karty, notebooky,..**
  - Rostoucí výkon miniaturních přenosných zařízení
  - Zvládá správu tajemství (secrets) s potřebnou entropií i kryptografické operace
  - Platí Moorův zákon – lze udržet tempo s útočníky

Analýza II – třetí strany

- **Certifikační autority, poskytovatelé identit, federace,…**
- **Organizační a logistické problémy závislých stran**
  - Atributy
  - Postupy ověřování
  - Zodpovědnost
  - Prosazení nápravných opatření
- **Komplikovaný organizační vztah 3 subjektů**
- **Princip důvěry (závislosti) není slučitelný s principy řízení informační bezpečnosti**

ALUCID® – základní principy

- Automatic Liberal User Centric electronic IDentity
- Navrženo od základů – ne vylepšování stávajícího
- Navrženo jako ICT infrastruktura metodami systémového návrhu
- Nové způsoby myšlení o eID – odděluje identifikaci od pojmenování
- Nové principy, nové metody
- Interní dynamika a externí stabilita

ALUCID® – základní principy

- Uživatelská centričnost – univerzálně použitelný token
- PEIG® - Personal Electronic Identity Gadget
- Plná automatizace celého životního cyklu eID
- Uživatelem téměř neviditelné fungování
- Nulový informační obsah eID – pseudonáhodná čísla
- Žádná třetí strana

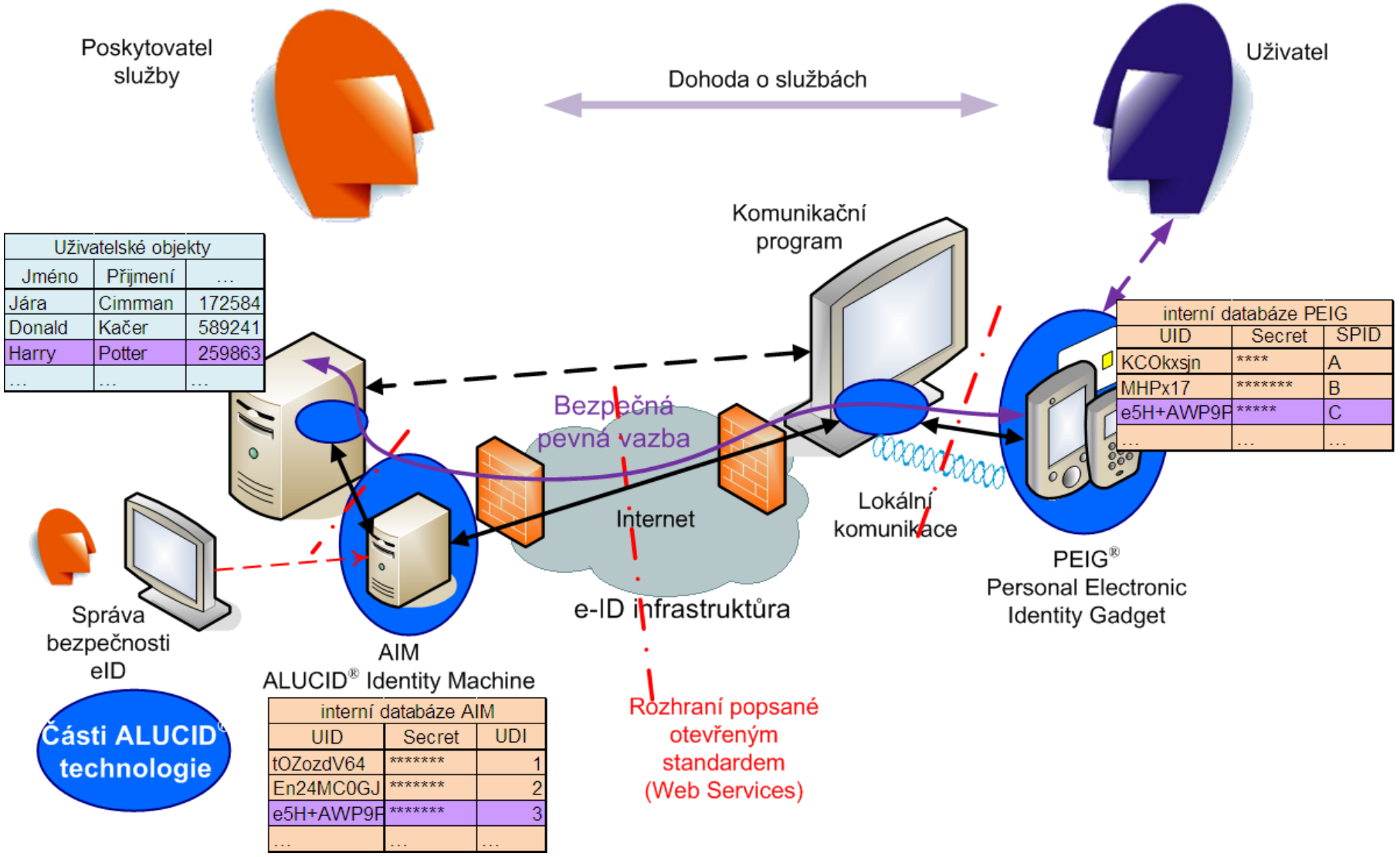
ALUCID® – základní principy

- Integrovaná automatizovaná správa bezpečnosti
- Kompletní autentizační služba pro aplikace (informační systémy)
- Rozhraní dle mezinárodních standardů (SOAP – WS)
- Standardní kryptografie
- Dobrovolné používání
- Otevřenost pro budoucí rozvoj

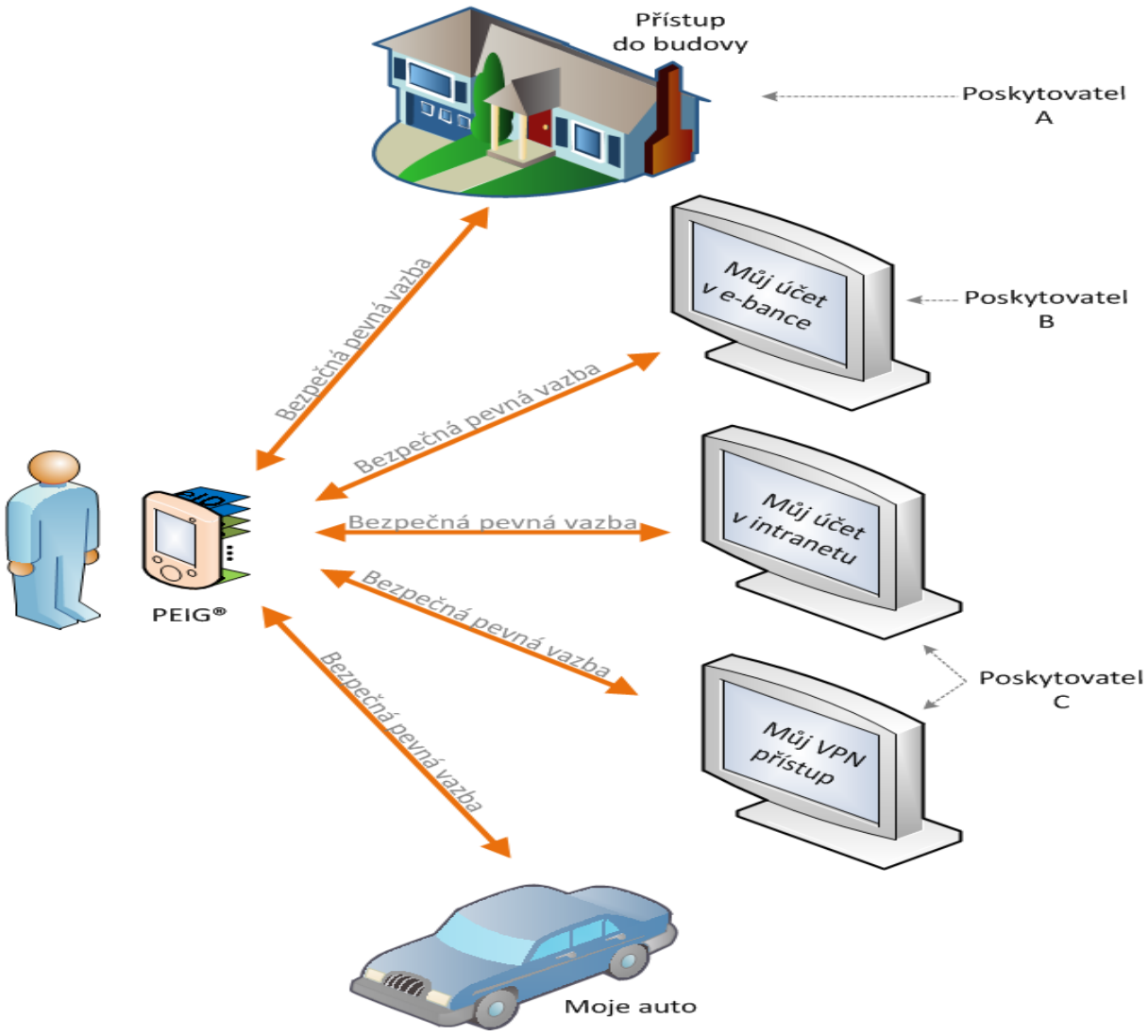
ALUCID® – základní principy

- **Dvě základní komponenty**
  - PEIG – univerzální zhmotněná elektronická identita v ruce uživatele
  - AIM – (ALUCID Identity Machine) – síťová služba elektronické identity pro poskytovatele (provozovatele ICT) – virtuální appliance
- **Dvě základní uživatelské abstrakce**
  - Permanent Secure Link – pevná bezpečná vazba mezi PEIG a interním záznamem v informačním systému
  - Personal Object – obecný kontejner pro informace o uživateli včetně potřebné funkčnosti

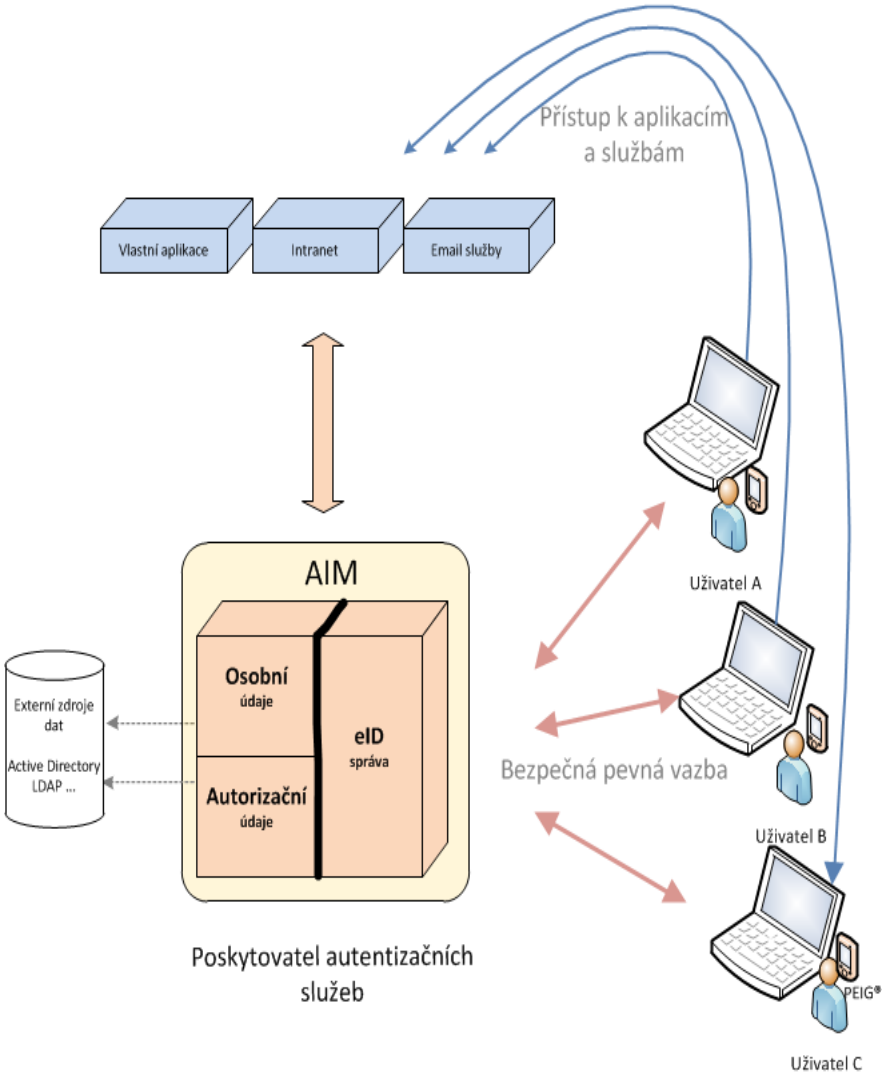
ALUCID® – základní principy



ALUCID® – pohled uživatele



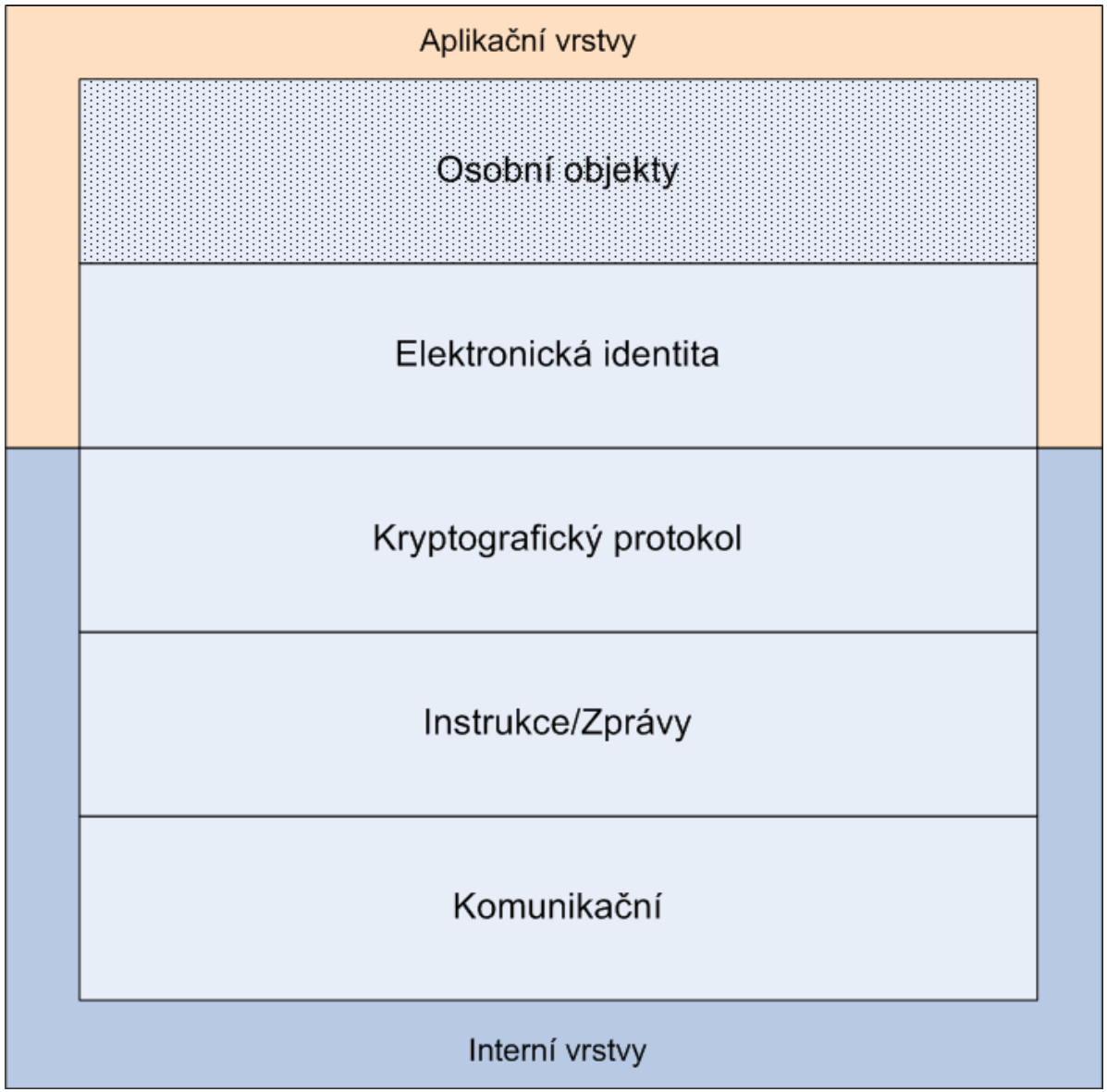
ALUCID® – pohled provozovatele ICT systému



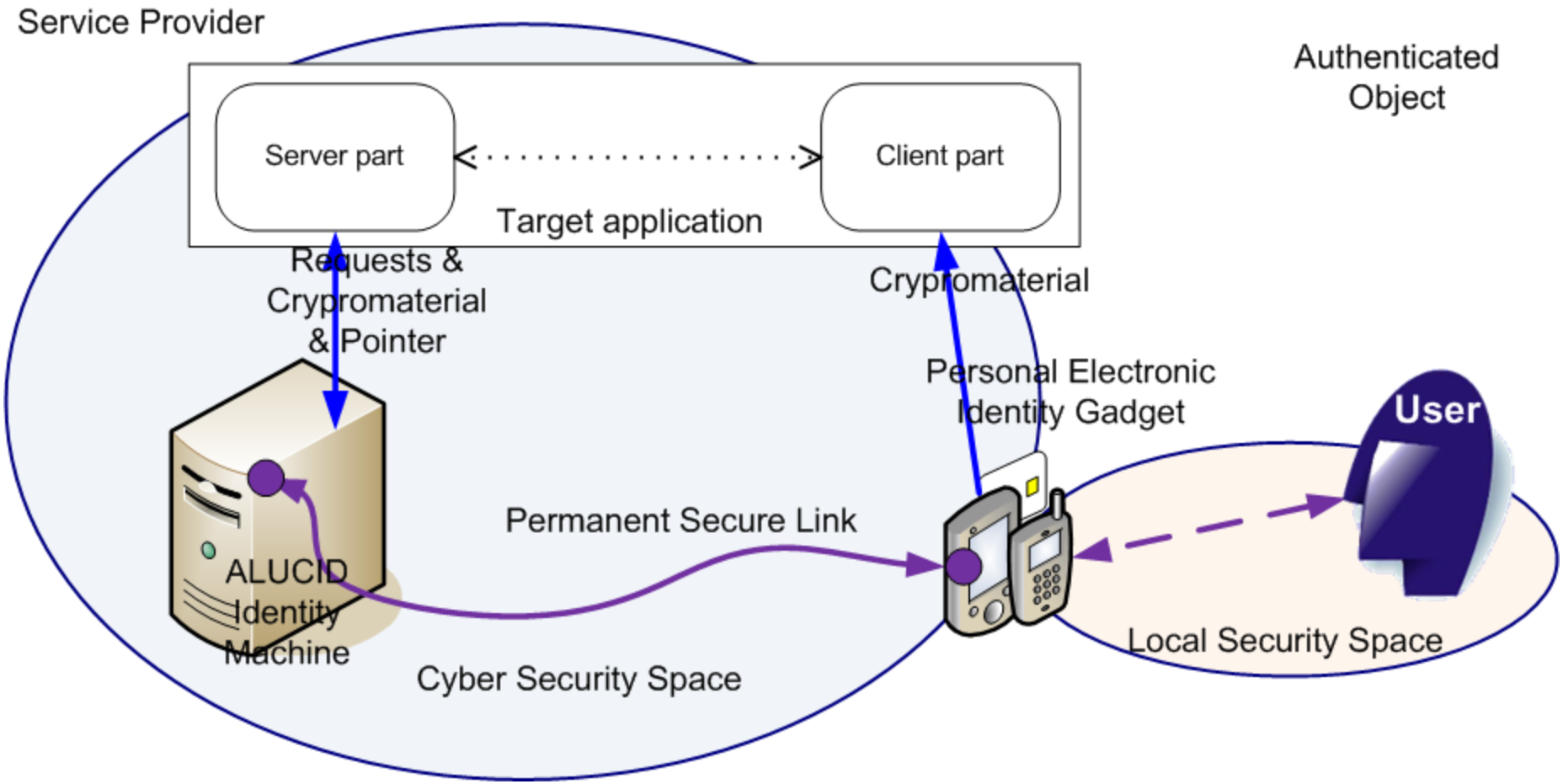
ALUCID® – vrstvový model

- **Standardní způsob popisu sítí**
- **Umožňuje zjednodušeně popsat složité systémy**
- **Každá vrstva popisuje specielní problematiku**
  - Používá služeb nižších vrstev
  - Poskytuje služby vyšším vrstvám (a cílovému užití)

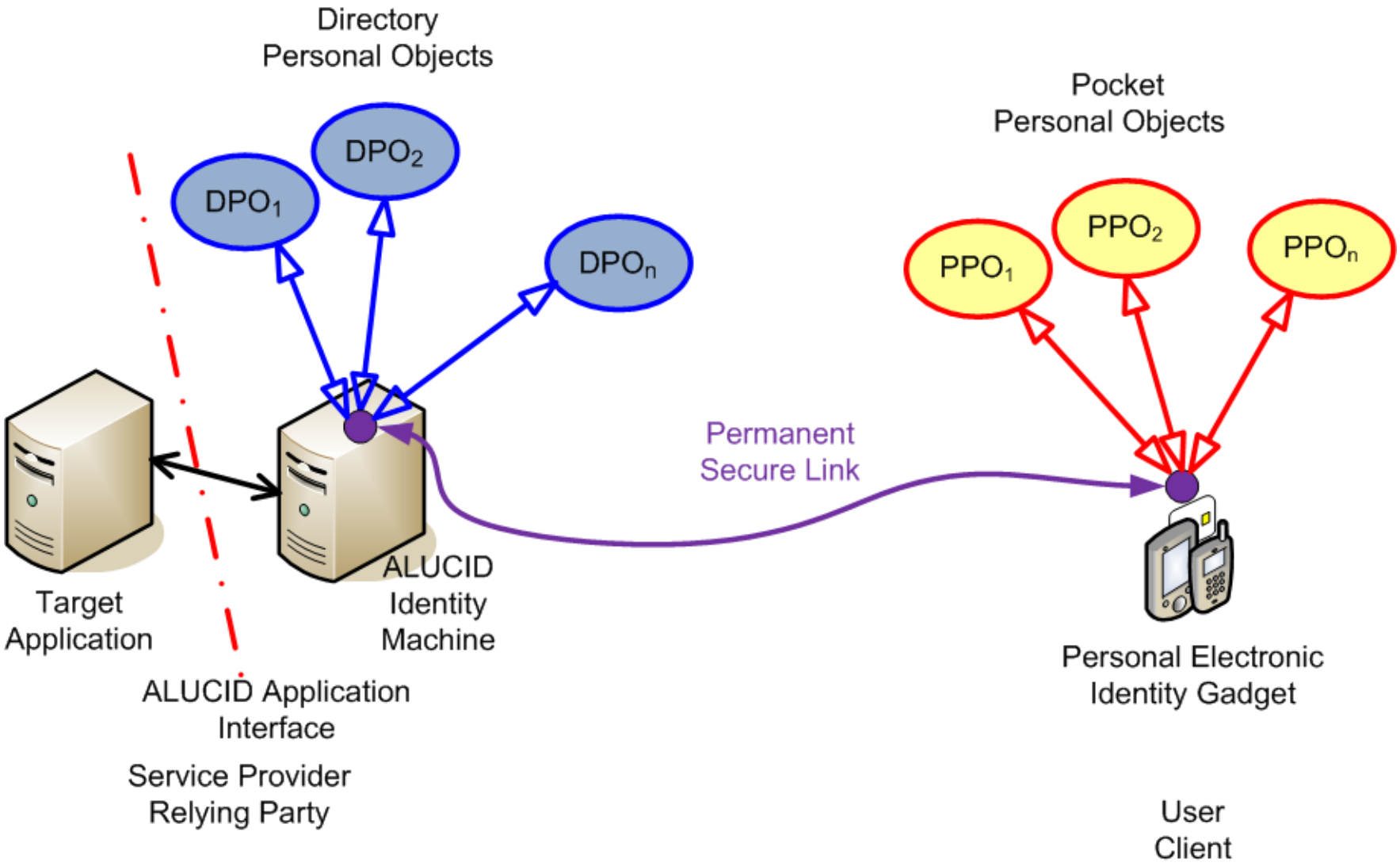
ALUCID® – vrstvový model



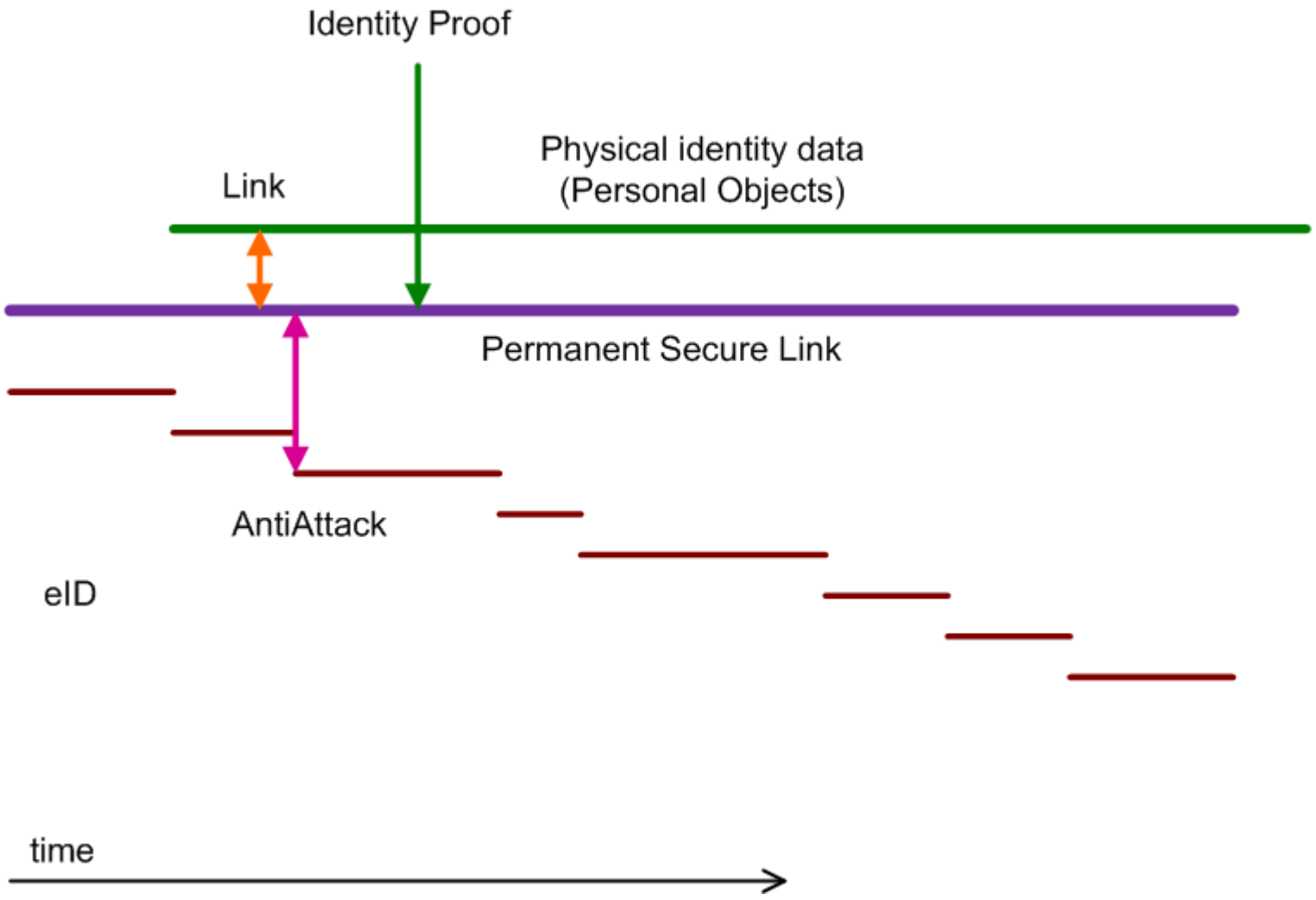
ALUCID® – vrstva elektronické identity



ALUCID® – vrstva osobních objektů



ALUCID® – životní cyklus identity

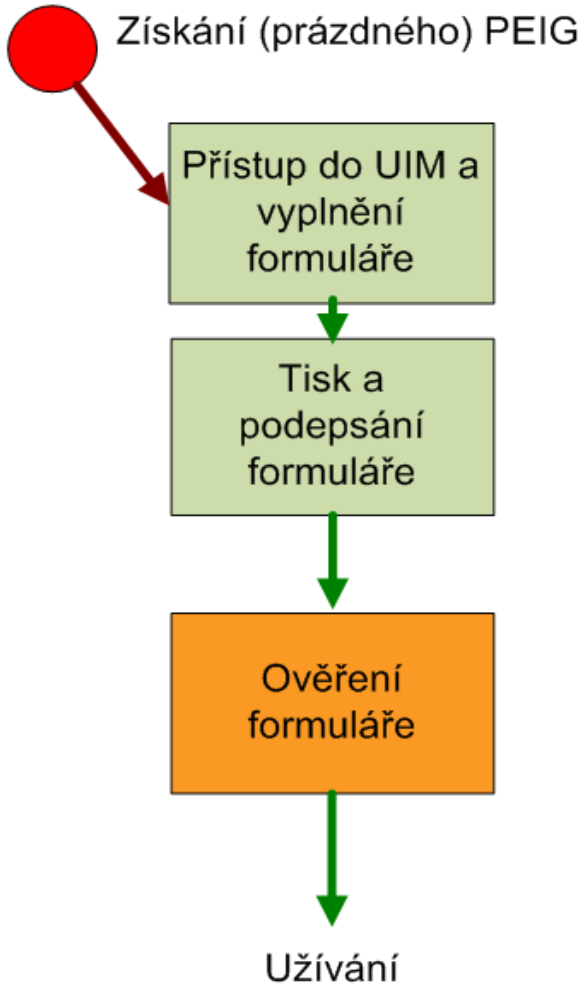


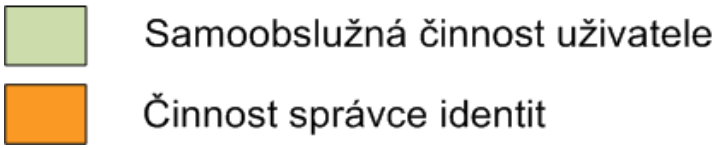
Ověření fyzické identity

- **Identity Proofing**
- **Bezpečné ověření údajů o fyzické identitě (a přístupových právech) a svázání elektronickou identitou**
- **UIM – User Identity Management**
- **Scénáře:**
  - Aktivační klíč
  - Podepsaný formulář

Scénář „Aktivační klíč“

Scénář „Podepsaný formulář“





Ošetření krizových stavů

Zajištění přístupu v nestandardní situaci

- dočasné zapomenutí PEIG
- poškození PEIG
- změna osobních údajů uživatele
- vypršení platnosti prostředků elektronické identity

Řešení:

- náhradní /rezervní PEIG
- nova verifikace údajů bez změny el. identity
- automatické prodlužování platnosti

Zamezení přístupu v nestandardní situaci

- ztráta / odcizení PEIG (HW nosiče)
- pokus o neoprávněný přístup s odcizeným PEIG
- ukončení pracovního poměru, ukončení oprávnění přístupu, změna oprávnění

Řešení:

- přechodné zablokování přístupu
- zničení elektronické identity při zneužití
- změna přístupových práv přímo v databázi

Systémová řešení

- **Integrace s cílovými aplikacemi**
  - Adaptery
  - Přizpůsobení aplikace
- **Sdílení správy uživatelů**
  - Sdílený AIM
  - Provázání fyzických identit bez propojení elektronických identit - Identity Link
- **Vícevrstvá ochrana IS**

Shrnutí

- Technologie ALUCID je přihlášena na patentových úřadech v EU, Spojených státech, Brazílii, Číně, Indie, Mexiku, Kanadě, Japonsku, Rusku
- První pilotní implementace:
  - Ministerstvo kultury ČR (od r. 2009),
  - Krajský úřad kraje Vysočina – krajský projekt eHealth (od 12/2010)
- Spolupráce s odborníky: např. kryptografie - RNDr. Vlastimil Klíma

- ANECT je členem mezinárodního konsorcia projektu PASSIVE financovaného Evropskou komisí (Policy-Assessed system-level Security of Sensitive Information processing in Virtualized Environments); cílem projektu je vývoj řešení nebo metody pro zpracování citlivých informací ve virtuálním prostředí. ALUCID bude využit jako nástroj pro autentizaci (6/2010 – 6/2012).
- ANECT je členem evropské tematické sítě SSEDIC (Scoping the Single European Digital Identity Community) podporované Evropskou komisí (od 6/2010), jejímž cíle je formulovat podklady pro strategii univerzální evropské elektronické identity.

Praktická ukázka

Děkuji za pozornost

Otázky?

Komentáře?

ALUCID přibližuje digitální svět všem - bez potřeby technických znalostí