EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

Libor Neumann, ANECT a.s.
Petr Pavlinec, KÚ Vysočina

Praktické zkušenosti s nasazením silné autentizace ALUCID ® na KÚ Vysočina v oblasti eHealth.

Ministerstvo průmyslu a obchodu

OPPI

Agenda

- motivace pilotního projektu
- ALUCID ® = automatická elektronická identita; technologické principy, vlastnosti, výklad pojmů
- co předcházelo reálnému nasazení na KÚ Vysočina – scénáře pro založení uživatelů
- ošetření krizových stavů
- integrace s cílovou aplikací
- zkušenosti z realizace pilotního projektu, úskalí a přínosy

Motivace pilotního projektu

Koncepce eHealth kraje Vysočina	- **koncepce eHealth – tendr na aplikaci DRG**
	- **Prostředí zdravotnictví:**
	  - citlivé osobní údaje
	  - uživatelé bez specielních IT dovedností

Pohled uživatele	- **uživatelsky jednoduchá autentizace do aplikace DRG**
Pohled správce aplikace	- **jednoduchá a bezpečná správa identit uživatelů a řízení přístupových práv**

ALUCID ® – klíčové pojmy a principy

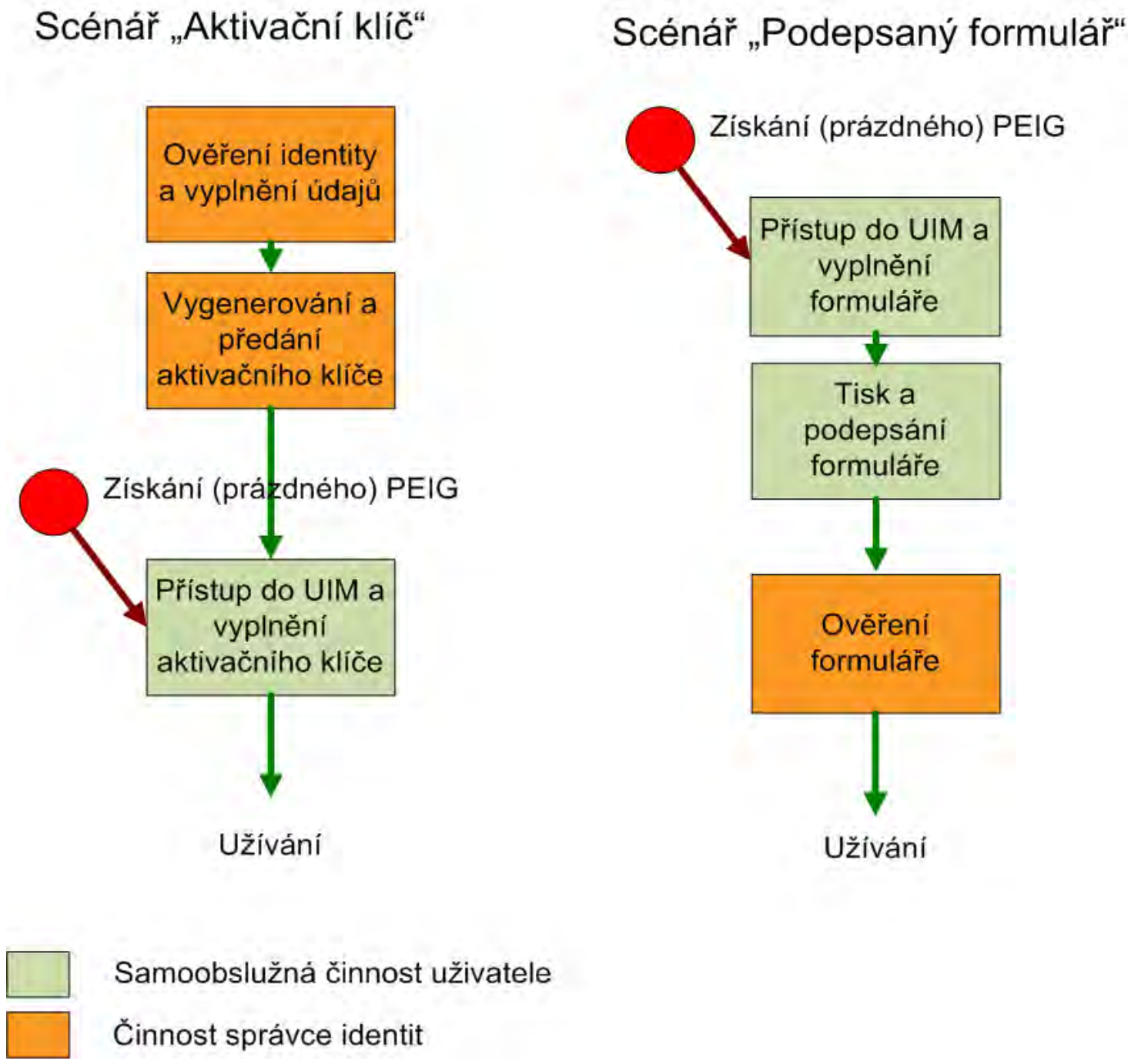
Vlastnosti	- automatická elektronická identita se silnou autentizací - elektronická identita je zcela nezávislá na skutečné identitě uživatele - jediné zařízení pro řadu služeb s odlišnými požadavky na úroveň zabezpečení
Základní prvky (pojmy)	- PEIG = Personal Electronic Identity Gadget – personalizovaná elektronická identita uložená ve zvoleném mobilním zařízení - AIM = ALUCID Identity Machine – poskytuje elektronickou identitu jako službu cílové aplikaci
Klíčové principy	- Pevná bezpečná vazba (permanent secure link = PSL) mezi PEIG® uživatele a cílovou aplikací - Plně automatizované řízení elektronické identity v průběhu celého životního cyklu - Správa bezpečnostních parametrů

ALUCID® = Automatic Liberal and User Centric Electronic IDentity

Co předcházelo nasazení na KÚ Vysočina

Analýza požadavků	- jak poznat, kdo je kdo, jaké přístupové právo má komu být přiděleno - potřeba správy uživatelů nezávislé na aplikaci (pro následné využití v dalších aplikacích) - zautomatizovat proces autentizace, vyloučit lidský faktor z celého životního cyklu elektronické identity
User Identity Management	- proces správy uživatelů – potřeba vyřešit rozporný požadavek zvýšení bezpečnosti a současně zjednodušení pro uživatele - scénář „aktivační klíč“ - scénář „podepsaný formulář“

ALUCID® vychází z životních situací fyzického světa a maximálně využívá možností kyberprostoru


Scénář „Aktivační klíč“
Ověření identity a vyplnění údajů
Vygenerování a předání aktivačního klíče
Získání (prázdného) PEIG
Přístup do UIM a vyplnění aktivačního klíče
Užívání
Scénář „Podepsaný formulář“
Získání (prázdného) PEIG
Přístup do UIM a vyplnění formuláře
Tisk a podepsání formuláře
Ověření formuláře
Užívání
Samoobslužná činnost uživatele
Činnost správce identit

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

Integrace s cílovou aplikací

SWLab DRG	- speciální webová aplikace (Java, standardní web server) - klasická autentizace login/pasword - integrace byla brzděna implementací ALUICID
Rozhraní ALUCID ®	- standardní webová služba (Web service SOAP) - implementace SOAP se ukázal jako zbytečně pracný - užití knihovny Java objektů (SDK)

Přístupová práva k cílové aplikaci se uživateli přidělují jediným atributem v UIM. Pokud tento atribut není vyplněn, uživatel nemá právo přistoupit k cílové aplikaci pomocí ALUCID ®. To nijak neblokuje používání ALUCID ® v jiných aplikacích.

ALUCID® shrnutí zkušeností z pilotního projektu – úskalí a přínosy

Podněty pro komerční release ALUCID2011

- Zjednodušení instalace – ALUCID® je dodáván ve formě virtuální appliance
- Součástí produktu jsou prostředky usnadňující integraci do web aplikací
- Součástí dodávky je instalátor PEIG, sloužící k vytvoření PEIG pro uživatele

Podněty pro budoucí vývoj

- Vývoj prostředků pro snazší integraci ALUCID® se standardními systémy
- Návrh nových funkcionalit, které v jiných autentizačních mechanismech neexistují (replikace PEIG, možnost opakovaného využití verifikované identity mezi systémy)
- Požadavek automatizované správy a bezpečné distribuce prostředků elektronického podpisu

Přínosy

- Ověření implementace v prostředí jedné aplikace pro několik organizací
- Vyřešení základních problémů využití nové technologie v prostředí eHealth

Závěr

Poděkování

Odboru informatiky Krajského úřadu Vysočina

i dodavateli cílové aplikace firmě SWLab, s.r.o.

za vstřícnost a trpělivost při přípravě a realizaci pilotního projektu nasazení ALUCID®.

ALUCID® přibližuje digitální svět všem - bez potřeby technických znalostí