
ORACLE®

eIDAS - zkušenosti s implementací řízení přístupu a federací identit

ISSS 2016 – Hradec Králové

Miloš Matůš

Petr Zeman

Aleš Novák

3. dubna 2016

eIDAS - zkušenosti s implementací řízení přístupu a federací identit

Případové studie řešení bezpečného přístupu občanů k veřejným službám:

- Portály nizozemského ministerstva hospodářství a zemědělství
  - Využití eID pro poskytování přístupu k veřejným službám
- Ústřední portál veřejné správy Slovensko
  - Poskytovatel eID pro eGoverment na Slovensku

Představení zákazníka

- MinEZ (Ministerie van Economische Zaken)
  - Sloučené ministersto hospodářství a zemědělství v Nizozemsku
- Webové a mobilní aplikace ministerstva a podřízených organizací
- Přístup osob a zaměstnanců
- eID role – Service Provider

Government of the Netherlands

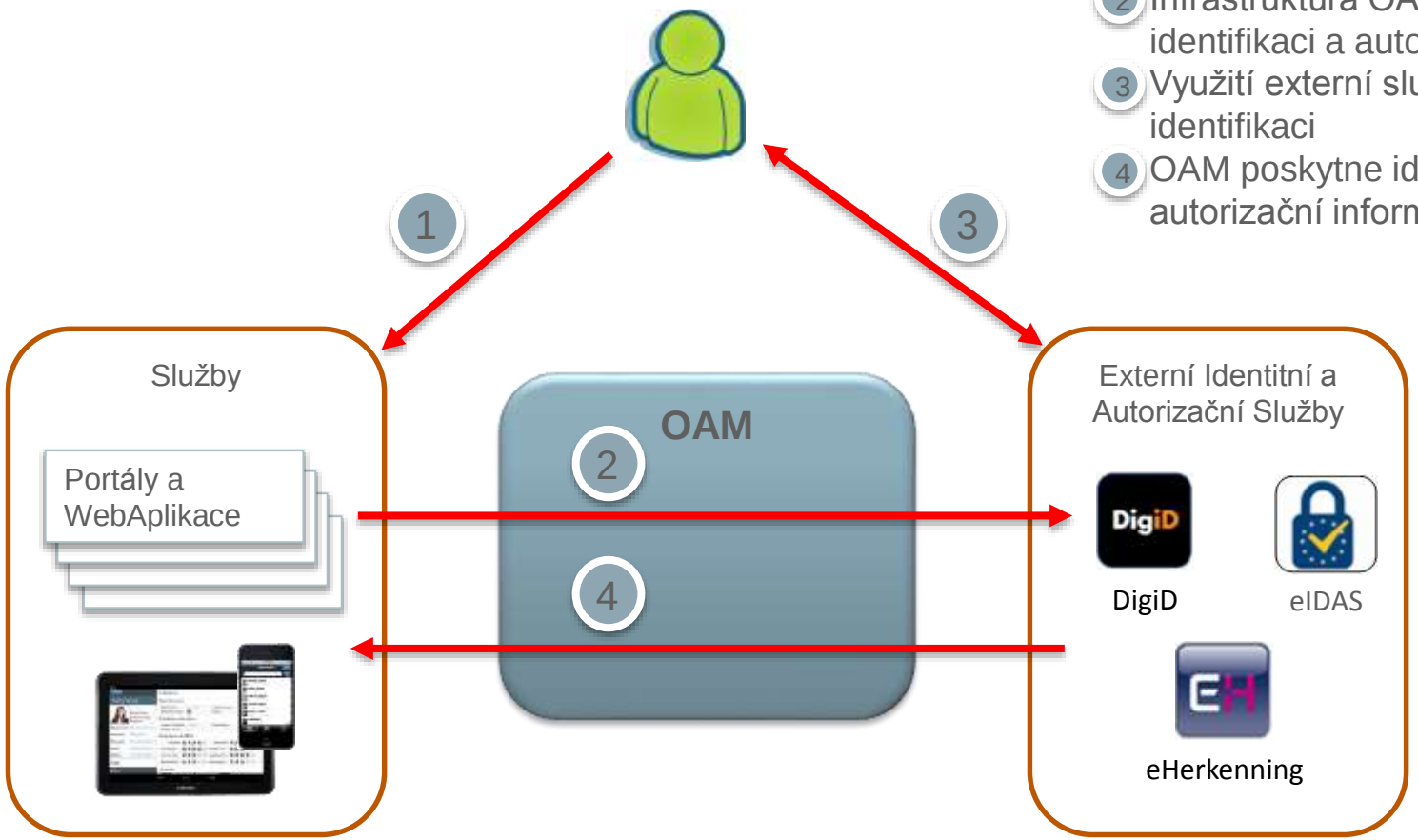
Výchozí stav a cíle řešení

- „Problémy“
  - Velké množství různorodých přihlašovacích mechanismů a řešení.
  - Jen některé aplikace podporovaly národní identity providery (eHerkenning a DigiD).
  - Problematický přístup k aplikacím v rámci EU (eIDAS - eID, STORK-PEPS), 09/2018.
  - Nekompatibilita řešení s národními bezpečnostními audit požadavky.

- Cílový stav
  - Implementace řešení jednotného digitálního přístupu ke službám ministerstva a podřízených organizací nejen prostředky eID.
  - Přístup jak pro Nizozemské tak i pro jiné subjekty v rámci EU prostředky eID.
  - SSO(Single Sign-On) řešení dostupné (24x7).
  - Periodicky auditované prostředí dle národního bezpečnostního centra pro kybernetickou bezpečnost (Nederlandse Orde van Register EDP-Auditors)

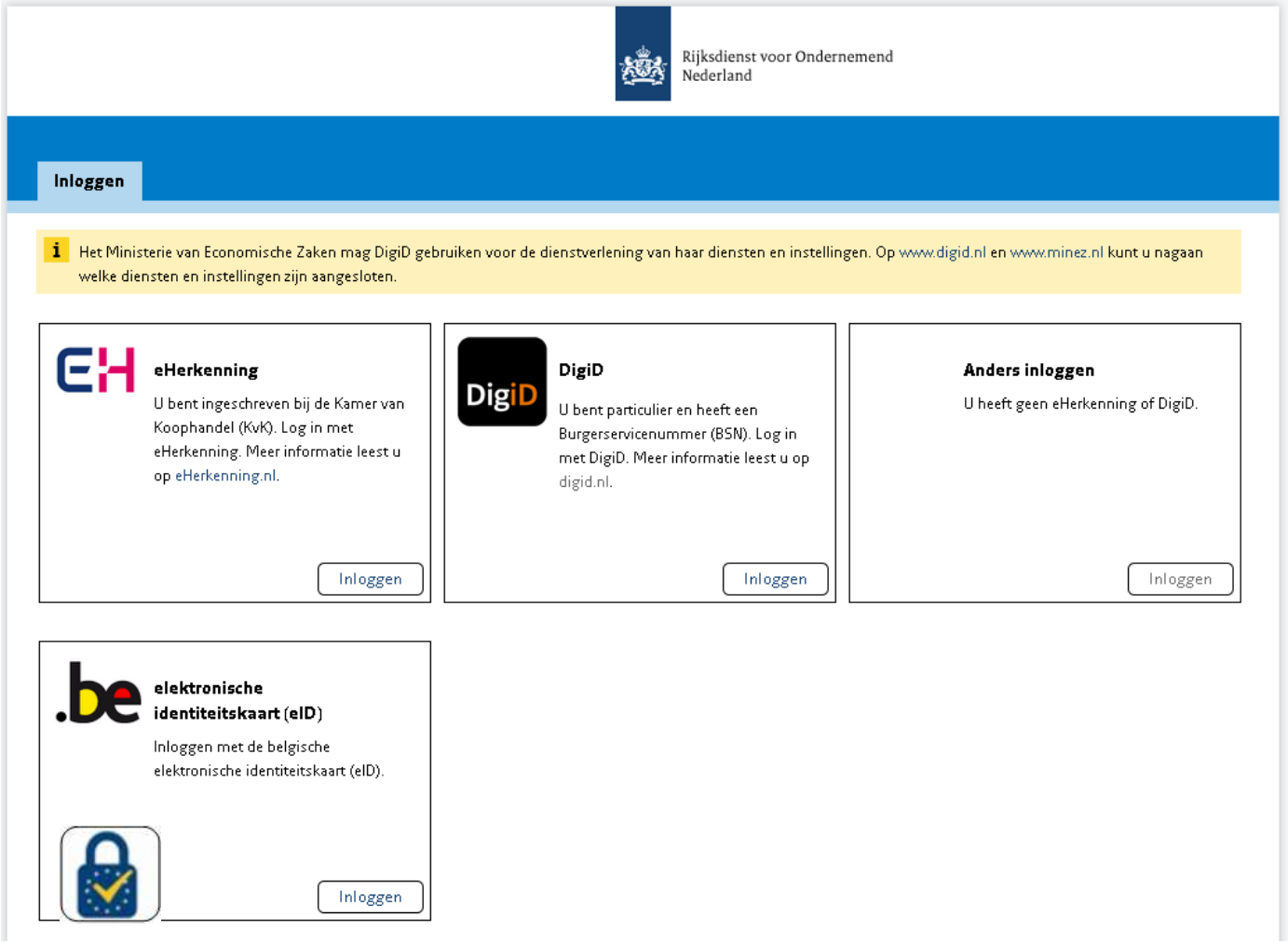
Popis řešení - produkt Oracle Access Manager (OAM)

1. Osoba/zaměstnanec přistupující ke službě veřejné správy
2. Infrastruktura OAM řešící identifikaci a autorizaci
3. Využití externí služby pro identifikaci
4. OAM poskytne identitu a autorizační informace aplikacím.



Government of the Netherlands

Přihlašovací dialog



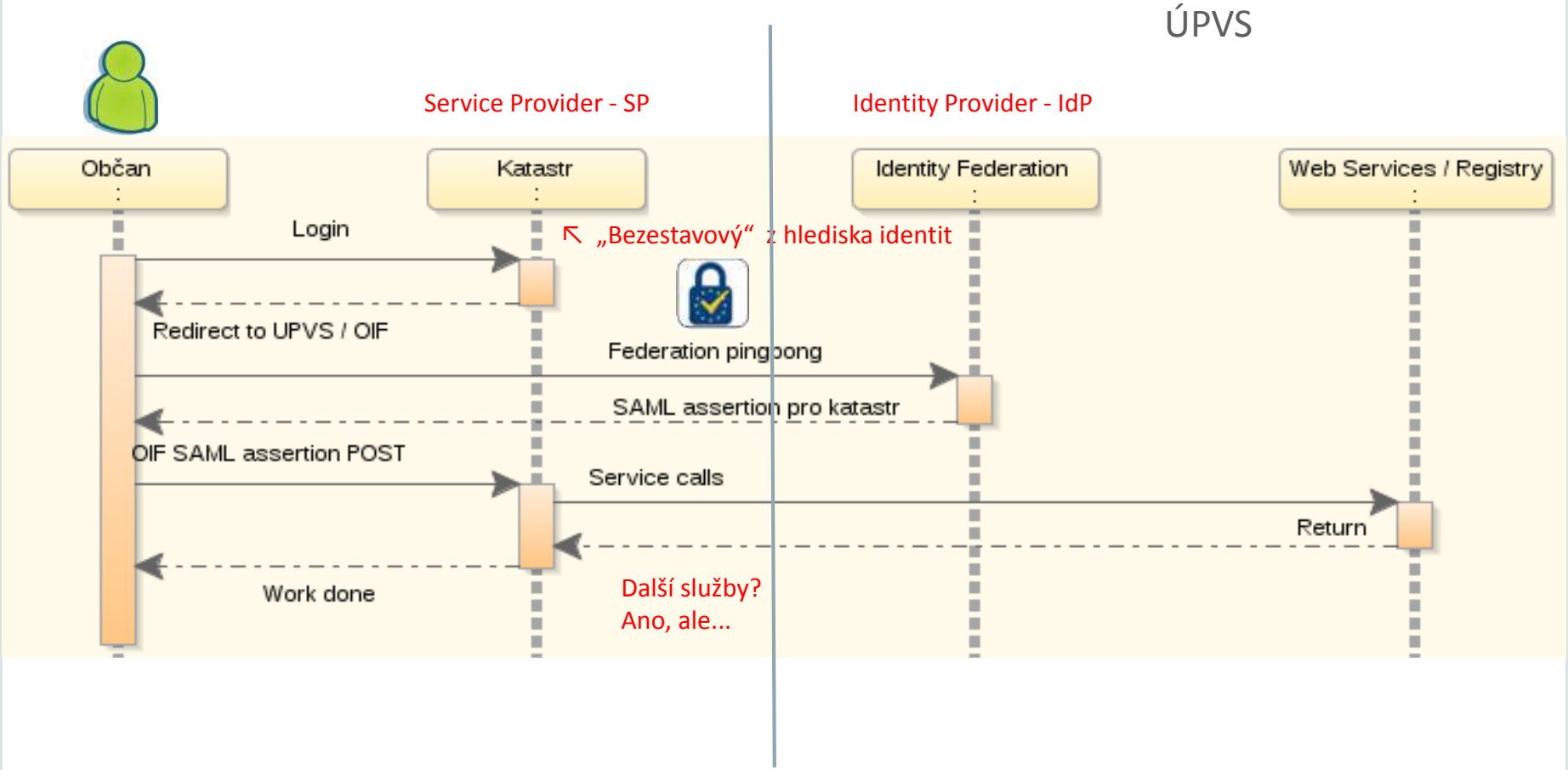
Ústredný Portál Verejnej Správy

- Jednotný bod elektronické komunikce občana (resp. instituce) se státem prostřednictvím elektronické schránky
- Řešení životních situací efektivním způsobem
- Klíčový systém eGovernment-u, jednotný přístup k eGov službám
- Identity Provider

Požadavky na ÚPVS IAM

- Správa 6,5 milionu identit a jejich a přístupových oprávnění
- Federace identit / Internet SSO mezi ÚPVS a ISVS pomocí SAML 2.0
- Podpora více autentizačních prostředků (eID karta, sms token, grid,..)
- Webové služby pro správu identit, rolí,..

Příklad federačního flow



Volání web services

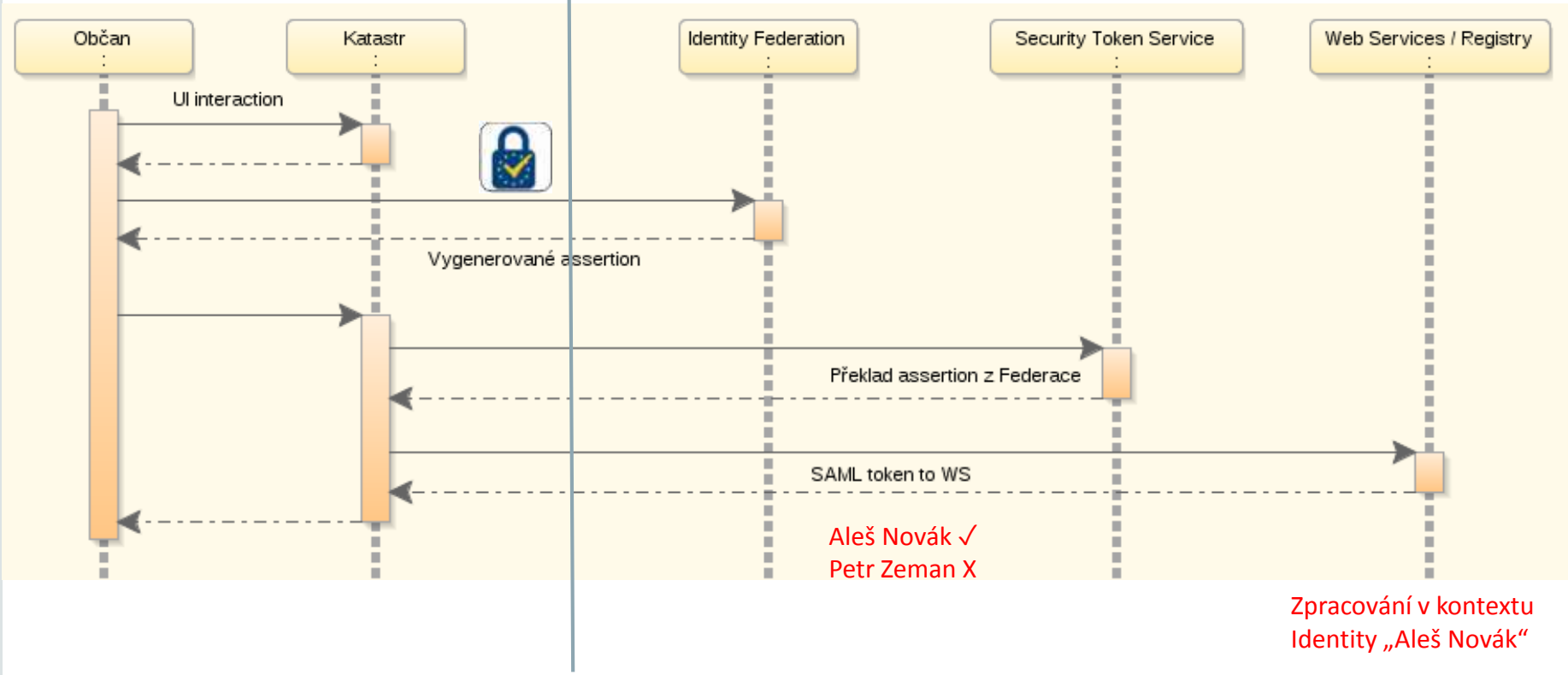
Ano ale...

- V případě útoku na service providera může útočník „vysát“ data o všech identitách
- → nutnost omezit komunikaci jen na kontext koncového uživatele
- Oracle Security Token Service umí vyrobit SAML token vhodný pro web services na základě SAML assertion z Oracle Identity Federation
  - Obsahuje původní data o identitě
  - Vydává ÚPVS
- ÚPVS web services omezují komunikaci na kontext koncového uživatele

Flow včetně Security Token Service

Aleš Novák

ÚPVS



Zpracování v kontextu Identity „Aleš Novák“

Zkušenosti s implementací eIDAS řešení

- Delší doba zřízení infrastruktury – závislost na externích Identity Providerech, bezpečnostní audity
- Rychlá integrace stávajících aplikací (hodiny)

- Adaptace webových služeb pro propagaci identit
- Tokeny pro federaci (SAML, OpenID) versus standardy z WS-SecurityPolicy

Výhody Oracle řešení řízení přístupů

- Praktické zkušenosti s využitím eID.
- Veřejně referencovatelné řešení ověřené jak v rolích Service Provider tak i Identity Provider.
- Řešení založené na standardech (SAML, OpenID, ...).
- Rychlá implementace hotového řešení.
- Dodatečné zabezpečení identit a jejich propagace na koncové systémy.
- Bezpečné a robustní.
- Bez nutnosti vlastní správy identit.

Děkujeme za pozornost.