UMPRUM Vysoká škola uměleckoprůmyslová v Praze

Perun na VŠUP

Jan Burian
VŠUP v Praze

Konference e-infrstruktury CESNET 2017

Obsah

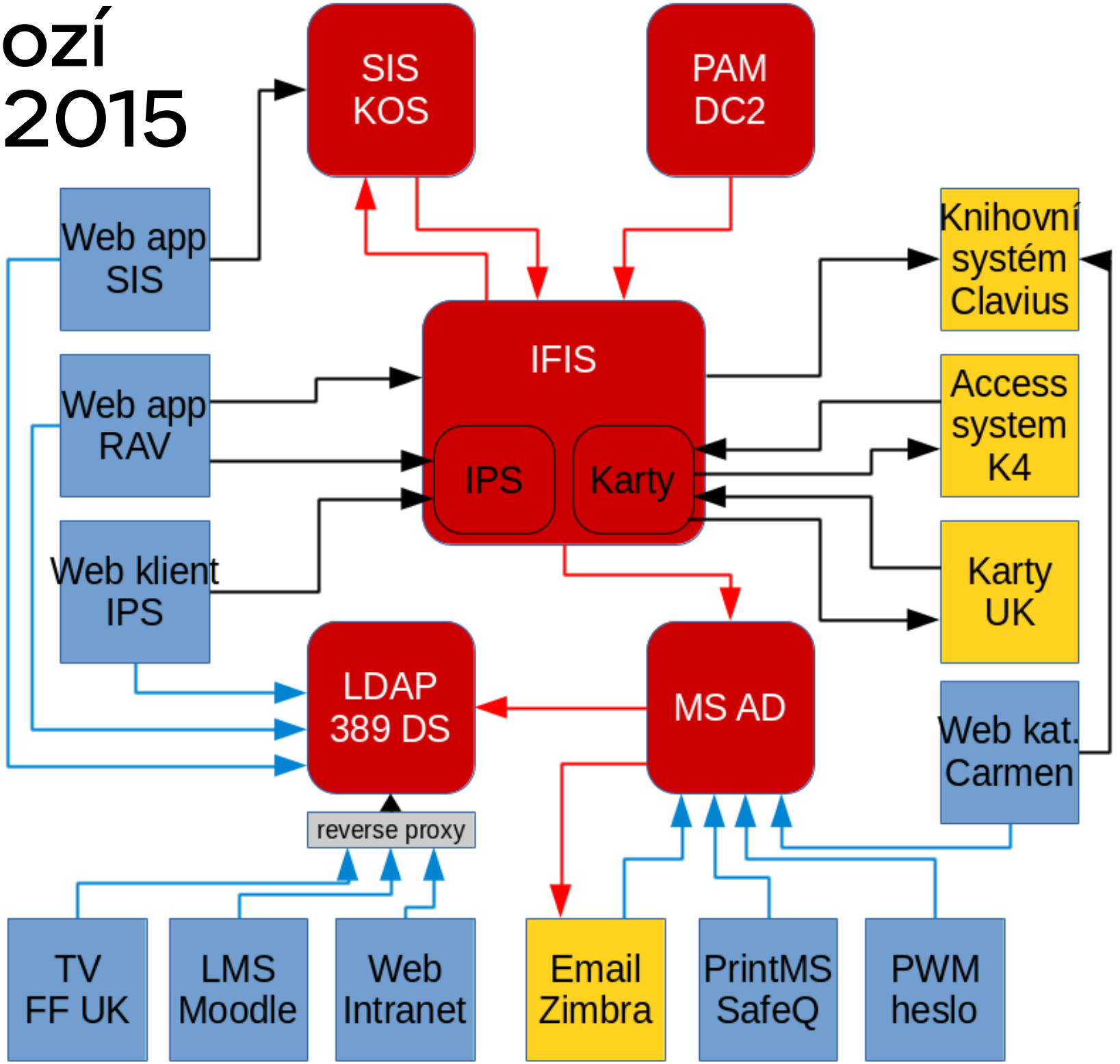
- Výchozí stav - CRO
- Změna – proč?
- Výběr řešení
- Příprava - projekt
- Implementace
- Komplikace
- Současný stav
- Přínosy
- Výhled do budoucna

Používané systémy

UM
PR
UM

• Studijní IS	KOS (ČVUT)
• PAM systém	DC2 (Datacentrum)
• Finanční IS	iFIS (BBM)
• Directory server	MS AD
• Email server	Zimbra Collaboration
• Knihovní systém	Tritius (LANius)
• Přístupový systém	K4 (IMA)
• Web / Intranet	PHP web app

Výchozí stav 2015



Výchozí stav - nevýhody

- Naprogramované řešení „na míru" bez administračního rozhraní
- Jakékoliv úpravy musí řešit programátor dodavatele na zakázku
- Nedostatečné rozlišení zaměstnanců
- Synchronizace z PAM se spouští ručně
- Není řešeno mazání účtů, pouze jejich zneplatnění v MS AD
- Není řešeno mazání emailových schránek

Změna – proč?

- Revize a vylepšení procesů
- Více informací o studentech a zaměstnancích do ostatních systémů
- Rozlišení zaměstnanců
- Kompletní životní cyklus identit
- Vyšší míra automatizace
- Řízení přístupů
- Bezpečnost
- Auditovatelnost

Výběr řešení – jaké?

UM
PR
UM

- Identity Management System
- Open Source
- Podpora
- OpenIDM, Open IAM, Evolveum midPoint
- CzechIDM - BCV Soulutions
- Perun - CESNET / MU

Příprava - projekt

- Projekt v rámci FR CESNET 2015
- Cíle:
  - centralizace správy identit a přístupů na zdroje
  - revize předávaných údajů a automatizace
  - kompletní správa emailových schránek
  - doplnění workflow životního cyklu identit
  - centralizace správy hesel
  - připojení aplikací jako příjemců dat
  - připojení do federace identit eduID.cz

Implementace - 1. fáze

- Instalace IAM systému Perun
- Napojení na zdroje dat (SIS, PAM, FIS)
- Předávání dat (SIS, PAM, Intranet)
- Správa uživatelů a skupin v doméně (MS AD)
- Správa uživatelů pro eduroam (FreeRadius)
- Instalace a konfigurace Shibboleth IdP pro eduID.cz

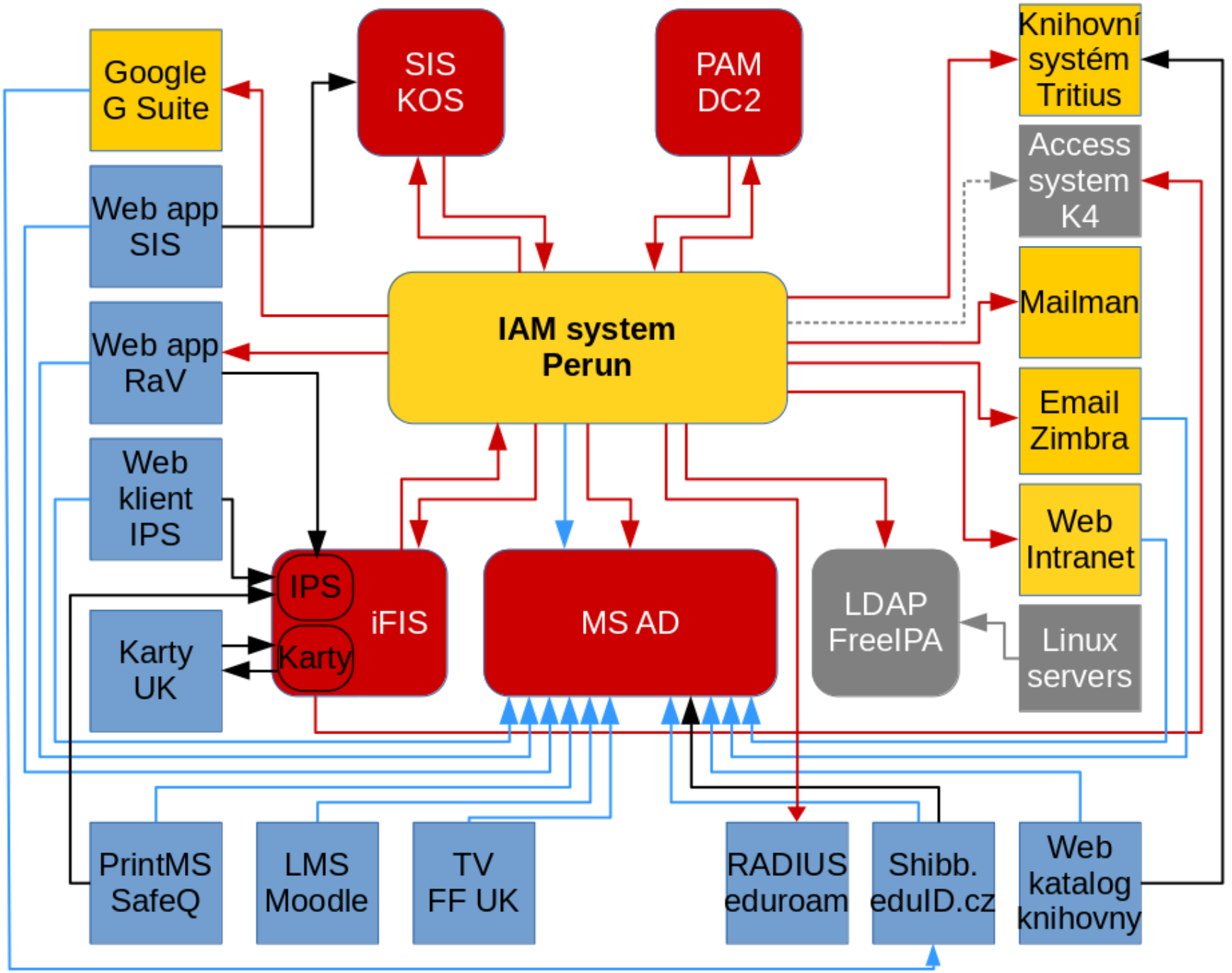
Implementace - 2. fáze

- Dokončení napojení iFIS
  - přenos osob a vztahů
- Napojení knihovního systému Tritius
  - přenos osob
- Napojení emailového serveru Zimbra
  - správa schránek a mailing listů
- Dokončení kompletního managementu hesel v Perun

Implementace - další

- Nad rámec projektu byly napojeny další systémy:
  - freeradius a zapojení do eduroam
  - rezervační a výpůjční systém RaV
  - napojení na cloudové služby Google G Suite for Education (Disk, Groups)
- Provedena analýza připojení přístupového systému pro správu osob a přístupových skupin

Současný stav



Komplikace, změny

- Napojení iFIS pro předávání dat
  - personální komplikace na straně dodavatele
- Přenos vztahů osob na Web / Intranet
  - Perun není navržen na přenos komleptní sady dat s vazbou na osobu
- Ukládání sekundárního hesla pro eduroam
  - původní záměr ukládat do MS AD
  - nakonec zápis do souboru users na RADIUS server

Přínosy

- centralizovaná správa identit a přístupů na jednom místě
- přehled o aktuálně platných přístupech dané identity na jednom místě
- správa skupin nejen pro AD, která umožňuje efektivně přidělovat oprávnění a přístupy a aplikovat nejen bezpečnostní politiky
- automatizace kompletního životního cyklu identit
  = ukončování identit dle platnosti vztahu k organizaci
- mazání účtů a dat v koncových systémech po vypršení ochranné lhůty - karantény
- zajištění platnosti dat o osobách a jejich elektronických identitách v koncových systémech
- integrace změn a nastavení hesel do stávajících aplikací
  = eliminace jednoúčelových aplikací
- možnost rozvoje a propojení dalších systému do budoucna
- připojení do federací eduID.cz a eduroam

Výhled do budoucna

- Změna PAM systému
- Podpora pro HelpDesk – reset hesla
- Napojení na přístupový systém K4
- Předávání vybraných identit do adresářové služby IPA
- Napojení na centrální sběr logů?
- Revize předávání údajů a přístupu k nim v souvislosti s GDPR?

Dotazy

Děkuji za pozornost.

Dotazy?

jan.burian@vsup.cz