

UMPRUM Vysoká škola
uměleckoprůmyslová
v Praze

UMPRUM
Identity
2015

Jan Burian, VŠUP v Praze

VŠUP v číslech



- 631 aktivních studentů
- 134 zaměstnanců
- Roční obměna cca 100 osob
- 1 fakulta – 1 IT pracoviště
- IT: 4,5 úvazku + outsourcing
- 5 informačních systémů
- 3 autentizační systémy
- 2 aplikační servery (email, web/intranet)

Používané systémy



- Studijní IS
 - PAM systém
 - Finanční IS
 - LDAP
 - Email server
 - Knihovni systém
 - Přístupový systém
 - Web / Intranet
- KOS (ČVUT)
 - DC2 (Datacentrum)
 - iFIS (BBM)
 - MS AD, 389 DS
 - Zimbra Collaboration
 - Clavius (LANius)
 - K4 (IMA)
 - PHP web app

Současné řešení



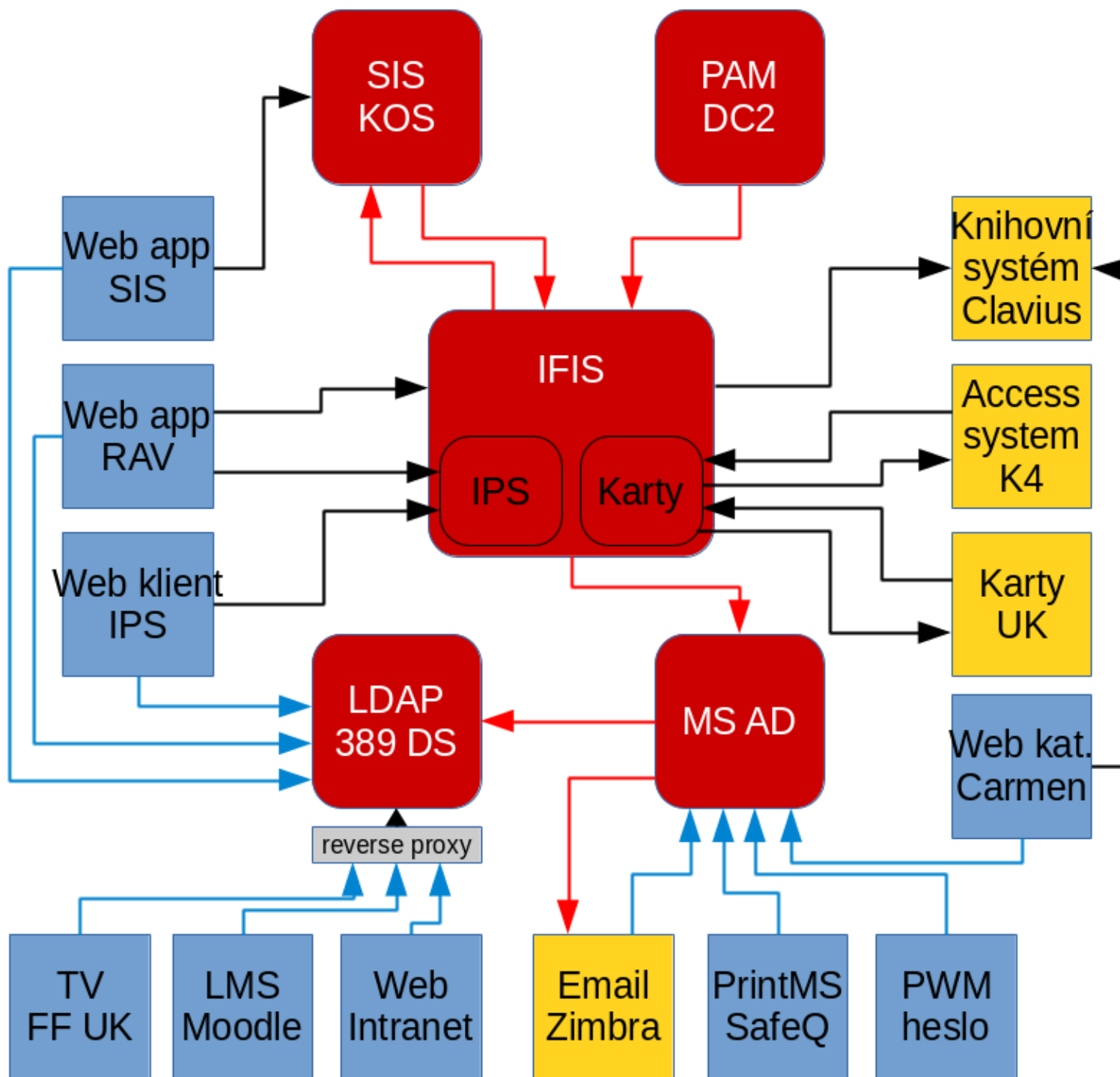
- Zástupnou funkci IdM systému plní iFIS spolu s MS AD
- Sbírá informace o osobách a vztazích ze SIS a PAM systému
- Vytváří a aktualizuje účty v MS AD
- Předává informace o účtech zpět do SIS
- Z MS AD probíhá jednosměrná automatická synchronizace účtů na linux LDAP server
- Na emailovém serveru je nastaven auto provisioning účtů na základě kontroly nových účtů ve specifických ou v MS AD

Současné řešení



- 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

Současné řešení



Nové řešení – proč?



- Vylepšení procesů
- Více informací o studentech a zaměstnancích do ostatních systémů
- Rozlišení zaměstnanců
- Kompletní životní cyklus identit
- Vyšší míra automatizovanosti
- Řízení přístupů
- Bezpečnost
- Audit

Nové řešení – jaké?



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

Plánované řešení



- Informace o osobách, studiích a pracovních poměrech jsou předávány do IdM systému
- IdM systém předává informace do ostatních systémů dle jejich potřeby:
 - SIS (osoby, účty)
 - Do iFIS (osoby, vztahy, spojení), z iFIS (karty)
 - MS AD, LDAP – zakládání a aktualizace účtů
 - Zimbra – spravuje emailové schránky
 - Tritius (knihovní sys.) – plní a aktualizuje DB osob
 - Web / Intranet – plní a aktualizuje DB osob
 - EduID – spravuje atributy pro ověřování identit
 - Přístupový sys. - spravuje přístupové skupiny

Plánované řešení

