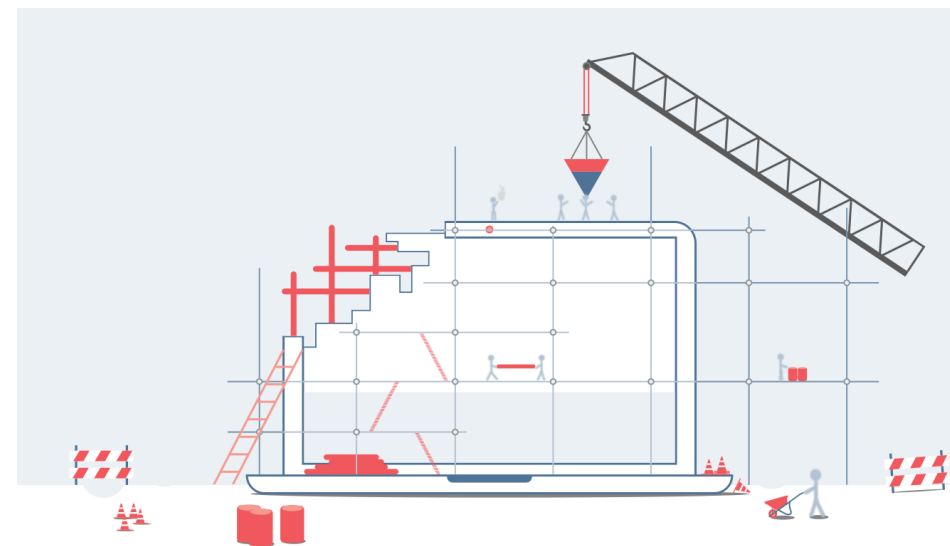


Justiční autentizační a autorizační systém JAAS

Příklady dobré praxe z oblasti
elektronických mandátů a zmocnění

Zasedání pracovní skupiny pro architekturu a řízení ICT

31.1. 2022



Ing. Eva Vidová

odbor informatiky
vedoucí oddělení rozvoje služeb a architektury

Ing. David Šetina

enterprise architect

Ing. Petr Kramosil

enterprise architect


Situace MSp v oblasti autentizace a autorizace uživatelů

- Proprietární způsoby autentizace v jednotlivých systémech -> duplicity
- Přístupy zástupců právnických osob
- Soulad s legislativou a architektonickými principy – NIA
- Univerzální centrální komponenta



POMOCÍ POSKYTOVATELŮ IDENTITNÍCH SLUŽEB

 Přihlášení pomocí katalogu autentizačních a autorizačních služeb

 Přihlášení pomocí poskytovatele ISDS (datové schránky)

 Přihlášení pomocí identity občana

 Od 1.9.2021 omezeno pouze pro vybrané osoby

© 2022 TECHNISERV IT, SPOŁ. S R.O. Verze 3.0.21273.3 [20210930]

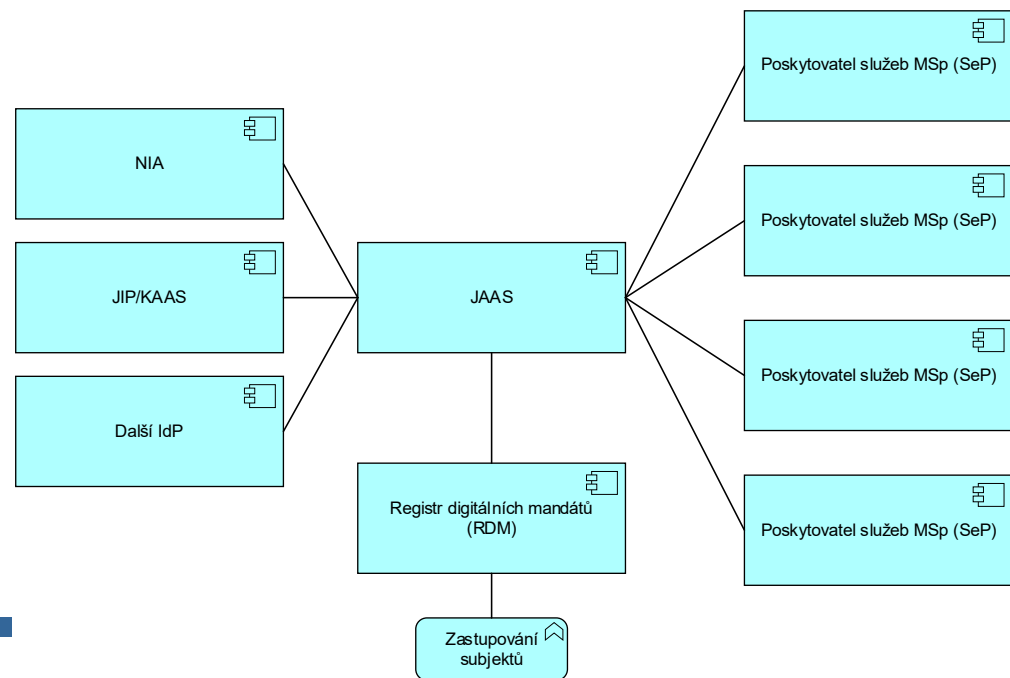
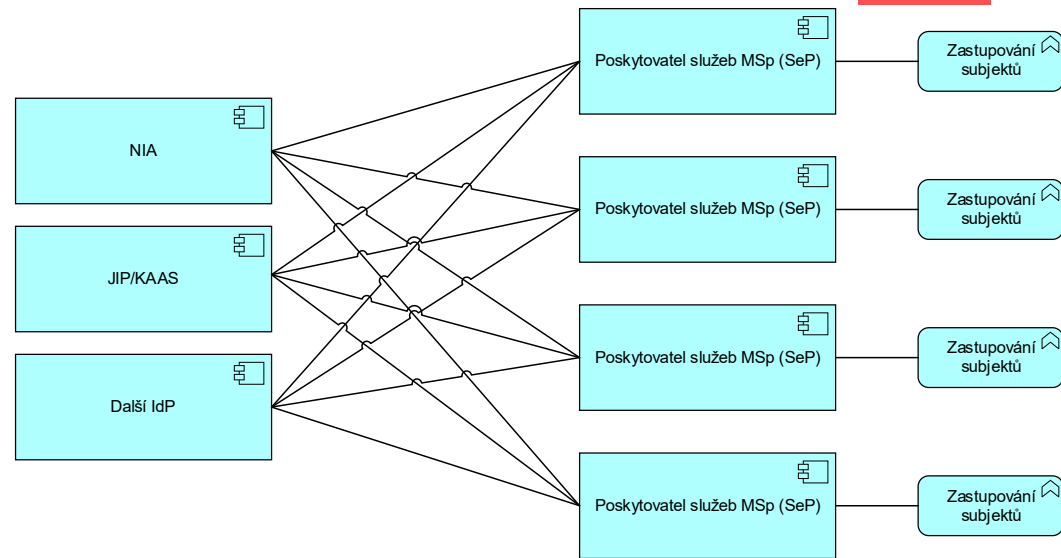
Varianty řešení

➤ Integrace každého dílčího systému MSp na NIA a další IdP, individuální řešení zastupování

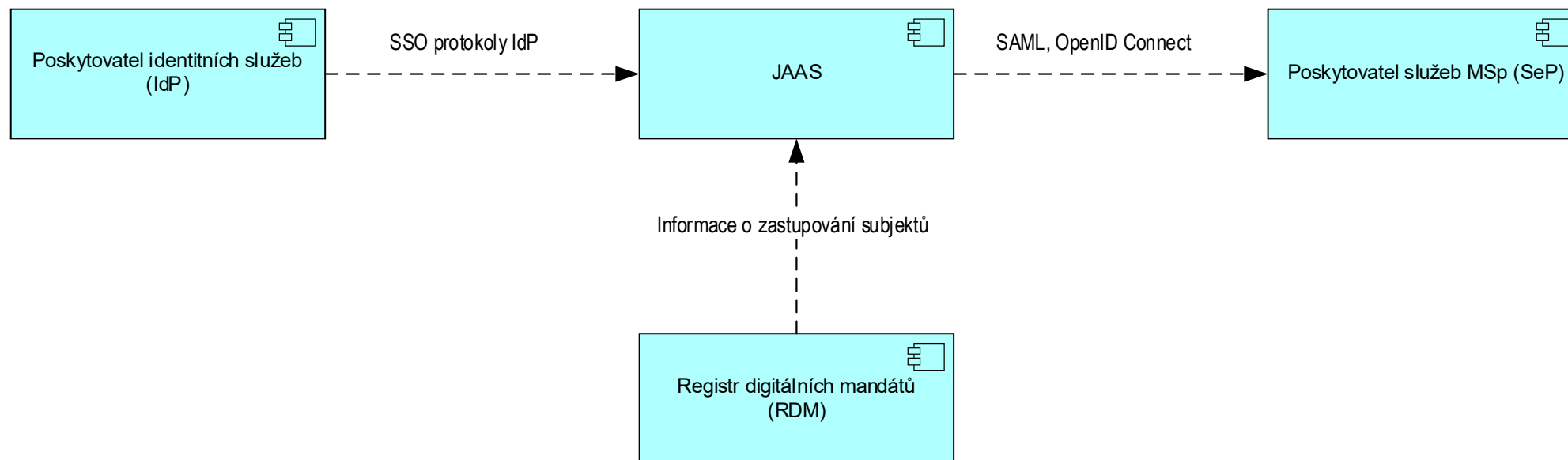
- ☹️ duplicitní implementace v SeP
- ☹️ opakovaná integrace na IdP

➤ Vytvoření jednotného systému, sdílené služby – JAAS

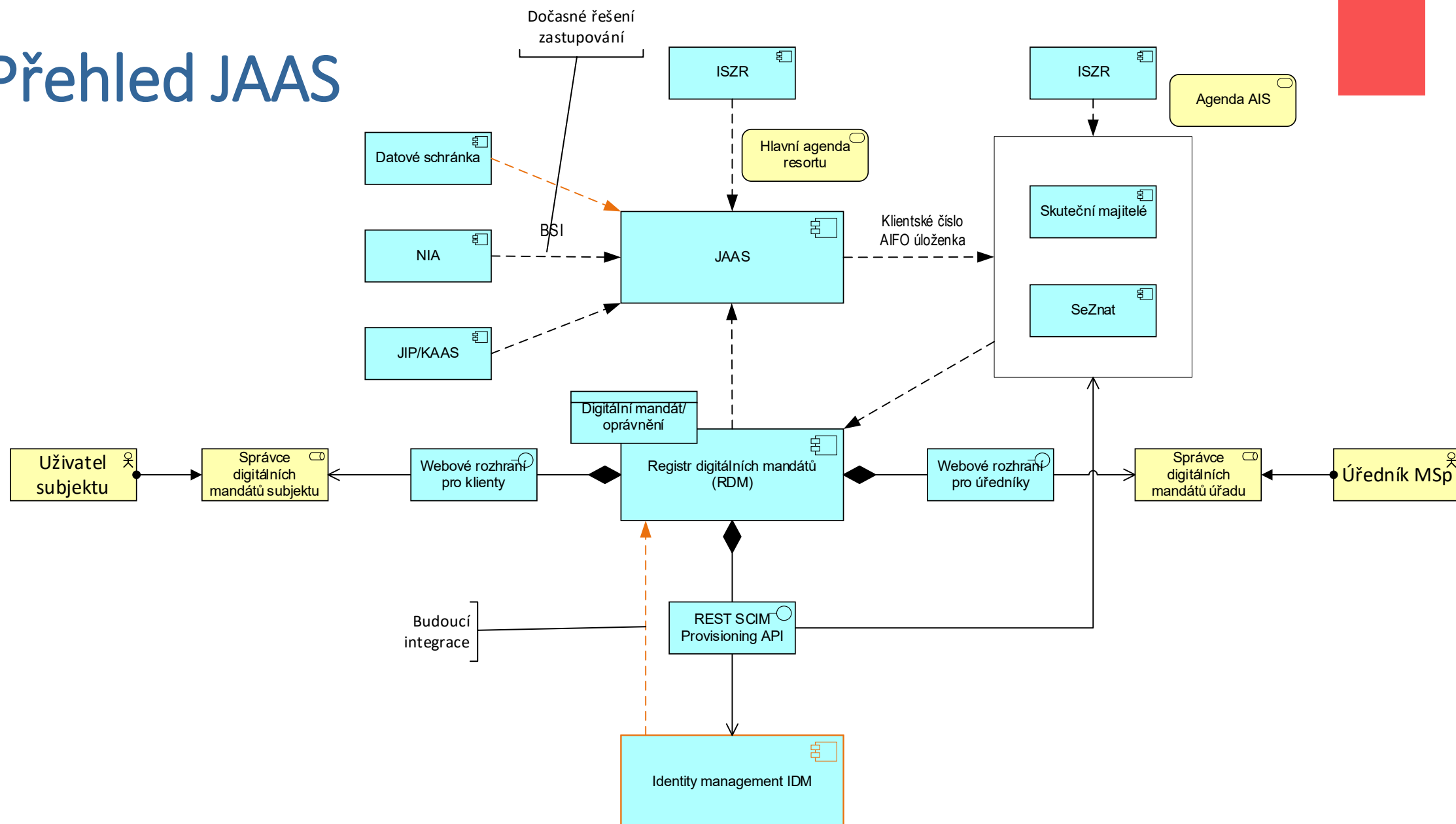
- 👍 sdílení a přepoužití funkcionalit
- 👍 centrální napojení na IdP a řešení zastupování
- 👍 odstínění aplikací od detailů IdP



Přehled JAAS



Přehled JAAS



Centrální služba JAAS/RDM shrnutí 1

- zprostředkovává SeP MSp přístup k externím autentizačním (IdP) a autorizačním službám
- odstiňuje SeP MSp od detailů komunikace s externími IdP tak, že pro každý SeP MSp je proces autentizace a autorizace zcela identický, bez ohledu na to, jaký IdP byl pro autentizaci či autorizaci zvolen
- zajišťuje jednotné bezpeční přihlášení a odhlášení (SSO) do/ze všech systémů MSp tak, že uživatelé se přihlašují/odhlašují pouze jednou
- umožňuje do systému jednotného přihlášení/odhlášení SSO zapojit další IdP a externí SeP
- generuje a eviduje unikátní klientské číslo každého klienta přistupujícího k on-line službám resortu MSp

Centrální služba JAAS/RDM shrnutí 2

- umožňuje přístup k zaručeným informacím o ověřené identitě napojeným aplikacím, v okamžiku prvního přístupu klienta např. předává AIFO úloženkou prostřednictvím IszrUlozMapaAifo a iszrPodejMapaAifo, v případě opakovaného přístupu předává klientské číslo
- zajišťuje federaci identit z interních a externích zdrojů, mapuje externí identity na interní uživatelské účty
- publikuje webové služby umožňující oprávněným externím systémům (jako jsou IDM, AIS atd.) provádět potřebné změny a nastavení v RDM
- poskytuje samoobslužné uživatelské rozhraní pro klienty veřejné správy umožňující spravovat uživatelské profily a digitální mandáty
- poskytuje obslužné rozhraní pro pověřené úředníky MSp umožňující spravovat uživatelské profily, mandáty, uživatelské účty, role a další atributy

Dotazy





ĎEKUJEME ZA POZORNOST

Ing. Eva Vidová
evidova@msp.justice.cz
+420 776 747 024