NEWPS.CZ

Auditní stopa a věrohodnost dokumentu

Tomáš Řemelka

Delivery Director

ISSS 2013, Hradec Králové

Co vás čeká?

- Auditní stopa a věrohodnost dokumentu
- Úřad a komunikující skupiny osob
- Řízení přístupů
- Řízení identit
- Závěr

Co je to „věrohodný“ dokument?

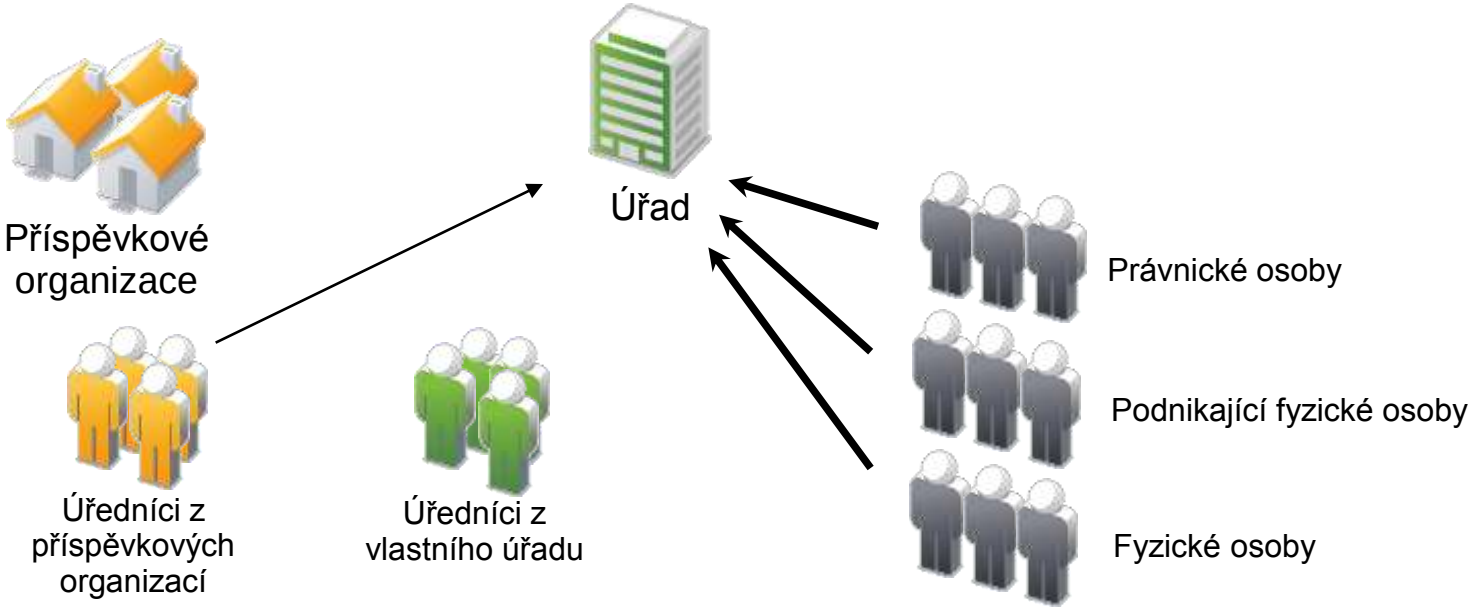
- Papírové dokumenty
  - Vlastnoruční podpis OPRÁVNĚNÉ osoby
  - Případně opatřený úředně ověřeným podpisem
- Elektronické dokumenty
  - „Elektronický podpis“ (Zaručený el. Podpis) OPRÁVNĚNÉ osoby
  - Kvalifikované časové razítko

Co víme o podepisující osobě?

- Podpisy/časová razítka neříkají nic o osobě, která dokument podepsala.
- Jak ověříme, že měla oprávnění dokument vystavit/podepsat?
- Nijak.
  - Musí to ošetřit samotný úřad, z nějž daný dokument pochází.
- Jak?
  - Řízením přístupu a uživatelských identit.

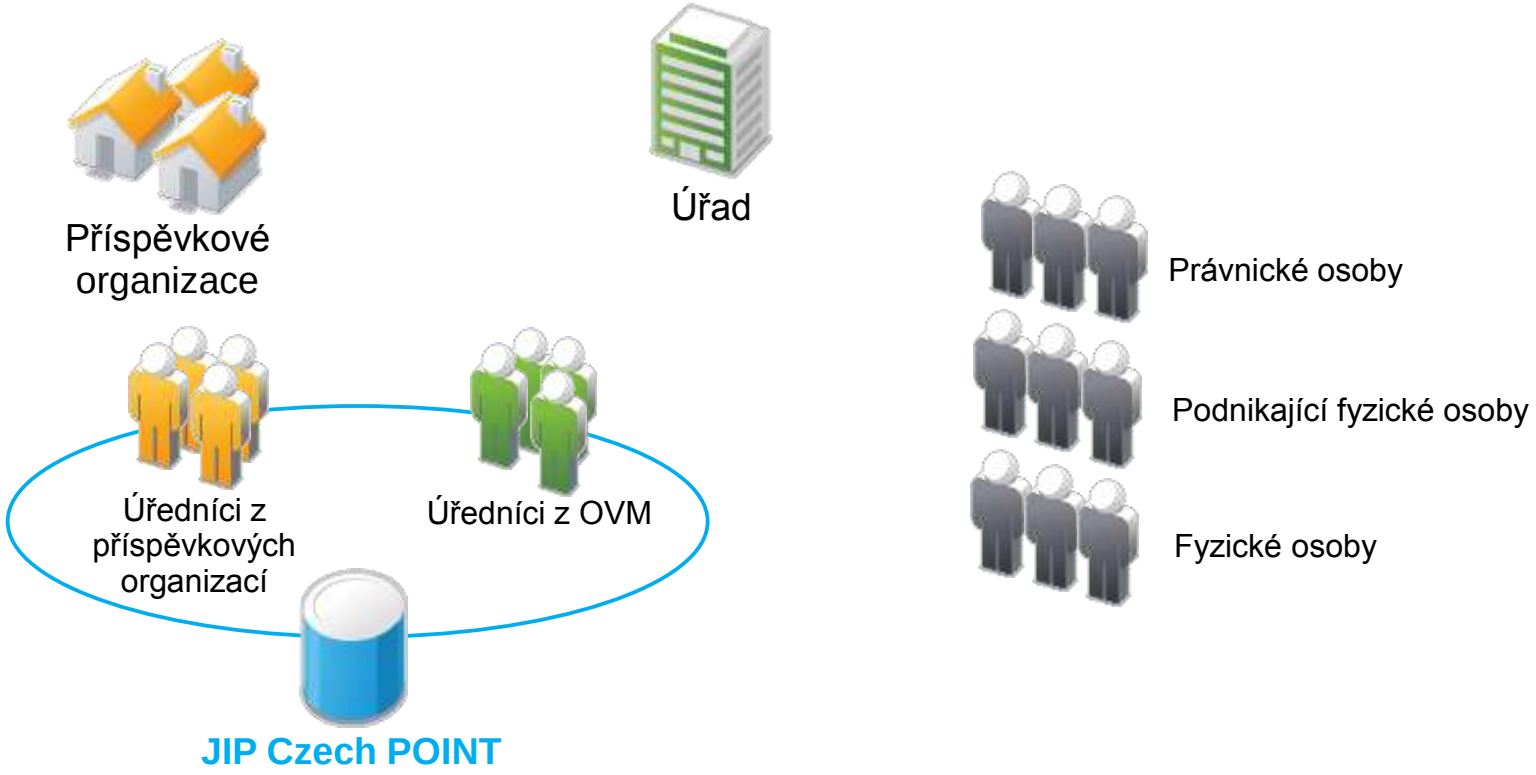
Úřad a komunikující skupiny osob

Situace na úřadech



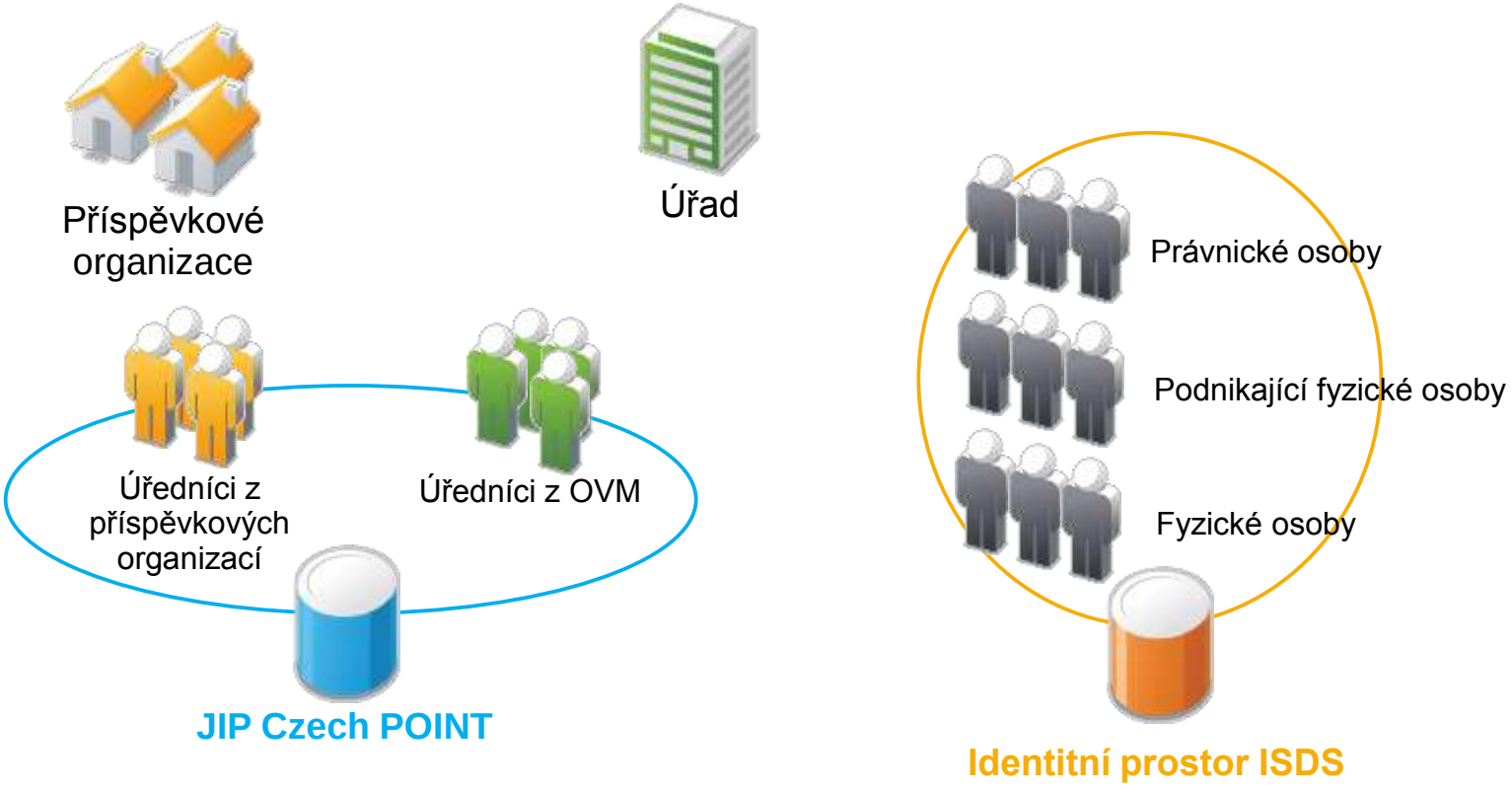
- Úřad zaměstnává vlastní úředníky, případně do jeho aplikací přistupují úředníci z jiných institucí (např. příspěvkových organizací)
- Úřad komunikuje s právnickými osobami, podnikateli a fyzickými osobami

Kde jsou uloženy uživatelské účty úředníků?



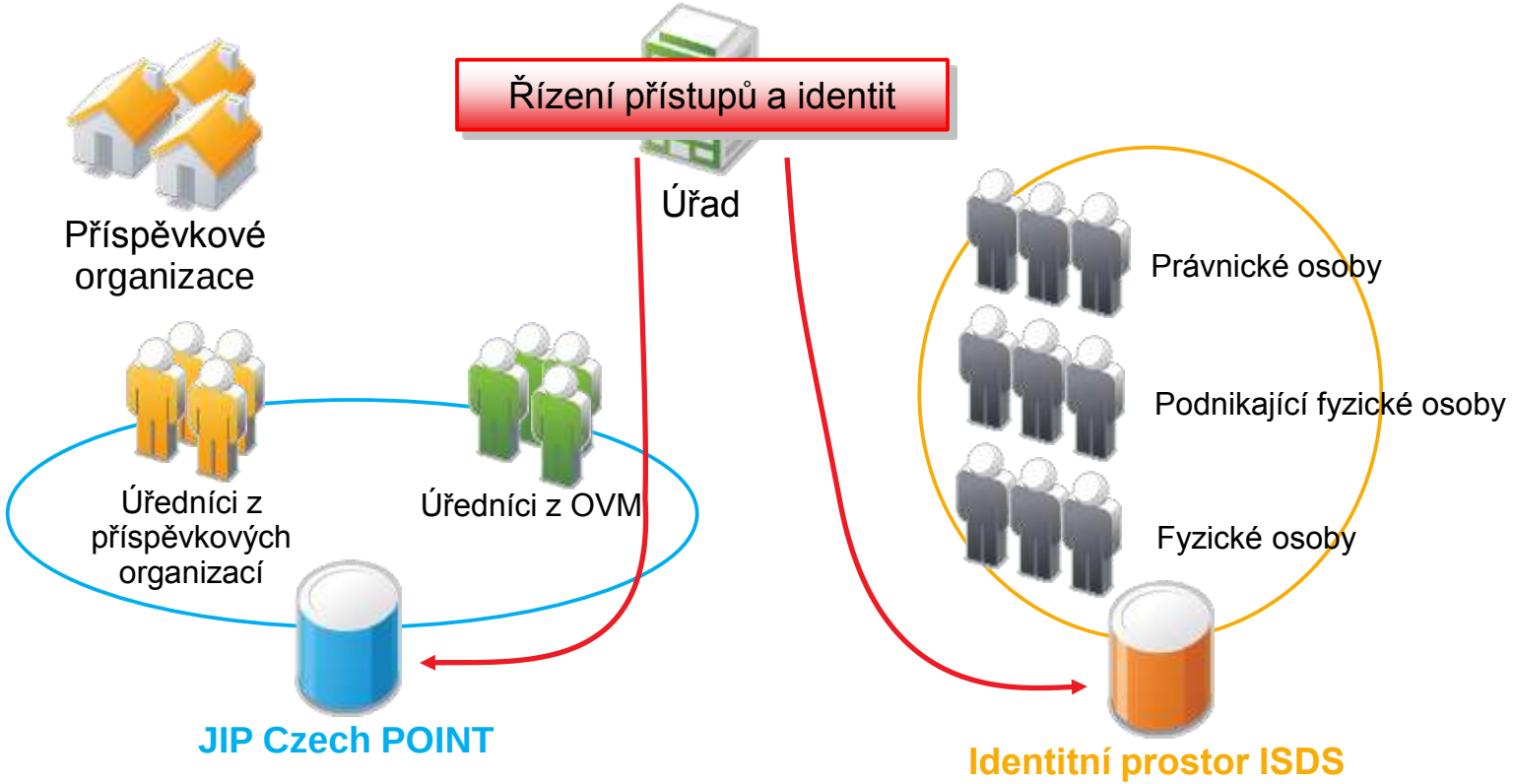
- Uživatelské účty úředníků z OVM (příp. příspěvkových organizací) jsou uloženy v JIP Czech POINT

A co účty PO/podnikatelů/FO?



- Právnické osoby, podnikatelé mají zřízenu datovou schránku, fyzické osoby na žádost
  - tedy mají vlastní uživatelský účet v identitním prostoru ISDS.

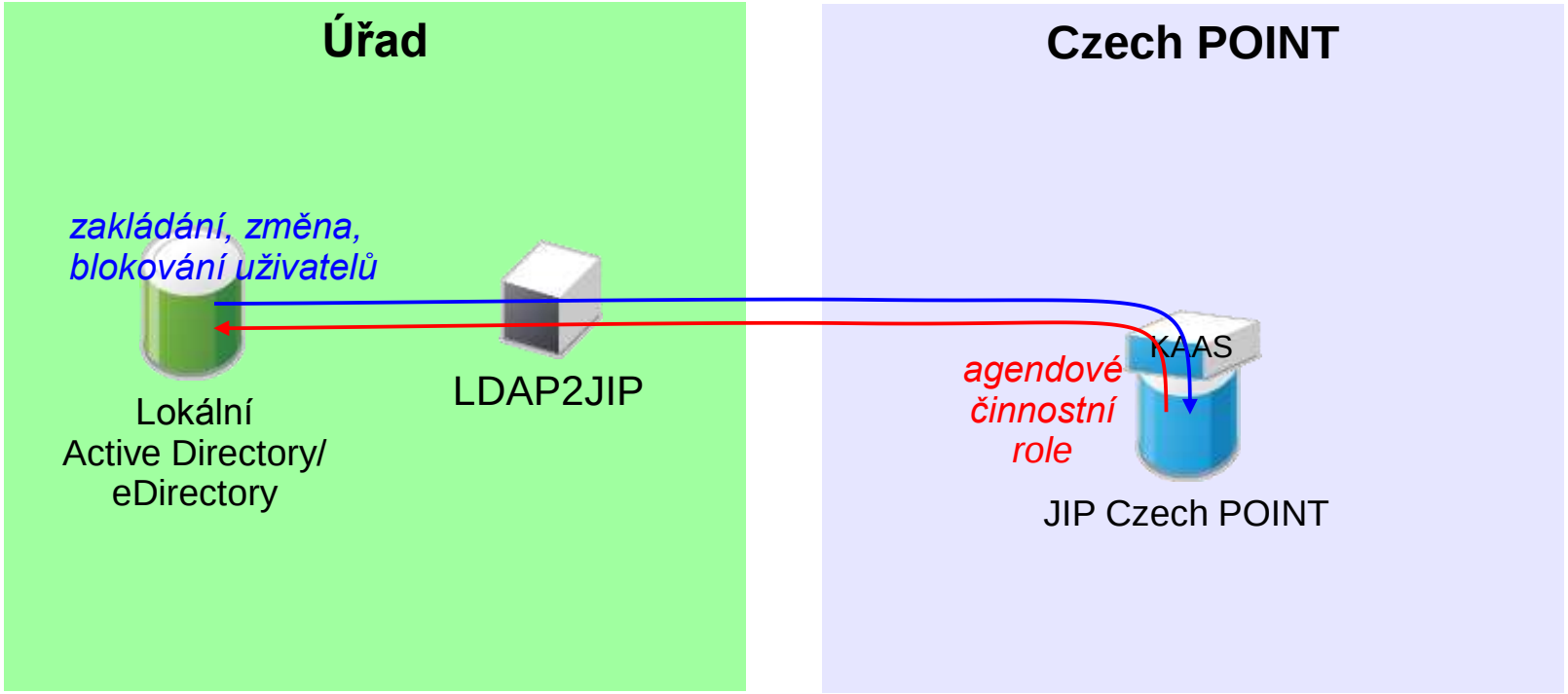
Jak lze tyto účty využívat?



- Pomocí řešení pro řízení přístupů a identit, které je napojeno na tyto adresáře uživatelských identit.

Řízení identit

LDAP2JIP_konektor



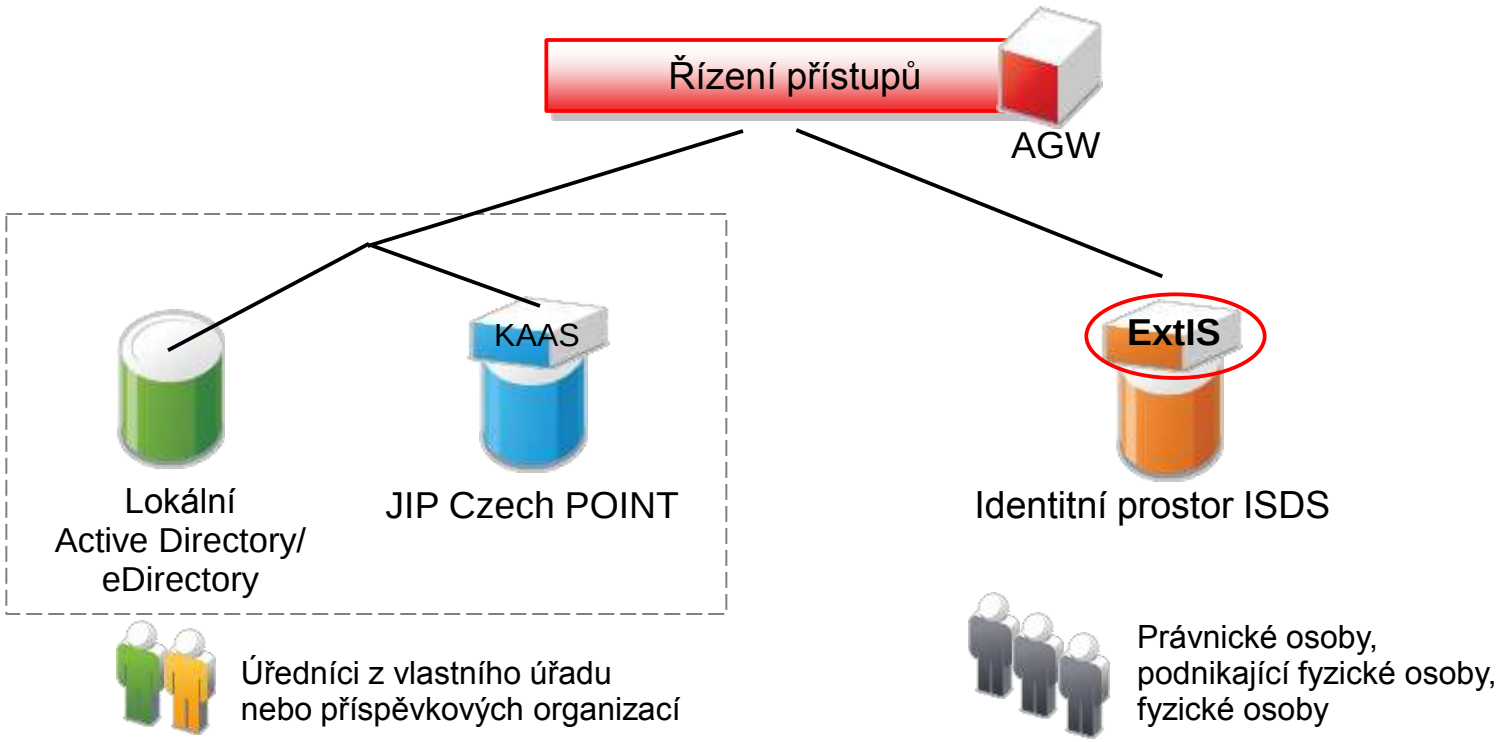
- Obousměrná synchronizace uživatelských identit mezi lokálním adresářem a JIP Czech POINT

LDAP2JIP - přínosy

- Správa uživatelů na jediném místě – uvnitř úřadu nebo v JIP
- Jeden uživatelský účet pro přístup do lokálních aplikací, ale i do Czech POINT, Czech POINT@office, AIS RPP Působnostní, ISUI
- Agendové činnostní role pro přístup do ZR
- **Eliminace rizika zapomenutého uživatele**
- **Eliminace rizika neopr. přístupu k datům**

Řízení přístupů

Ověřování uživatelů



- AGW ověřuje přistupující úředníky do aplikací vůči lokálnímu adresáři (AD, eDirectory) v úřadu a/nebo vůči JIP Czech POINT prostřednictvím rozhraní KAAS.
- AGW ověřuje PO/PFO/FO vůči ISDS pomocí nového rozhraní ExtIS.

AGW – přístupová brána

- Přístupový bod uživatelů do aplikací úřadu
- Zajišťuje auditní stopu přístupů uživatele
- Ověřování uživatelů vůči více zdrojům (adresářům) uživatelských identit
- Vícefaktorová autentizace
  - Uživatelské jméno a heslo
  - Certifikáty
  - OTP (HW/SW token, nebo SMS)

Shrnutí

- AGW – řešení pro řízení přístupů
  - ověřování OPRÁVNĚNÝCH uživatelů z více zdrojů
  - vícefaktorová autentizace
  - Auditní stopa přístupů uživatele
- LDAP2JIP – řešení pro řízení identit
  - umožňuje správu uživatelů na jednom místě
  - agendové činnostní role
  - eliminace rizika zapomenutého uživatele

NEWPS.CZ

Děkuji za pozornost

tremelka@newps.cz