ARCHITEKTURA PŘIPOJENÍ ERECEPTU A EPOUKAZU K NIA

20. 9. 2021

Petr Pilař a Vítězslav Košina

Agenda

- Požadavky
- Návrh
- Implementace

Úvod

- Co je ePoukaz?
- Zákon o zdravotnických prostředcích upravuje předepisování a výdej zdravotnických prostředků. Prostředky se mohou vydávat na listinný nebo elektronický poukaz. Systém výdeje v elektronické podobě je podobný jako v systému eRecept a proto je tento systém součástí systému eRecept a pro lepší srozumitelnost se nazývá ePoukaz.

- Proč přístup pomocí NIA?
- Je to standardizovaný, jednoduchý a s ohledem na možnost využití bankovních identit (> 6 mil. osob) perspektivní způsob.
- Dojde ke zvýšení bezpečnosti.
- Umožní omezit používání elektronického podpisu a zjednodušit tím celý proces.

Požadavky na řešení

- Systémové řešení
- Přístup pomocí NIA k ePoukazu, k eReceptu, do identitního portálu.
- Musí být použitelné v budoucnu i pro další agendové systémy SÚKL.

- Evoluční přístup
- Přístup pomocí NIA rozšiřuje stávající autentifikaci a autorizaci přistupujících osob, nenahrazuje ji.

- Přihlášení pomocí tenkého a tlustého klienta
- Většina nemocničního, lékárenského a ambulantního SW je ve verzi tlustého klienta.
- U tenkého klienta požadavek na identifikaci místa přístupu a osoby po přihlášení.

- Prodloužení platnosti přihlášení
- Přihlášení pro uživatele platí do půlnoci (pro přihlášené po 22:00 další celý den).
- Dávkové operace je možné provádět o den déle.

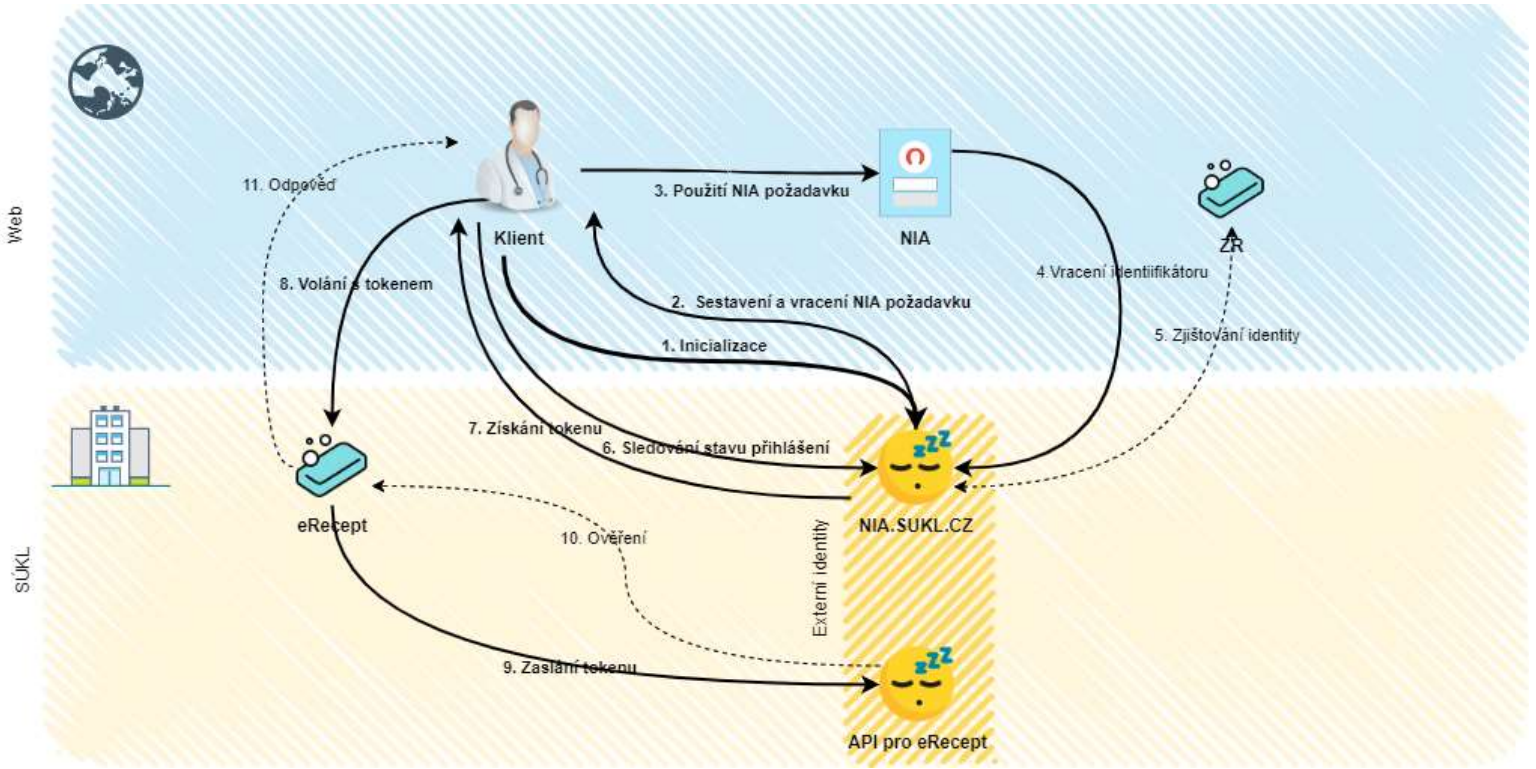
Architektura

- Realizace pomocí REST API (pro všechny typy klientů)
- Datový formát JSON
- Registrace SÚKL webových a případně mobilních aplikací
- V rámci registrace se definuje formát odpovědi (struktura a obsah)
- V rámci registrace se definuje cílové chování (redirect)
- Více API end pointů – požadavky na různé chování a různá data po přihlášení
- Zabezpečení API autentizačním certifikátem pracoviště
  - Těžký klient musí uvést registrovaný login přistupující osoby

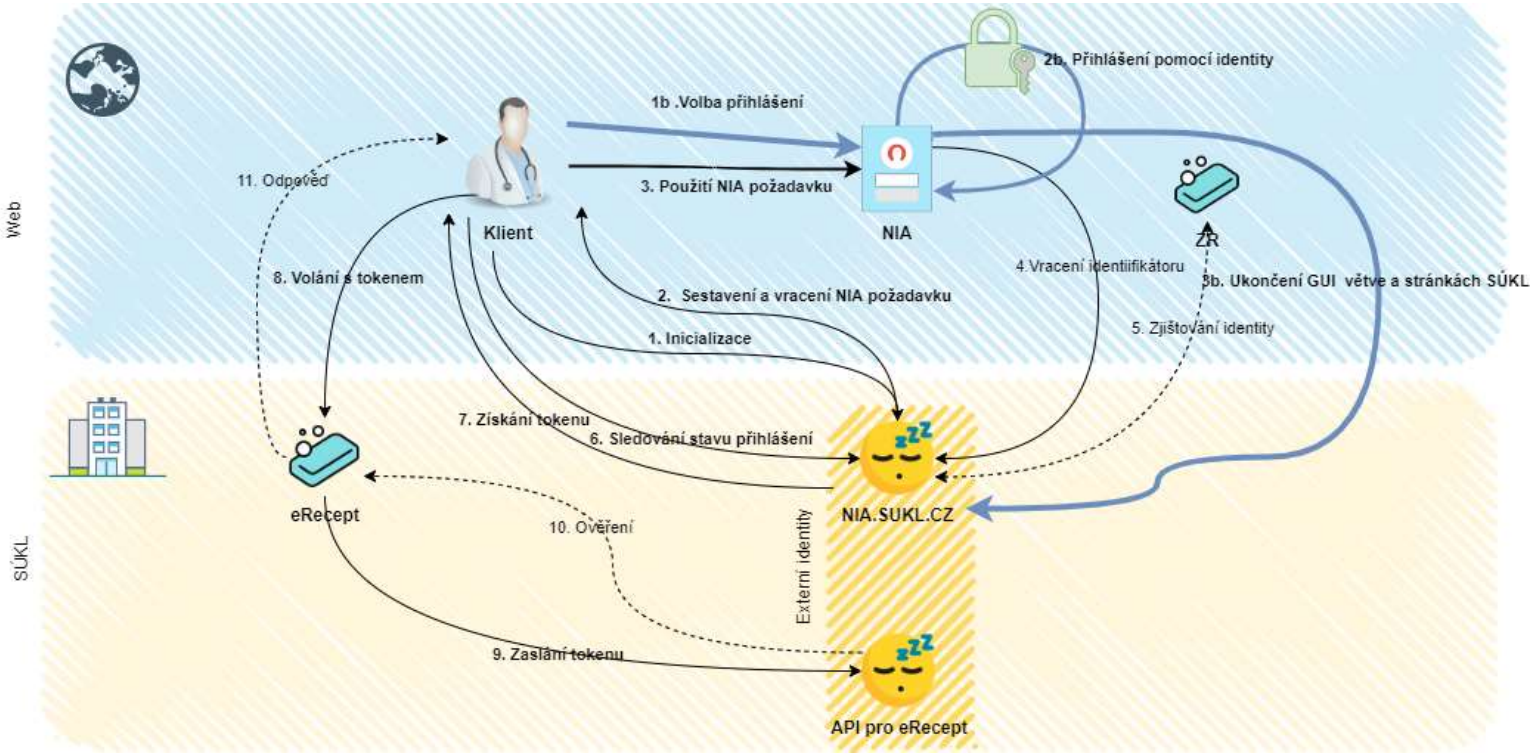
Architektura II

- Přidělení JWT tokenu (standard) na základě:
  - Úspěšné NIA autentizace
  - Dřívějšího ztotožnění osoby v ROB
  - Validace BSI <-> AIFO
  - Registrace v Externích identitách SÚKL
- JWT token je závislý na aplikaci, která volala NIA (ePoukaz, žádost o …)
- JWT token je možné použít pouze na vybraná API volání
- JWT token má odlišnou platnost než SAML a je možné jej kdykoliv zneplatnit
- Speciální použití JWT tokenu pro eRecept a ePoukaz (dvě platnosti)

Big picture



Big picture s GUI větví



Implementační problémy

- NIA se standardně řeší v rámci jedné web aplikace
- NIA resp. SAML se standardně nepoužívá pro tlusté klienty
- Neexistuje/Nenalezena použitelná referenční implementace
- Zcela nová implementace včetně návrhu

Děkujeme za pozornost

SÚKL
PETR PILAŘ
Šrobárova 48, 100 41 Praha 10
tel.: +420 272 185 896
e-mail: petr.pilar@sukl.cz

IBA CZ S.R.O.
VITĚZSLAV KOŠINA
Radlická 751/113e, Praha 5, 158 00
tel.: +420 602 171 095
e-mail: vitezslav.kosina@ibacz.eu