Přihlašování k NIA z mobilních aplikací

Identita občana

Josef Knotek (SZR)
Jiří Holaň (NEURODOT Consulting)
Robert Hernady (Microsoft)

neurodot consulting

SPRÁVA ZÁKLADNÍCH REGISTRŮ

Microsoft

Základní funkce

Umožnit poskytovatelům služeb (SeP) vytvoření takových vlastních mobilních aplikací a vlastních backendových API, které dohromady budou umět ověřit identitu občana prostřednictvím volání webových služeb, tedy nevizuálně bez interakce občana.

Mobilní aplikace bude muset být uživatelem nejprve registrována v NIA a následně bude umožňovat opakované přihlašování k NIA na pozadí ve jménu uživatele. Tzn. uživatel nebude muset znovu zadávat své přihlašovací údaje.

Mobilní aplikace předává informace o provedeném přihlášení do systému poskytovatele služeb, který následně z NIA získá detaily o přihlášeném uživateli.

Platnost registrace bude mobilní aplikace opakovaně kontrolovat vůči NIA, aby uživatel mohl např. při ztrátě zařízení možnosti nevizuálního přihlašování zabránit.

Předpoklady pro implementaci přihlašování z MA

SeP

Poskytovatel služby musí

- vytvořit svoji mobilní aplikaci
- rozšířit svůj informační systém o rozhraní (API) pro komunikaci s mobilní aplikací pro příjem informací o přihlášeném uživateli
- provést registraci svého API a mobilní aplikace v NIA
- definovat a zaregistrovat sadu atributů, které budou obsahem JWT (JSON Web Token)

NIA

NIA poskytuje

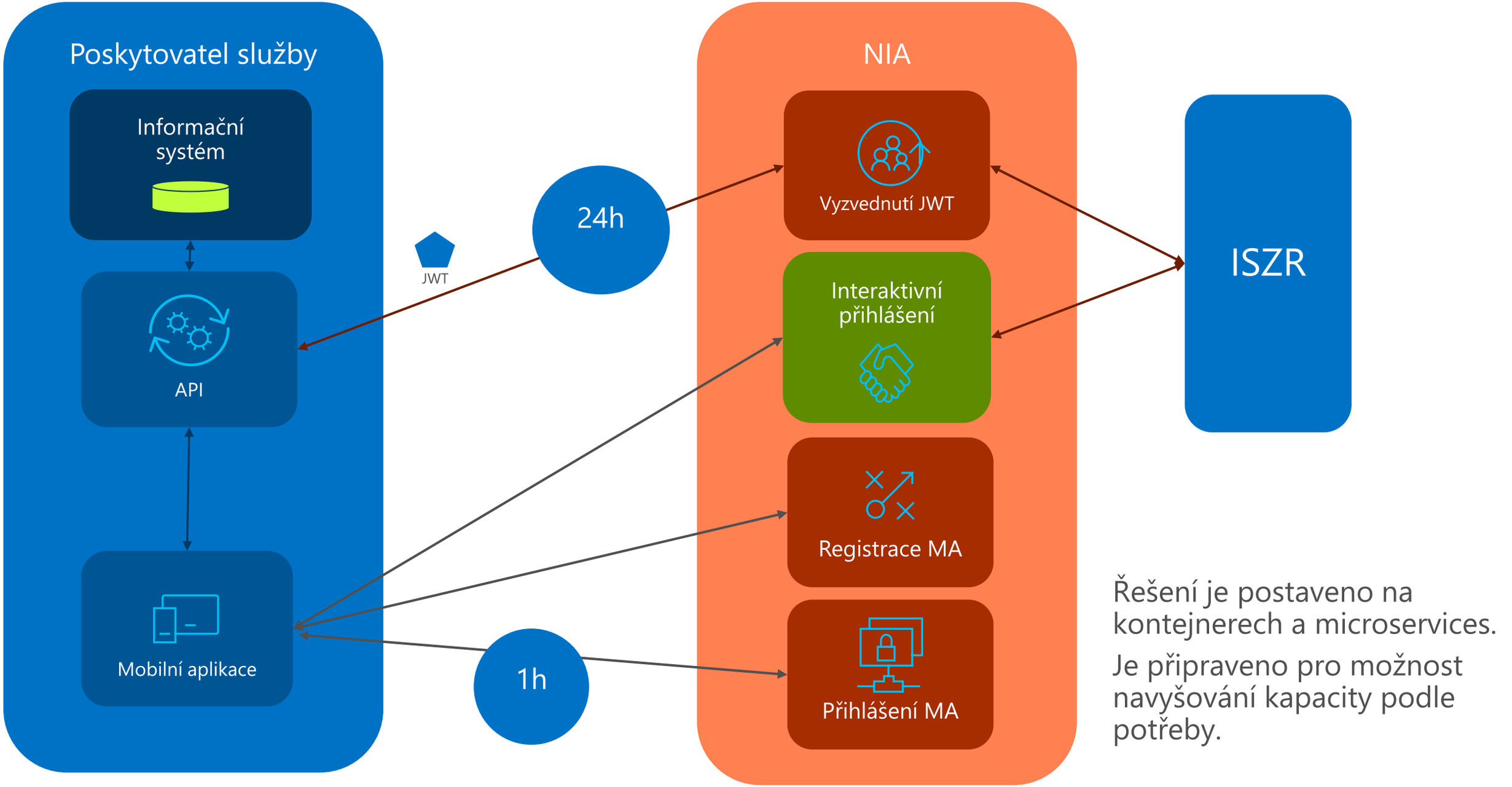
- rozhraní pro registraci mobilní aplikace
- rozhraní pro přihlášení mobilní aplikace
- rozhraní pro API, které si bude z NIA vyzvedávat JWT

U

Uživatel

- nainstaluje si aplikaci od poskytovatele služby
- po prvním spuštění aplikace provede interaktivní přihlášení přes NIA, které zajistí registraci aplikace v NIA
- bude používat funkce mobilní aplikace
- podle potřeby bude opakovat interaktivní přihlášení z aplikace pokud z nějakého důvodu bude registrace v NIA zrušena/zneplatněna

Základní architektura



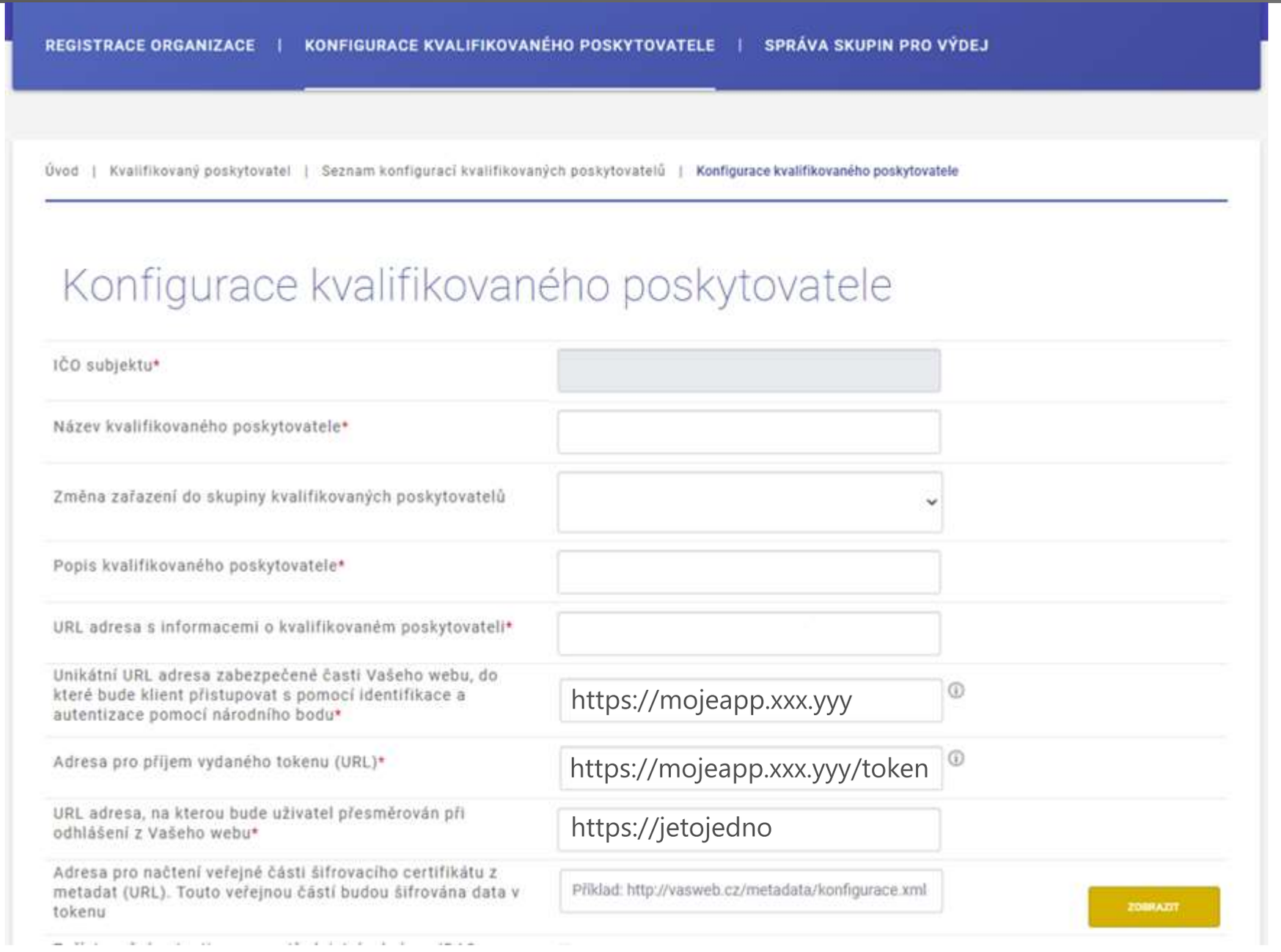
Řešení je postaveno na kontejnerech a microservices.

Je připraveno pro možnost navyšování kapacity podle potřeby.

Obecná registrace poskytovatele služeb na NIA

Zvýrazněné jsou klíčové části registrace

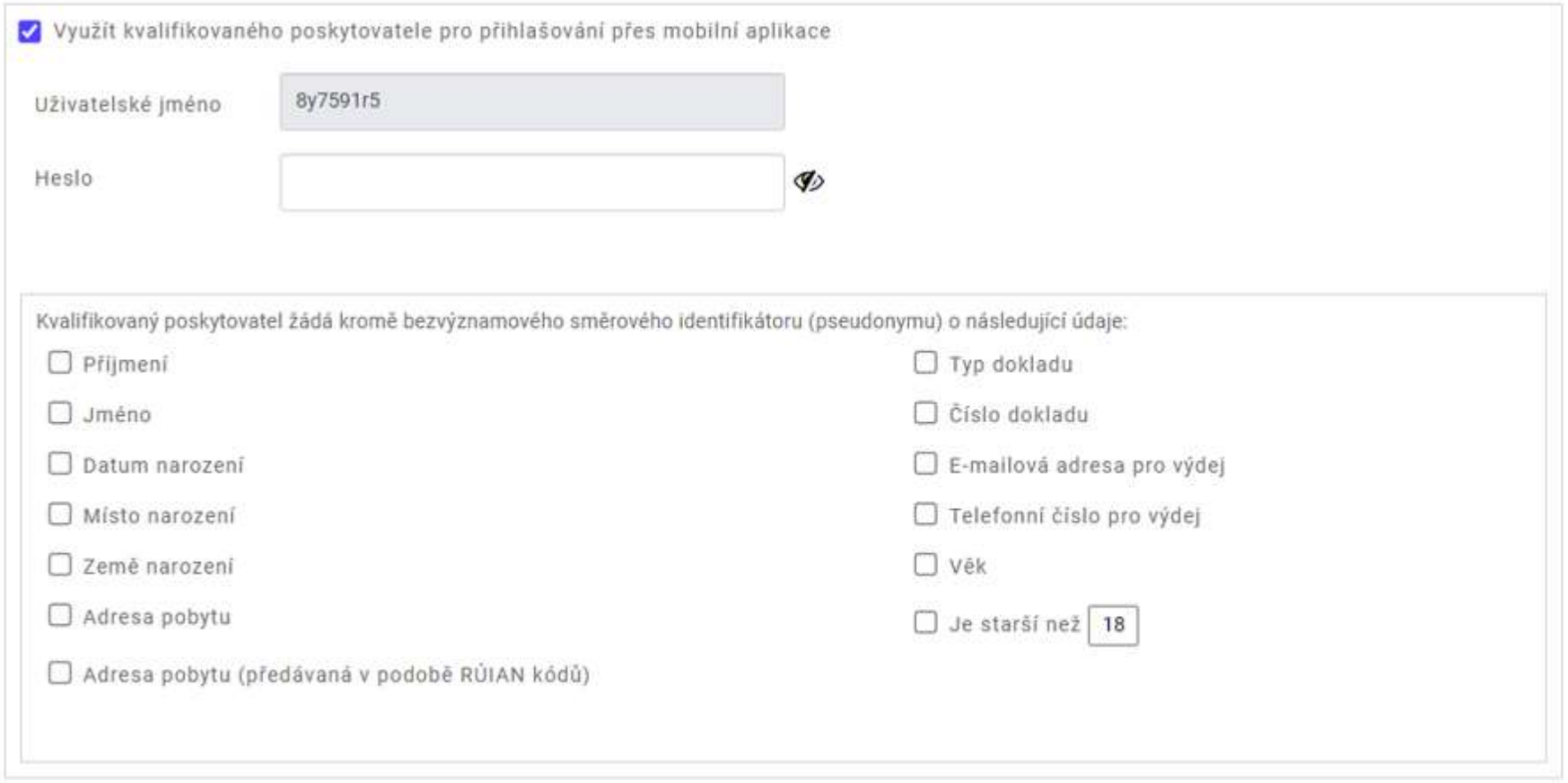
- Realm (unikátní URL)
- URL pro embedded browser pro odchycení Access tokenu
- URL pro odhlášení není používáno



Registrace poskytovatele služeb – mobilní aplikace

Jméno a heslo pro přihlašování API

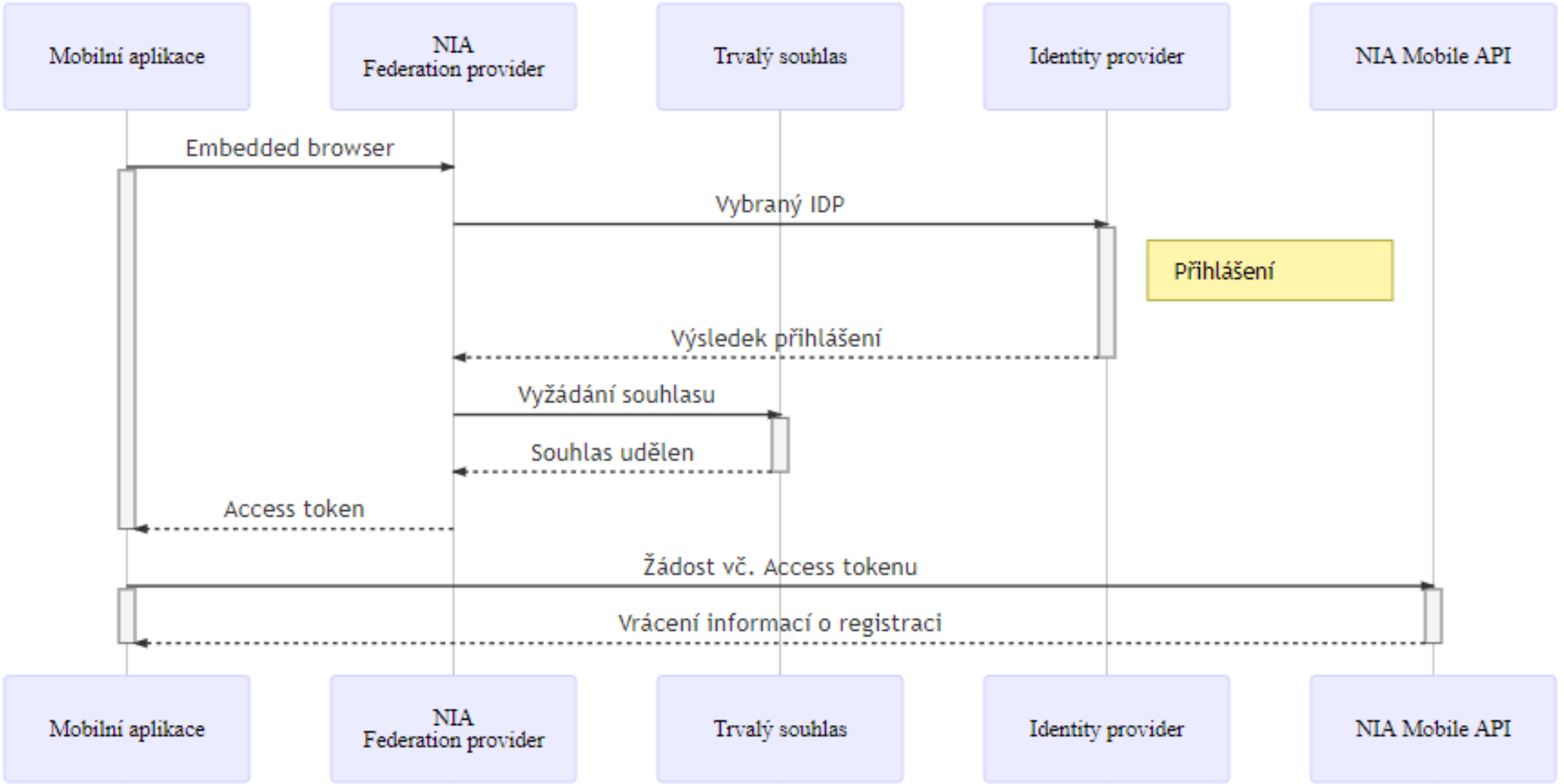
Výběr atributů, které API bude dostávat v JWT



Varování

Změna atributů anebo identifikátoru (realm) vede k tomu, že se zruší registrace (tzv. hromadné odvolání vydaných trvalých souhlasů) všech doposud registrovaných mobilních aplikací a uživatelé se musí znovu interaktivně přihlásit.

Registrační proces



Registrační proces

1. Po prvním spuštění aplikace anebo v případě, že registrace aplikace již není platná, provede mobilní aplikace přesměrování na NIA Federation providera. Doporučenou metodou je využití tzv. embedded browser. Jedná se o způsob, kdy je prohlížeč zobrazen, jako součást mobilní aplikace a neotevírá se samostatné okno prohlížeče. Způsob využití a programování záleží na operačním systému mobilní platformy a na frameworku použitého pro programování mobilní aplikace.

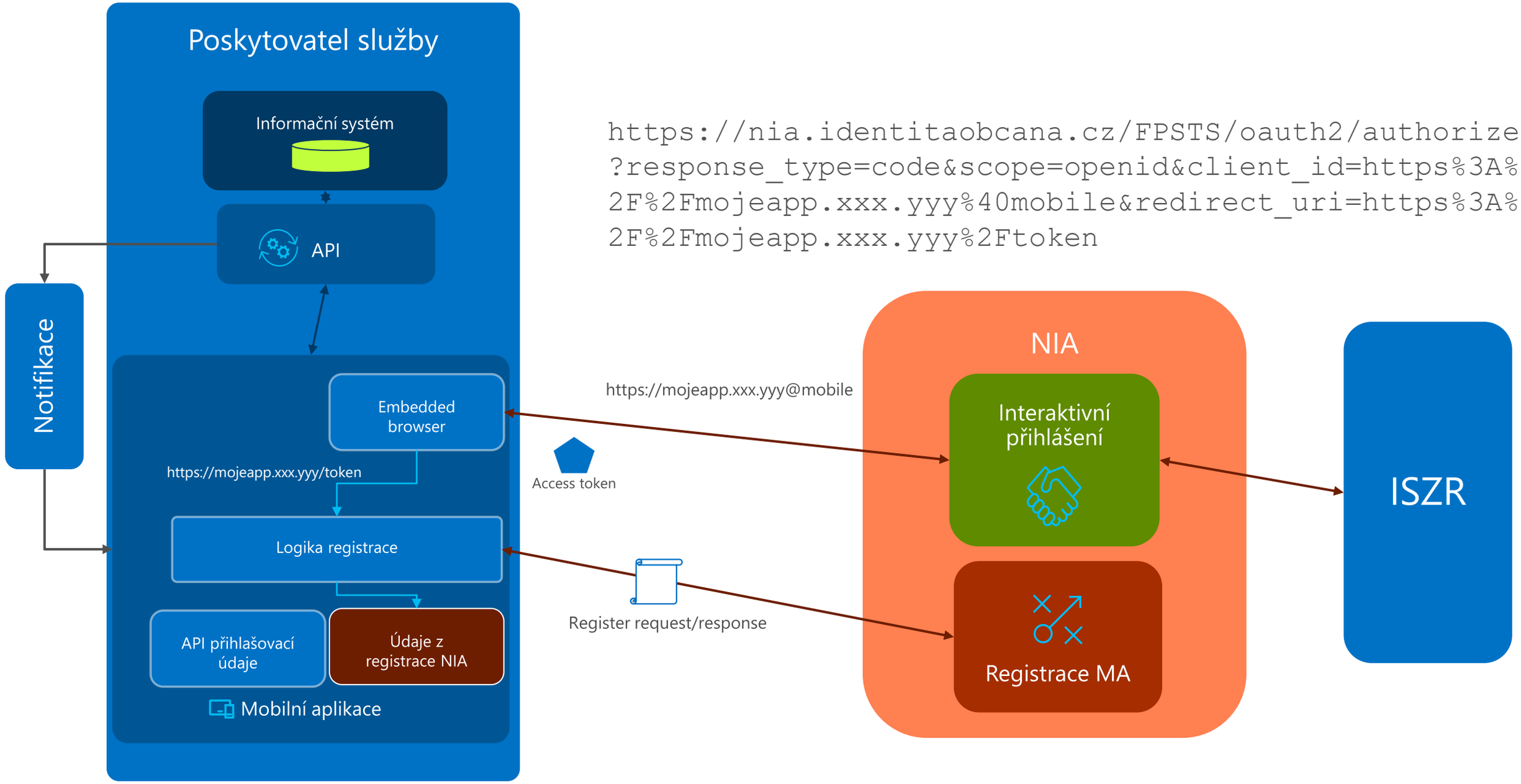
2. Uživatel provede přihlášení zvolenou přihlašovací metodou a musí udělit trvalý souhlas s vydáváním atributů, které jsou poskytovatelem služeb vyžadovány. Po poskytnutí trvalého souhlasu bude aplikaci vrácen access token. Tento access token bude následně použit pro autorizaci volání webové služby pro registraci mobilní aplikace.

3. Mobilní aplikace zašle žádost o registraci mobilního zařízení na definovanou URL NIA pro registraci.

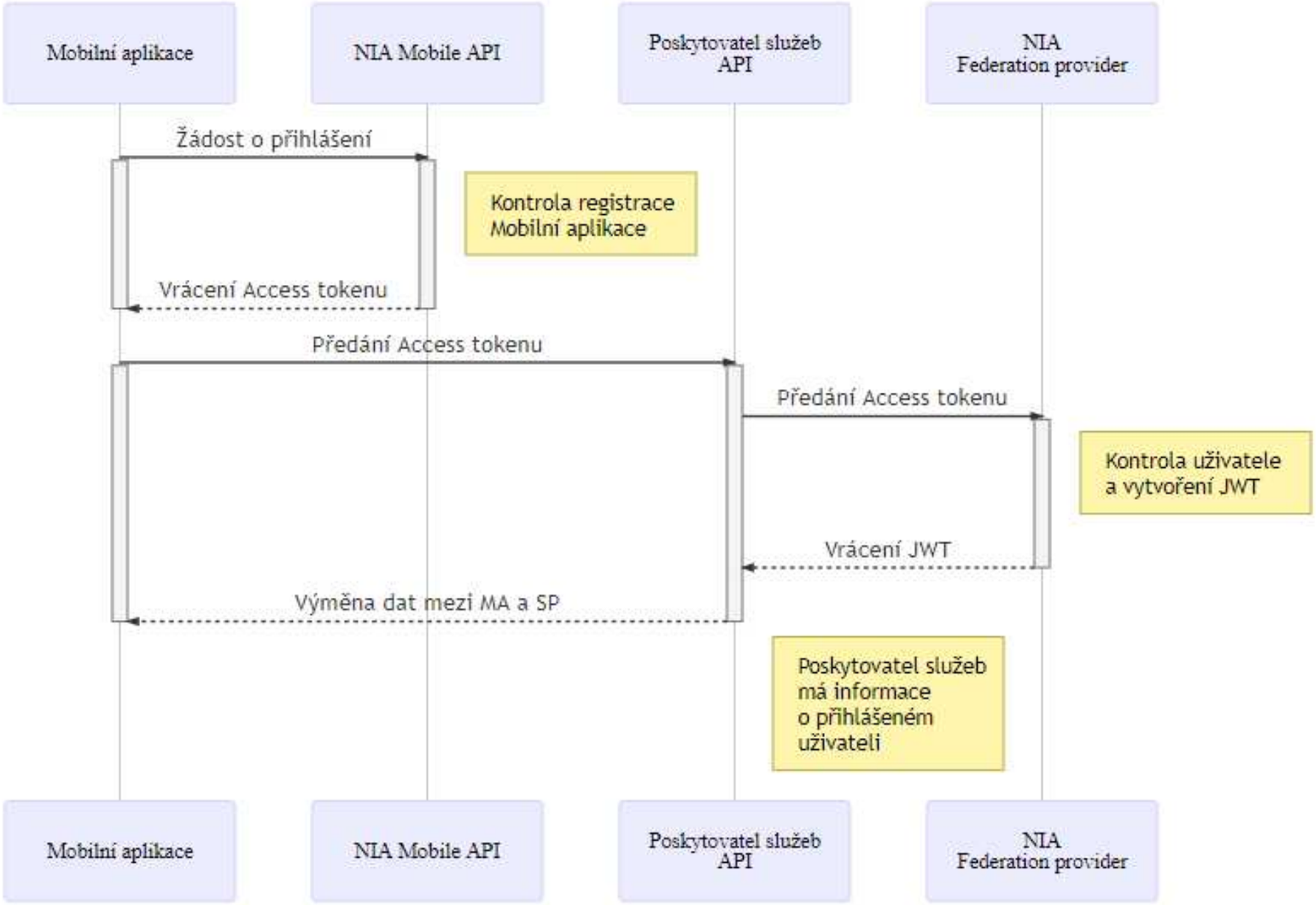
4. NIA žádost o registraci přijme. Vygeneruje unikátní identifikátor mobilní aplikace, rozlišovací identifikátor a tajemství pro výpočet OTP. OTP je vytvářeno dle RFC6238 .

5. Mobilní aplikace přijme odpověď a do zabezpečeného úložiště mobilního zařízení uloží registrační údaje, které budou následně sloužit pro přihlašování mobilní aplikace.

Mobilní aplikace a registrační proces



Přihlašovací proces



Přihlašovací proces

1. Mobilní aplikace vytvoří žádost o přihlášení.
2. Žádost o přihlášení bude zaslána na definované URL.
3. Rozhraní přijme žádost a vyhledá zařízení v databázi mobilních aplikací. Pokud je aplikace nalezena, pokračuje zpracování dále. Jinak je vytvořena chybová zpráva o tom, že mobilní aplikace není registrována a mobilní aplikace musí znovu zahájit proces registrace.
4. Vytvoří se odpověď Login response.
5. Mobilní aplikace zpracuje odpověď, ze které získá Access Token.
6. Mobilní aplikace zavolá rozhraní (API) Service Providera (protokol je plně v kompetenci SePa) a předá Access token, popř. další informace, které bude vyžadovat tvůrce aplikace.
7. SeP (API) připraví žádost o vydání tokenu a zavolá službu NIA FP pro vydání JWT na základě Access Tokenu. Komunikace bude založena na specifikaci OAuth. Při volání musí SeP poskytnout své přihlašovací údaje a Access Token.
8. NIA FP ověří registraci SePa.
9. NIA FP vytvoří JWT na základě Access Tokenu, který bude obsahovat zaregistrované atributy a vrátí JWT.
10. SeP (API) má příslušné informace o přihlášeném uživateli. SeP může na základě získaných informací o uživateli provádět své požadované operace.

Zabezpečení datových zpráv - šifrování

Zprávy pro registraci a login jsou zabezpečeny šifrováním.

Pro šifrování je použitá kombinace algoritmů AES_256/ECB/NoPadding a RSA/ECB/PKCS1Padding.

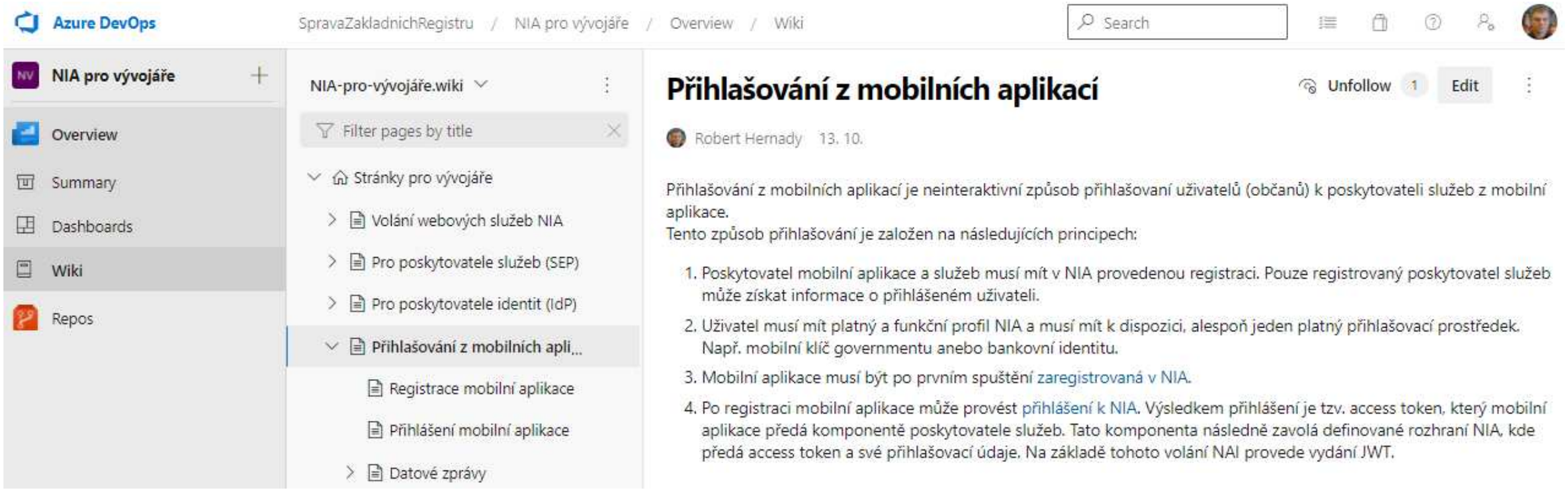
Strana, která připravuje zprávu k odeslání nejdříve vygeneruje AES klíč, kterým provede zašifrování datové zprávy.

Takto zašifrovanou zprávu vloží do elementu Data v datové obálce.

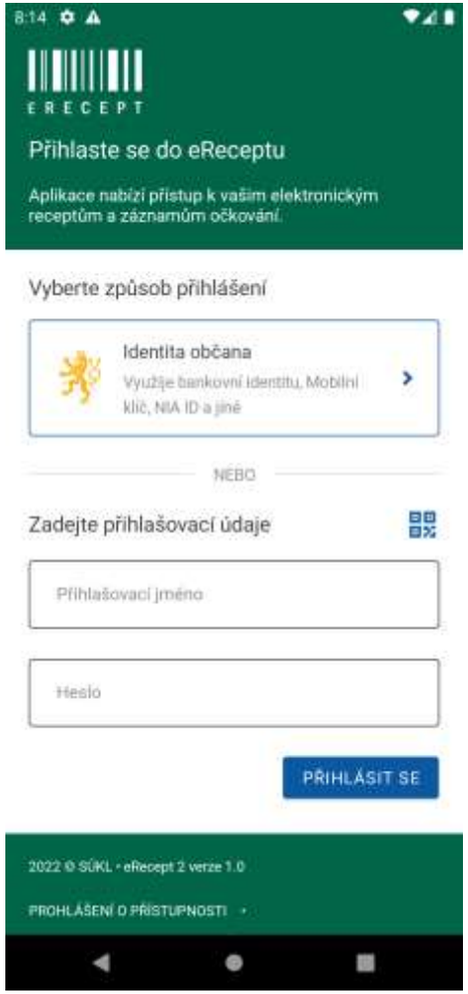
Dále odesílající strana zašifruje AES klíč veřejným klíčem strany, která zprávu přijímá a výsledek vloží do elementu Key v datové obálce.

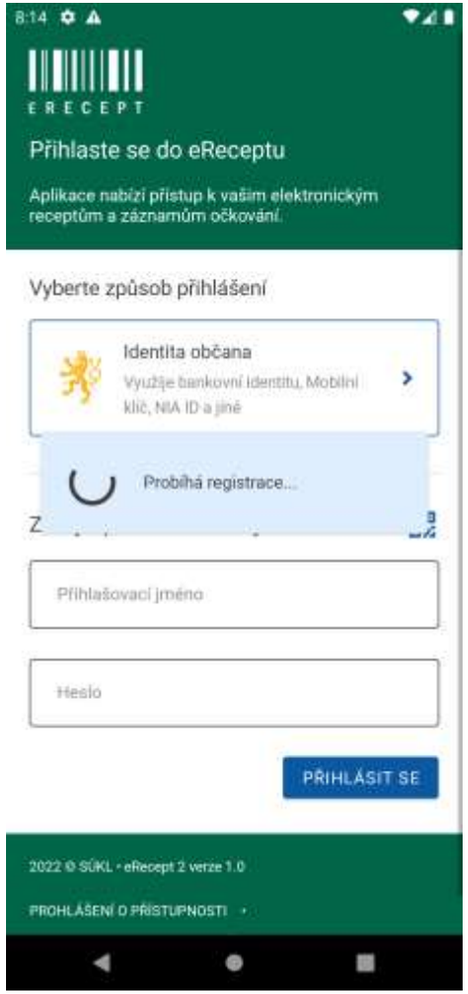
Wiki pro vývojáře

https://dev.azure.com/SpravaZakladnichRegistru/NIA%20pro%20v%C3%BDvoj%C3%A1%C5%99e



Příklad realizace mobilní aplikace - eRecept





Microsoft Cloud pomáhá digitalizaci

Dotazy