

Přihlašování k NIA z mobilních aplikací



Identita
občana

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



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

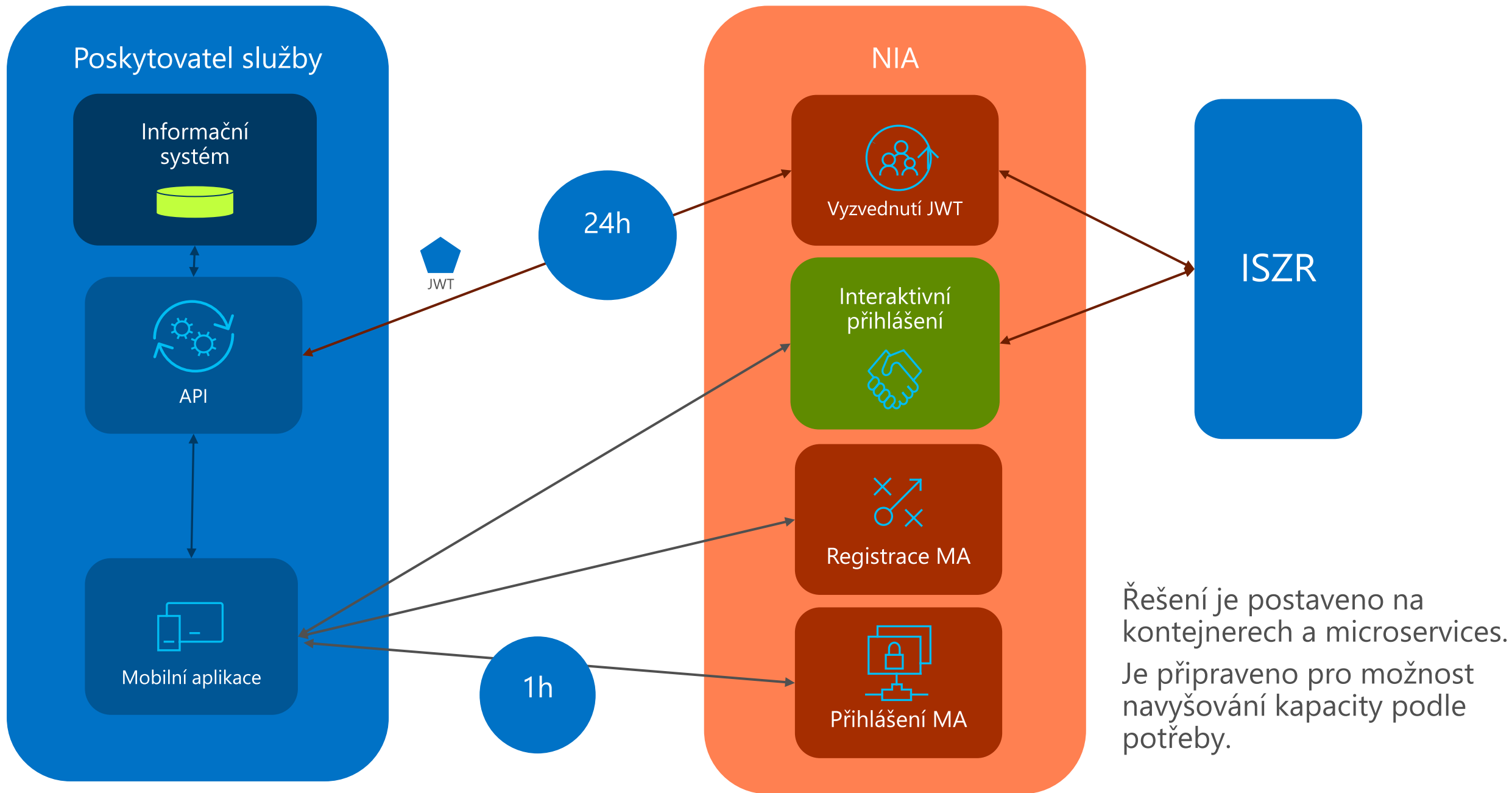
- rozhraní pro registraci mobilní aplikace
- rozhraní pro přihlášení mobilní aplikace
- rozhraní pro API, které si bude z NIA vyzvedávat JWT

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



Obecná registrace poskytovatele služeb na NIA

Zvýrazněné jsou klíčové části registrace

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

REGISTRACE ORGANIZACE | KONFIGURACE KVALIFIKOVANÉHO POSKYTOVATELE | SPRÁVA SKUPIN PRO VÝDEJ

Úvod | Kvalifikovaný poskytovatel | Seznam konfigurací kvalifikovaných poskytovatelů | Konfigurace kvalifikovaného poskytovatele

Konfigurace kvalifikovaného poskytovatele

IČO subjektu*	<input type="text"/>
Název kvalifikovaného poskytovatele*	<input type="text"/>
Změna zařazení do skupiny kvalifikovaných poskytovatelů	<input type="text" value="▼"/>
Popis kvalifikovaného poskytovatele*	<input type="text"/>
URL adresa s informacemi o kvalifikovaném poskytovateli*	<input type="text"/>
Unikátní URL adresa zabezpečené části Vašeho webu, do které bude klient přistupovat s pomocí identifikace a autentizace pomocí národního bodu*	<input type="text" value="https://mojeapp.xxx.yyy"/> ⓘ
Adresa pro příjem vydaného tokenu (URL)*	<input type="text" value="https://mojeapp.xxx.yyy/token"/> ⓘ
URL adresa, na kterou bude uživatel přesměrován při odhlášení z Vašeho webu*	<input type="text" value="https://jetojedno"/>
Adresa pro načtení veřejné části šifrovacího certifikátu z metadat (URL). Touto veřejnou částí budou šifrována data v tokenu	<input type="text" value="Příklad: http://vasweb.cz/metadata/konfigurace.xml"/>

ZOBRAZIT


Registrace poskytovatele služeb – mobilní aplikace

Jméno a heslo pro přihlašování API

Výběr atributů, které API bude dostávat v JWT

Využít kvalifikovaného poskytovatele pro přihlašování přes mobilní aplikace

Uživatelské jméno

Heslo 

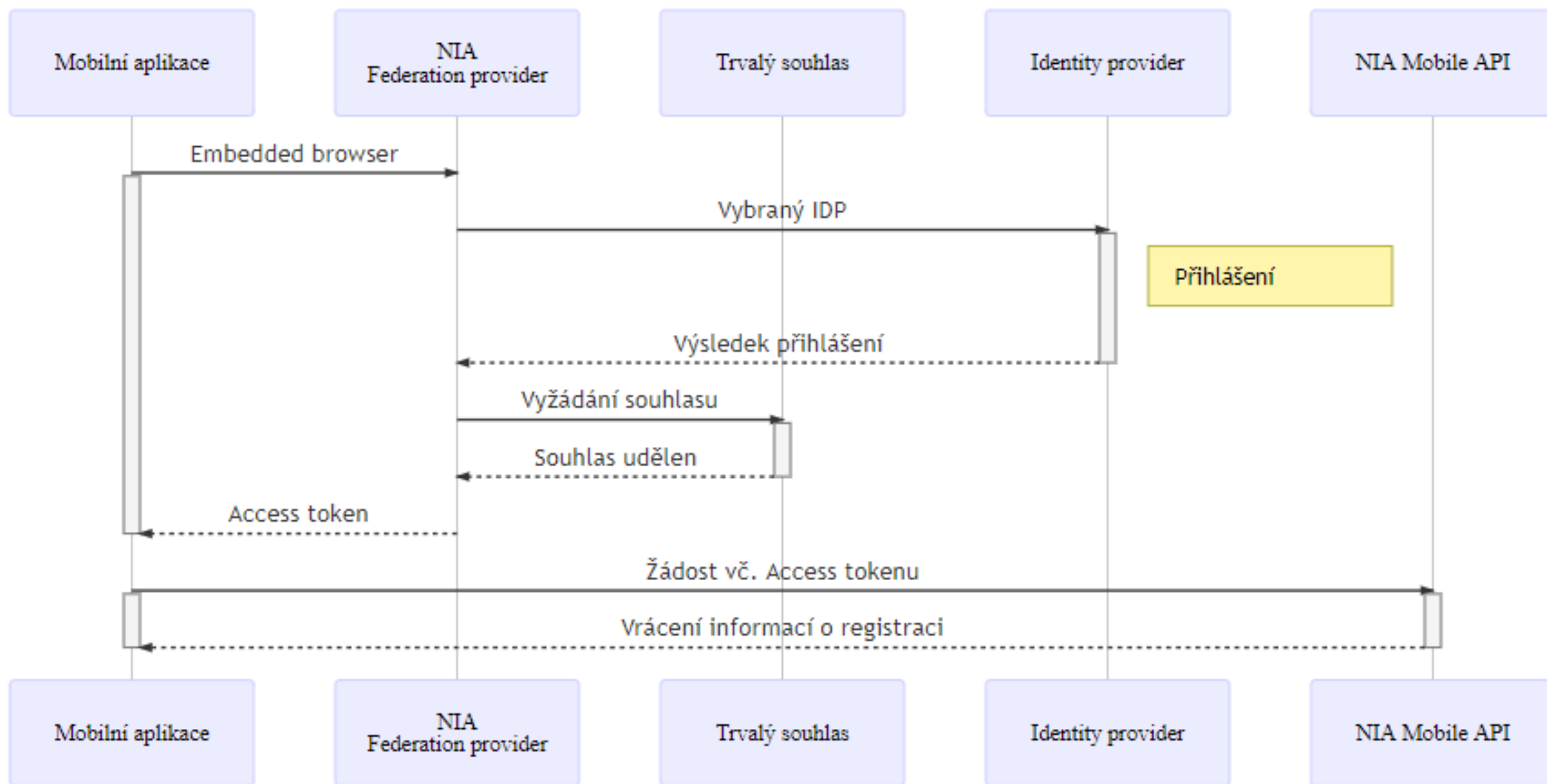
Kvalifikovaný poskytovatel žádá kromě bezvýznamového směrového identifikátoru (pseudonymu) o následující údaje:

<input type="checkbox"/> Příjmení	<input type="checkbox"/> Typ dokladu
<input type="checkbox"/> Jméno	<input type="checkbox"/> Číslo dokladu
<input type="checkbox"/> Datum narození	<input type="checkbox"/> E-mallová adresa pro výdej
<input type="checkbox"/> Místo narození	<input type="checkbox"/> Telefonní číslo pro výdej
<input type="checkbox"/> Země narození	<input type="checkbox"/> Věk
<input type="checkbox"/> Adresa pobytu	<input type="checkbox"/> Je starší než <input type="text" value="18"/>
<input type="checkbox"/> Adresa pobytu (předávaná v podobě RÚIAN kódů)	

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.

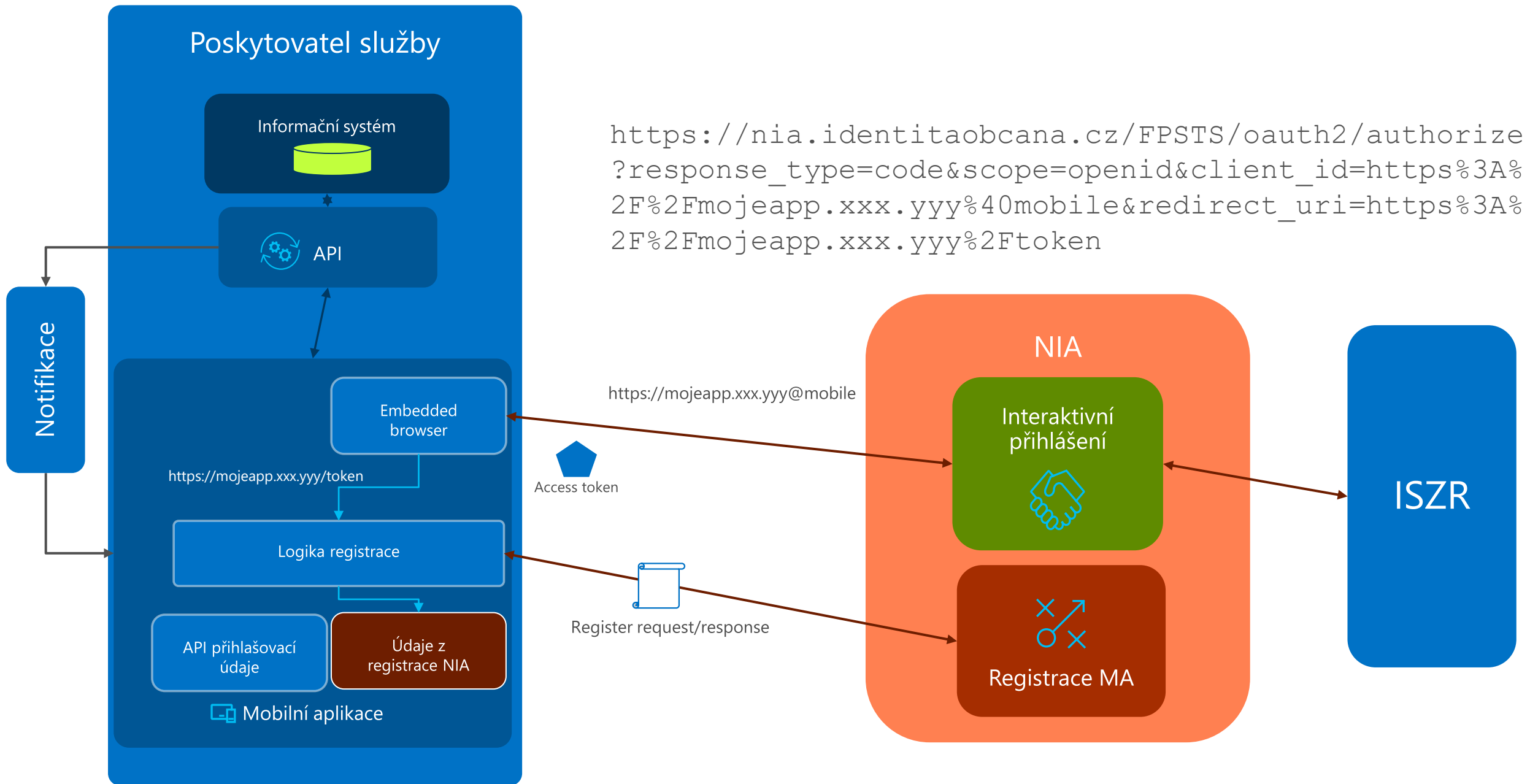
Registrační proces



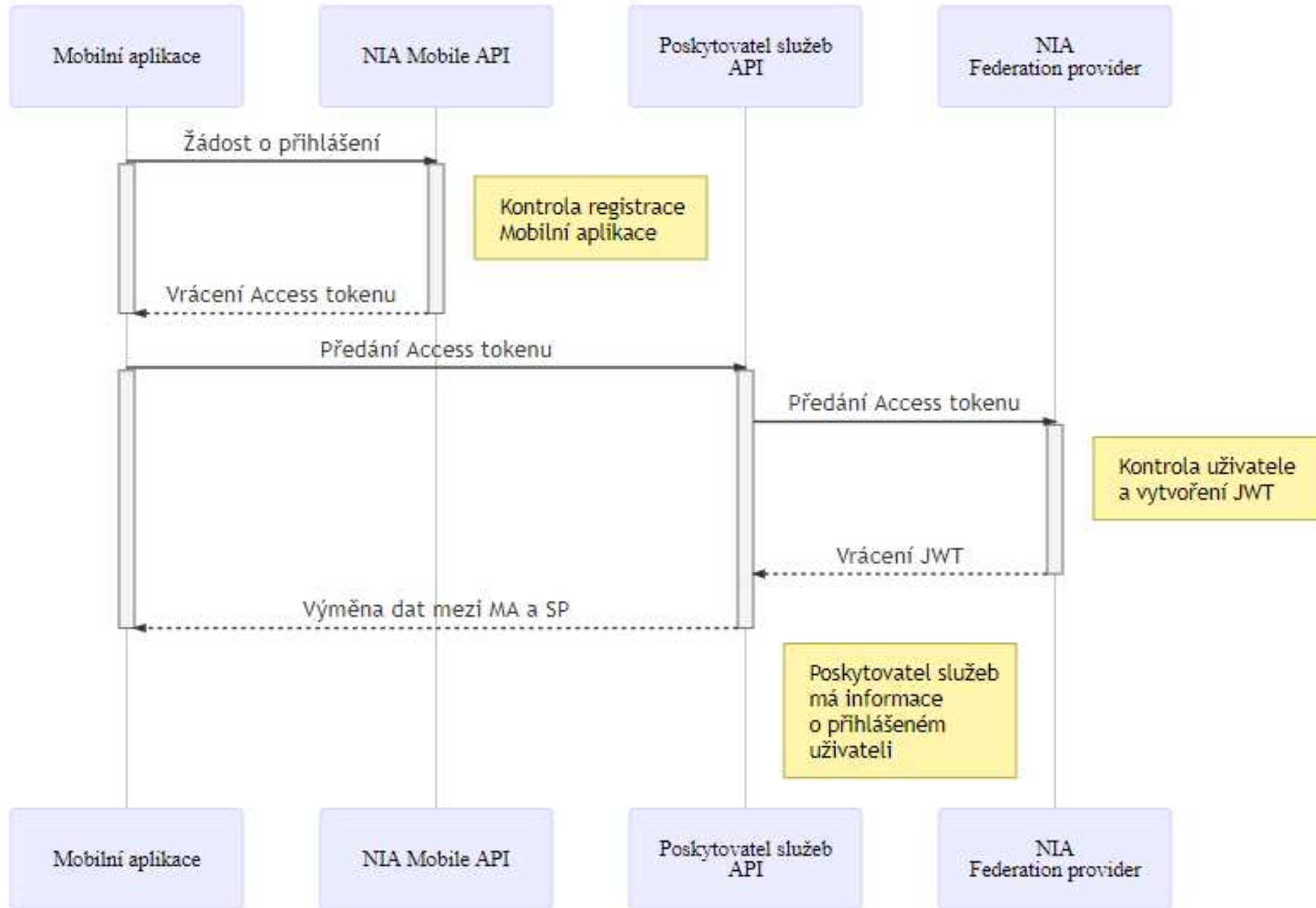
Registrační proces

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 neotevřít 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 použita 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.

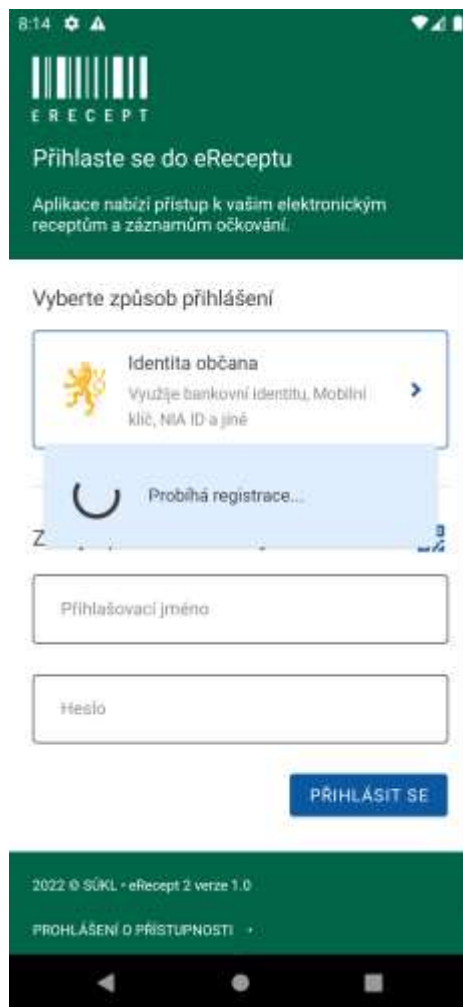
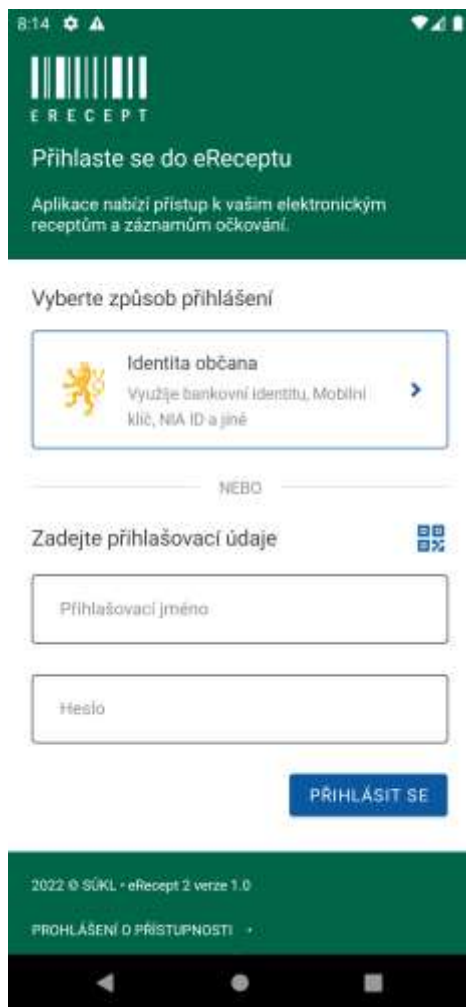
Wiki pro vývojáře

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

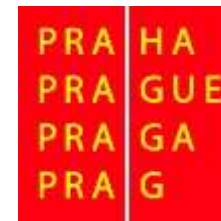
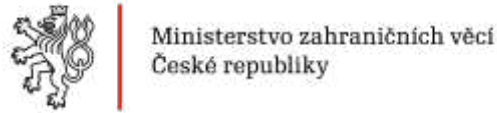
The screenshot shows the Azure DevOps interface. The top navigation bar includes the Azure DevOps logo, the breadcrumb path 'SpravaZakladnichRegistru / NIA pro vývojáře / Overview / Wiki', a search box, and user profile icons. The left sidebar contains a navigation menu with items: 'NIA pro vývojáře', 'Overview', 'Summary', 'Dashboards', 'Wiki', and 'Repos'. The main content area displays the article 'Přihlašování z mobilních aplikací' by Robert Hernady, dated 13. 10. The article text explains that mobile app authentication is non-interactive and based on the following principles:

1. Poskytovatel mobilní aplikace a služeb musí mít v NIA provedenou registraci. Pouze registrovaný poskytovatel služeb může získat informace o přihlášeném uživateli.
2. Uživatel musí mít platný a funkční profil NIA a musí mít k dispozici, alespoň jeden platný přihlašovací prostředek. Např. mobilní klíč governmentu anebo bankovní identitu.
3. Mobilní aplikace musí být po prvním spuštění **zaregistrovaná v NIA**.
4. Po registraci mobilní aplikace může provést **přihlášení k NIA**. Výsledkem přihlášení je tzv. access token, který mobilní aplikace předá komponentě poskytovatele služeb. Tato komponenta následně zavolá definované rozhraní NIA, kde předá access token a své přihlašovací údaje. Na základě tohoto volání NAI provede vydání JWT.

Příklad realizace mobilní aplikace - eRecept



Microsoft Cloud pomáhá digitalizaci





Dotazy