

**Kancelária Lepšie Služby**

**Definícia jednotného rozhrania služby MobileID**

**(zadanie pre štátnych operátorov DEUS a NASES)**

|  |  |
| --- | --- |
| **VERZIA DOKUMEnTU** | r1.0 (Final) |
| **dáTUM VYDANIA**  **id DOKUMENTU**  **aUTOR**  **Spolupracovali** | 03.12.2019  UPVIIJednotneRozhranieMobileID\_r12\_final.docx  ÚPPVII (Kancelária Lepších služieb)  Dokument vznikol za účasti pracovníkov oboch budúcich štátnych operátorov služby MobileID – DEUS aj NASES |

# Obsah

[Obsah 2](#_Toc26269729)

[Predslov k dvom operátorom a jednotnému rozhraniu mID 3](#_Toc26269730)

[1. Scenár: Samoobslužná registrácia mobilnej identity. 4](#_Toc26269731)

[2. Scenár: Prihlasovanie mobile2mobile. 6](#_Toc26269732)

[2.1 Scenár prihlasovania, v ktorom ide len o využitie identity 7](#_Toc26269733)

[2.1.1 Komunikácia A3S (Aplikácia tretej strany) – mID (aplikácia jedného z operátorov) 7](#_Toc26269734)

[2.1.2 Proces po zavolaní mID 8](#_Toc26269735)

[2.1.3 Komunikácia miD (aplikácia jedného z operátorov) – A3S 9](#_Toc26269736)

[2.1.3.1 Služba overenia identitných údajov 10](#_Toc26269737)

[2.2 Scenár prihlasovania, v ktorom ide aj o získanie autorizácie pre vyvolávania OpenAPI služieb 10](#_Toc26269738)

[2.2.1 Komunikácia A3S – user-agent (prehliadač) 12](#_Toc26269739)

[2.2.2 Proces po zavolaní user-agent-a (prehliadač) 12](#_Toc26269740)

[2.2.3 Komunikácia user-agent (prehliadač) – A3S 12](#_Toc26269741)

[3. Scenár: Prihlasovanie desktop2mobile. 13](#_Toc26269742)

[3.1.1 Komunikácia web tretej strany – user-agent (prehliadač) 14](#_Toc26269743)

[3.1.2 Proces po zavolaní prehliadača 14](#_Toc26269744)

[3.1.3 Komunikácia user-agent (prehliadač) – A3S 15](#_Toc26269745)

[4. Scenár: Podpisovanie v eGov z centrálnej komponenty ÚPVS (CPK). 16](#_Toc26269746)

[4.1.1 Komunikácia CPK → mID 17](#_Toc26269747)

[4.1.2 Komunikácia web/mobilná aplikácia OVM -> CPK 17](#_Toc26269748)

# 

# Predslov k dvom operátorom a jednotnému rozhraniu mID

Na ÚPVII bolo prijaté rozhodnutie, spustiť bezodkladne dodávku služby mobilnej autentifikácie a autorizácie (ďalej v dokumente „služba mID“) s cieľom zabezpečiť, aby táto služba, minimálne vo verzii 1.0, začala slúžiť a zjednodušovať prihlasovanie a autorizáciu občanom a podnikateľom Slovenskej republiky – vysoko prioritná funkcionalita už do 3 mesiacov od spustenia prác.

Pre tento účel bolo rozhodnuté, že štát spustí službu mID s konceptom nie jedného, ale dvoch alternatívnych štátnych operátorov. To prakticky znamená, že v ekosystéme štátneho IT budú vedľa seba fungovať dve čo najviac autonómne (fyzické) riešenia, od dvoch organizácií (NASES aj DEUS). Z vecnej povahy predchádzajúceho konštatovania vyplýva aj otvorenosť celého konceptu, v prípade, že v budúcnosti bude operátorov viac. Odkomunikovať dôvody takéhoto rozhodnutia, nie je úlohou a ani obsahom tohto dokumentu – úlohou dokumentu a zároveň ÚPVII Kancelárie Lepších služieb, je zadefinovať a zafixovať **„jednotné (logické) rozhranie“ služby mID**, ktoré pod sebou na jednej strane umožní čo najvyššiu mieru autonómnej prevádzky dvoch riešení, na strane druhej zjednoduší využívanie služby mID organizáciami tak vo vnútri štátu (OVM), ako aj z komerčného sektora. Pre využívajúce organizácie tak bude jedno, na akého operátora sa pripájajú, vždy bude spôsob jeho využívania rovnaký (to šetrí ich implementačný čas a zjednodušuje využívanie služby mID).

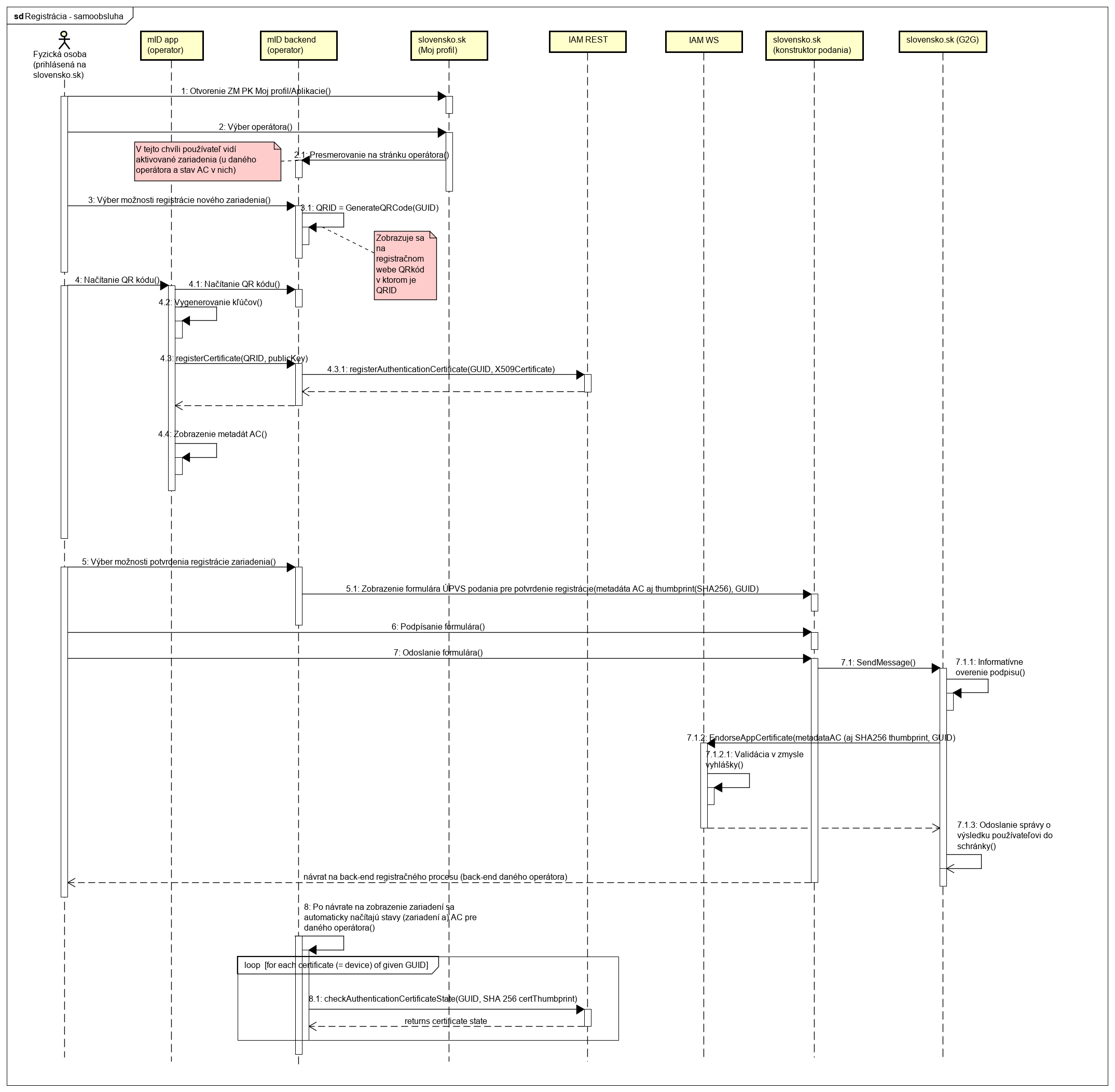
V rámci fázy 1 je tak potrebné, aby obaja operátori implementovali.:

* Povinne:
  + Najvyššia priorita (vyžadované delivery do 3 mesiacov od spustenia prác): Scenár samoobslužnej registrácie mobilnej identity a scenáre pre Prihlasovanie –mobile2mobile, aj desktop2mobile.
  + NASES, keďže zároveň plní úlohu Federačnej autority - navyše univerzálne rozhranie a pripojenie oboch operátorov do federovaného identitného systému.
  + Štandardná priorita (vyžadované delivery do 6 mesiacov od spustenia prác): Autorizácia (podpis) klikom pomocou CPK.
* Voliteľne: Podpisovanie pre komerčný sektor – scenár mobile2mobile, aj desktop2mobile (nepodlieha zatiaľ záväznej špecifikácii ÚPVII aj keď v budúcnosti môže).

# Scenár: Samoobslužná registrácia mobilnej identity.

Vzhľadom na to, že scenár samoobslužnej registrácie (alebo deaktivácie) mobilnej identity nie je integračný pre organizáciu využívajúcu služby mID (je to scenár, ktorý implementujú operátori), je tento v rámci dokumentu popísaný ako základný tok krokov. Slúži tak na ilustráciu, ako proces (samo)registrácie aktívnej identity prebieha. Doprevádzajúca schéma (sekvenčný diagram) poskytuje požadovanú nižšiu úroveň detailu identitu.

1. Pre zachovanie čo najvyššej miery autonómnosti riešení oboch opertárov, „jednotné rozhranie“ pre registráciu a zrušenie mobilnej idenity predpokladá iba existenciu jedného miesta – konkrétne portálu ÚPVS, odkiaľ bude existovať **rovnocenné a rovnako vidieteľné prelinkovanie** do registračných systémov oboch operátorov (samozrejme zachová sa SSO).
2. V rámci registračného systému daného operátora musí občan (jeho identita) vidieť „svoje“ aktivované zariadenia (v jednom zariadení má jedna identita jeden aktívny autentifikačný certifikát, teda pre jednu identitu daný certifikát vlastne určuje aj zariadenie). Na začiatku občan nemá aktivované (u daného operátora) žiadne zariadenia (a teda ani jemu prislúchajúci autentifikačný certifikát).
3. Občan zvolí „zaregistrovať nové zariadenie“. Operátor mu zobrazí QR kód, nasnímaním ktorého z mobilnej aplikácie mID daného operátora (ktorú si občan na predmetné zariadenie stiahol) sa spustí proces vygenerovania páru privátneho a verejného kľúča v mobilnom zariadení.
4. Operátor zaregistruje k danému kľúčovému páru prislúchajúci autentifikačný certifikát (formát X509) do Centrálneho Registra autentifikačných certifikátov v prevádzke NASES. AC je zatiaľ v stave neaktívny.
5. Registračný proces u operátora pokračuje prípravou žiadosti (cez ÚPVS konštruktor správ), podpisom a odoslaním ktorej – občan potvrdí aktiváciu daného AC. V tomto bode musí používateľ vizuálne skontrolovať zhodu meta údajov certifikátu a thumbprintu uvedeného v žiadosti na podaní a údajmi o certifikáte/thumbprinte, ktoré si používateľ zobrazí v mobilnom zariadení (konštruktor správ aj mobilná aplikácia operátora toto zobrazenie musia podporovať).
6. Daný AC je následne úspešne aktivovaný (asynchrónny proces) a občan končí registračný proces opäť na obrazovke, kde vidí svoje spravované zariadenia (aj so stavom AC z registra AC, ktoré k nim prislúchajú).



Zhrnutie a dôležité doplnenia pre samoobslužný scenár.:

* Novovzniknutá mobilná identita musí byť v samoobslužnom scenári odvodená z eID a pri jej aktivácii musí byť „verejná“ časť odvodenej identity – využívaná pre prihlasovanie (a dodatočnú autentifikáciu ÚPVS) - uložená v tzv. centrálnom registri autentifikačných certifikátov ÚPVS.
* Aj keď proces a rozhrania to umožňujú, v tejto chvíli môže jeden občan mať v rámci jedného operátora v jednej chvíli aktivované len **N** zariadení. Kontrolu na počty aktívnych zariadení pre jednu identitu - bude robiť operátor aj CRAC.
* Potvrdenie aktivácie autentifikačného certifikátu v registri autentifikačných certifikátov, vykonáva občan elektronickou žiadosťou, ktorá obsahuje elektronický formulár. Správa obsahujúca žiadosť je vo formáte SkTalk.(formulár a jeho fungovanie v konštruktore podania pripraví NASES – bude fungovať jeden formulár pre všetkých operátorov). Pričom podpisuje sa vyplnený formulár obsahujúci dohodnuté údaje o žiadateľovi (meta údaje podľa obrázka) ako aj odtlačok registrovaného certifikátu (aby nebolo potrebné podpisovať v rámci podania aj prílohy) a to kvalifikovaným elektronickým podpisom.
* Pre zrušenie certifikátu – musí register autentifikačných certifikátov poskytovať operátorom synchrónnu službu (to už nejde cez podanie).

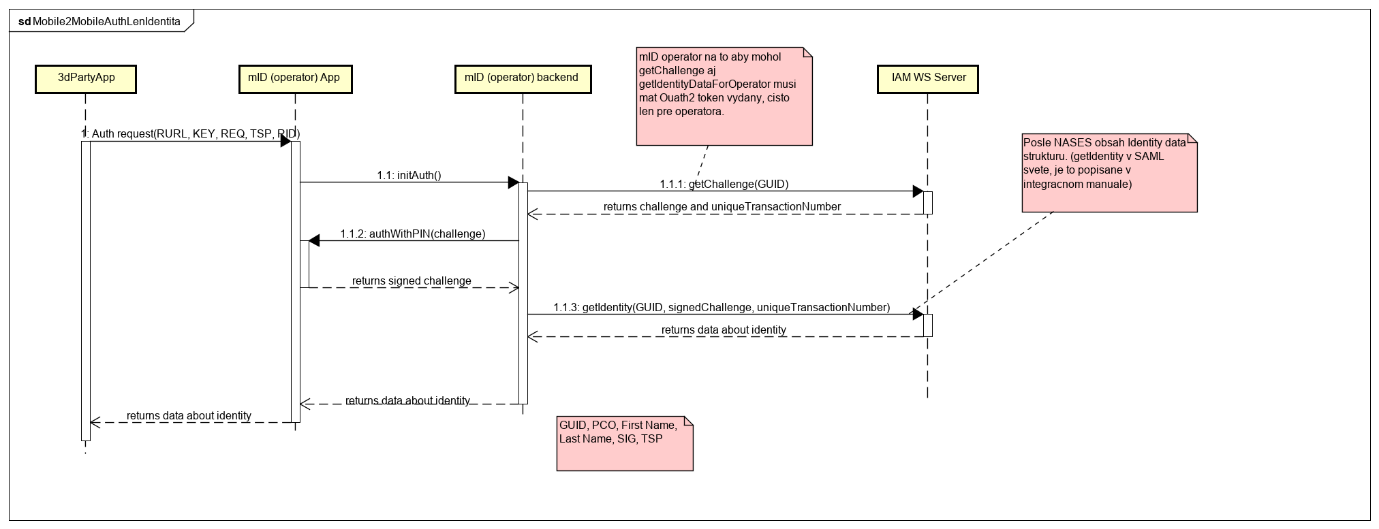
# Scenár: Prihlasovanie mobile2mobile.

V tomto scenári **mobilná** aplikácia tretej strany (je jedno či špecializovaná aplikácia OVM poskytujúca služby danej agendy, alebo špecializovaná biznis aplikácia komerčného subjektu) využije služby prihlásenia mID pomocou **mobilnej** aplikácie jedného zo štátnych operátorov (DEUS, alebo NASES). Všetky mobilné aplikácie (tretej strany, aj jedného, alebo oboch operátorov) sú nainštalované na mobilnom zariadení občana, či podnikateľa.

Pri prihlasovaní (pomocou mobilnej aplikácie operátora) je potrebné uvažovať v dvoch špecializovaných scenároch.:

* V tom prvom ide tretej strane len o využitie identity (typicky len overenie si údajov zadaných od občana voči štátnej identite), resp. len využitie údajov o identite. Tretia strana nepotrebuje a nechce byť súčasťou ekosystému štátneho OpenAPI. V tomto scenári teda tretia strana využíva informácie na overenie identity vo svojich interných procesoch, nechystá sa vyvolávať ďalšie eGov služby, publikované v ekosystéme štátneho OpenAPI. Pre zabezpečenie toho, aby mID nemohol použiť ktokoľvek je nutné aplikáciu tretej strany (A3S) resp. jej návratovú URL schému (v prípade http/https aj hostname) zaregistrovať u registrátora operátorov mID (whitelisting). Súčasťou registrácie je odovzdanie verejného kľúča asymetrického ECC páru registrátorovi mID (t.j. poskytovateľ pred registráciou vygeneruje ECC kľúčový pár), ktorý zároveň pridelí A3S identifikačný kód. Pre ECC je použitá krivka secp256r1
* V druhom ide tretej strane nie len o prihlásenie (autentifikáciu), ale aj o získanie autorizácie občana, či podnikateľa, aby aplikácia v jeho mene mohla vyvolávať služby, publikované v ekosystéme štátneho OpenAPI.

## Scenár prihlasovania, v ktorom ide len o využitie identity



### Komunikácia A3S (Aplikácia tretej strany) – mID (aplikácia jedného z operátorov)

1. mID aplikácia (jedného alebo druhého operátora) "počúva" na definovanej URI schéme, napr. mid-sk (resp. mid-sk-test, mid-sk-dev)
2. Ak je hostname "authenticate", ide o požiadavku na poskytnutie údajov o identite a aplikácia očakáva resp. podporuje nasledovné povinné (pokiaľ nie je uvedené inak) parametre:
   1. RURL - URL adresa na ktorú mobilná aplikácie po autentifikácií presmeruje. RURL musí obsahovať schému, ktorá je v zozname podporovaných (konfigurácia na backende) resp. ak je schéma HTTP resp. HTTPS, tak musí byť podporovaný hostname.
   2. REQ - (nepovinné) zoznam atribútov, ktoré majú byť vrátené. Podporované hodnoty: PCO, GUID, FN, LN. Hodnoty sú oddelené čiarkou. Pokiaľ REQ nie je uvedený, vrátené je GUID
   3. TSP - timestamp requestu vo formáte ISO8601 s presnosťou na milisekundy: yyyy-mm-dd**T**HH:MM:SS.SSS. Bez časovej zóny, resp. timestamp je v UTC
   4. NONCE - 32 bajtový náhodný reťazec generovaný s dostatočnou entrópiou v hex formáte
   5. RID - (nepovinné) referenčné alfanumerické ID transakcie. Slúži na kontrolu a párovanie na strane A3S. Odporúčame použiť formát guid.
3. Reťazec parametrov pospájaný cez oddeľovač | (pipe, ascii 0x7C) je zašifrovaný symetrickým kľúčom tzv. shared secret odvodeným od centrálneho verejného kľúča mID ekosystému (spoločným pre všetkých mID operátorov) a privátneho kľúča A3S. Algoritmus AES/GCM/NoPadding, 12 bajtový náhodný IV (inicializačný vektor) je vložený na začiatok reťazca.
4. Výsledné paramere URL sú:
   1. a3s - kód aplikácie tretej strany pridelený pri registrácií (nutné posielať nezašifrované, keďže mID na základe tejto informácie vyberie príslušný verejný kľúč a vypočíta z neho shared secret)
   2. params - šifrovaný reťazec v uppercase hex formáte

**Príklad URL:**

*mid-sk://authenticate?a3s=MYDATA&params=A1B2C3...*

**Príklad RURL:**

*mydata://mid*

**Príklad parametrov pred šifrovaním:**

*RURL=mydata://mid|REQ=PCO,FN|TSP=2019-12-01T00:01:33.123*|*NONCE=A1B1C1....*

### Proces po zavolaní mID

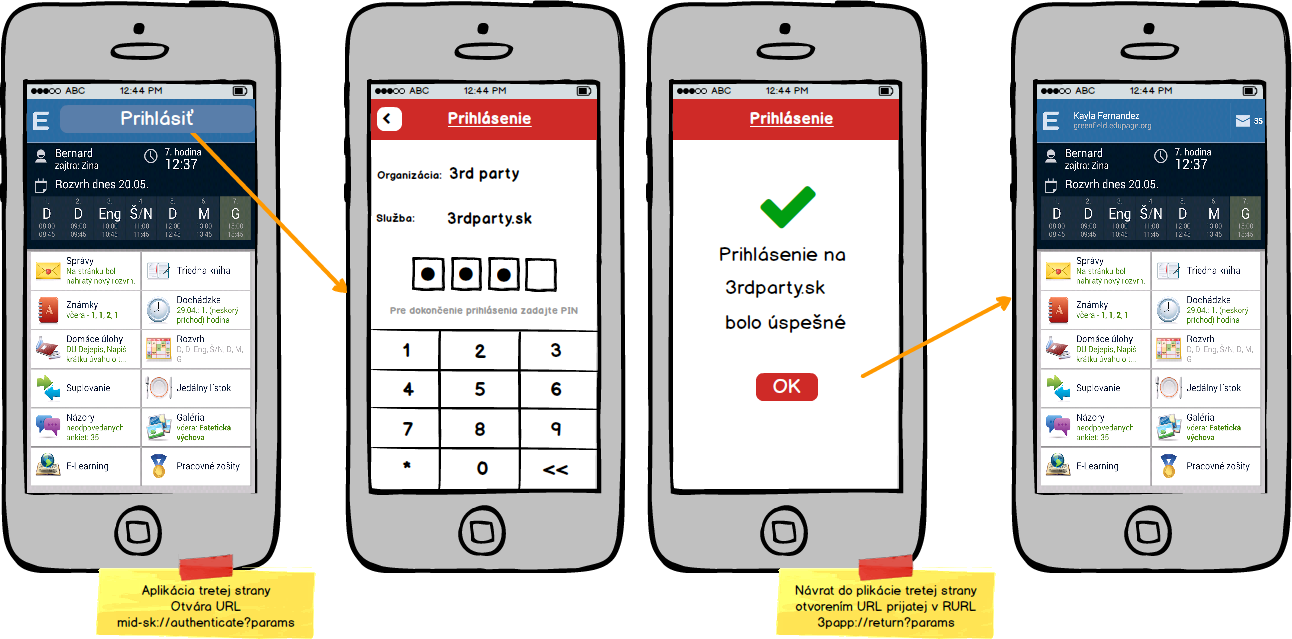
1. mID aplikácia (daného operátora) cez svoj back-end vyžiada IAM WS o prihlasovací challenge. Vo výsledku je vrátené aj číslo transakcie (pomocou ktorého si IAM páruje neskôr kontrolu podpísaného challenge). Na to aby mohol back-end mID aplikácie vyvolať túto službu, musí mať predtým vydaný Oauth2 token, získa ho jednorázovo pomocou Ouath2 client credentials flow (<https://tools.ietf.org/html/rfc6749#section-4.4>), obnovuje napr. raz za deň.
2. mID aplikácia autentifikuje používateľa (PINom, prípadne biometriou), pričom výstupom autentifikácie, je práve podpísaný challenge pomocou privátnej časti autentifikačného certifikátu používateľa (na mobile).
3. mID backend požiada IAM (WS) o informácie, pričom vráti údaje o identite. .
4. mID aplikácia zo získaných údajov "posunie" vybrané údaje volajúcej aplikácii (detailne popísané nižšie)

### Komunikácia miD (aplikácia jedného z operátorov) – A3S

Vyžiadané údaje o identite odovzdáva mID aplikácia (daného operátora) aplikácií tretej strany volaním URL, ktorú mID dostala v parametri RURL. mID aplikácia pridá nasledovné parametre (zoznam parametrov závisí od zoznamu požadovaných parametrov v requeste):

1. PCO - počítačové číslo osoby, ak ho mID poskytol IAM
2. GUID - jedinečný identifikátor osoby, získaný pri registrácii osoby z IAM
3. FN - krstné meno
4. LN - priezvisko
5. TSP - timestamp odpovede vo formáte ISO8601 s presnosťou na milisekundy: yyyy-mm-dd**T**HH:MM:SS.SSS. Bez časovej zóny, resp. timestamp je v UTC
6. RID - mID vráti RID z požiadavky na autentifikáciu
7. OPID - ID mID operátora
8. NONCE - 32 bajtový náhodný reťazec generovaný s dostatočnou entrópiou v hex formáte
9. SIG - ECDSA podpis SHA256 hash-u textového reťazca vyskladaného z kľúča hodnoty, znaku =, hodnoty, oddelené znakom | (pipe, ascii 0x7C). Príklad PCO=xxx|GUID=yyy resp. GUID=yyy (ak nie je dostupné PČO). Poradie PCO, GUID, FN, LN, TSP, RID, OPID, NONCE. Ak hodnota nebola požadovaná (v REQ) alebo poskytnutá (RID), nie je súčasťou odpovede, ani podpisu. Na podpis je použitý privátny kľúč konkrétneho mID operátora (A3S podpis overuje verejným kľúčom konkrétneho operátora).

Celý reťazec pospájaný cez oddeľovač & (ampersand, ascii 0x26) je zašifrovaný symetrickým kľúčom tzv. shared secret odvodeným od centrálneho verejného kľúča mID ekosystému (spoločným pre všetkých mID operátorov) a privátneho kľúča A3S. Algoritmus AES/GCM/NoPadding, 12 bajtový náhodný IV (inicializačný vektor) je vložený na začiatok reťazca a takýto celok je prevedený do hexadecimálneho formátu. Zároveň, ak bol súčasťou požiadavky RID, je tento URL encodovaný pripojený za zašifrovaný reťazec znakom & a prefixom RID=.



|  |
| --- |
| **Zhrnutie zabezpečenia**   1. Ak A3S obsahuje aj back-end, požiadavka je šifrovaná na strane servera A3S symetrickým kľúčom tzv. shared secret odvodeným od centrálneho verejného kľúča mID ekosystému (spoločným pre všetkých mID operátorov) a privátneho kľúča A3S. Ak A3S nemá back-end, šifrovanie vykonáva aplikácia. 2. Dešifrovanie je možné iba za pomoci privátneho kľúča mID, ktorý je uložený na serveri mID (presnejšie - symetrickým kľúčom tzv. shared secret odvodeným od centrálneho privátneho kľúča mID ekosystému (spoločným pre všetkých mID operátorov) a verejného kľúča A3S). 3. Mobilné zariadenie nevie dešifrovať a získať obsah požiadavky 4. Odpoveď je podpísaná privátnym kľúčom mID na serveri mID 5. Podpis je možné overiť verejným kľúčom mID - zabezpečená autentickosť odpovede 6. Odpoveď je šifrovaná symetrickým kľúčom tzv. shared secret odvodeným od centrálneho privátneho kľúča mID ekosystému (spoločným pre všetkých mID operátorov) a verejného kľúča A3S). Odpoveď vie dešifrovať iba server A3S (alebo len aplikácia ak A3S nemá back-end) |

### Služba overenia identitných údajov

Poskytnytie údajov popísaných v kapitole 2.1.3 podlieha súhlasu dotknutej osoby s poskytnutím osobných údajov (GDPR) s výnimkou GUID.

Pokiaľ prevádzkovateľ A3S nechce takýto súhlas získavať, je možné pri autentifikácii získať iba GUID a následne využiť REST službu *verifyIdentityData(params)*, ktorú poskytuje mID operátor.

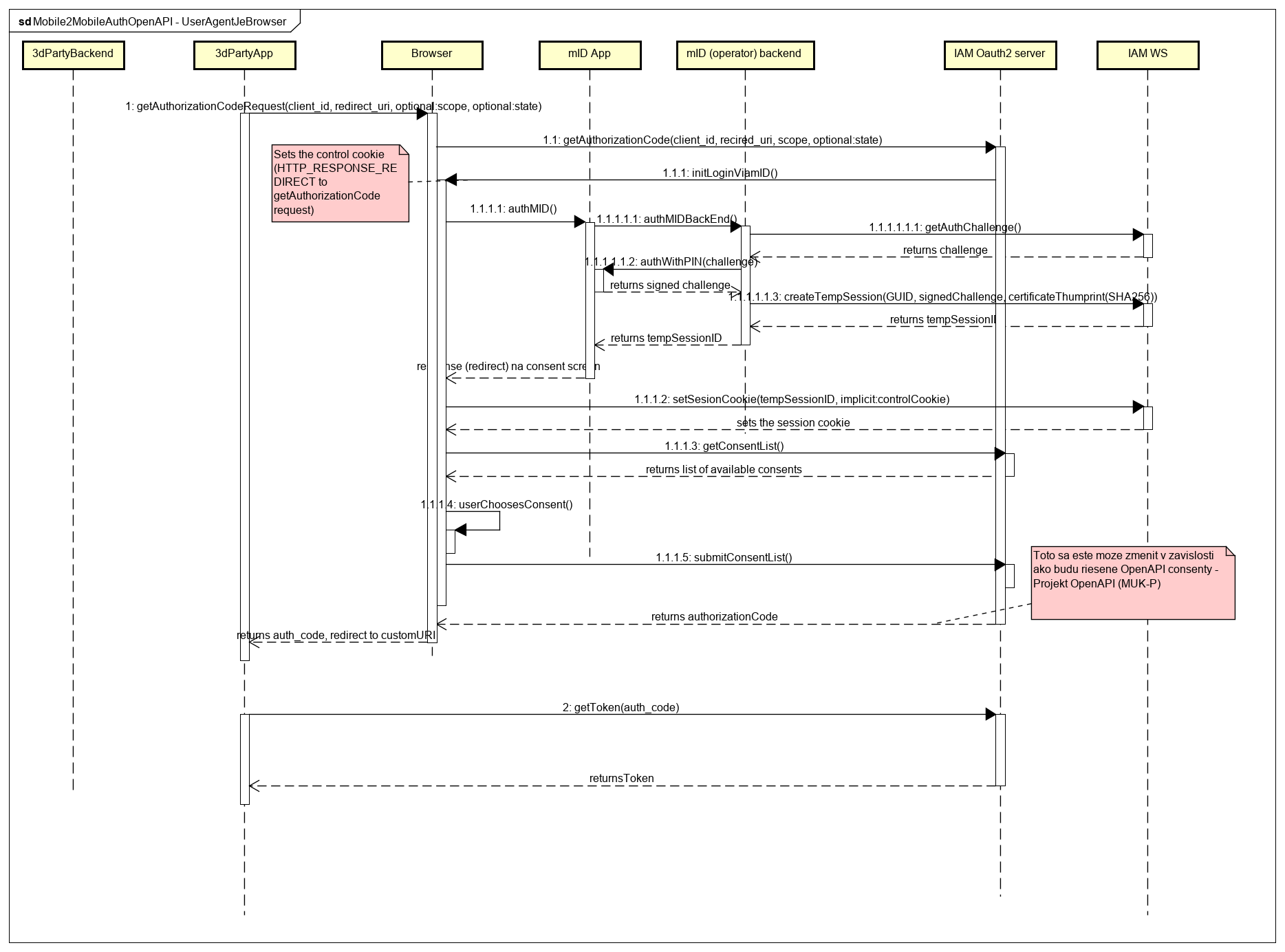
Vstupné parametre služby:

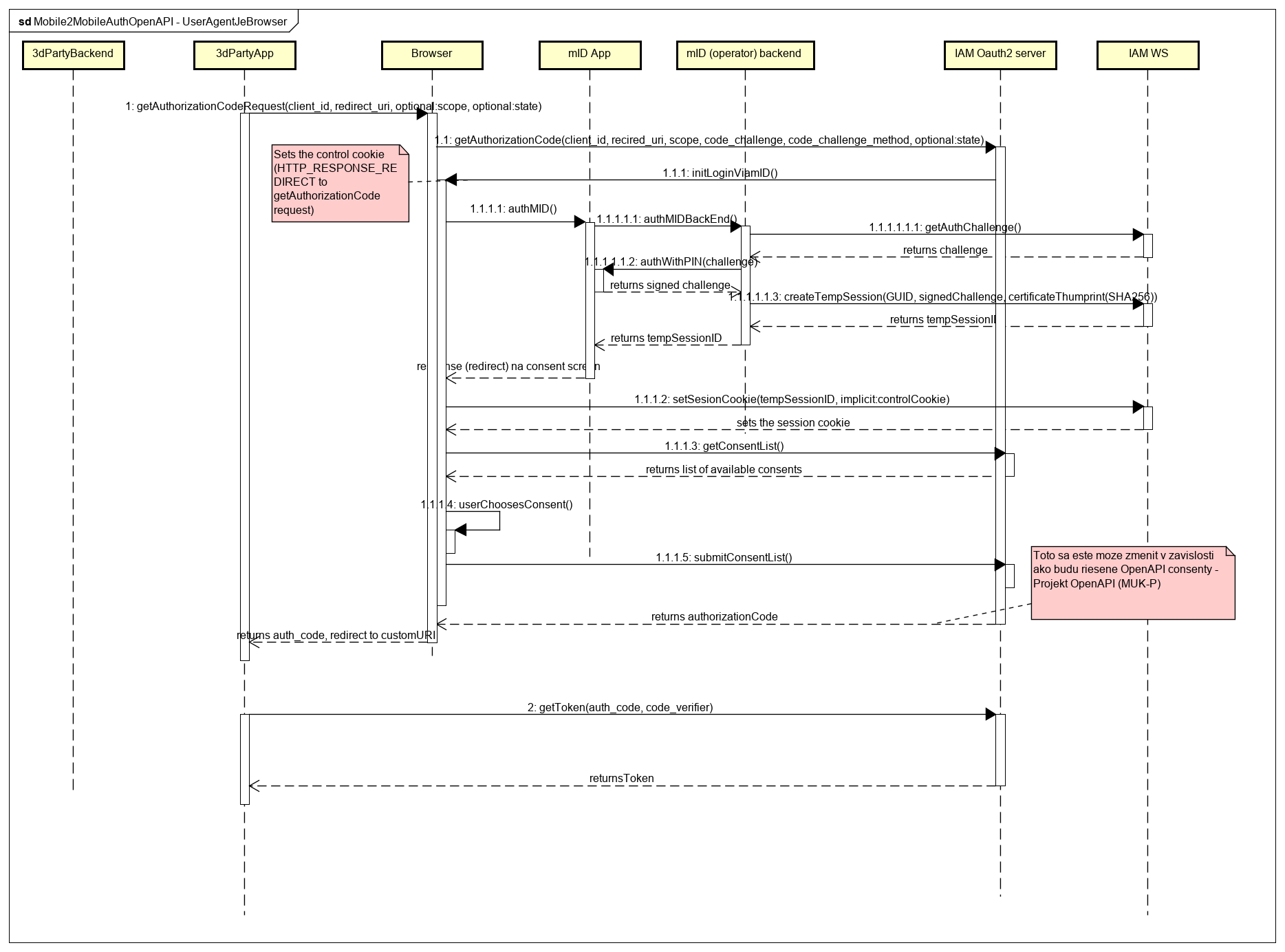
* Pole obsahujúce dvojice dataType a dataValue
  + *dataType* (string) - môže obsahovať hodnoty: FN, LN, PCO
  + *dataValue* (string) - hotnota, ktorá má byť porovnaná s hodnotou, ktorú pozná mID operátor
* *guid* (string) - GUID osoby, ktorej dáta majú byť porovnané

Výstupom je pole dvojíc datatype a boolean (match) parameterov. M*atch parameter*, nadobúda hodnoty *true/false*, podľa toho, či sa uvedený údaj zhoduje s údajom u mID operátora.

## Scenár prihlasovania, v ktorom ide aj o získanie autorizácie pre vyvolávania OpenAPI služieb

V tomto prípade sa jedná o  flow, definovaný v rámci protokolov OpenIDConnect a Ouath2.0 (tzv. authorization code grant: <https://tools.ietf.org/html/rfc6749#section-4.1>). Detailný popis bude predmetom detailnej analýzy v rámci fázy 1 a podľa možnosti hneď po detailnej analyse aj kryptoanalytikom skontrolovaný.





### Komunikácia A3S – user-agent (prehliadač)

1. A3S vyvolá URL (do prehliadača na danom zariadení), na ktorej IAM "počúva" na Oauth2 request.

### Proces po zavolaní user-agent-a (prehliadač)

1. IAM (cez user-agent-a/prehliadač) vyvolá autentifikáciu (login) pomocou mID aplikácie. V rámci tohto kroku nastaví v prehliadači kontrolnú cookie (obsahuje id dočasnej session (tempSessionID), použitie popísané v bode 5.).
2. mID aplikácia spustí v spolupráci so svojím back-endom autentifkáciu (detail môže byť špecifický pre každého operátora), back-end mID požiada IAM WS o challenge.
3. mID aplikácia autentifikuje používateľa (PINom, prípadne biometriou), výsledkom je mID app podpísaný challenge odoslaný na mID back-end.
4. mID back-end požiada IAM o vytvorenie tempSession (ako parameter posiela podpísaný challenge, identifikáciu používateľa – GUID a odtlačok certifikátu)
5. IAM vydá tempSessionID (na pozadí skontroluje certifikát a podpísaný challenge) a to prejde až do user-agent-a (prehliadač), pričom je opäť zavolané URL IAM-u (consent screen) – pričom sa nastaví sessionCookie (zoficiálni sa tak tempSession). Pri nastavení sessionCookie, musí user-agent kvôli bezpečnosti použiť tempSessionID aj controlCookie.
6. Používateľ zvolí v prehliadači consent
7. User-agent (prehliadač) požiada o vydanie autorizačného kódu, na základe sessionID, consent-u

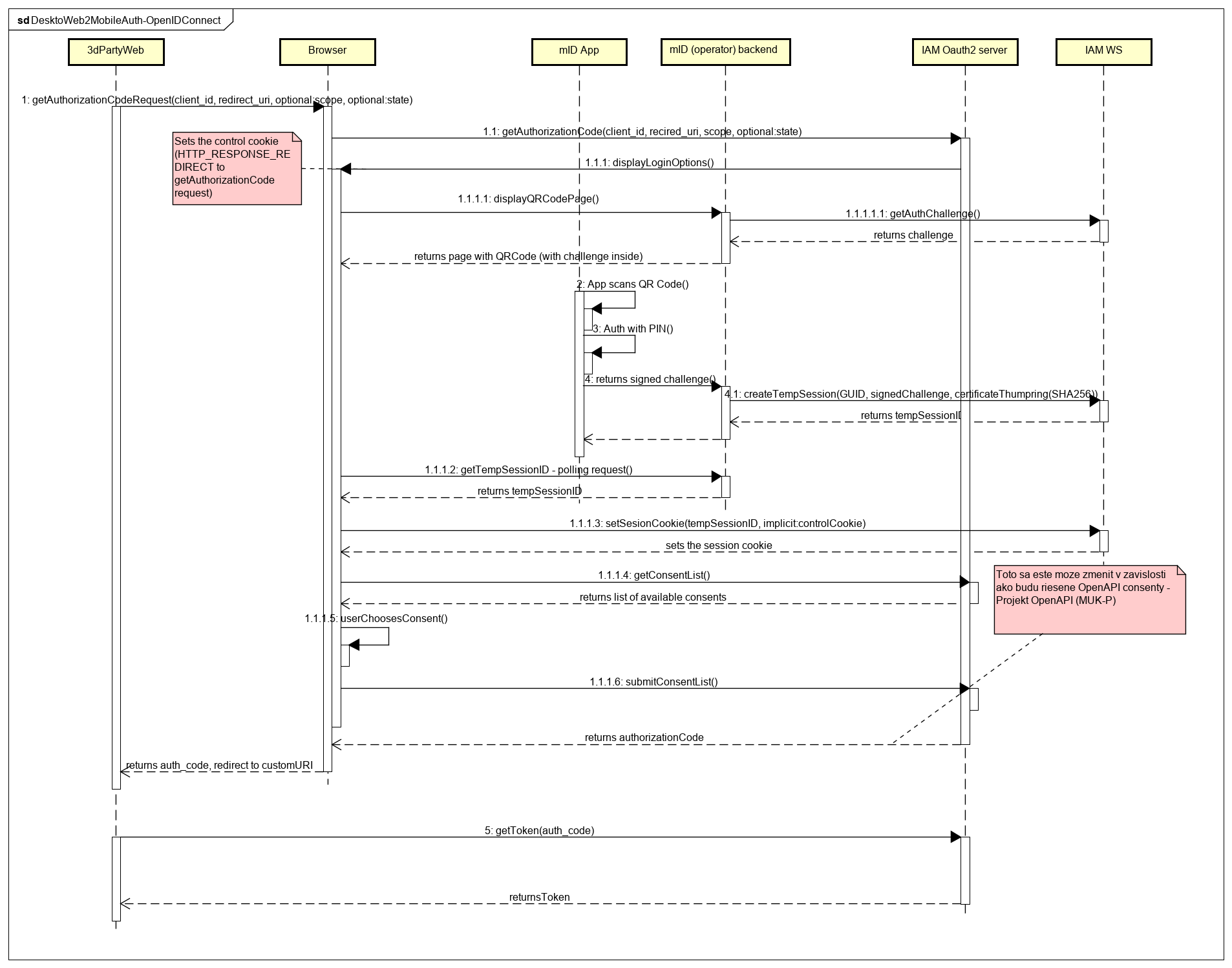
### Komunikácia user-agent (prehliadač) – A3S

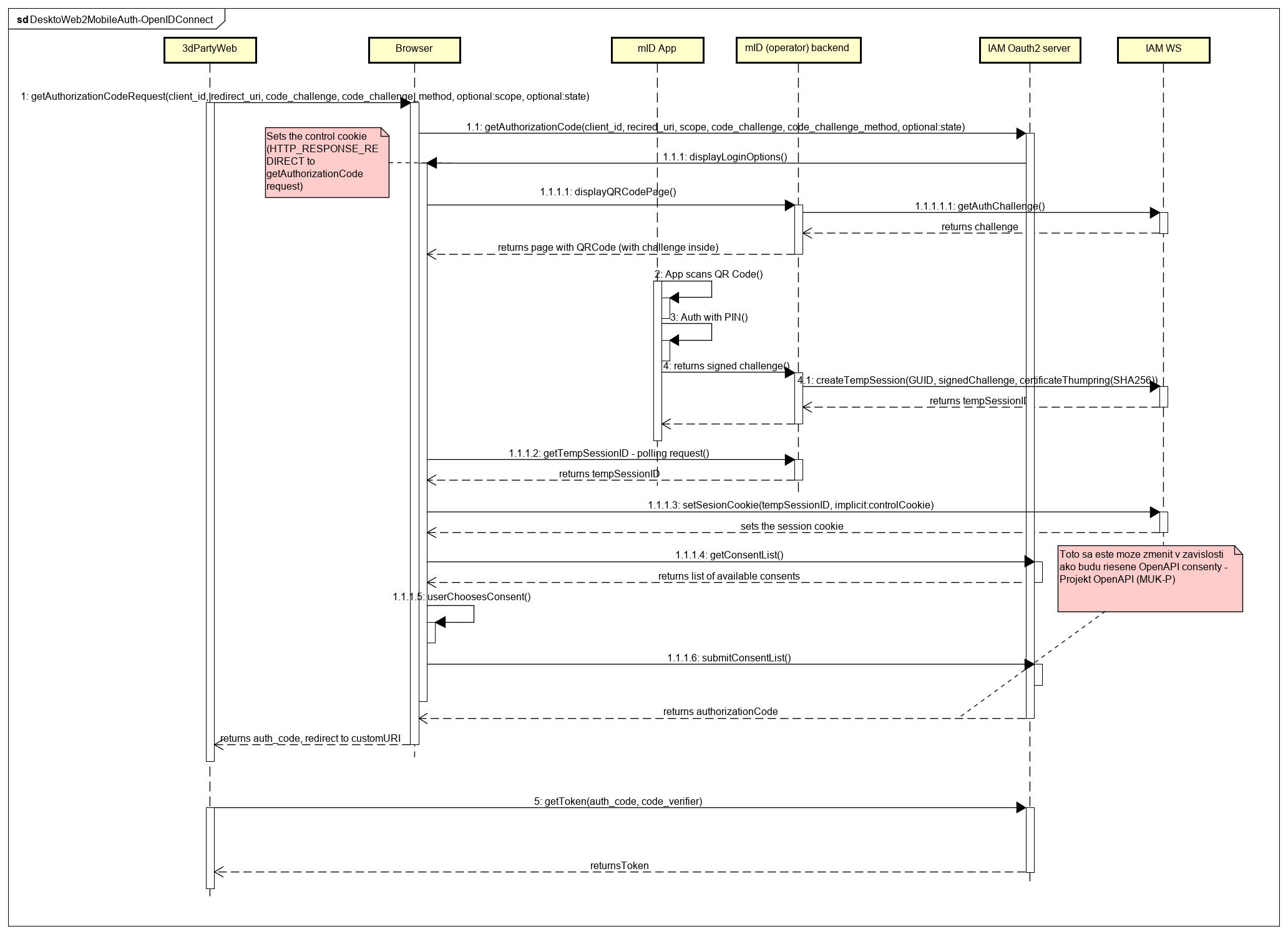
1. Autorizačný kód odovzdáva user-agent (prehliadač) aplikácii tretej strany volaním URL, ktorú dostal v parametri redirect\_uri.
2. Aplikácia je následne zodpovedná za priame vyzdvihnutie autorizačného tokenu pomocou autorizačného kódu.

# Scenár: Prihlasovanie desktop2mobile.

V tomto scenári **web** tretej strany (je jedno či web OVM poskytujúci služby danej agendy, alebo web komerčného subjektu) využije služby prihlásenia mID pomocou **mobilnej** aplikácie jedného zo štátnych operátorov (DEUS, alebo NASES). Web danej organizácie môže byť využívaný aj na inom zariadení, než je nainštalovaná mID aplikácia jedného z operátorov.

Pri prihlasovaní desktop2mobile nemá zmysel členiť scenáre na „len využívanie mobilnej identity“ a na „prihlásenie s cieľom získať autorizáciu v ekosystéme OpenAPI“, pretože web tretej strany interaguje priamo s IAM-om (resp. jeho časťou – autorizačným serverom).Opäť sa tak jedná o štandardizovaný flow, definovaný v rámci protokolov OpenIDConnect a Oauth2.0 (tzv. authorization code grant: <https://tools.ietf.org/html/rfc6749#section-4.1>)





### Komunikácia web tretej strany – user-agent (prehliadač)

1. Web tretej strany vyvolá URL (prehliadač daného desktopu), an ktorej IAM "počúva" na Oauth2 request.

### Proces po zavolaní prehliadača

1. IAM (cez user-agent-a/prehliadač) ponúkne zoznam podporovaných mID operátorov, pomocou ktorých je možné vykonať autentifikáciu. V rámci tohto kroku nastaví v prehliadači kontrolnú cookie.
2. Používateľ si v prehliadači zvolí, s ktorým operátorom prebehne prihlásenie. Je presmerovaný na back-end daného operátora.
3. Back-end mID operátora požiada IAM WS o challenge a zobrazí QR kód.
4. Používateľ pomocou mID aplikácie načíta QR kód a autentifikuje sa (PINom, prípadne biometriou), výsledkom je podpísaný challenge na mID back-ende.
5. mID back-end požiada IAM o vytvorenie tempSession (ako parameter posiela podpísaný challenge, identifikáciu používateľa – GUID a odtlačok certifikátu)
6. IAM vydá tempSessionID (na pozadí skontroluje certifikát a podpísaný challenge) a tá prejde na mID back-end, odkiaľ si ju web back-endu (na ktorom je prehliadač používateľa) cez polling request vyzdvihne.
7. Prehliadač je presmerovaný na URL IAM-u (consent screen) – pričom sa nastaví sessionCookie (zoficiálni sa tak tempSession). Pri nastavení sessionCookie, musí user-agent kvôli bezpečnosti použiť tempSessionID aj controlCookie.
8. Používateľ zvolí v prehliadači consent
9. User-agent (prehliadač) požiada o vydanie autorizačného kódu, na základe sessionID, consent-u

### Komunikácia user-agent (prehliadač) – A3S

1. Autorizačný kód odovzdáva user-agent (prehliadač) aplikácii tretej strany volaním URL, ktorú dostal v parametri redirect\_uri.
2. Aplikácia je následne zodpovedná za priame vyzdvihnutie autorizačného tokenu pomocou autorizačného kódu.

# Scenár: Podpisovanie v eGov z centrálnej komponenty ÚPVS (CPK).

V tomto scenári **web, prípadne mobilná aplikácia** OVM využije služby centrálneho podpisového komponentu ÚPVS pre autorizáciu klikom (**tzv. CPK – centrálny podpisovací komponent**). CPK zrealizuje autorizáciu klikom nasledovným spôsobom:

Elektronický dokument, ktorý je predmetom autorizácie CPK opečatí spoločne s elektronickou autentifikačnou doložkou kvalifikovaným certifikátom elektronickou pečate NASES (prípadne ÚPVII). Autentifikačnú doložku CPK vytvorí vyplním elektronického formulára údajmi o identite, ktorej identifikátor získa z opakovanej autentifikácie (prihlasovací token). Opakovanú autentifikáciu realizuje napríklad prostredníctvom mID ale aj eID kartou. Za týmto účelom sa v kontexte tohto dokumentu rozumie:

• Elektronickým dokumentom: vyplnený elektronický formulár (typicky podanie) alebo súbory v takom formáte, ktorých podpisovanie je podporované službami CEP

Autentifkačnou doložkou: elektronický formulár vyplnený údajmi o identite, ktorá bola pri autorizácii klikom autentifikovaná. Elektronický formulár autentifikačnej doložky bude registrovaný v module eForm

CPK teda v rámci autorizácie klikom vždy vyvolá opakované prihlásenie používateľa. Konkrétny spôsob prihlásenia, ktorý CPK poskytne, bude závislý od toho, akým prostriedkom bol používateľ prihlásený pri prechode z A3Smobilnej resp webovej aplikácie OVM do CPK (za predpokladu zafungovania SSO pre oauth2 resp. saml2) Ak túto možnosť nebude možné použiť, tak typ autentifikácie zvolí používateľ. Voľbu realizuje na prihlasovacej obrazovke IAM, ktorá sa zobrazí vo webovom prehliadači (responzíva webová stránka). Na tento účel podľa vyššie uvedených podmienok bude teda možné prihlásenie vykonať aj cez službu jedného, alebo druhého operátora mID bez toho že by bol ktorýkoľvek z nich uprednostnený.

Súčasťou služby autorizácie klikom v CPK je aj vizualizácia podpisovaného elektronického formulára (typicky podania) používateľovi aplikovaním podpisovej transformácie. Vizualizácia iného elektronického dokumentu bude realizovaná nasledovne: Zobrazený bude iba názov súboru s možnosťou stiahnutia. S obsahom dokumentu sa môže používateľ oboznámiť tak, že si elektronický dokument stiahne a vizualizuje jeho obsah v asociovanej aplikácii v závislosti od formátu dokumentu.

Overenie autorizácie klikom tak ako je navrhnuté bude možné realizovať štandardnými prostriedkami a službami CEP, pričom integrácia na vybrané overovanie služby CEP je už v súčasnosti umožnená aj komerčnému sektoru.

Súčasťou služby autorizácie CPK nie je v tejto fáze vyhotovenie elektronického podpisu použitím certifikátu uloženého v mobilnom zariadení. Takýto podpis totiž nemá oporu v eGov zákone, jeho použitie v autorizácii klikom eGov zákon nevyžaduje. Za predpokladu, že by pre jeho vytvorenie nebol použitý kvalifikovaný certifikát, tak na overenie takéhoto podpisu nie je navyše možné použiť štandardné prostriedky podateľne a v neposlednej miere ani neprispieva k zvýšeniu dôveryhodnosti autorizácie klikom.

### Komunikácia CPK → mID

Komunikácia CPK na mID prebieha za účelom vykonania opakovanej autentifikácie, ktorá bude realizovaná principiálne obdobným scenárom ako je popísaný v scenári 4: Prihlasovanie desktop2mobile. Súčasťou komunikácie bude však navyše sada údajov, týkajúcich sa podpisovaného obsahu (napr. SHA256 autorizovaného dokumentu, transactionID a pod.) posielaná z CPK cez IAM smerom dole do metódy prihlásenia. Tým má byť zabezpečené to, aby používateľ pracujúci v mID mal možnosť skontrolovať (zobrazením sady údajov), že opakovaným prihlásením v mID realizuje autorizáciu toho obsahu, nad ktorým v CPK inicioval podpis klikom.

Neskôr vo fáze 2., bude navyše možné túto komunikáciu doplniť o reťazec obsahujúci podpis, ktorý po prihlásení používateľa zašle mID do IAM a aby sa tak tento reťazec mohol stať súčasťou autorizačnej doložky. Formulár autorizačnej doložky bude už vo fáze 1 obsahovať nepovinné pole, kde bude možné tento reťazec uviesť. Inicializácia dodatočnej autentifikácie z CPK prostredníctvom tejto komunikácie teda prebieha za účelom získania údajov pre vytvorenie autorizačnej doložky v CPK pri podpisovaní klikom.

### Komunikácia web/mobilná aplikácia OVM -> CPK

Komunikácia prebehne cez sadu webových služieb, ktorých poskytovateľom je CPK a ktoré budú zverejnené na MUK-P. Prístup k službe bude zabezpečený cez IAM token. Táto sada rozhraní umožní:

* Štart session
* Nahratie dokumentov k  autorizácii
* Spustenie autorizácie
* Prevzatie autorizovaných dokumentov (výsledok autorizácie)

Konečná špecifikácia jednotlivých rozhraní nie je predmetom tohto dokumentu, bude upresnená v rámci detailnej analýzy.