Mesto Košice

Príloha č.1

Konto Košičana (KK) - Profil Košičana (PK)

Autentifikácia

|  |  |
| --- | --- |
| Zmluva |  |
| Verzia dokumentu | 0.4 |
| Autor dokumentu | Peter Stavný |
| Vlastník dokumentu | Mesto Košice |
| Dátum vydania |  |

Denník zmien:

| Verzia | Dátum | Revidoval | Popis | Označenie zmien |
| --- | --- | --- | --- | --- |
| 0.1 | 19.01.2024 | Peter Stavný | Iniciálna verzia dokumentu | Bez revízie |
| 0.2 | 21.01.2024 | Peter Stavný | Registrácia pošta, pridané KID | Bez revízie |
| 0.3 | 06.01.2024 | Peter Stavný | Prepracovanie dokumentu - zmena migrácie dát. Prepracované registrácie. Pridanie registračných, prihlasovacích scenárov použitia. Scenár pre zabudnutého hesla. Nové diagramy a ich popis. | Bez revízie |
| 0.3 | 19.01.2024 | Peter Stavný | Zmena LCS Norris middleware na KKProfile, doplnenie diagramu toku access tokenov | Bez revízie |
| 0.4 | 19.04.2024 | Peter Stavný | Zmenili sme aj path pre endpoint - PUT /v1/kk/ad/profiles na /v1/kk/ad/profiles/activate, len formálne, nie obsahovo. Nový endpoint /v1/kk/ad/profiles/code  pre validáciu aktivačného kódu v prvom kroku registrácie Konta Košičana. | Bez revízie |
| 0.5 | 29.04.2024 | Peter Stavný | Úprava názvov custom claimov v JWT tokenoch podľa Azure B2C špecifikácie, pridanie custom claimu extension\_role, úprava zmena hesla procesu | Bez revízie |
| 0.6 | 23.06.2025 | Peter Stavný | UCR3 - Registrácia pomocou eID a mID | Bez revízie |

Obsah

[1 Slovník pojmov 3](#_Toc201600686)

[2 Zoznam obrázkov 3](#_Toc201600687)

[3 Zoznam tabuliek 3](#_Toc201600688)

[4 Návrh riešenia 4](#_Toc201600689)

[*4.1* Biznisové služby modulu *Autentifikácie* 4](#_Toc201600690)

[4.2 Aktivačný (registračný) kód 5](#_Toc201600691)

[4.3 Jedinečný identifikátor KK - extension\_kid 5](#_Toc201600692)

[4.4 Úroveň registrácie – extension\_qaa 5](#_Toc201600693)

[4.5 Kategória občana - extension\_category 6](#_Toc201600694)

[4.6 Role v systéme KK - extension\_role 6](#_Toc201600695)

[4.7 AD claims 7](#_Toc201600696)

[4.8 OAuth2 a OIDC 8](#_Toc201600697)

[4.8.1 Access-Refresh JWT token 8](#_Toc201600698)

[4.9 Biznis architektúra 10](#_Toc201600699)

[4.9.1 Biznis architektúra autentifikácie (TO-BE) 10](#_Toc201600700)

[4.10 Aplikačná architektúra 11](#_Toc201600701)

[4.10.1 Aplikačná architektúra autentifikácie (AS-IS Fáza 1) 11](#_Toc201600702)

[4.10.2 Aplikačná architektúra autentifikácie (AS-IS Fáza 2) 12](#_Toc201600703)

[4.11 Technologická architektúra 16](#_Toc201600704)

[4.11.1 Technologická architektúra autentifikácie (AS-IS Fáza 1) 16](#_Toc201600705)

[4.11.2 Technologická architektúra autentifikácie (AS-IS Fáza 2) 17](#_Toc201600706)

[4.12 Biznisové služby a procesy KK (E2E) 17](#_Toc201600707)

[4.12.1 UCR1 – Registrácia pomocou pošty mesta Košíc - email, heslo 17](#_Toc201600708)

[4.12.2 UCR2 - Registrácia pomocou občianskeho preukazu na kontaktnom mieste mesta Košíc 19](#_Toc201600709)

[4.12.3 UCR3 - Registrácia pomocou eID a mID 20](#_Toc201600710)

[4.12.4 UCR4 - Registrácia federáciou s externými identity providerami 23](#_Toc201600711)

[4.12.5 UCR5 - Registrácia pomocou mena a hesla bez aktivačného kódu 23](#_Toc201600712)

[4.12.6 UCA1 - Prihlasovanie pomocou email-hesla 24](#_Toc201600713)

[4.12.7 UCA2 - Prihlasovanie pomocou mID a eID (trust) 25](#_Toc201600714)

[4.12.8 UCA3 - Prihlasovanie pomocou pin-u a biometrie v mobilnej aplikácii Konta Košičana 25](#_Toc201600715)

[4.12.9 UCH1 - Zabudnuté heslo 26](#_Toc201600716)

[4.12.10 UCD1 - Deaktivácia Konta Košičana občanom 27](#_Toc201600717)

[4.12.11 UCD2 – Deaktivácia Konta Košičana administrátorom 27](#_Toc201600718)

[5 Skratky a značky 28](#_Toc201600719)

# Slovník pojmov

|  |  |
| --- | --- |
| Pojem | Vysvetlenie |
| Autentifikácia | Proces identifikácie a overenia identity v informačnom systéme. |
| Autorizácia | Tento dokument nepoužíva variácie slova autorizácia vo význame eGov, teda najmä v spojení s autorizovaním úkonov (napr. podpisovanie).  V rámci dokumentu je využívaný v zmysle "riadenia prístupu k službe" informačného systému. |
| Validácia | Overovanie a kontrola špecifikácie na základe preddefinovaných parametrov |
| Registrácia | Proces vytvorenia identity v informačnom systéme. |

# Zoznam obrázkov

[Obrázok 1 Biznis architektúra autentifikácie 9](#_Toc159250362)

[Obrázok 2 Aplikačná architektúra autentifikácie AS-IS 10](#_Toc159250363)

[Obrázok 3 Aplikačná architektúra autentifikácie TO-BE 11](#_Toc159250364)

[Obrázok 4 Toky tokenov v architektúre – Person to System 14](#_Toc159250365)

# Zoznam tabuliek

[Tabuľka 1 AD claims 7](#_Toc159250366)

# Návrh riešenia

Z výsledkov analýzy súčasného stavu vyplýva že, mesto nerealizuje na väčšine portálov formu jednotnú **autentifikáciu**, čo aj vyplýva z ich súčasnej funkcionalít. Samozrejme v portáli *eSlužby mesta Košíc* používajú eID, mID a v mobilnej aplikácii *Zimná údržba* email - heslo. Ani jedna z autentizácii nie je plne v správe mesta Košíc.

Návrh preto odporúča vytvorenie jednotného autentizačného modulu v správe mesta Košíc a to pomocou emailu a hesla. Autentizácia občanov bude následne po je zavedení, slúžiť pre autorizáciu a identifikáciu občanov voči službám mesta Košíc.

Pri preberaní možnosti autentifikačných servisov sme sa zamerali na nasledujúce požiadavky:

* Mesto Košice je výlučným vlastníctva osobných dát občanov mesta Košíc,
* Servis by mal poskytovať aj autentifikáciu a manažment aplikácií (mobilných, webových, backendových príp. natívnych) poisťujúcich k autentifikačnému prostriedku
* Servis by mal poskytovať federáciu s inými identity providerami (Google, Facebook, OIDC, atď.)
* Pre poskytnutie autentifikácie väčšine platforiem by mal poskytovať OAuth2 autentifikáciu a JWT tokeny (OIDC – OpenID Connect).
* Servis by mal poskytnúť jednoduchú administráciu a konfiguráciu pre DEVOPS tímy
* Samozrejme musí podporiť bonusové procesy Konta Košičana pre potreby registrácie a autorizácie.
* Mitigácia možného vendor locku.

S ohľadom na horeuvedené požiadavky sa zvažovali cloudové aj on-premise riešenia ako sú Keylock, IdentityServer4 a Microsoft Entra.

Pre toto riešenie bolo predbežne zvolené cloudové Azure riešenie of Microsoftu - **Microsoft Entra - Enternal ID** (<https://learn.microsoft.com/en-us/entra/external-id/customers/overview-customers-ciam>) resp. **Azure Active Directory B2C** <https://learn.microsoft.com/en-gb/azure/active-directory-b2c/> (ďalej AD).   
   
Nasledujúce procesy, integrácie a realizácia je popisovaná z ohľadom na zvolený produkt.

## Biznisové služby modulu *Autentifikácie*

Biznisové a aplikačné servisy *Autentifikácie* zahŕňajú nasledujúcu funkcionalitu a služby:

* Registráciu občana
  + UCR1 - Registrácia pomocou pošty mesta Košíc
  + UCR2 - Registrácia pomocou občianskeho preukazu na kontaktnom mieste mesta Košíc
  + UCR3 - Registrácia pomocou eID a mID
  + UCR4 - Registrácia federáciou s externými identity providerami
  + UCR5 - Registrácia pomocou emailu a hesla bez aktivačného kódu
* Autentifikácia a autorizácia občana
  + UCA1 - Prihlasovanie pomocou email-hesla
  + UCA2 - Prihlasovanie pomocou mID a eID (trust)
  + UCA3 - Prihlasovanie pomocou pin-u a biometrie v mobilnej aplikácii Konta Košičana
* Manažment hesiel
  + UCH1 - Zabudnuté heslo
* Deaktiváciu účtu
  + UCD1 – Deaktivácia Konta Košičana občanom
  + UCD2 – Deaktivácia Konta Košičana administrátorom

Z pohľadu dát doménového udržiavania dát občana Košíc budú v identity providerovi udržiavane len dáta nevyhnutné pre registráciu a generovanie JWT tokenov. Všetky ostatné personálne dáta občana Košíc (Profil) bude bezpečne uložené a manažované v backoffice servisoch LCS Norris.

## Aktivačný (registračný) kód

Ide o registračný aktivačný kód vygenerovaný v procese vytvárania platobných výmerov za miestne dane a poplatky alebo v procese registrácie pomocou kancelárie prvého kontaktu v backoffice systéme LCS Norris pre registrovaných občanov mesta Košíc.

*Pravidlá pre aktivačný kód:*

* Jedinečný 9 miestny alfanumerický string
* Kód má platnosť 6 mesiace
* Kód s minimom osobných dát (meno, priezvisko, rodne číslo) je možné overiť s prostredníctvom REST API

## Jedinečný identifikátor KK - extension\_kid

Ide o jedinečný identifikátor konta Košičana – **extension\_kid** - naprieč ekosystému Košíc vygenerovaný v systéme LCS Norris. Samotný identifikátor je aj súčasťou prístupových tokenov vydávaných identity providerom v Azure AD B2C.

*Pravidlá pre identifikátor extension\_kid:*

* Jedinečný per identitu občana. Ani deaktivácia konta tento identifikátor nezneplatňuje.
* Formát je UUID, canonical textual representation, [RFC 4122](https://datatracker.ietf.org/doc/html/rfc4122) (príklad "55B87557-B5AF-4823-B82B-6695B181C56E"),
* Týmto identifikátormi budú previazané všetky osobné dáta a dáta občana v databázach LCS Norris ako aj v databázach aplikácii ďalších systémov vyvíjaných pre mesto Košice.

## Úroveň registrácie – extension\_qaa

Atribút vyjadruje úroveň registrácie podľa eIDAS 2. Ide o string enumerátor s nasledovnými hodnotami:

|  |  |  |  |
| --- | --- | --- | --- |
| Číslo | Hodnota | Popis |  |
| 1. | low | Úroveň nízka. | Registračný user flow pre proces:   * Registrácia pomocou emailu a hesla bez aktivačného kódu * Registrácia federáciou s externými identity providerami |
| 2. | substantial | Úroveň stredná. | Registračný user flow pre proces: |
| 3. | high | Úroveň vysoká. | Registračný user flow pre proces:   * Registrácia pomocou pošty mesta Košíc s aktivačným kódom * Registrácia pomocou občianskeho preukazu na kontaktnom mieste mesta Košíc s aktivačným kódom * Registrácia pomocou eID a mID |

## Kategória občana - extension\_category

Kategorizácia je bližšie rozobraná v analýze hlavného dokumentu DNR v sekcii [Koncept návrhu Konta Košičana.](MK-KKaKES-DNR-02.docx)

|  |  |  |  |
| --- | --- | --- | --- |
| Číslo | Hodnota | Popis |  |
| 1. | **honorable** | Čestný občan mesta Košíc | ToDo. |
| 2. | **certified** | Certifikovaný košican | Registračný user flow pre proces:   * Registrácia pomocou pošty mesta Košíc s aktivačným kódom |
| 3. | **citizen** | Košican | Registračný user flow pre proces:   * Registrácia pomocou občianskeho preukazu na kontaktnom mieste mesta Košíc s aktivačným kódom * Registrácia pomocou eID a mID |
| 4. | **fellow** | Spolukošičan | Registračný user flow pre proces:   * Registrácia pomocou občianskeho preukazu na kontaktnom mieste mesta Košíc s aktivačným kódom |
| 5. | **visitor** | Návštevník | Registračný user flow pre proces:   * Registrácia bez aktivačného kódu |

## Role v systéme KK - extension\_role

|  |  |  |  |
| --- | --- | --- | --- |
| Číslo | Hodnota | Popis |  |
| 1. | **obcan** | Registrovaný občan | Registrovaný občan do aplikácii Konta Košičana (Defaultna hodnota pre scenár autentifikácie a autorizácie občana) |
| 2. | **admin** | Registrovaný administrátor | Registrovaný administrátor v systéme Konta Košičana |
| 3. | **system** | Registrovaná aplikácia | Registrovaná aplikácia v systéme Konta Košičana |

## AD claims

Pre registračné účely nutné rozšíriť default sadu atribútov – claims v AD. Pôjde o atribúty **extension\_kid, extension\_pin, extension\_pco, extension\_qaa, extension\_privacyAgreement**. Pre potrebu doplnenia claimov zrealizuje nová Azure App servisa realizujúca aj vlastný sign-in a sign-up user flow.

Zatiaľ čo pin, givenName, surname a extension\_privacyAgreement sa vyplní v priebehu registrácie, **extension\_kid** a **extension\_pco** sa vyplní pomocou API konektorov po úspešnej registrácii pri validácii zo systému LCS Norris. Taktiež **extension\_qaa** sa nastaví podľa typu user flowu (custom polices).

|  |  |  |  |
| --- | --- | --- | --- |
| Názov stĺpca | Typ | Dostupnosť | Popis |
| extension\_kid | String | Povinný | **(Custom claim)** UUID, canonical textual representation, [RFC 4122](https://datatracker.ietf.org/doc/html/rfc4122), Jedinečný identifikátor konta Košičana, vygenerovaného v systéme LCS Norris. Ex.: "55B87557-B5AF-4823-B82B-6695B181C56E" |
| givenName | String | Povinný | Meno používateľa |
| surname | String | Povinný | Priezvisko |
| extension\_pin | String | Povinný | **(Custom claim)** Rodné číslo občana bez rozdeľovača, pr.:7510290001 |
| extension\_pco | String | Nepovinný (len ak existuje) | **(Custom claim)** Počítačové číslo osoby v systémoch ÚPVS z RFO MV SR, ex.: pco:// 7510290001, *na RegExp: ^pco:\/\/[0-9]{1,}$* |
| extension\_qaa | String | Povinný | **(Custom claim)** Úroveň zabezpečenia registrácie podľa eIDAS2 (nízka, stredná a vysoká) [low, substantial, high], pr.: " substantial" |
| email | String | Povinný | Email používateľa |
| mobilePhone | String | Nepovinný (len ak existuje) | Telefónne číslo občana evidované v systéme LCS Norris, ak existuje |
| extension\_privacyAgreement | Boolen | Povinný | **(Custom claim)** Súhlas používateľa som spracovaním, ochranou osobných údajov a ich zásad (privacy and policy) a dátovou politikou (data policy). |
| extension\_Code | String | Povinný (len pre registračnú fázu) | **(Custom claim)** Registračný aktivačný kód vygenerovaný v procese vytvárania platobných výmerov za miestne dane a poplatky alebo v procese registrácie pomocou kancelárie prvého kontaktu v backoffice systéme LCS Norris pre registrovaných občanov mesta Košíc. Pr.: "123456789" |
| extension\_category | String |  | **(Custom claim)** Kategória občana Pr.: "citizen" |
| extension\_role | String |  | **(Custom claim)** Role z pohľadu žiadateľa o autentifikáciu pr.: " občan" |

Tabuľka 1 AD claims

## OAuth2 a OIDC

Bude predmetom v ďalších verziách návrhu

Pre potreby autentifikácie KK je vybraní **OpenID Connect** server s **OAuth2** protokolom, ktorý bude v **Azure AD B2C** nakonfigurovaný ako hlavný identity provider pre všetky integrované aplikácie (<https://learn.microsoft.com/en-us/azure/active-directory-b2c/protocols-overview>, <https://learn.microsoft.com/en-us/azure/active-directory-b2c/openid-connect>, ). Autentifikácia využije **Authorization Code grant flow** (<https://learn.microsoft.com/en-us/azure/active-directory-b2c/authorization-code-flow>)

Koncept autorizačného prostriedku pomocou JWT tokenov nenahrádza súčasnú autorizáciu pomocou **WebSSO** SAML tokenov. WebSSO SAML sa bude aj naďalej na portáloch používať a bude používané paralelne popri JWT a teda platnosť oboch sa bude udržiavať oddelene od seba.

Týmto prístupom môže starší systém aj ďalej využívať WebSSO sliding sesson tak ako doteraz a žiadať o JWT Access token pomocou WebSSO tokenu.

### Access-Refresh JWT token

Access a refresh JWT tokeny, ktoré budú vydávane po úspešnej autentifikácii občanom, plne rešpektujú nastavenia a platnosti nastavení AD B2C Identity providera podľa špecifikácie uvedenej v dokumentácii (<https://learn.microsoft.com/en-us/azure/active-directory-b2c/tokens-overview#token-types>).

Je však nutné pridať nové atribúty do payload sekcie JWT tokenu, ktoré boli vyzbierané v priebehu registrácie a to **extension\_kid, extension\_qaa, extension\_pco, extension\_role** a **extension\_category.**

Príklad:

{

"typ": "JWT",

"alg": "RS256",

"kid": "5B3nRxtQ7ji8eNDc3Fy05Kf97ZE"

}.{

"aud": "f26f3070-593b-480c-a9bb-32ab3b98edaf",

"iss": "https://098be6b4-0eb7-46df-81a0-550d3e7804e3.ciamlogin.com/098be6b4-0eb7-46df-81a0-550d3e7804e3/v2.0",

"iat": 1706017855,

"nbf": 1706017855,

"exp": 1706021755,

"aio": "ATQAy/8VAAAANNPYhJidPM9ymHDwRWswJ3E5VTVZbaGkr2ZigZZzE8+21OJrOR3RvIOotrDMCTxS",

"nonce": "defaultNonce",

"rh": "0.AZgAtOaLCbcO30aBoFUNPngE43Awb\_I7WQxIqbsyqzuY7a-YALI.",

"sub": "mIHGcNfZa--nXXqOfXso8nUmeLIl6JzbYUtFXX1LoMI",

"tid": "098be6b4-0eb7-46df-81a0-550d3e7804e3",

"uti": "U59JcR3rS0Gon\_vgcUsAAA",

"ver": "2.0",

**"extension\_kid": "098be6b4-0eb7-46df-81a0-550d3e7804e3",**

**"extension\_qaa": "high",**

**"extension\_category": "citizen",**

**"extension\_role": "obcan",**

**"extension\_pco": "pco://7510290001"**

}.[Signature]

## Biznis architektúra

Návrh uvažuje s vytvorením služieb pre používateľov, ktorých poskytovanie bude podporené sústavou biznis procesov. Dôležitá je natívna integrovateľnosť vytvorených komponentov a opakovaná použiteľnosť kódov alebo stavebných prvkov.

### Biznis architektúra autentifikácie (TO-BE)



Obrázok 1 Biznis architektúra autentifikácie

## Aplikačná architektúra

### Aplikačná architektúra autentifikácie (AS-IS Fáza 1)



Obrázok 2 Aplikačná architektúra autentifikácie AS-IS

V súčasnosti je autentifikačný proces reprezentovaný na web portály eSlužby Košice jednotným prihlasovaním pomocou WebSSO pre prístup k službám eGov. Ide tu prihlasovanie sa pomocou eID, mID a eIDAS. Autentifikačný protokol je SAML2. WebSSO nesie informácie o autentifikovanej osobe (subjekte) a v prípade právnickej osoby, OVM resp. SZCO aj informácie o organizácii v ktorej zastúpení bola prihlásená osoba.

Údaje slúžia k predvypneniu údajov vo formulároch, token k prístupu k službám ÚPVS a autorizácii formulárov (podpisovaniu).

Registračný proces v tomto prípade nie je nutný nakoľko prihlasovanie prebieha pomocou eID (očianskeho preukazu s čipom) alebo pomocou autentifikačnej aplikácie mID (Slovensko v mobile).

Hlavné komponenty aplikačnej architektúry pre procesy autentifikácie sú **IAM ÚPVS** s jeho prihlasovacou stránkou a **portál eSlužieb Košice**.

### Aplikačná architektúra autentifikácie (AS-IS Fáza 2)



Obrázok 3 Aplikačná architektúra autentifikácie TO-BE

Hlavný komponent aplikačnej architektúry pre profile Košičana je **KKProfile servis** s REST API rozhraním a **LCS Norris**, Portál **eSlužieb Košice** sa rozširujúci sa o **Osobnú zónu** konta Košičana, **Aure Entra** –**Azure AD B2C** so web app servisom **KKUFW** v Azure Cloude a mobilná aplikácia **Konto Košičana**.

|  |  |
| --- | --- |
| **KKProfile servis** | Servis má za úlohu:   * Sprostredkovať konsolidované osobné dáta o občanoch Košíc, ktoré mesto eviduje v systéme LCS Norris a Helios. * Konsolidovať už existujúce osobné dáta pre potreby Profilu Košičana. * Zapisovať a konsolidovať nové osobné dáta občanov Košíc. * Kooperovať prostredníctvom REST API rozhrania s Azure AD B2C a KKUFW pri registrácii a prihlasovaní občanov. * Sprostredkovať osobné dáta autorizovaným osobám pomocou REST API rozhrania. * Sprostredkovať občanovi jeho konania, podania a komunikáciu s mestom vo forme konsolidovaných procesov. * Reagovať na zmeny dotýkajúce sa Profilu Košičana a ich procesov v systéme LCS Norris a Helios * Vystaviť privátne a verejné REST API pre prístup autorizovaným osobám a aplikáciám. * Autorizuje požiadavky validáciou JWT tokenov voči Azure AD B2C identity providerovi.   Jednotlivé prípady použitia KKProfile servis sú uvedené v dokumente <MK-KKaKES-DNR-PR-01-Profil-Kosicana.docx>. |
| **Azure Microsoft Entra - AD B2C** | Azure služba plní úlohu:   * Vytvára produkčného a testovacieho ténanta pre Konto Košičana * Poskytuje služby OIDC a OAuth2 identity providera. * Registruje aplikácie pre použitie prihlasovacieho a registračného user flowu. * Registruje aplikácie akceptujúce JWT access tokeny osôb Konta Košičana. * Customizuje prihlasovací a registračný user flowu ako aj policies podľa UIX. Pre customizáciu využíva vlastný template uložený vo webovej aplikácii KKUFW. * Vkladá custom claim-y pre prihlasovací a registračný user flowu. V prípade * Orchestruje prihlasovací a registračný user flow a policies podľa potrieb UIX. * Registruje API Connector-i vytvárané v KKUFW pre validácie a vypĺňanie custom claim-ov * Manažuje grupy a registrovaných používateľov. * Poskytuje prihlasovanie pomocou emailu a hesla. * Poskytuje manažment hesiel. * Poskytuje deaktiváciu účtov.   <https://learn.microsoft.com/en-us/entra/identity-platform/application-model>,  <https://learn.microsoft.com/en-us/entra/identity-platform/custom-extension-overview>,  <https://learn.microsoft.com/en-us/entra/external-id/customers/how-to-add-attributes-to-token>,  <https://learn.microsoft.com/en-us/azure/active-directory-b2c/user-flow-overview>,  <https://learn.microsoft.com/en-us/azure/active-directory-b2c/custom-policy-overview>,  <https://learn.microsoft.com/en-us/azure/active-directory-b2c/user-flow-custom-attributes?pivots=b2c-custom-policy>,  <https://learn.microsoft.com/en-us/azure/active-directory-b2c/customize-ui-with-html?pivots=b2c-custom-policy>,  <https://learn.microsoft.com/en-us/azure/active-directory-b2c/tokens-overview#token-types>, |
| **KKUFW** | Webová aplikácia vytvorená pomocou Azure služby App Services plní úlohu:   * Poskytuje vlastný template pre prihlasovací a registračný user flow. * Poskytuje web stránky v responzívnom template web stránky aj pre mobilné aplikácie. * Poskytuje API Connector pre validáciu claim-ov registračnom flow-e. * Poskytuje kontajner pre možné custom claim-y. * Vytvára spojenie s LCS Norris middlewarom pre validáciu registrujúcich sa osôb prostredníctvom REST API. * Vytvára spojenie s LCS Norris middlewarom pre vyplnenie claimov registrujúcich sa osôb. * Rozhoduje o úrovni QAA registrácie do claim-u extension\_qaa a zapisuje ho do Profilu Košičana v LCS Norris cez KKProfile servis REST API.   Prípady použitia pri komunikácii s KKProfile servis sú uvedené v dokumente <MK-KKaKES-DNR-PR-01-Profil-Kosicana.docx>. |
| **Konto Košičana** | Mobilná aplikácia Konta Košičana z pohľadu autentifikácie:   * Konzumuje službu prihlasovania sa pomocou email a hesla * Štartuje službu registrácia pomocou pošty mesta Košíc – email, heslo * Štartuje službu registrácia pomocou občianskeho preukazu na kontaktnom mieste mesta Košíc * Reflektuje na metodiku access-refresh tokenov v procese prístupu a validácie požiadaviek na API rozhraniach. |
| **Portál eSlužieb Košice** s **Osobnou zónou** | Web portál eSlužieb Košice z pohľadu autentifikácie:   * Konzumuje službu prihlasovania sa pomocou emial a hesla * Štartuje službu registrácia pomocou pošty mesta Košíc – email, heslo * Štartuje službu registrácia pomocou občianskeho preukazu na kontaktnom mieste mesta Košíc * Realizuje službu registrácia pomocou eID a mID * Realizuje službu prihlasovanie pomocou eID a mID (trust), získaním JWT tokenov z Azure AD B2C. * Reflektuje na metodiku access-refresh tokenov v procese prístupu a validácie požiadaviek na API rozhraniach. * Realizuje službu deaktivácie konta Košičana |

#### Toky tokenov v architektúre – Person to System

Ide predovšetkým o API volania, ktoré vyžadujú tokeny prihláseného občana KK (neskôr aj token administrátora), pre prístup a manažment osobných údajov.



Obrázok 4 Toky tokenov v architektúre – Person to System

## Technologická architektúra

### Technologická architektúra autentifikácie (AS-IS Fáza 1)

A diagram of a software application

AI-generated content may be incorrect.

Obrázok 5 Technogická architektúra AS-IS Fáza 1

### Technologická architektúra autentifikácie (AS-IS Fáza 2)

A diagram of a software flowchart

AI-generated content may be incorrect.

Obrázok 6 Technologická architektúra AS=IS

## Biznisové služby a procesy KK (E2E)

V tejto kapitole je popísaný budúci stav end-to-end biznis služieb a procesov KK.

### UCR1 – Registrácia pomocou pošty mesta Košíc - email, heslo

<https://learn.microsoft.com/en-us/entra/external-id/customers/overview-solutions-customers>

<https://learn.microsoft.com/en-us/entra/external-id/customers/how-to-manage-customer-accounts>

|  |  |
| --- | --- |
| Kód | RO\_P1.01 |
| Názov | Registrácia pomocou pošty mesta Košíc - email, heslo |
| Popis | Registrácia pomocou pošty mesta Košíc s vytvorením autentifikačného prostriedku pomocou emailu a hesla pozostáva z viacerých časovo nezávislých procesov. V prvom kroku ide o proces stotožnenia už evidovaných občanov mesta Košíc prostredníctvom aktivačných kódov generovaných v systéme LCS Norris a ich priradeniu k platobným výberom k daniam a poplatkom posielaným občanom v listinnej podobe.  Počas generovania aktivačných kódov sa v databáze vytvorí tabuľka identít PKProfilu Košičana (<MK-KKaKES-DNR-PR-01-ProfilObcana.docx> – Objekt PKIdentity ), do ktorej budú sumarizované existujúce údaje zo systému LCS Norris a Helios. Zároveň sa pre objekty identity vygeneruje jedinečný identifikátor Konta Košičana (kid).  Azure AD B2C zaregistruje email s požadovanými dátami občana a odošle na emailový účet email s validačným kódom pre validáciu emailu. Následne zozbiera požadované dáta a aktivačný kód, ktorý overí v KKProfile servis a dokončí registráciu. |
| Vstupné podmienky | * Azure AD B2C tenant je nakonfigurovaný. * Ténant má nakonfigurovaného identity providera na OIDC pre poskytovanie JWT tokenov. * Ténant má nakonfigurovanú aplikáciu pre KKUFW. * Ténant má nakonfigurovanú aplikáciu pre KKProfile servis. * KKProfile servis servis je integrovaný pre prístup k OIDC discovery a jwks\_uri. * Servis provider eSlužby Košice je integrovaný pre prístup k OIDC discovery a jwks. * Servis provider eSlužby Košice má integrované prihlasovací a registračný flow Azure AD B2C. * Mobilná aplikácia má integrované prihlasovací a registračný flow Azure AD B2C. * Tenant ma vytvorenú vlastnú tempate aplikáciu s custom user flowom pre prihlasovanie a registráciu podľa UIX. * Tenant má vytvorenú aplikáciu resp. službu pre validáciu (activationCode) a doplnenie claimov v custom user flowe (extension\_pco, extension\_qaa, ...) * KKUFW je integrovaná s KKProfile servis pre využitie privátneho API, * KKProfile servis servis má dostupné privátne API. * KKProfile servis zrealizoval [UCPK1](MK-KKaKES-DNR-PR-01-Profil-Kosicana.docx) – Vytvorenie profilu Košičana z existujúcich dát v systéme LCS Norris a Helios 1 * KKProfile servis podporuje [UCPK2](file:///Users/peter.stavny/Documents/Bussines/In-Watts/MADSolution/DNR/MK-KKaKES-DNR-PR-01-Profil-Kosicana.docx) - Získanie a overenie existencie profilu Košičana z Azure AD B2C * KKProfile servis podporuje [UCPK3](file:///Users/peter.stavny/Documents/Bussines/In-Watts/MADSolution/DNR/MK-KKaKES-DNR-PR-01-Profil-Kosicana.docx) – Zmenu existujúceho profilu Košičana z Azure AD B2C s aktivačným kódom * eProfile servis má vystavený privátny POST endpoint **/kk/ad/profiles/register** |
| Výstupné podmienky | * Občan má vytvorený účet v s Azure AD B2C. * Účet je označený extension\_qaa levelom „high“ v PKProfile Košičana * Je vytvorený a priradený záznam (log) o registrácii a aktivácii konkrétneho profilu občana, časový záznam je dostupný pre prihláseného používateľa v atribúte *created* resp. *modified*. |
| Obmedzenia | * ... |
| Hlavný scenár | 1. Vygenerovanie aktivačného kódu v LCS Norris pri konsolidácii dát každého evidovaného občana v LCS Norris a Helios podľa [UCPK1](file:///Users/peter.stavny/Documents/Bussines/In-Watts/MADSolution/DNR/MK-KKaKES-DNR-PR-01-Profil-Kosicana.docx). 2. Mestská pošta zabezpečí vytlačenie aktivačného kódu v papierovej forme a vloženie listu s kódom, adresou registračnej stránky a informáciami o registrácii k odosielaniu platobných výmerov do emailovej schránky do obálky s platobnými výmermi k daniam a poplatkom. 3. Mestská pošta doručí obálky do rúk občanom mesta Košíc. 4. Občan otvorí v prehliadači adresu portálu eSlužieb Košíc (<https://www.esluzbykosice.sk/>) a zvolí prihlásenie/registráciu pomocou aktivačného kódu 5. Azure AD B2C požiada občana o email, aktivačný kód, meno, priezvisko a rodné číslo podľa UIX flowu. 6. Azure AD B2C overí email občana odoslaním overovacieho kódu do emailovej schránky občana. 7. Občan vpíše overovací kód do požadovaného políčka a pokračuje v registrácii vložením mena priezviska, rodného čísla a aktivačného kódu. 8. Občan potvrdí podmienky Privacy a policy, resp. aj Data Policy ohľadom GDPR a potvrdí registráciu. 9. Azure AD B2C overí aktivačný kód pomocou extension aplikácie KKUFW a KKProfile servis podľa scenára [UCPK2](file:///Users/peter.stavny/Documents/Bussines/In-Watts/MADSolution/DNR/MK-KKaKES-DNR-PR-01-Profil-Kosicana.docx) - Získanie a overenie existencie profilu Košičana z Azure AD B2C.    1. Ak je výsledok overenia negatívny zobrazí občanovi chybu príslušnú chybu.    2. Ak je overenie pozitívne pokračuje v procese 10. KKUFW overí zhodnosť zadaných údajov meno, priezvisko a rodné číslo s údajmi PKProfile z odpovede KKProfile servis-u.     1. Ak je výsledok overenia negatívny zobrazí občanovi chybu príslušnú chybu.     2. Ak je overenie pozitívne pokračuje v procese 11. KKUFW aktivuje účet volaním požiadavky do KKProfile servis podľa scenára [UCPK3](file:///Users/peter.stavny/Documents/Bussines/In-Watts/MADSolution/DNR/MK-KKaKES-DNR-PR-01-Profil-Kosicana.docx) - Zmenu existujúceho profilu Košičana z Azure AD B2C s aktivačným kódom.     1. Ak je výsledok zápisu negatívny zobrazí občanovi chybu príslušnú chybu.     2. Ak je overenie pozitívne pokračuje v procese 12. KKUFW zmodifikuje AD custom claim-y. 13. KKUFW zavolá registračný endpoint **/kk/ad/eprofiles/register** s PKProfilom z enpointu **/kk/ad/profiles/validate** 14. eProfile modul zaregistruje nové konto Košičana. 15. Azure AD B2C úspešne dokončí registráciu a presmeruje občana späť portálu eSlužieb Košíc s JWT access a refresh tokenom. |
| Alternatívny scenár |  |

### UCR2 - Registrácia pomocou občianskeho preukazu na kontaktnom mieste mesta Košíc

|  |  |
| --- | --- |
| Kód | RO\_P1.02 |
| Názov | Registrácia pomocou občianskeho preukazu na kontaktnom mieste mesta Košíc |
| Popis | Registrácia pomocou občianskeho preukazu na kontaktnom mieste mesta Košíc s vytvorením autentifikačného prostriedku pomocou emailu a hesla je identický s UCR1 až na časť odosielania aktivačného kódu mestskou poštou.  V tomto prípade môže dôjsť k situácii, že PKIndetita v LCS Norris a Helios neexistuje. Proces predpokladá, že pracovníčka pred generovaním aktivačného kódu založí v systéme LCS Norris a Helios občanovi zložku. Na takto novo evidovaného občana zareaguje systém resp. KKProfile servis vytvorením PKProfile objektu občana. |
| Vstupné podmienky | * Azure AD B2C tenant je nakonfigurovaný. * Ténant má nakonfigurovaného identity providera na OIDC pre poskytovanie JWT tokenov. * Ténant má nakonfigurovanú aplikáciu pre KKUFW. * Ténant má nakonfigurovanú aplikáciu pre KKProfile servis. * KKProfile servis servis je integrovaný pre prístup k OIDC discovery a jwks\_uri. * Servis provider eSlužby Košice je integrovaný pre prístup k OIDC discovery a jwks. * Servis provider eSlužby Košice má integrované prihlasovací a registračný flow Azure AD B2C. * Mobilná aplikácia má integrované prihlasovací a registračný flow Azure AD B2C. * Tenant ma vytvorenú vlastnú tempate aplikáciu s custom user flowom pre prihlasovanie a registraciu podľa UIX. * Tenant má vytvorenú aplikáciu resp. službu pre validáciu (activationCode) a doplnenie claimov v custom user flowe (extension\_pco, extension\_qaa, ...) * KKUFW je integrovaná s KKProfile servis pre využitie privátneho API, * KKProfile servis servis má dostupné privátne API. * KKProfile servis zrealizoval [UCPK1](MK-KKaKES-DNR-PR-01-Profil-Kosicana.docx) – Vytvorenie profilu Košičana z existujúcich dát v systéme LCS Norris a Helios 1 * KKProfile servis podporuje [UCPK2](file:///Users/peter.stavny/Documents/Bussines/In-Watts/MADSolution/DNR/MK-KKaKES-DNR-PR-01-Profil-Kosicana.docx) - Získanie a overenie existencie profilu Košičana z Azure AD B2C * KKProfile servis podporuje [UCPK3](file:///Users/peter.stavny/Documents/Bussines/In-Watts/MADSolution/DNR/MK-KKaKES-DNR-PR-01-Profil-Kosicana.docx) – Zmenu existujúceho profilu Košičana z Azure AD B2C s aktivačným kódom. * eProfile servis má vystavený privátny POST endpoint **/kk/ad/profiles/register** |
| Výstupné podmienky | * Občan má vytvorený účet v s Azure AD B2C. * Účet je označený extension\_qaa levelom „high“ v PKProfile Košičana * Je vytvorený a priradený záznam (log) o registrácii a aktivácii konkrétneho profilu občana, časový záznam je dostupný pre prihláseného používateľa v atribúte *created* resp. *modified*. |
| Obmedzenia | * ... |
| Hlavný scenár | 1. Občan požiada pracovníčky kancelárie prvého kontaktu o vygenerovanie aktivačného kódu pre registrácii na Konto Košičana. 2. Pracovníčka požiada občana o občiansky preukaz a preverí jeho identitu. 3. Pracovníčka následne overí na stránkach Ministerstva vnútra SR či nejde o stratení alebo odcudzený občiansky preukaz pomocou čísla občianskeho preukazu (<https://www.minv.sk/?stratene-a-odcudzene-doklady>). 4. Pracovníčka vyhľadá občana v backoffice systéme LCS Norris.    1. Ak je výsledok vyhľadania negatívny zaeviduje občana v systéme    2. Ak je overenie pozitívne pokračuje v procese 5. Pracovníčka požiada systém LCS Norris vygenerovanie aktivačného kódu pre overeného občana. 6. Pracovníčka vytlačí aktivačný kód v papierovej forme. 7. Prípad použitia UCR1 krok 4 až 13. |
| Alternatívny scenár |  |

### UCR3 - Registrácia pomocou eID a mID

|  |  |
| --- | --- |
| Kód | RO\_P1.03 |
| Názov | Registrácia pomocou eID a mID |
| Popis | Prípad použitia sleduje registráciu akéhokoľvek občana do Konta Košičana pomocou občianskeho preukazu prostredníctvom prihlásenia sa do UPVS cez IAM WS stránky. Teda prihlásenie pomocou eID a mID. Po validácii adresy trvalého bydliska sa registrovanému občanovi priradí qaaLevel na high a category podľa nasledovných kritérii:   * Ak na adresu trvalého alebo prechodného pobytu v Košiciach – citizen * Ak platí dane a poplatky – certified * Ak nemá adresu trvalého alebo prechodného pobytu v Košiciach - nevytvarame |
| Vstupné podmienky | * Požadované dáta pre kategóriu **citizen** a **certified** existujú v systéme LCS Norris a Helios * Je podpísaná Dohoda o integračnom zámere s NASES * Je zaregistrovaný servis provider v slovensko.sk cez EKR * Je infraštruktúrne prepojenie UPVS s servis providerom mesta Košíc * KKProfile servis zrealizoval [UCPK16](MK-KKaKES-DNR-PR-01-Profil-Kosicana.docx) – Vytvorenie profilu Košičana pomocou WebSSO z existujúcich dát v systéme LCS Norris a Helios 1 * Občan vlastní občiansky preukaz s čipom |
| Výstupné podmienky | * Občan má vytvorený účet v Azure AD B2C. * Profil občana je vytvorený * Profil občana je aktivovaný, **isActive = true** * Profil občana má vygenerované **kid** a **regCode** (jedinečný identifikátor KK a aktivačný kód) * Profil občana má nastavené atribúty na default hodnoty a atribúty **qaaReg = low**, **category = podľa kategorizácie uvedenej hore**. * Je vytvorený a priradený záznam (log) o vytvorení konkrétneho profilu občana, časový záznam je dostupný pre prihláseného používateľa v atribúte ***created***. |
| Obmedzenia | * ... |
| Hlavný scenár | 1. Občan prechádza registračným procesom pomocou eID. 2. Občan je presmerovaný z konto.kosice.sk portálu do moje.kosice.sk na registráciu pomocou eID. 3. moje.kosice.sk servise provider presmeruje občana na prihlasovaciu stránku UPVS IAM, kde sa občan prihlási pomocou eID, mID, SVM resp. eIDAS. 4. moje.kosice.sk servise provider prijme WebSSO token občana a požiada o doplnenie údajov - email. 5. Následne moje.kosice.sk servise provider zavolá KKUFW endpoint **/v1/kkuf/registrations/upvs-validate** s vloženými údajmi **email**, **givenName**, **surname,** **pin** a **address** v tele požiadavky s nedekódovaným WebSSO tokenom. 6. KKUFW servis prijme požiadavku a overí integritu požiadavky.    1. Ak je overenie negatívne vráti chybovú odpoveď 400 s popisom chyby.    2. Ak je overenie pozitívne pokračuje v procese 7. KKUFW servis prijme požiadavku, dekóduje WebSSO token a overí identitu občana voči UPVS IAM pomocou OBO tokenu a GetIdentity volania.    1. Ak je overenie negatívne vráti chybovú odpoveď 400 s popisom chyby.    2. Ak je overenie pozitívne pokračuje v procese 8. KKUFW servisa zavolá KKProfile servisu endpoint **/v1/kk/ad/profiles/upvs-validate** s vloženými údajmi **email**, **givenName**, **surname,** **pin** a **address** v tele požiadavky s dekódovaným WebSSO tokenom. 9. KKProfile servis vyhľadá v databáze LCS Norris PKIdentity so zodpovedajúcimi atribútmi **givenName**, **surname** a **pin**.    1. Ak je vyhľadanie pozitívne a účet je nie je aktívny pokračuje v procese       1. V PKIdentity **isActive** na **true**.       2. V PKIdentity **expRegCode** na **0**.       3. V PKIdentity **category** na **visitor**.       4. V PKIdentity **qaaReg** na **qaaReg** z tela požiadavky.       5. KKProfile servis vytvorí kladnú odpoveď 201 s PKIdentity objektom v tele odpovede.    2. Ak je vyhľadanie pozitívne a účet je aktívny       1. KKProfile servis vytvorí chybovú odpoveď 400 s chybovým objektom v tele odpovede – účet registrovaný.    3. Ak je vyhľadanie negatívne, ale trvalá adresa je v rámci Košíc servisa vytvorí PKIdentity z údajov v requeste       1. V PKIdentity nastaví **isActive** na **true**.       2. V PKIdentity nastaví **expRegCode** na **0**.       3. V PKIdentity nastaví **category** na **citizen**.       4. V PKIdentity **qaaReg** na **high** z tela požiadavky.       5. KKProfile servis vytvorí kladnú odpoveď 201 s PKIdentity objektom v tele odpovede. 10. KKUFW aplikácia príjme odpoveď a pokračuje v dokončení registračného procesu.     1. Ak je odpoveď negatívna vráti chybovú odpoveď 400 s popisom chyby.     2. Ak je odpoveď pozitívna pokračuje v procese 11. KKUFW aplikácia pomocou Azure GraphAPI vytvorí novú identitu v Azure na základe prijatých údajov meno, heslo a kid a odošle potvrdzovací email 12. Občan otvorí a email, klikne na linku, ktorá ho presmeruje na nastavenie hesla, po ktorom sa registračný proces dokonči a občan je schopný sa prihlásiť do konta Košičana |
| Alternatívny scenár |  |

### UCR4 - Registrácia federáciou s externými identity providerami

Bude predmetom v ďalších verziách návrhu

### UCR5 - Registrácia pomocou mena a hesla bez aktivačného kódu

|  |  |
| --- | --- |
| Kód | RO\_P1.05 |
| Názov | Registrácia pomocou mena a hesla bez aktivačného kódu |
| Popis | Registrácia sa vykoná priamo pomocou registračného flovu z Azure AD B2C bez aktivačného kódu. Čo v prípade kategorizácie vytvorí buď citizen resp. visitor účet avšak na úrovni extension\_qaa nízka „low“  V tomto prípade ako bolo spomenuté, môže dôjsť k situácii, že PKIndetita v LCS Norris a Helios neexistuje. Aj keď sa predpokladá, že na novo evidovaného občana zareaguje systém resp. KKProfile servis vytvorením PKProfile objektu občana avšak bez aktivačného kódu. |
| Vstupné podmienky | * Azure AD B2C ténant je nakonfigurovaný. * Ténant má nakonfigurovaného identity providera na OIDC pre poskytovanie JWT tokenov. * Ténant má nakonfigurovanú aplikáciu pre KKUFW. * Ténant má nakonfigurovanú aplikáciu pre KKProfile servis. * KKProfile servis je integrovaný pre prístup k OIDC discovery a jwks\_uri. * Servis provider eSlužby Košice je integrovaný pre prístup k OIDC discovery a jwks. * Servis provider eSlužby Košice má integrované prihlasovací a registračný flow Azure AD B2C. * Mobilná aplikácia má integrované prihlasovací a registračný flow Azure AD B2C. * Ténant ma vytvorenú vlastnú tempate aplikáciu s custom user flowom pre prihlasovanie a registráciu podľa UIX. * Ténant má vytvorenú aplikáciu resp. službu pre validáciu (activationCode) a doplnenie claim-ov v custom user flowe (extension\_pco, extension\_qaa, ...) * KKUFW je integrovaná s KKProfile servis pre využitie privátneho API, * KKProfile servis servis má dostupné privátne API. * KKProfile servis podporuje [UCPK4](file:///Users/peter.stavny/Documents/Bussines/In-Watts/MADSolution/DNR/MK-KKaKES-DNR-PR-01-Profil-Kosicana.docx) – Vytvorenie nového profilu Košičana z Azure AD B2C. |
| Výstupné podmienky | * Občan má vytvorený účet v s Azure AD B2C. * Účet je označený extension\_qaa levelom „high“ v PKProfile Košičana * Je vytvorený a priradený záznam (log) o registrácii a aktivácii konkrétneho profilu občana, časový záznam je dostupný pre prihláseného používateľa v atribúte *created* resp. *modified*. |
| Obmedzenia | * ... |
| Hlavný scenár | 1. Občan otvorí v prehliadači adresu portálu eSlužieb Košíc (<https://www.esluzbykosice.sk/>) a zvolí prihlásenie/registráciu pomocou aktivačného kódu 2. Azure AD B2C požiada občana o email, aktivačný kód, meno, priezvisko a rodné číslo podľa UIX flowu. 3. Azure AD B2C overí email občana odoslaním overovacieho kódu do emailovej schránky občana. 4. Občan vpíše overovací kód do požadovaného políčka a pokračuje v registrácii vložením mena priezviska, rodného čísla a bez zadania aktivačného kódu, ktorý nevlastní. 5. Občan potvrdí podmienky Privacy a policy, resp. aj Data Policy ohľadom GDPR a potvrdí registráciu. 6. Občan je upozornení že bez zadania aktivačného kódu bude mať nižšie oprávnenie a obmedzený prístup k funkcionalitám službám mesta Košíc. 7. KKUFW aktivuje účet volaním požiadavky do KKProfile servis podľa scenára [UCPK4](file:///Users/peter.stavny/Documents/Bussines/In-Watts/MADSolution/DNR/MK-KKaKES-DNR-PR-01-Profil-Kosicana.docx) - Vytvorenie nového profilu Košičana z Azure AD B2C.    1. Ak je výsledok zápisu negatívny zobrazí občanovi chybu príslušnú chybu.    2. Ak je overenie pozitívne pokračuje v procese 8. KKUFW zmodifikuje AD custom claim-y. 9. Azure AD B2C úspešne dokončí registráciu a presmeruje občana späť portálu eSlužieb Košíc s JWT access tokenom. |
| Alternatívny scenár |  |

### UCA1 - Prihlasovanie pomocou email-hesla

|  |  |
| --- | --- |
| Kód | PO\_P1.01 |
| Názov | Prihlasovanie pomocou email-hesla |
| Popis | Prihlasovanie sa vykoná priamo pomocou registračného flow-u z Azure AD. |
| Vstupné podmienky | * Azure AD B2C tenant je nakonfigurovaný. * Ténant má nakonfigurovaného identity providera na OIDC pre poskytovanie JWT tokenov. * Servis provider eSlužby Košice je integrovaný pre prístup k OIDC discovery a jwks. * Servis provider eSlužby Košice má integrované prihlasovací a registračný flow Azure AD B2C. * Mobilná aplikácia má integrované prihlasovací a registračný flow Azure AD B2C cez MSAL knižnice. * Ténant ma vytvorenú vlastnú tempate aplikáciu s custom user flowom pre prihlasovanie a registráciu podľa UIX. * KKUFW je integrovaná s KKProfile servis pre využitie privátneho API, |
| Výstupné podmienky | * Občan je prihlásený v portáli eSlužby Košice. |
| Obmedzenia | * ... |
| Hlavný scenár | 1. Občan otvorí v prehliadači adresu portálu eSlužieb Košíc (<https://www.esluzbykosice.sk/>) a zvolí prihlásenie emailom a heslom 2. Portálu eSlužieb Košíc presmeruje občana na prihlasovaciu stránku Azure AD B2C. 3. Azure AD B2C požiada občana o email a heslo. 4. Občan vloží email a heslo a potvrdí prihlásenie. 5. Azure AD B2C overí email a heslo občana.    1. Ak je výsledok overenia negatívny zobrazí občanovi chybu príslušnú chybu.    2. Ak je overenie pozitívne pokračuje v procese 6. Azure AD B2C úspešne dokončí prihlásenie a presmeruje občana späť portálu eSlužieb Košíc s JWT access a refresh tokenom. |
| Alternatívny scenár | 1. Občan otvorí v mobilnú aplikáciu Konto Košičana. 2. Občan požiada o prihlásenie a je presmerovaný na obrazovku prihlásenia Azure AD B2C. 3. Azure AD B2C požiada občana o email a heslo. 4. Občan vloží email a heslo a potvrdí prihlásenie. 5. Azure AD B2C overí email a heslo občana.    1. Ak je výsledok overenia negatívny zobrazí občanovi chybu príslušnú chybu.    2. Ak je overenie pozitívne pokračuje v procese 6. Azure AD B2C úspešne dokončí prihlásenie a presmeruje pomocou URL schémy JWT access a refresh token. 7. Mobilná aplikácia zobrazí úspešné prihlásenie. |

### UCA2 - Prihlasovanie pomocou mID a eID (trust)

Bude predmetom v ďalších verziách návrhu

|  |  |
| --- | --- |
| Kód | PO\_AO.01 |
| Názov | Prihlasovanie pomocou mID a eID (trust) |
| Popis |  |
| Vstupné podmienky |  |
| Výstupné podmienky |  |
| Obmedzenia |  |
| Hlavný scenár |  |
| Alternatívny scenár |  |

### UCA3 - Prihlasovanie pomocou pin-u a biometrie v mobilnej aplikácii Konta Košičana

Bude predmetom v ďalších verziách návrhu

|  |  |
| --- | --- |
| Kód | PO\_AO.02 |
| Názov | Prihlasovanie pomocou pin-u a biometrie v mobilnej aplikácii Konta Košičana |
| Popis |  |
| Vstupné podmienky |  |
| Výstupné podmienky |  |
| Obmedzenia |  |
| Hlavný scenár |  |
| Alternatívny scenár |  |

### UCH1 - Zabudnuté heslo

<https://learn.microsoft.com/en-us/azure/active-directory-b2c/add-password-reset-policy?pivots=b2c-custom-policy>,

<https://github.com/azure-ad-b2c/samples/tree/master/policies/embedded-password-reset>

|  |  |
| --- | --- |
| Kód | PO\_MH.01 |
| Názov | Zabudnuté heslo |
| Popis | Zmena hesla sa vykoná priamo pomocou reset password flow-u v Azure AD. |
| Vstupné podmienky | * Azure AD B2C tenant je nakonfigurovaný. * Ténant má nakonfigurovaného identity providera na OIDC pre poskytovanie JWT tokenov. * Ténant má nakonfigurované vlastné reset password policy. * Servis provider eSlužby Košice je integrovaný pre prístup k OIDC discovery a jwks. * Servis provider eSlužby Košice má integrované prihlasovací, registračný a reste password flow Azure AD B2C. * Mobilná aplikácia má integrované prihlasovací, registračný a reset password flow Azure AD B2C cez MSAL knižnice. * Ténant ma vytvorenú vlastnú tempate aplikáciu s custom user flowom pre prihlasovanie, registráciu a reset password podľa UIX. * KKUFW je integrovaná s KKProfile servis pre využitie privátneho API, |
| Výstupné podmienky | * Občan je úspešne nastavil nové heslo a prihlásil sa v portáli eSlužby Košice. |
| Obmedzenia | * ... |
| Hlavný scenár | 1. Občan otvorí v prehliadači adresu portálu eSlužieb Košíc (<https://www.esluzbykosice.sk/>) a zvolí prihlásenie emailom a heslom 2. Portálu eSlužieb Košíc presmeruje občana na prihlasovaciu stránku Azure AD B2C. 3. Azure AD B2C požiada občana o email a heslo. 4. Občan si nepamätá heslo a zvolí si linku Zabudnuté heslo. 5. Azure AD B2C zobrazí stránku pre zadanie emailu a po potvrdení odošle overovací kód do emailu občana 6. Občan prepíše kód do políčka overovacie kódu a potvrdí ho. 7. Azure AD B2C zobrazí stránku so zadaním nového hesla a potvrdením nového hesla. 8. Občan zadá nového heslo a potvrdí 9. Azure AD B2C overí heslo a vráti sa na stránku prihlasovania. |
| Alternatívny scenár | 1. Občan otvorí v mobilnú aplikáciu Konto Košičana. 2. Občan požiada o prihlásenie a je presmerovaný na obrazovku prihlásenia Azure AD B2C. 3. Azure AD B2C požiada občana o email a heslo. 4. Občan si nepamätá heslo a zvolí si linku Zabudnuté heslo. 5. Azure AD B2C zobrazí stránku pre zadanie emailu a po potvrdení odošle overovací kód do emailu občana 6. Občan prepíše kód do políčka overovacie kódu a potvrdí ho. 7. Azure AD B2C zobrazí stránku so zadaním nového hesla a potvrdením nového hesla. 8. Občan zadá nového heslo a potvrdí 9. Azure AD B2C overí heslo a vráti sa na stránku prihlasovania. |

### UCD1 - Deaktivácia Konta Košičana občanom

Bude predmetom v ďalších verziách návrhu

|  |  |
| --- | --- |
| Kód | PO\_DO.01 |
| Názov | Deaktivácia Konta Košičana občanom |
| Popis | Deaktivácia Konta Košičana občanom pomocou aplikácie |
| Vstupné podmienky | * Azure AD B2C tenant je nakonfigurovaný. * Ténant má nakonfigurovaného identity providera na OIDC pre poskytovanie JWT tokenov. * Administrátor B2C má rolu pre administráciu používateľov |
| Výstupné podmienky | * Občan je úspešne deaktivovaný a nevie prihlásil sa v portáli eSlužby Košice. |
| Obmedzenia |  |
| Hlavný scenár | 1. Administrátor otvorí Azure Entra Admin centrum a vyhľadá v zozname používateľov občana s požadovaným emailom. |
| Alternatívny scenár |  |

### UCD2 – Deaktivácia Konta Košičana administrátorom

|  |  |
| --- | --- |
| Kód | PO\_DO.02 |
| Názov | Deaktivácia Konta Košičana administrátorom |
| Popis | Deaktivácia Konta Košičana administrátorom v Azure portáli. |
| Vstupné podmienky | * Azure AD B2C tenant je nakonfigurovaný. * Ténant má nakonfigurovaného identity providera na OIDC pre poskytovanie JWT tokenov. * Administrátor B2C má rolu pre administráciu používateľov |
| Výstupné podmienky | * Občan je úspešne deaktivovaný a nevie prihlásil sa v portáli eSlužby Košice. |
| Obmedzenia |  |
| Hlavný scenár | 1. Administrátor otvorí Azure Entra Admin centrum a vyhľadá v zozname používateľov občana s požadovaným emailom. 2. V nastaveniach občana deaktivuje účet |
| Alternatívny scenár |  |

# Skratky a značky

V tomto dokumente sú použité nasledujúce skratky a značky:

| Skratka / Pojem | Vysvetlenie / Popis |
| --- | --- |
| AAA | Autentifikácia, autorizácia a audit. |
| AD | Azure Active Driectory B2C. |
| Admin GUI | Rozhranie pre správu a konfiguráciu aplikácií, spravidla pre rolu Administrátor (Admin). |
| API | **Application Platform Interface**, rozhranie aplikačnej platformy spravidla na komunikáciu medzi systémami. |
| API First | Prístup, ktorý určuje spôsob návrhu a vývoja aplikačného softvéru, tak aby API vznikalo ešte pred samotnou implementáciou. |
| API GW | Verejná integračná platforma (API Gateway). |
| AS | Aplikačná služba (AS) je služba, ktorá sprístupňuje automatizované správanie aplikačnej funkcie, resp. aplikačného komponentu, ktorý je súčasťou informačného systému verejnej správy. |
| AS–IS | Aktuálny stav bez realizácie projektu. |
| BOK | Bezpečnostný osobný kód. |
| BPaaS | Business-process-as-a-Service. |
| BPMN | Business Process Model and Notation. |
| CAMP | Centrálna API Manažment Platforma. |
| CEP | Centrálna elektronická podateľňa. |
| CI/CD | Kontinuálna integrácia a dodávka. |
| CIP | Centrálna integračná platforma. |
| CISSP | Certified Information Systems Security Professional. Certifikát pre oblasť informačnej bezpečnosti. |
| CMS | Systém na správu obsahu (Content Management System). |
| CPU | Centrálna procesorová jednotka. |
| CSRÚ | Centrálna Správa Referenčných Údajov - informačný systém. |
| CÚD | Centrálne úradné doručovanie - rozšírenie modulu MED. |
| DB | Databáza (Database). |
| DevOps | Prístup riadenia založený na spolupráci vývoja a prevádzky. |
| DNR | Detailný návrh riešenia. |
| DOS | Pokus útočníka zamedziť používateľom prístup k službám počítača alebo k sieti. Komunikácia medzi používateľmi je natoľko preťažená, že nemôže adekvátne prebiehať. Napadnutý počítač je zvyčajne potrebné reštartovať, aby mohol poskytovať plnohodnotné služby (Denial of Service).  Cieľom sa stávajú najčastejšie web servery a účelom útoku je vyradiť ich z činnosti. |
| EA | Enterprise architektúra. |
| eDesk | Modul elektronických komunikačných stránok ÚPVS. |
| eForm | Modul elektronických formulárov ÚPVS. |
| eGOV | eGovernment. |
| eID | Elektronická identifikačná karta. |
| EKR | Externé komunikačné rozhranie modulu eDesk. |
| ESB | Podniková zbernica služieb (Enterprise Service Bus). |
| FAQ | Často kladené otázky (Frequently Asked Questions). |
| FO | Fyzická osoba. |
| G-Cloud | Vládny cloud (Government cloud). |
| G2G | Government To Government. |
| Git | Systém slúžiaci na riadenie revízií. |
| GovNET | Zabezpečená štátna sieť spravovaná Národnou agentúrou pre sieťové a elektronické systémy. |
| GUI | Grafické používateľské rozhranie (Graphical User Interface). |
| GUID | Globally Unique Identifier. |
| HDD | Pevný disk (skratka HDD z angl. hard disk). |
| HTML | Hypertextový značkový obsah (Hypertext Markup Language). |
| HTTP | Hypertextový prenosový protokol (Hypertext Transfer Protocol). |
| HW | Hardvér (Hardware). |
| IaaS | Infraštruktúra ako služba (Infrastructure as a Service). |
| IAM | Modul pre autentifikáciu používateľa. |
| IAM STS | Služba na vydanie SAML tokenov cez integračné rozhranie. |
| IAM WS | Synchrónne služby modulu IAM poskytujúce funkcionalitu nad identitou. |
| IČO | Identifikačné číslo organizácie. |
| ID | Identifikačné číslo. |
| ID-SK | Jednotný dizajn manuál elektronických služieb Slovenska. |
| IDP | Identity provider. |
| IIS | Internet Information Services. |
| IOM | Integrované obslužné miesto. |
| IS | Informačný systém |
| IS CSRU | Informačný systém Centrálnej správy referenčných údajov. |
| IS VS | Informačný systém verejnej správy. |
| ISO | International Organization for Standardization. Organizácia vydávajúca medzinárodné štandardy. |
| IT | Informačné technológie. |
| IT TOGAF | Medzinárodne akreditovaný certifikát, potvrdzujúci znalosti v oblasti Enterprise Architektúry. |
| IT VS | Informačné technológie verejnej správy. |
| JSON | JavaScript Object Notation. Štandardný formát súborov a formát výmeny údajov. |
| KC | Kontaktné centrum. |
| EP | Elektronický podpis. |
| KEP | Kvalifikovaný elektronický podpis, používa sa aj QES. |
| KK | Konto Košičana |
| KP | Katalóg požiadaviek. |
| KPI | Kľúčový ukazovateľ výkonnosti (Key performance Indicator). |
| KS | Koncová služba (KS) je služba, ktorá napĺňa určitú potrebu používateľa pri komunikácii s verejnou správou. Prostredníctvom koncovej služby sa uskutočňuje komunikácia občana s inštitúciou verejnej správy (G2C), podnikateľa s inštitúciou verejnej správy G2B), inštitúcie verejnej správy s inštitúciou verejnej správy (G2G), ak sú v postavení aplikácie práva a účastníka konania a inštitúcie verejnej správy so zahraničnou inštitúciou verejnej správy (G2A). |
| LDAP | Lightweight Directory Access Protocol. Protokol pre ukladanie a prístup k dátam. |
| MEF / eForm | Modul elektronických formulárov. |
| MEP | Platobný modul (modul elektronických platieb). |
| META IS | Centrálny metainformačný systém verejnej správy. |
| MF SR | Ministerstvo financií SR. |
| MH SR | Ministerstvo hospodárstva SR. |
| mID | Mobilné ID reprezentované mobilnou aplikáciou Slovensko v mobile. |
| MIRRI | Ministerstvo investícií, regionálneho rozvoja a informatizácie SR . |
| MK SR | Ministerstvo kultúry SR. |
| MPSVaR SR | Ministerstvo práce, sociálnych vecí a rodiny SR. |
| MŠVVaŠ SR | Ministerstvo školstva, vedy, výskumu a športu SR. |
| MV SR | Ministerstvo vnútra SR. |
| MVC | **Model View Controller** - návrhový vzor, ktorý sa bežne používa na vývoj používateľských rozhraní. |
| NASES | Národná agentúra pre sieťové a elektronické služby vznikla 1. januára 2009 ako príspevková organizácia Úradu vlády Slovenskej republiky (ďalej ako „ÚV SR“) za účelom plnenia odborných úloh v oblasti informatizácie spoločnosti vyplývajúcich zo zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, správy a prevádzkovania elektronických komunikačných sietí a služieb, pre Úrad vlády Slovenskej republiky (ktoré ÚV SR vyplývajú z § 24 ods. 3 zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy, ako aj §5 ods. 2 zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov), a aj pre ostatné orgány štátnej správy, právnické osoby a fyzické osoby, ktoré požadujú informácie, údaje z informačných systémov, databáz a registrov verejnej správy. Od 1. januára 2019 bola NASES delimitovaná pod Úrad podpredsedu vlády pre investície a informatizáciu (súčasné Ministerstvo investícií, regionálneho rozvoja a informatizácie SR). |
| NBÚ | Národný bezpečnostný úrad. |
| NET | Platforma pre vývoj webových aplikácií. |
| Nginx | Webový server. |
| NKIVS | Národná koncepcia informatizácie verejnej správy. |
| OP | Občiansky preukaz. |
| OPZ | Opis predmetu zákazky. |
| Oracle | Systém riadenia bázy dát. |
| OS | Operačný systém. |
| OST | Object Storage, objektové úložisko ÚPVS. |
| OVM | Orgán verejnej moci. |
| OWASP | Open Web Application Security Project. Určuje základné opatrenia pre zabezpečenie webu. |
| PaaS | Platforma ako služba (Platform as a Service). |
| PK | Prístupový komponent. |
| PO | Právnické osoby. |
| RAM | Pamäť s priamym prístupom alebo RAM (angl. Random Access Memory). |
| RAW data | Surové (RAW) dáta. |
| Rest API | Representational State Transfer. Architektúra rozhraní. |
| RFO | Register fyzických osôb. |
| RPO | Register právnických osôb. |
| SaaS | Softvér ako služba (Software as a Service). |
| SAML | Security Assertion Markup Language - Standard založený na XML (). |
| SLA | Service level Agreement, servisná zmluva. |
| SOAP | Simple Object Access Protocol. |
| SP | Service provider – poskytovateľ služby, spravidla právnická osoba alebo inštitúcia. |
| SQL | Štruktúrovaný vyhľadávací jazyk (Structured Query Language). |
| SR | Slovenská republika. |
| SSL | Secure Sockets Layer. |
| SVM | Slovensko v mobile. |
| SW | Softvér (Software). |
| SZČO | Samostatne zárobkovo činná osoba. |
| TEST | Prostredie pre vykonanie funkčných testov na strane Zhotoviteľa. |
| TO-BE | Budúci stav. |
| UAT | Prostredie určené pre vykonanie používateľských akceptačných testov (user acceptance testing environment). |
| UI | Používateľské rozhranie (User Interface). |
| UIR | Univerzálne integračné rozhranie. |
| UIR | Univerzálne integračné rozhranie - synchrónne rozhranie modulu G2G pre príjem SkTalk správ. |
| UML | Unified Modeling Language. Modelovací jazyk určený na vizualizáciu, špecifikáciu, navrhovanie a dokumentáciu programových systémov. |
| ÚPVII / ÚPPVII / ÚPPVIaI | Úrad podpredsedu vlády pre investície a informatizáciu (súčasné Ministerstvo investícií, regionálneho rozvoja a informatizácie SR). |
| ÚPVS | Ústredný portál verejnej správy. |
| URL | Uniform Resource Locator. Definuje doménovú adresu servera, umiestnenie zdroja na serveri a protokol, ktorým je možné k zdroju pristupovať. |
| USR | Univerzálne synchrónne rozhranie ÚPVS |
| ÚV SR | Úrad vlády Slovenskej republiky. |
| UX | Používateľský zážitok ( User Experience ). |
| VS | Verejná správa. |
| WEB SSO | Jednorazová jednotná autentifikácia na jednom mieste cez webový prehliadač. |
| WSDL | Web Services Description Language. |
| WYSIWYG | Princíp verného prenosu vizuálnej informácie (What You See Is What You Get). |
| XML | Extensible Markup Language. |
| XPATH | Dotazovací jazyk na výber uzlov z dokumentu XML. |
| XSD | XML Schema Definition. |
| XSLT | Jazyk určený na transformovanie XML. |
| XSS | Metóda narušenia WWW stránok využitím bezpečnostných chýb v skriptoch. |
| Z.z. | Zbierka zákonov. |
| ZoD | Zmluva o dielo. |
| ŽS | Životná situácia. |