Mesto Košice

Príloha č.5

Autentifikácia Aplikácii

Autentifikácia

|  |  |
| --- | --- |
| Zmluva |  |
| Verzia dokumentu | 0.1 |
| Autor dokumentu | Peter Stavný |
| Vlastník dokumentu | Mesto Košice |
| Dátum vydania |  |

Denník zmien:

| Verzia | Dátum | Revidoval | Popis | Označenie zmien |
| --- | --- | --- | --- | --- |
| 0.1 | 10.02.2024 | Peter Stavný | Iniciálna verzia dokumentu | Bez revízie |

Obsah

[1 Slovník pojmov 3](#_Toc158571483)

[2 Zoznam obrázkov 3](#_Toc158571484)

[3 Zoznam tabuliek 3](#_Toc158571485)

[4 Návrh riešenia 4](#_Toc158571486)

[4.1 Biznisové služby modulu Autentifikácie aplikácie 4](#_Toc158571487)

[4.2 OAuth2 a OIDC 4](#_Toc158571488)

[4.2.1 Access token 4](#_Toc158571489)

[4.3 Biznis architektúra 6](#_Toc158571490)

[4.3.1 Biznis architektúra autentifikácie (TO-BE) 6](#_Toc158571491)

[4.4 Aplikačná architektúra 7](#_Toc158571492)

[4.4.1 Aplikačná architektúra autentifikácie (TO-BE) 7](#_Toc158571493)

[4.5 Biznisové služby a procesy KK (E2E) 8](#_Toc158571494)

[5 Skratky a značky 9](#_Toc158571495)

# 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 6](#_Toc158571420)

[Obrázok 3 Aplikačná architektúra autentifikácie TO-BE 7](#_Toc158571421)

# Zoznam tabuliek

**No table of figures entries found.**

# Návrh riešenia

Pre identifikáciu a autentifikáciu občana je využitý OIDC OAuth2 servis Microsoft Entra – Azure AD B2C. Teda prístup občana k jednotlivým API je validovaný pomocou access tokenu vydanému po prihlásení sa na API rozhraniach jednotných servisov. Aby mohli tieto servisy validovať tieto tokeny, musia byť integrované na Azure AD B2C identity providera.

Pre integráciu a autentifikáciu aplikácii je určený OAuth2 **client credential flow** s JWT access tokenom (<https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth2-client-creds-grant-flow#get-a-token>). Tento token je možné následne overiť pomocou registrovaných verejných kľúčov jwks. A to nielen na úrovni OIDC servisu ale aj ostatných integrovaných servisov a aplikácii.

Práve tento, access token bude slúžiť:

* pre autorizáciu verejného REST API bez autorizácie osôb (ak nejde o Open Data endpointy)
* pre autorizáciu privátneho REST API, aj keď sa tam nachádza autorizácia

Teda pre registráciu aplikácii a následnú autentifikácii bolo 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).

Druhým veľmi podstatným atribútom pre autorizáciu aplikácie je Application ID, vygenerované v Microsoft Entra – Azure AD B2C pre integrovanú aplikáciu pri registrácii aplikácie (<https://learn.microsoft.com/en-gb/azure/active-directory-b2c/application-types>, <https://learn.microsoft.com/en-gb/azure/active-directory-b2c/tutorial-register-applications#app-registrations>).

## Biznisové služby modulu Autentifikácie aplikácie

Sú zhodné so službami Microsoft Entra – Azure AD B2C a identity providerom OIDC.

## OAuth2 a OIDC

### Access token

JWT access tokeny, ktoré budú vydávane po úspešnej autentifikácii aplikácie, 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>).

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",

}.[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 (TO-BE)



Obrázok 2 Aplikačná architektúra autentifikácie TO-BE

Hlavný komponent aplikačnej architektúry pre autentifikáciu aplikácií je Azure AD B2C identity provider **OIDC** servis, ktorý registrovaným aplikáciám vydáva ID\_token na základe OAuth2 Client Credential Flow-u. Jednotlivé služby poskytované cez API rozhrania tokeny validujú pomocou verejných JWK kľúčov poskytovaných OIDC servisom cez discovery jws\_uri endpoint.

|  |  |
| --- | --- |
| **KKProfile servis** | Servis má za úlohu:   * Autentifikuje sa voči OIDC * Validuje access tokeny iných aplikácii. |
| **Azure Microsoft Entra - AD B2C** | Azure služba plní úlohu:   * Registruje aplikácie * Generuje aplikačné prístupové prostriedky * Manažuje claimy JWT tokenov. |
| **OIDC** | Služba   * Autentifikuje aplikácie * Generuje access tokeny * Poskytuje validačné služby aplikáciám (discovery a jwks\_uri) |
| **KKUFW** | Servis má za úlohu:   * Autentifikuje sa voči OIDC |
| **Konto Košičana** | Mobilná aplikácia Konta Košičana z pohľadu autentifikácie:  Servis má za úlohu:   * Autentifikuje sa voči OIDC |
| **Portál eSlužieb Košice** | Servis má za úlohu:   * Autentifikuje sa voči OIDC. |

## Biznisové služby a procesy KK (E2E)

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

Sú zhodné so službami Microsoft Entra – Azure AD B2C a identity providerom OIDC.

# 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. |