# Bod 2 programu spoločného zasadnutia PS 2 a PS 4 9. február 2022

# (PS 4 – T8, T53)

# Návrh atribútov JSON Web Token používanom s protokolom REST a OpenID Connect pre použitie s API GW

Obsah

[1.1 Koncept návrhu JWT tokenov 1](#_Toc93238291)

[1.2 Autorizácia FO 3](#_Toc93238292)

[1.3 Access JWT token 3](#_Toc93238293)

[1.4 Refresh JWT token 6](#_Toc93238294)

[1.4.1 QAA Level 7](#_Toc93238295)

[1.4.2 AuthResourceType 8](#_Toc93238296)

[1.4.3 AuthResourceSubType 8](#_Toc93238297)

[1.5 Systém-to-systém autentifikácia 9](#_Toc93238298)

## Koncept návrhu JWT tokenov

Koncept autorizačného prostriedku pomocou JWT tokenov nenahrádza súčasnú autorizáciu pomocou WebSSO SAML tokenov. WebSSO SAML sa môže aj naďalej na portáloch používať a bude pravdepodobne používané paralelne popri JWT a teda platnosť oboch sa bude udržiavať oddelene od seba, pričom sa očakáva, že Identity provider CAMP bude na základe WebSSO SAML vydávať JWT tokeny, čím umožní používať služby integrované na CAMP API GW cez REST volania.

Identity provider CAMP umožní pre staršie systémy integrované cez jednotné prihlásenie sa pomocou WebSSO ÚPVS získať z CAMP IdP Access a Refresh JWT token, kde Access JWT nesie priamo v atribúte **saml** samotný WebSSO token. API GW a Identity provider projektu CAMP WebSSO SAML token akceptuje ako platný autorizačný prostriedok na príslušnej úrovni QAA a poskytne cez REST rozhranie prístup k službám ÚPVS napojených cez API GW zbernicu, pričom API GW bude interne na backende pre prístup k týmto službám používať STS tokeny vyžiadané z IAM ÚPVS v mene príslušnej identity alebo pomocou WebSSO tokenu.

Týmto prístupom môže starší systém aj ďalej využívať WebSSO sliding sesson tak ako doteraz a žiadať o JWT Access token pomocou WebSSO tokenu. Taktiež tým nebude integrovaný systém nútený k prihlasovaniu sa cez IdP OIDC server. V prípade, že starší systém prejde na OAuth2, riadenie predlžovania JWT Access tokenu preberie JWT Refresh token. Ten sa samozrejme nastaví pre webovú platformu tak, aby sa paralelne predlžoval JWT access token v súlade s WebSSO.

Zároveň WebSSO token nie je povinný. Projekt CAMP ráta do budúcna aj s tým, že sa používajú iné typy autentifikácie a bude poskytovať autentifikačné prostriedky na nižších úrovniach QAA, ktoré ÚPVS IAM nepodporuje a WebSSO token nie je vydávaný. Druhým dôvodom je, že mnohé systémy tretích strán majú implementované aj vlastné autentifikačné prostriedky pre prístup k ich chráneným zdrojom a samotný WebSSO token nevydáva interne ani mID platforma (vydáva ho ÚPVS IAM na základe potvrdenia prihlásenia identity z mID). V  prípade identít namapovaných na IdP CAMP bude vedieť CAMP získavať a manažovať STS tokeny vydávané ÚPVS IAM, ktoré nebudú súčasťou JWT tokenov.

## Autentifikácia pre fyzické osoby

Podstatnými zmenami voči terajšiemu riešeniu vydávania tokenov WebSSO je vydávanie JWT tokenov len na fyzické osoby (**FO**). Taktiež JWT tokeny nebudú niesť informácie o zastupovaniach a type identity. Tieto informácie si v prípade potreby ich použitia integrované subjekty budú musieť dotiahnuť, po úspešnej autentifikácii, pomocou autorizovaných služieb vystavených na CAMP API GW zbernici – pripravovanou novou REST službou **GetIdentity** (odlišnou od služby ÚPVS IAM). CAMP bude v JWT používať odlišný technický identifikátor osoby než ÚPVS IAM, pričom oba bude možné získať touto novou službou.

Nakoľko JWT tokeny nebudú limitované parametrami "delegationType", "SubjectID" ani "IdentityType", nebude nutné v spojení s manažmentom oprávnení (permission) požadovať prihlasovanie pre každé zastupovanie, ako to je momentálne. S jedným tokenom bude realizovaný do všetkých chránených zdrojov, ku ktorým má autorizovaná osoba práva.

JWT tokeny nebudú obsahovať ÚPVS role, nakoľko komunikáciu s ÚPVS cez REST s JWT bude sprostredkúvať CAMP, ktorý bude riešiť príslušné oprávnenia. Na rozhrania ÚPVS bude naďalej možné pristupovať aj priamo, mimo CAMP, avšak len cez SOAP rozhrania.

## Access JWT token

Access token je vydávaný IdP OIDC serverom pre prístup k zdrojom cez verejnú API GW na 5 minút pre mobilné zariadenia. Hodnota je konfigurovateľná podľa platforiem využívajúcich služby autorizácie. Po uplynutí platnosti tohto tokenu je nutné token obnoviť pomocou Refresh JWT tokenu.

HEADER: ALGORITHM & TOKEN TYPE

{

"alg": "RS256",

"typ": "JWT"

}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Atribút | Meno | Typ | Popis |
| 1 | alg | Algorithm | String | algoritmus používaný na podpísanie alebo šifrovanie JWT tokenu. Pre aplikáciu SVM **RS256.** |
| 2 | typ | Type | String | Obsah, ktorý sa podpisuje alebo šifruje (zvyčajne „JWT“). Pre aplikáciu SVM **JWT.** |

PAYLOAD:DATA

{

"sub": "{ identityId }",

"iss": "api.slovensko.sk/idp/oidc",

"aud": [ "{applicationId}", "{deviceId}" ],

"iat": 098123654,

"exp": 098123654,

"qaa": "3",

"saml": "MTIzZTQ1NjctZTg5Yi0xMmQzLWE0NTYtNDI2NjE0MTc0MDAx...",

"authRes": "2",

"subAuthRes": "AR"

}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Atribút | Meno | Typ | Popis |
| 1 | sub | Subject | String | Identifikátor pre používateľa. Na koho sa atribút odkazuje. Pre aplikáciu SVM jedinečný identifikátor FO v CAMP **identityId.** IdentityId hodnota je odlišná od ÚPVS IdentityId, avšak CAMP bude poskytovať službu pre získanie údajov o tejto IdentityId mapovaním s identifikátorom ÚPVS. |
| 2 | iss | Issuer | String | Identifikuje, kto vydal JWT. Pre aplikáciu SVM **url** **OIDC servera** |
| 3 | aud | Audience | Array<String> | Identifikuje príjemcov, pre ktorých je JWT určená. Každý, kto má v úmysle spracovať JWT, sa musí identifikovať s hodnotou v zozname. Ak ten, ktorý žiadosť spracúva, neidentifikuje svoju hodnotu v zozname, keď je tento nárok prítomný, musí byť JWT zamietnutý. Pre aplikáciu SVM jedinečný identifikátor aplikácie SVM **applicationId** a jedinečný identifikátor mobilného zariadenia **deviceId** |
| 4 | iat | Issued time | Number | Identifikuje čas, kedy bol JWT vydaný. Časová pečiatka Unixu v sekundách. |
| 5 | exp | Expiration time | Number | Identifikuje čas uplynutia platnosti a po uplynutí ktorého sa JWT nesmie prijať na spracovanie. Časová pečiatka Unixu v sekundách. |
| 6 | qaa | String |  | QAA level v zmysle číselníka. Pre SVM je hodnota **3** |
| 7 | per | Permissions | Array<String> | Zoznam oprávnení udelených používateľovi a aplikácii, pre ktorý je token vydaný. **V prvej iterácii nepovinný.** |
| 8 | saml | WebSSO token | String | WebSSO token z IAM ÚPVS. WebSSO je **nepovinný**. |
| 9 | authRes | Autentification resource type | String | AuthResourceType v zmysle číselníka-  Typ autentifikačného prostriedku použitého pre získanie tokenu |
| 10 | authResSub | Autentification resource subtype | String | AuthResourceSubType v zmysle číselníka - Podtyp autentifikačného prostriedku použitého pre získanie tokenu. Je **nepovinný** ak nexistuje pre daný authRes |

## Refresh JWT token

Access token je vydávaný IdP OIDC serverom pre obnovovanie Access JWT po dobu 30 minút. Hodnota je konfigurovateľná. Po uplynutí platnosti tohto tokenu je opätovné prihlásenie sa Autentifikačného JWT tokenu.

HEADER: ALGORITHM & TOKEN TYPE

{

"alg": "RS256",

"typ": "JWT"

}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Atribút | Meno | Typ | Popis |
| 1 | alg | Algorithm | String | algoritmus používaný na podpísanie alebo šifrovanie JWT tokenu. Pre aplikáciu SVM **RS256.** |
| 2 | typ | Type | String | Obsah, ktorý sa podpisuje alebo šifruje (zvyčajne „JWT“). Pre aplikáciu SVM **JWT.** |

PAYLOAD:DATA

{

"sub": "{ identityId }",

"iss": "api.slovensko.sk/idp/oidc",

"aud": [ "{applicationId}", "{deviceId}" ],

"iat": 098123654,

"exp": 098123654,

"qaa": "3",

"authRes": "7",

"subAuthRes": "AR"

}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Atribút | Meno | Typ | Popis |
| 1 | sub | Subject | String | Identifikátor pre používateľa. Na koho sa atribút odkazuje. Pre aplikáciu SVM jedinečný identifikátor FO v CAMP **identityId.** IdentityId hodnota je odlišná od ÚPVS IdentityId, avšak CAMP bude poskytovať službu pre získanie údajov o tejto IdentityId mapovaním s identifikátorom ÚPVS. |
| 2 | iss | Issuer | String | Identifikuje, kto vydal JWT. Pre aplikáciu SVM **url** **OIDC servera** |
| 3 | aud | Audience | Array<String> | Identifikuje príjemcov, pre ktorých je JWT určená. Každý, kto má v úmysle spracovať JWT, sa musí identifikovať s hodnotou v zozname. Ak ten, ktorý žiadosť spracúva, neidentifikuje svoju hodnotu v zozname, keď je tento nárok prítomný, musí byť JWT zamietnutý. Pre aplikáciu SVM jedinečný identifikátor aplikácie SVM **applicationId** a jedinečný identifikátor mobilného zariadenia **deviceId** |
| 4 | iat | Issued time | Number | Identifikuje čas, kedy bol JWT vydaný. Časová pečiatka Unixu v sekundách. |
| 5 | exp | Expiration time | Number | Identifikuje čas uplynutia platnosti a po uplynutí ktorého sa JWT nesmie prijať na spracovanie. Časová pečiatka Unixu v sekundách. |
| 6 | qaa | String |  | QAALevel level v zmysle číselníka. Pre SVM je hodnota **3** |
| 7 | per | Permissions | Array<String> | Zoznam oprávnení udelených používateľovi a aplikácii, pre ktorý je token vydaný. **V prvej iterácii nepovinný.** |
| 8 | saml | WebSSO token | String | WebSSO token z IAM ÚPVS. WebSSO je **nepovinný**. |
| 9 | authRes | Autentification resource type | String | AuthResourceType v zmysle číselníka -  Typ autentifikačného prostriedku použitého pre získanie tokenu. Napríklad: „2“ pre preukazy s čipom vydávané MV SR. |
| 10 | authResSub | Autentification resource subtype | String | AuthResourceSubType v zmysle číselníka - Podtyp autentifikačného prostriedku použitého pre získanie tokenu. Je **nepovinný** ak neexistuje pre daný authRes. Napríklad: „GC“ pre alternatívny autentifikátor. |

### QAA Level

Úrovne zabezpečenia na základe typ autentifikačného prostriedku použitého pre získanie tokenu podľa integračného manuálu pre systémy ISVS na modul IAM

|  |  |
| --- | --- |
| # | Poznámka |
| 1 | ÚPVS Prihlásenie prihlasovacím menom alebo cez sociálnu sieť |
| 2 | ÚPVS Prihlásenie prihlasovacím menom a dodatočne overenie GRID kartou (vydanou systémom eDemokracia/ÚPVS) |
| 3 | ÚPVS Prihlásenie pomocou autentifikačného certifikátu, MobileID alebo zahraničným prostriedkom elektronickej identifikácie podľa [Nariadenia EP a Rady 910/2014 (eIDAS)](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910) s úrovňou zabezpečenia (Level of Assurance) „pokročilá“ (substantial) |
| 4 | ÚPVS Prihlásenie eID kartou alebo zahraničným prostriedkom elektronickej identifikácie podľa Nariadenia EP a Rady 910/2014 (eIDAS) s úrovňou zabezpečenia (Level of Assurance) „vysoká“ (high) |

### AuthResourceType

Typ autentifikačného prostriedku použitého pre získanie tokenu podľa integračného manuálu pre systémy ISVS na modul IAM. Pre JWT používa vlastné číselné hodnoty, ktoré sa odlišujú od IAM UPVS (pozn.: od čísla 5, ktoré má v IAM číslo 9).

|  |  |  |
| --- | --- | --- |
| Textovy identitfikator  (hodnota v JWT) | Popis | Poznámka |
| 1 | Meno + heslo | SN nadobúda hodnotu identifikátora identity UID modulu IAM.  Príklad: E0000000040 |
| 2 | eID | SN nadobúda hodnotu čísla eID karty prevzatého z autentifikačného rozhodnutia (SAML response) eID AS MVSR pri prihlásení sa používateľa.  Príklad: AA123456 |
| 3 | GRID karta | SN nadobúda hodnotu identifikátora GRID karty v module IAM. |
| 4 | Certifikát |  |
| 5 | EIDAS |  |
| 6 | TU | V súčasnosti sa neplánuje táto hodnota využívať v rámci JWT vzhľadom na autentifikáciu fyzickej osoby. SN nadobúda hodnotu identifikátora identity UID modulu IAM.  Príklad: T0000000141 |
| 7 | MOBILEID |  |

### AuthResourceSubType

Podtyp autentifikačného prostriedku použitého pre získanie tokenu podľa integračného manuálu pre systémy ISVS na modul IAM

|  |  |  |  |
| --- | --- | --- | --- |
| # | Autentifikačný prostriedok | Textový identifikátor (hodnota v SAML aj v JWT) | Poznámka |
| 1 | eID | ID | Identity card. pre **občiansky preukaz s čipom** (**eID**) |
| 2 | **eDoPP** | AR | Residence permit. Pre **doklad o pobyte cudzinca s čipom** |
|  |  | AS | Special. Pre **doklad o pobyte cudzinca s čipom** |
|  |  | AF | Family member. Pre **doklad o pobyte cudzinca s čipom** |
| 3 | Alternativny autentifikátor | GC | Government card |

## Systém-to-systém autentifikácia

V prípade autentifikácie systém-to-systém sa nebude prihlasovať FO. V tomto prípade zvažujeme autentifikáciu technikou APIKey-Sharedkey integrovanou s LDAP systémom technických účtov a zároveň mTLS.

mTLS - Mutual authentication alebo two-way authentication (nezamieňať si to dvojfaktorovou autentifikáciou) ktorá sa týka dvoch strán, ktoré sa navzájom autentifikujú v rovnakom čase v autentifikačnom protokole.

Vzájomná autentifikácia je žiaducou vlastnosťou verifikačných schém, ktoré prenášajú citlivé údaje, aby sa zaistila bezpečnosť údajov. Vzájomnú autentifikáciu možno vykonať pomocou dvoch typov poverení: používateľských mien a hesiel (alebo APIKey-Sharedkey) a certifikátov verejného kľúča.