CAAIS: Autentizace uživatelů pomocí OIDC

Verze 1.1

9.5.2022



Zpracoval: Milan Babic

Obsah

[1. Úvod 4](#_Toc103021781)

[2. Proces autentizace pomocí OIDC 5](#_Toc103021782)

[2.1. Diagram autentizace uživatele 5](#_Toc103021783)

[2.2. Předpoklady pro využívání autentizace založené na OIDC 6](#_Toc103021784)

[2.2.1 Registrace a konfigurace AIS v CAAIS 6](#_Toc103021785)

[2.2.2 Ověřovací certifikát 7](#_Toc103021786)

[2.2.3 Přístupové role pro AIS 7](#_Toc103021787)

[2.3. Zpracování osobních údajů 8](#_Toc103021788)

[3. Technická specifikace autentizace 9](#_Toc103021789)

[3.1. Endpoint s OIDC konfigurací 9](#_Toc103021790)

[3.2. Serverové klíče 9](#_Toc103021791)

[3.3. Popis endpointu pro přihlášení uživatele 9](#_Toc103021792)

[3.4. Rozhraní stránky AIS pro návrat po úspěšném přihlášení 10](#_Toc103021793)

[3.5. Seznam atributů uživatele (identity) v ID tokenu 11](#_Toc103021794)

[3.6. Získání tokenů 11](#_Toc103021795)

[3.7. Úroveň záruk (Level of Assurance) 13](#_Toc103021796)

[4. Zkratky, pojmy, definice 15](#_Toc103021797)

[5. Přílohy 16](#_Toc103021798)

Seznam tabulek

[Tabulka 1: Seznam query parametrů 9](#_Toc103021799)

[Tabulka 2: Seznam atributů v ID tokenu 11](#_Toc103021800)

[Tabulka 3: Hodnoty LoA 13](#_Toc103021801)

Verze dokumentu

|  |  |  |  |
| --- | --- | --- | --- |
| **Verze** | **Stručný popis změn** | **Zpracoval** | **Datum** |
| 1.0 | Nový dokument | Milan Babic | 9.5.2022 |
| 1.1 | Přidání atributů do odpovědi (viz kapitola 3.5) | Milan Babic | 15.11.2023 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Úvod

Účelem tohoto dokumentu je popsat technické detaily uživatelské autentizace do agendových informačních systémů (AIS), které jsou registrovány v systému CAAIS. Uživatel používá přihlašovací údaje do systému CAAIS-IdP (modul interního IdP CAAIS), který zde plní funkci autentizačního informačního systému dle § 56a zákona č. 111/2009 Sb., o základních registrech.

Komunikace a předávání údajů o uživateli je prováděna pomocí protokolu OIDC, který se využívá pro výměnu autentizačních a autorizačních dat. Prostřednictvím OIDC protokolu se v rámci přesměrovávání uživatele mezi AIS a CAAIS předává definovaná sada atributů (viz kapitola 3.5), která je podmnožinou všech atributů, které jsou o uživateli (identitě) v systému CAAIS-IdP vedeny. Při autentizaci OIDC protokolem se ani nevolají žádné další webové služby CAAIS (např. editační) pro získání ostatních atributů.

URL pro získání potřebných informací pro komunikaci jsou následující:

|  |  |
| --- | --- |
| Prostředí | Adresa |
| testovací NAKIT | https://rest-openidconnectapi.caais-test-ext.gov.cz/.well-known/openid-configuration  https://rest-openidconnectapi.caais-test-ext.gov.cz/.well-known/oauth-authorization-server |
| provozní | https://rest-openidconnectapi.caais.*[doména]*/.well-known/openid-configuration  https://rest-openidconnectapi.caais.*[doména]*/.well-known/oauth-authorization-server  kde *[doména]* je **gov.cz** nebo **cms2.cz** |

# Proces autentizace pomocí OIDC

Proces autentizace uživatele otevírajícího si stránku AIS pomocí protokolu OIDC skrze CAAIS je popsán v následující části.

V OIDC jsou definovány 4 základní role účastnící se komunikace:

* Resource owner = uživatel
* Relying party = v našem případě AIS
* OpenID Provider = v našem případě CAAIS
* Identity Provider = v našem případě CAAIS-IdP

CAAIS bude podporovat proces přihlášení Authorization Code Flow, který je detailně popsaný v kapitole 2.1.

## Diagram autentizace uživatele



1. Uživatel otevře webovou stránku AIS
2. Pokud systém AIS zjistí, že není uživatel přihlášen, přesměruje uživatele na autorizační endpoint na CAAIS. Na této přihlašovací stránce CAAIS si uživatel zvolí způsob přihlášení a zadá přihlašovací údaje.
3. Systém CAAIS ověří, že autentizační metoda vybraná uživatelem splňuje úroveň LoA, která je pro daný AIS nakonfigurována v CAAIS. Provádí-li se autentizace pomocí interního CAAIS-IdP, komponenta CAAIS-IdP ještě navíc ověří správnost zadaných přihlašovacích údajů uživatele vůči uloženým údajům.
4. Pokud je autentizace úspěšná, provede CAAIS načtení informací o uživateli ze své DB. Následně se v CAAIS na základě přístupových rolí přidělených uživateli ověří, zda je oprávněn přistoupit do AIS. Pokud ano, pokračuje se dalším krokem. Jinak se uživateli zobrazí hláška o zamítnutí přístupu.
5. CAAIS vygeneruje OIDC odpověď.
6. A uživatel je s touto odpovědí přesměrován na definovanou adresu AIS (viz kapitola 3.4).
7. V systému AIS se zpracuje OIDC odpověď, ve které se nachází parametr "code".
8. Následně jej AIS odešle přes HTTP POST dotaz na token endpoint na CAAIS, kde se ověří právě získaným "code" parametrem a svým ověřovacím certifikátem. CAAIS zkontroluje obdržený "code" parametr a certifikát.
9. Pokud jsou validní, odešle AISu Access token a ID token uživatele.
10. AIS ověří, že ID token obdržený v odpovědi je validní a na základě informací o uživateli získaných z odpovědi posoudí, zda umožní uživateli přístup.

## Předpoklady pro využívání autentizace založené na OIDC

Pro používání OIDC autentizace platí podobné předpoklady, jako pro klasickou/přímou autentizační webovou službu CAAIS (viz dokument „CAAIS: Autentizační webová služba - Procesní popis“).

### Registrace a konfigurace AIS v CAAIS

AIS musí být v systému CAAIS nejdříve zaregistrován pod definovaný subjekt, což se provádí na základě elektronického formuláře, který zástupce AIS odesílá na definovanou datovou schránku.

U takto registrovaného AIS následně provede lokální administrátor subjektu konfiguraci těchto primárních údajů:

* **Povolená návratová URL pro SAML a OIDC** – seznam návratových adres AIS, kam je uživatel přesměrován po autentizaci
* **Ověřovací certifikát** – AIS se při volání token endpointu v CAAIS musí autentizovat ověřovacím certifikátem (více viz kapitola 2.2.2.).

### Ověřovací certifikát

AIS používá ověřovací certifikát při získávání Access tokenu a ID tokenu při přímé komunikaci s CAAIS.

Tento certifikát musí být typu komerční serverový a musí být zaregistrovaný v nastavení AIS (viz kapitola 2.2.1) a musí být vydaný podporovanou certifikační autoritou:

* I.CA
* PostSignum
* eIdentity
* NCA

V konfiguraci AIS v CAAIS může být zaregistrován pouze jeden ověřovací certifikát.

### Přístupové role pro AIS

V systému CAAIS je možné jednotlivým AIS definovat přístupové role, které pak daný AIS využívá pro řízení přístupu uživatelů. Nejdříve se číselník těchto přístupových rolí vytvoří u AIS a pak se tyto role přidělí konkrétním subjektům, které mají mít přístup do tohoto AIS. Lokální administrátoři těchto subjektů pak tyto přístupové role přidělují jednotlivým uživatelům daného subjektu.

Pokud nemá AIS žádné takové přístupové role vytvořeny, povolí systém CAAIS přístup do takového AIS všem uživatelům z libovolného subjektu. Za nastavení těchto rolí je tedy zodpovědný AIS.

## Zpracování osobních údajů

Modul CAAIS-IdP (interní IdP v systému CAAIS) splňuje požadavky § 56a zákona č. 111/2009 Sb., o základních registrech pro autentizační informační systém. Na základě toho mohou být v CAAIS uloženy osobní údaje uživatelů, které jsou následně předávány systémům AIS.

# Technická specifikace autentizace

V následujících kapitolách jsou uvedeny podrobné specifikace pro komunikaci systémů AIS se systémem CAAIS pomocí protokolu OIDC.

## Endpoint s OIDC konfigurací

V OIDC je definovaný endpoint na poskytování OIDC konfigurace daného Autorizačního serveru. Vrací JSON, který obsahuje základní konfiguraci, jako např. URL standardních OIDC endpointů.

Na CAAIS bude dostupný na url:

|  |  |
| --- | --- |
| Prostředí | Adresa |
| obecné | https://rest-openidconnectapi.[doména\_prostředí]/.well-known/openid-configuration  Kde [doména\_prostředí] odpovídá URL definované v úvodní kapitole, tedy např. caais-test-ext.gov.cz, caais.gov.cz, caais.cms2.cz |

## Serverové klíče

CAAIS podepisuje vydávané JWT (JSON Web Tokeny). Následně poskytuje endpoint, kde je možné získat veřejné klíče, které se musí použít na AIS pro ověření obdržených tokenů.

Na caais bude tento endpoint dostupný na url:

|  |  |
| --- | --- |
| Prostředí | Adresa |
| obecné | https://rest-openidconnectapi.[doména\_prostředí]/oauth2/jwks  Kde [doména\_prostředí] odpovídá URL definované v úvodní kapitole, tedy např. caais-test.ocp.cea01.dscen.cz, caais-test-ext.gov.cz, caais.gov.cz, caais.cms2.cz |

## Popis endpointu pro přihlášení uživatele

Pokud na AIS přistoupí nepřihlášený uživatel, provede AIS přesměrování na autorizační endpoint CAAISu.

Tabulka níže obsahuje seznam dostupných query parametrů, které se posílají na CAAIS při žádosti o přihlášení uživatele. Některé z nich jsou povinné.

Tabulka 1: Seznam query parametrů

|  |  |  |
| --- | --- | --- |
| Parametr | Povinný | Popis |
| client\_id | ano | Identifikátor Relying Party (AIS), v hodnotě se bude posílat zkratka pro AIS. |
| redirect\_uri | ano | Sem je po úspěšném přihlášení uživatel přesměrován. Musí odpovídat hodnotě, která je u AIS nakonfigurovaná jako návratová URL. |
| scope | ano | Seznam oprávnění, které Relying Party vyžaduje od Resource Ownera – seznam hodnot oddělených mezerou. Viz kapitola 3.5. |
| response\_type | ano | Typ odpovědi po úspěšném přihlášení uživatele. Musí obsahovat hodnotu „code“. |
| nonce | ne | Parametr, užívaný k zabránění tzv. „replay“ útokům. Obsahuje náhodně vygenerovanou hodnotu. Pokud ji AIS pošle, CAAIS přidá „nonce“ claim do ID tokenu. AIS poté musí ověřit, že obdržená hodnota v daném claimu odpovídá odeslané hodnotě. Doporučujeme použivat pro zvýšení bezpečnosti. |
| state | ne | Parametr, na ochranu před CSRF útoky, většinou obsahuje náhodnou hodnotu. Po úspěšném přihlášení uživatele provede CAAIS přesměrování na AIS a pošle tuto hodnotu v parametrech. AIS by měl následně ověřit, že obdržená hodnota odpovídá té, kterou odeslal při přesměrování uživatele na CAAIS. Slouží pro zvýšení bezpečnosti a umožňuje identifikovat odpověď na žádost o přihlášení. |

Základní struktura URL použitá při žádosti o přihlášení:

|  |
| --- |
| URL pro žádost o přihlášení |
| https://*caais-host*/oauth2/authorize?client\_id=*ais\_shortcut*&redirect\_uri=*redirect\_url* &scope=*openid%20profile*&response\_type=*code*&state=*state*&nonce=*nj66oa9le9d*  kde *caais-host* je placeholder pro URL daného prostředí (viz úvodní kapitola) |

## Rozhraní stránky AIS pro návrat po úspěšném přihlášení

Po úspěšném ověření CAAIS přesměruje uživatele zpátky na AIS URL, která byla poslána v parametru „redirect\_uri“. Do adresy doplní vygenerovaný kód, který AIS může následně použít na získání Access a ID tokenů. Souběžně s tím, pokud AIS poslal parametr „state“, CAAIS doplní ještě stejný paramert se stejnou hodnotou.

Základní struktura URL, na kterou CAAIS přesměruje uživatele po přihlášení:

|  |
| --- |
| URL pro přesměrování po přihlášení |
| https://*redirect\_uri*?code=*hodnota*&state=*identifikátor\_z\_požadavku* |

## Seznam atributů uživatele (identity) v ID tokenu

CAAIS může vracet v ID tokenu uživatele následující údaje o autentizovaném uživateli.

AIS definuje při žádosti o přihlášení parametr „scope“, skrze který může specifikovat údaje, které chce o uživateli získat. Jednotlivé hodnoty v parametru „scope“ jsou odděleny mezerou. Parametr „scope“ musí vždy obsahovat hodnotu „openid“.

Tabulka 2: Seznam atributů v ID tokenu

|  |  |  |  |
| --- | --- | --- | --- |
| Atribut | Claim v ID tokenu | Potřebný scope | Atribut z datového modelu |
| Příjmení | family\_name | profile | "Profil"."Fyzická osoba"."příjmení" (Profile.PhysicalPerson.lastName) |
| Jméno | given\_name | profile | "Profil"."Fyzická osoba"."jméno" (Profile.PhysicalPerson.firstName) |
| Datum narození | birthdate | birthdate |  |
| Místo narození | birthplace | birthplace |  |
| Země narození | country\_of\_birth | country\_of\_birth |  |
| Pseudonym | sub | oidc | "Mapování SeP"." SePBSI" (ServiceMapping.sepBsi) pro daný "Profil"."uživatelské jméno" (Profile.loginName), poznámka - BSI se generuje v CAAIS nové, nemigruje se z JIP/KAAS |
| PristupoveRole | access\_roles | profile | Seznam přístupových rolí do AIS přiřazených uživateli.  "Profil"."Přístupová role" (Profile.AccessRole)  pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role, dotahují se přes ně odpovídající přístupové role. Dále se dotahují i delegované přístupové role přes "Vazební profil".  V seznamu přístupových rolí se vrací pouze role pro daný AIS, do kterého se uživatel autentizuje. |
| role | role | profile | Kód přístupové role.  "Přístupová role"."zkratka" (AccessRole.shortcut) |
| CinnostniRole | activity\_roles | profile | Seznam činnostních rolí přiřazených uživateli.  "Profil"."Činnostní role" (Profile.ActivityRole) – pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role dotahují se přes ně odpovídající činnostní role a agendy. Dále se dotahují i delegované činnostní role a agendy přes "Vazební profil". |
| KodAgendy | agenda\_code | profile | Kód agendy činnostní role.  "Činnostní role"."Agenda"."kód" (ActivityRole.Agenda.code) |
| KodCinnostniRole | activity\_role\_code | profile | Kód činnostní role.  "Činnostní role"."kód" (ActivityRole.code) |
| Zkratka subjektu | legal\_entity\_shorcut | subject | "Subjekt"."zkratka" (Subject.shortcut) |
| IČO subjektu | lei | subject | "Subjekt"."ič" (Subject.identificationNumber) |
| Uživatelské jméno | username | profile | "Profil"."uživatelské jméno" (Profile.loginName) |
| Titul před jménem | degree\_before | profile | "Profil"."Fyzická osoba"."titul před" (Profile.PhysicalPerson.degreeBefore) |
| Titul za jménem | degree\_after | profile | "Profil"."Fyzická osoba"."titul za" (Profile.PhysicalPerson.degreeAfter) |
| Přístupové role | access\_roles | role | "Profil"."Přístupová role" (Profile.AccessRole) pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role, dotahují se přes ně odpovídající přístupové role. Dále se dotahují i delegované přístupové role přes "Vazební profil".  V seznamu přístupových rolí se vrací pouze role pro daný AIS, do kterého se uživatel autentizuje.  V atributu bude formát JSON, např. takto:  ""access\_roles"": [  {  ""access\_role\_code"": ""editor""  },  {  ""access\_role\_code"": ""spravce""  }  ] |
| Kód přístupové role | access\_role\_code | role | "Přístupová role"."zkratka" (AccessRole.shortcut) |
| Činnostní role | activity\_roles | role | "Profil"."Činnostní role" (Profile.ActivityRole) – pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role, dotahují se přes ně odpovídající činnostní role a agendy. Dále se dotahují i delegované činnostní role a agendy přes "Vazební profil".  V atributu bude formát JSON, např. takto:  {  ""activity\_roles"": [  {  ""agenda\_code"": ""K100"",  ""activity\_role\_code"": [  ""CR1111"",  ""CR2222""  ]  },  {  ""agenda\_code"": ""K101"",  ""activity\_role\_code"": [  ""CR3333"",  ""CR4444""  ]  }  ]  } |
| Kód agendy | agenda\_code | role | "Činnostní role"."Agenda"."kód" (ActivityRole.Agenda.code) |
| Kód činnostní role | activity\_role\_code | role | "Činnostní role"."kód" (ActivityRole.code) |
| Email | email | contact | "Profil"."email" (Profile.email) |
| Název subjektu | legal\_entity\_name | subject | "Subjekt"."název" (Subject.name) |
| Email subjektu | legal\_entity\_email | subject | "Subjekt"."Kontakt"."Email"."adresa" (Subject.Contact.Email.address) kde "Email"."Typ emailu"."název" (Email.EmailType.name) = "Oficiální" |
| Typ instituce | institution\_type | subject | "Subjekt"."Typ instituce"."kód" (Subject.InstitutionType.code) |
| Osoba ztotožněna | person\_identified | profile | "Profil"."Fyzická osoba"."osoba evidována v rob" (Profile.PhysicalPerson.personInRob) |
| Datum úmrtí | date\_of\_death | deathdate | "Profil"."Fyzická osoba"."datum úmrtí" (Profile.PhysicalPerson.deathDate) |
| Doklady | document\_ids | document | V CAAIS je pouze 1 doklad |
| Doklad (+ atribut Typ) | document\_id (+ atribut type) | document | "Profil"."Fyzická osoba"."číslo dokladu" (Profile.PhysicalPerson.documentId) a "Profil"."Fyzická osoba"."druh dokladu" (Profile.PhysicalPerson.documentType)  V atributu bude formát JSON, např. takto:  {  ""document\_ids"": [  {  ""type"": ""Občanský průkaz"",  ""document\_id"": ""111""  },  {  ""type"": ""Pas"",  ""document\_id"": ""222""  }  ]  } |
| Identifikátor OVM | public\_organization\_identifier | subject | "Subjekt"."kód ovm v rovm" (Subject.ovmInRovmCode) |
| Identifikátor SPUÚ | authorized\_private\_entity\_personal\_data\_user\_identifier | subject | "Subjekt"."kód spuú" (Subject.spuuCode) |
| Autorizační token | time\_limited\_id | role | Technický atribut pro ukládání tokenů (neuveden v DM) |

|  |
| --- |
| **Příklad Request** |
| *https://rest-openidconnectapi.caais-dev.cms2.cz/oauth2/authorize*  *?client\_id=oidcdebugger*  *&redirect\_uri=https://oidcdebugger.com/debug*  *&scope=openid profile birthdate birthplace country\_of\_birth subject subject contact deathdate document*  *&response\_type=code*  *&response\_mode=query*  *&state=eofxtp0lrx*  *&nonce=uyk9aalvwnb* |

## Získání tokenů

Ve chvíli, kdy má AIS k dispozici „code“ získaný po přihlášení uživatele, musí jej přeposlat na token endpoint na CAAIS, aby získal Access token a ID token. Získání musí proběhnout pomocí HTTP POST dotazu a AIS se musí autentizovat ověřovacím certifikátem. AIS pošle v dotazu:

* svoji zkratku
* obdrženou hodnotu „code“
* „redirect\_uri“, která byla použita při přihlášení uživatele.
* „grant\_type“ s hodnotou „authorization\_code“

Struktura dotazu vypadá následovně:

|  |
| --- |
| Struktura dotazu |
| POST http://cert-openidconnectapi.caais-test.ocp.cea01.dscen.cz/oauth2/token  Content-Type: application/x-www-form-urlencoded  grant\_type=authorization\_code&  code=*obdrzena\_hodnota\_code*&  client\_id=*AIS\_zkratka*&  redirect\_uri=*redirect\_uri* |
| **Příklad Request** |
| *POST https://cert-openidconnectapi.caais-dev.cms2.cz/oauth2/token HTTP/1.1*    *Accept-Encoding: gzip,deflate*    *Content-Type: application/x-www-form-urlencoded*    *Host: cert-openidconnectapi.caais-dev.cms2.cz*    *Accept-Encoding: gzip,deflate*    *Content-Type: application/x-www-form-urlencoded*    *Content-Length: 230*    *Host: cert-openidconnectapi.caais-dev.cms2.cz*    *Connection: Keep-Alive*    *User-Agent: Apache-HttpClient/4.5.5 (Java/11.0.22)*        *grant\_type=authorization\_code&code=BN9c3cg1HLAk9-deLaZrMKGVQp-zoccjYR-CHiSuIpkS8xrrC7VNvtXEqN880bJGW2gWhSh5OQIskjzEqfrtL1ILciY7Bt0KEmlE4ZyVzJbsUSakgT1yfveGLjD\_pEGA&client\_id=oidcdebugger&redirect\_uri=https://oidcdebugger.com/debug* |

CAAIS ověří obdržené údaje. Pokud jsou správné, odešle v odpovědi Access token a ID token. Odpověď může pak vypadat následovně:

|  |
| --- |
| Ukázka odpovědi |
| {  "access\_token": "*zakódovaný access token*",  "scope": "openid profile birthplace birthdate country\_of\_birth",  "id\_token": "*zakódovaný id token*",  "token\_type": "Bearer",  "expires\_in": 300  } |
| **Příklad Response** |
| *{*  *"access\_token": "eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiI3ZTM0OWU2OS1iOGQ1LTQwOWEtOWMyNC03NDA3N2JiMjk4MTAiLCJhdWQiOiJvaWRjZGVidWdnZXIiLCJuYmYiOjE3MTc3NDc1NjMsInNjb3BlIjpbImJpcnRoZGF0ZSIsImJpcnRocGxhY2UiLCJvcGVuaWQiLCJzdWJqZWN0IiwicHJvZmlsZSIsImNvbnRhY3QiLCJkb2N1bWVudCIsImNvdW50cnlfb2ZfYmlydGgiLCJkZWF0aGRhdGUiXSwiaXNzIjoiaHR0cHM6Ly9yZXN0LW9wZW5pZGNvbm5lY3RhcGkuY2FhaXMtZGV2LmNtczIuY3ovIiwiZXhwIjoxNzE3NzQ3ODYzLCJpYXQiOjE3MTc3NDc1NjMsImNsaWVudF9jZXJ0X3NoYTI1NiI6ImRXU2VXQlRraEQwdk15cVJHWW0xUjFNcEhSZ0psLTRDY3FTOURuaDBETlUifQ.jukXdUcqAWR351BD0nCBjb-aM1oPuhGBRwqcUC1vb9Q3wc6B7jgNUjef9YIg-Ta87pRP18-FnmZIOIkHdaWvPAPRJ5ld-f9ga6VSNty\_QmHB3LI3SN885\_kxR6-XzlUhtw7IHAWjnugfOVwDdR62MgMalwV2MjfH3EvUp9WYwgSqF1fyeBexW4WjEB4xL5xJUrH5QgU2z9oKPlzGB92NhhNjv-c9dG8Q59KyY15thvtuGzWgc2y1ZUtHZikqNG98ZB1Ip12kI6lTvpcRZHMrbhw6kYBLly2C2C4rxNyX-Hkt\_gtH6v8eB6JqaygPqyFpZebijGGaNmsCAUwHGsw0sg",*  *"refresh\_token": "zVGwm\_ugeq94Bdu2u-5Q868cIYpSDbU9mxwyz5TI1HiqpEmx8hQgvXaZE-lYIVX0Liw5P7aXP00ZzwBf5qXpVX9QRY2qdrYZxktoY5QRxnTidk2k28a-bQDmFybQQ\_sG",*  *"scope": "birthdate birthplace openid subject profile contact document country\_of\_birth deathdate",*  *"id\_token": "eyJhbGciOiJSUzI1NiJ9..j6pfDOHukAyHWZsE-BgIUVshCLpF1FkTNm1TPlPxl12IWhE1ZLl4FSYde4xeM2Lcz-zoSeVYXKJlKIM9hG1O0QITwDZ0cjPDm2Ip-hHU-cPkHpPeFLODt4Ac67TBwdRk9Q1XJQoNAQdzDBFFxMEt7\_PWo\_cnTQH7pjQJy0ht60AWUYoZatPzVpM6sYOSIIZ5hwnNS6lFgyJ4SVZ6egMtfA06aP23Pnw2-ExDc5wBV\_xtUIhVmaaiZb24u4pE7UPKH\_FOCYO76CEEYsLD3sBWctwqAGddzXyqjqd4NPuMEfkOnSGiuiqZ8s9KsuZ1nMGKCZyDZFtHTOTZqL90t9gbQg",*  *"token\_type": "Bearer",*  *"expires\_in": 299*  *}* |

|  |
| --- |
| Ukázka dekódovaného obsahu z Access tokenu |
| {  "sub": "f5df7c90-dd20-407a-8446-926cc81aeaf7",  "aud": "cert-client",  "nbf": 1650542033,  "scope": [  "openid profile birthplace birthdate country\_of\_birth"  ],  "iss": "http://localhost:9000",  "exp": 1650542333,  "iat": 1650542033,  "client\_cert\_sha256": "qJaNLoji-swhNsXzL2c\_o59PNNiD0bu6uCk45ZC2Ndc"  } |
| **Příklad dekódovaného obsahu z Access tokenu** |
| *{'sub': '7e349e69-b8d5-409a-9c24-74077bb29810', 'aud': 'oidcdebugger', 'nbf': 1717747563, 'scope': ['birthdate', 'birthplace', 'openid', 'subject', 'profile', 'contact', 'document', 'country\_of\_birth', 'deathdate'], 'iss': 'https://rest-openidconnectapi.caais-dev.cms2.cz/', 'exp': 1717747863, 'iat': 1717747563, 'client\_cert\_sha256': 'dWSeWBTkhD0vMyqRGYm1R1MpHRgJl-4CcqS9Dnh0DNU'}* |

|  |
| --- |
| Ukázka dekódovaného obsahu z ID tokenu |
| {  "sub": "CZ/ES/b5e81148-2bd1-4f44-ba75-0c0359d3be7d",  "family\_name": "Doe",  "given\_name": "John",  "birthplace": "Brno",  "birthdate": "2020-02-08",  "country\_of\_birth": "UK",  "aud": "ais-shortcut",  "azp": "ais-shortcut",  "iss": "https://caais-host",  "exp": 1650543833,  "iat": 1650542033,  "nonce": "xl3vfhfsos"  } |

|  |
| --- |
| **Příklad dekódovaného obsahu z ID tokenu** |
| *{'sub': '7e349e69-b8d5-409a-9c24-74077bb29810', 'birthdate': '1966-10-25', 'person\_identified': True, 'legal\_entity\_email': 'radnice@mestoholysov.cz', 'iss': 'https://rest-openidconnectapi.caais-dev.cms2.cz/', 'lei': '253367', 'public\_organization\_identifier': '00253367', 'azp': 'oidcdebugger', 'authorized\_private\_entity\_personal\_data\_user\_identifier': '', 'country\_of\_birth': 'Česko', 'exp': 1717749363, 'iat': 1717747563, 'degree\_after': 'PhD.', 'email': 'miluse@ficnarova.cz', 'document\_ids': {'document\_ids': [{'type': 'P', 'document\_id': '11111931'}]}, 'institution\_type': 6, 'given\_name': 'Miluše', 'nonce': 's7onzu01uve', 'degree\_before': 'PhDr.', 'aud': 'oidcdebugger', 'birthplace': 'Souňov', 'legal\_entity\_shorcut': 'HOLYSOV', 'family\_name': 'Ficnarová', 'legal\_entity\_name': 'Město Holýšov', 'username': 'miluse\_ficnarova'}* |

## Úroveň záruk (Level of Assurance)

V systému CAAIS je přiřazení úrovní záruk definováno pouze pro certifikované autentizační systémy (IdP) – např. NIA. Pokud se uživatel autentizuje pomocí NIA, vrací se v odpovědi přihlašovací metody do AIS taková úroveň LoA, kterou NIA předal.

Autentizuje-li se uživatel pomocí vnitřního systému CAAIS-IdP, vrací se v odpovědi vždy nejnižší úroveň LoA, podle toho, která byla použita v SAML (viz tabulka níže):

* http://eidas.europa.eu/NotNotified/LoA/low
* http://eidas.europa.eu/LoA/NotNotified/low“ (podle toho která hodnota byla použita v requestu).

Úroveň LoA znamená míru důvěryhodnosti, s jakou se uživatel autentizoval. Nejčastěji se používají úrovně nízká, značná a vysoká. V systému CAAIS se pracuje s těmito LoA:

Tabulka 3: Hodnoty LoA

|  |  |
| --- | --- |
| LoA | Standardizovaný identifikátor |
| nízká | http://eidas.europa.eu/NotNotified/LoA/low  http://eidas.europa.eu/LoA/low  http://eidas.europa.eu/LoA/NotNotified/low (hodnota někdy nesprávně používána zahraničními systémy, CAAIS ji také podporuje) |
| značná | http://eidas.europa.eu/NotNotified/LoA/substantial  http://eidas.europa.eu/LoA/substantial |
| vysoká | http://eidas.europa.eu/NotNotified/LoA/high  http://eidas.europa.eu/LoA/high |

Požadované LoA se uvádí v SAML requestu v atributu "AuthnContextClassRef". V atributu "Comparison" (hodnoty "exact", "minimum", "maximum" nebo "better") se pak definuje způsob porovnávání požadované LoA a dostupné LoA. Pro SAML requesty odesílané do systému CAAIS se doporučuje hodnota "minimum".

V SAML response se ve stejném atributu "AuthnContextClassRef" pak vyplní skutečné LoA podle způsobu autentizace uživatele.

# Rozšíření funkcionalit OIDC ve verzi 1.1

* Přidání dalších atributů do OIDC response podle seznamu atributů v legacy autentizačních službách

# Zkratky, pojmy, definice

|  |  |
| --- | --- |
| **Zkratka nebo pojem** | **Vysvětlení** |
| Access token | Token vydaný Autorizačním serverem – poskytuje uživatelské oprávnění. |
| AIFO | Agendový identifikátor fyzické osoby |
| AIS | Agendový informační systém |
| Autentizace | Ověření identity uživatele |
| Autorizace | Ověření přístupových oprávnění uživatele (často následuje po autentizaci). |
| CAAIS | Centrální autorizační a autentizační informační systém, náhrada JIP/KAAS. V OIDC vystupuje v roli Autorizačního serveru. |
| CAAIS-IdP | Interní Identity Provider v rámci systému CAAIS |
| Claim | Údaje o uživateli. |
| DB | Databáze |
| GUID | Globally unique identifier |
| ID token | Token vydaný Autorizačním serverem. Obsahuje vyžádané uživatelské údaje. |
| IdP | Identity Provider |
| JIP | Jednotný identitní prostor - zabezpečený adresář orgánů veřejné moci a uživatelských účtů úředníka, který je součástí systému |
| JSON | JavaScript Object Notation: textový formát dat |
| JWT | JSON Web Token: webový token, obsahující JSON data, jejich podpis a hlavičku – definovaný pomocí RFC 7519 standardu. |
| KAAS | Katalog autentizačních a autorizačních služeb |
| LoA | Level of Assurance = Úroveň záruk |
| OIDC | OpenId Connect  Protokol pro výměnu autentizačních a autorizačních dat |
| Query parametr | Parametr zasílaný v URL. |
| URL | Uniform Resource Locator |

# Přílohy

Dokument je bez příloh.