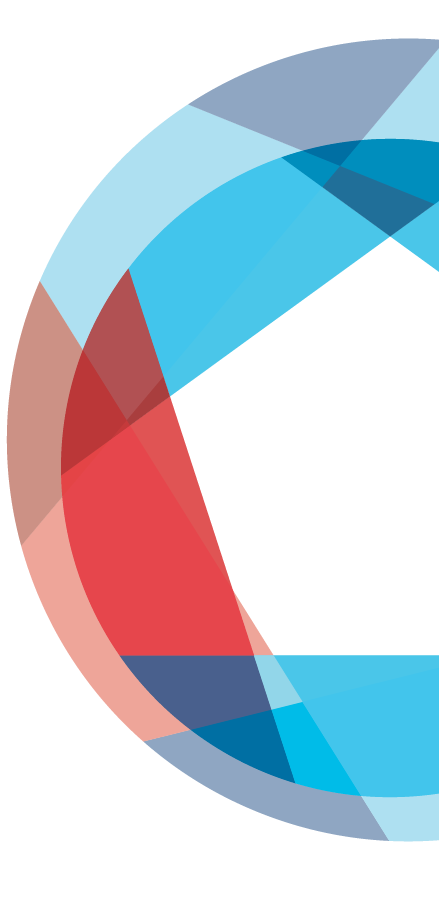
CAAIS: Autentizační webová služba – Procesní popis

Verze 1.0

10.5.2022



Zpracoval: Milan Babic

Obsah

[1. Úvod 4](#_Toc103111466)

[2. Autentizační služby CAAIS 5](#_Toc103111467)

[2.1. Typy autentizačních služeb 5](#_Toc103111468)

[2.2. Předpoklady pro využívání autentizačních služeb 5](#_Toc103111469)

[2.2.1 Registrace a konfigurace AIS v CAAIS 5](#_Toc103111470)

[2.2.2 Ověřovací certifikát 6](#_Toc103111471)

[2.2.3 Přístupové role pro AIS 6](#_Toc103111472)

[2.3. Zpracování osobních údajů 7](#_Toc103111473)

[3. Autentizační webová služba (klasická) 8](#_Toc103111474)

[3.1. Diagram procesu autentizace a autorizace 8](#_Toc103111475)

[3.2. Sekvenční diagram komunikace a předávání dat 11](#_Toc103111476)

[4. Přímá autentizační webová služba 14](#_Toc103111477)

[4.1. Diagram procesu autentizace a autorizace 15](#_Toc103111478)

[4.2. Sekvenční diagram komunikace a předávání dat 17](#_Toc103111479)

[5. Odhlášení uživatele z CAAIS nebo NIA 20](#_Toc103111480)

[5.1. Diagram procesu odhlášení 20](#_Toc103111481)

[5.2. Sekvenční diagram komunikace a předávání dat 21](#_Toc103111482)

[6. Zkratky, pojmy, definice 23](#_Toc103111483)

[7. Přílohy 24](#_Toc103111484)

Verze dokumentu

|  |  |  |  |
| --- | --- | --- | --- |
| **Verze** | **Stručný popis změn** | **Zpracoval** | **Datum** |
| 1.0 | Nový dokument | Milan Babic | 10.5.2022 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Úvod

Účelem tohoto dokumentu je popsat proces uživatelské autentizace do agendových informačních systémů (AIS), které jsou registrovány v systému CAAIS. Uživatel používá buď 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, nebo se uživatel ověřuje pomocí NIA.

Systémy AIS využívají volání autentizačních webových služeb systému CAAIS jednak pro ověření identity uživatele, kteří do AIS přistupují a jednak k načtení dat o tomto přihlašovaném uživateli a jeho subjektu.

Dále jsou zde popsány předpoklady, které musí AIS splnit, aby mohl autentizační služby volat.

# Autentizační služby CAAIS

## Typy autentizačních služeb

V systému CAAIS jsou implementovány následující typy autentizačních služeb:

* **(klasická) autentizační webová služba CAAIS** - neautentizované uživatele musí AIS nejdříve přesměrovat na přihlašovací stránku CAAIS-IdP, kde se následně po úspěšném ověření uživatele v další komunikaci předává **autentizační token**. Přesměrování z AIS do CAAIS a zpět je zde plně automatické.
* **přímá autentizační webová služba CAAIS** - pro neautentizované uživatele musí AIS nabízet odkaz na speciální přihlašovací stránku CAAIS-IdP, kde se následně po úspěšném ověření uživatele pro další komunikaci vygenerují **jednorázové přihlašovací údaje** (jméno + heslo), které musí uživatel ručně zadat do přihlašovací stránky AIS. V tomto případě není přesměrování z AIS do CAAIS a zpět automatické.

V obou případech tyto služby poskytují systémům AIS ověření uživatele buď přihlašovacími údaji pro modul CAAIS-IdP nebo pomocí NIA a dále obě vrací údaje o uživateli a subjektu, ve kterém je uživatel zařazen.

Liší se v jednotlivých krocích procesu autentizace a v požadovaných vstupních údajích předávaných v requestech.

## Předpoklady pro využívání autentizačních služeb

### 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:

* **Návratová URL po autentizaci** – návratová adresa AIS, kam je uživatel přesměrován po autentizaci ze strany AIS
* **URL pro odhlášení** - návratová adresa AIS, kam je uživatel přesměrován po odhlášení v CAAIS
* **Ověřovací certifikát** – AIS se při volání autentizační služby CAAIS musí autentizovat ověřovacím certifikátem (více viz kapitola 2.2.2.).

Může také pro daný AIS definovat další osoby do role garant AIS, který může následně také spravovat daný AIS v CAAIS.

### Ověřovací certifikát

AIS při volání autentizačních služeb používá ověřovací certifikát pro autentizaci vůči 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 (např. Běžný uživatel, Editor, Administrátor), 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 (OVM), které mají mít přístup do tohoto AIS. Subjektům mohou být přiděleny všechny tyto přístupové role nebo jen jejich podmnožina. 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.

Pozor - tyto přístupové role neodpovídají činnostním rolím, které se používají pro přidělování oprávnění k referenčním údajům v základních registrech.

## 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-IDP uloženy osobní údaje uživatelů, které jsou následně předávány systémům AIS.

# Autentizační webová služba (klasická)

Zjednodušený proces autentizační webové služby CAAIS je následující:

* Neautentizovaný uživatel je z AIS přesměrován do CAAIS.
* Uživatel si vybere způsob přihlášení.
* Pokud je vybráno ověření pomocí NIA, je uživatel přesměrován do NIA, kde si zvolí identifikační prostředek a jeho prostřednictvím prokáže svoji identitu.
  + Ověřený uživatel je přesměrován zpět do CAAIS.
* Pokud je vybráno ověření v CAAIS-IdP, zadá uživatel odpovídající přihlašovací údaje a CAAIS ověří jejich platnost v CAAIS-IdP.
  + Ověřený uživatel je poté přesměrován zpět do AIS.
  + Požadavek AIS je pak předán do autentizační webové služby CAAIS a v odpovědi jsou vráceny údaje o autentizovaném uživateli.

AIS musí tedy pro využívání tohoto typu služby na jedné straně implementovat podporu přesměrování neautentizovaných uživatelů do CAAIS a na straně druhé poskytnout webovou stránku pro akceptaci ověřeného uživatele z CAAIS.

Komunikace mezi systémy AIS a CAAIS musí být zabezpečena protokolem TLS.

## Diagram procesu autentizace a autorizace

Na následujícím diagramu je detailně popsán proces autentizace a autorizace.



1. Uživatel otevře webovou stránku AIS. Pokud systém AIS zjistí, že není uživatel přihlášen, je přesměrován na webovou stránku CAAIS, kde si uživatel zvolí způsob přihlášení.

Varianta **a)** Pokud si uživatel vybral přihlášení prostřednictvím NIA, provedou se následující kroky:

* + 2) Uživatel je přesměrován do NIA, kde si zvolí identifikační prostředek, pomocí něhož se ověří jeho identita a uživatel pak vybere údaje, které o něm mohou být předány do CAAIS.
  + 3) Uživatel je pak přesměrován zpátky do CAAIS spolu s vybranými osobními údaji.
  + 4) Z těchto údajů si systém CAAIS vytáhne atribut AIFO, pomocí kterého se pokusí vyhledat odpovídající uživatelský účet (profil) v CAAIS. Pokud je těchto účtu nalezeno více, uživatel si vybere ten, pod nímž se chce do AIS přihlásit.

Varianta **b)** Pokud si uživatel vybral přihlášení pomocí autentizačních metod v CAAIS-IdP, provedou se následující kroky:

* + 2) Uživatel vyplní své přihlašovací údaje.
  + 3) V systému CAAIS-IdP se ověří jejich správnost.
  + 4) Po úspěšné autentizaci systém CAAIS načte ze své DB informace o uživateli, subjektu (OVM/SPUÚ), ke kterému je přiřazen, a přidělených rolích.

Další kroky jsou již shodné:

1. Systém CAAIS ověří, že autentizační metoda vybraná uživatelem splňuje úroveň LoA, která je pro daný AIS nakonfigurována v CAAIS. Dále se v CAAIS na základě přístupových rolí přidělených uživateli ověří, zda je oprávněn přistoupit do AIS. Pokud ano, vygeneruje se v CAAIS pro uživatele autentizační token s omezenou dobou platnosti. Jinak se uživateli zobrazí hláška o zamítnutí přístupu.
2. Uživatel je přesměrován s tímto tokenem na definovanou adresu AIS (v konfiguraci AIS).
3. Autentizační modul AIS pak zavolá autentizační webovou službu CAAIS spolu s autentizačním tokenem pro načtení informací o uživateli.
4. Pokud systém CAAIS zjistí, že je token platný, předá zpět do AIS požadované informace o uživateli. Pokud je volaná správná verze služby, CAAIS v odpovědi předá osobní údaje uživatele podle § 56a odst. 3 zákona č. 111/2009 Sb., o základních registrech. Podle získaných údajů pak AIS rozhodne, zda umožní/neumožní přistup uživateli do AIS. Pokud je token neplatný, vrací se z CAAIS do AIS chybový kód.

## Sekvenční diagram komunikace a předávání dat

Na následujícím diagramu je detailně popsána komunikace mezi uživatelem a systémy AIS, CAAIS a NIA.



1. Uživatel se pokusí otevřít webovou stránku AIS. Pokud systém AIS zjistí, že uživatel již nemá aktivní session, přesměruje uživatele na CAAIS.
2. Na přihlašovací stránce CAAIS si uživatel zvolí způsob přihlášení.
3. Pokud bylo zvoleno přihlášení pomocí NIA provedou se tyto kroky:
4. Přesměrování uživatele do NIA.
5. Uživatel zde vybere identifikační prostředek, kterým chce prokázat svoji identitu.
6. Pomocí tohoto identifikačního prostředku se provede v NIA autentizace.
7. Uživatel vybere údaje, které o něm mohou být předány do CAAIS.
8. Přesměrování uživatele zpátky do CAAIS i s jeho údaji.
9. Systém CAAIS dle AIFO z těchto údajů nalezne ve své DB odpovídající uživatelské účty (profily) a pokračuje se dále na krok 5).
10. Pokud bylo zvoleno přihlášení pomocí autentizačních metod v CAAIS-IdP, provedou se tyto kroky:
11. Uživatel vyplní své přihlašovací údaje na přihlašovací stránce CAAIS-IdP.
12. V systému CAAIS-IdP se ověří správnost těchto údajů.
13. V CAAIS se provede kontrola autentizační metody, kterou vybral uživatel, zda splňuje úroveň LoA, která je pro daný AIS nakonfigurována v CAAIS.
14. V CAAIS se provede kontrola, že uživatel má dostatečná oprávnění pro přístup do AIS.
15. V CAAIS se vygeneruje autentizační token pro uživatele.
16. Do webového prohlížeče uživatele odešle systém CAAIS HTTP response s příslušným autentizačním tokenem a informací, že má být přesměrován na definovanou adresu AIS.
17. Uživatel je spolu s autentizačním tokenem přesměrován na tuto adresu AIS.
18. Autentizační modul AIS se pokusí autentizovat přistupujícího uživatele (kroky 11-16)
19. Autentizační modul AIS provolá synchronní autentizační službu CAAIS pro získání údajů uživatele. Parametrem volání je autentizační token.
20. V CAAIS se provede kontrola tokenu.
21. Pokud je token platný, předají se údaje uživatele do AIS a zneplatní se session uživatele.
22. Uživatel je pro daný AIS autorizován a má oprávnění pracovat s AIS.

Získaní údajů o uživateli z CAAIS může být neúspěšné z následujících příčin:

1. Pokud je token neplatný, vrací autentizační služba tuto chybu a AIS ji prezentuje hláškou o neúspěšném přihlášení.
2. Pokud je autentizační služba nedostupná, prezentuje to AIS jako hlášku "nedostupná autentizační služba".

# Přímá autentizační webová služba

Zjednodušený proces přímé autentizační webové služby CAAIS je následující:

* Neautentizovaný uživatel na přihlašovací stránce AIS klikne na odkaz a přejde na speciální stránku CAAIS, kde se generuje jednorázové přihlašovací jméno a heslo.
* Uživatel si vybere způsob přihlášení.
* Pokud je vybráno ověření pomocí NIA, je uživatel přesměrován do NIA, kde si zvolí identifikační prostředek a jeho prostřednictvím prokáže svoji identitu.
  + Ověřený uživatel je přesměrován zpět do CAAIS.
* Pokud je vybráno ověření v CAAIS-IdP, zadá uživatel odpovídající přihlašovací údaje a CAAIS ověří jejich platnost v CAAIS-IdP.
* Systém CAAIS v obou případech pak vygeneruje jednorázové přihlašovací údaje a zobrazí je uživateli.
* Uživatel zadá jednorázové přihlašovací údaje na stránce AIS.
* AIS předá požadavek s těmito údaji na autentizační službu CAAIS, kde se provede ověření a zpět do AIS se vrátí údaje o autentizovaném uživateli.
* Ověřený uživatel je poté přesměrován zpět do AIS
  + Požadavek AIS je pak předán do autentizační webové služby CAAIS a v odpovědi jsou vráceny údaje o autentizovaném uživateli.

AIS musí tedy pro využívání tohoto typu služby zobrazovat na přihlašovací stránce odkaz na speciální přihlašovací stránku CAAIS pro vygenerování jednorázových přihlašovacích údajů.

Komunikace mezi systémy AIS a CAAIS musí být zabezpečena protokolem TLS.

## Diagram procesu autentizace a autorizace



1. Uživatel otevře webovou stránku AIS, kde klikne na odkaz a přejde na speciální stránku CAAIS, kde se generují jednorázové přihlašovací údaje. Zde si uživatel zvolí způsob přihlášení.

Varianta **a)** Pokud si uživatel vybral přihlášení prostřednictvím NIA, provedou se následující kroky:

* + 2) Uživatel je přesměrován do NIA, kde si zvolí identifikační prostředek, pomocí něhož se ověří jeho identita a uživatel pak vybere údaje, které o něm mohou být předány do CAAIS.
  + 3) Uživatel je pak přesměrován zpátky do CAAIS spolu s vybranými osobními údaji.
  + 4) Z těchto údajů si systém CAAIS vytáhne atribut AIFO, pomocí kterého se pokusí vyhledat odpovídající uživatelský účet (profil) v CAAIS. Pokud je těchto účtu nalezeno více, uživatel si vybere ten, pod nímž se chce do AIS přihlásit.

Varianta **b)** Pokud si uživatel vybral přihlášení pomocí autentizačních metod v CAAIS-IdP, provedou se následující kroky:

* + 2) Uživatel vyplní své přihlašovací údaje.
  + 3) V systému CAAIS-IdP se ověří jejich správnost.
  + 4) Po úspěšné autentizaci systém CAAIS načte ze své DB informace o uživateli, subjektu (OVM/SPUÚ), ke kterému je přiřazen, a přidělených rolích.

Další kroky jsou již shodné:

1. Systém CAAIS ověří, že autentizační metoda vybraná uživatelem splňuje úroveň LoA, která je pro daný AIS nakonfigurována v CAAIS. Dále se v CAAIS na základě přístupových rolí přidělených uživateli ověří, zda je oprávněn přistoupit do AIS. Pokud ano, vygeneruje se v CAAIS jednorázové uživatelské jméno a heslo s omezenou dobou platnosti a zobrazí se uživateli. Jinak se uživateli zobrazí hláška o zamítnutí přístupu.
2. Uživatel tyto jednorázové údaje přepíše do přihlašovací stránky AIS a potvrdí přihlášení.
3. Autentizační modul AIS pak zavolá přímou autentizační webovou službu CAAIS spolu s jednorázovými přihlašovacími údaji pro načtení informací o uživateli.
4. Pokud systém CAAIS zjistí, že jsou jednorázové přihlašovací údaje platné, předá zpět do AIS požadované informace o uživateli. Pokud je volaná správná verze služby, CAAIS v odpovědi předá osobní údaje uživatele podle § 56a odst. 3 zákona č. 111/2009 Sb., o základních registrech. Podle získaných údajů pak AIS rozhodne, zda umožní/neumožní přistup uživateli do AIS. Pokud je token neplatný vrací se z CAAIS do AIS chybový kód.

## Sekvenční diagram komunikace a předávání dat

Na následujícím diagramu je detailně popsána komunikace mezi uživatelem a systémy AIS, CAAIS a NIA.



1. Uživatel si otevře přihlašovací stránku AIS.
2. Na přihlašovací stránce AIS klikne na odkaz a přejde na speciální stránku CAAIS, kde se generují jednorázové přihlašovací údaje.
3. Na přihlašovací stránce CAAIS si uživatel zvolí způsob přihlášení.
4. Pokud bylo zvoleno přihlášení pomocí NIA provedou se tyto kroky:
5. Přesměrování uživatele do NIA.
6. Uživatel zde vybere identifikační prostředek, kterým chce prokázat svoji identitu.
7. Pomocí tohoto identifikačního prostředku se provede v NIA autentizace.
8. Uživatel vybere údaje, které o něm mohou být předány do CAAIS.
9. Přesměrování uživatele zpátky do CAAIS i s jeho údaji.
10. Systém CAAIS dle AIFO z těchto údajů nalezne ve své DB odpovídající uživatelské účty (profily) a pokračuje se dále na krok 6).
11. Pokud bylo zvoleno přihlášení pomocí autentizačních metod v CAAIS-IdP, provedou se tyto kroky:
12. Uživatel vyplní své přihlašovací údaje na přihlašovací stránce CAAIS-IdP.
13. V systému CAAIS-IdP se ověří správnost těchto údajů.
14. V CAAIS se provede kontrola autentizační metody, kterou vybral uživatel, zda splňuje úroveň LoA, která je pro daný AIS nakonfigurována v CAAIS.
15. V CAAIS se provede kontrola, že uživatel má dostatečná oprávnění pro přístup do AIS.
16. V CAAIS se vygenerují jednorázové přihlašovací údaje s omezenou dobou platnosti a zobrazí se uživateli.
17. Uživatel tyto jednorázové přihlašovací údaje přepíše do přihlašovací stránky AIS a potvrdí přihlášení.
18. Autentizační modul AIS se pokusí autentizovat přistupujícího uživatele (kroky 11-16)
19. Autentizační modul AIS provolá synchronní autentizační službu CAAIS pro získání údajů uživatele. Parametrem volání jsou také ty jednorázové přihlašovací údaje zadané uživatelem.
20. V CAAIS se provede kontrola správnosti jednorázových přihlašovacích údajů.
21. Pokud jsou jednorázové přihlašovací údaje správné, předají se údaje uživatele do AIS a tyto jednorázové přihlašovací údaje se zneplatní.
22. Uživatel je pro daný AIS autorizován a má oprávnění pracovat s AIS.

Získaní údajů o uživateli z CAAIS může být neúspěšné z následujících příčin:

1. Pokud jsou jednorázové přihlašovací údaje neplatné, vrací autentizační služba tuto chybu a AIS ji prezentuje hláškou o neúspěšném přihlášení.
2. Pokud je autentizační služba nedostupná, prezentuje to AIS jako hlášku "nedostupná autentizační služba"

# Odhlášení uživatele z CAAIS nebo NIA

V případě, že uživatel provádí odhlášení v systému AIS (např. tlačítkem "Odhlásit se" nebo odkazem pro odhlášení), měl by systém AIS v tu chvíli z bezpečnostních důvodů volat rozhraní pro odhlášení poskytované systémem CAAIS. Pokud byl uživatel přihlášen přes NIA, systém CAAIS zařídí odhlášení i z tohoto systému.

Zjednodušený proces odhlášení je následující:

* Uživatel odhlašovaný v AIS je přesměrován na odhlašovací adresu CAAIS.
* Uživatel je odhlášen z CAAIS + z NIA, pokud byl přihlášen přes NIA.
* Uživatel je přesměrován zpět do AIS.
* Uživateli je v AIS zobrazena informace o úspěšném odhlášení.

Průběh odhlášení je následující. Uživatel je přesměrován z AIS na definovanou adresu CAAIS a zde dojde k odhlášení uživatele z CAAIS a případně také z NIA. Nakonec je uživatel přesměrován zpět do AIS, kde může být dokončeno jeho odhlášení např. notifikací o úspěšném odhlášení uživatele.

URL pro odhlášení, kam je uživatel přesměrován z CAAIS do AIS je definována v konfiguraci AIS v CAAIS (viz kapitola 2.2.1).

## Diagram procesu odhlášení



1. Uživatel v AIS zvolí odhlášení a následně je přesměrován do CAAIS. Systém CAAIS zjistí, jakým způsobem byl uživatel přihlášen.
2. Pokud byl uživatel přihlášen prostřednictvím NIA, provedou se kroky a) a b). Pokud nebyl přes NIA, pokračuje se krokem 3).
3. Uživatel je přesměrován do NIA, kde se provede odhlášení.
4. NIA přesměruje uživatele zpět do CAAIS.
5. Uživatel je odhlášen z CAAIS a přesměrován zpět na odhlašovací adresu AIS.

## Sekvenční diagram komunikace a předávání dat

Na následujícím diagramu je detailně popsána komunikace mezi uživatelem a systémy AIS, CAAIS a NIA.



1. Uživatel v AIS zvolí odhlášení a následně je přesměrován do CAAIS.
2. Systém CAAIS zjistí, jakým způsobem byl uživatel přihlášen. Pokud byl uživatel přihlášen prostřednictvím NIA provedou se následující kroky:
3. Uživatel je přesměrován do NIA.
4. Uživatel je odhlášen z NIA
5. Uživatel je přesměrován zpět do CAAIS.
6. Uživatel je odhlášen z CAAIS.
7. Uživatel je přesměrován zpět na odhlašovací adresu AIS.

# Zkratky, pojmy, definice

|  |  |
| --- | --- |
| **Zkratka/pojem** | **Vysvětlení** |
| 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 |
| CAAIS-IdP | Interní Identity Provider v rámci systému CAAIS |
| JIP | Jednotný identitní prostor - zabezpečený adresář orgánů veřejné moci a uživatelských účtů úředníka, který je součástí systému |
| KAAS | Katalog autentizačních a autorizačních služeb |
| LoA | Level of Assurance = Úroveň záruk |
| NIA | Národní bod pro identifikaci a autentizaci |
| OVM | Orgán veřejné moci |
| SPUÚ | Soukromoprávní uživatel údajů podle § 2 zákona č. 111/2009 Sb., o základních registrech |
| Subjekt | Orgány veřejné moci, soukromoprávní uživatelé údajů a jiné úřady nebo právnické osoby evidované v CAAIS. |
| Token | Slouží pro uložení a přenos autentizačních a autorizačních data, díky kterým je držiteli tohoto SW tokenu (nejde o HW zařízení) umožněno vstoupit do systém a provádět zde definované činnosti. |
| URL | Uniform Resource Locator |
| WS | Webová služba |

# Přílohy

Dokument je bez příloh.