DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

Centrální autentizační a autorizační systém (CAAIS)

Popis Centrálního autentizačního a autorizačního informačního systému

Centrální autorizační a autentizační informační systém (CAAIS) slouží k jednotné autentizaci a autorizaci uživatelů (single sign-on) státní správy do Agendových informačních systémů (AIS) a také ke správě a řízení uživatelských rolí v těchto AIS, které komunikují se systémem CAAIS. Postupně nahradí původní JIP/KAAS. Pozice CAAIS je zakotvena v § 56a zákona č. 111/2009 Sb., o základních registrech.

Výhody používání Centrálního autentizačního a autorizačního informačního systému

CAAIS pozvedá autentizační a autorizační služby na novou úroveň. Je koncepčně modernější a jeho architektura je sjednocena s prostředím Národní identitní autority, jejímž prostřednictvím se dá do systému i přihlašovat. CAAIS totiž funguje na principu tzv. federačního hubu, který umožňuje připojení dalších poskytovatelů identit (Identity Providerů).

V případě CAAIS ovšem nejde jen o dalšího poskytovatele identit. Systém usnadní všem administrátorům správu a přiřazování uživatelských rolí. Obsahuje komfortnější funkce, jako hromadné přiřazování rolí a vytváření šablon pro jejich správu v přehledném a responsivním uživatelském rozhraní. Pro plánovaný další rozvoj je vystaven ve škálovatelné modulární architektuře.

Na rozdíl od systému JIP/KAAS rozhoduje DIA o využívání bez licenčních omezení, což představuje finanční úsporu.

Současný stav

Systém CAAIS se skládá ze dvou modulů:

- CAAIS – vlastní systém uchovávající a poskytující autorizační údaje. Patří sem
  - uživatelské rozhraní (GUI) pro správu subjektů (alias úřadů, OVM/SPUÚ, právnických/fyzických osob), jejich AIS, uživatelů a jejich rolí pro přístupy do AIS
  - webové služby pro strojovou správu těchto údajů
  - rozhraní poskytující autorizační služby AIS
- CAAIS IdP – interní identity provider (poskytovatel identit) pomocí něhož se mohou uživatelé autentizovat. Podobnou funkci autentizace uživatele nabízí například systémy NIA, ISDS nebo bankovní identita.

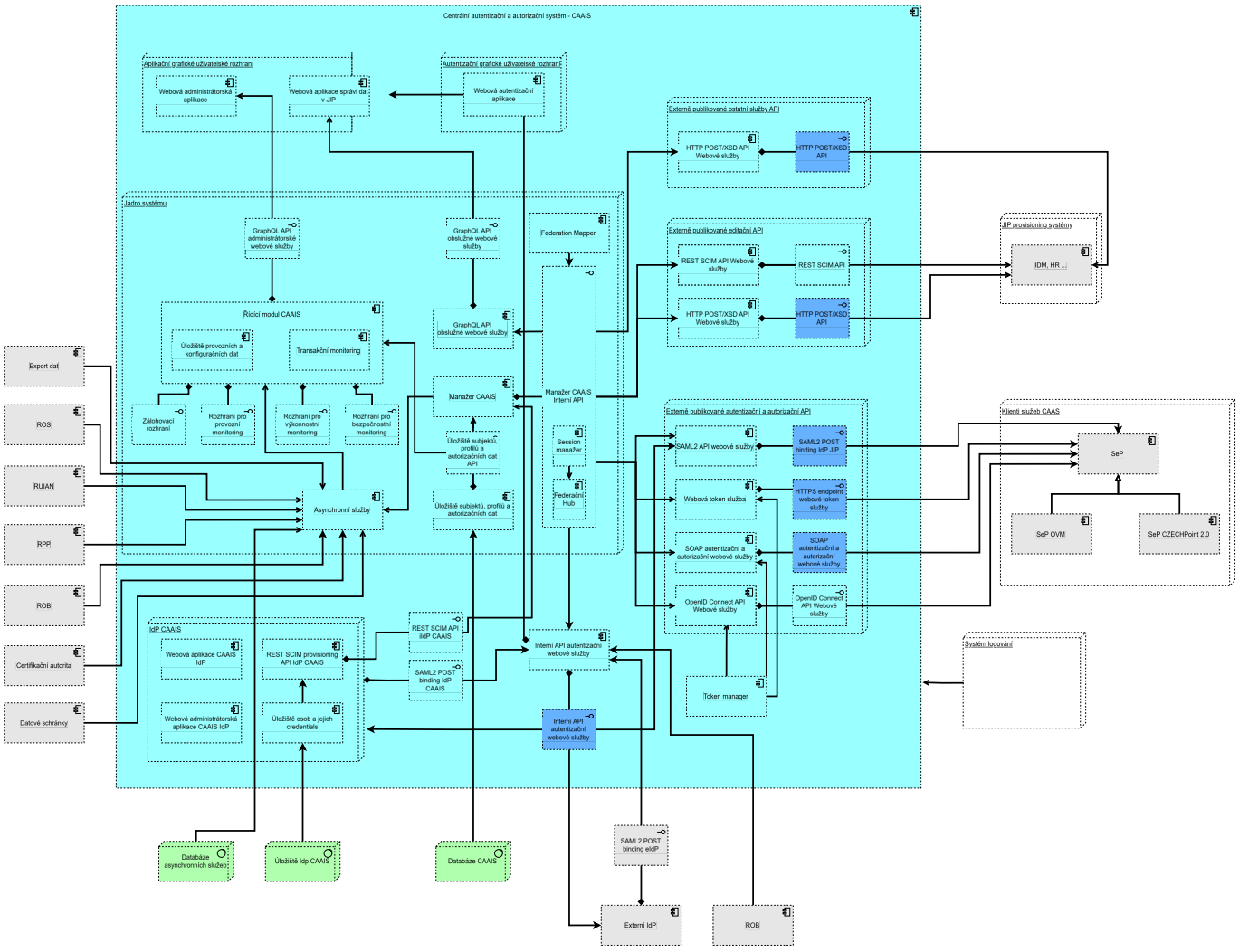
Aby uživatel mohl autorizaci pomocí CAAIS využívat, musí být v systému založen jeho profil (obvykle jiným uživatelem, který již v systému existuje – např. lokálním nebo národním administrátorem). Následně se uživatel může prostřednictvím CAAIS přihlašovat do AIS, ke kterým mu byla v CAAIS přiřazena role. Autentizuje se přitom prostřednictvím CAAIS IdP nebo NIA.

Přihlášení do CAAIS GUI se řídí stejnými pravidly, jako přihlášení k jiným AIS. Proto aby se mohl uživatel přihlásit do systému CAAIS GUI musí mít přiřazenu alespoň jednu z následujících rolí, které umožňují v systému CAAIS provádět různé akce:

- Běžný uživatel – vidí a spravuje pouze svoje vlastní údaje (tzv. svůj profil)
- Garant (správce) AIS – spravuje svoje AIS pod svým subjektem, konfiguruje přístupové role pro tyto AIS a ty přiděluje jednotlivým subjektům

- Lokální administrátor (LA) – spravuje data svého subjektu, jeho uživatele a jejich přístupové role do AIS. Podobně jako garant AIS může také i spravovat svoje AIS.
- Národní čtenář – vidí všechno, co Národní administrátor, ale nemá žádné právo editovat. Jedná se o roli určenou např. pro pracovníky service desku.
- Správce komunikační platformy – uživatel s tímto oprávněním má přístupnou záložku Novinky a nápověda. Může zde chystat články, které se pak zobrazují na přihlašovací stránce a v samotné aplikaci.
- Statutární zástupce – jeho hlavní funkcí je zakládat lokální administrátory. Může ale spravovat také ostatní uživatele aplikace CAAIS podobně jako Lokální administrátor. (Tato role se nepřiřazuje, ale je odrazem právního stavu.)
- Národní administrátor (NA) – může spravovat data všech subjektů v systému CAAIS.
- Systémový administrátor – spravuje konfiguraci různých systémových proměnných nutných pro správný běh systému CAAIS (např. různé číselníky, přístupová oprávnění do CAAIS, seznam IdP atd.)

Diagram popisu současného stavu



Systém CAAIS nabízí více alternativních protokolů, aby bylo možné implementovat ten, který nejlépe vyhovuje používanému frameworku AIS nebo zkušenostem.

1. OpenID Connect (OIDC),
2. Security Assertion Markup Language (SAML) 2.0,
3. JIP/KAAS (legacy).

Pokud aplikace dosud nepoužívala JIP/KAAS, či je vyvíjena aplikace nová, doporučuje se zvolit standardní protokoly OIDC nebo SAML.

Protokol JIP/KAAS (legacy) je zamýšlen pro stávající aplikace jako přímá náhrada služeb JIP/KAAS, kde stačí pouze změnit URL koncových bodů pro volání webových služeb bez nutnosti zasahovat do odladěného kódu aplikace. V dokumentaci je tento protokol popisován jako klasická a přímá autentizační webová služba.

Dále CAAIS poskytuje webové služby pro automatizaci správy uživatelů, což je výhodné pro větší organizace s vlastním Identity Management řešením. Tyto služby, v dokumentaci označované jako editační, odpovídají službám dostupným v JIP/KAAS.

V provozu jsou 3 prostředí.

1. **Školící prostředí** - https://caais-edu.gov.cz/login pro všechny uživatele, kteří si chtějí vyzkoušet práci s CAAIS. Lokální administrátoři si mimo jiné vyzkouší správu svého subjektu i uživatelů, garanti AIS zas přidělování přístupových práv ke svému systému. Školicí prostředí není napojeno na externí systémy, jako jsou základní registry a datové schránky. Data jsou do něj z produkčního prostředí přenášena zpravidla jednou týdně, což může znamenat, že poslední změny nebo aktualizace na produkci nebudou ve školicím prostředí po určitý čas zohledněny (včetně aktualizace agend a činnostních rolí z registru práv a povinností).
2. **Testovací prostředí** - https://caais-test-ext.gov.cz/login Testovací prostředí CAAIS je zamýšleno především pro potřeby integračních testů jednotlivých agendových informačních systémů (AIS) s CAAIS (navázání komunikace mezi AIS a CAAIS, úspěšné přihlášení uživatele, přenos autorizačních údajů v očekávaném rozsahu a formátu). Využívají jej proto především dodavatelé a techničtí provozovatelé AIS. Testovací prostředí není propojeno s Národní identitní autoritou (NIA), Datovými schránkami (ISDS), ani se Základními registry (ISZR). Počet záznamů v datové sadě testovacího prostředí je proti produkčnímu prostředí významně redukován.
3. **Produkční prostředí** - https://caais.gov.cz/login Plně funkční prostředí s napojením na externí systémy a provedenou migrací jednotlivých subjektů (OVM, SPUÚ) a stávajících agendových informačních systémů (AIS). Postupně nahradí původní JIP/KAAS.

Pravidla Centrálního autentizačního a autorizačního informačního systému

Aby bylo možné využití autentizačních a autorizačních služeb, je nutné splnit následující:

V rámci počátečního přenosu dat mezi JIP/KAAS a CAAIS již došlo k **migraci jednotlivých subjektů (OVM, SPUÚ)**. K subjektům byly zároveň dotaženy jejich působnosti dle Registru práv a povinností (RPP) a jejich statutární zástupci z registru osob a RPP. **Migrovány byly i stávající agendové informační systémy (AIS)**, ale v případě, **že AIS dříve nevyužíval JIP/KAAS, nebo je to nově vznikající AIS** je nutné jej v systému CAAIS nejdříve **zaregistrovat**, což provede v CAAIS **lokální administrátor** subjektu, jenž plní roli **správce daného AIS**.

Před prvním připojením AIS k CAAIS se velmi doporučuje nejprve otestovat integraci AIS proti testovacímu prostředí CAAIS. Pro získání přístupu na testovací prostředí je třeba zaslat stručnou žádost e-mailem na caais@dia.gov.cz.

I když došlo k počátečnímu přenosu dat mezi JIP/KAAS a CAAIS je nutné založit účet lokálního administrátora. Tento účet může vytvořit statutární zástupce, nebo lze vyplnit online formulář https://caais.gov.cz/la-create a výsledný XML soubor odeslat do datové schránky CAAIS ejmm527.

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.

Dalším krokem, který by měl lokální administrátor v systému CAAIS vykonat je migrace uživatelských profilů z JIP/KAAS. (Pokud jde o subjekt s jednotkami uživatelů, je lepší si je založit znovu ručně.) Před samotnou migrací je doporučeno provést ještě v JIP/KAAS revizi uživatelů a zablokovat ty, které není potřeba přenášet, třeba z důvodu, že už v organizaci nepracují. Doporučuje se nejdříve přenos nasimulovat.

Lokální administrátor následně provede pro AIS konfiguraci primárních údajů (návratová URL po autentizaci, URL pro odhlášení, ověřovací certifikát). Systém nabízí zpětně kompatibilní rozhraní s JIP/KAAS. Správci AIS nezadávají provozovatelům žádné změnové požadavky. Struktura dat i technické specifikace zůstávají stejné.

Administrátor může také pro daný AIS definovat další osoby do role garant AIS. Garant pak může také spravovat daný AIS v CAAIS.

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 a musí být vydaný podporovanou certifikační autoritou** (I.CA, PostSignum, eIdentity, NCA). V konfiguraci AIS v CAAIS může být zaregistrován pouze jeden ověřovací certifikát pro JIP/KAAS legacy, právě jeden podpisový a právě jeden šifrovací pro SAML a více certifikátů pro OIDC.

Budoucí stav

V budoucnu se očekává přechod všech současných systémů na CAAIS a v případě nově vznikajících, jejich přednostní implementace CAAIS. Rozšířením identitních prostředků se ulehčí práce úředníků.

U CAAIS se plánuje využití protokolu SCIM, jako další alternativy ke stávajícím.

Předpokládá se i úplné vypnutí systému JIP/KAAS, jakmile bude uveden do provozu systém Czech POINT 2.0 v rámci projektu „Generační obnova informačního systému Czech POINT“. Do té doby zůstává nadále v platnosti přihlašování výhradně pomocí JIP/KAAS u pracovníků kontaktních míst veřejné správy Czech POINT do rozhraní Czech POINT.

caais, jip, kaas