



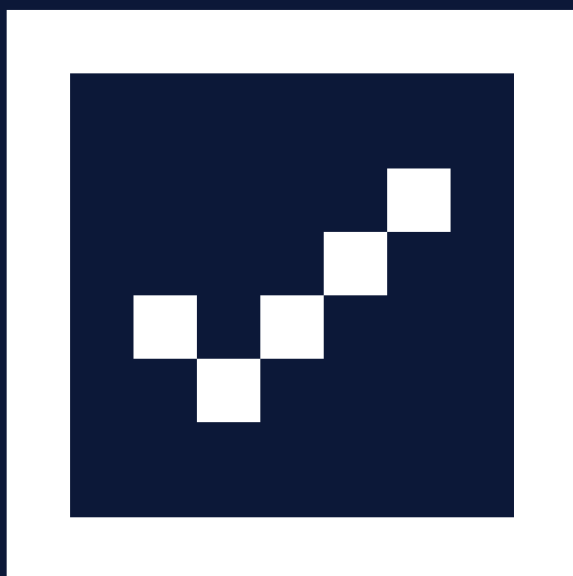
Financováno
Evropskou unií
NextGenerationEU



NÁRODNÍ
PLÁN OBNOVY



Digitální
a informační
agentura



CAAIS pro správce AIS

28. května 2026

Richard Chudoba; Vojtěch Art; Pavel Tesař



Rychlý přehled CAAIS

- generační obměna a náhrada za JIP/KAAS
- nevyhovující technologie a licenční podmínky; datová suverenita
- stejná filosofie, zpětná kompatibilita, nové možnosti
- rozvoj do budoucna

- **Protokoly:**
 - autentizace: JIP/KAAS (legacy), OIDC, SAML 2.0
 - správa: JIP/KAAS editační WS (legacy), SCIM (v přípravě)



Harmonogram

- 2024 pilot CAAIS
 - integrace pilotních AIS k CAAIS
- 2025 sunset JIP/KAAS, sunrise CAAIS
 - připojení nových AIS k JIP/KAAS není povolováno
 - integrace nových AIS s CAAIS
- 2026 rollout
 - rollout CAAIS na OVM (obce)
 - rollout CAAIS na AIS: přepojení stávajících integrací AIS z JIP/KAAS na CAAIS
- 2027 EoL JIP/KAAS
 - JIP/KAAS jen pro interní potřeby CzechPOINT



Nutnost nebo příležitost?

- systémy s připravovaným rozvojem
 - příležitost použít standardní protokoly namísto proprietárních (levnější, rychlejší)
 - příležitost využít nové funkcionality
 - příležitost pro nové rozvojové požadavky na autentizační a autorizační systém
- stabilizované systémy
 - nutnost z důvodu EoL JIP/KAAS
 - technicky snadné: jen konfigurační změna bez potřeby vývoje



Strategie

Sunrise & Sunset: Dočasný souběh

- po přechodnou dobu souběžné přihlašování uživatelů pomocí JIP/KAAS, tak pomocí CAAIS
- vhodná zejména pro větší systémy nebo systémy s velkým počtem uživatelů

+ není nutná těsná koordinace s uživateli
+ lepší uživatelská zkušenost
+ nižší riziko selhání

– vyžadována úprava AIS dodavatelem
– z důvodu napojení na dva systémy složitější správa a podpora

Big bang: Velký třesk

- náhlé (obvykle o víkendu) přepojení z JIP/KAAS na CAAIS
- vhodná:
 - pro malé systémy s omezeným počtem uživatelů
 - při generační obměně AIS
 - pragmaticky, pokud nelze provést ani drobný vývoj AIS

+ rychlé provedení změny
+ jednodušší správa a podpora (napojení jen na jeden systém)
+ při zachování JIP/KAAS legacy: jen záležitost konfigurace

– potřeba těsné koordinace s uživateli
– vyšší riziko výpadku

<https://docs.caais.gov.cz/integrace/integrace/2-jip-ais.html#strategie-prechodu>

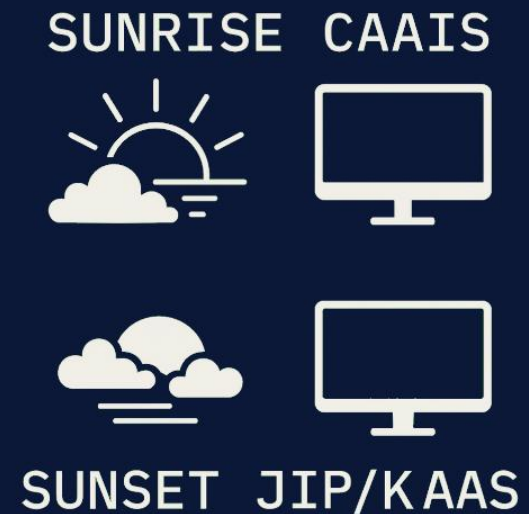


Strategie – Sunrise & Sunset

- **Souběžné přihlašování:** JIP/KAAS + CAAIS
- **Přechodné období:** 6–9 měsíců (sunrise/sunset)
- **Úprava AIS:** podpora více způsobů přihlášení
- **Rozsah změn:** při zachování JIP/KAAS spíše drobné úpravy

Obvyklý harmonogram

- 1. Úprava AIS, aby podporoval více autentizačních systémů současně.
 - 2. Integrace vývojového prostředí AIS proti integračnímu (testovacímu) CAAIS.
 - 3. Vytvoření konfigurace AIS v produkčním CAAIS a nastavení infrastruktury (firewall).
 - 4. Nasazení verze AIS s podporou JIP/KAAS a CAAIS do produkce.
= Počátek sunrise period pro CAAIS a sunset period pro JIP/KAAS.
 - 5. Komunikace s uživateli na počátku sunrise period CAAIS.
 - 6. Komunikace s uživateli před koncem sunset period JIP/KAAS.
 - 7. Ve vhodném okamžiku znepřístupnit či odstranit podporu JIP/KAAS.
- Kalendářně odhadujeme trvání kroků 1–4 na dva až čtyři měsíce, zejména kvůli rychlosti uzavření smlouvy na úpravy AIS a kapacit na straně dodavatele.





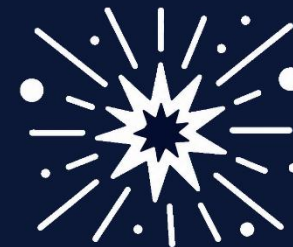
Strategie – Big Bang

- rychlé přepojení z JIP/KAAS na CAAIS (typicky přes víkend)
- **Zásadní podmínka:** komunikace s uživateli a jejich součinnost
- **Scénář 1:** zachování AIS, pouze změna konfigurace (JIP/KAAS legacy protokol)
- **Scénář 2:** nová verze AIS se standardy OIDC / SAML 2.0 místo JIP/KAAS protokolu

Obvyklý harmonogram

- 1. Integrace neprodukčního prostředí AIS proti integračnímu (testovacím) CAAIS.
 - 2. Vytvoření konfigurace AIS v produkčním CAAIS – zejména přístupové role.
 - 3. Komunikace s uživateli, aby si zajistili nastavení potřebných oprávnění (přístupových rolí) v CAAIS.
 - 4. Dokončení konfigurace AIS (certifikáty, endpointy) v produkčním CAAIS.
 - 5. Velký třesk. Změna konfigurace AIS; nastavení infrastruktury AIS (firewall)
 - 6. Dočasně zvýšené nároky na L1 podporu AIS a CAAIS.
- Kalendářně odhadujeme trvání na jeden až tři měsíce, zejména z důvodu komunikace s uživateli v kroku 3.

BIG BANG CAAIS





Nastavení AIS v CAAIS prakticky

- Konfigurace AIS přeneseny z JIP/KAAS do CAAIS včetně rolí k 06/2025.
- Konfigurace zatím neaktivní.

- 1. Požádejte svého lokálních administrátora CAAIS, aby vám založil účet v CAAIS a učinil vás správcem konfigurace vašeho AIS.
- 2. V spolupráci s dodavatelem ověřte a případně doplňte konfiguraci. Doplňte certifikáty(*).
- 3. Konfiguraci aktivujte.

(*) Klientský komerční certifikát od CA uznávané v rámci eIDAS.



Nastavení AIS v CAAIS prakticky

Konfigurace AIS

⚠ Vyplňte správně, nesrovnalosti mohou znemožnit činnost.

Povolené v doménách (2 vybraných) *

Typ volání SAML *

URL pro odhlášení

Návratová URL po autentizaci

Povolená návratová URL pro SAML a OIDC

Vyžadovat přiřazení přístupové role ⓘ

Formát SAML NameId *

SAML ALIASY

ZÁKLADNÍ ÚDAJE DOPLŇJÍCÍ ÚDAJE KONTAKTY CERTIFIKÁTY PŘÍSTUPOVÉ ROLE SUBJEKTY LOA

Autentizační certifikáty

1. certifikát

Sériové číslo	10abf3f4ae4ee5564
Stav	Aktivní
Certifikační autorita	C=CZ, OID.2.5.4.97=NTRCZ-26439395, O="První certifikační autorita, a.s.", CN=L.CA Public CA/RSA 06/2022
Platnost od	4. listopadu 2025 v 13:16:46
Platnost do	4. listopadu 2026 v 13:16:46

Šifrovací certifikáty

Podepisovací certifikáty



Uživatelská podpora

- Příručka pro systémové integrátory
<https://docs.caais.gov.cz/integrace/>
- Kontakt na podporu a zřízení přístupu
na integrační prostředí
caais@dia.gov.cz
- Součinnost při oslovení uživatelů





Známé situace a jejich řešení

- **AIS zapisuje auditní záznamy**
netřeba řešit, váží se na identitu v autentizačním systému
- **Uživatel má rozpracované workflow**
dokončí pod identitou, kde započalo
- **AIS váže své údaje k uživateli**
současné přihlášení uživatele k JIP/KAAS a CAAIS ke spárování údajů (např. při prvním přihlášení přes CAAIS)



Shrnutí

- Generační obměna a náhrada za JIP/KAAS



- Strategie: Sunrise & Sunset × Big Bang
- Integrační příručka: <https://docs.caais.gov.cz/integrace/>



CALL FOR ACTION

NYNÍ

- Stát se správcem konfigurace AIS v CA AIS – do konce Q2 2026
- Vstoupit v komunikaci s dodavatelem AIS: Rozhodnutí ohledně strategie přechodu a autentizačního protokolu – nejpozději Q3 2026

NÁSLEDNĚ

- Dodavatel může požádat o přístup k integračnímu prostředí e-mailem na caais@dia.gov.cz
- Pomůžeme s oslovením uživatelů ke správnému nastavení rolí



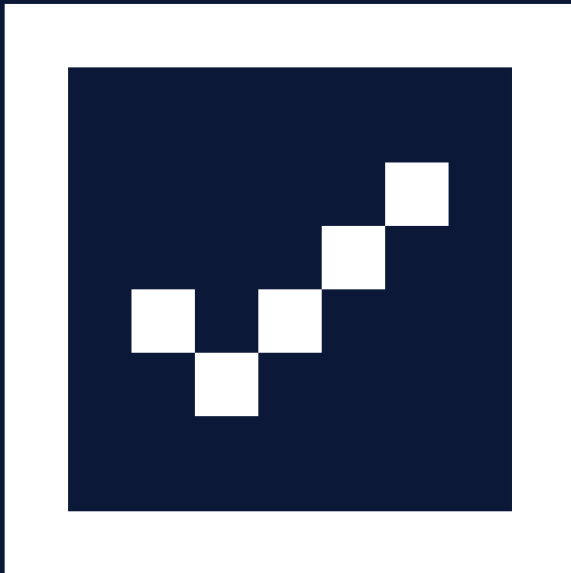
Financováno
Evropskou unií
NextGenerationEU



NÁRODNÍ
PLÁN OBNOVY



Digitální
a informační
agentura



Děkujeme za pozornost

Richard Chudoba; Vojtěch Art; Pavel Tesař