

Provozní podmínky e-INFRA CZ AAI

Záznam o změnách:

verze	datum	změny
1.0.1	2026-01-27	Aktualizace čísla normy ISO/IEC v části 1.6 z 27001:2014 na 27001:2023
1.0.0	2025-05-20	První verze

1. Úvod	5
1.1. Definice e-INFRA CZ AAI	5
1.2. Vymezení základních pojmů	5
1.3. Provozovatel e-INFRA CZ AAI	6
1.4. Provozovatelé Služeb	6
1.5. Uživatelé e-INFRA CZ AAI	6
1.5.1. Úrovně uživatelů	6
1.6. Technické podmínky provozu e-INFRA CZ AAI	7
1.7. Organizační podmínky provozu e-INFRA CZ AAI	7
2. Zpracování osobních údajů	8
2.1. Předávání osobních údajů službám	8
3. Životní cykly	9
3.1. Životní cyklus uživatelského účtu a členství ve virtuálních organizacích	9
3.1.1. Registrace (přihláška) do virtuální organizace	9
3.1.2. Aktivní členství	9
3.1.3. Neaktivní členství	9
3.1.4. Zánik členství	10
3.1.5. Životní cyklus v hierarchických virtuálních organizacích	10
3.1.6. Zánik uživatelského účtu	10
3.1.7. Životní cyklus členství ve společné VO e-INFRA CZ	10
3.2. Životní cyklus virtuální organizace	10
3.2.1. Vytvoření virtuální organizace	10
3.2.2. Provoz virtuální organizace	11
3.2.3. Zánik virtuální organizace	11
3.3. Životní cyklus skupiny	11
3.3.1. Vytvoření skupiny	11
3.3.2. Provoz skupiny	12
3.3.3. Zánik skupiny	12
3.4. Životní cyklus členství ve skupině	12
3.4.1. Vznik členství ve skupině	12
3.4.1.1. Vznik přímého členství	12
3.4.1.2. Vznik nepřímého členství	12
3.4.2. Aktivní členství ve skupině	12
3.4.3. Neaktivní členství ve skupině	13
3.4.4. Zánik členství ve skupině	13
3.5. Životní cyklus servisního účtu	13
3.5.1. Vytvoření servisního účtu	13
3.5.2. Správa servisního účtu	13
3.5.3. Zánik servisního účtu	14
3.6. Životní cyklus Facility	14
3.6.1. Vytvoření Facility	14
3.6.2. Provoz Facility	14
3.6.3. Zánik Facility	15
4. Práva a povinnosti	16

4.1. Uživatelé	16
4.2. Provozovatele e-INFRA CZ AAI	16
4.3. Uživatelé s vyšším oprávněním	16
4.3.1. Správce virtuální organizace	16
4.3.2. Správce služby	17
4.3.3. Vlastníka servisního účtu	17
5. Podmínky připojování Služeb	19
6. Poskytování virtuální organizace	20
7. Závěrečná ustanovení	21

1. Úvod

1.1. Definice e-INFRA CZ AAI

Autentizační a autorizační infrastruktura e-infrastruktury e-INFRA CZ (dále jen **e-INFRA CZ AAI**) je určená pro správu uživatelských účtů a jejich bezpečné ověřování (autentizaci) a schvalování (autorizaci) při přístupu ke službám připojeným k e-INFRA CZ AAI.

Uživatelé mohou díky e-INFRA CZ AAI využívat služeb e-INFRA CZ bez potřeby vytvářet nové účty pro každou jednotlivou službu. Autentizace a autorizace je řízena centrálně, což zvyšuje bezpečnost a uživatelský komfort. Tím je zajištěno bezpečné a pohodlné sdílení a používání vědeckých zdrojů mezi různými institucemi na národní i mezinárodní úrovni.

Služby mohou díky e-INFRA CZ AAI snadno řídit přístup uživatelů a implementovat [Podmínky přístupu k e-infrastruktuře e-INFRA CZ \(Access Policy & Acceptable Use Policy\)](#). Služby se mohou rozhodnout nevyužívat AAI a řešit autentizaci a autorizaci jiným vhodným způsobem.

e-INFRA CZ AAI je vybudována podle mezinárodního doporučení [AARC Blueprint Architecture](#) a poskytuje následující funkce:

- registraci uživatelů,
- registraci služeb,
- správu informací o uživateli,
- správu informací o službách,
- řízení přístupu uživatelů ke službám,
- řízení vydávání informací o uživateli službám,
- překlad mezi různými autentizačními protokoly (SAML2, OIDC, OAuth 2.0),
- spojení více různých způsobů autentizace jednoho uživatele do jednoho účtu.

e-INFRA CZ AAI je určena uživatelům definovaným v [sekci 1.5.](#) a organizacím provozujícím služby definovaným v [sekci 1.4.](#)

1.2. Vymezení základních pojmů

Pojmy **e-INFRA CZ** a **Provozovatelé konsorcia e-INFRA CZ** jsou definovány v dokumentu [Podmínky přístupu k e-infrastruktuře e-INFRA CZ](#)

Virtuální organizace (dále jen **VO**) je skupina uživatelů, která má stanovená pravidla pro členství a životní cyklus.

V hierarchii VO se nadřazená VO nazývá **rodičovská VO** a podřazená VO se nazývá **členská VO**.

Služba je instance softwarového systému, ke které mohou uživatelé přes síť přistupovat a používat ji. Služba může mít webové uživatelské rozhraní, ale může být přístupná i jinými protokoly, např. SSH, NFS, S3.

Uživatel je definován v [sekci 1.5.](#)

Uživatelský účet je buď reprezentace fyzické osoby (Uživatele e-INFRA CZ AAI) nebo reprezentace neosobního (obvykle strojového) přístupu (tzv. **servisní účet**).

1.3. Provozovatel e-INFRA CZ AAI

Provozovatelem e-INFRA CZ AAI je CESNET, zájmové sdružení právnických osob, které bylo provozem pověřeno na základě dohody [Provozovatelů konsorcia e-INFRA CZ](#).

1.4. Provozovatelé Služeb

Provozovatelem každé Služby připojené k e-INFRA CZ AAI musí být vždy organizace s právní subjektivitou (právnická osoba). Provozovatel Služby zodpovídá za její provoz.

Přístup uživatele ke Službám se řídí podmínkami přístupu, které pro každou službu stanovuje její provozovatel. Podmínky přístupu k dané Službě musí její provozovatel zveřejnit na svých webových stránkách, popř. na webových stránkách služby.

1.5. Uživatelé e-INFRA CZ AAI

Uživatelem je fyzická osoba, která se zaregistruje do e-INFRA CZ AAI.

1.5.1. Úrovně uživatelů

e-INFRA CZ AAI rozlišuje dvě úrovně uživatelů, podle kterých mohou služby řídit přístup uživatelů ke službě:

Registrovaným uživatelem může být kdokoliv, kdo je schopen autentizovat se některým z podporovaných způsobů a zaregistrovat si uživatelský účet.

Podporované způsoby autentizace jsou:

- účet v organizaci zapojené do české akademické federace identit eduID.cz
- účet v organizaci zapojené do mezinárodní inter-federace eduGAIN
- vybrané účty nezaručující skutečnou identitu osoby, např.: ORCID, MojeID, Microsoft, Apple, Google, LinkedIn, GitHub
- autentizační mechanismus provozovaný e-INFRA CZ.

Oprávněným uživatelem e-INFRA CZ může být:

- zaměstnanec a student následujících typů organizací registrovaných v České republice:
 - veřejné, státní i soukromé základní, střední i vysoké školy,
 - Akademie věd ČR a jí zřizované organizace,
 - výzkumné organizace ve smyslu zákona č. 130/2002 Sb., o podpoře výzkumu, experimentálního vývoje a inovací z veřejných prostředků a s pravidly veřejné podpory (dále jen **zákon č. 130/2002**),
 - další organizace zřízené za účelem realizace vědecké, výzkumné, vzdělávací, kulturní, vývojové nebo inovační činnosti. V takovém případě je příslušná organizace povinna zajistit, aby její zaměstnanci e-infrastrukturu využívali pouze v souvislosti s těmito výše uvedenými činnostmi a v souladu zejména se zákonem č. 130/2002 Sb.,
- zaměstnanec nebo student zahraniční organizace, splňující podmínky definované výše pro národní uživatele. V případě těchto uživatelů mohou být uplatněny dodatečné individuálně stanovené podmínky přístupu.

- osoba, která není zaměstnancem žádného z výše uvedených typů organizací, pokud používá e-infrastrukturu výhradně k vědecké, výzkumné, vzdělávací, vývojové nebo inovační činnosti ve smyslu zákona č. 130/2002 Sb.

Oprávněnost uživatele je pravidelně kontrolována a e-INFRA CZ AAI vydává službám příznak, zda má uživatel úroveň oprávněného uživatele, či ne.

Příznak oprávněného uživatele získají automaticky uživatelé, kteří podle pravidel federace eduID.cz spadají do [Research & Education](#) komunity a autentizují se do e-INFRA CZ AAI účtem z organizace zapojené do federace eduID.cz.

Další uživatelé, kteří mohou být oprávněným uživatelem, ale kteří nezískají příznak oprávněného uživatele automaticky, o něj mohou požádat.

Na příznak oprávněného uživatele není právní nárok a o jeho přidělení rozhoduje ve sporných případech provozovatel e-INFRA CZ AAI.

1.6. Technické podmínky provozu e-INFRA CZ AAI

1. e-INFRA CZ AAI je poskytována v „best effort“ režimu bez záruky konkrétní dostupnosti, předpokládaná dostupnost je 99% času;
2. provozovatel e-INFRA CZ AAI vynakládá veškeré možné úsilí, aby e-INFRA CZ AAI byla dostupná s minimálními výpadky, a za tímto účelem implementuje opatření pro zálohování a obnovu;
3. provozovatel e-INFRA CZ AAI má zavedený systém řízení bezpečnosti informací (ISMS), je držitelem certifikace dle ČSN EN ISO/IEC 27001:2023;
4. všechny časové údaje v e-INFRA CZ AAI jsou uváděny ve středoevropském časovém pásmu.

1.7. Organizační podmínky provozu e-INFRA CZ AAI

1. Dokumentace k e-INFRA CZ AAI je dostupná na adrese <https://docs.e-infra.cz> a uživatel je povinen ji prostudovat před kontaktováním podpory.
2. Uživatelská podpora je dostupná na adrese support@e-infra.cz a korespondence je zaznamenávána v systému řízení požadavků.
3. Požadavky jsou vyřizovány v pracovní dny v době od 9:00 do 17:00 s reakční dobou zpravidla do konce následujícího pracovního dne.
4. Provozovatel pravidelně provádí aktivity plánované údržby s cílem zvyšovat kvalitu poskytovaných služeb a udržení množství výpadků na minimum, a bude je provádět primárně mimo pracovní hodiny v době 17:00 - 9:00.

2. Zpracování osobních údajů

Sbírané osobní údaje a jejich zpracování v e-INFRA CZ AAI se řídí dle dokumentu [Informace o zpracování osobních údajů v e-INFRA CZ](#). Dále pro zpracování osobních údajů platí:

1. uživatel při registraci a následné autentizaci do e-INFRA CZ AAI předává svoje osobní údaje provozovateli e-INFRA CZ AAI
2. zpracování osobních údajů v e-INFRA CZ AAI se řídí dle pravidel jednotlivých virtuálních organizací, ve kterých je uživatel členem
3. při registraci do virtuální organizace „e-INFRA CZ“, reprezentující všechny uživatele e-infrastruktury e-INFRA CZ, jsou osobní údaje předány Provozovatelům konsorcia e-INFRA CZ, kteří jsou společným správcem osobních údajů
4. při registraci do jiných virtuálních organizací je uživatel vždy v přihláškovém formuláři upozorněn, která organizace (právnícká osoba) je v dané virtuální organizaci správcem osobních údajů
5. osobní údaje členů virtuální organizace jsou přístupné správcům virtuální organizace a správcům skupin v rámci stejné virtuální organizace. Správcem virtuální organizace nebo skupiny může být kterýkoliv z uživatelů, aniž by musel být členem dané VO nebo skupiny.
6. osobní údaje jsou zpracovávány po dobu existence uživatelského účtu, není-li výslovně uvedeno jinak (následně jsou osobní údaje smazány či anonymizovány)
7. osobní údaje uživatelů e-INFRA CZ AAI jsou zpracovávány výlučně na území České republiky

2.1. Předávání osobních údajů službám

Za správu osobních údajů uvnitř každé služby je vždy odpovědný provozovatel dané služby ve smyslu sekce [1.4](#).

Provozovatel e-INFRA CZ AAI uvolňuje provozovateli dané služby ty osobní údaje, které jsou potřebné pro poskytnutí služby uživateli. Jsou-li takto předávány osobní údaje jinému správci osobních údajů, je uživatel na tuto skutečnost upozorněn při žádosti o přístup ke službě (v závislosti na technických možnostech služby buď při autentizaci uživatele ke službě, příp. při registraci do skupiny, které je služba zpřístupněna).

3. Životní cykly

3.1. Životní cyklus uživatelského účtu a členství ve virtuálních organizacích

Fyzická osoba uživatele je v e-INFRA CZ AAI reprezentována uživatelským účtem. Na uživatelský účet je navázáno jedno nebo více členství ve virtuálních organizacích.

Uživatelský účet vzniká při registraci do první virtuální organizace.

Speciální místo mezi virtuálními organizacemi zaujímá VO „e-INFRA CZ“, která je určena pro všechny uživatele e-infrastruktury e-INFRA CZ a je vrchní rodičovskou VO v hierarchii.

Každé členství ve virtuální organizaci má vlastní životní cyklus definovaný správcem dané virtuální organizace. Životní cyklus členství ve virtuální organizaci lze rozdělit do několika fází, které odrážejí proces registrace, získání přístupu ke službám, jejich využívání, kontrolu členství a případné ukončení používání. Tento cyklus je popsán v následujících krocích:

3.1.1. Registrace (přihláška) do virtuální organizace

1. přihlášku do virtuální organizace uživatel podává vyplněním a odesláním registračního formuláře (přihlášky)
2. přihláška může být podle nastavení virtuální organizace buď schválená automaticky, nebo zásahem správce
3. po schválení přihlášky uživateli vzniká aktivní členství v dané virtuální organizaci

3.1.2. Aktivní členství

1. po dobu aktivního členství uživatel může využívat služby zpřístupněné dané virtuální organizaci
2. doba platnosti aktivního členství se nastavuje individuálně pro každou virtuální organizaci (např. jeden rok, dva roky od posledního použití, nebo ručně řízené správcem)
3. před vypršením doby platnosti aktivního členství může být uživateli zasláno upozorněním s odkazem na žádost o prodloužení (dle nastavení virtuální organizace)

3.1.3. Neaktivní členství

1. neaktivní členství může být způsobeno:
 - vypršením doby platnosti aktivního členství
 - zablokováním členství ve VO z bezpečnostních důvodů
2. po dobu neaktivního členství může mít uživatel omezený přístup ke službám zpřístupněným dané virtuální organizaci. Osobní data a nastavení vztahující se k dané virtuální organizaci zůstávají zachována

3.1.4. Zánik členství

1. členství uživatele ve virtuální organizaci zaniká odebráním uživatelského účtu z virtuální organizace, které může proběhnout automaticky nebo zásahem správce
2. zánikem členství dochází ke smazání osobních dat a nastavení vztahujících se k dané virtuální organizaci

3.1.5. Životní cyklus v hierarchických virtuálních organizacích

1. virtuální organizace mohou tvořit hierarchii
2. registrací do členské virtuální organizace automaticky vzniká členství v rodičovské virtuální organizaci
3. členství uživatele v členské VO se řídí jejím životním cyklem. Životní cyklus členů rodičovské VO se řídí podle životních cyklů podřízených členských VO následujícím způsobem:
 - a. pokud je uživatel aktivním členem alespoň jedné z podřízených členských VO, je aktivním členem rodičovské VO
 - b. pokud uživatel nemá aktivní členství v žádné z podřízených členských VO v hierarchii, jeho životní cyklus v rodičovské VO se řídí jejím životním cyklem

3.1.6. Zánik uživatelského účtu

1. pokud uživatel není členem ani v jedné virtuální organizaci, bude jeho uživatelský účet po uplynutí doby šesti měsíců smazán

3.1.7. Životní cyklus členství ve společné VO e-INFRA CZ

1. členem VO e-INFRA CZ může být libovolný registrovaný uživatel e-INFRA CZ AAI
2. společná VO e-INFRA CZ je rodičovskou hierarchickou VO a životní cyklus členství se řídí pravidly dle sekce [3.1.5](#)
3. členství uživatelů ve VO e-INFRA CZ, která nejsou ovlivněna členstvím v podřízených členských VO dle bodu [3.1.5](#), jsou platná 2 roky od registrace do VO e-INFRA CZ nebo od okamžiku ztráty posledního aktivního členství v některé z podřízených členských VO, podle toho, co nastalo později
4. uživatelé, kterým vyprší aktivní členství ve VO e-INFRA CZ během následujících 2 měsíců, nebo již vypršelo, mají možnost si požádat o jeho prodloužení, resp. opětovnou aktivaci a to na další 2 roky od schválení takové žádosti

3.2. Životní cyklus virtuální organizace

3.2.1. Vytvoření virtuální organizace

Virtuální organizace (VO) je struktura vytvořená v rámci e-INFRA CZ AAI, která umožňuje sdružovat a spravovat uživatele, služby a zdroje pro specifický účel. Slouží zejména organizacím a komunitám z akademického, výzkumného nebo vzdělávacího prostředí, které potřebují bezpečně sdílet a využívat data, nástroje a výpočetní kapacity. VO umožňuje

snadnou koordinaci zdrojů, správu uživatelských účtů a nastavování přístupových oprávnění, což podporuje efektivní spolupráci na výzkumných iniciativách.

- podmínky pro vytvoření VO jsou uvedeny v sekci [Poskytování virtuální organizace](#)
- VO vytváří provozovatel e-INFRA CZ AAI na žádost žadatele
- žadatel musí stanovit dobu potřeby VO, nebo bude nastaveno na dobu neurčitou s pravidelnou revizí
- VO může být vytvořena až po splnění souvisejících povinností - dodržení interních pravidel pro životní cyklus služby, uzavření smlouvy o zpracování osobních údajů s provozovatelem e-INFRA CZ AAI apod.

3.2.2. Provoz virtuální organizace

- v rámci provozu VO správce spravuje členství a nastavení VO dle svých potřeb a možností systému
- správce VO domlouvá zpřístupnění služeb zapojených do e-INFRA CZ členům své virtuální organizace s příslušnými správci služeb
- správce VO může omezit přístup ke službě na konkrétní skupiny uživatelů definované v rámci VO

3.2.3. Zánik virtuální organizace

- pokud správce VO nestanoví pevnou dobu potřebnosti VO, tak je potřebnost kontrolována každý rok. Pokud nebude reagovat na výzvu provozovatele e-INFRA CZ AAI, bude VO zrušena po uplynutí doby dvou měsíců.
- VO může být zrušena na žádost správce kdykoliv
- VO ruší provozovatel e-INFRA CZ AAI na žádost správce
- VO může být zrušena až po splnění souvisejících povinností - dodržení interních pravidel pro životní cyklus služby, ukončení smlouvy o zpracování osobních údajů s provozovatelem e-INFRA CZ AAI apod.

3.3. Životní cyklus skupiny

3.3.1. Vytvoření skupiny

Skupina je množina členů stejné VO, kteří sdílejí společný přístup k určitým zdrojům a službám. Každá skupina je podřízena konkrétní VO. Skupiny mohou tvořit stromovou hierarchii (členové všech podskupin jsou zároveň členy nadskupin) a je možné mezi nimi vytvářet relace množinové inkluze členství (mimo hierarchii). Za vytváření, správu a rušení skupin odpovídá správce virtuální organizace, který může určit jiného uživatele jako správce skupiny (dále jen **delegovaný správce skupiny**).

- vytváření skupin je odpovědností správce VO
- delegovaní správci skupin mají právo vytvářet podskupiny v hierarchii
- právo vytvářet skupiny přímo podřízené VO lze samostatně delegovat
- pro skupinu lze vytvořit registrační formulář, notifikace a stanovit životní cyklus členů skupiny (s omezeními danými životním cyklem dané VO i životním cyklem členství ve VO)

3.3.2. Provoz skupiny

- správce VO řídí členství ve skupině a nastavení skupiny dle svých potřeb a možností systému, případně to deleguje na delegovaného správce skupiny
- správce VO rozhoduje o přiřazení skupin k jednotlivým službám, ke kterým má VO přístup
- kontrola potřebnosti skupiny je odpovědností správce VO

3.3.3. Zánik skupiny

- o zániku skupiny rozhoduje správce VO, případně delegovaný správce skupiny
- zánikem VO zanikají všechny její skupiny

3.4. Životní cyklus členství ve skupině

3.4.1. Vznik členství ve skupině

Členství ve skupině může být buď přímé, nebo nepřímé. Přímé členství vzniká přidáním člena VO přímo do skupiny. Nepřímé členství vzniká na základě vazeb mezi skupinami (hierarchie skupin nebo množinová inkluze skupin).

3.4.1.1. Vznik přímého členství

- přidáním správcem VO nebo správcem skupiny
- registrací pomocí přihláškového formuláře
- synchronizací z externího systému

3.4.1.2. Vznik nepřímého členství

- ve stromové hierarchii skupin členové podskupin jsou nepřímými členy nadskupin
- při množinové inkluzi členové inkludované skupiny jsou nepřímými členy cílové skupiny

3.4.2. Aktivní členství ve skupině

- člen může mít v jedné skupině nejvýše jedno přímé členství a libovolný počet nepřímých členství zároveň
- po dobu aktivního přímého nebo nepřímého členství může uživatel používat služby zpřístupněné dané skupině
- doba přímého aktivního členství může být stanovena na neurčito nebo může mít stanovené určité datum expirace
- před vypršením přímého členství může být uživateli zasláno upozornění s odkazem na žádost o prodloužení členství
- nepřímé členství zůstává aktivní, dokud je uživatel aktivním členem alespoň v jedné podřízené skupině v hierarchii nebo v inkludované skupině

3.4.3. Neaktivní členství ve skupině

- po dobu neaktivního členství uživatel může mít omezen přístup ke službám zpřístupněným dané skupině. Osobní data a nastavení vztahující se k dané skupině zůstávají zachována.
- neaktivní členství může být způsobeno:
 - vypršením členství v dané skupině
 - zablokováním z bezpečnostních důvodů

3.4.4. Zánik členství ve skupině

- uživatel, který přestane být členem VO, automaticky přestane být členem všech jejích skupin
- přímé členství může být zrušeno manuálně správcem VO nebo delegovaným správcem skupiny
- přímé členství může být zrušeno synchronizací z externího systému
- nepřímé členství je zrušeno, pokud jsou odstraněny vazby mezi skupinami nebo uživatel přestane být členem všech skupin s vazbou
- přímé i nepřímé členství je zrušeno při smazání skupiny

3.5. Životní cyklus servisního účtu

3.5.1. Vytvoření servisního účtu

Servisní účet není reprezentací fyzické osoby, nýbrž je vytvořen za účelem strojového přístupu (*machine-to-machine*), například při automatizaci procesů. Každý servisní účet má vždy jasné definovaného vlastníka. Vzniká vždy za určitým účelem, ale ten se v e-INFRA CZ AAI neeviduje. Za správné využívání a zabezpečení servisního účtu nese plnou odpovědnost jeho vlastník.

Při tvorbě servisního účtu platí, že:

- je vytvořený správcem některé VO
- má vždy jednoho nebo více vlastníků
- podléhá standardnímu členství ve VO a skupinách (kromě pravidel expirace), tedy musí mít vyplněné všechny požadované atributy

3.5.2. Správa servisního účtu

Se servisním účtem lze provádět následující operace:

- změny vlastníků servisního účtu
- změny členství ve VO a skupinách
- konfigurace loginu a hesla

Pravidla expirace členství servisního účtu ve VO jsou následující:

- členství servisního účtu ve VO je platné, pokud alespoň jeden z vlastníků má platné členství ve stejné VO a servisní účet není ve stavu *Disabled*
- kontrola a úprava expirací je na pravidelné bázi (denně)

- pokud jsou všichni vlastníci vyexpirovaní, tak dojde k okamžité expiraci servisního účtu
- při přidání nebo odebrání vlastníka bude přepočítaná expirace
- v okamžiku, kdy dojde k expiraci servisního účtu, dojde k odeslání upozornění vlastníkům účtu

3.5.3. Zánik servisního účtu

- probíhá stejně jako v případě zániku běžného uživatelského účtu, viz sekci [Zánik uživatelského účtu](#)
 - zánik členství servisního účtu ve VO se řídí dle nastavených pravidel VO
 - pokud servisní účet není členem ani v jedné VO, tak je následně smazán ze systému

3.6. Životní cyklus Facility

3.6.1. Vytvoření Facility

Objekt Facility v rámci systému AAI reprezentuje zařízení, skupinu zařízení nebo softwarový systém (např. výpočetní cluster, datové úložiště, webový nebo poštovní server), ke kterému je řízen přístup. Facility představuje službu a je základní jednotkou řízení přístupu; pokud se jedná o skupinu zařízení, mají jednotnou konfiguraci.

Přístup na Facility získávají členové virtuálních organizací prostřednictvím tzv. prostředků (*Resources*). Správce Facility je zodpovědný za přidělování prostředků (*Resources*) jednotlivým virtuálním organizacím. Správce VO je zodpovědný za přiřazování skupin členů VO k těmto prostředkům.

- podmínky pro vytvoření Facility reprezentující službu jsou uvedeny v sekci [Podmínky připojování služeb](#)
- Facility může vzniknout dvěma způsoby:
 - podáním a schválením žádosti libovolného uživatele prostřednictvím registrační aplikace (*SPadmin*). Žadatel se stává správcem Facility.
 - manuálním vytvořením provozovatelem e-INFRA CZ AAI
- správce Facility může určit další správce Facility

3.6.2. Provoz Facility

- v rámci provozu správce Facility spravuje nastavení Facility dle svých potřeb a možností systému
- správce Facility domlouvá zpřístupnění členům virtuálních organizací s příslušnými správci VO
- správce Facility je zodpovědný za vytváření a rušení prostředků (*Resources*) pro jednotlivé VO
- e-INFRA CZ AAI předává do služby, která je reprezentovaná Facility, údaje o uživateli, jak je popsáno v sekci [Předávání osobních údajů službám](#)

3.6.3. Zánik Facility

- potřebnost Facility je pravidelně kontrolována každý rok. Pokud správce Facility nepotvrdí její potřebnost, bude Facility zrušena po uplynutí doby dvou měsíců od odeslání žádosti o potvrzení.
- správce Facility ji může sám zrušit v administrativním rozhraní systému Perun nebo v aplikaci SPadmin

4. Práva a povinnosti

4.1. Uživatelé

Uživatel je oprávněn:

1. spravovat svůj uživatelský účet (měnit kontaktní údaje a další nastavení)
2. využívat e-INFRA CZ AAI pro přístup ke službám

Uživatel je povinen:

1. zabezpečit svůj uživatelský účet proti zneužití, ztrátě nebo odcizení
2. poskytovat součinnost provozovateli e-INFRA CZ AAI
3. udržovat všechny svoje údaje aktuální
4. nezneužívat nalezených chyb systému k získání vyšších oprávnění, ale hlásit je provozovateli e-INFRA CZ AAI
5. hlásit ztrátu či zneužití svých přístupových údajů na kontakty uvedené na webové stránce <https://csirt.cesnet.cz/>

4.2. Provozovatele e-INFRA CZ AAI

Provozovatel je oprávněn:

1. spravovat a monitorovat e-INFRA CZ AAI
2. pozastavit přístup uživateli při porušení pravidel nebo bezpečnostních rizicích
3. rozhodovat o připojování a odpojování služeb
4. měnit technické parametry e-INFRA CZ AAI

Provozovatel je povinen:

1. reagovat rychle a efektivně na výpadky a bezpečnostní incidenty, hlásit je relevantním stranám a zajistit nápravu
2. informovat uživatele o relevantních změnách v e-INFRA CZ AAI

4.3. Uživatelé s vyšším oprávněním

Uživatel s vyšším oprávněním je uživatel, kterému byla přiřazena administrativní oprávnění v rámci e-INFRA CZ AAI. Musí splňovat všechny povinnosti uživatele dle 4.1 a navíc využívat osobní údaje uživatelů jen k účelům, pro které byly získány.

V následujících sekcích jsou upřesněná práva a povinnosti pro speciální případy uživatelů s vyššími oprávněními.

4.3.1. Správce virtuální organizace

Správce VO je oprávněn:

1. využívat VO v souladu s účelem, pro který byla založena
2. vytvářet servisní účty, [viz sekci 4.3.3.](#)

Správce VO je povinen:

1. dodržovat pravidla správy VO v souladu s [Podmínkami užití e-INFRA CZ \(Acceptable Use Policy, AUP\)](#) (část III dokumentu Podmínky přístupu k infrastruktuře e-INFRA CZ)
2. zajišťovat nezbytnou spolupráci se správcí e-INFRA CZ AAI pro plynulé fungování systémů a služeb
3. nastavit a udržovat pravidla pro vznik členství a jeho životní cyklus
4. nastavit a udržovat registrační formulář a šablony oznámení pro uživatele
5. umístit do registračního formuláře odkaz na informace o zpracování osobních údajů
6. proškolení uživatele, na které delegoval část svých oprávnění
7. sbírat pouze osobní údaje definované v sekci [Zpracování osobních údajů](#) nebo definované smlouvou s provozovatelem e-INFRA CZ AAI
8. oznámit provozovateli e-INFRA CZ AAI všechny změny mající vliv na životní cyklus VO (předávání VO jinému správci, ukončení činnosti VO)
9. zajistit oznámení změny účelů sběru, rozsahu a zpracování osobních údajů uživatelům, kteří jsou členy VO
10. zajistit, aby alespoň jeden ze správců VO byl oprávněným uživatelem e-INFRA CZ (podle sekce [1.5.1.](#) těchto podmínek)

4.3.2. Správce služby

Správce služby je oprávněn:

1. udělit uživateli zákaz přístupu ke službě, pokud uživatel porušil provozní podmínky služby nebo představuje bezpečnostní riziko
2. měnit konfiguraci služby v e-INFRA CZ AAI

Správce služby je povinen:

1. proškolení další správce služby, na které delegoval část svých oprávnění
2. zajistit oznámení provozovateli e-INFRA CZ AAI o zahájení procesu ukončení služby
3. udržovat aktuální dokument s provozními podmínkami služby a informaci o zpracování osobních údajů a oznamovat uživatelům všechny jejich změny
4. udržovat aktuální údaje o službě evidované v e-INFRA CZ AAI
5. oznamovat bezpečnostní incidenty týkající se uživatelů e-INFRA CZ na kontakty uvedené na webové stránce <https://csirt.cesnet.cz/>

4.3.3. Vlastníka servisního účtu

Při přidělení vyšších oprávnění servisnímu účtu přechází příslušná práva a povinnosti na jeho vlastníky.

Vlastník servisního účtu je oprávněn:

1. přidávat a odebírat další vlastníky servisního účtu
2. spravovat servisní účet obdobným způsobem jako uživatelský účet, včetně autentizačních mechanismů

Vlastník servisního účtu je povinen:

1. zajistit, že servisní účet má vždy alespoň jednoho vlastníka
2. požádat Provozovatele e-INFRA CZ AAI o zrušení servisního účtu, pokud pomine jeho potřeba
3. proškolit nové vlastníky servisního účtu
4. nezneužívat servisní účet pro osobní přístupy

5. Podmínky připojování Služeb

1. K e-INFRA CZ AAI je možné připojovat následující Služby:
 - a. Služby Provozovatelů konsorcia e-INFRA CZ
 - b. Služby provozované jinými organizacemi, jsou-li tyto služby určené pro podporu vědecké, výzkumné, vzdělávací, kulturní, vývojové nebo inovační činnosti
2. Žádost o připojení Služby podává pověřený pracovník organizace (dále jen “žadatel” nebo “správce Služby”), která je jedním z Provozovatelů konsorcia e-INFRA CZ, anebo organizace, která má za tímto účelem uzavřenou smlouvu s provozovatelem e-INFRA CZ AAI.
3. Organizace s právem žádat o připojení Služby k e-INFRA CZ AAI musí jmenovat odpovědnou osobu (dále jen “administrativní kontakt”), která jejím jménem potvrzuje správnost údajů a oprávněnost každé žádosti podané žadatelem jménem jeho organizace, a to typicky při přesunu Služby do produkčního prostředí. Administrativní kontakt zároveň vystupuje v roli správce všech Služeb připojených jeho organizací.
4. Žadatel musí u každé Služby uvést povinné údaje popisující připojovanou Službu, především pak údaje o jejím provozovateli, jaké osobní údaje a za jakým účelem sbírá a další údaje nezbytné pro technické připojení služby k e-INFRA CZ AAI.
5. O připojení Služby rozhoduje Provozovatel e-INFRA CZ AAI. Na připojení Služby není právní nárok. Po schválení žádosti je každá Služba zařazena do testovacího prostředí a žadatel se stává správcem Služby. Přístup uživatelů ke Službě v testovacím prostředí je typicky omezen a uživatelé jsou o této skutečnosti informováni při přístupu ke Službě.
6. Po úspěšném otestování Služby v testovacím prostředí je možné požádat o její přesun do produkčního prostředí. Ten podléhá schválení ze strany administrativního kontaktu organizace žadatele a provozovatele e-INFRA CZ AAI.
7. Správce Služby má povinnost udržovat informace poskytnuté při registraci Služby aktuální.
8. Správce služby má právo přidávat a odebírat další osoby z role správce služby.
9. Změna technických a evidenčních údajů připojené Služby podléhá dalšímu schválení provozovatelem e-INFRA CZ AAI.
10. Správce služby může požádat o zrušení, resp. odpojení Služby od e-INFRA CZ AAI. Žádost podléhá schválení provozovatelem e-INFRA CZ AAI.
11. Provozovatel e-INFRA CZ AAI si vyhrazuje právo připojenou Službu kdykoliv odpojit nebo k ní omezit přístup, a to především z důvodů:
 - a. ukončení nebo porušení smluvního vztahu s provozovatelem e-INFRA CZ AAI
 - b. zjištění dlouhodobé technické nefunkčnosti Služby
 - c. nečinnost správce Služby nebo administrativního kontaktu jeho organizace

6. Poskytování virtuální organizace

Virtuální organizace může být zřízena pro:

1. oprávněného uživatele e-INFRA CZ (osobu) pro potřeby řízení přístupů jeho týmu nebo vědecké komunity ke službám připojeným k e-INFRA CZ AAI
2. organizaci pro potřeby řízení přístupů jejích uživatelů ke službám připojeným k e-INFRA CZ AAI

Pro zřízení virtuální organizace musí být splněny následující podmínky:

1. jmenování správců VO
2. definovaný životní cyklus členství ve VO a podmínky členství ve VO
3. definovaný účel a doba potřebnosti existence VO
4. pokud je VO zřízena pro organizaci, a organizace požaduje sběr osobních údajů nad rámec stanovený těmito podmínkami v sekci [Zpracování osobních údajů](#), organizace se stává správcem těchto osobních údajů a je povinna uzavřít písemnou smlouvu o zpracování osobních údajů s provozovatelem e-INFRA CZ AAI jako zpracovatelem
5. pokud je VO zřízená pro osobu, není sběr osobních údajů ani jejich použití k jiným účelům nad rámec stanovený těmito podmínkami možný

Na zřízení VO není právní nárok a o jejím zřízení rozhoduje provozovatel e-INFRA CZ AAI.

7. Závěrečná ustanovení

1. Tyto provozní podmínky e-INFRA CZ AAI nabývají účinnosti dnem jejich zveřejnění.
2. Provozovatel e-INFRA CZ AAI si vyhrazuje právo podmínky kdykoliv upravit nebo doplnit, přičemž změny budou oznámeny uživatelům prostřednictvím vhodných komunikačních kanálů.