

# Federační politika *eduID.cz*

Verze 1.1

## Obsah

1. Úvod.....	1
2. Definice.....	1
3. Obecná ustanovení.....	3
4. Vymezení rolí a povinností subjektů zapojených do federace.....	3
4.1. Operátor federace.....	3
4.2. Poskytovatelé identity.....	4
4.3. Poskytovatelé služeb.....	4
4.4. Uživatelé.....	5
5. Zapojení organizace do federace.....	5
6. Opuštění federace.....	6
7. Postup při řešení bezpečnostních incidentů.....	6
8. Pravomoci, dodržování politiky a sankce.....	6
9. Odpovědnost.....	6
10. Závěrečná ustanovení.....	6

## 1. Úvod

- 1.1. *eduID.cz* je česká národní akademická federace identit, jejímž cílem je poskytnout svým členům rámec pro vzájemné využívání identit uživatelů při řízení přístupu k síťovým službám při respektování ochrany osobních údajů.
- 1.2. Tento dokument definuje organizační zásady provozu federace *eduID.cz*.

## 2. Definice

Pro účely této politiky se užitými termíny rozumí následující:

### 2.1. *Federace identit*

Sdružení organizací provozujících služby *poskytovatelů identit* a/nebo *poskytovatelů služeb*.

### 2.2. *Poskytovatel identity*

Služba, která vytváří a spravuje identifikační informace a poskytuje autentizaci pro *poskytovatele služeb*.

### 2.3. *Poskytovatel služby*

Poskytuje službu (např. konektivitu, aplikaci, výpočetní výkon, přístup k informačním skladům apod.); k řízení přístupů ke službě využívá autentizaci a *atributy* uživatelů poskytované *poskytovatelem identity*.

#### 2.4. *Atribut*

Datová struktura popisující charakteristickou vlastnost objektu. *Poskytovatel služby* obvykle využívá atributy popisující *uživatele* poskytnuté *poskytovatelem identity* pro řízení přístupu ke službě.

#### 2.5. *Operátor federace*

Poskytuje centrální služby federace (registrace členů, správa *metadat* a další).

#### 2.6. *Metadata*

Soubor informací popisujících jednotlivé členy federace, jejich role, služby, které poskytují, technické údaje umožňující využívání jejich služeb, kontakty na odpovědné osoby a další provozní data.

#### 2.7. *eduID.cz*

Oficiální název české akademické federace identit.

#### 2.8. *Člen federace*

Organizace, která přistoupila k federaci, aby provozovala služby *poskytovatele identity* a/nebo *poskytovatele služeb*.

#### 2.9. *Provozovatel poskytovatele identity/služby*

*Člen federace* provozující danou službu *poskytovatele identity* či *poskytovatele služby*.

#### 2.10. *Administrativní kontakt*

Osoba jmenovaná členem federace. Zastupuje *člena federace* při jednáních s *operátorem federace* a jmenuje *technické kontakty poskytovatelů služeb* a *poskytovatelů identity* provozovaných členem.

#### 2.11. *Technický kontakt*

Osoba jmenovaná *administrativním kontaktem* provozovatele poskytovatele identity/služby. Zastupuje konkrétního *poskytovatele identity* či *poskytovatele služby* při jednání s *operátorem federace*.

#### 2.12. *Zásady pro přístup do sítě národního výzkumu a vzdělávání nové generace (Access Policy, dále jen „AP“)*

Dokument, který určuje podmínky pro přístup subjektů k síti národního výzkumu a vzdělávání.

#### 2.13. *Identita*

Souhrn atributů popisujících daný subjekt (obvykle *uživatele*).

#### 2.14. Autentizační údaje

Údaje sloužící k ověření totožnosti *uživatele* poskytovatelem identity (obvykle uživatelské jméno a heslo).

#### 2.15. Uživatel

Osoba užívající službu provozovanou *poskytovatelem služby*.

### 3. Obecná ustanovení

- 3.1. *eduID.cz* slouží organizacím zapojeným do sítě CESNET2 při plnění jejich výzkumných a vzdělávacích cílů.
- 3.2. Členové *eduID.cz* jsou povinni se při využívání služeb federace řídit touto politikou. Její nedodržení je důvodem k vyloučení člena z federace.
- 3.3. Členové *eduID.cz* jsou povinni při využívání služeb federace dbát na zachování bezpečnosti osobních údajů uživatelů a to minimálně v míře dané právními předpisy a těmito zásadami.
- 3.4. Členové federace dodržují při provozu svých technických prostředků technické podmínky stanovené operátorem federace.

### 4. Vymezení rolí a povinností subjektů zapojených do federace

#### 4.1. Operátor federace

- 4.1.1. Roli operátora federace *eduID.cz* (dále *operátor federace*) vykonává sdružení CESNET z. s. p. o.
- 4.1.2. Operátor federace koordinuje dění ve federaci a je vykonavatelem federační politiky.
- 4.1.3. Operátor federace zajišťuje technickou podporu organizacím zapojeným do federace, a to v souvislosti se zapojením jejich technických prostředků do federace a řešením případných bezpečnostních incidentů.
- 4.1.4. Operátor federace definuje po dohodě se členy federace technická pravidla pro provoz *eduID.cz*.
- 4.1.5. Operátor federace definuje po dohodě se členy federace syntaxi a sémantiku povinných a doporučených atributů pro využití v *eduID.cz*.
- 4.1.6. Operátor federace provádí registraci a ruší registraci členů federace.
- 4.1.7. Operátor federace spravuje a publikuje metadata federace na základě podkladů dodaných jednotlivými členy.
- 4.1.8. Operátor federace neodpovídá za data přenášená mezi poskytovatelem identity a poskytovatelem služby.
- 4.1.9. Je-li to nezbytně nutné (např. z bezpečnostních nebo provozních důvodů), je operátor federace oprávněn vyřadit jednotlivé členy z publikovaných metadat.

- 4.1.10. Operátor federace uzavírá po dohodě se členy federace dohody o spolupráci s jinými federacemi identit (*inter-federální peering*). O uzavřených dohodách informuje členy federace.
- 4.1.11. Operátor federace má právo rozhodovat spory mezi členy federace.
- 4.1.12. Veškerá komunikace s operátorem federace probíhá prostřednictvím kontaktů uvedených na informačním portálu [www.eduID.cz](http://www.eduID.cz).

## **4.2. Poskytovatelé identity**

- 4.2.1. Poskytovatel identity spravuje identity uživatelů včetně jejich autentizačních údajů. Provozovatel poskytovatele identity je odpovědný za bezpečnost těchto dat a jejich ochranu proti zneužití.
- 4.2.2. V případě kompromitování autentizačních dat uživatele, nebo oprávněného podezření na ně, zablokuje poskytovatel identity okamžitě autentizační službu pro daného uživatele až do vydání nových autentizačních dat.
- 4.2.3. Poskytovatel identity vede záznamy o autentizaci uživatelů a o attributech, které poskytl jednotlivým poskytovatelům služeb tak, aby bylo možno v případě potřeby dohledat skutečnou identitu uživatele. Tyto záznamy uchovává po dobu 3 měsíců.
- 4.2.4. Provozovatel poskytovatele identity je odpovědný za správnost a úplnost údajů, které poskytovatel identity poskytuje provozovatelům služeb.
- 4.2.5. Poskytovatel identity podporuje vydávání atributů podle definic uvedených v seznamu povinných a doporučených atributů vydaných operátorem federace. Po dohodě s provozovatelem poskytovatele služby může vydávat i další atributy.
- 4.2.6. Provozovatel poskytovatele identity vystupuje vůči svým uživatelům jako prosazovatel pravidel platných v *eduID.cz* včetně této politiky.
- 4.2.7. Provozovatel poskytovatele identity spolupracuje s provozovatelem poskytovatele služby a operátorem federace při řešení bezpečnostních incidentů a případů porušení pravidel federace.
- 4.2.8. Provozovatel poskytovatele identity zajišťuje svým uživatelům technickou podporu a informace potřebné k využívání služeb federace. Zejména zajišťuje poučení uživatelů o správném a bezpečném nakládání s autentizačními údaji.
- 4.2.9. Provozovatel poskytovatele identity určí alespoň jednu osobu jako technický kontakt poskytovatele identity (z důvodů zástupnosti je vhodné určit technických kontaktů více). Technický kontakt komunikuje s operátorem federace a technickými kontakty poskytovatelů služeb, řeší technické problémy a bezpečnostní incidenty. Změnu technického kontaktu musí provozovatel poskytovatele identity neprodleně oznámit operátorovi.

## **4.3. Poskytovatelé služeb**

- 4.3.1. Poskytovatel služby musí vyžadovat od poskytovatelů identity pouze atributy nutné pro poskytnutí služby. Seznam požadovaných atributů dodá provozovatel poskytovatele služby spolu s popisem služby operátorovi federace.
- 4.3.2. Provozovatel poskytovatele služby se zavazuje používat data poskytnutá mu poskytovateli identity pouze pro zajištění přístupu ke službě. Zejména nesmí poskytovat získaná data třetím stranám.

- 4.3.3. Provozovatel poskytovatele služby spolupracuje s operátorem federace a provozovateli poskytovatelů identity při řešení bezpečnostních incidentů a případů porušení pravidel federace.
- 4.3.4. V případě bezpečnostních incidentů na zařízeních a systémech poskytujících službu provozovatel poskytovatele služby neprodleně informuje operátora federace a všechny poskytovatele identit, jejichž uživatelům službu poskytuje.
- 4.3.5. Provozovatel poskytovatele služby určí alespoň jednu osobu jako technický kontakt poskytovatele služby. Technický kontakt komunikuje s operátorem federace a technickými kontakty poskytovatelů identity, řeší technické problémy a bezpečnostní incidenty. Změnu technického kontaktu musí provozovatel poskytovatele služby neprodleně oznámit operátorovi federace.

#### **4.4. Uživatelé**

- 4.4.1. Uživatel je povinen řídit se pravidly definovanými svým provozovatelem poskytovatele identity a provozovatelem poskytovatele služby. Pokud se tato pravidla liší, platí přísnější varianta.
- 4.4.2. Uživatel je plně odpovědný za svoje autentizační údaje i za jejich zneužití. Musí postupovat tak, aby jejich zneužití v maximální možné míře předešel. V případě jejich prozrazení je povinen tuto skutečnost neprodleně oznámit svému provozovateli poskytovatele identity.
- 4.4.3. Uživatel je povinen okamžitě reagovat na výzvy a pokyny svého poskytovatele identity, poskytovatele služby a operátora federace.

### **5. Zapojení organizace do federace**

- 5.1. Do federace *eduID.cz* se může připojit každá organizace, která splňuje AP. Musí přitom splňovat technické podmínky a dodržovat tuto politiku. Konečné rozhodnutí, zda bude nebo nebude organizace přijata do federace *eduID.cz*, náleží operátorovi federace.
- 5.2. Organizace, které nesplňují AP, se mohou k federaci připojit, pokud poskytují služby organizacím připojeným podle bodu [5.1](#). Organizace připojené podle tohoto odstavce nesmějí v rámci federace provozovat službu poskytovatele identity. Konečné rozhodnutí, zda bude nebo nebude organizace přijata do federace *eduID.cz*, náleží operátorovi federace.
- 5.3. Aktem „přistoupení“ se pro potřeby těchto zásad rozumí oficiální jmenování administrativního kontaktu, tj. osoby, která zastupuje organizaci při jednání s operátorem federace a jmenuje technické kontakty odpovědné za jednotlivé poskytovatele identity a služeb provozované organizací.
- 5.4. Organizace svým přistoupením k *eduID.cz* souhlasí s těmito zásadami v plném rozsahu a zavazuje se je dodržovat.
- 5.5. Členství ve federaci *eduID.cz* je pro organizaci bezplatné.
- 5.6. Organizace musí vybudovat technickou strukturu, která odpovídá zásadám zveřejněným na informačním portálu [www.eduID.cz](http://www.eduID.cz).
- 5.7. Organizace se svým přistoupením k *eduID.cz* zavazuje spolupracovat s operátorem federace a v odpovídajícím čase reagovat na jeho výzvy.

## 6. Opuštění federace

- 6.1. Rozhodne-li se člen o své vůli opustit federaci, musí tento záměr ohlásit operátorovi federace písemně s předstihem alespoň 1 měsíc. Během této doby se připraví operátor federace na provedení technického odpojení a oznámí tuto skutečnost na informačním portálu [www.eduID.cz](http://www.eduID.cz).
- 6.2. Rozhodne-li operátor federace o vyloučení člena z federace, oznámí tuto skutečnost členovi a na informačním portálu [www.eduID.cz](http://www.eduID.cz) a vyřadí metadata jím provozovaných služeb z publikovaných metadat.

## 7. Postup při řešení bezpečnostních incidentů

Při zjištění bezpečnostního incidentu (eventuálně porušování této politiky, AP, či dalších pravidel závazných pro provoz sítě a služeb) musí veškeré dotčené subjekty zapojené do federace vyvinout maximální úsilí k odstranění problému, a to podle okolností v nejkratším možném čase. Porušení této zásady bude považováno za porušení politiky ze strany těchto subjektů. O všech bezpečnostních incidentech v rámci federace musí být neprodleně informován operátor federace.

## 8. Právomoci, dodržování politiky a sankce

- 8.1. Vykonavatelem této politiky je operátor federace, tedy sdružení CESNET z. s. p. o.
- 8.2. Na členství organizace ve federaci *eduID.cz* není právní nárok.
- 8.3. Veškeré změny v této politice budou oznámeny minimálně 3 měsíce před jejich účinností a budou v rámci možností konzultovány se všemi členy federace. Pokud bude pro člena nová verze politiky nepřijatelná, musí federaci nejpozději do data nabytí účinnosti změn opustit (podle článku 6 tohoto dokumentu). Neučiní-li tak, deklaruje tím svůj plný souhlas s novým zněním federační politiky.
- 8.4. Autoritativní a konečné rozhodnutí přísluší vždy operátorovi federace, a to zejména v případech, kdy se jedná o přijetí organizace do federace, jejím vyloučení z federace nebo v případech uplatňování sankcí. Rovněž pro výklad federační politiky je autoritativním orgánem operátor federace.

## 9. Odpovědnost

Česká národní akademická federace identit *eduID.cz* a sdružení CESNET z. s. p. o. jako její operátor neposkytují žádné garance týkající se dostupnosti a funkčnosti systémů zapojených do federace.

## 10. Závěrečná ustanovení

Tento dokument nabývá platnosti a účinnosti dnem 1. října 2008.

V Praze dne X. 9. 2008

Ing. Jan Gruntorád, CSc., v. r.  
Ředitel sdružení CESNET