

Roamingová politika

federace eduroam.cz

Čl. 1 Úvod

- 1.1. Sdružení CESNET, z. s. p. o. (dále jen CESNET), jeho členové a ostatní připojené nebo spolupracující instituce provozují ve svých prostorách lokální počítačové sítě. Jejich společným zájmem je zajistit pro své uživatele roaming mezi těmito lokálními sítěmi.
- 1.2. Tento dokument vymezuje vztahy mezi jednotlivými členy české federace eduroam a navazuje tak na evropskou konfедераční politiku eduroam, která definuje pravidla pro spolupráci jednotlivých federací.
- 1.3. Název a logo eduroam jsou registrovanou ochrannou známkou GÉANT association.

Čl. 2 Definice pojmů

Pro účely této politiky se užitými termíny rozumí následující:

- 2.1. eduroam je akademický roamingový systém poskytující síťovou konektivitu pro své uživatele v připojených organizacích. Přístup je založen na zabezpečené autentizaci v domácí instituci.
- 2.2. Česká federace eduroam je uskupení organizací zapojených do systému eduroam v rámci České republiky. Pro potřeby tohoto dokumentu se dále federací eduroam myslí česká federace eduroam.
- 2.3. Světová konfederace eduroam je uskupení jednotlivých národních federací eduroam. Federace jsou zpravidla zastoupeny organizacemi, které provozují síť národního výzkumu a vzdělávání - NREN (v ČR tuto roli zastává CESNET).
- 2.4. Access Policy (Podmínky přístupu k e-infrastruktuře CESNET, dále jen AP) je soubor pravidel definujících, kdo a za jakých okolností smí využívat služeb e-infrastruktury CESNET.
- 2.5. Poskytovatel identity je organizace, u které má uživatel veden svůj účet (např. jméno a heslo – ověřovací údaje potřebné pro přihlášení k síti). Obvykle se jedná o domovskou instituci, k níž má uživatel organizačně právní vztah – je jejím zaměstnancem, studentem atp.
- 2.6. Poskytovatel zdrojů je organizace, která uživatelům eduroamu poskytuje konektivitu. Rozhodnutí o poskytnutí konektivity se provede na základě autentizačního dotazu zasláného poskytovateli identity daného uživatele.

Čl. 3 Vymezení rolí a povinností subjektů zapojených do federace eduroam

3.1. Správce federace

- 3.1.1. Roli správce federace eduroam (dále jen správce federace) vykonává v rámci České republiky CESNET.
- 3.1.2. Správce federace koordinuje dění ve federaci a je vykonavatelem roamingové politiky na národní úrovni, přičemž postupuje v souladu s evropskou konfедераční politikou.
- 3.1.3. Správce federace provozuje národní infrastrukturu eduroam v souladu s technickými pravidly definovanými v evropské konfедераční politice. Infrastruktura zajišťuje především odpovědi na autentizační dotazy serverů členů federace a napojení na nadřazenou evropskou infrastrukturu.
- 3.1.4. Správce federace provozuje monitorovací systém dostupnosti zdrojů sítě.
- 3.1.5. Je-li to nezbytně nutné (např. z bezpečnostních nebo provozních důvodů), je správce oprávněn na národních autentizačních serverech omezit nebo zcela odepřít přístup pro jednotlivé uživatele nebo celé organizace. O tomto kroku musí informovat dotčené organizace.
- 3.1.6. Správce zajišťuje technickou podporu organizacím zapojeným do federace, a to v souvislosti s jejich napojením na národní autentizační servery a řešením případných provozních a bezpečnostních incidentů.
- 3.1.7. Veškerá komunikace se správcem federace probíhá prostřednictvím kontaktů uvedených na stránkách www.eduroam.cz.

3.2. Poskytovatelé identity

- 3.2.1. Úkolem poskytovatele identity je především odpovídat na autentizační dotazy přicházející od poskytovatelů zdrojů. Poskytovatelem identity je domácí organizace uživatele, která má k dispozici informace nutné pro jeho ověření.
- 3.2.2. Poskytovatel identity je odpovědný za autoritativní rozhodnutí, zda má či nemá uživatel právo přístupu ke zdrojům federace (vyjma případů definovaných v bodě 3.1.5).
- 3.2.3. Poskytovatel identity ověřuje pozitivně pouze ty uživatele, se kterými má organizačně právní (pracovní nebo studijní) vztah.
- 3.2.4. Poskytovatel identity prosazuje u svých uživatelů dodržování této federační politiky a vlastních pravidel, která musí být v souladu s touto federační politikou.
- 3.2.5. Poskytovatel identity musí od svých uživatelů důsledně vyžadovat dodržování AP.

- 3.2.6. Poskytovatel identity nesmí v rámci federace pozitivně ověřovat sdílené účty (s výjimkou testovacího účtu podle bodu 3.2.10).
- 3.2.7. Poskytovatel identity musí přijímat a řešit oznámení o bezpečnostních incidentech, nedodržování AP a federační politiky svými uživateli. U závažných incidentů je povinen neprodleně těmto uživatelům přístup ke zdrojům eduroam odepřít.
- 3.2.8. Poskytovatel identity musí svým uživatelům zajistit technickou podporu, základní informace o roamingovém systému eduroam a platné legislativě.
- 3.2.9. Autentizační servery poskytovatele identity musí být dostupné a reagovat na autentizační dotazy od oprávněných subjektů federace.
- 3.2.10. Pro testovací účely musí poskytovatel identity vytvořit správci federace testovací účet. Tento účet slouží pouze pro testování autentizačního serveru daného poskytovatele identity a ověření funkčnosti celé autentizační infrastruktury. Testovací účet udržuje správce federace i poskytovatel identity v tajnosti (tj. nepředává ho třetím stranám).

3.3. Poskytovatelé zdrojů

- 3.3.1. Poskytovatelem zdrojů je každý subjekt, který nabízí svou konektivitu uživatelům roamingového systému eduroam.
- 3.3.2. Poskytovatel zdrojů je povinen v nezbytně nutné míře spolupracovat při technické podpoře uživatelů s jejich poskytovatelem identity.
- 3.3.3. Poskytovatel zdrojů je oprávněn v průběhu řešení bezpečnostních incidentů odepřít přístup konkrétním zařízením, uživatelům anebo celým realmům podle závažnosti incidentu.
- 3.3.4. Poskytovatel zdrojů by měl pokryté prostory viditelně označit logem eduroam.

3.4. Uživatelé

- 3.4.1. Uživatel je povinen řídit se pravidly pro přístup k síti definovanými svým poskytovatelem identity (domácí organizace).
- 3.4.2. Uživatel je plně odpovědný za svoje přihlašovací údaje i za jejich zneužití. Musí postupovat tak, aby jejich zneužití v maximální možné míře předešel. V případě jejich diskreditace je povinen tuto skutečnost neprodleně oznámit svému poskytovateli identity.
- 3.4.3. Při problémech se uživatel obrací na pracovníky podpory svého poskytovatele identity.

3.5. Společná ustanovení

- 3.5.1. Organizace provozuje autentizační servery a další infrastrukturu v souladu s publikovanými technickými požadavky a navazující dokumentací. Tyto

servery jsou napojeny na národní autentizační servery a zajišťují tak technické připojení dané organizace k federaci eduroam.

- 3.5.2. Organizace zapojené do federace jsou povinny logovat a uchovávat po dobu 6 měsíců všechny informace o autentizačním provozu, které jsou potřebné k identifikaci konkrétního uživatele využívajícího zdroje federace (uživatelské identity, mapování IP adres a podobně).
- 3.5.3. Odpovídající části logů je organizace oprávněna použít v případě řešení bezpečnostních incidentů nebo technických problémů sítě a jejích služeb. V těchto případech, je-li to nezbytné, je oprávněna poskytnout uložené informace i třetím stranám (dotčeným členům federace a orgánům činným v trestním řízení).
- 3.5.4. Organizace se zavazují v rámci federace spolupracovat při řešení provozních problémů sítě, monitoringu dostupnosti sítě a bezpečnostních incidentů.
- 3.5.5. Každá organizace musí určit nejméně jednu osobu jako technický kontakt. Technický kontakt je zodpovědný za komunikaci s ostatními členy federace v technických záležitostech a při řešení bezpečnostních incidentů (pokud nemá organizace vlastní CSIRT tým, viz 6.2). Organizace je povinná neprodleně informovat správce federace o změnách technických kontaktů způsobem zveřejněným na stránkách www.eduroam.cz.
- 3.5.6. Každá organizace provozuje informační www stránky, které by měly obsahovat především kontakty na technickou podporu, návody a další užitečné informace pro uživatele eduroamu.
- 3.5.7. Organizace poskytující identitu (ve smyslu bodu 3.2) musí být současně poskytovatelem zdrojů (ve smyslu bodu 3.3). Z tohoto pravidla může být udělena zvláštní výjimka, která musí být schválena správcem federace a oznámena všem členům federace.
- 3.5.8. Nové organizace jsou připojovány vždy jako celek, nikoli samostatně po organizačních složkách. Připojení více organizačních složek samostatně je možné pouze výjimečně v odůvodněném případě. Toto pravidlo se nevztahuje na organizace a složky připojené před 1. 1. 2017.
- 3.5.9. V systému eduroam musí být vždy zajištěn bezpečný a důvěryhodný přenos autentizačních dat. Uživatelské autentizační údaje musí být při přenosu mezi klientským zařízením a poskytovatelem identity šifrovány, aby nemohlo dojít k jejich diskreditaci.
- 3.5.10. Autentizační infrastruktura eduroamu nesmí být využívána k jiným účelům než je uvedeno v této politice.

Čl. 4 Zapojení organizace do federace eduroam

- 4.1. Do systému eduroam se v rámci české federace eduroam může připojit jako **poskytovatel identity** každá organizace, která splňuje AP a technické požadavky.

- 4.2. Do systému eduroam se v rámci české federace eduroam může připojit jako **poskytovatel zdrojů** každá organizace, která splňuje technické podmínky.
- 4.3. Organizace svým přistoupením k systému eduroam souhlasí s touto roamingovou politikou v plném rozsahu a zavazuje se ji dodržovat.
- 4.4. Aktem přistoupení se pro potřeby této politiky rozumí technické napojení autentizačních serverů organizace k národním autentizačním serverům.
- 4.5. Konečné rozhodnutí o přijetí organizace náleží správci federace.
- 4.6. Členství ve federaci eduroam je pro organizaci bezplatné.
- 4.7. Organizace nesmí za služby poskytnuté v rámci systému eduroam účtovat žádné poplatky.

Čl. 5 Opuštění federace eduroam

- 5.1. Rozhodne-li se organizace opustit federaci eduroam a dále nespolupracovat v rámci roamingového systému eduroam, oznámí tento záměr správci federace spolu s požadovaným datem odpojení.
- 5.2. Pokud dochází k odpojení organizace z důvodů porušení pravidel, zablokuje správce federace neprodleně veškerý autentizační provoz dané organizace, čímž organizaci technicky izoluje od zbytku federace eduroam. Doba izolace trvá 1 měsíc. Pokud v této lhůtě organizace odstraní nedostatky, izolace bude zrušena a organizace bude dále vystupovat jako plnohodnotný člen federace. Pokud během lhůty izolace organizace problém neodstraní, dojde k úplnému odpojení od federace.
- 5.3. Veškeré skutečnosti o uvalení izolace na organizaci (zejména důvody, termíny, případné zrušení izolace atd.) oznamuje správce federace neprodleně dotčené organizaci. Během izolace je organizace stále vedená v seznamu připojených organizací.
- 5.4. Po odpojení organizace od federace eduroam musí tato neprodleně odstranit veškeré odkazy na systém eduroam. Jde zejména o informace na webových stránkách, loga, anoncované SSID na rádiových sítích atd.

Čl. 6 Postup při řešení bezpečnostních incidentů

- 6.1. Všichni členové federace jsou povinni dle svých možností předcházet bezpečnostním incidentům.
- 6.2. Pokud má organizace vlastní bezpečnostní tým, řeší se incidenty v kooperaci nebo pod vedením tohoto týmu.
- 6.3. V případě zjištění incidentu, který přesahuje lokální organizaci, je tato povinna informovat ostatní dotčené členy. V případě incidentu většího rozsahu nebo závažných dopadů je organizace povinna informovat i správce federace.

- 6.4. Kontakty na členy národní federace jsou k dispozici v seznamu technických kontaktů spravovaných správcem federace.
- 6.5. Pokud člen nereaguje adekvátně na výzvu ke spolupráci, je řešení incidentu eskalováno ke správci federace.
- 6.6. Zprostředkování kontaktu na zahraniční členy eduroamu a řešení incidentů s nimi souvisejícími zajišťuje správce federace.
- 6.7. Všechny organizace zúčastněné v incidentu musí vyvinout maximální úsilí k vyřešení incidentu.
- 6.8. Poskytovatel identity původce incidentu je povinen poskytnout součinnost dle 3.2.7.
- 6.9. Poskytovatel dotčených zdrojů je oprávněn do doby vyřešení incidentu zamezit původci incidentu přístupu ke zdrojům.
- 6.10. Pokud poskytovatel identity nereaguje v přiměřené době na výzvu poskytovatele zdrojů k řešení incidentu a incident byl eskalován dle bodu 6.5 nebo 6.6, je poskytovatel zdrojů oprávněn zablokovat veškerý autentizační provoz poskytovatele identity na dobu nezbytně nutnou. O tomto kroku musí být informován správce federace i dotčený poskytovatel identity.

Čl. 7 Právomoc, dodržování politiky a sankce

- 7.1. Vykonavatelem této roamingové politiky je správce federace, tedy CESNET.
- 7.2. Na členství organizace ve federaci eduroam není právní nárok.
- 7.3. Na využívání služeb systému eduroam v roli „uživatel“ (ve smyslu čl. 3.4.1) není právní nárok. Vytvoření pravidel pro přístup uživatelů ke službě eduroam je plně v kompetenci příslušného poskytovatele identity.
- 7.4. Veškeré změny v této roamingové politice budou oznámeny minimálně 3 měsíce před jejich účinností a budou konzultovány se všemi členy české federace eduroam. Pokud bude pro organizaci nová verze politiky nepřijatelná, musí se od federace nejpozději do data nabytí účinnosti změn odpojit (podle článku 5 tohoto dokumentu). Pokud zůstane nadále technicky připojená, zavazuje se tím nové znění federační politiky dodržovat.
- 7.5. Autoritativní výklad této roamingové politiky a konečné rozhodnutí v rámci federace přísluší vždy správci federace.

Čl. 8 Odpovědnost

- 8.1. Česká federace eduroam a CESNET jako správce této federace neposkytuje žádné garance týkající se dostupnosti a funkčnosti systému eduroam v rámci federace.
- 8.2. Systém je provozován v „best effort“ režimu.
- 8.3. Přistoupení k této politice nezavazuje žádnou z členských organizací povinnosti dodržovat právní přepisy.

Čl. 9 Závěrečná ustanovení

- 9.1. Tento dokument nabývá platnosti a účinnosti 1. 10. 2017 a je platný v rámci české federace eduroam.
- 9.2. Tato politika je dostupná v české a anglické verzi. Dojde-li k rozporu mezi těmito verzemi, přednost má verze česká.
- 9.3. V rámci české federace eduroam je tento dokument nadřazen evropské konfедераční politice eduroam. Nastane-li nesrovnalost mezi těmito dvěma dokumenty, postupuje se v rámci ČR podle ustanovení uvedených v této federální politice.
- 9.4. Správce federace vydává a udržuje dokument "**Technické požadavky a doporučení pro členy federace eduroam.cz**". O jeho změnách informuje všechny členy federace.