NIIF eduroam szabályzat

v2.0, 2016-05-13

A jelen dokumentum aktuális változata a http://www.eduroam.hu/ oldalról indulva érhető el. Bővebb tájékoztató az eduroamról az „Eduroam ismertető” című dokumentumban [ERI] található.

A jelen szabályzat betartása kötelező az eduroam [RFC7593] föderációban részt vevő NIIF tagintézmények, azok eduroam felhasználói, valamint a magyarországi központi eduroam infrastruktúra üzemeltetője számára.

A jelen szabályzat hatályba lépésének időpontja 2016. július 1. A föderációs szerződést a szabályzat aktuális verziójának NIIF Intézet általi publikálása (2016. május 17.) előtt aláíró intézményeknek további 8 hónap (2017. március 1-ig) áll rendelkezésükre a szabályzat új előírásainak teljesítésére.

1. Fogalmak

Az ***eduroam szövetség*** egy intézményi szövetség, amelynek elsődleges célja, hogy a jogosult felhasználók ne csak a saját intézményükben, hanem más eduroam tagintézményekben is hozzáférhessenek az Internethez. Ezt az eduroam szövetség az ***eduroam szolgáltatás*** nyújtásával valósítja meg.

Eduroam felhasználó az a személy, aki igénybe veszi az eduroam szolgáltatást.

Eduroam tagintézmény minden olyan intézmény, mely felhasználói és/vagy szolgáltatása révén részt vesz az eduroam szövetségben.

Eduroam közösség az eduroam felhasználók és az eduroam tagintézmények együttese.

A ***magyarországi eduroam föderáció*** a magyarországi eduroam tagintézmények szövetsége. A magyarországi eduroam föderáció célja az eduroam szolgáltatás működtetése Magyarországon, úgy, hogy az szerves része legyen a nemzetközi eduroam szolgáltatásnak.

Az ***eduroam infrastruktúra*** az eduroam tagintézmények által használt számítógép-hálózati (Internet) alapinfrastruktúrára épülő, elsősorban hardver és szoftver elemekből álló rendszer, amely lehetővé teszi az eduroam szolgáltatás működését. Az eduroam infrastruktúrát és (ezáltal az eduroam szolgáltatást) az eduroam tagintézmények, vagy azok egyes szervezeti egységei üzemeltetik.

A ***magyarországi központi eduroam infrastruktúra*** (röviden: ***központi infrastruktúra***) az eduroam infrastruktúrának, azon belül a felhasználói azonosítási (autentikációs) hierarchiának az a része, amely a magyarországi eduroam tagintézményeket egymással, valamint külföldi eduroam tagintézményekkel köti össze.

Felhasználói jogosítvány (röviden: ***jogosítvány***) az az adatcsoport (felhasználóazonosító és jelszó, vagy tanúsítvány és kulcspár), aminek „bemutatásával” a felhasználó igénybe veheti az eduroam szolgáltatást. A jogosítványok tartalmazzák a felhasználó azonosítóját (önállóan vagy a tanúsítvány részeként), valamint egy érzékeny, titkos adatot (jelszó vagy a kulcspár titkos része), amelynek titokban tartása lehetővé teszi a felhasználó számára, hogy a jogosítványát más ne használhassa.

Egy felhasználó ***saját intézmény***e az az intézmény, amelyikkel a felhasználó tanulói, hallgatói, vagy munkavállalói jogviszonyban áll. Ez a felhasználó az adott intézmény ***saját felhasználó***ja. Minden jogosítvány egyértelműen köthető egy intézményhez, amelyik azt kibocsátotta. Az eduroam szolgáltatás igénybevételéhez szükséges jogosítványt minden felhasználónak saját

intézménye bocsátja rendelkezésére.

Vendéglátó intézmény az az intézmény, ahol a felhasználó igénybe veszi az eduroam szolgáltatást a saját intézményén kívül. Ilyenkor a vendéglátó intézményben ő ***vendég felhasználó***nak minősül.

Az eduroam autentikáció műszaki megvalósítása hierarchikus, fa struktúrájú rendszerben történik, aminek az egyes csomópontjait és leveleit domain nevek azonosítják. Az ***eduroam domain név*** egy Internet domain név, ami az adott csomópontot (ország, intézmény stb.) azonosítja az eduroam felhasználói azonosítási (autentikációs) hierarchiában. A DNS struktúrához hasonlóan egy intézményt több eduroam domain név is azonosíthat.

2. Általános és adminisztratív követelmények

2.1. Felhasználókra vonatkozó előírások

2.1.1. Tájékozódás, felhasználói magatartás

2.1.1.1. A felhasználók kötelesek megismerni és betartani annak az intézménynek a rájuk vonatkozó szabályzatait, amelyben az eduroam szolgáltatást igénybe veszik, legyen az akár saját intézményük, akár egy vendéglátó intézmény. Amikor a felhasználók magyarországi eduroam tagintézményben veszik igénybe az eduroam szolgáltatást, akkor értelemszerűen kötelesek betartani az NIIF Felhasználói Szabályzatát [NIIFAUP] is, hiszen az minden ilyen intézményre érvényes. A vendég felhasználók ezen felül kötelesek betartani saját intézményük szabályzatait is, kivéve azokat az előírásokat, amelyek kifejezetten csak a saját intézmény területére, hálózatára vonatkoznak.

2.1.1.2. A felhasználóknak ajánlott a vendéglátó intézmény vonatkozó szabályzatait előzetesen, már a szolgáltatás igénybevétele előtt megismerni. Amennyiben erre nincs módjuk, úgy kötelesek a vendéglátó intézmény szabályzatainak megismerésével kezdeni tevékenységüket a szolgáltatás igénybevétele elején.

2.1.1.3. A felhasználók kötelesek megismerni az eduroam szolgáltatás működését, mielőtt a szolgáltatást igénybe vennék. (Ehhez saját intézményük rendelkezésükre bocsátja a szükséges információt.) Kötelesek továbbá tájékozódni saját intézményük műszaki ügyfélszolgálatának elérhetőségéről, mielőtt a szolgáltatást saját intézményükön kívül igénybe vennék.

2.1.1.4. A felhasználók kötelesek az eduroam szolgáltatás igénybevétele során maximális körültekintéssel járni el annak érdekében, hogy tevékenységük ne terhelje túlzott mértékben az eduroam tagintézmények hálózati és egyéb erőforrásait, ne veszélyeztesse az intézmények hálózati és egyéb infrastruktúrájának biztonságát, épségét.

2.1.2. Személyes adatok kezelése

2.1.2.1. A felhasználók közül a szolgáltatást azok vehetik igénybe, akik az eduroam működtetéséhez szükséges adatokat a szolgáltató (saját intézmény) rendelkezésére bocsátják. A felhasználó tudomásul veszi, hogy saját intézménye eduroam felhasználói adatbázisában a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvényben meghatározott személyes adatok is találhatók: ilyennek minősül bármely természetes személlyel összefüggésbe hozható adat, vagy az abból levonható következtetés (pl. név, cím, telefonszám, e-mail cím,

felhasználói azonosító, jelszó). A felhasználó tudomásul veszi, hogy ezek az adatok az eduroam szolgáltatás céljaira felhasználhatók. A szolgáltató vállalja, hogy ezen adatokat az adatvédelmi törvény előírásai szerint kezeli, és kizárólag a szolgáltatás nyújtásával összefüggésben használja fel.

2.1.2.2. A felhasználó tudomásul veszi, hogy az eduroam szolgáltatás igénybevétele során statisztikai és hibadiagnosztikai céllal naplóadatokat rögzíthetnek az autentikációs folyamatról, illetve a hálózathoz történő csatlakozásról az eduroam infrastruktúra üzemeltetői. A rögzített naplóadatokat az eduroam szövetség tagjai statisztika készítésén, valamint hibák diagnosztizálásán kívül más célra nem használják. Statisztikai adatokat az eduroam tagintézmények közzétehetnek anonimizált formában. Személyes adatokat is tartalmazó naplóadatokat az eduroam szövetség tagjai sem egymás, sem harmadik fél számára nem adnak ki, kivéve a műszaki célú hibakeresés érdekében egymásnak, illetve a hatályos jogszabályokban előírt esetekben és módon az eljáró hatóságok számára.

2.1.3. Felhasználói jogosítványok kezelése

2.1.3.1. A felhasználók kötelesek jogosítványaik érzékeny részét (jelszót, kulcspár titkos részét) titokban tartani. Ezeket kizárólag az eduroam szolgáltatást üzemeltető műszaki személyzetnek személyesen hozhatják tudomására, kizárólag akkor, ha ez az eduroam szolgáltatás igénybevételéhez szükséges hibaelhárításban elengedhetetlen.

2.1.3.2. Amennyiben egy felhasználó úgy tudja vagy gyanítja, hogy jogosítványa érzékeny része illetéktelen tudomására jutott, köteles haladéktalanul értesíteni erről saját intézményét. Köteles továbbá a kitudódott jogosítvány letiltását kérni, illetve – amennyiben erre önállóan lehetősége van – letiltani vagy megváltoztatni azt.

2.2. Intézményekre vonatkozó előírások

2.2.1. Felhasználók tájékoztatása

2.2.1.1. Az intézmények kötelesek a jelen szabályzatot megismertetni saját felhasználóikkal.

2.2.1.2. Az intézmények kötelesek az eduroam szolgáltatásról – különös tekintettel az adott intézményben elérhető szolgáltatásra, és a felhasználókra vonatkozó szabályzataikra – tájékoztatni az eduroam felhasználókat.

2.2.2. Felhasználói adatbázis, személyes adatok kezelése

2.2.2.1. Az intézmények kötelesek saját felhasználóik adatbázisát naprakész állapotban tartani, és biztosítani ezáltal, hogy az arra jogosult saját felhasználóik igénybe vehessék, és kizárólag ők vehessék igénybe az eduroam szolgáltatást az intézményükhöz tartozó felhasználói azonosítóval és jogosítvánnyal.

2.2.2.2. Az intézmények kötelesek maximális körültekintéssel eljárni az eduroam szolgáltatás nyújtása során annak érdekében, hogy a felhasználók jogosítványai biztonságban legyenek.

2.2.2.3. Az eduroam infrastruktúra üzemeltetői statisztikai és hibadiagnosztikai céllal rögzíthetnek naplóadatokat az autentikációs folyamatról, valamint a felhasználók hálózathoz történő csatlakozásáról. Az intézmények a rögzített naplóadatokat kötelesek bizalmasan kezelni. Statisztikai információt csak anonimizált formában tehetnek közzé, azaz kizárólag személyes adatok nélkül, úgy, hogy az érintett felhasználók kilétére azokból következtetni ne lehessen. Személyes adatokat is

tartalmazó naplóadatokat az érintett felhasználó és az eduroam szövetség tagintézményein kívül másnak ki nem adhatnak, kivéve a hatályos jogszabályokban előírt esetekben és módon az eljáró hatóságoknak. Az eduroam szövetségen belül, tagintézmények között adatok megosztása és felhasználása kizárólag műszaki problémák megoldása érdekében lehetséges.

2.2.3. Biztonsági incidensek

2.2.3.1. Amennyiben hálózati biztonsági incidens történik az eduroam szolgáltatás nyújtása vagy igénybevétele során, úgy az érintett intézmények kötelesek egymással és a magyarországi központi eduroam infrastruktúra üzemeltetőjével együttműködni az incidens kezelésében.

2.2.3.2. Az intézmények korlátozhatják mind saját, mind vendég felhasználóik hozzáférését az eduroam szolgáltatáshoz, amennyiben ezt biztonsági okok szükségessé teszik. Ilyen eseményekről a vendéglátó intézmény köteles értesíteni az NIIF-CSIRT-öt.

2.2.3.3. Az intézmények felelősséggel tartoznak az eduroam közösségnek saját felhasználóik megfelelő magatartásáért az eduroam szolgáltatás igénybevétele során.

2.2.4. Kapcsolattartás, ügyfélszolgálat

Az felhasználók eduroammal kapcsolatos műszaki problémáinak kezelésében elsődlegesen saját intézményük feladata a segítségnyújtás. A saját intézmény illetékes munkatársai természetesen együttműködhetnek ennek érdekében a föderáció egyéb érintett intézményeivel.

2.2.4.1. Az intézmények kötelesek kapcsolattartót kijelölni és megadni az eduroammal kapcsolatos műszaki kérdések és problémák kezelésére, aki/amely mind saját felhasználóik, mind az eduroam szövetség tagintézményei számára rendelkezésre áll. A műszaki kapcsolattartó lehet természetes személy vagy szervezeti egység. A műszaki kapcsolattartónak elérhetőnek kell lennie munkaidőben telefonon és e-mailen egyaránt.

2.2.4.2. Az intézmények kötelesek műszaki támogatást (ügyfélszolgálat) nyújtani saját felhasználóiknak, bárhol is veszik igénybe az eduroam szolgáltatást.

2.2.4.3. A vendéglátó intézmény köteles együttműködni a vendég felhasználó saját intézményével az eduroam szolgáltatás igénybevétele során a vendég felhasználók műszaki támogatásában. Amennyiben a támogatási folyamat során kiderül, hogy egy vendég felhasználó problémájának megoldásában saját intézménye nem tud érdemben segíteni, viszont a vendéglátó intézmény tud, úgy a vendéglátó intézmény köteles műszaki támogatást nyújtani közvetlenül a vendég felhasználónak, egyszerűsítve ezzel a támogatási folyamat hátralevő szakaszát.

2.2.4.4. Az intézmények kötelesek együttműködni a központi infrastruktúra üzemeltetőjével az eduroam szolgáltatás megbízható és biztonságos üzemeltetése, valamint a felmerülő hibák időben történő elhárítása érdekében.

2.2.5. Csatlakozás az eduroam föderációhoz

2.2.5.1. Az eduroamhoz csatlakozni kívánó NIIF tagintézményeknek szerződést kell kötniük a magyarországi központi eduroam infrastruktúra üzemeltetőjével a jelen szabályzatban foglaltak kölcsönös betartásáról.

2.2.5.2. Az intézmény csatlakozáskor köteles megadni, illetve egyeztetni a csatlakozáshoz szükséges adminisztratív és műszaki paramétereket, különösképpen a jelen szabályzatban is előírtakat:

- műszaki kapcsolattartók ill. ügyfélszolgálat elérhetőségei
- eduroam domain név (vagy nevek)
- RADIUS IP címek és UDP portok, ezek felügyeletére szolgáló hostok címei
- RADIUS forgalom titkosításához használt jelszók (shared secret)
- tesztelési és felügyeleti célokra szolgáló jogosítványok

2.3. A központi infrastruktúra üzemeltetőjére vonatkozó előírások

2.3.1. Az eduroam infrastruktúra üzemeltetése

2.3.1.1. A magyarországi központi eduroam infrastruktúra üzemeltetője az országos kutatói hálózatot működtető NIIF Intézet.

2.3.1.2. A központi infrastruktúra üzemeltetője köteles gondoskodni arról, hogy a magyarországi eduroam szolgáltatás a nemzetközi részeként, a felhasználók számára transzparens módon működjön.

2.3.1.3. A központi infrastruktúra üzemeltetője köteles együttműködni a magyarországi és külföldi eduroam tagintézményekkel, az eduroam infrastruktúra üzemeltetőivel, az eduroam szolgáltatás megbízható és biztonságos üzemeltetése, valamint a felmerülő hibák időben történő elhárítása érdekében.

2.3.2. Felhasználók tájékoztatása

2.3.2.1. A központi infrastruktúra üzemeltetője köteles az eduroam szolgáltatásról tájékoztatni az eduroam felhasználókat.

2.3.3. Személyes adatok kezelése

2.3.3.1. Az magyarországi központi eduroam infrastruktúra üzemeltetője köteles maximális körültekintéssel eljárni annak érdekében, hogy a felhasználók jogosítványai biztonságban legyenek.

2.3.3.2. A központi infrastruktúra üzemeltetője statisztikai és hibadiagnosztikai céllal rögzíthet naplóadatokat az autentikációs folyamatról, valamint a felhasználók hálózathoz történő csatlakozásáról. A rögzített naplóadatokat köteles bizalmasan kezelni. Statisztikai információt csak anonimizált formában tehet közzé, azaz kizárólag személyes adatok nélkül, úgy, hogy az érintett felhasználók kilétére azokból következtetni ne lehessen. Személyes adatokat is tartalmazó naplóadatokat az érintett felhasználó és az eduroam szövetség tagintézményein kívül másnak ki nem adhat, kivéve a hatályos jogszabályokban előírt esetekben és módon az eljáró hatóságoknak. Az eduroam szövetségen belül, tagintézmények között adatok megosztása és felhasználása kizárólag műszaki problémák megoldása érdekében lehetséges.

2.3.4. Ügyfélszolgálat

2.3.4.1. A központi infrastruktúra üzemeletetője ügyfélszolgálatot működtet, amelynek feladata a tagintézményekkel történő kapcsolattartás, technikai konzultáció, valamint a

hibabejelentések fogadása a központi infrastruktúrát érintő kérdésekben. Az ügyfélszolgálat telefonon és e-mailen folyamatosan, valamint munkanapokon 8.00 órától 18.00 óráig személyesen is rendelkezésre áll.

2.3.5. Csatlakozás a szövetséghez, tagsági viszony

2.3.5.1. A központi infrastruktúra üzemeltetője köteles együttműködni az NIIF tagintézményekkel annak érdekében, hogy az arra alkalmas, csatlakozni kívánó intézmények csatlakozhassanak az eduroam szövetséghez.

2.3.5.2. A központi infrastruktúra üzemeltetője a csatlakozni kívánó intézményekkel szerződést köt a jelen szabályzatban foglaltak kölcsönös betartásáról. A szerződést aláíró és a szabályzatban foglaltakat teljesítő intézményeket regisztrálja, és integrálja az eduroamba.

2.3.5.3. A központi infrastruktúra üzemeltetője köteles figyelemmel kísérni, hogy a magyarországi eduroam tagintézmények megfelelnek-e a jelen szabályzat előírásainak. Ha egy tagintézmény nem felel meg az előírásoknak, akkor a központi infrastruktúra üzemeltetője köteles az intézmény illetékeseinek figyelmét felhívni erre a problémára, a kijelölt kapcsolattartón keresztül.

2.3.5.4. Amennyiben azt biztonsági okok szükségessé teszik, illetve amennyiben egy magyarországi eduroam tagintézmény nem teljesíti a jelen szabályzatban előírtakat, úgy a központi infrastruktúra üzemeltetője műszaki intézkedésekkel felfüggesztheti az adott tagintézmény részvételét az eduroamban a probléma elhárításáig.

3. Műszaki követelmények

3.1. Általános előírások

Ez a fejezet vonatkozik a magyarországi eduroam tagintézményekre és a országos központi infrastruktúra üzemeltetőjére egyaránt.

3.1.1. RADIUS infrastruktúra

3.1.1.1. [kötelező]
Az eduroam autentikációs rendszerében működő RADIUS szervereknek eleget kell tenniük az alábbi műszaki feltételeknek:

- megfelelnek az [RFC2865]-nek és az [RFC2866]-nak
- válaszolnak az ICMP echo kérésekre, bárhonnan is érkeznek az Internetről (az esetleges DoS támadásokkal szemben korlátozható az ilyen üzenetek gyakorisága)
- naplózzák az accounting üzeneteket és az autentikációs folyamatokat

3.1.1.2. [ajánlott]
Az eduroam autentikációs rendszerében működő RADIUS szervereknek ajánlott az alábbi UDP portokon fogadni a RADIUS kéréseket:

- 1812-es porton az autentikációs kéréseket
- 1813-as porton az accounting kéréseket

3.1.2. Eduroam domainek

3.1.2.1. [kötelező]
Az eduroam autentikációs hierarchiában a DNS-hez hasonlóan minden csomópont (ill. a csomópont összes RADIUS szervere) felelős a hozzá tartozó eduroam domainért és annak al-domainjeiért, kivéve a hierarchiában alatta levő csomópontok eduroam domainjeit és azok al-domainjeit.

3.1.3. Autentikáció

Annak érdekében, hogy a RADIUS üzenetek ne keringhessenek a végtelenségig a hálózatban, az eduroam RADIUS szerverek (ill. tartalékolt szerver párok) egy fa hierarchiába vannak rendezve. A fa topológia körmentes, tetszőleges két pontja közt egy és csak egy út van. Ezért az üzenetek végtelen hurokban való keringésének megelőzéséhez csak azt szükséges biztosítani, hogy minden csomópont kizárólag olyan csomópontnak küldjön vagy küldjön tovább üzenetet, ami a fában a tőle a célcsomóponthoz vezető úton található, vagy maga a célcsomópont (vagyis minden üzenetnek minden továbbítási lépésben közelebb kell jutnia a cél csomóponthoz).

Külön figyelmet érdemel, hogy az adott csomópont milyen domainekért felelős, és hogy az ezekbe irányuló kérdéseket ne küldje sehova (pl. az `intezmeny.hu` csomópont az `akarmi.intezmeny.hu` domain üzeneteit ne küldje a „default irányként” használt `hu` csomópont felé).

3.1.3.1. [kötelező]
Meg kell előzni a RADIUS üzenetek hurokba kerülését.

- RADIUS üzeneteket TLS és UDP felett egyaránt kizárólag az autentikációs szerverek fa struktúrájának olyan csomópontjába szabad továbbítani, ami az adott csomópontból nézve az üzenet célcsomópontjáig vezető úton van, vagy maga a célcsomópont. UDP használata esetén ez mindig a szomszédos csomópont, TLS használata esetén lehet távolabbi csomópont is. (Az autentikációs fa struktúrában az adott csomópontot alkotó, egymás tartalékaként működő RADIUS szerverek nem küldhetnek egymásnak eduroam RADIUS üzeneteket.)
- Tilos olyan `access-request` és `accounting-request` üzenetet bárhova küldeni vagy továbbküldeni, amiben a `User-Name` paraméterben szereplő domainért az adott RADIUS szerver felelős.

3.1.3.2. [kötelező]
Ha egy `access-request` üzenet továbbításakor arra nem érkezik időben válasz, és a kérdéses csomópont két (tartalékolt) RADIUS szerverből áll, akkor újra kell küldeni a RADIUS üzenetet, a csomópont másik RADIUS szerveréhez.

3.1.3.3. [kötelező]
Az eduroam autentikációs folyamat során biztosítani kell, hogy a felhasználók jogosítványainak érzékeny része mindvégig biztonságosan, megfelelő módon titkosítva közlekedjen a hálózaton a felhasználó végberendezése és saját intézményének autentikációs infrastruktúrája között. (Ez csak jelszó használata esetén merül fel, hiszen tanúsítvány használatakor a jogosítvány érzékeny része nem kerül ki a hálózatra.)

3.1.3.4. [kötelező]
A RADIUS üzenetek továbbításakor az `EAP-Message` attribútumot minden esetben változatlanul kell hagyni.

3.1.4. Naplózás

3.1.4.1. [kötelező]
A naplóbejegyzéseket megbízható dátummal és időbélyeggel kell ellátni, mely legalább századmásodpercre pontos.

3.1.4.2. [kötelező]
A naplózott accounting és autentikációs információt legalább 2 hónapig meg kell őrizni. Hibaelhárításkor és biztonsági incidensek kezelésében az adott esetre vonatkozó naplórészleteket az illetékes eduroam tagintézmények rendelkezésére kell bocsátani.

3.1.4.3. [kötelező]
A naplózott adatokat legkésőbb 6 hónap elteltével meg kell semmisíteni. A naplóadatokból készült anonimizált statisztikák tetszőleges ideig megőrizhetők.

3.1.4.4. [kötelező]
A naplózott accounting és autentikációs információ személyes adatokat is tartalmazhat, ezért azokat mindig megfelelő körültekintéssel kell kezelni, hogy illetéktelen fél tudomására ne juthassanak.

3.2. Intézményekre vonatkozó előírások

Ez a fejezet a magyarországi eduroam tagintézményekre vonatkozik.

3.2.1. Eduroam domain név

Az eduroam autentikáció struktúrájából adódóan Magyarországon erősen ajánlott `.hu` végződésű neveket használata eduroam domain névként, de kivételes esetekben lehetséges nem országhoz tartozó domain név (pl. `.edu`) használata is. Az ütközések elkerülése, valamint az egyszerű használhatóság érdekében az intézményeknek (valamelyik) saját DNS nevüket (vagy neveiket) kell intézményi eduroam domain névként használniuk.

3.2.1.1. [kötelező]
Minden intézménynek meg kell határoznia saját eduroam domain nevét (vagy neveit) az eduroamhoz való csatlakozáskor.

3.2.1.2. [kötelező]
Minden intézményi eduroam domain névnek az intézményhez tartozó, `.hu` végződésű, vagy nem országhoz köthető Internet DNS névnek kell lennie.

3.2.1.3. [ajánlott]
Ha az intézményhez több `.hu` végződésű domain is tartozik, akkor ajánlott ezek közül olyat használni intézményi eduroam domain névként, amit az intézmény általában elsődlegesen használ az Interneten. Praktikus, ha az intézmény eduroam domain neve állandó, vagy legalábbis minél ritkábban változik.

3.2.1.4. [ajánlott]
Intézményi eduroam domain neveknél a nem országhoz tartozó top level domainek használata kerülendő.

3.2.2. Vendég felhasználók tájékoztatása

Az eduroam felhasználókat tájékoztatni kell az eduroam szolgáltatásról, hogy azt nehézségek nélkül vehessék igénybe. Az eduroam szolgáltatás alapvető jellegéből adódóan sok tekintetben világszerte egységes, de természetesen mindenütt lehetnek helyi sajátosságok, előfordulhatnak kizárólag az adott intézményre érvényes tudnivalók. A vendég felhasználókról feltételezhető, hogy

ismerik az eduroam szolgáltatást (hiszen erről a saját intézményük tájékoztatja őket), ezért velük elsősorban az adott intézményre jellemző konkrétumokat kell megismertetni.

Fontos, hogy a potenciális vendég felhasználók előzetesen, a vendéglátó intézmény meglátogatása előtt tájékozódhassanak az intézményben elérhető eduroam szolgáltatásról. Emellett praktikus, ha a vendég felhasználók a helyszínen is könnyen hozzájuthatnak ezekhez az információkhoz, hiszen előfordulhat, hogy nem is tervezték, hogy az adott intézménybe látogatnak, vagy ugyan tervezték, de nem állt módjukban az ott elérhető eduroam szolgáltatásról előzetesen tájékozódni.

3.2.2.1. [kötelező]
Minden intézmény köteles az eduroam használatáról a vendég felhasználóknak szóló információkat az Internetről bárhonnan, bárki számára elérhetővé tenni.

3.2.2.2. [kötelező]
Az információkat elérhetővé kell tenni HTTP-vel, magyar és angol nyelven.

3.2.2.3. [kötelező]
Az információkat HTTP-vel elérhetővé kell tenni az intézmény központi honlapjáról (nyitóoldal) egyetlen közvetlen hyperlinken keresztül, vagy a `http://eduroam.intezmeny.hu/` című oldalról (ahol `intezmeny.hu` az intézmény elsődlegesen használt domain neve).

3.2.2.4. [ajánlott]
Amennyiben az intézmény (valamelyik) eduroam domain neve nem egyezik meg az intézmény által elsődlegesen használt Internet domain névvel, akkor a vendég felhasználóknak szóló információkat ajánlott elérhetővé tenni a `http://eduroam.intezmeny.hu/` című oldalról is (ahol `intezmeny.hu` az intézmény fent említett eduroam domain neve).

3.2.2.5. [ajánlott]
Feltéve, hogy az intézmény informatikai hálózatáról szóló információk eleve elérhetők HTTP-vel, az eduroamról szóló információkat praktikus ezek közé beilleszteni, és az előző pontokban említett `http://eduroam.intezmeny.hu/` című weboldalról automatikusan átirányítani ide a HTTP klienseket.

3.2.2.6. [kötelező]
Az eduroamról szóló információkat tartalmazó weboldalakon kötelező az eduroam logó használata, a logóhoz tartozó használati útmutató szerint. (Az eduroam logó és a hozzá tartozó használati útmutató elérhető a http://www.eduroam.org/ oldalról indulva.)

3.2.2.7. [ajánlott]
Feltéve, hogy az intézmény központi honlapjáról elérhető az eduroam információkat tartalmazó oldal, az oda vezető hyperlinknél ajánlott az eduroam logó használata.

3.2.2.8. [kötelező]
A vendég felhasználóknak szóló információknak tartalmaznia kell az alábbiakat:

- az intézményben érvényes, az eduroam felhasználókra vonatkozó szabályzatok
- a hálózathoz való csatlakozásához szükséges tudnivalók
- az intézményben hol érhető el a szolgáltatás
- milyen IEEE szabványoknak felel meg a WLAN (802.11a, 802.11b, 802.11g, 802.11n, 802.11ac stb.)
- milyen WLAN paramétereket kell beállítani a kliensen (SSID, titkosítás, autentikáció stb.)

- milyen IP paramétereket kell beállítani a kliensen (IPv4 DHCP stb.)
- van-e a hálózati rétegben vagy afelett bármi korlátozás (NAT, tűzfal, proxy stb.)
- az eduroam szolgáltatást érintő ismert fennálló problémák ill. tervezett leállások
- hivatkozás az országos eduroam website-ra (http://www.eduroam.hu/)
- hivatkozás az eduroam website-ra (http://www.eduroam.org/)
- műszaki kapcsolattartó elérhetőségei, ahova saját és vendég felhasználók és más eduroam tagintézmények fordulhatnak az eduroamot érintő műszaki kérdésekben

Az eduroam szövetség térképes adatbázisban tartja nyilván a helyszíneket, ahol elérhető az eduroam szolgáltatás. Erre a térképre a magyarországi tagintézmények adatait a központi infrastruktúra üzemeltetője teszi fel.

3.2.2.9. [kötelező]
Az intézményeknek közölniük kell az eduroam szolgáltatási helyszíneik adatait. Épületenként a következő paramétereket kell megadni a térképes adatbázishoz:

- az épület rövid megnevezése (elsősorban nem cím, hanem pl. „R épület”, „Könyvtár” stb.; ilyen ismert megnevezés hiányában a közterület nevéből és házszámból álló cím)
- WGS84 koordináták (GPS koordináták)
- SSID (ha nem „eduroam”, a 3.2.6.10. pontnak megfelelő esetben)

3.2.3. Saját felhasználók tájékoztatása

A vendég felhasználóknak szóló információk az előző fejezetben leírtak szerint bárki számára, így az intézmény saját felhasználói számára is elérhetőek kell, hogy legyenek. Ezeken az információkon túl a saját felhasználóknak szükséges további tájékoztatást is nyújtani az eduroam szolgáltatással kapcsolatban, mint pl. az eduroam használatáról szóló alapvető tudnivalókat, vagy a saját felhasználói jogosítványaikkal kapcsolatos információkat. Amennyiben az intézmény úgy ítéli meg, természetesen hozzáférhetővé teheti a saját felhasználóinak szóló információkat is mindenki számára.

3.2.3.1. [kötelező]
A kifejezetten csak saját felhasználóknak szóló információkat úgy kell közzétenni, hogy azok egyértelműen elkülöníthetők legyenek a vendég felhasználóknak szóló információktól.

3.2.3.2. [kötelező]
Az információkat elérhetővé kell tenni HTTP-vel, magyar nyelven.

3.2.3.3. [kötelező]
Az intézmény saját felhasználóit köteles tájékoztatni

- az eduroam alapvető működéséről
- az eduroam használatának módjáról, felhasználói azonosítókról, jogosítványokról
- az intézményen kívüli felhasználás lehetőségéről
- műszaki kapcsolattartójának (ügyfélszolgálat) elérhetőségeiről, ahol saját felhasználóik számára támogatást nyújtanak az eduroammal kapcsolatos kérdésekben
- az intézményi RADIUS által használt tanúsítvány ellenőrzésének pontos módjáról

3.2.3.4. [ajánlott]
Az eduroam alapvető működéséről szóló tájékoztató lehet egyszerűen egy hivatkozás az NIIF Intézet erről szóló leírására.

3.2.4. RADIUS infrastruktúra

3.2.4.1. [kötelező]
Minden intézmény köteles RADIUS szervert üzemeltetni, mely ellátja az intézmény eduroam domain nevéhez tartozó csomópont feladatait az eduroam autentikációs hierarchiában. Ez a RADIUS szerver elérhető kell, hogy legyen a 1812-1813 UDP vagy az előre egyeztetett portokon a központi infrastruktúra üzemeltetője által megadott címekről (magyarországi központi eduroam RADIUS szerverek, felügyeleti hostok). Amennyiben az intézmény több eduroam domain nevet is használ, úgy a fentieknek teljesülnie kell az intézmény összes eduroam domain nevére. Több eduroam domain név használata esetén egy RADIUS szerver felelős lehet egyszerre több eduroam domainért is.

3.2.4.2. [ajánlott]
A nagyobb megbízhatóság érdekében ajánlatos második, a fent említett elsődleges RADIUS szerverrel azonos jellemzőkkel bíró szerver üzemeltetése is.

Az intézményi RADIUS tanúsítványának felhasználók általi ellenőrzése kritikus pont a felhasználói jogosítványok biztonságos kezelésében. A RADIUS oldali tanúsítvány megfelelő ellenőrzésének hiányában a felhasználó nem tudhatja, hogy jogosítványát helyes módon saját intézménye autentikációs infrastruktúrájához juttatja-e el az eduroam szolgáltatás igénybevételekor, vagy illetéktelen, esetlegesen a jogosítvánnyal visszaélni kívánó kezekbe adja.

A tanúsítvány ellenőrzésének megfelelő módja kétféle lehet. Jól ismert CA által aláírt tanúsítvány esetén a tanúsítvány érvényességét és a tanúsítvány tárgyaként megjelölt domain nevet is ellenőrizni kell (hiszen ilyen tanúsítványhoz bárki hozzájuthat). Saját intézményi CA esetén elegendő lehet a tanúsítvány érvényességének az ellenőrzése kizárólag az adott CA tanúsítvány használatával, ha tudható, hogy az adott CA nem állít ki egyéb tanúsítványokat. Mivel a tanúsítványban szereplő név ellenőrzésére nem minden kliens képes (pl. az aktuális Android verziók sem), a saját CA használata nagyobb biztonságot ad.

3.2.4.3. [ajánlott]
A nagyobb biztonság érdekében ajánlott az intézményi RADIUS számára saját CA üzemeltetése.

A GÉANT Association elkészítette (és fejleszti) az eduroam CAT-et (Configuration Assistant Tool), mely a felhasználóknak könnyíti meg saját készülékeiken az eduroam beállítását, többek közt a fent tárgyalt tanúsítvány ellenőrzést. A CAT elérhető szolgáltatásként: az intézményeknek elegendő a központilag üzemeltetett rendszerbe (https://cat.eduroam.org/) felvinni a szükséges paramétereket ahhoz, hogy felhasználóik igénybe vehessék a CAT-et.

3.2.4.4. [ajánlott]
A felhasználók készülékeinek beállítását megkönnyítendő ajánlott az eduroam CAT használata.

Annak érdekében, hogy a nemzetközi irányból érkező RADIUS üzenetek a magyarországi központi RADIUS szerverekig UDP helyett hatékonyabban, TLS felett juthassanak el, célszerű a külföldi eduroam RADIUS szerverek tudtára hozni ezt a lehetőséget: Az intézmény felhasználóinak azonosítójában szereplő domain névhez ajánlatos hozzárendelni a magyarországi központi eduroam RADIUS szervereket a megfelelő NAPTR DNS bejegyzések használatával, melyek az említett RADIUS szerverek RADIUS/TLS szolgáltatását megadó, a központi infrastruktúra üzemeltetője által létrehozott `_radsec._tcp.eduroam.hu` SRV bejegyzésekre mutatnak.

A szükséges NAPTR bejegyzések formája és tartalma a következő:

```
intezmeny.hu.
    IN NAPTR 100 10 "s" "x-eduroam:radius.tls" "" _radsec._tcp.eduroam.hu.
```

A fenti bejegyzésben mindent változatlanul kell hagyni, kivéve az `intezmeny.hu.` címkét.

3.2.4.5. [ajánlott]
Az intézményeknek ajánlott a felhasználóik azonosítóinak `@` utáni részében használt összes domain névre NAPTR DNS bejegyzést készíteni az `x-eduroam:radius.tls` szolgáltatásra, amelyek a `_radsec._tcp.eduroam.hu` SRV bejegyzésre mutatnak.

3.2.5. Autentikáció

3.2.5.1. [kötelező]
A RADIUS `access-request` üzeneteket a `User-Name` paraméter értéke alapján továbbítani kell az eduroam autentikációs szerverek fa struktúrájának ágai mentén a paraméterben szereplő domainért felelős csomópont irányába, amennyiben az adott csomópont nem felelős a kérdéses domainért.

Az eduroam felhasználók azonosítása hierarchikus rendszerben történik. Minden felhasználói azonosító a felhasználó saját intézményének eduroam domain nevére végződik, így a felhasználói azonosító implicite megadja a felhasználó saját intézményének helyét az autentikációs hierarchiában.

3.2.5.2. [kötelező]
Az intézmény eduroam felhasználóit az [RFC4282] szerinti NAI azonosítja. Az azonosítók az intézmény eduroam domain nevére végződnek, melyet közvetlenül '.' vagy '@' karakter előz meg.

A felhasználók autentikációjakor a felhasználó hordozható hálózati készüléke (laptop, táblagép, mobiltelefon stb.) és a felhasználó saját intézményének RADIUS szervere között EAP üzenetváltás történik. Az autentikációs döntést a saját intézmény RADIUS szervere hozza meg (kivéve, ha egy vendég felhasználó hozzáférését másutt – pl. a vendéglátó intézményben – korlátozzák). Vendég felhasználók autentikációja során az EAP üzeneteket az eduroam RADIUS szerverek továbbítják (proxy) egymás közt a vendéglátó intézmény RADIUS szerverétől a saját intézmény RADIUS szerveréig (és vissza), a felhasználói azonosítóban szereplő eduroam domain név alapján.

3.2.5.3. [kötelező]
Az eduroam felhasználókat Extensible Authentication Protocollal [RFC3748] kell autentikálni.

3.2.5.4. [ajánlott]
Az eduroam felhasználókat ajánlott EAP-TTLS, PEAP, vagy EAP-TLS protokollokkal autentikálni.

3.2.5.5. [kötelező]
A vendég felhasználók számára biztosítani kell tetszőleges EAP autentikáció használatának lehetőségét.

3.2.5.6. [kötelező]
Az eduroam kliensek csatlakozási próbálkozásakor küldött RADIUS `access-request` üzenet `Calling-Station-Id` mezőjének az eduroam kliens MAC címét, a `NAS-IP-Address` mezőnek pedig a szolgáltatást nyújtó WLAN access point IP címét kell tartalmaznia.

3.2.5.7. [kötelező]
Az EAP autentikációs folyamat végén a saját intézmény RADIUS szervere

szimmetrikus kulcsú titkosításhoz szükséges kulcs adatokat kell generáljon, majd azt az [RFC3580] 3.16 pontja szerint továbbítania kell az `access-accept` RADIUS üzenetben.

3.2.5.8. [kötelező]
A központi infrastruktúra üzemeltetője számára tesztelési célokra egy intézményi felhasználói azonosítót kell biztosítani (a hozzá tartozó jelszóval), amit az intézmény RADIUS szerverei elfogadnak EAP-TTLS, és PEAP autentikációval egyaránt.

A Chargeable User Identity (CUI) a felhasználót a vendéglátó intézmény számára anonim módon, de egyértelműen azonosító, időben stabil érték. Az eduroamban CUI a felhasználó azonosítójából és a vendéglátó intézmény nevéből egyirányú függvénnyel képzett érték, így egyrészt a CUI-ból a vendéglátó nem tudja a felhasználó azonosítóját kinyerni, másrészt két vendéglátó intézmény a CUI alapján nem tudja megállapítani, hogy a mindkettőjüknél megforduló felhasználó ugyanaz a személy. A CUI használatának célja, hogy statisztikák készítéséhez és incidensek kezeléséhez a vendéglátó intézmények a vendég felhasználókat egyértelműen azonosíthassák, hiszen ennek hiányában csak a felhasználó saját intézményét és mobil eszközének MAC címét látnák.

3.2.5.9. [kötelező]
Ha saját felhasználókra vonatkozó, más vendéglátó intézményből jövő autentikációs kérés tartalmaz az [RFC5580] szerinti Operator-Name, és az [RFC4372] szerinti Chargeable-User-Identity RADIUS attribútumot egyaránt, akkor a CUI generálása és használata kötelező. A generált CUI kizárólag az Operator-Name és a felhasználó azonosító függvénye kell, hogy legyen, ezek mindegyikétől függnie kell, és abból a felhasználó azonosítót a saját intézményen kívül másnak nem szabad tudnia visszafejteni.

3.2.5.10. [ajánlott]
A CUI generálására javasolt módszer a felhasználó azonosítójának, az Operator-Name értékének, valamint egy fix titkos karaktersorozatnak az összefűzése, majd ezekre egy kriptográfiai hash függvény (pl. SHA-256) kiszámítása.

A felhasználót végső soron autentikáló RADIUS szerver (saját intézményének szervere) megadhat olyan RADIUS attribútumokat, amik meghatározzák az access point számára a VLAN-t, amibe a felhasználó csatlakozhat. Ezeknek csak akkor van értelme, ha a VLAN-ok használata az autentikációs szerver és az access point között egyeztetett módon történik – ellenkező esetben ilyen attribútumok hibát, a felhasználó csatlakozásának meghiúsulását okozhatják. Ez jellemzően a felhasználó saját intézményében való csatlakozásakor áll fenn, de elképzelhető a VLAN-ok használatának egyeztetése két intézmény között is.

3.2.5.11. [kötelező]
Saját felhasználók azonosításakor az intézmény RADIUS szerverének csak abban az esetben szabad Tunnel-Type, Tunnel-Medium-Type, valamint Tunnel-Private-Group-ID RADIUS attribútumokat megadnia, ha az autentikációs kérés a saját hálózatából, vagy olyan helyről érkezik, amivel ezen az attribútumok használata egyeztetve van.

3.2.6. WLAN infrastruktúra

Az eduroam a kölcsönösség elve alapján működik: bármely intézmény felhasználói igénybe vehetik a szolgáltatást világszerte minden eduroam tagintézményben, saját intézményük pedig hozzáférést biztosít minden vendég eduroam felhasználó számára.

Az esetenként országonként eltérő spektrum etikett, valamint egyéb helyi jellemzők miatt az eduroam felhasználók WLAN kliensei különböző képességűek lehetnek. Ezt is szem előtt tartva úgy kell hozzáférést biztosítani a hálózathoz, hogy azt lehetőleg minden eduroam felhasználó képes legyen igénybe venni.

3.2.6.1. [kötelező]
Minden intézmény köteles legalább egy WLAN access pointot üzemeltetni az intézményben, amit a vendég felhasználók igénybe vehetnek. Az access pointnak az alábbi jellemzőkkel kell rendelkeznie:

- megfelel az IEEE 802.11b vagy 802.11g ajánlásnak
- működik a 2,4 GHz-es sáv 1-11 csatornája valamelyikén
- enterprise WPA2/AES titkosítást használ
- olyan helyen üzemel, ahol azt az intézménybe látogató vendég felhasználók igénybe vehetik

3.2.6.2. [ajánlott]
Lehetőleg minél több olyan access pointot célszerű üzemeltetni, amit a vendég eduroam felhasználók igénybe vehetnek. Praktikus lehet az intézmény teljes WLAN infrastruktúráján eduroam szolgáltatást nyújtani, hogy az intézmény saját felhasználói is ezzel a módszerrel csatlakozzanak az intézményi WLAN-hoz mindenütt az intézmény területén.

3.2.6.3. [kötelező]
Minden access pointnak, ahol az eduroam szolgáltatás igénybe vehető, meg kell felelnie az IEEE 802.11 fizikai és adatkapcsolati rétegre vonatkozó ajánlásai közül legalább egynek (pl. 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac stb.).

3.2.6.4. [ajánlott]
A 2.4 GHz-es frekvencia-tartományban működő access pointokat ajánlott az 1-es, 6-os, ill. 11-es csatornákon működtetni.

3.2.6.5. [kötelező]
Az intézményi eduroam infrastruktúrán kötelező enterprise WPA2/AES vagy IEEE 802.11i használata.

3.2.6.6. [kötelező]
Az eduroam szolgáltatás kizárólag „eduroam” SSID-vel vagy „eduroam-” kezdetű SSID-vel nyújtható. Amennyiben a 3.2.6.10. pontban leírt körülmény nem áll fenn, az eduroam szolgáltatást „eduroam” SSID-vel kell nyújtani.

3.2.6.7. [kötelező]
Az „eduroam” SSID vagy bármilyen „eduroam”-mal kezdődő SSID csak az eduroam szolgáltatásban használható.

3.2.6.8. [ajánlott]
„eduroam” SSID esetén annak hirdetése IEEE 802.11 beacon keretekben.

3.2.6.9. [kötelező]
Nem „eduroam” SSID esetén az SSID hirdetése IEEE 802.11 beacon keretekben.

Ismert probléma, hogy ha egy helyen több intézmény eduroam szolgáltatása is elérhető, akkor azonos SSID esetén a WLAN kliens rendszerint a felhasználó által nem, vagy csak nehézkesen befolyásolható módon választ WLAN access pointot, és azt pl. a pillanatnyi rádiós vételi viszonyoknak megfelelően változtatja is. Ha a váltáskor a kliens a másik intézmény hálózatába kerül, akkor értelemszerűen változik számára az IP környezet, de erről a kliens nem értesül, hiszen az azonos SSID miatt az IP környezet változatlanságát feltételezi. Ebben az esetben megszakad az IP kapcsolat.

A fenti probléma elkerülhető eltérő SSID-k használatával. Ez ugyan valamivel kényelmetlenebbé teszi a felhasználók számára az eduroam használatát, de ennél sokkal nagyobb nyereség a probléma elkerülése.

3.2.6.10. [kötelező]
Ha több intézmény eduroam WLAN infrastruktúrája által lefedett területnek van nem üres metszete (vagyis azok valahol egymással átfedésben vannak), akkor az érintett intézmények közül csak egy használhatja az „eduroam” SSID-t, a többi érintett intézménynek „eduroam-” kezdetű, egymástól eltérő, az intézményre utaló, könnyen érthető karaktersorozatra végződő SSID-t kell használnia. Az SSID-k egyeztetése és közös meghatározása az érintett intézmények feladata.

3.2.7. Hálózati kapcsolat

A vendég és saját felhasználók számára IP hálózati kapcsolatot nyújt minden tagintézmény az eduroam szolgáltatás keretében. Annak érdekében, hogy a felhasználók könnyen és hatékonyan használhassák az eduroam szolgáltatást, (a lehetőségekhez képest) szabad hozzáférést kell nyújtani számukra az Internethez.

3.2.7.1. [kötelező]
A felhasználók számára IPv4 kapcsolatot kell biztosítani az Internethez.

3.2.7.2. [ajánlott]
A felhasználók számára ajánlott IPv6 kapcsolatot biztosítani az Internethez.

3.2.7.3. [kötelező]
A felhasználók számára kötelező átengedni az eduroam kliensek által kezdeményezett alább felsorolt IPv4 forgalmat (PAT használata esetén csak a TCP-t és UDP-t ezek közül):

- TCP 22: SSH
- TCP 80, 443, 3128, 8080: HTTP, HTTPS
- TCP 21: FTP
- IP 50 (ESP), IP 51 (AH), UDP 500, 4500, TCP 10000: IPsec
- TCP/UDP 1194: OpenVPN
- IP 47: GRE
- TCP 1723: PPTP
- TCP 465, 587: SMTPS, message submission
- TCP 110, 995: POP3, POP3S
- TCP 143, 220, 993: IMAP, IMAPS
- TCP 1494: Citrix ICA
- TCP 3389: RDP
- TCP 5900: VNC
- UDP 53, TCP 53: DNS
- TCP 389, 636: LDAP, LDAPS
- TCP 5222: XMPP/Jabber
- IP 41, TCP 3653: IPv6 tunnel broker

3.2.7.4. [kötelező]
A felhasználók számára kötelező átengedni minden ICMP forgalmat. Címfordítás

(NAT) alkalmazása esetén a gerinchálózat felől természetesen csak az azonosítható módon az adott felhasználónak szóló ICMP forgalmat kell átengedni.

3.2.7.5. [ajánlott]
A felhasználók számára ajánlott minden IPv4 és IPv6 forgalmat átengedni.

3.2.7.6. [kötelező]
A felhasználók számára kötelező rekurzív feloldásra alkalmas DNS szervert üzemeltetni.

3.2.7.7. [kötelező]
A felhasználók számára DHCP-vel kell IPv4 címet osztani, valamint a default gateway és a rekurzív DNS szerver címét közölni.

3.2.7.8. [ajánlott]
Stateless Address Autoconfiguration alkalmazása ajánlott a felhasználók IPv6 címének és az IPv6 default gateway beállításához.

3.2.7.9. [ajánlott]
Az IPv6-on elérhető rekurzív feloldásra alkalmas DNS szerver címének közlésére ajánlott DHCPv6 használata.

3.3. A központi infrastruktúra üzemeltetőjére vonatkozó előírások

Ez fejezet kizárólag az országos központi infrastruktúra üzemeltetőjére vonatkozik.

A magyarországi központi eduroam infrastruktúra üzemeltetője az országos kutatói hálózatot müködtető NIIF Intézet.

A központi infrastruktúra üzemeltetője az autentikációs hierarchiában a `hu` eduroam domain csomópontjáért felelős. A magyarországi eduroam tagintézmények közt, valamint a magyarországi tagintézmények és az autentikációs hierarchia gyökere között továbbítja a szükséges RADIUS üzeneteket. Ezzel kapcsolatos feladatai szerepelnek ebben a fejezetben.

A központi infrastruktúra üzemeltetője természetesen emellett nyújthat saját és vendég felhasználóknak eduroam szolgáltatást – e tekintetben rá is az „Intézményekre vonatkozó előírások” című fejezetben leírtak érvényesek.

3.3.1. Felhasználók tájékoztatása

3.3.1.1. [kötelező]
A központi infrastruktúra üzemeltetője `http://www.eduroam.hu/` címen elérhető web szervert köteles üzemeltetni az eduroam felhasználók és tagintézmények tájékoztatása, naprakész információkkal való ellátása céljából. Minden információt köteles magyar, a külföldi felhasználóknak és tagintézményeknek (is) szóló információkat pedig magyar és angol nyelven közzé tenni. Az információknak tartalmazniuk kell az alábbiakat:

- magyarországi eduroam tagintézmények listája, hivatkozással az intézmények vendég felhasználóknak szóló tájékoztató weboldalára
- ismertető leírás az eduroam alapvető működéséről
- az eduroam szolgáltatást érintő ismert fennálló problémák ill. tervezett leállások
- hivatkozás az eduroam website-ra (`http://www.eduroam.org/`)
- ügyfélszolgálat elérhetőségei, ahova eduroam tagintézmények fordulhatnak az eduroamot érintő műszaki kérdésekben

3.3.1.2. [ajánlott]
Ajánlott a kizárólag magyarországi felhasználóknak szóló információkat is közzétenni magyar és angol nyelven egyaránt.

3.3.1.3. [kötelező]
A 3.2.2.9. pont szerint az intézmények által szolgáltatott adatokat a központi infrastruktúra üzemeltetője felviszi az eduroam térképes adatbázisára.

3.3.2. Központi RADIUS infrastruktúra

3.3.2.1. [kötelező]
A központi infrastruktúra üzemeltetője köteles két RADIUS szervert üzemeltetni, melyek azonos funkciójúak, egymás tartalékai. Ezek a RADIUS szerverek az eduroam autentikációs hierarchiában a `hu` csomópont feladatait látják el.

3.3.2.2. [kötelező]
A központi infrastruktúra RADIUS szerverei meg kell, hogy feleljenek az [RFC6614]-nek, így TLS feletti RADIUS üzenetváltásra is alkalmasnak kell lenniük.

3.3.2.3. [kötelező]
A központi infrastruktúra RADIUS szervereinek az [RFC6614] által alapértelmezettként meghatározott 2083-as TCP porton kell fogadniuk a RADIUS/TLS kapcsolatokat.

3.3.2.4. [kötelező]
A központi infrastruktúra RADIUS szervereit megadó, `_radsec._tcp.eduroam.hu` SRV bejegyzést kell készítenie és fenntartania a központi infrastruktúra üzemeltetőjének, hogy a tagintézmények erre hivatkozhassanak az általuk használt NAPTR bejegyzésekben.

3.3.2.5. [ajánlott]
Nemzetközi irányokba a lehetőség fennállása esetén ajánlott a RADIUS/TLS használata.

3.3.2.6. [kötelező]
TLS használata esetén a magyarországi központi infrastruktúra RADIUS szerverei F-Ticks napló üzeneteket kell, hogy küldjenek az európai eduroam statisztikákat gyűjtő szervereknek.

3.3.3. Autentikáció

3.3.3.1. [kötelező]
Ha a `User-Name` paraméter értéke alapján nem a `hu` csomópont felelős a kérdéses domainért, akkor a RADIUS `access-request` üzeneteket továbbítani kell

- (hazai és külföldi domain esetén) az eduroam autentikációs szerverek fa struktúrájának ágai mentén a paraméterben szereplő domainért felelős csomópont irányába, vagy
- (külföldi domain esetén) TLS felett a DNS-ből lekérdezett illetékes csomópont irányába.

Valós eduroam felhasználók csak intézményeknél lehetnek, ahol tanulói, hallgatói, vagy munkavállalói jogviszonyuk van. A `hu` csomóponton viszont hasznos lehet virtuális felhasználók létrehozása tesztelési célokra.

3.3.3.2. [kötelező]
A központi infrastruktúra üzemeltetője kizárólag tesztelési, felügyeleti,

hibadiagnosztikai célra definiálhat eduroam felhasználókat olyan eduroam domainben, amiért a `hu` csomópont felelős.

3.3.4. Üzemeltetés, hibaelhárítás

3.3.4.1. [kötelező]
A központi infrastruktúra üzemeltetője köteles naprakész nyilvántartást vezetni a magyarországi eduroam tagintézményekről.

3.3.4.2. [kötelező]
A központi infrastruktúra üzemeltetője köteles a magyarországi tagintézmények RADIUS szervereinek, valamint saját RADIUS szervereinek működőképességét automatikus felügyeleti rendszerrel monitorozni. A felügyeletnek része kell, hogy legyen az intézményi teszt azonosítókkal történő periodikus autentikációs kísérlet EAP-TTLS vagy PEAP használatával. Intézményi probléma észlelése esetén értesítenie kell az intézményi műszaki kapcsolattartót.

3.3.4.3. [ajánlott]
A tagintézmények RADIUS szervereinek aktuális állapotát ajánlott HTTP felületen elérhetővé tenni mindenki számára az Interneten.

Irodalomjegyzék

ERI: Eduroam ismertető, http://www.eduroam.hu/
NIIFAUP: A Nemzeti Információs Infrastruktúra Fejlesztési Program Felhasználói Szabályzata, http://www.niif.hu/aup/
RFC2865: C. Rigney, S. Willens, A. Rubens, W. Simpson, Remote Authentication Dial In User Service (RADIUS), 2000
RFC2866: C. Rigney, RADIUS Accounting, 2000
RFC3580: P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese, IEEE 802.1X RADIUS Usage Guidelines, 2003
RFC3748: B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, Extensible Authentication Protocol, 2004
RFC4282: B. Aboba, M. Beadles, J. Arkko, P. Eronen, The Network Access Identifier, 2005
RFC4372: F. Adrangi, A. Lior, J. Korhonen, J. Loughney, Chargeable User Identity, 2006
RFC5580: H. Tschofenig, F. Adrangi, M. Jones, A. Lior, B. Aboba, Carrying Location Objects in RADIUS and Diameter, 2009
RFC6614: S. Winter, M. McCauley, S. Venaas, K. Wierenga, Transport Layer Security (TLS) Encryption for RADIUS, 2012
RFC7593: K. Wierenga, S. Winter, T. Wolniewicz, The eduroam Architecture for Network Roaming, 2015

Verziókövetés:

Változat	Dátum	Módosítás leírása	Szerző	Jóváhagyás
0.2	2007-04-30	első változat	Jákó András, Mohácsi János	
0.9	2008-02-08	hyperlinkek hozzáadása, IPv6 konfigurációs ajánlások hozzáadása	Mohácsi János, Jákó András	
0.9b	2008-06-04	pontosítások	Borús András, Kovács Csaba, Mohácsi János	

0.10	2008-09-11	a dokumentum átszervezése: a műszaki követelmények és a definíciók bekerültek a szabályzatba; definíciók pontosítása	Jákó András	
0.11	2008-09-26	sajtóhibák javítása	Jákó András	
1.0	2008-11-13	1.0 verzió az NIIF MT 2008-10-09-i határozata alapján	Jákó András, Mohácsi János	
2.0a1	2014-02-14	2.0 tartalmi változások első csoportja; a tartalmi változásokat felsoroló „Változások” fejezet hozzáadása; sajtóhibák javítása	Jákó András	
2.0a2	2014-02-21	2.0 tartalmi változások második csoportja	Jákó András	
2.0a3	2016-03-31	További apró tartalmi változások, sajtóhibák javítása, ill. a „Változások” fejezet áthelyezése a kísérő dokumentumba.	Jákó András	
2.0b1	2016-04-06	Központi térképre vonatkozó követelmények. Intézményközi egyeztetésre előkészített változat.	Jákó András, Mohácsi János	
2.0	2016-05-13	Az intézményközi egyeztetés alapján az accounting üzenetek proxyzására vonatkozó előírás módosítása, sajtóhibák javítása. 2.0 verzió véglegesítése.	Borús András, Jákó András, Keresztury Balázs, Mohácsi János	