Roamingová politika, návrh

1.0 Úvod

1.1 Tento dokument vymedzuje vzťahy a pravidla týkajúce sa poskytovania a príjmania prístupu k Internetu v roamingu pre členov slovenskej eduroam federácie a nadväzuje tak na európsku konfederačnú politiku, ktorá určuje pravidlá pre spoluprácu jednotlivých federácii.

1.2 *eduroam* vznikol v rámci európskeho projektu národných výskumnych a vzdelávacích sietí s cieľom poskytnúť komunite svojich používateľov prístup k internetu počas návštevy participujúcej organizácie, teda v roamingu. Názov *eduroam* vznikol skrátením slov “educational roaming” a spolu s logom *eduroam* sú registrovanou ochrannou známkou spoločnosti TERENA (The Trans-European Research and Education Networking Association).

1.3 Viac informácií o eduroam je dostuných na *www.eduroam.org*.

2.0 Definícia pojmov

2.1 *eduroam* je akademický roamingový systém poskytujúci sieťové pripojenie pre svojich používateľov v participujúcich organizáciách. Prístup je založený na zabezpečenej autentifikácii v domácej inštitúcii.

2.2 Slovenská eduroam federácia je zoskupenie organizácií zapojených do systému eduroam v rámci Slovenskej republiky, a to v akejkoľvek role (viď sekcia 4). Pre potreby tohto dokumentu sa eduroam federáciou myslí slovenská eduroam federácia.

2.3 Európska eduroam konfederácia je zoskupenie jednotlivých národných eduroam federácii v rámci Európy. Federácie sú spravidla zastúpené organizáciami, ktoré prevádzkujú siete národného výskumu a vzdelávania – NREN (v SR túto rolu zastáva SANET).

2.4 Poskytovateľ identity je subjekt, u ktorého má používateľ vedené svoje overovacie údaje potrebné pre prihlásenie k sieti. Zväčša sa jedná o domovskú inštitúciu, ku ktorej má používateľ organizačno právny vzťah – je zamestnancom, študentom a pod. Poskytovateľ identity má oprávnenie a povinnosť rozhodnúť o povolení či zamietnutí autentifikačnej požiadavky na prístup používateľa k zdroju (napr. sieťovej konektivite).

2.5 Poskytovateľ zdrojov je subjekt, ktorý poskytuje používateľom sieťové služby. Rozhodnutiu o tom čí používateľ má alebo nemá právo využiť požadovaný zdroj predchádza autentifkácia používateľa prenesená na poskytovateľa identity daného používateľa. Poskytnutie ktorejkoľvek zo služieb zabezpečovaných poskytovateľom zdrojov autorizuje sám poskytovateľ zdrojov.

3.0 Vymedzenie rolí a povinností subjektov zapojených do eduroam federácie

3.1 Správca eduroam federácie

3.1.1 Rolu správcu eduroam federácie (ďalej len správca) vykonáva v rámci Slovenskej republiky SANET. Správca je vykonávateľom roamingovej politiky na národnej úrovni, pričom postupuje v súlade s európskou konfederačnou politikou.

3.1.2 Rola SANETu je trojaká, (1) koordinuje dianie a poskytuje podporu na službu eduroam technikom nominovaným organizáciami participujúcimi vo federácii , a (2) udržuje prepojenie s európskou eduroam komunitou a jej autentifikačnými servermi, a (3) prispieva k ďalšiemu rozvoju konceptu eduroam.

3.1.3 SANET zaisťuje správu a rozvoj národnej siete autentifikačných serverov, ktorá spája participujúce organizácie. Správca nepreberá záväzky za žiadne následky, ktoré sú dôsledkom zneužitia alebo výpadkov, prípadne straty prístupu k službe. Poskytovatelia identít a poskytovatelia zdrojov v eduroam, či už sa nachádzajú v rovnakej alebo iných federáciách, neberú na zodpovednosť jeden druhého.

3.1.4 SANET zaisťuje technickú podporu v súvislosti s napojením sa do federácie, ďalej zaisťuje technickú podporu a údržbu dedikovanej stránky s informáciami o službe, roamingovej politike, pravidlách a mailing list.

3.1.5 SANET koordinuje komunikáciu medzi pariticipujúcimi organizáciami tak, aby pravidlá obsiahnuté v tejto politike boli dodržané v primeranom čase a ako nástroj poslednej inštancie má právo zaviesť technické opatrenia.

3.1.6 SANET bude s technikmi nominovanými participujúcou organizáciou spolupracovať pri testovaní jedného alebo viacerých z nasledovných aspektov (1) počiatočné pripájanie sa, (2) autentifikačné a autorizačné procesy a (3) ponúkané autorizované služby, a pri kontrole (1) činností súvisiacich s logovaním a (2) príslušného nastavenia funkcionality autentifikačného servera v súlade s roamingovou politikou.

3.2 Poskytovatelia identít

3.2.1 Rolou poskytovateľa identít (teda domovskej organizácie používateľa) je fungovať ako poskytovateľ osobných prístupových údajov pre registrovaných zamestnancov a študentov. Rovnako poskytovateľ identít vykonáva funkciu technickej podpory a podpory služby pre svojich používateľov, ktorí požadujú prístup k službe eduroam u poskytovateľa zdrojov, teda u hostiteľa. Iba osoby nominované organizáciou ako technický kontakt môžu smerom na SANET v mene svojich používateľov eskalovať požiadavky týkajuce sa technickej podpory, podpory služby alebo požiadavky týkajúce sa bezpečnosti.

3.2.2 Poskytovateľ identít je povinný spolupracovať so SANETom v súvislosti s témou bezpečnosti, zneužitia a podobne.

3.3 Poskytovatelia zdrojov

3.3.1 Rola poskytovateľa zdrojov je poskytnúť prístup k internetu overeným používateľom eduroam (založené na dôvere, že autentifikačná kontrola používateľa jeho poskytovateľom identity, teda domovskou organizáciou používateľa, a následná odozva su právoplatné). Poskytovateľ zdrojov sám autorizuje poskytnutie ktorejkoľvek zo služieb, ktoré zabezpečuje.

3.3.2 V prípade, že dochádza k monitorovaniu aktivity používateľa musí poskytovateľ zdrojov jasne oznámiť tento fakt vrátane informácie ako je aktivita používateľa monitorovaná, dáta o nej uchovávané a prístupné a to takým spôsobom, aby konal v súlade s legislatívou.

3.3.3 Poskytovateľ zdrojov sa musí riadiť touto roamingovou politikou a dodržiavať postupy a pokyny v nej uvedené.

3.3.4 Poskytovateľ zdrojov musí spolupracovať so SANETom vo všetkých záležitostiach týkajúcich sa eduroam.

3.4 Požívatelia

3.4.1 Rola používateľa je v princípe vždy rola hosťa, ktorý požaduje prístup k internetu u poskytovateľa služby eduroam. Používateľ musí dodržiavať pravidlá definované v prevádzkovom poriadku svojho poskytovateľa identity a zároveň rešpektovať prevádzkový poriadok hostiteľskej organizácie. V prípadoch keď sa predpisy líšia, platia tie striktnejšie. Používatelia musia ako minimum dodržiavať relevantné zákony krajiny, kde sa fyzicky nachádzaju, či už je to doma alebo v zahraničí.

3.4.2 Používatelia su zodpovední za svoje prístupové údaje, za používanie svojich prístupových údajov a služieb, ktoré im môžu sprístupniť.

3.4.3 Na používateľovi spočíva zodpovednosť aby sa primeraným spôsobom uistil, že je pripojený k pravej eduroam službe (na základe doporučení svojej domovskej organizácie), skôr ako vyplní a odošle svoje prístupové údaje. Primárnym spôsobom ako to dosiahnuť je overiť platnost serverového certifikátu, ktorý je používateľovi prezentovaný pri prihlasovaní sa, ešte predtým než zadá svoje prístupové údaje.

3.4.4 Používateľ musí bezodkladne oznámiť svojej domácej organizacii ak si myslí, že došlo k odhaleniu alebo zneužitiu jeho prístupových údajov.

3.4.5 Používateľ by mal hostiteľskej organizácii (ak je to možné) a domácej organizácii oznámiť chyby týkajúce sa eduroam služby.

4.0 Základná služba

4.1 Poskytovatelia identít musia prevádzkovať autentifikačný server v súlade s technickými pokynmi a roamingovou politikou eduroam dostupnými na www.sanet.sk/eduroam/policy.pdf. Kvôli udržaniu dostupnosti služby je odporúčaná prevádzka sekundárneho autentifikačného servera.

4.2 Autentifikačný server poskytovateľa identít musí byť dostupný z národných autentifikačných serverov SANETu pre účel autentifikácie a účtovania.

4.3 Poskytovateľ identít musí vytvoriť eduroam testovací účet (eduroam používateľské meno a heslo), ktorý sprístupní spávcovi federácie SANET. Testovací účet napomôže pri realizácii nového pripojenia, pokračujúceho monitorovania, podpore a pri odhaľovaní chýb. Ak dôjde k zmene hesla testovacieho účtu, domovská organizácia musi včas upovednomiť správcu federácie SANET.

4.4 Poskytovateľ zdrojov môže ponúknuť viaceré prístupové média, avšak ako minimum je vyžadovaný bezdrôtový prístup IEEE 802.11b, zatiaľ čo 802.11g je odporúčaný.

4.5 Poskytovateľ zdrojov musí poskytnúť SSID “eduroam” a autentifikáciu prostredníctvom IEEE 802.1X Extensible Authentication Protocol (EAP), s výnimkou EAP-MD5, a tým podporiť konzistentnú úroveň služby a minimálnu úroveň bezpečnosti. SSID “eduroam” by malo byť oznamované.

4.6 Poskytovateľ zdrojov musí ako minimum implementovať metódu IEEE 802.1X a poskytovať šifrovaciu schému WPA/TKIP, alebo lepšiu.

4.7 Poskytovateľ zdrojov musí ako minimum umožniť:

- Štandardnú IPSec VPN: IP protokol 50 (ESP) a 51 (AH) obojsmerne; UDP/500 (IKE) na

výstupe

- OpenVPN 2.0: UDP/1194
- IPv6 Tunnel Broker service: IP protokol 41 obojsmerne
- IPsec NAT-Traversal UDP/4500
- Cisco IPSec VPN nad TCP: TCP/10000 na výstupe
- PPTP VPN: IP protokol 47 (GRE) obojsmerne; TCP/1723 na výstupe
- SSH: TCP/22 na výstupe
- HTTP: TCP/80 na výstupe
- HTTPS: TCP/443 na výstupe
- IMAP2+4: TCP/143 na výstupe
- IMAP3: TCP/220 na výstupe
- IMAPS: TCP/993 na výstupe
- POP: TCP/110 na výstupe
- POP3S: TCP/995 na výstupe
- Passive (S)FTP: TCP/21 na výstupe
- SMTPS: TCP/465 na výstupe
- SMTP submit with STARTTLS: TCP/587 na výstupe
- RDP: TCP/3389 na výstupe
- SIP: UDP/5060 obojsmerne
- RTP: UDP/16384 až po UDP/16484 obojsmerne

4.8 Poskytovateľ zdrojov by mal vyhradiť dedikovanú virtuálnu lokálnu sieť (VLAN) pre návštevníkov autentifikovaných v rámci eduroam, ktorá by mala byť oddelená od ostatných sieťových služieb organizácie.

4.9 Za prístup k sieti v rámci eduroam nesmie poskytovateľ zdrojov účtovať žiadne poplatky. Eduroam je založený na modeli zdieľaného prístupu, kde si poskytovatelia zdrojov vzájomne ponúkaju a prijímajú prístup k Internetu pre svojich používateľov.

5.0 Logovanie

5.1 Poskytovateľ zdrojov aj poskytovateľ identít musia logovať každú autentifikačnú požiadavku; nasledné informácie musia byť zaznamenané

(1) dátum a čas prijatia autentifikačnej požiadavky;

(2) výsledok autentifikácie oznámený autentifikačnou databázou;

(3) poskytovatelia identít aj vnútornú identitu požiadavky;

(4) hodnota atribútu používateľské meno (user name) v požiadavke (tkz. vonkajšia EAP-identita).

(5) hodnota atribútu calling station id v požiadavke.

5.2 Poskytovateľ zdrojov aj poskytovateľ identít musia logovať každú účtovnú požiadavku; nasledovné informácie musia byť zaznamenané

(1) dátum a čas prijatia účtovnej požiadavky;

(2) hodnota atribútu používateľské meno (user name) v požiadavke;

(3) hodnota atribútu ID účtovnej relácie (accounting session ID);

(4) druh stavu účtovnej požiadavky (accounting status type).

5.3 Poskytovateľ zdrojov musí logovať každú DHCP transakciu zahŕňajúc

(1) dátum a čas vystavenia DHCP pridelenia klientovi;

(2) MAC adresa klienta;

(3) IP adresa alokovaná klientovi.

5.4 Poskytovateľ zdrojov musí uchovávať logy uvedené v sekcii 5.3 minimálne po dobu šesť mesiacov a maximálne po dobu dvanásť mesiacov. Vzájomná súčinnosť ohľadom obsahu logov je obmedzená na nominované technické kontakty v systéme eduroam a technické kontakty správcu federácie SANET pre použitie v súvislosti s riešením bezpečnostných incidentov alebo zneužítím siete, ktoré bolo ohásené správcovi federácie.

5.5 Všetky relevantné logy musia byť vytvárané s využitím synchronizácie voči spoľahlivému zdroju času.

6.0 Podpora

6.1 Poskytovateľ identít musí poskytnúť podporu svojim používateľom žiadajúcim o prístup u poskytovateľa zdrojov.

6.2 Poskytovateľ zdrojov by mal poskytnúť technickú podporu používateľom žiadajúcim o prístup k eduroam a v nevyhnutnej miere spolupracovať pri riešení s ich poskytovateľom identity.

6.3 Poskytovateľ zdrojov musí miestne informácie týkajúce sa eduroam publikovať na

dedikovaných stránkach web servera svojej organizácie s minimálnymi nasledovnými informáciami,

(1) Text, ktorý potvrzduje súlad s obsahom tohto dokumentu (vrátane url odkazu) o roamingovej politike publikovanom na www.eduroam.sk;

(2) Url odkaz na dokument s informáciami o pravidlách používania siete u poskyvateľa zdrojov alebo jeho ekvivalent;

(3) Zoznam alebo mapu zobrazujúcu pokrytie prístupu k eduroam;

(4) Detail ohľadom nastavenia eduroam SSID, je oznamované alebo nie je oznamované;

(5) Detaily autentifikačného procesu a ponúkané autorizované služby;

(6) Detaily ohľadom používania netransparentného aplikačného proxy servera vrátane konfiguračného návodu pre používateľov (ak je tento bod relevantný);

(7) Url odkaz na web stránku www.eduroam.sk a zobrazenie loga eduroam s označením ochrannej známky;

(8) Kde dochádza k monitorovaniu aktivity používateľov, musí poskytovateľ zdrojov tento fakt jasne oznámiť, aby vyhovel národnej legislatíve, vrátane informácie ako je aktivita používateľov monitorovaná, akú dobu budú informácie o aktivite používateľov držané a kto má k nim prístup.

(9) Kontaktné údaje na príslušnú technickú podporu, ktorá zodpovedá za služby v súvislosti s eduroam.

7.0 Komunikácia

7.1 Poskytovateľ identít musí SANET oboznámiť s kontaktnými údajmi dvoch nominovaných technikov a o akejkoľvek zmene v kontaktných údajoch musí SANET včas vyrozumieť.

7.2 Poskytovateľ identít musí menovať prostredníka a jeho kontaktné údaje, ktorý reaguje pri témach týkajúcich sa bezpečnosti. Môže ísť o rovnakú osobu ako nominovaný technický kontakt.

7.3 Pripojené organizácie musia včas informovať SANET o nasledovných incidentoch: (1) narušenie bezpečnosti; (2) zneužitie; (3) poruchy služby; (4) zmeny v riadení prístupu (napr. povolenie alebo blokovanie prístupu používateľa alebo realmu/domény)

8.0 Právomoci, dodržiavanie politiky a sankcie

8.1 Vykonávateľom tejto roamingovej politiky je správca eduroam federácie, teda SANET.

8.2 Všetky zmeny v tejto roamingovej politike budú konzultované s organizáciami

zapojenými do federacie.

8.3 Napojením autentifikačných serverov organizácie k autentifikačým serverom správcu federácie potvrdzuje organizácia svoj plný súhlas s touto roamingovou politikou a zaväzuje sa ju dodržiavať. Každá z pripojených organizácii bude mať lehotu jeden mesiac od dátumu nadobudnutia účinnosti zmien, kedy zostane naďalej pripojená na znak súhlasu so znením roamingovej politiky alebo ukončí napojenie svojich autentifikacných serverov ako znak neprijateľnosti novej verzie politiky.

8.4 V prípadoch naliehavej potreby s cieľom chrániť integritu a bezpečnosť systému eduroam má SANET právo prerušiť alebo obmedziť prístup k eduroam len na tie z pripojených organizácii, ktoré sa dokážu prispôsobiť požadovaným zmenám. SANET informuje pripojené organizácie o takýchto incidentoch, výpadkoch a spôsoboch nápravy.

8.5 SANET emailom odoslaným na nominovaný technický a/alebo bezpečnostný kontakt pripojenej organizácie upozorní na technický rozpor alebo porušenie politiky alebo na incident vyžadujúci si riešenie. Ak upozornenie zostane bez včasnej reakcie, prípadne ak rozpor alebo incident majú dopad na bezpečnosť a integritu systému eduroam, má SANET právo blokovať prístup organizácie k eduroam.

8.6 Poskytovateľ zdrojov môže zabrániť využívaniu svojej siete používateľmi prislúchajúcimi ku konkrétnemu poskytovateľovi identít nastavením autentifikačného servera tak, že odmietne konkrétny realm/doménu. V niektorých prípadoch môže byť poskytovateľ zdrojov oprávnený blokovať jednotlivého návštevníka.

8.7 Poskytovateľ identít má právo obmedziť alebo úplne zablokovať prístup svojho používateľa k eduroam v konfigurácii vlastného autentifikačného servera alebo odstránením používateľa z autentifikačnej databázy.

8.8 Poskytovateľ identít musí tiež zaistiť, že jeho vnútorné predpisy oprávňujú podrobiť používateľov, ktorí porušia túto politiku, zodpovedajúcemu disciplinárnemu konaniu nezávisle od lokácie používateľov.