Polska polityka eduroam

(szkic wersja 0.04)

1. Pojęcia wstępne

1.1. Definicje i zastrzeżenia

1.1.1. Niniejszy dokument określa zasady współpracy przy utrzymaniu usługi powszechnego, mobilnego dostępu do Internetu w ramach polskiego środowiska naukowego.

1.1.2. ***eduroam*** jest zastrzeżonym znakiem towarowym zarejestrowanym przez organizację TERENA i jest skrótem od „*educational roaming*" – inicjatywy, która wyrosła z działań europejskich akademickich sieci komputerowych.

1.1.3. Znak oraz nazwa ***eduroam*** mogą być używane tylko w odniesieniu do inicjatywy ***eduroam*** i zasobów z nią związanych. Dodatkowe informacje i dokumenty na temat formalnych aspektów ***eduroam*** są dostępne pod adresem www.eduroam.org.

1.1.4. Podstawowym celem ***eduroam*** jest międzynarodowa współpraca w zakresie upowszechnienia dostępu do Internetu pracownikom i studentom instytucji akademickich i naukowych.

1.1.5. Pojęcie ***eduroam*** obejmuje zarówno projekt pilotowy o zasięgu ogólnoświatowym, jak również usługę sieci GEANT2.

1.1.6. ***eduroam*** jest tworzony w postaci federacyjnej struktury zaufania, której podmiotami są:

1. krajowe federacje ***eduroam,***
2. instytucje występujące w roli koordynatorów krajowych federacji ***eduroam,***
3. europejska konfederacja ***eduroam*** jako stowarzyszenie europejskich federacji krajowych,
4. konfederacje ***eduroam*** w innych regionach świata.

1.2. Europejska konfederacja *eduroam*

1.2.1. Celem działania europejskiej konfederacji ***eduroam*** jest koordynacja współpracy krajowych federacji ***eduroam***.

1.2.2. Zasady działania europejskiej konfederacji ***eduroam*** określa *Europejska Polityka eduroam*.

1.3. Polska federacja *eduroam*

1.3.1. Krajowym koordynatorem polskiej federacji ***eduroam*** jest Poznańskie Centrum Superkomputerowo-Sieciowe (PCSS) działające w imieniu Konsorcjum PIONIER.

1.3.2. Operatorem polskiej federacji ***eduroam*** jest Uczelniane Centrum Informatyczne Uniwersytetu Mikołaja Kopernika w Toruniu (UCI UMK).

1.3.3. Polska federacja ***eduroam*** działa w oparciu o:

1. *Polską Politykę eduroam*,
2. *Europejską Politykę eduroam*,
3. umowy zawarte między członkami federacji a PCSS,
4. umowę między PCSS i UMK w sprawie pełnienia roli operatora polskiej federacji ***eduroam***,
5. umowę PCSS – TERENA w sprawie udziału Polski w europejskiej konfederacji ***eduroam***.

1.4. Operator polskiej federacji *eduroam*

1.4.1. Zadania operatora polegają na:

1. reprezentowaniu polskiej federacji ***eduroam*** w konfederacji europejskiej,
2. nadzorowaniu i koordynowaniu rozwoju ***eduroam*** w Polsce,
3. prowadzeniu krajowego serwera pośredniczącego i nadzorowaniu działania krajowego serwera zapasowego,
4. udziale w ciałach koordynujących międzynarodowy rozwój ***eduroam***,
5. monitorowaniu sprawności serwerów uwierzytelniających członków polskiej federacji ***eduroam***,
6. koordynowaniu obsługi zdarzeń niepożądanych (nadużyć prawa, etykiety itp.) związanych z działaniem ***eduroam***,

7. przyjmowaniu zgłoszeń od nowych członków federacji ***eduroam***,
8. utrzymywaniu serwisu www.eduroam.pl,
9. przygotowywaniu umów między PCSS a członkami federacji.

1.5. Członkowie polskiej federacji *eduroam*

1.5.1. Członkiem polskiej federacji ***eduroam*** może być instytucja posiadająca status:
1. szkoły wyższej,
2. instytutu badawczego.

1.5.2. Podstawowym warunkiem przystąpienia do polskiej federacji ***eduroam*** jest wyrażenie zgody na występowanie w roli instytucji udzielającej gościnnego dostępu do Internetu oraz akceptacja postanowień niniejszej polityki.

1.5.3. Każdy członek polskiej federacji ***eduroam*** ma prawo do występowania w roli instytucji uwierzytelniającej i tym samym zapewnienia swoim użytkownikom dostępu do Internetu na terenie wszystkich instytucji współpracujących z ***eduroam***.

1.5.4. Obowiązki członków polskiej federacji ***eduroam***

Jako i*nstytucja udzielająca gościnnego* dostępu do Internetu członek federacji ***eduroam*** zobowiązuje się do:
1. bezpłatnego udostępnienia sieci bezprzewodowej prowadzonej zgodnie ze „***Specyfikacją Techniczną***", wszystkim osobom, które mogą zostać poprawnie uwierzytelnione przez innych członków ***eduroam***;
2. prowadzenia serwisu WWW pod adresem http://eduroam.(nazwa_domenowa_instytucji), w którym muszą być zawarte podstawowe informacje dla gości w językach polskim i angielskim zgodnie ze „***Specyfikacją techniczną***".

Jako *instytucja uwierzytelniająca* członek federacji eduroam zobowiązuje się do:
1. potwierdzania tożsamości zarejestrowanych osób za pomocą serwera uwierzytelniającego;
2. utrzymywania zapisów wszystkich operacji uwierzytelnienia, zgodnie z wymaganiami opisanymi w „***Specyfikacji technicznej*"**;
3. współpracy z operatorem polskiej federacji ***eduroam*** w wypadkach naruszenia bezpieczeństwa, etykiety sieciowej, prawa itp.;
4. udzielania wsparcia technicznego zarejestrowanym przez nią osobom pragnącym skorzystać z zasobów ***eduroam*** udostępnianych lokalnie i w innych instytucjach biorących udział w projekcie.

1.5.5. Członkowie polskiej federacji ***eduroam*** nie będą występować względem siebie z roszczeniami cywilno-prawnymi z tytułu ewentualnych incydentów sieciowych.

1.6. Zasoby *eduroam*

1.6.1. Przez zasoby ***eduroam*** rozumie się punkty (bezprzewodowe i przewodowe) dostępu do sieci, łącznie z mechanizmami uwierzytelniania użytkowników.

1.6.2. Zasoby ***eduroam*** muszą być oznakowane logo ***eduroam***, przy czym dopuszczalne jest oznakowanie całych budynków, bądź obszarów w tych budynkach, gdzie sieć jest dostępna.

1.7. Użytkownicy

1.7.1. Użytkownikiem ***eduroam*** może być osoba związana z instytucjami uwierzytelniającymi stowarzyszonymi w ***eduroam***.

1.7.2. Użytkownik jest odpowiedzialny za wszelkie działania sieciowe dokonane po uwierzytelnieniu przy pomocy jego danych uwierzytelniających. W przypadku podejrzenia, że dane uwierzytelniające mogły się dostać w ręce osób trzecich, użytkownik jest zobowiązany do niezwłocznego zawiadomienia o tym fakcie administratora w swojej instytucji macierzystej.

1.7.3. Użytkownik powinien dołożyć starań, aby przed wysłaniem danych uwierzytelniających upewnić się, że korzysta z autentycznej usługi eduroam (zgodnie z zaleceniami swojej instytucji macierzystej).

1.7.4. Użytkownik musi być świadomy, że fakt gościnnego korzystania z sieci jest odnotowywany w logach systemowych zarówno instytucji udostępniającej zasoby jak i jego macierzystej instytucji uwierzytelniającej.

1.7.5. Użytkownik musi działać zgodnie z lokalnym prawem i regulaminem sieci komputerowej, z której korzysta.

2. Specyfikacja techniczna

2.1. Słowa kluczowe używane w tekście

2.1.1. Słowa „MUSI”, „POWINIEN” „NIE WOLNO” i ich odmiana, pisane wielkimi literami są używane zgodnie z definicją ich angielskich odpowiedników określonych w RFC 2119, w szczególności słowo „POWINEN” należy rozumieć w taki sposób, że niespełnienie warunku opatrzonego tą klauzulą jest dopuszczalne tylko w szczególnie uzasadnionych przypadkach.

2.2. Rola instytucji udostępniająca zasoby

2.2.1. Sieć bezprzewodowa udostępniana jako zasób ***eduroam*** podlega następującym zasadom:

1. sieć MUSI być zgodna ze standardem IEEE 802.11b, przy czym zaleca się stosowanie urządzeń zgodnych z 802.11g;
2. dodatkowo sieć MOŻE stosować standard 802.11a;
3. nazwa sieci (SSID) MUSI mieć wartość „eduroam”;
4. SSID eduroam POWINIEN być rozgłaszany;
5. sieć MUSI wspierać szyfrowanie WPA-TKIP w połączeniu z 802.1x (tzw. WPA-Enterprise);
6. przy dostępie do sieci NIE WOLNO stosować portali WWW wymagających wprowadzenia danych uwierzytelniających użytkownika.

2.2.2. Sieć przewodowa udostępniana jako zasób ***eduroam*** MUSI stosować uwierzytelnianie 802.1x.

2.2.3. Sieci udostępniane jako zasób ***eduroam*** MUSZĄ w sposób przezroczysty traktować protokół EAP.

2.2.4. Gościnny dostęp do Internetu, udostępniany jako zasób ***eduroam***, POWINIEN być otwarty.

2.2.5. W ramach gościnnego dostępu do internetu, udostępnianego jako zasób eduroam MUSI być zagwarantowany dostep do usług:

1. Standard IPSec VPN: IP protokoły 50 (ESP) and 51 (AH); UDP/500 (IKE);
2. OpenVPN 2.0: UDP/1194
3. IPv6 Tunnel Broker service: IP protokół 41
4. IPsec NAT-Traversal UDP/4500
5. Cisco IPSec VPN over TCP: TCP/10000
6. PPTP VPN: IP prtokół 47 (GRE); TCP/1723;
7. SSH: TCP/22;
8. HTTP: TCP/80;
9. HTTPS: TCP/443;
10. IMAP2+4: TCP/143;
11. IMAP3: TCP/220;
12. IMAPS: TCP/993;
13. POP: TCP/110;
14. POP3S: TCP/995;
15. Passive (S)FTP: TCP/21;
16. SMTPS: TCP/465;
17. SMTP submit z STARTTLS: TCP/587;
18. RDP: TCP/3389.

2.2.6. Instytucja udostępniająca zasoby MOŻE stosować przezroczyste proxy zabezpieczające przed wysyłaniem spamu i propagacją wirusów.

2.2.7. Instytucja udostępniająca zasoby, we własnym interesie, POWINNA stosować środki techniczne umożliwiające identyfikację użytkowników działających w sieci. Brak odpowiednich środków i logów uniemożliwi przeniesienie odpowiedzialności za naruszenia prawa dokonane z sieci gościnnej. W szczególności:

1. wskazane jest aby gościnny dostęp do Internetu był realizowany w wydzielonym VLAN-ie;
2. w ramach gościnnego dostępu do Internetu NIE POWINNNO się stosowań adresów prywatnych i

NAT;

3. stosowane środki techniczne POWINNY pozwalać na powiązanie działań użytkownika ***eduroam*** z konkretną sesją uwierzytelnienia, w szczególności niemożliwa powinna być zmiana adresu IP na inny niż nadany użytkownikowi w czasie logowania do sieci.;

2.2.8. Instytucja udostępniająca zasoby MUSI przechowywać logi wiążące adresy IP z sesjami uwierzytelniania. Czas przechowywania logów NIE MOŻE być krótszy niż 6 miesięcy. Logi MUSZĄ być znakowane czasem synchronizowanym za pomocą protokołu NTP i MUSZĄ zawierać:

1. czas uwierzytelnienia i przydzielenia adresu IP,
2. adres MAC klienta,
3. adres IP klienta,

2.2.9. Instytucja MUSI prowadzić po polsku i angielsku informacyjny serwis WWW przeznaczony dla gości i zawierający przynajmniej:

1. logo ***eduroam*** wraz z odsyłaczem do strony www.eduroam.pl;
2. tekst stwierdzający przynależność instytucji do polskiej federacji ***eduroam*** i akceptację niniejszej polityki (łącznie z odsyłaczem do dokumentu umieszczonego w ogólnopolskim serwisie ***eduroam***)
3. informacje o obszarze, na którym jest udostępniana usługa ***eduroam***;
4. informacje techniczne o udostępnianych zasobach ***eduroam***, a więc: rodzaju protokołu bezprzewodowego (802.11b, 802,11g, 802.11a), rozgłaszaniu lub nierozgłaszaniu SSID eduroam, rodzaju szyfrowania (WPA/TKIP, WPA2/AES itp.);
5. informacje o stosowanych ogranicznikach dostępu (stosowanych filtrach) oraz o zakresie zbieranej informacji o połączeniach;
6. informacje (lub odsyłacz) do lokalnych zasad korzystania z sieci.

2.3. Rola instytucji uwierzytelniającej

2.3.1. Serwer uwierzytelniający instytucji uwierzytelniającej MUSI stosować bezpieczne metody EAP. EAP-MD5 jest uważany za niedostatecznie bezpieczny i w związku z tym NIE MOŻE być stosowany. Zalecanymi metodami EAP są TLS, TTLS-PAP, PEAP.

2.3.2. Instytucja uwierzytelniająca MUSI dołożyć starań, aby oprogramowanie 802.1x, z którego korzystają uwierzytelniane przez nią osoby, było skonfigurowane w sposób uniemożliwiający przesłanie danych uwierzytelniających do niepowołanego serwera.

2.3.3. Instytucja uwierzytelniająca MUSI dołożyć starań, aby osoby przez nią uwierzytelniane znały podstawowe zasady bezpieczeństwa przy korzystaniu z sieci bezprzewodowych.

2.3.4. Instytucja uwierzytelniająca MUSI przechowywać logi systemowe dotyczące uwierzytelnień ***eduroam*** dokonanych spoza jej własnej sieci. Czas przechowywania logów NIE MOŻE być krótszy niż 6 miesięcy. Logi MUSZĄ być znakowane czasem synchronizowanym za pomocą protokołu NTP i MUSZĄ zawierać:

1. czas otrzymania zlecenie uwierzytelnienia,
2. identyfikator uwierzytelniającego zlecenia protokołu RADIUS,
3. rezultat uwierzytelnienia,
4. dane pozwalające na zidentyfikowanie użytkownika, którego uwierzytelniono.

2.3.5. Instytucja MUSI udostępnić operatorowi polskiej federacji ***eduroam*** konto testowe służące do monitorowania poprawności pracy serwera uwierzytelniającego tej instytucji.

2.3.6. Instytucja MUSI wyznaczyć administratorów odpowiedzialnych za kontakty z operatorem polskiej federacji ***eduroam***.

3. Incydenty sieciowe

3.1. Pod pojęciem incydentów sieciowych rozumiane będą naruszenia prawa, naruszenia etykiety internetowej oraz naruszenia lokalnych regulacji instytucji udostępniających zasoby przez użytkowników ***eduroam*** korzystających z gościnnego dostępu do Internetu.

3.2. Naruszenia prawa

3.2.1. W przypadkach, kiedy z instytucją udostępniającą zasoby skontaktują się właściwe organy ścigania, w celu pozyskania informacji na temat konkretnego incydentu z udziałem adresu IP przydzielonego w efekcie poprawnego uwierzytelnienia eduroam, instytucja MUSI:

1. zlokalizować fragmenty logów odpowiadających danemu incydentowi i przekazać je uprawnionym organom ścigania, razem z informacją, że zlokalizowanie konkretnej osoby będzie możliwe we współpracy z pozostałymi elementami struktury ***eduroam*** i kontaktami do operatora polskiej federacji ***eduroam;***
2. poinformować operatora polskiej federacji ***eduroam*** o wystąpieniu incydentu i przekazać mu dane na temat czasu sesji uwierzytelniania i odnotowanego identyfikatora użytkownika.

3.2.2. Operator polskiej federacji ***eduroam*** ustala (być może z operatorem głównego serwera ***eduroam***) dane instytucji uwierzytelniającej odpowiedzialnej za użytkownika i przekazuje te dane organom ścigania.

3.2.3. Tylko macierzysta instytucja uwierzytelniająca może przekazać dane osobowe użytkownika i czyniąc to MUSI stosować się do ograniczeń stawianych przez ustawę o ochronie danych osobowych.

3.3. Naruszenia etykiety sieciowej i lokalnych regulacji

3.3.1. W przypadkach, kiedy incydenty nie naruszają prawa, ale są działaniami niepożądanymi z punktu widzenia instytucji udostępniającej zasoby, administrator ***eduroam*** w tej instytucji zawiadamia o incydencie operatora polskiej federacji ***eduroam***.

3.3.2. Operator polskiej federacji ***eduroam*** przejmuje sprawę, w celu zawiadomienia instytucji macierzystej użytkownika o problemie i spowodowania, by incydent nie mógł się powtórzyć.

3.3.3. Instytucja udostępniająca zasoby ma prawo zablokować uwierzytelnianie wszystkich użytkowników związanych z instytucją, której użytkownik spowodował incydent. Możliwość uwierzytelniana powinna zostać przywrócona po wyjaśnieniu sprawy.

4. Ustalenia końcowe

4.1. Instytucją odpowiedzialną za wdrażanie niniejszej polityki jest krajowy koordynator polskiej federacji ***eduroam***.

4.2. Wszelkie zmiany niniejszej polityki będą dokonywane w drodze konsultacji z członkami polskiej federacji ***eduroam***.

4.3. Instytucje partycypujące obecnie w pilotowym projekcie eduroam będą musiały przejąć niniejszą politykę w terminie 3 miesięcy od jej ogłoszenia. W przypadku odmowy przyjęcia niniejszej polityki, instytucja zostanie odłączona od struktury uwierzytelniającej ***eduroam***.