Polska polityka eduroam

(wersja 1.0 z dnia 31.03.2008)

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 *Service Activity 5* sieci GEANT2.

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

1. krajowe federacje ***eduroam***;
2. operatorzy krajowych, akademickich sieci komputerowych reprezentujący krajowe federacje ***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* i dokument definiujący usługę ***eduroam*** – *eduroam Service Definition and Implementation Plan*.

1.3. Usługa eduroam w polskiej sieci PIONIER

1.3.1. ***eduroam*** jest usługą dodaną dostępną w sieci PIONIER i sieciach MAN Konsorcjum PIONIER adresowaną do środowiska nauki w Polsce.

1.3.2. Usługa ***eduroam*** jest świadczona w szkielecie sieci PIONIER przez operatora sieci PIONIER, a w sieciach MAN kierowanych przez członków Konsorcjum PIONIER – przez jednostki wiodące poszczególnych sieci MAN.

1.3.3. Usługa polega na dostarczeniu mechanizmów pozwalających na uwierzytelnianie użytkowników w sieci komputerowej, z wykorzystaniem standardu 802.1x i serwera uwierzytelniającego instytucji.

1.3.4. Usługa ***eduroam*** umożliwia zainteresowanym Instytucjom uruchomienie uwierzytelnianego gościnnego dostępu na swoim terenie, ponadto pracownicy i studenci Instytucji korzystającej z usługi eduroam uzyskują możliwość korzystania z gościnnego dostępu we wszystkich sieciach eduroam na świecie.

1.3.5. Korzystanie z usługi ***eduroam*** jest możliwe pod warunkiem akceptacji zasad składających się na niniejszą Polską Politykę eduroam i spełnienia warunków określonych w tej Polityce.

1.3.6. Rolę Polskiej Federacji eduroam (w znaczeniu używanym w Europejskiej Polityce eduroam) pełni Konsorcjum PIONIER oraz instytucje, które złożyły deklarację chęci korzystania z usługi ***eduroam*** i zaakceptowały zasady Polskiej Polityki eduroam.

1.3.7. Operatorem ***eduroam*** w Polsce (National Roaming Operator w znaczeniu określonym przez *Europejską Politykę eduroam*) jest Instytut Chemii Bioorganicznej PAN – Poznańskie Centrum Superkomputerowo-Sieciowe (PCSS), działające w imieniu Konsorcjum PIONIER.

1.3.8. Usługa ***eduroam*** w Polsce jest realizowana w oparciu o:

1. *Polską Politykę eduroam*;
2. *Europejską Politykę eduroam* i *eduroam Service Definition and Implementation Plan*;
3. deklaracje chęci korzystania z usługi ***eduroam*** złożona przez jednostki zainteresowane;
4. porozumienie między PCSS i UMK w sprawie koordynowania przez UCI UMK usługi ***eduroam*** w Polsce;
5. deklarację przystąpienia do *Europejskiej Konfederacji eduroam* podpisaną przez Operatora usługi ***eduroam*** w Polsce.

1.4. Operator usługi *eduroam* w Polsce

1.5. Zadania Operatora polegają na:

1. reprezentowaniu konsorcjum PIONIER w *Europejskiej Konfederacji eduroam*;
2. nadzorowaniu przestrzegania *Europejskiej Polityki eduroam*;
3. nadzorowaniu wdrażania i przestrzegania niniejszej Polityki;
4. przyjmowaniu deklaracji chęci przyłączenia do usługi ***eduroam***.

1.6. Koordynator usługi *eduroam* w Polsce

1.6.1. Koordynatorem ***eduroam*** w Polsce, na mocy porozumienia z Operatorem, jest Uniwersytet Mikołaja Kopernika – Uczelniane Centrum Informatyczne (UCI UMK).

1.6.2. Zadania Koordynatora polegają na:

1. nadzorowaniu i koordynowaniu rozwoju ***eduroam*** w Polsce;
2. udziale w ciałach koordynujących międzynarodowy rozwój ***eduroam***;
3. prowadzeniu krajowego serwera pośredniczącego i nadzorowaniu działania krajowego serwera zapasowego w ramach sieci PIONIER;
4. monitorowaniu sprawności serwerów uwierzytelniających instytucji korzystających z usługi ***eduroam***;
5. koordynowaniu obsługi zdarzeń niepożądanych (nadużyć prawa, etykiety itp.) związanych z działaniem ***eduroam***;
6. utrzymywaniu serwisu www.eduroam.pl w ramach sieci PIONIER;
7. przygotowywaniu formalności związanych z przystępowaniem do usługi ***eduroam***.

1.7. Regionalni koordynatorzy usługi *eduroam* w Polsce

1.7.1. Instytucje będące członkami Konsorcjum PIONER mogą występować w roli regionalnych koordynatorów usługi ***eduroam***.

1.7.2. Zadania regionalnego koordynatora polegają na:

1. udzielaniu wsparcia instytucjom zlokalizowanym w obsługiwanym regionie, korzystającym lub pragnącym korzystać z usługi ***eduroam***;
2. prowadzeniu regionalnego serwera pośredniczącego w ramach sieci PIONIER;
3. współpracy z krajowym Koordynatorem usługi ***eduroam***.

1.8. Instytucje korzystające z usługi *eduroam*

1.8.1. Z usługi ***eduroam*** może korzystać instytucja dołączona do sieci PIONIER bezpośrednio lub za pośrednictwem sieci jednego z członków Konsorcjum PIONIER i posiadająca status:

1. szkoły wyższej;
2. instytutu badawczego.

1.8.2. Instytucja, która zamierza korzystać z usługi ***eduroam*** musi wyrazić zgodę na uruchomienie gościnnego dostępu do Internetu oraz zaakceptować postanowienia niniejszej Polityki.

1.8.3. Wyrażenie woli korzystania z usługi ***eduroam*** jest dokonywane poprzez podpisanie deklaracji przez osobę upoważnioną do reprezentowania instytucji.

1.8.4. Deklaracje chęci korzystania z usługi ***eduroam*** przyjmuje Operator za pośrednictwem Koordynatora.

1.8.5. Każda instytucja korzystająca z usługi ***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***.

1.8.6. Obowiązki instytucji korzystającej z usługi ***eduroam***

Jako *instytucja udzielająca gościnnego* dostępu do Internetu **instytucja** zobowiązuje się do:

1. zapewnienia dostępu do swojej sieci wszystkim osobom, które zostały poprawnie uwierzytelnione przez inne instytucje stowarzyszone w ***eduroam***, na warunkach określonych w „***Specyfikacji technicznej***".;
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 **Instytucja** 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 Koordynatorem usługi ***eduroam*** w Polsce 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 ***eduroam***.

1.8.7. Instytucje korzystające z usługi ***eduroam*** nie będą występować względem siebie z roszczeniami cywilno-prawnymi z tytułu ewentualnych incydentów sieciowych.

1.8.8. Rezygnacja z korzystania z usługi ***eduroam*** powinna być poprzedzona 3-miesięcznym okresem wypowiedzenia.

1.9. Zasoby *eduroam*

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

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

1.10. Użytkownicy

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

1.10.2. 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. Dane kontaktowe administratora są podawane w odpowiednim serwisie internetowym instytucji macierzystej.

1.10.3. Użytkownik powinien dołożyć starań, aby przed wysłaniem danych uwierzytelniających upewnić się, że korzysta z autentycznego zasobu ***eduroam*** (zgodnie z zaleceniami swojej instytucji macierzystej).

1.10.4. 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.

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

1.10.6. Użytkownik ***eduroam*** może korzystać z gościnnego dostępu wyłącznie na swój własny użytek.

2. Specyfikacja techniczna

2.1. Słowa kluczowe używane w tekście

2.1.1. Słowa „MUSI”, „MOŻE”, „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. Struktura uwierzytelniająca

2.2.1. Struktura serwerów Radius usługi ***eduroam*** w Polsce składa się z:

1. serwerów udostępniających zasoby;
2. serwerów uwierzytelniających (często pełniących również rolę serwera udostępniającego zasoby);
3. regionalnych serwerów pośredniczących;
4. krajowych serwerów pośredniczących.

2.2.2. Rolą serwerów pośredniczących jest przekazywanie zleceń uwierzytelnienia, dotyczących gościnnego dostępu do sieci ***eduroam***. Serwer pośredniczący POWINIEN być zdublowany.

2.2.3. Dodatkową rolą serwera pośredniczącego jest monitorowanie ruchu i zapewnienia dodatkowego poziomu bezpieczeństwa w strukturze zaufania.

2.2.4. Wszelkie dane archiwalne dotyczące procesu uwierzytelniania MUSZĄ być traktowane jako poufne i odpowiednio chronione.

2.2.5. Serwery pośredniczące MUSZĄ monitorować występowanie atrybutów Tunnel-Type, Tunnel-Medium-Type i Tunnel-Private-Group-ID, ponieważ pojawianie się ich zazwyczaj jest spowodowane błędem w konfiguracji serwerów lokalnych i może doprowadzać do zakłóceń działania usługi ***eduroam***. W przypadku wykrycia występowania takich atrybutów, administrator serwera pośredniczącego zgłasza ten fakt administratorowi serwera, który generuje pakiety zawierające te atrybuty.

2.3. Rola instytucji udostępniającej zasoby

2.3.1. 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 standardy 802.11a, 802.11n;
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.

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

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

2.3.4. Pakiety uwierzytelniające z nazwą użytkownika zawierającą ***realm*** nie należący do polskiej instytucji MUSZĄ być kierowane przez strukturę usługi ***eduroam*** do krajowych serwerów pośredniczących.

2.3.5. Pakiety uwierzytelniające z nazwą użytkownika zawierającą ***realm***, który nie odpowiada domenie zarejestrowanej przez daną instytucję udostępniającą zasoby, POWINNY być kierowane do serwera usługi ***eduroam*** w Polsce stojącego w hierarchii bezpośrednio powyżej serwera danej instytucji. Odstępstwa od tej reguły MUSZĄ być uzgadniane z administratorami regionalnych serwerów pośredniczących lub Koordynatorem usługi ***eduroam*** w Polsce.

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

2.3.7. W ramach gościnnego dostępu do Internetu, udostępnianego jako zasób eduroam, MUSI być zagwarantowany dostęp do usług:

1. Standard IPSec VPN: IP protokoły 50 (ESP) and 51 (AH) (oba wejście i wyjście); UDP/500 (IKE) (tylko wyjście);
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 (tylko wyjście);
6. PPTP VPN: IP protokół 47 (GRE) (wejście i wyjście); TCP/1723 (tylko wyjście);
7. SSH: TCP/22 (tylko wyjście);
8. HTTP: TCP/80 (tylko wyjście);
9. HTTPS: TCP/443 (tylko wyjście);
10. IMAP2+4: TCP/143 (tylko wyjście);
11. IMAP3: TCP/220 (tylko wyjście);
12. IMAPS: TCP/993 (tylko wyjście);
13. POP: TCP/110 (tylko wyjście);
14. POP3S: TCP/995 (tylko wyjście);
15. Passive (S)FTP: TCP/21 (tylko wyjście)+ inne wysokie porty wykorzystywane zgodnie z protokołem Passive (S)FTP (wyjście);
16. SMTPS: TCP/465 (tylko wyjście);
17. SMTP submit z STARTTLS: TCP/587 (tylko wyjście);
18. RDP: TCP/3389 (tylko wyjście)
19. SIP: TCP/UDP/5060-5061 (tylko wyjście).+inne wysokie porty wykorzystywane zgodnie z protokołem SIP
20. FRING: TCP/18182(wychodzący) TCP/UDP 52000-53800(wychodzące)

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

2.3.9. 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.

2.3.10. Instytucja udostępniająca zasoby we własnym interesie POWINNA przechowywać logi wiążące adresy IP z sesjami uwierzytelniania. Czas przechowywania logów NIE POWINIEN być krótszy niż 6 miesięcy. Jeżeli logi są utrzymywane, to MUSZĄ być znakowane czasem synchronizowanym za pomocą protokołu NTP i MUSZĄ zawierać:

1. czas uwierzytelnienia i przydzielenia adresu IP;
2. identyfikator (EAP outer identity) osoby uwierzytelnionej;
3. adres MAC klienta;
4. adres IP klienta.

2.3.11. 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 zawierający informację o dostępności zasobów ***eduroam*** na terenie Instytucji i akceptację niniejszej polityki (łącznie z odsyłaczem do dokumentu umieszczonego w ogólnopolskim serwisie ***eduroam***)

3. informacje o obszarze, na którym jest udostępniane są zasoby ***eduroam***;
4. informacje techniczne o udostępnianych zasobach ***eduroam***, a więc: rodzaju protokołu bezprzewodowego (802.11b, 802,11g, 802.11a, 802.11n), 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) o lokalnych zasad korzystania z sieci.

2.4. Rola instytucji uwierzytelniającej

2.4.1. 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.

2.4.2. 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.

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

2.4.4. Instytucja uwierzytelniająca MUSI prowadzić serwis internetowy zawierający kontakt do administratora serwera uwierzytelniającego.

2.4.5. 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. wartość atrybutu Calling-Station-Id zawartą w pakiecie uwierzytelniającym;
3. dane pozwalające na zidentyfikowanie użytkownika, którego uwierzytelniono.

2.4.6. Instytucja MUSI udostępnić Koordynatorowi usługi ***eduroam*** w Polsce konto testowe służące do monitorowania poprawności pracy serwera uwierzytelniającego tej instytucji.

2.4.7. Instytucja MUSI wyznaczyć administratorów odpowiedzialnych za kontakty z Koordynatorem usługi ***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***; instytucja jest również zobowiązana do przekazania kontaktów do Koordynatora usługi ***eduroam*** w Polsce;
2. poinformować Koordynatora usługi ***eduroam*** w Polsce o wystąpieniu incydentu i przekazać mu dane na temat czasu sesji uwierzytelniania i odnotowanego identyfikatora użytkownika.

3.2.2. Koordynator usługi ***eduroam*** w Polsce ustala (być może wspólnie z operatorem regionalnego serwera pośredniczącego lub 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 Koordynatora usługi ***eduroam*** w Polsce.

3.3.2. Koordynator usługi ***eduroam*** w Polsce 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 ***Poznańskie Centrum Superkomputerowo-Sieciowe***.

4.2. Wszelkie zmiany niniejszej polityki będą dokonywane w drodze konsultacji z instytucjami korzystającymi z usługi ***eduroam*** w Polsce

4.3. Instytucje partycypujące obecnie w pilotowym projekcie eduroam będą musiały złożyć deklarację o przyjęciu niniejszej polityki w terminie 6 miesięcy od jej ogłoszenia. W przypadku odmowy przyjęcia niniejszej ***polityki***, instytucja zostanie odłączona od struktury uwierzytelniającej ***eduroam***.