Projekt nr. POIG.02 03. 00-00-028/08-01
www.platon.pionier.net.pl
PLATFORMA OBSŁUGI NAUKI PLATON
KOORDYNATOR: INSTYTUT CHEMII BIOORGANICZNEJ PAN
POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE
ul. Noskowskiego 12/14, 61-704 Poznań, (+48 61) 858 20 00, fax: (+48 61) 852 59 54, e-mail: office@man.poznan.pl, www: http://www.man.poznan.pl

Realizacja wdrożenia usługi eduroam w sieci PIONIER

Tomasz Wolniewicz, UCI UMK (twoln@umk.pl)
dokument przygotowany w ramach projektu PLATON
wersja 1.0 – lipiec 2012

Spis treści

1. Wstęp

W dokumencie [1] opisany został plan wdrożenia usługi eduroam w sieci PIONIER. Teraz porównujemy ten plan ze stanem usługi w momencie zakończenia projektu PLATON.

Usługa eduroam w Polsce jest częścią usługi o zasięgu ogólnoświatowym, dlatego jej wdrożenie musi przebiegać w synchronizacji z działaniami na poziomie europejskim, te z kolei wymagają uzgodnień na poziomie globalnym.

eduoram na świecie okazał się ogromnym sukcesem. Usługa jest dostępna w praktycznie wszystkich rajach Europy, w USA, Kanadzie, Australii, Chinach, Japonii. Zakres dostępności jest różny, ale zainteresowanie cały czas rośnie.

W Polsce z eduroam można skorzystać w 54 instytucjach, w 43 miejscowościach (dane z momentu przygotowywania raportu, informacje akttualne są dostępna na stronie http://www.eduroam.pl).

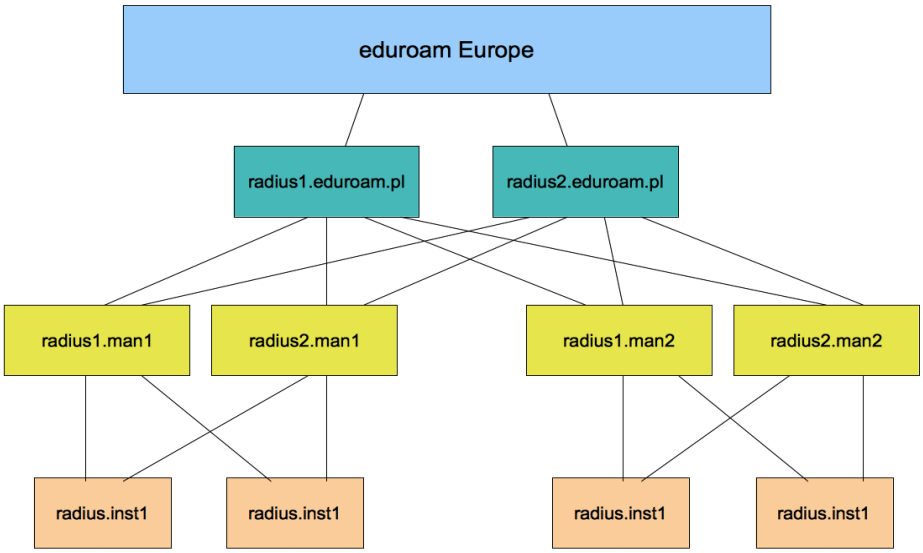
Uruchomiono zakładaną w projekcie strukturę serwerów regionalnych. Rozszerzeniem w stosunku do projektu było zbudowanie 21 sieci bezprzewodowych tworzących szkielet dostępu do eduroam oraz wzorzec implementacji sieci w instytucjach. Połączenia między serwerami regionalnymi a ser-

werami krajowymi zaimplementowano w oparciu o protokół RADIUS over TLS (znany wcześniej pod nazwą RadSec). Stan wdrożenia można uznać za bardziej niż zadowalający.

2. Analiza porównawcza stanu wdrożenia i projektu.

2.1. Hierarchiczna struktura serwerów pośredniczących

Wdrożona została trzypoziomowa struktura serwerów zbudowana dokładnie według założeń projektu i obejmująca: serwery krajowe, serwery regionalne i serwery instytucji. Serwery regionalne ułatwiają roaming między instytucjami jednej sieci MAN. Każdy z serwerów jest zdublowany.



2.1.1. Faza I – budowa statycznej hierarchii serwerów pośredniczących połaczonych protokołem RADIUS

W momencie przygotowywania projektu nie było jeszcze wiadomo, jaki będzie rozwój oprogramowania. Jako jedną z możliwości rozważano zastosowanie oprogramowania radsecproxy, pod warunkiem, że oprogramowanie to osiągnie odpowiedni poziom dojrzałości. Ponieważ ten warunek został spełniony i oprogramowanie zapewnia właściwy poziom stabilności, konfigurowalności oraz zbierania statystyk, to zostało ono użyte we wszystkich polskich serwerach pośredniczących.

Stworzenie struktury serwerów zakończyło planowaną fazę I wdrożenia.

2.1.2. Faza II – wdrożenie protokołu RadSec oraz dynamicznego doboru partnera

W modelu eduroam uwierzytelnienie użytkownika wymaga odszukania właściwego serwera macierzystego w oparciu o część domenową (realm) identyfikatora użytkownika. W pierwotnym modelu, odszukanie serwera macierzystego bazuje na prostej zasadzie przekazania nieznanego identyfikatora do wyższego poziomu struktury, aż do momentu, gdy któryś z serwerów stwierdzi, że zna właściwą ścieżkę. Prostota tego rozwiązania pozwoliła na szybkie wdrożenie eduroam na świecie, ale była od początku obarczona wadami. Dlatego od kilku lat planowane jest rozwiązanie alternatywne polegające na odnajdowaniu właściwego serwera macierzystego na podstawie wpisów do bazy DNS. Ten system został nazwany dynamicznym odnajdywaniem partnera i został opisany w [2]

Podstawową trudnością przy implementacji dynamicznego odnajdywania partnera jest zapewnienie właściwej struktury zaufania. W modelu hierarchicznym każdy serwer ufa swoim sąsiadom, a potwierdzenie tożsamości serwera polega na znajomości właściwego klucza identyfikacyjnego przez każdą ze stron. W modelu dynamicznym, bazowanie na kluczach wspólnych jest niemożliwe i zostało zastąpione negocjacją połączenia TLS, na które następnie nałożone zostaje połączenie protokołu RADIUS.

RADIUS nałożony na TLS i TCP jest często określany nazwą RadSec. W procesie standaryzacji zmieniono nazwę na RADIUS over TLS. To nowe rozwiązanie jest opisane w dwóch RFC: [3] i [4].

Zasady weryfikacji partnera w systemie dynamicznego doboru partnera nie są opisane w oficjalnych dokumentach IETF, eduroam musiał jednak zaproponować rozwiązanie, które można wdrożyć w systemie produkcyjnym. Zaproponowane rozwiązanie polega na użyciu podejścia opartego na standardach i uzupełnionego o zasady weryfikacji i politykę wystawiania certyfikatów. W czasie zestawiania połączenia TLS sprawdzany jest certyfikat drugiej strony. Certyfikat musi być zgodny z zapisami w DNS, musi być wystawiony przez jeden z zaufanych urzędów certyfikacji, a dodatkowo musi zawierać identyfikator usługi eduroam. Spełnienie tych warunków gwarantuje, że odnaleziony serwer faktycznie ma prawo obsługiwać dany realm, a ponadto, że reprezentuje instytucję, która jest związana regułami eduroam.

Faza II polskiego projektu zakładała stopniowe przechodzenie do systemu dynamicznego zestawiania połączeń z częściowym pominięciem struktury statycznej.

Pierwszym krokiem fazy II było przeniesienie statycznych połączeń pomiędzy serwerami pośredniczącymi z protokołu RADUIS na protokół RadSec. W momencie tworzenia projektu, RadSec nie był jeszcze standardem. Od tego czasu przygotowane zostały RFC, a nowy protokół uzyskał nazwę RADIUS over TLS. Implementacja protokołu w oprogramowaniu radsecproxy i Radiator jest stabilna i może być używana produkcyjnie. Od dwóch lat eszystkie połączenia między serwerami regionalnymi a serwerami krajowymi pracują w tym protokole, podobnie jak połączenia między serwerami krajowymi a europejskimi. Serwery korzystają z darmowego oprogramowania radsecproxy. Tym samym zaimplementowano w całości pierwszą część fazy II.

Jako kolejne kroki fazy II przewidziano wdrożenie systemu dynamicznego wyboru partnera w usłudze eduroam. Nakreślone terminy i zakres tego wdrożenia okazały się nierealne. W momencie przygotowywania projektu, zasada dynamicznego doboru partnera była na etapie szkicu, ale oczekiwano stosunkowo szybkiego przygotowania zarówno specyfikacji, jak i implementacji. Niestety ten proces okazał się dużo bardziej czasochłonny niż początkowo przewidywano i stabilne implementacje ukazały się dopiero w pierwszej połowie roku 2012. W momencie pisania obecnego raportu, usługa dynamicznego wyboru została pilotowo wdrożona na części serwerów regionalnych. W tej fazie wpisy DNS dotyczące wybranych instytucji wskazują na właściwy serwer regionalny. Serwer regionalny jest wybierany jako właściwy dla uwierzytelnienia użytkownika i przekazuje zlecenie certyfikacji do serwera macierzystego. W tym modelu, instytucje wdrażają typowe serwery RADIUS i zestawiają statyczne połączenia RADIUS z serwerami regionalnymi, mogą zatem działać na dowolnych serwerach RADIUS (typowo FreeRADIUS). Serwery regionalne biorą na siebie całą złożoność odszukiwania i odpowiadania na połączenia w modelu dynamicznym. Takie rozwiązanie znacząco zmniejsza liczbę serwerów pośredniczących przy każdym ze zleceń, a jednocześnie uwalnia administratorów instytucji od konieczności obsługi protokołu RADIUS over TLS.

Połączenia dynamiczne utrudniają proces zbierania statystyk oraz lokalizowania problemów. Również z tych powodów, pozostawienie ostatniego szczebla struktury hierarchicznej jest korzystne.

W perspektywie najbliższych lat przewidujemy szerokie wdrożenie modelu dynamicznego poprzez serwer regionalny, natomiast model dynamiczny bezpośrednio w instytucji końcowej będzie prawdopodobnie stosowany tylko wyjątkowo.

3. Budowa wzorcowych sieci bezprzewodowych

Projekt PLATON zakładał zbudowanie infrastruktury serwerów eduroam oraz przygotowanie bezprzewodowych sieci dostępowych u partnerów. Budowa tych sieci miała doprowadzić do znaczącego wzrostu dostępności eduroam w Polsce, a jednocześnie przygotowania zaplecza eksperckiego we

wszystkich MAN-ach konsorcjum PIONIER. Zakupiono zaawansowane systemy bezprzewodowe trzech producentów: Meru Networks, Cisco i Trapeze/Juniper. Na każdy z systemów składają się dwa kontrolery i 50 zarządzanych przez nie punktów dostępowych. Systemy będzie można w przyszłości rozbudowywać ze środków własnych partnerów.

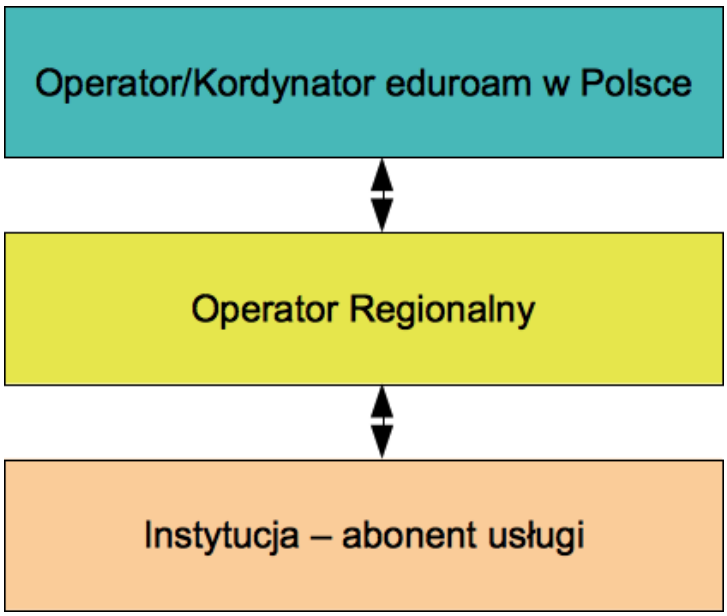
4. Zarządzanie eduroam w Polsce

4.1. Struktura zarządzania usługą eduroam

Usługa eduroam w Polsce jest świadczona w strukturze konsorcjalnej, tzn. członkowie Konsorcjum PIONIER są usługodawcami na terenie własnych sieci miejskich. Nieliczne przypadki abonentów podłączonych do sieci PIONIER bez pośrednictwa sieci miejskich są obsługiwane bezpośrednio przez Operatora sieci PIONIER.

Zarządzanie usługą jest koordynowane przez Uczelniane Centrum Informatyczne Uniwersytetu Mikołaja Kopernika. Krajowe serwery eduroam są umieszczone na UMK i w Poznańskim Centrum Superkomputerowo-Sieciowym. Serwery regionalne są umieszczone u członków Konsorcjum.

Instytucje, które chcą rozpocząć korzystanie z eduroam składają u Operatora Regionalnego deklarację, Operator Regionalny przyjmuje zgłoszenie i uruchamia usługę poprzez dopisanie danych instytucji do bazy eduroam, wprowadzenie odpowiednich wpisów w konfiguracji serwerów regionalnych oraz zgłoszenie potrzeby aktualizacji konfiguracji serwerów krajowych.



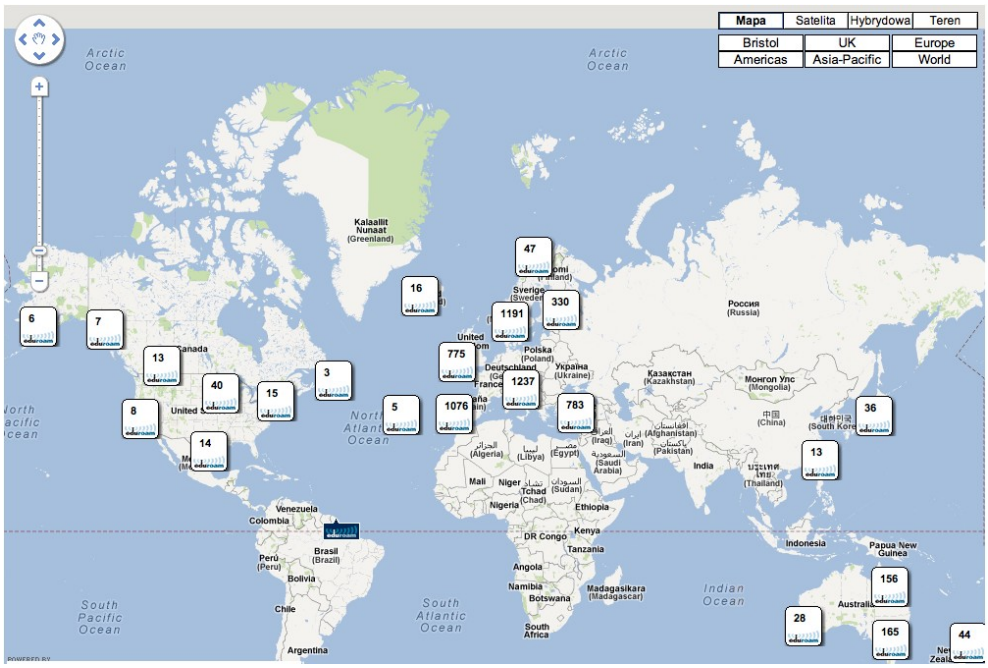
4.2. Baza eduroam

Baza eduroam jest narzędziem wspomagającym zarządzenie usługą, a jednocześnie jest elementem wsparcia użytkowników udostępniając listę lokalizacji, w których dostępny jest Internet za pośrednictwem eduroam. Baza jest dostępna poprzez polski portal eduroam http://www.eduroam.pl.

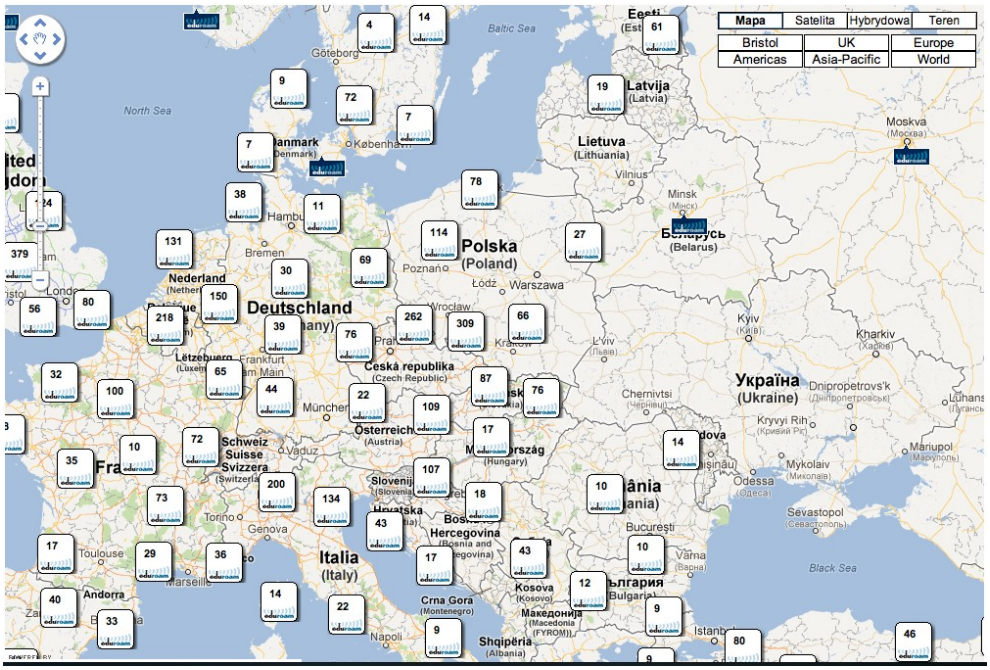
Koordynator zarządza listą administratorów regionalnych. Administratorzy regionalni wprowadzają dane instytucji, na rzecz których świadczona jest usługa i tworzą konta administratorów lokalnych. Administratorzy lokalni wprowadzają informacje o lokalizacjach, w których można korzystać z eduroam.

Mapa lokalizacji na polskim portalu eduroam

Zawartość polskiej bazy eduroam jest na bieżąco synchronizowana z bazą europejską, dzięki czemu polskie lokalizacje są widoczne w portalu globalnym.



Globalna mapa eduroam



Globalna mapa eduroam - obszar Europy

4.3. Monitorowanie infrastruktury

Infrastruktura serwerów pośredniczących eduroam jest regularnie monitorowana. Serwery krajowe są monitorowane z poziomu europejskiego, natomiast serwery regionalne są testowane narzędziami własnymi.

5. Możliwe zagrożenia dla wdrożenia projektu

W projekcie zidentyfikowano kilka obszarów potencjalnych zagrożeń i podano propozycje jak im zapobiegać. Poniżej analizujemy te zagrożenia z perspektywy kilku lat.

5.1. Poprawność obsługi incydentów sieciowych

Usługa eduroam ma dobrze zdefiniowane procedury obsługi incydentów, ale w ciągu kliku lat działania usługi w Polsce tylko jeden raz mieliśmy do czynienia ze zgłoszeniem nadużycia dostępu gościnnego. Incydent został zgłoszony administratorom serwera macierzystego użytkownika, którzy skontaktowali się z użytkownikiem i wyjaśnili sprawę. Na Uniwersytecie Mikołaja Kopernika, kilkakrotnie zdarzyły się przypadki otrzymania zgłoszenia o prawdopodobnym naruszeniu praw autorskich. Za każdym razem system identyfikacji użytkownika zdał egzamin i pozwolił na uruchomienie lokalnych procedur obsługi takich przypadków.

5.2. Nakładanie się zasięgów sieci bezprzewodowych

Sytuacja, w której sieci eduroam propagowane przez różne instytucje częściowo nakładają się zasięgiem, powoduje kłopotliwe dla użytkownika przełączanie pomiędzy różnymi sieciami, konieczność zmiany adresu IP itp. W projekcie wdrożenia przewidziane zostały dwa rozwiązania takich sytuacji, ale jak do tej pory w polskim eduroam taki przypadek nie wstąpił i nie było konieczności reagowania na niego. Nie jest to jednak sytuacja czysto teoretyczna, np. w okolicach Russel Square w Londynie występuje problem nakładania się kilku sieci eduroam. Rozwój standaryzacji (892.11u, włączony obecnie w standard IEEE 802.11-2012) prawdopodobnie pozwoli rozwiązać ten problem, zanim w Polsce się z nim zetkniemy w większym wymiarze. Nowy standard definiuje dodatkowe identyfikatory rozgłaszane przez sieć, dzięki czemu urządzenia nie będą miały możliwość rozróżniania urządzeń pracujących w eduroam, ale należących do różnych sieci. Ponieważ tworzenie sieci eduroam o zmodyfikowanych SSID, uniemożliwi skorzystanie z nich większości użytkownikom, to po konsultacjach z administratorami eduroam podjęta została decyzja o zabronieniu stosowania takich SSID, tzn. określone zostało, że wszystkie sieci eduroam muszą korzystać z SSID eduroam, a ew. problemy z nakładaniem się zasięgów powinno się rozwiązywać poprzez współpracę między instytucjami.

5.3. Różne typy szyfrowania

W momencie przygotowywania projektu wdrożenia szyfrowanie WPA/TKIP było najpopularniejszym rozwiązaniem, mającym dobre wsparcie w sprzęcie i zapewniającym wysokie bezpieczeństwo transmisji. Nowocześniejsze rozwiązanie WPA2/AES wymagało nowocześniejszych kart sieciowych oraz wsparcia w systemach operacyjnych. Obecnie WPA/TKIP jest już uważane za przestarzałe i narażone na ataki, w nowym sprzęcie bezprzewodowym może nawet nie mieć wsparcia. Z kolei WAP2/AES stał się obowiązkowy, a w stosunku do WAP/TKIP ma wiele przewag. Nowy europejski, a w ślad za nim również polski regulamin eduroam nakłada obowiązek stosowania WPAS2/AES;WPA/TKIP jest jedynie opcjonalny. Ta zmiana była już od dłuższego czasu oczekiwane przez środowisko, ponieważ utrzymywanie WPA/TKIP jest postrzegane jako osłabienie parametrów sieci.

Z uwagi na zwiększenie kompatybilności ze starszymi urządzeniami i systemami operacyjnymi, na razie rekomendujemy utrzymanie WPA/TKIP, ale nie będziemy już tego narzucać poprzez wymóg regulaminowy.

5.4. Anonimowość użytkowników i nadużywanie połączenia gościnnego

Zasady uwierzytelniania w eduroam zapewniają możliwość zidentyfikowania każdego użytkownika, wymaga to jednak współpracy między instytucją udostępniającą sieć a instytucją uwierzytelniającą. W pewnych sytuacjach nawiązanie tej współpracy może trwać zbyt długo, albo żądanie instytucji udostępniającej sieć, by użytkownikowi odebrać uprawnienie do korzystania z sieci, może zostać zakwestionowane przez instytucję macierzystą. Z tych powodów wskazane jest umożliwienie

częściowej identyfikacji wyłącznie przez instytucję udostępniającą sieć. Identyfikacja polega na przydzieleniu unikatowego identyfikatora każdemu użytkownikowi i przekazanie go jako wartość atrybutu Chargeable-User-Identity. Identyfikator pozwala wyłącznie na stwierdzenie, że ta sama osoba łącząca się wielokrotnie do sieci, również z różnych urządzeń, jest rozpoznawana jako jedna a nie wiele różnych. Dzięki temu istnieje możliwość założenie filtrów na konkretnego użytkownika. Wprowadzenie takiego systemu identyfikacji użytkowników było polskim wkładem w eduroam, zarówno sam pomysł, jak i implementacje rozwiązań powstały w polskim projekcie eduroam. Zaimplementowane rozwiązanie jest od dłuższego czasu używane produkcyjnie na Uniwersytecie Mikołaja Kopernika i będzie wprowadzane szerzej. Udało się również doprowadzić do pierwszego wdrożenia obsługi Chargeable-User-Identity bezpośredni w kontrolerze bezprzewodowym. Zrobiła to firma Meru Networks, która jest dostawcą systemów bezprzewodowych dla części partnerów projektu PLATON.

6. Podsumowanie

Usługa eduroam uzyskała znaczną popularność w polskim środowisku akademickim. Została wdrożona produkcyjnie i ułatwia dostęp do sieci zarówno w kraju jak i za granicą. eduroam jest rozpoznawalnym znakiem, a według niezależnych badań nazwa sieciowa eduroam jest w czołówce najpopularniejszych nazw na świecie. Światowy sukces eduroam potwierdza słuszność polskiej decyzji, aby do tego projektu dołączyć we wczesnej fazie.

Polska jest jednym z najbardziej aktywnych europejskich partnerów eduroam. Rozwiązania przygotowane w polskim projekcie są często wzorem do wdrożenia w skali globalnej.

Zakres wdrożenia w Polsce jest dobry, ale usługa powinna być dostępna szerzej. Być może kolejne ułatwienia, takie jak automatyczne instalatory, przyczynią się do dalszego wzrostu liczby przyłączonych instytucji.

Bardzo ważna jest rola Operatorów Regionalnych, którzy mają bezpośrednie kontakty z instytucjami w swoim regionie.

Wdrożenie eduroam ma szansę stać się podstawą dla nowej usługi sieci PIONIER – federacji SAML zapewniającej jednorodny sposób uwierzytelniania w wielu usługach sieciowych.

Zbudowane w projekcie sieci bezprzewodowe mają wielu użytkowników i są bardzo ważnym uzupełnieniem zasobów dostępowych w polskich, akademickich sieciach MAN.

7. Bibliografia

1. Wolniewicz, T, Górecka-Wolniewicz M., Ołtuszyk Z. „Koncepcja wdrożenia usługi eduroam w sieci PIONIER” http://www.eduroam.pl/Dokumentacja/koncepcja_polska-1.0.pdf
2. Winter, S. and M. McCauley, „NAI-based Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS”, Work in Progress, June 2012.
3. DeKok, A., „RADIUS over TCP”, RFC 6613, May 2012.
4. Winter, S., McCauley, M., Venaas, S., and K. Wierenga, „Transport Layer Security (TLS) Encryption for RADIUS”, RFC 6614, May 2012.