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

Jak rozpocząć korzystanie z eduroam

poradnik dla instytucji planujących uruchomienie usługi eduroam

Maja Górecka-Wolniewicz, UCI UMK (mgw@umk.pl)
Tomasz Wolniewicz, UCI UMK (twoln@umk.pl)
dokument przygotowany w ramach projektu B-R eduroam-PIONIER
zaktualizowany w ramach projektu PLATON
wersja 2.0 – sierpień 2012

Spis treści

1. Wstęp

eduroam jest przedsięwzięciem o skali ogólnoświatowej, które w każdym z krajów jest realizowanie przez odpowiednią krajową sieć. W Polsce eduroam jest wdrażany i zarządzany przez konsorcjum PIONIER, a podstawowe zręby usługi powstały w ramach projektu PLATON jako Usługa U2 (eduroam). Poniżej zamiennie używany terminu usługa U2 oraz dostęp do eduroam.

W niniejszym dokumencie opisujemy kroki przygotowawcze do tego, by instytucja mogła korzystać z dostępu do eduroam. Zamieszczone wskazówki mają jedynie stanowić pomoc w podjęciu decyzji i rozpoczęciu kroków formalnych. Niezbędne jest zapoznanie się z całym polskim Regulaminem *eduroam* (http://www.eduroam.pl/regulamin).

2. Zakres usługi dostępu do edroam

Usługa eduroam polega na dostarczeniu narzędzi, które umożliwiają proste uruchomienie bezpiecznego dostępu gościnnego. Dostęp do eduroam mogą uzyskać wszystkie instytucje będąca użytkownikami sieci PIONIER, czyli jednostki oświatowe, jednostki administracji rządowej i samorządowej, instytucje kulturalne, biblioteki, jednostki służby zdrowia, instytucje wyższej użyteczności i pożytku publicznego, które posiadają umowę na dostęp do sieci szerokopasmowej PIONIER.

Instytucje korzystające z eduroam mają dodatkowo prawo do automatycznego uzyskania przywileju uwierzytelniania własnych użytkowników, co w praktyce oznacza, że pracownicy oraz studenci instytucji uprawnionych będą mogli podłączyć się do sieci w każdym miejscu na świecie, gdzie eduroam jest dostępna.

Może się zdarzyć, że jakaś instytucja chce na swoim terenie uruchomić dostęp gościnny, ale z różnych powodów nie jest zainteresowana, aby uruchamiać własny serwer zarządzania swoimi użytkownikami. W niniejszym dokumencie opisujemy w skrócie niezbędne warunki uruchomienia usłu-

gi eduroam w obu zakresach,. Dla uproszczenia każdy zakres jest opisany w oddzielnej części, w szczególności część opisująca

3. Dokumenty regulujące działanie usługi eduroam

Dostęp do eduroam jest świadczony w sieci PIONIER i sieciach miejskich zarządzanych przez członków konsorcjum PIONIER, jako część usługi przyłączenia do sieci PIONIER.

Wszystkie dokumenty są dostępne na stronie .http://www.eduroam.pl/regulamin

Dokumenty podstawowe:

- *Polski Regulamin eduroam* – opisuje wszystkie aspekty działania usługi w Polsce;
- *Zasady działania europejskiej usługi eduroam (eduroam Service Definition)* – dokument o zasięgu ponad-krajowym, niezbędny ponieważ eduroam jest usługą o zasięgu ogólnoświatowym.

Dokumenty towarzyszące:

- *Deklaracja chęci korzystania z eduroam*, wraz z załącznikiem dotyczącym zgłoszenia administratorów usługi;
- *Potwierdzenie uruchomienia usługi eduroam* wystawiane przez regionalnego Operatora eduroam.

Niezbędnym warunkiem do korzystania z eduroam jest wyrażenie zgody na udostępnianie gościnnego dostępu zgodnie z warunkami technicznymi eduroam oraz zaakceptowanie Regulaminu eduroam i złożenie deklaracji chęci korzystania z usługi właściwemu Operatorowi eduroam.

Uruchomienie dostępu do eduroam następuje w wyniku wystąpienia do właściwej jednostki wiodącej (operatora) miejskiej sieci komputerowej po spełnieniu niezbędnych warunków technicznych (dane kontaktowe oraz formularz wniosku są dostępne poprzez portal http://www.eduroam.pl/).

Usługa PLATON U2 eduroam jest świadczona bez dodatkowych opłat. Operatorzy sieci miejskich mogą oferować dodatkowe usługi odpłatne, np. hostingu serwera RADIUS.

4. Uruchomienie usługi eduroam w zakresie gościnnego dostępu

Informacje zawarte w tej części dotyczą wyłącznie instytucji, które chcą udostępnić łączność eduroam za pośrednictwem swojej sieci, ale nie będą korzystały z możliwości uwierzytelniania użytkowników własnych. Wdrożenie eduroam w szerszym zakresie jest opisane w części 5 i niniejszą część można pominąć.

Szczegółowy wykaz warunków technicznych jest zawarty w *Regulaminie dostepu do eduroam*, tutaj przedstawiamy kilka najważniejszych. Niektóre z poniższych warunków mogą być spełnione poprzez outsourcing.

- Nasza instytucja musi być użytkownikiem sieci PIONIER, zgodnie z definicja podaną w części 2.
- Musimy udostępnić SSID eduroam.
- SSID eduroam musi być zabezpieczone szyfrowaniem typu WPA2-Enterprise i musi wspierać szyfrowanie WPA2/AES, sieć może dodatkowo wspierać szyfrowanie WPA/TKIP.
- Dostęp do Internetu udostępniany poprzez SSID eduroam nie powinien być poddawany blokowaniu ani filtrowaniu (z wyjątkiem filtrowania poczty elektronicznej w obronie przez rozsyłaniem spamu), jeżeli jednak uważamy, że pewien poziom filtrowania jest niezbędny, to musimy zapewnić przynajmniej taki dostęp do sieci, jaki został określony przez Regulamin eduroam.
- Serwer RADIUS uwierzytelniający użytkowników w sieci eduroam musi zostać połączony z właściwym serwerem regionalnym usługi eduroam.
- Logi serwera RADIUS muszą być przechowywane przez okres min 6 miesięcy w celu rozwiązywania problemów zgłaszanych przez użytkowników usługi. Logi serwera RADIUS są

również ważnym dowodem w przypadkach wystąpienia incydentów sieciowych. W celu zapewnienia spójności czasowej logów, wszystkie serwery muszą synchronizować czas (np. przy pomocy protokołu NTP)

- Musimy prowadzić stronę informacyjną pod adresem http://eduroam.domena_instytucji, na której musi się znaleźć podstawowa informacja dla gości (po polsku i po angielsku);
- Musimy przekazać dane kontaktowe administratorów lokalnych usługi eduroam do bazy europejskiej (chyba, że przekazała zarządzanie Regionalnemu Operatorowi eduroam, który wyznaczy własnych administratorów).
- Informacje o lokalizacjach, w których udostępniamy eduroam muszą zostać wprowadzone do bazy eduroam na portalu www.eduroam.pl.

5. Uruchomienie uwierzytelniania własnych użytkowników.

5.1. Główne warunki formalne

Uwierzytelnianie własnych użytkowników, czyli danie im możliwości dostępu do zasobów eduroam na całym świecie, musi być realizowane na zasadach wzajemności, tzn my oferujemy dostęp do naszej sieci i w zamian za to otrzymujemy dostęp do innych. Z tego powodu, uruchomienie dostępu gościnnego jest niezbędnym warunkiem do utrzymania uprawnienia do uwierzytelniania własnych użytkowników w eduroam. Dostęp gościnny powinien być uruchomiony w maksymalnie szerokim zakresie.

5.2. Warunki techniczne w skrócie

Szczegółowy wykaz warunków technicznych jest zawarty w *Regulaminie dostępu do eduroam*, tutaj przedstawiamy kilka najważniejszych. Niektóre z poniższych warunków mogą być spełnione poprzez outsourcing, ale formalna odpowiedzialność zawsze leży na jednostce korzystającej z usługi eduroam.

- Musimy uruchomić gościnny dostęp bezprzewodowy dla sieci o nazwie eduroam zgodnie z opisem w części 4.
- Musimy uruchomić serwer RADIUS uwierzytelniający naszych użytkowników.
- Musimy uruchomić stronę internetową z informacjami dla naszych użytkowników, na tej stronie muszą się też znaleźć informacje o Regulaminie Usługi eduroam.
- Logi serwera uwierzytelniającego muszą być przechowywane przez minimum 6 miesięcy. Logi te są zabezpieczeniem dla innych instytucji na wypadek wystąpienia incydentów spowodowanych przez naszych użytkowników an terenie tych instytucji. Pamiętajmy, aby dane identyfikacyjne użytkowników udostępniać wyłącznie upoważnionym instytucjom. Możemy jednak skorzystać z posiadanych informacji w celu zwrócenia uwagi użytkownikowi, że ktoś zgłasza zastrzeżenia do jego zachowania.
- Musimy udostępniać Koordynatorowi eduroam i Regionalnemu Operatorowi eduroam konto testowe do celów monitorowania poprawności działania swojego serwera RADIUS.

6. Zalecenia

Poniższe punkty są wymienione w polskim *Ragulaminie dostępu do eduroam* jako zalecane, ale ponieważ służą tylko ochronie interesów własnych instytucji, to stosowanie się do nich jest opcjonalne.

- Używanie adresów publicznych – jest to praktyka zalecana przez politykę eduroam, ponieważ umożliwia odnajdowanie osób odpowiedzialnych za ew. incydenty sieciowe, jednak w sytuacjach, gdy takie rozwiązanie jest niemożliwe z powodów technicznych, instytucja może

stosować adresy prywatne, przyjmując do wiadomości, że rozwiązywanie problemów będzie utrudnione.

- Przechowywanie informacji o przydzielonych adresach IP – podobnie jak powyżej, przechowywanie poprawnych logów systemowych jest głównym narzędziem przy rozwiązywaniu incydentów sieciowych, a zatem jest w interesie instytucji, by posiadać odpowiednie informacje i stosować system uniemożliwiający zmianę przydzielonego adresu IP.

7. Uwagi

eduroam dla własnych użytkowników – nie są stawiane żadne warunki odnośnie minimalnej grupy własnych użytkowników, którzy mają mieć dostęp do usługi eduroam – w interesie instytucji jest, by była to grupa jak najszersza, ale jest to autonomiczna decyzja instytucji, np. jeżeli uczelnia nie dysponuje centralną bazą kont studenckich, to nie musi czekać na jej stworzenie, by zacząć korzystać z eduroam.

8. Zlecana kolejność postępowania

1. sprawdź, czy Twoja instytucja spełnia podstawowe warunki formalne opisane w części 4 lub 5;
2. przejrzyj materiały na stronach http://www.eduroam.pl, w szczególności http://www.eduroam.pl/regulamin;
3. skontaktuj się z właściwym Regionalnym Operatorem eduroam (adresy na http://www.eduroam.pl/index.php?lang=pl&page=kontakt-reg);
4. zgłoś Operatorowi Regionalnemu, że Twoja instytucja jest zainteresowana korzystaniem z eduroam samo zgłoszenie nie stanowi zobowiązania wobec usługodawcy, a umożliwi Operatorowi Regionalnemu założenie Ci konta na portalu administratorów eduroam, dając Ci dostęp do materiałów wewnętrznych);
5. przygotuj instalację sieci bezprzewodowej zgodną ze standardem WPA2-Enterprise (nie używaj nazwy eduroam do czasu faktycznego włączenia usługi), na tym etapie przydatne mogą być materiały publikowane na stronie

   http://www.eduroam.pl/index.php?page=doc&lang=pl.