DOSTĘP DO SIECI EDUROAM dla systemu



ETAP I Instalacja certyfikatów w systemie

Na początku należy pobrać i zapisać na dysku poniższy certyfikat:

http://net.ifj.edu.pl/certyfikaty/ca.der

Rozpoczęto pobieranie pliku:			
📮 ca.der			
Typ pliku: der File			
Adres: http://net.ifj.edu	.pl		
Po zakończeniu pobierania:			
🔘 Otwórz za p <u>o</u> mocą	Przeglądaj	L.	
Zapisz plik			
🗌 Z <u>a</u> pamiętaj tę decyzji	e dla wszystkich pliki	ów tego typu	

Czy cł	ncesz otworzyć ten plik?
	Nazwa: D:\download\ca.der
- 8	Wydawca: Nieznany wydawca
	Typ: Certyfikat zabezpieczenia
	Od: D:\download\ca.der
🗸 Zaw	Otwórz Anuluj
۲	Pliki pochodzące z Internetu mogą być użyteczne, ale ten typ pliku może być szkodliwy dla komputera. Jeśli nie masz zaufania do źródła nie totwierał teno oprogramowania. Jekie lest zagroziej?

Po zapisaniu certyfikatów na dysku kliknij prawym klawiszem myszy na jednym z pobranych plików certyfikatów, a następnie wybieramy polecenie **Zainstaluj certyfikat**



Po wyborze polecenia Zainstaluj certyfikat został uruchomiony Kreator importu certyfikatów.

Certyfikaty należy zainstalować w magazynie: **Zaufane główne urzędy certyfikacji**. W celu prawidłowego wyboru magazynu postępuj zgodnie z poleceniami

wyświetlanymi na ekranie:



Kreator importu certyfikatów	
Magazyn certyfikatów Magazyny certyfikatów to obszary systemowe, w których przechowywane są certyfikaty.	
System Windows może automatycznie wybrać magazyn certyfikatów; możesz jednak określić inną lokalizację dla certyfikatu.	
Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu	
Omieść wszystkie certyfikaty w następującym magazynie	
Magazyn certyfikatów:	
Dowiedz się więcej o <u>magazynach certyfikatów</u>	
< Wstecz Dalej > Anuluj	
Wybieranie magazynu certyfikatów	
Wybierz magazyn certyfikatów, którego chcesz użyć.	
Osobistv Zaufanie główne urzędy certyfikacji Zaufanie przedsiębiorstwa Image: Certyfikacji Pośrednie urzędy certyfikacji Image: Certyfikaty niezaufane Certyfikaty niezaufane Image: Certyfikacji innych firm Pokaż magazyny fizyczne OK	
Kreator importu certyfikatów	×
Magazyn certyfikatów Magazyny certyfikatów to obszary systemowe, w których przechowywane są certyfikaty. System Windows może automatycznie wybrać magazyn certyfikatów; możesz jednak określić inną lokalizację dla certyfikatu. Ø Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu Ø Umieść wszystkie certyfikaty w następującym magazynie Magazyn certyfikatów: Zaufane główne urzędy certyfikacji	
Dowiedz się więcej o <u>magazynach certyfikatów</u>	

eator importu certyfikatów	
	Kończenie pracy Kreatora importu certyfikat ostanie zaimportowany po kliknięciu przydsku Zakończ. Wybrane zostały następujące ustawienia: Magazyn certyfikatów wybrany przez uzytkownika Zaufr Zawartość Certy
	К Р.
trzeżenie o zabezpieczenia	< Wstecz Zakończ Anuluj
Za chwilę zostani rzekomo reprezer IFJ PAN - CA Roo	ie zainstalowany certyfikat z urzędu certyfikacji, który ntuje: pt
System Windows pochodzi od "IFJ przez skontaktow pomocna następ	: nie może potwierdzić, czy certyfikat rzeczywiście PAN - CA Root". Jego pochodzenie można potwierdzić vanie się z "IFJ PAN - CA Root". W procesie będzie ująca liczba:
Odcisk palca (sha Ostrzeżenie: Jeśli ten certyfika będzie automaty ten urząd certyfik odciskiem palca t oznacza, że decyc	a1): D2393F47 752C8376 47DB111B 0A0333CF 177C908F t główny zostanie zainstalowany, system Windows cznie ufać każdemu certyfikatowi wystawionemu przez kacji. Instalacja certyfikatu z niepotwierdzonym to potencjalne zagrożenie.Kliknięcie przycisku "Tak" dujesz się podjąć to ryzyko.
Czy chcesz zainst	talować ten certyfikat? Tak . Nie
eator importu certyfika	atów
	ОК

ETAP II Konfiguracja dostępu do sieci EDUROAM.

Chcąc rozpocząć korzystanie z sieci **WI-FI** sprawdzamy czy znajdujemy się w jej zasięgu:

Obecnie połączono z:	+9
Sieć niezidentyfikowana Brak dostępu do sieci	
Połączenie sieci bezprzewodowej	•
eduroam	lite.
IFJ	1800
IFJ-TYMCZASOWA	2.11
Otwórz Centrum sieci i udostępn	iania

Będąc w zasięgu sieci WI-FI eduroam otwieramy centrum sieci i udostępniania systemu Windows i klikamy link Zarządzaj sieciami bezprzewodowymi:



🚱 💭 🗢 📶 « Sieć i Internet 🔸 Zarządzaj sieciami bezprzewodowymi W oknie zarządzania sieciami + 49 bezprzewodowymi jeżeli istnieje Zarządzaj sieciami bezprzewodowymi, które używają (Połączenie sieci bezprzewodowej) połączenie eduroam to go System Windows próbuje łączyć się z tymi sieciami w przedstawionej poniżej kolejności. usuwamy, a następnie klikamy Dodaj, Właściwości karty Typy profilów Centrum sieci i udostępniania przycisk Dodaj: šaj sieć bezprzewodowa odyfikować oraz których kolejność mozesz zmieniać (1) Typ: Dowolna obsługiwana Polacz auto 1 element W oknie W jaki sposób chcesz 📲 Ręczne nawiązywanie połączenia z siecią bezprzewodową dodać sieć? wybieramy W jaki sposób chcesz dodać sieć? Ręcznie utwórz profil sieciowy: Nęcznie utwórz profil sieciowy Tworzy nowy profil sieciowy lub lokalizuje istniejącą sieć i zapisuje profil dla sieci na komputerze. Musisz znać nazwę sieci (SSID) i klucz zabezpieczeń (jeśli jest stosowany). Utwórz sieć ad hoc Tworzy sieć tymczasową dla udostępniania plików lub połączenia internetowego. Anuluj W następnym kroku kreatora w pole Nazwa sieci wpisujemy: 😋 📲 Ręczne nawiązywanie połączenia z siecią bezprzewodową eduroam, typ zabezpieczeń wybieramy: WPA2-Enterprise, Wprowadź informacje o sieci bezprzewodowej, którą chcesz dodać. typ szyfrowania wybieramy: AES. Nazwa sieci: eduroam Typ zabezpieczeń: WPA2-Enterprise Chcąc automatycznie łączyć się z siecią eduroam będąc w jej Typ szyfrowania: AES zasięgu zaznaczamy opcję: Klucz zabezpieczeń: 📃 Ukryj znaki Uruchom to połaczenie automatycznie. Uruchom to połączenie automatycznie 🔲 Połącz, nawet jeśli sieć nie wykonuje emisji Ostrzeżenie: jeśli wybierzesz tę opcję, może to zagrozić prywatności komputera. Następnie klikamy przycisk Dalej: Dalej N Anuluj

W ostatnim kroku kreatora wybieramy **Zmień ustawienia połączenia**: 🌙 💷 Ręczne nawiązywanie połączenia z siecią bezprzewodową

Pomyślnie dodano: eduroam

Zmień ustawienia połączenia	N
Otwórz właściwości połączenia, aby można było zmienić ustawienia.	43

Zamknij

Pojawi się okno **Właściwości sieci bezprzewodowej**, w którym w zakładce **Zabezpieczenia** wybieramy metodę uwierzytelniania sieci: **Microsoft: Chroniony protokół EAP** (**PEAP**) i klikamy przycisk **Ustawienia**:

Połączenie Zabezpie	czenia
Nazwa:	eduroam
SSID:	eduroam
Typ sieci:	Punkt dostępu
Dostępność sieci:	Wszyscy użytkownicy
📝 Połącz automaty	cznie, gdy ta sieć jest w zasięgu
📃 Połącz z siecią p	referowaną, jeśli jest dostępna
📄 Połącz, nawet je	śli sieć nie emituje nazwy (SSID)
🕎 Włącz ustawieni	a połączenia Intel
Konfiguruj	
	\square

ſyp zabezpieczeń:	WPA2-Enterprise	•]
Typ szyfrowania:	AES	•
Wybierz metode uwie	erzytelniania sieci:	
Microsoft: Chronion	v protokół EAP (PEA 🔫 👘	stawienia
	1 - 1	-
Zapamiętaj moje j przy każdym logo	poswiadczenia dla tego połą: waniu	zenia
F. 74	100000	
	R	
	2	
(\$	
Ustawienia zaawan	sowane	

W oknie **Właściwości** chronionego protokołu EAP zaznaczamy opcję: Podczas łączenia **Weryfikuj certyfikat** serwera i na liście zaufanych głównych urzedów certyfikacji zaznaczamy: **IFJ PAN – CA Root** wybieramy metodę uwierzytelniania: **Bezpieczne** hasło (EAP-MSCHAP v2) i klikamy przycisk **Konfiguruj**:

-	
odczas łączenia:	
🔽 Weryfikuj certyfikat serwera	
Połącz tylko z tymi serwerami:	
Zaufana déwna urzedu certufikaciju	
CTE CuberTrust Clebel Deet	12
GTE Cyber Hust Global Root	
Michel Kraemer	
Microsoft Root Authority	-
Microsoft Root Certificate Authority	
Thawte Premium Server CA	
thawte Primary Root CA	*
•	•
lub zaufanych urzędów certyfikacji ybierz metodę uwierzytelniania:	enjardene on
	▼ Konfiguruj
Bezpieczne hasło (EAP-MSCHAP v2)	
Bezpieczne hasło (EAP-MSCHAP v2) Włącz szybkie łączenie ponowne Wymuś ochronę dostępu do sieci Rozłącz, jeśli serwer nie przedstawi obiektu T kryptograficznego	LV powiązania
Jezpieczne hasło (EAP-MSCHAP v2) Włącz szybkie łączenie ponowne Wymuś ochronę dostępu do sieci Rozłącz, jeśli serwer nie przedstawi obiektu T kryptograficznego Włącz prywatność tożsamości	LV powiązania
Bezpieczne hasło (EAP-MSCHAP v2) Włącz szybkie łączenie ponowne Wymuś ochronę dostępu do sieci Rozłącz, jeśli serwer nie przedstawi obiektu T kryptograficznego Włącz prywatność tożsamości	LV powiązania

W oknie Właściwości protokołu EAP MSCHAPv2 odznaczamy opcję Automatycznie użyj nazwy logowania i hasła (oraz domeny, jeżeli istnieje) systemu Windows i wciskamy przycisk Ok:

W oknie **Właściwości sieci bezprzewodowej** w zakładce **Zabezpieczenia** wciskamy przycisk **Ustawienia zaawansowane**:

Jeżeli nie ma przycisku Ustawienia zaawansowane (Windows Vista) to pomijamy ten punkt oraz następny, naciskamy Ok, Ok i wykonujemy kolejne punkty konfiguracji.

odczas łączenia:	
	a second a second s
Automatycznie uz oraz domeny, jeź	żyj mojej nazwy logowania i hasła jeli istniele) systemu Windows
Automatycznie u: oraz domeny, jeż	żyj mojej nazwy logowania i hasła żeli istnieje) systemu Windows
Automatycznie u: oraz domeny, jeż	żyj mojej nazwy logowania i hasł żeli istnieje) systemu Windows

ołączenie Zabezpiec	zenia
Typ zabezpieczeń:	WPA2-Enterprise
Typ szyfrowania:	AES 🔻
Microsoft: Chronion	v protokół EAP (PEA 🔹 Ustawienia
Microsoft: Chronion	y protokół EAP (PEA 🔹 Ustawienia
Microsoft: Chronion Zapamiętaj moje przy każdym logo	y protokół EAP (PEA 🔻 Ustawienia poświadczenia dla tego połączenia waniu
Microsoft: Chronion Zapamiętaj moje przy każdym logo	y protokół EAP (PEA 🔹 Ustawienia poświadczenia dla tego połączenia waniu
Microsoft: Chronion Zapamiętaj moje przy każdym logo	y protokół EAP (PEA 🔹 Ustawienia poświadczenia dla tego połączenia wwaniu
Microsoft: Chronion Zapamiętaj moje przy każdym logo Ustawienia zaawan	y protokół EAP (PEA 🔹 Ustawienia poświadczenia dla tego połączenia wwaniu
Microsoft: Chronion Zapamiętaj moje przy każdym logo Ustawienia zaawan	y protokół EAP (PEA 🔹 Ustawienia poświadczenia dla tego połączenia waniu

W oknie **Ustawienia** zaawansowane wybieramy tryb uwierzytelniania na: **Uwierzytelnianie użytkownika** i wciskamy: **Ok**, **Ok** i **Zamknij:**

Uwie	rzytelnianie	użytkownika	Zap	isz poświa	dczenia	
Uwier	zytelnianie	użytkownika lub	komputer	a		
Uwie	zytelnianie	użytkownika	N	ALL HICOVY		
Uwiel Włacz	zyteinianie	goscia jednokrotna dla	vij tel cieci			
U Wiącz	i ejesu acje	jeunoù où iaj die	r tej sieu		Q.,	
@ W	ykonaj bezj	osrednio przed	logowanie	m użytkow	nika	
Maker	ykonaj bezi zmalna onó	iosreanio po iog	owaniu uz dachiu	ytkownika	181	
TTT 7-	maine opo	unionio (mischain	-Hermite	10	1000	
dia	alogowych j	odczas rejestra	cji jednokr	otnej		
Ta uw	sieć używa vierzytelnie	i oddzielnych wir nia komputera i i	tualnych s użytkownik	sieci LAN do ca	2	

Podczas łączenia się z siecią eduroam niezbędne będzie wprowadzenie dodatkowych informacji uwierzytelniających: Wprowadź poświadczenia użytkownika.

Nazwa użytkownika: Państwa adres e-mail, np: jan.kowalski@ifj.edu.pl oraz

Hasło: ***

(z systemu rejestracji)

Jeżeli wykonaliśmy wszystkie poprzednie czynności zgodnie z instrukcją od tej chwili będąc w zasięgu sieci **eduroam**, mamy działające połączenie bezprzewodowe z siecią **eduroam**:



W przypadku trudności ze skonfigurowaniem dostepu do sieci **eduroam** prosimy o kontakt <u>admin@ifj.edu.pl</u> Tel 8293 – Dział Sieci Komputerowych