

**Propozycje tematów projektów grupowych inżynierskich na r.
akad. 2017/18
KTIN**

1. AIS over IPv6: System dystrybucji i wizualizacji danych AIS w sieci bezprzewodowej wykorzystującej IPv6
2. Szacowanie przepływności transmisji danych w sieciach bezprzewodowych z wykorzystaniem sieci neuronowej
3. Projekt i instalacja heterogenicznej stacji bazowej systemu netBaltic
4. System zdalnego dostępu do treści stron WWW oraz synchronizacji plików w środowisku sieci odpornej na opóźnienia transmisji (Delay Tolerant Network)
5. System masowej dystrybucji plików dla potrzeb udostępniania map nawigacyjnych
6. Aplikacja do bezpośredniej komunikacji między jednostkami pływającymi
7. Automatyczny tester parametrów jakościowych łącza bezprzewodowego
8. Realizacja niezawodnej transmisji informacji dla odbiorcy biznesowego
9. Projekt i implementacja rozwiązania VPN dla odbiorcy biznesowego ze szczególnym uwzględnieniem aspektu niezawodności transmisji
10. Integracja istniejących baz danych do spójnego systemu zarządzania klientami usług typu DNS w CI TASK
11. Projekt i implementacja symulatora sieci pierścieniowej
12. Projekt i implementacja „małego” Internetu Rzeczy
13. Symulator komunikacji statków na Bałtyku z wykorzystaniem danych historycznych AIS
14. Aplikacja do wieloetapowego przekazywania wiadomości w sieciach DTN o sporadycznej łączności
15. Interaktywny firewall sieciowy
16. Implementacja wymiany certyfikatu użytkownika na podpisany przez inny urząd certyfikacji przy użyciu standardowego protokołu
17. Implementacja mechanizmu rotacji certyfikatów w sieci niewrażliwej na opóźnienia (DTN)

Temat w języku polskim	AIS over IPv6: System dystrybucji i wizualizacji danych AIS w sieci bezprzewodowej wykorzystującej IPv6
Temat w języku angielskim	AIS over IPv6: AIS data dissemination over IPv6 networks
Opiekun pracy	mgr inż. Michał Hoefl
Konsultant pracy	
Cel pracy	<p>Celem projektu jest opracowanie systemu dystrybucji danych AIS poprzez sieć Wi-Fi do mniejszych jednostek niewyposażonych w odbiorniki AIS. Będzie to narzędzie ułatwiające poruszanie się mniejszym jednostkom (łódkom, małym jachtom) oraz zwiększające bezpieczeństwo żeglugi. W przypadku dostępności danych GPS na mniejszej jednostce powinna być one rozgłaszane w formacie AIS do jednostek większych. System powinien składać się z dwóch elementów:</p> <ul style="list-style-type: none"> - modułu rozgłaszającego dane AIS/GPS - modułu odbierającego dane oraz aplikacji webowej/mobilnej do wizualizacji
Zadania	<ol style="list-style-type: none"> 1. Zapoznanie się dokumentacją systemu AIS 2. Opracowanie architektury rozwiązania 3. Implementacja 4. Testy
Literatura	1. Dostępna u opiekuna pracy
Uwagi	

Temat w języku polskim	Szacowanie przepływność transmisji danych w sieciach bezprzewodowych z wykorzystaniem sieci neuronowej
Temat w języku angielskim	Neural networks for throughput estimation in wireless networks
Opiekun pracy	mgr inż. Michał Hoefl
Konsultant pracy	
Cel pracy	Wiele czynników wpływa na efektywną przepływność transmisji danych w sieciach bezprzewodowych. Dokładne oszacowanie tego parametru nie jest zadaniem łatwym. W ramach projektu należy zaimplementować sieć neuronową, która wykorzystując dostępne parametry np. współczynnik strat pakietów, przepustowość łącza itp. pozwoli na oszacowanie efektywnej przepływności dostępnej dla połączeń TCP
Zadania	<ol style="list-style-type: none"> 1. Zapoznanie się szczegółami działania protokołu TCP 2. Zapoznanie się z istniejącymi metodami szacowania przepływności 3. Opracowanie metody dedykowanej dla sieci bezprzewodowych 4. Implementacja 5. Testy
Literatura	<ol style="list-style-type: none"> 1. S. M. H. Shah, A. u. Rehman, A. N. Khan and M. A. Shah, "TCP throughput estimation: A new neural networks model," <i>2007 International Conference on Emerging Technologies</i>, Islamabad, 2007, pp. 94-98 2. B.V. Ghita, S.M. Furnell, B. Lines, and E.Ifeachor: TCP performance estimation using neural networks modelling 3. M. Dondo and J. Treurniet: Investigation of a Neural Network Implementation of a TCP Packet Anomaly Detection System
Uwagi	

Temat w języku polskim	Projekt i instalacja heterogenicznej stacji bazowej systemu netBaltic
Temat w języku angielskim	Heterogeneous base station of the netBaltic system – project and implementation
Opiekun pracy	mgr inż. Michał Hoefl
Konsultant pracy	
Cel pracy	W ramach projektu należy zaprojektować połączenie komponentów dostępnych technik transmisji m.in.: WiMAX, IEEE 802.11ac, D-Star oraz elementów systemu netBaltic i elementów antenowych, a następnie zainstalować i przetestować je względem zasięgowym i jakościowym przygotowaną instalację.
Zadania	<ol style="list-style-type: none"> 1. Projekt połączenia komponentów w szafie zewnętrznej 36U 2. Instalacja komponentów 3. Uruchomienie stacji bazowe (potencjalne miejsce - Hel) 4. Testy instalacji
Literatura	<ol style="list-style-type: none"> 1. Dokumentacja systemu RADWIN Fiber-in-Motion 2. Dokumentacja systemu WiMAX Breeze 3. Dokumentacja urządzeń MIKROTIK z interfejsami IEEE 802.11ac
Uwagi	

Temat w języku polskim	System zdalnego dostępu do treści stron WWW oraz synchronizacji plików w środowisku sieci odpornej na opóźnienia transmisji (Delay Tolerant Network)
Temat w języku angielskim	Web-browsing and file synchronization solution in Delay Tolerant Network (DTN) environment
Opiekun pracy	Mgr inż. Krzysztof Gierłowski
Konsultant pracy	
Cel pracy	<p>W przypadku niektórych systemów sieciowych (np. komunikacji morskiej) nie dysponujemy stałą, nieprzerwaną łącznością między urządzeniami. W takim wypadku niemożliwe jest bezpośrednie korzystanie z wielu popularnych usług Internetowych.</p> <p>Celem projektu jest stworzenie rozwiązania, pozwalającego na zamawianie przez użytkownika danych z określonych stron WWW lub aktualizacji określonych plików, które zostaną mu następnie dostarczone w postaci wiadomości. Wiadomości te (wielkości nawet do dziesiątków MB) mogą na swojej drodze do adresata być przechowywane przez routery przez dłuższe okresy czasu, aż pojawi się łączność sieciowa niezbędna do ich dalszego przekazania.</p>
Zadania	<ol style="list-style-type: none"> 1. Zaprojektowanie ogólnej architektury systemu – części transmisyjnej oraz usługowej. 2. Projekt i implementacja mechanizmów przekazywania paczek danych w sieci. 3. Projekt i implementacja usług synchronizacji plików oraz obrazowania stron WWW w postaci paczek przeznaczonych do przeglądania offline. 4. Opracowanie demonstratora systemu.
Literatura	<ol style="list-style-type: none"> 1. Delay-Tolerant Networking Research Group (DTNRC) website. 2. IETF service and protocol specifications.

Temat w języku polskim	System masowej dystrybucji plików dla potrzeb udostępniania map nawigacyjnych
Temat w języku angielskim	Maritime navigation map distribution system
Opiekun pracy	Mgr inż. Krzysztof Gierłowski
Konsultant pracy	
Cel pracy	<p>Mapy nawigacyjne i pogodowe stanowią jeden z podstawowych instrumentów bezpieczeństwa żeglugi. Dostarczenie ich w niezawodny sposób, w odpowiednio krótkim okresie czasu do jednostek pływających przebywających na morzu jest więc nieodzowne, lecz w chwili obecnej zadanie to napotyka na problemy techniczne oraz ekonomiczne (mały zasięg systemów transmisji klasycznej i duży koszt łączności satelitarnej).</p> <p>Celem projektu jest opracowanie i implementacja aplikacji pozwalających na rozpowszechnianie danych nawigacyjnych poprzez przekazywanie ich w systemie, gdzie łączność nawiązywana jest jedynie sporadycznie pomiędzy jednostkami pływającymi znajdującymi się chwilowo w bliskiej odległości.</p>
Zadania	<ol style="list-style-type: none"> 1. Przegląd mechanizmów komunikacji morskiej wyspecyfikowanych w ramach projektu NetBaltic 2. Opracowanie projektu aplikacji pozwalającej na dystrybucję danych nawigacyjnych 3. Implementacja aplikacji i testy wstępne 4. (opcjonalnie) Testy w warunkach zbliżonych do rzeczywistych warunków wykorzystania systemu
Literatura	<ol style="list-style-type: none"> 1. Dokumentacja dotycząca systemów generowania map nawigacyjnych dostępna w ramach projektu NetBaltic 2. Dokumentacja dotycząca systemów dostarczania danych dostępna w ramach projektu NetBaltic 3. Dokumentacja stosowanych obecnie systemów synchronizacji treści

Temat w języku polskim	Aplikacja do bezpośredniej komunikacji między jednostkami pływającymi
Temat w języku angielskim	Maritime ship-to-ship communication system
Opiekun pracy	Mgr inż. Krzysztof Gierłowski
Konsultant pracy	
Cel pracy	<p>Komunikacja bezprzewodowa pomiędzy jednostkami pływającymi posiada wiele podobieństw do komunikacji lądowej, jednakże istnieją także znaczące różnice. Projekt NetBaltic przewiduje zastosowanie popularnych technik transmisji bezprzewodowej do zastosowań morskich, celem zapewnienia komunikacji pomiędzy statkami oraz statkami i infrastrukturą brzegową.</p> <p>W celu realizacji tego zadania, konieczne jest opracowanie aplikacji pozwalającej na konfigurację i monitorowanie pracy interfejsów bezprzewodowych popularnych technik transmisji (jak np. WiFi, WiMAX, LTE i inne) tak, aby umożliwiały jak najskuteczniejszą łączność pomiędzy statkami.</p> <p>Celem pracy jest opracowanie aplikacji pozwalającej na:</p> <ul style="list-style-type: none"> - automatyczną konfigurację interfejsów bezprzewodowych różnych typów, - wykrywanie sąsiednich jednostek i monitorowanie jakości łączności którą dysponujemy z nimi, - przesyłanie danych do sąsiednich jednostek pomimo chwilowych przerw w łączności (spowodowanych np. falowaniem morza).
Zadania	<ol style="list-style-type: none"> 1. Przegląd popularnych technik transmisji możliwych do zastosowania na morzu 2. Opracowanie projektu aplikacji pozwalającej automatyczną konfigurację interfejsów, wykrywanie sąsiednich jednostek i przesyłanie danych 3. Implementacja aplikacji i testy wstępne 4. (opcjonalnie) Testy w warunkach zbliżonych do rzeczywistych warunków wykorzystania systemu
Literatura	<ol style="list-style-type: none"> 1. Dokumentacja system komunikacyjnego dostępna w ramach projektu NetBaltic 2. Dokumentacja urządzeń komunikacji bezprzewodowej (WiFi, WiMAX, LTE, RADWIN)

Temat w języku polskim	Automatyczny tester parametrów jakościowych łącza bezprzewodowego
Temat w języku angielskim	Automatic tester of wireless link quality
Opiekun pracy	Mgr inż. Krzysztof Gierłowski
Konsultant pracy	
Cel pracy	<p>W wielu wypadkach mamy obecnie do czynienia z bezprzewodowym dostępem sieciowym. Doświadczenie pokazuje, iż jakość komunikacji różni się w znaczący sposób nie tylko pomiędzy różnymi technikami transmisji bezprzewodowej (np. WiFi a WiMAX), czy nawet pomiędzy różnymi wersjami tej samej techniki (np. IEEE 802.11g, a IEEE 802.11ac), lecz nawet pomiędzy systemami złożonymi tych samych urządzeń. W tej sytuacji bardzo przydatne byłoby opracowanie urządzenia, które umożliwiałoby automatyczne przetestowanie jakości łączności oferowanej przez dany system dostępu.</p> <p>Celem pracy jest zaprojektowanie i implementacja takiego urządzenia na platformie RPi2 lub dostępnych komputerów przemysłowych (ECN-680A / UNO-3083). Możemy założyć, że dysponujemy możliwością podłączenia urządzeń po obu stronach testowanego łącza.</p>
Zadania	<ol style="list-style-type: none"> 1. Przegląd parametrów łącza komunikacyjnego i wybór zbioru obsługiwanych przez tester 2. Zaprojektowanie i implementacja testera na platformie RPi2 lub dostępnych komputerów przemysłowych (ECN-680A / UNO-3083). 3. Testy w urządzeniu w warunkach laboratoryjnych. 4. (opcjonalnie) Testy urządzenia w ramach projektu NetBaltic.
Literatura	<ol style="list-style-type: none"> 1. Dokumentacja ITU i IETF dotycząca sposobów testowania i parametrów jakościowych łączy. 2. Dokumentacja urządzeń na których zaimplementowane zostanie oprogramowanie testera.

Temat w języku polskim	Realizacja niezawodnej transmisji informacji dla odbiorcy biznesowego
Temat w języku angielskim	Implementation of reliable transmission for business recipients
Opiekun pracy	Dr hab. inż. Jacek Rak
Konsultant pracy	Dr hab. inż. Jacek Rak
Cel pracy	Celem pracy jest zaproponowanie i praktyczna realizacja rozwiązania zapewniającego niezawodny przesył informacji dla klienta biznesowego.
Zadania	<ol style="list-style-type: none"> 1. Przegląd literatury z zakresu aspektów niezawodnej transmisji, odporności sieci na awarie węzłów/łączy. 2. Projekt rozwiązania 3. Konfiguracja sprzętowa rozwiązania 4. Testowanie i demonstracja rozwiązania
Literatura	<ol style="list-style-type: none"> 1. Materiały dostępne w bazie IEEE Xplore 2. Literatura podana przez prowadzącego
Uwagi	-

Temat w języku polskim	Projekt i implementacja rozwiązania VPN dla odbiorcy biznesowego ze szczególnym uwzględnieniem aspektu niezawodności transmisji
Temat w języku angielskim	Design and implementation of a VPN solution for a business user with focus on transmission reliability
Opiekun pracy	Dr hab. inż. Jacek Rak
Konsultant pracy	Dr hab. inż. Jacek Rak
Cel pracy	Celem pracy jest realizacja projektu, jak i praktycznej implementacji rozwiązania wirtualnej sieci prywatnej ze szczególnym uwzględnieniem aspektu niezawodności transmisji w obliczu ewentualnych awarii węzłów / łączy sieci
Zadania	<ol style="list-style-type: none"> 1. Przegląd literatury z zakresu architektur sieci VPN oraz mechanizmów niezawodnej transmisji w obliczu awarii węzłów/łączy. 2. Projekt rozwiązania 3. Konfiguracja sprzętowa rozwiązania 4. Testowanie i demonstracja rozwiązania
Literatura	<ol style="list-style-type: none"> 1. Materiały dostępne w bazie IEEE Xplore 2. Literatura podana przez prowadzącego
Uwagi	-

Temat projektu/pracy dyplomowej inżynierskiej (jęz. pol.)	Integracja istniejących baz danych do spójnego systemu zarządzania klientami usług typu DNS w CI TASK
Temat projektu/pracy dyplomowej inżynierskiej (jęz. ang.)	Integration of existing databases to produce one management system for DNS clients in CI TASK
Opiekun pracy	dr inż. Krzysztof Nowicki
Konsultant pracy	mgr inż. Łukasz Wiszniewski
Cel pracy	Optymalizacja i rozwój systemu ułatwiającego administrowanie klientami posiadającymi domeny w CI TASK
Zadania do wykonania	<ol style="list-style-type: none"> 1. Zapoznanie się ze sposobem zarządzania domenami w CI TASK. 2. Zapoznanie się z istniejącymi bazami danych w CI TASK. 3. Projekt zintegrowanej bazy danych. 5. Implementacja zaprojektowanego rozwiązania. 6. Testy działania. 7. Wdrożenie systemu
Źródła	<ol style="list-style-type: none"> 1. Dokumentacja systemu BIND 2. Standard DNS: RFC 1034 oraz RFC 1035 3. praca inżynierska panów A. Voss i P. Milewski
Liczba wykonawców	2-4
Uwagi	Przy realizacji projektu możliwość odbycia praktyk w CI TASK

Temat projektu/pracy dyplomowej inżynierskiej (jęz. pol.)	Projekt i implementacja symulatora sieci pierścieniowej
Temat projektu/pracy dyplomowej inżynierskiej (jęz. ang.)	Design and implementation of Simulator of Ring Network
Opiekun pracy	dr inż. Krzysztof Nowicki
Konsultant pracy	
Cel pracy	Celem pracy jest realizacja projektu symulatora sieci pierścieniowej, dedykowanego do przeprowadzania dydaktycznych ćwiczeń laboratoryjnych.
Zadania do wykonania	<ol style="list-style-type: none"> 1. Przegląd literatury z zakresu sieci pierścieniowych 2. Projekt rozwiązania 3. Konfiguracja programowo-sprzętowa rozwiązania 4. Demonstracja rozwiązania na zajęciach dydaktycznych 5. Ocena możliwości wykorzystania symulatora do badań wydajności pracy sieci pierścieniowych
Źródła	<ol style="list-style-type: none"> 1. Industrial Ethernet Book, ISSN 1470-5745, czasopismo dostępne w wersji papierowej u opiekuna projektu 2. Instrukcje laboratoryjne do zajęć z sieci komputerowych dostępne u opiekuna projektu 3. „Ogólna literatura sieciowa”
Liczba wykonawców	2-4
Uwagi	

Temat projektu/pracy dyplomowej inżynierskiej (jęz. ang.)	Design and implementation of a "small" Internet of Things
Opiekun pracy	dr inż. Krzysztof Nowicki
Konsultant pracy	
Cel pracy	Celem projektu jest wykonanie demonstracyjnej sieci typu IoT.
Zadania do wykonania	<ol style="list-style-type: none"> 1. Przegląd literatury z zakresu Internetu Rzeczy 2. Przegląd rozwiązań Internetu Rzeczy 3. Wybór sensorów i urządzeń M2M 4. Wybór technologii bezprzewodowej 5. Projekt sieci pokazowej 6. Implementacja sieci pokazowej 7. Demonstracja sieci na zajęciach dydaktycznych dla wybranych grup studenckich
Źródła	1. Miller Michael: Internet rzeczy, Wydawnictwo Naukowe PWN, 2016
Liczba wykonawców	2-4
Uwagi	

Temat w języku polskim	Symulator komunikacji statków na Bałtyku z wykorzystaniem danych historycznych AIS
Temat w języku angielskim	Simulator of ships communication using historical AIS data from Baltic Sea
Opiekun pracy	dr inż. Wojciech Gumiński
Konsultant pracy	
Cel pracy	Celem projektu jest zebranie statystyk możliwości komunikacji jednostek pływających po Bałtyku z wykorzystaniem dostępnych danych historycznych AIS. Symulacja wykorzystując pozycje statków z danych AIS powinna określać sąsiedztwo oraz możliwość komunikacji bezpośredniej i wieloetapowej przy założonych zasięgach dostępnych technologii transmisji danych.
Zadania	<ol style="list-style-type: none"> 1. Przegląd stanu sztuki dotyczący sieci DTN 2. Implementacja komunikacji z bazą danych historycznych AIS 3. Implementacja wizualizacji i statystyk 4. Implementacja wybranych algorytmów przekazywania wiadomości
Literatura	<ol style="list-style-type: none"> 1. K. Fall, „A delay-tolerant network architecture for challenged internets” Computer Communications Review, New York 2003 2. „Internet na Bałtyku” Studium wykonalności, Gdańsk 2014, http://www.netbaltic.pl 3. Gumiński W.: „Koncepcja realizacji usług w sieci o nieciągłej i sporadycznej łączności”; Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne. -, nr. 12 (2016), s.1339-1342
Uwagi	

Temat w języku polskim	Aplikacja do wieloetapowego przekazywania wiadomości w sieciach DTN o sporadycznej łączności
Temat w języku angielskim	
Opiekun pracy	dr inż. Wojciech Gumiński
Konsultant pracy	
Cel pracy	Celem projektu jest implementacja modułu transportowego umożliwiającego buforowanie i wieloetapowe przekazywanie wiadomości niezależnych od treści w sieciach o sporadycznej i nieciągłej łączności. Należy zaimplementować algorytmy przekazywania wiadomości zawierające różne mechanizmy unikania duplikatów i optymalizacji czasu dostarczenia wiadomości. Komunikacja z sąsiadami powinna się odbywać w trybie punkt-punkt z wykorzystaniem protokołu TCP w sieci IPv6. Implementacja aplikacji w języku C# w środowisku dotNET (dotNET Core i Mono w systemie Linux).
Zadania	<ol style="list-style-type: none"> 1. Przegląd stanu sztuki dotyczący sieci DTN 2. Implementacja komunikacji IPv6 3. Implementacja wybranych algorytmów przekazywania wiadomości 4. Testy i opracowanie wyników
Literatura	<ol style="list-style-type: none"> 1. K. Fall, „A delay-tolerant network architecture for challenged internets” Computer Communications Review, New York 2003 2. „Internet na Bałtyku” Studium wykonalności, Gdańsk 2014, http://www.netbaltic.pl 3. Gumiński W.: „Koncepcja realizacji usług w sieci o nieciągłej i sporadycznej łączności”; Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne. -, nr. 12 (2016), s.1339-1342
Uwagi	

Temat projektu/pracy dyplomowej inżynierskiej (jęz. pol.)	Interaktywny firewall sieciowy
Temat projektu/pracy dyplomowej inżynierskiej (jęz. ang.)	Interactive network firewall
Opiekun pracy	dr inż. Tomasz Gierszewski
Konsultant pracy	
Cel pracy	Firewalle można podzielić na osobiste, mające świadomość aplikacji oraz pozwalające na interakcję użytkownika oraz sieciowe, które nie posiadają żadnej z tych cech. Celem pracy jest implementacja firewalla sieciowego w systemie z rodziny Linux lub BSD, który pozwoli interaktywnie decydować o nowych regułach dla ruchu sieciowego. Firewall powinien zatem posiadać jedną z dwóch wymienionych cech firewalla osobistego – być interaktywny dla operatora, który z nim pracuje. W ramach pracy należy także zaproponować sposób utrzymywania połączenia TCP do czasu podjęcia decyzji przez operatora. Interfejs może być zrealizowany w dowolnej formie, pod warunkiem przedstawienia możliwie obszernego opisu ruchu sieciowego. Firewall powinien mieć możliwość dodania reguł dokładnie przystających do prezentowanego ruchu lub, z wykorzystaniem popularnych uogólnień – np. większej podsieci, w której zawiera się adres.
Zadania do wykonania	<ol style="list-style-type: none"> 1. Opracowanie sposobu opóźnienia zestawienia połączenia TCP w sposób pozwalający na reakcję operatora. 2. Opracowanie zbioru informacji prezentowanych operatorowi oraz zbioru akcji możliwych do podjęcia 3. Projekt rozwiązania 4. Implementacja i testy funkcjonalne
Źródła	<p>Sposób działania TCP oraz opcji DEFER_ACCEPT: https://labs.ripe.net/Members/gih/the-curious-case-of-the-crooked-tcp-handshake</p> <p>Połączenie TCP w Pythonie: https://jvns.ca/blog/2014/08/12/what-happens-if-you-write-a-tcp-stack-in-python/</p>
Liczba wykonawców	3
Uwagi	

Temat projektu/pracy dyplomowej inżynierskiej (jęz. pol.)	Implementacja wymiany certyfikatu użytkownika na podpisany przez inny urząd certyfikacji przy użyciu standardowego protokołu
Temat projektu/pracy dyplomowej inżynierskiej (jęz. ang.)	Implementation of end-entity certificate rotation based on standard protocol with the change of certification authority
Opiekun pracy	dr inż. Tomasz Gierszewski
Konsultant pracy	
Cel pracy	Istnieje kilka protokołów, które pozwalają automatycznie wystawiać oraz wymieniać certyfikaty na nowe: CMP, CMC, SCEP. SCEP jest najpopularniejszym rozwiązaniem, ale w typowym modelu użycia zakłada weryfikację dotychczasowego i podpisywanie nowego certyfikatu przez ten sam urząd certyfikacji (CA). Natomiast CMP pozwala na przedstawiony w tytule scenariusz, ale jest mało popularny w rozwiązaniach OpenSource. Celem projektu jest rozwiązanie postawionego problemu w taki sposób, aby podmiot przedstawił się własnym dotychczasowym certyfikatem, uzyskał jego pomyślną weryfikację, a następnie otrzymał nowy materiał kryptograficzny od innego CA.
Zadania do wykonania	<ol style="list-style-type: none"> 1. Analiza istniejących rozwiązań rotacji certyfikatów 2. Projekt rozwiązania problemu 3. Wybór technik i narzędzi 4. Implementacja i testowanie funkcjonalne
Źródła	<ol style="list-style-type: none"> 1. Draft RFC - Simple Certificate Enrollment Protocol: https://tools.ietf.org/html/draft-nourse-scep-23 2. RFC 6402 – Certificate Management over CMS (CMC) 3. Krytyka SCEP: http://security.stackexchange.com/questions/56142/what-is-the-different-between-cmp-and-scep-protocol 4. Otwartoźródłowa wersja biblioteki cryptlib: https://www.cs.auckland.ac.nz/~pgut001/cryptlib/index.html
Liczba wykonawców	3
Uwagi	

Temat projektu/pracy dyplomowej inżynierskiej (jęz. pol.)	Implementacja mechanizmu rotacji certyfikatów w sieci niewrażliwej na opóźnienia (DTN)
Temat projektu/pracy dyplomowej inżynierskiej (jęz. ang.)	Implementation of certificate rotation procedure dedicated for delay-tolerant networks (DTNs)
Opiekun pracy	dr inż. Tomasz Gierszewski
Konsultant pracy	
Cel pracy	Sieci niewrażliwe na opóźnienia cechuje brak ciągłości w komunikacji wieloskokowej, najczęściej bezprzewodowej. Oznacza to, że paczki danych przesyłane są na podobieństwo serwerów proxy – węzeł przyjmuje paczkę i czeka na dogodny moment do dalszej transmisji. W takim środowisku nie można przeprowadzić typowego uwierzytelnienia w oparciu o kryptografię asymetryczną, bo wymaga ono jednoczesności. Ponadto, sieć często cechuje niskie zaufanie do węzłów tranzytowych. Dlatego paczki są podpisane i zaszyfrowane certyfikatami, co uniemożliwia odtajnienie ich zawartości oraz czyni manipulację niezasadną (wykrywalną). W takim środowisku należy zaproponować i zrealizować obsługę paczek, które obok paczek z danymi pozwolą przesłać żądanie certyfikatu oraz odpowiedź z podpisanym, nowym certyfikatem węzła.
Zadania do wykonania	<ol style="list-style-type: none"> 1. Opracowanie teorii dotyczącej kryptografii asymetrycznej wykorzystującej certyfikaty X.509 2. Przygotowanie lub integracja ze środowiskiem emulacji sieci DTN 3. Projekt rozwiązania 4. Implementacja i testy funkcjonalne 5. Demonstracja w środowisku emulacyjnym
Źródła	<ol style="list-style-type: none"> 1. Strona domowa projektu netBaltic, przykładu sieci DTN w strefie C: http://netbaltic.pl/ 2. Różnorodna literatura na temat kryptografii asymetrycznej, w szczególności podpisu i szyfrowania w oparciu o certyfikaty – element pracy
Liczba wykonawców	3
Uwagi	