

Zdalny dostęp i zasilanie bazy ORACLE 9i z wykorzystaniem XML oraz infrastruktury klucza publicznego

Kazimierz Frączkowski

*Wydziałowy Zakład Informatyki, Wydział Informatyki i Zarządzania Politechniki Wrocławskiej
e-mail: fraczkowski@ci.pwr.wroc.pl*

Abstrakt

Artykuł dotyczy zrealizowanego systemu informatycznego, którego celem jest zdalne połączenie rozproszonych aplikacji lokalnych poprzez Internet z Centralną Bazą Danych (CBD) wykorzystującą ORACLE 9i w Data Centre (DC). W przekazie dokumentów z lokalnych ośrodków zastosowano bezpieczny kanał komunikacyjny i infrastrukturę klucza publicznego (PKI) w tym: szyfrowanie informacji, skrót informacji, podpis elektroniczny. Lokalne aplikacje rozmieszczone na terenie całego kraju realizują takie zadania jak: testowanie połączenia z serwerem w DC, import słowników z bazy centralnej, przygotowanie wniosków-dokumentów do wysłania, wysłanie wniosków do weryfikacji, przyjęcie wyników weryfikacji. Centralnie realizowane są następujące zadania: przygotowanie i wysłanie słowników na szczebel lokalny, przyjęcie wniosku ze szczebla lokalnego, wstawienie wniosku do bazy centralnej, weryfikacja przyjętego wniosku, wysłanie odpowiedzi o rezultacie weryfikacji. Format przesyłanych danych to XML. System generuje raporty na stronie www, w oparciu o dane zebrane w CBD.

Referat przeznaczony jest dla kierowników projektów, członków zespołów biorących udział w realizacji projektów w którym wykorzystuje się bazę danych ORACLE 9i oraz infrastrukturę klucza publicznego PKI do bezpiecznego przesyłu danych w sieci Internet.

Wprowadzenie

Podpis cyfrowy dający możliwość potwierdzania źródła informacji oraz jej niezaprzeczalność tak po stronie odbiorcy jak i wysyłającego, daje podstawy pełnego wykorzystania elektronicznego przesyłania dokumentów oraz zdalnego tworzenia i autoryzacji dokumentów. Ta technologia usankcjonowana prawnie z dniem 16.08.2002 stanowiła podstawę prezentowanego systemu REJESTR [2]. Celem tego systemu jest dostarczenie podmiotom zajmującym się prowadzeniem rejestrów, nowoczesnego narzędzia do *tworzenia elektronicznych rejestrów*. System zapewnia odpowiednią agregację, walidację, archiwizację oraz prezentację utworzonych danych w określony sposób, oraz serwis informacyjny poprzez strony Internetowe www. Sukcesywnie zbierane i przechowywane dane poprzez zaimplementowane mechanizmy lokalnej aplikacji oraz ich analiza i prezentacja, stanowią źródło *informacji* pomocne poszczególnym podmiotom zainteresowanym kształtowaniem polityki w obrębie wybranego sektora gospodarki czy usług, monitorowaniem jej stanu oraz jako źródło aktualnej informacji konsumenckiej dla wszystkich użytkowników systemu z poziomu www.

Podstawowa funkcjonalność systemu ma zapewnić:

1. Przedstawicielom administracji rządowej działającej w terenie sprawne narzędzie kontroli i nadzoru nad zakładami właściwego sektora funkcjonującymi na ich terenie. Obecna forma prowadzenia rejestru, bardzo często w wersji "teczkowo - papierowej" nie jest efektywnym narzędziem do bieżącego monitorowania działalności podmiotów.
2. W sposób znaczący wzmocni instrumenty statystyczno - planistyczne, będące w posiadaniu wojewody, właściwego ministra oraz przedstawicieli organizacji samorządowych.
3. Poprawne gromadzenie danych w poszczególnych rejestrach poprzez mechanizm ich bieżącej weryfikacji na szczeblu centralnym. Zapewnienie poprawności REGON, TERYT oraz stosowanej kodyfikacji dla poszczególnych zakładów, jednostek organizacyjnych oraz wchodzących w ich skład komórek.
4. Efektywne wyszukiwanie zakładów pod różnymi względami, poprzez prezentację całej bazy adresowej zakładów i ich komórek na stronach WWW.
5. Przetestowanie pilotażowego projektu dotyczącego centralnego przesyłania danych w sektorze medycznych z wykorzystaniem podpisu elektronicznego i PKI.

1. Architektura Systemu REJESTR

Koncepcja systemu REJESTR zakładała wykorzystanie najlepszych i sprawdzonych rozwiązań w zakresie technologii informatycznych przy minimalizacji nakładów finansowych na całość przedsięwzięcia. Doświadczenia, zasoby sprzętowe oraz zaplecze użytkownika systemu wskazywało na potrzebę zaadaptowaniu istniejącej bazy technicznej i organizacyjnej wykorzystywanej dotychczas do prowadzenia rejestrów zakładów, w celu zbudowania nowoczesnego systemu informacyjnego.

W systemie tym zastosowano rozwiązania informatyczne dedykowane do systemów rozproszonych wykorzystujące w zakresie komunikacji sieć publiczną Internet oraz centralne bazy danych umieszczone w specjalizowanym *Data Center*.

Techniczne i organizacyjne zabezpieczenie wymaganej funkcjonalności systemu REJESTR zrealizowano poprzez dedykowaną w tym celu infrastrukturę sprzętową oraz media transmisyjne z wykorzystaniem sieci Internet (Rys.1.1).

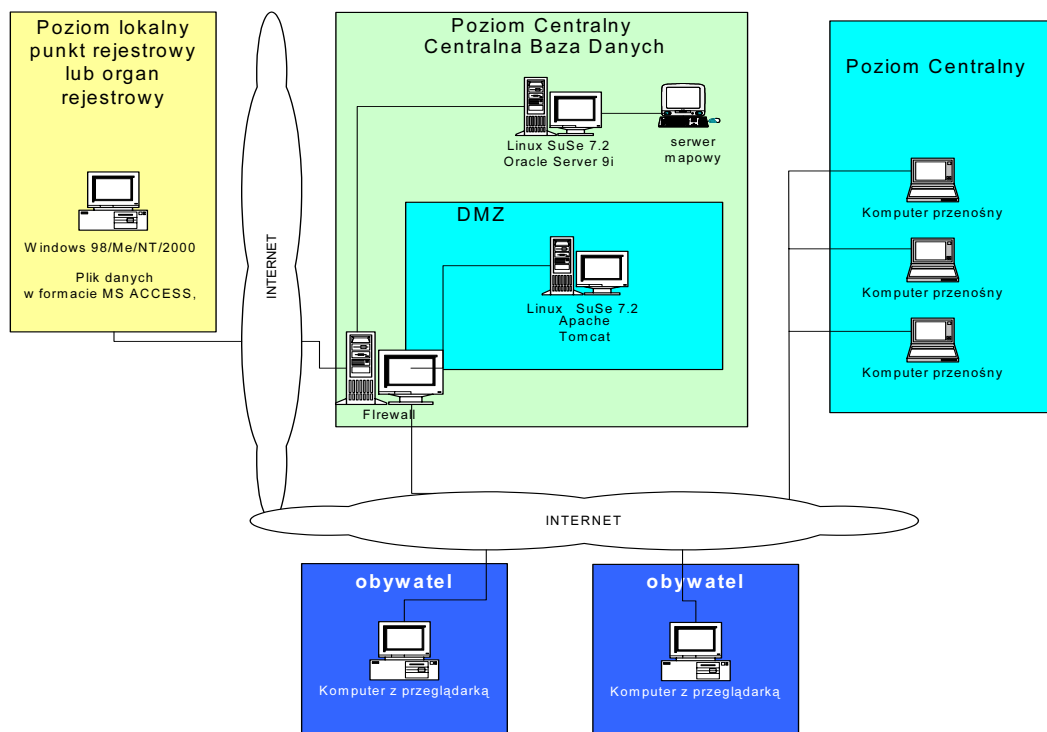
Poziom lokalny przez który rozumiemy organy rejestrowe, wyposażone w komputery klasy PC z Windows 98/Me/2000 z zainstalowanym oprogramowaniem i przeglądarką internetową. Każdy komputer z poziomu lokalnego ma zabezpieczony dostęp do Internetu. Poziom lokalny wybranej (wydzielonej) funkcjonalności systemu stanowi ogół obywateli, którzy poprzez dowolny komputer z przeglądarką internetową i dostępem do Internetu, mogą przeglądać zawartość wybranych informacji publikowanych z REJESTRU.

Poziom centralny stanowią elementy techniczne i oprogramowanie narzędziowe niezbędne do bezpiecznej komunikacji i przesyłania danych poprzez Internet z poziomu lokalnego do poziomu centralnego i na odwrót. Wyposażenie poziomu centralnego to:

- urządzenia i oprogramowanie systemowe w *Data Center*.

Data Center obsługę komunikacji z zewnętrzną siecią Internet zabezpiecza poprzez *Firewall* oraz dedykowany serwer na którym działa serwer webowy pełniący rolę serwera aplikacyjnego oraz publikacyjnego. Na serwerze webowym publikowane są informacje statystyczne, dostępne są listy adresowe zarejestrowanych podmiotów. W oparciu o serwer webowy Apache uzupełniony poprzez serwer aplikacyjny Tomcat oferowane są aplikacje napisane w języku Java (tzw. servlety). Podstawową usługą oferowanymi w ramach serwera aplikacyjnego jest przesył informacji. W celu umożliwienia przesyłu informacji w ramach serwera komunikacyjnego zostały założone konta użytkowników poziomu lokalnego, za pomocą których następuje przesyłanie danych przez tych użytkowników do serwera operacyjnego tzw. Centralnej Bazy Danych (CBD), którym jest odrębny komputer z wymaganym poziomem bezpieczeństwa pracy, zdefiniowanej przez poziom usługi *outsourcingowej Data Center*.

Dane z komputera w którym jest przechowywana Centralna Baza Danych, są replikowane codziennie do komputera środowiska produkcyjnego i monitorującego.



Rys. 1.1 Schemat organizacyjny posadowienia zasobów i aplikacji użytkowych zapewniających funkcjonalność Systemu- REJSTR.

1.1. Specyfikacja elementów funkcjonalnych systemu

System Tworzenia i Aktualizacji REJESTRU, posiada strukturę przedstawioną w Tabeli 1.1.

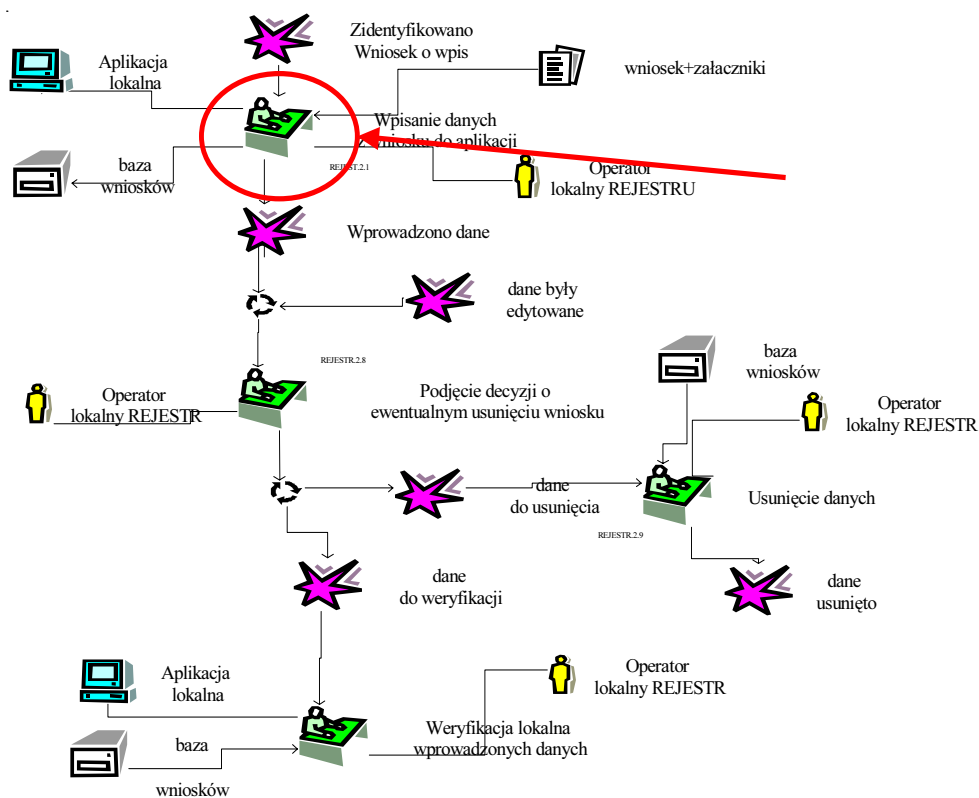
Tabela 1.1. Struktura systemu REJESTR

Nazwa systemu	Lp	Nazwa podsystemu	Lokalizacja
REJESTR	1	Podsystem rejestracji wniosków	Poziom lokalny REJESTR
	2	Podsystem komunikacyjny	Poziom lokalny REJESTR
	3	Podsystem komunikacyjny	Poziom centralny CBD
	4	Serwis informacyjny REJESTR	Poziom centralny CBD
	5	Podsystem gromadzenia i przetwarzania danych	Poziom centralny CBD

Modelowanie procesów związanych z System Tworzenia i Aktualizacji REJESTRU, wykonano przy pomocy metodologii **Architecture of Integrated Information Systems (ARIS)**, która okazała się:

- dobra we współpracy z klientem
- modele ARIS są przejrzyste i zrozumiałe dla osób nie związanych z informatyką
- gwarantuje kompletną specyfikacją wymagań
- wygodna w tworzeniu
- perspektywa organizacji
- Perspektywa funkcji
- perspektywa danych
- perspektywa procesów
- zapewnia wsparcie narzędziowe całego cyklu produkcyjnego

Modele ARIS operują na różnych poziomach abstrakcji -od koncepcji do implementacji. Zapewnia to wsparcie od etapu analizy do wdrożenia. Na rys.1.2. przedstawiono przykładową fazę modelowania procesu obsługi wniosków.



Rys. 1.2. Proces obsługi wniosku o wpis zakładu do REJESTRU.

1.2. Technologie i narzędzia informatyczne zastosowane w systemie

REJESTR

Baza danych **Oracle 9i** na serwerze Linux SuSe

- Tabele, perspektywy, trigery
- Ładowanie do tabel danych w **formacie XML**

Serwer aplikacyjny **Tomcat** z klasami **Javy**

Serwer webowy **Apache**

System dwuszczeblowy (organ rejestrowy wojewódzki, centrala)

System trzywarstwowy (BD, Serwer aplikacyjny, prezentacja – przeglądarka)

Prezentacja wyników i statystyk na stronie **www**. Wykorzystano **serwlety i JSP**

Infrastrukturę klucza publicznego (PKI)

- Zbudowano komponenty kryptograficzne wykorzystujące certyfikaty (kryptografia asymetryczna) zapewniające integralność i niezaprzeczalność przesyłanych danych.
- Wykorzystano karty mikroprocesorowe

Wykorzystano **INTERNET** Podsystem komunikacyjny

Wykorzystano **XML** w aplikacji lokalnej i centralnej (podsystem rejestracji wniosków)

Serwis mapowy z wykorzystaniem **ArcIMS i ArcSDE** (geometria map w BD)

- integracja danych opisowych z BD REJESTR z geometria zapisaną w strukturach SDE
- zastosowano warstwę podziału administracyjnego kraju do gminy
- przygotowano BD REJESTR do integracji z warstwą ulic i miejscowości
- zdalne zarządzanie ArsIMS i ArcSDE
- Outsourcing

Data Centre pełni funkcję administratora systemu poprzez udostępnienie infrastruktury technicznej i komunikacyjnej. Zdalne administrowanie systemem REJEST odbywa się poprzez opracowaną aplikację administratora centralnego.

2. Mechanizmy bezpieczeństwa przesyłu dokumentów

Podsystem komunikacji użyty w rozwiązaniu do wymiany danych opiera się na powszechnie stosowanym w Internecie protokole transportowym HTTP (ang. *HyperText Transfer Protokol*). Ze względu na to, że protokół HTTP oraz HTTPS (bezpieczna wersja protokołu HTTP) nie zapewnia takich atrybutów bezpieczeństwa jak niezaprzeczalność utworzenia dokumentu zdecydowano się na zastosowanie dedykowanych rozwiązań. Opracowany na potrzeby podsystemu komunikacji mechanizm bezpieczeństwa zapewnia:

- **Niezaprzeczalność** – odbiorca informacji ma mechanizm potwierdzający, że dany dokument został stworzony przez określoną instytucję/osobę
- **Poufność** – nikt nie uprawniony nie może zapoznać się z informacją podczas transmisji
- **Integralność** – podczas transmisji nikt nie może dokonywać zmian w dokumentach tak aby nie zostało to wykryte

Dla zapewnienia wysokiego poziomu bezpieczeństwa w rozwiązaniu wykorzystane zostały mechanizmy kryptograficzne [3]. Zastosowano ogólnie wykorzystywane algorytmy kryptograficzne tj. DES, 3DES, RSA, SHA1 oraz klucze o długości gwarantującej bezpieczeństwo zabezpieczanej informacji. Na bazie tych algorytmów zastosowano mechanizm podpisu cyfrowego, który gwarantuje niezaprzeczalność oraz integralność danych. Ponadto w rozwiązaniu wykorzystano certyfikaty zgodne z normą X.509v3 (ISO9595-8). Aby dokumenty były rozpoznawane jako dane ze znacznikami, wykorzystano XML (eXtensible Markup Language – rozszerzalny język znaczników). W języku XML każdy może tworzyć swoje własne znaczniki: ukryte etykiety, takie jak <kod pocztowy> lub <przychodnia>, które adnotują strony www albo poszczególne fragmenty ich zawartości.

2.1. Karty elektroniczne

Użytkownicy systemu REJESTR wykorzystujący w pełni funkcjonalność tego systemu 2dysponują kartami elektronicznymi [1]. Na każdej z nich znajdzie się:

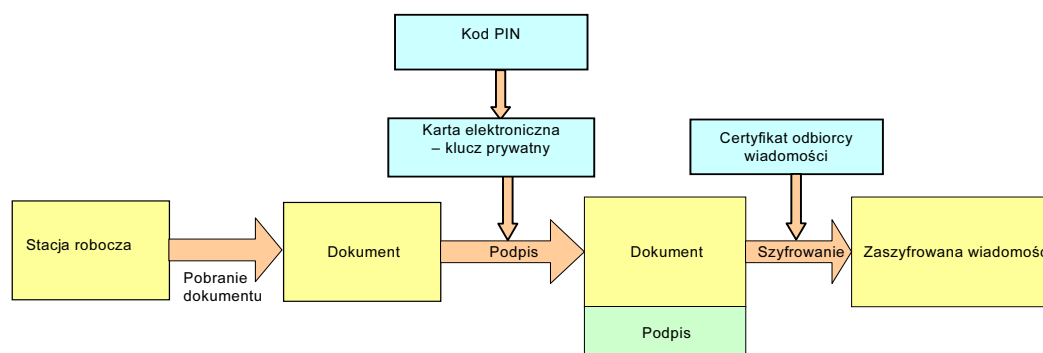
- certyfikat użytkownika,
- klucz publiczny,
- klucz prywatny.

Aby przygotować podpisany dokument osoba posiadająca odpowiednią kartę musi użyć znajdującego się na niej klucza prywatnego. Dzięki elektronicznemu podpisowi zapewniona jest jednoznaczna identyfikacja osoby przeprowadzającej tą operację. Mechanizm podpisu elektronicznego wykorzystywany jest do zapewniania bezpieczeństwa przesyłanym dokumentom. Mechanizm ten zapewni również:

- **integralność** – informacja w przesyłanym dokumencie nie może zostać zmieniona lub zniszczona przez podmioty nieupoważnione. Każda zmiana zostanie wykryta a zmienione dokumenty nie przyjęte w centrali REJESTR.

- **niezaprzeczalność** – brak możliwości wyparcia się swego uczestnictwa w całości lub części wymiany danych przez użytkownika karty uczestniczącego w wymianie elektronicznych dokumentów. Dzięki tej właściwości podpisu elektronicznego, centrala REJESTR odbiera tylko 2te dokumenty, które zostały podpisane przez osoby jej znane,
- **rozliczalność** – właściwość zapewniająca, każdy użytkownik dysponujący kartą odpowiada za swoje działania wykonane w systemie

Ze względów bezpieczeństwa jej użycie (pobranie klucza prywatnego) – podczas wykonywania operacji podpisu elektronicznego – wymaga podania kodu PIN karty. Kod PIN jest buforowany na czas zalogowania użytkownika w systemie operacyjnym lub do momentu wyciągnięcia karty z czytnika. Dzięki przyjęciu takiego rozwiązania podczas wykonywania kolejnej operacji podpisu nie będzie potrzeby podawania kodu PIN. Wyciągnięcie karty lub wyłączenie stacji roboczej spowoduje wyczyszczenie buforu zawierającego kod PIN. Ponowna próba wykonania operacji podpisu wymaga podaniu kodu PIN. Oprócz mechanizmu podpisu elektronicznego przy wysyłaniu wiadomości do centrali REJESTR został wykorzystany mechanizm szyfrowania wiadomości. Zgodnie ze standardami szyfrowania asymetrycznego do tego celu wykorzystano certyfikat odbiorcy. Efektem zastosowania tego mechanizmu jest **poufność** informacji, tzn. informacja nie zostanie udostępniona jakimkolwiek nieuprawnionym do odbioru danej wiadomości podmiotom. Wiadomość wysłana z punktów rejestrowych zostaje odczytana tylko i wyłącznie przez centrum REJESTR.



Rys. 2.1. Opis mechanizmu wykonania podpisu elektronicznego przedstawia

2.1.1. Certyfikaty na karcie

Na każdej z kart elektronicznych przekazanych użytkownikom aplikacji REJESTR znajduje się certyfikat, para kluczy (publiczny oraz prywatny). Aby aplikacja działała poprawnie należy:

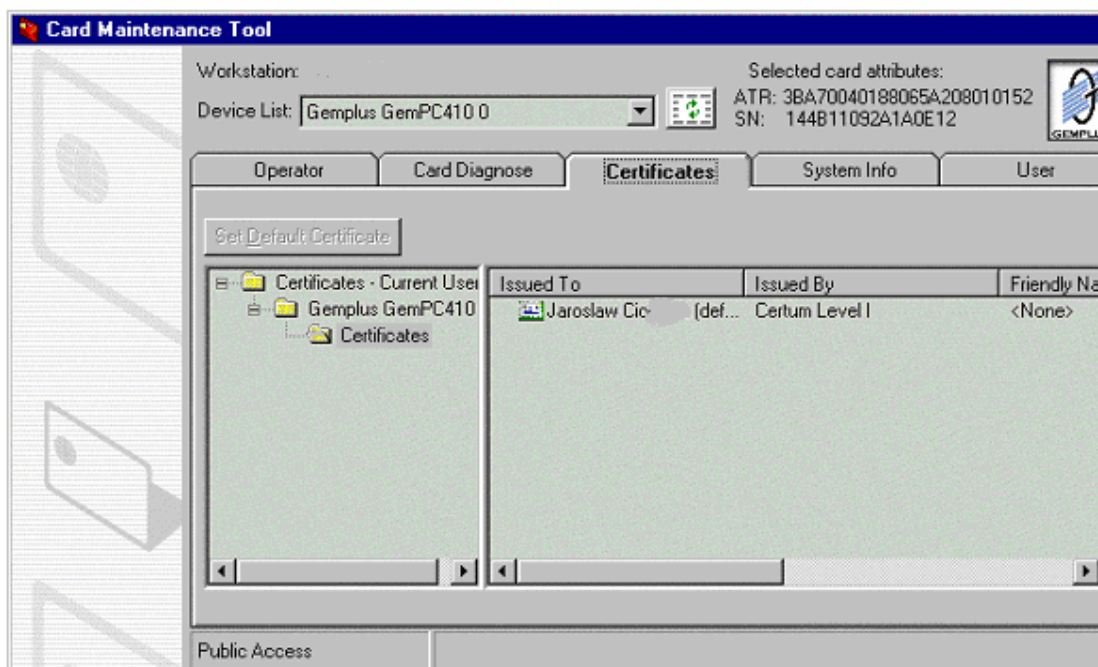
- wykonać diagnozę karty (na okoliczność obecności certyfikatów)
- Rejestrację certyfikatów

```

o Key Sets:
- Key set #1
  Name : a0b0f506-14a3-11d6-a649-00a0244db0e9
  Default : true
  Exchange Key Pair:
  o Size : 1024
  o Certificate:
  [
  X.509v3 certificate,
  Subject is OID.1.2.840.113549.1.9.1=kowalskij@poznan.pl, CN=Jan Kowalski,
  O=Private Data Encryption, C=PL
  Key: algorithm = [RSA], unparsed keybits =
  0000: 30 81 89 02 81 81 00 EA FB 7B 9E C3 CE 41 31 72 0.....A1r
  0010: BC 48 26 C5 74 25 56 C5 E1 72 BC F8 C9 5D 20 C3 .H&t%V.r...] .
  0020: 71 F1 12 51 28 3B A7 3C BC 34 FE BD 1D 90 FA BE q.Q(;.<4.....
  0030: E5 BD 83 C9 1E 4F 60 85 DA 09 9D 8C 15 2A A3 0C .....O'.....*.
  0040: 5D FE FD E1 17 D4 58 5A EB A8 1B 3C 1D 38 D6 DD ]....XZ...<8..
  0050: 3F 0B 5D 80 2F F5 30 82 C0 62 55 48 8E 84 B8 0F ?././0..bUH....
  0060: 21 4F 81 96 01 81 ED 19 17 22 82 7E CD 82 74 2F !O....."....t/
  0070: F3 9A E2 60 87 8A CB 0B 9C A4 93 D8 79 FA B7 A9 ...'.....y...
  0080: A3 2F D9 6D FA 18 E3 02 03 01 00 01 ./m.....
  Validity <Tue Jan 29 12:11:58 GMT+01:00 2002> until <Mon Apr 29 13:11:58
  GMT+02:00 2002>
  Issuer is CN=Certum Level I, O=Unimor Sp. z o.o., C=PL
  Issuer signature used [MD5withRSA]
  Serial number = 0206e0
  ]

```

Ryc. 2.2. Przykładowe informacje znajdujące się na karcie

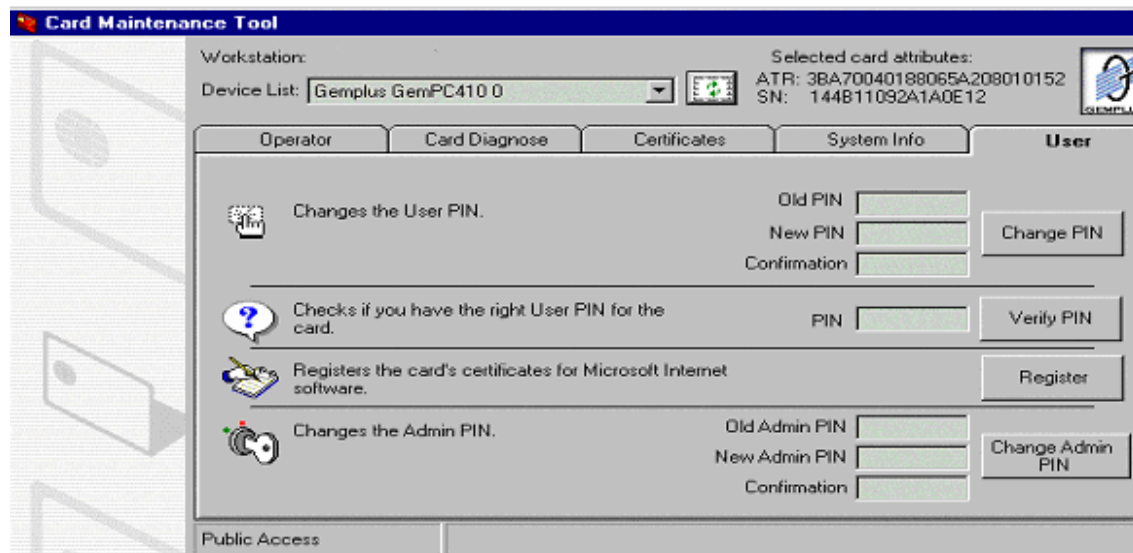


Rys. 1.3. Weryfikacja obecności certyfikatu

Uzyskanie pełnej funkcjonalności aplikacji REJESTR wymaga aby znajdujący się na karcie certyfikat został zarejestrowany w systemie operacyjnym komputera. Dodatkowo certyfikat ten musi być ważny .

W przypadku komputera z zainstalowanym systemem operacyjnym Windows 2000, znajdujący się na karcie certyfikat powinien zostać automatycznie zarejestrowany w systemie.

Jeżeli jednak po weryfikacji okaże się, że certyfikat nie znajduje się w systemie (patrz • Weryfikacja obecności certyfikatu w systemie) wykonaj powyższe czynności.



Rys. 2.4. Rejestracja certyfikatu w systemie

- Weryfikacja obecności certyfikatu w systemie

Po zarejestrowaniu w systemie znajdującego się na karcie certyfikatu należy zweryfikować jego obecności w systemie operacyjnym używając w tym celu Internet Explorera.

Wnioski

1. Eksploatacja systemu wskazuje na właściwy wybór narzędzi i technologii oraz dowodzi, że Internet w polskich warunkach, może pełnić rolę medium komunikacyjnego w zakresie przekazu dokumentów i aktualizacji. centralnych BD z użyciem Oracle 9i.
2. Zastosowanie podpisu elektronicznego przy wprowadzanych danych podnosi jakość wprowadzanych danych oraz rzetelność pracy operatorów.
3. System informatyczny o zasięgu ogólnopolskim stanowi ważne doświadczenie w budowie innych systemów współpracujących z systemem REJESTR np. kolejne segmenty działalności danego sektora gospodarki czy świadczeń społecznych oraz rozwoju usług konsumenckich przez Internet.

Biografia:

1. Monika Kubas, Marian Molski.: Karta elektroniczna bezpieczny nośnik informacji. Mikom, Warszawa 2002.
2. Magdalena Marucha: "Nowa ustawa o podpisie elektronicznym", "Monitor Prawniczy" 2/2002
3. Reihard Wobst: Kryptologia. Budowa i łamanie zabezpieczeń. Wydawnictwo RM Warszawa 2002.