# Comarch PKI - Comarch Centrum Certyfikacji

Technologie informatyczne znalazły zastosowanie w medycynie wiele lat temu poprawiając tym samym możliwości obsługi i diagnozowania pacjentów. Mając na uwadze bezpieczeństwo rozwiązań informatycznych oraz zarządzanie użytkownikami w placówkach służby zdrowia, należy skupić się na niezbędnym elemencie związanym z ochroną zasobów. Jest nim infrastruktura klucza publicznego (PKI), czyli wydawanie certyfikatów umożliwiających uwierzytelnianie i autoryzację użytkowników, zabezpieczających pocztę, serwery WWW oraz kanały komunikacyjne,

Infrastruktura Klucza Publicznego (Comarch PKI) - jest obszarem technologicznym, silnie powiązanym z polityką bezpieczeństwa, który umożliwia posługiwanie się podpisem elektronicznym. Jest to element niezwykle ważny zarówno dla lekarzy, którzy są twórcami elektronicznej dokumentacji chorego oraz dla samego pacjenta, ponieważ Comarch PKI stwarza nowe możliwości techniczne w kwestii podpisywania oświadczeń woli.

Infrastruktura Klucza Publicznego (PKI) włączona w system sieciowy jednostki medycznej i uwzględniona w jej polityce bezpieczeństwa stanowi podstawę do budowania relacji zaufania pomiędzy placówką leczniczą i pacjentem.

Comarch PKI zapewnia zgodność z wymogami formalnymi, takimi jak:

- Ustawa o podpisie elektronicznym
- Ustawa o ochronie informacji niejawnych
- Rozporządzenie dotyczące podstawowych wymagań bezpieczeństwa teleinformatycznego

W obszarze zastosowania Infrastruktury Klucza Publicznego Comarch proponuje rozwiązania najwyższej jakości:

**Comarch CertificateAuthority (CA)** jest autorskim oprogramowaniem Comarch, umożliwiającym pełną implementację systemu opartego na Infrastrukturze Klucza Publicznego (PKI). Comarch CA jest rozwiązaniem do obsługi certyfikatu w całym cyklu jego życia – od złożenia wniosku po wygaśnięcie lub unieważnienie. Rozwiązanie ma budowę modułową, dzięki czemu może pracować w środowisku rozproszonym.

Główne moduły rozwiązania:

- Moduł RA (Registration Authority) służy użytkownikowi do składania wniosków
- Moduł RA Operator (Registration Authority Operator), służy do akceptacji wniosków
- Moduł CA (Certificate Authority), służący do wystawiania zaakceptowanych wniosków w RA Operator


Rysunek 1. Proces wydawania certyfikatu

COMARCH e-Zdrowie

**Comarch SOPEL** (System Obsługi Podpisu Elektronicznego) - jest kompletną implementacją Bezpiecznego Urządzenia służącego do weryfikacji kwalifikowanego podpisu elektronicznego oraz bezpiecznego oprogramowania do składania podpisu elektronicznego w myśl Ustawy o Podpisie Elektronicznym.

Zastosowanie systemu umożliwia korzystanie ze wszystkich benefiçjów związanych z możliwością kontaktu z pacjentami/partnerami w formie elektronicznej, równocześnie zapewniając cechy bezpieczeństwa, takie jak:

- **niezaprzeczalność** (podmiot nie może wyprzeć się faktu nadania pewnej wiadomości),
- **integralność** (każda zmiana wiadomości przez osoby niepowołane jest w łatwy sposób wykrywalna).

Podpis elektroniczny znajduje szczególne zastosowanie w przypadku kontaktów drogą elektroniczną z dużą liczbą anonimowych lub okazjonalnych petentów czy też konieczności przechowywania dokumentów w celach dowodowych.

**Comarch SmartCard** - mikroprocesorowa karta kryptograficzna, służąca do bezpiecznego przechowywania informacji wrażliwych (klucze prywatne, hasła, klucze kryptograficzne).

**Comarch SmartCard BIO** – jest to rozwinięcie karty COMARCH SmartCard umożliwiające przechowywanie templejtów biometrycznych na karcie wykorzystywanych w procesie uwierzytelniania Match-On-Card

**Comarch Token** - rozwiązanie bazujące w części sprzętowej na tokenach USB łączących cechy karty mikroprocesorowej kryptograficznej i czytnika kart w jednym urządzeniu, a w części programowej na systemie informatycznym Comarch.

**Comarch SmartCard Workshop** - system służący do zarządzania cyklem życia kart smart card oraz tokenów kryptograficznych.

## Korzyści biznesowe

Wdrożenie Centrum Certyfikacji wraz z Infrastrukturą Klucza Publicznego zapewnia:

- możliwość stworzenia rozbudowanej infrastruktury klucza publicznego (wiele rozproszonych jednostek rejestracyjnych)
- obsługę standardu X.509v3 (bezpieczne kanały komunikacji (2SSL, VPN), szyfrowana/podpisywana poczta email (S/MIME), silne uwierzytelnianie/autoryzacja)
- współpracę z urządzeniami kryptograficznymi (karty kryptograficzne – certyfikaty użytkowników, urządzenia HSM – klucze Urzędów Certyfikacji)
- znakowanie czasem – wykorzystanie sprzętowych modułów czasu rzeczywistego
- duże możliwości adaptacyjne do indywidualnych wymagań
- pełną zgodność oraz współpracę z szeroką gamą oprogramowania kryptograficznego
- szerokie możliwości publikowania certyfikatów oraz CRL'i – poprzez mail, ftp, WWW, LDAP

## Produkty powiązane

- Comarch Bezpieczeństwo Danych
- Comarch Zarządzanie Tożsamością i Dostępem

**Comarch SA**
Al. Jana Pawła II 39 a
31-864 Kraków
Polska
**tel.:** +48 12 64 61 000
**fax:** +48 12 64 61 100
**e-mail:** info@comarch.pl

**www.comarch.pl/e-zdrowie**

www.comarch.com www.comarch.pl www.comarch.de www.comarch.ru www.comarch.fr



PL-2012.10