CryptoTech
eSECURITY SOLUTIONS

CryptoCard multiSIGN

CryptoCard multiSIGN jest specjalizowaną kryptograficzną kartą mikroprocesorową przeznaczoną do realizacji kwalifikowanego i niekwalifikowanego podpisu elektronicznego oraz funkcji identyfikacji i silnego uwierzytelniania użytkowników. Karta ta, uzupełniona o oprogramowanie podpisujące i uwierzytelniające, stanowi doskonałe narzędzie wspierające szeroką gamę rozwiązań pracujących w ramach Infrastruktury Klucza Publicznego (PKI). Wsparcie dla dominujących na rynku standardów pozwala na użycie karty w typowych zastosowaniach wewnątrz organizacji (takich jak dostęp do komputerów, sieci i innych zasobów) oraz w pełni realizować ideę podpisu cyfrowego.

CryptoCard multiSIGN może zawierać aplikację niekwalifikowanego podpisu elektronicznego lub certyfikowaną aplikację podpisu kwalifikowanego. W tym drugim przypadku karta stanowi komponent techniczny zgodny z wymaganiami polskiego prawa stawianymi dla bezpiecznych urządzeń do składania kwalifikowanego podpisu elektronicznego. Oferujemy również unikalną wersję karty realizującą jednocześnie obie wersje podpisu elektronicznego łącząc zalety obu zastosowań.

Główne cechy rozwiązania:

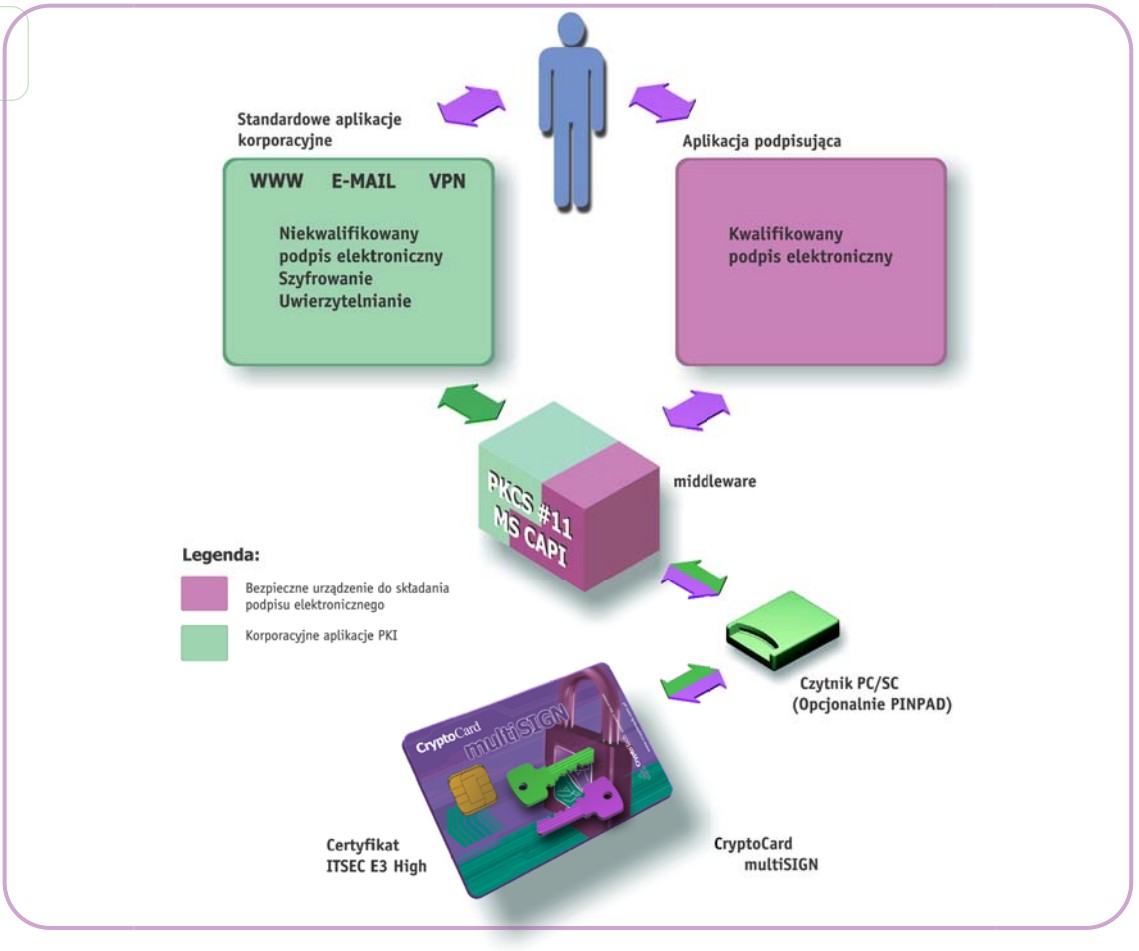
- 32 kB pamięci
- podpisywanie i szyfrowanie RSA 1024 bity
- DES, 3DES, MAC i SHA-1 realizowany na karcie
- generowanie kluczy na karcie
- wsparcie dla standardów przemysłowych (PKCS#11, #15, MS CAPI, PC/SC)
- certyfikowane bezpieczeństwo ITSEC E3 High dla aplikacji i ITSEC E4 High dla układu elektronicznego
- uznany producent systemu operacyjnego dla najbardziej wymagających aplikacji klasy digitalID - Setec Oy
- pełne wsparcie dla środowiska Windows 2000, XP i 2003
- Linux RedHat 9+, Debian Woody+, Suse i podobne
- ograniczone wsparcie dla Windows 98 i NT4.0
- wsparcie dla pracy terminalowej Cytrix Metaframe i MS Terminal Services
- możliwe łączenie z aplikacjami dedykowanymi

Bezpieczny podpis elektroniczny

CryptoCard multiSIGN może obejmować aplikację bezpiecznego podpisu elektronicznego, która łącznie z platformą sprzętową i systemem operacyjnym karty jest certyfikowana do poziomu ITSEC E3 high i stanowi komponent techniczny będący częścią bezpiecznego urządzenia do składania podpisu elektronicznego. Tym samym karta CryptoCard multiSIGN wraz z dostarczanym standardowym oprogramowaniem kryptograficznym "middleware" może współdziałać z aplikacją podpisującą tworząc łącznie bezpieczne urządzenie do składania podpisu.

Zastosowania korporacyjne

Ta sama karta CrytoCard multiSIGN może być wykorzystywana równocześnie do wielu różnych celów niekoniecznie związanych z bezpiecznym podpisem. Odpowiednio duża ilość pamięci pozwala przechowywać wiele informacji, kluczy, certyfikatów pozwalających realizować różne funkcje np. zestawiać bezpieczne połączenie z serwerem WWW (SSL), podpisywać wysyłane wiadomości pocztowe (S/MIME) i służyć jako identyfikator przy logowaniu do domeny Windows2000/2003.



Bezpieczeństwo

Mechanizmy zarządzania kluczami, podpisu i szyfrowania są zlokalizowane na karcie. Karta zarówno generuje klucze, przechowuje je w pamięci, jak również przy ich użyciu podpisuje dane na zlecenie zewnętrznych aplikacji po weryfikacji kodu PIN użytkownika.
Certyfikowana aplikacja bezpiecznego podpisu elektronicznego chroniona jest oddzielnym kodem PIN użytkownika. Jednorazowe podanie kodu PIN pozwala na złożenie wyłącznie pojedynczego podpisu kwalifikowanego.
W przypadku umieszczenia na karcie obu aplikacji są one całkowicie izolowane i chronione odrębnymi kodami PIN (max. 4 kody PIN). Analogicznie jak w przypadku kart SIM kody PIN są związane z kodami PUK. Służą one do odblokowania dostępu do danych w przypadku kilkukrotnego podania błędnego kodu PIN.
Wysoki poziom bezpieczeństwa karty potwierdzony jest odpowiednimi certyfikatami. System operacyjny certyfikowany jest na poziomie pewności ITSEC E3 high zgodnie z profilem bezpieczeństwa wymaganym przez polskie i europejskie standardy dotyczące bezpiecznego urządzenia do składania podpisu. Układ elektroniczny karty certyfikowany jest do poziomu ITSEC E4 high.

Standardy

Oprogramowanie middleware dedykowane dla obsługi karty CryptoCard multiSIGN realizuje standardy PKCS#11 v2.01 i v2.11 a wewnętrzne struktury aplikacji zgodne są z PKCS #15. Oprogramowanie to zawiera również certyfikowany przez firmę Microsoft moduł CSP do pracy poprzez interfejs CryptoAPI 2.0. Ponieważ interfejsy te wykorzystują standard PC/SC, możliwe jest używanie szerokiej gamy czytników w środowisku Windows. Oprogramowanie wspiera również wybrane typy bezpiecznych czytników kart wyposażonych w PINPAD do osiągnięcia wysokiej poufności wprowadzanego kodu PIN. Karta w pełni spełnia wymagania stawiane przez polską ustawę o podpisie elektronicznym dla komponentu technicznego bezpiecznego urządzenia do składania podpisu elektronicznego oraz wymagania prawodawstwa europejskiego.

Współpraca

Karta CryptoCard mulitSIGN współpracuje z oprogramowaniem liderów rynku PKI: Baltimore, RSA Security, Entrust, CheckPoint, Netscape, Microsoft, Novell, PGP i wielu innych. CryptoTech w ramach oferowanych usług wykonuje, na bazie dostępnego oprogramowania komercyjnego oraz własnych rozwiązań, kompletne systemy PKI, zarówno do zastosować wewnątrz jak i na zewnątrz organizacji.
Jako uzupełnienie CryptoCard multiSIGN w ramach bezpiecznego urządzenia do składania podpisu elektronicznego oferowane są aplikacje podpisujące i narzędzia integracyjne dla produktów firmy trzecich.

CryptoTech Sp. z o.o., ul. Wadowicka 6E, 30-415 Kraków, PL
tel.: (12) 260 92 92, fax: (12) 260 92 26
e-mail: info@cryptotech.com.pl, www.cryptotech.com.pl