POLITECHNIKA GDAŃSKA

WYDZIAŁ ELEKTRONIKI, TELEKOMUNIKACJI I INFORMATYKI

System przechowywania danych z oprogramowaniem kryptograficznym
CPV: 30233000-1 i 48211000-0

Poz.1 – Licencja edukacyjna na oprogramowanie infrastruktury klucza publicznego (PKI) opiewające łącznie na zbiór funkcjonalności zdefiniowanych w poniższej tabeli:

Licencja na oprogramowanie Certificate Authority (CA) **Wymagania**:
Graficzny interfejs umożliwiający edycję ustawień i zarządzanie certyfikatami
Wsparcie interfejsu PKCS#11
Połączenie z HSM (Hardware Security Module)
Obsługa połączeń pomiędzy komponentami na bazie TCP/IP zabezpieczona protokołem TLS w wersji 1.2 z silnym uwierzytelnieniem na poziomie sieci lokalnej i rozległej WAN
Obsługa relacyjnych baz danych typu Oracle czy Microsoft SQL
Musi posiadać możliwości konfiguracyjne dotyczące dodatkowego zabezpieczenia podczas procedur administracyjnych tj. Aby stworzyć/usunąć lub zarządzać nowym drzewem CA, zautoryzować się muszą jednocześnie co najmniej 2 osoby posiadające odpowiednie uprawnienia
System zarządzania uprawnieniami danych użytkowników do konkretnych elementów centrum autoryzacji oparty na rolach
Musi posiadać system do generowania zestawień z relacyjnej bazy danych dotyczących certyfikatów
Wsparcie dla LDAP
Skalowalność do 40 tysięcy wydawanych certyfikatów na godzinę
Wsparcie do archiwizowania/odzyskiwania kluczy kryptograficznych i zapisu z wykorzystaniem HSM
W bazie SQL muszą być przechowywane dane takie jak:
Wszystkie wyemitowane certyfikaty użytkowników końcowych wraz z ich kluczami publicznymi
Wszystkie dane użytkowników administrujących systemem
Dane o kartach inteligentnych, na które zostały wydane certyfikaty
Informacje o odwołanych certyfikatach
Oprogramowanie musi posiadać dodatkowe moduły odpowiedzialne za:
Przyjmowanie żądań nowych certyfikatów od użytkowników
Obsługa wniosków dla nowych certyfikatów
Generowanie i rozsyłanie list CRL do serwerów LDAP
Publikowanie wygenerowanych certyfikatów
Poszukiwanie i informowanie o wygasających certyfikatach
Obsługa drukarek PIN i PUK do bezpiecznego drukowania kopert z danymi
Zarządzanie kartami, na które zostały wygenerowane certyfikaty
Wymagania dla PKI
PKI powinno oferować pełną rozliczalność i audytowalność czynności podejmowanych przez administratorów
System może oferować wymaganie poświadczeń dwóch administratorów w przypadku szczególnie krytycznych operacji
System powinien oferować funkcjonalność samoobsługi użytkowników pod względem np. zmiany kodu PIN, odblokowania karty/tokenu USB kodem PUK, zablokowania karty np. na czas urlopu
PKI powinno zapewniać możliwość powiadamiania o zbliżającym się terminie wygaśnięcia z konfigurowalnym okresem wyprzedzenia
PKI powinno zapewniać możliwość obsługi certyfikatów zaufanych wystawionych przez inne CA, w szczególności zapewnienia mechanizmów powiadamiania o terminie ich wygasania
W zamawianym rozwiązaniu przewiduje się instalację bez zapewnienia mechanizmów wysokiej dostępności
Licencja na oprogramowanie do potwierdzania ważności certyfikatów online **Wymagania**:
Oprogramowanie musi być kompatybilne (dodatek, moduł lub wtyczka) z oprogramowaniem Certificate Authority

Musi umożliwiać sprawdzanie ważności certyfikatu online
Musi być kompatybilne z: RFC 2560, RFC 5280 i PKCS#11
Musi być kompatybilne z różnymi modelami HSM (Hardware Security Module)
Musi umożliwiać potwierdzanie ważności certyfikatów z głównym certyfikatem drzewa (Root CA) z którego został wydany
Musi zapewnić wsparcie dla standardu X.509 oraz list CRL, które będą mogły być dostarczane poprzez LDAP
Musi wspierać wszystkie popularne przeglądarki internetowe (minimum): - Internet Explorer min. w wersji 10 - Mozilla Firefox min. wersja Quantum - Safari od systemu Mac OS X 10.7 - Opera od wersji 8
Musi wspierać popularne aplikacje pocztowe minimum: - Microsoft Outlook min. w wersji 2013 - Mozilla Thunderbird
Musi wspierać certyfikaty kwalifikowane wydawane przez certyfikowane centra certyfikacji, oraz niekwalifikowane wystawiane przez wewnętrzne centra certyfikacji
Oprogramowanie musi umożliwiać pracę (minimum):
W trybie fail-over z użyciem zewnętrznego urządzenia Load Balancer
Na systemach rodziny Windows serwer minimum 2012R2 lub Red Hat Enterprise Linux
Licencja na oprogramowanie do kryptograficznej personalizacji kart **Wymagania:**
Oprogramowanie musi być samodzielnym modułem (z możliwością podłączenia go do większego systemu zarządzania), za pomocą którego będzie możliwość generowania prywatnych i publicznych kluczy kryptograficznych wewnątrz karty inteligentnej (smartcard)
Proces generowanie kluczy kryptograficznych musi być oparty o algorytm ANSI X9.17 oraz standard RSA
Musi pozwolić na wstępną pre-personalizację
Oprogramowanie musi posiadać:
Możliwość ustawienia domyślnych profili kart. W skład profilu muszą wchodzić dane takie jak: - struktura danych na karcie - role dostępu - zawartość poszczególnych obszarów danych - długość kluczy kryptograficznych - ilość kluczy kryptograficznych - identyfikator przypadku użycia certyfikatu skorelowanego z certyfikatem Profil/szablon karty musi mieć możliwość zapisu do pliku w celu ponownego wykorzystania.
Oprogramowanie musi obsługiwać:
Stosowanie niezależnych procedur wydawania certyfikatów dla kart inteligentnych podłączanych z użyciem standardu PS/SC, CT-API, Native
Różne rodzaje czytników kart inteligentnych podłączanych między innymi za pomocą USB
Dodatkowy sprzęt w postaci wyspecjalizowanych drukarek do nanoszenia spersonalizowanych grafik bezpośrednio na kartę
Min. system Windows Server 2008 oraz obowiązkowo systemy operacyjne serwerów które będą dostarczane w niniejszym postępowaniu
Licencja na oprogramowanie do implementacji protokołów autoenrolmentu **Wymagania**:
Musi umożliwiać implementację wybranych protokołów autoenrolmentu
Automatyczna rejestracja nowych urządzeń sieciowych w celu wydania im certyfikatu elektronicznego
Wsparcie oprogramowania serwera WWW takie jak np. Apache czy Tomcat
Musi umożliwiać zarządzanie wszystkimi kluczami kryptograficznymi z poziomu jednej aplikacji
Musi umożliwiać monitoring wykorzystywanych zasobów
Musi wspierać szyfrowanie sprzętowe oraz programowe

Obsługa protokołów:
CMC (Certificate Management over CMS) - wsparcie standardu PKCS#10 - zapytania typu aplikacja/PKCS#7, S/MIME - PKCS#7 - certyfikaty w standardzie X.509 (PKIX-Cert)
CMP (Certificate Management Protocol v2)
SCEP (Simple Certificate Enrollment Protocol)
EST (Enrollment over Secure Transport)
WinEP (Windows Enrollment Proxy) - proces wydawania certyfikatów dla których dane znajdują się w usłudze Active Directory (Microsoft) - szablony certyfikatów Microsoft - obustronny SSL w momencie łączenia się oprogramowania do autoenrolmentu z centrum certyfikacji
Gwarancja minimum:12 miesięcy

poz.2 – 25 szt. Dwusystemowy czytnik kart chipowych – stykowy i bezstykowy – na złącze USB

Interfejs USB 2.0
Zgodność z protokołem CCID
Funkcjonalność bezstykowa: - wparcie standardów ISO/IEC 14443 część 4 typu A i B oraz MIFARE Classic - prędkość odczytu/zapisu do 848 kb/s - wbudowana antena o zasięgu do 50 mm - wbudowna funkcjonalność antykolizyjna w przypadku zbliżenia większej liczby kart - wsparcie dla rozszerzonych datagramów APDU (do 64 kB)
Funkcjonalność stykowa: - wsparcie standardu ISO/IEC 7816 klasy A, B i C (5 V, 3 V i 1,8 V) - wsparcie standardu CAC (Common Access Card) - wsparcie standardu PIV (Personal Identity Verification Card) - wsparcie standardu kart procesorowych pracujących z protokołami T=0 i T=1 - wsparcie dla kart pamięci - złącze SAM zgodne ze standardem ISO/IEC 7816
Interfejs programowy – PC/SC, CT-API nabudowany na PC/SC
Brzęczyk i dwie diody LED kontrolowane programowo
Wsparcie dla systemu Android od wersji 3.1
Zgodność ze standardami: ISO 14443, ISO 7816, FIPS 201, PC/SC, CCID
Gwarancja minimum:12 miesięcy

Poz.3 150 szt. Karta kryptograficzna (chipowa) biała, bez nadruku, z interfejsami stykowym i bezstykowym

Charakterystyka fizyczna karty zgodna z ISO/IEC 7816-1, zastosowany wymiar karty to ID-1.
Karta jest urządzeniem typu „dual interface” (dostęp do jednego procesora poprzez interfejs stykowy i bezstykowy).
Interfejs stykowy jest zgodny z ISO/IEC 7816 klasy A, B i C (5V, 3V i 1.8V). Polecenia i odpowiedzi przesyłane podczas komunikacji infrastrukturą informatyczną powinny mieć strukturę zgodną z wariantem rozszerzonym APDU (64 kB) określonym w normie ISO/IEC 7816-4.
Interfejs bezstykowy spełnia wymagania norm ISO/IEC 14443 typ A. Protokół komunikacji jest zgodny z normami ISO/IEC 14443-1, ISO/IEC 14443-2, ISO/IEC 14443-3 oraz ISO/IEC 14443-4 (protokół T=CL).
Zamawiający musi mieć możliwość umieszczenia swojej aplikacji w karcie. Aplikacja Zamawiającego jest dostępna zarówno poprzez interfejs stykowy jak i bezstykowy karty. Pojemność dostępnej pamięci EEPROM przed zainstalowaniem dodatkowych aplikacji, musi wynosić co najmniej 16 kilobajtów

Java Card Virtual Machine, RTE oraz API karty są zgodne ze specyfikacją Java Card Classic 3.0.4 lub nowszą. Card Management i API są zgodne z Global Platform 2.1.1. lub nowszą.
Karta umożliwia generowanie kluczy kryptograficznych o długości do 4096 bitów przeznaczonych do użycia przez algorytm RSA, podpisywanie za pomocą algorytmu RSA, obsługa funkcji skrótu SHA-1, SHA-256, SHA-512 obsługą algorytmów DES, 3DES, AES w trybach ECB i CBC. Algorytm AES powinien obsługiwać klucz o długości 256 bitów.
Karty muszą posiadać generator liczb losowych wykorzystywany przez kartę do generowania ziarna dla generatora deterministycznego zgodnego z zaleceniem NIST 800-90
Karta powinna zawierać emulację MIFARE Plus 4k, MIFARE DESFire EV1 8k
Gwarancja minimum:12 miesięcy

Poz.4 – 25 szt. Klucz uwierzytelniający USB

Interfejs: USB-A, opcjonalnie USB-A i NFC
Obsługiwane protokoły: FIDO2, FIDO U2F, smart card (PIV), Yubico OTP, OpenPGP, OATH-TOTP, OATH-HOTP, Challenge-Response
Sprzętowy moduł do ochrony materiału kryptograficznego i wykonywania operacji kryptograficznych
Wsparcie dla algorytmów kryptograficznych: RSA (klucze długości 2048, 3072 i 4096 bitów), ECC p256, ECC p384
Kompatybilność z kartami PIV, dostępność oprogramowania middleware dla systemów Windows
Możliwość logowania do osobistego konta Microsoft zamiast hasła od aktualizacji 1809 systemu Windows 10
Możliwość współpracy z platformami mobilnymi Android oraz iOS
Możliwość współpracy z rozwiązaniami LastPass, Dashlane, Facebook, Dropbox, Twitter
Gwarancja minimum:12 miesięcy

Poz.5 – 10 szt. Przenośny moduł HSM USB

Wsparcie interfejsów kryptograficznych: - Microsoft CNG (KSP) - PKCS#11 (Windows, Linux, macOS)
Wsparcie funkcji skrótu: SHA-1, SHA-256, SHA-384, SHA-512
Obsługa algorytmu RSA: klucze 2048, 3072 i 4096 bitów, podpis zgodny z PKCS#1v1.5 i PSS, odszyfrowywanie zgodne z PKCS#1v1.5 i OAEP
Pojemność pamięci: maks. 128 kB, możliwość składowania min. 127 kluczy RSA 2048, min. 68 kluczy RSA 4096 lub min. 255 kluczy ECC o dowolnej obsługiwanej długości
Generator liczb losowych True Random Number Generator – TRNG wykorzystywany do zainicjowania zgodnie z normą NIST SP 800-90 AES 256 CTR_DRBG
Możliwość importu i eksportu kluczy zaszyfrowanych (Key wrap) algorytmami AES-128, AES-192 i AES-256 w trybie zgodnym z wytycznymi NIST AES-CCM Wrap
Gwarancja minimum:12 miesięcy