Karta CryptoCard Graphite

CryptoCard Graphite jest nowym modelem kryptograficznej karty mikroprocesorowej w ofercie CryptoTech. Karta ta jest bezpośrednim następcą karty CryptoCard Carbon, kontynuującej sukcesy wcześniejszego modelu CryptoCard multiSIGN, który zyskał na rynku polskim dużą popularność i ustanowił standard de facto funkcjonalności dla elektronicznej karty PKI.

Karta może służyć równocześnie do składania podpisu elektronicznego, szyfrowania danych i korespondencji, identyfikacji oraz uwierzytelniania użytkowników czy kontroli dostępu do zasobów i pomieszczeń. CC Graphite jest urządzeniem uniwersalnym i może być wykorzystywany zarówno przez osoby indywidualne jak i duże firmy.

Interfejs zbliżeniowy

Wymagania w stosunku do kart coraz częściej łączą dwa oddzielne obszary zastosowań kart elektronicznych. Pierwszy związany jest z procesorem stykowym i realizowaną przez niego funkcjonalnością podpisu, szyfrowania i uwierzytelniania, a drugi to typowa dla firm potrzeba rejestracji czasu pracy czy kontroli dostępu do pomieszczeń, realizowana zwykle przez karty zbliżeniowe. Karta CC Graphite może być wyposażona w część stykową i zbliżeniową i służyć obu tym celom równocześnie, co upraszcza życie użytkownikowi karty, ale także obniża koszty zakupu i zarządzania kartami.

Na rynku obecnych jest bardzo wiele typów kart zbliżeniowych i ich odmian. Dzięki pełnej kontroli nad cyklem produkcji karta CryptoCard Graphite może zostać dostarczona praktycznie z każdym typem części zbliżeniowej (konfiguracja hybrydowa). Najczęściej spotykanymi odmianami są MIFARE®, Unique, Indala i iClass.

Identyfikator

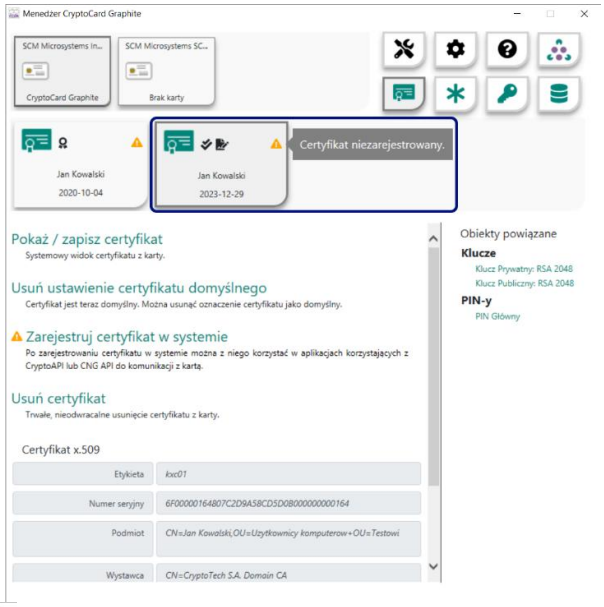
W zastosowaniach firmowych karta plastikowa często używana jest jako identyfikator pracownika. CC Graphite również może służyć jako identyfikator. Wygląd karty może być zdefiniowany przez klienta. W najprostszej wersji może być to karta biała, gotowa do zadruku danymi użytkownika podczas jej wydawania, w procesie indywidualnej personalizacji z wykorzystaniem specjalizowanych drukarek do kart plastikowych. Dla zastosowań o większej skali dostępny jest wysokiej jakości zadruk offsetowy i wszystkie dostępne opcje stosowane w produkcji kart plastikowych, łącznie z dodatkowymi elementami zabezpieczającymi jak hologramy czy gilosze.

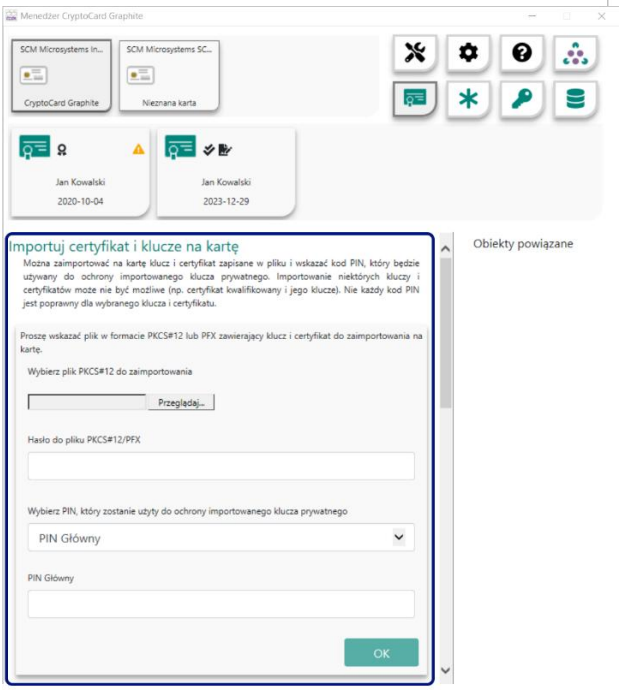
Podpis elektroniczny

Podobnie jak poprzednie rozwiązania z oferty CryptoTech, także kartę CryptoCard Graphite można używać do składania podpisu elektronicznego we wszystkich jego odmianach przewidzianych polskim i europejskim prawem (w tym zgodnie z rozporządzeniem eIDAS). W przypadku podpisu bezpiecznego, karta stanowi tzw. urządzenie QSCD (Qualified Signature Creation Device) wg specyfikacji przewidzianej w eIDAS i spełniającej wymagania polskiego prawa dla bezpiecznego podpisu weryfikowanego kwalifikowanym certyfikatem klucza publicznego. Zgodnie ze standardami i przepisami technicznymi, obszar karty odpowiedzialny za obsługą i ochronę danych służących do generowania takiego podpisu jest wydzielony i podlega szczególnej kontroli jego używania i zarządzania.

Oprogramowanie

Karta ściśle współpracuje z dedykowaną dla niej nową edycją oprogramowania CryptoCard Suite, które pozwala na zarządzanie zawartością karty oraz pośredniczy w komunikacji pomiędzy programami korzystającymi z karty (logowanie do systemów operacyjnych, programy pocztowe, przeglądarki internetowe czy aplikacje podpisujące) a kartą włożoną do czytnika.



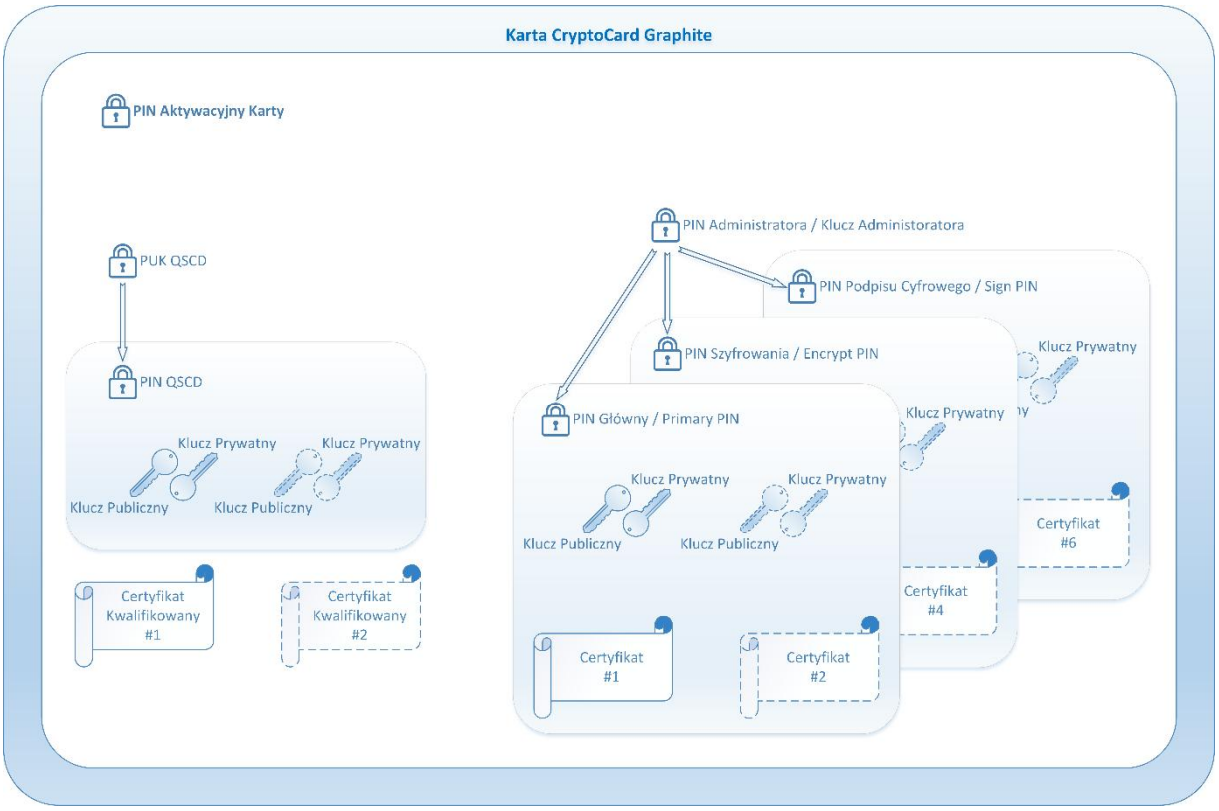


CryptoCard Suite jest oprogramowaniem pośredniczącym (ang. middleware), w pełni zgodnym ze standardami branżowymi PKCS#11 v2.01 i nowszymi oraz CryptoAPI i CNG API. Nowa karta wyposażona jest w interfejs programowy dla nowych systemów operacyjnych Windows i współpracuje za pośrednictwem modułu zgodnego z Microsoft Smart Card miniDriver v7 API, używane go przez CSP i KSP.

Sprzęt

Karta wykorzystuje nowoczesny procesor, wyposażony w 64kB pamięci EEPROM oraz koprocesor kryptograficzny wykonujący operacje z kluczem RSA o długości do 2048 bit, a także, zyskujące na popularności, podpisy oparte na tzw. krzywych eliptycznych ECC (Elliptic Curve Cryptography) o długości klucza 256 bit. Komunikacja pomiędzy oprogramowaniem wykorzystującym kartę a procesorem karty może być szyfrowana, co jest dodatkowym zabezpieczeniem przed zaawansowanymi atakami.

Platforma karty bazuje na specyfikacji JavaCard v2.2.2 oraz GlobalPlatform v2.1.1, a aplikacja PKI zainstalowana na karcie jest certyfikowana wraz z całą platformą wg CommonCriteria EAL4+ i znajduje się na oficjalnej liście urządzeń SSCD i QSCD zgodnych z eIDAS.



Specyfikacja techniczna

pamięć	do 64 kB
podpisywanie i szyfrowanie RSA	klucze do 2048 bitów
podpisywanie ECC GF(p)	klucze 256 bitów (wkrótce), 384, 512, 521 bitów na życzenie
wspierane algorytmy	RSA, ECC, DES/3DES, AES, SHA1 (ograniczone) SHA-256, SHA-384
wsparcie dla Secure Messaging	Tak
generowanie kluczy	na karcie (RSA,ECC)
protokoły	T=0
wsparcie dla standardów przemysłowych	PKCS#11, MS CAPI/CSP/CNG, miniDriver, PC/SC
certyfikowane bezpieczeństwo aplikacji podpisu kwalifikowanego (QSCD)	CC EAL 4+
certyfikowana platforma sprzętowa	CC EAL 5+
wsparcie dla środowisk	Windows 8, 8.1, 10 (obsługa systemów operacyjnych 32/64bit), Linux (via PKCS#11), MacOSX (PKCS#11) oraz ograniczone wsparcie dla Windows 7.
inne	wsparcie dla usług Terminal Services