Oprogramowanie do podpisu elektronicznego i zarządzania kartami kryptograficznymi, dostarczane przez centra certyfikacji
– ustawienia dla Systemu e-Deklaracje

I. Informacja o centrach certyfikacji

Rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne jest opublikowany przez Narodowe Centrum Certyfikacji (NCCert) na stronie www.nccert.pl

Oferowane w zestawach do podpisu oprogramowanie :

1. **K**walifikowane **C**entrum **C**ertyfikacji **K**luczy **CenCert** (www.cencert.pl)– „**PEM-HEART Signature**" *wersja 3.9.13.11* – składanie podpisu i zarządzanie kartami (*https://www.cencert.pl/Oprogramowanie%20PEMHEART/*)
2. **C**entrum **O**bsługi **P**odpisu **E**lektronicznego **K**rajowej **I**zby **R**ozliczeniowej S.A. (www.elektronicznypodpis.pl)– „**SZAFIR**" *wersja 2.0.0 build 595* – składanie podpisu (*nowa karta Graphite*), „**CryptoCard Suite**" *wersja 2.1.170* – zarządzanie pozostałymi kartami (*http://www.elektronicznypodpis.pl/informacje/aplikacje/, http://www.elektronicznypodpis.pl/informacje/pakiet-szafir-dla-kart-graphite/)*
3. **C**entrum **U**sług **Z**aufania **Sigillum** (www.sigillum.pl)- „**PWPW Sign**"*5.2.6* – składanie podpisu, „**CryptoCard Suite**" *wersja 2.1.170* (*karta Carbon*) lub „**IDProtect Client"** *wersja 7.13.03 (nowa karta **Dark**)* - zarządzanie kartami (*https://sigillum.pl/Pliki*)
4. **P**owszechne **C**entrum **C**ertyfikacji **CERTUM** (www.certum.pl) – „**proCertum SmartSign + SimplySign Desktop**" *wersja 8.1.21.0 build 2966* – składanie podpisu, „**proCertum CardManager**" *wersja 3.2.0.156* – zarządzanie kartami (*https://certum.pl/certum/cert.oferta_oprogramowanie_biblioteki.xml*)
5. **C**entrum **C**ertyfikacji **EuroCert** (www.eurocert.pl) – „**EuroCert SecureDoc**" *wersja 2.0.3.2* – składanie podpisu, „**Charismathics Smart Security Interface Standard**" – zarządzanie kartami wersja 5.0.3, 5.2.2 i 5.4.3
   https://eurocert.pl/index.php/oprogramowanie
   https://eurocert.pl/pub/Oprogramowanie/eurocert_oprogramowanie.exe
   https://eurocert.pl/pub/Oprogramowanie/SecureDoc/SecureDoc_2_setup.exe

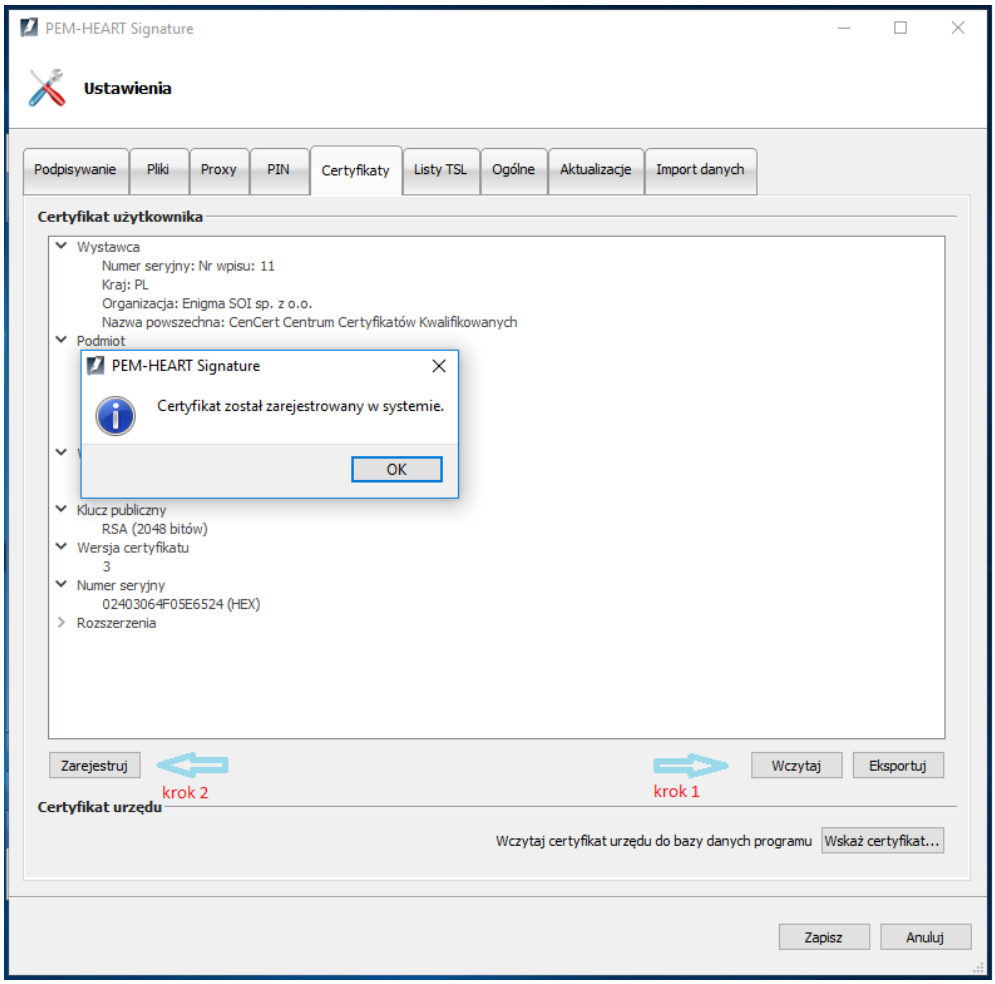
Dokument uwzględnia:* - stan na dzień 25.06.2019 r.

** - Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2016 poz.1579)

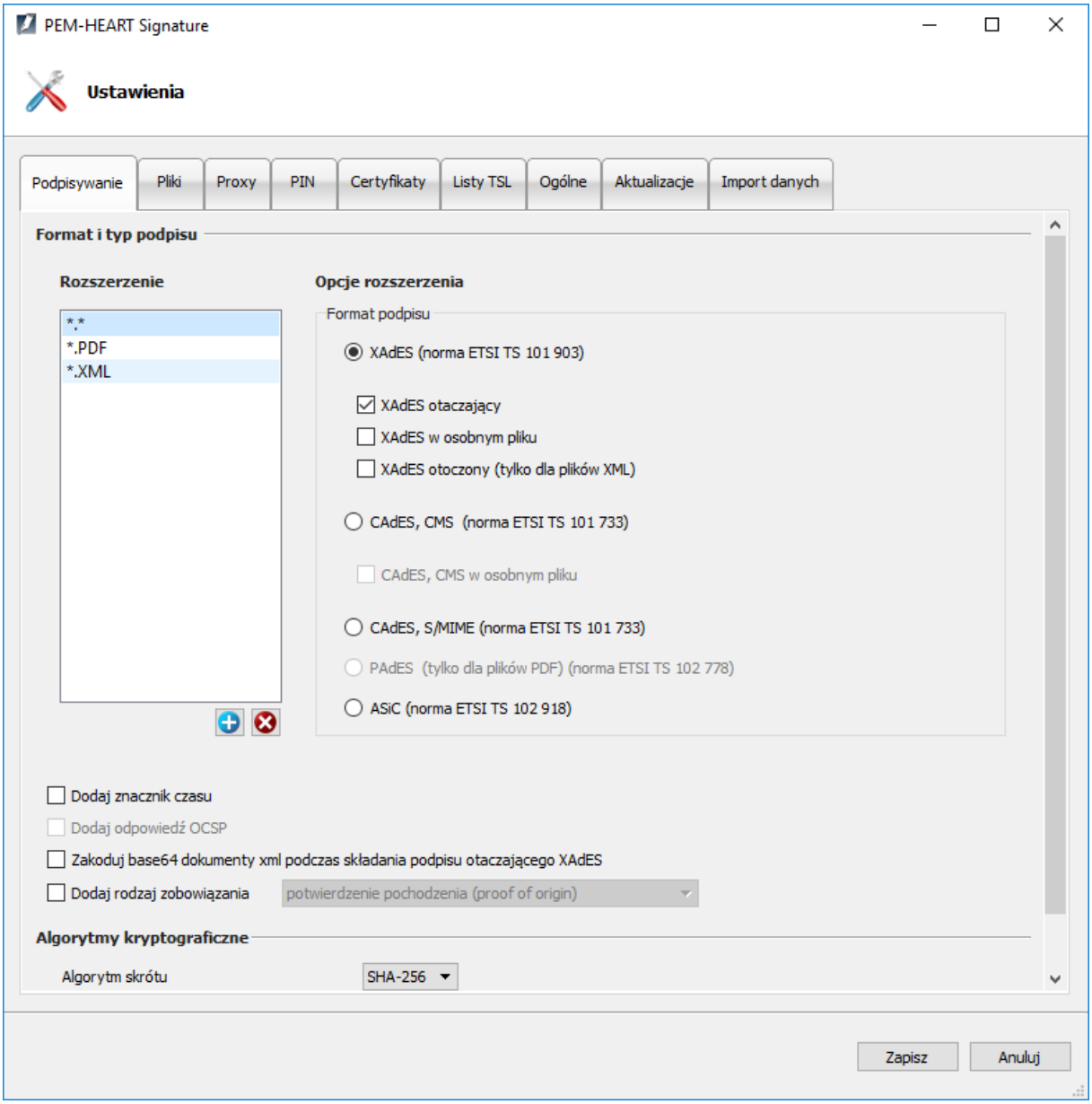
*Art. 137. **Do dnia 1 lipca 2018 r.** do składania zaawansowanych podpisów elektronicznych lub zaawansowanych pieczęci elektronicznych **można stosować funkcję skrótu SHA-1**, chyba że wymagania techniczne wynikające z aktów wykonawczych wydanych na podstawie rozporządzenia 910/2014 wyłączą możliwość stosowania tej funkcji skrótu.*

II. Ustawienia oprogramowania

1. **CenCert** - „**PEM-HEART Signature**”
   a. instalacja certyfikatu w systemie

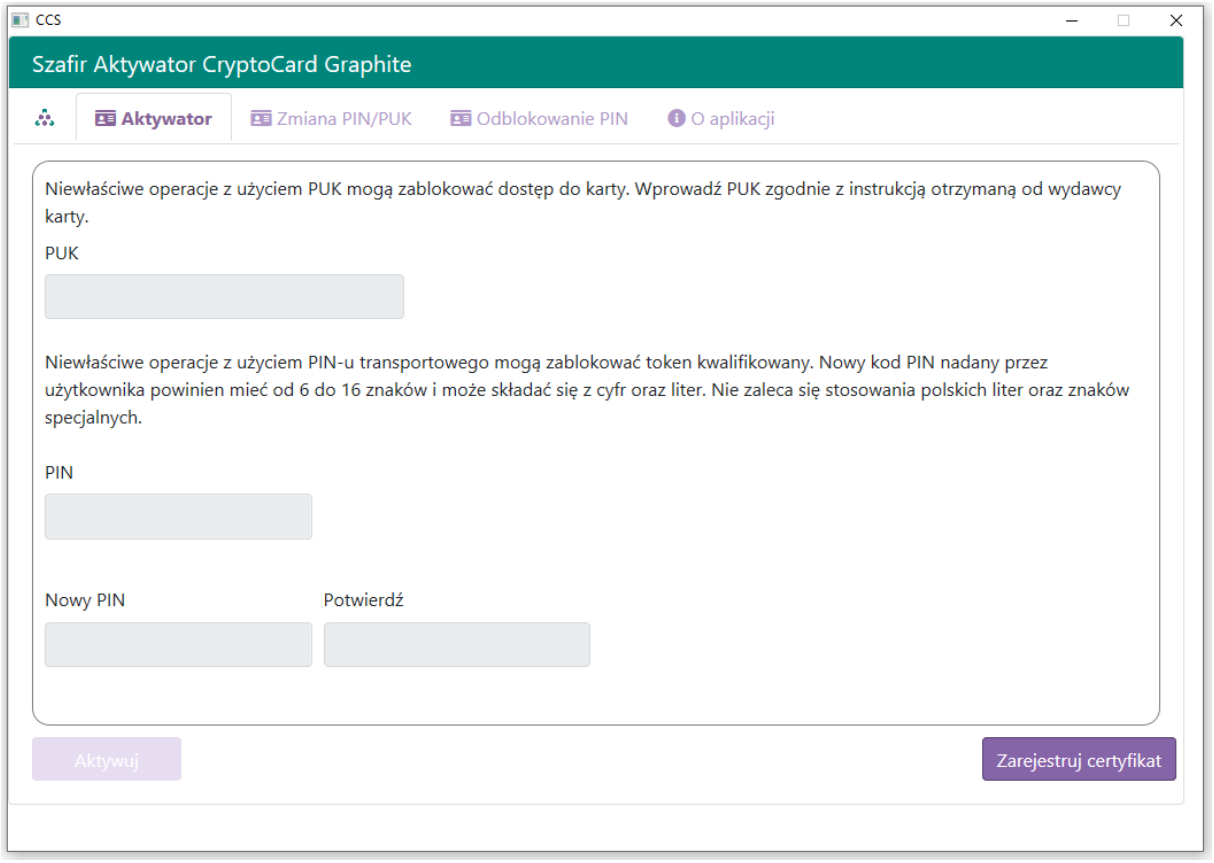


   b. konfiguracja formatu podpisu

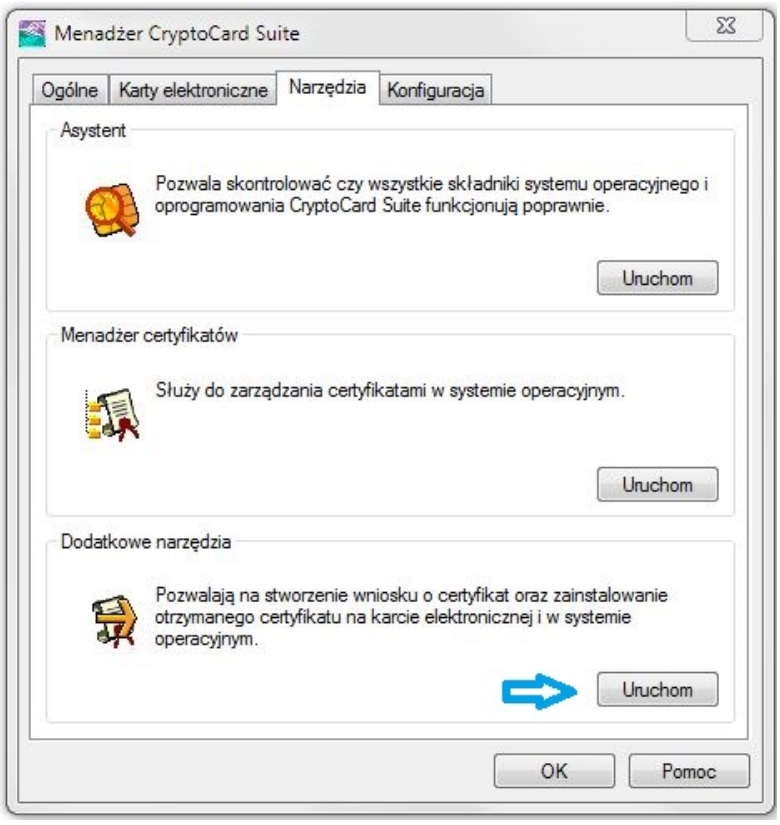

PEM-HEART Signature
Ustawienia
Podpisywanie
Pliki
Proxy
PIN
Certyfikaty
Listy TSL
Ogólne
Aktualizacje
Import danych
Format i typ podpisu
Rozszerzenie
.
*.PDF
*.XML
Opcje rozszerzenia
Format podpisu
XAdES (norma ETSI TS 101 903)
XAdES otaczający
XAdES w osobnym pliku
XAdES otoczony (tylko dla plików XML)
CAdES, CMS (norma ETSI TS 101 733)
CAdES, CMS w osobnym pliku
CAdES, S/MIME (norma ETSI TS 101 733)
PAdES (tylko dla plików PDF) (norma ETSI TS 102 778)
ASiC (norma ETSI TS 102 918)
Dodaj znacznik czasu
Dodaj odpowiedź OCSP
Zakoduj base64 dokumenty xml podczas składania podpisu otaczającego XAdES
Dodaj rodzaj zobowiązania
potwierdzenie pochodzenia (proof of origin)
Algorytmy kryptograficzne
Algorytm skrótu
SHA-256
Zapisz
Anuluj

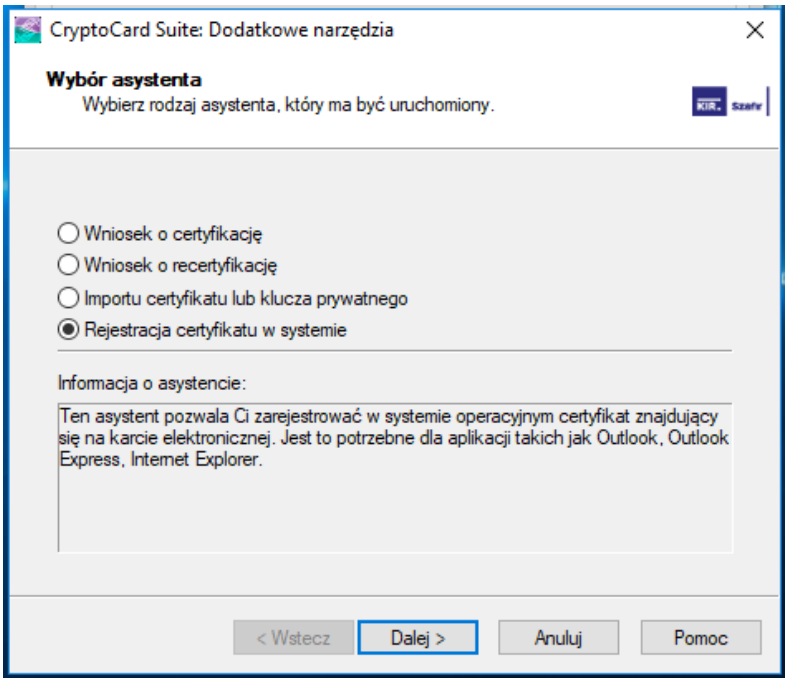
2. KIR S.A.

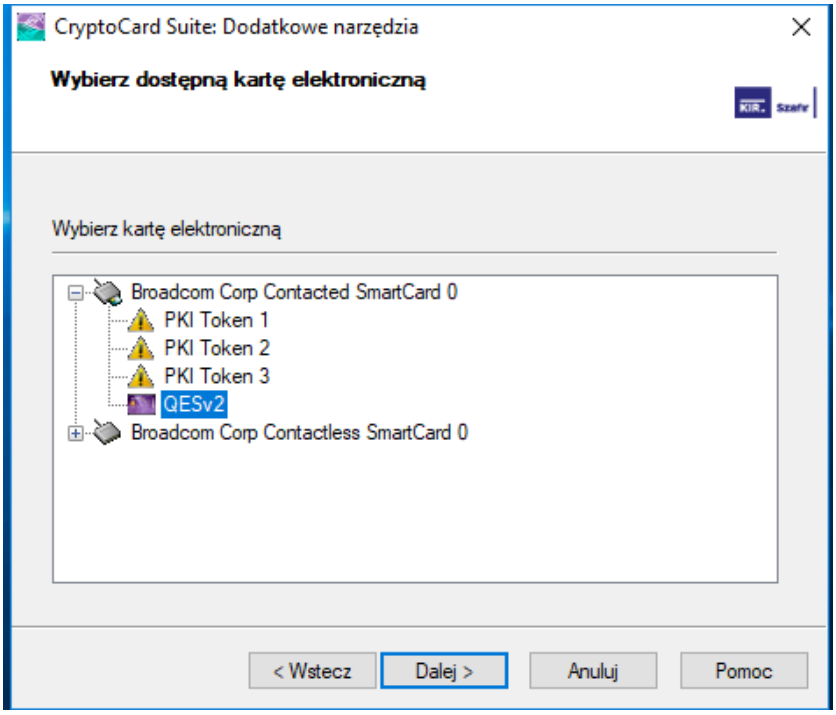
a. „**Szafir Aktywator Cryptocard Graphite**" - instalacja certyfikatu w systemie operacyjnym

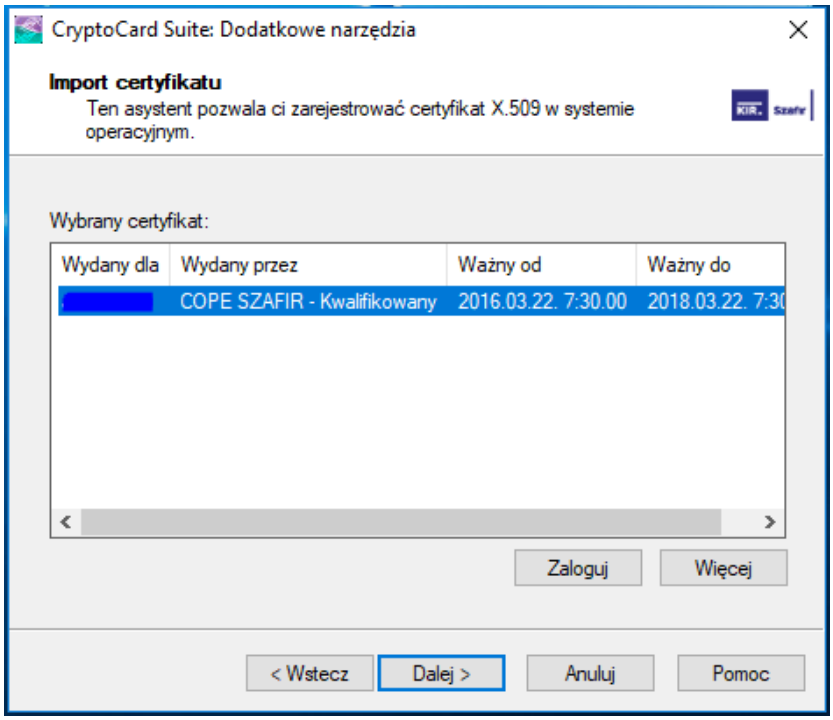


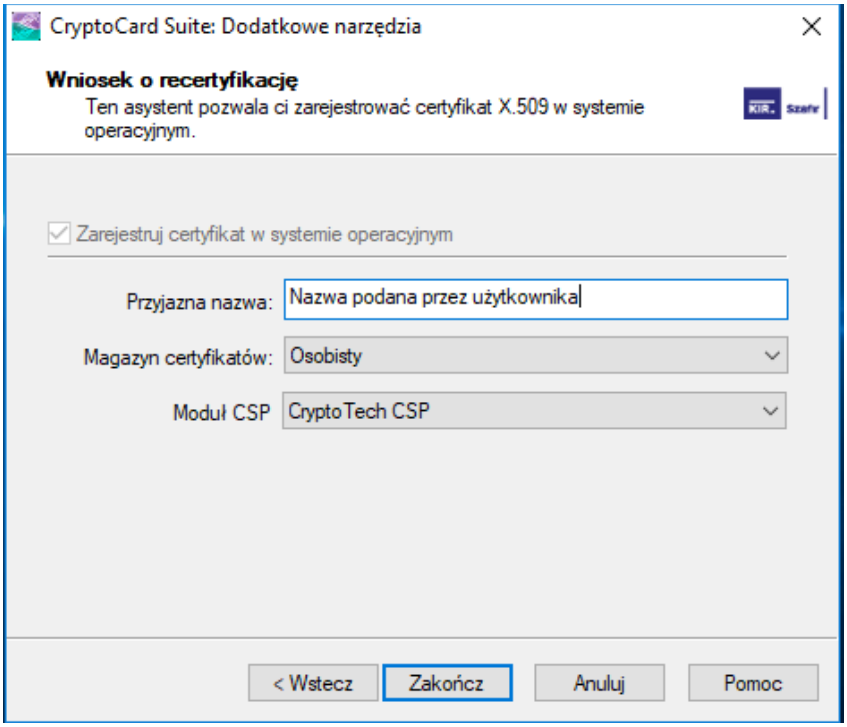
b. „**CryptoCard Suite**" - instalacja certyfikatu w systemie operacyjnym – kolejne kroki



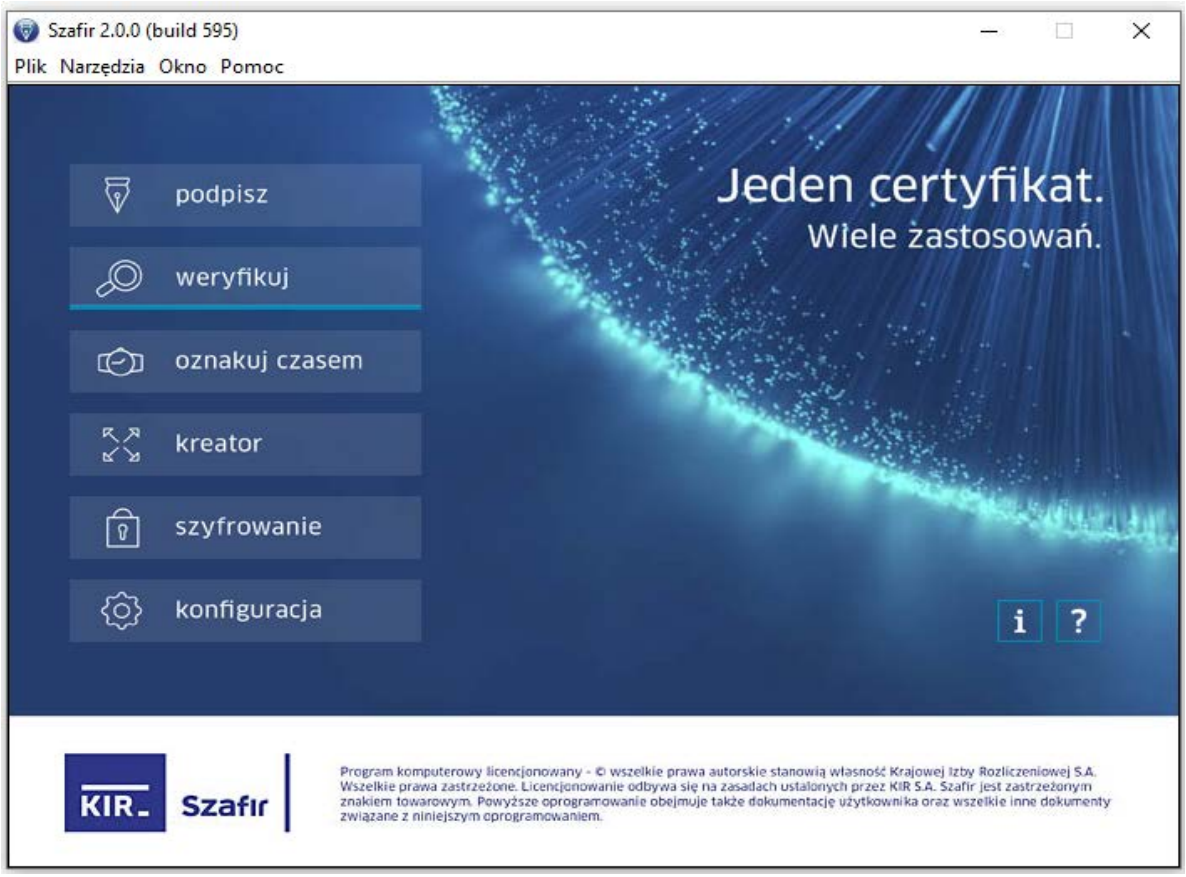

CryptoCard Suite: Dodatkowe narzędzia
Wybór asystenta
Wybierz rodzaj asystenta, który ma być uruchomiony.
Wniosek o certyfikację
Wniosek o recertyfikację
Importu certyfikatu lub klucza prywatnego
Rejestracja certyfikatu w systemie
Informacja o asystencie:
Ten asystent pozwala Ci zarejestrować w systemie operacyjnym certyfikat znajdujący się na karcie elektronicznej. Jest to potrzebne dla aplikacji takich jak Outlook, Outlook Express, Internet Explorer.
< Wstecz
Dalej >
Anuluj
Pomoc

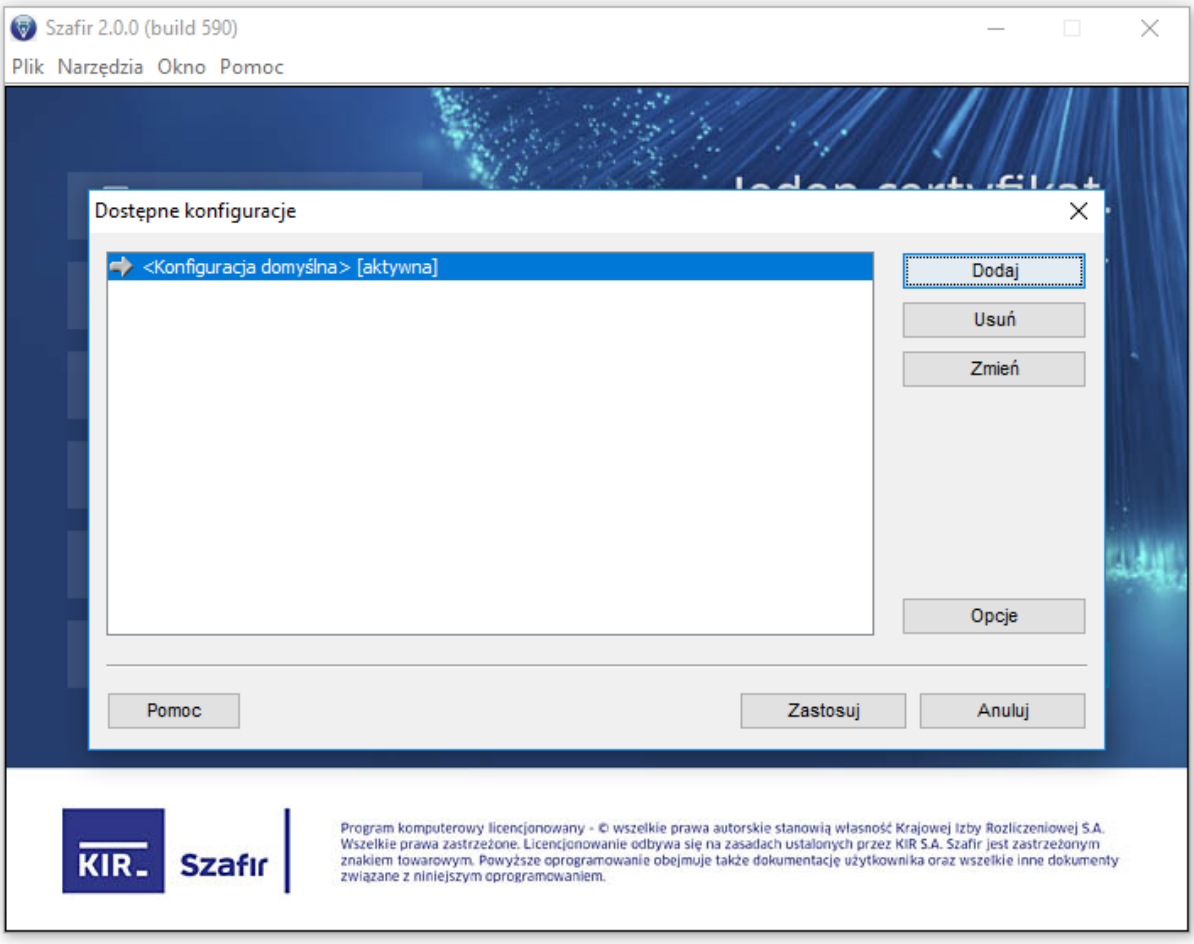

CryptoCard Suite: Dodatkowe narzędzia
Wybierz dostępną kartę elektroniczną
Wybierz kartę elektroniczną
Broadcom Corp Contacted SmartCard 0
PKI Token 1
PKI Token 2
PKI Token 3
QESv2
Broadcom Corp Contactless SmartCard 0
< Wstecz
Dalej >
Anuluj
Pomoc

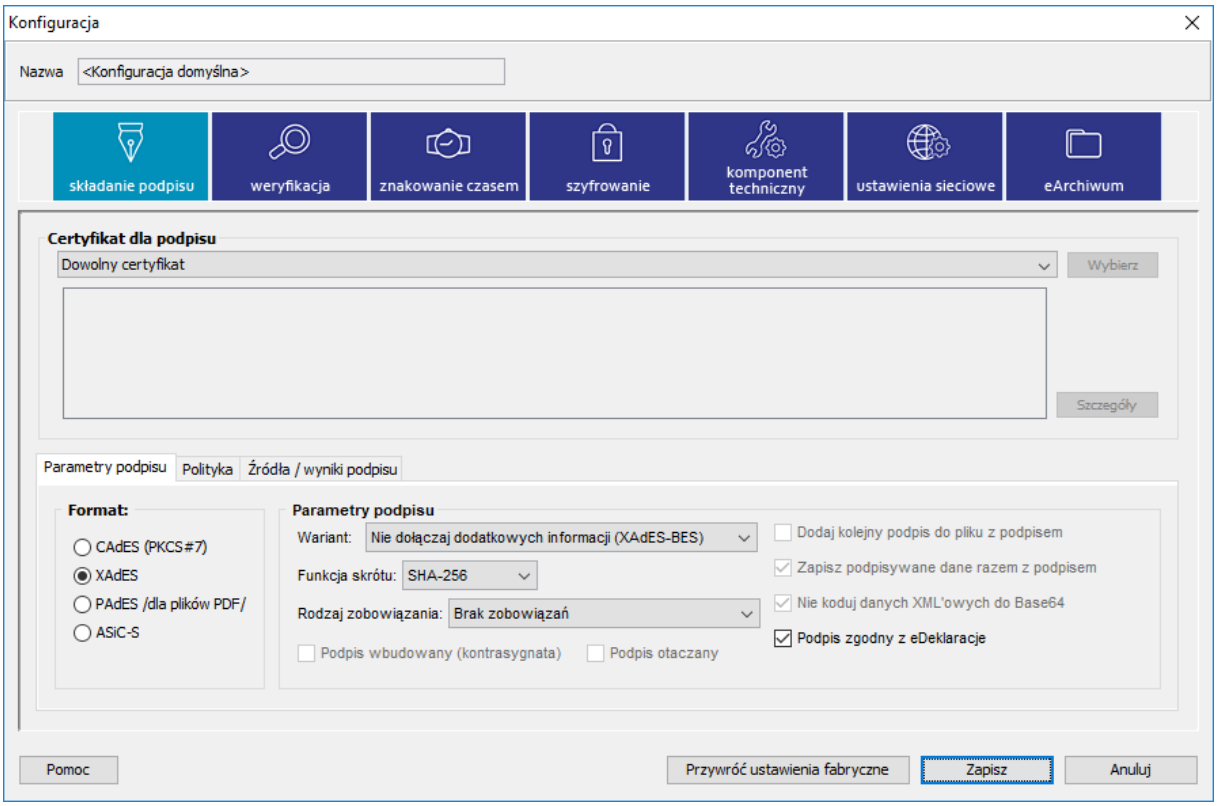

CryptoCard Suite: Dodatkowe narzędzia
Import certyfikatu
Ten asystent pozwala ci zarejestrować certyfikat X.509 w systemie operacyjnym.
Wybrany certyfikat:
Wydany dla
Wydany przez
Ważny od
Ważny do
COPE SZAFIR - Kwalifikowany
2016.03.22. 7:30.00
2018.03.22. 7:3
Zaloguj
Więcej
< Wstecz
Dalej >
Anuluj
Pomoc


CryptoCard Suite: Dodatkowe narzędzia
Wniosek o recertyfikację
Ten asystent pozwala ci zarejestrować certyfikat X.509 w systemie operacyjnym.
Zarejestruj certyfikat w systemie operacyjnym
Przyjazna nazwa:
Nazwa podana przez użytkownika
Magazyn certyfikatów:
Osobisty
Moduł CSP
CryptoTech CSP
< Wstecz
Zakończ
Anuluj
Pomoc

c. **„SZAFIR”** - konfiguracja formatu podpisu



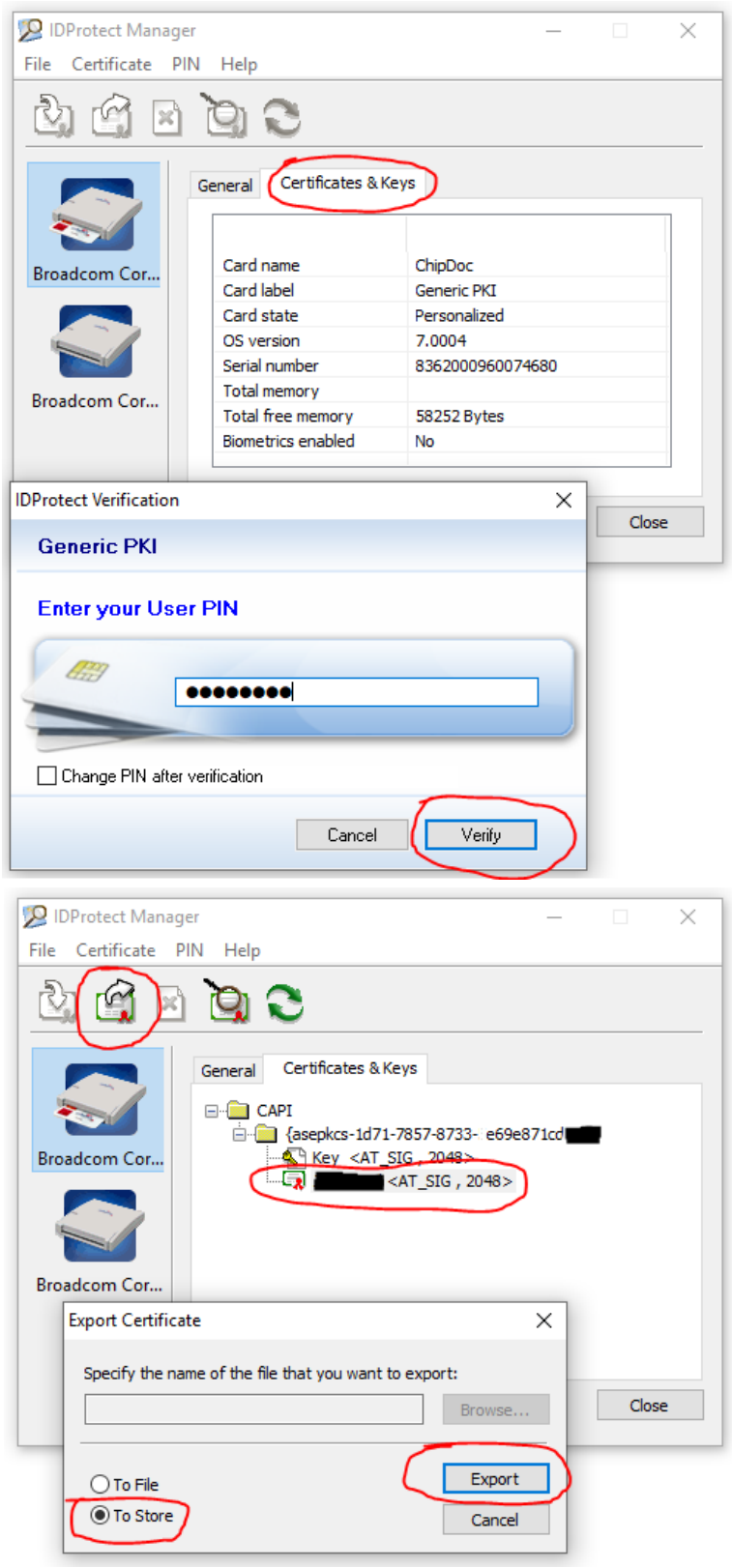



Konfiguracja
Nazwa
<Konfiguracja domyślna>
składanie podpisu
weryfikacja
znakowanie czasem
szyfrowanie
komponent techniczny
ustawienia sieciowe
eArchiwum
Certyfikat dla podpisu
Dowolny certyfikat
Wybierz
Szczegóły
Parametry podpisu
Polityka
Źródła / wyniki podpisu
Format:
CAdES (PKCS#7)
XAdES
PAdES /dla plików PDF/
ASiC-S
Parametry podpisu
Wariant:
Nie dołączaj dodatkowych informacji (XAdES-BES)
Funkcja skrótu:
SHA-256
Rodzaj zobowiązania:
Brak zobowiązań
Podpis wbudowany (kontrasygnata)
Podpis otaczany
Dodaj kolejny podpis do pliku z podpisem
Zapisz podpisywane dane razem z podpisem
Nie koduj danych XML'owych do Base64
Podpis zgodny z eDeklaracje
Pomoc
Przywróć ustawienia fabryczne
Zapisz
Anuluj

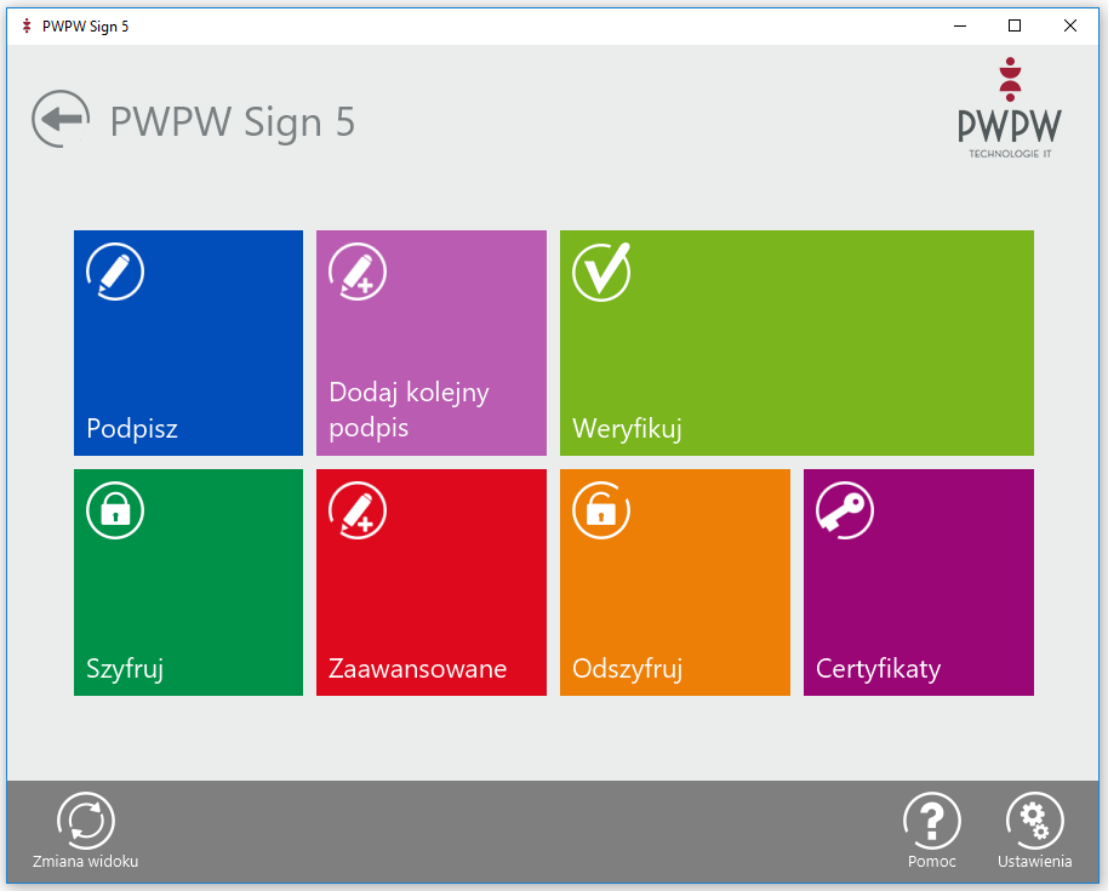
3. Sigillum

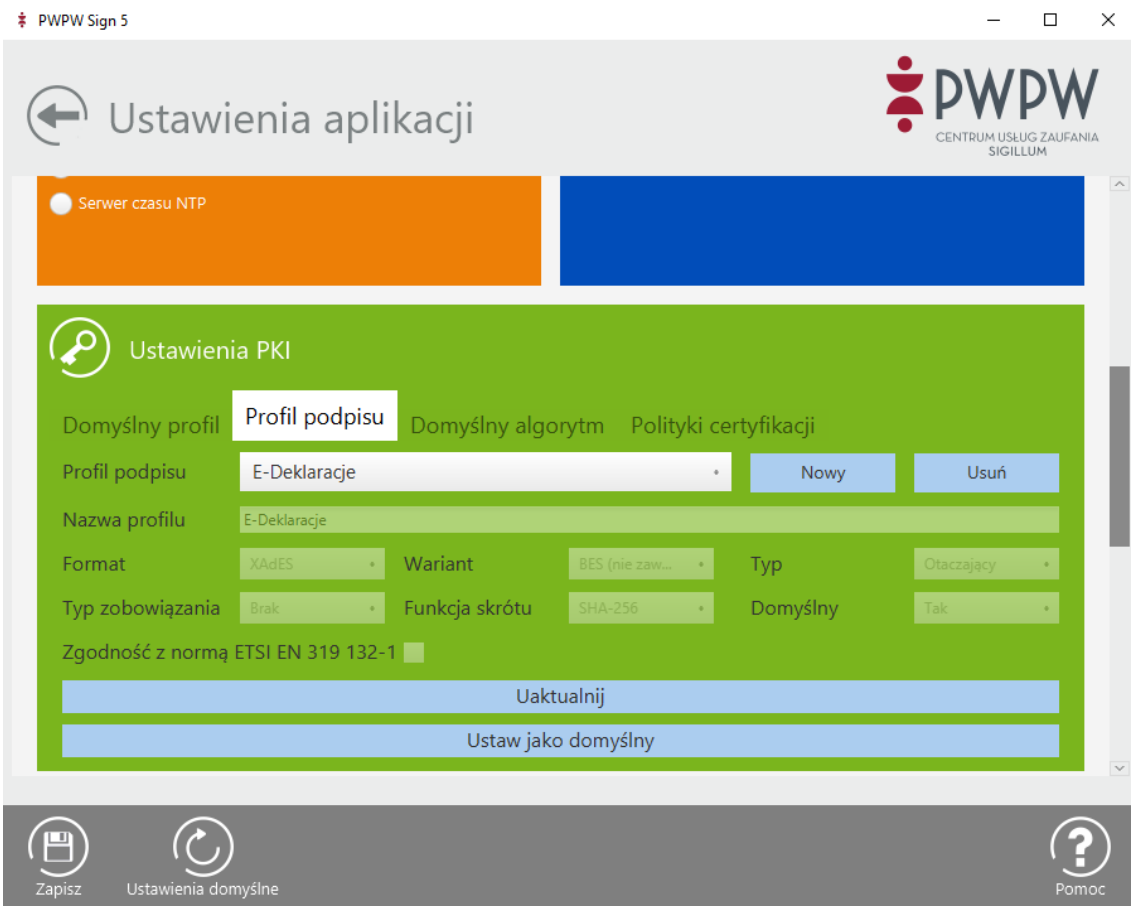
a. „**CryptoCard Suite**” - instalacja certyfikatu w systemie operacyjnym – identycznie jak w pkt 2.a

b. „**IDProtect Manager**” - instalacja certyfikatu w systemie operacyjnym



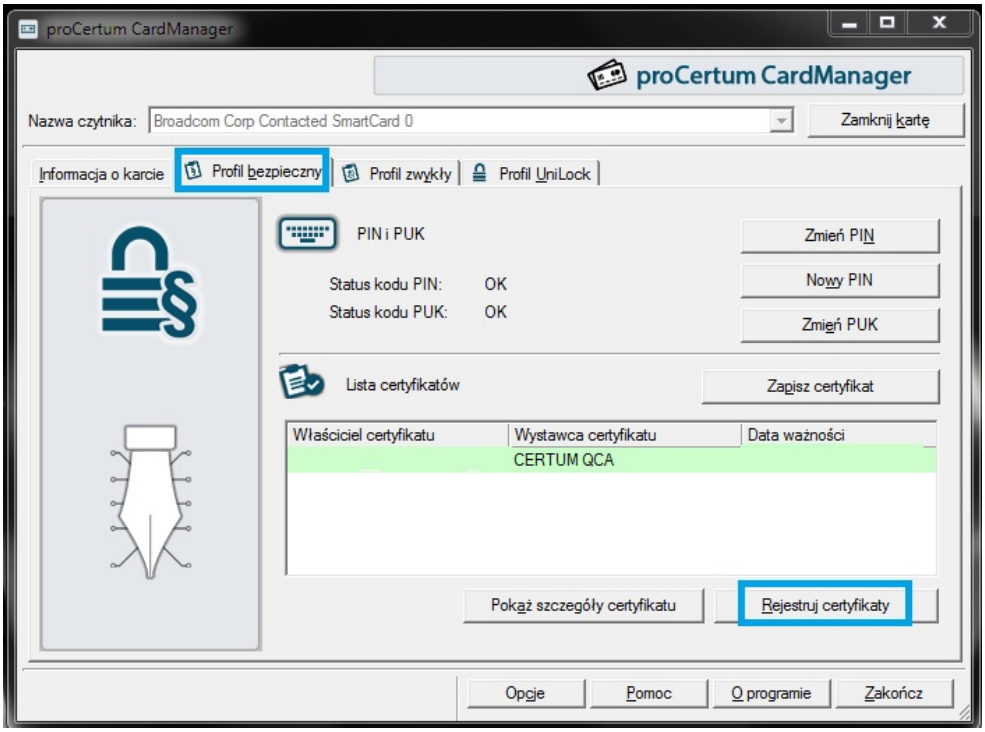
c. **„PWPW Sign 5”** - konfiguracja formatu podpisu



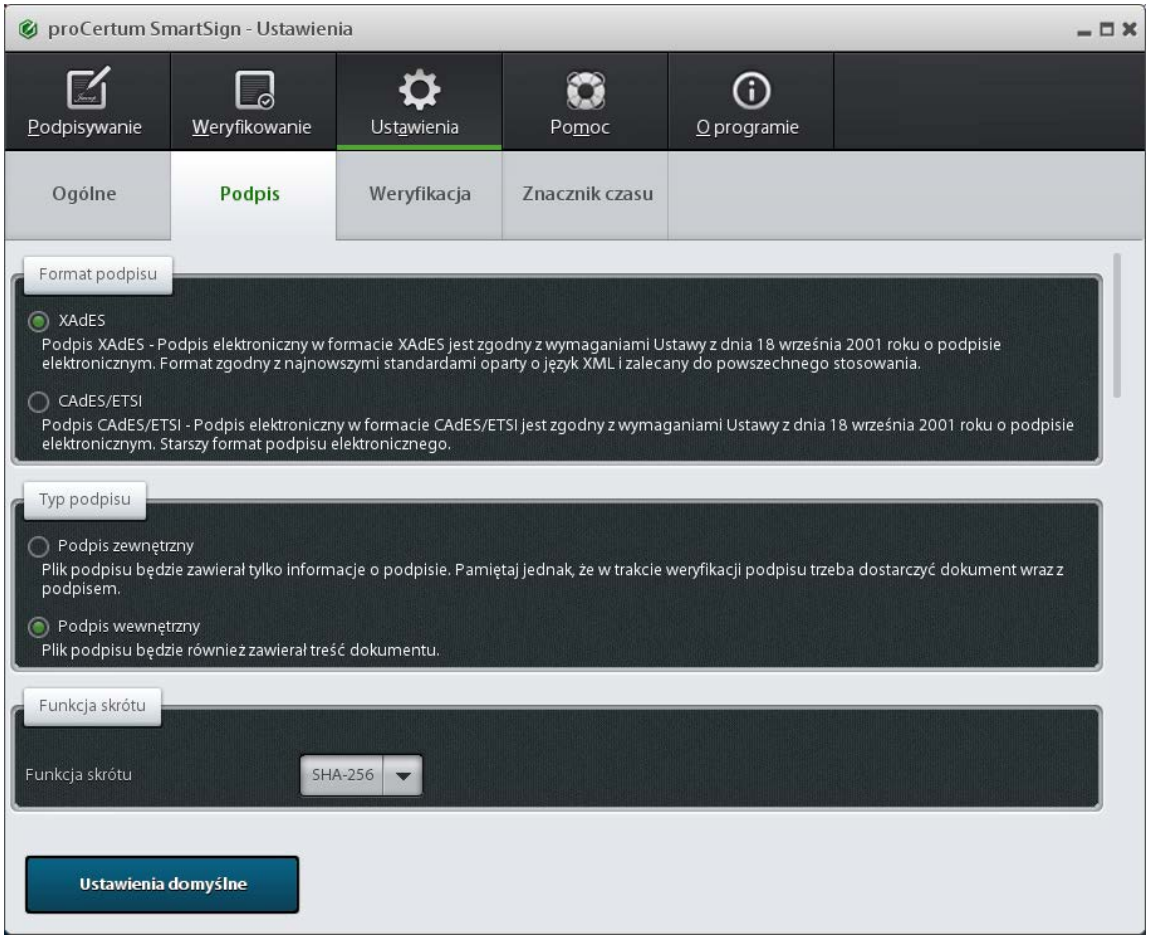


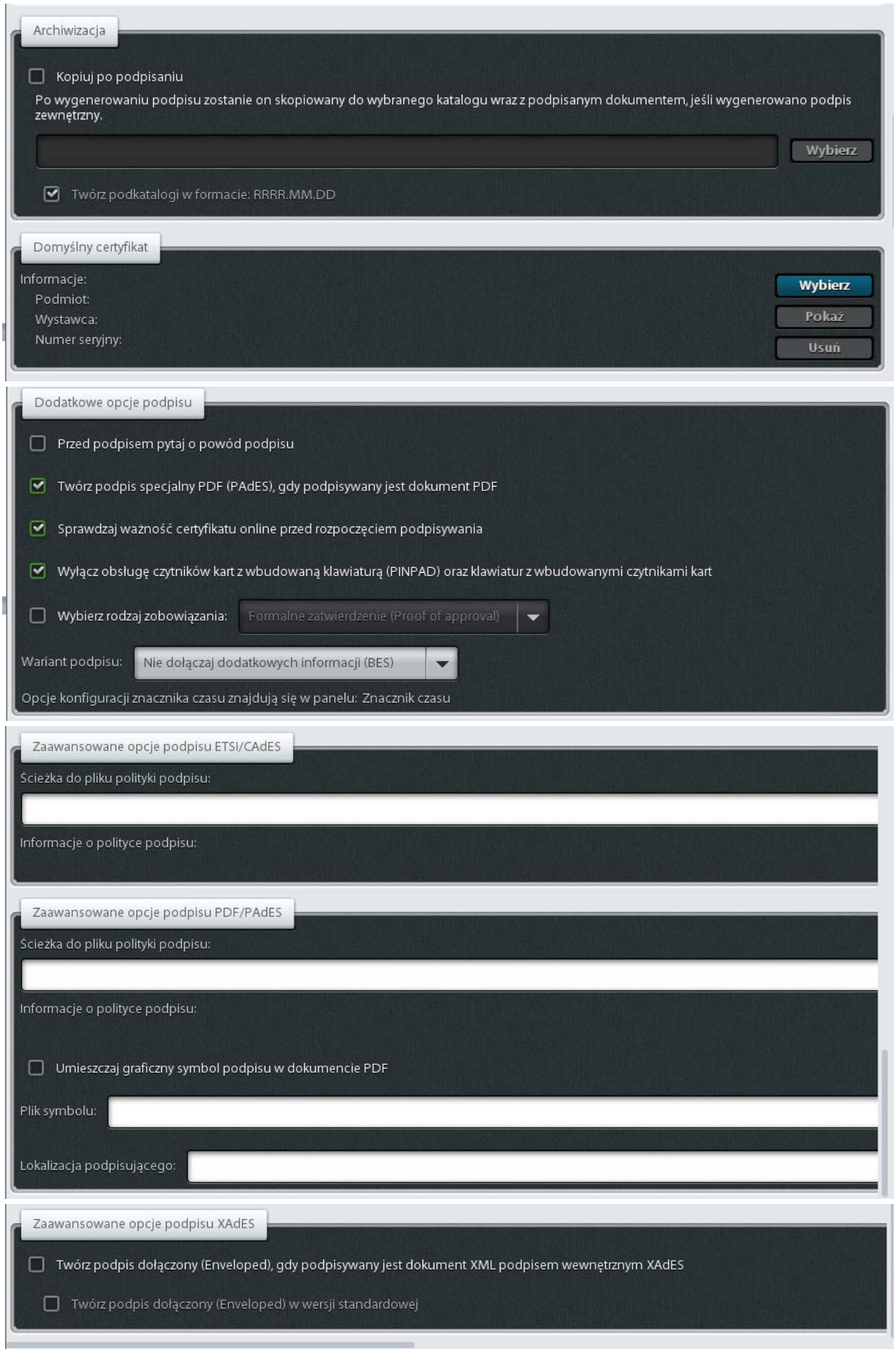
4. CERTUM

a. **„proCertum CardManager”** - instalacja certyfikatu w systemie operacyjnym



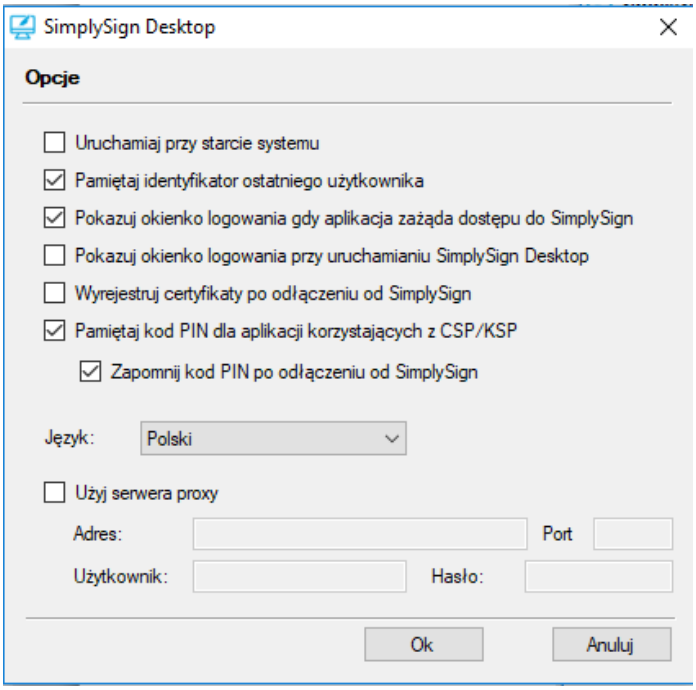
b. **„proCertum SmartSign”** - konfiguracja formatu podpisu



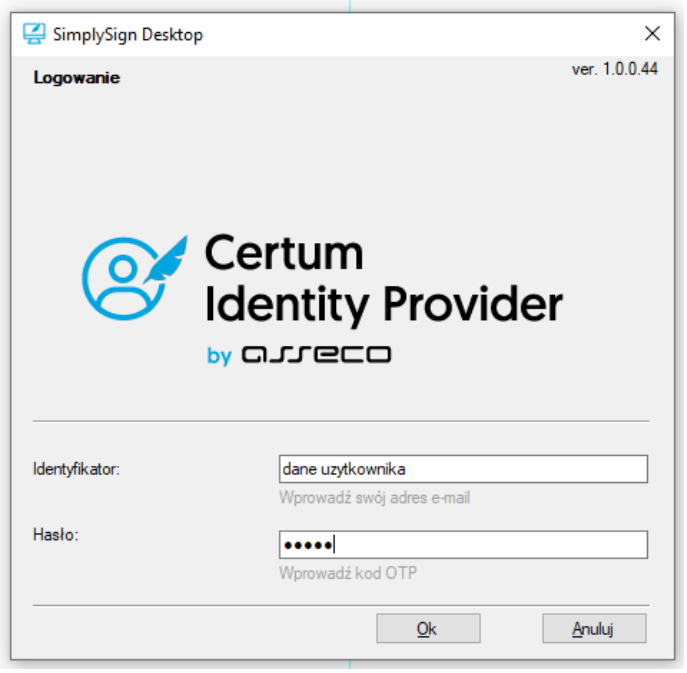

Archiwizacja
Kopiuj po podpisaniu
Po wygenerowaniu podpisu zostanie on skopiowany do wybranego katalogu wraz z podpisanym dokumentem, jeśli wygenerowano podpis zewnętrzny.
Wybierz
Twórz podkatalogi w formacie: RRRR.MM.DD
Domyślny certyfikat
Informacje:
Podmiot:
Wystawca:
Numer seryjny:
Wybierz
Pokaż
Usuń
Dodatkowe opcje podpisu
Przed podpisem pytaj o powód podpisu
Twórz podpis specjalny PDF (PAdES), gdy podpisywany jest dokument PDF
Sprawdzaj ważność certyfikatu online przed rozpoczęciem podpisywania
Wyłącz obsługę czytników kart z wbudowaną klawiaturą (PINPAD) oraz klawiatur z wbudowanymi czytnikami kart
Wybierz rodzaj zobowiązania:
Formalne zatwierdzenie (Proof of approval)
Wariant podpisu:
Nie dołączaj dodatkowych informacji (BES)
Opcje konfiguracji znacznika czasu znajdują się w panelu: Znacznik czasu
Zaawansowane opcje podpisu ETSI/CAdES
Ścieżka do pliku polityki podpisu:
Informacje o polityce podpisu:
Zaawansowane opcje podpisu PDF/PAdES
Ścieżka do pliku polityki podpisu:
Informacje o polityce podpisu:
Umieszczaj graficzny symbol podpisu w dokumencie PDF
Plik symbolu:
Lokalizacja podpisującego:
Zaawansowane opcje podpisu XAdES
Twórz podpis dołączony (Enveloped), gdy podpisywany jest dokument XML podpisem wewnętrznym XAdES
Twórz podpis dołączony (Enveloped) w wersji standardowej

c. **SimplySign Desktop** (dostępnej z paska zadań, *po kliknięciu prawym klawiszem myszki*)

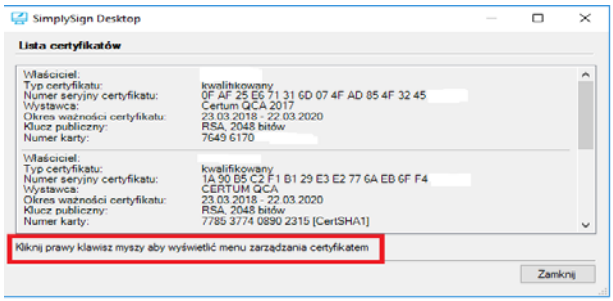
Konfiguracja aplikacji



Logowanie do aplikacji *SimplySign Desktop*

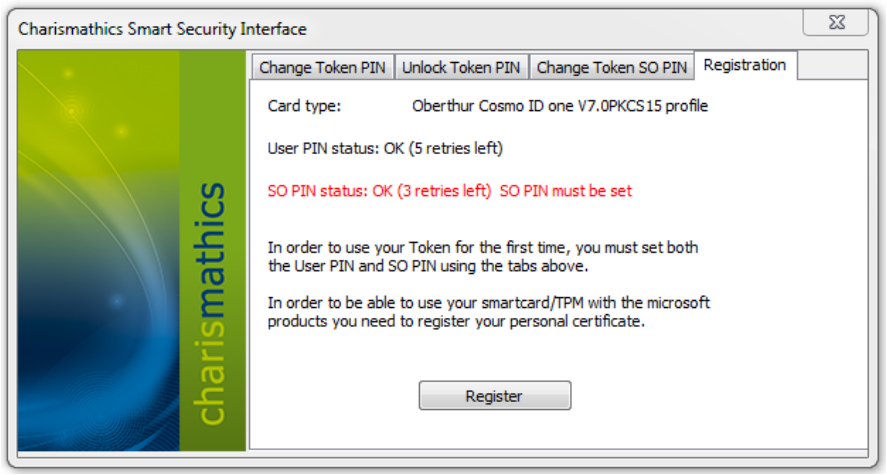


Lista dostępnych certyfikatów w aplikacji (*przykład poniżej pokazuje listę obejmującą 2 certyfikaty, standardowo użytkownik na liście będzie miał 1 certyfikat*)

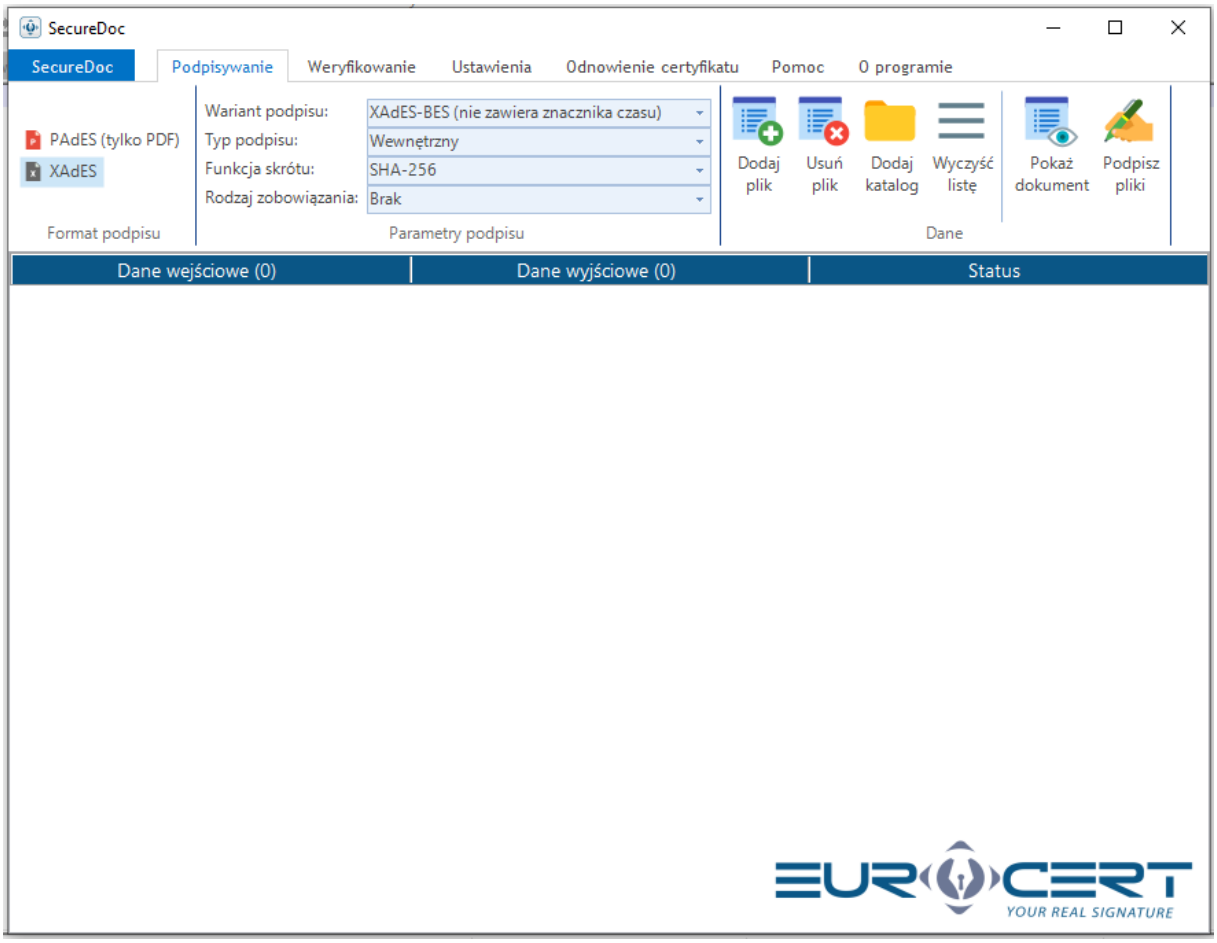


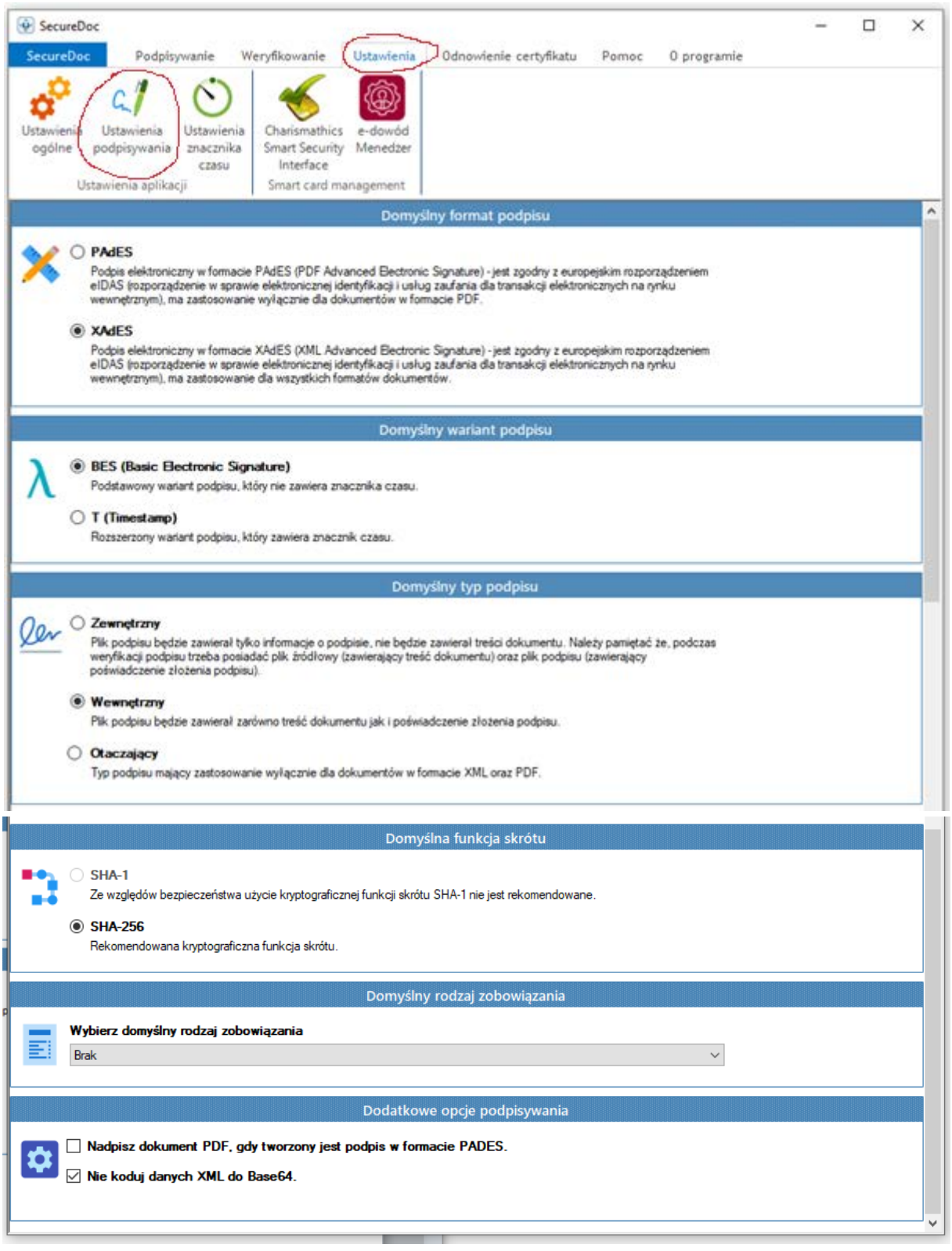
5. EuroCert SecureDoc

a. „**Charismathics Smart Security Interface**" - instalacja certyfikatu w systemie operacyjnym



b. **„EuroCert SecureDoc"** - konfiguracja formatu podpisu




SecureDoc
SecureDoc
Podpisywanie
Weryfikowanie
Ustawienia
Odnowienie certyfikatu
Pomoc
O programie
Ustawienia ogólne
Ustawienia podpisywania
Ustawienia znacznika czasu
Ustawienia aplikacji
Charismathics Smart Security Interface
e-dowód Menedżer
Smart card management
Domyślny format podpisu
PAdES
Podpis elektroniczny w formacie PAdES (PDF Advanced Electronic Signature) - jest zgodny z europejskim rozporządzeniem eIDAS (rozporządzenie w sprawie elektronicznej identyfikacji i usług zaufania dla transakcji elektronicznych na rynku wewnętrznym), ma zastosowanie wyłącznie dla dokumentów w formacie PDF.
XAdES
Podpis elektroniczny w formacie XAdES (XML Advanced Electronic Signature) - jest zgodny z europejskim rozporządzeniem eIDAS (rozporządzenie w sprawie elektronicznej identyfikacji i usług zaufania dla transakcji elektronicznych na rynku wewnętrznym), ma zastosowanie dla wszystkich formatów dokumentów.
Domyślny wariant podpisu
BES (Basic Electronic Signature)
Podstawowy wariant podpisu, który nie zawiera znacznika czasu.
T (Timestamp)
Rozszerzony wariant podpisu, który zawiera znacznik czasu.
Domyślny typ podpisu
Zewnętrzny
Plik podpisu będzie zawierał tylko informacje o podpisie, nie będzie zawierał treści dokumentu. Należy pamiętać że, podczas weryfikacji podpisu trzeba posiadać plik źródłowy (zawierający treść dokumentu) oraz plik podpisu (zawierający poświadczenie złożenia podpisu).
Wewnętrzny
Plik podpisu będzie zawierał zarówno treść dokumentu jak i poświadczenie złożenia podpisu.
Otaczający
Typ podpisu mający zastosowanie wyłącznie dla dokumentów w formacie XML oraz PDF.
Domyślna funkcja skrótu
SHA-1
Ze względów bezpieczeństwa użycie kryptograficznej funkcji skrótu SHA-1 nie jest rekomendowane.
SHA-256
Rekomendowana kryptograficzna funkcja skrótu.
Domyślny rodzaj zobowiązania
Wybierz domyślny rodzaj zobowiązania
Brak
Dodatkowe opcje podpisywania
Nadpisz dokument PDF, gdy tworzony jest podpis w formacie PADES.
Nie koduj danych XML do Base64.