

The CryptToken[®]



Ronny Guber

Content

- 1. MARX Data Security and Microplan**
- 2. Field of application**
- 3. CrypToken[®] 2000 and M2048**

MARX Data Security and Microplan

- **20 Years of Software Protection**
- **Branches in Germany and USA**
- **Official MARX distributor in Poland:**



Securing the Digital WorldSM

Strong User Authentication



Securing the Digital WorldSM

Easy integration, easy installation



Driverless installation

CrypToken M2048 on CCID
enabled operating systems

CrypToken® 2000 and CrypToken® M2048



CT 2000

- AES, RSA (driver level)
- additional Smarx API
- 32 or 64 kB memory

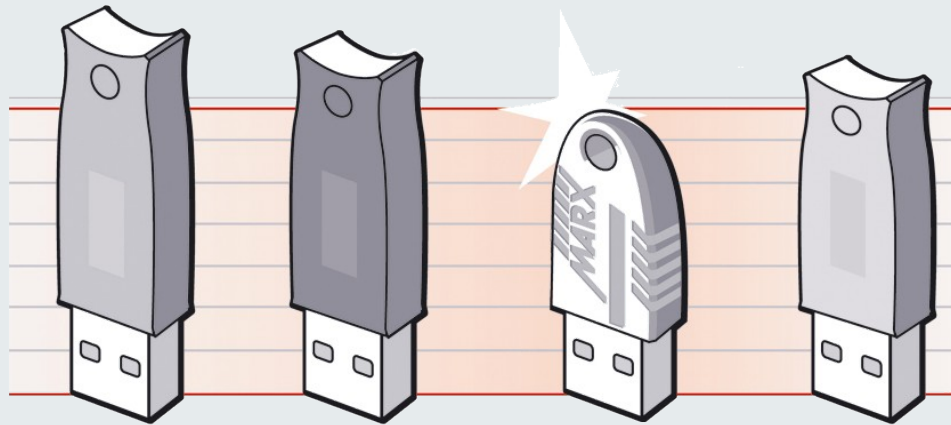


CT M2048

- MULTOS smart card operating system
→ ITSEC Level E6 high
- AES, RSA
- 64 kB memory

CrypToken[®] 2000 and CrypToken[®] M2048

- shortest token available (35 mm)
- shock resistant metal case
- waterproof
- radiation protected



Securing the Digital WorldSM



CrypToken M2048

Daniel Rode

CrypToken[®] M2048 – główne cechy:

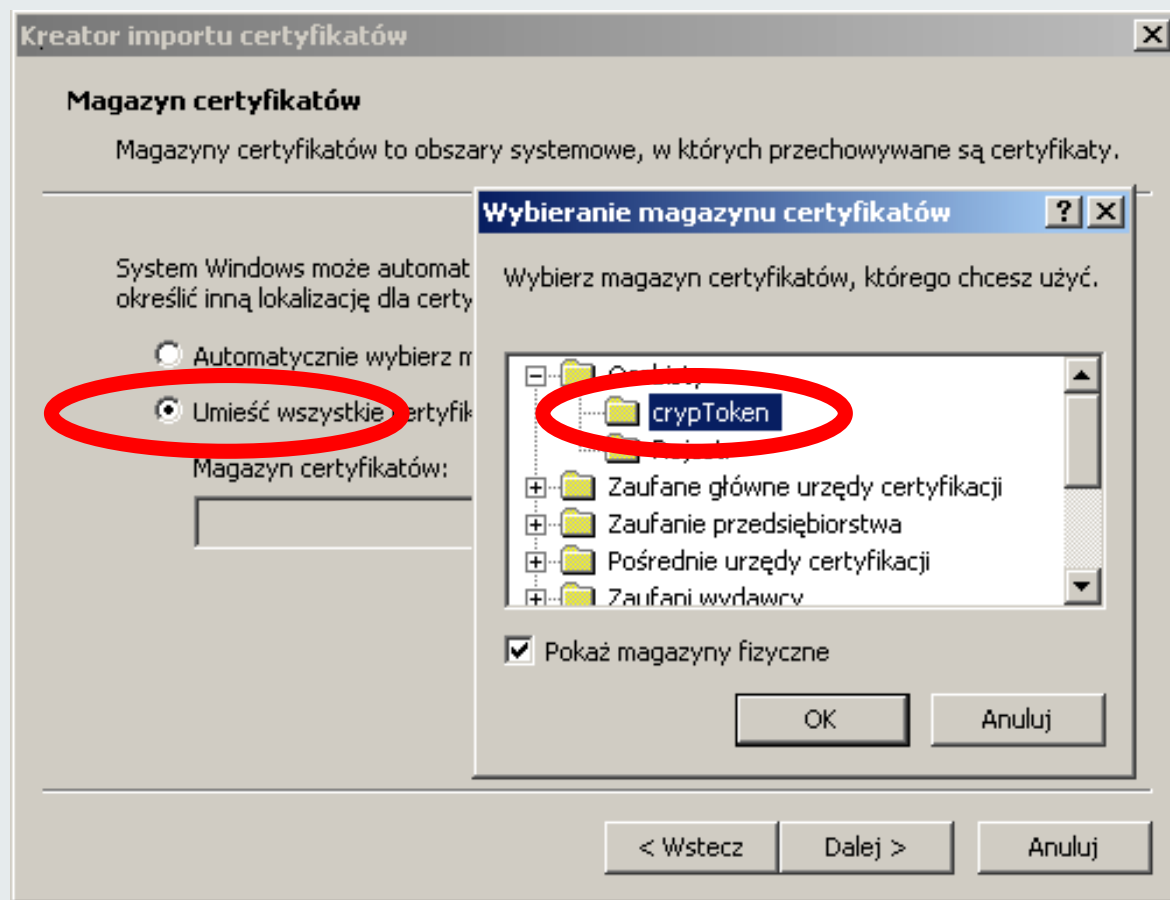
- 64 kB pamięci,
- wbudowane wsparcie dla RSA i AES,
- system operacyjny MULTOS (ITSEC Level E6 high),
- wsparcie dla standardów PKCS#11 i MS-CAPI.

CrypToken® M2048 – podstawowe zastosowanie:

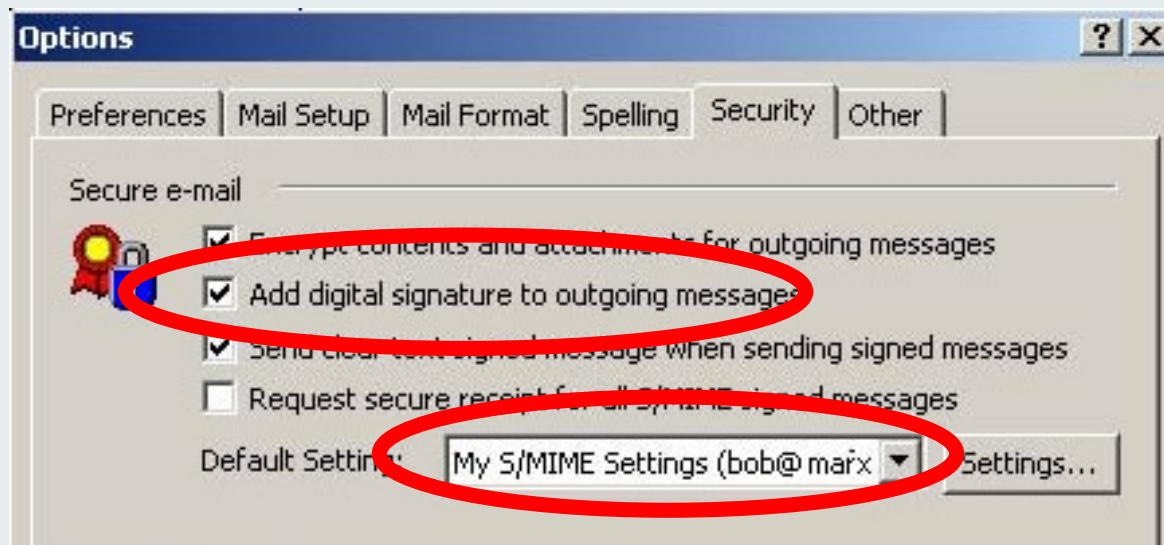
- podpisy cyfrowe, szyfrowanie wiadomości,
- bezpieczny dostęp do www (WebSecurity),
- VPN,
- integracja z PGP,
- inne rozwiązania oparte o PKCS#11/MS-CAPI,
- inne rozwiązania korzystające z systemu MULTOS.

Podpis cyfrowy z CrypToken® M2048:

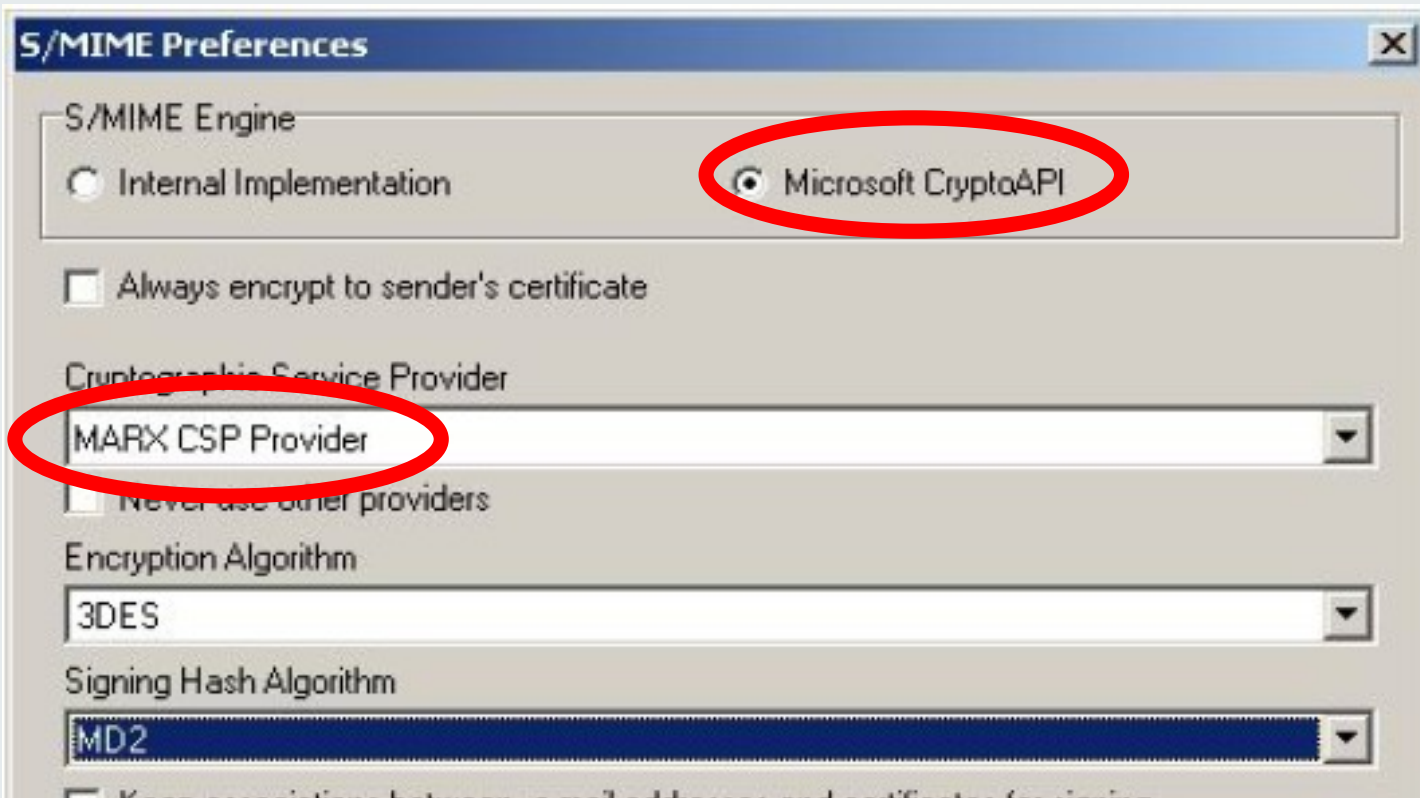
- **CrypToken jest używany jako Bezpieczny Kontener dla klucza prywatnego i związanego z nim certyfikatu.**
- **kompatybilny ze standardami PKCS #11 i MS-CAPI.**
- **wsparcie dla najpopularniejszych klientów pocztowych: MS Outlook Express, MS Outlook Professional 2000/2002/2003, The Bat, Mozilla Email Client,**
- **2-czynnikowa autoryzacja,**
- **klucz prywatny zawsze „pod ręką”.**



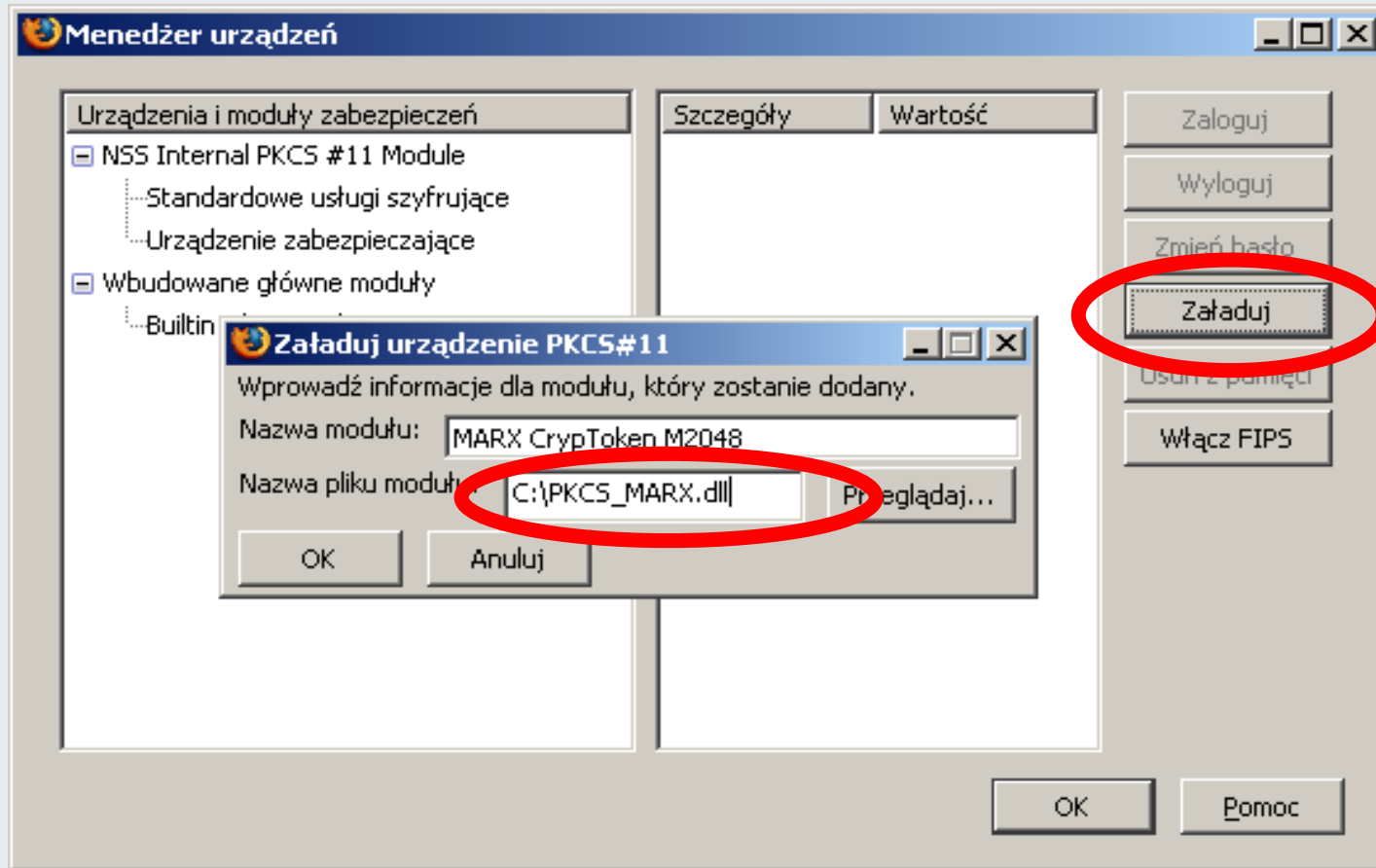
Import certyfikatu do CrypToken'a (MS-CAPI).



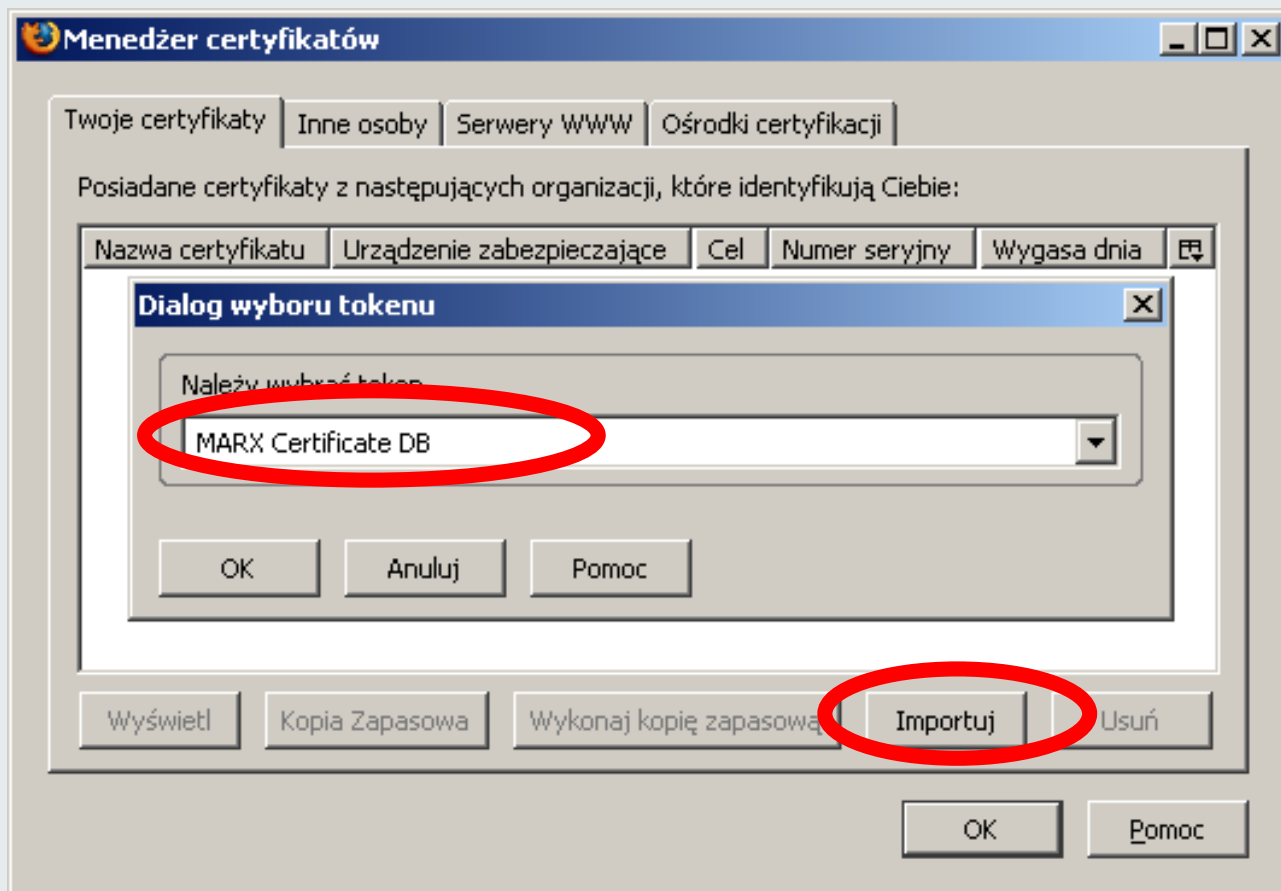
Konfiguracja programu pocztowego Microsoft Outlook



Konfiguracja programu pocztowego The Bat!



Instalacja urządzenia zabezpieczającego CryptToken w aplikacji Mozilla



Import certyfikatu do CrypToken'a (PKCS #11).

Zabezpieczenia wiadomości

Aby wysyłać i odbierać wiadomości podpisane cyfrowo lub zaszyfrowane, należy określić certyfikat podpisu osobistego oraz certyfikat szyfrujący.

Podpis cyfrowy

Certyfikat, który będzie używany do cyfrowego podpisywania wysyłanych wiadomości:

Podpisz cyfrowo wiadomości

Szyfrowanie wiadomości

Certyfikat, który będzie używany do szyfrowania wysyłanych wiadomości:

Domyślne ustawienia szyfrowania

Nigdy (nie używaj szyfrowania)

Wymagaj (nie można wysłać wiadomości bez szyfrowania)

Wybierz certyfikat

Certyfikat: **MARX Certificate DB: Zaimportowany certyfikat [01]**

Szczegóły wybranego certyfikatu:

Wystawiony dla: E=uto@microplan.pl,CN=microplan,OU=microplan,O=microplan,L=poznan,ST=wlkp,C=PL
Numer seryjny: 01
Ważny od 2005-11-24 12:01:00 do 2006-11-24 12:01:00
Cel: Klient, Podpis, Szyfrowanie
Wystawiony przez: E=hh@ii.com,CN=aa,OU=gg,O=ff,L=ee,ST=dd,C=BB
Przechowywany w: MARX Certificate DB

Konfiguracja programu pocztowego Mozilla.

WebSecurity z CrypToken® M2048:

- **Bezpieczny Kontener na certyfikat użytkownika,**
- **może być użyty na dowolnym komputerze,**
- **rozwiązanie wspierane przez różne przeglądarki internetowe i systemy operacyjne (klient),**
- **rozwiązanie wspierane przez różne serwery www obsługujące protokół SSL (serwer),**
- **zwiększone bezpieczeństwo dzięki 2-czynnikowemu uwierzytelnianiu (“posiadanie” i “wiedza”),**
- **uwierzytelnienie serwera i klienta,**
- **lepsza kontrola dostępu, jeden CrypToken – jeden użytkownik.**

Sieci VPN z CrypToken[®] M 2048:

- **Bezpieczny Kontener na prywatny klucz x.509,**
- **może być użyty na dowolnym komputerze,**
- **zwiększone bezpieczeństwo dzięki 2-czynnikowemu uwierzytelnianiu (“posiadanie” i “wiedza”).**

Integracja CrypToken[®] M2048 z PGP:

- **CrypToken jako niezawodny Bezpieczny Kontener dla osobistej pary kluczy,**
- **działa z PGPmail,**
- **działa jako plugin PGPmail do klientów pocztowych,**
- **działa z PGPdisk.**

Inne rozwiązania z CrypToken® M2048:

- może być efektywnie wykorzystany z dowolnym rozwiązaniem korzystającym ze standardu PKCS #11 lub MS-CAPI,
- przeznaczony do rozwiązań PKI służących do identyfikacji użytkowników i używających par kluczy oraz certyfikatów,
- silne uwierzytelnianie w różnych systemach sieciowych (także rozległych),
- niepodatny na żadną znaną metodę hackowania.



System MULTOS i CrpToken® M2048:

Dzięki zastosowaniu systemu operacyjnego MULTOS w rozwiązaniu CrpToken, możliwe jest załadowanie na klucz dowolnej aplikacji napisanej dla tego systemu, wykorzystującej SmartCard'y.

Securing the Digital WorldSM

Inne rozwiązania oferowane przez MARX'a:

Inne rozwiązania oparte na sprzęcie firmy MARX:

- **ochrona oprogramowania,**
- **kontrola dostępu do stacji roboczych,**
- **kontrola zdalnego dostępu (SSH, ftp, itp.),**
- **inne rozwiązania (implementacja własna; dołączone biblioteki).**



Dziękujemy za uwagę!

Daniel Rode

daniel.rode@microplan.pl

www.microplan.pl

www.marx.pl

+48 61 851 89 16

Securing the Digital WorldSM