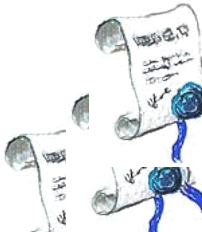
Karty elektroniczne w PKI - znane ataki i sposoby przeciwdziałania im

CONFidence 2005

Adam Augustyn - *ad*
am.augustyn@cryptotech.com.pl

Plan prezentacji

- Czym są karty elektroniczne?
- Najczęstsze ataki?
- Jak się bronić?
- Wnioski

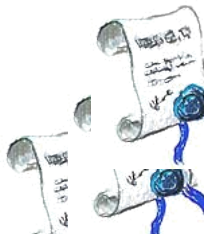


Czym są karty elektroniczne?

- Norma ISO-7816
- Procesor x51 / RISC
- Pamięć 32 kB / 64kB EEPROM
- RSA (1024/2048 bit), DSA
- DES, 3DES, AES, MAC, SHA1
- Sprzętowy generator liczb losowych
- Zarządzanie pamięcią
- Certyfikaty dla układu / OS / aplikacji
- Generowanie kluczy na karcie

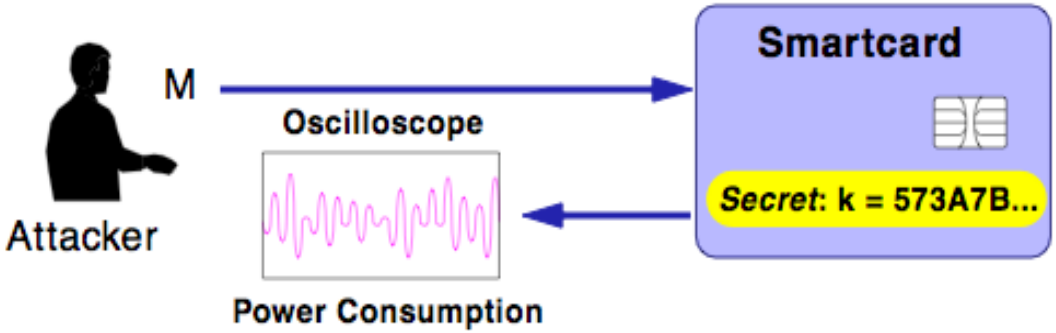
Najczęstsze ataki?

- Ataki fizyczne
- Czy klucz był kiedyś poza kartą?
- Podczas pracy:
  - komunikacja z kartą
  - wprowadzanie kodu PIN
  - uprawnienia
  - wieloaplikacyjność
- Ataki na aplikacje korzystające z kart elektronicznych
- Bezpieczne urządzenie - "*What you see is what you sign*"???



Ataki fizyczne na układ elektroniczny

- Próby odczytania pamięci EEPROM
- SPA / DPA / TA / DFA
- Nie tylko klucze – także PIN!
- Zmuszanie karty do pracy w anormalnych warunkach
- **Sprzętu nie da się poprawić!**



Przykład:

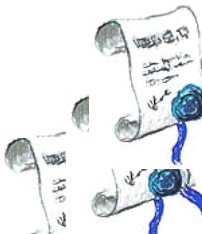
Compute: M^e mod N

```
exp1(M, e, N)
{
  R = M
  for ( i = n - 2 down to 0)
  {
    R = R^2 mod N
    if ( ith bit of e is a 1)
      R = R·M mod N
  }
  return R
}
```

Secret Key

Example: e = 83 → 1010011

i	e	R
-	1	M
5	0	M^2
4	1	M^5
3	0	M^{10}
2	0	M^{20}
1	1	M^{41}
0	1	M^{83}

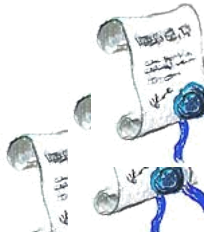


Obrona:

- Konstrukcja fizyczna układu elektronicznego
- Monitoring zewnętrznych parametrów fizycznych
- Sumy kontrolne i wykrywanie błędów
- Zakłócanie poboru mocy
- Losowy czas wykonywania operacji
- Transakcyjność

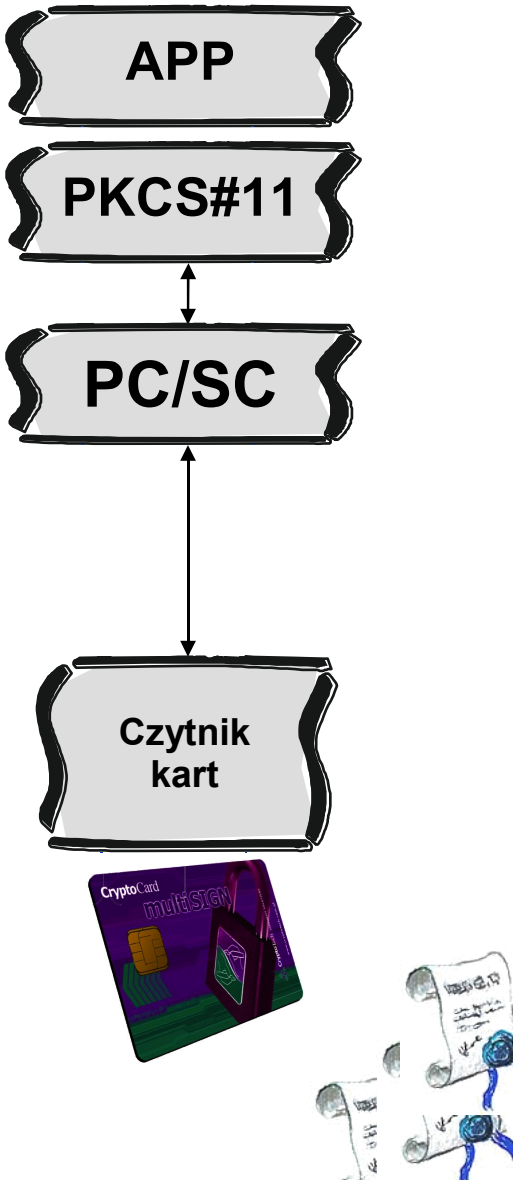
Czy klucz był kiedyś poza kartą?

- Jak był generowany klucz RSA
- Liczby losowe
- Dlaczego czasami klucz RSA musi być poza kartą?
- Jak archiwizować klucze?
- Bezpieczna postać vs. bezpieczne środowisko
- Jakie klucze archiwizować (SSL vs. ważne dane)?



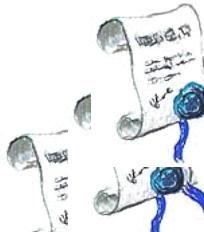
Podsłuchiwanie komunikacji

- Wiele warstw programowo-sprzętowych
- Możliwe ataki zdalne
- Secure messaging
  - Symetryczne szyfrowanie komunikacji
  - Asymetryczne szyfrowanie
    - TCP/IP i SSL
- Podpisywanie kodu (TCG?)
- Pozostają problemy z uwierzytelnieniem aplikacji do karty



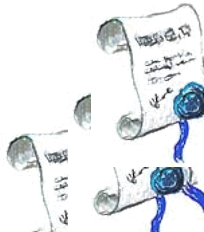
Przechwycenie PIN-u

- Win32 – Spy
- Wirtualne desktopy?
- Czytnik z PINpad-em
- Problemy:
  - Cena???
  - PC/S.C. 2.0
  - Brak wsparcia w aplikacjach
  - Fizyczne szpiegowanie
  - Analiza zużycia przycisków



Buforowanie PIN-u

- Wygodne ;)
- Wymagane przez niektóre aplikacje
  - Wielokrotne wykonywanie operacji
  - Brak GUI (Winlogon)
  - Najczęściej zła praktyka!!!
- Jak przechowywany jest PIN?
- DLL-injection
- Umożliwienie dostępu do innych zasobów karty!
- Czy są jakieś rozwiązania...?

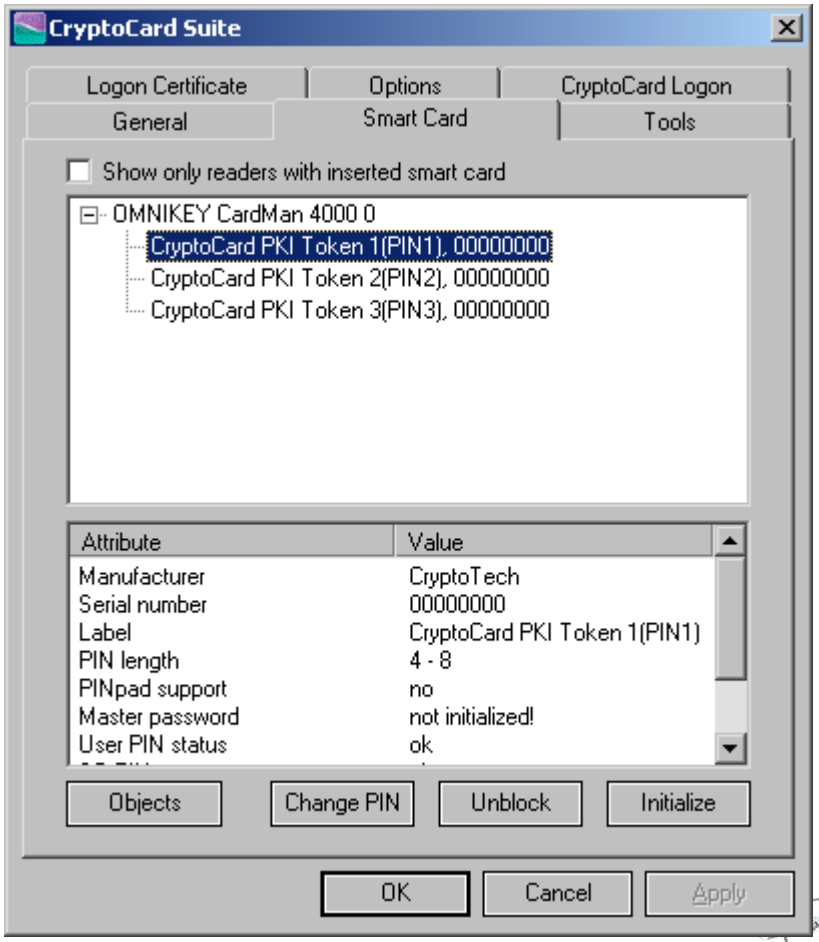


Rozwiązania - 1

- Ograniczanie operacji:
  - czasem
  - ilością
- Różnice w implementacjach
- Monitorowanie aktywności karty
- Przyszłość: Smartcards FireWall?

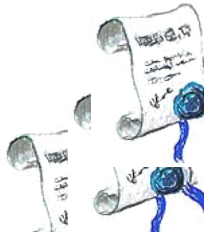
Rozwiązania - 2

- Ochrona sekretów różnymi PINami
- Możliwość konfigurowania zachowania wirtualnych tokenów
- Czasami mniej wygodne
- Dynamiczne zarządzanie pamięcią karty



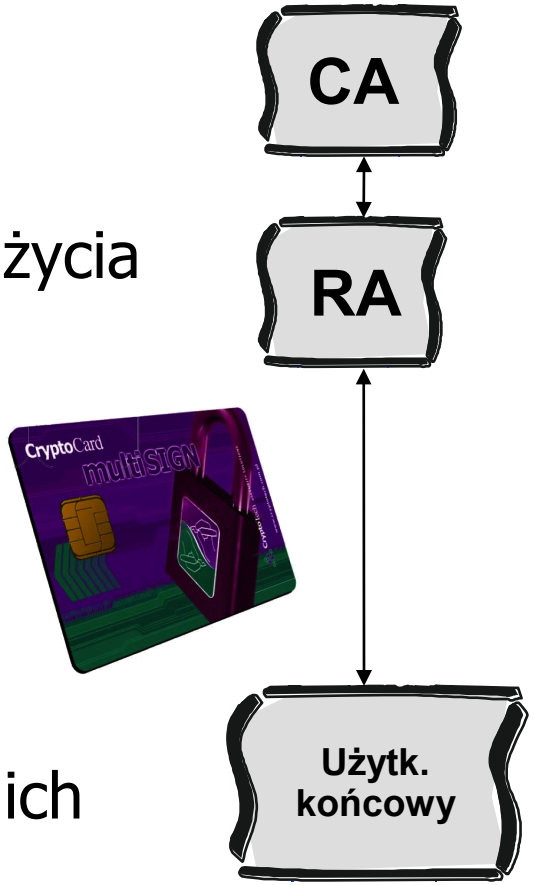
Rozwiązania - 3

- Biometria zamiast PIN
- Match On Card
- Wymaga wsparcia przez OS karty



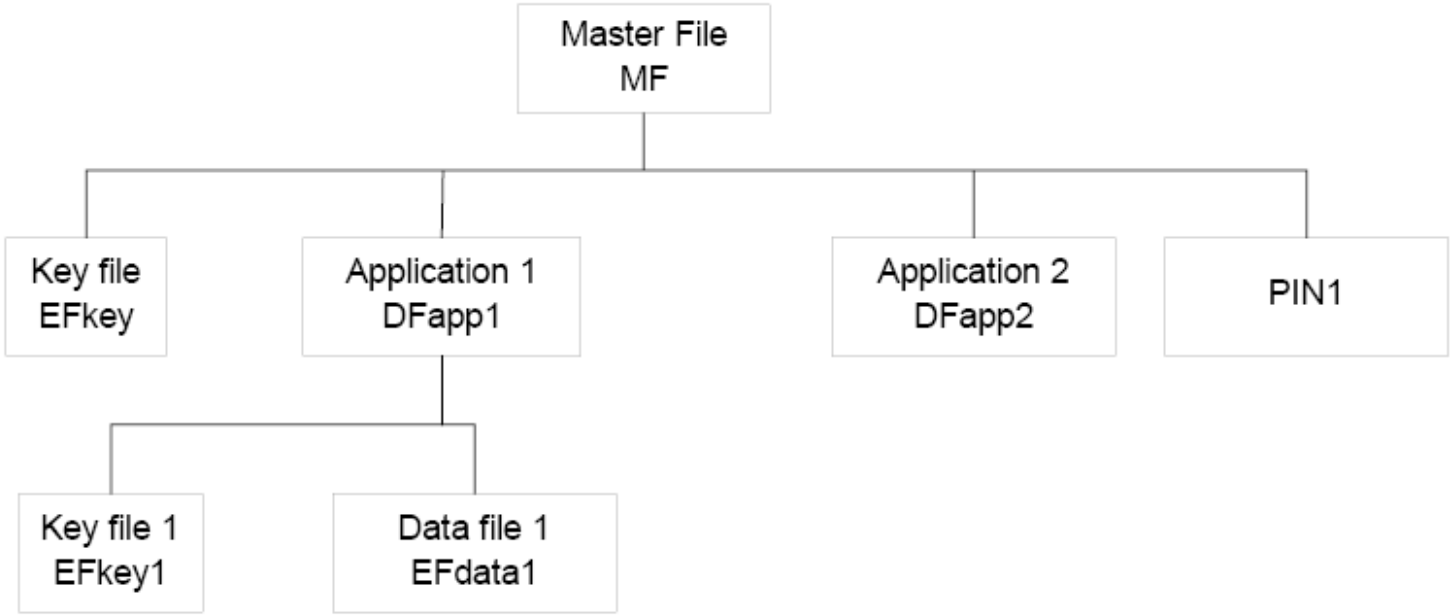
Czas życia karty

- Jak karta jest dostarczana
- Kto miał do niej dostęp i na jakim etapie życia karty
- Czy i jakie kod(y) PIN zostały zmienione
- „Zero PIN delivery” & „Initial PIN” – gwarancja że klucz nie był jeszcze użyty
- Kiedy karta przestaje być potrzebna…
- Wymaga także wprowadzenia odpowiednich procedur!



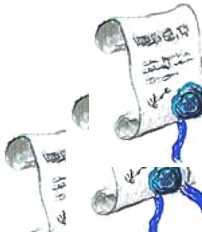
Wieloaplikacyjność

- Złe zaprojektowanie uprawnień
- Błędy OS
- JavaCard – błędy VM



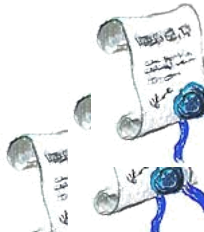
Inne problemy

- Odblokowywanie karty – PUK / PIN SO
- Wiarygodność SN
- Błędy w oprogramowaniu
  - MS CA - CRYPT_ARCHIVABLE
- What you see is what you sign?
  - Trudności z wiarogodnym wyświetlaniem zawartości
  - Makra, pola specjalne zależne od czasu lub środowiska
  - Aktywne skrypty, ‘wtyczki’
  - Brak specyfikacji formatów plików
  - Publiczne środowisko?



Mimo wszystko – karta twoim przyjacielem!

Wszystkie przedstawione problemy są niczym w porównaniu z problemami przy przechowywaniu kluczy na dyskach czy w pamięci komputerów.



Pytania…

Adam Augustyn - adam.augustyn@cryptotech.com.pl

www.cryptotech.com.pl