Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

IR EXCELLENCE IN RESEARCH

Wydział Informatyki

BEZPIECZNE OBLICZENIA OPARTE NA SPRZĘCIE I OPROGRAMOWANIU

dr hab. inż. Jerzy Pejaś, prof. ZUT

Wydział Informatyki

Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie

1

O czym będzie mowa w tym wykładzie?

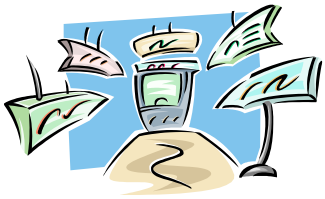
AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

1. Karty elektroniczne
2. Sprzętowe moduły kryptograficzne
3. Bezpieczne obliczenia w niezaufanych serwerach

(1) i (2) na podstawie wykładów:

W. Chocianowicz



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

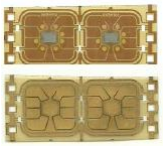
Wydział Informatyki

Karty elektroniczne

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

- Elektroniczna karta identyfikacyjna (*Integrated Circuit(s) Card – ICC*) to plastikowa karta o znormalizowanych wymiarach, zawierająca jeden (lub więcej) elektronicznych układów scalonych.
- W sensie funkcjonalnym jest to:
  - **nieulotna pamięć**;
  - podukłady umożliwiające komunikację ze światem zewnętrznym (interfejs wejścia/ wyjścia)
  - mniej lub bardziej złożone struktury sprzętowo-programowe służące do kontroli dostępu do pamięci oraz zarządzania jej zasobami.



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

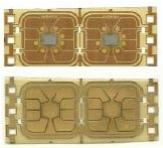
3

Karty elektroniczne

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

- Główne cechy:
  - brak wewnętrznego zasilania;
  - stosunkowo mała moc obliczeniowa;
  - pamięć jest zabezpieczona przed dostępem fizycznym, w praktyce nawet posiadając zaawansowane laboratorium trudno jest odczytać jej zawartość;
  - używana do wykonywania protokołów uwierzytelniania – karta wykonuje podpisy elektroniczne, szyfruje ciągi bajtów – sekret (klucz) nigdy nie opuszcza karty;
  - podstawowe zastosowania: identyfikacja, kontrola dostępu, płatności elektroniczne.



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

4

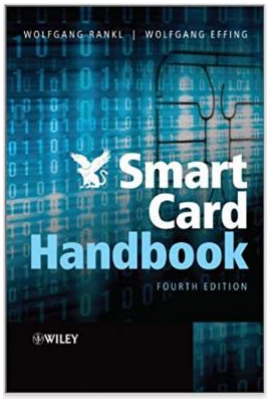
Karty elektroniczne

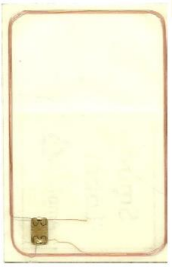
AGENDA

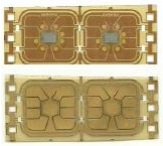
- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

Podręcznik:

W. Rankl, W. Effing, „Smart Card Handbook”







Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Krótki rys historyczny 1/4

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

- Za początek dynamicznego rozprzestrzeniania się plastikowych kart identyfikacyjnych przyjmuje się wczesne lata pięćdziesiąte ubiegłego stulecia, kiedy to taką formę trwałego identyfikatora upoważniającego do korzystania z usług związanych z płatnościami zainicjowała korporacja Diners Club. Wkrótce podążyły w jej ślady Visa i Mastercard
- Dążenie do zautomatyzowania czynności identyfikacji posiadacza karty doprowadziło do osadzenia na powierzchni karty paska magnetycznego. Niemniej jednak ostatecznym krokiem w procesie identyfikacji było złożenie podpisu na rachunku przez posługującego się kartą magnetyczną klienta.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Krótki rys historyczny 2/4

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

1968 – Niemcy - Zgłoszenie patentowe dotyczące wbudowania w plastikową kartę identyfikacyjną układu scalonego zwiększającego bezpieczeństwo danych identyfikacyjnych. Uznaje się tą datę za datę narodzin elektronicznych kart identyfikacyjnych (popularnie zwanych „smart cards”/”chip cards”).

Helmut Groettrup
1916-1981

Juergen Dethloff
1924 (Stettin) – 2002

1970 - Podobny patent w Japonii - Kunitaka Arimura.

1974 – Francja – Patent Rolanda Moreno - koncepcja umieszczenia w układzie scalonym nie tylko pamięci nieulotnej, ale także podsystemu zarządzającego dostępem do tej pamięci.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Krótki rys historyczny 3/4

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

1977 – Francja – Michel Ugon z Honeywell Bull „wynalazł” pierwszą kartę procesorową.

1983 - We Francji uruchomiono pilotażową aplikację z kartami elektronicznymi służącymi do realizacji płatności za rozmowy telefoniczne w telekomunikacji publicznej (technologia EPROM). W tym samym roku rozpoczęto podobne eksperymenty w Niemczech (technologia EEPROM).

1985 – Prezentacja pierwszej karty elektronicznej z procesorem.

1987 – 6 milionów procesorowych kart płatniczych i 25 milionów kart telefonicznych we Francji.

1991 – Giesecke & Devrient produkuje pierwsze karty SIM.

1994 - Europay, Mastercard i Visa publikują pierwszy „draft” specyfikacji standardu EMV dotyczącego kart płatniczych z układem scalonym.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Krótki rys historyczny 4/4

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

1996 – 20 milionów telefonów komórkowych z kartami SIM.

1996 – Pierwsza wersja specyfikacji PC/SC (Personal Computer/Smart Card), rozwiązania „kartowe" jako CSP (Cryptographic Service Provider).

1971 – Pierwsze posiedzenie ISO/TC 95/SC 17 „Office Machines. Credit Cards".

1987 – Opublikowana pierwsza norma dotycząca kart elektronicznych ISO 7816-1 „Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics".

1988 – Podkomitet po różnych fazach reorganizacyjnych staje się częścią ISO/IEC JTC1 („Information technology") jako SC 17 „Identification cards and related devices".

1999 – Podkomitet ISO/IEC JTC1 SC17 zmienia nazwę na „Information technology. Identification cards and personal identification".

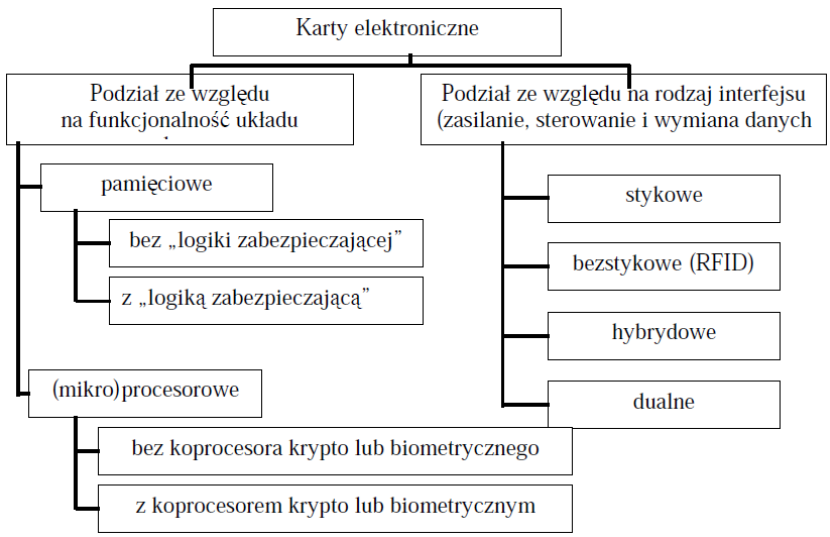
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Klasyfikacja kart elektronicznych

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Klasyfikacja kart elektronicznych

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

- **Karty stykowe** - Interfejs galwaniczny
- **Karty bezstykowe** - Wymiana danych oraz dostarczenie energii zasilającej za pośrednictwem odpowiedniej modulacji natężenia pola magnetycznego lub elektrostatycznego
- **Karty dualne („combi-cards") i hybrydowe** - Połączenie w jednej karcie dwóch technologii; oba układy niezależne („coexistent technologies") lub możliwość współpracy z tą samą pamięcią nieulotną obu układów interfejsu (reguła: odrębne „profile" praw dostępu)
- **Karty pamięciowe** - Bezpośredni dostęp do pamięci w trybie zapisu lub odczytu; dostęp przez wskazanie bezwzględnego adresu w obszarze pamięci.
- **Karty procesorowe** - Pamięć nieulotna (EEPROM, Flash) jest zorganizowana w formie drzewiastej struktury katalogów i plików (dostęp przez wybór konkretnego pliku i wskazanie „offsetu" bajtu(-ów), numeru(-ów) rekordu(-ów) lub identyfikatora(-ów) obiektu(-ów)) albo niezależnych równoległych plików aplikacyjnych (np. cardlety JavaCard).

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Klasyfikacja kart elektronicznych ze względu sposób fizycznej realizacji komunikacji

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

rodzaj kart		częstotliwość sygnału taktującego	rodzaj interfejsu	prędkość komunikacji	odległość od urządzenia interfejsowego (czytnika, IFD)
stykowe (contact)		3.57 MHz	galwaniczny	9.6 kb/s (~kilka Mb/s dla USB)	0
bezstykowe (contactless)	"klasyczne" (closed-coupled - CICC)	4.91 MHz	pojemnościowy i/lub indukcyjny	9.6 kb/s	~2 mm
	zbliżeniowe (proximity - PICC)	13.56 MHz	indukcyjne	106 kb/s	~10 cm
	dystansowe (vicinity – VICC)	13.56 MHz	indukcyjne	~10 kb/s	~70 cm
	mikrofalowe (microwave)	2.45 GHz (5.80 GHz ?)	fale radiowe	~Mb/s	kilka m

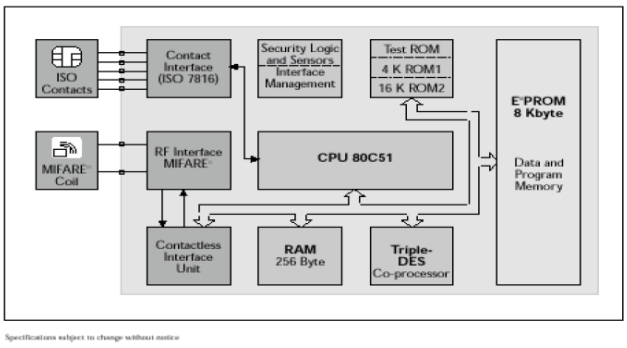
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Przykładowa architektura karty 1/2

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia



Przykład architektury sprzętowej dualnej karty procesorowej (MIFARE PRO - PHILIPS)

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

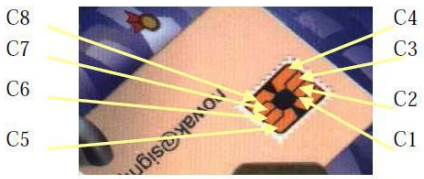
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

13

Przykładowa architektura karty 2/2

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia



Contact No.	Assignment	Contact No.	Assignment
C1	VCC (Supply voltage)	C5	GND (Ground)
C2	RST (Reset signal)	C6	VPP Variable supply voltage (e.g. programming voltage)
C3	CLK (Clock signal)	C7	I/O (Data input/output)
C4	AUX1	C8	AUX2

NOTE Insert below table 1:

In addition to the contacts assigned in this part, the contact AUX1 is assigned to function code (FCB) for type 2 synchronous cards (ISO/IEC 7816-10).

If an interface device provides a USB interface, VBUS shall be connected to VCC, D+ to AUX1 and D- to AUX2.

Przyporządkowanie styków karty elektronicznej

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

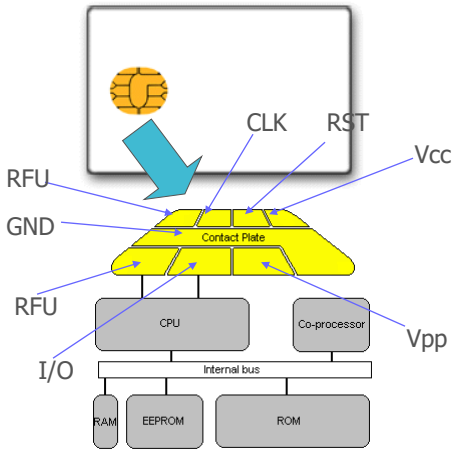
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

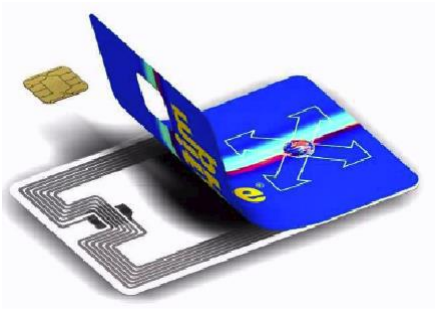
14

Co znajduje się wewnątrz karty?

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia





Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Zastosowania kart elektronicznych

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

- Karty SIM (GSM, UMTS) i telefoniczne
- Kontrola dostępu fizycznego i logicznego
- Karty płatnicze (w tym elektroniczne portmonetki)
- Karty zdrowia (pacjentów i personelu medycznego)
- Tokeny uwierzytelniające
- Podpis elektroniczny
- Obsługa głosowań
- Dokumenty, np. legitymacje studenckie, paszporty, dowody osobiste
- Karty lojalnościowe
- Karty miejskie i regionalne
- Identyfikacja bagażu, zwierząt, towarów w handlu, zasobów bibliotecznych

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Stykowe karty procesorowe

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

Zadania systemu operacyjnego karty

Procesy realizowane podczas sesji współpracy „świata zewnętrznego” z kartą:

- Dwukierunkowe przesyłanie danych (polecenia i odpowiedzi: „commands and responses”)
- Przechowywanie danych
- Przetwarzanie danych nie wymagających ochrony
- Szyfrowanie i deszyfrowanie dużych strumieni danych
- Obliczanie kryptograficznych sum kontrolnych i funkcji skrótu
- Obliczanie podpisów cyfrowych
- Obsługa protokołów uwierzytelniania wykorzystujących parametry zależne od czasu

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

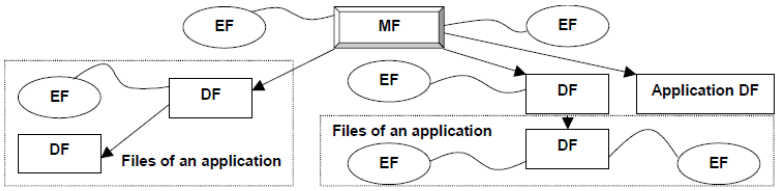
Stykowe karty procesorowe

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

Logiczna organizacja pamięci

Zasoby pamięciowe karty procesorowej zorganizowane są w formie hierarchicznej struktury drzewiastej plików...



...lub niezależnych równoległych plików aplikacyjnych:

DF może być DF aplikacyjnym z opcjonalną własną wewnętrzną hierarchią innych DF-ów oraz odpowiednią architekturą zabezpieczeń. (wg ISO/IEC 7816-4)

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

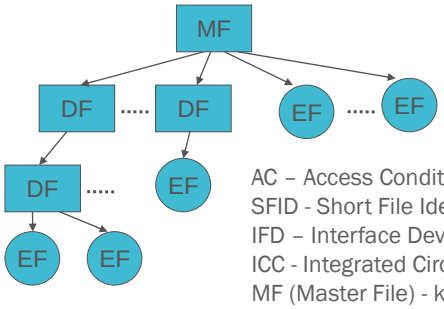
Wydział Informatyki

Stykowe karty procesorowe

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

- Dane przechowywane są na karcie w EEPROM
  - System operacyjny karty pozwalający na tworzenie i zarządzanie strukturami plikowymi



Typy plików:
- plik binarny niestrukturalizowany
- pliki z rekordami o stałej długości
- pliki z rekordami o zmiennej długości

AC – Access Condition
SFID - Short File Identifier
IFD – Interface Device
ICC - Integrated Circuit Card
MF (Master File) - korzeń drzewa katalogów - 3F.00;
DF (Dedicated File) - odpowiednik katalogu w systemach operacyjnych komputerów;
EF (Elementary File) - pliki z danymi.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

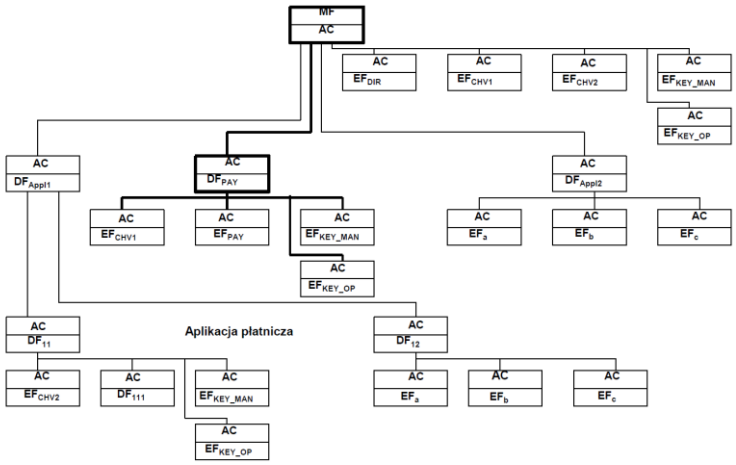
Wydział Informatyki

Stykowe karty procesorowe

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

Przykład logicznej „drzewiastej" konfiguracji zasobów pamięci karty procesorowej (wg. PN-EN-726-5)



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Stykowe karty procesorowe

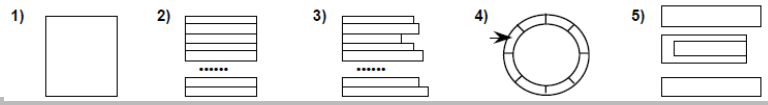
AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

Pliki elementarne dzielą się na dwie kategorie:

- pliki wewnętrzne (internal files) – przeznaczone do przechowywania danych interpretowanych wyłącznie przez system operacyjny karty (np. dla potrzeb sterowania, kontroli i zarządzania zasobami pamięciowymi);
- pliki robocze (working files) – przeznaczone do przechowywania danych nie interpretowanych przez system operacyjny karty, a więc użytkowanych wyłącznie przez „świat zewnętrzny”.

Według normy ISO/IEC 7816-4 dane w plikach elementarnych mogą być zorganizowane jako pojedyncze bajty (lub inne skwantowane porcje danych, np. słowa 16-bitowe) (pliki binarne – transparent (1)), rekordy liniowe o stałej długości lub zmiennej długości (linear with records of fixed or variable size (2, 3)), rekordy cykliczne o stałej długości (cyclic with records of fixed size (4)) lub obiekty o strukturze obiektowej zgodnej z notacją ASN.1 (TLV (5)).



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

21

Wymiana danych między kartą elektroniczną i „światem zewnętrznym”

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

- Bezpośrednio po zasileniu stykowej karty procesorowej należy wymusić tzw. „odpowiedź na reset” (ATR – Answer To Reset).
- Karta powinna odpowiedzieć sekwencją bajtów określającą obsługiwane protokoły, a także inne parametry związane z komunikacją.
- W ATR zawiera się także często informację o systemie operacyjnym (i jego wersji), producencie systemu, przeznaczeniu karty, jej możliwościach, a także stanie zasobów pamięciowych karty (karta niespersonalizowana, zablokowana całkowicie, itp.).
- Reset można także wymusić w dowolnej fazie współpracy z kartą, po to by np. zmienić protokół komunikacyjny (mechanizm Protocol and Parameters Selection - PPS).
- Komunikacja karty procesorowej ze „światem zewnętrznym” odbywa się w trybie dialogu „polecenie- odpowiedź” (command-responce).
- Stroną inicjującą dialog (wysyłającą pakiet-ramkę polecenia) jest zawsze „świat zewnętrzny”, reprezentowany przez tzw. czytnik karty elektronicznej (wbudowany w terminal).

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

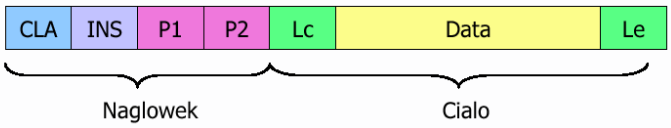
22

APDUs – Application Protocol Data Units

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

- Rozkaz APDU



- **CLA**: bajt klasy (np. ‘ 0X‘ dla ISO 7816-4/-7/-8, ‘A0‘ dla GSM)
- **INS**: bajt instrukcji
- P1: bajt parametru 1
- P2: bajt parametru 2
- Lc: długość rozkazu w bajtach (długość pola danych w rozkazie APDU)
- Le: spodziewana długość w bajtach (długość pola danych w odpowiedzi APDU, minimum: 0x00)

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

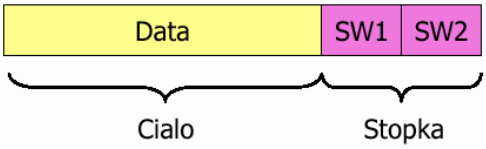
Wydział Informatyki

APDUs – Application Protocol Data Units

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

- Odpowiedz APDU



- SW1: słowo statusu (1 bajt)
- SW2: słowo statusu (2 bajty)

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

APDU – application protocol data unit

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

W warstwie transportowej sposób przesyłania zależy od rodzaju protokołu. Ramki APDU są przenoszone za pośrednictwem TPDU (transport protocol data units).

- Dla procesorowych kart stykowych najczęściej stosowane są protokoły (określone w ISO/IEC 7816-3):
- T = 0 – „starszy”, zorientowany na znaki (bajty), stosowany np. w kartach SIM;
- T = 1 – „nowszy”, zorientowany na bloki, z korekcją błędów i „łańcuchowaniem” bloków.
- Dla procesorowych kart zbliżeniowych ramki APDU przenoszone są zazwyczaj zgodnie z protokołem T= CL (wg. ISO/IEC 14443-4).

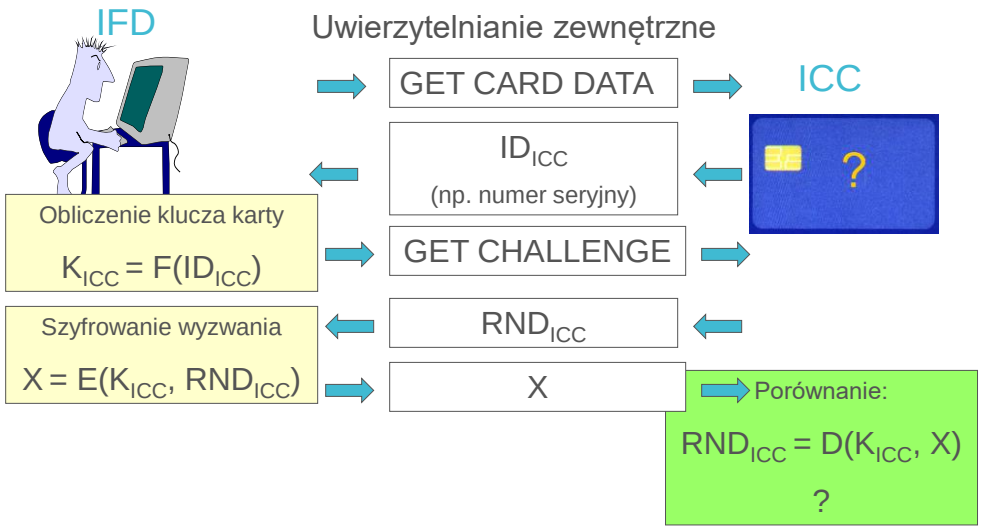
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Uwierzytelnianie za pomocą kryptografii symetrycznej

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia



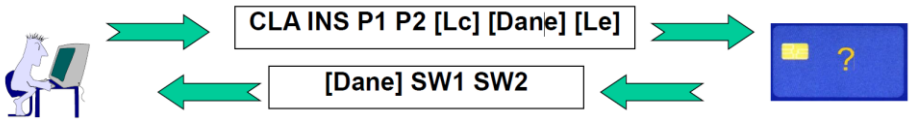
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

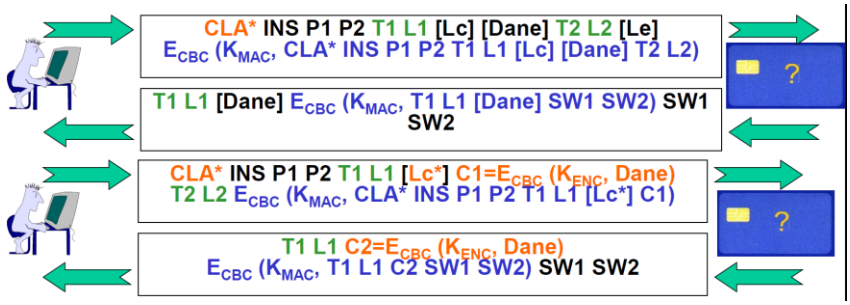
Kryptograficzna ochrona wymiany danych (SM – Secure Messaging)

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia



Niezależne klucze sesyjne do realizacji usługi poufności (K_{ENC}) i integralności (K_{MAC}) negocjowane są np. podczas procesu uwierzytelniania



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Przykłady poleceń „rozumianych” przez kartę (ISO/IEC 7816 - 4,8,9,13) 1/3

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

Zarządzanie plikami:

- CREATE FILE
- DELETE FILE
- ACTIVATE FILE
- DEACTIVATE FILE
- TERMINATE EF, DF,
- TERMINATE CARD USAGE (MF)
- SELECT FILE
- APPLICATION MANAGEMENT REQUEST
- LOAD APPLICATION
- REMOVE APPLICATION

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Przykłady poleceń „rozumianych” przez kartę (ISO/IEC 7816 - 4,8,9,13) 2/3

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

Usługi bezpieczeństwa:

- VERIFY
- EXTERNAL (/MUTUAL) AUTHENTICATE
- INTERNAL AUTHENTICATE
- GENERAL AUTHENTICATE
- GET CHALLENGE
- MANAGE SECURITY ENVIRONMENT
- PERFORM SECURITY OPERATION
- GENERATE ASYMMETRIC KEY PAIR
- RESET RETRY COUNTER

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Przykłady poleceń „rozumianych” przez kartę (ISO/IEC 7816 - 4,8,9,13) 3/3

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

Operacje PSO (PERFORM SECURITY OPERATION):

- COMPUTE CRYPTOGRAPHIC CHECKSUM
- VERIFY CRYPTOGRAPHIC CHECKSUM
- HASH
- COMPUTE DIGITAL SIGNATURE
- VERIFY DIGITAL SIGNATURE
- VERIFY CERTIFICATE
- ENCIPHER
- DECIPHER

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Sprzętowe moduły kryptograficzne

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

Moduł Kryptograficzny: wydzielony moduł sprzętowy (hardware) i/ lub programowy (software, firmware) zawierający zaimplementowane mechanizmy, procesy i/lub algorytmy kryptograficzne i umieszczony w obszarze kryptograficznym (cryptographic boundary)

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Zastosowanie modułów kryptograficznych

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

- Przechowywanie kluczy kryptograficznych i materiału kluczowego
- Szyfrowanie i deszyfrowanie danych
- Obliczanie wartości podpisów cyfrowych i ich weryfikacja
- Tworzenie logicznej zawartości tzw. tokenów dla protokołów uwierzytelniania
- Bezpieczne zarządzanie kluczami i materiałem kluczowym (dystrybucja kluczy, archiwizacja, itp.)
- Odtwarzanie sekretów podzielonych przy pomocy metod progowych, itp.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Wymagania dotyczące modułów kryptograficznych

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

- Ochrona modułu kryptograficznego przed nieuprawnionym wykorzystaniem lub działaniem
- Zapobieganie nieuprawnionemu ujawnieniu tajnych (nie publicznych) danych przechowywanych w module kryptograficznym
- Zapobieganie nieuprawnionym i/lub niewykrywalnym modyfikacjom modułu, np. nieuprawnionemu usuwaniu, zamianie lub wprowadzaniu do modułu kluczy kryptograficznych
- Właściwa implementacja algorytmów i metod kryptograficznych
- Sygnalizacja tzw. “stanu operacyjnego”
- Sygnalizacja wszelkich stanów awaryjnych i błędnych oraz uniemożliwienie wykorzystania tych stanów do ujawnienia wrażliwych danych przechowywanych w module.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Przykłady sprzętowych modułów kryptograficznych

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

- Elektroniczne karty identyfikacyjne (omówione wcześniej)
- Sprzętowe moduły bezpieczeństwa (HSMs - Hardware Security Modules)
- SAMs – Security Application Modules
- PIN-pady

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Przykład akceleratora kryptograficznego SSL/TLS

SUN Crypto Accelerator – PCIe X6000a LP Card SUN-3010-B

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

35

Przykład modułu zaprojektowanego do kryptoanalizy (1)

COPACOBANA – Cost-Optimized Parallel Code Breaker

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

S. Kumar, C. Paar, J. Pelzl, G. Pfeiffer i M. Schimmler „Breaking Ciphers with COPACOBANA - A Cost-Optimized Parallel Code Breaker" (CHES 2006),

March 15, 2007: Duration of brute-force attack against DES is less than a week

With further optimization of our implementation, we could achieve a clock frequency of 136MHz for the brute fore attack with COPACOBANA. Now, the average search time for a single DES key is **less than a week**, precisely 6.4 days. The worst case for the search has been reduced to 12.8 days now.

https://www.copacobana.org/photos/photo_v1.jpg

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

36

Przykład modułu zaprojektowanego do kryptoanalizy (2)

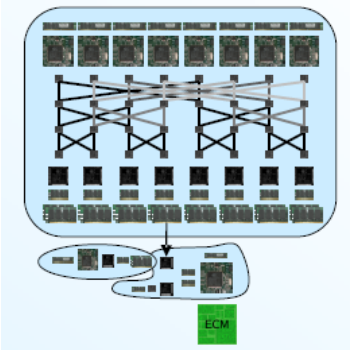
AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

SHARK - A Realizable Special Hardware Sieving Device for Factoring 1024-bit Integers

EDIZONE GmbH, Uni Bochum, Uni Bonn (SHARCS Workshop, 2005)

Krok przesiewania algorytmu sita ogólnego ciała liczbowego (GNFS) dla 1024-bitowej liczby całkowitej w ciągu roku o kosztach poniżej 200 milionów $.



- 2300 identycznych „maszyn”
- małe specjalizowane układy ASIC
- standardowy RAM
- architektura modularna
- konwencjonalne szyny danych

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Dokumenty normatywne wykorzystywane w ocenie modułów kryptograficznych

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

FIPS PUB 140-2:2001 - „Security requirements for cryptographic modules”

Poziomy bezpieczeństwa 1-4

- Nadchodzi nowa wersja FIPS 140-3

ISO/IEC 15408 - „Information technology - Security techniques - Evaluation criteria for IT security” (Common Criteria - CC)

Protection Profiles (PP), Targets of Evaluation (TOE), Evaluated Assurance Levels (EAL 1-7)

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

FIPS PUB 140-2 - wymagania (1/4)

	Poziom 1	Poziom 2	Poziom 3	Poziom 4
Specyfikacja modułu	Specyfikacja modułu kryptograficznego, obszaru kryptograficznego, zatwierdzonych algorytmów i zatwierdzonych trybów działania. Opis modułu kryptograficznego obejmujący wszystkie komponenty hardware'owe, software'owe i firmware'owe. Określenie polityki bezpieczeństwa dla modułu.			
Porty i interfejsy modułu	Interfejsy obligatoryjne i opcjonalne. Specyfikacja wszystkich interfejsów i wszystkich ścieżek wejściowych i wyjściowych dla danych.		Porty danych dla niechronionych parametrów bezpieczeństwa logicznie lub fizycznie oddzielone od innych portów danych.	
Role, usługi i uwierzytelnianie	Logiczne oddzielenie obligatoryjnych i opcjonalnych ról i usług.	Uwierzytelnianie operatora oparte na rolach lub tożsamości.	Uwierzytelnianie operatora oparte na rolach lub tożsamości.	
Model „skończonej" maszyny stanu	Specyfikacja modelu „skończonej" maszyny stanu. Stany obligatoryjne i opcjonalne. Diagram przejść między stanami oraz specyfikacja tych przejść.			

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

39

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

FIPS PUB 140-2 - wymagania (2/4)

	Poziom 1	Poziom 2	Poziom 3	Poziom 4
Bezpieczeństwo fizyczne (*doprecyzowane dalej dla różnych konfiguracji sprzętowych*)	Sprzęt o właściwościach typowych dla produkcji masowej.	Pojedynczy operator. Kod wykonywalny. Zatwierdzona technika kontroli integralności.	Wykrywanie manipulacji i reakcja na nie dla obudowy i zamykanych otworów dostępowych.	Wykrywanie manipulacji i reagująca na nie powłoka. EFP (*Environmental failure protection*) lub EFT (*Environmental failure testing*).
Środowisko operacyjne	Pojedynczy operator. Kod wykonywalny. Zatwierdzona technika kontroli integralności.	Referencyjne PP na poziomie EAL2 z określonymi mechanizmam i uznaniowej kontroli dostępu (DAC) oraz audytem.	Referencyjne PP + zaufana ścieżka na poziomie EAL3 + modelowanie polityki bezpieczeństwa	Referencyjne PP + zaufana ścieżka na poziomie EAL4.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

40

FIPS PUB 140-2 - wymagania (3/4)

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

	Poziom 1	Poziom 2	Poziom 3	Poziom 4
Zarządzanie kluczami kryptograficznymi	Mechanizmy zarządzania kluczami: generowanie liczb (bitów) losowych i kluczy, ustanawianie kluczy, dystrybucja kluczy, wprowadzanie/wyprowadzanie kluczy, przechowywanie kluczy i ich zerowanie.			
	Klucze tajne i prywatne ustanawiane za pomocą metod ręcznych można wprowadzać i wyprowadzać w postaci jawnej.		Klucze tajne i prywatne ustanawiane za pomocą metod ręcznych muszą być wprowadzane i wyprowadzane w postaci zaszyfrowanej lub z wykorzystaniem metod podziału wiedzy (metody progowe).	
EMI/EMC (Electromagnetic Interference /Compatibility)	47 CFR FCC Część 15. Podczęść B, Klasa A (Użytek biznesowy). Mają zastosowanie wymagania FCC (dla technik radiowych).		47 CFR FCC Część 15. Podczęść B, Klasa B (Użytek domowy).	
Testy auto-diagnostyczne	Testy podczas włączania zasilania: testy algorytmów kryptograficznych, testy integralności oprogramowania (software/firmware), testy funkcji krytycznych. Testy warunkowe.			

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

41

FIPS PUB 140-2 - wymagania (4/4)

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

	Poziom 1	Poziom 2	Poziom 3	Poziom 4
Wiarygodność projektowania	Zarządzanie konfiguracją (CM). Bezpieczna instalacja i tworzenie. Zgodność projektu z polityką. Dokumenty o charakterze instrukcji.	System CM. Bezpieczna dystrybucja. Specyfikacja funkcjonalna.	System CM. Bezpieczna dystrybucja. Specyfikacja funkcjonalna.	Model formalny. Szczegółowe uzasadnienia projektowe (dowody nieformalne). Warunki wstępne i po implementacji.
Łagodzenie skutków innych ataków	Specyfikacja łagodzenia skutków ataków, dla których aktualnie nie są dostępne testowalne wymagania.			

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

42

FIPS PUB 140-2 - wymagania (4/4)

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

	Poziom 1	Poziom 2	Poziom 3	Poziom 4
Wiarygodność projektowania	Zarządzanie konfiguracją (CM). Bezpieczna instalacja i tworzenie. Zgodność projektu z polityką. Dokumenty o charakterze instrukcji.	System CM. Bezpieczna dystrybucja. Specyfikacja funkcjonalna.	System CM. Bezpieczna dystrybucja. Specyfikacja funkcjonalna.	Model formalny. Szczegółowe uzasadnienia projektowe (dowody nieformalne). Warunki wstępne i po implementacji.
Łagodzenie skutków innych ataków	Specyfikacja łagodzenia skutków ataków, dla których aktualnie nie są dostępne testowalne wymagania.			

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

43

FIPS PUB 140-2 - bezpieczeństwo fizyczne (1/2)

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

	Wymagania ogólne	Jeden układ scalony	Wiele wbudowanych układów scalonych	Wiele układów scalonych w samodzielnym module
Poziom 1	**Elementy o właściwościach typowych dla produkcji masowej (ze standardową pasywacją).**	Brak wymagań dodatkowych.	Obudowa i usuwalna pokrywa o właściwościach typowych dla produkcji masowej (jeżeli są stosowane).	Obudowa o właściwościach typowych dla produkcji masowej.
Poziom 2	**Ujawnianie manipulacji (np. pokrywa, obudowa lub pieczęć).**	Nieprzezroczysta, ujawniająca manipulacje powłoka na układzie lub obudowie.	Nieprzezroczysta, ujawniająca manipulacje powłoka/obudowa lub blokady antywłamaniowe dla drzwiczek i zdejmowalnych pokryw.	Nieprzezroczysta, ujawniająca manipulacje powłoka lub blokady antywłamaniowe dla drzwiczek i zdejmowalnych pokryw.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

44

FIPS PUB 140-2 - bezpieczeństwo fizyczne (2/2)

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

	Wymagania ogólne	Jeden układ scalony	Wiele wbudowanych układów scalonych	Wiele układów scalonych w samodzielnym module
Poziom 3	**Ujawnianie manipulacji (np. pokrywa, obudowa lub pieczęć).**	Nieprzezroczysta, ujawniająca manipulacje powłoka na układzie lub mocna obudowa odporna na usunięcie i penetrację.	Nieprzezroczysta obudowa obwodu z wieloma układami lub rozwiązania zgodne z wymaganiami poziomu 3 dla wielu układów scalonych w samodzielnym module.	Nieprzezroczysta obudowa obwodu z wieloma układami lub mocna obudowa doznająca poważnych uszkodzeń podczas prób usunięcia/ penetracji.
Poziom 4	**EFP lub EFT dla temperatury i napięcia.**	Nieprzezroczysta, odporna na usunięcie powłoka układu.	Pokrywa wykrywająca manipulacje oraz obwód reagujący na nie i zerujący pamięć.	Pokrywa wykrywająca i reagująca na manipulacje oraz obwód reagujący na nie i zerujący pamięć.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

FIPS PUB 140-2 – wymagania dla systemu operacyjnego

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

- Jeżeli moduł kryptograficzny nie jest "zamknięty" w sensie programowym, tzn. operator może załadować do modułu pewne fragmenty "kodów wykonywalnych" (dotyczy to zwłaszcza programowych modułów kryptograficznych uruchamianych na "zwykłych" samodzielnych komputerach, serwerach i sieciowych stacjach klienckich), to wówczas ocenie podlega również bezpieczeństwo systemu operacyjnego współpracującego z modułem.
- Szczególnie wnikliwie powinny być w takim przypadku przeanalizowane możliwości "niezamierzonej" i "zamierzonej" penetracji zasobów pamięciowych modułu kryptograficznego przez innych operatorów lub procesy.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

PKCS #11: Cryptographic Token Interface Standard (1/4)

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

- Specyfikacja (standard de facto) określająca kryptograficzny interfejs programowy (CAPI) dla „urządzeń” przechowujących dane kryptograficzne i wykonujących operacje kryptograficzne.
- Interfejs nosi nazwę własną CRYPTOKI.
- Umożliwia uzyskanie interfejsu niezależnego od „urządzenia” oraz umożliwiającego współdzielenie zasobów (wiele aplikacji komunikujących się z wieloma „urządzeniami” jednocześnie) widzianych jako logiczne urządzenie, zwane „tokenem kryptograficznym”.
- Specyfikacja odwołuje się do notacji ASN.1 i specyfikacji ANSI C.
- Aktualna wersja to OASIS PKCS #11 v2.40:

http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/os/pkcs11-base-v2.40-os.html

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

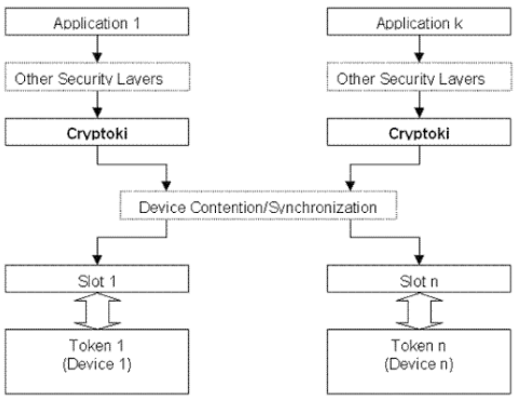
Wydział Informatyki

PKCS #11: Cryptographic Token Interface Standard (2/4)

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

Model ogólny CRYPTOKI



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

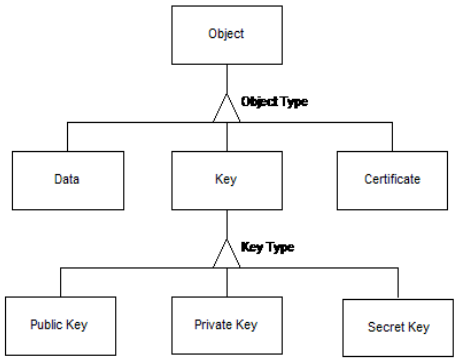
Wydział Informatyki

PKCS #11: Cryptographic Token Interface Standard (3/4)

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

- Token w Cryptoki na poziomie logicznym jest widziany jako urządzenie, które przechowuje obiekty i może wykonywać funkcje kryptograficzne.
- Cryptoki definiuje trzy klasy obiektów: Dane, Certyfikaty i Klucze.
- Obiekt danych jest definiowany przez aplikację.
- Obiekt certyfikatu przechowuje certyfikat klucza publicznego.
- Obiekt klucza przechowuje klucz szyfrowania. Kluczem szyfrującym może być klucz publiczny (RSA, DSA lub Diffie-Hellman), klucz prywatny (RSA, DSA lub Diffie-Hellman) lub klucz tajny (RC2, RC4, DES itp.).



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

PKCS #11: Cryptographic Token Interface Standard (4/4)

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

- Określa się dwie kategorie użytkowników interfejsu:
  - Security Officers (SO),
  - zwykli użytkownicy.
- Aplikacja może otworzyć jedną lub wiele sesji komunikacyjnych z tokenem;
- Każda z sesji może być w trybie R/O (Read Only) lub R/W (Read/Write), zaś wybór trybu decyduje o możliwościach manipulacji obiektami w tokenie.
- Dopóki użytkownik się nie zaloguje, to otwarta sesja ma charakter publiczny.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Bezpieczne obliczenia w niezaufanych serwerach

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

- W przypadku gdy istnieje konieczność wykonania dużej liczby obliczeń, które łatwo zrównoleglić można do tego wykorzystać chmurę obliczeniową (serwery zewnętrzne).
- Gdy obliczenia nie mogą być publiczne to chmura musi być prywatna (pod kontrolą osoby wykonującej obliczenia)
- Jednak możliwe jest wykonywanie obliczeń których argumenty i wynik muszą być prywatne z zachowaniem dwóch warunków:
  1. Niezaufana chmura (serwer) nie mogą poznać przetwarzanych danych
  2. Podmiot zlecający obliczenia musi mieć możliwość weryfikacji rezultatu obliczeń

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Bezpieczne obliczenia w niezaufanych serwerach

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

Typy chmur pod względem zaufania:

- chmura zaufana - zaufana chmura nie odbiega od swojej deklarowanej funkcjonalności (również zachowuje prywatność danych).
- złośliwa chmura (malicious cloud) - złośliwa chmura to skorumpowana chmura, który może arbitralnie odbiegać od deklarowanej funkcjonalność (jest aktywnym przeciwnikiem).
- częściowo-uczciwa chmura (semi-honest or honest-but-curious cloud) – chmura ta nie odbiega od swojej deklarowanej funkcjonalności, ale zapisuje wszystkie informacje które powinny zostać prywatne (jest pasywnym przeciwnikiem).
  - Ten typ odpowiada zwykle publicznym chmurom, które mogą kłamać w aspekcie jakości ich usług oraz nie można zweryfikować, czy chmura jest bezpieczna (trzeba zaufać deklaracji dostawcy).

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Bezpieczne obliczenia w niezaufanych serwerach

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

Przypadek użycia:

- Urząd skarbowy w państwie X wymaga podpisu elektronicznego w każdej elektronicznej deklaracji.
- Podatnicy wysyłają różne formularze w ciągu roku do urzędu z tytułu rozliczeń VAT. Jednakże, w każdym miesiącu jest wyznaczony termin ostateczny. W tym okresie liczba formularzy podatkowych otrzymanych przez urząd skarbowy w przeliczeniu na minutę wzrasta stukrotnie.
- Urząd wykorzystuje outsourcing obliczeniowy do obsługi zwiększonej liczby obliczeń (głównie weryfikacji podpisów cyfrowych). Dzięki temu nie jest konieczne posiadanie dodatkowych serwerów, które w pozostałym okresie byłyby bezczynne.
- Urząd musi stosować techniki kryptograficzne gwarantujące bezpieczeństwo informacji, ze względu na wrażliwy charakter informacji znajdujących się w deklaracjach podatkowych.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Bezpieczne obliczenia w niezaufanych serwerach

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

Model wg Hohenberger and Lysyanskaya (uproszczona wersja):

- Algorytm Alg. dzielimy na dwie części T (wykonywana lokalnie przez serwer S) i U (wykonywana w chmurze C);
- Kroki działania:
  1. Serwer S wykonuje T i dodatkowo wykonuje obliczenia zaciemniające argumenty wysłane do C konieczne do wykonanie drugiej części algorytmu U.
  2. Chmura C wykonuje część algorytmu U i zwraca rezultat do S.
  3. S wykonuje na rezultacie otrzymanym od C obliczenia pozwalające mu sprawdzić czy wynik jest poprawny.

Hohenberger S., Lysyanskaya A. (2005) How to Securely Outsource Cryptographic Computations. In: Kilian J. (eds) Theory of Cryptography. TCC 2005. Lecture Notes in Computer Science, vol 3378. Springer, Berlin, Heidelberg

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Bezpieczne obliczenia w niezaufanych serwerach

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

Podstawowe właściwości:

- Efektywność – mierzymy poprzez porównanie czasu wykonanie algorytmu Alg. lokalnie oraz z użyciem chmury; efektywne algorytmy wykonują się szybciej z użyciem chmury.
  - Czasami wykorzystuje się nieefektywne algorytmy, gdyż w ten sposób nie trzeba implementować wszystkich obliczeń na S – np. gdy S to karta elektroniczna to nie trzeba na niej obliczać odwzorowań dwuliniowych.
- Weryfikowalność – stopień prawdopodobieństwa z jakim serwer może zweryfikować, czy wynik otrzymany od serwerów jest poprawny; gdy wynosi 1 to zawsze sprawdzenie zwraca rezultat poprawny, a gdy np. 0.5 to mamy prawdopodobieństwo 50%, że rezultat sprawdzenia jest poprawny.
- Prywatność – chmura nie pozna przesłanych jej argumentów; czasami rezygnujemy z prywatności, gdyż wystarczy tylko możliwość weryfikacji poprawności.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Bezpieczne obliczenia w niezaufanych serwerach

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

Przykład algorytmu (efektywność < 1, weryfikowalność = 1):

The card and the terminal are given as input a description of the groups $\mathcal{G}_1$, $\mathcal{G}_2$ and $\mathcal{G}_T$, and a description of the bilinear map $e : \mathcal{G}_1 \times \mathcal{G}_2 \rightarrow \mathcal{G}_T$. The card and the terminal receive the generators G_1 and G_2; we also assume that the card receives $e(G_1, G_2)$. The card is given as input the points A and B and must eventually output $e(A, B)$. Recall that $\mathcal{G}_1$, $\mathcal{G}_2$ and $\mathcal{G}_T$ are additive groups of order p.

1. The card generates a random $g_1 \in \mathbb{Z}_p$ and a random $g_2 \in \mathbb{Z}_p$, and queries the three following pairings to the terminal :

$$\alpha_1 = e(A + g_1.G_1, G_2), \quad \alpha_2 = e(G_1, B + g_2.G_2)$$

$$\alpha_3 = e(A + g_1.G_1, B + g_2.G_2)$$

2. The card checks that $\alpha_1, \alpha_2, \alpha_3 \in \mathcal{G}_T$, by checking that $(\alpha_i)^p = 1$ for $i = 1, 2, 3$. Otherwise, the card outputs $\perp$ and halts.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Bezpieczne obliczenia w niezaufanych serwerach

AGENDA

- Karty elektroniczne
- Sprzętowe moduły kryptograficzne
- Bezpieczne obliczenia

3. The card computes a purported value for $e(A, B)$:

$$e_{AB} = \alpha_1^{-g_2} \cdot \alpha_2^{-g_1} \cdot \alpha_3 \cdot e(G_1, G_2)^{g_1 g_2} \quad (1)$$

4. The card generates four random values $a_1, r_1, a_2, r_2 \in \mathbb{Z}_p$ and queries the pairing :

$$\alpha_4 = e(a_1.A + r_1.G_1, a_2.B + r_2.G_2)$$

5. The card computes :

$$\alpha'_4 = (e_{AB})^{a_1 a_2} \cdot (\alpha_1)^{a_1 r_2} \cdot (\alpha_2)^{a_2 r_1} \cdot e(G_1, G_2)^{r_1 r_2 - a_1 g_1 r_2 - a_2 g_2 r_1} \quad (2)$$

and checks that $\alpha'_4 = \alpha_4$. In this case, the card outputs e_{AB}; otherwise it outputs $\perp$.

Chevallier-Mames B., Coron JS., McCullagh N., Naccache D., Scott M. (2010) Secure Delegation of Elliptic-Curve Pairing. In: Gollmann D., Lanet JL., Iguchi-Cartigny J. (eds) Smart Card Research and Advanced Application. CARDIS 2010. Lecture Notes in Computer Science, vol 6035. Springer, Berlin, Heidelberg

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

IIR EXCELLENCE IN RESEARCH

DZIĘKUJĘ ZA UWAGĘ

Wydział Informatyki