



Nowe karty wieloaplikacyjne

Autor: | Agnieszka Dąbrowska



**II Krajowa Konferencja Użytkowników
Systemów Elektronicznej Legitymacji Studenckiej
Poznań 10.06.2010**



Plan prezentacji

- ↓ Nowe karty wieloaplikacyjne
- ↓ Dostępne interfejsy kart i ich zastosowanie
 - ↓ Stykowy
 - ↓ Bezstykowy
 - ↓ ISO,
 - ↓ Mifare.
- ↓ Rodzaje kart
 - ↓ Karty natywne,
 - ↓ Karty Java Card,
- ↓ Certyfikacja produktów kartowych
- ↓ Oferta Oberthur
 - ↓ Karty + oprogramowanie middleware
 - ↓ Narzędzia deweloperskie



Dostępne interfejsy kart i ich zastosowanie

Interfejs stykowy

- ↓ ISO 7816
- ↓ Protokół komunikacji T=0, T=1



Interfejs bezstykowy

- ↓ T=CL
 - ↓ Dostępne komendy APDU Case 4
 - ↓ Brak różnic z interfejsem stykowym (ISO 7816) na poziomie komend APDU
 - ↓ Dwa alternatywne standardy: Type A oraz Type B
- ↓ Mifare
 - ↓ Przechowywanie danych oraz proste operacje arytmetyczne
 - ↓ Protokół poziomej Aplikacji
 - ↓ Brak możliwości wysyłania komend APDU przez Mifare
 - ↓ Niektóre karty T=CL Type A mogą emulować Mifare

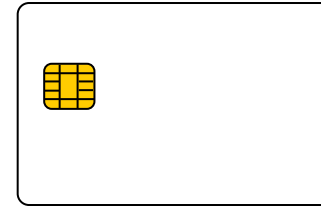




Dostępne interfejsy kart i ich zastosowanie

↓ Karta stykowa

- ↓ Jeden mikroprocesor osadzony wraz z płytką kontaktową na karcie
- ↓ Pracuje wyłącznie w trybie STYKOWYM



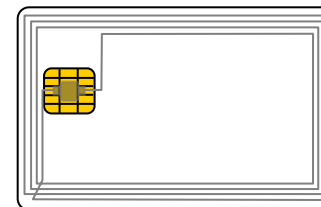
↓ Karta bezstykowa

- ↓ Jeden mikroprocesor podłączony do anteny i zatopiony w plastiku
- ↓ Pracuje wyłącznie w trybie BEZSTYKOWYM



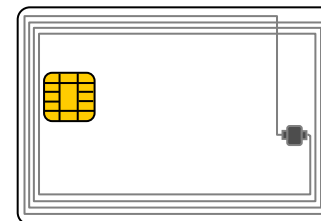
↓ Karta dualna

- ↓ Jeden mikroprocesor osadzony wraz z anteną i płytką kontaktową na karcie
- ↓ Pracuje w trybie BEZSTYKOWYM oraz STYKOWYM



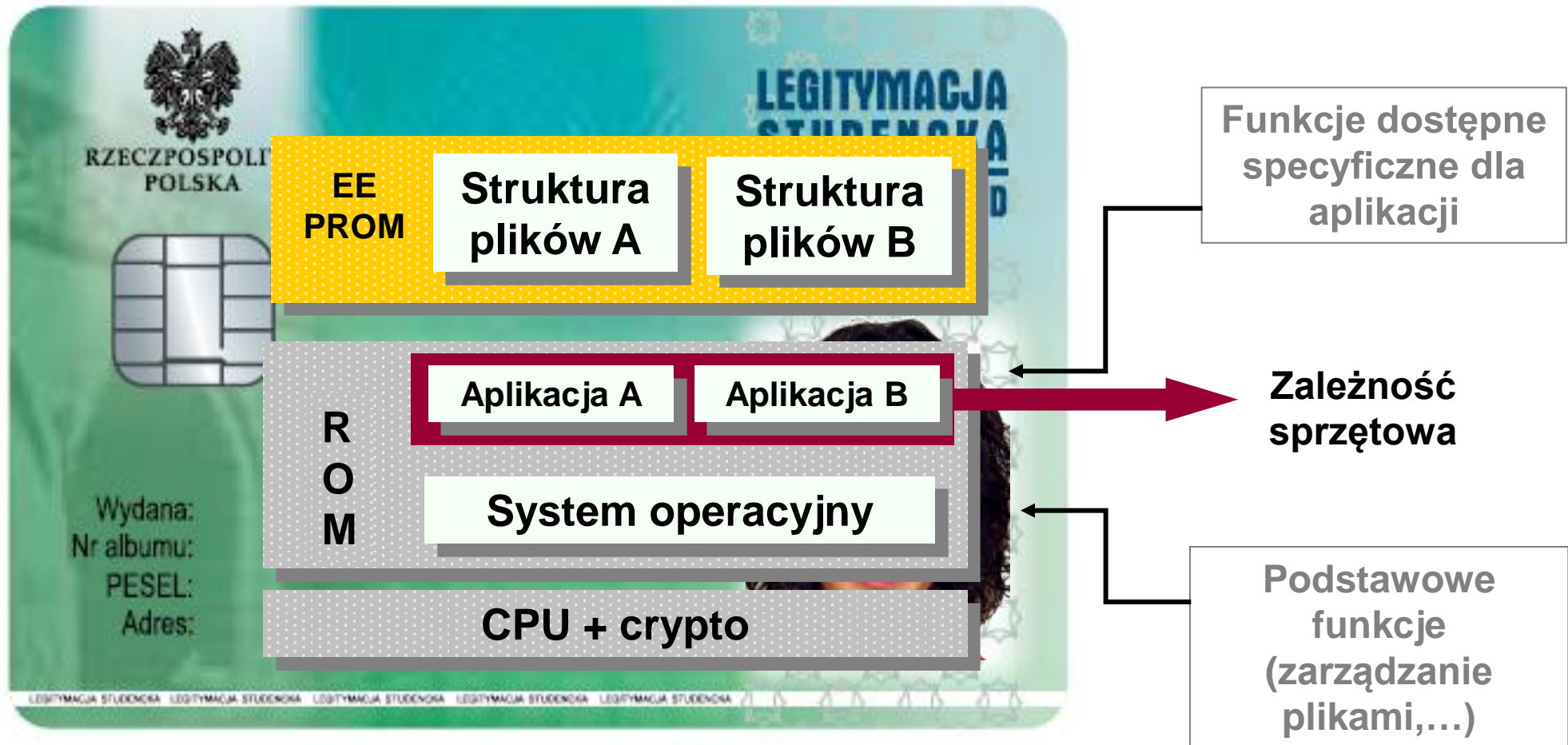
↓ Karta hybrydowa

- ↓ DWA niezależne mikroprocesory bez połączenia między nimi
 - ↓ jeden osadzony wraz z płytką kontaktową na karcie, pracujący wyłącznie w trybie STYKOWYM
 - ↓ drugi połączony z anteną zatopiony w plastiku pracujący wyłącznie w trybie BEZSTYKOWYM





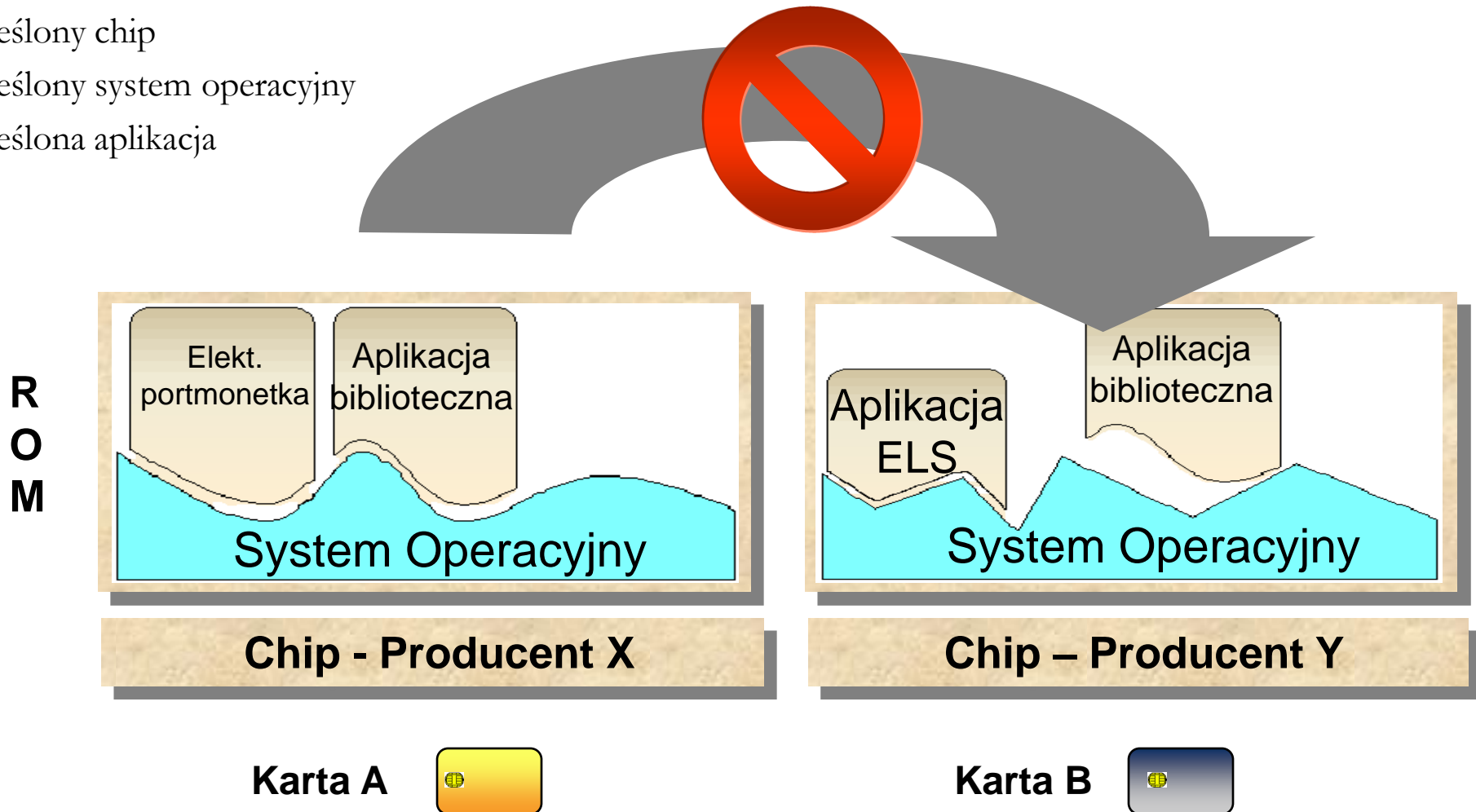
Rodzaje kart – karta natywna





Rodzaje kart – karta natywna

- ↓ Określony chip
- ↓ Określony system operacyjny
- ↓ Określona aplikacja





Rodzaje kart – karta natywna

Ograniczenia

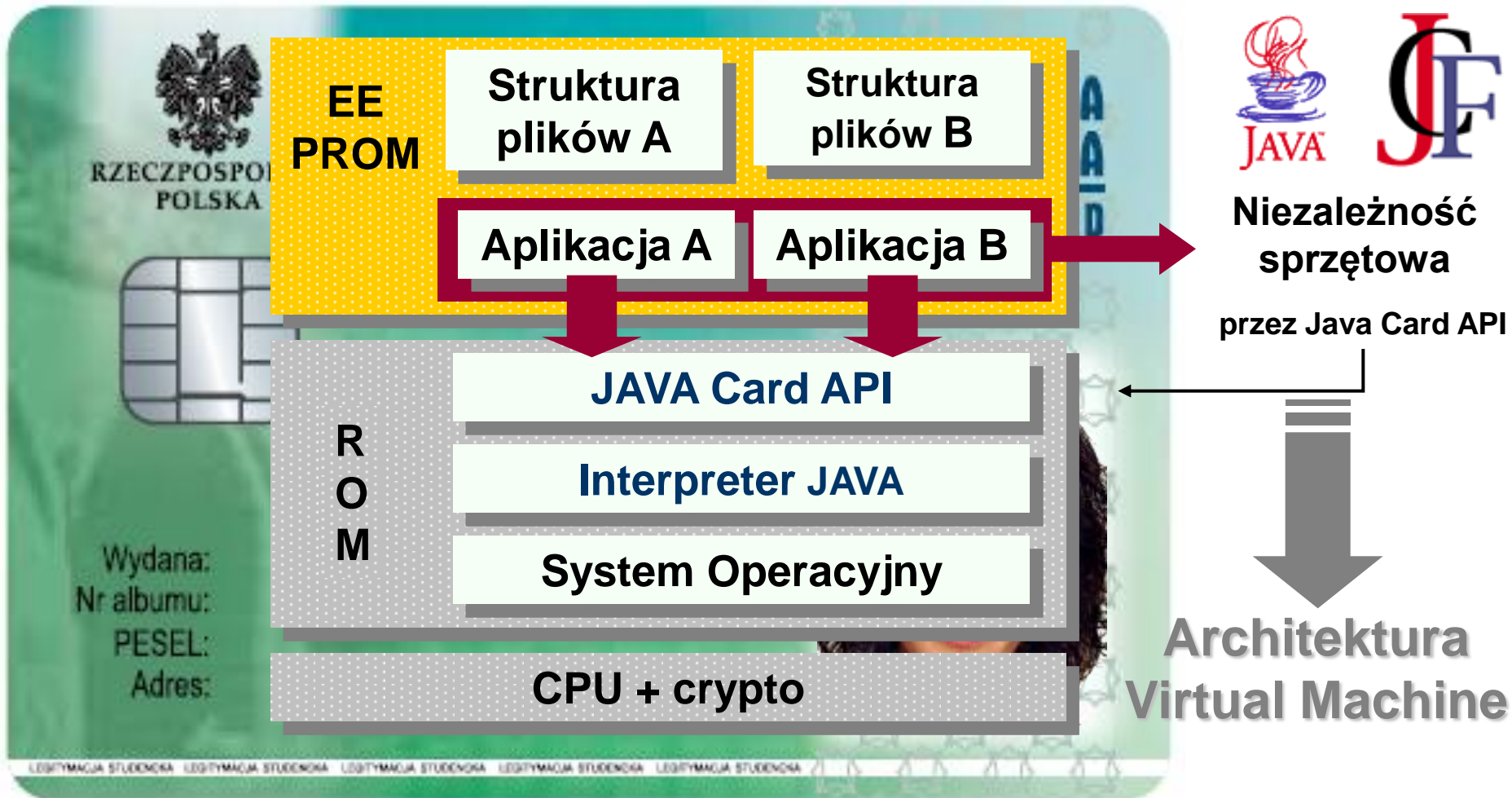
- ↓ Development jest skomplikowany oraz czasochłonny
- ↓ Zastosowanie nowego chipa/karty oznacza przepisanie/adaptację aplikacji
- ↓ Większość kart zawiera jedną (wcześniej przygotowaną) aplikację
- ↓ Brak funkcjonalności post-issuance:
 - ↓ Dogranie nowej aplikacji oznacza ponowne wydanie karty
 - ↓ Dostarczenie nowych usług po wydaniu karty jest ograniczone lub niemożliwe

Zalety

- ↓ Bardziej efektywna w zakresie szybkości działania
- ↓ Podobna funkcjonalność (ale ograniczenia post-issuance)
- ↓ Mniejsza cena

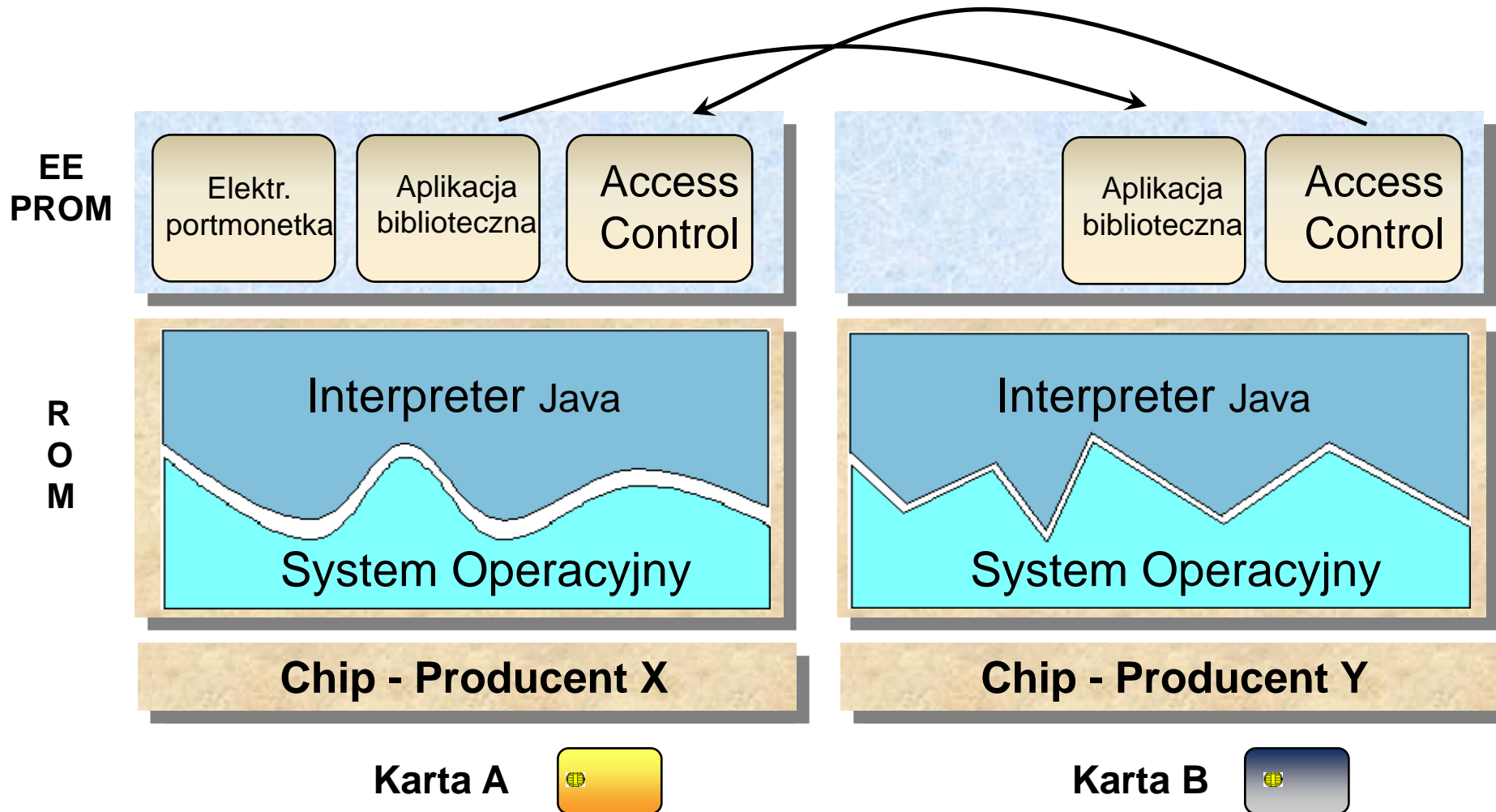


Rodzaje kart – karta Java





Rodzaje kart – karta Java





Rodzaje kart – karta Java

Zalety

- ↓ Koszty szkolenia programistów
- ↓ Dostępne narzędzia deweloperskie
- ↓ Szeroko używany język programowania
- ↓ Przenoszalność kodu Java

- ↓ Wiele usług na jednej karcie
- ↓ Dodawanie funkcjonalności możliwe również w trakcie „życia” karty
- ↓ Czas wdrożenia krótszy

Ograniczenia

- ↓ Wymagane więcej pamięci RAM
- ↓ Zasady bezpieczeństwa dotyczące ładowania, kasowania aplikacji zależne są od producenta karty
- ↓ Niektóre aplikacje mogą nie przenosić się (wykorzystujące Proprietary API producenta karty)

GLOBALPLATFORM
ADVANCING STANDARDS FOR SMART CARD GROWTH





Certyfikacja

↓ Co to jest certyfikat ?

Standard ewaluacji produktów kartowych oraz aplikacji. Określa wymagania funkcji bezpieczeństwa oraz miary zabezpieczeń.

↓ Jakiego rodzaju certyfikaty wymagane są na polu kart identyfikacyjnych z cyfrowym podpisem?

↓ **FIPS 140-2** -> ewaluacja modułów kryptograficznych

↓ **FIPS 201** -> PIV (Personal Identity Verification) ewaluacja

↓ **Common Criteria (EAL4+, EAL5+)** -> kryptografia + fizyczne zabezpieczenia obszaru deweloperskiego

↓ Jak sprawdzić czy dany produkt posiada certyfikację ?

↓ **FIPS140:** <http://csrc.nist.gov/cryptval/140-1/1401vend.htm>

↓ **FIPS201:** <http://fips201ep.cio.gov/apl.php>

↓ **Common Criteria:** <http://www.commoncriteriaportal.org/products.html>

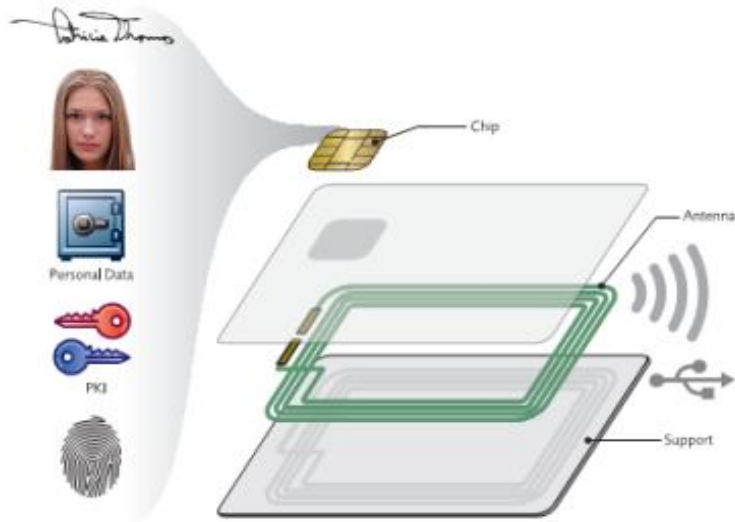




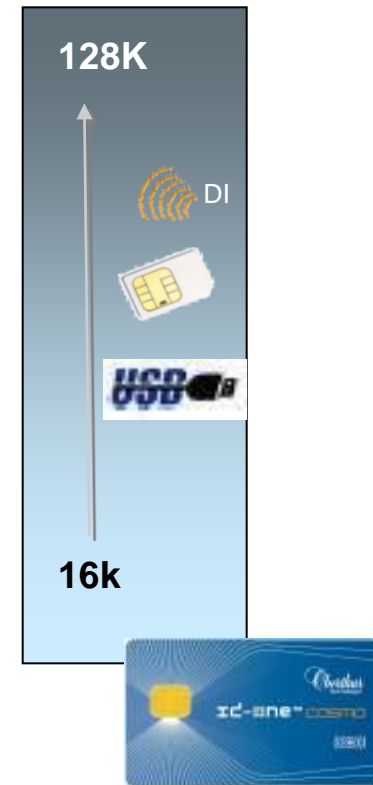
Oferta produktowa

id-:ne

COSMO to rozwiązanie oparte na systemie operacyjnym **Java OS**



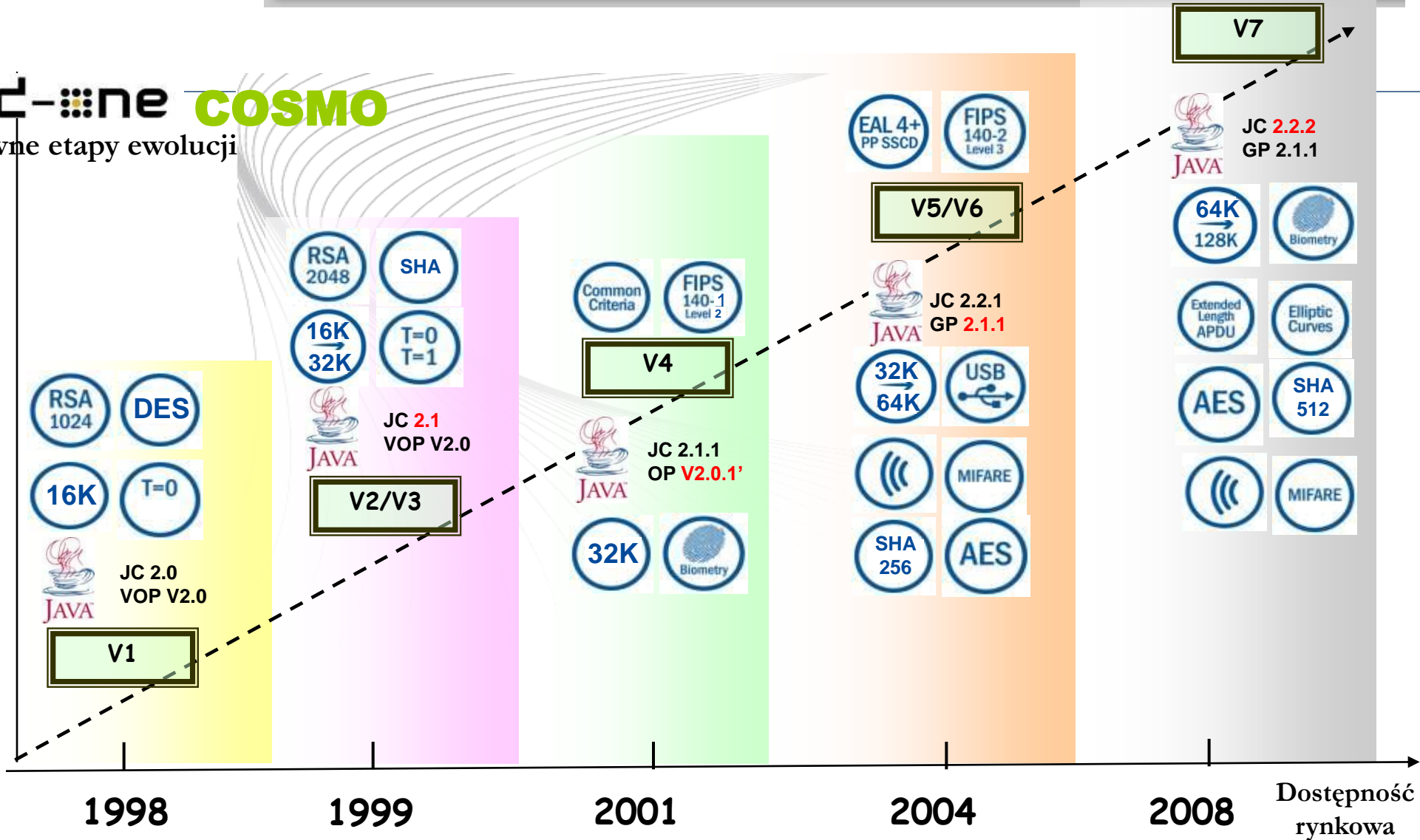
Rozwiązanie wielozadaniowe





IC-:ne COSMO

Główne etapy ewolucji





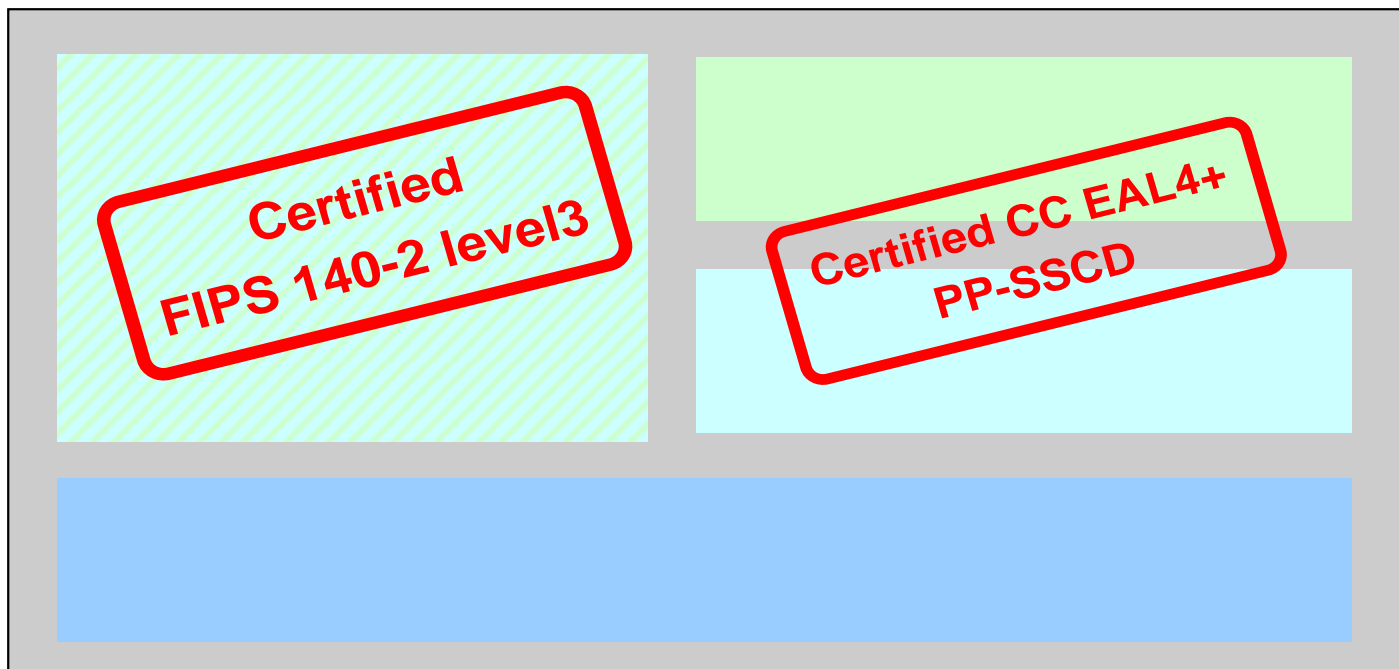
Systemy operacyjne karty i aplikacje ID-One™ Cosmo

- ↓ **Multi-aplikacyjny** system operacyjny
- ↓ **50 milionów** komponentów ID-One Cosmo dostarczonych do klientów rządowych i samorządowych (armia USA, agencje rządowe USA, dowody tożsamości dla obywateli Maroka, karty CNS we Włoszech, itp.)
- ↓ Zgodność z najnowszymi standardami: **Javacard 2.2.2** i Global Platform
- ↓ **Wysoki poziom bezpieczeństwa**: FIPS 140-2 poziom 3, certyfikat Common Criteria do EAL5+
- ↓ **Do 128k** pamięci EEPROM,
- ↓ Stykowy, bezstykowy, USB interface chip
- ↓ Opcjonalny **Odcisk Palca Match On card** (format ISO 19794)





Przegląd normalizacji i certyfikacji bezpieczeństwa





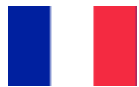
Oberthur Javacard – na który rynek?



Paszporty elektroniczne – Belgia



Identyfikator dla pracowników rządowych – Australia (centerlink)



Karta Total Corporate



Paszporty elektroniczne – Tajlandia



Karta korporacyjna dla notariuszy francuskich



Dowody tożsamości – Maroko



Karta zdrowotna – Włochy



Ministerstwo Obrony – Szwecja



Karta biometryczna – Wybrzeże Kości Słoniowej



Ministerstwo Obrony USA – karta Identyfikacyjna



Karta identyfikacyjna pracownika usług przewozowych USA












Przepustka – Ministerstwo Obrony Singapuru



Polska Policja – autoryzacja



id-:ne Konfiguracje Cosmo V7.0

Typ Cosmo V7.0	Pojemność pamięci EEPROM w KB 	contact 	dual 	contactless 	Certyfikacja 
Entry	16 ↔ 20	✓	✓	✓	
Basic	32 ↔ 40	✓	✓	✓	
Standard	64 ↔ 80	✓	✓	✓	
Large	128	✓	✓	✓	



ID-One Cosmo V7.0 - cechy



↓ Chip(y)

- ↓ EEPROM:16K do 128K
- ↓ Dostępny od 2 różnych producentów



↓ Certyfikacja

- ↓ FIPS 140-2 L3 -> Q409
- ↓ CC EAL5+ dla platformy otwartej -> Q409
- ↓ Uwaga: Wszystkie chipy posiadają certyfikację na poziomie (co najmniej) CC EAL5+



↓ Platforma otwarta

- ↓ JC 2.2.2
- ↓ GP 2.1.1



↓ Kryptografia

- ↓ DES/3DES (CBC,ECB)
- ↓ AES 128,192&256 bitów
- ↓ RSA do 2048 bitów
- ↓ EC-DSA GF(p) do 521bitów
- ↓ Generator kluczy RSA&EC-DSA na płycie
- ↓ SHA do 512
- ↓ Zgodna z algorytmem Suite B NSA
- ↓ Diffie-Helman API (RSA&EC)
- ↓ Dłuższe komendy APDU dla JC2.2.2
- ↓ Możliwość wczytania danych
- ↓ biometrycznych. Metoda Match-On-Card



↓ Protokół

- ↓ T=0/T=1 T=CL, typ A/typ B
- ↓ Mifare 1K (opcjonalnie)
- ↓ USB 2.0 (72K)



Open Platform Cosmo V7 CC EAL5+

Platforma otwarta jest certyfikowana po implementacji profilu Java Card Protection, w tym **mechanizmów ładowania aplikacji**: oznacza to, że poziom certyfikacji EAL5+ **platformy zachowuje ważność nawet w przypadku załadowania apletu nie poddanemu ewaluacji.**









ID-ONE COSMO V7.0a EAL5+ Standard Large Dual





Przegląd aplikacji

Zakres	Oferta PKI	Oferta podpisu kwalifikowanego	Oferta FIPS
Produkt	Authentic* 	ID-One Classic → koniec VI 2010 IAS-ECC* 	PIV* GICS* 
Zgodność ze standardami	<i>Brak</i>	↓ eSign K ↓ Europejska Karta Obywatela (ECC)	FIPS 201
Certyfikacja	<i>Brak</i>	EAL4+ PP-SSCD 	FIPS 201 FIPS 140-2 poziom 3  
Korzyści	↓ Elastyczna oferta ↓ Dedykowana do silnej autoryzacji	↓ Dedykowana do projektów podpisu kwalifikowanego ↓ Projekty europejskie (eID, eRP, eGov...)	↓ zastosowania LAC & PAC ↓ Wszystkie projekty e-Gov

* W pełni zintegrowane z middleware (PKCS#11, CSP, minidriver, Linux, Mac OS)



Oferta Oberthur dla Elektronicznych Legitymacji Studenckich

Applet IAS /Authentic ?

↓ Funkcjonalność

- ↓ Interfejsy bezstykowe Mifare™ oraz T=CL
- ↓ Interfejs stykowy ISO 7816
- ↓ Obsługa cyfrowych certyfikatów X.509
- ↓ Wsparcie dla wielo-aplikacyjności

↓ Hardware & software

- ↓ ID-One Cosmo 2048bit RSA chip do 128Kb pamięci
- ↓ Javacard 2.2 oraz Global Platform 2.1.1
- ↓ Applet IAS/Authentic załadowany i skonfigurowany

↓ Certyfikacja

- ↓ Common Criteria EAL 4+ PP SSCD
- ↓ FIPS 140-2 Level 3

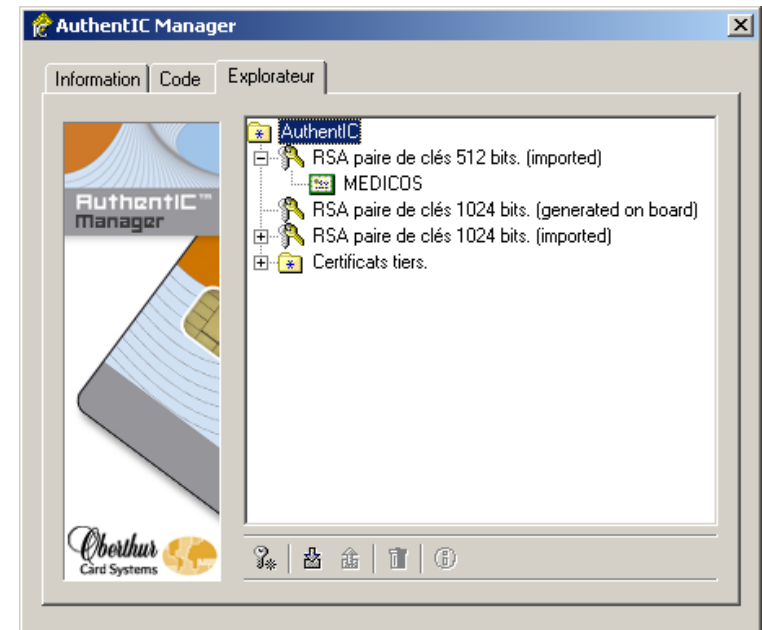




Oprogramowanie klienckie dla podpisu elektronicznego

↓ ID-One Classic Middleware (Authentic Web Pack)

- ↓ Biblioteki kryptograficzne zabezpieczające aplikacje lokalne oraz sieciowe
- ↓ Obsługa kart Oberthur
- ↓ Wsparcie dla PKCS#11 również pod Windows Vista™ i Windows 7™
- ↓ Wspierane systemy operacyjne:
 - ↓ Microsoft Windows NT SP4
 - ↓ Microsoft Windows 2000 SP4
 - ↓ Microsoft Windows XP SP2
 - ↓ Microsoft Windows Server® 2003 SP1
 - ↓ Windows Vista™ SP2
 - ↓ Windows 7™
 - ↓ Mac OS X V10.5
 - ↓ Linux RedHat enterprise 5, Linux Fedora Core 7,
Linux Ubuntu 8.04 Hardy, Linux Ubuntu 9.04



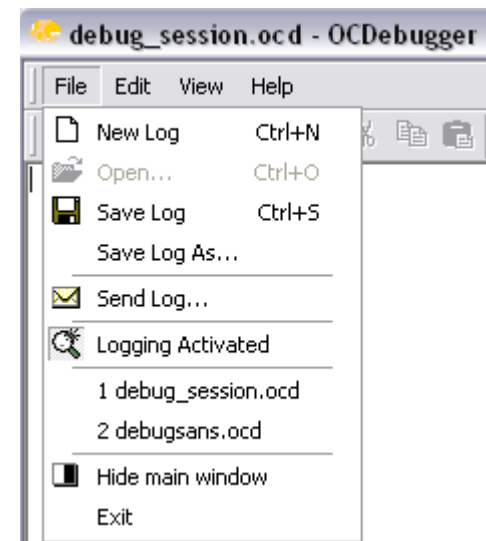


ID One Cosmo Development Kit – pakiet deweloperski



Application Loader

Version 1.4.1





Dziękuję serdecznie za uwagę!

Pytania?



Monika Paszko

Area Sales Manager

tel: +48 604 144 034

m.paszko@oberthurcs.com

Agnieszka Dąbrowska

ID Regional Technical Support

tel: +48 601 135 975

a.dabrowska@oberthurcs.com