

Nowe mechanizmy w wersji 3 Java Card

Mateusz LESZEK (138775)

Plan prezentacji

1. *Java Card 3*
2. *Nowe mechanizmy w Java Card 3.X*
3. *Edycje Java Card 3.X –
Classic vs Connected*

Karty inteligentne wprowadzone w latach osiemdziesiątych posiadały pojedynczy układ scalony na każdej karcie, z bardzo ograniczonymi zasobami (zwłaszcza RAM).

Najpopularniejsze mają od 4 do 8 Kb RAM i 32 do 64 Kb EEPROM oraz wykorzystując wolne 8-bitowe procesory i wykorzystuje bardzo ograniczony podzbiór funkcji i możliwości, który zapewnia Java.

Java Card 3

JavaCard 3

- Wprowadzony w 2009 r
- Jest odpowiedzią na rosnące zasoby i możliwości kart elektronicznych
- Wprowadza nowe mechanizmy bezpieczeństwa,
- APDU to przeżytek – Servlet
- Wielowątkowość

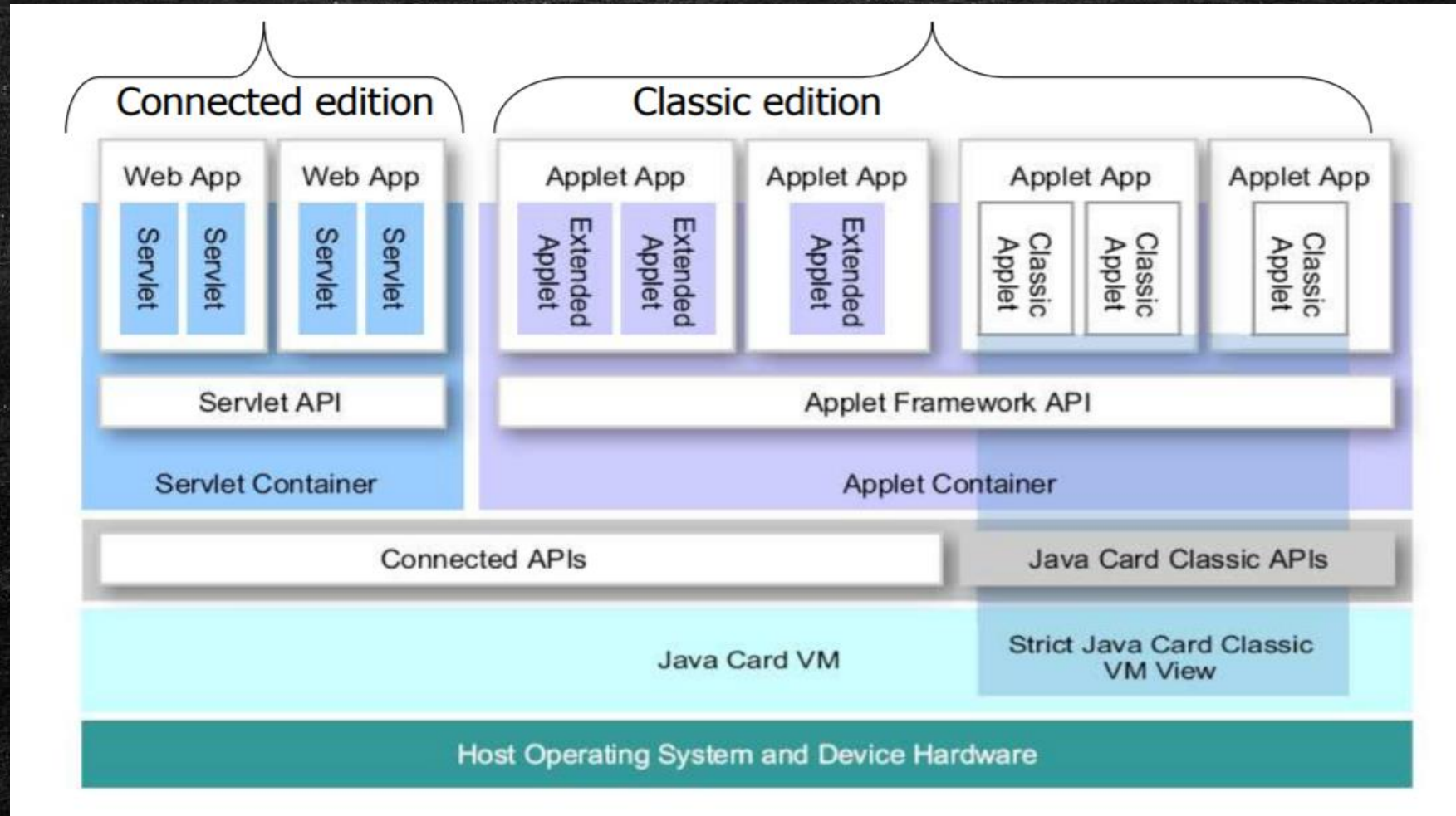
Główne cele projektowania technologii kart Java to mobilność i bezpieczeństwo, czyli enkapsulacja danych, firewall, kryptografia i applet.

Edycje Java Card 3.X – Classic vs Connected

Edycje Java Card 3.X – Classic vs Connected

- JavaCard w wersji 3 oferuje dwie edycje: Classic oraz Connected.
- Najprościej:
 - Classic – ewolucja,
 - Connected – rewolucja.
- Możliwość wyboru edycji do aktualnych zastosowań.
- Złoty środek?

Architektura Java Card 3.0



Java Card Classic Edition

- ewolucja Java Card 2.2.2,
- bardzo podobne ograniczenia na poziomie językowym,
- 16-bitowa maszyna wirtualna Java Card VM and APIs,
- aplikacje bazujące na APDU,
- lepsze wsparcie dla komunikacji bezstykowej, nowe ISO7816-4
- obsługa nowych algorytmów szyfrowania.

Java Card Connected Edition

- nowe funkcjonalności,
- 32-bitowa Java VM,
- wielowątkowość,
- obsługa zdarzeń,
- TCP/IP,
- Odpowiedni dla serwerów sieciowych Smart Card - obsługuje aplikacje Java Card 2.2/

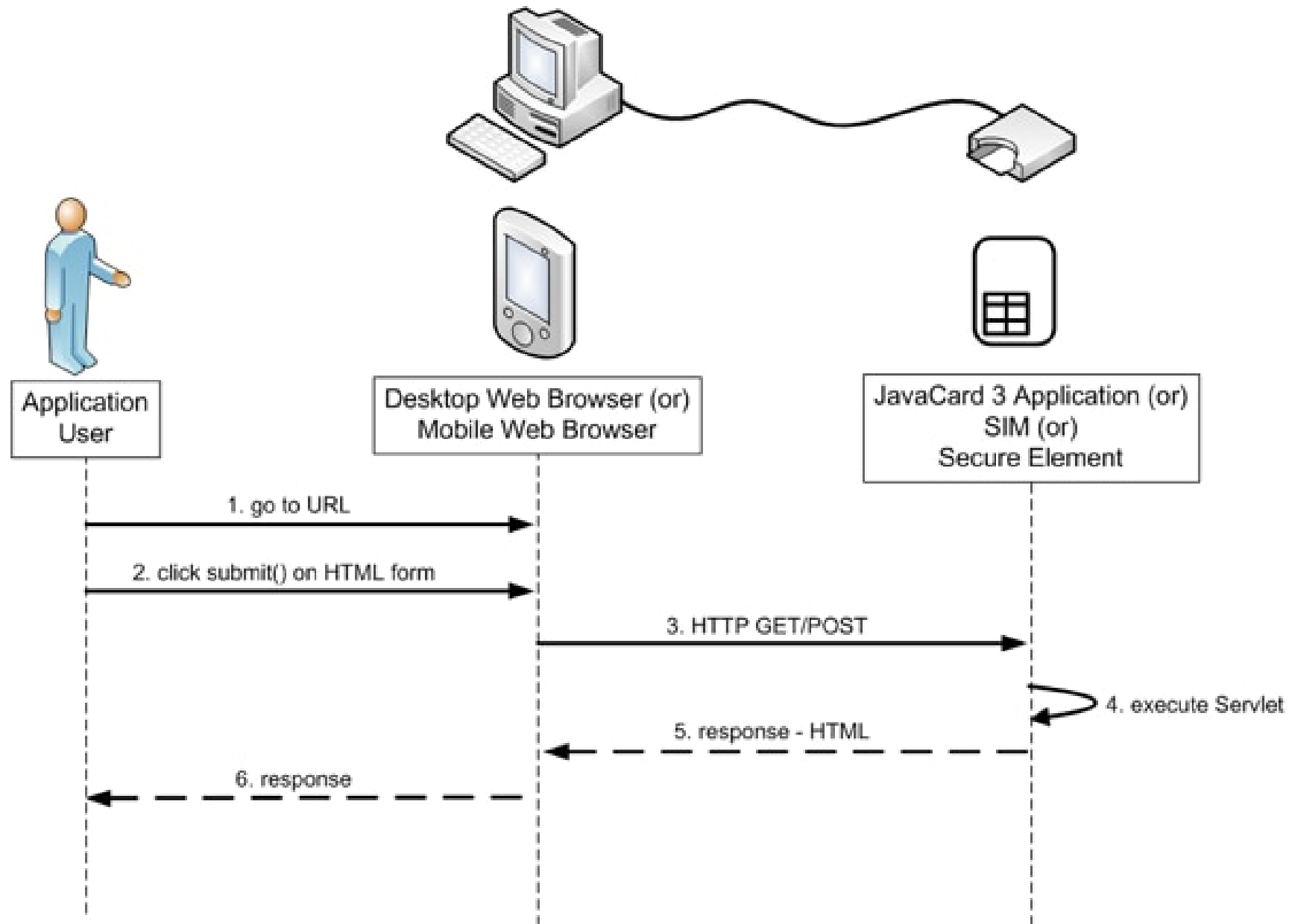
Nowe mechanizmy w Java Card 3.X

Co nowego

- Interfejs API oparty na podzbiorze CLDC z funkcjami Java 6
- byte, short, int, long, char i java.lang.String
- Wątki
- Serwlety
- Zbieranie śmieci
- TCP / IP
- HTTP i HTTPS
- pliki .class
- pliki instalacyjne .war
- Dynamiczne ładowanie klas
- Tablice 2-D
- 32-bitowe procesory
- 24kB pamięci RAM

Serwlet

- Serwlet to aplikacja działająca na serwerze sieci Web:
 - Działa na „kontenerze sieciowym”
 - Kontener WWW wysyła żądania do serwletów
- Aplikacja serwletu może przetwarzać przychodzące żądania.
- Serwlety często są warstwą prezentacji aplikacji.



Funkcje Servletu

- `doGet()` method handles HTTP GET requests
- `doPost()` method handles HTTP POST requests
- `doPut()` method handles HTTP PUT requests
- `doDelete()` method handles HTTP DELETE requests
- `doHead()` method handles HTTP HEAD requests
- `doOptions()` method handles HTTP OPTIONS requests
- `doTrace()` method handles HTTP TRACE requests

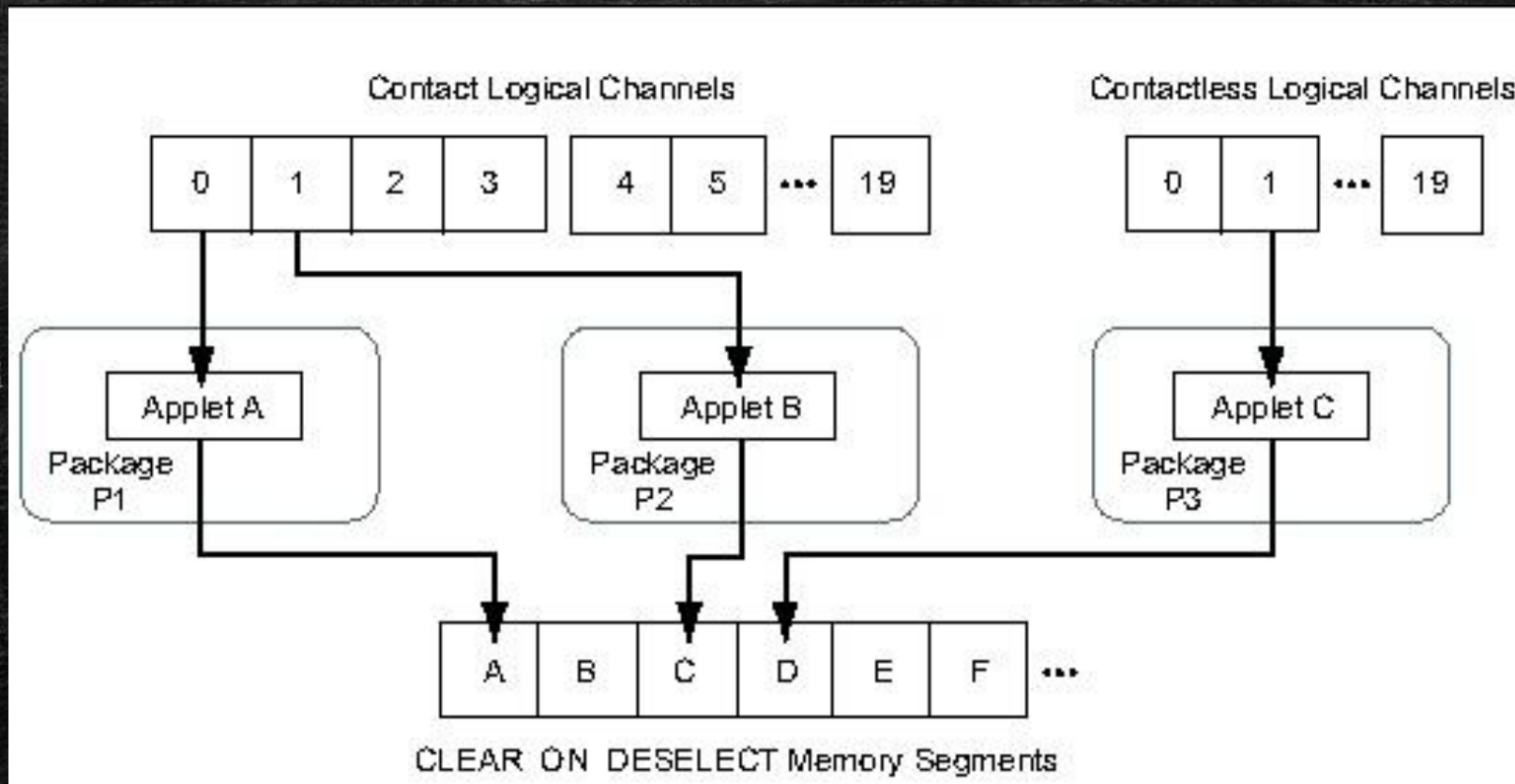
Sesje i zdarzenia

- W Java Card 3.0 aplikacje mogą monitorować zdarzenia:
 - zarejestrowanie zadania do automatycznego ponownego uruchomienia,
 - rejestracja w celu powiadomienia o ważnych wydarzeniach,

Kanały logiczne

- Użycie kanałów logicznych pozwala na zrównoleglone wykonywanie do kilku aplikacji na karcie przy użyciu jednego interfejsu komunikacyjnego.
- Java Card 3 umożliwia otwarcie 20 kanałów [0...19]. (Java Card 2.1.1 pozwalał na 4)
- Są wybierane za pomocą deklaracji bitów CLA.
- Dzięki nim aplikacje mogą być adresowane niezależnie na poziomie logicznym. Stan karty (zweryfikowane kody PIN itp.) są pamiętane oddzielnie dla każdego z używanych kanałów logicznych.

Kanały logiczne



Zatem, dlaczego klasa $CLA=C0$
nie może być dalej
wykorzystywana do własnych
zastosowań?

... a no dlatego

- APDU o klasie CLA = 0xC0 jest przeznaczona do obsługi kanału czwartego.

Źródło:

- JCREclassic Spec 3.0.1
- Forwarding APDU Commands To a Logical Channel)
- Strona: 4-9
- Tabela: 4-2

CLA byte encoding	Semantic details
%b1001 yyzz	(Type 4) not last command in chain, with SM
%b1010 00zz	(Type 4) last or only command in chain, no SM
%b1011 00zz	(Type 4) not last command in chain, no SM
%b1010 yyzz	(Type 4) last or only command in chain, with SM
%b1011 yyzz	(Type 4) not last command in chain, with SM
%b1100 zzzz	(Type 16) last or only command in chain. no SM
%b1101 zzzz	(Type 16) not last command in chain, no SM
%b11y0 zzzz	(Type 16) last or only command in chain, with SM
%b11y1 zzzz	(Type 16) not last command in chain, with SM

NOTATION

u	undefined
y	Secure Messaging indicator See ISO 7816-4:2005 Specification Section 6 for further information.
z	Logical channel indicator Type 4 supports logical channels [0..3] Type 16 supports logical channels [4..19]

Podsumowanie

- Java Card 3.0:
 - jest potężny,
 - integruje nowoczesne koncepcje programistyczne,
 - obsługuje złożone aplikacje,
 - staje się elementem sieci.
- Nie zapominaj, że platformy są nadal ograniczone.
- Wydajność może pozostać problemem.

Literatura

- Development Kit User's Guide, Java Card™Platform, Version 3.0.3 Connected Edition, 2010, Oracle.
- Java Card 3.0 :
<http://java.sun.com/javacard/3.0/>
- Java Card 2.2.1:
<http://java.sun.com/javacard/2.2.1/>

Dziękuję za uwagę