Java Card™ Platform Evolution: Future Directions

Tanjore Ravishankar,
Florian Tournier,
Thierry Violleau

Java Card Team
Sun Microsystems, Inc.

TS-3925

Goal

Preview future Java Card™ technology and its role in connected security architectures

Agenda

Java Card Technology Today

Requirements and Uses Cases for the Next Generation

Preview of Next Generation Technology

- Evolution of Platform Features
- Infrastructure and Connectivity
- Use Case Analysis

Agenda

Java Card Technology Today

Requirements and Uses Cases for the Next Generation

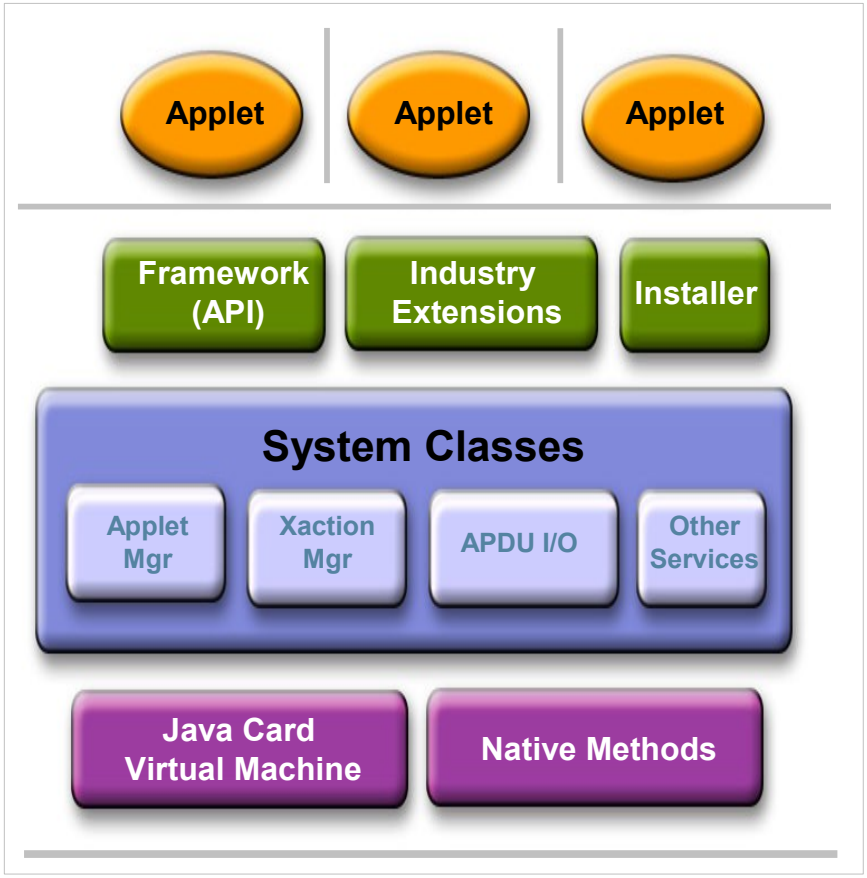
Preview of Next Generation Technology

- Evolution of Platform Features
- Infrastructure and Connectivity
- Use Case Analysis

Java Card Technology

Smart Card Security

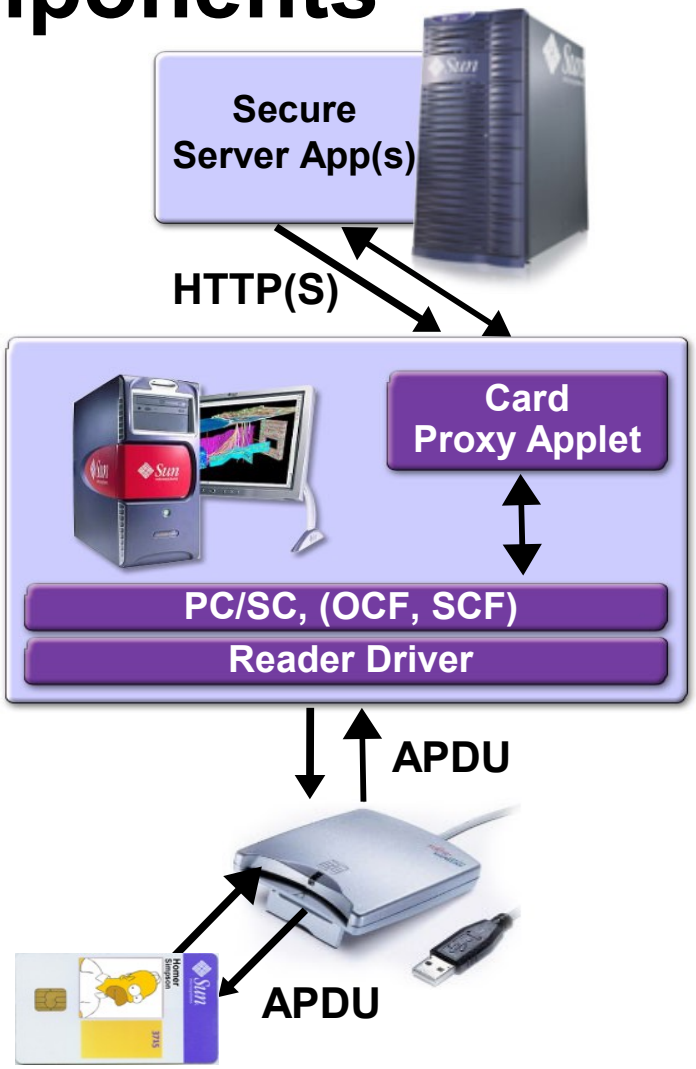
- Java Card 2.2.2 Specifications
- Subset of Java™ SE platform and Java programming language
- Split-VM Architecture
- Persistent VM model
- Firewall model isolates contexts and applets
- ISO7816 Communication I/F and protocol
- Transaction management



Server and Client Components

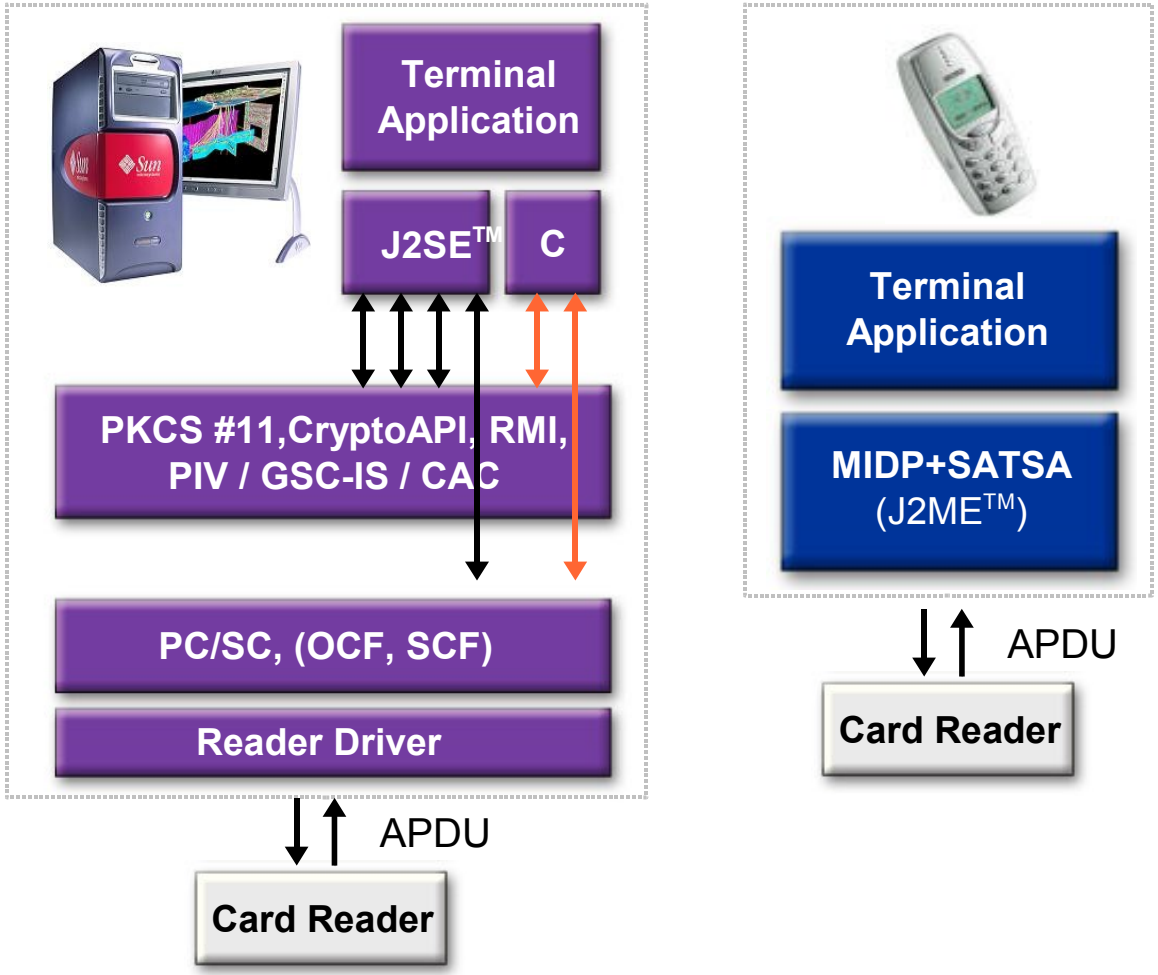
Infrastructure Layers

- Server
  - Secure Server Application
  - Card Proxy Applet
- Client
  - Secure Client Application
  - PC/SC card access framework
  - Card reader driver layer
  - Card Reader



Client Components

Software Layers



Typical Applications

- Desktop Client
  - Login authentication
  - Email signing
- Handheld Client
  - Personal Information
  - Mobile Ticketing
- POS Terminal Client
  - Card Holder Authentication
  - Debit/Credit applications
  - Loyalty applications
- Web authentication
  - Single sign-on
- Wireless communication
  - Transmission Privacy
  - Billing Service
  - Phone book backup service

Agenda

Java Card Technology Today

Requirements and Uses Cases for the Next Generation

Preview of Next Generation Technology

- Evolution of Platform Features
- Infrastructure and Connectivity
- Use Case Analysis

Market Perspective

Java Card Technology Adoption

- Over 1.6 Billion cards deployed
- Java Card technology caters to most market needs
  - Telecom, Civic/Corporate ID, Finance, Pay TV, Transport
  - Interoperability and security
  - Availability of products, tools, infrastructure and content
- Java Card platform 2.2.2 available since March 06
  - Contactless, ID/E-passport
- 100's of products worldwide

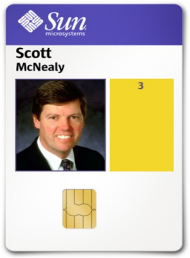
SIM Cards

Secure Flash Memory

Passports

Java POWERED

USB Tokens



Smart Cards

Contactless

Challenges Moving Forward

Why a New Java Card Platform?

- Hardware capabilities are increasing exponentially
- Utilization of card services can be improved
- Issuers are still struggling with the deployment of smart cards and applications
- Sun and Java Card platform licensees are developing next generation technology
  - Commercial Deployment: 2008 and beyond
  - Retain the key attributes of Java Card technology: Interoperability, Security, Compactness, Compatibility

Next Generation Smart Card Platform

Traditional vs. High-end Smart Card Hardware (2007+)

8/16 bit CPU	**32 bit CPU**
~ 2K RAM	**16K RAM**
48–64K ROM	**>256K ROM**
8–32K EEPROM	**>128K EEPROM, or Several MB Flash**
External Clock: 1–5 MHz	**Internal Clock: 50 MHz**
Serial I/O Interface 9.6–30K Baud Half Duplex	**High Speed Interfaces** **1.5 Mb/s–12 Mb/s** **Full Duplex**

Give Control to the User Over Card Services

The Case for a Next Generation Java Card Technology

- Simplify end-user interactions with the card
  - Bring a web look-and-feel to card applications
- Leverage latest hardware to create new usage patterns
  - Manage and manipulate large data objects
  - Enable parallel execution over multiple comm channels
- Free developers from the constraints of card protocols
  - Serve content via IT-accepted internet protocols
  - Facilitate smart card integration in webservices infrastructure based on http/xml

Reduce Deployment Complexity

The Case for a Next Generation Java Card Technology

- Facilitate the management of cards and applications
  - Manage cards as any entity on a TCP/IP network
- Use standard IDEs for the development of Java Card technology-based applications
- Simplify the roll-out of terminal infrastructures
  - Eliminate card-specific software on the terminal
  - Remove the complexity of syncing terminal and card applications

Sample Use Cases

Give Control to the User Over Card Services

- Securely manage private data from a web browser
  - Browse content like phone book entries in a SIM card
  - Remote browsing of card content (“home-page on SIM”)
- Stream DRM content from a SIM card to a phone
- Perform online network authentication and contactless payment simultaneously
- Enable card-initiated connections to back-end services
  - Perform a complete end-to-end financial transaction
  - Cryptographically authenticate a card holder to the back-end

Sample Use Cases

Reduce Deployment Complexity

- Manage securely and remotely a fleet of card through the network using standard network protocols
  - Using standard back-end applications, integrating with device management infrastructures
- Program/debug applications on a standard IDE, then load unmodified on the card
- Use cards on a PC without specific installed software
- Provide automatic data backup/sync services
  - The card securely, pro-actively connect to off-card backup services or applications

Next Generation Requirements

Retain the Characteristics of Java Card Technology

- Backward compatibility
- Scalability
  - Address variability in different market segments
- Security
  - Enhanced Crypto
  - Specific support for smart card hardware

Enable Advanced Smart Card Features

- Network-oriented communication
  - High speed Interface
  - TCP/IP integration
- Client and Server communication models
- “More main-stream” language features

Agenda

Java Card Technology Today

Requirements and Uses Cases for the Next Generation

Preview of Next Generation Technology

- Evolution of Platform Features
- Infrastructure and Connectivity
- Use Case Analysis

Next Generation Java Card Platform

Proposed Enhancements

- VM technology
  - 32 bit VM
  - .class file loading
  - Concurrent execution of apps/multithreading
  - On-card byte-code verification
  - Automatic GC
- Security
  - Enhanced context-isolation
  - Policy-based security

Next Generation Java Card Platform

Proposed Enhancements

- Network-oriented communication
  - ISO 7816 and TCP/IP communication support
  - Communication over USB, MMC
  - Concurrent contact/contact-less card access
  - Embedded web server
  - Service static and dynamic content through HTTP(s)
  - Client and server communication mode
  - Generic communication API

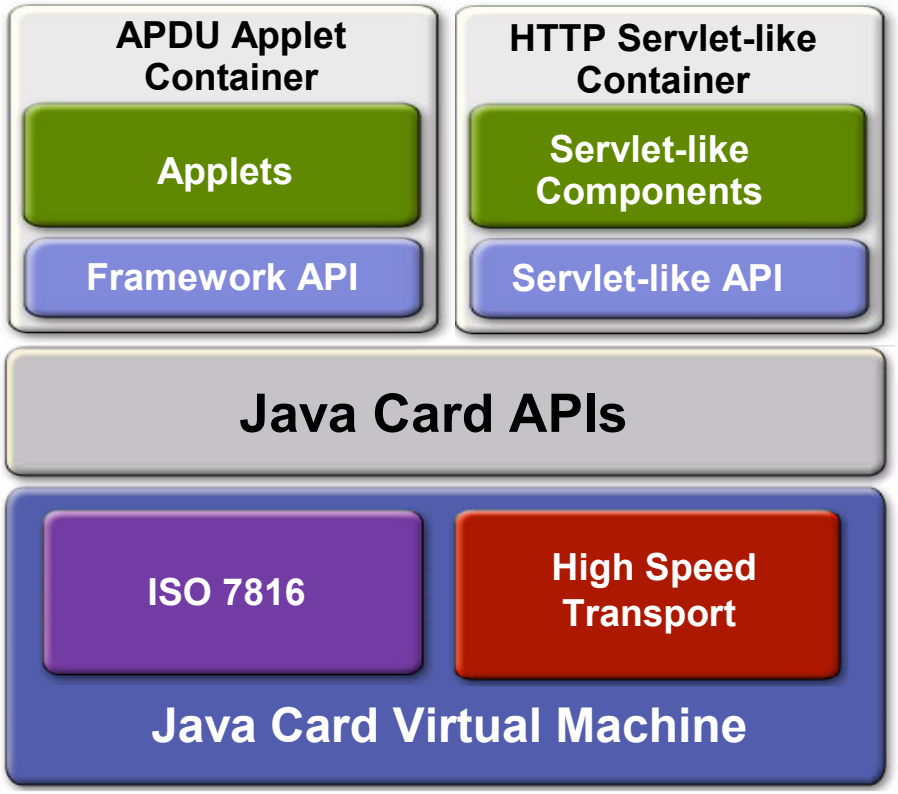
Next Generation Java Card Platform

Proposed Enhancements

- Programming model
  - Fully backward compatible
  - Support additional Java language types: char, long
  - String support
  - Multi-dimensional arrays
  - Support for large data structures—Multimedia content
  - Application models
    - Classic APDU-based applet model
    - HTTP servlet-like model
  - Enhanced inter-application communication framework
  - Generic event framework
  - Evolutive cryptography framework

Next Generation Java Card Platform

Proposed Software Stack

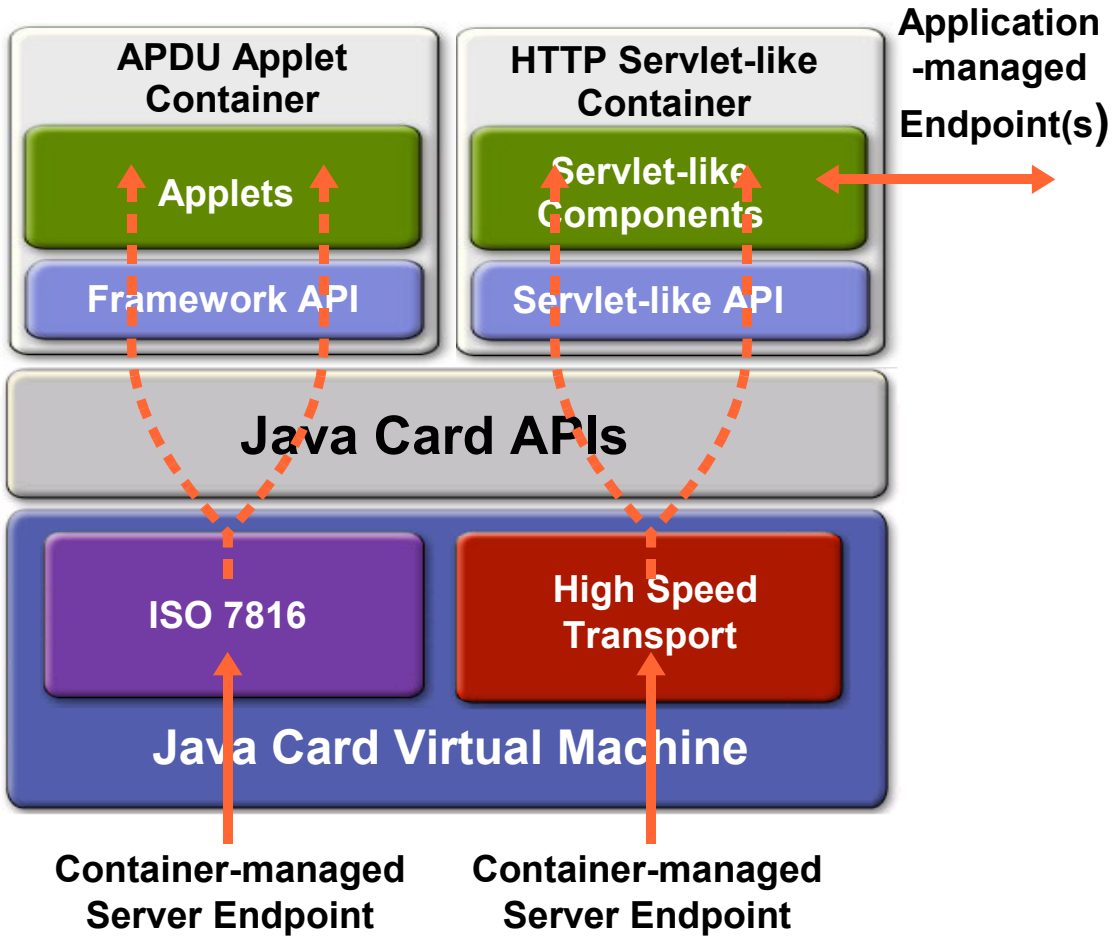


Next Generation Java Card Platform

Communication Model

Two Levels

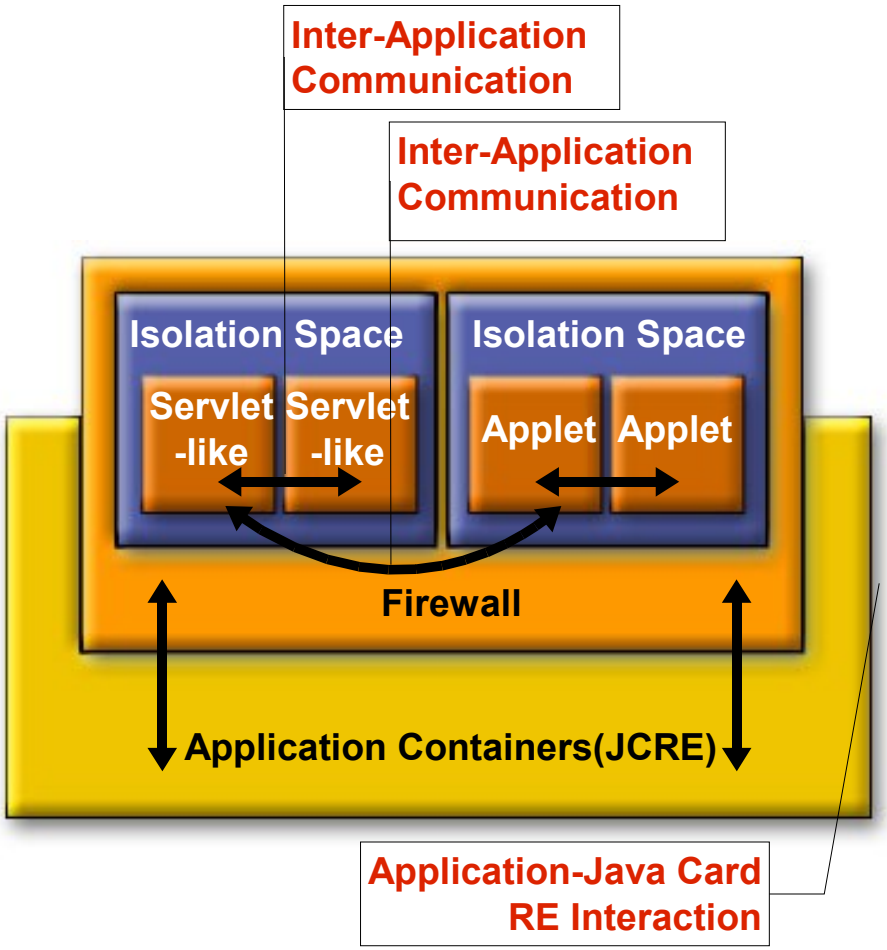
- Container-handled communications
  - Connection endpoints handled by containers
  - Request processing delegated to application components
- Application-handled communications
  - Connections initiated/handled at the application level
  - Can implement both client and server communication model



Next Generation Java Card Platform

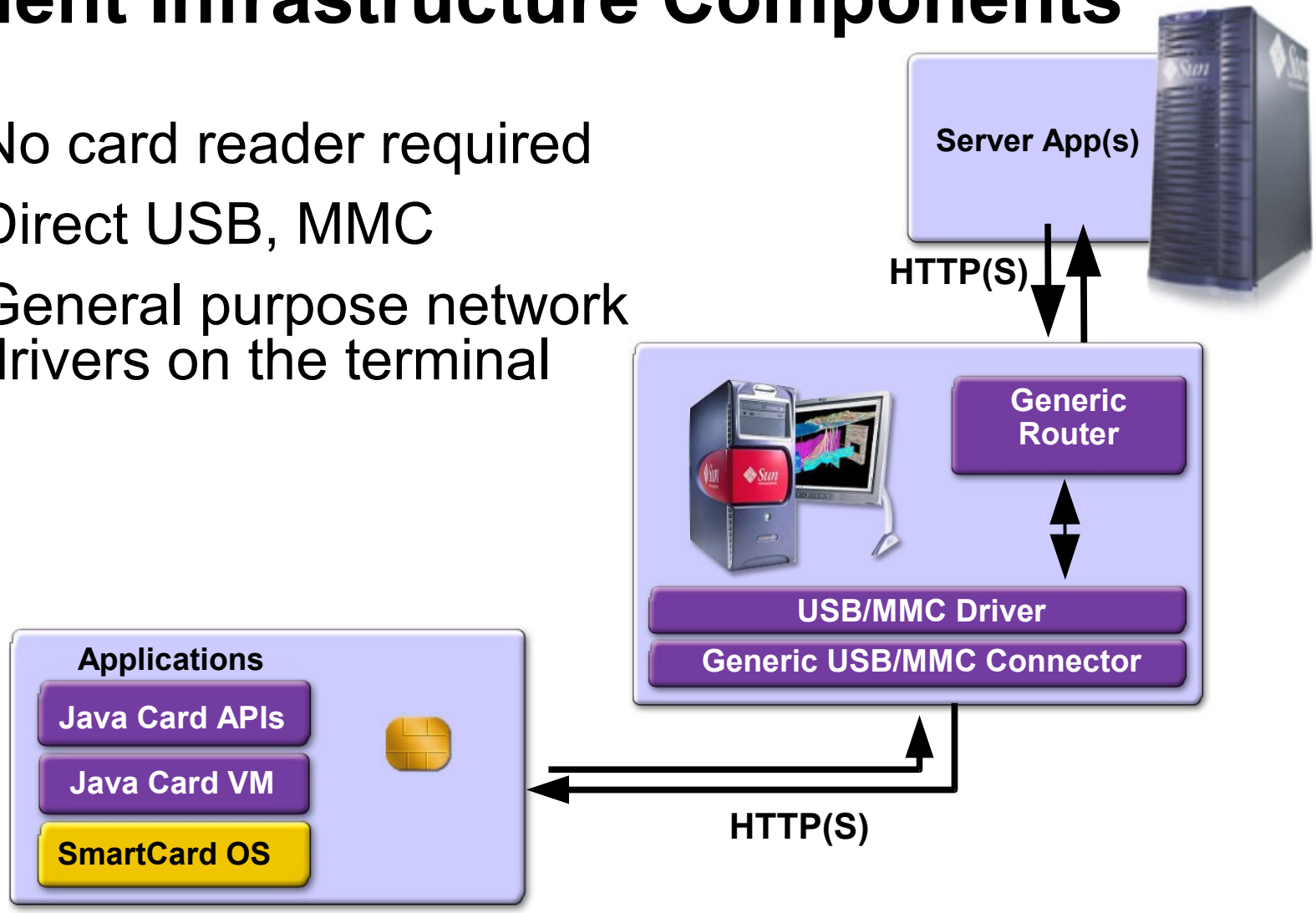
Security Containment Model

- Applications run in secure isolation spaces
  - Components from the same application can interact (share data)
- Containers run in Java Card RE isolation space
- Inter-application and Application-Java Card RE interactions restricted by Firewall
- Policy-based access control across Firewall



Client Infrastructure Components

- No card reader required
- Direct USB, MMC
- General purpose network drivers on the terminal



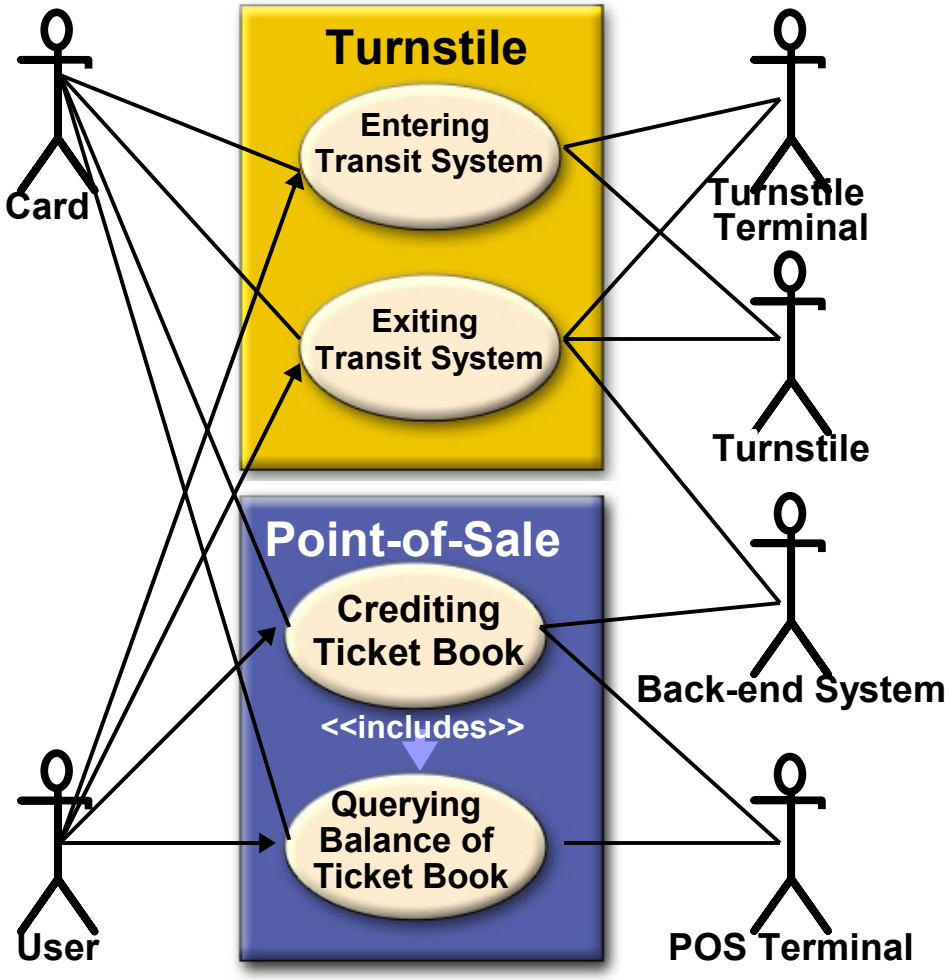
Next Generation Applications

- End-to-end secure applications
  - Servers communicating directly with cards
  - Security does not depend on trusted client device
  - Secure banking transactions
    - Debit/credit
- DRM applications
- Browser-enabled applications
  - Private information self-management

A Transit/Mobile Ticketing Application

Typical Use Cases

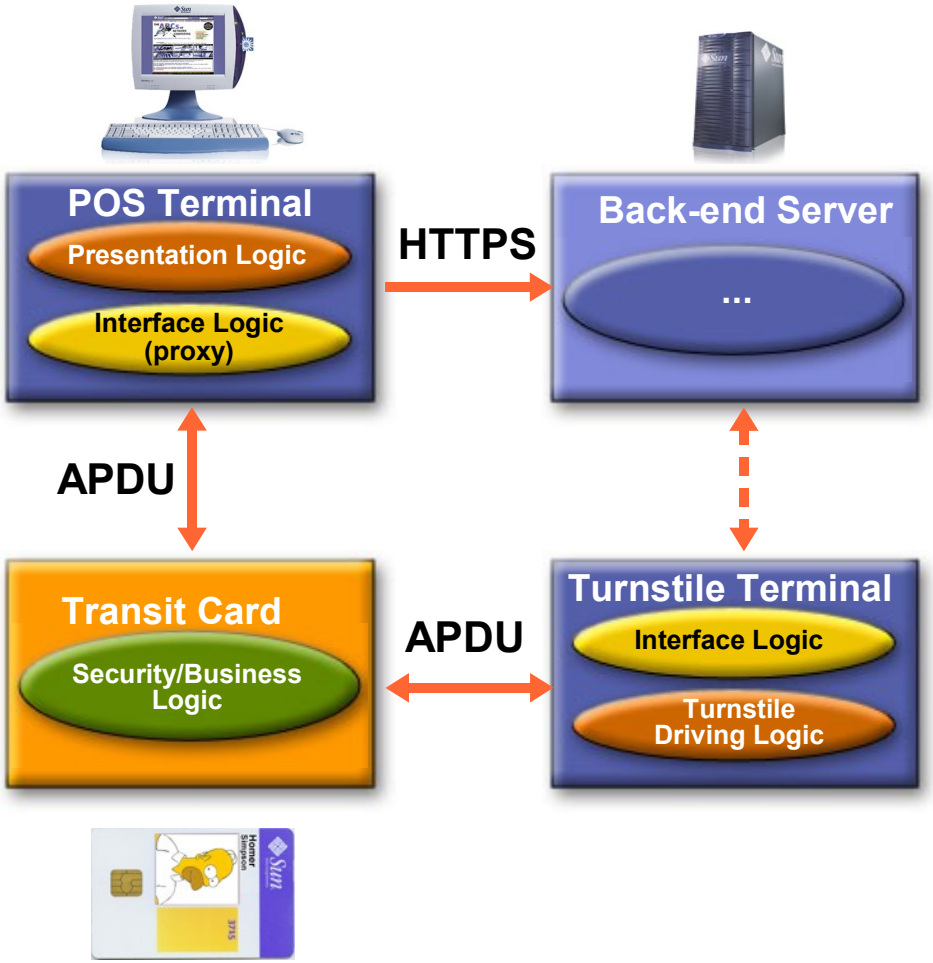
- Turnstile subsystem
  - Use cases
    - Entering
    - Exiting
  - Actors
    - Card and card holder
    - Turnstile and terminal
    - Back-end system
- POS subsystem
  - Use cases
    - Crediting
    - Querying balance
  - Actors
    - Card and card holder
    - POS terminal
    - Back-end system



A Transit/Mobile Ticketing Application

Architecture of a Classic APDU Applet-based Application

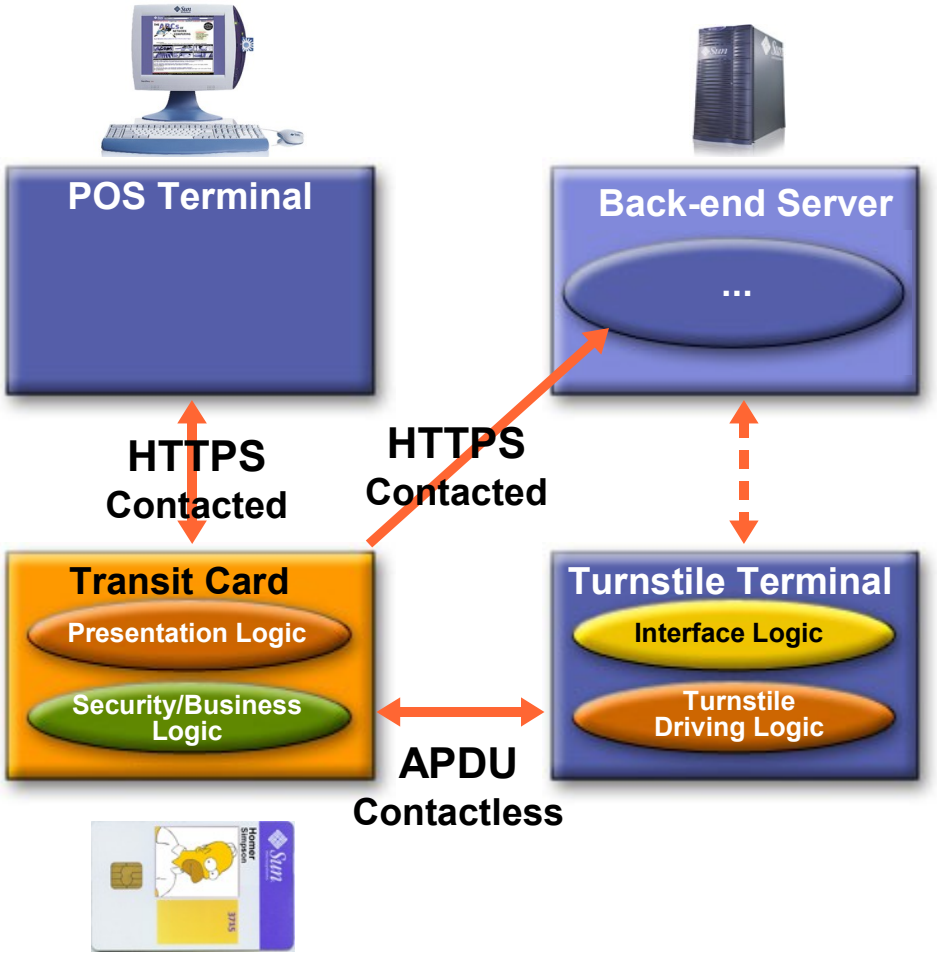
- Functional partitioning
  - Card
    - Security + Business logic
  - POS terminal
    - Card interface logic
    - Presentation logic (UI)
    - Back-end interface logic
  - Turnstile terminal
    - Card interface logic
    - Turnstile driving logic
  - Back-end server
    - Out-of-scope



A Transit/Mobile Ticketing Application

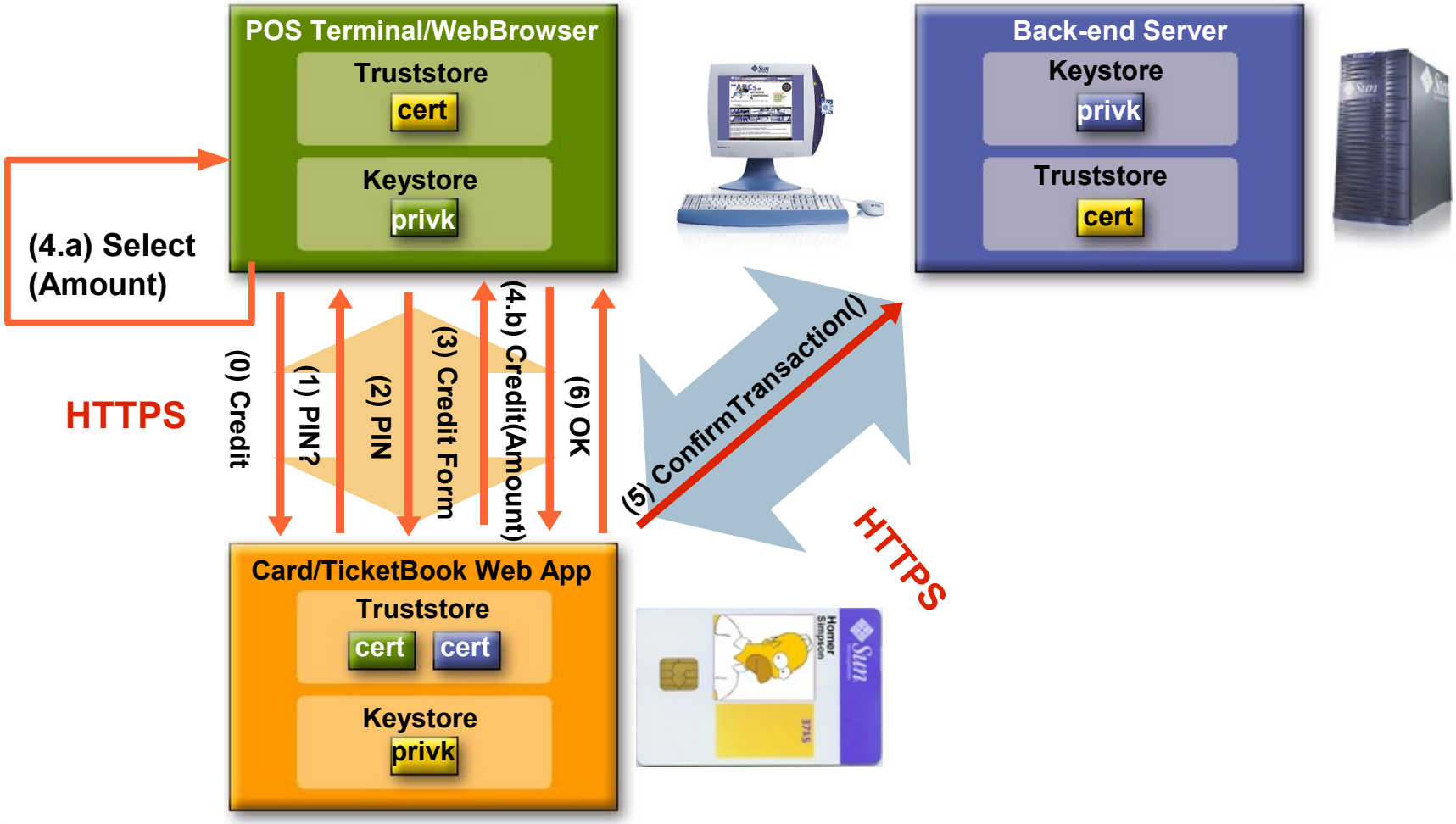
Architecture of a Connected Application

- Functional partitioning
  - Presentation (UI) implemented by card
  - Interaction b/w card and terminal: (X)HTML over HTTP(S)
  - Interaction w/back-end handled by card: structured data (binary or text) over HTTP(S)
  - Thin terminal application client (browser) simplifies deployment



Transit/Mobile Ticketing Application

POS Interactions



Summary

- Next generation Smart Card hardware
  - 16K RAM, >256K ROM
  - USB, MMC communication interfaces
  - Card connects directly to client device
    - No card reader required
- Directions for Next generation Java Card technology
  - Fully backward compatible
  - Mainstream Java language programmable
    - 32 bit VM, .class file loading, automatic GC
  - Enables end-to-end security—Server-to-Card
    - HTTP servlet-like model
    - TCP/IP communication networks

For More Information

- URL: http://java.sun.com/products/javacard
- Pavilion Sun Booth
  - Pod #731: Java Card Technology
  - Pod #732: Java Card Applications for the Mobile Environment
- Other Java Card Technical Sessions and BOFs
  - Mobility General Session (TS-3203)
  - New White Card Schemes and Java Card™ Technology (TS-3814)
  - XXL—Large Java™ Platform (U)SIM Cards—"The Advanced Mobile Communication Enabler for the Future" (TS-9925)
  - DReaM: Secure End-to-End Interoperable DRM Using Java™ Technology (TS-3326)
  - Measuring the Performance of the Java Card™ Platform Card (BOF-2816)
  - Reviewing the Deployment Strategies and Issues with TCP/IP-Connected Java Card™ Technology (BOF-2890)

Q&A

Tanjore Ravishankar,
Florian Tournier,
Thierry Violleau

Java Card™ Platform Evolution: Future Directions

Tanjore Ravishankar,
Florian Tournier,
Thierry Violleau

Java Card Team
Sun Microsystems, Inc.

TS-3925