JavaOne℠

Sun's 2001 Worldwide Java Developer Conference

Java Card™ Technology-based Corporate Card Solutions

Jack C. Pan,
Leader and Sr. Architect
Hervé Garcia,
Tech. Project Manager

eConsumer Emerging Technologies,
Citibank

Overall Presentation Goal

The objectives are to provide

1) an overview and
2) an in-depth technical discussion

of a smart card based Corporate ID badge program using the latest multi-application, Java Card™ technology

Learning Objectives

- As a result of this presentation, you will be able to:
  - Understand the SmartCard and Java Card technologies at a high level
  - Obtain an overview of the Sun Corporate Badge ID Program
  - Understand the Java Card and Open Platform technologies deployed in the program
  - Learn the architectural and technical lessons from such a program

Speaker's Qualifications

- Jack Pan is responsible for the delivery of the Sun Corporate Badge solution from Citibank
- Hervé Garcia is the overall Technical Lead for the Sun Corporate Badge program from Citibank
- Both Jack and Hervé are active contributors in smart card industry consortiums such as Java Card Forum and Global Platform

Presentation Outline

- Overview of SmartCard and Java Card™ technologies
- Overview of the Sun Corporate Badge Program
- Detailed discussion of Java Card and Open Platform technologies deployed in the program
- In depth discussion of architectural and technical lessons learned from the program

JavaOne℠

Sun's 2001 Worldwide Java Developer Conference

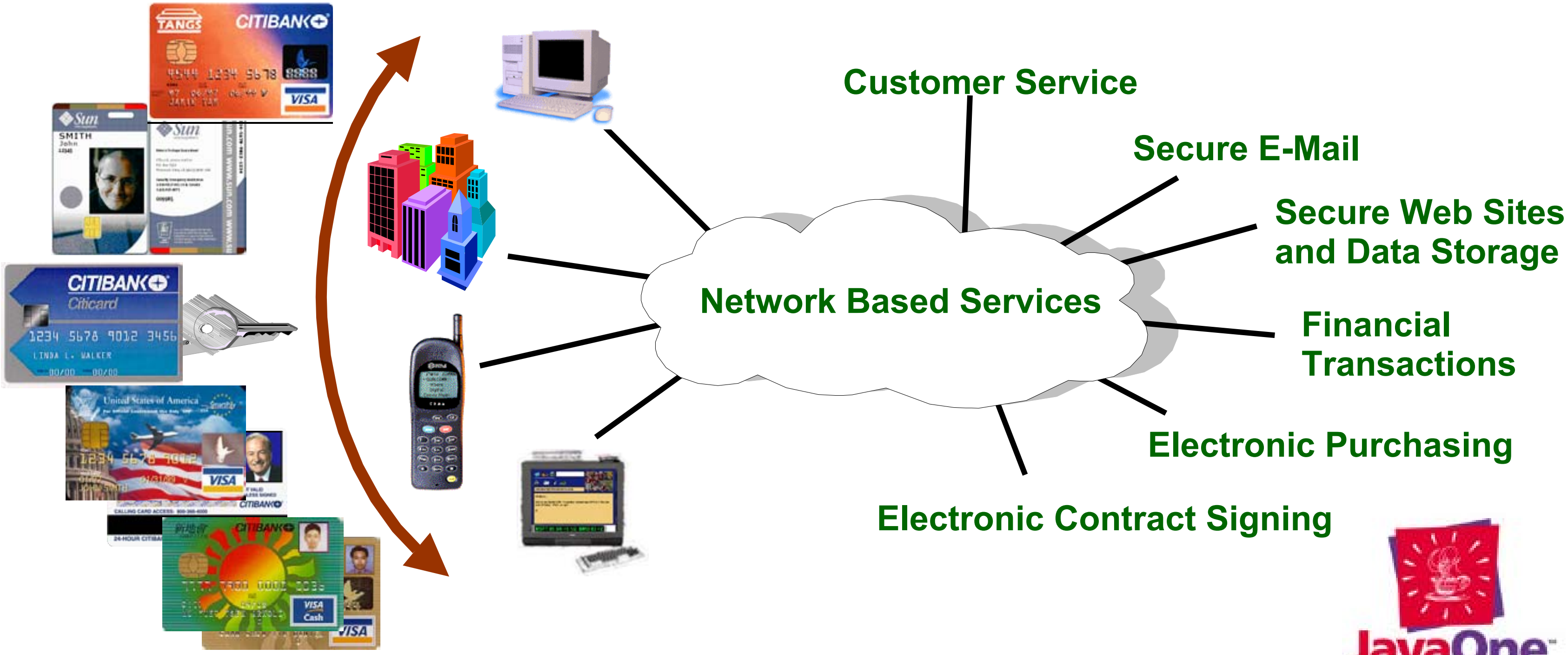
Overview of SmartCard and Java Card™ Technologies

What Is a Smart Card?

- A credit-card sized plastic card with an embedded computer chip.
  - Microprocessor “intelligent” vs. Memory “dumb”
  - Contact vs. Contactless
  - Hybrid vs. Combi
  - Single vs. Multiple Applications
- Other Technologies/Functions
  - Mag stripe
  - Bar code
  - Embossing
  - Signature panel
  - Biometrics

The Role of Smart Card

- Value-add in this Internet Age:
  - Secure authentication token
  - Aggregation of multiple applications



Network Based Services

Customer Service

Secure E-Mail

Secure Web Sites and Data Storage

Financial Transactions

Electronic Purchasing

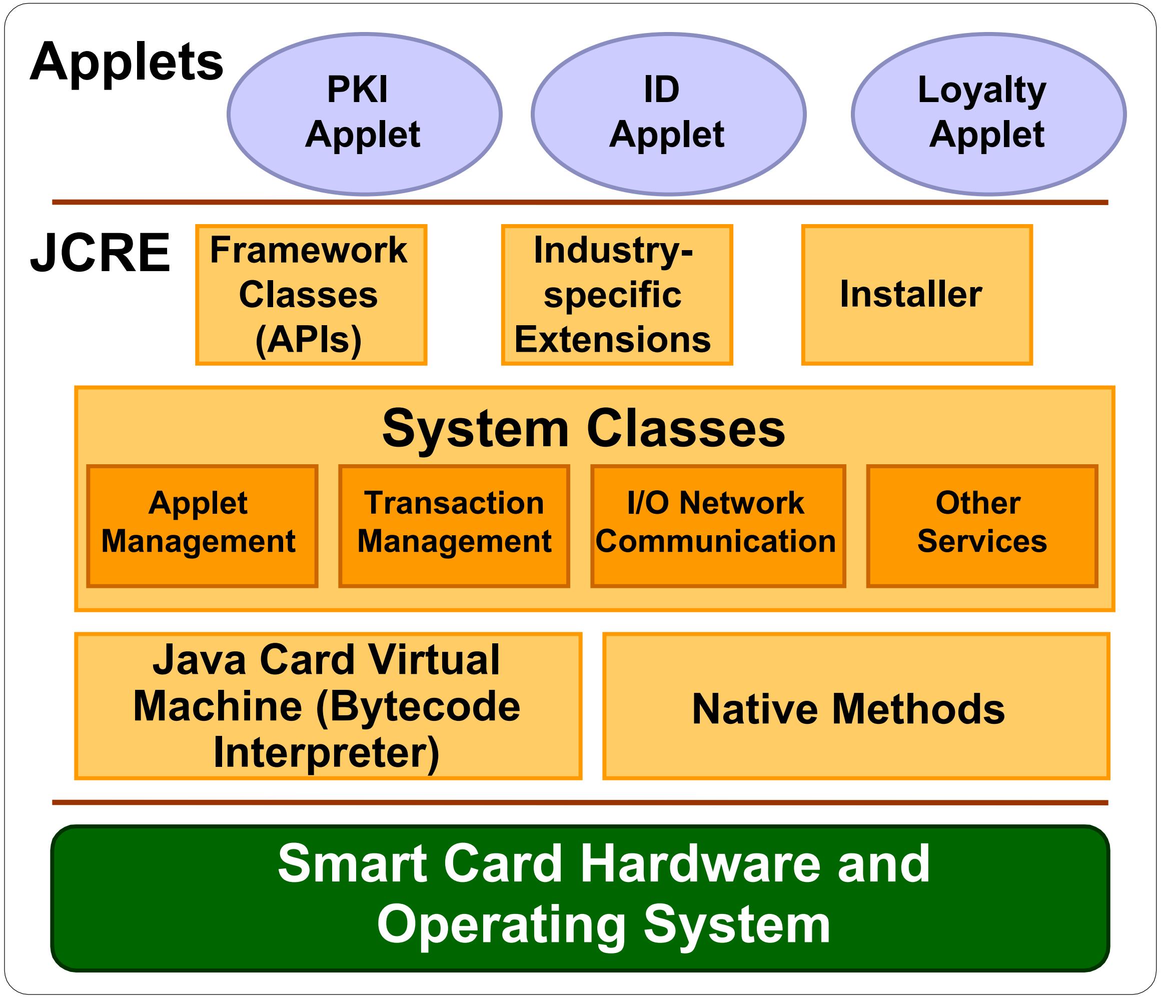
Electronic Contract Signing

What Is Java Card™ Technology?

- Java Card technology
  - Defines a platform on which Java™ technology-based applets can run on smart cards and other memory constrained devices
- Java Card programming language
  - A subset of the Java programming language is supported (e.g., no threads, long, etc.)
- Java Card virtual machine (JCVM)
  - Off-card piece does conversion from class file to CAP file while On-card piece does bytecode interpretation

What Is Java Card™ Technology? (Cont.)

- Java Card runtime environment (JCRE)



Applets

PKI Applet

ID Applet

Loyalty Applet

JCRE

Framework Classes (APIs)

Industry-specific Extensions

Installer

System Classes

Applet Management

Transaction Management

I/O Network Communication

Other Services

Java Card Virtual Machine (Bytecode Interpreter)

Native Methods

Smart Card Hardware and Operating System

Java Card™ Technology-based Government/GSA Card Program

- Launched since May, 1999
- Standard Credit Card
- Official Employee Badge
- Building Access
- Web Server Access
- Digital Certificates
- Calling Card
- Property Management
- e-Boarding
- Biometrics

The High End Multi-application Smart Card Technology Based on Java Card 2.0/Open Platform 1.0

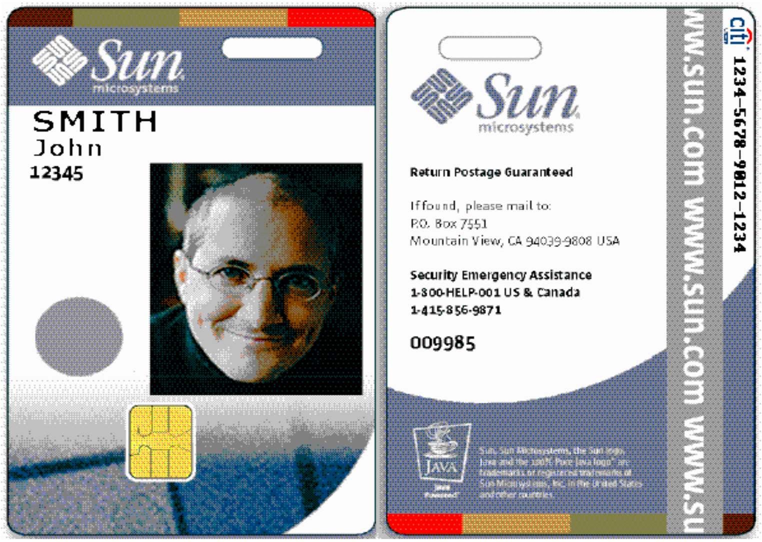
JavaOne℠

Sun's 2001 Worldwide Java Developer Conference™

Overview of the Sun Corporate Badge Program

Sun Microsystems' Corporate Badge Program

- A corporate ID badge for Sun's global deployment (50,000 cards)
- Joint SIT to start in 3Q, 2001; Re-badge to start in 1Q, 2002
- Based on Java Card 2.1/Open Platform 2.0 w/29K EEPROM space


Sun microsystems
SMITH
John
12345
Sun microsystems
Return Postage Guaranteed
If found, please mail to:
P.O. Box 7551
Mountain View, CA 94039-9808 USA
Security Emergency Assistance
1-800-HELP-001 US & Canada
1-415-856-9871
009985
JAVA
Java Powered
Sun, Sun Microsystems, the Sun logo, Java and the 100% Pure Java logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.
www.sun.com www.sun.com www.su
citi
1234-5678-9012-1234

Sun Microsystems’ Corporate Badge Program (Cont.)

- Building Access (Mifare & Mag-stripe)
- Sun Ray™ workstations Session Mobility
- System Login (secure storage of ID/Password) via WinTel, Solaris™ or Sun Ray workstations
- Remote Access Authentication (e.g., challenge-response, synchronous, or VPN based)
- Multiple digital certificates (e.g., for encryption and authentication)
- Card and Application Life Cycle Management System (LCMS) and Second Tier
Customer Service

JavaOne℠

Sun's 2001 Worldwide Java Developer Conference™

Java Card™ and Open Platform Technology-based Solutions

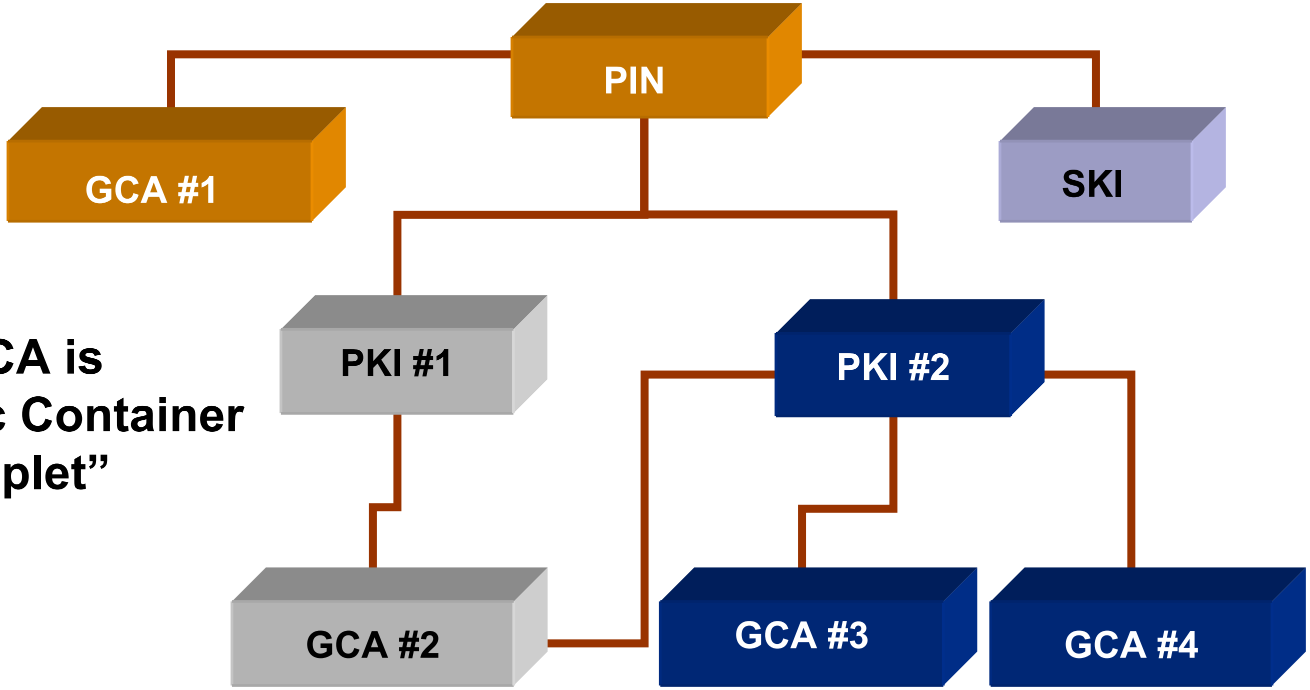
Sun Corporate Badge— *A Multi-application Implementation of Java Card™ Technology*

- Use leading-edge features of the Java Card platform:
  - Real multi-application implementation with independence between applications
  - Use Shareable interface to share PIN authentication within card
  - Use crypto API for RSA, including on-card key generation
  - Use instantiation parameters to define applets behavior for run-time
  - Allows applets update post-issuance

Sun Corporate Badge Chip Card Applications

- ID: Store user identification and manage PIN
- Login: Login to Wintel, SunRay and Solaris platforms
- PKI: Generate and store key pairs and certificates; used for encryption, e-mail, SSL authentication; compatible with PSM and PKCS#11 client software
- SKI: Store symmetric key X9.9 for Sun.net access; generate response from X9.9 challenge
- Quick Password: Secure and convenient storage of user private passwords

Card Applets Relationship



GCA is
“Generic Container
Applet”

One Application Requires Several Card Applets

App. Management System Must Track Card Applets Configuration

Life Cycle of the Smart Card: Open Platform

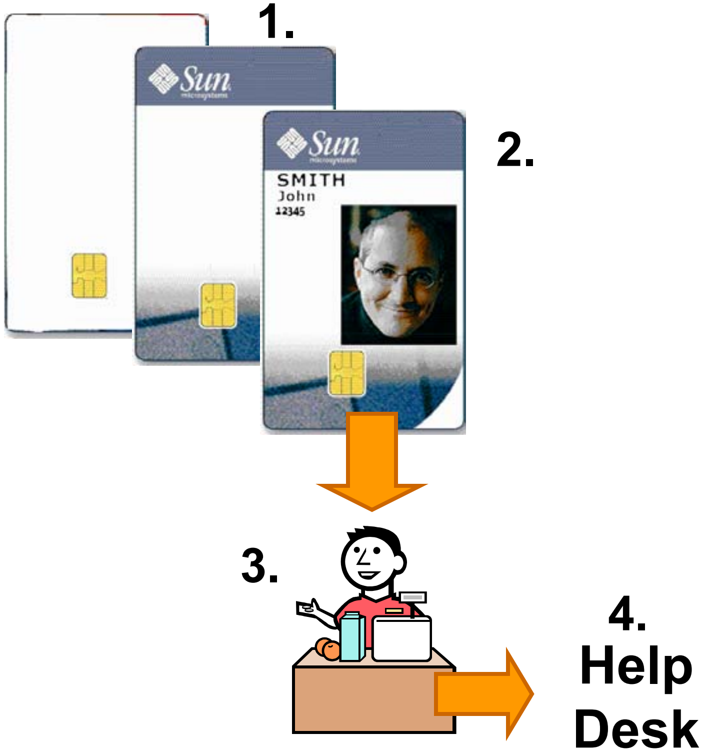
- Open Platform (OP) is defined by a consortium; becomes an industry standard for Smart Cards
- Specifies the interface between the outside world and the Card’s JVM
- Defines life cycle states for entities of the card: platform and applets
- Secure channel brings end-to-end cryptography: from chip to back-end system (data authenticity, confidentiality, integrity)
- Services are exposed via Java™ APIs for card applets

JavaOne℠

Sun's 2001 Worldwide Java Developer Conference

Architectural and Technical Lessons learned from the Sun Corporate Badge Program

Life Cycle of a Smart Card



1.

2.

3.

4. Help Desk

1. **Manufacture** card: build, print card background and serial number and load applets
2. **Issue** card: Print name and picture; load chip with personal information
3. **Use and update** applications
4. **Track and replace** for lost, stolen, revoked cards

- Requires Card Life Cycle Management System (LCMS)
- Requires back-end Application Servers

What Is the Card Life Cycle Management System? (LCMS)

- The LCMS Tracks and maintains information about a card life cycle
- Design principles
  - Based upon the Open Platform standard
  - Separates the platform management from the application management
  - Handles card life cycle and card software configuration
  - Does not process application transactions
- Based on a principle of privacy so that it does not store any application data.

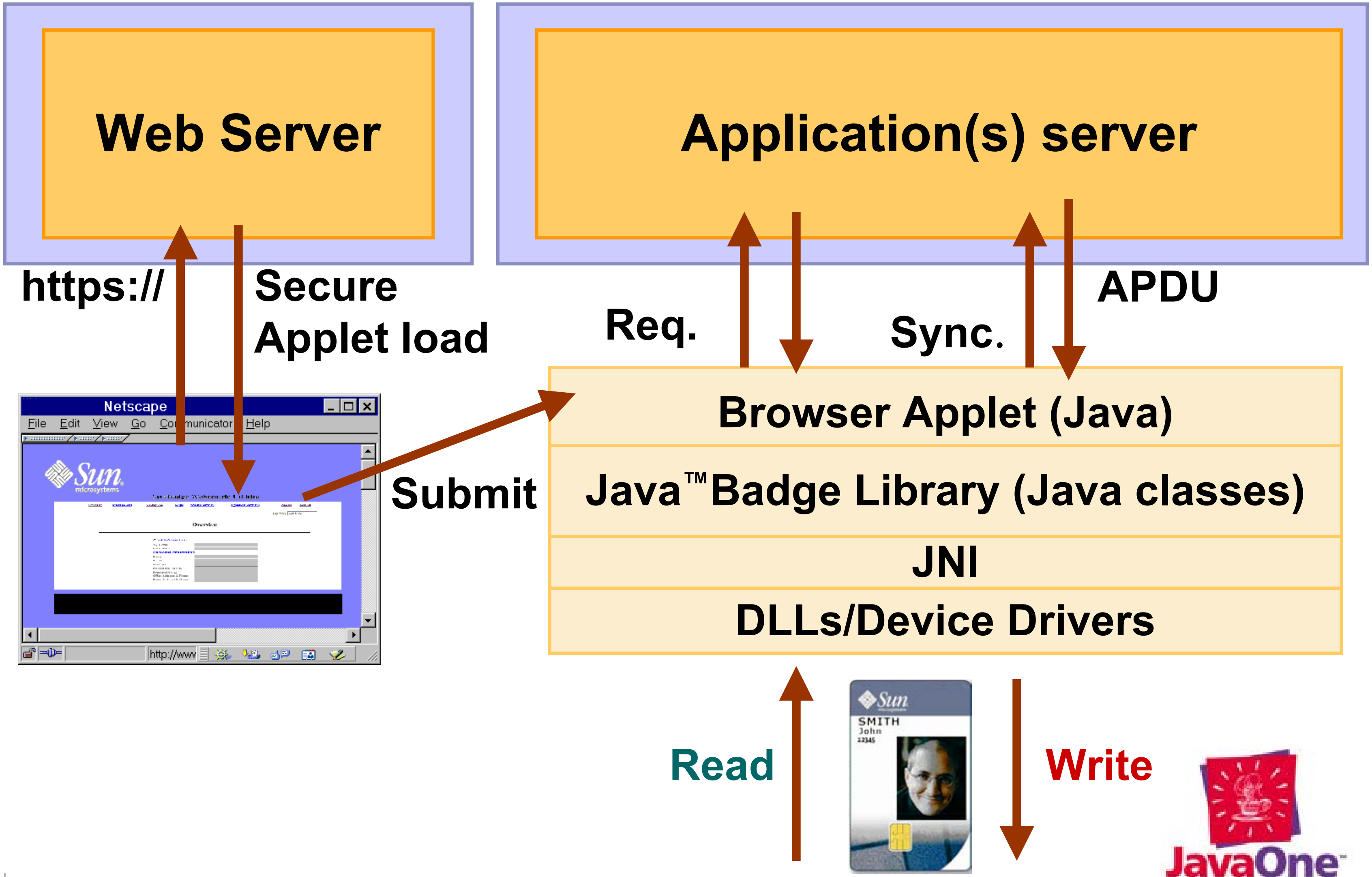
LCMS Architecture Leverage on Standards

- Partitioning allows many corporations to use the service
- Has standard interfaces for back-end systems or Application Servers within the corporation
- Is platform ‘agnostic’—uses platform independent languages and protocols Java™, XML…
- => Makes economical sense to use the Internet as a transport: any corporation has access
  - XML based messaging: Open, Easy to develop interfaces, works with any platform
  - SSL with client authentication: brings confidentiality, integrity, authenticity

The Application Server Concept

- A system within the corporation which interfaces with the LCMS to handle application transactions
- Performs card personalization and application transactions for one application
- Can be centralized or distributed
- Runs on any platform (Solaris™ OS, Win NT...)
- Communicates with LCMS through Internet, using HTTPS+XML as transport
- Communicates with client using Servlets and Java™/JavaScript™ technologies in browser
- Communicates with other enterprise servers with other protocols (e.g. LDAP)

The Application Server Principle



Web Server

Application(s) server

https://

Secure Applet load

Req.

Sync.

APDU

Submit

Browser Applet (Java)

Java™ Badge Library (Java classes)

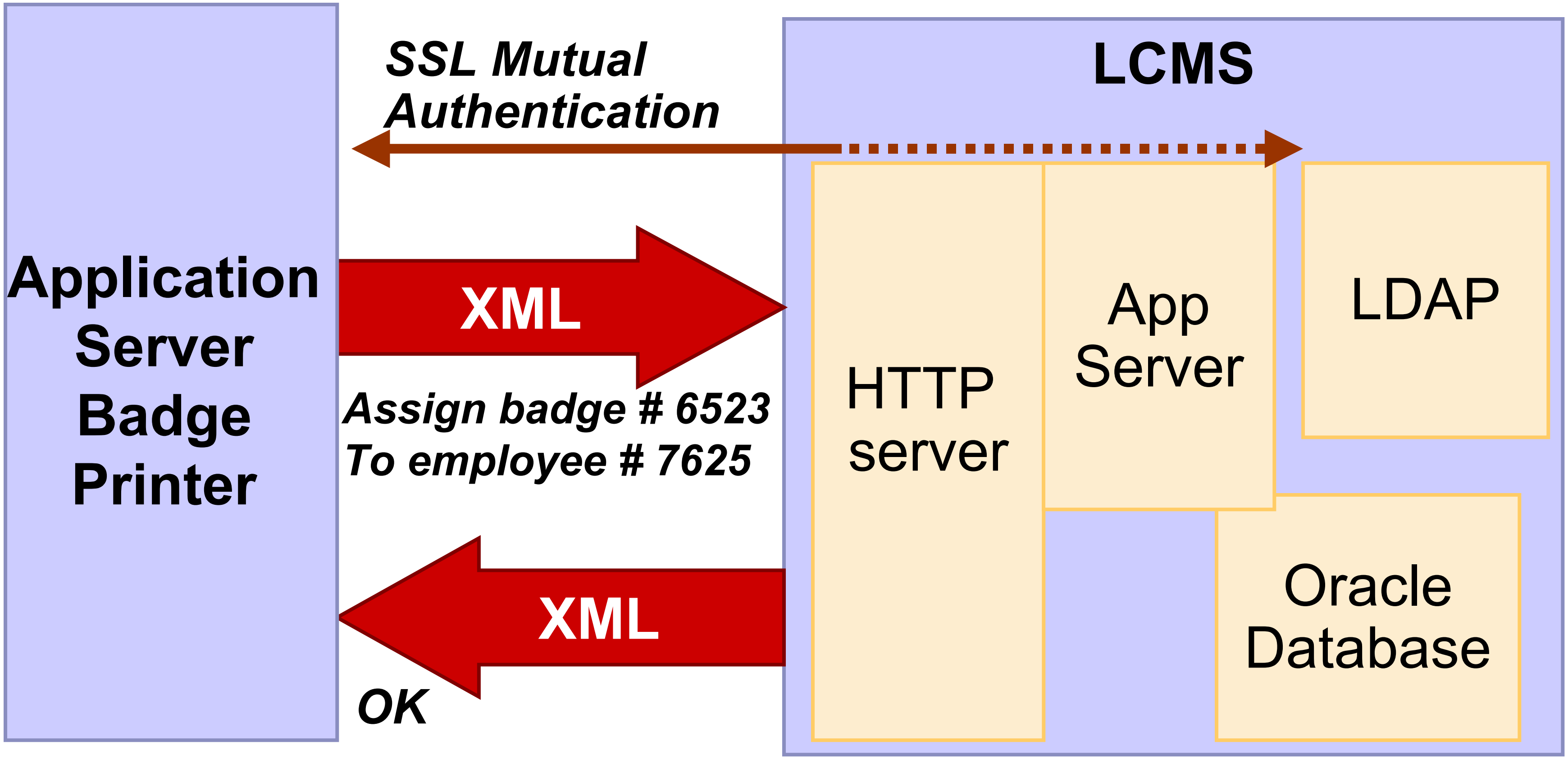
JNI

DLLs/Device Drivers

Read

Write

Example of Messaging to LCMS



Application Server Badge Printer
SSL Mutual Authentication
LCMS
XML
Assign badge # 6523 To employee # 7625
XML
OK
HTTP server
App Server
LDAP
Oracle Database

Badge Printer Submits the Issuance Message

XML Message to LCMS

- Message example: Badge Printer to LCMS

```
<..Message header..>
        <CardUniqueId>6523</CardUniqueId>
        <EmployeeId>7625</EmployeeId>
        <State>CS_PRINTED</State>
        <Time>2001-08-24T13:20:00.000
      05:00</Time>
    <..Message footer..>
```

Summary

- Use Smart Cards: essential in ensuring secure transactions over the Internet for added security, convenience and mobility
- Focus on the infrastructure: Build a scalable, multi-application support ready for evolution
- Use Java Card™ Technology: It is dominating the multi-application smart card world (e.g., GSM, Logical Access, Financial applications, etc.)
- Use XML: for system intercommunication to alleviate platform dependency and to take advantage of built-in browser security
- Use Java™ technology: Most components are out there to build solutions that alleviate platform dependency; Java™, Java Card™, JSP™, JSSE, EJB™, JDBC™,etc.

JavaOne℠

Sun's 2001 Worldwide Java Developer Conference™

Q&A

JavaOne℠

Sun's 2001 Worldwide Java Developer Conference*