

**ITR-4**

4<sup>th</sup> Infocomm  
Technology  
Roadmap  
Seminar

**iDA**

INFOCOMM  
DEVELOPMENT  
AUTHORITY OF  
SINGAPORE

# Glimpse into the Future of Information Security Technology

Chan Keen Wai  
Director, iSec

**26 November 2002**

collaborate

communicate

innovate

# Outline

- Challenges
- Past Generation
- Present Generation
- Information Security Principles
- Moving Forward
- Building Blocks
- Conclusion

# Challenges

- Automation
- Action at a Distance
- Technique Propagation
- Ever Changing Threats
- Heterogeneous Security Systems
- Overflow Of Information

## Systems

- PCs
- Web Servers

## Security Focus

- Firewalls
- Anti-virus
- VPNs

# Present

- Systems
  - PCs, Servers, PDAs, Phones, etc
  - Web Services
  - Wireless Network, Hotspots, etc
  
- Security Focus
  - Multiple Firewalls
  - Enterprise Anti-Virus System
  - Intrusion Detection System
  - Content Filtering
  - VPN
  - Single Sign On

# Present

- Security Management
  - Vendor Proprietary Interfaces
  
- Bridge/Patch
  - Agent
    - Capture and Transmit
    - Translate Raw Data
  - Interoperation/Alliances
    - One to One (bi-directional)
    - One to Many (uni-directional)

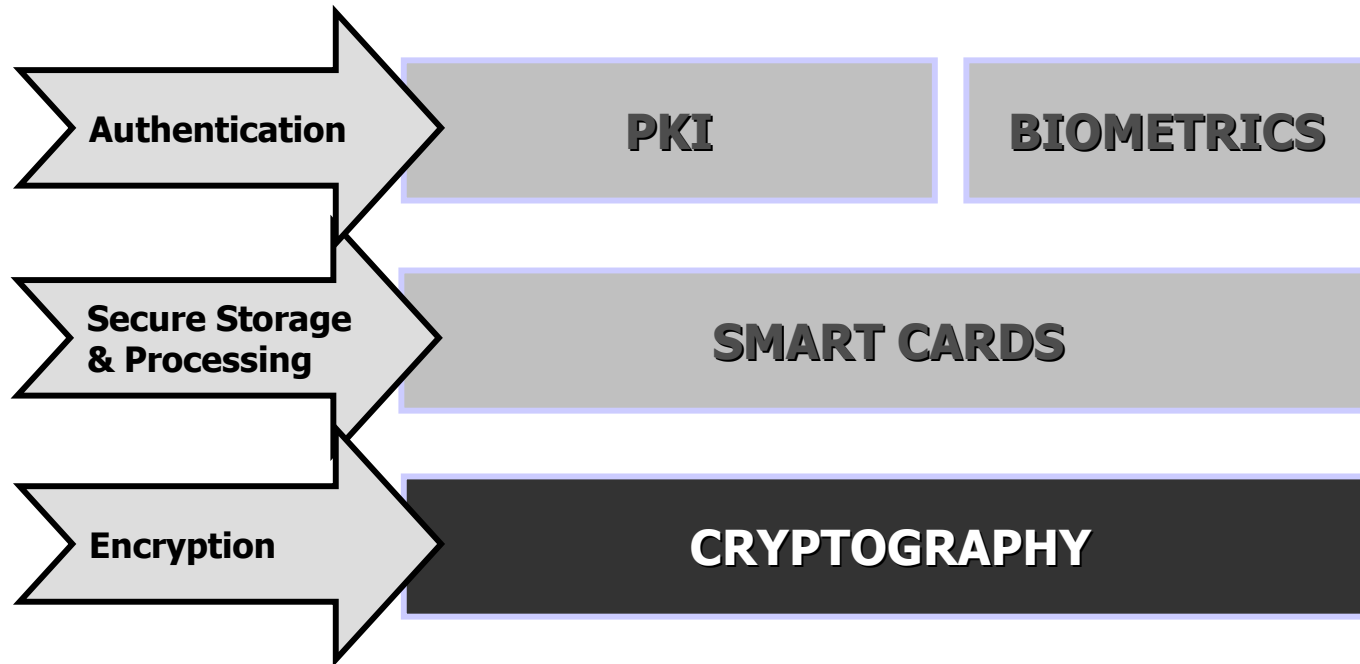
# Information Security Principles

- Defence in Depth
  - Layers of Controls
  
- Time Based Security
  - Protection > Detect + Response

## Central Security Management

## Outsourcing of Security Services

# Building Blocks



- Cryptography
- Smart Cards
- Biometrics
- PKI

# Cryptography

## ■ The Implicit Backbone of Security

### Key Trends

- DES phased out by 3DES & AES, with AES being dominant
- RSA dominant. ECC emerging for mobile devices
- Quantum Cryptography emerges on the radar
- ECC studies to push Identity-Based Cryptography
- Hardware-based cryptographic devices

# Smart Cards

- A protected storage and processing environment for electronic credentials and other data and applications

## Key Trends

- Single multi-application smart card as commerce services converge
- EMV de-facto basic financial standard
- Smart Card Operating Systems moving towards open platforms; Multos & JavaCard

# Biometrics

- Potential for Widespread Biometrics as it expands beyond Niche Applications

## Key Trends

- Iris Recognition expected to be 2nd largest technology in terms of revenues
- Privacy issues arise against biometrics
- ISO/IEC standards for biometric API and identity verification in smart cards in 2004
- ISO/IEC standards for biometric in travel document in 2005

# PKI

- Best technology for strong authentication but have barriers to overcome

## Key Trends

- PKI in a Card
- Wireless PKI for Mobile Services
- Lightweight PKI
- Outsourcing of PKI Operations

# Open Standards

## Common Open Policy Service (COPS)

- IETF Draft for Policy Provisioning
- Simplicity
- Interoperability
- Security

# Central Security Management

## Characteristics

- Monitoring
- Consolidation
- Correlation
- Investigation
- Correction
- Reporting

# Monitoring

- Inspect logs and alerts for security exceptions
  
- Patterns of Potential Security threats, such as:
  - Firewall intrusion attempts
  
  - Inordinate number of requests in a short time period

# Consolidation

- Central Management Console
- Bring together network and system event logs and alerts
- Data normalization

# Correlation

- Identifying pattern over very large number of events
- Infer an alarm from a set of related events

# Investigation

- Analyze all available information; determine what happened
- Disseminate information per policy, using secure channels
- Collect and preserve evidence, including chain of custody
- Root-Cause Analysis

# Correction

- Contain damage
- Eliminate all means of intruder access
- Return systems to normal operation
- Perform tasks in response to an event
- Faster fault correction

# Report

- Central report system
- Types
  - Trend analysis
  - Security status of Lines of Business or critical assets
  - Attack types
  - Targeted assets
  - Response times and resolution

# Outsourcing of Security Services

- Scarcity and Expense of Staff
- 24/7 Management
- Not core Business

# Conclusion

- Force Multiplier
- Data to Information/Intelligence
- Quick Resolution

# In Collaboration With

Infocomm Security Technologies for E-Commerce



# Thank You