Killer Application of PKI
(Panel Discussion)

Kwok- Yan Lam
4 October 2004
What Is A Killer Application?

- Killer application of PKI will help make PKI successful

- How do we measure the success of PKI?
  - Number of people using PKI?
  - Number of applications using PKI?
  - Number of organizations using PKI?
  - Importance of people using PKI?
  - Importance of applications using PKI?
  - Importance of organizations using PKI?
  - Amount of money protected by PKI systems?
  - Amount of money made by PKI providers?
What Is A Killer Application?

- It is difficult to quantify and may be wrong to quantify

- What should be the criteria for being successful?
PKI is Successful IF ...

- When you need strong security, you use PKI
  - Any organization
  - Any application
  - Any user

- Killer application uses PKI because of its strength and have insignificant reasons against it
  - The need is obvious – value of data is high
  - Affordable to adopt
  - Cost of deployment is much lower than value of data
  - Low development cost
  - Low integration cost
  - Low user resistance
Killer Application of PKI

- Intrinsic nature
  - The security assurance of PKI is needed
  - The cost of PKI is justifiable
  - The overhead of PKI is justifiable

- Design and implementation features
  - Easy to use and operate
  - Easy to deploy regardless of system platform and architecture
  - Easy to integrate with different application and end user interfaces

- NOT just the nature of application BUT ALSO the design/implementation of the application system
Our Past Experience

- Secure Document Exchange platform for e-Government
  - Require strong security protection
- Design features
  - Support different system platforms
  - Support client-server or peer-to-peer deployment model
  - Integrate easily with mail, web, notes, custom-built applications or as desktop
  - Support different smart tokens and different certificates
- Currently used extensively by a large number of government agencies
In the Near Future

- Smart Passport for Automated Border Control
  - Require strong security assurance
  - Symmetric systems cannot handle cross-border situation
- Design features
  - Smart passport support biometrics identification
  - IC performs biometrics and returns verification results to immigration control officer
  - Visited country has to trust the smart passport
- To be available soon and expect to see pervasive adoption of PKI
  - Due to policy of the US enforced since 1 Oct 2004
  - May further explore multi-application IC
School of Software
Tsinghua University
Beijing 100084
People’s Republic of China

Email: lamky@tsinghua.edu.cn