Biometrics & Smart Cards In Use Today

Christer Bergman
President and CEO, Precise Biometrics
In Use Today...

Alan L. Herto
Chief, Systems Integrity Division
Requirements

- Improved IT security & stronger authentication
- Cost efficient & scalable technology
- Robust & proven products
- Independent technology
Chosen Biometric Technology

- Match-on-Card: Brings biometrics, smart cards and PKI together

Match-on-Card Definition

- The process of matching a biometric sample against a reference template inside the secure environment of a smart card.
- The reference template cannot be read out from the card, but only used internally by the matching process.
PKI & Fingerprint Match-on-Card

PKI with PIN-codes

PKI with Biometrics

Secure INTERNET

4563 6437

Secure INTERNET
Why Match-on-Card?

- **Scalability**
  The matching is performed locally on the card – the system scalability doesn’t have any limit – the matching is fast and independent of open networks.

- **Security**
  Two factor authentication – demanding both a valid smart card, where fragments of your fingerprint are securely stored – and your fingerprint.

- **Privacy**
  The template never leaves the secure environment – it cannot be copied or stolen – the privacy issue is radically resolved.
Technology Interoperability

- Through open standards and cooperation with several partners, Precise Biometrics’ products work with various security applications, smart cards and readers.
Standards Interoperability

- ANSI/NIST-ITL 1-2000
- ANSI/INCITS 381-2004
- MULTOS Biometry API
- Open Card Framework
- JCF Biometry API
- ISO 7816-11
- ISO 14443
- GSC-IS
- MAD
- FIPS 140-2
Provider Interoperability

ActivCard MOC  beTRUSTed MOC
Datakey MOC  Hypercom MOC
I/O Software MOC  ISL
Schlumberger MOC  SCSquare MOC
Siemens MOC  Tarmin MOC
SUN MOC  Utimaco MOC
AFIS readers
Billionton
Cherry MOC  Keysource MOC
Digitus MOC  Precise Biometrics MOC
Targus

Axalto MOC
Datakey MOC
Keycorp MOC
Miotec MOC
Oberthur MOC
Orga MOC
Philips/IBM MOC
Siemens MOC
SCSquare MOC
SUN MOC
Independent Technology

- Multiple suppliers
  - "Match-on-Card" should work with different readers and major applications on the market

- Works on all cards
  - "Match-on-Card" should be designed to run on all processor smart cards - Java, MULTOS, ISO 7816

- High Performance
  - "Match-on-Card" should have high performance in terms of speed and accuracy, even as an applet or codelet

- Standard compliance
  - "Match-on-Card" should comply with major standards in the field – ensuring full interoperability with all types of cards and biometrics
Department of State
Biometrics, SMART Cards & PKI - In Use Today

IRM/OPS/ITI/SI

Alan L. Herto
(Hertoal@state.gov)
Biometrics, PKI Mission at State

• Mission:
  - To provide the Department of State with a robust Biometric/PKI that will improve IT security while reducing cost and increasing customer satisfaction
  - To satisfy the requirements of the President’s Management Agenda and the GPEA, e–Sign, e–Gov, and FISMA legislation
• Near Term Goal:
  - Elimination of Passwords on the Department OpenNet+ system (over 45,000 users)
• Future Goal:
  - Enable Single Sign On (SSO) to critical Department applications
• Current Status:
  - At IOC, FOC by December 2006
  - Over 1000 readers deployed and another 4200 in Diplomatic Pouch for Overseas Diplomatic Facilities
  - Requires Windows XP and Active Directory
  - Providing One on One training to users
  - Re-Enrollment Training for LRAs and RSOs
• Card memory limitations:
  – Current memory usage on 32 kb card
  – Current PKI Certificates/Keys 12 kb
  – Current Physical Access Data 5 kb
  – Future Biometrics Logical Access 4 kb (879 per finger)
  – Future add PKI requirements 10kb

  Total Over 31 kb

  – Some space may be recoverable by only using 2 fingers for the biometrics
  – Very limited for other applications such as medical information or secondary biometric information
Performance Issue

• Unique Global Environment
  – Foreign Service Nationals (FSNs), Hostile Intelligence Services, Downtown Locations = High Vulnerability
  – 168 Countries with over 275 Diplomatic Facilities really equals global
  – Poor in country Infrastructure, Low bandwidth, High latency results in Customer perception that the System is slow
  – While the applications work, protocols, applications and hardware need to be tuned to address global deployments
## Network Impact to Users

<table>
<thead>
<tr>
<th>Test Type</th>
<th>64 Kbps</th>
<th>64Kbps Latency and Error Rate</th>
<th>9.6 Kbps</th>
<th>9.6 Kbps Latency and Error Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Creation</td>
<td>93.6 sec</td>
<td>600 ms at 10^{-5}</td>
<td>154.8 sec</td>
<td>1000 ms at 10^{-5}</td>
</tr>
<tr>
<td>1st Login</td>
<td>9.2 sec</td>
<td>600 ms at 10^{-5}</td>
<td>27.3 sec</td>
<td>1000 ms at 10^{-5}</td>
</tr>
<tr>
<td>Recovery Profile</td>
<td>121.9 sec</td>
<td>600 ms at 10^{-5}</td>
<td>170.3 sec</td>
<td>1000 ms at 10^{-5}</td>
</tr>
<tr>
<td>DN Change</td>
<td>97.9 sec</td>
<td>600 ms at 10^{-5}</td>
<td>163.4 sec</td>
<td>1000 ms at 10^{-5}</td>
</tr>
<tr>
<td>Key Update</td>
<td>164.0 sec</td>
<td>600 ms at 10^{-5}</td>
<td>335.1 sec</td>
<td>1000 ms at 10^{-5}</td>
</tr>
<tr>
<td>Login After Key</td>
<td>9.3 sec</td>
<td>600 ms at 10^{-5}</td>
<td>66.3 sec</td>
<td>1000 ms at 10^{-5}</td>
</tr>
</tbody>
</table>

IRM/OPS/ITI/SI
Questions about the STATE DEPARTMENT Biometrics & PKI Programs
Department of State
Biometrics, SMART Cards &
PKI - In Use Today

IRM/OPS/ITI/SI
BACK-UP SLIDES
PKI Deployment

• Cross Certified with Federal Bridge at High Assurance Level
• Domestic deployment 99% complete (remaining waiting for Windows XP deployments)
• PKI hardware and software installed on over 15,000 desktops, 872 overseas
• Over 17,000 Smart IDs with PKI certificates have been issued
• Complete Overseas deployment by End of 2006

IRM/OPS/ITI/SI
• **Immigration Visa Allocation & Management System Web (IVAMSWEB)**

• **Joint State - Homeland Security deployment**
  – IVAMS is now a PKI enabled system providing Visa control numbers to over **88** DHS Bureau of Citizenship & Immigration Services field offices around the country
  – This system saved US tax payers over **$718,600** last year
  – PKI enabling the system has allowed its use over the internet, resulting in reducing processing time from days in some cases to hours
• Adoption Tracking Service (ATS)
  – Now in development by Consular Affairs Bureau to collect, store, and retrieve adoption-related information both domestically and globally
  – PKI system will issue certificates to approved Non-Governmental adoption agencies for access control purposes
  – This system will provide a higher level of assurance to families that the documents provided are correct and come from a legitimate agency
• Machine Readable Travel Document infrastructure and service is now in development and will be piloted by the end of this year
  - The Bureau of Consular Affairs asked the PKI team to develop the infrastructure and service to digitally sign passport data
  - In conjunction with the International Civil Aviation Organization, (ICAO) the Department worked to establish an international standard and support a better solution for border security
  - Pilot will address Official and Diplomatic Passports first; standard Tourist passports to be incorporated in 2005
  - Enhanced Border Security and Visa Entry Reform Act of 2002 requires biometrics; this application ensures the integrity of the MRTD passports containing biometrics
E-Forms & Secure Mail

• Digital Signature of Standard DoS forms
  - Leave and Earnings
  - Employee Evaluation Reports, etc.
  - Integration work and user Pilot proceeding

• Secure Email, Code Signing
  - Using Entrust Entelligence/Express E-Mail Plug-In, version 6.1
    • Provides Encryption and Digital Signature
  - Code Signing of WEB applets for internal use
Contact Information

Mike Sulak
202-647-2147
SulakMA@state.gov
PKI Contact Information

Tin Cao
Branch Chief
(202) 203-5068
CaoTT@state.gov

Steve Gregory
PKI
(202) 203-5190
GregorySE@state.gov

Blanca Neve
Biometrics
(202) 203-5013
NeveBM@state.gov