Obstacles to PKI Deployment and Usage
- OASIS Survey Results and Draft Action Plan
Agenda

- Background
- Sample Size and Demographics
- Applications
- Obstacles
- Conclusions
- Follow-up Survey
- Action Plan
Background

- OASIS PKI TC formed January ’03
  - Objective: Address issues related to successful deployment of digital certificates
  - TC determined importance of identifying obstacles to PKI deployment and usage

- Survey developed then deployed from June 9 to 22, 2003
  - Invited standard bodies, industry associations, vendors and user associations

- Target Audience
  - Anyone with an opinion, but most interested in those with expertise or experience
Sample Size & Demographics

- Responses
  - 217 answered with 216 considered valid
  - No duplicates or frivolous answers detected
  - Most reflected careful consideration and included textual answers
  - 80% provided email addresses for any follow-up surveys
  - Over 25% provided detailed descriptions of obstacles

- Profiles
  - 44% worked in IT
  - Others included 20 Consultants and 6 Architects
  - Over ½ had a strong technical component in their jobs
  - Over 75% had 5 or more years experience in InfoSec/Privacy
  - 90% have either helped deploy PKI or developed PKI-related software
Primary Job Function
Years Experience with Information Security/Privacy

- 1 year: 1%
- 2 years: 5%
- 3 years: 10%
- 4 years: 10%
- 5 years: 20%
- 6-10 years: 30%
- 11-15 years: 15%
- 16 or more years: 10%
- Not Applicable: 5%
- No Answer: 0%
PKI Experience

- Read About PKI
- Considered Using PKI
- Used PKI
- Helped Deploy PKI
- Developed PKI-related Software

Percentage: 0% to 100%
Employer Sector or Industry

- Government
- Manufacturing (Computer-related)
- Other Services
- Finance
- Education
- Health Care
- Sales
- Manufacturing (non-Computer)
- Other
- No Answer

Bar chart showing the distribution of employer sectors or industries.
Employer Size (number of employees)
Primary Work Location

- North America: 60%
- Europe: 20%
- Asia: 10%
- Australia: 5%
- South and Central America: 5%
- Africa: 0%
Applications

- Participants asked to rate various PKI supported applications as:
  - Most Important
  - Important
  - Not Important

- Weight Ranking
  - Responses were allotted 2 points for Most Important and 1 point for Important
  - Weight ranking computed by dividing the total score by the number of answers
  - For “Other” applications, participants entered applications not in selection list and rated them.

- All applications (except Secure RPC) considered at least “Important” by over 50%
- No application considered “Most Important” by a majority
- Indicates PKI is truly a horizontal, enabling technology with many applications
PKI Application Weights

- Document Signing
- Web Server Security
- Secure Email
- Web Services Security
- Virtual Private Network
- Electronic Commerce
- Single Sign On
- Secure Wireless LAN
- Code Signing
- Secure RPC
- Other Application
Obstacles

- Participants presented a list of obstacles and requested to rank each as:
  - Major Obstacle
  - Minor Obstacle
  - Not an Obstacle

- Write-in responses were solicited and ranked the same way

- Ranking
  - Responses were weight ranked using the same technique as applied for Application Weights
  - No obstacle was ranked “Not an Obstacle” by the majority, indicating all were relevant
  - Top two obstacles rated as “Major” by the majority, top six rated “Major” by a substantial number

- 92% indicated they would use PKI more if obstacles were removed.
PKI Obstacles – Weighted Ranking

- Software Applications Don't Support It
- Costs Too High
- PKI Poorly Understood
- Poor Interoperability
- Hard to Get Started – Too Complex
- Hard for End Users to Use
- Lack of Management Support
- Too Much Legal Work Required
- Hard for IT to Maintain
- Other Obstacle
## Additional PKI Obstacles

<table>
<thead>
<tr>
<th>Summary</th>
<th>Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient ROI/business justification/need</td>
<td>9</td>
</tr>
<tr>
<td>Enrollment too complicated</td>
<td>5</td>
</tr>
<tr>
<td>Smart card problems (cost, driver and OS problems, readers rare)</td>
<td>5</td>
</tr>
<tr>
<td>Revocation hard</td>
<td>5</td>
</tr>
<tr>
<td>Standards (too many, incompatible, changing, poorly coordinated)</td>
<td>4</td>
</tr>
<tr>
<td>Too much focus on PKI technology, not enough on business need</td>
<td>4</td>
</tr>
<tr>
<td>No universal CA</td>
<td>2</td>
</tr>
<tr>
<td>Too complex</td>
<td>2</td>
</tr>
<tr>
<td>Insufficient skilled personnel</td>
<td>2</td>
</tr>
<tr>
<td>Poor implementations</td>
<td>2</td>
</tr>
</tbody>
</table>
Follow-up Survey

- **Motivation**
  - Original survey results indicated more detailed information needed in order to build an action plan

- **Response**
  - Mixed success: 89% respondents participated in the initial survey but overall response was low (74 vs. 216 for the original survey)
  - Many demographic measures unchanged but some differences noted:
    - IT Management down to 26% from 29%
    - S/W Developers down to 9% from 12%
    - Consultants up to 20% from 10%
  - Few differences noted in Application Importance

- Concluded the follow-up survey may be useful in developing the Action Plan
Better Understanding of Obstacles

- Method
  - Participants asked to rank obstacles by relative importance by allocating 10 points among the obstacles
  - Added clarifying questions regarding the obstacles
  - Asked for suggestions on how to address the obstacles
  - Added six additional obstacles identified by respondents in the original survey
Obstacles Ranked by Importance

Software Applications Don't Support It
Costs Too High
PKI Poorly Understood
Too Much Focus on Technology, Not Enough on Need
Poor Interoperability
Hard to Get Started – Too Complex
Lack of Management Support
Hard for End Users to Use
Enrollment Too Complicated
Too Much Legal Work Required
Smart Card Problems
Hard for IT to Maintain
Insufficient Need
Revocation Hard
Standards Problems
Applications Ranked by Need for Improvements in PKI Support

- Document Signing
- Secure Email
- Electronic Commerce
- Single Sign On
- Secure Wireless LAN
- Web Services Security
- Web Server Security
- Virtual Private Network
- Code Signing
- Secure RPC
How Application Support for PKI is Insufficient

- Application support is inconsistent
  - Many applications have no support at all
  - Applications with support vary widely in what services are supported making it difficult to deploy PKI
  - Interoperation is nearly impossible prompting respondents to call for detailed standards to ensure interoperability

- Suggestions for improvement
  - Create guidelines for each type of application on how PKI support should be implemented
  - Encourage vendors to include PKI features in applications (e.g. smart card support)
Costs Ranked by Most Problematic
Other Cost Questions

- “Would you say that these cost problems are largely eliminated if the number of users involved is large (amortizing large fixed costs)?”
  - Yes: 31%  No: 45%  No Response: 24%

- “Do your comments about costs pertain primarily to outsourced PKI services, in-house PKI, or both?”
  - Outsourced: 9%  In-house: 23%  Both: 24%  No Response: 24%

- Comments on what to do to help reduce costs include:
  - Promote specific standards that avoid the need for customization
  - Outsource
  - Encourage free PKI S/W and free CAs for low-assurance applications
Parties Ranked by Greatest Need for PKI Understanding

- Senior Management
- Users
- IT Management
- IT Staff
- Vendors
- Other
Where the Most Serious Interoperability Problems Arise

- Path Validation
- Smart Card
- Unusual Certificate Contents
- Cross-Certification
- Certificate Issuance
- Certificate Revocation
- Protocols that Use PKI
- Other
Interoperability Comments

- Standards are inadequate
- In some cases (e.g. certificate management) there are too many standards
- In others (as with smart cards) there are too few
- When present, standards are frequently too flexible and too complex
- Overly flexible and complex standards create an environment where implementation from different vendors rarely interoperate
Action Plan

- Status
  - An initial draft is circulating within the OASIS PKI TC with a schedule to announce it in February 2004
  - In the interim, the TC will be asking all stakeholders (users, vendors, standards groups, and experts) to review, comment on, and support the plan

- Features
  - Develop specific profiles or guidelines on standards use
  - Promote interoperability and testing events, possibly with branding and certification
  - Provide a “cookbook” with easy steps for building a simple PKI
  - Provide free software and CAs so people can set up and test PKI in low assurance scenarios
Realities

- The OASIS PKI TC recognizes it cannot act independently in developing and implementing this Action Plan.

- The PKI TC will consult with as many parties as possible to gather feedback and support.

- The PKI TC recognizes that many of the actions should be undertaken by others.

- In a sense, this serves as a Call to Action for the industry:
  - It may seem presumptuous for the PKI TC to issue such a call, but the TC is only passing on the requests made by hundreds of PKI users and customers expressed through the survey.

- The PKI TC will work with relevant parties before announcing this plan so the document can become a consensus plan with buy-in from all concerned.
Invitation

- All stakeholders are invited to join the OASIS PKI TC and participate in our efforts to advance the successful use of digital certificates.

- The PKI TC is requesting stakeholders to review and comment on the draft Action plan.

- The PKI TC will post the plan for external review in November and December.
Discussion