OASIS PKI Action Plan – Overcoming Obstacles to PKI Deployment and Usage

Steve Hanna, Co-Chair, OASIS PKI Technical Committee
Internet 2 Members Meeting
April 19, 2004

Agenda

- OASIS PKI Technical Committee
- PKI Obstacles Survey
- PKI Action Plan
- How You Can Help

OASIS PKI Technical Committee

- Objective
  - Address issues related to successful deployment of digital certificates
- Membership
  - Open to any OASIS Member (minimal cost)
  - Currently 21 Voting Members
  - Mix of PKI vendors, customers, consultants, and others with PKI interest
- Activities
  - PKI Obstacles Survey
  - PKI Action Plan
- http://www.oasis-open.org/committees/pki

OASIS

PKI Obstacles Survey

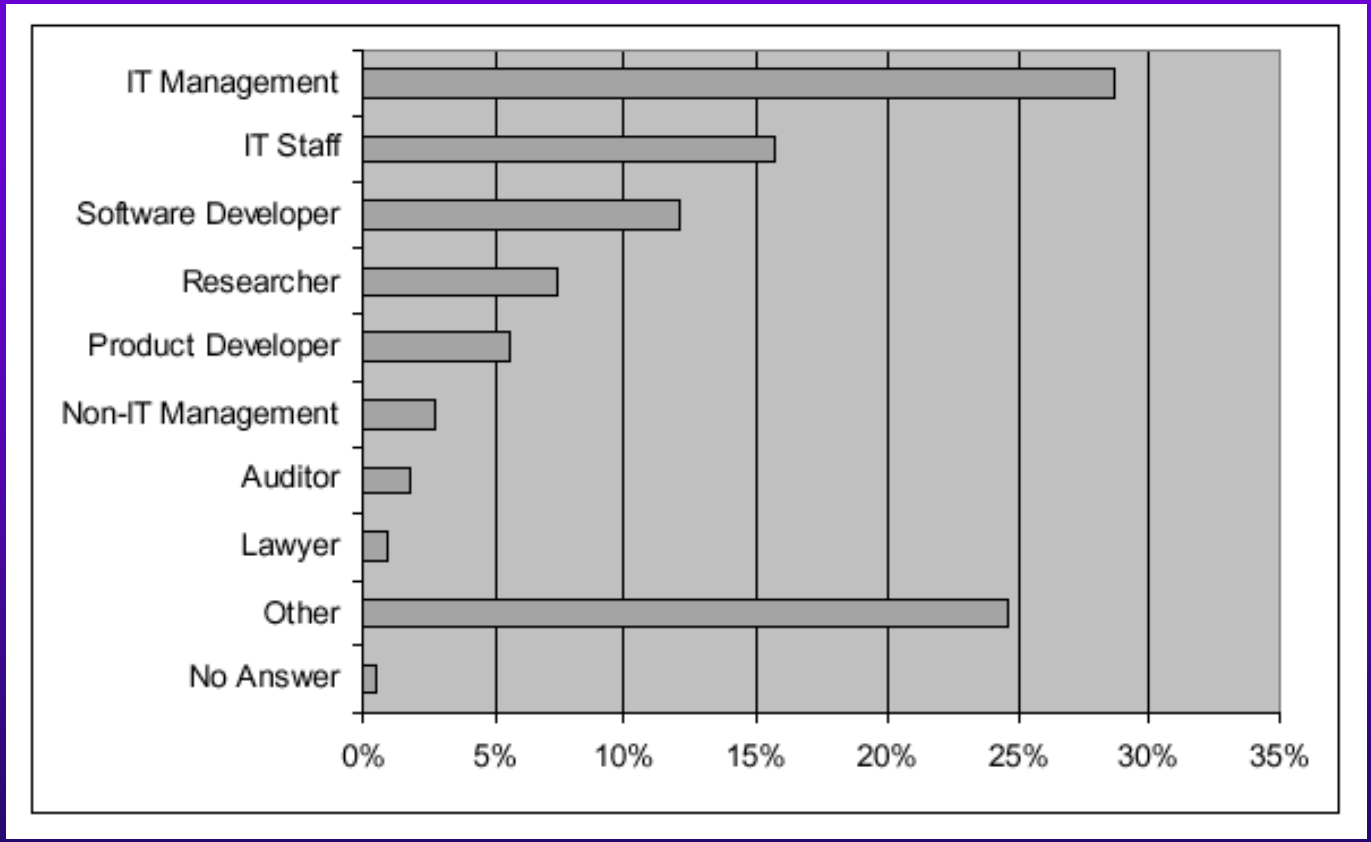
- Objective
  - Identify primary obstacles to PKI deployment and usage
- Target Audience
  - Anyone with an opinion, but most interested in those with significant PKI expertise or experience
  - Invitations sent to email lists related to PKI: standards bodies, industry associations, vendors, and user associations
- Two surveys run in Summer 2003
  - Initial Survey in June
  - Follow-up Survey in August

Sample Size & Demographics

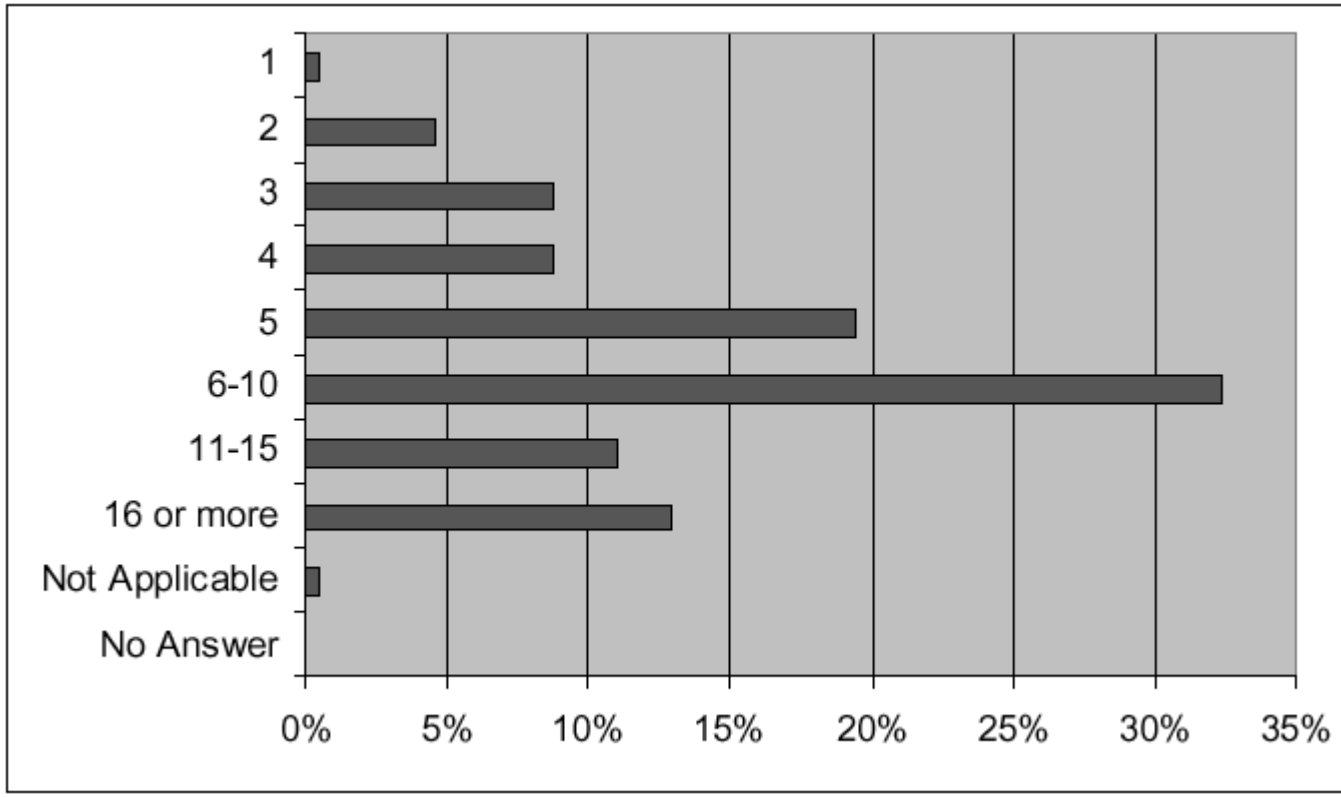
- Responses
  - 217 answered with 216 considered valid
  - No duplicates or frivolous answers detected
  - Most reflected careful consideration and included textual answers
  - 80% provided email addresses for any follow-up surveys
  - Over 25% provided detailed descriptions of obstacles
- Profiles
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

OASIS

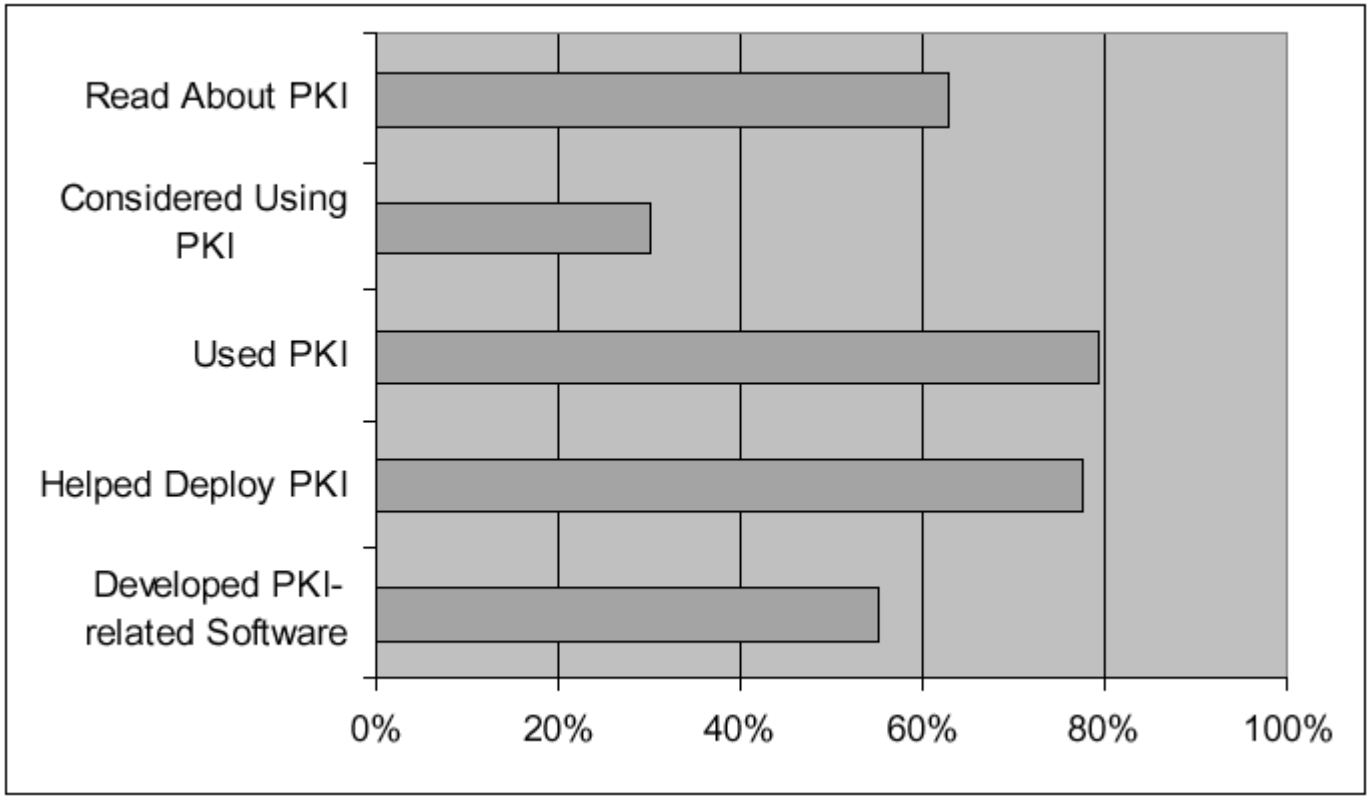
Primary Job Function



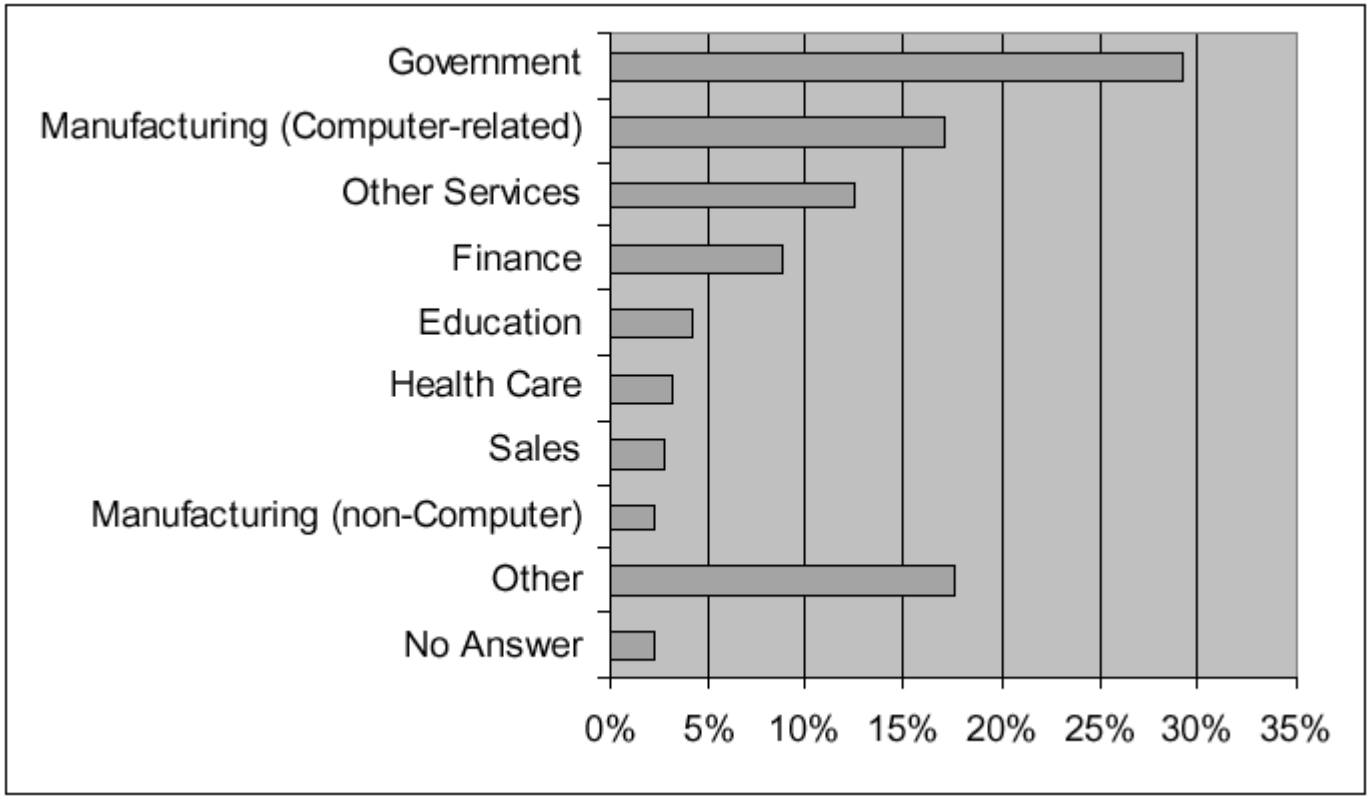
Years Experience with Information Security/Privacy



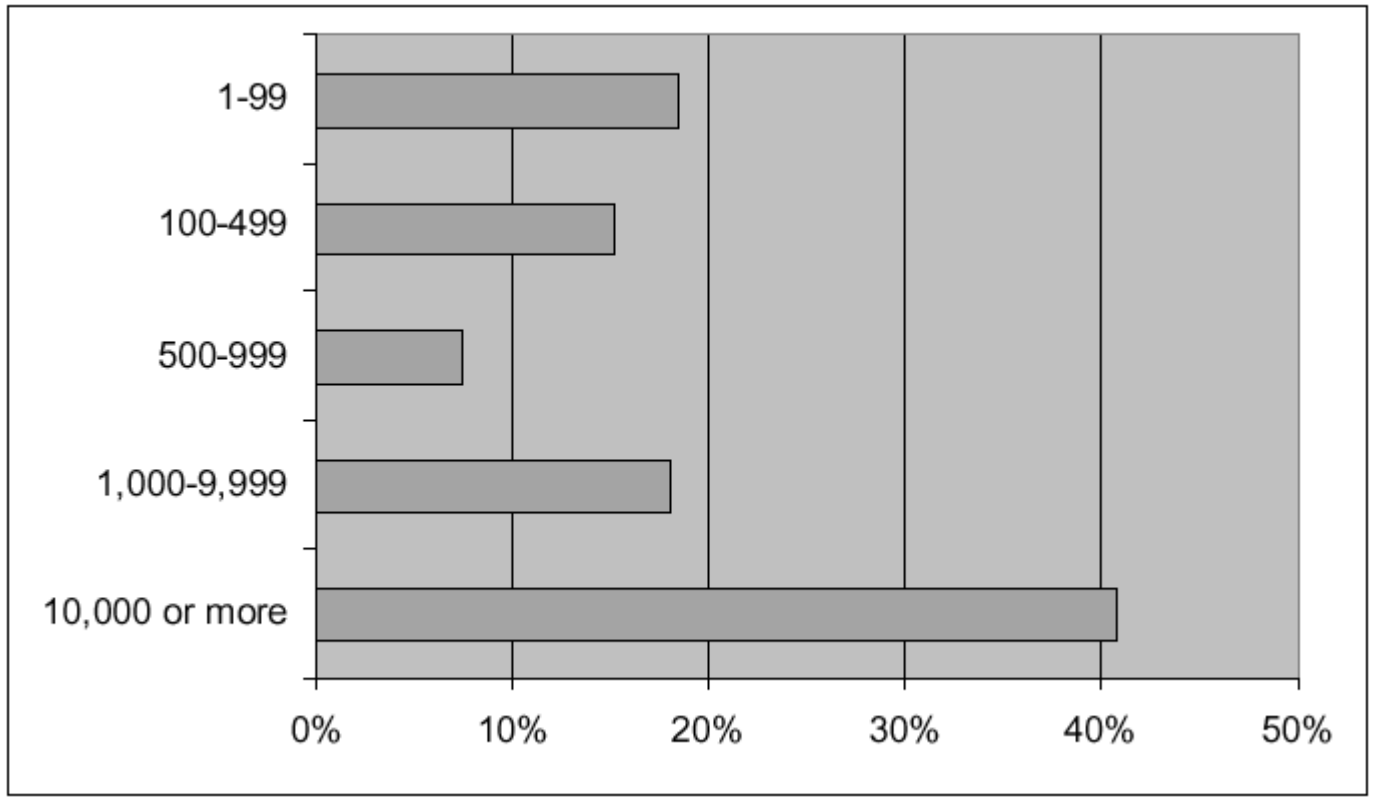
PKI Experience



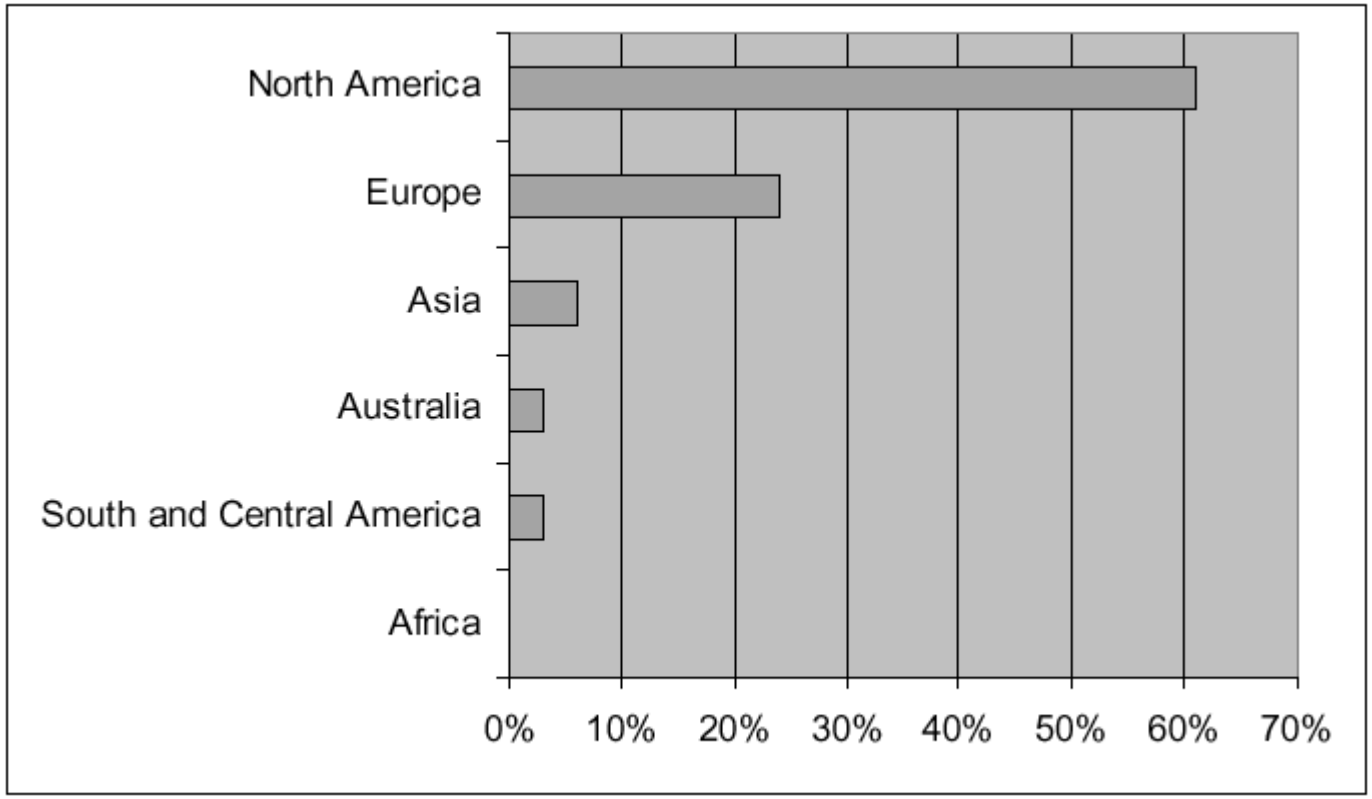
Employer Sector or Industry



Employer Size (number of employees)



Primary Work Location

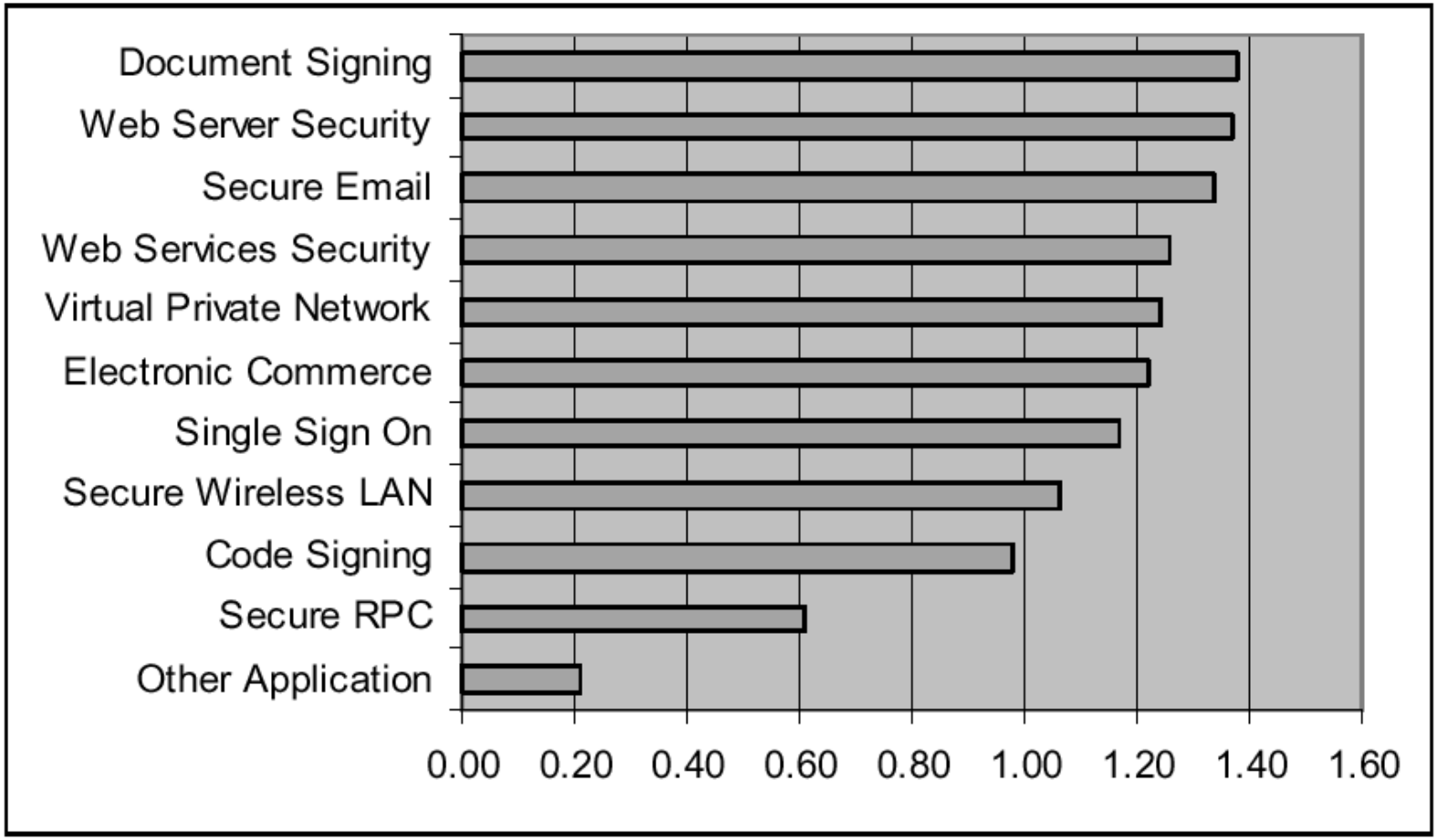


Applications

- 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

OASIS

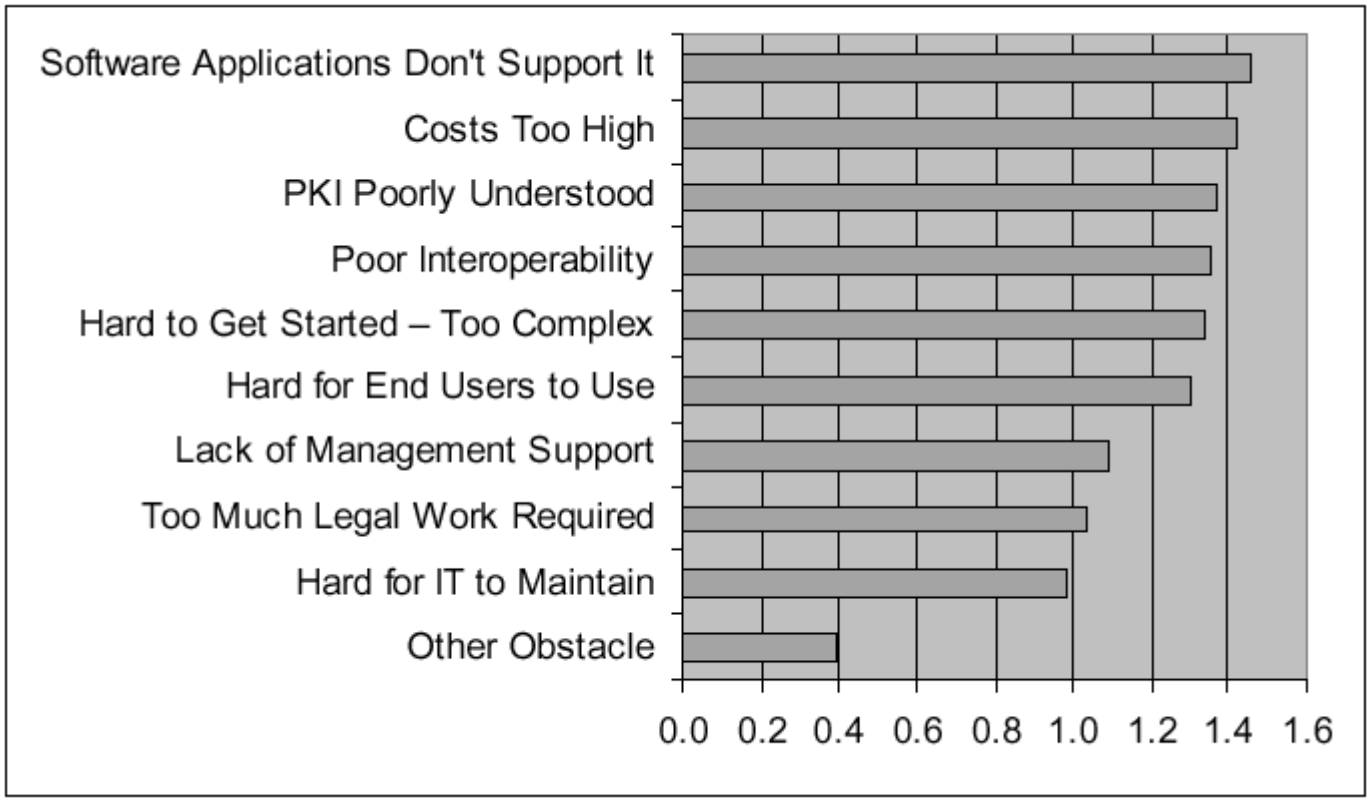
PKI Application Weights



Obstacles

- Participants presented a list of obstacles and requested to rank each as:
  - Major Obstacle
  - Minor Obstacle
  - Not an Obstacle
- Write-in responses (“Other”) 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



Additional PKI Obstacles

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

OASIS

Follow-up Survey

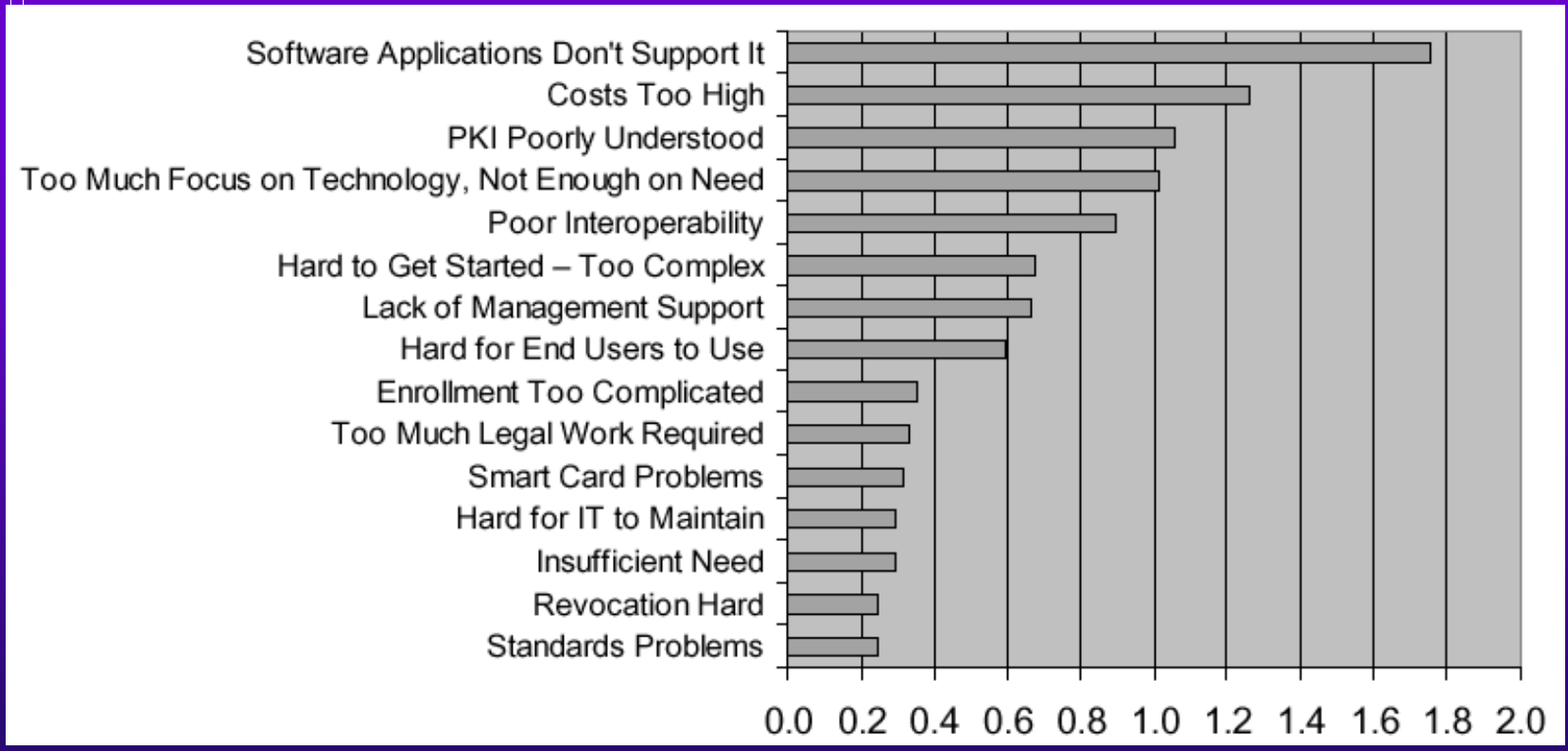
- Motivation
  - Original survey results indicated more detailed information needed in order to build an action plan
- Response
  - Mixed success: 89% respondents participated in the initial survey but overall response was low (74 vs. 216 for the original survey)
  - Many demographic measures unchanged 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

OASIS

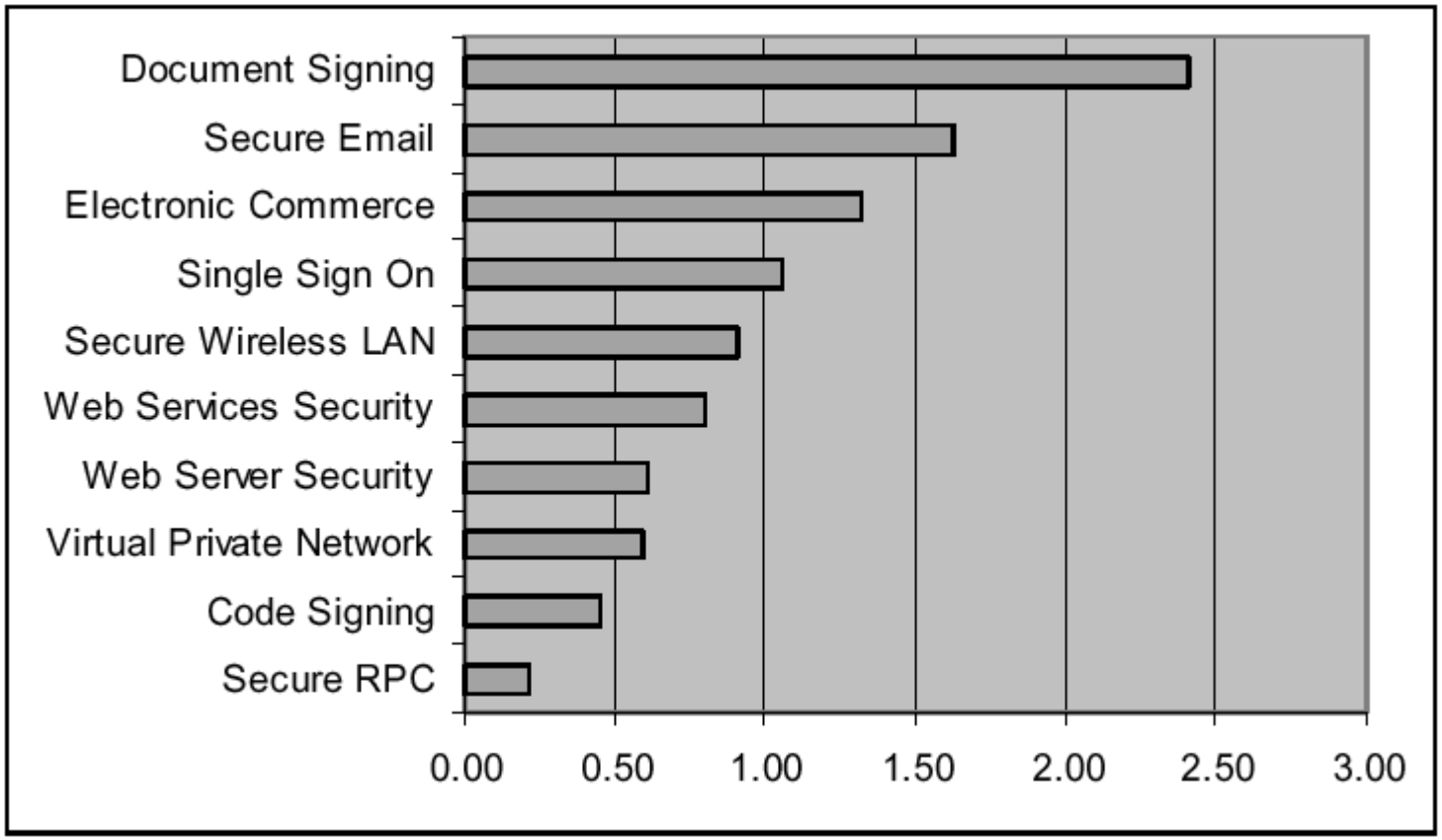
Better Understanding of Obstacles

- 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



Applications Ranked by Need for Improvements in PKI Support

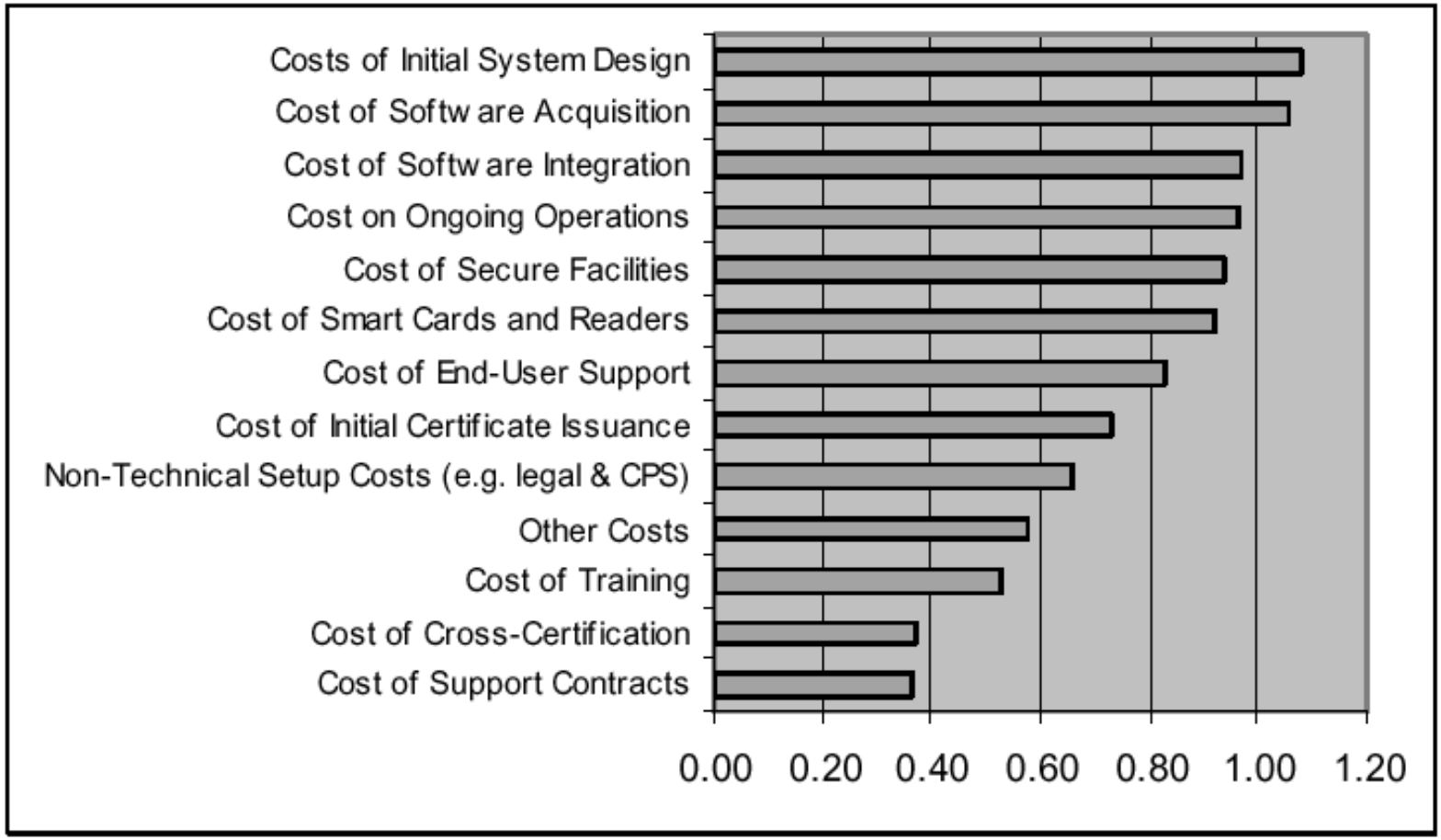


OASIS

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 OS's (e.g. smart card support)

Costs Ranked by Most Problematic



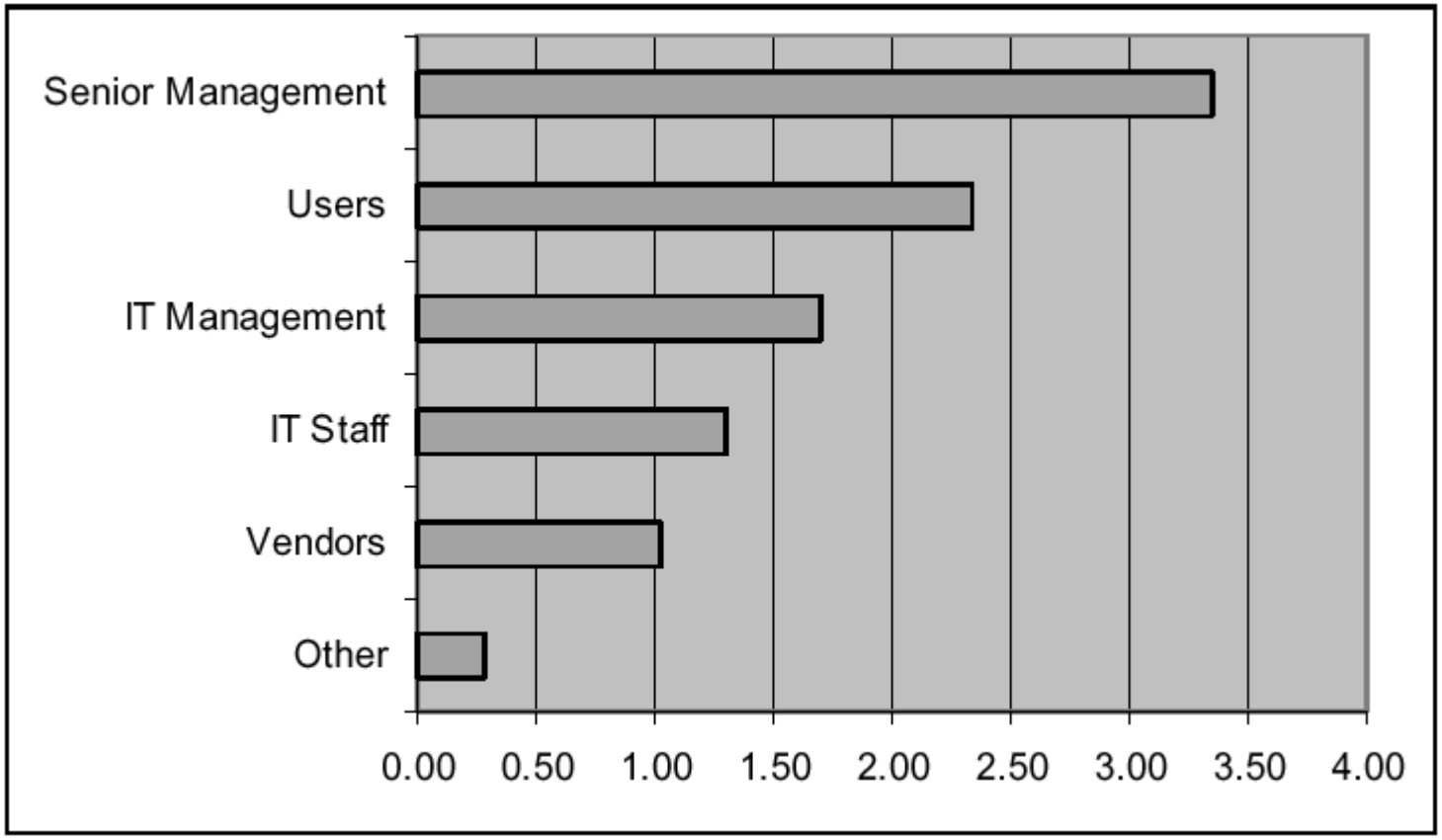
OASIS

Other Cost Questions

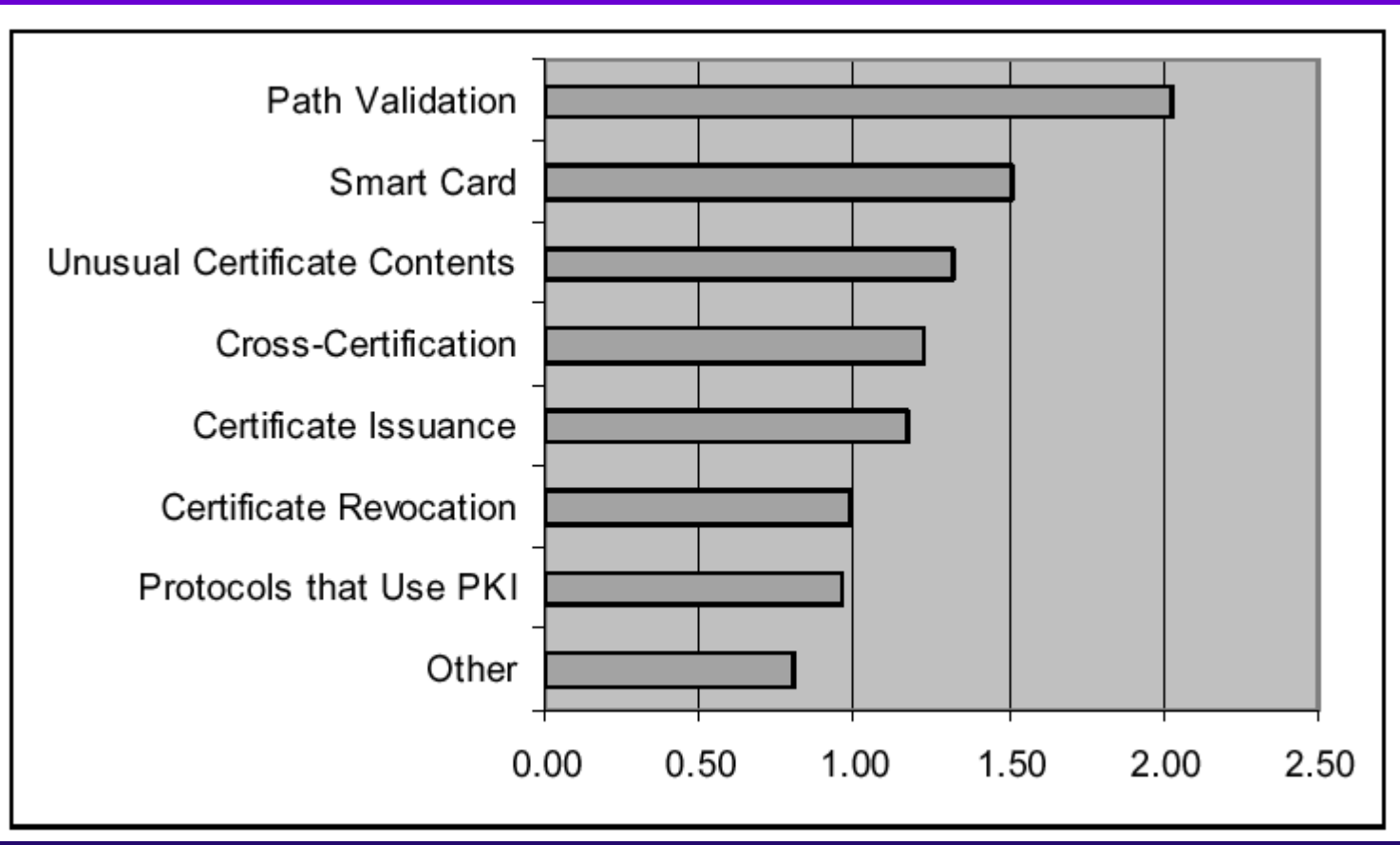
- "Would you say that these cost problems are largely eliminated if the number of users involved is large (amortizing large fixed costs)?"
  - Yes: 31% No: 45% No Response: 24%
- "Do your comments about costs pertain primarily to outsourced PKI services, in-house PKI, or both?"
  - Outsourced: 9% In-house: 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

OASIS

Parties Ranked by Greatest Need for PKI Understanding



Where the Most Serious Interoperability Problems Arise



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

OASIS

OASIS PKI Action Plan

- Status
  - Drafted by OASIS PKI TC based on survey responses
  - Circulated widely for review and revised in response
  - Announced at RSA Conference, February 2004 with 24 Individual Supporters and 8 Organizational Supporters
  - Implementation starting

Action Items

- Develop Application Guidelines for PKI Use
- Increase Testing to Improve Interoperability
- Ask Application Vendors What They Need to Add PKI Support
- Gather and Supplement Educational Materials on PKI
- Explore Ways to Lower Costs

Action Plan for the Industry

- 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

OASIS

How You Can Help

- Read the PKI Action Plan
  - http://www.oasis-open.org/committees/pki/pkiactionplan.pdf
- Sign On as an Individual or Organizational Supporter
- Join the OASIS PKI TC
  - http://www.oasis-open.org/join
- Help Implement the PKI Action Plan
- To follow up, contact pki-tc-chairs@lists.oasis-open.org

OASIS

Discussion