Analysis of August 2003 Follow-up Survey on Obstacles to PKI Deployment and Usage

Prepared and Published by the OASIS Public Key Infrastructure (PKI) Technical Committee (TC)

Author: Steve Hanna (Sun Microsystems, Inc.)

Date: October 1, 2003

Version: 1.0

FINAL

Table Of Contents

---

1. Background to the Survey

The OASIS Public Key Infrastructure (PKI) Technical Committee (TC) was formed in January 2003 with the express purpose of addressing issues related to the successful deployment of digital certificates. Further information on the OASIS PKI TC can be found at: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pki

During initial meetings of the PKI TC, the members agreed that an important role for the TC would be to identify obstacles to PKI deployment and usage so that those obstacles can be addressed. The TC members had many opinions about which obstacles are most critical, but it was agreed to conduct a survey to obtain a more objective analysis.

A web-based survey was conducted in June 2003, asking respondents to identify the most important obstacles to PKI deployment and usage. This survey was successful in attracting a large number of highly qualified respondents, who identified certain specific obstacles. A short summary of that survey's results is included in Appendix A of this document. For more details, see the full report at
http://www.oasis-open.org/committees/pki/pkiobstaclesjune2003surveyreport.pdf

After reviewing the results of this survey, the PKI TC determined that more detailed information was needed in order to decide how to address them. For instance, "Costs Too High" was one of the most commonly cited obstacles. In order to address this obstacle, the PKI TC needed to know which costs were most problematic.

Therefore, the PKI TC prepared a follow-up survey, posted it on the web, and asked people who responded to the first survey and provided an email address to complete the follow-up survey. This document analyzes the responses to the follow-up survey and provides conclusions and recommendations.

2. Survey Sample

Invitations to participate in the Follow-up Survey were sent only to people who responded to the June 2003 Survey and provided an email address. This was intended to maintain consistency between the initial survey respondents and the follow-up survey, avoid the need to impose on others by sending out many invitations, and enable us to tie follow-up responses to demographic information collected with the June 2003 Survey.

This approach met with mixed success. Most respondents to the Follow-up Survey (89%) had previously responded to the June 2003 Survey, so we were able to tie in demographic information. Unfortunately, the small set of invitations sent out (and perhaps the August timing of the survey) resulted in a fairly small number of responses (74 vs. 216 for the June 2003 Survey).

2.1. Validity of Survey Responses

The low number of responses, combined with the fact that the respondents are self-selected from a self-selected pool, increases the risk that the responses are not indicative of opinions throughout the target sample. The results could be skewed by a small number of opinionated respondents. To determine whether this is likely, it is useful to compare the demographics and opinions of the Follow-up Survey respondents and the June 2003 Survey respondents.

2.2. Demographic Analysis of Respondents

The June 2003 Survey analysis includes an in-depth demographic analysis of the respondents for that survey. Instead of including a similar analysis here, we will only point out the demographic differences between the June 2003 Survey respondents and the Follow-up Survey respondents.

The Follow-up Survey respondents were more experienced with PKI. For each of the five categories of PKI involvement in the June 2003 Survey (Read About PKI, Considered Using PKI, Used PKI, Helped Deploy PKI, and Developed PKI-related Software), the Follow-up Survey respondents scored higher than or equal to the June 2003 Survey respondents. However, the differences here were all less than 10% so this may not be significant.

The percentage of respondents who listed their Primary Job as IT Management was down from 29% in the June 2003 Survey to 26% in the Follow-up Survey, the percentage of Software Developers was down from 12% to 9%, and the percentage of consultants was up from 10% to 20%. Again, it’s not clear if these changes are significant. However, they may be.

More impressive than these differences is the number of demographic measures that are mostly unchanged from the June 2003 Survey to the Follow-up Survey. Geographic representation, Years of Experience with Information Security/Privacy, Employer Size, and Employer Sector or Industry are largely unchanged.

2.3. Opinion Analysis of Respondents

Comparing the opinions of the entire pool of June 2003 Survey respondents against those of the Follow-up Survey respondents also shows few differences. The four most important applications are the same. The five most important obstacles are the same. The only noticeable difference is that the "Hard for End Users to Use" obstacle is rated somewhat lower by the Follow-up Survey respondents. Maybe this is because the Follow-up Survey respondents are more experienced with PKI so they don't notice the usability problems.

2.4. Checking for Undue Influence

With a small number of respondents, a few respondents with strong opinions can substantially influence survey results. Likewise, a large number of respondents from a single organization can bias results. This can happen through a planned effort or through unplanned coincidence.

To check for cases where a small number of respondents with strong opinions are outweighing a larger number of respondents with more moderate opinions, we look not only at the mean (average) response to a question but also at the median response. If the mean and the median are close, then the respondents generally agree on the answer. Of course, finding a small number of respondents with strong opinions is not necessarily bad. It's just important to recognize when this is happening.

In the responses to the Follow-up Survey, only one response shows a substantial difference between the mean and the median. When respondents were asked to assign points to identify where the most serious interoperability problems arise in PKI deployment and usage, Cross-Certification got a mean rating of 1.23 points out of 10. But the median response here was 0. More than half of the respondents (56%, actually) didn't assign any points to this item. But several respondents gave a high point value (3, 5, or even 7), which caused it to have a high total point value. Our suspicion is that many respondents have little or no experience with cross-certification. But those who have such experience consider it a large interoperability problem.

To check whether a single organization had undue influence on the survey results, we checked the email addresses of the respondents. Based on this data, no single organization had an excessive number of respondents (more than 10%).

One final check was made to look for undue influence. We checked whether any question had an especially low response rate. This would make it easy for a small number of respondents to influence the results for that question and call into question their validity. We found that all questions were answered by at least 67% of the survey participants. Combined with the analysis described earlier in this section, our concerns about undue influence were allayed.

2.5. Conclusion regarding Validity of Survey Sample

As mentioned above, the small number of survey respondents raises concerns that the Follow-up Survey responses may not be indicative of opinions throughout the target sample. However, a closer examination of the responses argues against this for the following reasons.

First, the opinions of the Follow-up Survey respondents closely match the opinions of the entire pool of June 2003 Survey respondents. Second, the demographics of the Follow-up Survey respondents also match well with the demographics of the entire pool of June 2003 Survey respondents. Third, an examination of the email addresses and demographics of respondents shows no sign of "packing" by any group. Fourth, the original target sample for these surveys was fairly loosely defined:

> The sample (target audience) of the PKI TC's PKI Deployment Obstacles survey can include anyone who has an opinion on this topic, but we are most interested in people who actually have some expertise or experience in this area. Therefore, we will focus our outreach on IT managers and staff who have worked on or considered PKI deployment, employees of PKI vendors and resellers, and lawyers or consultants who have worked on or observed PKI deployments.

This is a very good description of the respondents to the June 2003 Survey and the Follow-up Survey, although the makeup of the survey respondents is slightly different between the two surveys.

We conclude that the responses to the Follow-up Survey may be useful in developing an Action Plan to address obstacles to PKI deployment and usage. The small sample size means that we cannot do useful demographic correlations or state with great confidence that the opinions of the respondents are representative of a larger pool. But the opinions of the respondents still shed light on the obstacles encountered by those who attempt to deploy and use PKI. And the textual comments, anecdotes, and recommendations of the respondents may prove quite useful.

3. Understanding Obstacles Better

The goal of the Follow-up Survey was to better understand the obstacles to PKI deployment and usage identified by the June 2003 Survey so that the obstacles can be addressed. In order to accomplish this goal, respondents were asked to rank the obstacles by relative importance, answer clarifying questions regarding the obstacles, and offer suggestions for how the obstacles could be addressed. This section describes the responses to these questions.

3.1. Using Points to Indicate Relative Importance

For many of these questions, respondents were asked to allocate 10 points among a set of items. This allowed the respondents to allocate points according to the importance of each item, in their view. For instance, one item might get 6 points, one 4 points, and the other items in that question 0 points.

Respondents were told that they could allocate more than 10 points if they wanted. The results would be normalized to 10 points. This system seemed to work fine.

As described in section 2.4, we looked for cases where a small number of respondents with strong opinions might outweigh a larger number of respondents with more moderate opinions, by considering not only the mean (average) response to a question but also the median response. Except for one case described in section 3.6, we found no substantial disparities between the mean and the median. We interpret this to mean that most of the results from the ranking questions reflect common opinions among the respondents, not a vocal minority.

3.2. Ranking Obstacles

Participants were asked to rank obstacles to PKI deployment and usage, indicating which they believe to be most important. In addition to the nine obstacles included in the June 2003 Survey, we included six others that had been suggested by respondents to June 2003 Survey. Table 1 and Figure 1 show the results (the average point value for each item, after normalizing).

Obstacles	Points	Rank
Software Applications Don't Support It	1.76	1
Costs Too High	1.26	2
PKI Poorly Understood	1.06	3
Too Much Focus on Technology, Not Enough On Need	1.01	4
Poor Interoperability	.90	5
Hard to Get Started – Too Complex	.68	6
Lack of Management Support	.66	7
Hard for End Users to Use	.59	8
Enrollment Too Complicated	.35	9
Too Much Legal Work Required	.33	10
Smart Card Problems	.32	11
Hard for IT to Maintain	.30	12
Insufficient Need	.29	13

Revocation Hard	.25	14
Standards Problems	.25	15

Table 1: Obstacles Ranked by Importance

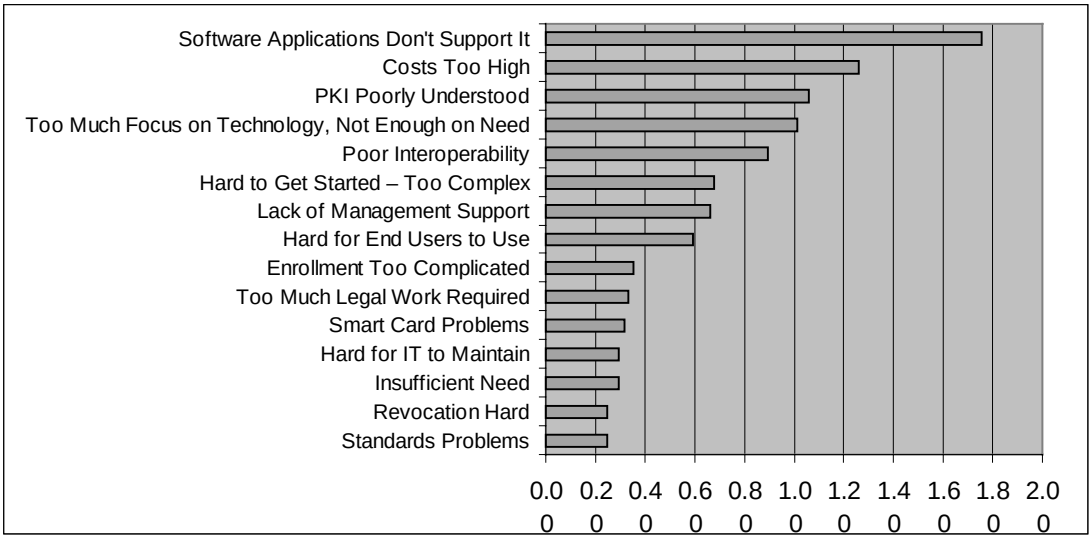

Figure 1: Obstacles Ranked by Importance

These responses match closely with the responses from the June 2003 Survey. The order of items in the list is almost the same. But the top few items stand out much more starkly from the rest. By providing a point system instead of only three categories as the June 2003 Survey did, respondents were able to indicate their opinions more clearly. It seems that although there are many "Major Obstacles" to PKI deployment and usage, a few of them are much more important than the others. The first four obstacles have more than half of the total points. And the number one obstacle ("Software Applications Don't Support It") has 39% more than any of the others. This suggests that focussing resources on these top four obstacles would have the greatest benefit, although work on the others might also be useful.

Another important outcome is that one obstacle not included on the original list is in this top four. That is "Too Much Focus on Technology, Not Enough on Need". Now that this obstacle has been identified and highlighted, it can be addressed.

3.3. Software Application Support

In the June 2003 Survey results, "Software Applications Don't Support It" was identified as the most important obstacle to PKI deployment and usage. Therefore, the Follow-up Survey asked several questions to better understand this obstacle and how it can be addressed.

First, respondents were asked to indicate which applications most critically need improvements in PKI support. The ranking system described in section 3.1 was used in conjunction with the application list from the June 2003 Survey. No other applications were cited by many respondents to the June 2003 Survey, so none were added to the list. Table 2 and Figure 2 show the results of this ranking exercise.

Applications	Points	Rank
Document Signing	2.41	1
Secure Email	1.63	2
Electronic Commerce	1.32	3
Single Sign On	1.06	4
Secure Wireless LAN	0.91	5
Web Services Security	0.80	6
Web Server Security	0.61	7
Virtual Private Network	0.59	8
Code Signing	0.45	9
Secure RPC	0.22	10

Table 2: Applications Ranked by Need for Improvements in PKI Support

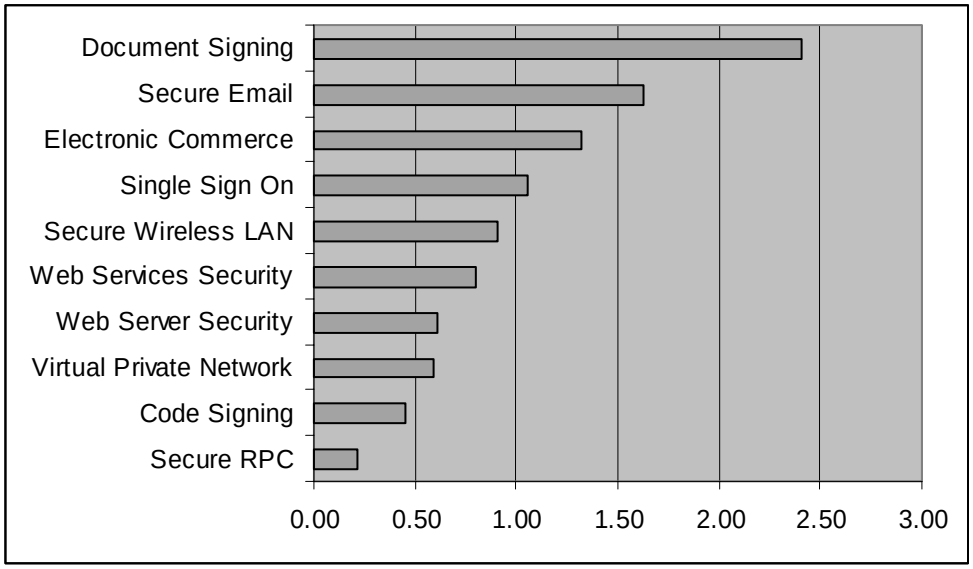

Figure 2: Applications Ranked by Need for Improvements in PKI Support

These results are even more striking than those seen when obstacles were ranked. The top three applications have more than 50% of the points. The number one application has almost 25% of the points. This indicates an opinion among the respondents that certain applications should receive the lion's share of the attention, at least for now.

The list of top rated applications in this analysis differs somewhat from those rated most highly in the June 2003 Survey. In that survey, the highest ranked application was Document Signing with Web Server Security and Secure Email following closely behind. Electronic Commerce came in sixth. So it's somewhat surprising to see Electronic Commerce rated so highly now and Web Server Security rated so low. However, Document Signing and Secure Email are clearly critical to the respondents of both surveys.

During the design of the Follow-up Survey, several PKI TC members pointed out that Document Signing actually encompasses three somewhat different applications: Signing Contracts (legally binding), Signing Electronic Forms (not contracts), and Signing

Documents before Dissemination (so recipients can verify their source and integrity). The Follow-up Survey included a question asking respondents to rate the importance of these three subcategories. Table 3 shows the results of this exercise.

Subcategories	Most Important	Important	Not Important	No Answer	Weight	Weight Rank
Signing Documents before Dissemination	38%	53%	9%	0%	1.28	1
Signing Electronic Forms	34%	58%	8%	0%	1.26	2
Signing Contracts	32%	49%	19%	0%	1.14	3

Table 3: Document Signing Subcategories Ranked

A quick look at the raw data shows that most respondents ranked only one of these subcategories as Most Important. There seems to be fairly even support for these three kinds of Document Signing.

The Follow-up Survey also asked for comments on how application support for PKI was insufficient. The extensive comments supplied will be considered by the PKI TC when planning future actions. To summarize briefly, application support for PKI is inconsistent. Many applications have no support. Those that do differ widely in what they support, which makes it very difficult to deploy a PKI. Interoperation between PKIs is nearly impossible. Respondents called for detailed standards to ensure interoperability.

The Follow-up Survey asked for comments on what the PKI TC or others could do to help improve application support for PKI. Again, the comments are too extensive to quote here but will be considered carefully by the PKI TC. One frequent suggestion was to create guidelines for each type of application on how PKI support should be implemented. Also, OS vendors should be encouraged to include PKI features (like smart card support).

3.4. Costs

In the June 2003 Survey results, “Costs Too High” was identified as the second important obstacle to PKI deployment and usage. Therefore, the Follow-up Survey asked several questions to better understand this obstacle and how it can be addressed.

First, respondents were asked to indicate which costs are most problematic in PKI deployment and usage. The ranking system described in section 3.1 was used. Table 4 and Figure 3 show the results of this ranking exercise.

Costs	Points	Rank
Cost of Initial System Design	1.08	1
Cost of Software Acquisition	1.06	2
Cost of Software Integration	.97	3
Cost of On-going Operations	.96	4
Cost of Secure Facilities	.94	5
Cost of Smart Cards and Readers	.92	6
Cost of End-User Support	.83	7
Cost of Initial Certificate Issuance	.73	8
Non-technical Setup Costs (e.g. legal & CPS)	.66	9

Other Costs	.58	10
Cost of Training	.53	11
Cost of Cross-Certification	.37	12
Cost of Support Contracts	.36	13

Table 4: Costs Ranked by Most Problematic

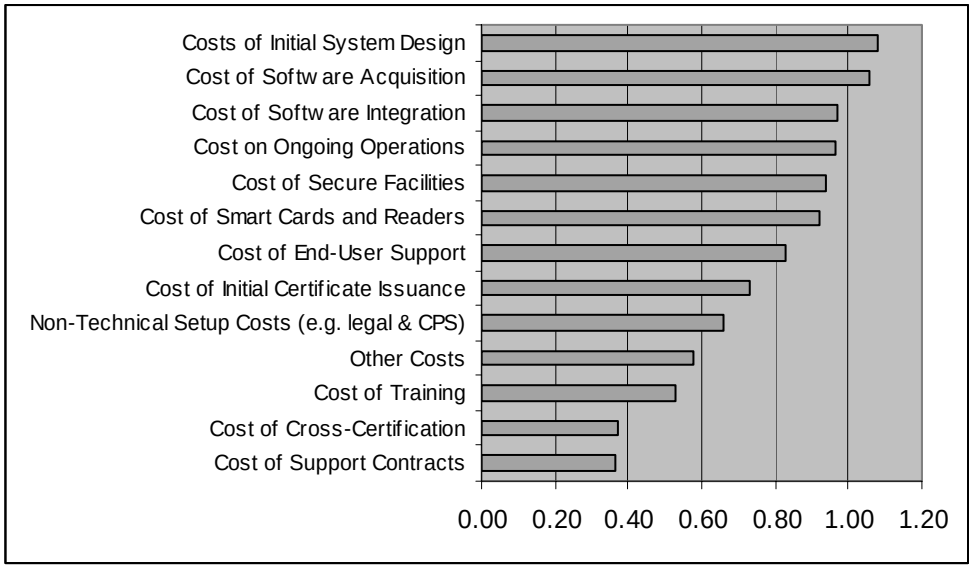

Figure 3: Costs Ranked by Most Problematic

Unfortunately, this is not very enlightening. The top six categories of costs are very close. One person changing a few points in their ratings could move an item up one or two slots. We can conclude with some confidence that the costs of cross-certification and support contracts are not a large concern. But going beyond that is difficult.

The Follow-up Survey also asked "Would you say that these cost problems are largely eliminated if the number of users involved is large (amortizing large fixed costs)?" The results for this question are included in Table 5.

	Yes	No	No Response
Cost Problems Eliminated with Large Number of Users	31%	45%	24%

Table 5: Cost Problems Eliminated with Large Number of Users

To further understand the nature of these costs, the Follow-up Survey asked "Do your comments about costs pertain primarily to outsourced PKI services, in-house PKI, or both?" The results are shown in Table 6.

	Outsourced PKI	In-house PKI	Both	No Response
Cost Comments Pertain Primarily to	9%	23%	43%	24%

Table 6: Cost Comments Pertain to Outsourced PKI or In-house

The Follow-up Survey asked for comments on what the PKI TC or others could do to help reduce costs. The comments are too extensive to quote here but will be considered

carefully by the PKI TC. A common theme was the ability to reduce costs by promoting specific standards that avoid the need for customization. Other themes were outsourcing and encouraging free PKI software and free CAs for low-assurance applications.

3.5. PKI Poorly Understood

In the June 2003 Survey results, "PKI Poorly Understood" was identified as the third most important obstacle to PKI deployment and usage. Therefore, the Follow-up Survey asked several questions to better understand this obstacle and how it can be addressed.

First, respondents were asked to indicate which parties most need greater PKI understanding. The ranking system described in section 3.1 was used. Table 7 and Figure 4 show the results of this ranking exercise.

Parties	Points	Rank
Senior Management	3.35	1
Users	2.34	2
IT Management	1.70	3
IT Staff	1.31	4
Vendors	1.02	5
Other	.29	6

Table 7: Parties Ranked by Greatest Need for PKI Understanding

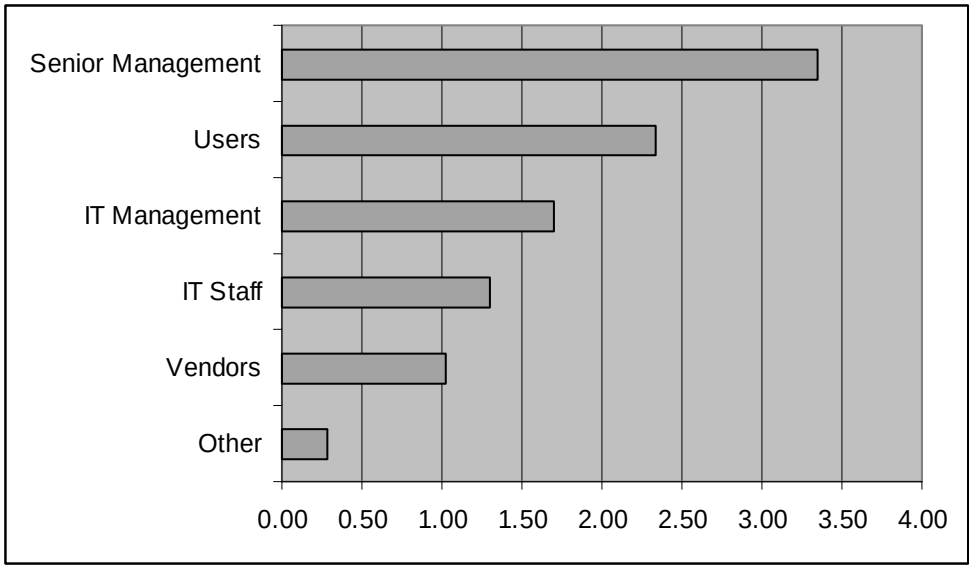

Figure 4: Parties Ranked by Greatest Need for PKI Understanding

A clear preference is expressed for educating senior management and users on PKI.

The Follow-up Survey also asked for comments on what the PKI TC or others could do to help increase understanding of PKI. The comments are too extensive to quote here but will be considered carefully by the PKI TC. A common theme was the need to explain in non-technical terms the benefits, value, and ROI of PKI and when it's appropriate (or not). Educational materials should unbiased and freely available to all. A cookbook (how-to

guide) on deploying PKI would also be useful (maybe paired with free tools for deploying a low-assurance PKI for testing purposes).

3.6. Interoperability

In the June 2003 Survey results, "Poor Interoperability" was identified as the fourth most important obstacle to PKI deployment and usage. Therefore, the Follow-up Survey asked several questions to better understand this obstacle and how it can be addressed.

First, respondents were asked to indicate where the most serious interoperability problems arise. The ranking system described in section 3.1 was used. Table 8 and Figure 5 show the results of this ranking exercise.

	Points	Rank
Path Validation	2.03	1
Smart Card	1.51	2
Unusual Certificate Contents	1.32	3
Cross-Certification	1.23	4
Certificate Issuance	1.17	5
Certificate Revocation	.99	6
Protocols that Use PKI (such as SSL or S/MIME)	.96	7
Other	.80	8

Table 8: Where the Most Serious Interoperability Problems Arise

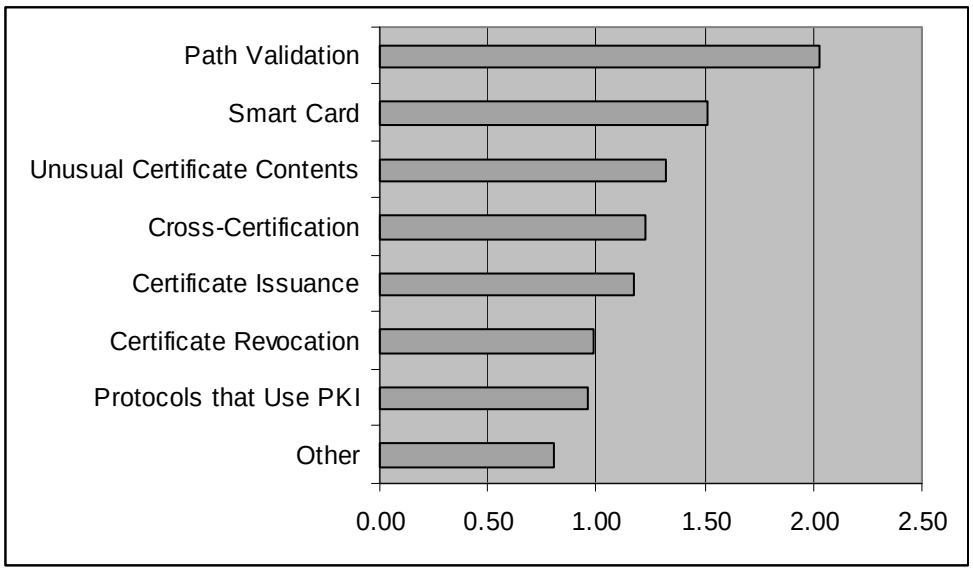

Figure 5: Where the Most Serious Interoperability Problems Arise

Looking at the median response for this question is interesting. The first three items have a median response of 1 or greater, indicating that most respondents consider this a problem. The fourth (Cross-Certification) has a median response of 0. More than half of the respondents (56%, actually) didn't assign any points to this item. But several respondents gave a high point value (3, 5, or even 7), which caused it to have a high total point value. In this case, it may be that many respondents have little or no experience with cross-

certification. But those who have such experience consider it a large interoperability problem.

Because interoperability is especially complex with PKI, the Follow-up Survey asked respondents to please describe any interoperability problems they wanted to highlight. The extensive comments supplied will be considered carefully by the PKI TC. The most common problem cited was standards: too many in some areas, too few in others, too ambiguous, poor implementations, no conformance testing, etc. Another concern was incompatible Certificate Policies.

The Follow-up Survey also asked for specific suggestions on things the PKI TC or others could do to help improve interoperability. Almost all of the respondents suggested creating profiles of PKI standards with interoperability testing, test suites, and certification.

3.7. Other Suggestions

The Follow-up Survey asked for other comments or suggestions, especially ideas for how to address the obstacles listed in the survey. The comments supplied here were rather diverse, but generally echoed the ones supplied earlier in the survey.

4. Conclusions

The Follow-up Survey successfully accomplished its goal: to clarify and better understand the obstacles to PKI deployment and usage identified in the June 2003 Survey. The results of this survey provide valuable details that the OASIS PKI TC can use in formulating its Action Plan for addressing these obstacles.

4.1. Survey Validity

The number of respondents was lower than hoped (only 74 vs. 216 for the June 2003 Survey), but a careful examination of the survey responses (in section 2 of this document) shows that they are fairly representative of the broader pool of June 2003 Survey respondents and that the survey results are sound and valid.

4.2. Prioritizing Obstacles

The Follow-up Survey used a new points-based rating system, allowing respondents to assign extra points to the items they feel are most critical. This system worked well in most cases, raising the most important items above the many other important ones. This will be critical in helping the PKI TC prioritize its efforts.

The top five obstacles to PKI deployment and usage identified by this survey are:

1. Software Applications Don't Support It
2. Costs Too High
3. PKI Poorly Understood
4. Too Much Focus on Technology, Not Enough On Need
5. Poor Interoperability

These are the same ones identified in the June 2003 Survey, except that the new item "Too Much Focus on Technology, Not Enough On Need" has pushed its way to the top. This obstacle was added to the Follow-up Survey along with several others that had been mentioned by several respondents on the June 2003 Survey. But it was the only new obstacle to receive high ratings.

The top obstacle ("Software Applications Don't Support It") had much higher ratings than the rest of the top five (40-80% greater) and the top five obstacles were substantially above the rest. This suggests that the PKI TC should focus only on these obstacles for now.

4.3. More Detail on Obstacles

The Follow-up Survey asked detailed questions about each of the top four obstacles identified in the June 2003 Survey. All PKI TC members should carefully review the analysis of these questions in sections 3.3 through 3.6. However, this summary will only highlight the most salient points.

Perhaps the most valuable part of the Follow-up Survey was the textual responses. For each of the top obstacles identified in the June 2003 Survey, respondents were asked to describe in their own words what causes these obstacles and what the PKI TC or others could do to address the obstacles. Certain themes were repeated over and over by many respondents. These themes pertain to several of the top obstacles. They are:

- Support for PKI is inconsistent. Often, it's missing from applications and operating systems. When present, it differs widely in what's supported. This increases cost and complexity substantially and makes interoperability a nightmare.
- Current PKI standards are inadequate. In some cases (as with certificate management), there are too many standards. In others (as with smart cards), there are too few. When present, the standards are too flexible and too complex. Because of the standards are so flexible and complex, implementations from different vendors rarely interoperate.

What can be done?

- Develop specific profiles or guidelines that describe how the standards should be used. These guidelines should be simple and clear enough that if vendors and customers implement them properly, PKI interoperability can be achieved. In some cases, standards may need to be created, merged or improved.
- Provide interoperability tests and testing events to improve interoperability. Branding and certification may also be desirable.
- Provide a "cookbook" with easy steps for building a simple PKI. Of course, more sophisticated PKIs will require customization.
- Provide free software and free CAs so people can set up a test PKI with little or no cost. This free software may only provide low assurance, but it will be useful for testing and as a way to encourage people to get started with PKI.

The Follow-up Survey respondents indicated that their most important applications are Document Signing, Secure Email, Electronic Commerce, and Single Sign On. Many of the steps listed above will apply to all applications, but in some cases application-specific efforts are needed (developing guidelines for PKI use in particular applications, interoperability testing for specific applications, etc.). In those cases, the PKI TC should focus on these applications first.

These recommendations of the Follow-up Survey respondents seem well-considered. Certainly, they address many of the top obstacles: Software Applications Don't Support It, Costs Too High, and Poor Interoperability. The "cookbook" suggestion addresses some concerns with respect to PKI Poorly Understood, but only for technical participants.

Below are the other recommendations for PKI Poorly Understood. Unfortunately, we did not ask for comments on the new obstacle Too Much Focus on Technology, Not Enough On Need. It had not been highlighted as a top obstacle until now.

- Explain in non-technical terms the benefits, value, and ROI of PKI. Also explain when PKI is appropriate (or not). Educational materials should unbiased and freely available to all.

- Educating senior management and users is most important. Technical folks will be able to figure it out eventually.

4.4. Next Steps

The PKI TC considered the results of this survey at its September 30, 2003 face-to-face meeting and agreed on a draft Action Plan to address the obstacles highlighted in the survey. This fall, the draft Action Plan will be circulated to PKI stakeholders (users, vendors, etc.) for comment and commitment. After revision, the Action Plan will be rolled out in Spring 2004 and put into practice. We hope that this will substantially reduce the obstacles cited in this survey.

Appendix A. Summary of June 2003 Survey Results

The OASIS PKI TC's June 2003 survey on Obstacles to PKI Deployment and Usage aimed to "identify the most commonly cited obstacles to PKI deployment and usage" so that the TC can later "explore ways to address these obstacles". The target sample was individuals with "some expertise or experience" with PKI, especially "IT managers and staff who have worked on or considered PKI deployment, employees of PKI vendors or resellers, and lawyers or consultants who have worked on or observed PKI deployments".

The June 2003 Survey met these goals. The 216 respondents had a variety of backgrounds and perspectives, but 99% had some PKI experience. An amazing 90% of respondents had either helped deploy PKI or developed PKI-related software.

The respondents were asked to indicate which PKI applications were Most Important or Important to them. Most respondents marked several PKI applications as Most Important and several others as Important. All of the applications listed had significant support among the respondents. This indicates that PKI is truly a horizontal, enabling technology with many applications.

The respondents were also asked to examine a list of possible Obstacles to PKI deployment and usage, ranking each one as a Major Obstacle, a Minor Obstacle, or Not an Obstacle. Two obstacles were stood out from the rest: Software Applications Don't Support It and Costs Too High. Several other obstacles were close behind: PKI Poorly Understood, Poor Interoperability, Hard to Get Started – Too Complex, and Hard for End Users to Use.

Respondents were also allowed to suggest other obstacles that should be added to the list. Six obstacles were cited by four or more respondents, so they were included in the list for the Follow-up Survey. Those were:

- Insufficient ROI/business justification/need
- Enrollment too complicated
- Smart card problems
- Revocation hard
- Standards (too many, incompatible, etc.)
- Too much focus on PKI technology, not enough on business need

Demographic information was collected from the June 2003 Survey respondents, such as Primary Job Function, Years of Experience in Information Security/Privacy, Primary Work Country, etc. Survey responses were examined for correlations with demographics. No such correlations were found, although the sample size was too small to conclude whether this was significant.

Email addresses were also collected so that survey results and invitations for future surveys could be sent to respondents. This proved invaluable in conducting the Follow-up Survey.