Analysis of June 2003 Survey on Obstacles to PKI Deployment and Usage

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

Date: July 17, 2003

Version: 0.3

DRAFT

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 Survey Sub-Committee was formed to facilitate the design and execution of this market research. A short, multiple-choice web-based survey was drawn up and subsequently reviewed and approved by the members of the PKI TC. The survey was hosted by OASIS at its facilities in Massachusetts, USA under the following URL: http://www.oasis-open.org/committees/pki/pkiobstacles.html

Major worldwide PKI standards bodies, industry associations, and technology vendors assisted by distributing an email invitation to participate in this survey to all of their members/stakeholders. In order to focus attention and move forward promptly, the survey was active for two weeks: from June 9, 2003 to June 22, 2003.

Special attention was given to the privacy policy of the survey. Participants were assured via a Privacy Note that the data collected in the survey would be reported in aggregate form and that individual responses would only be used by OASIS PKI TC members and OASIS staff members in tabulating results. If participants chose to provide their email address (which was optional), the PKI TC would send them a copy of the survey results and invitations to participate in future surveys conducted by the OASIS PKI TC, but their email address would not be used for any other purposes or disclosed to anyone outside of OASIS.

This document analyzes the responses to the survey and provides conclusions and recommendations.

2. Survey Sample

Before undertaking the survey, the PKI TC agreed that "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."

In this section, we examine the respondents. We conclude the section by examining whether the respondents are in fact representative of the intended survey sample and whether the sample is sufficient to provide meaningful conclusions.

2.1. Validity of Survey Responses

The total number of responses to the survey was 217. One of these responses was considered invalid, since only one of the questions was answered. All others were considered valid.

Because this was a web-based survey with no controls on multiple responses, the responses were checked carefully to detect any attempt to "stuff the ballot box", vote multiple times, or otherwise bias the survey. No duplicate entries were detected. And no frivolous answers were detected (such as humorous comments in the text boxes).

In fact, the answers seem to reflect careful consideration on the part of the respondents. Most respondents included some textual answer (not just checking off multiple choice questions) and no respondent checked all high or all low for questions that asked them to rank PKI applications and obstacles. Also, 80% of the respondents chose to supply an email address to receive survey results and follow-up surveys and more than 25% supplied a detailed description of the obstacles to PKI deployment and usage.

2.2. Primary Job Function

Respondents were asked to identify their Primary Job Function, choosing from a list of choices or entering their own under Other. A large variety of functions were represented, with almost half of the respondents (44%) in IT.

Of the respondents who entered Other for their Primary Job Function, 20 were Consultants and 6 were Architects. The remainder included Marketing, Business Development, and non-IT Management. If Consultant had been listed separately, it would have been the fourth most common Primary Job Function.

More than half of the respondents seem to have a strong technical component to their job (IT Management, IT Staff, Software Developer, etc.). But just as many seem to have a strong business component to their job (at least IT Management, IT Staff, Non-

IT Management, Auditor, Lawyer, Consultant, and Architect). So this group may provide a broad and deep understanding of the obstacles to PKI deployment and usage, going beyond a purely business or technical perspective.

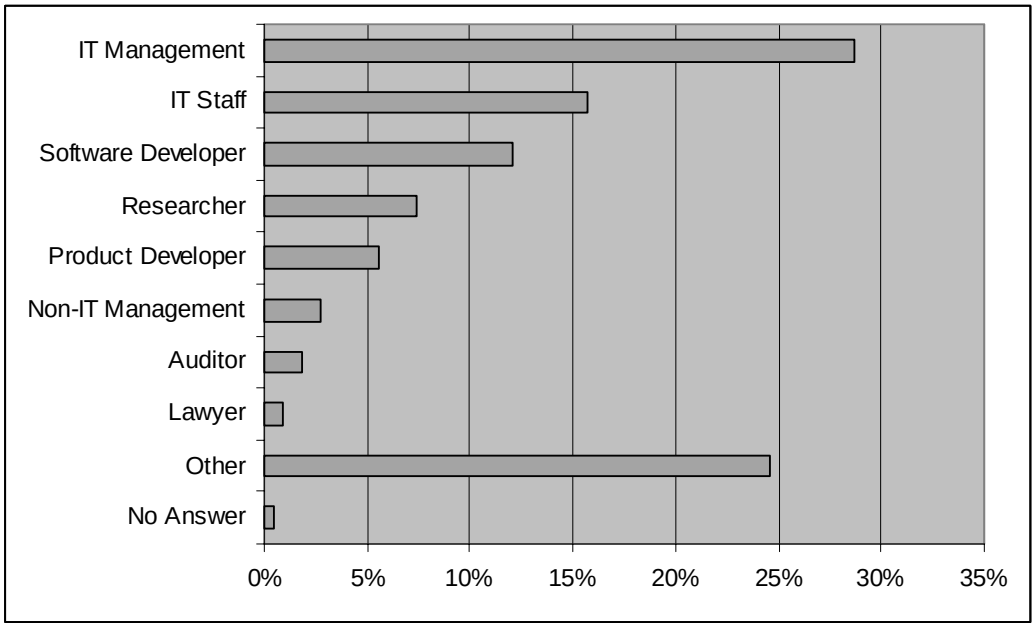

Figure 1: Primary Job Function

2.3. Years of Experience in Information Security/Privacy

More than 75% of the respondents indicated that they had 5 or more years of experience in Information Security/Privacy.

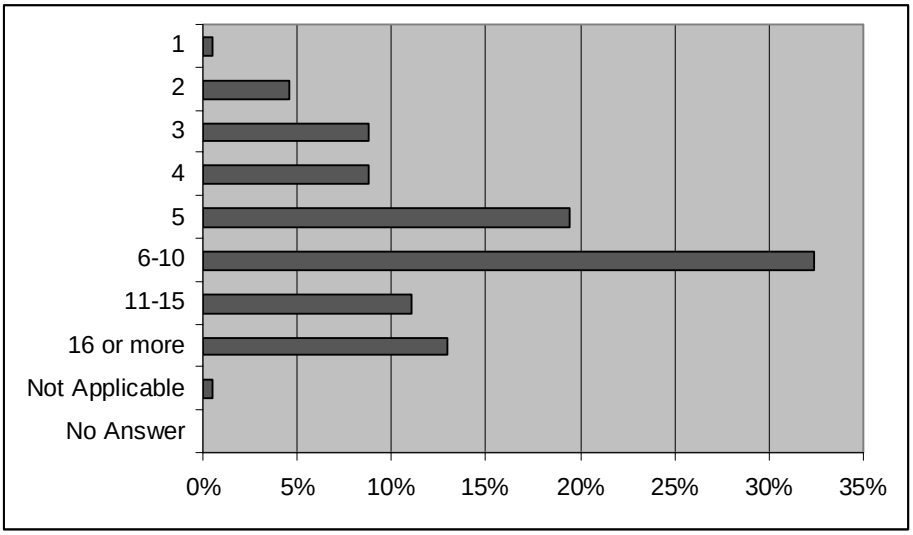

Figure 2: Years of Experience with Information Security/Privacy

2.4. PKI Experience

Respondents marked checkboxes to indicate which things they had done with PKI. They were asked to mark all categories that apply.

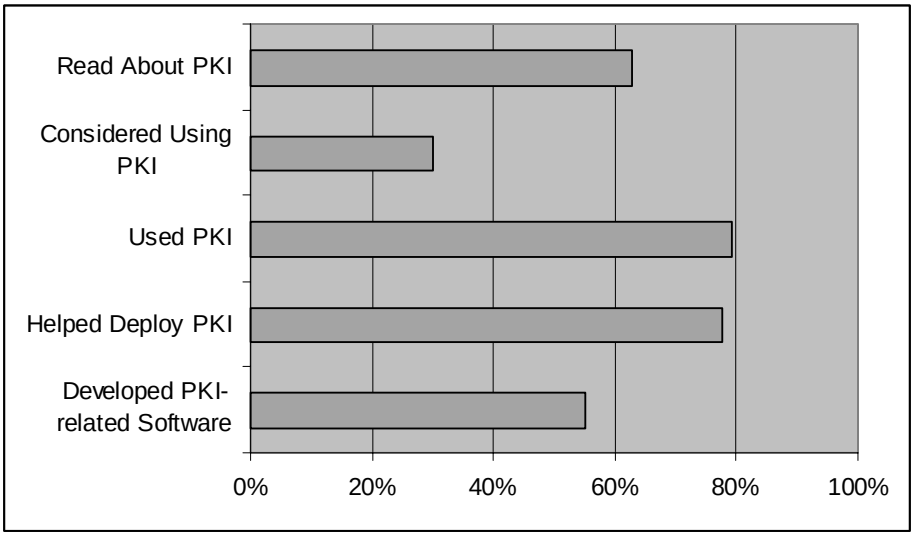

Figure 3: PKI Experience

Further analysis of the survey data shows that an amazing 90% of respondents have either Helped Deploy PKI or Developed PKI-related Software! Another 9% have used or considered using PKI. So the respondents are clearly very experienced with PKI.

From these numbers, it might appear that many respondents have helped deploy PKI without reading about it and that many have used PKI without considering doing so. While this may be true, it's more likely that PKI experts simply skipped these first two categories as not reflecting their current level of expertise.

2.5. Employer Sector or Industry

Nearly 30% of the respondents were employed by government. This was nearly matched by computer-related industries, which amounted to 28% if you include Other responses such as software (5% of respondents) and IT services/consulting (6%). A wide variety of other sectors and industries were also represented.

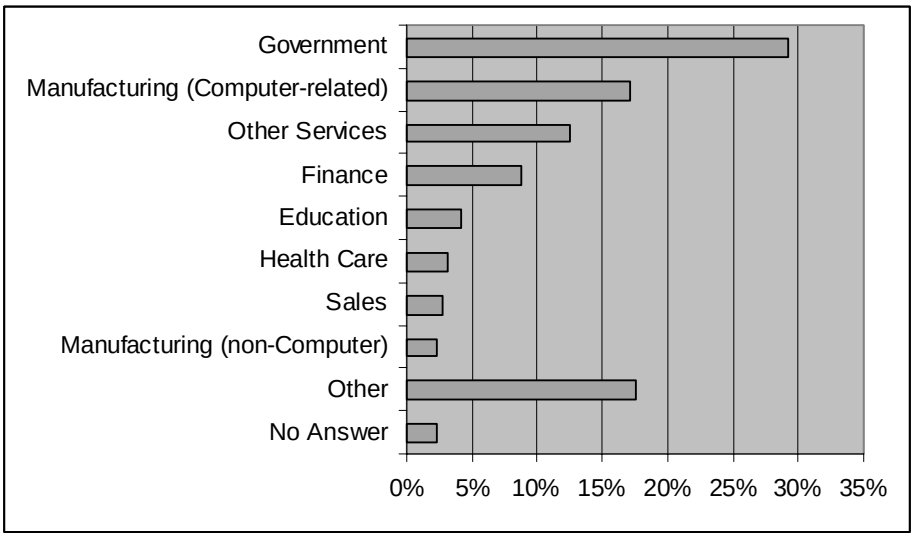

Figure 4: Employer Sector or Industry

2.6. Employer Size

Of the 216 respondents, nearly 60% work in large organizations of 1,000 employees or more. However, a significant number work at small to mid-sized organizations.

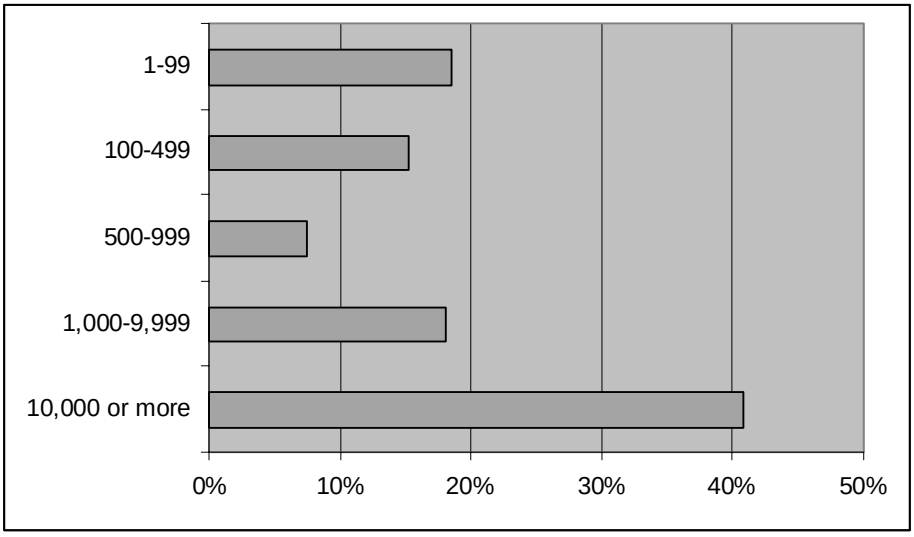

Figure 5: Employer Size (number of employees)

2.7. Primary Work Country

About 60% of the respondents listed their Primary Work Location as being in North America (USA 47%, Canada 13%). However, a significant number of participants listed European or Asian countries. More than 30 countries were represented, in total.

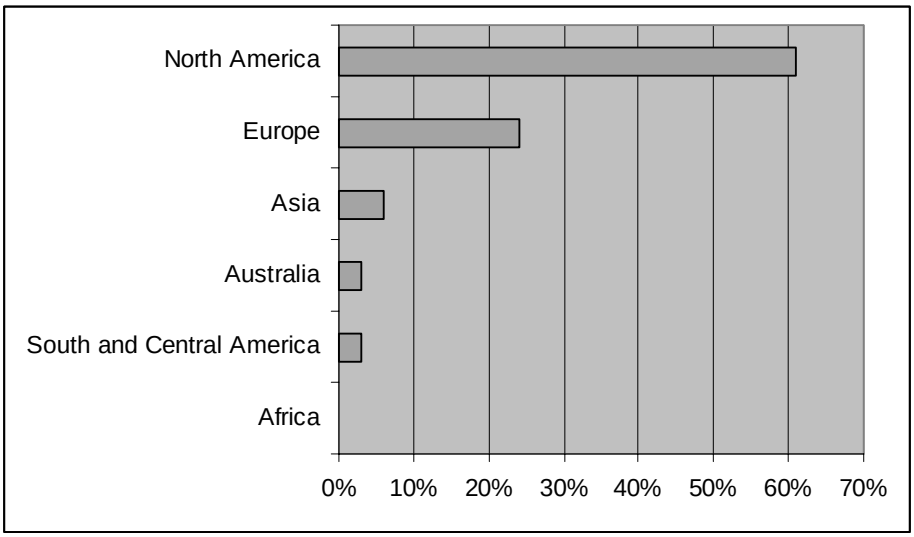

Figure 6: Primary Work Location

2.8. Scope of PKI Interest

Several questions asked about the scope of the respondents' PKI concerns. A substantial majority (77%) indicated that their interests extend beyond their primary work country. And even more (84%) indicated that their interests extend beyond their organization.

2.9. Adequacy of Sample

The survey respondents were self-selected, so they are probably not representative of all invitation recipients. And they are certainly not representative of all computer users or the population as a whole. The respondents have a great deal of experience and expertise with PKI and with Information Security and Privacy. They are professionals who have studied this technology and actually used it. It seems that the PKI TC successfully reached it target sample of "people who actually have some expertise or experience" with PKI.

Is the sample size large enough to draw meaningful conclusions? A general guideline is that at least 100 respondents are required to draw meaningful conclusions. And the respondents should be randomly selected so that they are representative of the population under study. Random selection of survey participants is rarely possible in practice. But it seems that the set of respondents is fairly representative of the group of "people who actually have some expertise or experience" with PKI. This can be verified somewhat by examining results carefully to see if there are significant differences across demographic groups. If so, the respondents' demographics may substantially bias the outcome.

The sample size is large enough to draw meaningful conclusions, as long as we are careful. But we cannot divide it into small demographic groups and hope that the

results from those groups are meaningful. For instance, the one respondent from Portugal cannot be considered representative of all residents of Portugal or even all PKI experts in Portugal.

3. Views and Opinions

In addition to the demographic information described in the previous section, the PKI Obstacles Survey asked two questions about the respondents' views and opinions regarding PKI applications and obstacles. This section presents the responses to those questions and investigates correlations between these responses and the demographics also collected.

3.1. PKI Applications

Participants in the survey were asked to rate various PKI applications as Most Important, Important, or Not Important to them. Respondents were also able to enter their own application under Other and rate its importance.

The complete results are presented in Table 1. The Weight column for each application was computed by adding 2 for each Most Important rating and 1 for each Important rating, then dividing by the total number of answers for that application. This allows a Weight Rank to be easily computed, giving the application with the highest Weight a rank of 1, the next highest Weight a rank of 2, and so on. Note that for Other Application, No Answer is considered to mean Not Important (since those respondents didn't think any other application was noteworthy).

Applications	Most Important	Important	Not Important	No Answer	Weight	Weight Rank
Document Signing	43%	47%	6%	3%	1.38	1
Web Server Security	42%	48%	6%	4%	1.37	2
Secure Email	40%	46%	8%	6%	1.33	3
Web Services Security	34%	53%	9%	4%	1.26	4
Virtual Private Network	33%	50%	11%	6%	1.24	5
Electronic Commerce	34%	48%	13%	5%	1.22	6
Single Sign On	28%	56%	12%	4%	1.17	7
Secure Wireless LAN	25%	48%	19%	8%	1.06	8
Code Signing	20%	50%	22%	8%	0.98	9
Secure RPC	6%	40%	40%	13%	0.61	10
Other Application	9%	3%	7%	81%	0.21	11

Table 1: PKI Applications Rated

Figure 7 shows graphically the ranks for the various applications.

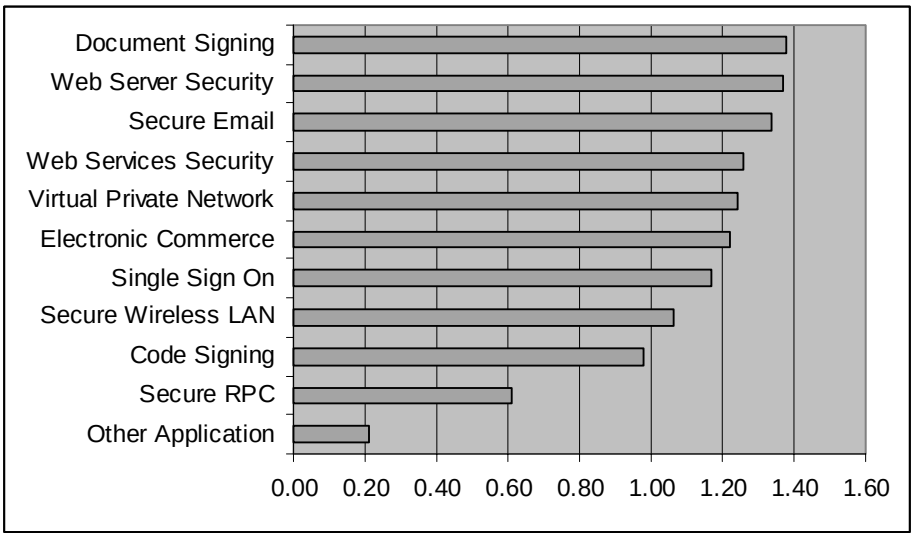

Figure 7: PKI Application Weights

All of the applications except Secure RPC are considered at least Important by more than 50% of the respondents. It's common for respondents to consider many applications Important. But no application is considered Most Important by a majority of the respondents. This indicates that PKI is truly a horizontal, enabling technology with many applications. And it may explain why different people have very different views of what PKI needs to do. They have different priorities.

The most common responses for Other Application were Identity Management, Non-Repudiation, and Document Encryption.

3.2. Obstacles to PKI Deployment and Usage

Question 4 in the survey asked respondents to identify and prioritize the obstacles to PKI deployment and usage. This is really the heart of the survey.

Respondents were presented with a list of possible obstacles and asked to rank each one as a Major Obstacle, a Minor Obstacle, or Not an Obstacle. Respondents were also able to describe an obstacle under Other and rank it in the same way. Obstacles were described in broad terms to avoid having a very long and detailed questionnaire. It will probably be necessary to have a follow-up survey to clarify exactly which Costs are Too High, for instance.

The complete results are presented in Table 2. As with the analysis of Application ratings above, a Weight column has been computed by adding 2 for each Major Obstacle rating and 1 for each Minor Obstacle rating, then dividing by the total number of answers for that obstacle. Then a Weight Rank is computed, giving the obstacle with the highest Weight a rank of 1, the next highest Weight a rank of 2, and so on. Note that for Other Obstacle, No Answer is considered to mean Not Important (since those respondents didn't think any other obstacle was noteworthy).

Obstacles	Major Obstacle	Minor Obstacle	Not an Obstacle	No Answer	Total	Weight	Weight Rank
Software Applications Don't Support It	54%	33%	10%	3%	100%	1.45	1
Costs Too High	53%	34%	12%	2%	100%	1.42	2
PKI Poorly Understood	47%	41%	11%	1%	100%	1.37	3
Poor Interoperability	46%	39%	12%	3%	100%	1.35	4
Hard to Get Started – Too Complex	46%	39%	13%	2%	100%	1.34	5
Hard for End Users to Use	43%	42%	13%	3%	100%	1.30	6
Lack of Management Support	30%	44%	21%	5%	100%	1.09	7
Too Much Legal Work Required	25%	50%	22%	3%	100%	1.03	8
Hard for IT to Maintain	20%	55%	21%	4%	100%	0.99	9
Other Obstacle	18%	3%	5%	74%	100%	0.39	10

Table 2: PKI Obstacles Rated

Figure 8 shows graphically the ranks for the various obstacles.

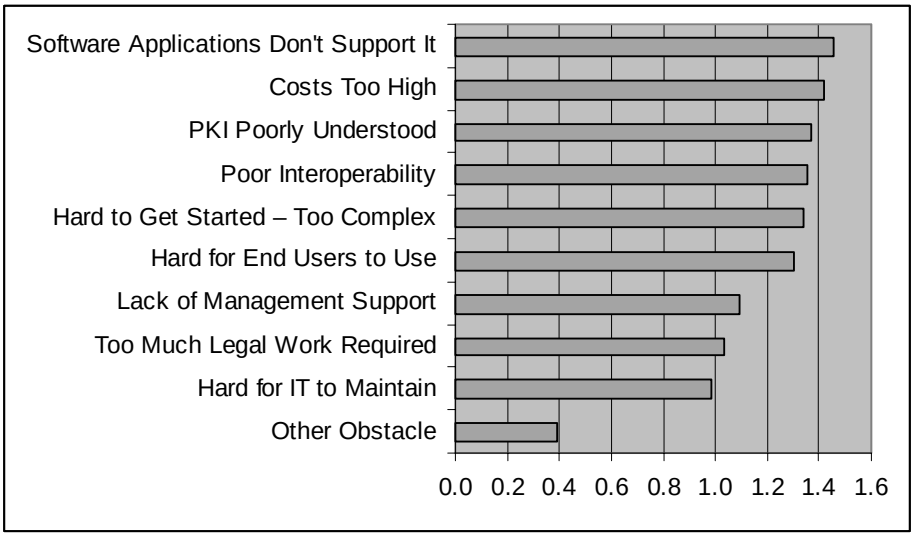

Figure 8: PKI Obstacle Weights

None of these obstacles is ranked Not an Obstacle by the majority of the respondents. So all of them are relevant. But the bottom three (Lack of Management Support, Too Much Legal Work Required, and Hard for IT to Maintain) are ranked as a Minor Obstacle by about 50% of the respondents and ranked as Not an Obstacle by another 20% of the respondents. We can conclude that these are less critical than the others.

The top two obstacles are identified as a Major Obstacle by a majority of the respondents. But all of the top six are considered a Major Obstacle by a substantial number of respondents and only considered Not an Obstacle by about 10% of the respondents. We might conclude that all six are important and the top two are the highest priority.

The good news is that 92% of the respondents indicated they would use PKI more if these obstacles were removed.

3.3. Other Obstacles

A significant number of respondents (48, 22% of the total) described an "Other" obstacle (entering a separate textual description). In most of these cases, the respondents rated this obstacle as a Major Obstacle. This section examines these obstacles, considering that some of them may be widely held concerns that were simply not articulated by other respondents.

A separate text field was also provided in the survey, inviting respondents to "say more about obstacles to PKI deployment and usage". Many respondents (58, 27% of the total) entered text in this area. And 6 more sent an email to the PKI TC chair with more comments. Some users attached long documents to their emails. All of the information contained in these responses and emails was considered and evaluated carefully by the survey analysis team, but it cannot be reproduced verbatim in this report because of privacy concerns.

We might expect that a widely held concern would be cited by more than one respondent. Therefore, we will focus our attention on obstacles that were described by multiple respondents and are not already on the list of obstacles included in the survey. Some interpretation is required to prepare this list, since the descriptions of these obstacles supplied by respondents are sometimes unclear.

Table 3 lists these obstacles and the number of respondents who cited them.

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

Table 3: Additional PKI Obstacles

Since these obstacles were cited by several respondents, we may want to consider including them in a follow-up survey so they can be ranked along with the others originally listed.

3.4. Demographic Analysis of Applications and Obstacles

As noted earlier, our sample size is small enough that we cannot break down the sample into many small demographic subgroups to see if those different groups answered differently. At least, any conclusions that we draw will probably not be statistically significant. However, for large demographic groups (those constituting 30% or more of the sample) that exhibit substantial variances from the rest of the sample (more than 10%), we may be able to see some possibly valid indications. A few such analyses have been done. This section presents the conclusions.

Government sector respondents (29% of the whole) rank Document Signing 10% higher and Code Signing 11% lower than the total sample. In contrast, respondents in the Computer-related Manufacturing sector (17% of the whole) rank Code Signing 12% higher than the total sample and Document Signing 10% lower. This is not surprising, since Governments produce a lot more documents than code and computer firms typically do the opposite.

Rankings of Obstacles are rather similar across all sectors, levels of PKI experience, Years in Information Security/Privacy, or Region (looking at U.S./non-U.S.). The sample is not large enough to draw any conclusions about differences by Primary Job, Country, or intent to use PKI beyond company boundaries.

This similarity in Obstacle Ranking across demographic differences may suggest that the obstacles affect most sectors and regions the same way. If so, that may mean that working to address those obstacles will benefit all sectors and regions.

4. Conclusions

4.1. Summary of Survey Results

As noted earlier, our sample size is small enough that we cannot break down the sample into many small demographic subgroups to see if those different groups The survey seems to have been successful. We reached the intended audience, those with "expertise or experience" with PKI. We got enough responses with broad enough demographics to be fairly confident that our respondents are representative of their peers. And we got 173 email addresses of motivated respondents, who may be willing to participate in follow-up surveys.

Most respondents have several PKI applications that they consider to be Most Important and several others that are Important. All the applications listed had significant support among the respondents. This indicates that PKI is truly a horizontal, enabling technology with many applications.

As for obstacles to PKI deployment and usage, there are many. Those most consistently cited as Major Obstacles were Software Applications Don't Support It and Costs Too High. But several other obstacles were close runners-up: PKI Poorly Understood, Poor Interoperability, Hard to Get Started – Too Complex, and Hard for End Users to Use. All of these were considered Major Obstacles by 40% of the respondents or more.

In addition, ten obstacles not listed in the survey were cited by multiple respondents. Of these, six were cited by four or more respondents.

No particular patterns emerged from demographic analysis of the results. Obstacles were rated similarly by respondents across all sectors and regions.

4.2. Next Steps

Before we can take action to address the obstacles identified in this survey, we really need to have more detail about some of the obstacles. For instance, what sorts of costs are causing the most problems? Is it cost of system design, cost of CA software, cost of certificates, cost of modifying applications, cost of training end users, cost of maintaining the system, cost of help desk support, or some other cost? Until we know that, we won't be able to figure out how to address the Costs Too High obstacle.

The PKI TC has agreed that a follow-up survey will be conducted with the survey respondents who supplied email addresses, asking them to provide details on the most top obstacles. In this survey, we can also ask them to rank the obstacles as to where they think we should expend our resources (maybe using a system where each respondent gets 10 points they can allocate among the obstacles). We will also ask the respondents to rate and rank the top six (or maybe top ten) obstacles cited by multiple respondents but not included in our original survey, since these might be considered as important or more important than the obstacles we originally listed.

After the follow-up survey has been completed, we should have a clear understanding and agreement on what the primary obstacles are. Then the PKI TC will meet and agree on specific steps to be taken to address these obstacles.

We promised to send a report on the survey results to the survey respondents. Therefore, we will complete this report, post it on our web site, and send a URL to the respondents who gave us their email address. However, we will delay widespread distribution of these results until we have completed the follow-up survey and agreed upon steps to address the obstacles.

We will use the following timeline for these next steps:

July-August 2003:

- PKI TC review Survey Report and approve publication
- Survey SC design and implement follow-up survey to obtain more detail on identified obstacles and rank newly identified obstacles

September 2003:

- PKI TC agree on specific work items to address major obstacles
- PKI TC publish Analysis of Obstacles and Work Items Agenda