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 11, 2003

Version: 0.2

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 followup 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.

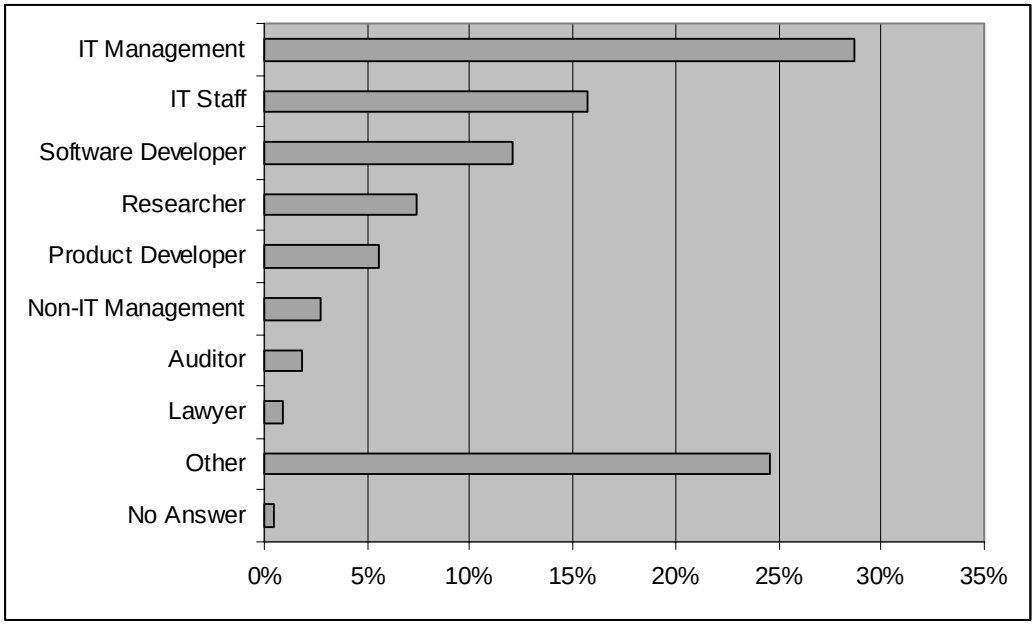

Figure 1: Primary Job Function

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.

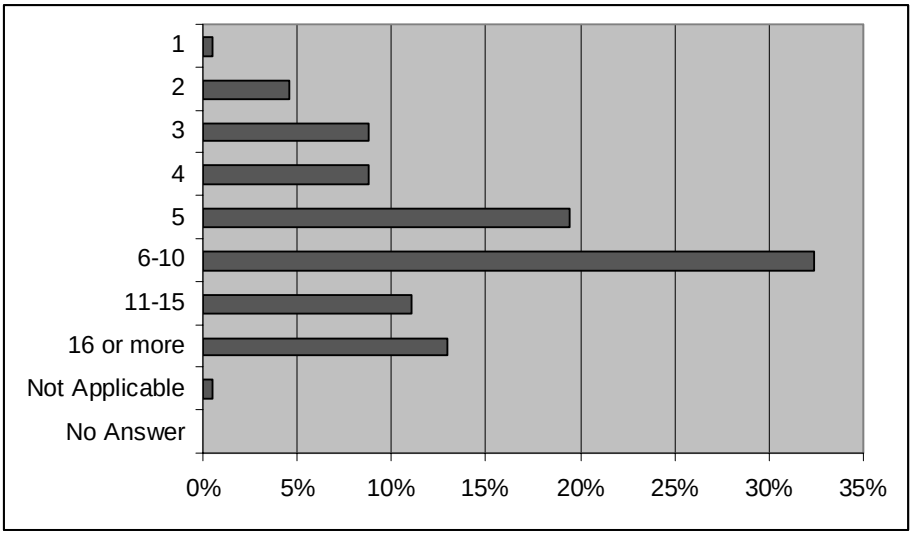

Figure 2: Years of Experience with Information Security/Privacy

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. For purposes of analysis, those chart includes an additional category that shows how many respondents checked either the Helped Deploy PKI or Developed PKI-related Software categories.

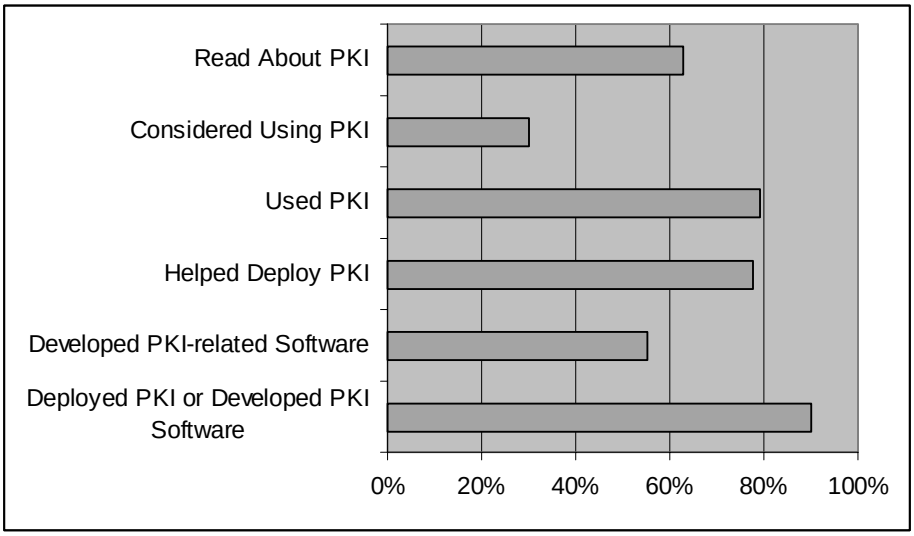

Figure 3: PKI Experience

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.

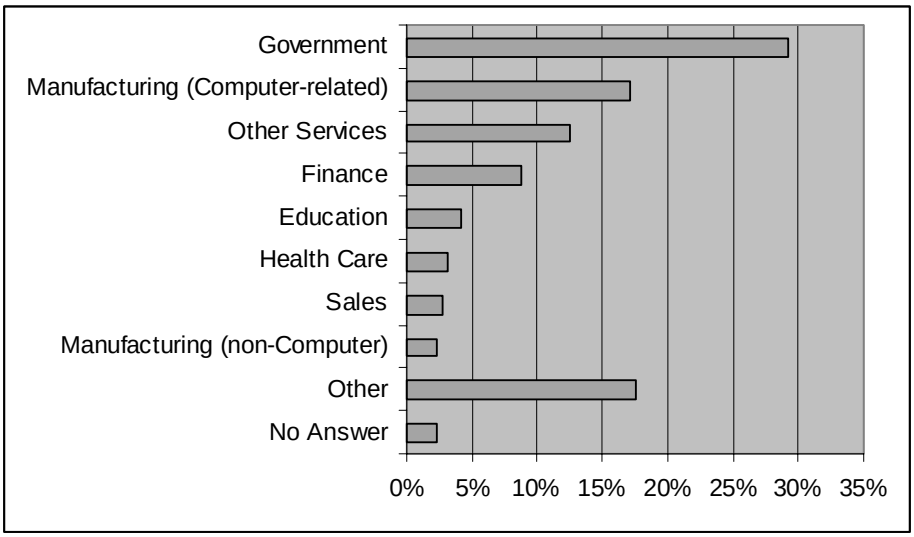

Figure 4: Employer Sector or Industry

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.

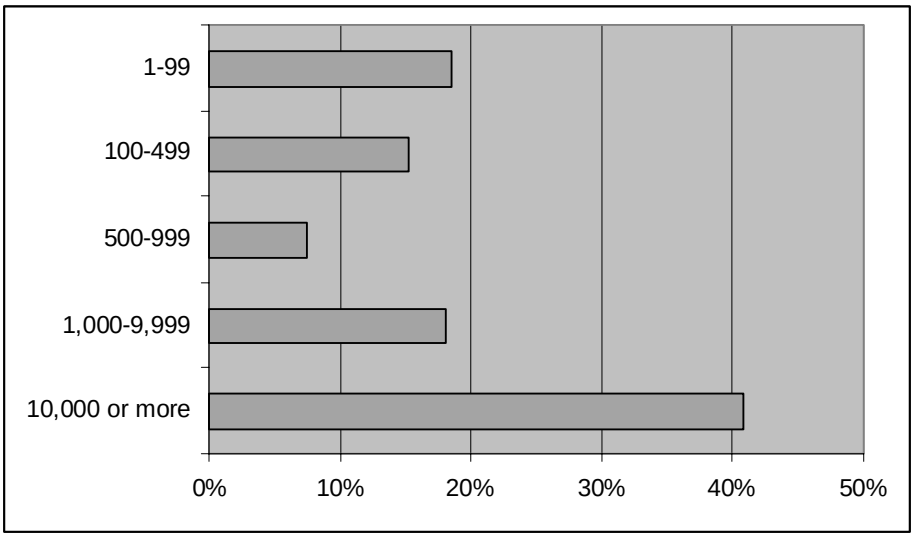

Figure 5: Employer Size (number of employees)

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.

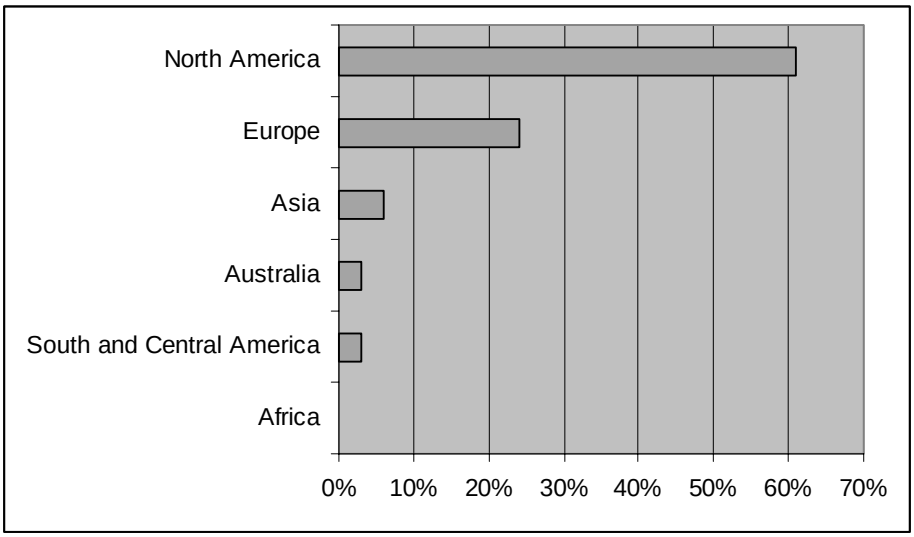

Figure 6: Primary Work Location

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.

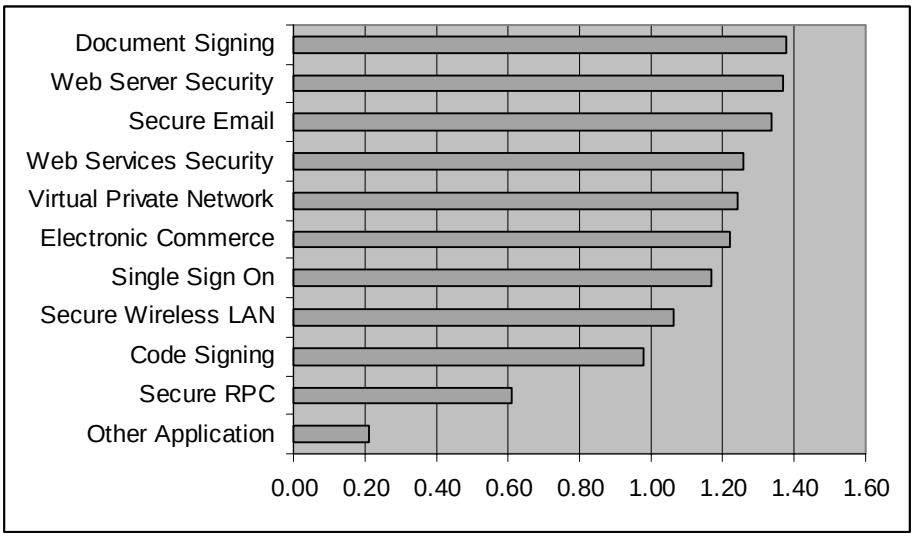

Figure 7: PKI Application Weights

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	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.

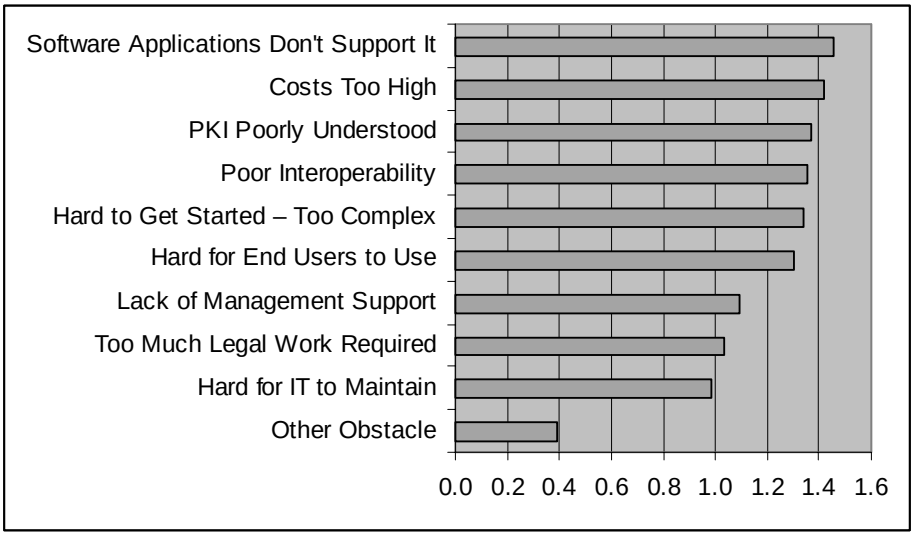

Figure 8: PKI Obstacle Weights

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. Therefore, it's worth considering these obstacles carefully. Some of them may be widely held concerns that were simply not articulated by other respondents. The textual descriptions entered in this field are included in Appendix A for reference.

A separate text field was 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. These responses are included in Appendix B for reference. And 6 more sent an email to the PKI TC chair with more comments. These emails (with identifying information removed) are included in Appendix C. Some users attached long documents to their emails. These have been archived and will be made available to the PKI TC, but they will not be distributed more widely because they include intrinsically identifying information.

We might expect that a widely held concern would be cited by more than one respondent. Therefore, we will focus our attention in this section 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 followup 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 and Recommendations

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 followup 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. Recommendations

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 Survey Subcommittee recommends that a followup survey 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 should 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.

We can also ask the respondents if they would like to help address these obstacles. To do so, they can join the PKI TC. Or they can simply agree that we'll send them our list of action items and they can sign on to specific ones.

Also, of course, we should revise and correct this report as needed, then post it on our web site and send a URL to the respondents who gave us their email address.

In order to validate the results of this survey, gather additional insights, and build support, we should ask other expert bodies such as EEMA to review this report and provide their comments.

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 should meet (perhaps in a face-to-face meeting) and agree on specific steps to be taken to address these obstacles.

We propose the following timeline for 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
- PKI TC members solicit review of and feedback on Survey Report by expert bodies (e.g. EEMA)

September 2003:

- PKI TC review results of follow-up survey and approve publication
- PKI TC agree on specific work items to address major obstacles
- Publish analysis of Obstacles and Work Items Agenda

This will be discussed at the next PKI TC meeting.

Appendix A: Other Obstacles

Survey respondents were allowed to describe and rate an "Other" obstacle (entering a separate textual description). These responses are included here for reference. They are unedited.

Difficult to deploy
Scheduling the rollout of PKI at the same time as the app
Hard to debug, easy to install insecurely
greatest burden placed on party with least to gain
too many standards that keep changing
(1) Certificate/key management on client side.
(2) Too strong association with SSL and LDAP.
(3) Poorly understood by developers/designers.
no to little infrastructure to support public key
Buggy software
Users don't need PKI very much.
operating systems and applications doesn't support smart
cards by default, smart card driver and middleware problems, applications
inflexible use of PKI and directory
Lack of supporting elements
Lack of agreement among standardization bodies
Lack of public / govenment adoption
Software developers using PKI technology may not be
aware of all the necessary steps to take to maintain security, privacy and
non-repudiation requirements for extended period of time
Doesn't scale.
Lack of PKI Enabled Applications and Industry understanding
Formerly high costs of smartcards, readers, and middleware
Lack of deployment standards. For instance, there are no standards one
can draw upon to help determine what kind of physical security is
recommended for the PKI enclave given support for spceific levels of assurance.
PKI vendors make money from selling PKI - not protecting the interests of its customers
Most PKI tries to bind names to keys and names are worthless in our applicaitons.
Technical expertise is hard to find.
Lack of easy development tools for applications
Misconception that PKI only supports high assurance applications, Privacy concerns overstated
It is hard to get infrastructure projects like PKI started in organisations.
Normaly the scope is only a project where authentication plays a role.
PKI is then considered to be too heavy.
Lack of low-cost infrastructure support, especially in certificate issuance
Lack of IMPLEMENTED fundamental security procedures within companies
+ Confusion of PKI definition and its area of use
inter-domain PKI poorly understood
User registration
Inteoperability, lack of egal precedence, distributed trust model, CRL checking, S/MIME
availability of CA
See comments below
The Business requirement is not there
lack of applications
No benefit, - Cost to much compared to the usability, this is the major obstracle for public deployment.
ROI
Application or protocol specific requirements vary and are complicated for PKI infra services

Hard for user to get started. Too cumbersome & takes too
long for initial customer authentication proof process
Lack of universal certification authority
revocation, the distributed nature, prevents the Timeshare model.
CP and CPS difficult to create properly
Certificate validation and path discovery
Too late--as goes amazon.com (running SSL/TLS), so goes (most of) the world!
Identification & Authentication
unclear objectives for use across the enterprise; inconsistent security functions across applications
The MAJOR problem we have found in a deployed PKI is revocation
and recovery process and the items that cause this process.
Nearly 70% of all revocation/recovery is associated with forgotten passwords.
Low mobility of users when keys are on SmartCard - SC readers are not a standard PC device yet
Poor understanding of what PKI can offer.

Appendix B: Lengthy Statements about Obstacles

A separate text field was 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. These responses are included here for reference. They are unedited.

Business or Commercial decisions will justify the setup and use of PKI. Thus, more efforts should be focused on the biz usage of PKI.
The party with most of the burden of implementing PKI (signer) has the least to gain from it. Typically some other party (issuer) assumes most of the risk even without PKI.
PKI does not address the real problem, which is authorization. The biggest obstacle is lack of education, and that's education of designers, developers, infrastructure planners, whatever you want to call them.
PKI architects (myself included) tend to try to solve too many problems with this solution. We need to clarify the *REAL* business problem at hand, and solve it.
One of the major problems with PKI is that it appears to me that it is a technology solution looking for a problem. Obviously, it is sound technology but many of the vendor offerings are very loose and without merit. Many of the dialogue boxes that one encounters in PKI are non-sensical and plainly legally wrong. The technology has in my opinion been oversold by vendor sales people and over engineered by the technologist. The old X509 v3 certificate is now too complicated and attempts to hold too much information. This results in misinterpretation of the standards which results in a lack of interoperability. The wording of the PKIX standards are at times indecipherable (yes I know this is a pun). The technology will in the end result in the development of gateway technology being developed which will act conversion centers for messages developed using different vendors. Much the same way as the EDIFACT gateways in EDI that Harbinger was able to secure. That is, an EDIFACT message for the transport industry is not the same as a pharmacy industry EDIFACT message and so it needs to be converted between the industries even though both messages were EDIFACT compliant. Complexity breeds a total lack of interoperablity. This causes a major impediment for the market place to trust and see value in the technology.
Complexity leads to incorrect implementations which in turn lead to work-arounds which can be considered security problems.
X509 and PKIX standard is poorly deployed or interpreted by application and service, which creates a misleading message 'PKI is expensive and hard to understand and deploy'
Your survey implies that your 'obstacles' are valid.
Requiring a specific procedure to get the status of certificates. For example, it is impossible for every software to build certification paths and check them. The s.c. four-corner model pushed primarily by banks, creates major deployment hassles for relying parties and unwanted 'markup' on business messages.
Many applications assume too much about certificate profile and directory namespace. Applications force to use certain certificate profile, subject name and directory namespace. If several applications need to be used, there may be a huge conflict. PKI product vendors seems not to know enough about real world implementation problems. Everything is fine, if vendors 'model' is followed, but there's no flexibility in design and implementation. Vendors have already decided, what's the best way to use PKI (client software, registration, etc.) and if organizations model doesn't match that - there's trouble. Application vendors doesn't seem to know how they applications use PKI. When designing PKI solution for selected set of applications, it would help, if the vendors would be able to tell how the application works. I had recent experience with a VPN-vendor and we had to debug ourselves how the PKI and directory was used and what were the requirements. Common answer is 'oh, we support X.509 certificates'.
PKI is used as a goal, not as mean to an end.
Basically, PKI support for end-client services and applications does not exist. Layman applications (browsers, e-mail client) do no integrate smoothly. Documentation is awful. When anybody is working with PKI you must know exactly what is happening anytime. Has anybody see explained how IE or Netscape verify a certificate?
Software companies have not embraced the technology fully, and many have not enabled their applications to use it, until forced to do so. Few are asking for PKI enabled apps and until more do so the vendors still push back.
Only a few engineers who understand PKI enough.

There are too many standards - for example - each browser implements a 'standard' which is incompatible with the other 'standards'
Since the cost is high, it is difficult to convince management for addition hardware. Training is another issue that stops us from rolling out secure mail.
PKI needs to be integrated into off-the-shelf system and application software.
PKI adds significant administrative overhead. I do not believe there will be wide adoption of PKI until issuing, revoking & replacing certificates on a large scale becomes feasible. Smart cards could solve this problem, but they are still too expensive, and aren't well supported.
The advantages of elliptic curve math for *not* requiring key storage is very very difficult to get across to anyone. A charge per certificate is an out-dated costing model. I would suggest a more backend pricing scheme. Many of the organizational reasons for non-use is cost.
Too much focus on problems, not enough on business needs & requirements
The initial barrier for deploying PKI is also too high. For example, for S/MIME to be fully interoperable, certificates must trace back to commonly recognized CAs. Other issues such as document recovery support (in case of encrypted messages), and legal issues (in case of digital signatures) are also hurdles
Apps do not adhere to the standards, e.g. if your cert does not include an email address, you cannot send signed S/MIME msgs, while you should according to the standard.
Poor interoperability between cryptographic modules (eg: PKCS #11 V1 & V2, CAPI, etc.)
LRA function is important for the proper identification of users, however it is time consuming and very difficult to manage in remote areas where users need desktop certs and client software. Client software is another issue when the PC is owned by the user. Who is responsible when the software crashes the user's machine? Remembering strong passwords is an issue when users access PKI infrequently, or infrequent use results in premature expiry of the cert.
PKI largely still too theoretical. Would benefit tremendously with more real-world applications that really work. User registration (again, in the real world) continues to pose huge challenges.
The added functionality provided by secure applications is trivial as compared to applications that people actually purchase. This means that even if the cost and complexity of PKI were dramatically reduced overnight, PKI would still not be used on any large scale. PKI was standardized before the technology had evolved sufficiently to define functionality that provides tangible benefits for users. To perhaps oversimplify, there is no business case for electricity but there are a great many business cases for 'useful' products that utilize electric motors. The few knowledgeable users who attempted to voice their opinions within the standards process (PKIX, for example) were quickly and effectively shouted down by so-called security experts, many of whom appear to possess a rather narrow range of expertise and little, if any, grace.
A client private key that is kept on disk is little better than a password ... need secure key storage (e.g. smart cards).
The fact that you are taking this survey, and its content, shows that we as an industry still don't get it. 'PKI' is technology in search of a problem to solve. When PKI is buried in market-disrupting services, then it will sell. And probably not in large quantities at first. Which would you rather be - an anonymous hero or a well-known failure? PKI is currently the latter.
The basic traditional use for which PKI was proposed is flawed and does not fit the business model and requirements. PKI is best suited to certain niche areas.
Although standards exist, they seem to be all over the place. So, other than implementing the lowest common denominator functionality yourself, it is difficult to evaluate, choose, and integrate any PKI technology/products.
Too few public services for the average citizen, to justify the investment in time to get and install a certificate. In the organisation itself, the need is limited to sign-on. This applies both to our company itself and our customers. The digital signature are only needed, in a few cases. The real usage will be for identification in webservices, and for signing data in transit ie. XML signature.
Deployment of PKI is started straight with smart cards, moving from usernames and passwords directly to PIN and smart card. That way software based PKI is not established in between and the PKI itself remains strange and difficult to end users, because it is not common and familiar in any form.
Lack of business application with an ROI are the inhibiting factor. New regulations will help drive PKI.

X.509-STYLE PKI IS A POOR SOLUTION FOR ACCESS CONTROL AND DATA AUTHENTICATION Digital certificates were invented a quarter of a century ago, for the specific purpose of facilitating the encryption of messages using public key cryptography. They were never intended to be the basis for access control and data authentication. Consequently, today's commercial PKI offerings (which are all based on digital identity certificates and attribute certificates that are linked to identity certificates) do not take into account any of the scientific advancements in access control and data authentication made in the past 25 years. They offer no protection against the lending of access rights and a myriad of other attacks, do not respect any of the privacy principles that are commonly codified in law, and suffer from a host of performance drawbacks (which certificates were intended to eliminate in the first place) due to their heavy reliance on trusted online repositories. Security Drawbacks PKI based on identity and X.509-style attribute certificates does, at best, a mediocre job of protecting electronic security: 1. Systemically relying on user identification more often enables than prevents fraud, as the dramatic rise in identity fraud over the past decade shows. Criminals who manage to steal identity certificates or to assume the identities of unwitting people will be able to misuse certificates in cyberspace on a global scale, while their victims take the blame. Also, CAs will have to establish identities on the basis of legacy paper-based systems, and will thus inherit their insecurity. For example, identities may have been erroneously or maliciously swapped or forged. 2. By relying heavily on central data repositories, identity certificates push the door wide open to devastating abuses of security holes. It is difficult for organizations to protect their online databases against misuse by hackers, let alone by insiders. Furthermore, data records may be outdated, and may be the result of misattributions due to identity theft. 3. Identity certificates offer no intrinsic cryptographic protection to discourage certificate holders from transferring (copies of) their credentials and access rights to other parties: the secret key of a certificate holder is simply a random number, and so revealing it to someone else has no direct negative consequences for that certificate holder. Particularly, when X.509-style identity and attribute certificates are used in closed applications they can only be used in limited ways, so that giving away copies of a secret key will not enable others to misrepresent themselves as the legitimate certificate holder in other applications. This defeats the entire purpose of identity certificates. 4. If the secret key of a certificate is generated and stored on a personal computer or the like, it is virtually impossible to prevent its compromise, loss, disclosure, modification, and unauthorized use. Processing an X.509-style certificate on a smartcard, on the other hand, suffers from numerous drawbacks: a. The computational, communication, and storage requirements exceed those that today's simple 8-bit smartcards offer. The addition of complex circuitry and software to a smartcard is expensive, can easily lead to new weaknesses in the internal defense mechanisms, and adversely affects reliability. The ability to protect smartcards against attacks such as differential power analysis hinges on having enough capability and space for a software solution. b. Since the goal of smartcards is to shield their internal operations, it is virtually impossible to verify that a card does not leak its card identifier, its access control code, data from other applications running on the same device, and so on; CAs must have strong trust in the honesty of their smartcard suppliers. c. The smartcard must be relied on to protect the security interests of its holder. Since standard smartcards do not have their own display and keyboard, user identification data must be entered on a terminal communicating with the card, and this terminal must be trusted not to capture the user's identification data. Likewise, any results that the card wants to communicate to its holder must be displayed on the terminal. The result is that a variety of fake-terminal attacks become possible. d. There is no way to verify that the secret keys within the smartcards are generated in such a manner that others cannot guess them. In particular, it is very hard to guarantee that the CA or the smartcard supplier cannot reconstruct all the secret keys. This makes the legal status of digital signatures highly doubtful. 5. While revocation is an exceptional circumstance, the task of verifiers to check the revocation status of unexpired certificates is not. They must either have the certificate status validated at the time of the transaction or regularly download a CRL update. This gives the Revocation Authority the power to falsely deny access to targeted certificate holders, by blacklisting their public keys. Worse, it gives an adversary the power to take the system down by breaking into the CRL repository, thereby defeating the main security advantage of off-line certificate verification. Similarly, any uniquely identifying data in a certificate (such as a key holder identifier, the public key, or the CA's signature) can be misused to deny a key holder access to PKI services, and to block his or her communication attempts in real time. For example, blacklists can be built into Internet routers, and transaction-generated data conducted with target public keys can be filtered out by surveil! lance tools. 6. Any digital signature made by a certificate holder can be used as non-repudiable transaction evidence not only by the legitimate receiver, but also by anyone else who sees the signed statement, including parties that have no right to the information. This leads to all sorts of risks, including conflicts with privacy legislation. It also exposes the CA, the verifier, and other legitimate parties partaking in the transaction to potentially unlimited legal liability. 7. To issue an X.509-style identity or attribute certificate, the CA must know the identity and any other attributes that go into the certificate. This prevents any data separation when that data resides in the databases of other organizations. (This is actually the main reason why the business model of Managed CA Services has never caught on.) Privacy Dangers

Digital identity certificates are widely touted as a means to protect privacy, since messages can be encrypted with the public key of the intended receiver. Nothing can be further from the truth. Confidentiality (that is, preventing a wiretapper from decrypting intercepted messages) does nothing to prevent all kinds of other privacy threats, such as parties tracing, linking, selling, or misusing the data in whatever manner they see fit. In fact, identity certificates have devastating consequences for privacy: 1. The actions of certificate holders can readily be traced and linked on the basis of the certificates presented, since a digital certificate is a unique bit string. In many cases, it is not only the verifiers who can trace and link the actions of the individuals they interact with, but also the CA. Specifically, this will be the case when verifiers deposit transcripts of their interactions to the CA (to enable central fraud detection or the computation of visitor behavior statistics), and in any closed application in which verifiers are effectively the same entity as the CA. This enables the compilation and distribution of detailed dossiers about individuals' habits, behavior, movements, preferences, characteristics, and so on. Furthermore, all the dossiers compiled by linking and tracing the actions of participants in one PKI can be tied to the dossiers compiled in other PKIs, and can be linked to a myriad of other sources of personal information. 2. When digital certificates are implemented in smartcards and other tamper-resistant devices, the privacy of certificate holders is even more at risk. A card can directly leak personal data, for instance by sending along additional data when engaging in a protocol, by encoding information in message fields or random numbers, and so on. Indeed, as Moreno, the inventor of the first generation of smartcards in the early seventies, warned, smartcards have the potential to become ``Big Brother's little helper.'' 3. CRLs are distributed to all verifiers, and potentially to anyone who requests them; in this manner, entities can collect data about key holders they have never communicated or transacted with. Online certificate validation services are even worse: they allow anyone to verify not only negative data but also positive data (such as the mere fact that one is a participant), and enable the Revocation Authority to learn in real time who communicates with whom. They are also undesirable from the perspective of verifiers, since third parties learn the identities of their visitors, their peak hours, and other data that is either competitive data or that must legally be protected. These undesirable properties make it impossible for individuals and verifiers alike to control how much data they actually disclose to other parties in the system. Identity certificates that specify a "pseudonym" instead of a real name, an approach that is often proposed in digital signature law, are not a valid solution: • "Pseudonymous" certificates that can only be obtained by certificate applicants who identify themselves do not prevent tracing; they provide no more privacy than Social Security numbers, credit card numbers, and health registration numbers, all of which a verifier can readily link to an identity by looking into any number of database entries to which the "pseudonyms" point. Moreover, the correlation is at all times known to the CA, typically the most powerful party in the system. Similarly, X.509-style attribute certificates that do not explicitly specify true names can be linked and traced as easily as identity certificates, on the basis of their public key or the signature of the CA. In fact, they worsen the privacy problem, since the dossiers that CAs, verifiers, and wiretappers can compile are even more complete. • The alternative of not requiring certificate applicants to identify themselves at all offers better privacy, but makes it impossible to ensure accountability, and to protect against lending, copying, discarding, and other misuses of certificates; it is not even possible to contain the damages due to fraud. The approach is also impractical in almost all applications. Even if the CA certifies only personal attributes that do not identify the certificate holder, such as age and marital status, often the only way for the CA to verify the attributes is by establishing the applicant's identity and using this to look up the attributes in a trusted database. Also, registration without identification may be difficult and would prevent applicants from building a long-term relation with the CA. More generally, the idea of issuing an identity certificate to an unidentified party does not make much sense in the first place. Performance Drawbacks The central database architecture on which X.509-style digital certificates rely creates numerous performance problems: 1. The transaction process requires a sufficient delay to identify and correct frauds or other undesirable conditions. This may result in organizations not being able to serve as many customers as they could otherwise, or in customers leaving and going elsewhere (especially when browsing on the Internet). 2. Online certificate validation is costly, hard to scale to large communities, and suffers from all the security problems of the central database paradigm. The distribution of CRLs or CRL-updates, on the other hand, requires verifiers to manage their own versions of a CRL and to deal with certificates they are not interested in, and creates a lag between the time a certificate becomes invalid and when it appears on the next CRL update. If validity periods are long, CRLs will grow and additional computing resources are needed for searching and storing them. 3. There is significant uncertainty in the outcome of the transaction process, because the certificate verifier makes its authorization decision on the basis of remotely stored data that may be erroneous or irrelevant, or simply because the online connection fails (e.g., due to peak load or a natural disaster). Also, requests for central database look-up may be dishonored for many reasons and may be expensive (many large databases are operated by commercial organizations such as consumer reporting bureaus). 4. In case the representatives of an organization are spread out geographically, central database verification may be expensive (due to communication costs or the difficulty of dealing with peak load) or may simply not be an option

because of the absence of network connections. These drawbacks can be alleviated by using an X.509-style attribute certificate that contains all the data for the verifier within it. However, this introduces a serious problem due to the fact that all the attributes within a certificate are systematically revealed when showing the certificate. Quoting the authors of the SPKI/SDSI standard, ``because [...] certificates will carry information that, taken together over all certificates, might constitute a dossier and therefore a privacy violation, each [...] certificate should carry the minimum information necessary to get a job done." This implies that all the data pertaining to a single party must be distributed across many digital certificates that are issued to that party, which introduces serious administrative overhead. Moreover, this means that a single certificate is not suitable to serve its holder in multiple applications.
We are a scientific oriented organisation in an international political arena. This makes CPs and CPSs very difficult. 1. Time it takes for customer to carry out the initial identification process to get a certificate is the primary obstacle. 2. Has been expensive and complex to build PKI into web services applications.
There really are 4 C's limiting the use of PKI: cost, complexity, convenience and cross-certification. We also have concerns related to the accumulation/centralization of personal information needed to fuel the authentication system for PKI/single sign-on. While some applications are less demanding, certificate management including effective certificate revocation is vital. CA services in particular need to become a commodity, with possibly more tailored RA services to suit different apps. But perhaps a PKI cert should be issued to every Australian.
Unfortunately PKI is developing a bad name in the corporate and commercial sectors for being expensive to both implement and maintain within a single enterprise. The emerging model would be to move to a utility that provides the back-office CA and focus on getting more ubiquitous usage through pki enabled apps and cost effective deployments. Universal secure email would be a good place to start in the business community.
People have different opinions on PKI and its uses. The main one being 'PKI is a technology'. In my view, PKI is a business solution than has technology considerations. Too many IT folks pay more attention to the certificate issuance and little on key management, recovery, key rollover, and especially ease-of-use for the end user.
PKI today is treated (by PKI vendors) as a major enterprise project while it should be a commodity transparently available and at a low (minimal) cost
We were able to work through the CP and CPS, but I would suspect that many organizations would have difficulty with the documentation and legal aspects.
Cost cost cost cost cost. PKI is no different than an e-mail server. However, PKI companies want to sell what should be a $2000 piece of software for $50,000-$100,000 +. This is stupid.
Microsoft CAPI does not (correctly) support plug-in validation (e.g., Valicert). Microsoft applications behave irradically when it comes to certificate validation.
Hierarchical trust is an un-natural act. PKIs requiring CRLs are fatally flawed.
Biggest problem is that more applications need to be PKI-enabled - to accept certs for authentication, digital signatures, and/or persistent encryption. As more become enabled, the demand for certs will increase - and that will promote interoperability, single-credential sign-on, etc.
Most do not understand that PKI is not difficult, just complex; that once it is understood, it is relatively simple. In addition, vendors sell it as more difficult than it needs to be and don't offer the simple solutions.
The cumbersome, complex and unnecessary X509 digital cert format is a major problem...
We have a global PKI infrastructure and it is corporate policy that access into the corporate network is by certificate. The main issues we face are lack of applications to utilise it, user resistance to certs based on previous experience, the perception that anything to do with the Internet is quick and cheap so why can't we just use SSL like everyone else, cost of cert management. My main headache at the moment is how do we safely and efficiently extend to work with 3rd parties and external contractors.
PKI vendors and consultant always tell you that you need to spend millions of dollars, regardless of how minor your needs are. For example, if you want to issue few hundred certificates to your employees for internal use, the free Microsoft Certificate Server is as good as any high-priced PKI software. You also do not need to spend hundreds of thousands of dollars on CP and CPS since your employees are already bound by other employment agreements.
We have observed some difficulties regarding the privacy. The principal difficulty is the constitution of a database of all the users at the CA. It is probably not a major obstacle in a small business but it is a problem in government organization

PKI deployment in an already established corporate infrastructure runs into obstacles such as directory server limitations, legacy data sources, and interoperability between departments within an organization. PKI's that change the way a firm does business are destined to fail, the registration and use of the certificates has to fold into current use practices. We have found that the time it takes to integrate and develop a registration process that fits the firm, is well worth the time to deploy. Also, the management of the infrastructure is often VERY expensive, the cost to manage components has to be addressed since it is often mundane procedures. My team and I have deployed 6 PKI's and have a great deal of experience in the associated problems encountered. We have fought the battles including the usual 6 months to determine what a DN should look like, what extensions do I really need in my certificate, and I forgot my passwords can you help? Currently we deploy a hybrid model, named such since it uses both central and distributed key generation features where appropriate in the certificate generation function. This model has been designed to address the obstacles and lessons learned in the previous 2 deployment models. Each new component provides a solution for an obstacle previously determined to be of major concern. Forgotten passwords, split key reconstitution for friendly recovery solutions, automated phone help, and high assurance identity processes, each is a unique component that can be included and assure success in the deployment of the PKI.
Daily used applications still don't offer the sufficient level of support to PKI - common business processes still use hard copy documents instead of signed e-documents. The mobility of users is the second issue - the users can usually use SmartCard to make digital signatures in the office, but outside of their company there are total absence of SC readers to be able to use digital signatures for personal purpose, e.g. signing private mails, banking transactions, declaration of income etc.
The present complexity and ongoing management costs associated with operating a CA and using PKI make it unaffordable unless economies of scale (large number of users) possible. Management and public assumptions around use of more simplistic approaches like PINs and SSL, and general lack of security concerns (or awareness) all add up to a 'tough sell' for what is clearly the best available solution at this stage.

Appendix C: Email Responses

Some survey respondents sent an email response to the survey. These responses have not yet been included in this report, but they will be soon.