

Identifying and Overcoming Obstacles to PKI Deployment and Usage

Stephen R. Hanna
Sun Microsystems, Inc.
steve.hanna@sun.com

Jean Pawluk
Inovant
jpawluk@visa.com

Abstract

Public Key Infrastructure (PKI) is a fundamental security technology used in many applications. Nevertheless, PKI deployment has been slow. Why? In June and August 2003, the OASIS PKI Technical Committee conducted two surveys aimed at identifying the top obstacles to PKI deployment and usage and soliciting suggestions for how these obstacles can be overcome. This paper presents the results of those surveys and summarizes the PKI Action Plan that the PKI TC has developed in response.

1. Introduction

Around the world, security threats are escalating and the demands that business and personal information be safeguarded are mounting. Business, governments, and consumers want access to their information in a mode that is easy to use, yet secure.

Public Key Infrastructure (PKI) is a fundamental security technology used in many applications to provide those security assurances. For a number of years, the promise of PKI has been challenged by its complexity and the costs of deployment.

The OASIS PKI Technical Committee was formed in January 2003 to tackle the issue of how to successfully deploy and use Public Key Infrastructure. As early adopters of PKI technology, many members of the committee have first-hand experience with the challenges of implementing PKI technology. As a result of their combined experiences, the committee decided that an impartial survey was needed to further identify the critical obstacles to widespread use of PKI.

A short, multiple-choice web-based survey was prepared and hosted on the group's web site in June 2003. Invitations to participate in the survey were distributed to standards and industry groups as well as security vendors and their customers around the globe.

After reviewing the June 2003 survey results [1], the OASIS PKI Technical Committee prepared a second survey to gather more detailed data about specific obstacles. This second survey was publicized to the participants in the original survey during August 2003 [2].

The data gathered through these surveys provides a clear view of the obstacles impeding PKI deployment and usage. The survey respondents also provided specific suggestions for addressing these obstacles with a clear consensus emerging from the many responses.

Based on this consensus, the OASIS PKI Technical Committee developed a PKI Action Plan [3] with five specific action items addressing the top five obstacles identified in the surveys. After several months of public review and comment, the committee has published the PKI Action Plan and begun implementation.

Implementing the plan will require cooperation from many parties: vendors, customers, standards groups, etc. If these groups can overcome their differences and work together, the obstacles to PKI deployment may be greatly reduced.

2. Review of Previous Work

For several years, starting in 1997, the "Year of PKI" was proclaimed by vendors selling the promise that public key infrastructure would revolutionize security by safeguarding electronic transactions. While PKI has been very successful in certain realms (secure web browsing), the full scope of these declarations is yet to be fulfilled.

According to the findings of Burton Group research originally published in 2001 and in late 2002 [4], progress in PKI deployment has been made over the past decade, but very slowly. "While public key security potential is vast, public key infrastructure (PKI) continues to struggle with interoperability,

complexity and application integration issues that slow customer adoption. PKI's sophistication hasn't translated into mass enterprise deployments."

The Burton Group researchers state that "The major applications using PKI today remain web-based authentication and virtual private networks (VPN), though the use of digital signature based electronic forms applications continues to grow".

They also stated, "Much of the complexity retarding PKI arises because a complete PKI requires multiple products from multiple vendors" including the PKI enabled application, a certificate authority vendor, a directory services vendor, and the vendor specific software for hardware clients and servers. A functional PKI may also include scenarios "that include smart cards and other cryptographic devices, professional services or system integration services, access management portals, certificate validation services... and more".

These concerns about PKI are reflected in numerous similar articles and papers in the trade press, conferences, and workshops [5], [6].

3. June 2003 Survey Results

In the June 2003 survey conducted by the OASIS PKI Technical Committee [1], the participants were asked to rate the importance of several common PKI applications and the importance of commonly cited obstacles to PKI deployment and usage. They were also asked to provide demographic information, which was used to check for survey bias and correlations between demographics and opinions. Finally, they were asked to list applications and obstacles missing from the survey.

3.1. Survey Sample

The June 2003 survey was open to anyone with an opinion on PKI obstacles, but aimed at people with

expertise or experience in this area. Therefore, the survey invitations were sent to organizations and email discussion lists dedicated to PKI.

The 216 survey respondents were found to be a group of experienced group of industry professionals with serious PKI experience.

A large variety of job titles and functions were found among the respondents. Many of them had both technical and business functions included within their scope of their job duties. More than 75% of the respondents had at least 5 years of experience in Information Security / Privacy.

With over 90% of the respondents having either deployed or developed PKI software, they were very experienced with PKI. The majority of the participants were from the USA and Canada (60%) however over 30 countries were represented with many participants from Europe or Asia.

3.2. Analysis of Applications

Survey respondents 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 area under Other (such as Identity Management, Non-Repudiation, and Document Encryption) and rate its importance.

For analysis, these ratings were combined into a weight by assigning 2 points for each respondent who rated an application Most Important and 1 point for each rating of Important. By computing these weights, the applications can be ranked by importance (as indicated by the respondents).

As shown in Table 1, most applications were found to be important but no one application stood out as the most important.

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: Application Weight Rank

Application weights are shown graphically in Figure 1.

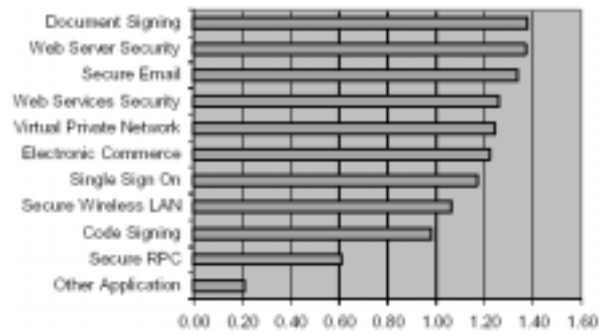


Figure 1 PKI Application Weights

These results affirm the view that PKI is a foundational technology used in many applications.

As business, governments and consumers all have different PKI needs, they also have different concerns about the importance of the listed applications. The survey results showed strong correlations between respondents' employment sector and their rating of applications. Government sector respondents ranked Document Signing 10% higher and Code Signing 11% lower than the total sample. In contrast, respondents in the Computer-related Manufacturing sector ranked 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.

3.3. Analysis of Obstacles

In a manner similar to the rating of applications, respondents were presented with a list of possible obstacles to PKI deployment and usage 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 rate it in the same way.

Weights were computed by assigning 2 points to Major Obstacles and 1 point to Minor Obstacles. Using these weights, ranks were computed. The results are shown in Table 2.

The PKI Obstacles weight ranking is shown graphically in Figure 2.

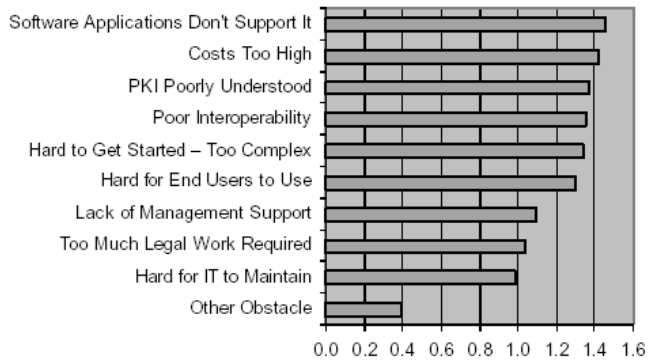


Figure 2 PKI Obstacle Weights

Many survey participants listed other obstacles to PKI deployment and usage. Here is a list of the obstacles that were cited by several respondents:

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

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 Weight Rank

Unfortunately, the outcome of the survey question on obstacle ratings was inconclusive. Many obstacles had similar weights. Obstacles were broadly defined so it was not clear what respondents meant. In addition, several obstacles cited as Other Obstacles were noted by multiple respondents, indicating that the list of obstacles was incomplete. Therefore, the OASIS PKI Technical Committee Survey decided to conduct a followup survey to clarify the obstacles and ratings.

4. August 2003 Survey Results

The OASIS PKI Technical Committee’s August 2003 survey [2] introduced a new points-based rating system that allowed respondents to clearly indicate priorities. It added “Other” obstacles cited by multiple participants in the June 2003 survey. It asked several questions designed to refine the broad categories used in the June survey. Moreover, it asked respondents to suggest ways that the obstacles could be addressed.

4.1. Survey Sample

The OASIS PKI Technical Committee sent invitations only to people who responded to the June 2003 Survey and provided an email address. This allowed us to use the previously gathered demographic data in analyzing the results while avoiding the need to ask for such data again. We found that the respondents to the August 2003 survey were similar in demographics and opinions to the earlier respondents.

4.2. Analysis of Obstacles

Instead of asking respondents to rate obstacles as a Major Obstacle, a Minor Obstacle, or Not an Obstacle, the August 2003 survey asked respondents to allocate 10 points among the obstacles listed, giving points to each item according to its importance. This allowed respondents to heavily weight items that were especially important to them. The results are shown in Table 3.

Obstacle	Average 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 3: PKI Obstacles Point Rank

The point-based rankings reveal a substantial difference between the top five obstacles, which account for about 60% of the points, and the remaining ten obstacles. This does not mean that the lower-rated obstacles are not important. Most of them were rated as Most Important or Important by a majority of the respondents to the June 2003 survey. But the top five obstacles are just *more* important to the survey respondents.

The results were carefully checked for any sign that a small number of respondents might be skewing the results by throwing more votes than average to one item. This was not found to be true. In fact, the obstacle rankings were consistent across many demographic lines (experience, geography, industry sector, etc.). This was true for almost all opinions expressed in both surveys (except application ranking, as noted above).

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 the standards are so

flexible and complex, implementations from different vendors rarely interoperate.

5. PKI Action Plan

The two surveys conducted in June and August 2003 allowed the OASIS PKI Technical Committee to identify the primary obstacles to PKI deployment and usage and to develop a PKI Action Plan [3] to address the obstacles. Here is a brief synopsis of that Action Plan.

5.1. Call for Industry-Wide Participation

The OASIS PKI Technical Committee recognizes that it cannot act independently in implementing this Action Plan. PKI involves many parties: customers and users, CA operators, software developers (for applications, PKI components, platforms, and libraries), industry and standards groups, lawyers, auditors, security experts, etc. This PKI Action Plan was developed based on input from all of these parties. The OASIS PKI Technical Committee calls on these parties to assist in its implementation.

5.2. Action Items

Develop Application Guidelines for PKI Use

For the three most popular PKI applications (Document Signing, Secure Email, and Electronic Commerce), specific guidelines should be developed describing how the standards should be used for this application. These guidelines should be simple and clear enough that if vendors and customers implement them properly, PKI interoperability can be achieved.

PKI TC members will contact application vendors, industry groups, and standards groups to determine whether such guidelines already exist and if not who could/should work on creating them. In some cases, standards may need to be created, merged or improved. If application guidelines already exist, the PKI TC will simply point them out.

Who: PKI TC Guidelines Subcommittee, Application Vendors, and Industry and Standards Groups

When: Spring 2004 for initial work

Increase Testing to Improve Interoperability

Provide conformance test suites, interoperability tests, and testing events for the three most popular applications (Document Signing, Secure Email, and Electronic Commerce) to improve interoperability.

Certificate management protocols and smart card compatibility are also a concern. Branding and certification may be desirable. The PKI TC will work with organizations that have demonstrated involvement in or conduct of PKI interoperability testing or conformance testing to identify and encourage existing or new efforts in this area. Interoperability has many aspects. See the PKI Interoperability Framework white paper at <http://www.pkiforum.org/whitepapers.html> for details.

Who: PKI TC Testing Subcommittee with Industry and Standards Groups

When: Spring 2004 for initial work

Ask Application Vendors What They Need

OASIS PKI TC members will ask application vendors for the three most popular applications (Document Signing, Secure Email, and Electronic Commerce) to tell us what they need to provide better PKI support. Then we will explore how these needs (e.g. for quantified customer demand or good support libraries) can be met.

Who: PKI TC Ask Vendors Subcommittee, in cooperation with application vendors

When: Spring 2004 for initial work

Gather and Supplement Educational Materials on PKI

Explain in non-technical terms the benefits, value, ROI, and risk management effects of PKI. Include specific examples of PKI applications with real benefits and ROI. Also explain when PKI is appropriate (or not). Educational materials should be unbiased and freely available to all. If these materials already exist, the PKI TC will simply point them out. Otherwise, it will develop them in cooperation with others.

When: January – August 2004

Explore Ways to Lower Costs

Encourage the software development community (including the open source community) to provide options for organizations to conduct small pilots and tests of PKI functionality at reasonable costs—in effect reducing cost as a barrier to the use of PKI. Of course, operating a production PKI involves many costs other than software acquisition so an effort will be undertaken to gather and disseminate best practices for cost reduction in PKI deployments around the world.

Who: PKI TC Lower Costs Subcommittee, software development community, customers, etc.

When: Initial efforts in 2004

6. Conclusions

The results of the surveys conducted by the OASIS PKI Technical Committee identify the primary obstacles to PKI deployment and usage, as judged by the survey respondents. They also provide suggestions for addressing those obstacles.

Based on these results and on feedback from many PKI users, vendors, and other stakeholders, the OASIS PKI Technical Committee has prepared a PKI Action Plan to address the obstacles identified. Implementing the PKI Action Plan will be challenging but it provides some hope that PKI deployment will be easier and the benefits of PKI (strong and scalable security) will be widely realized.

7. Acknowledgments

Without the hard work and dedication of the members of the OASIS PKI Technical Committee, the results documented here would never have come to light. The survey respondents are thanked for their hard-won insights, which serve as a primary source for this paper. In addition, the PKI Action Plan reviewers and supporters are thanked for their assistance in hopes that it will lead to the successful completion of the PKI Action Plan.

Thanks to OASIS for granting permission for portions of the PKI Action Plan and survey analyses to be reproduced in this paper.

Thanks to The Burton Group for allowing us to quote one of their research reports.

8. References

[1] OASIS Public Key Infrastructure Technical Committee, "Analysis of June 2003 Survey on Obstacles to PKI Deployment and Usage", August 8, 2003
<http://www.oasis-open.org/committees/pki/pkiobstaclesjune2003surveyreport.pdf>

[2] OASIS Public Key Infrastructure Technical Committee, "Analysis of August 2003 Follow-up Survey on Obstacles to PKI Deployment and Usage", October 1, 2003
<http://www.oasis-open.org/committees/pki/pkiobstaclesaugust2003surveyreport.pdf>

[3] OASIS Public Key Infrastructure Technical Committee, "PKI Action Plan", February 2004
<http://www.oasis-open.org/committees/pki/pkiactionplan.pdf>

[4] Dan Blum and Gerry Gebel, "Public Key Infrastructure: Making Progress, But Many Challenges Remain, V2", Directory and Security Strategies Research Report No. 612, Burton Group, Utah, February 13, 2003, pp. 5-7, <http://www.burtongroup.com>

[5] United States General Accounting Office, "Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies", (GAO-04-157), Washington D.C., December 2003
<http://www.gao.gov/cgi-bin/getrpt?GAO-04-157>

[6] Peter Gutmann, "PKI: It's Not Dead, Just Resting", IEEE Computer, August 2002, pp. 41-49

9. Copyright Notices

Copyright 2004 Sun Microsystems, Inc. All Rights Reserved.

Copyright 2004 Inovant. All Rights Reserved.

For portions reproduced from OASIS documents:

Copyright OASIS Open 2004. All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to OASIS, except as needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it into languages other than English.