

PKI Action Plan

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

Editor: Steve Hanna (Sun Microsystems, Inc.)

Date: October 6, 2003

Version: 0.2

DRAFT

Table Of Contents

<u>Table Of Contents</u>	2
<u>1. Introduction</u>	3
<u>1.1. About the OASIS PKI TC</u>	3
<u>2. Survey Results</u>	4
<u>2. The PKI Action Plan</u>	6
<u>2.1. Action Items</u>	6
<u>2.2. Next Steps</u>	7

Copyright (C) OASIS Open 2003. 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.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

1. Introduction

Public key infrastructure (PKI) was invented more than 20 years ago. Today, it is used in many important standards and protocols (such as SSL/TLS, IPSEC, etc.). Millions of times each day, someone visits a secure web site for shopping or banking and PKI is used to secure the connection.

Yet PKI has not reached its full potential. PKI can be used to authenticate people, avoiding the need to remember dozens of PINs and passwords. It can be used to secure commercial transactions and protect the privacy of emails and telephone conversations. But high costs and interoperability problems have limited the use of PKI.

The OASIS Public Key Infrastructure Technical Committee (the OASIS PKI TC) has started an effort to address the primary obstacles to PKI deployment and usage. This PKI Action Plan calls for a united effort to address these obstacles. Such an effort will bring reduced costs and greater security, benefiting all parties: PKI users and prospective users, software vendors, etc.

Therefore, the OASIS PKI TC is asking all PKI stakeholders (users, vendors, standards groups, and experts) to review, comment on, and support this PKI Action Plan. We plan to announce the Action Plan in February 2004 and begin executing the plan at that time. Within two years, PKI deployment should be substantially easier.

1.1. About the OASIS PKI TC

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=pmi

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.

2. Survey Results

An initial survey was conducted in June 2003, asking respondents to identify the most important obstacles to PKI deployment and usage. This survey was successful in attracting a large number of highly qualified respondents, who identified certain specific obstacles. A follow-up survey conducted in August 2003 refined the PKI TC's understanding of the obstacles. The results from these surveys are available at <http://www.oasis-open.org/committees/pki/pkiobstaclesjune2003surveyreport.pdf> and <http://www.oasis-open.org/committees/pki/pkiobstaclesaugust2003surveyreport.pdf>

Readers should consider reading these reports to gain a more complete understanding of the obstacles identified by survey respondents. However, we will present here a brief summary to set the stage for the PKI Action Plan.

More than 200 respondents participated in the PKI TC surveys. These respondents had a variety of backgrounds and perspectives, including large numbers of IT management and staff. An amazing 90% of respondents had either helped deploy PKI or developed PKI-related software.

The top five obstacles to PKI deployment and usage identified by the surveys are:

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

Other obstacles were also cited, but these five were rated much higher than the others.

The survey respondents indicated that their most important applications are Document Signing, Secure Email, Electronic Commerce, and Single Sign On. Document Signing was further broken down into Signing Forms, Signing Contracts, and Signing Documents before Dissemination, with roughly equal interest in each of these three subcategories.

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. They are:

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

What can be done?

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

The PKI TC has considered these recommendations carefully and prepared a draft PKI Action Plan based on them and also on the experience of the PKI TC members. With respect to the last two items, there are already efforts underway in these areas by others in the industry. The PKI TC will simply provide pointers to these efforts.

2. The PKI Action Plan

The PKI TC recognizes that it cannot act independently in developing and 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. Without support from all these parties, this PKI Action Plan cannot be implemented.

The PKI TC will consult with all these parties and attempt to gather feedback and support for this plan before rollout (currently scheduled for February 2004).

Comments on this plan are most welcome. They may be sent to pki-comment@lists.oasis-open.org.

The PKI TC also recognizes that many of these actions should be undertaken not by the PKI TC, but by others. In that sense, this document is a Call to Action for the industry. It may be presumptuous for the TC to issue such a call, but the TC is only passing on the requests made by hundreds of PKI users and customers through its surveys. The TC will work with the relevant parties before announcing this plan so that the document can become a consensus plan with buy-in from all concerned.

All PKI stakeholders are invited to join the OASIS PKI TC and participate in our efforts to advance the successful use of digital certificates. Membership fees are quite low, especially for individuals and non-profit organizations. For more information, see <http://www.oasis-open.org/join>

2.1. Action Items

Name: Develop Application Guidelines for PKI Use

What: For the three most popular applications (Document Signing, Secure Email, and Electronic Commerce), develop specific guidelines that describe 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 members, Application Vendors, and Industry and Standards Groups

When: TBD

Name: Increase Testing to Improve Interoperability

What: 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. Branding and certification may also be desirable. If such efforts are already underway, the PKI TC will simply point them out.

Who: Industry and Standards Groups TBD

When: TBD

Name: Ask Application Vendors What They Need

What: 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 see if these needs (e.g. for quantified customer demand or good support libraries) can be met.

Who: PKI TC, in cooperation with application vendors TBD

When: TBD

Name: Provide Educational Materials on PKI

What: Explain in non-technical terms the benefits, value, ROI, and risk management effects of PKI. Also explain when PKI is appropriate (or not). Educational materials should unbiased and freely available to all. If these materials already exist, the PKI TC will simply point them out.

Who: PKI TC, in cooperation with others TBD

When: TBD

2.2. Next Steps

During October 2003, OASIS PKI TC members will contact as many PKI stakeholders as possible and ask them to review and comment on this draft Action Plan. The Action Plan will be revised in response to these comments and posted for an external review in November and December 2003. In January 2004, the PKI TC will prepare a final Action Plan and gather support for it. In February 2004, the Action Plan will be formally announced and work will begin on implementing it.

The PKI TC will conduct further surveys in future years to gauge progress on resolving obstacles to PKI deployment and usage. We expect that there should be measurable results within two years after initiating the PKI Action Plan.

If the PKI Action Plan is successful, it may be extended to include other items (such as application guidelines for other applications).