PKI Action Plan

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

Date: February 22, 2004

Version: 1.0

Table Of Contents

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 a number of barriers, including lack of applications, high costs, poor understanding of PKI, and interoperability problems have contributed to the limited use of PKI.

The OASIS Public Key Infrastructure Technical Committee (the PKI TC) is a group of PKI users, vendors, and experts with a common mission to address issues related to the successful deployment of digital certificates. 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. Two surveys on this topic were conducted. The survey results (summarized in section 2) clearly identified five primary obstacles to PKI deployment and usage and several recommendations for addressing those obstacles.

Based on the survey results, the PKI TC has developed this PKI Action Plan, which calls for a united effort to address the obstacles. Such an effort will bring reduced costs and greater security, benefiting all parties: PKI users and prospective users, software vendors, etc. However, it will require a united effort from all parties. The PKI TC can only play a coordinating or catalytic role.

Therefore, the OASIS PKI TC is asking PKI stakeholders (users, vendors, standards groups, and experts) to actively support this PKI Action Plan. We plan to announce the Action Plan in February 2004 and begin executing the plan at that time. The PKI TC believes that a serious effort by all parties to implement this plan will provide substantial improvements for all.

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 read 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 for PKI 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 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 in particular applications. 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 this PKI Action Plan based on them, on the experience of the PKI TC members, and on the many comments received on early drafts of this document.

For several of these action items, there are already efforts underway by others. The survey responses should serve to encourage these laudable efforts. The PKI TC will not attempt to duplicate these efforts but will instead provide pointers to them.

3. 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 intends to serve primarily as a catalyst or coordinator. 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 and by the many stakeholders who participated in the open review of the plan.

3.1. Action Items

Name: Develop Application Guidelines for PKI Use
What: For the three most popular 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

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. 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

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 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

Name: Gather and Supplement Educational Materials on PKI
What: 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.
Who: PKI TC Educational Subcommittee in cooperation with others
When: January – August 2004

Name: Explore Ways to Lower Costs
What: 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

3.2. Next Steps

In February 2004, this Action Plan will be formally announced. Then work will begin on implementing it. As mentioned above, this work effort will include many PKI stakeholders: customers, vendors, standards groups, experts, etc. If you would like to endorse the PKI Action Plan, join the PKI TC, or otherwise help this effort, please contact us at pki-tc-comment@lists.oasis-open.org.

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).

4. PKI Action Plan Supporters

4.1. Supporting Organizations and Individuals

The following organizations and individuals have endorsed the PKI Action Plan:

Organizations

Ascertia Limited
AssuredBytes Inc
Authora Inc.
Izecom BV
Paperless Chile
RSA Security Inc.
SETECS Corporation
Sun Microsystems, Inc.

Individuals (alphabetical by last name)

Sharon Boeyen, Entrust Inc.
Kefeng Chen, Ph.D. CISSP
Dr. Whitfield Diffie, Sun Fellow, Chief Security Officer, Sun Microsystems, Inc.
Joseph A. Doekbrijder, SwissSign AG
James Falkner, Enterprise Software Deployment Architect, Sun Microsystems, Inc.
Philip Fulchino, Director of Product Management, RSA Security, Inc.
Per Hagero, CISA, Principal Product Manager, PortWise AB
Stephen Hanna, Senior Staff Engineer, Sun Microsystems, Inc.
Jeremy Hilton CEng
Russ Housley, IETF Security Area Director, Founder of Vigil Security, LLC
Liaquat Khan, CTO, Ascertia Limited
June Leung
Lance Michalson, Michalsons Attorneys
Mr. Yasuo Miyakawa, Information-technology Promotion Agency, Japan
Dr. Sead Muftic, President/CEO, SETECS Corporation
Bakul Patel, VP Engineering, AssuredBytes Inc.
Dr. Radia Perlman, Distinguished Engineer, Sun Microsystems, Inc.
Jari Pirhonen, Information Security Manager & Security Consultant (CISSP, CISA),
  AtBusiness Communications Corp.
David Skyberg, Director of Engineering, RSA Security, Inc.
Ross Smith
Donald Teo
Pablo Vicuña Tupper, Paperless Chile, CDO Founder
Tia Walker, CEO, Authora Inc.
David L. Wasley, IT Infrastructure Planner, Univ. of Calif, Office of the President

4.2. OASIS PKI TC Members

Members of the OASIS PKI Technical Committee involved in developing the PKI Action Plan are:

Hemant Adarkar, Infosys
Paola Bassanese, U.K. Office of the e-Envoy
Sharon Boeyen, Entrust
Derek Brink, RSA Security, Inc.
Kefeng Chen, GeoTrust Inc.
Alex Deacon, VeriSign
Peter Doyle, Baltimore (now BeTrusted)
Paul Evans, Booz Allen Hamilton
Phil Fulchino, RSA Security
Andrew S. Gottfried, Lockheed Martin
Phil Griffin, Individual Member
Steve Hanna, Sun Microsystems, Inc.
Jeremy Hilton, Individual Member
Dr. Stephen Kent
Terry Leahy, Wells Fargo
June Leung, FundSERV
Mark Lundin, KPMG
John Messing, Individual Member
Tony Nadalin, IBM
Steve Orrin, Sanctum, Inc.
Jean Pawluk, Visa International
Virginia Roth, Novell
John Sabo, Computer Associates
David Skyberg, RSA Security, Inc.
Ross Smith, Government of Canada, Treasury Secretariat
Jeff Stapleton, KPMG
Ann Terwilliger, Visa International
Clifford Thompson, Individual Member
Krishna Yellepeddy, IBM