OASIS Mobilizes to Overcome Challenges to PKI Adoption

San Francisco, CA, USA; 23 February 2004 -- Members of the OASIS international standards consortium have published an Action Plan aimed at breaking down barriers to widespread adoption of Public Key Infrastructure (PKI) technology. Considered a foundational Internet security technology, PKI is used to authenticate people, secure commercial transactions, and protect the privacy of emails and telephone conversations.

"The industry's understanding of how digital certificates can be effectively used in e-business and e-government systems has greatly evolved from the early days of PKI," explained John Sabo of Computer Associates, co-chair of the OASIS PKI Technical Committee. "The Committee believes that the security benefits provided by PKI can become more widely available with our proposed plan for addressing the current obstacles to deployment. We believe that following through on this action plan, which incorporates input from PKI experts and adopters, can greatly benefit those implementing emerging Web and e-business standards."

The OASIS PKI Action Plan builds on the results of a series of surveys conducted by the OASIS PKI Technical Committee with IT staff who have deployed or attempted to deploy PKI. The surveys identified five primary obstacles to adoption: 1) poor or missing support in software applications, 2) high costs, 3) poor understanding of PKI among senior managers and end users, 4) interoperability problems, and 5) lack of focus on business needs.

The OASIS PKI Action Plan directly addresses these obstacles, calling for clear and specific guidelines for using PKI in the most relevant application types--document signing, secure email, and electronic commerce. The Plan also defines the need for interoperability testing, improved educational materials, best practices and other measures to reduce cost, and outreach to software application vendors.

"We're issuing an industry-wide Call-to-Action to increase use of a technology that is essential to achieve the level of security needed in today's world," said Steve Hanna of Sun Microsystems, CO-chair of the OASIS PKI Technical Committee. "The tactics spelled out in the OASIS PKI Action Plan are not difficult, but they do require the cooperative efforts of the entire community. That's why members of OASIS are calling on all PKI stakeholders--customers, vendors, standards groups, researchers and government--to join us in executing this Plan."

The OASIS PKI Action Plan is a work product of the OASIS PKI Technical Committee, whose members include Booz Allen Hamilton, Computer Associates, Entrust, FundSERV, IBM, KPMG LLP, RSA Security, Sun Microsystems, VISA International, Wells Fargo, and others. By working together to implement the Plan, the group believes that barriers to deployment can be measurably reduced and PKI usage increased.

Support for OASIS PKI Action Plan

Entrust
"As a public-key infrastructure pioneer, we have actively participated in the development of the OASIS PKI Technical Committee's Action Plan," said Sharon Boeyen, Principal Consultant with Entrust, Inc. "We fully support the goal of OASIS to increase awareness of PKI and foster the growth of Internet-scale federated identity management solutions based on the technology."

FundSERV
"Having been in the PKI arena for the past four years, FundSERV has experienced many of the obstacles identified by the survey. A clear and universal action plan like the one that has been defined by OASIS will be of immense benefit to the PKI community and help overcome barriers to adoption," said Amir Jafri, Vice President of Technology, FundSERV Inc.

Sun Microsystems
"Building public key infrastructure that realizes the promise of public key cryptography has proved more difficult than anyone imagined when Marty Hellman and I came up with the idea of public key systems in the 1970s," said Dr. Whitfield Diffie, Sun Fellow and Chief Security Officer of Sun Microsystems, Inc. "The OASIS PKI Action plan is an important step toward the eventual interoperability of all public key implementations. I am very pleased with Sun's contribution to OASIS and delighted with our endorsement of the Plan."

About OASIS

OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit, global consortium that drives the development, convergence, and adoption of e-business standards. Members themselves set the OASIS technical agenda, using a lightweight, open process expressly designed to promote industry consensus and unite disparate efforts. OASIS produces worldwide standards for security, Web services, conformance, business transactions, electronic publishing, topic maps and interoperability within and between marketplaces. Founded in 1993, OASIS has more than 2,500 participants representing over 600 organizations and individual members in 100 countries. [http://www.oasis-open.org](http://www.oasis-open.org) [1]

Additional information:

OASIS PKI Technical Committee

OASIS PKI Action Plan:

Press contact:
Carol Geyer
Director of Communications
OASIS
[carol.geyer@oasis-open.org](mailto:carol.geyer@oasis-open.org) [4]
+1.978.667.5115 x209