



OATH Delivers on 2006 Roadmap Early; Challenge/Response Internet-draft for Mutual Authentication Submitted to IETF

OATH Members Endorse Open Mutual Authentication

WASHINGTON CROSSING, PA, December 13, 2005 - The Initiative for Open AuTHentication (OATH), a consortium of leading authentication hardware and software companies, end user organizations and security professionals dedicated to advancing industry-backed standards for open authentication, today announced OATH members submitted a challenge/response internet-draft for mutual authentication to the Internet Engineering Task Force (IETF). The challenge/response internet-draft is a milestone on OATH's recently published 2006 technology roadmap released last month, and was completed ahead of schedule due to the cooperative efforts of OATH members Diversinet, PortWise and VeriSign.

The OATH-promoted algorithm is multi-faceted, built on values from a unique password, event trigger, static key, and challenge. This algorithm is then used to create one-time passwords and challenge-responses between two parties, such as a user and a website, resulting in mutual authentication. Mutual authentication goes beyond two-factor authentication, ensuring that both the user and the other party (e.g., website) are valid. The algorithm is based on a shared secret transformation using random numbers, digest, and hashing technologies. The challenge / response process requires that the server side send the client a “challenge” which the client uses along with the shared secret as the key in the transformation. The resulting number is called the “response” and is sent back to the server. Mutual authentication is especially effective for online banking and financial services applications as it offers a mechanism to demonstrate the authenticity of an institution's website as well as to validate the user, which guards against “phishing”. Mutual authentication is a key component of a multi-tiered security strategy to combat these threats and meet regulation guidelines. For more information, go to: <http://www.ietf.org/internet-drafts/draft-mraihi-mutual-oath-hotp-variants-00.txt>

“The OATH-promoted algorithm will help protect individual users from identity attacks that lead to transaction fraud, and adheres to new guidelines recently issued by the Federal Financial Institutions Examination Council (FFIEC),” said Stu Vaeth, Chief Security Officer, Diversinet and co-chair of the OATH Technical Focus Group. “The challenge/response algorithm is a natural addition to the initial HOTP algorithm released by OATH earlier this year, and will broaden the authentication choices available to customers.”

“Mutual authentication using the OATH-developed algorithm is a significant contribution to reducing the risk of online commerce,” said Kaushik Thakkar, vice president of business development, PortWise. “The 2006 OATH roadmap outlines a number of key developments and we will continue to provide resources for the delivery of these efforts.”

“Mutual Authentication is critical for today's on-line environment,” said Nico Popp, vice president, authentication, VeriSign Security Services. “The submission of this draft will drive better mutual authentication for financial institutions, customers and security providers.”

FFIEC recently released guidance to the financial services industry on risks and controls required to authenticate the identity of customers accessing Internet-based banking and financial services applications. The guidance reflects multiple legal, policy and technology issues to better protect customer information, guard against increased identity theft and fraud, and to reflect new authentication technologies available to provide risk mitigation strategies. The development of the new OATH algorithm for challenge/response addresses the mutual authentication guidance for online banking security from FFIEC.

Meeting this deliverable is further evidence of OATH's ability to drive industry-endorsed standards for royalty-free, open authentication technologies. OATH-compliant solutions are used to address security threats such as identity theft, phishing, internal security breaches and government compliance requiring a stronger level of authentication than usernames and static passwords. OATH's proven track record includes the development of the IETF HMAC OTP specification, adherence to Public Key Cryptography Standards (PKCS#11), and release of the OATH Reference Architecture.

About the Initiative for Open AuTHentication

The Initiative for Open AuTHentication (OATH) is the industry's leading collaboration of device, platform and application companies, and end user customers of authentication technologies. OATH participants hope to foster use of strong authentication across networks, devices and applications. OATH participants work collectively to facilitate standards and build a reference architecture for open authentication while evangelizing the benefits of strong interoperable authentication in a networked world. As OATH grows, the organization is actively seeking feedback and technology contributions from end-user participants who share a common vision for open authentication technology and the products that provide this important measure of security.

OATH is dedicated to helping customers reduce the cost and complexity of deploying strong authentication within enterprises, and across the Internet. Since its formation, OATH's membership includes security industry leaders from token manufacturers, platform vendors, smartcard providers, and security services companies. End user companies are joining OATH to add their voice and ideas towards the goal of open authentication.

Some current OATH members include: ActivIdentity, Inc.; Aladdin Knowledge Systems; AOL; ARM; Assa Abloy ITG; Authenex, Inc.; Aventail Corporation; Axalto; BMC Software; Checkpoint Software Technologies; Digital Persona; Diversinet Corp.; Entrust Technologies, Inc.; Forum Systems, Inc.; Gemplus Corp; IBM; IMCentric, Inc.; iovation, Inc.; IronKey; Juniper Networks, Inc.; K.K. Athena Smartcard Solutions; Livo Technologies SA; nCryptone; Passgo; Passlogix, Inc.; Phoenix Technologies Ltd.; PortWise, Inc.; Protocom Development Systems; RedCannon Security, Inc.; SafeNet, Inc.; SanDisk; Signify; Smart Card Alliance; TriCipher, Inc.; VASCO Data Security; Vocent; and VeriSign, Inc.

To learn how to participate, e-mail info@openauthentication.org or visit <http://www.openauthentication.org>.

All company and product names are trademarks of their respective holders

CONTACT:

Dan Chmielewski
Madison Alexander PR, Inc
949-231-2965
dchm@madisonalexanderpr.com

Joann Killeen
Madison Alexander PR, Inc.
310-476-6491
joannk@madisonalexanderpr.com