

# OATH Swears Authentication is the Next Big Thing

BY MARK WILLOUGHBY

Password authentication has long been seen by security experts as a chronic security weakness. At the recent Digital ID World conference, OATH announced submission of its HTOP one time password (OTP) algorithm to the IETF for standardization. But what, exactly, is OATH? And is its work likely to be significant step towards standardizing strong authentication, or just another effort by vendors to force a solution in their direction?

**T**he general lack of strong authentication is behind many of the problems seen on the Internet today. And in an era seeing billions being spent on heightened regulatory compliance, the identity community is beginning a bitter debate about marketplace trends that show huge increases in monthly phishing attacks and online fraud. Annual losses from identity theft are forecast to be in excess of \$40 billion next year. And massive



## OATH at a Glance

**Formation:** The Open Authentication Initiative (OATH, [www.openauthentication.org](http://www.openauthentication.org)) was announced in Feb. 2004 at the RSA Conference in San Francisco. VeriSign was the impetus behind its creation.

**Charter:** OATH aims to expand the market for strong, interoperable authentication by developing proposed industry standards that leverage existing technologies and standards bodies such as OASIS and the IETF.

**Membership:** Currently there is no cost to join OATH, although that may change as OATH develops a membership policy that includes different levels and participation. Currently OATH has 33 members of authentication stakeholders, mostly vendors with a small sample of academia and other industry bodies.

**Management:** OATH is directed by three committees that oversee decision-making, marketing and recruiting, and technology and standards proposals. A first draft of bylaws has been produced.

**Standards:** OATH's first standards proposal, submitted as a draft to the IETF in October, is HOTP, an algorithm for a Hashed Message Authentication Code (HMAC) One-Time Password (OTP). HOTP uses the SHA-1 hash function to create a secret key shared between a user device and validation server that synchronizes unique passwords for sequential use.

**Next:** OATH plans to expand membership, to develop standards proposals to flesh out the HOTP algorithm implementation and interoperation, and consider other authentication initiatives.

deployments of wireless devices supporting sensitive sessions and transactions compound the authentication problem.

Early in 2004, some security thinkers, correlating the industry trends, took matters into their own hands. They joined together and announced the Initiative for Open Authentication, better known as OATH ([www.openauthentication.org](http://www.openauthentication.org)), at the RSA Conference last February. Currently, OATH has 33 members, predominately from the vendor community, and claims its mission is to create a model for strong, interoperable authentication, to eliminate weak authentication as a barrier to e-commerce, and to grow the authentication marketplace.

### Controversy Arises

OATH's proposals will not become part of the industry fabric without debate. Standards wars have embroiled operating systems, networking, windowing systems, GUIs, RISC architectures, performance benchmarks, even the definition of a stan-

dard, the charters of their governing bodies, and the impartiality of their processes. Standards battles, however, serve a purpose. And when the dust settles, the result should be stronger standards.

Recently Dave Kearns, in his widely distributed electronic identity management newsletter, took issue with the formation of OATH, it's stated mission and impartiality, while questioning the first fruits of OATH's efforts to create some standards for interoperable authentication. Kearns ended by saying OATH "appears to be a stalking horse for VeriSign and that's not a bandwagon we should thoughtlessly jump on."

Fueling questions about OATH are the explosive growth forecasts for the global authentication marketplace. The Yankee Group predicts spending on authentication systems and tools will grow at a 12% annual rate from 2004-2008, nearly doubling from this year's \$1.4 billion to \$2.4 billion in 2008.

### Are Strong Authentication Standards Needed?

"Any group working to foster stronger authentication is good," said Gerry Gebel, an identity analyst with the Burton Group. He then added, "We've not heard a lot from OATH since its inception. For a standards group they're not being very forthcoming with who they are, how they're operating and what their intentions are."

Gebel believes stronger industry standards for authentication are unnecessary for federated identity networks, where "independent security domains are free to chose their own authentication policies and mechanisms. The idea that we need to address this with new standards is contrary to federated identity. Federated identity is not being stalled by token authentication or authentication issues," he said.

### Current Solutions are Expensive

OATH's proponents, however, claim all authentication, federated or not, will benefit. "A whole bunch of people in the security community have been saying that a big source of our security problems is static passwords," said Bob Blakley, an IBM chief scientist for security and privacy, and part of OATH's management team.

But fixing the weaknesses posed by static passwords today is expensive, Blakley said, which is why OATH's initial focus was to produce a standard for cost-effective one-time passwords (OTP.) Combining a static password, or "what you know" authentication method, with an OTP token, or "what you have" method greatly strengthens the probability that the user is valid. The leading OTP solution, RSA's SecureID, is costly and proprietary, Blakley said, and alternatives are needed to lower the cost of two-factor password authentication.

“The objective is to get rid of static passwords without having to add a lot of expensive infrastructure. We’re trying to get a solution to solve the one-time password problem in an open marketplace,” said Blakley. OATH’s first proposed standard, HOTP: An HMAC-based One Time Password Algorithm, was announced and submitted to the IETF at the Digital ID World conference in Denver on Oct. 26.

The underlying message behind the debate is twofold. The first is lingering animosity from VeriSign’s efforts earlier this year to re-direct misspelled URLs to a VeriSign Web site. VeriSign was deluged with a landslide of negative reaction from a multitude of Web users and subsequently reversed course, abandoning a policy widely viewed as a self-inflicted PR debacle.

In addition, OATH’s proposal to create stronger, open authentication with OTPs has strategic implications for RSA. Its SecureID one-time password products have achieved market dominance for two-factor token authentication. RSA reported \$192.8 million in sales of “authenticator product types”, comprising 74% of RSA’s \$260 million in 2003 revenues and a big proportion of its profits.

## OATH Sparks Questions

In his Dec. 6, 2004 newsletter entitled “Digging Deeper Into OATH Doesn’t Look so Good,” Dave Kearns questioned:

- 1. OATH’s** legitimacy, since Sun, Novell, Microsoft, and RSA are not members.
- 2. OATH’s** ability to create lower cost authentication without the participation of RSA.
- 3. OATH’s** claim to creating open standards, as opposed to existing standards from groups such as OASIS and its SAML standard, Liberty, WS-F, etc.
- 4. OATH’s** independence, citing licensing agreements that use VeriSign legal boilerplate.
- 5. The impartiality and veracity of OATH’s** first proposal for an authentication standard, saying OATH’s HMAC OTP proposal was authored by VeriSign employees exclusively.

Understanding the real value of OATH’s vision and the usefulness of its proposed standard requires a detailed examination of the facts.

### OATH’s Membership

OATH membership at this early stage, less than a year after its formation, is small. Mature and successful standards bodies typically number more than 100 members after a couple of years and the strongest have a good cross-section of vendors, users, academia and government. In addition to VeriSign and IBM, OATH’s membership includes Aladdin Knowledge Systems, ActivCard, Gemplus, VASCO, Aventail, BMC, Check Point, Entrust, Juniper Networks, Passlogix, Smart Card Alliance, Assa Abloy ITG, the Smart Card Alliance among others.

Currently, OATH’s membership currently is heavily tilted towards vendors. In his newsletter, Kearns cited the non-membership of Sun, Microsoft, Novell and RSA as an indicator of their lack of support. RSA has a standing invitation from OATH to join, and they cite OATH’s lack of user participation as a key reason they are sitting on the fence.

“RSA believes it’s best to be involved with standards bodies that include the customer’s voice,” said Brian Breton, a senior product

marketing manager at RSA. RSA is active in other standards bodies that count customers as members, Breton said, citing the Liberty Alliance, OASIS and the IEEE. “RSA has been evaluating the OATH consortium since its initiation. We’re continuing to evaluate the OATH initiative and to date we have not decided to join,” he said.

According to Darran Rolls, director of identity technology at Sun, “Sun is 100% in support of the goals and objectives of OATH. We chose to not directly participate in the progression of the standard primarily because of resource constraints and because they’re doing a good job.” Sun contributes to many initiatives, Rolls added, and “due to our strong participation in the Liberty Alliance, and how authentication interacts with the Liberty specification, we should focus our efforts on how the OATH effort interacts with Liberty.” Rolls said he expects to facilitate interaction between both Sun and the Liberty Alliance with OATH.

Novell, through a PR Spokesperson, simply said, “we don’t really have much to comment on regarding OATH. We are not participants, but we are always evaluating our involvement with different initiatives and standards bodies.”

Microsoft, through a PR spokesperson, declined to comment.

## OATH's Organization

OATH has organized into three permanent committees to advance their agenda. These three committees and their missions are:

- The Joint Coordination committee, headed by IBM's Bob Blakely, to coordinate management and decision-making
- The Marketing committee, directed by Stephen Axel of Aladdin Knowledge Systems, to promote OATH and stronger authentication
- The Technical committee, coordinated by Siddharth Bajaj of VeriSign, tasked with developing standards recommendations and coordinating with other standards bodies

OATH's membership will grow, according to Stephen Axel, the head of OATH's marketing committee. "OATH is in its infancy," Axel said. "We are building the strong authentication ecosystem now – the platform providers, device and service

providers. As we expand we absolutely will be adding users as members" as they attempt to broaden the family authentication standards beyond PKI, 802.1x and the various flavors of EAP (Extensible Authentication Protocols.)

Another priority, Axel said, is to create more OATH-specific infrastructure and to migrate away from the contract boilerplate and business infrastructure donated by VeriSign. Ultimately, OATH may even have professional management, depending on how the scope of work matures.

### Under the Hood – OATH's HOTP Standard Proposal

OATH does not consider itself to be an organization that creates industry standards, according to IBM's Bob Blakely. "There's already enough standards organizations – W3C, OASIS, IETF – around in the industry to get the work of standardization done. We felt we needed a community of interest to get people

together to agree on the problem and craft a solution," Blakely said.

OATH's members would then "put their weight behind it for entry into the standards effort" with the most appropriate existing standards body. "We designed the OATH organizational structure to be lightweight so that the technical work wouldn't get done in OATH, so that OATH wouldn't compete with standards bodies. The existing standards orgs are capable of taking any technical work forward," Blakely said.

The OATH HOTP standard (see sidebar, OATH's HOTP Process) was jointly authored by five members of the technical committee ([www.ietf.org/internet-drafts/draft-mraihi-oath-hmac-otp-01.txt](http://www.ietf.org/internet-drafts/draft-mraihi-oath-hmac-otp-01.txt)). VeriSign employs only one of the five authors.

"It's not dominated by any one company. There's a lot of active participants," said

Stu Vaeth, the CSO at Diversinet and the chair of OATH's technical committee. "VeriSign does not promote their agenda. We've been very pleased at how its been handled. Federated identities rely on authentication," Vaeth said. "If you can't trust your authentication there's no point in exchanging identities."

The benefits of OATH's HOTP proposed standard mirror those of any strong, two-factor authentication. A sequence OTP is also easier to deploy and manage, Vaeth said. It is deployed once with a one-time distribution of the secret key. The distribution of the secret key is not part of the initial proposal for a HOTP algorithm, but it should be made via a secure medium, Vaeth said.

HOTP requires no updating of keys and access to the secret keys stored on devices would likely be protected by a static password, Vaeth said, another implementation detail being considered for a future standard.

The HOTP proposal has two primary vulnerabilities. The first is the exposure to man-in-the-middle attacks shared by all sequence-based algorithms, if not properly implemented over secure channels. The second vulnerability is shared by all symmetric (secret) key systems, the compromise of the shared secret.

IBM's Blakley said it should take approximately 18 months for OATH's HOTP standard to emerge from the IETF. Meanwhile, OATH is busy planning its next standards proposal but "we have not yet agreed which one or two issues will be the next focus of activity" with contenders being an architecture for strong authentication and filling in

## How OATH's HOTP Works

**1. Generation of the shared secret:** For each OTP (One Time Password) generator (token) in the system, a unique 160-bit shared secret is generated and stored securely on the OTP validation server. Each unique secret is associated with a unique token ID at the validation server. The secret is to be shared only between the OTP validation server and the client token and it is used as the cryptographic input to generate a keyed hash for message authentication (HMAC) on which the HOTP algorithm is based.

**2. Secure provisioning of the secret:** The secret key is stored on the validation server and securely provisioned to the client token. The token can take many physical forms: a soft token on a PC or mobile device, a USB dongle, GSM SIM card, Java smart card, etc. The initial OATH HOTP algorithm specification does not address secret key provisioning, the details of which are planned for a future OATH specification.

**3. OTP generation:** The OATH HOTP algorithm uses a counter based on the HMAC-SHA-1 cryptographic standard. The client token generates a 20-byte HMAC-SHA-1 value based on the secret key and a unique counter value. The secret key is static while the counter value increments each time an OTP is needed. The 20-byte HMAC value is truncated to a minimum of six digits for the OTP value displayed on the token.

**4. OTP submission for remote access:** In a typical remote access scenario using 2-factor authentication, the user is prompted for both a static password and the dynamic OTP password via a login prompt. The user enters their static password followed by the OTP value displayed on their token. Both values are submitted over the network via an authentication protocol such as Radius, preferably over a secure channel, to an application server such as a VPN gateway or Web server.

**5. OTP validation:** The application server sends the user's OTP value to the validation server that matches the token ID for that user, computes its own HOTP value based on the stored secret key and the current counter value, and compares this value to the OTP submitted by the client. The result is passed back to the application server, which makes an access decision based on a combination of the static password and the OTP.

the blanks for managing and implementing HOTP.

### OATH in the Marketplace

Adam Smith would say that both OATH's detractors and its supporters have an economic stake in its future. In the inexorable march of technology, standardization invariably leads to wider adoption and usage in a more mature information infrastructure. If OATH is successful in creating new authentication standards, strong authentication becomes more widely adopted, distribution broadens and the infrastructure grows faster. This is the key objective of OATH's founders.

Vendors shipping OATH HOTP products plan to accelerate the growth in stronger authentication as they compete

with existing authentication methods and vendors. Competition invariably leads to better services and drives down costs. The increased competition promised by the OATH HOTP standard threatens the business models and profit margins enjoyed by vendors of proprietary authentication products.

Regardless of which side you find yourself in the OATH standards war, the constant rate of change in the technology marketplace is one of the few types of change that frequently escapes the law of unintended consequences. Odds are, with more choice, you're going to see lower prices for authentication services. ■

Mark Willoughby is a contributing writer to Digital ID World.