oath

initiative for open authentication

OATH FAQ

February 20, 2004

1. What is OATH?

Due to identify theft, proliferation of IP devices and myriad of other trends in digital identity management the need for ubiquitous strong authentication is clear. Open Authentication Reference Architecture (OATH) is a revolutionary new approach to driving the adoption of strong authentication technology across all networks. Based primarily on existing standards, OATH will ensure that secure credentials can be provisioned and verified by disparate software and hardware platforms, removing traditional barriers to widespread adoption and ultimately giving enterprise IT managers better control over their security environment.

OATH outlines a reference architecture for strong authentication with the following objectives:

- Propagate specifications for any vendor to manufacture an open, low cost multi-factor authentication device combining the most prevalent authentication methods (OTP, PKI, SIM)
- Enable strong authentication in enterprise applications, application servers and middleware with minimal effort for software developers and integrators
- Enable best-of-breed solutions through interoperable components that leverage existing standards and existing IT infrastructure
- Drive down the cost of physical tokens

The end goal is to make strong authentication available for users across all networks and devices.

2. Why is this important?

OATH’s importance is in the breath and approach to the reference architecture proposed:

- OATH proposes a model of Open Strong Authentication based primarily on existing standards that ensure secure credentials can be provisioned and verified by disparate software and hardware platforms.
- OATH will help drive strong authentication deep into the network fabric making deployment of strong authentication possible for large user populations in a variety of scenarios
- OATH is the only collaborative industry effort focused on expanding market opportunities all stakeholders – Device Manufacturers, Software Vendors and Service Providers

3. What is the situation today and how is it different from the environment OATH proposes?

User-ID and Password

Today, user-ID and password is the predominant method of user authentication. This is highly prone to hacking, and there is always a risk of someone stealing the information.

Online identities secured only by static passwords can be exploited, resulting in identity theft or compromised systems. Existing two-factor authentication approaches, while more effective, are often expensive and complex, and their lack of interoperability poses significant barriers to adoption.

In the 2002 FTC annual study on consumer complaints, identity theft for the third year running has been the most frequently cited reason why individuals contact consumer protection authorities. As most mainstream consumer services, such as banking, health care, and insurance, complete their migration to the network, these incidences will only increase.

The fundamental security mechanism to protect our personal information online remains fairly unsophisticated. An average person has more than a dozen passwords, which Hackers using dictionary programs and social engineering can crack without too much effort.

An industry-wide collaborative effort to promote Open Strong Authentication will remove these barriers and broaden enterprises' use of the Internet to communicate, collaborate, and conduct commerce in new ways.

Proprietary authentication methods

Some of the enterprises have made investment in OTP tokens that are based on a proprietary architecture. The operational cost of managing a proprietary infrastructure is significantly high and the customer is typically stuck with only one vendor. Inability to scale and interoperate, a proprietary infrastructure limits an organizations chances to leverage online commerce and business partner integration opportunities to gain a competitive edge.

In addition, end user is required to carry multiple devices for network access, facilities door access, name and password for corporate applications. The process to manage and provision these disparate authentication methods is very expensive, time consuming, and often prone to errors (think of all the access rights that need to be revoked when an employee leaves a firm).

OATH BASED STRONG AUTHENTICATION

Open standards for OTP generation, credential provisioning and validation will bring down the cost and complexity of strong authentication solutions. The open reference architecture provides a common framework for strongly authenticating people and devices across all networks.

The OATH reference architecture provides customers with vendor choice and flexibility to deploy different form factors based on user requirements (USB tokens, Smart Card, mobile devices). At same time enterprises can choose the right authentication method based on the security requirements – OTP, PKI, or SIM using a low cost hybrid token.

4. What are the key objectives of the OATH reference architecture?

The ultimate goal of the OATH is to provide a reference architecture to deliver strong authentication to build an open community where all people and all devices are strongly authenticated, while providing for interoperability and the possibility of federated identities.

The following lists some of the key objectives for the open blueprint.

- Proliferate low cost multi-function authentication devices (e.g. tokens, smart cards)
- Transform today's mobile devices into strong authentication devices (e.g. cell phones, PDAs, laptops)
- Propagate device credentials, strong authentication algorithms, and authentication client software across many network end-points (desktop computers, servers, switches, Wi-FI access points, set top boxes…)
- Build native support for strong device and user authentication in application development and identity management platforms (platform connectors)
- Increase the breadth of packaged applications that supports strong authentication (ERP, MRP, CRM application connectors)
- Enable best of breed solutions through interoperable components

To be effective, the reference architecture will be is jointly defined and published by key industry partners that share the vision of universal strong authentication. OATH lays the necessary ground for ubiquity, integration and interoperability. The resulting specification will decrease the risk and complexity of deploying strong authentication within an Enterprise or for an entire Internet community.

5. Who is leading this effort?

The OATH reference architecture is driven and endorsed by industry leaders like IBM, Axalto, Gemplus, and VeriSign. There are several vendors who have already started manufacturing tokens based on existing open standards referenced in the OATH roadmap white paper (for more information see www.openauthentication.org).

The founding members of OATH will be publishing the initial draft of the specifications for a broader review and adoption by Q3 2004.

6. Is it a paper vision or there is something that I can use today?

Products and services based on OATH will be shipping in the 2004 calendar year. Several prototypes devices and services are already in the process of field testing at selected customer sites. Early feedback is extremely positive and customer trails will be expanded throughout the year.

7. What is the nature of OATH organization – Consortium?

OATH is an initiative of key industry players who share a common goal and vision. OATH is not a new standards body, rather, OATH is an accelerator for change in the authentication market that will work with existing organizations to propagate new approaches for interoperability and open specifications for strong authentication where none exist.

8. What is the objective of the OATH founders?

The primary objectives are:

- Co-author an open specification for adoption by manufacturers of tokens, Smart Cards and mobile devices.
- Allow application developers to build necessary connectors for integration of strong authentication features as outlined in the OATH roadmap white paper.
- Work with various industry forums for adoption of an open authentication methods that will allow freedom of choice and lower costs for the enterprise customers.

9. Who can join the working group? How can I participate?

Currently, the specifications are being co-authored by founding members. The number of participants will be expanded throughout the calendar year. Vendors can currently join as a participating member, and receive periodic updates on the status of the specifications.

10. What are the benefits for joining this group?

Participating members will have the following benefits:

- Monthly status calls on the specifications
- Opportunity to submit recommendations to the founding members
- Access to test environments and certification guidelines

11. If I develop products based on the OATH, do I have to pay any royalty?

There is no royalty to any individual or organization building products based on OATH.

The primary goal is to propagate strong authentication based on the OATH reference architecture and specification as broadly as possible.

12. Can I certify my products for OATH compliance?

Yes. OATH will hold its first general meeting in Q2 2004. More information on specifications, testing and compliance will be available at that time.

13. Where can I find more information on OATH?

You can visit the following URLs to download the white-paper on the OATH: www.openauthentication.org