OATH :

An Initiative for Open AuTHentication
Who Are You Really Doing Business With?

"On the Internet, nobody knows you’re a dog."

The New York Magazine, July 5, 1993, Peter Steiner,
The Economic Promise of e-Business

Worldwide B2B eCommerce will reach $2.37 trillion in 2004 (eMarketer, 2003)


All resting on the trust of a simple password
So what is the big problem?

- Online Identity Theft
- YOU are online
  - You bank
  - Your Mortgage
  - Your Stocks
  - Your shopping
  - Your Tax Return
  - Etc…
- THEY are everywhere
  - Multi points of attack
  - Threat Network-effect
An Industry Wake-Up Call

- Static passwords are everywhere!
- Strong authentication -- the foundation for a trusted network/ eBusiness -- remains too expensive and complex for most businesses to deploy.
What is OATH?

The Open Authentication Reference Architecture (OATH) initiative is a group of companies working together to help drive the adoption of open strong authentication technology across all networks.
OATH: Mission

- Expand secure and safe on-line transactions for consumers and business users with strong, 2-factor authentication
- Leverage existing standards and create an open reference architecture for strong authentication which users and service providers can rely upon, and leverage to interoperate
- Reduce the cost and complexity of adopting strong authentication solutions
OATH = Strongly Authenticate Everyone, Everything, Everywhere

Increasing network interactions across all users types

All Users
- Employees
- Business partners
- Customers

All Networks
- Enterprise LAN
- Extranet
- Public Internet

All Devices
- Desktops
- Mobile Devices
- Servers
- P2P

Federated Identity

Proliferation of IP Devices & Web Services
1. Can we create cost-effective & user-friendly authentication devices?

- **High volume chipset**
  - SIM, eventually TPM…
  - Common OTP standard seems attractive to these folks

- **Increased flexibility**
  - Universal Key Concept
  - Multiple Methods on single device
    - OTP, PKI & SIM as base methods
  - Multiple credentials on single device
    - More tricky, but that is the grail!

- **Embedded in mobile and network devices**
  - Look! No token
  - Integral part of our Web-life style
  - In phones (SIM)
  - In PCs (SIM & TPM chips)
2. Can we minimize software infrastructure costs and make deployment easier?

- **Leverages existing infrastructure components**
  - Directory as “center of command”
  - Provisioning & SSO Servers
  - RADIUS Servers

- **Make architecture fit access Mgt strategy**
  1. Consolidate access management
  2. Strengthen credentials
  3. Federate authentication

- **Reuse established standards**
  - LDAP (user store consolidation)
  - Network app: 802.1x (EAP-TLS/PEAP/SIM)
  - Biz Apps: WS-something (more candidates here: WS-Trust, SASL SPML, XKMS)
3. Can we spread the use of these strong credentials across more apps and networks?

- **Federated identity to the rescue!**
  - **User - convenience:** won’t carry a security device unless it works everywhere
  - **IDP - facilitate integration & propagation:** want to integrate my strong credential beyond my internal systems, across my external service providers
  - **SP - decrease liability & cost:** I will accept someone’s else credentials unless they are more secure, especially if I did not have to pay for the hardware

- **Towards Federated hardware?**
  - Theory: easier to share anonymous and costly token that helps everyone’s security than actual user identity
  - Less contractual, liability, privacy issues
  - OATH token + Liberty Standards
Filling the standard gaps: OATH Roadmap

Auth Methods:
• OTP standard

Auth Framework:
Pluggable strong authentication modules architecture

Secret Provisioning Validation and provisioning Protocols:
EAP-OTP
WS- *

2004

2005

A humble beginning!
OATH Ecosystem
OATH Partners
Summary: OATH in a nutshell

Fundamental shift from proprietary to open solutions

- An industry-wide problem mandates an industry wide solution
  Two-Factor Authentication to stop identity theft across all the networks

- A reference architecture based on open standards will drive global deployment across
  1. Security and mobile devices (algorithms/agents)
  2. Network and business applications (connectors)
  3. Middleware (app servers, provisioning & SSO servers, directory schemas)

- Minimal bureaucracy to get the work done!
Thank You!

Info@openauthentication.org