oath
initiative for open authentication

OATH: Initiative for Open AuTHentication

Siddharth Bajaj
VeriSign

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,

oath
initiative for open authentication

Static Passwords are bad...

Everyone complains about the weather,
but no one does anything.

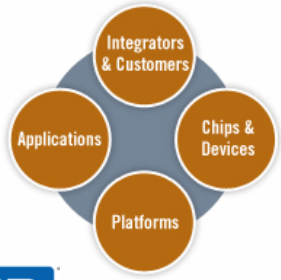
What is OATH?

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 Membership (80+)



Coordinating

Actividentity
Diversinet
Entrust
gemalto
security to be free
HID
IBM Tivoli
InCard Technologies
InfoSERVER
N-CRYPT
SanDisk
UPEK
VeriSign

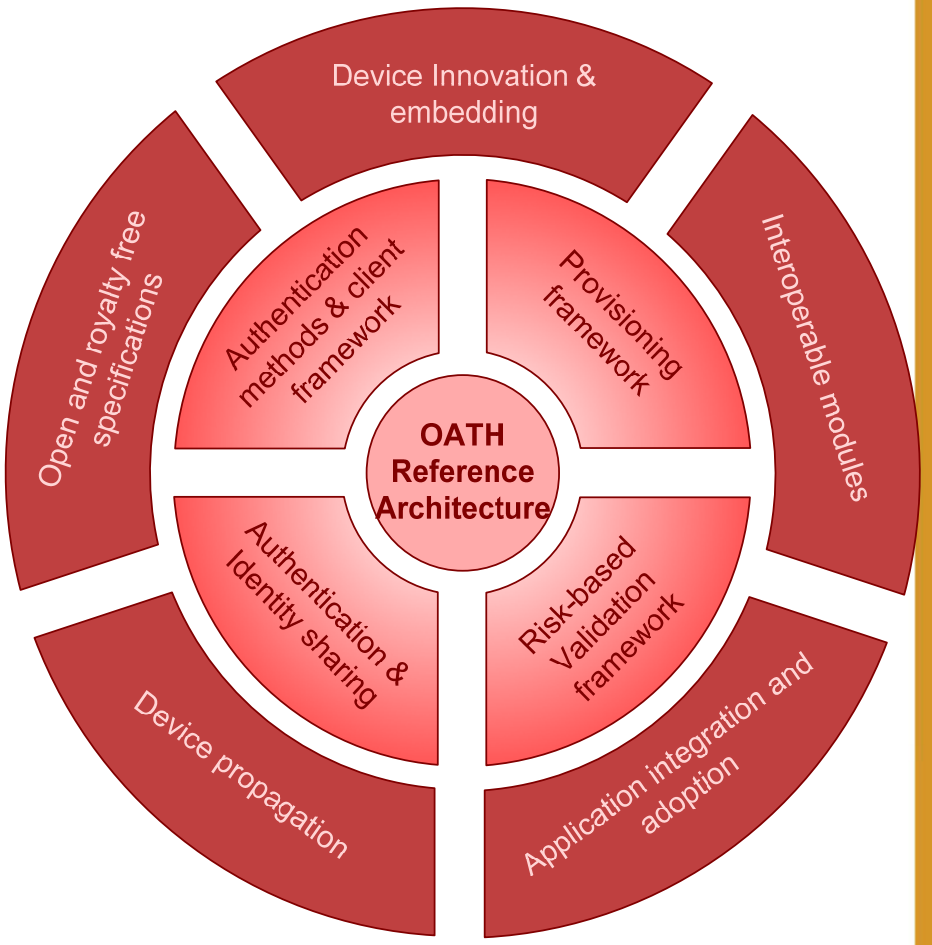
Contributing

Aladdin
ANX eBusiness
aradiom the phone reborn
Authenex
BIO-key INTERNATIONAL
BR TOKEN
Clareity Security
COMARCH INFORMATION TECHNOLOGY
CRYPTOMATHIC
DNP Dai Nippon Printing
DEEPNET SECURITY
DIVERSID AUTENTICACIÓN
DynamiCode Revolution for Your eAccess
FEITIAN WE BUILD SECURITY
fireID
Giesecke & Devrient
hp invent
i-sprint
IRONKEY
iretn
IdentiTa
KONICA MINOLTA
mobilEGOV THE DIGITAL DNA
movilok FOCUSED ON MOBILE INNOVATION
MXI SECURITY
nordic edge
PointSharp
nagraID SECURITY
PortWise
symwave
SmartDisplayer
THALES e-SECURITY
SALT GROUP
TOPPAN FORMS

oath initiative for open authentication

OATH Reference Architecture:
Establishes the 'common ground'

- **Sets the technical vision for OATH**
- **4 guiding principles**
  - Open and royalty-free specifications
  - Device Innovation & embedding
  - Native Platform support
  - Interoperable modules
- **v2.0 published in 2007**
  - Risk based authentication
  - Authentication and Identity Sharing



oath initiative for open authentication

Standardized Authentication Algorithms

-Open and royalty free specifications

-Proven security: reviewed by industry experts

-Choice: one size does not fit all

HOTP

-**Event-based OTP**

-Based on HMAC, SHA-1

-IETF RFC 4226

-Dec 2005

OCRA

-Based on HOTP

-**Challenge-response authentication**

-**Short digital signatures**

-8th draft, expected RFC 2009

TOTP

-**Time-based HOTP**

-2nd draft submitted to IETF

oath initiative for open authentication

OATH Adoption

50+ shipping products

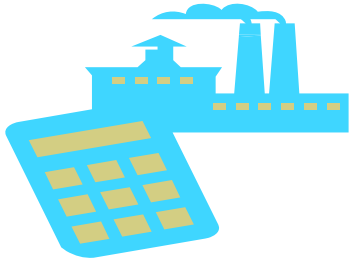
oath initiative for open authentication

Q11

Credential Provisioning

Token manufacturer offline model

- Portable Symmetric Key Container standard format (PSKC Internet-Draft)



Dynamic real-time model

- Dynamic Symmetric Key Provisioning Protocol (DSKPP Internet-Draft)
- OTA provisioning to mobile devices, or online to PC/USB

IETF KeyProv WG

- working toward RFC submissions

IETF

initiative for open authentication

Q5

OATH Progression

CHOICE of AUTHENTICATION METHODS

- HOTP ☑
- OCRA ☑
- TOTP ☑

2006-08

CREDENTIAL PROVISIONING & LIFECYCLE

- PSKC ☑
- DSKPP ☑

2007-08

APPLICATION INTEGRATION & ADOPTION

- Certification program
- WS Validation
- Auth & Identity Sharing work

2008+

oath
initiative for open authentication

OATH Authentication Sharing Models

Enables sharing of 2nd factor credential across sites – force multipliers!

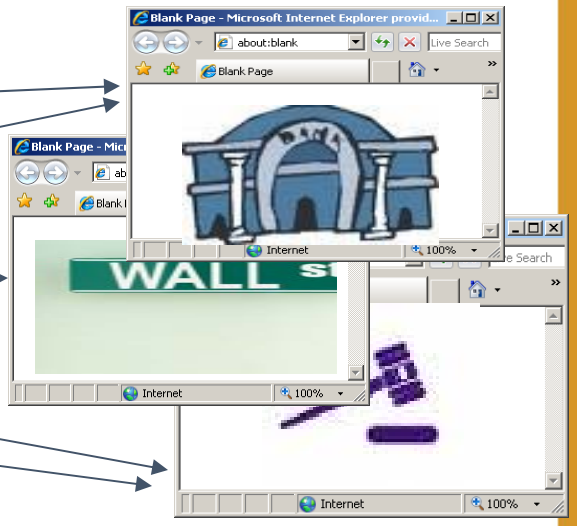
"Token Necklace" Dilemma

Sh
Ano
2nd

	A	B	C	D	E	F	G	H	I	J
1	1	7	3	9	3	4	5	5	4	9
2	9	2	5	3	6	2	8	4	1	3
3	4	6	9	1	4	6	2	8	0	7
4	1	5	2	4	8	5	0	1	7	2
5	6	8	6	8	1	7	4	0	8	0

OATH Token
ng Models

ralized
n Service
el
. Distributed Validation Model
3. Credential Wallet

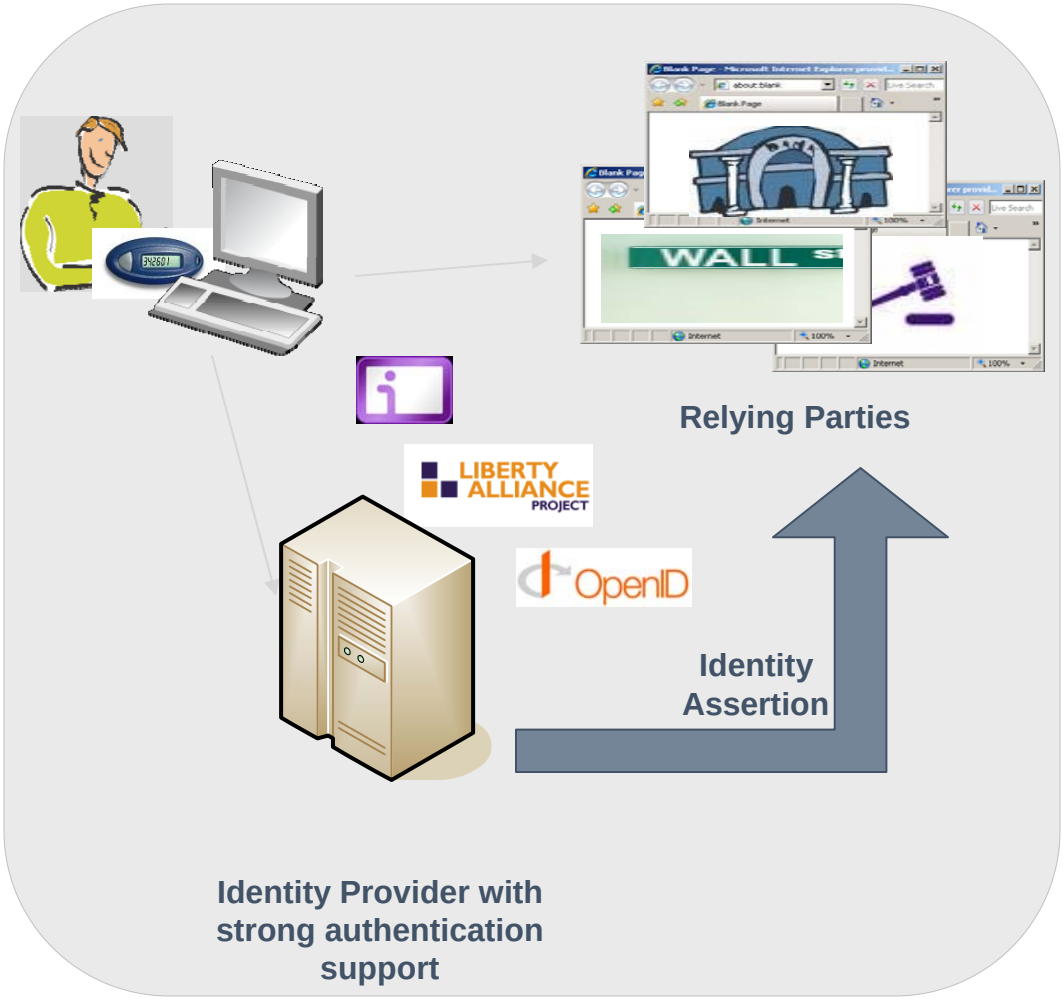


Online Bank, auction, brokerage, e-commerce sites, etc.

Simpler liability models…

oath
initiative for open authentication

Identity Federation & OATH



- **Identity is federated/shared across multiple sites**
  - Traditional federation (Liberty)
  - User-centric models (OpenID, CardSpace)
- **Single Identity becomes more valuable**
  - Needs to protected using strong authentication

Enable OATH credentials as first class citizens with these technologies!

oath
initiative for open authentication

Moving Toward More Pervasive Strong Auth

Lower barrier to adoption!

- **User Convenience**
  - Leverage devices users already carry today
  - Shared Credential
- **Lower TCO**
  - Interoperable multi-vendor solutions
  - Leverage existing devices
- **Reduce Time to Implement**
  - Online/OTA provisioning
  - Easier to integrate - standard web services and protocols

oath initiative for open authentication

Q10

OATH: *Driving a fundamental shift from proprietary to open solutions!*

- Open & Royalty free specifications
- User friendly form factors
- Embedding in existing devices

Device Innovation

Lower Cost

- One size does not fit all – risk based authentication
- Cost effective devices
- No vendor lock-in

- Interoperable standards enable enterprises to deploy components from multiple vendors in a single deployment
- Proven security!

Best of Breed Deployments

Device Portability

- Authentication & Identity Sharing models enable use of single device across multiple application and networks

Visit www.openauthentication.org

oath
initiative for open authentication

Questions & Answers

Thank You!

initiative for open authentication

Get Involved!

- **Visit the OATH website**
  - Download Reference Architecture v2
  - Download and review draft specifications
- **Engage - contribute ideas, suggestions**
  - Review public draft specifications
  - Get involved in developing specifications
- **Become a member!**
  - 3 levels - Coordinating, Contributing, Adopting
  - Join the TFG mailing list

References and Resources

- Initiative for Open AuTHentication (OATH)
  - http://www.openauthentication.org
- HOTP: An HMAC-Based One-Time Password Algorithm – RFC 4226
  - http://www.ietf.org/rfc/rfc4226.txt
- OATH Reference Architecture
  - http://www.openauthentication.org
- Other draft specifications
  - http://www.openauthentication.org