

Minutes of The OpenID Summit "Balancing Security and the User Experience"



Held at Symantec Headquarters on May 2, 2011

Meeting called to order by Don Thibeau at 12:15 pm with approximately 150 in attendance. Don thanks both meeting sponsors – Symantec and Google. Gives brief overview presentation (Appendix A)

Session One Panel Discussion: "Whither Secure Identity?"

Nico Popp of Symantec moderated a CTO roundtable discussion with Paul Agbabian CTO Norton, Brent Williams CTO Equifax, Tim Brown SVP Distinguished Engineer CA Technologies.

Nico, strong identification, good, bad and ugly

Education

What forms of authentication, enterprise – web with scalability, Nico et al.

Transactions – range from low value social to high value/backing assurance

PAUL: Most consumers want email only

Billing profile – relationships with others, who owns data and sharing policy, authenticating entity?

BRENT: Start high – Level 3 – going low easy. Low – High upgrade – difficult process

PAUL: Contradiction between sales and customer acquisition vs. security

BRENT: Some industries – health care, government, etc. Plus companies that need the data will set the bar higher.

TIM: Costs associated with security. Has to have value. Business model.

NICO: Identity proofing before issued strong identity.

BRENT: The identity to file sublime to ridiculous. Associations and assertions. Context of identity proofing. Drps, taxes, etc. Knowledge.

PAUL: All don't care absolutely. Consistency.

TIM: One click – Amazon believes risk < reward.

NICO: One time password?

TIM: Others are easily crackable, patterns on user id and social networking. Carrying a token doesn't work.

PAUL: Don't imply multi-factor identification. Originally attending for grouping.

NICO: Change gone or mobile?

PAUL: Mobile stronger security vs. PC and Mac

BRENT: Two types of OTP – Separate device vs. sure device – (pain in the derriere). Another layer on device. Some markets need two factor identification. Some places absolutely justified- Health care and government – Level 3 > a radical

NICO: Smartcard – PKI

TIM: Not a failure. Govt., yes – consumer – no.

PAUL: Mobile may change.

BRENT: PKI is not identification. Only an authentication comparable to SAML.

TIM: Incocard didn't fail based on technology. Consumer behaviorist. Business model. All about the money.

MIKE JONES: (Microsoft) Has to work for user.

PAUL: User experience must work always. Not just 9/10

BRENT: Risk based authentication experience. Mandated issues different – HIPPA
Benefit consumer: Adoption is very high, What's in it for me? Regulatory driver.

NICO: Risk-based authentication – Banks, Cookie, IP address

TIM: Cheapest and works – Log and audit log, new market Risk-based analysis, location, machine identifier, context (money in vs. money out)

BRENT: Will always look to Fraudsters, overcome RBI – look at risk spectrum

PAUL: Imperfect solution, right thing at the time. Not a good long term solution.

TIM: Government will make you re-login every six months. All workflow based.

NICO: Business model. Who is going to pay?

TIM: Trans global secure, collaboration and verification. Segmented communication on large projects. Consortiums of hospitals, loyalty programs. Business models work in these environments

PAUL: If you have a need to do, you pay as a company. Does security improve your sales? Symantec – highest perceived risk to consumers is identity theft vs. viruses.

BRENT: Questions for audience: New ways of doing multi factor authentication. Biometrics with ability to rescind.

Session Two Presentation: "What's Up with OpenID?"

Mike Jones of Microsoft and OpenID Foundation, Nat Sakimura, Chairman OpenID Foundation, and AB/Connect Working Group Co-chairs will update the collaboration of Facebook, Google, Microsoft and others on the next stage of evolution of the OpenID protocol.

Presentation: Mike, Nat, John. Attached as APPENDIX B

Revisions to open ID specs. SAML hasn't taken world by storm. FICAM Federal Intra Credential Access Mgmt. Spec work on open ID available on website.

QUESTIONS:

Eric Sachs: Open ID 2.0 – valid

Paul: yes and available – graceful transition and backward compatibility.

Audience: How to become a relying party

PAUL: You can drop JavaScript in your page. Identity provides: A function of risk-based analysis, A cost to identity provider

Audience: Why do we care about high assurance authentication? Why not focus on Level 1?

PAUL: Designing a security protocol with the ability to scale up and down is good.

Audience: Why Open ID?

PAUL: 1) No need to be identity provider 2) May break mobile apps.

Question: Interoperability – Initial registration – then API, data exchange, etc.

PAUL: 1) Dynamic client registration like OAUTH 2) API well defined for getting information of user.

Question: XML vs. JSON

JSON rich data representation – delegation and permissioning provides business capabilities

Session Three Panel Discussion: "The Latest in IdP and RP Best Practices"

Eric Sachs of Google will moderated a roundtable on identity provider and relying party best practices in online identity authentication with
Andy Wu of Yahoo!,
Dave Hebert Microsoft,
George Fletcher Aol, and
Chuck Mortimore, Salesforce.com

Question: What is primary info?

GEORGE: Email address – critical component relying parties.

ANDY : Email #1 attribute. Names – used as greeting. Photo URL

CHUCK: Aesthetic of protocol (user is in charge). Changing adoption of dynamic trust. Redirecting to different site didn't work. User experience and work flow.

How to use SAML vs. Open ID

GEORGE: Fixed federation model. Rich desktop apps. Otherwise all open ID

Is Open ID 100% reliable? Global vs. Pseudonyms?

ERIC: Google supports but doesn't see much usage.

Question: Global signout

GEORGE: Glad to see Open ID implementing. Less use of "vanity" addresses.

Issue: Relying parties. How to get massive numbers.

ANDY: Largest RP – wanted to raise user experience. Decision made on business grounds.

GEORGE: To de-open ID yourself you can create local password.

Issue: How to open up.

ANDY: Email address is primary identifier. A workflow process. Re: Gmail -just needs to confirm.

Issue: Interoperability

ANDY: Open ID identifier from Google always the same. Sync up via token.

GEORGE: IDP rely on same identifier. Linking identifiers is interesting in regards to social media. No answers.

CHUCK: Linkages vs. login vs. social networks. Treated much differently. Segmented use cases.

DAVE: Unique identifier within system and map depending use case. High secure ID vs. Easy ID cross through meta data. Consumer vs. commercial.

Question: Plaxo and Hybrid onboarding

GEORGE: Goal: Fewest # of clicks. Import contacts OAUTH1 to pull in data from Google.

Question: Mobile devices

CHUCK: Difficult challenges. None of devices optimized for gathering credentials. 45% of traffic over OAUTH, API, Mobile. Nature browsers for credential extra--- and federation. SAML for now. Open ID in future.

Question: Mobile login experience and hybrid onboarding for new users.

ERIC: Bind open ID to existing user ID. Shortcuts to open ID through metadata in email invites, etc.

Question: RP Change login box? No single answer.

ANDY: Simple as possible. Two buttons. Most don't notice. Trying to get assistance across desktop, mobile and tablet.

CHUCK: Range of consumer – large banking institutions. Segment logins by type of customers and trust decisions.

GEORGE: Yahoo! Implementation – cookie driver. AOL tries to be uniform but difficult design challenges.

DAVE: 600M active accounts. Removing things to make as simple as possible.

Question: Website wants to be a reliable party.

DAVE: Use what's there. Wild west will go away. Only a few ways to go.

GEORGE: Use a service. Only a unique use case can extract benefit.

CHUCK: Don't write your own. Treat it as a problem of customer acquisition and pipeline.

ANDY: Yahoo! had to build their own based on their business situation.

Question: Multifactor Authentication

ANDY: Looked at HW based token – too costly. In consumer world – software where new device will look for 2nd factor authentication.

CHUCK: Use case will prompt whether second challenge will be made. Mobile and tablet judged as risky. SMS message. Federate –

GEORGE: Hardware and OTP for high-risk cases. Banks as hackers get more sophisticated, this may become more necessary.

DAVE: Higher value transactions on user side are driving higher security demands. Risk analysis being used to push sophistication of solutions.

ERIC: Gmail users tend to opt out low adoption rates.

Audience Questions:

Marketing vs. Security

DAVE: Healthy tension between two factions.

Question: Consumer when things break up between OP and RP.

ERIC: Reliability issue. Backstop, one time link. Scan multiple RPs

Question: Login boxes. Standardization.

ERIC: Google been doing research combined with Microsoft. Good results will be reported next meeting.

Question: Browser vendors, what security features should they have?

ERIC: Single sign-up. Multiple browsers, across multiple platform.

CHUCK: Get rid of IE6 and IE7

DAVE: Use IE9. Also windows native application models.

Question: HTTP and HTTPS

ERIC: Open ID 2.0 will require HTTPS.

DAVE: Weakest link is open HTTP pages.

Session Four Panel Discussion: "Monetizing Identity Without Traumatizing Customers"

Don Thibeau of the OpenID Foundation moderated a panel discussion with investment leaders and identity industry leaders

David Walrod Bridgescale Partners,

Enrique Godreau Voyager Capital;

David Recordon Facebook,

Tony Nadalin Microsoft, and

Eric Sachs Google.

DAVID W: Privacy and regulatory issues are big risks and Bridgescale looks to have those risks mitigated before investing.

TONY: personal view... People have given up their privacy and little regulation involved. Microsoft tries to preserve integrity of data.

DAVID R: Products need to add value and control data. Engaging and useful.

ENRIQUE: Privacy concerns changing rapidly with new business models emerging. "Recognize" vs. "know"

DAVID W: This conference discusses features vs. industries. What is the monetization model?

ERIC: OpenID are enablers for other businesses. Removing friction.

Audience questions:

Question: What about monetization?

TONY: Not a lot of value since it's already out there.

ERIC: Cases like health IT are valuable

ENRIQUE: Predictable behavior online? What is best framework to use?

ERIC: Google has issues with making decisions on behalf of users.

DAVID W: Regulatory and customer acceptance risk

ENRIQUE: put user in charge. If they opt in, much higher adoption rates.

Question: User experience and ability to make choices.

ERIC: Privacy policies and terms of service. No one reads. Decisions made on value. Maybe read three sentences.

Question: Leaked data may not be authentic. We're in a "pure" age.

TONY: Assurance is not based on authenticity. Where it came from, how proofed. Today's systems self-asserted. No standards governing.

Question: Open source software

DAVID W: Huge lever, much more cost effective product development. Concern is contamination by proprietary code.

DAVID R: Contamination risk is FUD

DAVID W: Successful companies get sued.

Question: NIST and NSTIC (National Strategies for Trusted Identities in Cyberspace)

ERIC: Google has seen increased internet since RP announcement.

TONY: Government runs this. Closed process

Audience: Nine month spec announced hopeful this is a good thing.

Question: Investment opportunities in ID space.

ENRIQUE: Marketing value. Zero customer acquisition cost.

Audience: Consolidation occurring.

At this point there were no further questions and the meeting was brought to a conclusion at 4pm.

Minutes respectfully submitted by Rick Rasmussen

Attachments:

A) OpenID Foundation Summit PowerPoint

B) OpenID Specifications Work Update Security and UX Summit PowerPoint



WELCOME
The OpenID Summit
"Balancing Security and the User
Experience"

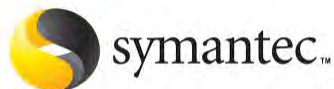
Co-sponsored by



Overview

The OpenID Foundation's 2011 series of OpenID Summits focus on use cases and topics of interest to developers, executives and analysts in the identity industry. This summit explores security and the user experience in open identity technologies.

Co-sponsored by





Agenda

12:00-13:00

- Lunch & Introductions – Led by Don Thibeau Executive Director OpenID Foundation, Eric Sachs, Google and Nico Popp, Symantec Host

13:00-16:00

- **Session One Panel Discussion: "Whither Secure Identity?"**
Nico Popp of Symantec will moderate a CTO roundtable discussion with Paul Agabian CTO Norton, Brent Williams CTO Equifax, Tim Brown SVP Distinguished Engineer CA Technologies.
- **Session Two Presentation: "What's Up with OpenID?"**
Mike Jones of Microsoft and OpenID Foundation, Nat Sakimura, Chairman OpenID Foundation, and AB/Connect Working Group Co-chairs will update the collaboration of Facebook, Google, Microsoft and others on the next stage of evolution of the OpenID protocol.



Agenda

- **Session Three Panel Discussion: "The Latest in IdP and RP Best Practices"**
Eric Sachs of Google will moderate a roundtable with Andy Wu of Yahoo!, Dave Hebert Microsoft, George Fletcher Aol, and Chuck Mortimore, Salesforce.com on identity provider and relying party best practices in online identity authentication.
- **Session Four Panel Discussion: "Monetizing Identity Without Traumatizing Customers"**
Don Thibeau of the OpenID Foundation will moderate a panel discussion with investment leaders; David Walrod Bridgescale Partners, Enrique Godreau Voyager Capital and identity industry leaders; David Recordon Facebook, Tony Nadalin Microsoft, and Eric Sachs Google.
- **16:00-17:00**
Discussion and feedback



Summit Speakers

Nico Popp - Vice President of Product Development, Trust Services, Symantec Corporation

- Nico Popp is Vice President of Product Development at VeriSign (now Symantec Corporation) where he leads the efforts to develop new products and services for cloud security. Prior to VeriSign, Popp was chief technical officer for RealNames Corporation. Popp was also co-inventor and engineering manager for WebObjects at NeXT Software and Apple Computer. Popp holds a M.S. degree in Robotics from Stanford University, and a B.S. in Aeronautics from Sup'Aero, France.

Eric Sachs - Product Manager, Google

- I am currently a Product Manager at Google where I designed another corporate ASP service which is called Google Apps For Your Domain. I've also helped build many other systems include Google Accounts, Google Health, orkut.com, as well as providing leadership in the standards community for OAuth, OpenID, Open Social, & Caja. Currently I am the Product Manager for the Google Security team and the counterpart to Google's CIO.

David Recordon - Senior Open Programs Manager at Facebook

- David leads open source and open standards initiatives. He joined Facebook from Six Apart where he focused on platform strategies, and previously worked at VeriSign in the emerging business group. David has played a pivotal role in the development and popularization of key social media technologies, such as OpenID and OAuth. In 2007, he became the youngest recipient of the Google-O'Reilly Open Source



Summit Speakers

Nat Sakimura (NRI), Chairman, OpenID Foundation

- Nat's goal is to create a world without the physical identifier to contact somebody or some service.

Anthony Nadalin - Partner architect at Microsoft

- Is working in the Government Engagement Team leading the Standards and Public Policy practice. Anthony spent 27 years with IBM where he was the Chief Security Architect responsible for the security strategy for software group products. Anthony participates in many standards organizations (OASIS, IEEE, W3C, ITU, ISO) aligning security strategy with standards.

Don Thibeau – Executive Director – OpenID Foundation

- Don is also Chairman of the Board of the Open Identity Exchange (OIX), a non-profit, technology-agnostic, multi-tenant platform for certification listing services and trust frameworks for identity authentication in global internet and telecommunications applications. He has held senior management positions with Kodak, LexisNexis, Qsent and TransUnion. Thibeau, a former Presidential appointee, has testified before Congress and speaks and writes white papers on data privacy, identity standards and technologies and related regulatory issues. He blogs on these issues at openid.net.



Summit Speakers

Brent Williams, CTO and Chief Architect, Identity Services , Equifax

- As Chief Architect, Brent is responsible for defining how Anakam products meet market requirements. Brent leads technical marketing of our products and solutions and is responsible for communicating product capabilities and value propositions to the identity management market place. Brent also leads Anakam's East Coast office, which specializes in government client program support. Brent graduated from the U.S. Naval Academy and went on to serve on nuclear submarines. In addition to his submarine duty, Brent was selected to serve at The White House supporting emergency preparedness activities and national security policy development. He completed his graduate degree in engineering at Johns Hopkins University.

Mike Jones, Director of Identity Partnerships, Microsoft

- Michael B. Jones is a Standards Architect at Microsoft. He is working to make people's online interactions seamless, secure, and more valuable. He was an author and editor of the OpenID Provider Authentication Policy Extension (PAPE) specification, is the editor of the OAuth 2.0 Bearer Token specification, is an editor for the OASIS Identity Metasystem Interoperability TC, is co-author of the emerging JSON Web Token (JWT) specification, which will be used by the OpenID Artifact Binding specification, and is an active member of the OpenID Artifact Binding working group. He was a researcher at Microsoft Research from 1992 to 2005 and earned his Ph.D. in Computer Science from Carnegie Mellon University in 1992. His interests include digital identity, privacy-protecting systems, distributed systems, networking, operating systems, musical performance, outdoor activities, and his fellow human beings.

5/2/2011

OpenID Foundation

7



Summit Speakers

Enrique Godreau III, Managing Director, Voyager Capital

- Enrique has been active in the information technology industry for nearly 30 years. His experience spans from research and development, to business management and, since 1997, venture capital investing. Enrique's primary focus is in digital media and wireless businesses. Enrique is involved with many professional, entrepreneurial, and community-based initiatives and is very excited to be serving on the Investment Committee for Global Partnerships. Enrique has a BS in Computer Science from Rensselaer Polytechnic Institute.

Chuck Mortimore, Product Management Director, Identity and Security at Salesforce.com

- Chuck is a Product Manger specializing in Identity, SaaS, PaaS, APIs, and Web Services, with an emphasis on making these simple and accessible to partners and developers. Chuck currently runs the Identity & Security Product Management for Salesforce.com.

David Walrod, Venture Partner, Bridgescale Partners

- David has been involved with investing in growth technology companies for most of his professional career. From 1999 to 2007, David was a general partner with Oak Investment Partners. David received his B.A. in physics from the University of California at Berkeley and earned a Ph.D. in solid state physics at the Massachusetts Institute of Technology. He also worked as a postdoctoral fellow at the MIT Research Lab of Electronics and completed a J.D. at the Harvard Law School.

5/2/2011

OpenID Foundation

8



Summit Speakers

Paul Agbabian, Chief Technology Officer, Norton/Symantec

- Paul is Chief Architect for the Compliance and Security Management Business Unit at Symantec Corporation. Paul Agbabian has been with Symantec for more than 10 years and has worked on Norton Antivirus for Netware, Norton Antivirus Corporate Edition, Symantec Enterprise Security Architecture, Security Information Manager (SIM), and other management technologies. His current responsibilities include technical direction for the policy compliance and SIM appliance products and technologies, as well as new technology research, partnerships, and acquisition related work. He chairs the Distributed Management Task Force (DMTF) Security workgroups and has represented Symantec in standards bodies since. Paul has a master of science in mechanical engineering from Caltech and a bachelor of science from the University of California at Los Angeles.

Tim Brown, SVP Distinguished Engineer, CA Technologies

- Tim Brown is a distinguished engineer and chief security architect for the Security and Compliance business unit at CA, Inc. He has worked with many companies and government agencies to implement sound and practical security policies and solutions. Recently he provided expert testimony at the Cyber Security R&D hearing before the (U.S.) House Committee on Science and Technology, Subcommittee on Research and Science Education. Prior to joining CA, Tim spent 12 years at Symantec. He is an avid inventor with 14 patents on file in the security field.



Summit Speakers

Andy Y Wu, Yahoo!

George Fletcher, AOL, Chief Architect for Identity Services



Thank you to our hosts and co-sponsors



Please fill out our short survey
[http://www.surveymonkey.com/s/
T6ZYL5](http://www.surveymonkey.com/s/T6ZYL5)



OpenID Specification Work Update

OpenID Summit – May 2, 2011

John Bradley – Independent

Mike Jones – Microsoft

Nat Sakimura – Nomura Research Institute



OpenID Spec Work Progressing

- Existing OpenID 2.0 specifications in use now
 - Already work fine for many use cases
- Active working occurring to extend specifications for new use cases
 - Mobile phones and other limited platforms
 - “Facebook Connect” style functionality for easy registration
 - Easier deployment than OpenID 2.0
 - Higher level of assurance use cases



Working Group

- Spec work occurring in “Artifact Binding” working group
- Incorporates submissions to former “Connect” working group
- Merger currently called “OpenID ABC”
 - *Almost certainly not final branding*
- OpenID specs developed via an open process
- All free to participate



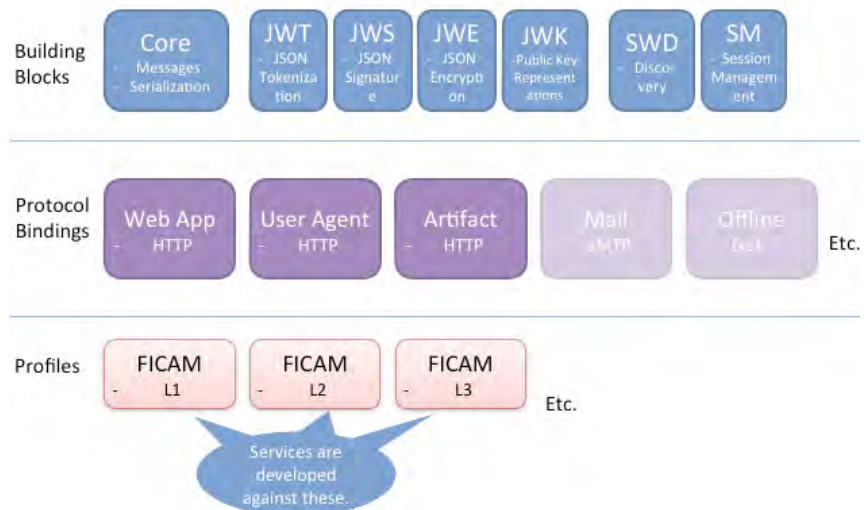
WG Participants

- Key working group participants:
 - Nat Sakimura – Nomura Research Institute – Japan
 - John Bradley – Independent – Chile
 - Breno de Medeiros – Google – US
 - Paul Tarjan – Facebook – US
 - Axel Nennker – Deutsche Telekom – Germany
 - Kick Willemse – Independent – Netherlands
 - Chuck Mortimore – Salesforce – US
 - Mike Jones – Microsoft – US
- By no means an exhaustive list!

OpenID New Spec Building Blocks

- Build on OAuth 2.0
- Use JavaScript Object Notation (JSON)
- JSON Web Token (JWT) claims representation
- Goal: Easy implementation on all modern web platforms

OpenID ABC Framework





Spec Progress

- Current status
 - Core – 80% done
 - Bindings – 80% done (pending OAuth 2.0 completion)
 - Discovery – 80% (working from SWD)
 - JWT – 90% done for tokens and signature
 - Encryption remains to be specified
 - OAuth 2.0 – 95%



Implementation Status

- OpenID ABC
 - Demo version of core and artifact binding available in PHP (BitBucket)
 - Core, Artifact Binding in Java
 - Code to be updated for recent updates
- JSON Web Token (JWT)
 - Implementations for Java, PHP, Python, Ruby, .NET



OpenID

ABC Capabilities

- Dynamic Clients
- Higher LoA
- Mobile Support
- UserInfo Endpoint
- Simple RPs
- Session Management
- OAuth 2 Integration
- Use of JWTs and JSON data structures
- Single Logout



OpenID

Open Spec Issues

- Kinds of identifiers supported
- Permissioning distributed attribute providers
- Claims specification and integration
- Trust metadata formats and transports
- OAuth 2 specification completion



OpenID

Use of Summits

- Munich: Brief participants on progress, specs - gather input
- Colorado: Interop work – potentially in cooperation with OSIS
- Tokyo: Test implementations; learn from implementation and deployment experiences
- London: Brief participants on progress, specs - gather input
- Nov IIW: Spec refinement and/or finalization



OpenID

Resources

- Artifact Binding Working Group Wiki Page
 - <http://wiki.openid.net/w/page/12995134/Artifact-Binding>
- Artifact Binding Mailing List
 - <http://lists.openid.net/mailman/listinfo/openid-specs-ab>
- OpenID Blog post “A Map for OpenID ABC”
 - <http://openid.net/2011/04/29/a-map-for-openid-abc/>
- Mike’s blog:
 - <http://self-issued.info/>



Open Discussion

- *Taking full advantage of us all being here!*