

Security Standards Workshop

Note : This document has very preliminary ideas on the workshop. At best it could act as a starting point for discussions.

1. Objectives

- Position the various standards activities (W3C/OASIS/notes/specifications)
 - Relationships
 - Dependencies
 - Convergence
- Present a preliminary architecture/roadmap of the various web service security pieces, how they fit together, where the holes are, etc.
- Presentation on major pieces by some of the experts
- Presentation by users and vendors on their view of challenges and opportunities related to security standards,
- Discussion with audience participation – the architecture/roadmap, identify missing pieces/gaps (need Vs what is there now) & opportunities for activities
 - Short term
 - Long term

2. Benefits

- To the audience – They will get a good view on where we, are in terms of security standards and how do they relate to each other. (We know there is not enough cohesion or coherence)
- From the audience – what do we need in terms of security, their priorities and (possibly) how should we proceed. The stress is on getting the feedback from the member base (and the user base + vendors)

- Stretch Goals : Crisp definition of next POA and assigned action items

3. Agenda

Proposed Venue: One full day during the XML One conference
Aug 26-30, Seaport Hotel, Boston, MA

Time	Description
9:00-9:30	Introduction
9:30 – 10:15	Security Standards Architecture - Relationships, Dependencies & Convergence <ol style="list-style-type: none"> 1. Security standards from OASIS and W3C. 2. Liaison between the various organizations and also inside OASIS like the Joint TC 3. Normalize nomenclature/vocabulary/taxonomy like channel security, message level security et al
10:15 - 10:30	Break
10:30 - 01:00	Detailed talk on various issues re standards (30 min each – 20 min talk, 10 min Q & A)
10:30 – 11:00	SOAP Security– Why, what, when, ..., OASIS Web Services Security TC (Let us do the hardest part first :o))
11:00 – 11:30	Topics on SAML - cover Kerberos, how it complements with other standards, ...
11:30 – 12:00	Identity Management – Liberty Alliance
12:00 – 12:30	Access Control & Digital Rights Management – XrML and XACML
12:30 – 01:00	Key Management – how the standards leverage key management and the current thinking on PKI et al
01:00 - 02:00	Lunch – Invited Speaker(s) (Topic TBD), Discussion. Future of Web Services Security (?)
02:00 – 03:20	Challenges & Opportunities - Users talk about their challenges, priorities, gaps in security standards. This could be a panel of 3-4 user organizations.

02:00 – 02:20	Security – User View – Manufacturing Sector
02:20 – 02:40	Security – User View – eGovernment
02:40 – 03:00	Security – User View – Financial Sector
03:00 – 03:20	Security – User View – Healthcare Sector
03:20 – 03:40	Security – Analysts' View-points (Panel of 2-3 Analysts) (Note : Might need little more time than 20 min)
03:40 – 04:00	Break
04:00 – 04:45	Open Discussion Panel – Issues and Action Items (Collect questions beforehand and discuss them)
04:45 – 05:00	Review and Action Items

4. Random Thoughts:

1. Should invite experts from users and vendors to hear the pluses and minuses of the current state of affairs
2. We could seek position mini-papers to discuss during the Challenges & opportunities sessions
3. Would be nice to get some prioritizations which could guide us on the next steps.
4. IMHO, we should come out of the workshop with some semi-concrete actions items – might be difficult to achieve
5. Which brings back to the number of folks – if we can get the right folks, the fewer the better, but if we are after visibility, the more the better.
 - a. To keep some sanity during the discussions, we could have a core team (say 20 invited experts) and the rest as observers

Version	0.04
Date	7/10/2002 9:23 AM
Reviewer(s)	
Author(s)	Krishna Sankar (ksankar@cisco.com)

