Minutes March 25

Kelvin – Call to order

Attendance called: Quorum was achieved (See Web Page for Attendance list.)
Minutes of the Last Meeting Approved

The Kavi system is now active and is being used by the TC. With respect to the documents on the wss web page, there are two URL's, a public and a private one. Use the public URL for documents and notices that are intended to be accessed by those that are not members of the WSS TC as well as the members of the TC. The private URL is accessible only to WSS members; therefore use the private URL for that data (documents, calanders, etc.) which are intended only for the WSS TC members. The Private data is available once you login to the Kavi system.

Automatic messages are sent by the Kavi system whenever a new document, calendar item, etc is sent.

The first item that was addressed in the telecom is the scenarios for the Interop. It was mentioned that items 76 through 80 were recently added to the issues list.

Tim – I don't believe that these (items 76 through 80) are relevant to the interop

Rob – Agreed, nothing related to the interop.

Ron – With respect to issue 78, I'm not sure that this is what was decided last week. Wouldn't it be simpler to just encrypt the username / password with public key of the server.

Chris - That would be unconventional.

Tim – Not clear why the certificate is included in the message.

Kelvin – Lets talk about scenarios and see if this clears up any problems.

Tim- When will a new draft of the X.509 profile will be issued?

Kelvin – Lets go to Item 5 and start talking about scenarios.

Chris – I put more information around scenarios, in order to try to make them more realistic. For example, where to use the X.509 user key identifier. To reference it, use two constants to identify the key.

Pete Dapkus - Last time we discussed using key references.

Chris – For this interop we'll just use a constant for the key identifier, or we can leave it out.

Ron – What would happen if there was no key identifier?

Chris – We could use the target's public key. But, target may have multiple keys, so this would be just a hint.

Kelvin – We would need keys and certs.

Chis – I will set this up and publish them.

Kelvin – Are the general scenarios that have been described sufficient or is something missing?

Chris – Want discussion of what companies will attend and what they will do, then we walk thru the scenarios.

Scenario 1 – a simple ping and get some text back. Send a user name and password in clear. For the interop we will use the reversed username for the password.

Ron- is the timestamp necessary

Chris – We can take them out. The spec says that if there is a header that you don't understand, then skip it.

As long as there is no mustUnderstand on the header.

Chris – I tried to keep as few variations as possible.

Ron – The Nonce and Timestamp are required in scenario 2.

Chris – take them out of scenario 2. I'll put in some descriptive text saying that in the operational case the Username token should have a timestamp. I want precision in the description of the scenarios.

Ron – The timestamp limits the possibility of reuse of the token / message.

?(Didn't get name) - interop has a clear text password

Chris - Scenario 3 adds an X.509 certificate; the body of the message is encrypted.
Scenario 4 – Changes one variable

Chris - Main thrust of the interop is to see if XML signature and encryption works

Ron – Not sure that Scenario 4 is necessary.

Chris – Want to ensure that a variation works.

Ron – Doesn't scenario 3 cover a change?

Chris – Yes, we can drop Scenario 4. Are there any objections to using the three scenarios for the interop.

There were no objection to using the three scenarios. Thus the interop will use the first three scenarios.

Chris – Who can be in the interop?

The following is a list of those who expressed interest in being in the Interop.

- Baltimore – what is time frame?
- Oracle – End of May not be do-able.
- BEA
- IBM
- Microsoft
- RSA
- Sun
- Systinet – will not be ready for mid May

=====

Chris - When shall we have the interop?

We'll make it agenda item on next call

Kelvin – I'll put stake in ground - Mid-May

Ron – May is bad for Sun.

Propose that we poll for different dates.

Chris – What should be the location? We should give people at least 5 weeks to prepare.

Kelvin – We should go to the west coast since last meeting was on the east cost.

Ron – Can the iterop be done remotely?

Chris – Very hard

Kelvin – We should have the interop, and then after we have had the interop we should have our F2F

Ron- Maybe someone can get something running on a web site for the interop.

Kelvin – Any issues beyond the interop that anyone wants to address?

Jerry- I'd like to discuss the phrase "security tokens". The problem is that security token is defined as something that makes a claim. What constitutes a token and what constitutes a claim? A token should have an XML description. Profiles should say what XML elements must be a security token. If there is a new profile it should say what is a security token and give the legal XML for it.

Chris – Two factors that we want in the specification

1. Want to distinguish signatures and claims.
2. Don't want to make other new things illegal.

A lengthy discussion took place on how to resolve this issue. The resolution was –

"Each profile should name what the tokens are for that profile. In addition the core should say what its tokens are. These (the tokens) should be defined in XML. Both the core and profiles should list whatever elements they mention/use that are not a security tokens."

TO DO FOR THE EDITORS: add the appropriate words to cover the above requirement for explicitly defining tokens. Chris will put out some sample wording.

Tim – XX causes the schema not to validate.

Chris – Working on cleaning up the XX. The WSS TC will have a solution. We will have to change this when OASIS come up with their solution

Motion to Adjourn; seconded.