OGSA Teleconference – Security Profile Review - April 7, 2008
==========

Hiro Kishimoto
Andreas Savva
Duane Merrill
Andrew Grimshaw (Minutes)
Blair Dillaway

Two draft minutes to approve.

December 6th call

January 11th Face to Face in London

Discussed the nature of the public comments.

Secure Adressing profile:

Yaushiro's comment: signing should be "MUST" not "SHOULD", Blair Dillway's said pretty much the same thing. Sven Van den Berghe had much the same comment.

Who signs it? It needs to be someone the client trusts?

Action: Duane will change it to a MUST, and will fix a few minor editorial nits.

Duane comment: he proposes mechanism to allow finer grain control.

Blair joined the call at 7:27 PM eastern.

We discussed whether it was an appropriate change.

Grimshaw said "keep it simple"

Blair opined that making the change might require putting the document through public comment.

Decided not make the modification.

Duane will modify the document, send it for last call, then we will send the document to the gfsg to be put out as a proposed recommendation.

Next discussion on the secure communication document

Discussed Yoshio Tanaka's comment about user name/password. While all agree there are risks, it is the most commonly used and should stay in. It is the one everyone knows how to do it – and it is in the HPC-Basic Profile

Sven Van den Berghe 4184:
For example, If someone sends me a security policy with a server certificate from an trusted source someone could have replaced the certificate leading to a man in the middle attack. E.g., a phishing attack.

Action: Need to elaborate the discussion about trusting the source. Must warn the reader that blindly trusting sources of security policy is not wise. It is particularly dangerous if trusting a server certificate that is passed in the document.

4183 – Sven Van den Berghe: This can be address by implementation discussion.

4186 – Blairs comments: about compliance with FIPS. Duane asked what Blair was getting at – Blair explained, Duane got it.

"Implementers" should check for this – bad things can happen.

Next telecom on the 21st.