Security Proposals and Issues Summary

Requirements (agreement so far)

1. Confidentiality
2. Integrity
3. Non-replay
4. Mutual Authentication
5. Authorization support

Historic Issues

Two approaches proposed:

1. Message level Integrity + transport layer security
   1. Message Level Integrity: WS-Security
   2. Transport Layer Security: TLS
2. Transport layer security, no specific message level security.
   1. TLS only

Original concerns:

TLS

TLS

Proxy

NSA B

NSA A

Domain B

Domain A

The main point of disagreement has been if TLS is good enough especially in the diagram described above, and do we need WS-Security to secure the message end-to-end.

**Big Question: We need to have a security model that production networks are comfortable with deploying in production, and not to satisfy near-term demonstration needs.**

**New Proposal**

1. Transport layer as the security model, no end-to-end message security
2. Mandatory token in the message within the security attributes section that can be used for authorization.