Institute for Defense Analyses
4850 Mark Center Drive • Alexandria, Virginia 22311-1882

The Case for Bi-Lateral End-To-End Strong Authentication

C. Chandersekaran
William R Simpson
Institute for Defense Analyses (IDA)

Prepared for:
Security for Access to Device APIs from the Web - W3C Workshop 10-11 December 2008, London

10 December 2008

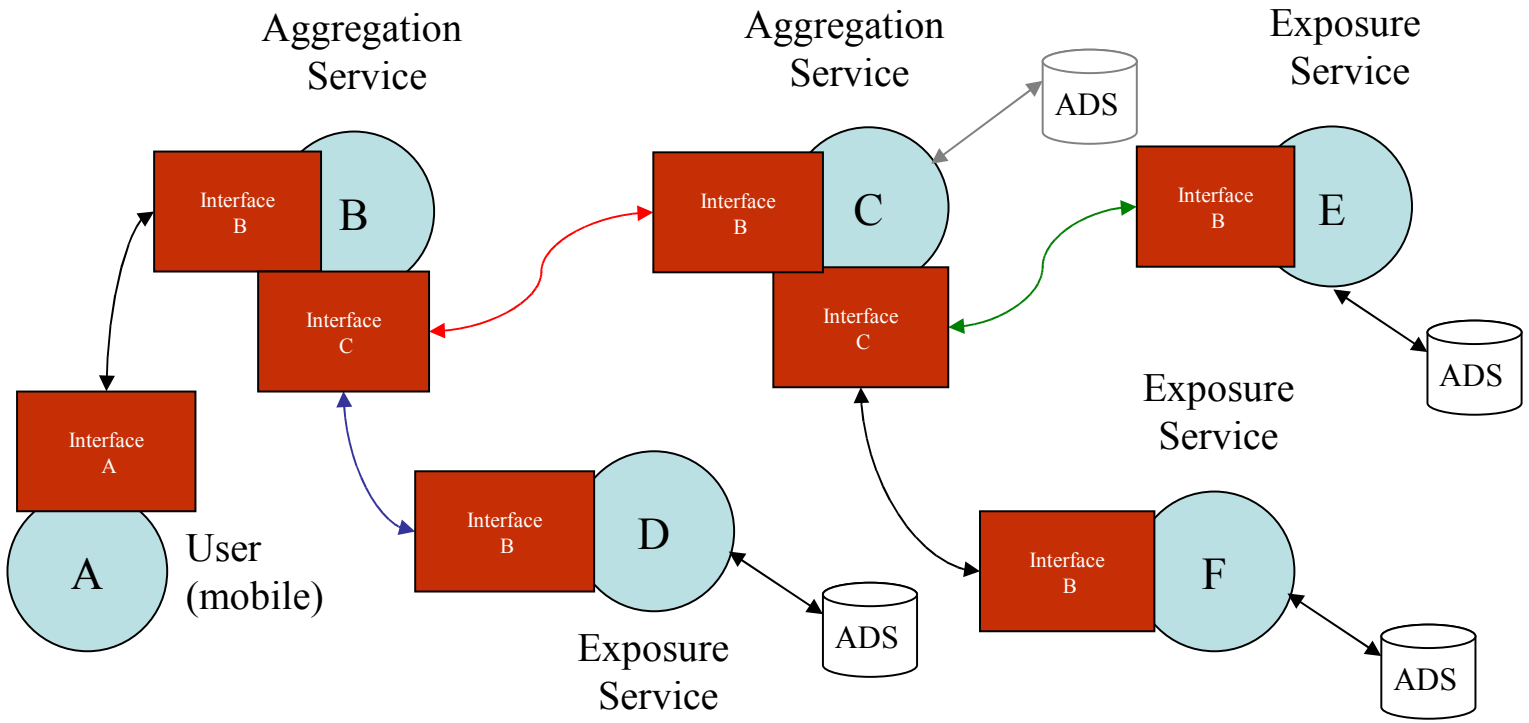
Agenda

- Need for strong authentication in IT systems
- Proposed authentication framework
- The hidden agent (Security Token Server)
- Summary
  - Advantages
  - Status in Air Force context

Need for a Strong Authentication Process

- In certain enterprises, the network is continually under attack.
  - An example might be a banking industry enterprise such as a clearing house for electronic transactions, defense industry applications, even credit card consolidation processes that handle sensitive data both fiscal and personal.
- The attacks have been pervasive and continue to the point that nefarious code may be present, even when regular monitoring and system sweeps clean up readily apparent malware.
- One way to continue operating in this environment is to not only know and vet your users, but also your software and devices. Even that has limitations when dealing with the voluminous threat environment.
- Today we regularly construct seamless encrypted communications between machines through SSL or other TLS.
  - These do not cover the “last mile” between the machine and the user (or service) on one end, and the machine and the service on the other end.
  - This last mile is particularly important when we assume that malware may exist on either machine, opening the transactions to exploits for eaves dropping, ex-filtration, session high-jacking, data corruption, man-in-the-middle, masquerade, blocking or termination of service, and other nefarious behavior.

The Service Provider concept

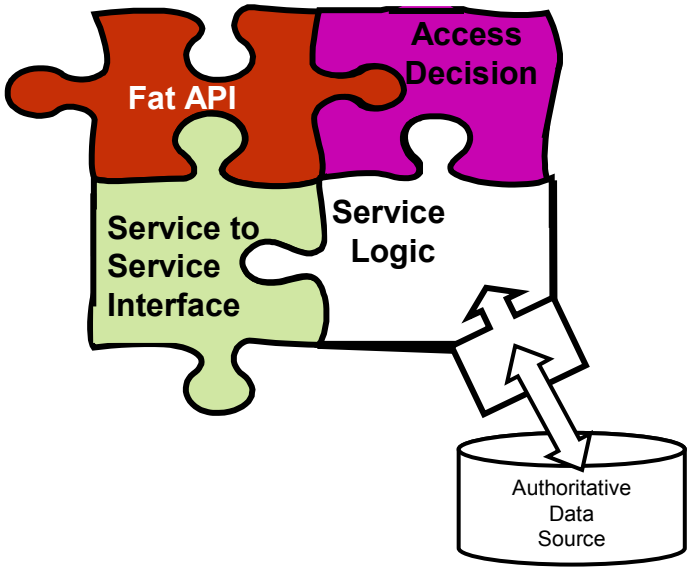


Key:
ADS – Authoritative Data Source
Exposure Service – a service that interfaces with an ADS
Aggregation Service – a service that calls other services and combine authoritative data from multiple ADS

A Structure for Bi-lateral End-to-End Authentication

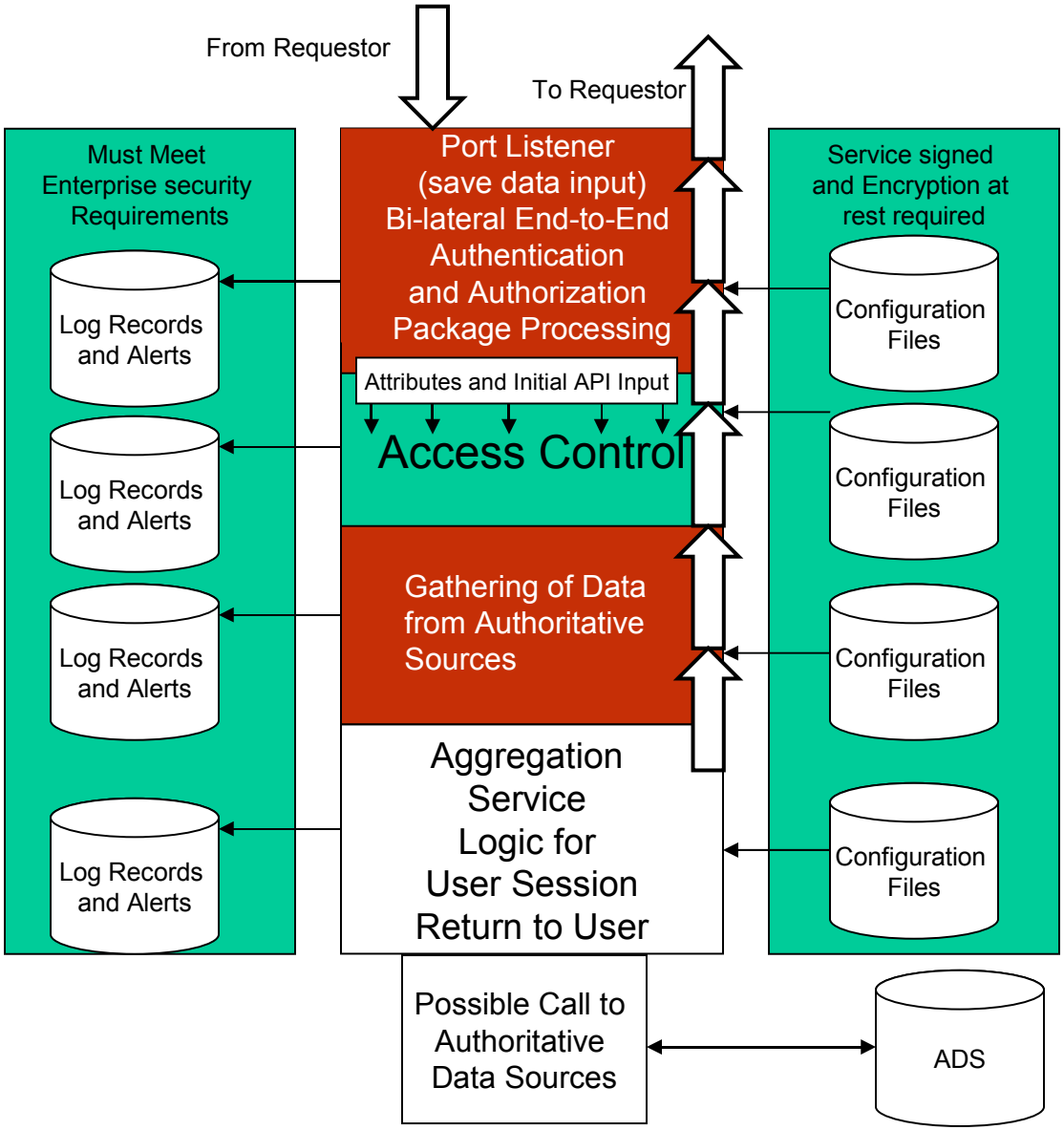
- To counter this we devise a system where all active entities (users, devices, and services) are named, registered and credentialed.
- We assume a single domain or at least a single enterprise where we have control of these details, but will address a federated case later.
- Credentials include asymmetric encryption keys.
- All services and devices exercise access controls and use SAML Assertions in their decision process. The requestor will not only authenticate to the service (not the server or device), but the service will authenticate to the requestor.
- The interface is termed a “Fat” API, or in the case of a browser or presentation system it is a “fat” browser.

The Service Provider as a Series of Interfaces

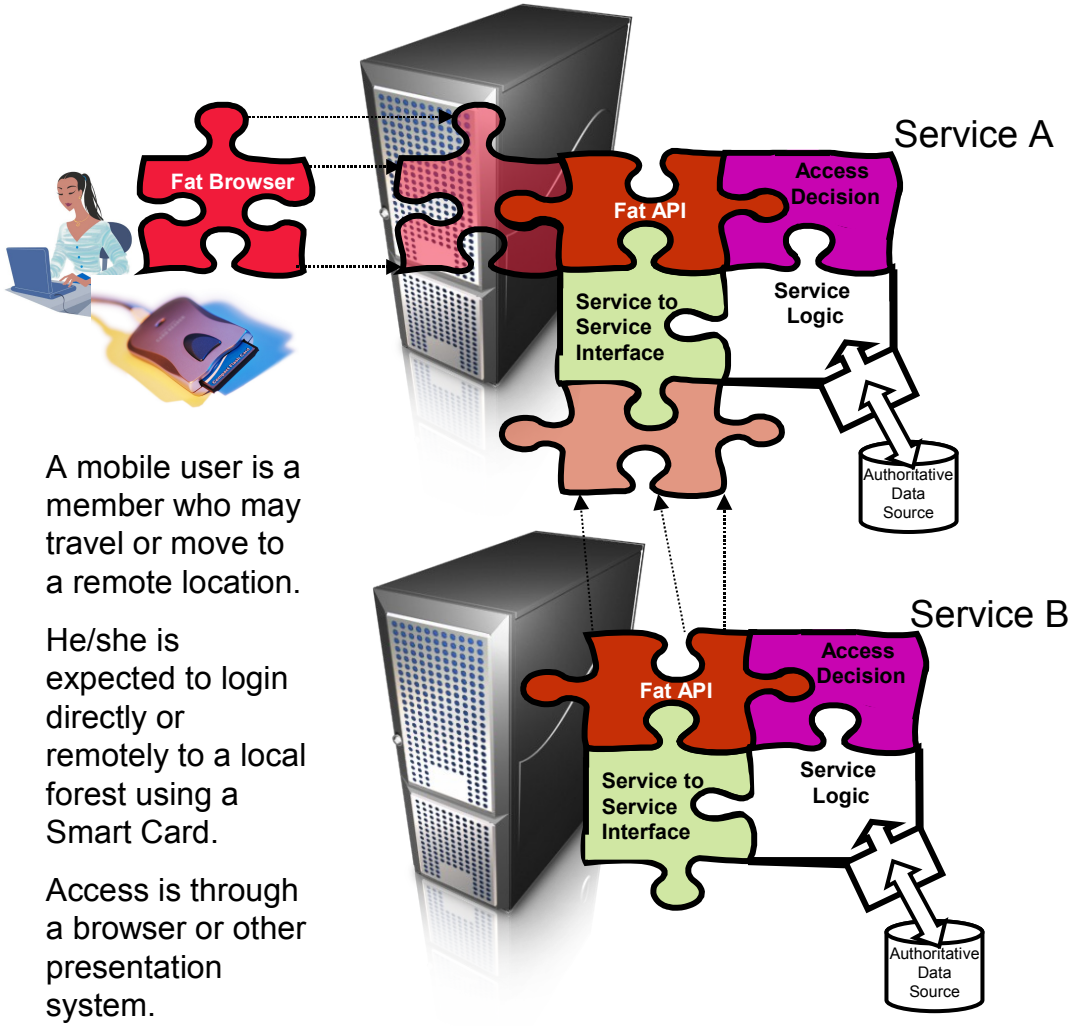


The “Fat” API completes a bi-lateral authentication with the requestor
The Access Decision determines whether the requestor has credentials for authorization
The Service to Service Interface completes a bi-lateral handshake with other service providers
The Service Logic may combine ADS, format and present data to authorized users.

Details of Service Components



The Interfaces Must be Compatible



A mobile user is a member who may travel or move to a remote location.

He/she is expected to login directly or remotely to a local forest using a Smart Card.

Access is through a browser or other presentation system.

Requestor logon from any location with CAC Card.

The Requestor must have a similar set of authentication requirements – Fat Browser

The Service to Service Interface must also have a similar set of authentication instructions.

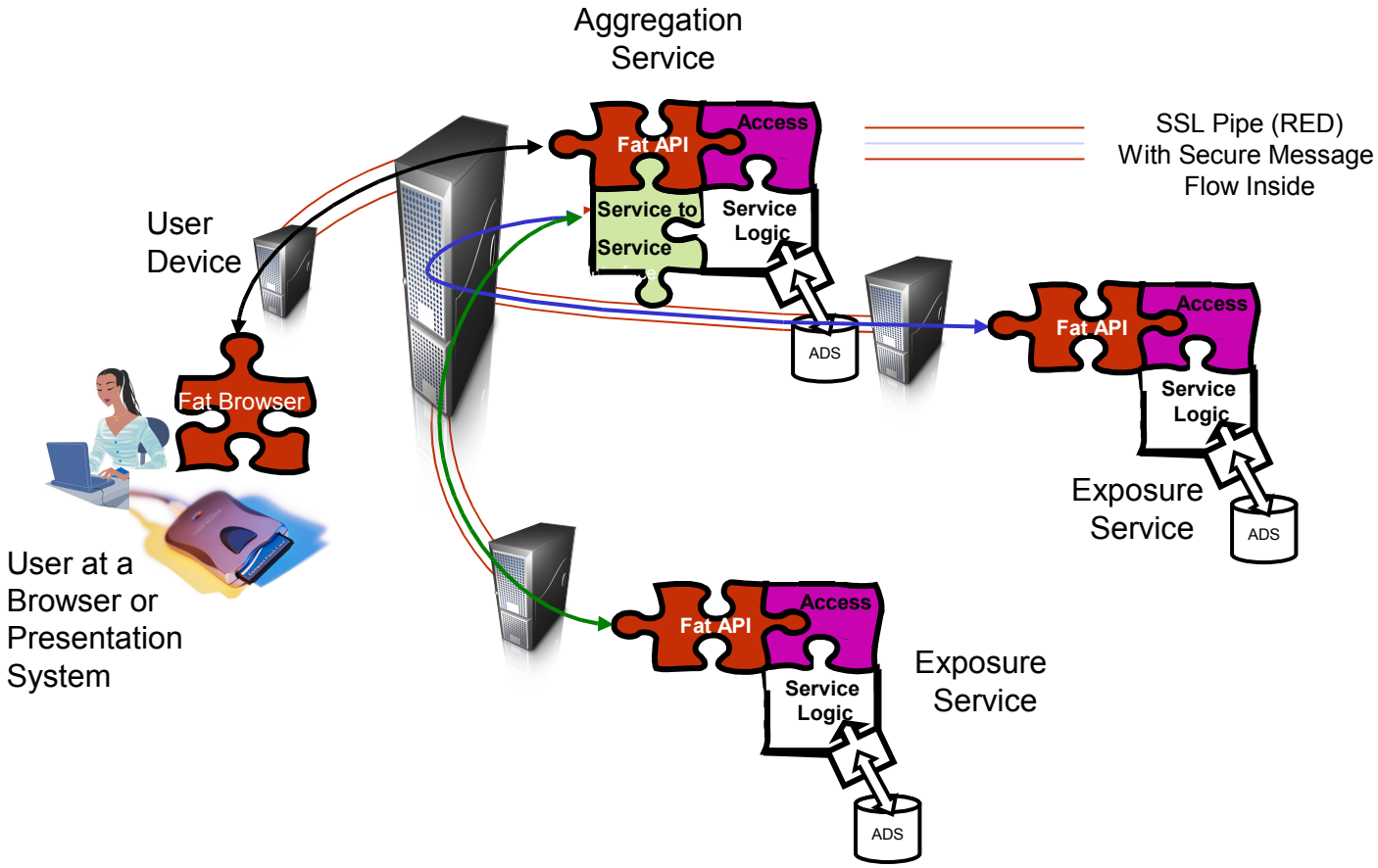
Three Software modules are Required:

- Fat Browser
- Fat API
- Service to Service call interface

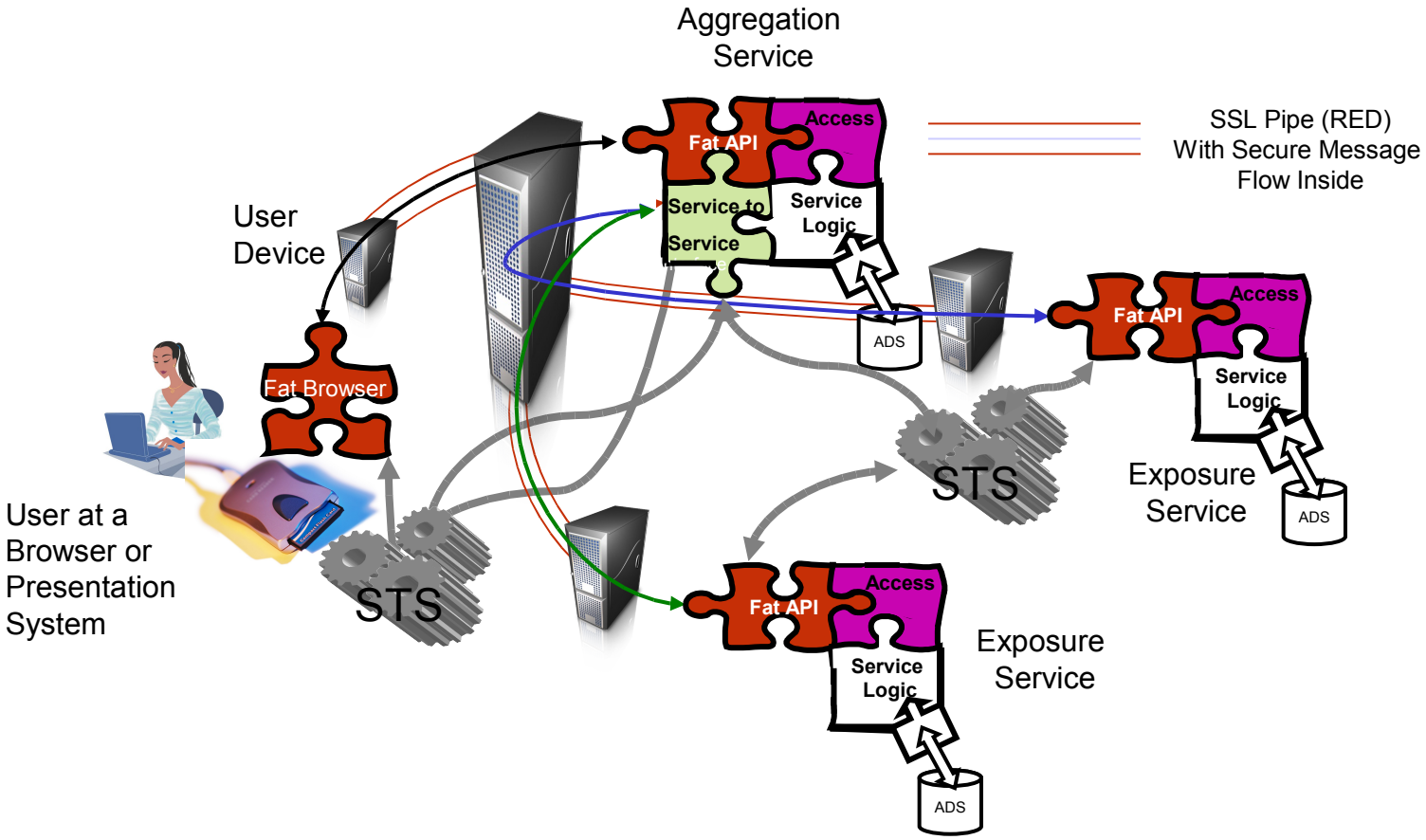
Bi-Lateral Authentication Process

- This two way authentication avoids a number of threat vulnerabilities.
- The requestor will initially authenticate to the server or device and set up an SSL connection to begin communication with the service.
- The primary method of authentication will be through the use of public keys in the X.509 certificate, which can then be used to set up encrypted communications, (either by X.509 keys or a generated session key).
- Session keys and certificate keys need to be robust and sufficiently protected to prevent malware exploitation.
- The preferred method of communication is secure messaging, contained in SOAP envelopes.

The End Result Is A Device To Device Sleeve With A End-to-End Reliable Messaging Content



Behind the Scenes, One or More Security Token Servers are Orchestrating the Interaction



Summary

- Several key pieces are missing to complete this scenario.
- On the user end we need WS-enabled browser with the ability to communicate with an ID processor and a Security Processor which together form a Security Token Server (STS).
- The STS will facilitate the exchange of credentials, aid in setting up the initial SSL, and provide the SAML package for consumption.
- The fat browser may be on a desktop or a mobile device.
- On the service provider end we need the software to encrypt/decrypt secure message.
  - If we assume for the moment that the user is tightly bound to the browser, then the user security context is maintained through the device and all the way to the service.
  - This context will assist in attribution and delegation and in monitoring insider behavior activity.
- The remaining threats of insider activity, ex-filtration of static data and denial-of service (DOS) attacks must be handled by other means, but behavioral modeling, static encryption and dynamic ports and protocols still apply to these threats.
- The fat browser, the fat API, and the Service to Service Interface packages are under development.

Additional Considerations

- Several additional features of the STS are needed which the OASIS standards have not addressed.
  - When the communication is across domains, an STS in each domain is needed and a mutual recognition of signature authority is needed.
  - If they are across enterprises we may need to do a remapping of the SAML assertions.
  - We need a good process for least privilege, delegation and attribution in each of these circumstances.
  - While WS-Federation standards assist; they do not specifically address attribute pruning, remapping, or multiple STS registered recognition.
- The process is not without draw-backs
  - Additional cycles are used in the bi-lateral authentication and the double encryption (both SSL and secure messaging).
  - This latter makes it unattractive for some applications where the threat environment is minimal.
  - However, there exist a number of environments where the added security is worth the cycles, or where higher performance cores are available.