Federated Trust Policy Enforcement by Delegated SAML Assertion Pruning

by
C. Chandersekaran, Institute for Defense Analyses
William R Simpson, Institute for Defense Analyses

General federation agreements between activities are being developed in the push to information sharing. These are often negotiated at top level where the individuals negotiating do not have a feel for the IT implications of such agreements if they are not specific enough to restrict as well as permit access. Amending such agreements may be a delicate and tedious process when it is discovered that the general agreement to share does not apply to – IP addresses, certain identities, some attribute assertions, etc. Firewall blocking at enterprise boundaries may have political implications and is generally a gross level approach as opposed to fine tuning. To allow for a more precise refinement of policy, the process of trust establishment may be delegated to the Security Token Service (STS) designated as the federation server. We note particularly that all federated activities must go through this server. Before providing the details of the delegation we review the federation approach below.

Communications across Forest Boundaries

Each Forest will have a security Token Server (STS) that is used to provide an environment for bi-lateral authentication, and the production of SAML packages for authorization. The initial communication between a user in his forest and a service in another Forest is shown in Figure 1.

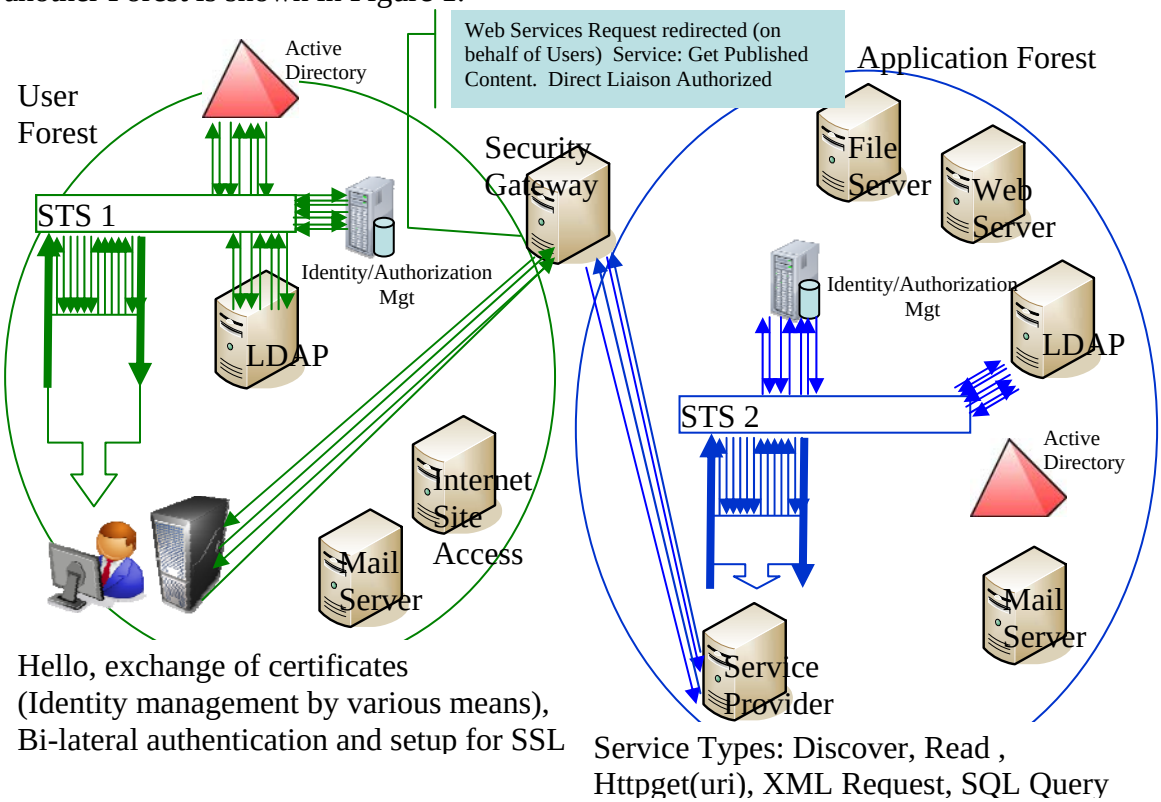

Figure 1 Cross-Forest Authentication

Once the authentication is completed an SSL is established between the user and the service provider, within which a WS Security package will be sent to the service. The WS Security package contains a SAML Token generated by the Security Token Server in the requestor's forest. The signature on this package may not be recognized in the application Forest as shown in Figure 2. The signature may be from a federated partner or within the enterprise. Service cannot be granted under these circumstances, and in fact the SAML package will not be examined for assertions. As a first step in granting access, the SAML package is forwarded to the local STS for resolution.

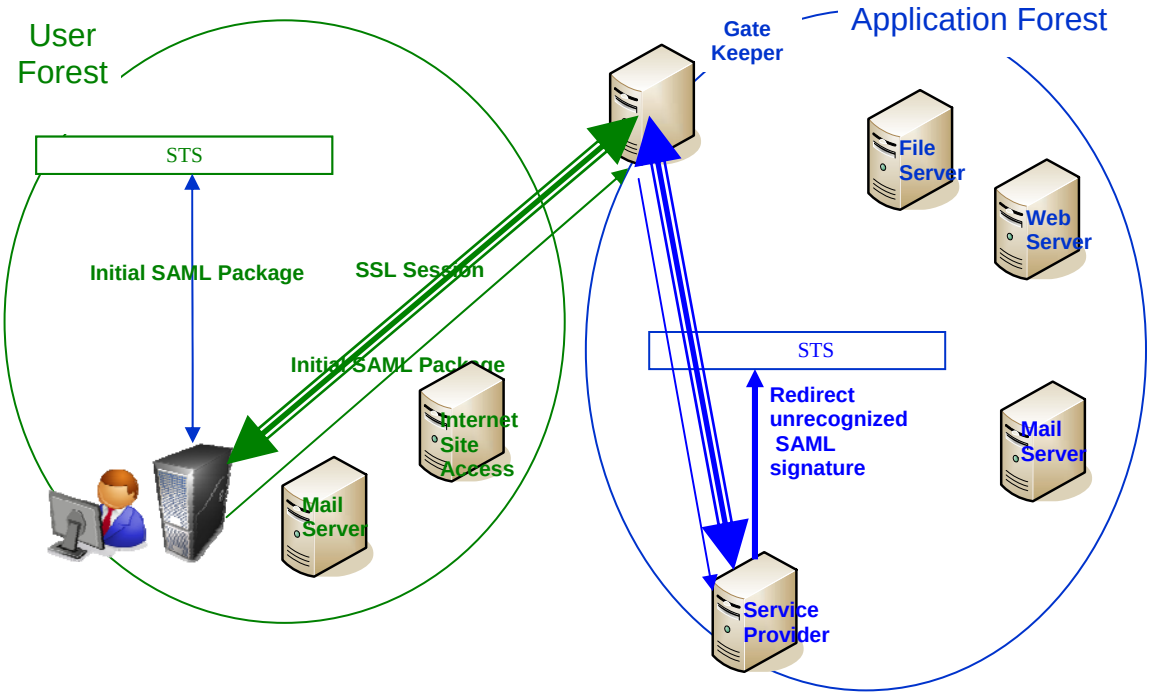

Figure 2 Request for SAML Package

In the redirection shown in Figure 2, the local STS must evaluate both the legitimacy of the request and the mappings required by federation. These exchanges are shown in Figure 3.

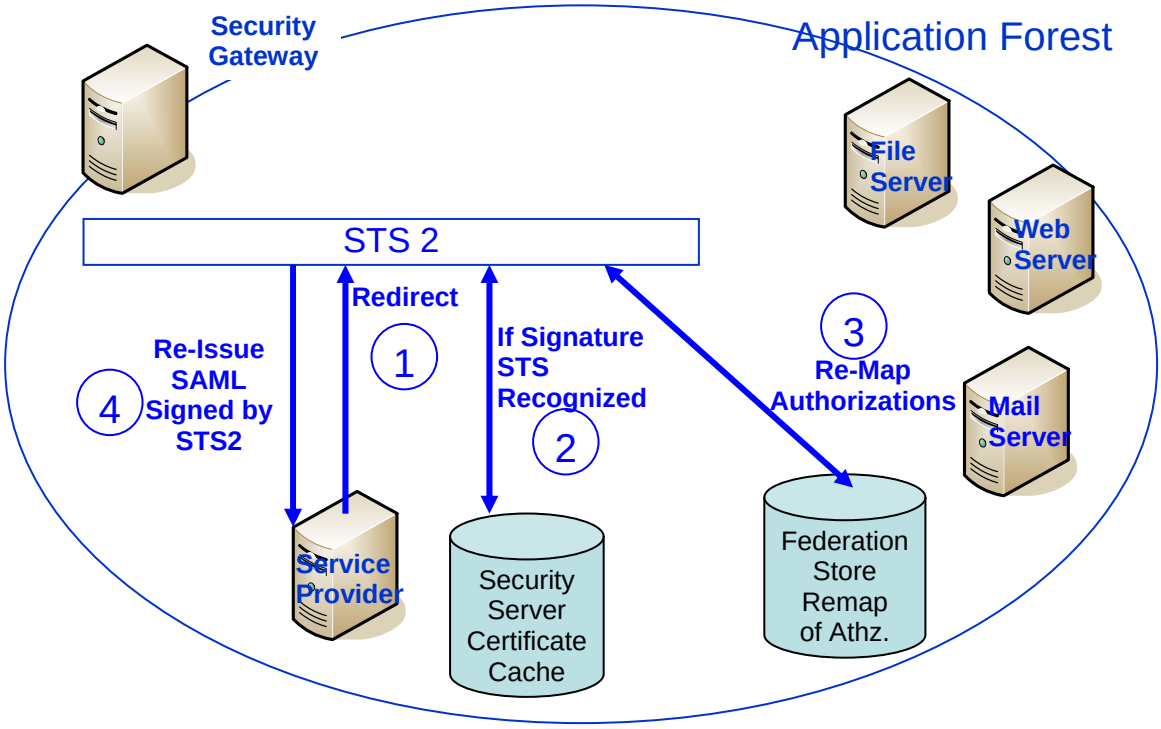

Figure 3 SAML Rework Requirements

The resolution takes place in several distinct steps:

1. The first step in the redirect to the local STS.
2. The local STS then will attempt to resolve the signature. It does this by consulting a cache of security server certificates that are authorized within the enterprise. If a match is found the STS will proceed to step 3. If not, the SAML package will fail, audit logs and alerts are generated, and authorization is not granted.
3. A match requires a comparison to the a federation store map which has translation of groups and roles as well as any restrictions placed upon the interaction by the federation agreement.
4. The last step is to reissue the SAML assertion package, signed by the local STS and return it to the application service where an access decision can be made.

Federation Data Requirements

In order to resolve the federation issues, the STS must have access to, or maintain a data base that contains the following:

- Public keys of federated servers for resolving signatures in SAML tokens.
- The following data is required for each such server.
    - A set of identity mapping tuples with the form identity1, intentity2.
    - A set of mapping tuples of the form attribute-a, attribute-b.

Delegation of Security Policy

In order to apply some fine tuning to the policy of sharing, the tuples for identity mapping can be mapped to null causing a failed authentication in the exchange for the specific identities. Further, attribute classes can be mapped to null causing a failure in

the authorization. IP addresses should still be blocked at the enterprise boundary. This delegation of the security policy enforcement can be accomplished without renegotiating the federation agreement.