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

# Federated Trust Policy Enforcement by Delegated SAML Assertion Pruning

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

The publication of this paper does not indicate endorsement by the US Department of Defense or IDA, nor should the contents be construed as reflecting the official position of these organizations.

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

10 December 2008

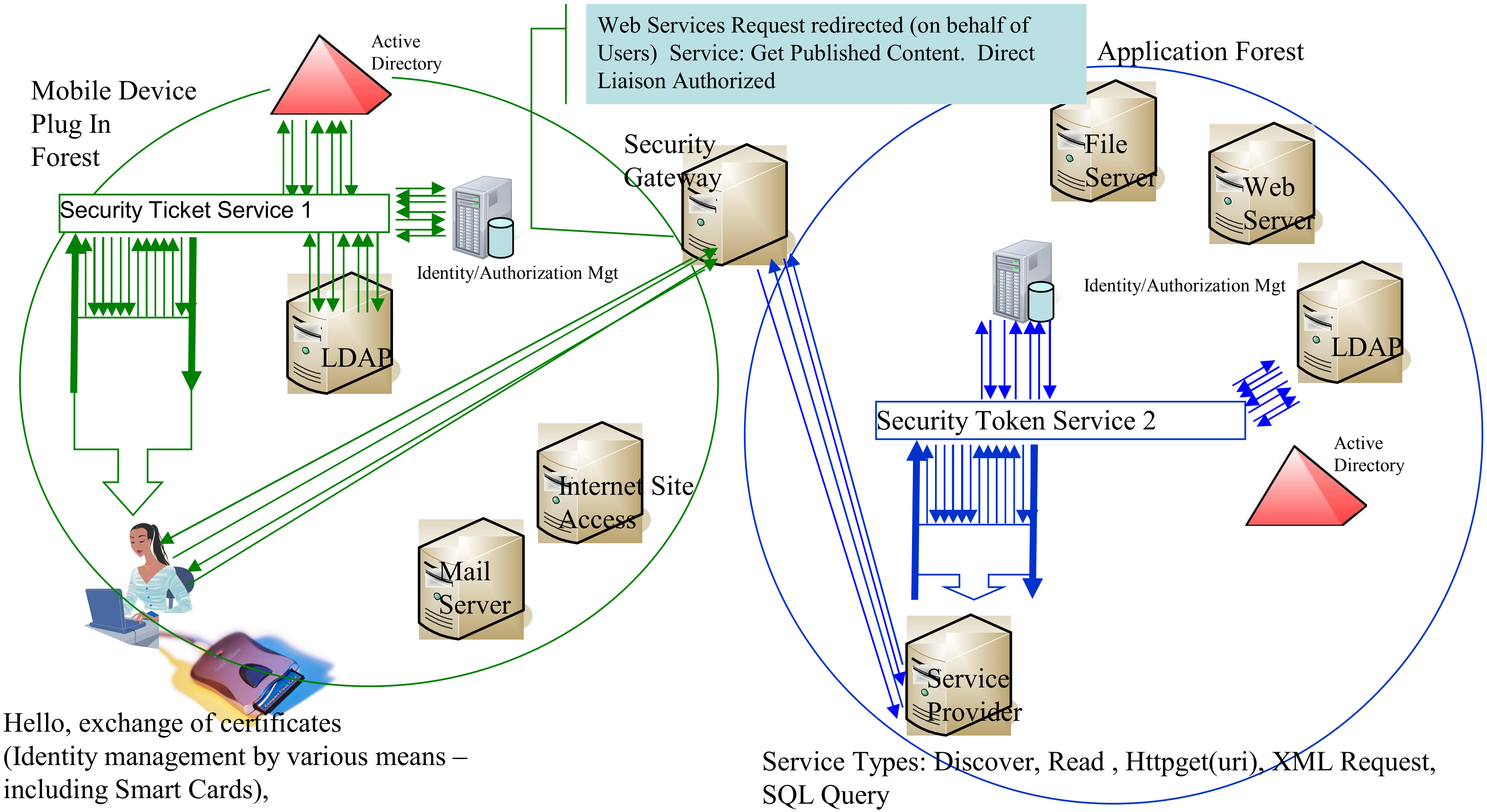
# Agenda

- Need for Federated policy enforcement.
- Communication across forest boundaries.
- Security Token Servers.
- Proposed enforcement framework.

# Need for Federated Policy Enforcement

- 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, compromised systems 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.

# The Token Server in Federation



Web Services Request redirected (on behalf of Users) Service: Get Published Content. Direct Liaison Authorized

Mobile Device Plug In Forest

Active Directory

Security Ticket Service 1

Identity/Authorization Mgt

LDAP

Security Gateway

Internet Site Access

Mail Server

Application Forest

File Server

Web Server

Identity/Authorization Mgt

LDAP

Security Token Service 2

Active Directory

Service Provider

Hello, exchange of certificates
(Identity management by various means – including Smart Cards),
Bi-lateral authentication and setup for SSL

Service Types: Discover, Read , Httpget(uri), XML Request, SQL Query

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.

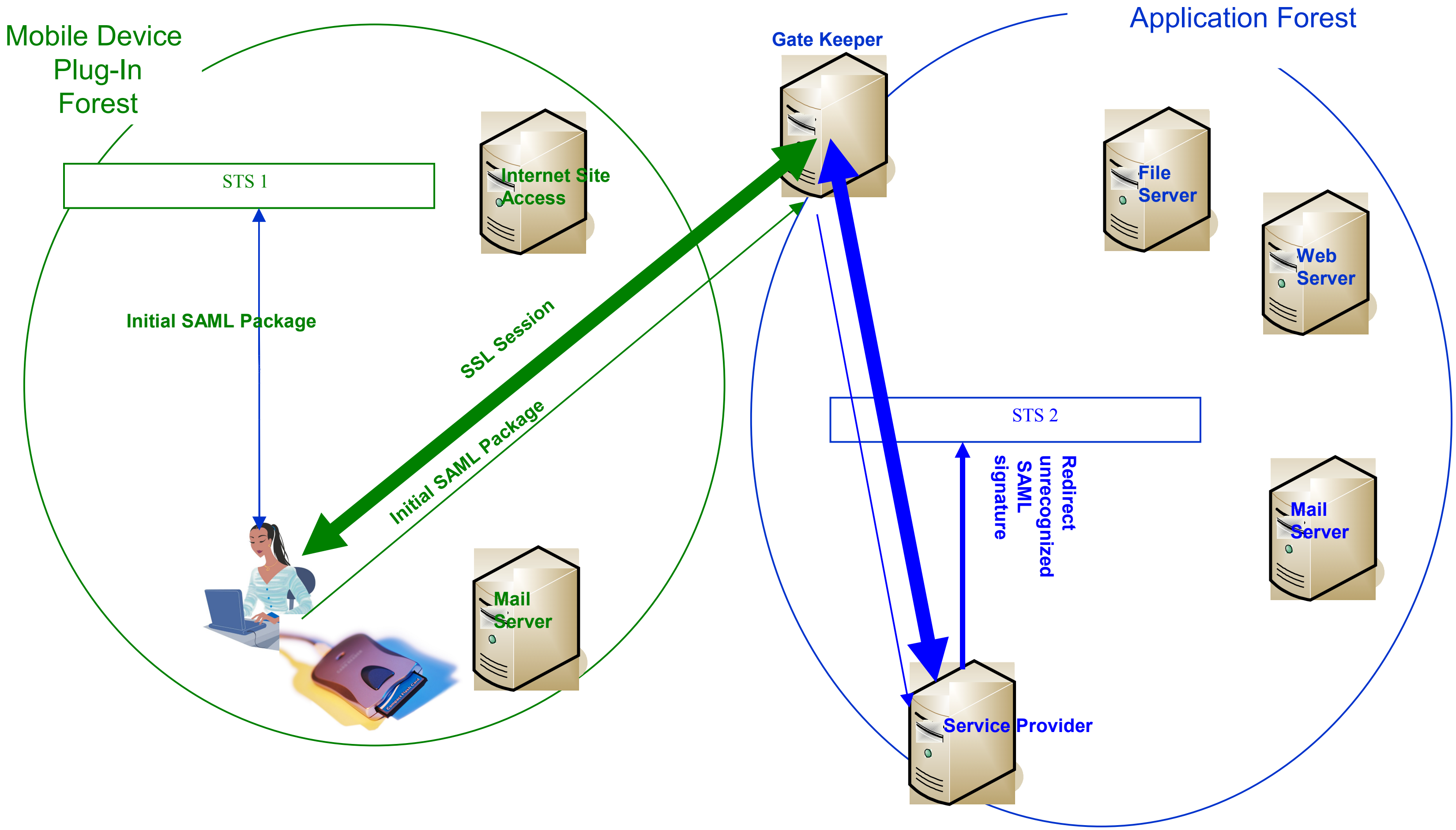
# SAML 2.0 Format

| Item | Field Usage | Recommendation | Notes |
|---|---|---|---|
| ***SAML Response*** | | | |
| Version ID | Version 2.0 | Required | |
| ID | (uniquely assigned) | Required | |
| Issue Instant | Timestamp | Required | |
| Issuer | Yes | Required | STS Name |
| Signature | Yes | Required | STS Signature |
| Subject | Yes For User A | Required | Must contain the X.509 Distinguished name or equivalent |
| ***Attribute Assertion*** | | | |
| Subject | Yes For User A | edipi | For Attribution |
| Attributes, Group and Role Memberships | Yes For User A | Required | |
| ***Conditions*** | | | |
| NotBefore | Yes | Required | TimeStamp - minutes |
| NotAfter | Yes | Required | TimeStamp + minutes |
| OneTimeUse | Yes | Required | Mandatory |

# SAML Resolution Across Forest Boundaries

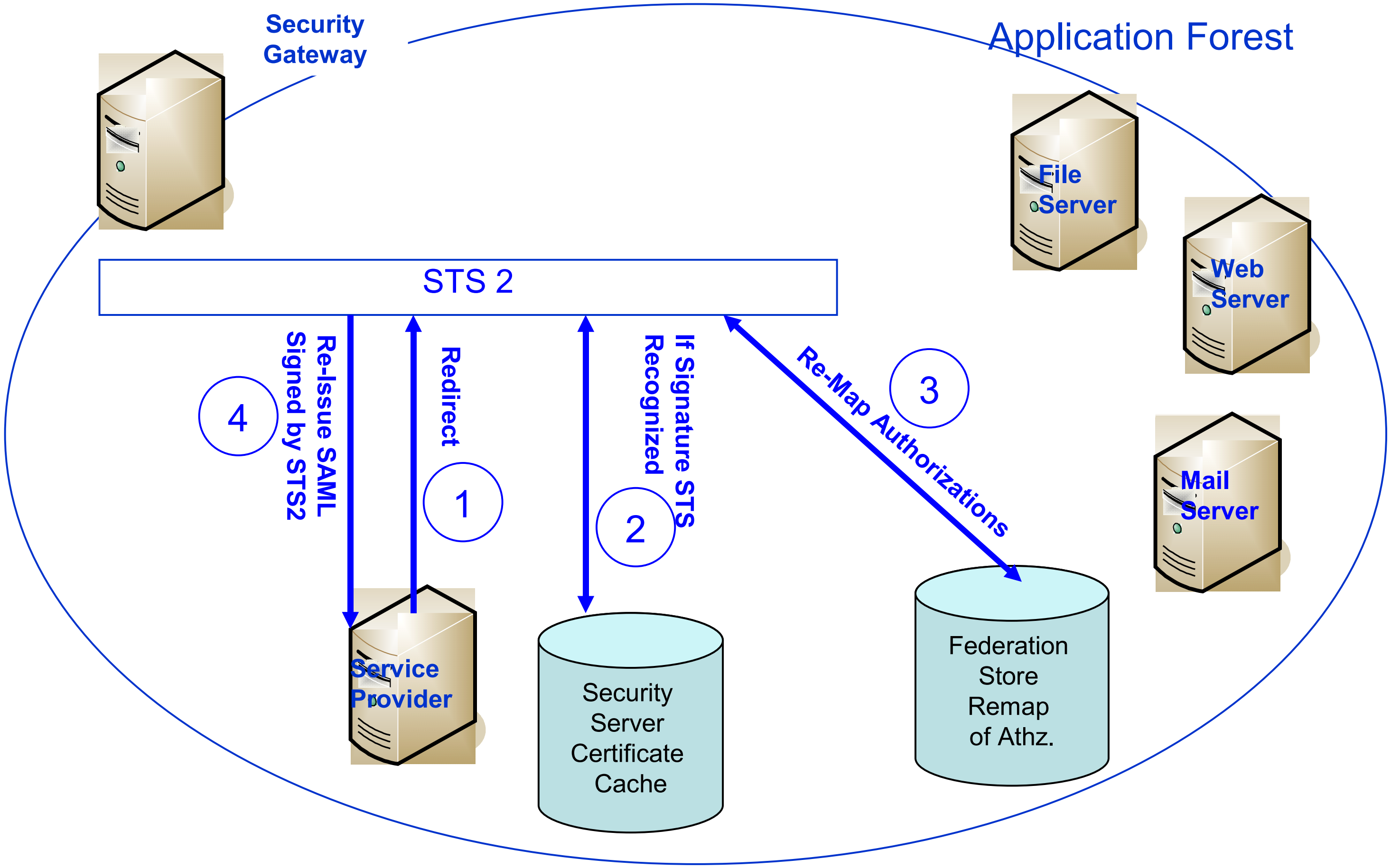
- Once the authentication is completed an SSL is established between the user device and the server, within which a WS Security package will be sent to the service.
- The WS Security package contains a SAML Token generated by the Security Token Server in the requestor’s forest. The signature on this package may not be recognized in the application.
- 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.

# SAML Resolution Across Forest Boundaries – Con't



An Unresolved SAML Package is forwarded to the local STS for resolution

# SAML Resolution Across Forest Boundaries – Con't



The local STS must evaluate both the legitimacy of the request and the mappings required by federation.

# 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 token 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.

# Additional Considerations

- Failed authentication and authorization may generate help desk and Enterprise Security analysis issues.
- Several additional features of the STS are needed which the OASIS standards have not addressed.
  - When the communication is across domains, then and 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.