Claims-Based Enterprise-Wide Access Control

Coimbatore Chandersekaran, and William R Simpson

***Abstract*— Access control is a primary consideration when standing up a high-assurance, internet-scale, and web-service based enterprise system for information sharing,. A generalized standards-based solution is presented. Central to this system is a process for access control that provides the fine-grained authorities for use by enterprise services. In all cases, the access control, rights and privileges are done by the web service itself, through its own Access Control Lists (ACLs), and are preceded by a bi-lateral authentication in both normal and federated service requests. The enterprise system relies on a unified naming and credentialing system for identity management which is not dealt with in this paper due to size constraints. This document provides the process by which access control and entities' claims are developed at the enterprise level. The claims are computed using enterprise attributes, use cases, policy statements and other data together with an Attribute Based Access Control (ABAC) / Policy Based Access Control (PBAC) engine described in this paper. These claims are then placed in a Security Assertion Markup Language (SAML) token to be used by the web service. The SAML is signed for integrity and encrypted for confidentiality. This is the first enterprise level scale-up that has provided a consistent enterprise solution to access control that has not used a centralized Access Control Service and relies solely on the provider service for access control and authority determination.**

***Index Terms*— Access Control, Claims Based Authorization, SAML, Enterprise Security**

I. INTRODUCTION

Entities in the Enterprise environment may be active or passive. Passive entities include information packages, static files and/or reference data structures. Passive entities are the target of activities and do not initiate activities and cannot assume the role of requester or provider. Active entities are those entities that change or modify passive entities, request or provide services, or participate in communication flows. Active entities are users, hardware, and services. All active entities in the enterprise have enterprise X.509 Public Key Infrastructure (PKI) certificates [6d], and their private keys are stored in tamper proof, threat mitigating storage. Communication between active entities in the enterprise requires full bi-lateral PKI, end-to-end authentication. Active entities must be named in accordance with enterprise naming instruction. Authorization in the operational environment is implemented by a verifiable access control claims-based process.

Manuscript received December 15, 2011; revised March 3, 2012. This work was supported in part by the U.S. Secretary of the Air Force and The Institute for Defense Analyses. The publication of this paper does not indicate endorsement by the Department of Defense or IDA, nor should the contents be construed as reflecting the official position of these organizations
Coimbatore Chandersekaran is with the Institute for Defense Analyses.(email: cchander@ida.org)
William R. Simpson is with the Institute for Defense Analyses, 4850 Mark Center Drive, Alexandria, Virginia 22311 USA and is the corresponding author phone: 703-845-6637, FAX: 703-845-6848 (e-mail: rsimpson@ida.org)

Claims are part of an authorization credential issued by a trusted Secure Token Server (STS) and signed by that entity to preserve integrity. A claims-based credential is sent to the provider in a Simple Object Access Protocol (SOAP) [1a] envelope containing a SAML token which includes issuance time and expiration time. Figure 1 displays two active entities performing authorization and Active Entity B retrieving content from a passive entity.

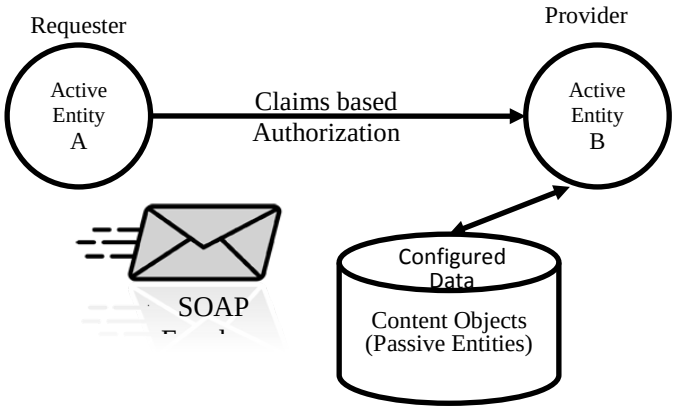

Fig. 1 Communication between Entities

II. CLAIMS BASED ACCESS CONTROL

For access control, the required credential is the SAML Token which is constructed at runtime by an STS that has access to Active Directory (AD) and an enterprise Attribute Store (EAS) as described below. The SAML may also be created by a trusted federation partner in accordance with federation agreements. In each case, the SAML is provided directly to the provider after authentication. The provider verifies and validates the SAML and extracts the claims as described below.

III. TOKEN USAGE

A request is initiated by an Active Entity for a SAML token to be issued for a specific service provider. The requester authenticates itself to the STS and based on the identity established during the authentication process, the STS obtains claims from the AD and the EAS for that identity. The STS incorporates these claims in a SAML token. The claims include groups and roles that satisfy use case and policy requirements for these web services. The claims can also include delegated responsibilities as describe below. The STS signs the SAML credential indicating to active entities that the claims are from the STS. If the STS is on the trusted list that each service developer is provided, then the claims can be recognized by the service provider. The service provider verifies and validates the SAML token. The claims included in the SAML token can be used to define the scope of the access which is defined in the use case for the service.

ISBN: 978-988-19251-3-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

A. *SAML Tokens*

The primary method for presenting access control claims is the SAML token. The SAML tokens are issued by the STS on a per invocation basis. SAML tokens contain claims asserting attributes, membership in groups and roles and extended claims that include authorized and approved delegated authorities. SAML token format is based on the current SAML standard [2e]. The use of SAML Tokens follows the WS-Security (WSS) framework for web service access using SOAP envelopes. The enterprise uses the WS-Security SAML Binding package.[2d] The SAML token is included in a SOAP message request. The SAML token is signed using the XML Signature standard [1d] and the contents protected using the XML Encryption standard [1c]. Table 1 describes the contents common to enterprise SAML assertions. While other information is included in the SAML standard (such as authentication data), only the information in Table 1 is used in the enterprise.

Table 1 SAML Requirements

Field	Required Content	Notes
SAML: Assertion		
Version ID	Version 2.0	Required
ID	(Unique value)	Required
Issue Instant	Timestamp	Required
Issuer	(content)	Required
Signature	(content)	Required
Subject	(content)	Required - Must contain the X.509 Distinguished Name
SAML: Attribute Statement		
Subject	Common Name	For identification in log files
Claims (Attributes, Groups and Roles)	(content)	Claims may include extended claims for delegation and will be pruned for least privilege when appropriate
SAML: Conditions		
NotBefore	(content)	Timestamp – minutes
NotAfter	(content)	Timestamp + minutes
STS Signature		

B. *Access Control is Implemented in Every Web Service*

Upon receipt of the SAML Token, the service identifies the signer of the token and extracts the signer's public key. If the public key is in the local security store, the signer is recognized.

- If the signer is recognized, the service validates the SAML token (signature validity, validity period, revocation status). If all checks are successful, the validation is successful; otherwise an authorization fail message is sent.
- If the signer is not recognized, the SAML token is sent to the Federation STS for possible federation resolution. The Federation STS returns either a new SAML token that it has signed (start over again) or an authorization failure message.

Access is granted when a requester presents a SAML token with an appropriate set of authorization claims to a service.

IV. ACCESS CONTROL DECISION

The authorization code in each service incorporates a claims-based process that validates access based on match between the service ACLs and the claims presented for successful authorization.

A. *Authorization Implementation*

The following steps are used to determine the requesters' access to a web service.

1. SAML token validation (see above).
2. Extract the group and role claims of the requester from the SAML token
3. Compared one by one the claims from the SAML token to elements in the Access Control List (ACL). A match allows access to the service. Lack of a match is an authorization failure.

If authorization fails, an error message is returned to the requester ("Web Service Issue. Please try again. If problems persist contact help desk. Code ####" – where #### is a session attribute for help desk use)

B. *Security Flows in the Environment*

The security model implemented as part of the enterprise implementation requires PKI based certificates of active entities and relies on details of claims to be incorporated in SAML token assertions to support authorization decisions by services.

Each web service must be registered in the EAS with a set of use cases. These use cases are used by the EAS in computing claims and these claims are stored in the EAS and made available to the STS. Further, a list of Trusted STSs is created in a store on each instance of an STS that will act as a federation server. Figure 2 shows the overall flow in the enterprise.

The EAS is described in detail in section VI. The claims may be extended for delegation.

C. *Trusted Security Token Service Store*

Federation is the recognition of entities that are certificated and provide claims from domains that are not recognized by the service. The web service in the enterprise has a limited number of recognized keys stored in the security related file.

Federation applies to any unrecognized signature in the SAML token, whether it is enterprise or not. The federation may be as complicated as coalition partners, or as simple as requests from other enterprise domains. The security model implemented as part of the enterprise implementation requires PKI based certificates of active entities and relies on details of claims to be incorporated in SAML token assertions to support authorization decisions. Further, a list of Trusted STSs is created in a store that is collocated with the STS.

This store supports the federation activity. In order to resolve the federation issues, the STS has available the following information:

- Public keys of federated security token servers for resolving signatures in SAML tokens.
  - Recognition of a signature results in an attempted reissuance of the SAML token as outlined below.

ISBN: 978-988-19251-3-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

o Non-recognition of the signature invalidates the SAML and prompts an invalid SAML return which causes an authorization failure.

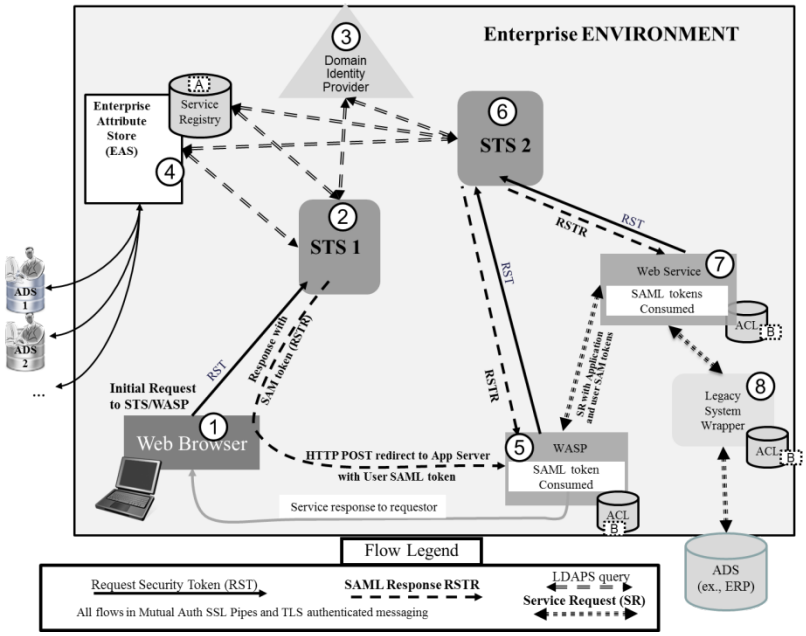

Fig. 2 General Flows during a User Session

- A set of identity-mapping tuples with the form identity1, intentity2 where * in Table 2 indicates no further remapping required. For simple federation, where requests are across enterprise domains, this mapping is "no change", and the names are in the appropriate form already. A null mapping on an identity, upon execution, invalidates the SAML and prompts an invalid SAML return which causes an authorization failure.
- A set of mapping n-tuples of the form claim a, claim b where * in Table 2 indicates no further remapping required. For simple federation, where requests are across enterprise domains, this mapping is not required, and the claims are in the appropriate form already.
- Mappings may include Boolean operations and may map to multiple alternatives. Boolean operations are not acceptable on the "map to" side. The mappings depend upon the federation agreement.
- In all mappings, "null" and "no change" mappings are acceptable. Null removes the claim or identity, while no change leaves the original claim or identity.
- An identity mapping invalidates the Holder Of Key (HOK) on the reissued SAML token. This step is skipped in the verification process.[1]
- The claims that are being mapped must match claims from sources on both sides:
  - Claims in the federation partner SAML must match the federation agreement exactly.
  - Claims in the re-issued enterprise SAML must match enterprise claims for the target service(s).
- Identities and claims are added to the federation store after an amendment to the federation agreement.

[1] HOK is the binding between the authentication and the authorization. Mapping identities denies this binding and should only be done after careful consideration.

The following data is available for each such recognized federated security token server:

- Policy changes for individuals or accesses are implemented by a "null" mapping so that the re-issued SAML eliminates the claims.
- Revocation of a federation agreement is accomplished by removing the federation partner from the trusted STS data store.

The basic information is shown in the following table:

D. *Elements of Federated Communication* [18]

Federated communications must meet all of the enterprise requirements, including:

- Naming and X.509 PKI certificates,
- Certificates issued by a recognized certificate issuer,
- Valid dates and not revoked,
- TLS mutual authentication, and
- SAML tokens from designated authorized STSs that meet all of the above requirements.

Table 2 Federation Data Requirements

Trusted STS Data Store			
	Original SAML	**Re-issued SAML**	
Enterprise STS 1	Enterprise STS Public Key		These STS signatures will be recognized on SAML tokens
Identity Mapping Block	*	*	
Claim Mapping Block	*	*	
Enterprise STS 2	Enterprise STS Public Key		
Identity Mapping Block	*	*	
Claim Mapping Block	*	*	
End Enterprise STS			
Federation Partner 1	Federation Public Key		Each Federation partner will have its own mapping requirements – in general federation partners are not provided actual ACL claims for authorization.
Identity Mapping Block	Identity 1	Identity 2	
	Identity A	Identity B	
	Identity Q	Identity B	
	Identity r	No change	
	Identity s	No change	
	…	…	
	No Further Identities accepted		
	*	*	
Claim Mapping Block	Claim 1 and Claim q	Claim 2	
	Claim A	Null	
	Claim n	Claim z, Claim q	
	Claim y and not Claim r	Claim 2	
	…	…	
	*	*	
End Federation Partner 1			
Federation Partner 2	Federation Public Key		Each Federation partner will have its own mapping requirements – in general federation partners are not provided actual ACL claims for authorization.
Identity Mapping Block	Identity x	Identity y	
	Identity Q	Identity R	
	…	…	
	All other identities accepted and not changed		
	*	*	
Claim Mapping Block	Claim n	Claim m	
	Claim o	Claim p	
	…	…	
	*	*	
End Federation Partner 2			
End Federation Partners			

ISBN: 978-988-19251-3-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

E. *Translation of Claims or Identities*

Claims or identities are translated as indicated in the federation agreement. The STS store provides a record of necessary translations and performs these translations prior to the re-issuance of SAML tokens. For simple federation, where requests are across enterprise domains, there is no mapping, as the claims or identities are in the appropriate form already.

V. ACCESS CONTROL LIST (ACL) STORE

Each web service is provisioned with an ACL. ACLs are developed to permit claim holders access and privilege with a specific web service. They evolve over time and many organizations have input. The initial ACLs are specified by the organization that is the owner of the information. In order to make a comprehensive process for access claims, the conditions and rationale are stored in use cases. Use cases are the collection of attributes, roles and policies that provide a basis for service use and include access, authorities such as read/modify/write/delete, sharing restrictions and other permissions. Each set of factors represent a set of capabilities to be applied to a class of users. The name of the use case corresponds to one element of the ACL. The designation of an assignment to a job class with certain roles is sufficient in many cases. ACLs are stored in the EAS. The use cases are stored with other information in the service registration process describe the next section on the trusted attribute store. Table 3 provides the data elements for this area.

Table 3 Access Control Data

Data Element	Description	Comments
Claim 1	allows access	allow authorization
Claim 2	allows access	allow authorization
…	up to 512 attributes	allow authorization
Claim a	denies access	deny authorization
Claim b	denies access	deny authorization
…	up to 512 attributes	deny authorization

The web service contains an administrative interface to the service for maintenance of this data. The administrator is responsible for providing this file, together with ***Distinguished Names, X.509 certificates,*** use cases, Web Service Description Language (WSDL)s, XML Schema Description (XSD)s and other registration data in a separately stored media package that is electronically signed by the administrator.

VI. TRUSTED ATTRIBUTE STORE

The Enterprise Attribute Store (EAS) is the data repository of information that is used for authorization claims. It must gather data, compute claims, provide for delegation and provide claims information about entities to trusted and authorized requesters. In doing this it must meet all enterprise security requirements and processes.

A. *Data Gathering*

The EAS consists of multiple sets of information. It contains:

1. User attributes imported through guards from authoritative sources to the EAS.
   a. User information as to rank, job class assignment, training, assigned roles, and other material such as citizenship, birth date, clearance information, etc. This data is contained in several ADSs and is updated frequently. An agent triggers the import on demand, periodically, or when updates are made to the ADS.
   b. Enterprise Organizational structure – updated less frequently, but contains a definition of job classes in terms of roles and authorities. An agent triggers the import which occurs periodically, or when updates are made to the ADS.
2. A web service registry containing Distinguished Names, X.509 certificates, WSDLs XSDs, ACLs, use cases and other web service base information. These are imported from physical storage media provided by the web service administrator. The EAS administrator develops the rules for claim mappings and supplies them to the PBAC/ABAC Engine (see below) through a secure administrator interface.
3. A PBAC/ABAC Engine - a software service that examines the attributes of an active entity, use case information of a web service and enterprise policy into claims for use in SAML tokens.
4. Claims for each active entity based upon the PBAC/ABAC Engine.
5. Extended claims based on delegation.
6. A trusted STS store, which is replaced each time an enterprise STS is added or replaced. This store is used to validate STS requests through the STS interface. The input is electronically signed by the STS administrator. These are imported from physical storage media, by the EAS administrator through a secure administrator interface.
7. Additional inputs that may be required by policy inputs to the PBAC/ABAC Engine - these inputs need electronic signatures for action. These are imported from either physical or electronic storage media, by the administrator of the EAS through a special administrator interface. An example would be restricted access on certain days of the week to certain services needed for senior level reporting. This policy rule would require a trusted time input.

The data gathering is shown in Figure 3.

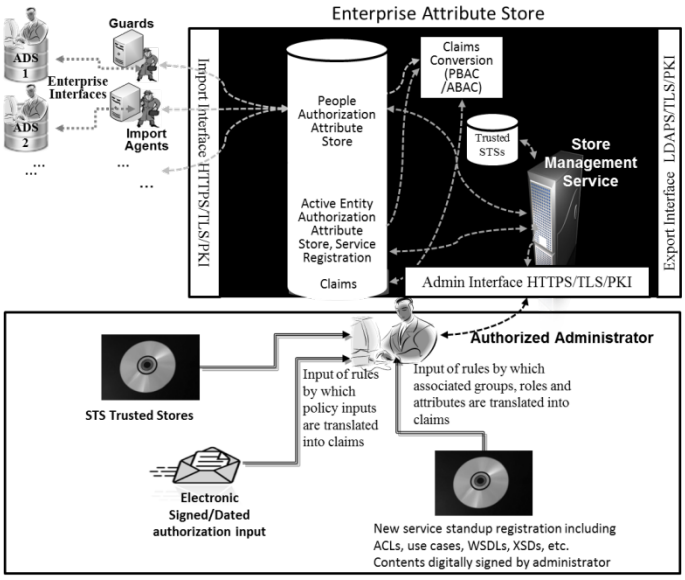

Fig. 3 Enterprise Attribute Store – Data Gathering

ISBN: 978-988-19251-3-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

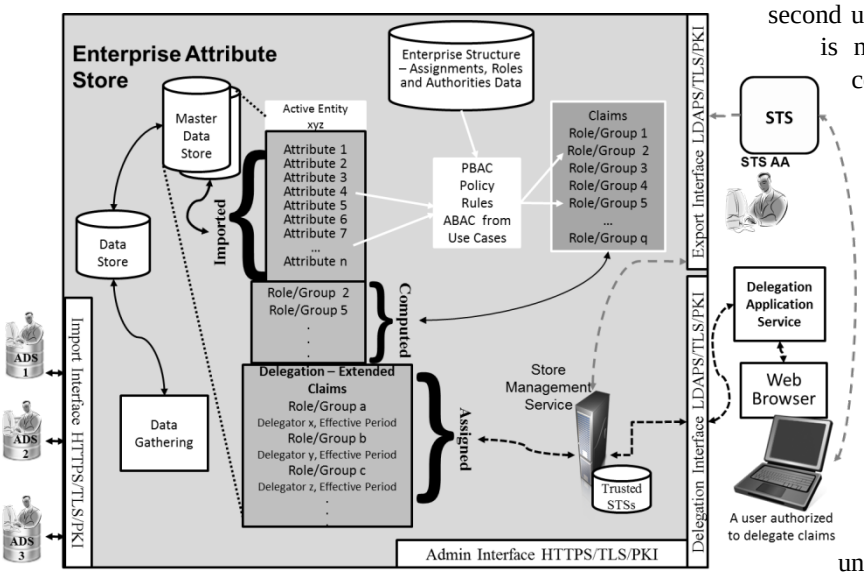

Fig. 4 Access to EAS and Delegation

B. *EAS Governance and Claims Computation*

The following steps are used to create an authorization process:

1. A change in Claims mapping is generated.
   - New service registration, providing use cases and ACLs.
   - A Policy change is forwarded to the configuration manager.
2. The EAS Configuration Manager maps these into rules for computing claims. He either does this manually or with the assistance of tools. The new rules are uploaded to the PBAC/ABAC Engine.
3. The Claims are computed and added to the claims store.
   - Roles, groups and claims are added to each active entity.
   - Expiration of appointments and/or reassignment of the individuals or any change of any attribute used in the claims process will require re-computing of claims for those active entities.
   - Changes in policy will require re-computing of claims.
   - Claims are generally approved for accessing individual services as needed to complete the service request. However, access requirements may change over time and any change to ACLs or use cases will require re-computing of claims.
4. When the requester does a Request for SAML Token (RST), the STS pulls the claims from the attribute store for the individual, places them in the SAML.
5. After authentication, the Web-application or Service parses the SAML retrieves the claims (roles and groups), compares these to the stored ACLs, and if a match is found, that person is allowed to establish a session with the Web-application or Service.
6. The attribute store grows and is extended as services and users are added.

A. *Providing for Delegation*

Delegation is the process by which Active Entity A can make a claim that normally is owned by Active Entity B. If the entity is a person, then delegation provides the claims that a user (Active Entity A) has been issued to a second user (Active Entity B) for the purpose of the second user making claims. The delegation service is not described in this paper due to space constraints.

B. *Providing Claims*

Claims are provided through an export interface which is restricted to a set of enterprise STSs, Web Services that provide web service links to the user and applications which require claims information. The process is shown in Figure 4.

VII. Trusted Security Token Server

An STS is a software service that meets the requirements listed below. Where specific requirements are to be met by the underlying software operating system and its hardware, these dependencies are documented and provided with the software. Security Token Service(s) (STS)s are established throughout the enterprise to issue SAML tokens to requesters as necessary to support authorization to SAML enabled services. SAML enabled services within the enterprise supports direct PKI-based user authentication. Transport Layer Security (TLS) is required for connections to the STS to provide confidentiality, preventing token capture or authentication replay attacks. The STS accepts requests from authenticated local requestors for SAML services.

The STS generates SAML tokens for the local requestor by communicating with the EAS and placing the requestor's claims in the SAML attributes section of the SAML token. The STS reduces these claims to the appropriate set of claims that can be used by the target application. The STS issues a SAML token that is digitally signed and includes an attribute statement (an attribute statement includes claims needed for access control). The STS accepts SAML tokens from foreign requesters, in accordance with defined federation agreements. The STS provides for the mapping of identities and claims when federation is required. The STS is an enterprise trusted software service and meets trust requirements including software vulnerability analyses and code protection. The STS has at least three interfaces as shown in Figure 5.

Interface 1. WS-Trust interface to accept Request for SAML Tokens. This (or a separate interface configured for this purpose [Alternate Interface]) is mediated to accept WS-Trust over HTTPS for web browser usage. This is used to request SAML tokens that contain the claims of the requester. In the case of HTTPS mediated requests the SAML is returned through the browser to the target provider. In the case of non-mediated requests, the SAML is returned to the requester.

Interface 2. WS-Federation interface to accept SAML tokens, test them against federation files and either return a re-issued SAML token or a message indicating failed authorization. This interface is used to initiate federation when the issuer of the SAML token is not recognized. The request includes the SAML token in question which is then checked against a federation list. If it is found to

ISBN: 978-988-19251-3-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

be a federation partner, a new SAML token is issued by the STS with any mappings required by federation. If the STS does not recognize the signature, then a failed authorization message is returned.

Interface 3. HTTPS interface for administration.

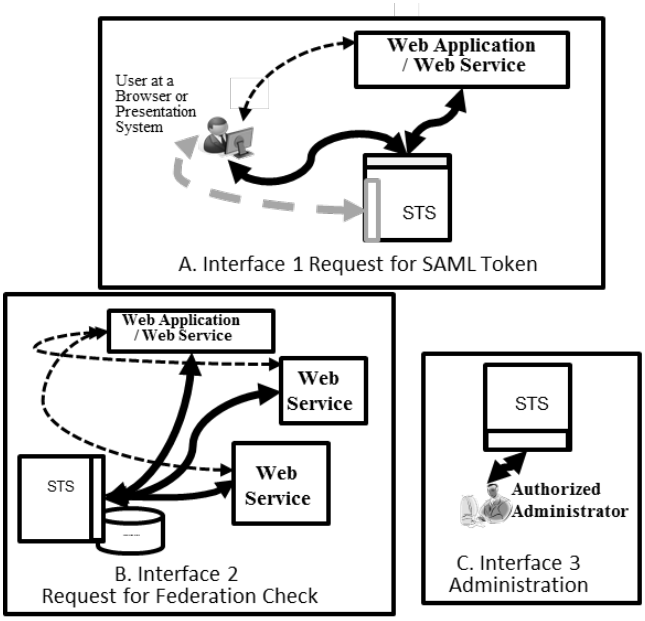

Fig. 5 STS Interfaces

VIII. SUMMARY

We have presented an enterprise level solution that has provided a consistent enterprise solution to access control. The solution is characterized by standards-based, local access control and authority decisions within the web-service. Many aspects of this architecture have been piloted and a full scale operational stand-up is currently in process. It is anticipated that this architecture will be more fully integrated at the enterprise level, more easily extended to future service offerings, and fully compatible with federated activities while maintaining a high assurance posture. To our knowledge, this is the first enterprise solution that does not use centralized access and policy enforcement points.

REFERENCES

[1]. World Wide Web Consortium (W3C):
a. "SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)", April 27, 2007.
b. W3C XML Schema Definition Language (XSD) 1.1 Part 1&2, 21 July 2011.
c. XML Encryption Requirements, 04 March 2002
d. XML Signature Syntax and Processing, 10 June 2008.
e. Web Services Description Language (WSDL) Version 2.0 Part 0-2, 26 June 2007.
f. Semantic Annotations for WSDL and XML Schema, 28 August 2007.
g. Web Services Architecture Requirements, 11 February 2004.
h. XHTML™ 1.1 - Module-based XHTML, 23 November 2010.

[2]. OASIS open set of Standards
a. N. Ragouzis et al., *Security Assertion Markup Language (SAML) V2.0 Technical Overview*, March 2008.
b. P. Madsen et al., *SAML V2.0 Executive Overview*, April 2005.
c. P. Mishra et al. *Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005.
d. S. Cantor et al. *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005.
e. S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005.
f. S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005.
g. F. Hirsch et al. *Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005
h. J. Hodges et al. *Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005.

[3]. Standard for Naming Active Entities on DoD IT Networks, Version 3.5, Sept. 23, 2010.

[4]. Federal Information Processing Standards Publication, FIPS PUB 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, May 25, 2001.

[5]. Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 3, July 2009.

[6]. Internet Engineering Task Force (IETF) Standards:
a. STD 66 (RFC3986) Uniform Resource Identifier (URI): Generic Syntax, T. Berners-Lee, R. Fielding, L. Masinter, January 2005
b. STD 9 (RFC0959) File Transfer Protocol, J. Postel, J. Reynolds, October 1985.
c. STD 5 (RFC0791) Internet Protocol, J. Postel, September 1981.
d. RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999.
e. *LDAPv3: Technical Specification*, **RFC 3377**, September 2002. *Authentication Methods for LDAP*. M. Wahl, H. Alvestrand, J. Hodges, R.L. Morgan. RFC 2829 May 2000.

[7]. Naming and Addressing: URIs, URLs, ..., Dan Connolly, Revision: 1.58 of 2006/02/27, Created 1993 by TimBL http://www.w3.org/Addressing/

[8]. Formally Assigned Uniform Resource Names (URN) Namespaces, Last Updated 2011-08-17, This is the Official IANA Registry of URN Namespaces, http://www.iana.org/assignments/urn-namespaces/urn-namespaces.xml

[9]. W. Yao, Fidelis: "*A Policy-Driven Trust Management Framework*", Lecture Notes in Computer Science 2692 (2003) 301-317.

[10]. J. Bacon , K. Moody , W. Yao, "*A Model of OASIS Role-Based Access Control and Its Support for Active Security*", ACM Transactions on Information and System Security (TISSEC) 5 (2002) 492-540.

[11]. R. Sandhu, Q. Munawer, "*The ARBAC99 Model for Administration of Roles*", Proceedings of the 15th Annual Computer Security Applications Conference, December 06-10, 1999, p.229.

[12]. C. Goh, A. Baldwin, "*Towards a More Complete Model of Role*", Proceedings of the 3rd ACM Workshop on Role-Based Access Control, Fairfax, Virginia, United States, 1998, pp.55-62.

[13]. R.S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman, "*Role-Based Access Control Models*", Computer 29 (1996) 38-47.

[14]. J. Wainer, A. Kumar, P. Barthelmess, "DW-RBAC: a formal security model of delegation and revocation in workflow systems", Information Systems 32 (2007) 365-384.

[15]. R. Fagin, "On an authorization mechanism", ACM Transactions on Database Systems (TODS) 3 (1978) 310-319.

[16]. William R. Simpson, Coimbatore Chandersekaran and Andrew Trice, The 1st International Multi-Conf. on Eng. and Tech. Innovation, *"Cross-Domain Solutions in an Era of Information Sharing"*, Volume I, pp.313-318, *Orlando, FL., June 2008*.

[17]. Coimbatore Chandersekaran and William R. Simpson, World Wide Web Consortium (W3C) Workshop on Security Models for Device APIs, *"The Case for Bi-lateral End-to-End Strong Authentication"*, 4 pp., London, England, December 2008.

[18]. William R. Simpson and Coimbatore Chandersekaran, 2nd International Multi-Conference on Engineering and Technological Innovation, Volume I, pp. 300-305, *"Information Sharing and Federation", Orlando, FL., July* 2009.

[19]. Coimbatore Chandersekaran and William R. Simpson, The 16th International Command and Control Research and Technology Symposium: CCT2011**,** Volume II, pp. 84-89, *"An Agent Based Monitoring System for Web Services"*, Orlando, FL., April 2011.

[20]. William R. Simpson and Coimbatore Chandersekaran, 1st International Conference on Design, User Experience, and Usability, part of the 14th International Conference on Human-Computer Interaction (HCII 2011), *"A Multi-Tiered Approach to Enterprise Support Services"*, 10pp, Orlando, FL., July 2011.

[21]. William R. Simpson, Coimbatore Chandersekaran and Ryan Wagner, Lecture Notes in Engineering and Computer Science, Proceedings World Congress on Engineering and Computer Science 2011, Volume I, *"High Assurance Challenges for Cloud Computing"*, pp. 61-66, San Francisco, October 2011.

ISBN: 978-988-19251-3-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)