A SAML Framework for Attribution, Delegation and Least Privilege[1]

By
Coimbatore S. Chandersekaran
William R. Simpson
Institute for Defense Analyses, 4850 Mark Center Dr.
Alexandria, Virginia 22311

[1] 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.

ABSTRACT

Delegation, Attribution and Least Privilege are an implicit part of information sharing. In operating systems like Windows there is no security enforcement for code running in kernel mode and therefore such code always runs with maximum privileges. The principle of least privilege therefore demands the use of a user mode solutions when given the choice between a kernel mode and user mode solution if the two solutions provide the same results. Discussions in this paper will be restricted to OSI model levels five and above. This paper describes the SAML delegation framework in the context of a large enclave-based architecture currently being implemented by the US Air Force. Benefits of the framework include increased flexibility to handle a number of different delegation business scenarios, decreased complexity of the solution, and greater accountability with only a modest amount of additional infrastructure required.

Keywords: Delegation, enterprise, information security, least privilege, attribution, information sharing.

TYPES OF DELEGATION

Person to Person Delegation

Delegation is the handing of a task over to another person, usually (although not limited to) a subordinate. It is the assignment of authority and responsibility to another person to carry out specific activities. It allows a subordinate to make decisions, i.e. it is a shift of decision-making authority from one organizational level to another one. This form of delegation is not treated in this paper. A compatible treatment of this delegation is included in [1].

Person and Service to Service Delegation

Delegation is implicit when invoking a service. In the Air Force enterprise an individual is assumed to delegate to a service the right to act upon its behalf. Further, it is assumed that any service invoking another service is delegating its authority to complete whatever portion of the service it has been authorized to perform. Delegation for a service is transitive and not personal. Delegation only lives during the session under consideration.

Attribution is provided when the service exercising privilege is identified as acting on behalf of the requestor who (implicitly) authorized the delegation.

Least Privilege is preserved by providing the agent with only that level of privilege necessary to do the task without exceeding his/her own authority.

PURPOSE

This paper will define the elements and process required for delegation, attribution and least privilege. The Air Force Enterprise Architecture provided in the reference[2] (not available to all) is assumed, particularly the use of a Security Token Server, credentialing of all active entities, and the use of SAML 2.0 for authorization.

[2] Air Force Information Assurance Enterprise Architecture, Version 1.25, SAF/XC, 11 April 2008.

SECURITY ENVIRONMENT

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. This Omni-present threat leads to a healthy paranoia of resistance to observation, intercept and masquerading. Despite this attack environment, the web interface is the best way to provide access to many of its users. 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.

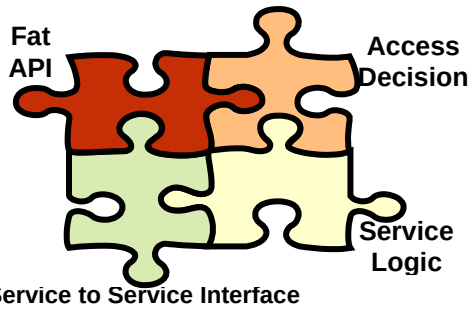

Figure 1 Components of a Service

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. In the Figure 1 we show the constituent makeup of a service.

The FAT API must be plug compatible with the Fat Browser and the Service-to Service Interface as shown in Figure 2. It is therefore important that these exercise compatible code segments.

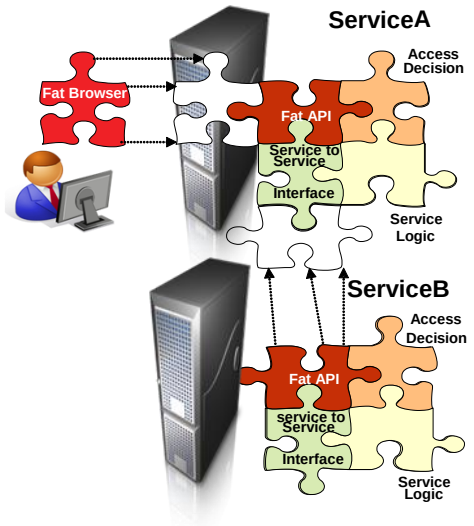

Figure 2 Fat Interfaces Must be Plug Compatible

In the Figure 3 we show two types of Services. The first is an Aggregation Service. This Service calls exposure services aggregates their output and returns the data to the user. The second is an Exposure Service that provides data from an authoritative data source. The "fat" Service call is different between services than between browser and service. The "fat" APIs will also be different for different environments (e.g., .NET or J2EE). The "fat" part of the API consists of:

- Port Listener
- (save data input)
- Bi-lateral End-to-End Authentication
- Consume the assertion package for authorization
- Pass Authorization credentials and input to the service

The initiating part on the "Fat" Browser and the Service-to-Service invocation must meet the compatibility issues. 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.

DELEGATION WHEN SERVICES ARE INVOLVED

Service delegations have the following assumptions:

User based requests:

- A request for service within the AF enterprise is an *implicit* request to a service provider to do what you are allowed to on my behalf to satisfy this request.
- Group/Role definition is fine grained enough to signify access throughout the process.

Service based requests:

- A request for service within the enterprise is an *explicit* request to a downstream service provider to do what you are allowed to on my behalf to satisfy this request.
- Group/Role definition is fine grained enough to signify access throughout the process.

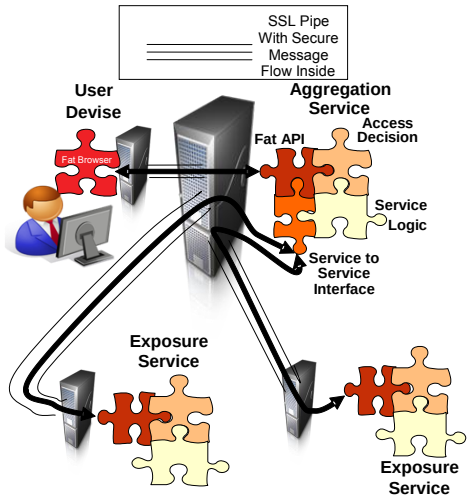

Figure 2 Steps in Invoking an Aggregation Service

- Non-aggregation services are atomic.

Other

- Only considering web-service calls above OSI level 4.
- Calls below level 5 on the OSI stack are not made by SAML authorization and do not follow this paradigm.

BASIC USE CASE

The basic use case is given in the Figure 4 and involves a user invoking an aggregation service which in turn invokes aggregation and other services.

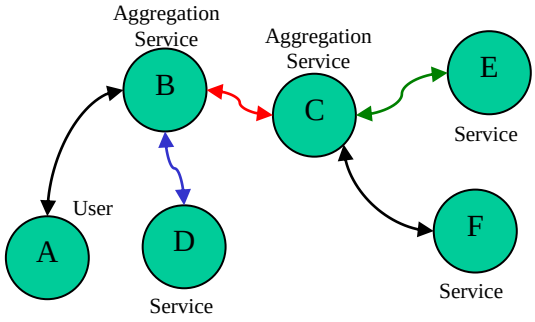

Figure 4 Use Case for Service Delegation

Communication for Authentication/Authorization

Each communication link in Figure 1 will be authenticated end-to-end with the X.509 certificates provided for each of the active entities. Authorization will be based upon the Security Assertion Markup Language (SAML)[3]. The delegation, attribution and least privilege will be handled by modification to the SAML token provided by the STS. The SAML token for user A to aggregation Service B is provided in the Table 1 below:

PRUNING ATTRIBUTES[4]

An individual or service requesting another service may contain many elements that are not relevant to the service request. This makes the SAML request overly large, increases the cycles for SAML consumption and

[3] SAML is based upon the Oasis series of standards for web services, specifically in our case SAML 2.0

[4] Since authorization decisions may require any of a combination of attributes, groups, and/or roles, these will be referred to generically as elements in the rest of this chapter.

evaluation may introduce additional latency and is a potential source for escalation of privilege. In order to combat these factors, the attribute assertion should be reduced to the minimum required to accomplish the service request.

Table 1 SAML 2.0 Format for User Request

Item	Field Usage	Recom-mendation	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**	**May be pruned for least privilege**
Conditions			
NotBefore	**Yes**	**Required**	**TimeStamp - minutes**
NotAfter	**Yes**	**Required**	**TimeStamp + minutes**
OneTimeUse	**Yes**	**Required**	**Mandatory**

REQUIRED ESCALATION OF PRIVILEGE

Certain services may require privilege beyond that of the original client. Examples include the Security Token Server (STS) that when called is expected to have access to the Active Directory (AD) and UDDI, even when the client does not have such privilege. An additional example would include payroll services that can provide average values without specifics. The service must be able to access all records in the payroll data base, even if the client it is acting on behalf of does not have this privilege. For purposes of this methodology, these required elements will be dealt with separately in both data pruning and service to service calls. Service developers should take care that the required escalation of privilege is required and that the newly aggregated data do not impose additional access restrictions. The data that has been aggregated and synthesized should be carefully scrutinized for such sensitivities. The process is not unlike the combining of data from multiple unclassified but sensitive data sources that may rise to a higher classification level when they are all present in one place.

DATA REQUIREMENTS - PRUNING ELEMENTS

In order to accomplish the reduction of the SAML assertion, the STS must know the target and the elements that are important to the target. Table 2 below presents such a data compilation. This table will be used in the subsequent example. An element is an attribute, role or group used in the authorization decision.

Table 2 Group and Role Pruning Data Requirement

Service	Uri	Relevant Attributes, Groups and Roles	Escalation of Privilege Required
AFPersonnel30	**…//afnetdol.pers.af23:622**	**Element1, Element3, Element4, Element5, Element6**	**Element6**
PERGeo	**…//afnetdol.perst.af45:543**	**Element4, Element5, Element6**	**Element6**
PerReg	**…//afnetdol.persq.af45:333**	**Element4**	
PerTrans	**…//afnetdol.persaw.af45:21862**	**Element6**	
BarNone	**…//afnetdol.persaxc.af45:1234**	**Element5**	
DimrsEnroll	**…//afnetdol.persws.af45:23567**	**Element1, Element3**	
…	**…**	**…**	
Endfile			

The combining of these elements is given for calling step i by:

Let N_{i+1}=New SAML Elements for i to call i+1
Let P_i = Prior Elements
Let R_{i+1}= Service Required Elements
Let H_i = Service Held elements
Let E_i = Required Escalation Elements

Then: $N_{i+1} = (P_i \cap (R_{i+1} \cap H_i)) \cup (E_i \cap R_{i+1})$

Where: $\cap$ is the intersection of sets and $\cup$ is the union of sets, $\acute{O}$ is the empty set (no members)

The formula may be read as the common elements in the prior SAML and the intersection of the held elements and those required by the next call ($(Pi \cap (R_{i+1} \cap H_i)$) - normal least privilege). These are added ($\cup$) to the required escalation elements that are required to be extended by the next call ($(E_i \cap R_{i+1})$ - extended least privilege by escalation of privilege). The initial call has no prior elements and P_1 is defined as the initial set of privilege elements. This reduces N_1 to $H_0 \cap R_1$ (Normal least privilege).

Subsequent Calls Require Saving the SAML Assertion

After the SAML is consumed and authorization is granted, the service must retain the SAML Attribute Assertion (Part of the Larger SAML Token) above. Specifically, the subject fields and the elements field to be used in further authorization. The specific instance is shown in Table 3.

Table 3 Retained Portion of SAML Token

Attribute Assertion			
Subject	**Yes For User A**	**EDIPI**	**For Attribution**
Attributes, Group and Role Memberships	**Yes For User A**	**Required**	**Mask for follow-on least privilege**

SAML Token Modifications for Further Calls

The Attribute Assertion of Table 3 is returned to the STS for modification of the normal SAML token. The SAML Token for the unmodified service call is given below:

Table 3 Unmodified SAML for Service B of Use Case

Item	Field Usage	Recom-mendation	Notes
SAML Response			
Version ID	**Version 2.0**	**Required**	
ID	**(uniquely assigned)**	**Required**	
Issue Instant	**Time-stamp**	**Required**	

Item	Field Usage	Recom-mendation	Notes
Issuer	Yes	Required	STS Name
Signature	Yes	Required	STS Signature
Subject	Yes For Service B	Required	Must contain the X.509 Distinguished name or equivalent
Attribute Assertion			
Subject	Yes For Service B	Cn for Service B	For Attribution
Attributes, Group and Role Memberships	Yes For Service B	Required	$N_{i+1} = (P_i \cap (R_{i+1} \cap H_i)) \cup (E_i \cap R_{i+1})$
Conditions			
NotBefore	Yes	Required	TimeStamp - minutes
NotAfter	Yes	Required	TimeStamp + minutes
OneTimeUse	Yes	Required	Mandatory

The Attribute Assertion is modified in the following way.

- The subject is modified to read "Service A OnBehalfOf" the returned SAML subject which in this case is the EDIPI (Electronic Data Interchange Personnel Identifier) of the user.
- The attribute, group and role membership (elements) are modified to include only elements that appear in both the Service B registry and the returned SAML Attribute Assertion.
- The modified SAML Token is provided in Table 4 below:

Table 4 Modified SAML Attribute Assertion for Further Calls

Item	Field Usage	Recom-mendation	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 Service B	Required	Must contain the X.509 Distinguished name
Attribute Assertion			
Subject	Yes contains A and B	Cn B OnBehalfOf EDIPI	For Attribution
Attributes, Group and Role Memberships	Yes B restricted by A	Required	$N_{i+1} = (P_i \cap (R_{i+1} \cap H_i)) \cup (E_i \cap R_{i+1})$
Conditions			
NotBefore	Yes	Required	TimeStamp - minutes
NotAfter	Yes	Required	TimeStamp + minutes
OneTimeUse	Yes	Required	Mandatory

Subsequent calls from Service A would use the modified token. Further, the subsequent service called would save the SAML Attribute Assertion for its further calls.

AN ANNOTATED NOTIONAL EXAMPLE

A User in the AFNETOPS Forest (Ted.Smith1234567890) through discovery finds the dashboard service on Air Force Personnel (AFPersonnel30) that he would like to invoke. The discovery has revealed that access is limited to users with Element1, Element3, Element4, Element5 or Element6, but that users without all of these authorizations may not receive all of the requested display. Ted does not have all of the required Elements, but is authorized for personnel data within CONUS and has Element membership in Element 1, Element 2, Element 3, Element 4, Element 7, and Element 12 + 27 other Elements not relevant. The AFPersonnel30 will typically display the following dashboard on Air Force Personnel:

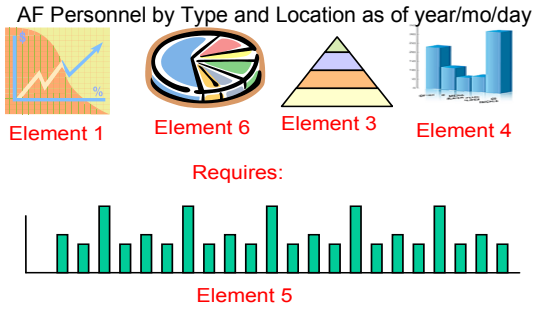

Figure 5 AFPeronnel30 with Display Outputs

The elements required would not typically be displayed. A partial calling tree for AFPersonnel30 is provided in Figure 6. The widgets that form the presentation graphics have not been included, but would be part of the calling tree, they do not have access requirements that modify the example and have been deleted for reduction of complexity. In the figure we show the elements that make up the privilege for each service (holds) and the elements required for access to the service (requires). This data is linked to Table 2, and must be synchronized with it. The element privileges for services without subsequent calls are unimportant, and many additional groups may be present but will be pruned on subsequent calls.

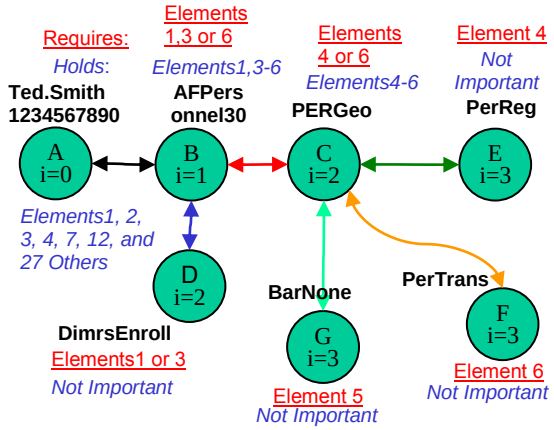

Figure 6 AFPersonnel30 Calling Tree

Note that each link in the calling graph requires bi-lateral authentication using certificates provided as credentials to each of the active entities, followed by the push of a SAML token for authorization. The first such token is presented in Table 5:

Table 5 Ted Smith SAML Push to AFPersonnel30

Item	Field Usage
SAML Response	
Version ID	Version 2.0
ID	0qwdrt009kkmn
Issue Instant	080820081943
Issuer	AFNETOPS STS12345
Signature	Lkhjsfoioiunmclscwl879ooeeujl99vcd78ffgg3422ft…
Subject	CN = TED.SMITH1234567890, OU = CONTRACTOR, OU = PKI, OU = DOD, O = U.S. Government, C = US
Attribute Assertion	

Item	Field Usage
Subject	**TED.SMITH1234567890**
Attributes, Group and Role Memberships	**Element1, Element3, Element4**[5] $N_1 = (R_2 \cup H_1)) \cup (E_1 \cap R_2)$ =((1, 2, 3, 4, 7, 12, +27)∩((1,3-6) = (1,3,4)) **=((Element1, Element3, and Element4))**
Conditions	
NotBefore	**080820081933**
NotAfter	**080820081953**
OneTimeUse	**Yes**

The Attribute Assertion Section is saved for subsequent calls. The call from AFPersonnel30 to service PERGeo will look like Table 6.

Table 6 AFPersonnel30 SAML Push to PERGeo

Item	Field Usage
SAML Response	
Version ID	**Version 2.0**
ID	**0qwdrt009kkmn**
Issue Instant	**080820081944**
Issuer	**AFNETOPS STS12345**
Signature	**Lkhjsfoioiunmclscwl879ooeeujl99xfg654bbgg34lli…**
Subject	**CN = e3893de0-4159-11dd-ae16-0800200c9a66, OU=USAF, OU=PKI, OU=DOD, O=U.S. GOVERNMENT, C=US**
Attribute Assertion	
Subject	**AFPersonnel30 OnBehalfOf TED.SMITH1234567890**
Group and Role Memberships	**Element 4**[6], **Element6**[7] $N_{i+1} = (P_i \cap (R_{i+1} \cap H_i)) \cup (E_i \cap R_{i+1})$ =((1, 3, 4) ∩ (4 ∩ 4-6) ∪ (6 ∩ 4-6) =((1, 3, 4) ∩ (4)) ∪ (6) =(4,6) + Elementt 4 and Element 6
Conditions	
NotBefore	**080820081934**
NotAfter	**080820081954**
OneTimeUse	**Yes**

The SAML Attribute Assertion is where the work is done. The subject has been modified to include the names of the calling tree and the Elements have been pruned to include only common items between the calling elements in the tree. Figure 7 shows the completion of the calling tree, including only the SAML Attribute Assertions in the blocks below.

Note that the calls to BarNone fails access (SAML does not contain required element 5) and while being stealth to the calling routine (which will return with no data after timeout) this failure will trigger alarms to SOA management monitors as follows:
Failed authorization (BarNone) attempt PERGeo on behalf of AFPersonnel30 on behalf of Ted.Smith1234567890 No data returned

The returned dashboard (without the element requirement annotations) is presented in Figure 8. Note that Element 6 privilege was provided by service escalation.

[5] An element is an attribute, role, group or combination of the previous. Elimination of Element 2, Element 7, Element 12 and 27 other elements based on pruning (see Table 5 under AFPersonnel30)
[6] An element is an attribute, role, group or combination of the previous. Elimination of Element 1 and Element 3 based on pruning (see Table 5 under PERGeo)
[7] Element 6 is a required escalation element.

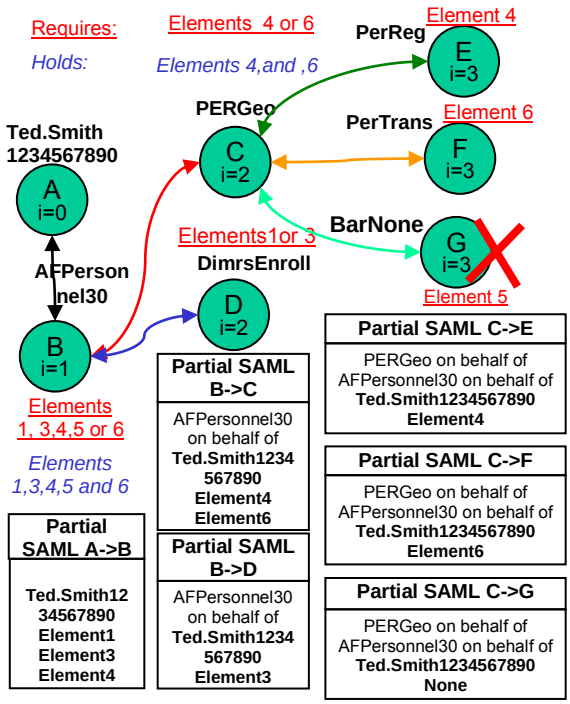

Figure 7 SAML Attribute Assertion of the Calling Tree

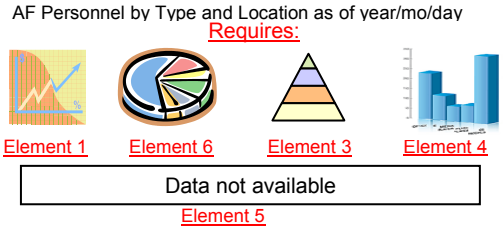

Figure 8 Dashboard Service AFPersonnel30 Case Result (with Annotation)

Additional Requirements on the STS and Services

The STS requirements are given in Table 7 below:

Table 7 STS Additional Requirements

Item	Requirement	Data Structure Required
Element Pruning by individual service call	Least Privilege reduction of Attributes, Groups and Roles in SAML Assertion	Yes, table of service attribute, group and role requirements for access. Must be synchronized with access managers.
Receive prior SAML Assertion	Need subject, attributes, groups and roles for further attribution and group definition	Internal only no external store required.
Apply prior SAML assertion to SAML	Includes modification of subject line in assertion as well as further pruning of elements	Internal only no external store required.

The additional requirements on the Services are given in Table 8 below:

Table 8 Service Additional Requirements

Item	Requirement	Data Structure Required
Hold SAML Assertion	Required only when subsequent service calls are to be performed on behalf of the requestor	Internal only no external store required, but must be held on a per thread basis

Item	Requirement	Data Structure Required
Send Prior SAML Assertion	When subsequent service calls are made.	Internal only no external store required, but must be transmitted on a per thread basis
Use Subject of SAML Assertion in Logs	Attribution Requirement	Log files in existence
Purge held SAML Assertion	When thread is complete.	none

Service Use Case Summary

The process of using SAML token modification for tracking of delegation, attribution and least privileges has both advantages and disadvantages.

Advantages

- Use of SAML standard without extension or violation
- Full attribution for data analyses and forensics.
- Least privilege is invoked on service to service calls
- Aggregation service does not need to filter response to user based on access credentials
- Federation works exactly the same way
- Peron-to-Person delegation compatible

Disadvantages

- Use of SAML standard in an way that SAML standard writers did not anticipate
- Service must store and covey SAML assertion invoking the thread
- STS currently does not process this data

REFERENCES

[1]. Simpson, William R., and Chandersekaran, Combinatore, The 8th International Conference on Computing, Communications and Control Technologies: CCCT 2010 , *"A Persona Framework for Attribution, Delegation, and Leas6t Privilege",* April 2010, *To Be Published*

[2]. Liu Air Force Information Assurance Strategy Team, *Air Force Information Assurance Enterprise Architecture*, Version 1.25, SAF/XC, 11 April 2008.

[3]. Air Force Information Assurance Strategy Team, *Federation*, Version 0.5, SAF/XC, 5 August 2008.

[4]. AFPD 33-3 Information Management, AF Portal Community of Practice: AF Information & Data Management Strategy – Implementation (Policy) https://wwwd.my.af.mil/afknprod/ASPs/CoP/OpenCoP.asp?Filter=OO-SC-AF-DM or http://www.e-publishing.af.mil/

[5]. COI Coordination Panel Charter, AF Portal Community of Practice: AF Information & Data Management Strategy – Implementation (COI Primer) https://wwwd.my.af.mil/afknprod/ASPs/CoP/OpenCoP.asp?Filter=OO-SC-AF-DM

[6]. COI Primer, AF Portal Community of Practice: AF Information & Data Management Strategy – Implementation (COI Primer) https://wwwd.my.af.mil/afknprod/ASPs/CoP/OpenCoP.asp?Filter=OO-SC-AF-DM

[7]. DoD Directive 8320.2 "Data Sharing in a Net-Centric Department of Defense" and DOD Guidance 8320.2-G "Guidance for Implementing Net-Centric Data Sharing", AF Portal Community of Practice: AF Information & Data Management Strategy – Implementation (Policy) https://wwwd.my.af.mil/afknprod/ASPs/CoP/OpenCoP.asp?Filter=OO-SC-AF-DM

[8]. Metadata Concept, AF Portal Community of Practice: AF Information & Data Management Strategy – Implementation (Metadata) https://wwwd.my.af.mil/afknprod/ASPs/CoP/OpenCoP.asp?Filter=OO-SC-AF-DM

[9]. Transparency Integrated Product Team (TIPT) information and proceedings AF Portal Community of Practice https://wwwd.my.af.mil/afknprod/ASPs/CoP/OpenCoP.asp?Filter=OO-TR-AF-39

[10]. Air Force Instruction (AFI) 31-501, Personnel Security Program Management

[11]. AFI 33-115, Network Management and Licensing Network Users and Certifying Network Professionals

[12]. AFI 33-119, Electronic Mail (E-mail) Management and Use

[13]. AFI 33-202, Computer Security

[14]. AFI 33-204, Information Protection Security Awareness, Training, and Education (SATE)

[15]. AFMAN 33-223, Identification and Authentication

[16]. AFMC Supplement 1, AFMAN 33-223, Identification and Authentication

[17]. CJCSI 3170.01E, Joint Capabilities Integration and Development System

[18]. CJCSI 6212.01D, Interoperability and Supportability of Information Technology and National Security Systems

[19]. DoDD 5000.1, The Defense Acquisition System

[20]. DoDD 4630.5, Interoperability and Supportability of Information Technology and National Security Systems

[21]. DoDD 8000.1, Management of DoD Information Resources and Information Technology

[22]. DoDD 8115.01, "DoD Information Technology Portfolio Management," October 10, 2005

[23]. DoDD 8115.1, Information Technology Portfolio Management

[24]. DoDD 8500.1, lnformation Assurance (IA), 24 OCT 02

[25]. DoDD 8530.1, Computer Network Defense (CND), 8 Jan 2001

[26]. DoDI 4630.8, Procedures for Interoperability and Supportability of Information Technology and National Security Systems

[27]. DoDI 5000.2, Operation of the Defense Acquisition System

[28]. DoDI 8500.2, Information Assurance Implementation, 6 FEB 03

[29]. DoDI 8520.2, Public Key Infrastructure (PKD and Public Key (PK) Enabling, 1 APR 04

[30]. DoDI 8115.02, "Information Technology Portfolio Management Implementation", October 30, 2006

[31]. JTF-GNO CTO 06-02, Tasks for Phase I of PKl Implementation, 17 JAN 06

[32]. DoD/CIO Memo, Approval of the Alternate Logon Token, 14 AUG 06

[33]. JTF-GNO WARNORD 07-37, Public Key Infrastructure Implementation, Phase 2, August 2007

[34]. The National Defense Strategy of the United States of America, March 2005

[35]. Department of Defense Net-Centric Data Strategy, May 9, 2003

[36]. Joint Concept of Operations for Global Information Grid NetOps, Version 3, August 4, 2006

[37]. OASIS open set of Standards (see Endnote)

[38]. "Guide to Secure Web Services: Recommendations of the National Institute of Standards and Technology", NIST-US Department of Commerce Publication, August 2007.

[39]. "Web Service Security: Scenarios, Patterns, and Implementation Guidance for Web Services Enhancements (WSE) 3.0", Microsoft Corporation, 2005

[40]. "WS-ReliableMessaging Specification", OASIS, June 2007

[41]. "WS-SecureConversation Specification", OASIS, March 2007

[42]. "WSE 3.0 and WS-ReliableMessaging", Microsoft White Paper, June 2005, http://msdn2.microsoft.com/en-us/library/ms996942(d=printer).aspx

[43]. FIPS PUB 196, Federal Information Processing Standards Publication. "Entity Authentication Using Public Key Cryptography", February 18, 1997

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
January 2010	Study	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A SAML Framework for Attribution, Delegation and Least Privilege	DASW01-04-C-0003
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Coimbatore S. Chandersekaran William R. Simpson	5e. TASK NUMBER C5127
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	IDA Nonstandard Document NS D-4170 Log no. 10-001006

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
	IDA
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution unlimited: 16 February 2010.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Delegation, Attribution and Least Privilege are an implicit part of information sharing. In operating systems like Windows, there is no security enforcement for code running in kernel mode and therefore such code always runs with maximum privileges. The principle of least privilege therefore demands the use of a user mode solution when given the choice between a kernel mode and user mode solution if the two solutions provide the same results. Discussions in this paper will be restricted to OSI model levels five and above. This paper describes the SAML delegation framework in the context of a large enclave-based architecture currently being implemented by the US Air Force. Benefits of the framework include increased flexibility to handle a number of different delegation business scenarios, decreased complexity of the solution, and greater accountability with only a modest amount of additional infrastructure required.

15. SUBJECT TERMS

Delegation, enterprise, information security, least privilege, attribution, information sharing

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
Unclassified					Dr. William R. Simpson
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include Area Code)
Unclass	Unclass	Unclass	Unlimited	6	(703) 845-6637