# Information Sharing and Federation[1]

Combinatore Chanderasekaran
Institute for Defense Analyses, 4850 Mark Center Dr.
Alexandria, Virginia 22311

William 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

Department of Defense (DoD) policy requires the Air Force to share information among authorized users both within the Air Force and across the Defense enterprise where a need and agreement are established – as the normal mode of operation for the business and warfighting mission areas. This paper defines the elements required for federation. Federation communication will be undertaken whenever communication is cross-forest within the Air Force Enterprise, and when communicating with other enterprises by a specific federation agreement.

**Keywords:** Federation, enterprise, information security, authentication, authorization, SAML, information sharing

## INTRODUCTION

No services, delayed services, inadequate services and poor information flow all hinder or prevent information sharing as the normal mode of operations. Information sharing requires availability, performance, integrity, and reliability.

- Availability – covers the traditional aspects of being there when needed, but in this information sharing environment it also means discovery and accessibility. The later derives from the metadata environment (MDE) environment being built into the Integrated Information Baseline (IIB) and extensive monitoring will be devoted to MDE services.
- Performance – information delayed is information denied. Excessive latency will not be tolerated and the need to share has a time component as well as an authoritative and currency component. The communities of interest (COIs) address authority and currency, and the network will monitor the performance aspects. Performance includes latency, bottlenecks, and saturation.
- Integrity – covers correct handling, tamper resistance and awareness, authorization, and authentication. The information assurance (IA) architecture addresses most of these elements. For federation, this step is particularly important.
- Reliability – covers the ability to complete delivery of information, fail-over, continuity of operations (COOP) and backup of critical information. Many of these elements are hardware related and are addressed through hardware monitoring and redundancy of hardware, software and data. Fail-over may be a management function when provisions are made for state tracking and re-direct when hardware and software failures occur.

## TOP LEVEL TENETS

Any service management solution for the enterprise (and indeed, any solution for any component of the enterprise) should be tested against a set of fundamental evaluation criteria or tenets. These tenets are separate from the “functional requirements” of a specific component (e.g., access control needs to be defined); they relate more to the attributes of the solution that make it able to be implemented, extensible, cost-effective, and supportive of the fundamental objectives of the enterprise. Our proposed top-level tenets are the following:

- The **zeroth** tenet is that the *enemy is embedded*. Current threat evaluation indicates that at the unclassified and NIPRNet [Unclassified but Sensitive Internet Protocol Router Network] level, attacks are often successful, and discovery and ferreting out the results of these attacks is difficult and problematic at best.
- The **first** tenet is *simplicity*. At a certain point (usually a lower point than you would suspect), added features come at the cost of greater complexity, less understandability, greater difficulty in administration, higher cost, and/or lower adoption rates that are unacceptable to the organization. Therefore, simplicity absolutely must be a primary goal of any access solution. That being said, there is a level of complexity that must be handled for security purposes and implementations should not overly simplify the problem for simplicity’s sake.
- The **second** tenet, and closely related to the first is *extensibility*. Any construct we put in place for an enclave should be extensible to the forest and the enterprise, and ultimately to cross-enterprise and coalition. It is undesirable to work a point solution or custom approach for any of these levels.
- The **third** tenet is *information hiding*. Essentially, information hiding involves only revealing the minimum set of information to the outside world needed for making effective, authorized use of a capability.
- The **fourth** tenet is *accountability*. In this context, accountability means being able to definitively identify and track what entity in the enterprise performed any particular operation (e.g., accessed a file or IP address, invoked a service). To enable accountability, it is necessary to prohibit online “impersonation,” in which principals share their credentials with another actor rather than delegating their authority. Without a delegation model, it is impossible to establish a chain of custody or do effective forensic analysis to investigate security incidents.
- This **fifth** tenet is *minimal detail* (to only add detail to the solution to the required level). This combines the principles of simplicity and information hiding, and preserves flexibility of implementation at lower levels.
- The **sixth** is the emphasis on a *service-driven* rather than a product-driven solution whenever possible. Using services makes possible the flexibility, modularity, and composition of more powerful capabilities.

- The **seventh** and final tenet is that *lines of authority* should be preserved and IA decisions should be made by policy and/or agreement at the appropriate level.

## COMMUNICATION ACROSS 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 Security Assertion Markup Language (SAML) packages for authorization. The communication between a user in his forest and a service in another forest is shown in Figure 1.

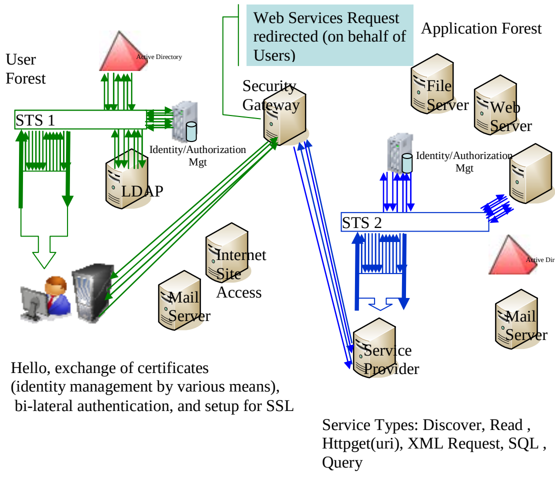
Web Services Request redirected (on behalf of Users)
Application Forest
User Forest
Active Directory
Security Gateway
File Server
Web Server
STS 1
Identity/Authorization Mgt
LDAP
Identity/Authorization Mgt
STS 2
Internet Site Access
Mail Server
Active Directory
Mail Server
Service Provider
Hello, exchange of certificates
(identity management by various means),
bi-lateral authentication, and setup for SSL
Service Types: Discover, Read ,
Httpget(uri), XML Request, SQL ,
Query

**Figure 1 Cross-Forest Authentication**

Once the authentication is completed, an SSL is established between the user and the service provider, within which a Web Service (WS) Security package will be sent to the service. The WS Security package contains a SAML token generated by the STS 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.

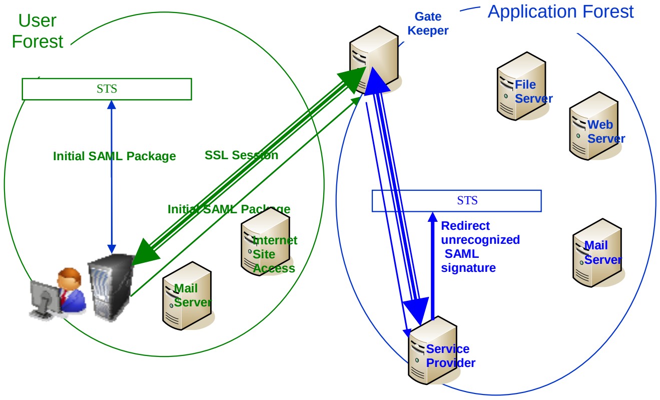

**Figure 2 Request for SAML Package**

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.

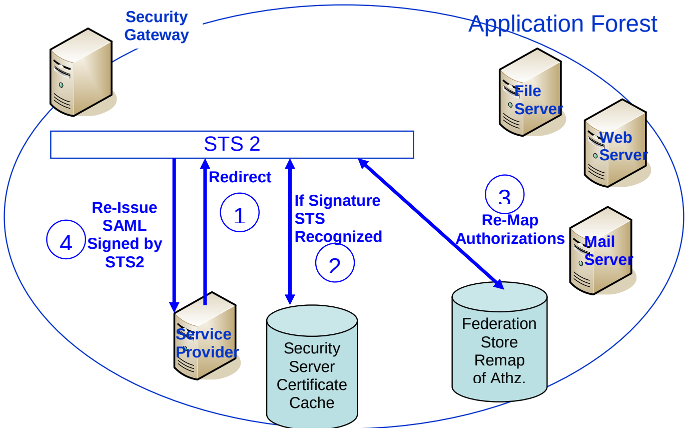

**Figure 3 SAML Rework Requirements**

The resolution takes place in several distinct steps:

1. The first step is the redirect to the local STS.
2. The local STS then tries 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 federation store map, which has translation of groups and roles as well as any restrictions mandated 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 for each such server.
    - A set of identity-mapping tuples with the form identity1, intentity2 where *,* indicates no further remapping required.
    - A set of mapping tuples of the form groupa, groupb where *,* indicates no further remapping required.

The basic form is shown in the following table:

**Table 1 Federation Data Requirements**

| | | | |
|---|---|---|---|
| Federation Partner 1 | | Federation Public Key | |
| Identity Block | Identity 1 | Identity 2 | |
| | Identity A | Identity B | |
| | … | … | |
| | * | * | |
| Group Mapping Block | | Group1 | Group 2 |
| | | Group A | Group B |
| | | … | … |
| | | * | * |
| Federation Partner 2 | | Federation Public Key | |
| Identity Block | Identity 1 | Identity 2 | |
| | Identity A | Identity B | |
| | … | … | |
| | * | * | |
| Group Mapping Block | | Group1 | Group 2 |
| | | Group A | Group B |
| | | … | … |
| | | * | * |
| Etc. | | | |

## ELEMENTS OF FEDERATED COMMUNICATION

***Naming and Identity***

Identity will be established by the requesting agency. In the DOD this is primarily through the Electronic Data Interchange Personal Identifier (EDIPI), but for other certificate authorities, their naming scheme will be honored. To avoid collision with the EDIPI, the identity used by all federated exchanges shall be the distinguished name as it appears on the primary credential provided by the certificate authority.

***Credentials***

Credentials are an integral part of the federation schema. Each identity requiring access shall be credentialed by a trusted credentialing authority. Further, the STS that will be used for generating SAML tokens must also be credentialed (primarily through the same credentialing authority, although others may be entertained.

**PKI required – X.509 Certificates**

The primary exchange medium for setting up authentication of identities and setting up cryptographic flows is the Public Key Infrastructure (PKI) embodied in an X.509 certificate.

***Certificate Services***

The certificate authority must use known and registered (or in specific cases defined) certificate revocation and currency checking software.

***Bi-Lateral Authentication***

The requestor will not only authenticate to the service (not the server), but the service will authenticate to the requestor. This two way authentication avoids a number of threat vulnerabilities. The requestor will initially authenticate to the server and set up a Secure Socket Layer (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). The preferred method of communication is secure messaging, contained in Simple Object Access Profile (SOAP) envelopes.

***Authorization Using SAML Packages***

All authorizations will be through the use of SAML packages in accordance with the SAML 2.0 specification provided by the Organization for the Advancement of Structured Information Standards (OASIS).

**Registration of the STS**

All STS that create and sign SAML packages must be registered. Information needed for such registration must be provided as part of the federation agreement.

**Recognizing STS Signatures**

STS signatures will be recognized only for registered STSs and may be repackaged by the local STS when such registration has been accomplished. Unrecognized signatures will not be honored and the refusal will be logged as a security relevant event.

**Certificate Caches**

Local STSs within the enterprise forests will maintain a certificate cache of all registered STSs to facilitate the re-issuance of SAML packages when appropriate.

***Translation of Roles and Groups***

Roles and groups may be translated as indicated in the federation agreement. The STS will keep a record of necessary translations and perform these translations prior to the re-issuance of SAML packages.

***Other Issues***

The registering of recognized STS and role/group translation are not initiated upon ratification of the federation agreement, but must be promulgated in an Air Force policy memorandum. The federation agreement may be an attachment to such a policy memorandum. This memorandum must be distributed to the appropriate organization for implementation by the appropriate service administrator. This maintains the lines of authority.

## FEDERATION AGREEMENTS

The federation is established by an agreement to share information. The agreement may be made at the appropriate level for the information shared and its implications. Coalition agreements for federation may be at the DoD level or higher. Sharing within the COI across federation boundaries may only require an agreement with enterprise operations and the COI. Agreements may be unilateral (e.g., the first party agrees to share information with the second party), or bilateral (both parties are offering to share information with each other). The agreement needs to spell out all of the information about how and why the information is shared together with information technology (IT) details such as Uniform Resource Identifiers, user and security server credentials, access tokens, etc.

***Within the Enterprise***

Federation within the Air Force may be established by policy memorandum from the appropriate authority within the Air Force to the appropriate office for implementation and may not require a formal federation agreement. Since groups and roles are registered within the Air Force Network, and because all Air Force STSs are registered with all Air Force domains, the IT part of a federation agreement need not be included. It may be desirable to have formal federation between certain elements within the Air Force and this will be determined on a case by case basis.

***With Parties Outside of the Enterprise***

Federation with all parties outside of the Air Force requires a formal federation agreement.

***Maintaining Lines of Authority***

**Federation Approvals**

Federations may be approved by the office within the Air Force (Department of Defense, Executive Branch, etc.) that has the information release authority. Exceptions exist, and certain federation partners may have to be approved at higher levels. The individual federation undertaken will determine the approval level.

**Promulgation of Policy**

Promulgation of policy that implements the federation agreement is by memorandum from the office within the Air Force (Department of Defense, Executive Branch, etc.) that has the information release authority, to the Air Force Office that has appropriate operational control of the data. See sub-section on federation approvals above.

**Modifying STS registries**

Federation cannot be achieved until STS registries have been modified to recognize the signature authority for SAML tokens. This is a required part of the federation agreement and may result in re-negotiation of the federation agreement if not present in the current draft.

**Modifying STS Federation Data Bases**

Any mapping of roles and groups that is required must be part of the federation agreement that is attached to the policy memorandum. Federation cannot be achieved if the service does not recognize the authorization roles or groups. This is a required part of the federation agreement and may result in re-negotiation of the federation agreement if not present in the current draft.

## SUMMARY

Federation elements are summarized below:

1. All communication between enterprise elements that cross forests or domains of security boundaries are subject to federation.
2. All communication between enterprise elements and external entities require a formal federation agreement.
3. Federation has political, rationale and IT components that must all be part of the federation agreement.
4. From an IT standpoint, the federation agreement must contain details of the services, token servers, required SAML attribute translations, and identity issues if any exist.
5. All federation partners must have PKI X.509 certificates for bilateral authentication.
6. All federation partners must have STSs for initiating and repacking SAML 2.0 packages.

## REFERENCES

[1]. 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/

[2]. 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

[3]. 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

[4]. 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

[5]. 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

[6]. 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

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

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

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

[10]. AFI 33-202, Computer Security

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

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

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

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

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

[16]. DoDD 5000.1, The Defense Acquisition System

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

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

[19]. DoDD 8115.01, “DoD Information Technology Portfolio Management,” October 10, 2005

[20]. DoDD 8115.1, Information Technology Portfolio Management

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[37]. “WS-ReliableMessaging Specification”, OASIS, June 2007

[38]. “WS-SecureConversation Specification”, OASIS, March 2007

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

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

# *Annex A: Example Federation Agreement*

## Preamble

This agreement for information sharing is between:

The Air Force Enterprise Air Operations COI
(POC: LtCol J.Tenanbaum, McDill AFB,
john.tennenbaum@pentagon.af.mil)

and

The Ministry of Information Assurance MOD
(POC: LtCol H. Smythe, Redack BBL,
Henry.smythe@redack.uk.ofcl)

**An agreement to share Air Operations recent and current throughout Europe:** *[It is appropriate to cite rationale for this agreement and any requirements that come from higher authority. The example here is bi-lateral. Some federation will be by uni-lateral sharing and the agreement must be tailored. This agreement is meant to be a model only and the individual circumstances may change the form and substance of this agreement. The agreement should satisfy both the human readable needs and the computer information system requirements.]*

## Duration

This document remains in effect until revoked by either of the authorities cited in this document.

## Lines of Authority

**Maintenance of this agreement:**

The Air Force Office of Coalition Forces, Pentagon 3-123, POC: Gen George Wright, george.wright@pentagon.af.mil

The Ministry of Defence, PK2I-53, London, POC: LtCol. Michael Friends, Michael.friends@mod.int.uk

**Implementation of this agreement:**

The AFNETOPS Office, Scott AFB 8-5, POC: Gen Henry Smith, henry.smith@scott.af.mil

The Ministry of Information Assurance, LU-2, Luton POC: LtCol. Robert McCarin, Robert.McCaren@mod.int.uk

## Responsibility

The Ministry of Information Assurance will be responsible for identifying, vetting, credentialing, and training individuals who will have access to the information of the US Air Force and for the maintenance of this list.

The Air Force Enterprise Air Operations COI Assurance will be responsible for identifying, vetting, credentialing, and training individuals who will have access to the information of the UK Ministry of Information Assurance and for the maintenance of this list.

## Classification

**This Document:** Secret

**USAF Information Shared:**
Sensitive but Unclassified

**UK Ministry of Assurance Information Shared:**
Sensitive but Unclassified

## Credentialing

**USAF:** DoD certificate authority, PKI issues X.509 certificates *[as much detail as necessary to provide root authority and validation]*.

**MOD:** MOD certificate authority, PKI issues X.509 certificates *[as much detail as necessary to provide root authority and validation]*.

## Identity and Requested Access

*[Data in this section may make the agreement at a higher level of classification than the information being shared.]* Members of **The Air Force Enterprise Air Operations COI** will be identified by The Distinguished Name on the DoD Issued X.509 Certificate, and will seek access from <URL, location, specific enclave within a forest, or other source information pertinent to the requestors of service>. The access will be directed to the following services within the **Eternal Enterprise XXX:**

1. <service name, url for entry, uri, and other information pertinent to access>
2. <service name, url for entry, uri, and other information pertinent to access>
3. <service name, url for entry, uri, and other information pertinent to access>

and

4. <service name, url for entry, uri, and other information pertinent to access>

The access sought is read only without edit, modification or deletion rights.

The requestor will present a SAML 2.0 Package, developed by the following security token server:

<token server name, url, uri, and other information pertinent to registration>

The X.509 Certificate for this server is DoD Issued and will be provide electronically.

*[Data in this section may make the agreement at a higher level of classification than the information being shared.]* Members of **The Ministry of Information Assurance MOD** will be identified by The Distinguished Name on the ZZZ Issued X.509 Certificate, and will seek access from <URL, location, specific enclave within a forest, or other source information pertinent to the requestors of service>. The access will be directed to the following services within **The Air Force Enterprise Air Operations COI:**

1. <service name, url for entry, uri, and other information pertinent to access>
2. <service name, url for entry, uri, and other information pertinent to access>
3. <service name, url for entry, uri, and other information pertinent to access>
4. <service name, url for entry, uri, and other information pertinent to access>

The access sought is read only without edit, modification or deletion rights.

### Authorization

*[Data in this section may make the agreement at a higher level of classification than the information being shared.]* The USAF requestor will present a SAML 2.0 Package, developed by the following security token server:

> <token server name, url, uri, and other information pertinent to registration>

Authorized members of the COI will have the following attributes present in the SAML Assertion.

1. Attribute1
2. Attribute 2
3. Attribute x
4. Attribute y

A maximum of 4 simultaneous users will be supported for a maximum of eight hour sessions. Session will timeout and be terminated with 5 minutes of inactivity.

and

*[Data in this section may make the agreement at a higher level of classification than the information being shared.]* The MOD requestor will present a SAML 2.0 Package, developed by the following security token server:

> <token server name, url, uri, and other information pertinent to registration>

The X.509 Certificate for this server is ZZZ Issued and will be provide electronically.

Authorized members of the The Ministry of Information Assurance MOD will have the following groups and roles present in the SAML Assertion.

1. Attribute x
2. Attribute y
3. Attribute 1
4. Attribute 2

A maximum of 4 simultaneous users will be supported for a maximum of eight hour sessions. Session will timeout and be terminated with 5 minutes of inactivity.

### Registration of Security Token Server Certificates

Bi-lateral registration of STS certificates will be undertaken and STS data bases will be updated. Authorization will be promulgated by Air Force Enterprise Policy and External Enterprise Policy as soon as practical.

### Special Considerations

Assistance at interpreting, formatting, displaying and integrating the information accessed will be provided bi-laterally.

This agreement may be uni-laterally revoked by either party with appropriate notice to the POCs above.