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


# Chained Authorization and Delegation (attribution) and Least Privilege Using SAML Packages


Coimbatore Chandersekaran
William R Simpson



Prepared for:
The Twenty First Annual systems and Software Technology Conference (SSTC 2009) 20-23 April 2009 in Salt lake City, Utah




23 April 2009

# Notes

- At this conference last year I covered an IT approach to delegation by persons with the use of personae.
- That brief is included as backup slides in your package
- This year I will cover an approach to delegation as it applies to service invocation.
- I will answer questions at the end of this presentation on either.

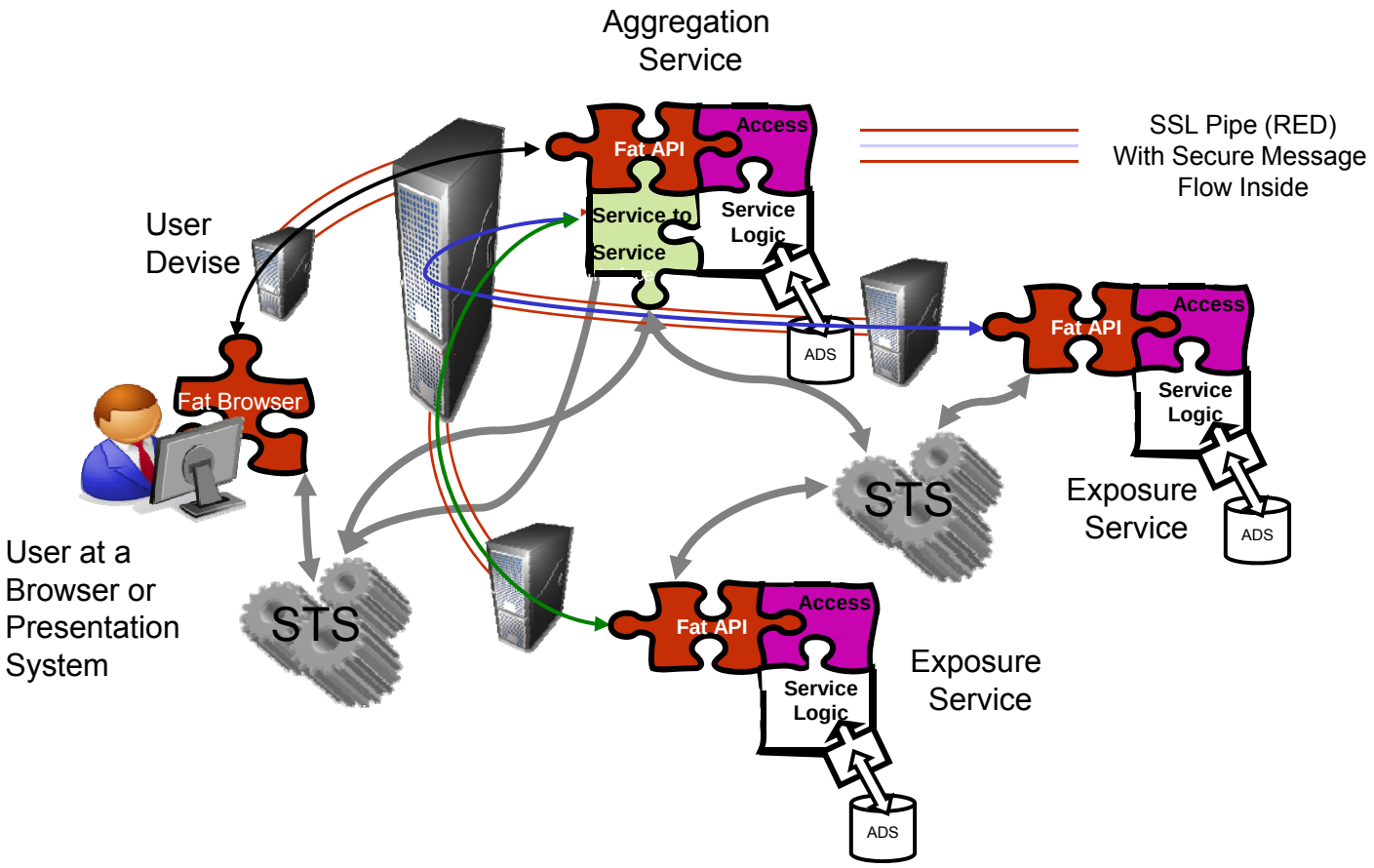
# High Level Tenets

0. ***The enemy is present***
1. *Simplicity*. Supporting cross-enclave and enterprise scenarios will automatically add a certain degree of complexity that will be challenging enough to handle in any case.
2. *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.
3. *information hiding*. involves only revealing the minimum set of information to the outside world.
4. *accountability*. being able to identify and track what entity in the enterprise performed any particular operation.
5. *minimal detail* to only add detail to the solution to the required level.
6. emphasis on a *service-driven* rather than a product-driven solution whenever possible.
7. *lines of authority* should be preserved.

# Information Security, Information Sharing, and the Connectivity Threat

0. ***The enemy is present***
1. Standard Naming of all active entities
   (people, devices, services)
2. Strong Credentialing of all active entities
   (Public Key Infrastructure)
3. Bi-Lateral *end-to-end* Authentication
4. SAML-Based Authorization
   (with binding to authentication)
5. Delegation
   (people-to-people, service-to-service, etc.)
6. Least Privilege
7. Audit
   (for real time behavior, compliance, and post incident forensics)
8. Anomalous Behavior Detection
   (insider threat)
9. Cyber attack resilience

# Communication to Aggregation Services Use Case



# Access Control Concepts

- A call to a Service is preceded by a bi-lateral authentication
- The call to a service includes a SAML token with secure transmission of access elements*
- The access elements are tested against a set of acceptable access elements to gain a session with the service
- Some services require escalation of privilege to complete their function
  - Example 1 – A security token server (STS will need acess to AD or UDDI even if the requestor does not have these privileges.
  - Example 2 – An aggregation service takes individual statistics and compares them to averages. The service needs access to all values to compute averages, even if the requestor can only access his own data.

*An element in this concept is a group, role, attribute or a combination of the previous that is held by a requestor and used for access control.

# Assumptions

- User based requests:
  - A request for service within the AF enterprise is an *implicit* delegation to a service provider to do what you are allowed to on my behalf to satisfy this request.
  - Attribute/Group/Role definition is fine grained enough to signify access throughout the process.
- Service based requests:
  - A request for service within the AF enterprise is an *explicit* delegation to a downstream service provider to do what you are allowed to on my behalf to satisfy this request.
  - Attribute/Group/Role definition is fine grained enough to signify access throughout the process.
  - Non-aggregation services are atomic.
- Other
  - Only considering web-service calls at or above OSI level 5.
  - Calls below level 5 on the OSI stack are not made by SAML authorization and do not follow this paradigm.

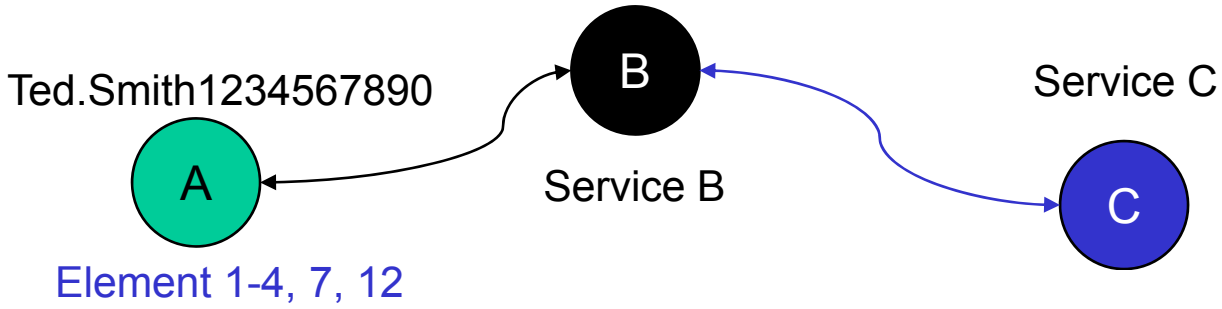
# SAML 2.0 Format

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

# Types of Elements

- $H_A$ – held elements in entity A
- $R_B$ – Required Elements for Access to entity B
- $E_B$ – Escalation of Privilege Required for entity B
- $P_B$ – Prior elements From SAML B used to Access B

| | | |
|---|---|---|
| Requires: | Elements (one of) 1,3-6 | Element (one of) 4-6 |
| Holds: | Element 1,3-6 | Element 4-6 |
| Escalation: | Group6 | Group6 |



# Requirements

- Service saves SAML Attribute Assertion from session establishment for follow-on work
- Service provides prior SAML Attribute Assertion to STS
- Logging of subjects for attribution by STS or Service
- Adjusting of attributes[1], roles and groups by STS for least privilege
  - Using prior

    SAML Assertion

    and
  - Service Registered Elements

    and
  - Service Required Escalation Elements
- STS creates least privilege SAML Package from modified elements.

1. An element is an attribute, role, group or combination of the previous.

# The Algorithm

The combing of these elements for least privilege is given by:

Let $N_{i+1}$=New SAML Elements for i to call i+1

Let $P_i$ = Prior Elements, if none exists, current elements held

Let $R_{i+1}$= Service Required Elements

Let $H_i$ = Service Held elements

Let $E_i$ = Required Escalation Elements

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

Where: $\cap$ is the intersection of sets and

$\cup$ is the union of sets

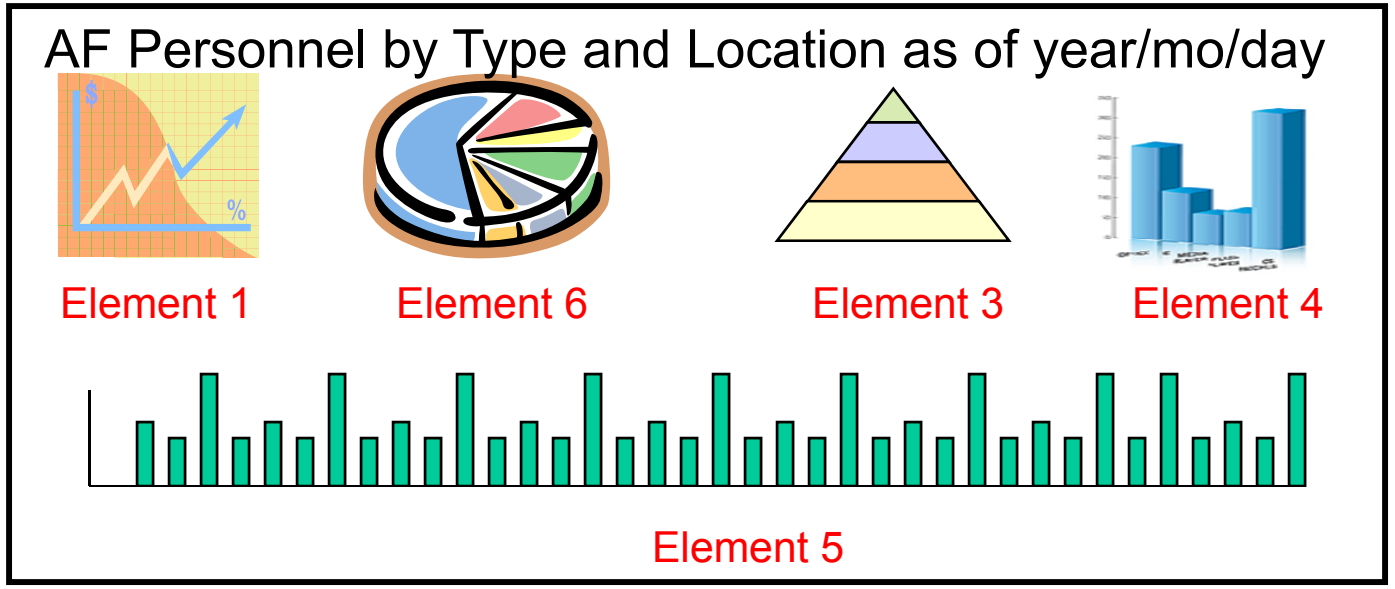
$\varnothing$ is the empty set (no members)

The formula may be read as the common elements in the prior SAML and the union of the held elements and those required by the next call (( $P_i \cap (R_{i+1} \cup H_i)$) - 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).

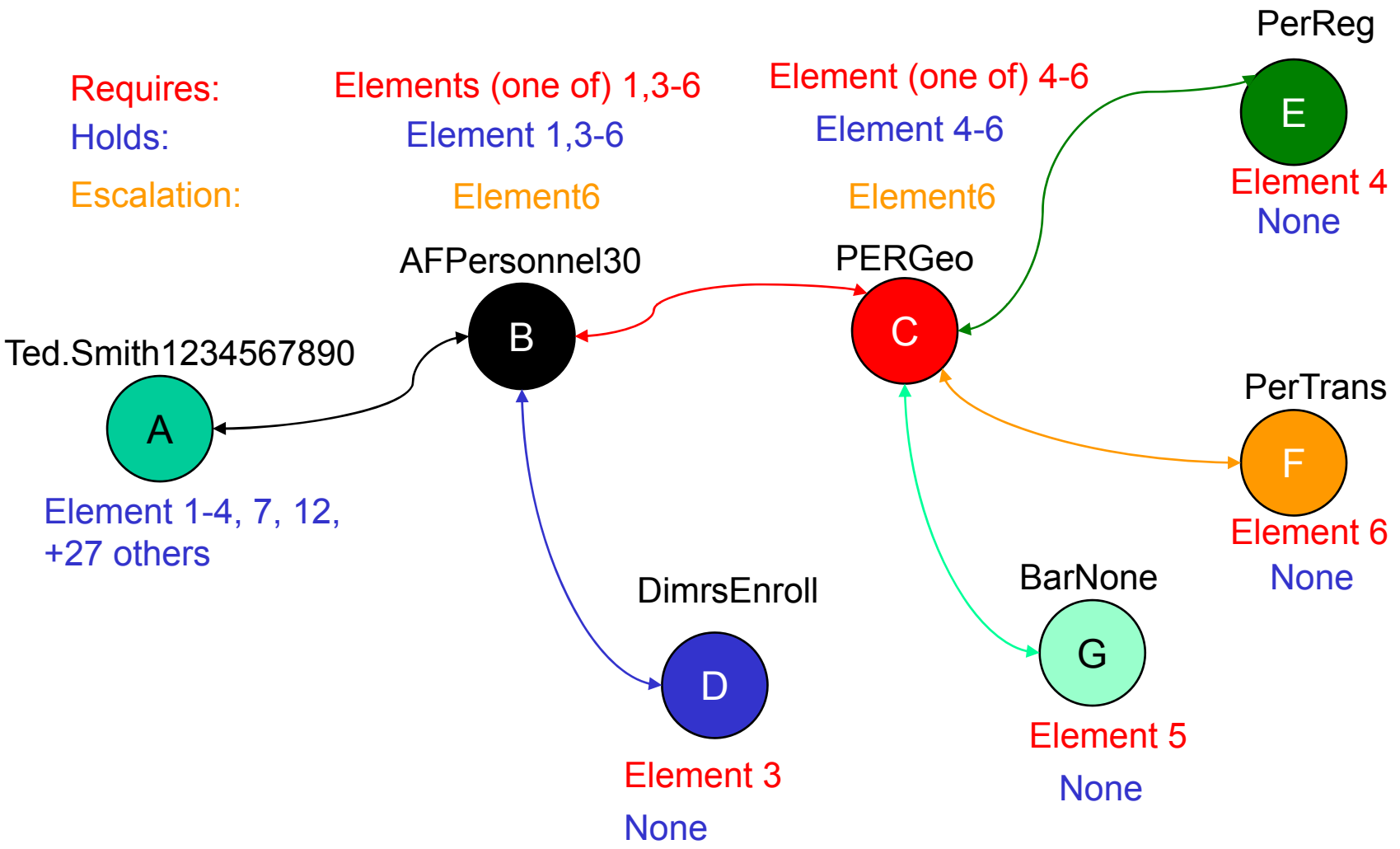
The initial call has no prior elements and $P_1$ is defined as the initial set of privilege elements.

# Notional Example

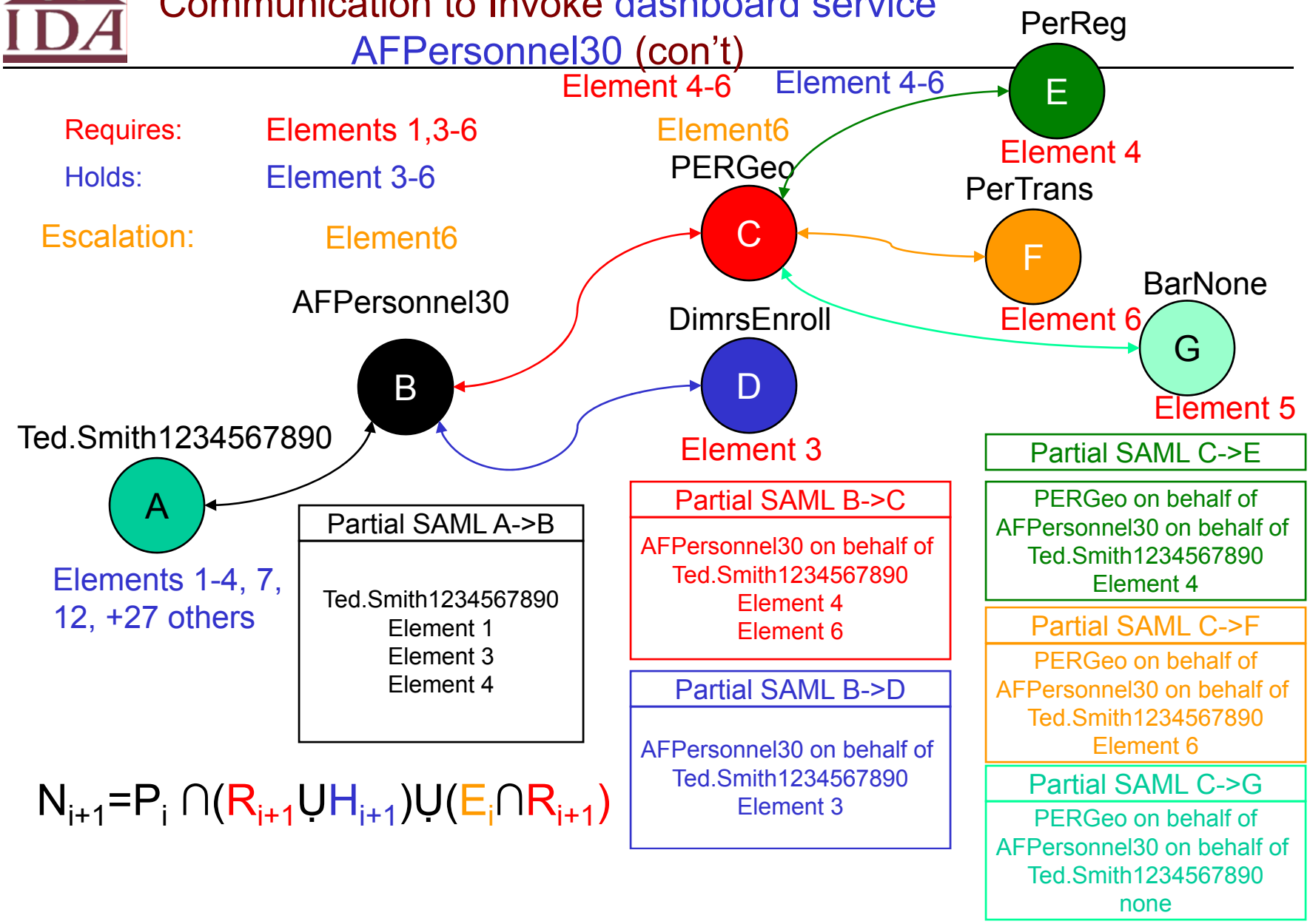
- User: Ted.Smith1234567890
- Through discovery finds a dashboard service on personnel in the AF (AFPersonnel30).
- Ted has the attribute, group and role authorization to use the service, but not all of the information it may provide (perhaps non-CONUS data).
- An element is an attribute, group, role, or combinations of these used to make an authorization decision.
- Ted has Elements 1, 2, 3, 4, 7,12 + 27 others
- AFPersonnel30 will allow invocation from one of element 1, 3-6 with the following breakdown needed for constituent parts.



# Communication to Invoke dashboard service AFPersonnel30

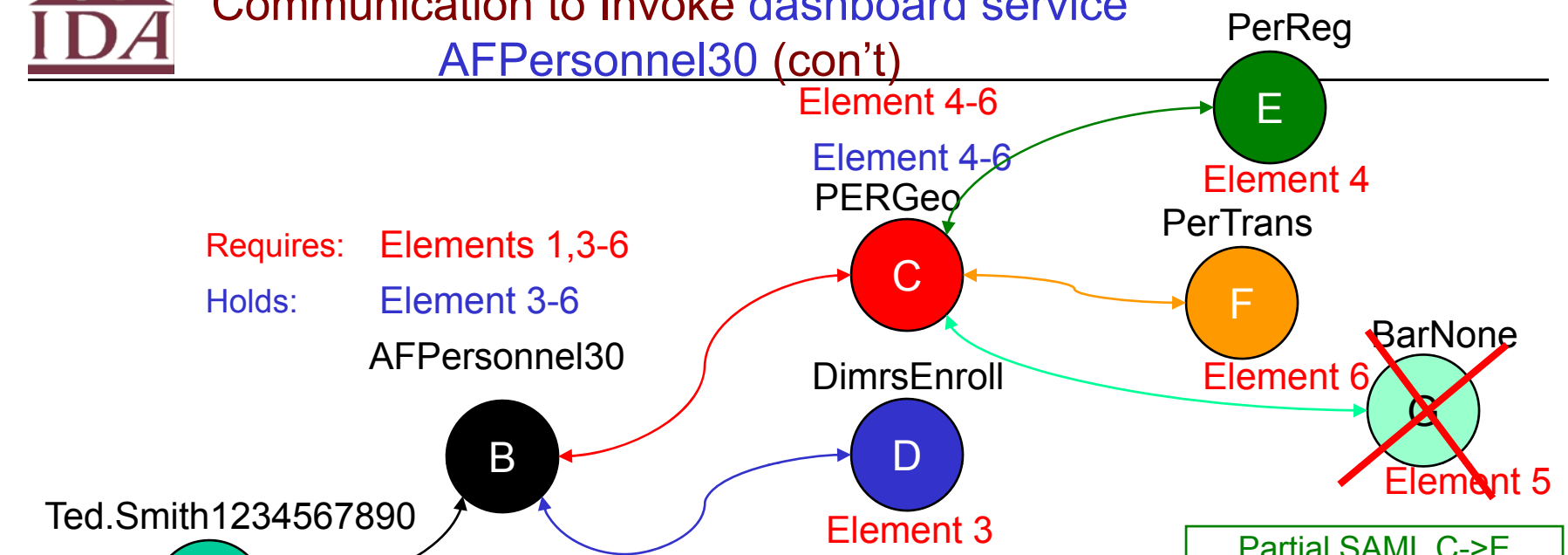


# Communication to Invoke dashboard service AFPersonnel30 (con't)




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

# Communication to Invoke dashboard service AFPersonnel30 (con't)




Elements1-4, 7, 12+27 others

**Partial SAML A->B**

Ted.Smith1234567890
Element 1
Element 3
Element 4

$N_1 = ( P_1 \cap (R_2 \cup H_2)) \cup (E_1 \cap R_2)$
$=((1, 2, 3, 4, 7, 12, +27more) \cap ((1,3-6) \cup (1,3-6)) \cup (\emptyset \cap 1,3-6)$
$=((1, 2, 3, 4, 7, 12, +27) \cap (( 1,3-6)) \cup ( \emptyset)$
**$=((1, 3, 4))$**

**Partial SAML B->C**

AFPersonnel30 on behalf of Ted.Smith1234567890
Element 4
Element 6

$N_{i+1} = ( P_i \cap (R_{i+1} \cup H_i)) \cup (E_i \cap R_{i+1})$
$=((1, 3, 4) \cap (4 \cup 4\text{-}6) \cup (6 \cap 4\text{-}6)$
$=((1, 3, 4) \cap (4)) \cup (6)$
**$=(4,6)$**

**Partial SAML B->D**

AFPersonnel30 on behalf of Ted.Smith1234567890
Element 3

**Partial SAML C->E**

PERGeo on behalf of AFPersonnel30 on behalf of Ted.Smith1234567890
Element 4

**Partial SAML C->F**

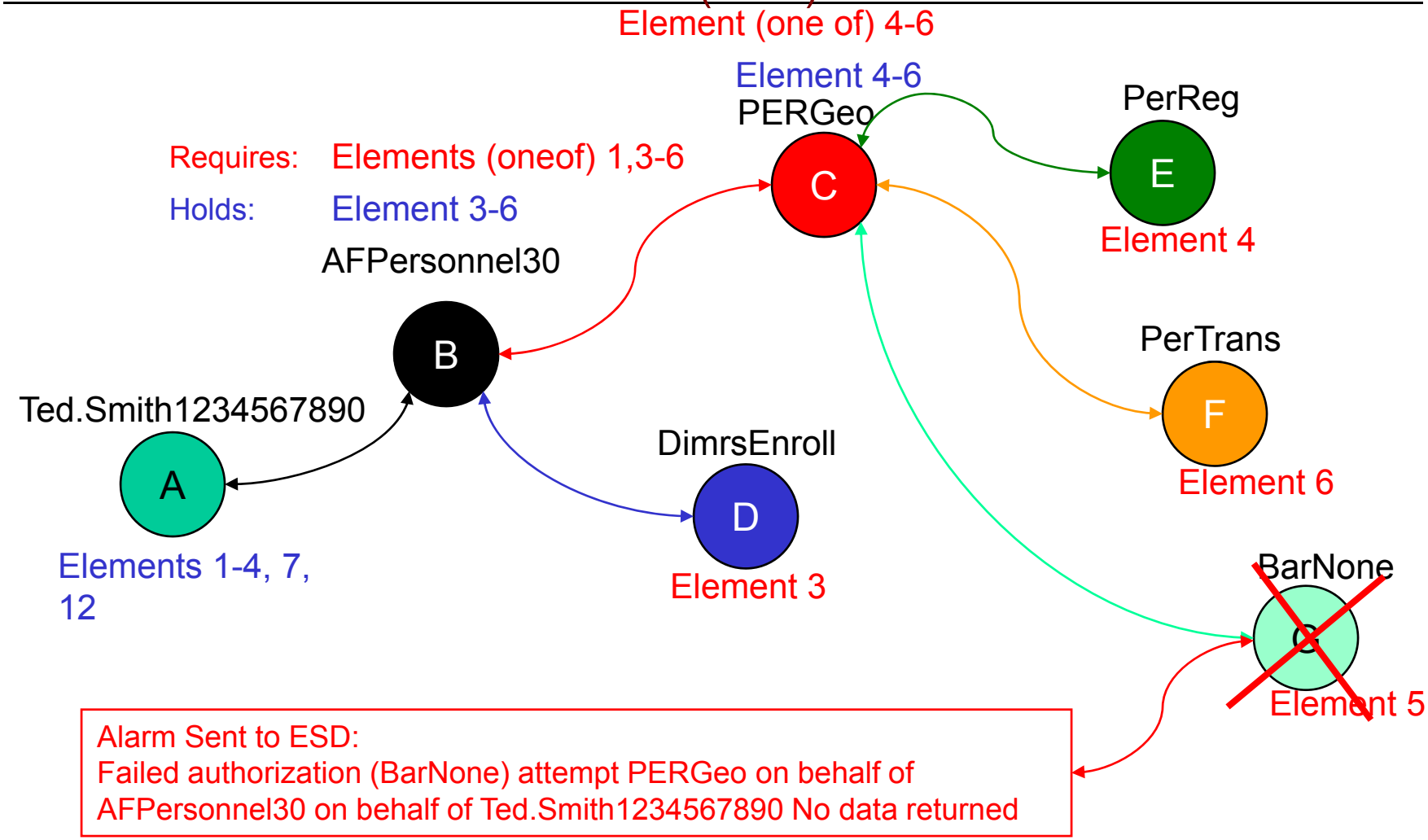
PERGeo on behalf of AFPersonnel30 on behalf of Ted.Smith1234567890
Element 6

**Partial SAML C->G**

PERGeo on behalf of AFPersonnel30 on behalf of Ted.Smith1234567890
No elements

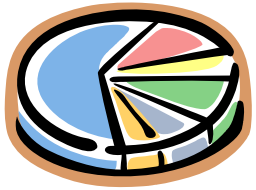
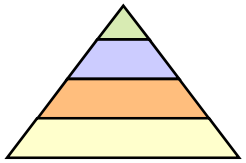
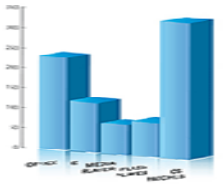
$$N_{i+1}=P_i \cap (R_{i+1} \cup H_{i+1}) \cup (E_i \cap R_{i+1})$$

# Communication to Invoke dashboard service AFPersonnel30 (con't)



# Dashboard Service AFPersonnel30 Case Result

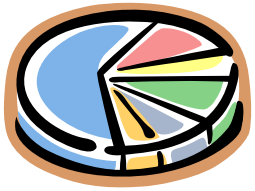
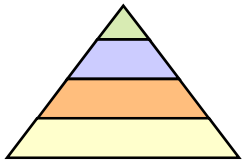
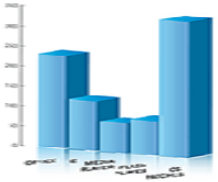
AF Personnel by Type and Location as of year/mo/day

Data not available

# Dashboard Service AFPersonnel30 Case Result (Rationale)

AF Personnel by Type and Location as of year/mo/day

Requires: Element 1 Element 6 Element 3 Element 4

Data not available

Element 5

Ted has Elements 1, 2, 3, 4, 7,12

The Pie requiring element 6 chart was provided because of privilege escalation,

However the specific bar chart at the bottom was not due to lack of privilege

# Pros and Cons of Methodology

- 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
  - Directly compatible with personae delegation
- Disadvantages
  - Use of SAML standard in an way that SAML standard writers did not anticipate
  - Implicit delegation invoked (would be better explicit)
  - Service must store and pass on prior SAML assertion when invoking the thread
  - STS must store and process data on service requirements and escalation of privilege
  - STS currently does not process this data

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

# Questions

## Chained Authorization and Delegation (attribution) and Least Privilege Using SAML Packages

Coimbatore Chandersekaran
William R Simpson

Prepared for:
The Twenty First Annual systems and Software Technology Conference (SSTC 2009) 20-23 April 2009 in Salt lake City, Utah



23 April 2009

# Backups

# Acronyms

- **AF:** Air Force
- **API:** Application Programming Interface
- **ADS:** Authoritative Data Source
- **CONUS:** Continental United States
- **ESD:** Enterprise Support Desk
- **EDIPI:** Electronic Data Interchange Personnel Identifier
- **OSI:** Open System Interconnection
- **Non-CONUS:** Not Continental United States
- **SAML:** Security Assertion Markup Language
- **SSL:** Secure Socket Layer
- **STS**: Security Token Service
- **X.509:** A Specific format for a security certificate

# Terms

- **Aggregation Services:** A service that draws data from multiple authoritative data sources and combines them in some way to provide information to the user.
- **Authorization:** Authorization is establishing that the requesting entity has privileges to access a requested resource or perform a particular operation.
- **Dashboard:** A presentation of multiple pieces of data in graphical form. The parts of the presentation may be configurable.
- **Delegation**: Delegation is the handing of a task over to another person, usually a subordinate. It is the assignment of authority and responsibility to another person to carry out specific activities.
- **Exposure Service:** A service that draws data directly from one authoritative data source
- **Least Privilege:** Access is restricted to only those elements and resources necessary to perform the assigned task.
- **SAML Attribute Assertion:** A portion of the SAML Token that deals with attributes.


# Last year's SSTC presentation on A Persona-Based Framework for Flexible Delegation and Least Privilege (updated)

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

# A Persona-Based Framework for Flexible Delegation and Least Privilege

Coimbatore Chandersekaran

William R Simpson

Andrew Trice



23 April 2009

# Agenda

- Need for delegation in IT systems
  - Extra challenges in Military/IT enterprises
- Proposed delegation framework
  - Persona concept
  - Scenarios
  - Registration service
- Support for least privilege
  - Need for least privilege
  - Scenarios
  - Registration service
- Delegation invocation process
- Summary
  - Advantages
  - Status in Air Force context

# Need for a Formal Delegation Process

- Continuity of operations
  - Acting for a boss/commander in their absence/incapacity
- Efficiency
  - Boss has official authority, but not the time or expertise
- Managing transitions
  - Overlapping roles for limited period during turnover

# Need for a Formal Delegation Process – Con't.

- Least privilege
  - "delegating to a role"--getting user to act in correct capacity
  - Not the least privilege of computer service to service interaction
- Delegation is bounded in time
  - Specific time period
  - Good until canceled / expired / delegate leaves / event completed
- Delegation is not
  - Normal Organization roles and duties
  - Transitive (must go from delegator to delegatee)
  - Active after the delegator has terminated, moved or is revoked.
- Need to provide accountability and attribution for delegated activity.

# Delegation -- Challenges in Military Enterprises

- Security clearance level restrictions
- Need for rapid deployment – the “chop”
- Legal restrictions / accountability
- Delegation across multiple security domains
- Persona definitions based on AF Enterprise IA architecture proposed for AFNetOps
  - All active entities are credentialed using PKI
  - Access Control by groups and roles (GBAC) but attributes may be used
  - Illustrations assume Active Directory (not necessary to concept)

# The Persona concept

- A persona is a special category of user that embodies only delegated privileges
  - **Advantage**: The persona appears as a “real” user and all mechanisms put in place for the user work, including identity, authorization and access, and federation.
    - Persona may be assumed only after “real” human user taking on persona explicitly chooses it, or may be mandated by current context (DEFCON, THREATCON, Trust Agreements, etc.)
    - The delegate persona is the responsible party for actions and attribution (delegator is still accountable)
    - The delegation must be recorded and registered in advance through a delegation registration service, and the delegation must be approved by written policy
    - Necessary data and mechanics must be implemented to support persona and provide traceability

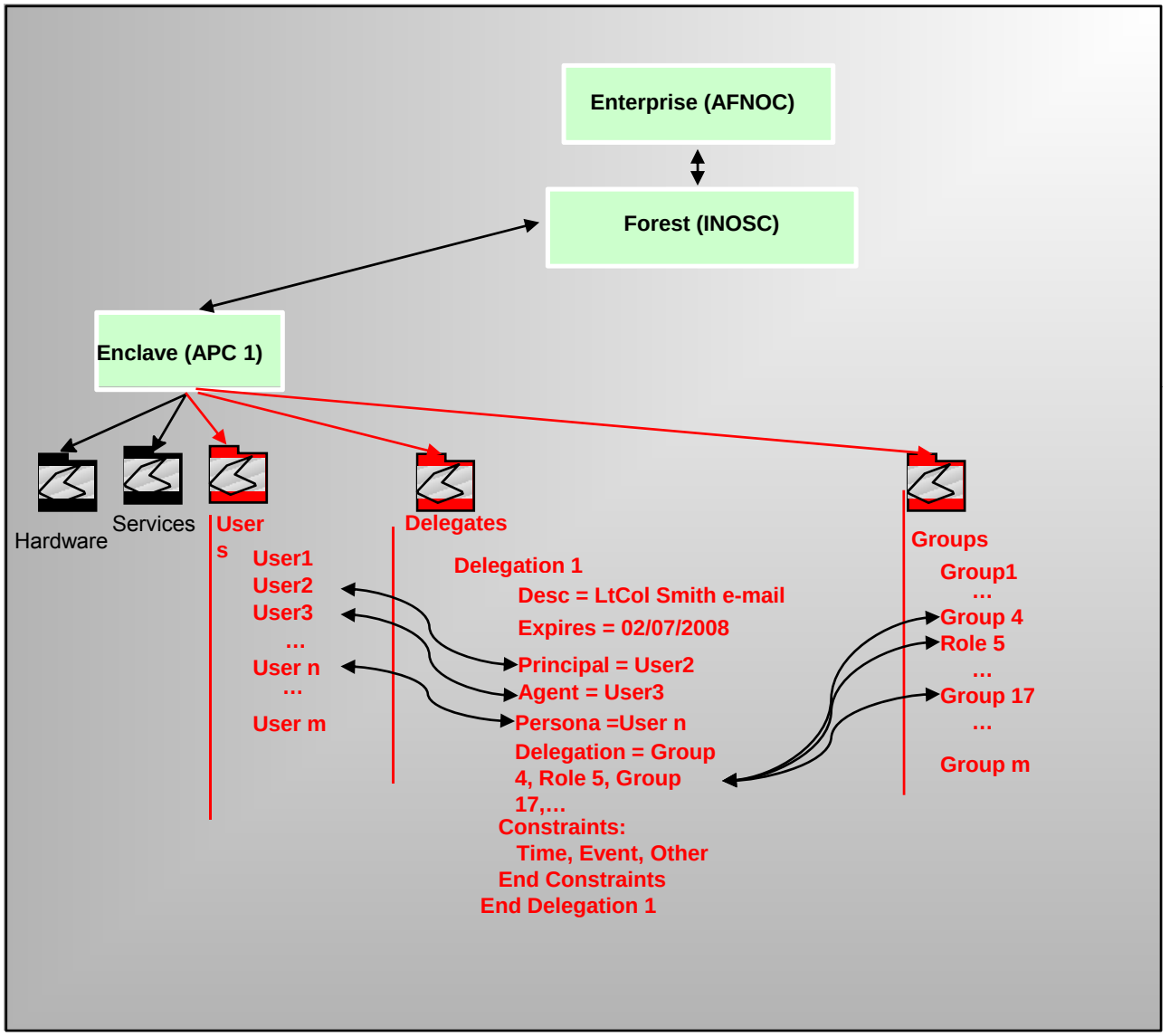
# The Persona concept– data and mechanics

- The existence of a persona delegation in the user file:
  - The logon script may include a call to the delegation service for possible revision of identification of the user.
  - Logon may include automatic delegation when external conditions require it.
- The system opens a session with:
  - Original credentials assigned to the individual
  - Or delegation credentials that are provided by the persona.
- The delegate persona is:
  - Persistent (in our illustration), although it should have an expiration date at the end of which it is renewed or expires (“persona non grata”).
  - May be transient in uses for coalition, temporary aliances, and other temporary events (dynamic delegation) – not dealt with at this time.
  - Not changeable, once chosen for the session.
- Audit records:
  - Verbose during delegation process
  - Follows normal record keeping during session
  - Attributed to persona and session number.

# The Persona concept– data and mechanics (Con't)

- The delegate persona can be retrieved as a delegate by query to the delegation data base.
- When a related persona is created, the attributes under the user are modified.
- The last entry may be provided with "Delegate", as an indication for delegation services. This field may have a default of "Normal", and a created Persona may have a value "Persona".
- Principal-agent delegation can be used to implement personas

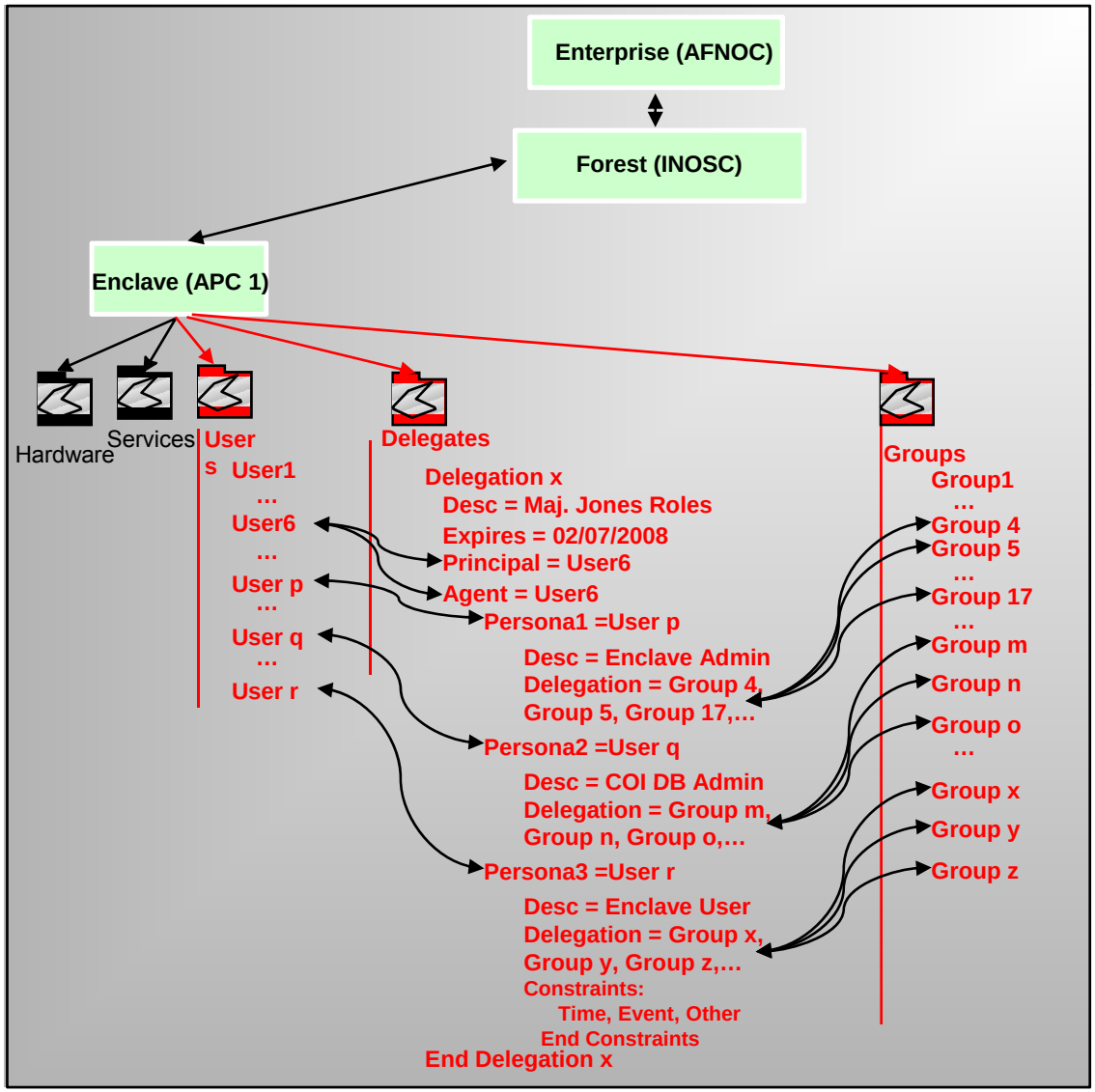
# Principal – Agent Delegation Architecture -- Registration



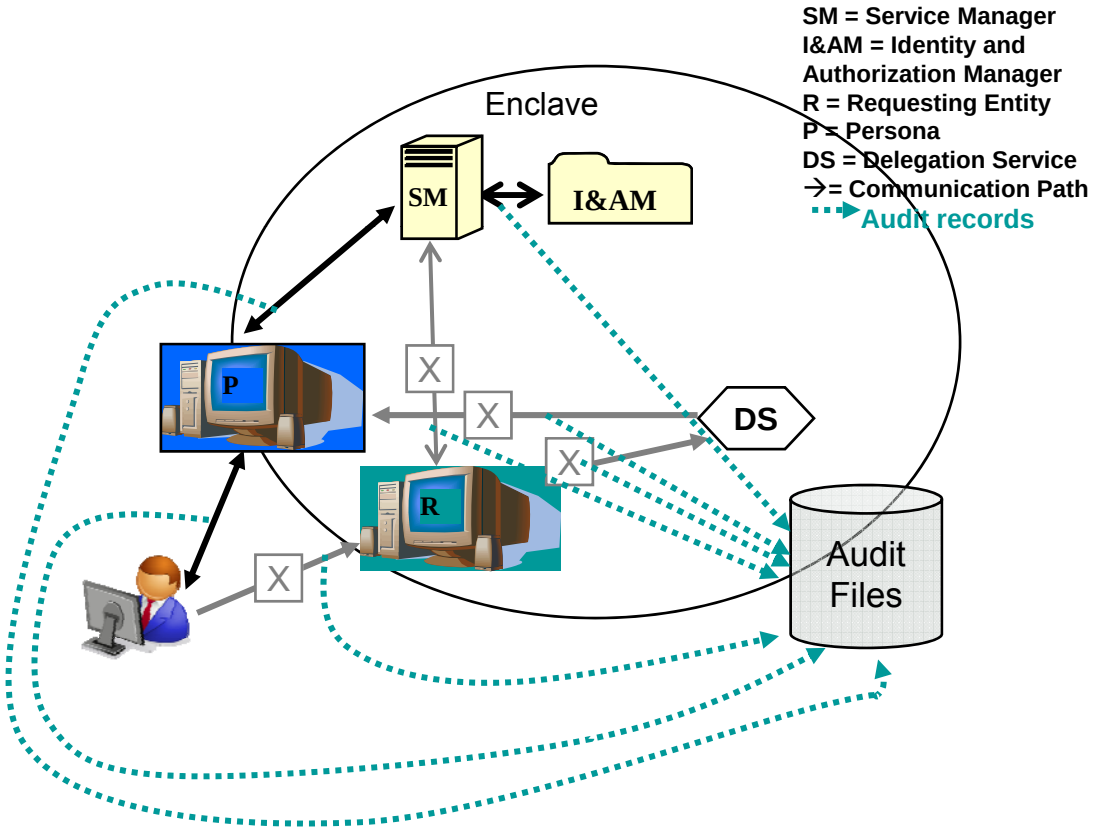
# Least privilege

- Concept:  A user must be able to access only such information and resources that are necessary to its legitimate purpose.
- Principle is an important design consideration in enhancing the protection of data and functionality from faults and malicious behavior.
- Need often arises to manage the extent of activity that can take place, or the cost of errors by the human operator.
  - User requests a catastrophic action and acknowledges the request without mulling over the consequences (formatting a hard drive, for one).
  - Under these circumstances the user will be left to establish the least privilege to accomplish the task.
- Principal-Principal delegation can be used to implement least privilege

# Principal – Principal Delegation Architecture -- Registration



# Delegation Invocation Process



# Additional Uses of Personae

- Impossible to foresee all uses at this time, but two are being actively explored:
  - Use of multiple personae during period of job overlaps (transfers or “Chops”)
  - Use of personae for attribution of virtual machines. The personae would need to be created at the time of virtual machine implementation.

# Summary

- Advantages
  - Flexibility and Usability
  - Tracking and accountability
  - Modest additional infrastructure needed
- Status in Air Force context
  - Is under consideration for incorporation as part of infrastructure build out