

United States Air Force

Integrity - Service - Excellence

SOA Security of GCSS-AF



Vincent Forester
GCSS-AF Security Architect /
Lockheed Martin
vincent.forester@lmco.com

U.S. AIR FORCE



What is SOA Security?

U.S. AIR FORCE

- **Service Oriented Architecture Security**
 - **The ability to abstract-out services required to perform security actions within an enterprise on behalf of application and user consumers**
- **Basic Philosophy**
 - **Security Services within an enterprise provide a means of comprehensive policy enforcement without belaboring business capability builders**
 - **Security Services are policy driven and maintain a central “source of truth” for such policies**
 - **Security Services utilize open standard mechanisms and protocols for exposing functionality**
 - **Security Services, at all cost, abstract explicit knowledge requirements away from consumers and developers**
 - **Security Services provide consistent and comprehensive enforcement of policy at enforcement points**



U.S. AIR FORCE

Security Services Overview: A Brief Sample of Services

Authentication

UID & Password

Software and ECA Certificates

Hardware Certificates (CAC)

SAML

WS-Security

WS-Federation and Liberty Alliance

Reduced Sign-On (RSO)

Friends & Family

Authorization

URL Based Course Grain

JAAS, CMS, JACC

Container Managed Security

Group Based Access Control

Role Based Access Control

Attribute Based Access Control

WS-Security, XACML

.NET Platform Authorization

Integrity & Confidentiality

PKI-Based Mutual Auth

Data Encryption, FIPS 140-2

PKI-Based SSL

Data Policy Protection

Protected Object Policies

Hashing, XML DigSig

Schema Validation

Virus Protection

Identity Management

Identity Management Workflow

Digital Signature

OCSP

AFDS Data Integration

ID Web Service

FAB, O&S, and App Admin

WS-Provisioning

Directory Integration and Sync

Self Service

Account Self Registration

CAC-Based Self Registration

Password Reset

Challenge Response Questions

Automated Role Request

User Profile

Electronic Form 41

Electronic DD 2875

Audit and Misc.

All Point Auditing

DNS Protection

Sure Route

WS-Trust Token Service

Key Storage

.NET Platform Security

Certificate Validation

Tiered Admin

Integrity - Service - Excellence



U.S. AIR FORCE

Authentication

- **Authentication**
 - **Validation of client identity**



U.S. AIR FORCE

GCSS-AF Authentication Mechanisms and Protocols

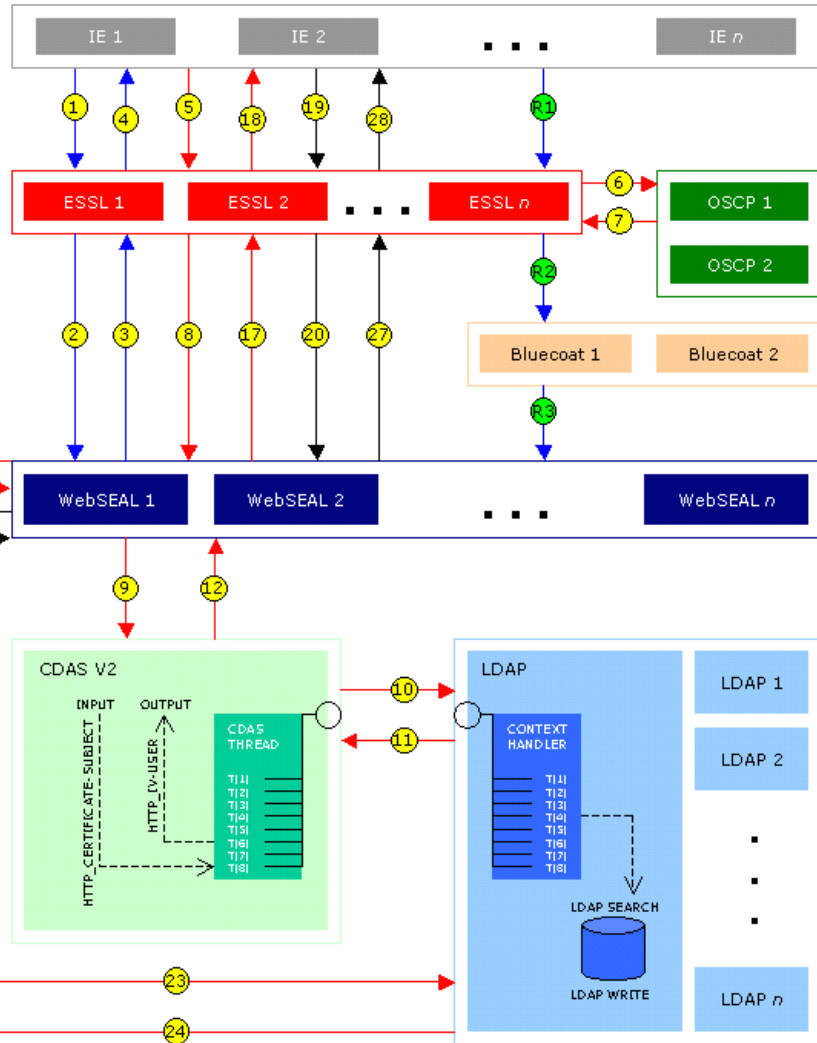
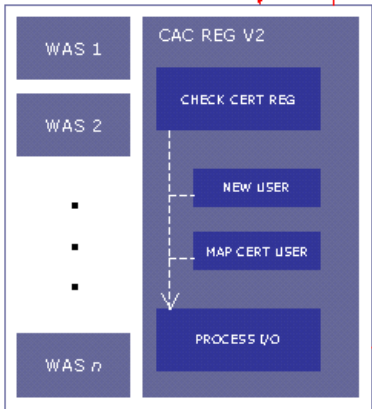
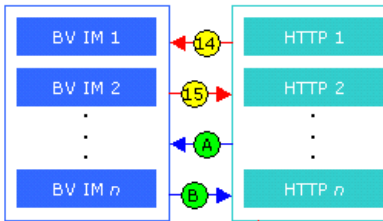
- **Authentication by Proxy**
 - **Forms Based UID/PW**
 - **X.509 (CAC) Identity Certificate (Hardware or Software; DoD or ECA)**
 - **Security Assertion Markup Language (SAML)**
 - **Liberty Alliance**
 - **Web Services Federation (WS-Federation)**
 - **Web Services Security (WS-Security)**
 - **PKI-Based Machine-Level SSL**
- **Implicit Authentication**
 - **Java Authentication and Authorization Service (JAAS)**
 - **Web Services Trust (WS-Trust); Token Issuance, Validation, and Exchange Service**
 - **Lightweight Directory Access Protocol (LDAP) Bind**



PK-E V2 Architecture

U.S. AIR FORCE

GCSS-AF Public Key – Enabled V2a Architecture Diagram
Eric Z. Maass, Lockheed Martin IS&S
May 2005

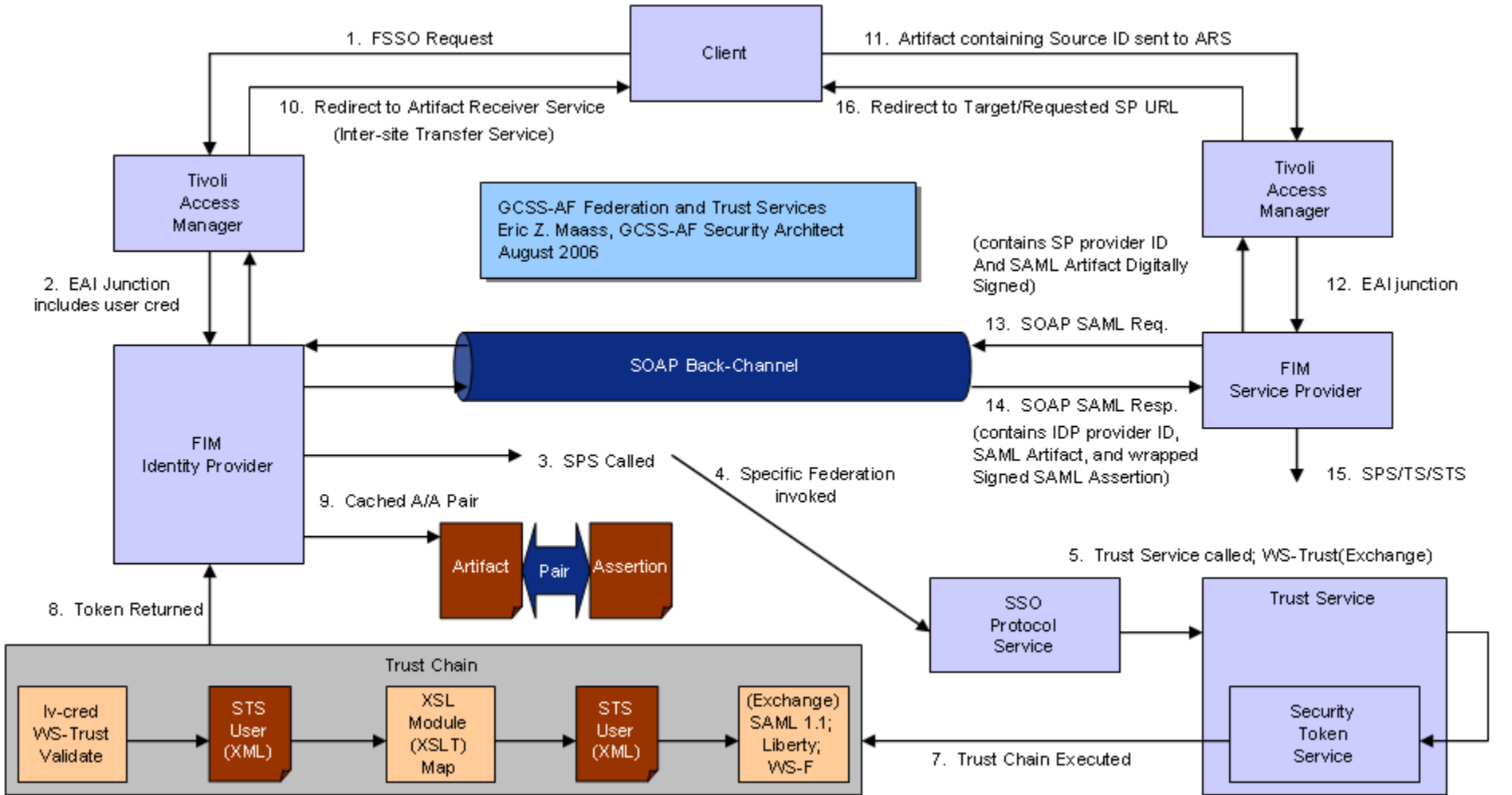


1. Request to www.my.af.mil
 2. ESSL forwards request to WebSEAL
 3. WebSEAL prompts for authentication with login page
 4. ESSL forwards login request to browser
 5. User clicks "CAC Login" initiating a request on pke.my.af.mil; client cert is flowed to ESSL during SSL negotiation
 6. ESSL requests cert status from AF OSCP
 7. AF OSCP returns status
 8. ESSL forwards request to WebSEAL with OSCP status code upon error
 9. Upon no OSCP error, WebSEAL calls CDAS V2 auth library and passes header parameter HTTP_Certificate_Subject inserted by ESSL
 10. CDAS V2 requests mapping of header to TAM user via LDAP
 11. LDAP returns TAM user name
 12. CDAS V2 returns IV_USER to webseald process; equals TAM user upon successful LDAP search or "newcertuser" otherwise
 13. WebSEAL forwards homepage request to HTTP server
 14. HTTP server forwards request to BV IM
 15. BV IM loginFilter returns meta-refresh logic for IV_USER = NEWCERTUSER or homepage for IV_USER = <tam_user>
 16. HTTP server forwards response
 17. WebSEAL forwards response
 18. ESSL forwards response
 19. If meta-refresh upon NEWCERTUSER, browser goes to CAC SELF REG; otherwise, user directed to www domain homepage
 20. ESSL forwards request; WebSEAL consumes failover cookie from pke domain if necessary
 21. WebSEAL forwards request
 22. HTTP forwards to WAS CAC REG V2
 23. CAC REG V2 performs interaction with user to bind TAM ID and CERT DN or create new TAM ID based on only CERT DN
 24. LDAP responds
 25. CAC REG V2 returns status
 26. HTTP forwards response
 27. WebSEAL forwards response
 28. ESSL forwards response
- A and B: Alternative path for 22 – 25 if user was already a registered CAC user.
- R1, R2, R3: Alternative path for commercial network users. Flow may be handed off to DISA bluecoat servers if required to flow through such



Federation and Trust Services

U.S. AIR FORCE



Integrity - Service - Excellence



Reduced Sign-On (RSO)

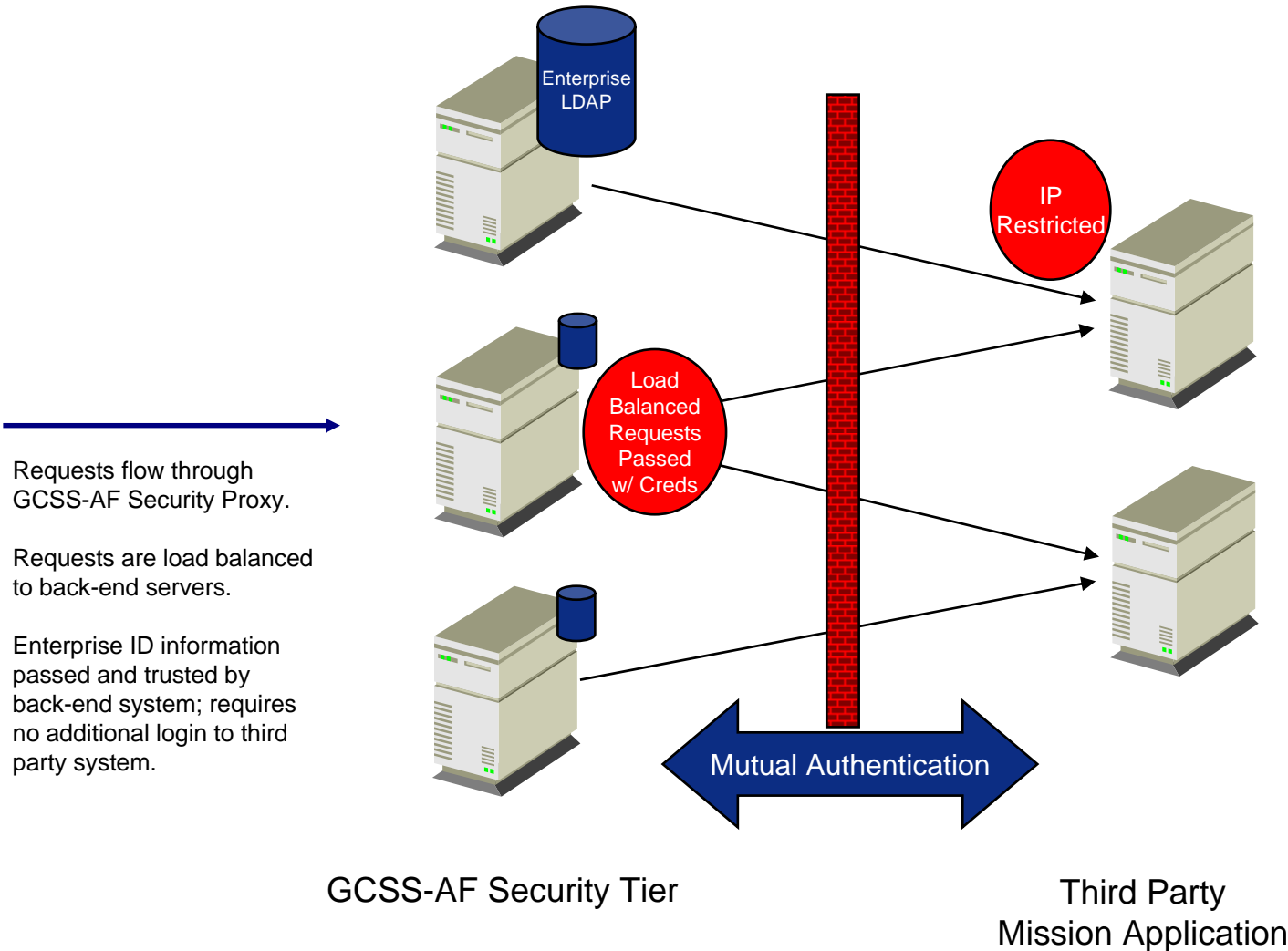
U.S. AIR FORCE

- **Allows AF Combat Support Applications to Utilize GCSS-AF Security**
 - **Secure connection between GCSS-AF security proxies and web front-end of mission application**
 - **Mutually authenticated SSL**
 - **Mission application trusts GCSS-AF credentials**
 - **UID is passed to mission application**
 - **Additional attributes can be passed as needed, examples being:**
 - **Client Certificate Attributes**
 - **DMDC Data**
 - **Enterprise LDAP Info**
 - **SAML assertion**
- **Quick-Turn Integration for Mission Applications**
 - **2 Hours – 2 Weeks**
 - **Proven, Perfected Process (CMMI-5)**



U.S. AIR FORCE

RSO Visual





Authorization / Access Control

U.S. AIR FORCE

- **Authorization / Access Control**
 - **Defines Principle, Resource, and Entitlements mapping; ultimately defines a client's rights when interacting with a specific resource**



Access Control Architecture

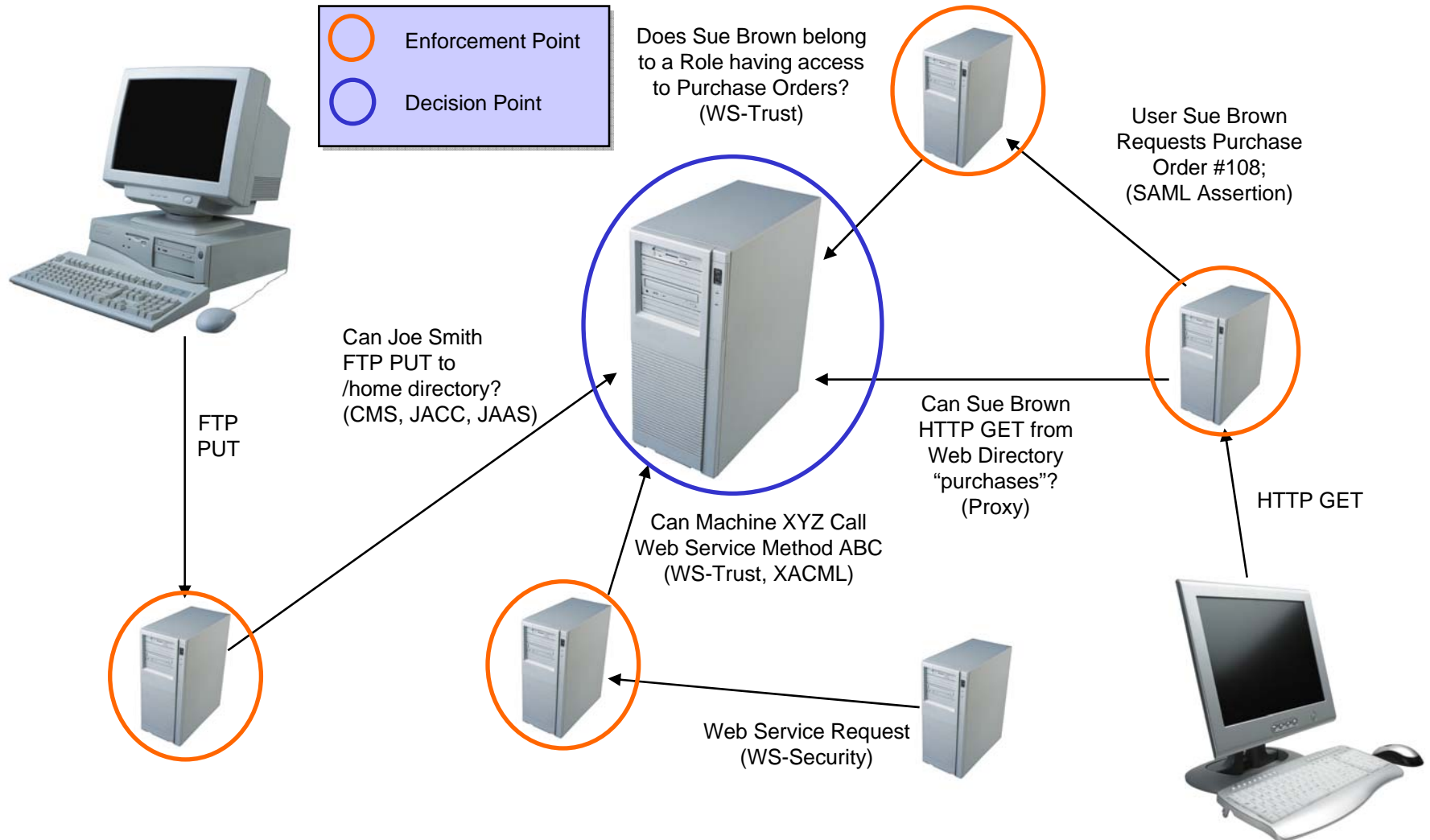
U.S. AIR FORCE

- **Access Control, Authorization, and Entitlements**
 - **Defines what a service, user, or other entity can access**
 - **Access Control, in a Service Oriented Architecture, has a centralized decision service**
 - **A *single* decision service is the “source of truth” for data for the entire enterprise**
 - **The decision service applies policy to data (or “objects”) to understand what services and users have, or do not have, access to them**
- **Access Control, in a Service Oriented Architecture, has multiple, often-decentralized enforcement points**
 - **Multiple access enforcement points act as clients to the decision service and can enforce the decisions made by the decision service over a variety of different protocols and technologies**



U.S. AIR FORCE

Access Control Architecture Visualized





GCSS-AF Authorization Enforcement Mechanisms and Protocols

U.S. AIR FORCE

■ Passive Authorization

■ Authorization by Proxy

- Supported on HTTP, SOAP/HTTP, FTP, MQ, and JMS protocols

■ Implicit Application Authorization

■ Authorization by Container Services

- Container Managed Security (CMS)
- Java Authorization Contracts for Containers (JACC)
- .Net Framework Authorization Services

■ Explicit Application Authorization

■ Coded Authorization Controls

- Java Authentication and Authorization Service (JAAS)
- .Net Framework Authorization Services
- Open Authorization API



U.S. AIR FORCE

Group, Role, and Attribute Based Access Control

- **GBAC, RBAC, and ABAC are all supported**
- **GBAC**
 - **Group-Based Access Control, GBAC, relies upon security administration creating groups for inclusion in ACLs that are consequently attached to resources**
- **RBAC**
 - **Role-Based Access Control, RBAC, relies upon security administration creating roles that designate a business function; users are added to roles based upon their responsibility in the organization**
- **ABAC**
 - **Attribute-Based Access Control, ABAC, is similar to RBAC in that it requires designation of Roles; however, ABAC populates membership to Roles based upon inspection of user attributes versus administrator designation**



GCSS-AF Policy Decision Service

U.S. AIR FORCE

- **Policy Decision Service (PDS)**
 - **Defines relationships between Users, Groups, Roles, Attributes, Resources, Entitlements, and Extended Policy**
 - **The PDS is the central “source of truth” for all policy data**
 - **Policy is defined once, while multiple enforcement entities may enact that policy**
 - **The PDS is communicated with via any of the previously mentioned open authorization protocols**
 - **Extended Policy may be defined that enacts Time of Day restrictions, Number of Query restrictions, etc. that are above and beyond traditional Access Controls**
 - **Policy is defined by Security Administrators (non-technical, subject matter experts in policy) via Point-and-Click interfaces; this abstracts security policy definition requirements from coders and engineers**

Integrity - Service - Excellence



U.S. AIR FORCE

Integrity and Confidentiality

■ Integrity

- Provides services to preserve the format, validity, intention, and identity of messages and data**

■ Confidentiality

- Provides services to preserve the secrecy and privacy of messages and data**



Integrity and Confidentiality Services

U.S. AIR FORCE

■ **Non-Invasive**

- **PKI-Based Mutual SSL**
- **Data Encryption (FIPS 140-2 Compliant) Services**
- **XML Schema Validation**
- **Hashing Services**
- **Virus Protection**

■ **Explicit**

- **Data Encryption Services**
- **XML Schema Validation**
- **Hashing Services**



U.S. AIR FORCE

Identity Management

■ Identity Management

- Provides services to manage client identity information throughout the enterprise**

■ Philosophy

- Identity information is based upon Systems of Record (SOR) within the enterprise**
- Each SOR is responsible for providing attributes for which it owns to the enterprise identity management repository and control system**
- The identity management system serves as the local, enterprise source of truth for all identity information; therefore, sub-servant identity repositories are provisioned and de-provisioned for the central source of truth**



Identity Management Services

U.S. AIR FORCE

■ **Core Infrastructure**

■ **Directory Integration**

- Any-to-Any Directory Integration (LDAP, JMS, Web Service, MQ, Flat File, etc)

■ **Provisioning System**

- Adapters to most major directories and operating systems for provisioning identity data

■ **GCSS-AF**

■ **AF and DoD HR Systems feed to:**

- **GCSS-AF Identity Management Core, feeds to:**
 - Active Directory
 - Netscape Directory
 - Oracle Internet Directory
 - IBM Directory Server

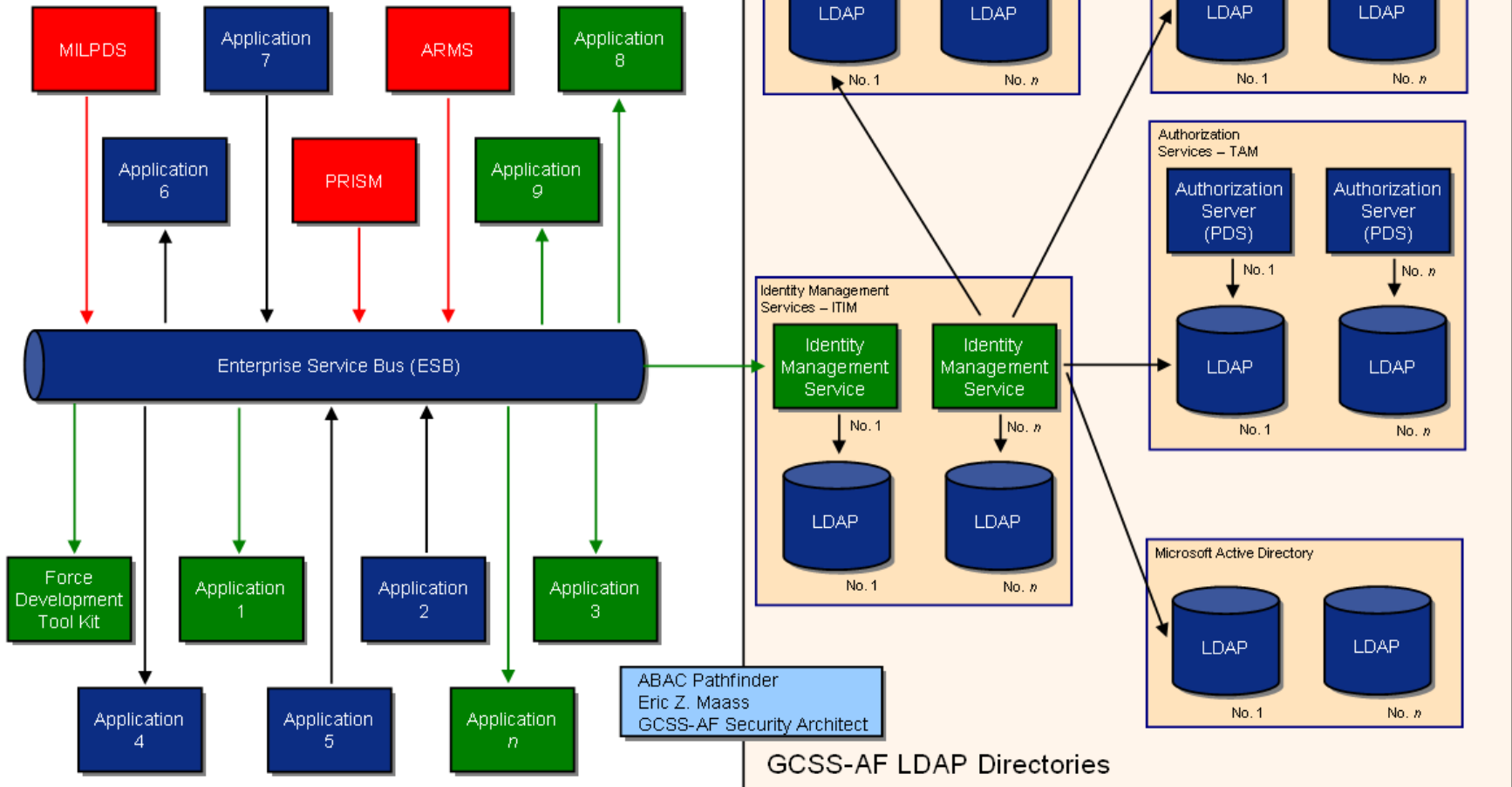
Integrity - Service - Excellence



GCSS-AF Identity Management Cross Section

U.S. AIR FORCE

MILPDS, ARMS, and PRISM are shown here publishing event data to the ESB, while multiple Air Force applications are subscribing to those events (Topic Trees) to receive them. The GCSS-AF Identity Management Services are enlarged here to show it as a subscriber to these Human Resources data events via LDAP.





Identity Management Services

U.S. AIR FORCE

- **Identity Management Workflow Support**
- **Web Services Provisioning (WS-Provisioning)**
- **Directory Service Markup Language (DSML)**
- **Identity Web Service (IDWeb and UDWS)**
 - **Expose enterprise identity data**
- **Client Digital Signature Support**
- **XML Digital Signature Support**
- **Delegated Administration for:**
 - **Operations and Support**
 - **Field Assistance Branch (FAB Help Desk)**
 - **Application Security Administrators**

Integrity - Service - Excellence



U.S. AIR FORCE

Self Service

■ Self Service

- Largely part of Identity Management, Self Service capabilities allow users and administrators more flexibility to interact with their accounts and services without infrastructure engineering support or help desks



Self Service Capabilities

U.S. AIR FORCE

- **Self Registration**
 - **UID/PW and CAC Supported**
- **Password Reset**
 - **Challenge/Response Questions Supported**
- **Automated Role Request**
- **Automated “Form 41” Request**
- **Automated “Form DD 2875” Request**
 - **Includes Workflow Automation Engine**
- **Self Servicing User Profile via Air Force Portal**



Example: Role Request Screen

U.S. AIR FORCE

Role Request Automation
Version 1.0

Portal Home

Select Application

Step 1 of 3

Instructions

This process will guide you through submission of a request for AF Portal Application access. This request will be submitted for approval and reviewed by the application owner.

Upon approval, a confirmation of access will be emailed to you. You will be able to access the requested application using the URL supplied in the confirmation email.

Step 1:
Select an application and click the **Next** button. To close the window and cancel processing, click the **Cancel** button. Select **A - Z** to filter the list on another starting letter.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z ALL

<input type="radio"/>	AF MICAP	AF Mission Capable Reports Builder [.mil/.com]
<input checked="" type="radio"/>	AFCT	Air Force Congressional Tracking
<input type="radio"/>	AFEMS	A Fictional Entry for Microsoft
<input type="radio"/>	ATOMS	Air Force Technical Order System Information [.mil/.com]
<input type="radio"/>	BCS	Base Customer Service
<input type="radio"/>	DAASINQ	Defense Automatic Addressing S [.mil/.com]
<input type="radio"/>	PROCT	Personnel Information Request

Clear Cancel Next >

© 2006, United States Air Force [Privacy Policy](#)

Done Local intranet

User Step 1 – Select Application

- Initial selection screen to allow the user (requestor) to indicate which application to request access.
- Allows filtering by initial letter of abbreviated name A – Z or ALL (ALL selection shown)



Audit, Misc. and Advanced Technologies

U.S. AIR FORCE

■ Audit Services

- Provide a means for accountability regarding actions pertaining to the security infrastructure**

■ Advanced Technologies

- Services being fielded as prototypes for advanced concepts in information assurance**
 - Partnerships with industry and government intelligence agencies**



Audit Services

U.S. AIR FORCE

- **All Points Audited**
- **Audit Logging**
 - **Supplied at each level of the security sub-system**
 - **UID**
 - **IP Address**
 - **Time / Date Stamps**
 - **URL Transactions and Addresses**
 - **Platform Details**
 - **Audit data maintained and archived**
 - **Common Audit and Reporting Service (CARS) allows for open XML standard for audit data making it reusable, importable, and addressable by various security services and commercial products supporting CARS**
- **Enterprise System Monitoring**
 - **Multiple products in use to measure and monitor system usage for security purposes**
- **Complex Event Processing**
 - **Allows for aggregation and alerting on complex streams of system events for the purpose of intrusion detection and prevention at the application stack layer**

Integrity - Service - Excellence



Network Security Services

U.S. AIR FORCE

■ Akamai Security Services

- Sure Route: utilizes vast network to route around “problem areas” on the network while optimizing performance**
- Origin DNS no longer exposed to public**
- Intrusion Detection**
- Site Shield allows only specific, controlled points of entry into sensitive networks**
- Availability**
 - Content and Services become highly survivable, geographically dispersed, and fast responding**
- Capacity**
 - Costly origin servers are taxed less; they only perform duty when need be and allow Akamai to proxy content and services to users for delivery**