AEROSPACE
Assuring Space Mission Success

Software Security Design Analysis For Net-centric NSS Systems

Richard Yee, CSSLP
Information Assurance Technology Department (IATD)

Ground System Architectures Workshop 2010

Computers and Software Division (CSD)
Engineering and Technology Group (ETG)
The Aerospace Corporation
1-4 March 2010

Honoring the Legacy. Assuring the Mission.
50 YEARS

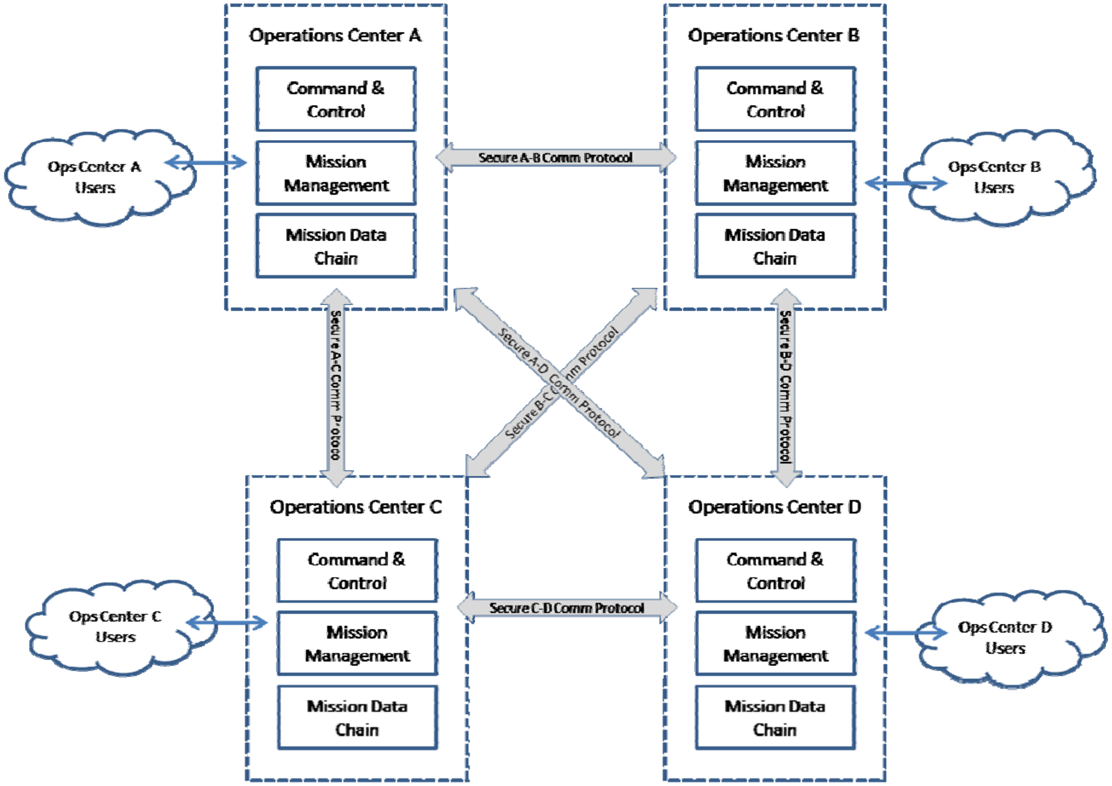
The Net-centric Charter

- DoD Joint Vision 2020 - Promotes information superiority as a critical component to full spectrum dominance on the battlefield

- Net-centric Warfare (or Operations) – US DoD military doctrine based on the premise that the ability to share information and services across all DoD weapons, sensor and C2 systems can lead to a competitive warfighting advantage

- Global Information Grid (GIG) – US DoD communications framework for supporting Net-centric Operations through the inter-connection of weapons, sensor and C2 systems across all military service branches

How Do Existing Systems Typically Share Data?



Stovepipe Design Characteristics

- System-to-system interactions occur via application-specific protocols conducted over dedicated and encrypted network connections
- Establishing new system-to-system interactions usually involves additional hardware, software and maintenance costs

Security Risks

- Coarse-grained security controls for system-to-system interactions results in the establishment of a high level of trust between systems
- Potential for introducing vulnerabilities due to the “ad-hoc” nature of developing new interactions

Any Security Benefits?

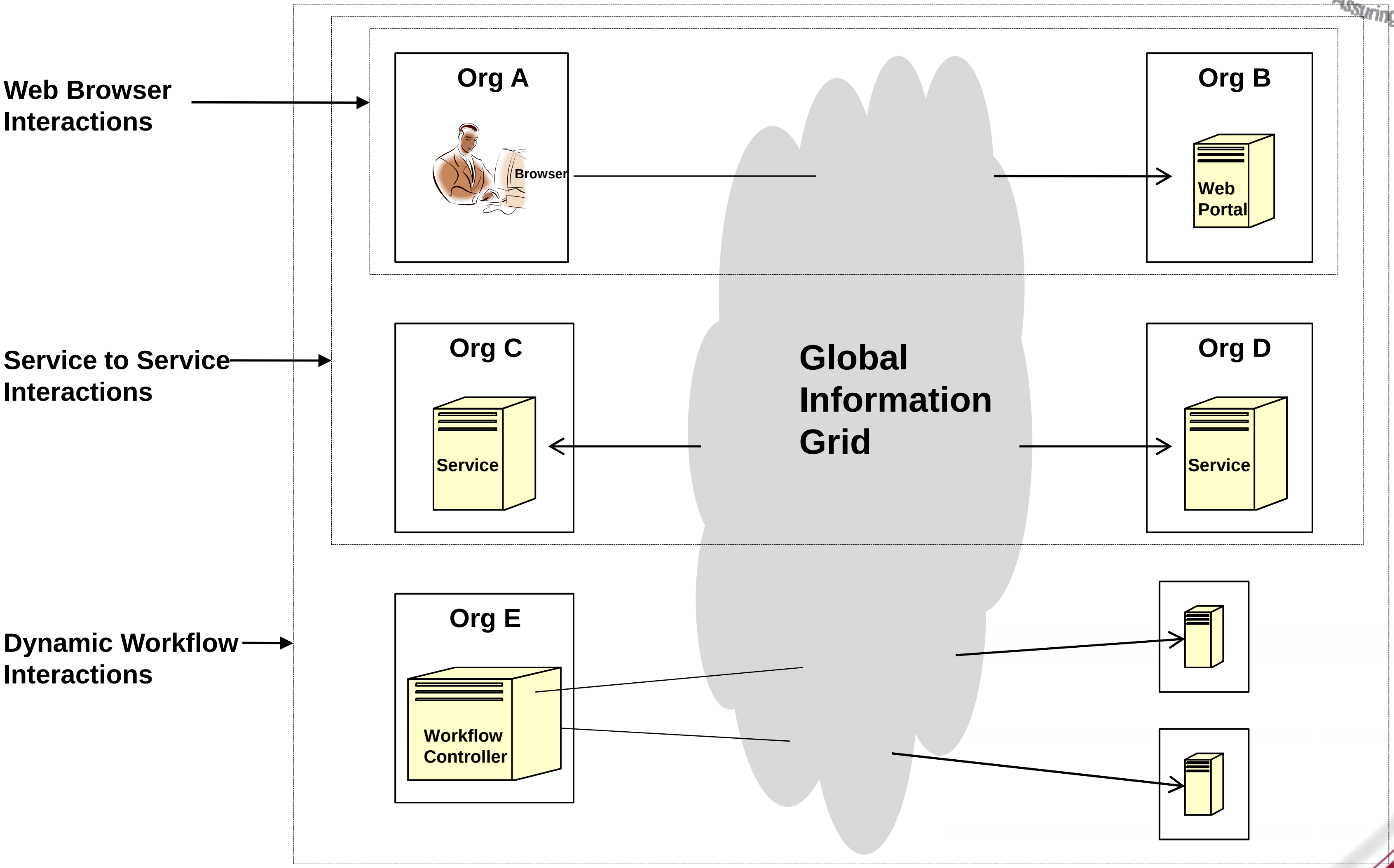
- Other than dedicated interactions, stovepipe systems are basically closed to the rest of the world
- Limited user population simplifies security policy management

Developing Software for Future Ground Systems

- Service-based software architectural design appears to be a good fit for enabling agile C2 nodes that can support Net-centric Operations
  - *Software systems are decomposed into discrete services that map to the mission operations and planning workflows of a SOC*
  - *Services have well-defined interfaces and are accessed using standard discovery and communication protocols*
  - *Service definition focuses on reusability in multiple, different application workflows*
  - *Governance policies provide predictable control over the lifecycle of services*

- The web services set of technologies appears to be a popular choice for implementing a service-based software architecture
  - *Designs based on SOAP and WS-* standards*
  - *Designs based on Representational State Transfer (REST)*
  - *Standards and best practices exist for securing service interactions*

Levels of Net-centric Interactions



Information Assurance In The Net-centric World

- Fundamental system security requirements never really change
  - *Identify and authenticate users/systems*
  - *Authorize user/system actions*
  - *Audit user/system actions in support of accountability*
  - *Protect the integrity and confidentiality of data in transit, process and storage*
  - *Protect system availability*

- Traditional IA mechanisms and policies associated with closed systems are still applicable, but not sufficient, for supporting a NetOps-enabled system

Net-centric Operations Expands Our Security Concerns

- Protection for interactions that potentially cross multiple security domains and use non-dedicated, potentially unsecured network connections
- Coarse-grain security controls are no longer adequate
  - *Support for workflows that are dynamically constructed from multiple services*
  - *Support for workflows comprised of services where each service is potentially owned and managed by a different organization*
- Security policy management increases in complexity
  - *User population is potentially very large*
  - *User population is not necessarily known upfront*
  - *User population is highly dynamic*
- Having a Net-centric Operations “door to the world” increases the risk of various cyber threats
  - *Denial-Of-Service (DOS)*
  - *Attack and Penetration*
  - *Data Exfiltration*

What is the Potential Impact of Net-centricity on System and Software Architecture?

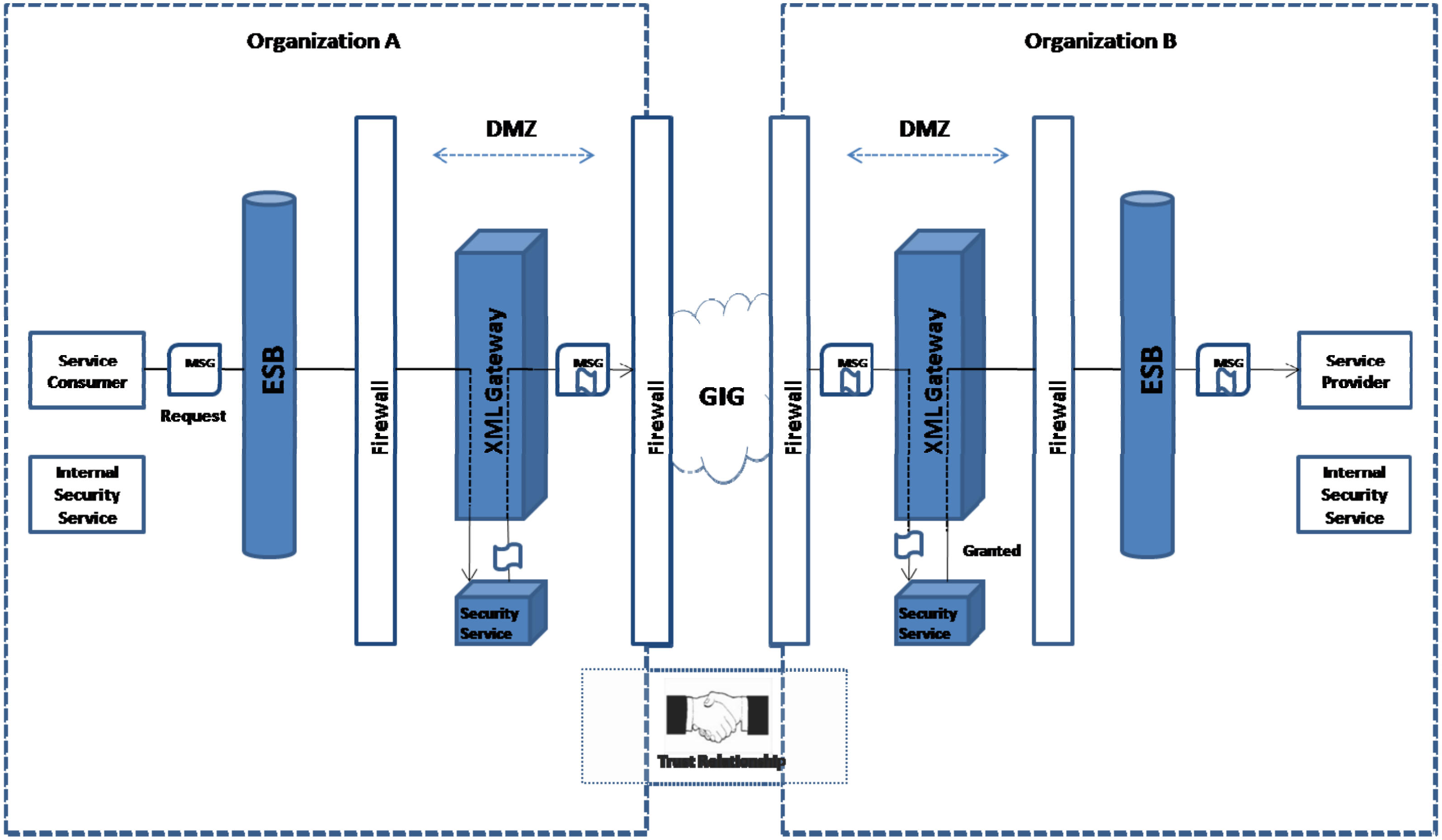
- *System architecture must be designed to support secure, flexible interactions with the outside "GIG" world*
  - Establishment of Demilitarized Zones (DMZs)
  - Firewalls/Proxies
  - Intrusion Detection Systems (IDSs)
  - External/Internal Resource Partitioning

- *Application infrastructure must become security aware*
  - Mechanisms for authenticating users/systems
  - Mechanisms for controlling access to service-based resources
  - Transport or message-level integrity/confidentiality protection

Policy Management and Net-centricity

- Application security policies for closed systems with limited user populations are fairly easy to understand and manage
  - *Centralized management of user security profiles for authentication*
  - *Simple user->permissions or Role-Based Access Control (RBAC) policies for authorization*
- A SOC exporting NetOps services can become quickly overwhelmed having to solely manage security policies that support the dynamic user populations of the Net-centric world
- The SOC authority may choose to offload, or delegate, a portion of policy management responsibilities to other organizational entities within the Net-centric user population
  - *A Memorandum Of Agreement (MOA) is formed with an organizational entity*
  - *The MOA allows the organizational entity to define a policy that dictates which of its users will have access to the NetOps services provided by the SOC*
  - *The MOA provides the basis for implementing a system-to-system trust relationship between the SOC and the organizational entity*

Conceptual Secure Service-Based Architecture Implementation



Information Assurance, Architecture and Net-centric Operations

- Cyber threats become an increased risk as we transition from closed systems to NetOps-capable systems

- Traditional IA policies and mechanisms for closed systems must be augmented by policies and mechanisms that specifically address Net-centric Operations

- Mitigating the risks of cyber threats requires us to design security into our systems from the ground up
  - *Design security into the system at the System Architecture level*
  - *Design security into the application at the Software Architecture level*

Additional Information

Contact Information

Name: Richard Yee

Email: Richard.F.Yee@aero.org

Phone: 310-336-2081

Detailed Report

Name: Software Security Design Analysis for Net-Centric NSS Systems

Aerospace Report #: TOR-2009(8550)-16

Questions?

AEROSPACE
Assuring Space Mission Success

Thank you

50 YEARS
Honoring the Legacy. Assuring the Mission.

Backup Charts

Net-centric Operations for Satellite Ground Systems

- A Satellite Operations Center (SOC) may want to provide data products and services to individuals and systems in other organizations

- Some candidate functionality exposed as NetOps services
  - *Resource Planning/Scheduling*
  - *Distributed Mission Planning*
  - *Status and Health*
  - *Mission Data Chain Products*

- Functionality internal to a SOC and not likely exposed as NetOps services
  - *Real-time Telemetry Processing*
  - *Real-time Track Processing*
  - *Command Processing*

Architectural Security Design Patterns

- Security Design Pattern – Security specialization of a design pattern, which is a time-tested, reusable solution to a design problem that tends to recur across systems

- Formally defining a design pattern usually consists of:
  - *Naming the pattern*
  - *Describing the problem, solution and any impacts*
  - *Providing examples*

- Provides a common language for engineering groups to effectively and efficiently communicate design ideas

- Some key security design patterns that support Net-centric Operations
  - *Basic Push/Pull Authorization Models*
  - *Brokered Authentication*
  - *Service Perimeter Guard*

A Basic Vocabulary for Authorization Design

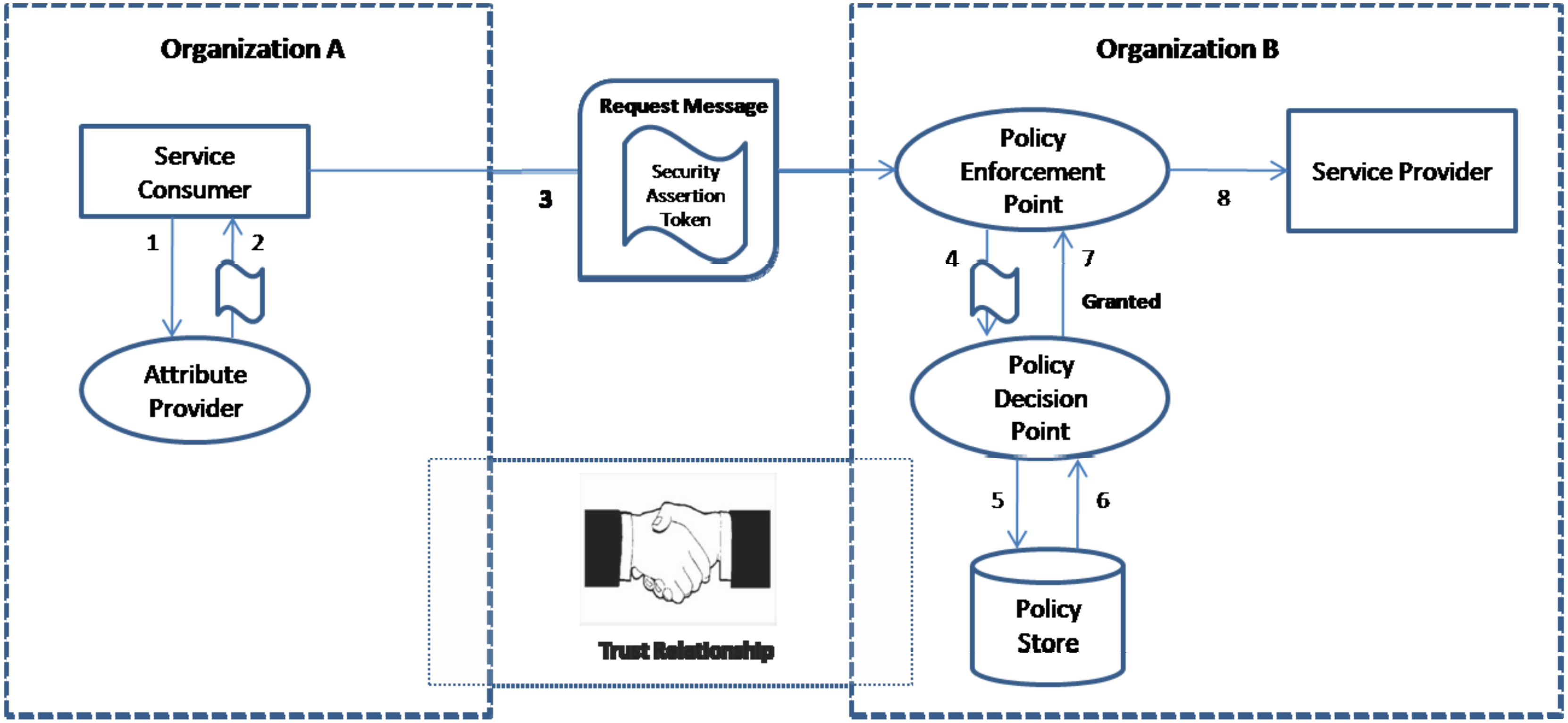
- Policy Store (PS) – Responsible for storing authorization policies

- Attribute Store (AS) – Responsible for retrieving or generating attribute-based security tokens in response to queries

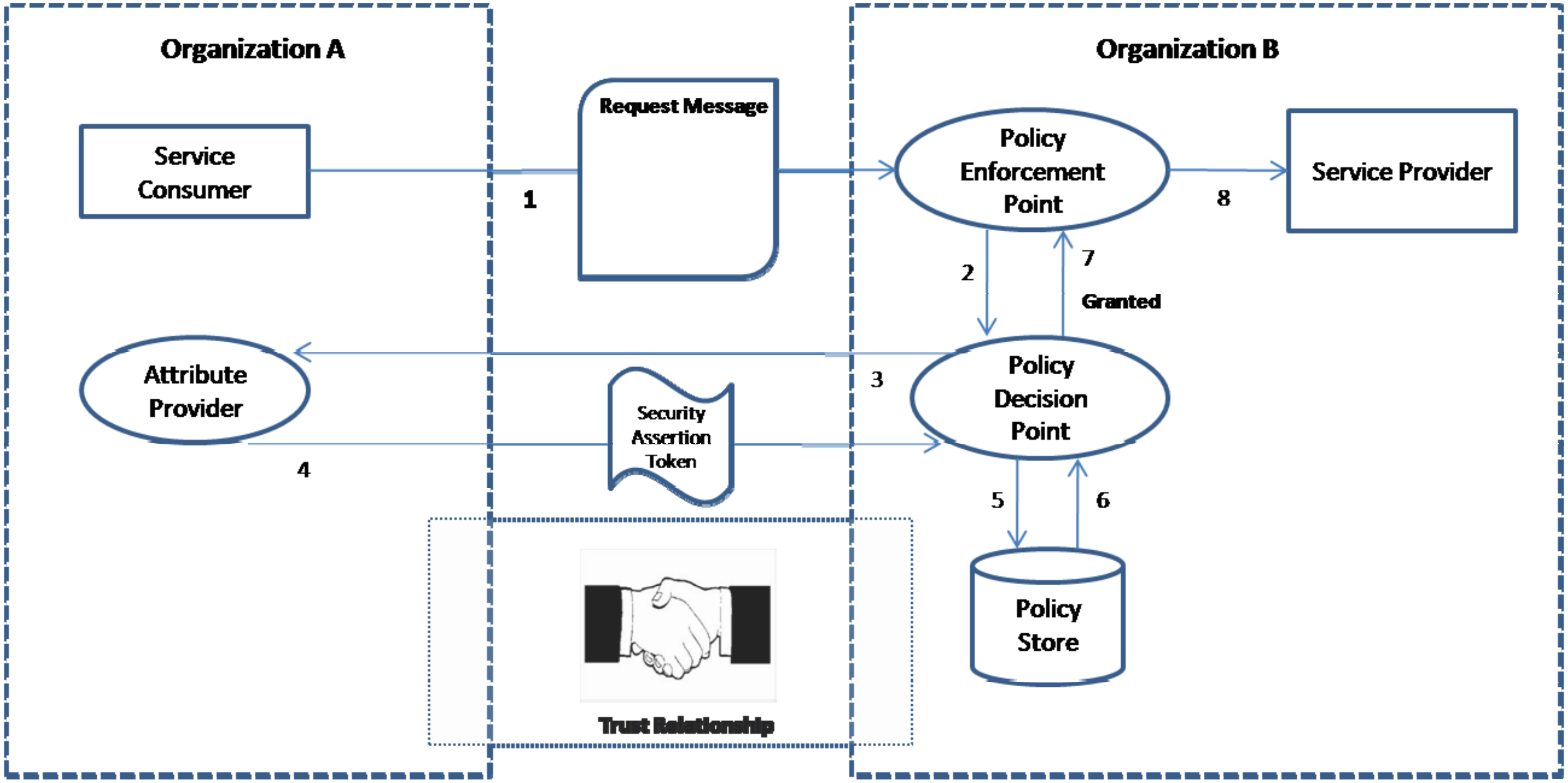
- Policy Decision Point (PDP) – Responsible for deciding whether to grant or deny access based on a calculation of attribute assertions associated with the requesting user and the authorization policy in place to protect access to services

- Policy Enforcement Point (PEP) – Responsible for granting or denying access to a protected service based on the decision it receives from the PDP

Push Authorization Model



Pull Authorization Model



Brokered Authentication Pattern

- Problem
  - *In the NetOps model, where there is a many-to-many interaction cardinality between consumers and services, and there is the potential for dynamic workflows, support for direct consumer-to-service trust relationships is not easily managed*
- Solution
  - *Introduce a Broker Security Service (BSS) into the organization's enterprise that is responsible for establishing organizational-level trust relationships*
  - *A consumer authenticates to its organization's BSS*
  - *The BSS issues a security token to the consumer that contains assertions (e.g. identity, organization affiliation, authorizations,…,etc.) acceptable to target services for authenticating (and possibly authorizing) the consumer*
  - *Potentially a design element of the Push/Pull Authorization models*
- Impacts
  - *The Broker Security Service can become a single point of failure for cross-organizational interactions, so proper fault management and high availability are key quality attributes*
- Implementation Technologies
  - *Public/Private Key Certificates and Public Key Infrastructure (PKI)*
  - *Security Assertion Markup Language (SAML) security tokens*
  - *WS-Trust Security Token Service (STS)*
  - *WS-Security (WSS)*

Service Perimeter Guard Pattern

- Problem
  - *Directly exposing NetOps services to GIG consumers can lead to several security risks*
    - Consumers have direct access to private network that the NetOps services reside on
    - Each NetOps service must be security aware (authentication, authorization,…,etc.)
    - NetOps services are directly exposed to a variety of cyber threats (e.g. DoS)
- Solution
  - *Introduce a Service Perimeter Guard boundary controller that is capable of proxying GIG consumer requests at the application message level and perform security functions such as authentication, authorization and availability protection*
  - *Potentially a design element of the Push/Pull Authorization models*
- Impacts
  - *All NetOps consumer-to-service interactions require intermediate processing by the Service Perimeter Guard, which can substantially impact performance*
- Implementation Technologies
  - *Web Service XML Gateway/Firewall*

Establishing a Trust Model for Conducting Secure Net-centric Operations

- Trust Relationship - an agreement between two entities on the policy or rules for sharing information/services
- A Pairwise Trust Relationship at the organizational level seems reasonable to implement
  - *SOC A trusts SOC B to determine which of B's users can access A's services*
  - *SOC B trusts SOC A to determine which of A's users can access B's services*
- A Trust Relationship may be implemented using a Public Key Infrastructure (PKI) (e.g. DoD PKI) and security tokens
- A security token is a form of security credential containing statements that assert facts about the token owner
  - *Common assertions include identity, organization and authorization attributes*
  - *RBAC becomes generalized to Attribute-Based Access Control (ABAC)*
  - *Integrity protected via digital signature (private key of public/private key pair)*
- Complex Trust Models may be too challenging to implement
  - *Trust relationships with multiple levels of delegation (e.g. "A" delegates policy management to "B", which in turn, delegates management to "C")*
  - *Increased management and technical complexity*