IA for GIG Net-Centric Enterprise Services

Track 8: C2 Technologies and Systems

Rod Fleischer, et. al.
SPARTA Inc.
San Diego, CA
rodf@sparta.com

Agenda

- **Introduction**
- **Service Oriented Architectures (SOA)**
  - Security Challenges
  - Strategies for mitigating SOA vulnerabilities
- **Conceptual NCES Security Approach**
- **Recommendations**
- **Conclusions**

Introduction

- **Motivation – we MUST:**
  - Share data (interoperate) with each other
  - Be secure in our communications – lives depend on it
  - Have data available where we need it, when we need it

- **New Service-Oriented Architecture technologies can solve these problems better than ever before**
  - We must explore and understand these technologies in order to apply them effectively

- **No silver bullets**
  - There are still critical security hurdles in the path to SOA adoption
  - We must thoroughly understand these challenges in order to apply the technologies correctly

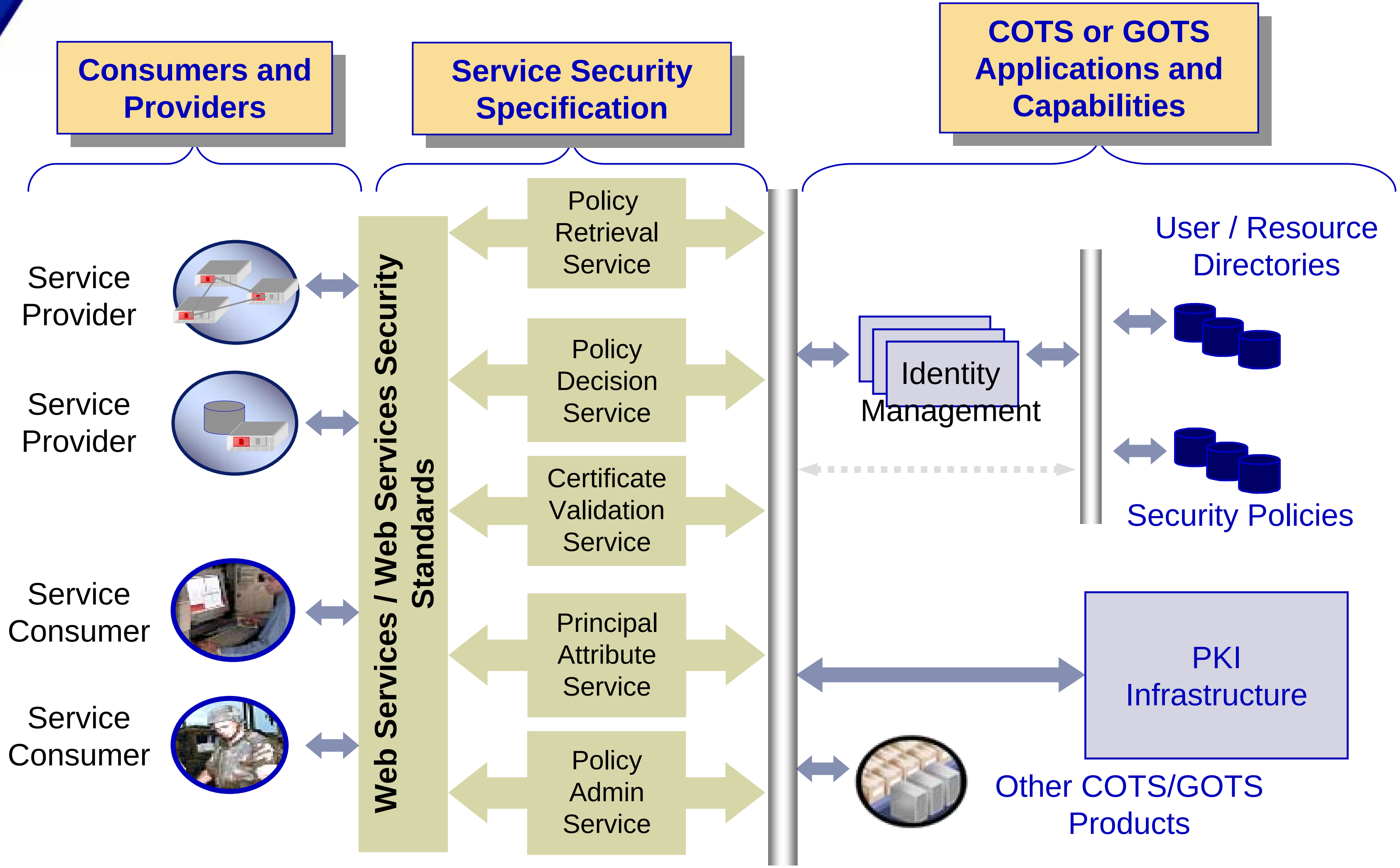
Service Oriented Architectures (SOAs)

Service Oriented Architectures

- **Interoperability is paramount**
  - Individual, loosely-coupled, independent services
  - Web services provide contract of operation
    - Clients need NO knowledge of underlying architecture
    - Implementation can be changed without client impact
  - Standards-based, no proprietary vendor-lock in

- **eXtensible Markup Language (XML) enables interoperability**
  - Simple Object Access Protocol (SOAP) used to exchange XML data
  - Standard, mature protocols
  - Well-structured XML enables firewall inspection
  - Enables Communities of Interest (COI) to exchange information in terminology appropriate to their ontology

Net-Centric Enterprise Services (NCES)



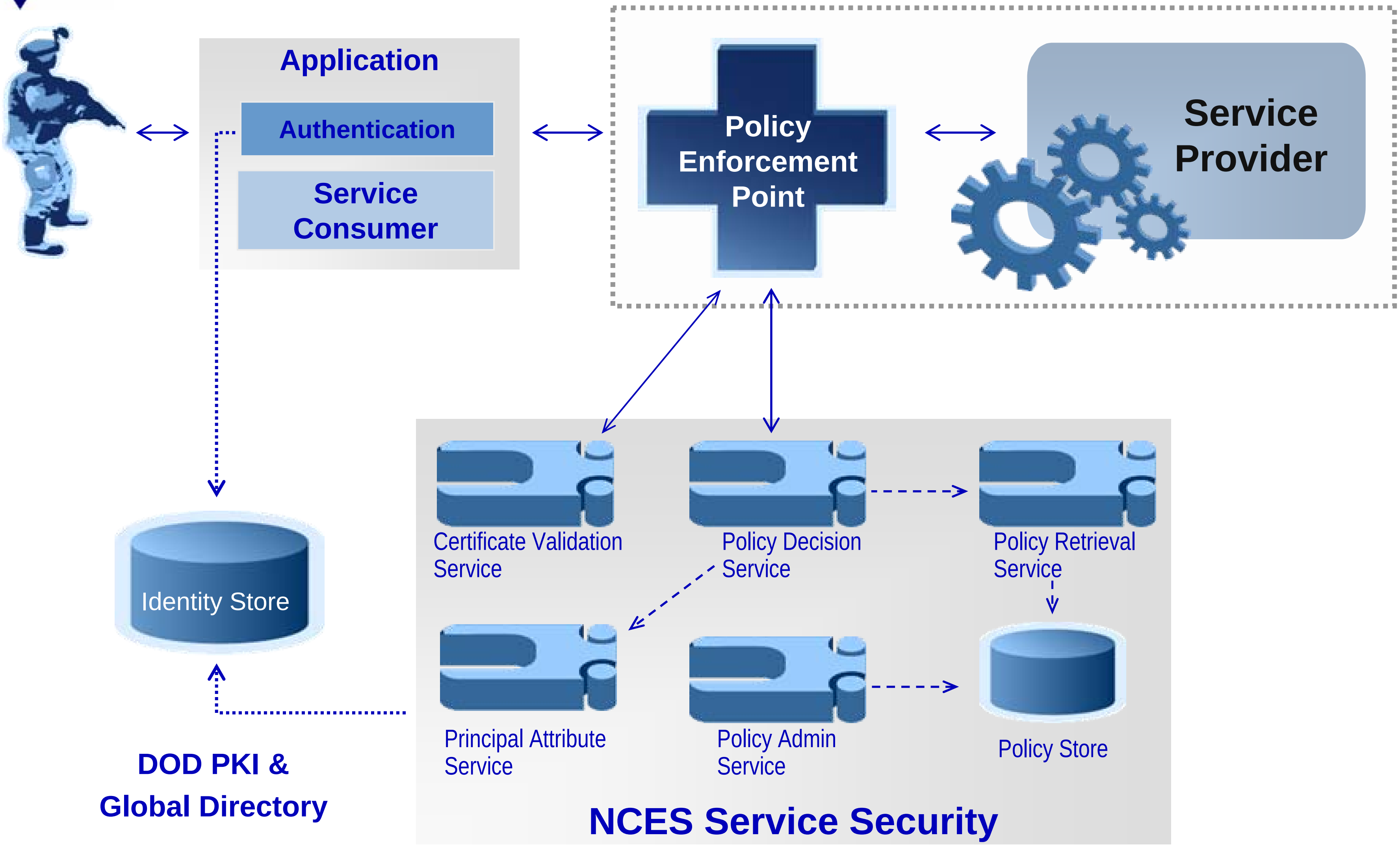
NCES is DoD's program to provide core services, including IA, for SOAs

XML Security Concerns

- **XML is *inherently* insecure due to flexible design**
  - Digital signatures invalidated if formatting changes
  - One-pass processing of encrypted data cannot be guaranteed if fields show up in non-optimal order
  - Potential for recursive, cyclical references to encrypted keys
  - Cryptographic data must be text-encoded to include in XML messages
    - This increases message size and bandwidth utilization

- **All of these could easily be used in Denial of Service (DoS) attacks**

Notional NCES Security Services



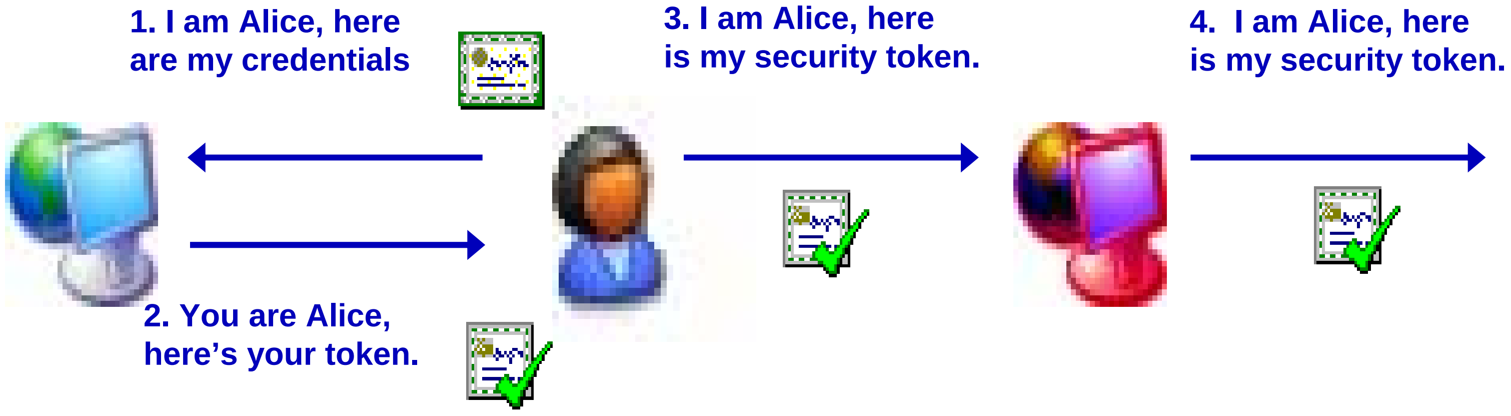
Access Control Assertions

- **Security Assertion Markup Language (SAML)**
  - Asserts client identity, requests access to resources
  - Provides mechanism for distributing policy decisions
  - Can be used as a ticket-granting mechanism
    - Tickets enable Single Sign On (SSO)
    - Indicates “ticket holder successfully authenticated at a particular time with a particular method”
    - Hypothetically vulnerable to replay attack unless precautions are taken

SAML provides great improvements in managing user identities (if precautions to prevent tampering are taken)

Replaying of Credentials

- **If precautions are not taken with Single Sign On (SSO), security tokens can be replayed**



1. I am Alice, here are my credentials

2. You are Alice, here's your token.

3. I am Alice, here is my security token.

4. I am Alice, here is my security token.

- **Security assertions and responses SHOULD:**
  - Include digital signatures
  - Rely on Public Key Infrastructure (PKI) for authentication
  - Include timestamps
  - Indicate specific allowed permissions
  - Be transmitted over SSL-enabled connections

Access Control Policy

- **eXtensible Access Control Markup Language (XACML) is used to define server-side access control policies**
  - Application-independent rules
  - Policies reference other policies
    - Scalability
  - Intelligent combination of competing or overlapping rule sets
  - Application developers can define their own conflict resolution algorithms if desired

- **Can be used for Attribute Based Access Control (ABAC)**
  - Uses attributes of subjects, resources, environment to evaluate rules
  - Much finer-grained than role-based or identity-based policy
  - Security classification labels can be used to create rules
    - Interoperability with Mandatory Access Control (MAC)

Policy is critical – it defines the "acceptable use" of a system, so it MUST be protected against unauthorized modification!

Protection of Policy

- **XACML policies define what is allowed in a system**
  - Therefore critically important to the system
  - Unauthorized modification MUST be prevented

- **Policies should never be transmitted or stored without protection**
  - Digital signatures should be used to guarantee integrity
  - Encryption should be used to guarantee confidentiality
    - SSL-enabled connections would be ideal

Bandwidth Considerations

- **Many GIG vulnerabilities stem from bandwidth starvation**
  - XML is very verbose, many tags for small amounts of data
  - Cryptographic data would need to be text-encoded
    - Increases data size by around 30%

- **Battlefields may have little or no available connectivity**
  - Satellite networks don't have large available bandwidth
  - Mobile Ad-Hoc Networks (MANETs) may not provide adequate wireless coverage of the battlefield

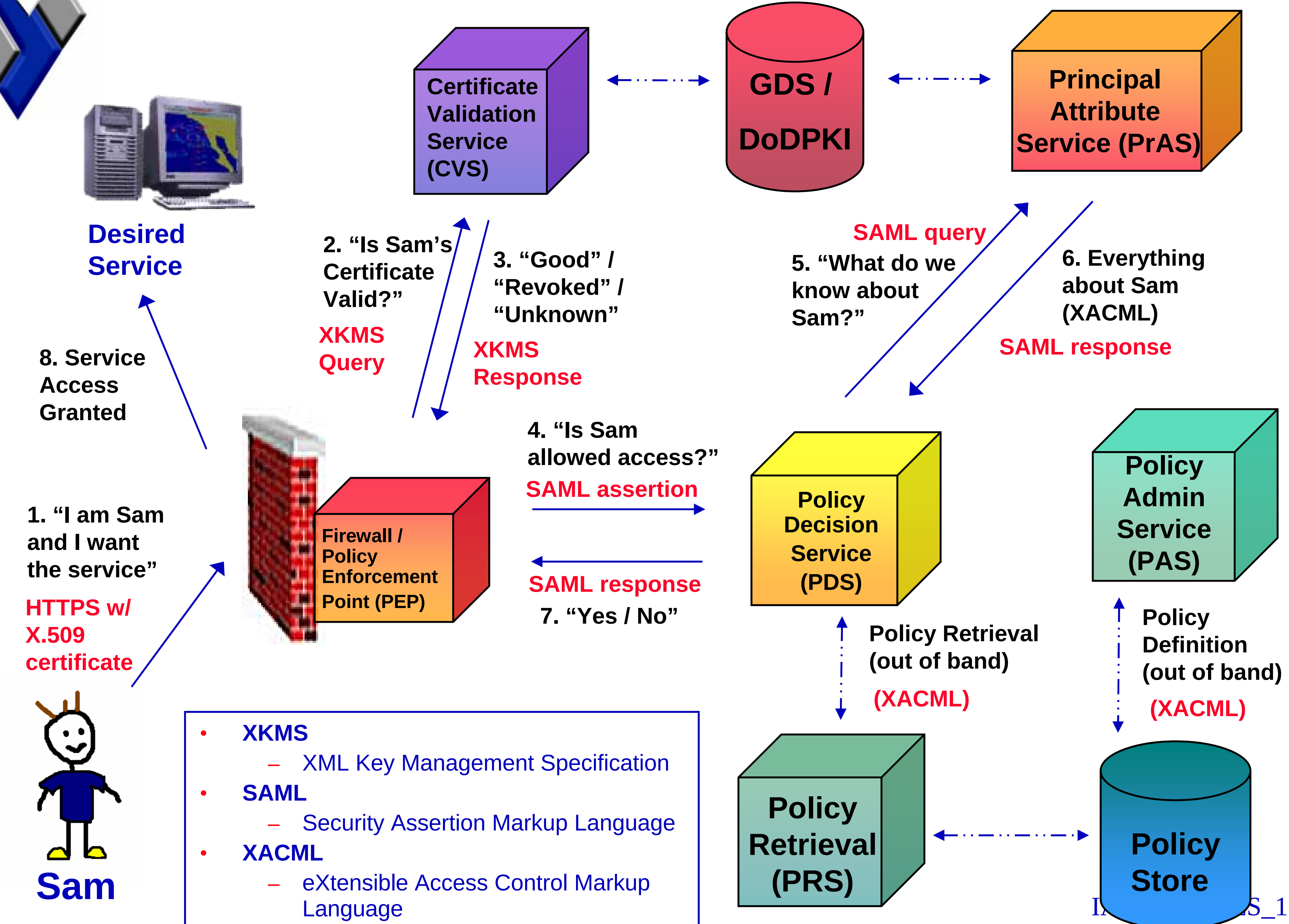
- **Emerging wireless technologies (e.g., 802.11n) may help alleviate the problem, but are still experimental**
  - Bandwidth usage must be considered and minimized when systems are engineered

Summary of Architecture Challenges

- **Policy must be authentic and unmodified**
  - Use digital signatures from policy authorities
  - Transmit policies over SSL
    - Don’t advertise policy to prying eyes, encrypt it
    - Data integrity checks to prevent in-transit modification
- **SAML can improve user authentication and policy enforcement**
  - Proper precautions must be taken to prevent abuse
- **Data MUST be secured, not just the architecture**
  - We must still examine the notional concept of operations in order to effectively apply data security

Conceptual Net-Centric Security Approach

Notional NCES Authentication Process



Certificate Validation Service (CVS)

GDS / DoDPKI

Principal Attribute Service (PrAS)

Desired Service

1. "I am Sam and I want the service"

HTTPS w/ X.509 certificate

Sam

Firewall / Policy Enforcement Point (PEP)

2. "Is Sam's Certificate Valid?"

XKMS Query

3. "Good" / "Revoked" / "Unknown"

XKMS Response

4. "Is Sam allowed access?"

SAML assertion

Policy Decision Service (PDS)

5. "What do we know about Sam?"

SAML query

6. Everything about Sam (XACML)

SAML response

SAML response

7. "Yes / No"

8. Service Access Granted

Policy Admin Service (PAS)

Policy Retrieval (out of band)

(XACML)

Policy Definition (out of band)

(XACML)

Policy Retrieval (PRS)

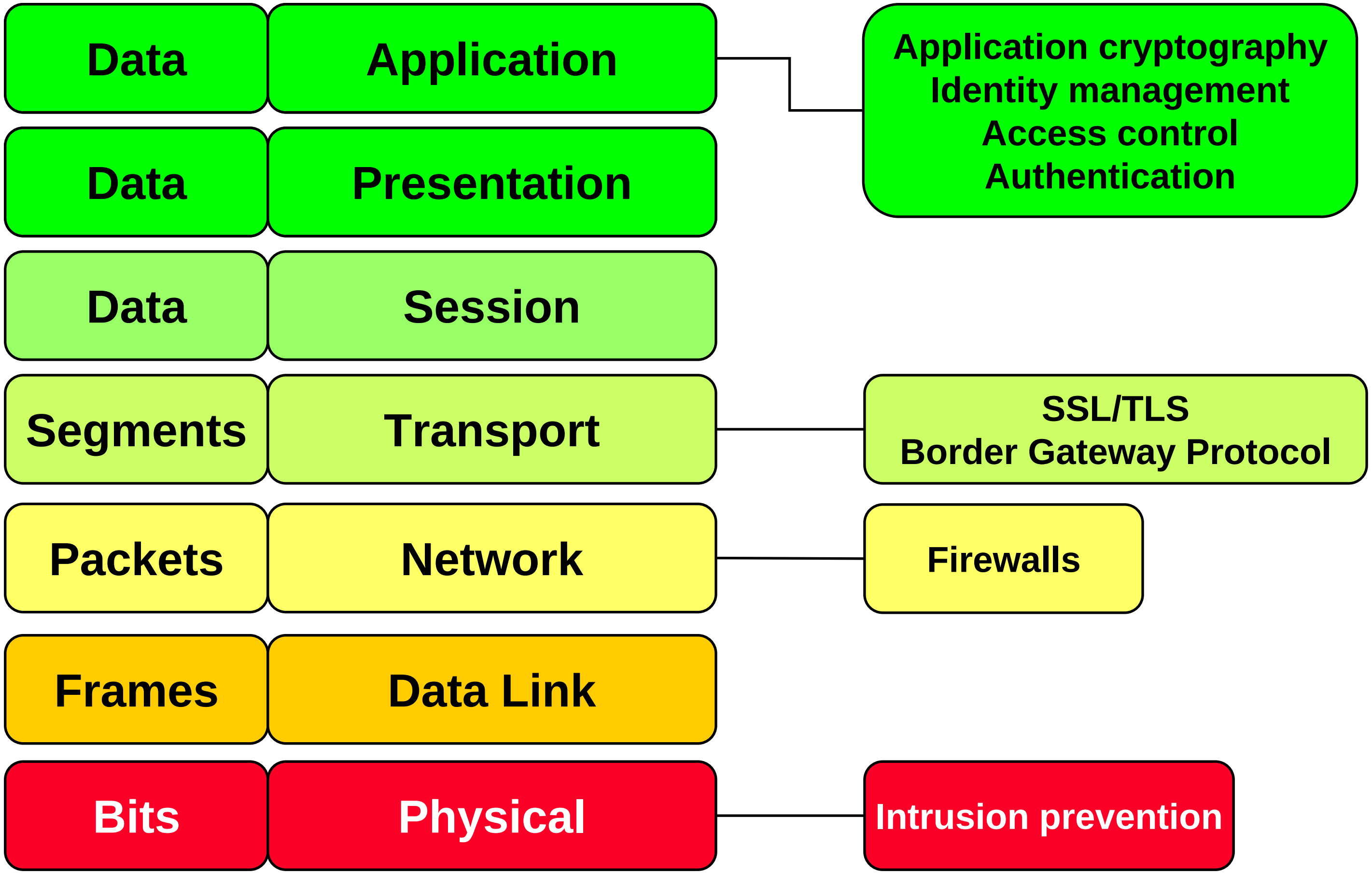
Policy Store

- **XKMS**
  - XML Key Management Specification
- **SAML**
  - Security Assertion Markup Language
- **XACML**
  - eXtensible Access Control Markup Language

Authentication Considerations

- **Federated Single Sign On (SSO) could reduce network utilization**
  - Security tokens prevent repeated queries against PDS
- **Security tokens must be protected against tampering**
  - PDS must apply digital signatures and expiration timestamp
  - PDS must explicitly define specific uses for the token
  - Security tokens should be transmitted in an encrypted fashion
- **User identification should be done via PKI**
  - Common Access Cards (CAC) could be used for identification
  - Contains PKI information in tamper-resistant chip
  - Much stronger authentication than usernames and passwords

Security at Multiple Layers



Data	Application	Application cryptography Identity management Access control Authentication
Data	Presentation	
Data	Session	
Segments	Transport	SSL/TLS Border Gateway Protocol
Packets	Network	Firewalls
Frames	Data Link	
Bits	Physical	Intrusion prevention

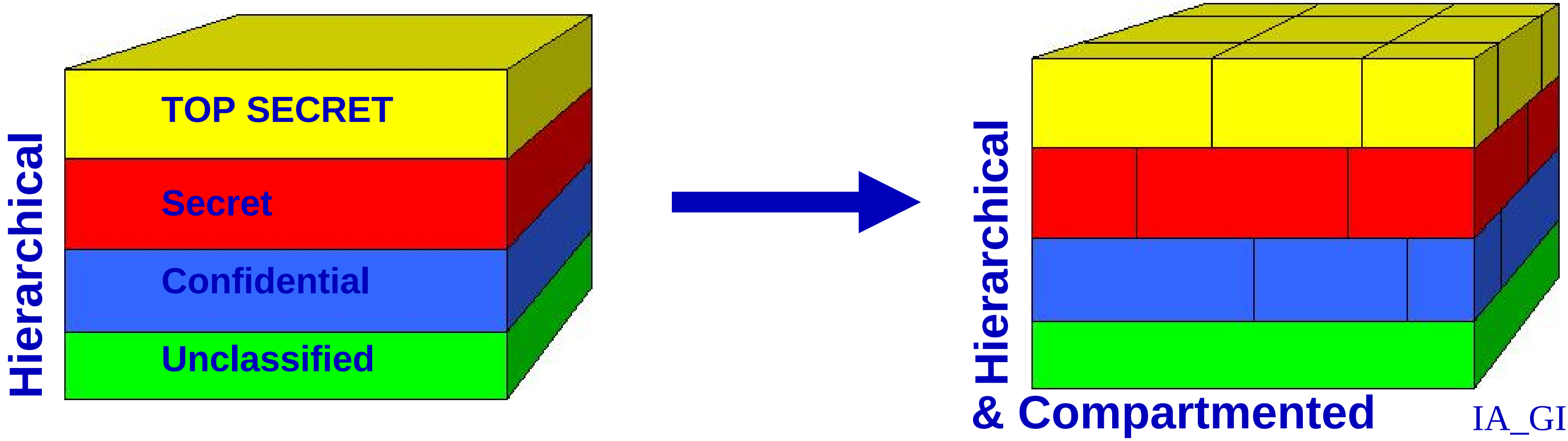
Effective security models pierce the entire network model to selectively protect key layers – Application layer alone is not enough, but too costly to try to protect all layers

Multi-Level Security

- **Enforces Mandatory Access Control (MAC) to prevent security failure**
  - OS provides **trusted** separation between security layers
  - Compartmented networks can be connected to the same machine
    - » Greatly facilitates ability to “Get Things Done”

- **Safely handle sensitive data that requires extreme protection**
  - Prevent disclosure to unauthorized people
  - Know who has seen what information
  - Correctly classify new data

- **Data can be stored both hierarchically and compartmentally**
  - “Vertical” hierarchies control access based on clearance
  - “Horizontal” compartments control access based on “need to know”



Recommendations

Multiple Forms of Access Control

- **Security must be applied at multiple levels to be truly effective**
  - Access control should also be applied in multiple ways
- **Role-Based Access Control (RBAC) should be used to define general access and privilege**
  - e.g. User, System Administrator
  - Coarse-grained access control suitable for governing general access to a system
- **Attribute-Based Access Control (ABAC) should be used for instances where users need specific privilege**
  - e.g. More than minimal privilege (User) and less than maximum (Administrator)
  - Analogous to granting SECRET clearance and access to specific compartments instead of TOP SECRET clearance

Cryptographic Message Syntax

- **XML suffers from security weaknesses due to its flexibility**

- **CMS (RFC3852) was developed specifically for transmitting cryptographic data in a known, accepted format**
  - Optimal parameter ordering for one-pass processing
  - Developed by IETF Information Assurance community
  - Accepted by High Assurance community
  - Mature protocol with high degree of assurance
  - Also known as Public Key Cryptography Standard #7 (PKCS#7)

- **CMS provides significant benefits**
  - Multiple, “nest-able” data protection mechanisms
  - Optimal bandwidth usage due to Abstract Syntax Notation One (ASN.1) Distinguished Encoding Rules (DER)
  - Very prevalent format used extensively in existing technology
  - Not tied to a particular key management scheme

Protect the Data, Not Just the Network

- **The data is important, the network is just a delivery vehicle**
  - Keep data security independent from network infrastructure
    - Less points of vulnerability, failure
    - Easier to accredit
  - Easier to change security or network infrastructure without breaking functionality
    - Data is protected regardless of its path through the network

- **Data in transit**
  - Encrypt data with session keys negotiated between sender and receiver

- **Data at rest**
  - Encrypted data must be stored along with the decryption key
  - The problem becomes key management and secure storage

Group Secure Association Key Management Protocol (GSAKMP)

- **GSAKMP is a Key Management protocol for peer-based systems**
  - Strong cryptographic key generation
  - Complete security policy definition and enforcement
  - Mutual suspicion, access control and authentication
  - Recovery of compromised groups via Logical Key Hierarchies (LKH)
  - Scalable to Internet size with delegated key servers
  - Internet Engineering Task Force (IETF) standard (RFC 4535)

- **Foundation security protocol used to implement Secure Group Objects (SGOs)**

- **SGOs are encrypted objects (such as data files) with an embedded GSAKMP group identifier**
  - Can theoretically be stored or transmitted to anywhere
  - Can only be read by group members
  - Lifespan is limited to lifespan of the associated group

For more information on GSAKMP: http://www.isso.sparta.com/gsakmp/ or http://www.securemulticast.org/

Group Policy Benefits

- **Access control through key management provides higher assurance than policy enforcement alone**

- **GSAKMP provides cryptographic group management**
  - Providing encryption and authentication keys
  - Acting as policy decision and enforcement point
  - Distributing group rules via Group Security Policy Token

- **The Group Security Policy Token provides**
  - Membership rules
  - Rules for acting as key server or group controller
  - Protocols required to access the group for management
  - Protocols required to access group communication
  - Security mechanisms used for the above protocols

Trusted Platform Module

- **Trusted OS provides assurance to store sensitive data**
- **Trusted Platform Module (TPM) provides assurance to store sensitive key material**

- **TPM provides capabilities to:**
  - Securely generate keys, restrict keys to specific uses
  - Provide remote summary of software on system for auditing
  - Seal data to the computer where it was encrypted
  - Bind data to keys located in TPM or another “trusted” key
    - Binding is used to implement Digital Rights Management (DRM), commonly used to control access to digital music

- **TPM dovetails with Multi-Level Security**
  - Data can be bound to a specific compartment
  - TPM can enforce access to keys, which are required to access compartments
    - Access control via key management

Secure Group Objects

- **Use GSAKMP to provide security for data at rest**
- **Secure Group Object (SGO) is defined as:**
  - A group resource encrypted with GSAKMP key material
  - Encrypted data is enveloped with group metadata
  - Data content is encrypted
    - SGO can be published, transmitted, or stored anywhere
  - Only authorized users can access the GSAKMP group and obtain the necessary decryption keys
- **Conceptually similar to TPM binding**
  - GSAKMP maintains access to keys instead of TPM
  - GSAKMP servers can be distributed
    - Multiple, replicated data repositories can be utilized

Conclusions

Conclusions

- **GIG architecture will benefit significantly from SOA IA concepts**
  - Existing protocols should be improved with IA mechanisms
- **Cryptographic Message Syntax should replace XML security protocols**
  - Accepted by High Assurance community
  - No denial of service vulnerabilities due to flexibility of XML
  - CMS payloads can be sent in SOAP messages to add assurance to existing web services
- **Multi-Level Security should be used for compartmenting data**
- **GSAKMP should be employed for cryptographic group key management**
  - Provide access control via key management scheme
  - Higher assurance than simple policy enforcement
  - Infrastructure for replicated databases of Secure Group Objects