Technical Assistance for Health Information Technology and Health Information Exchange in Medicaid and SCHIP

Identity Management for Interoperable Health Information Exchanges

Presented to the NASMD Medicaid Transformation Grants HIE Workgroup - March 26, 2008

Presented by:

John (Mike) Davis, Department of Veterans Affairs
Co-Chair HITSP ICM Workgroup

John Moerke, GE Healthcare
Co-Chair HITSP SP&I Technical Committee

Glen Marshall, Siemens Healthcare
Co-Chair HITSP SP&I Technical Committee

Walter G. Suarez, MD, Institute for HIPAA/HIT Education and Research
Co-Chair HITSP SP&I Technical Committee

Task 1: Define terms

- **Identity Management (IdM)**
  - The set of business processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities within a legal and policy context. - Burton Group™ 2003
  - The capability to manage (create, modify, delete) all user accounts and user profiles (and so forth) that can be identified with each person across the heterogeneous IT environment via a combination of user roles and business rules. [Gartner]
  - A system of procedures, policies and technologies to manage the lifecycle and entitlements of electronic credentials [GSA]

Task 1: Define terms (cont.)

- **Identity and Access Management (IAM)** –
  - Includes authentication and user provisioning (UP) management, password management, role matrix management, enterprise single sign-on, enterprise access management, federation, virtual and metadirectory services, and auditing. (Gartner)
- **Identity Credential Management (ICM) –**
  - Includes the management of credentials within an Identity Management or Identity and Access Management framework.

Identity Management [GSA]

- **A system of procedures, policies and technologies to manage the lifecycle and entitlements of electronic credentials**

Directory Services

Repositories for storing and managing accounts, identity information, and security credentials

Access Management

The process of authenticating credentials and controlling access to networked resources based on trust and identity

Identity Lifecycle Management

The processes used to create and delete accounts, manage account and entitlement changes, and track policy compliance

Technical Assistance for Health Information Technology and Health Information Exchange in Medicaid and SCHIP

Approaches to Identity Management

Two Views of Identity

- **Classic: Classic patient identity systems provide key fields necessary to correlate patient attributes to a record in a healthcare database.**
  - Correlation imprecision is allowed/expected.
  - Classic patient identity systems are not intended to provide (not authoritative for) IT access.

Two Views of Identity

- **Security Focused: Risk-based user identification and credential management. Today even the most basic authentication methods (e.g. password) are provided based upon risk-based assurance of identity.**
  - Security systems are not intended to provide (not authoritative for) identity (create, update attributes, etc.) NOT used for IT access.

Alignment of Concepts

Security Services

- **Primary Context:** Services are provided ***by*** identities (persons)
- **Secondary Context:** Persons (Identities) perform business functions in multiple contexts
- **Management:**
  - Identity can be provisioned
  - Identity can be authenticated
  - Identity can be authorized
  - Access by an identity can be controlled
  - Identity can be federation among members
  - Identity can be known in multiple contexts

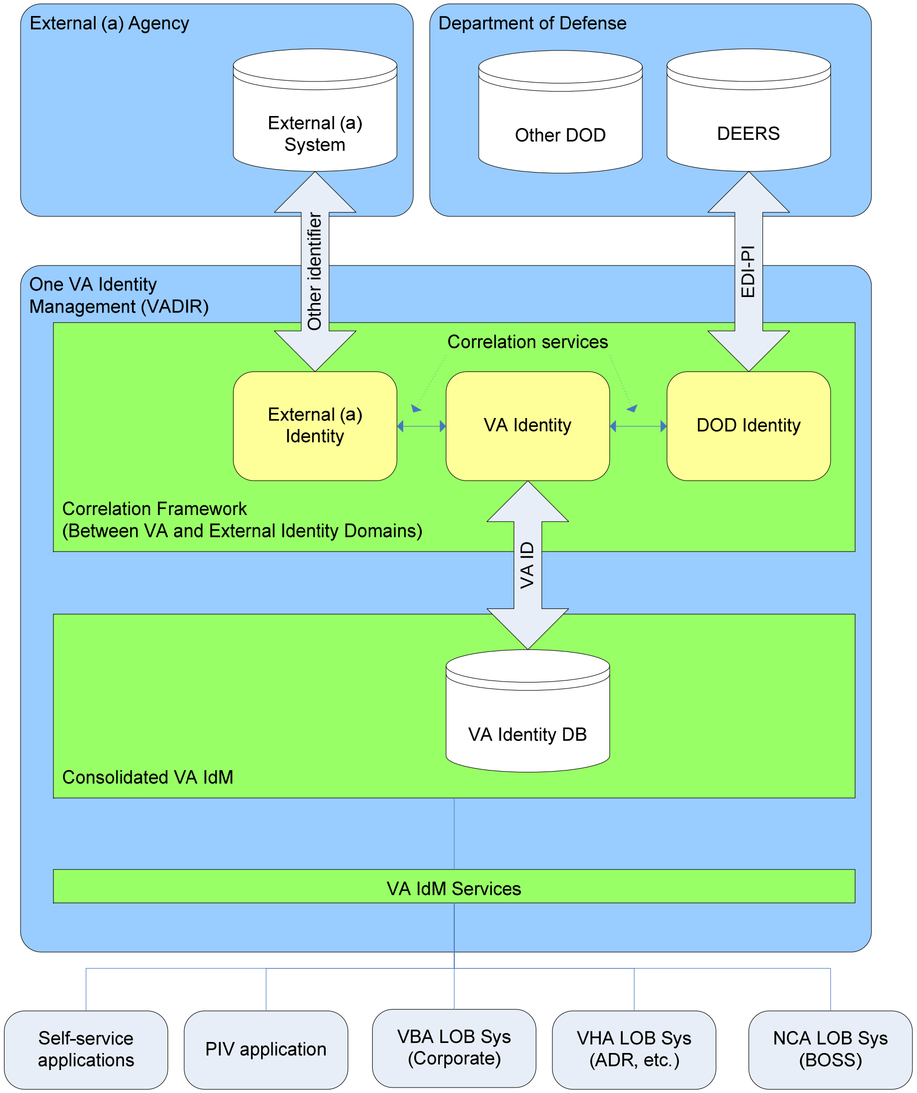
Identity Services

- **Primary Context:** Services and benefits are provided ***to*** identities (persons)
- **Secondary Context:** Multiple organizations collaborate in delivery of services and benefits to persons (identities)
- **Management:**
  - Identity can be consistently defined
  - Identity uniqueness can be identified
  - Identity can be provisioned
  - Identity traits can be updated
  - Identity can be known in multiple contexts

Identity Management Program (VA)

Collaboration

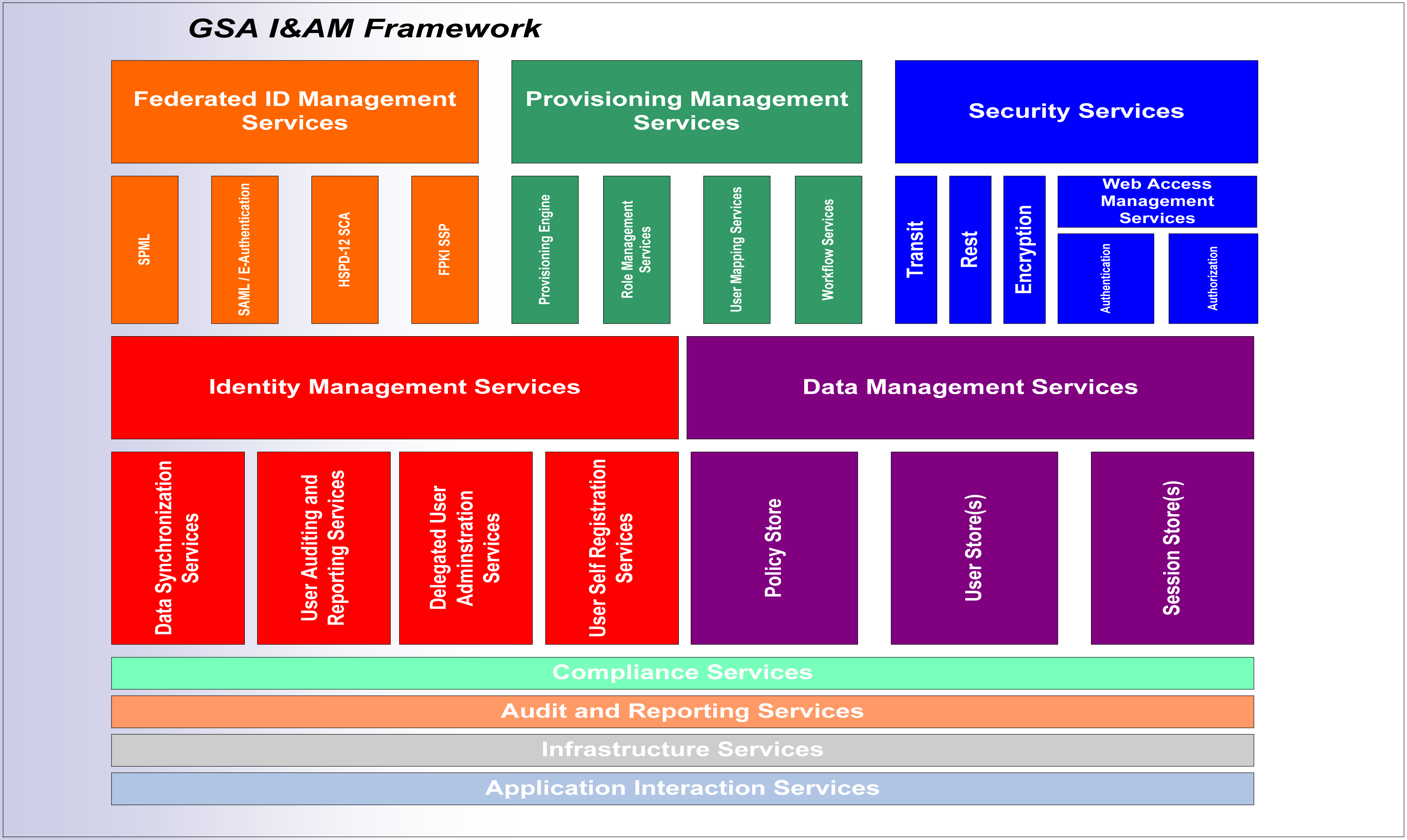
- **OneVA Identity Management**
  - Diagram presents view of possible to-be approach to identity management
  - Correlation service associates external systems’ identities with enterprise identities, enabling sharing information with external agencies
  - Consolidated identity domain covers line of business (LOB) systems
- **PIV**
  - Functions as LOB system
  - Would use identifier on smartcard for integration with enterprise systems
  - PIV issued smartcard controls access to resources
- **e-Authentication**
  - Identity Management DB can be used as additional secure identity database for authentication support for online systems



Relationship of Identity Management to other Business Processes

Authentication, Authorization and Access Control

I&AM Framework



GSA I&AM Framework

Federated ID Management Services

SPML

SAML / E-Authentication

HSPD-12 SCA

FPKI SSP

Provisioning Management Services

Provisioning Engine

Role Management Services

User Mapping Services

Workflow Services

Security Services

Transit

Rest

Encryption

Web Access Management Services

Authentication

Authorization

Identity Management Services

Data Synchronization Services

User Auditing and Reporting Services

Delegated User Adminstration Services

User Self Registration Services

Data Management Services

Policy Store

User Store(s)

Session Store(s)

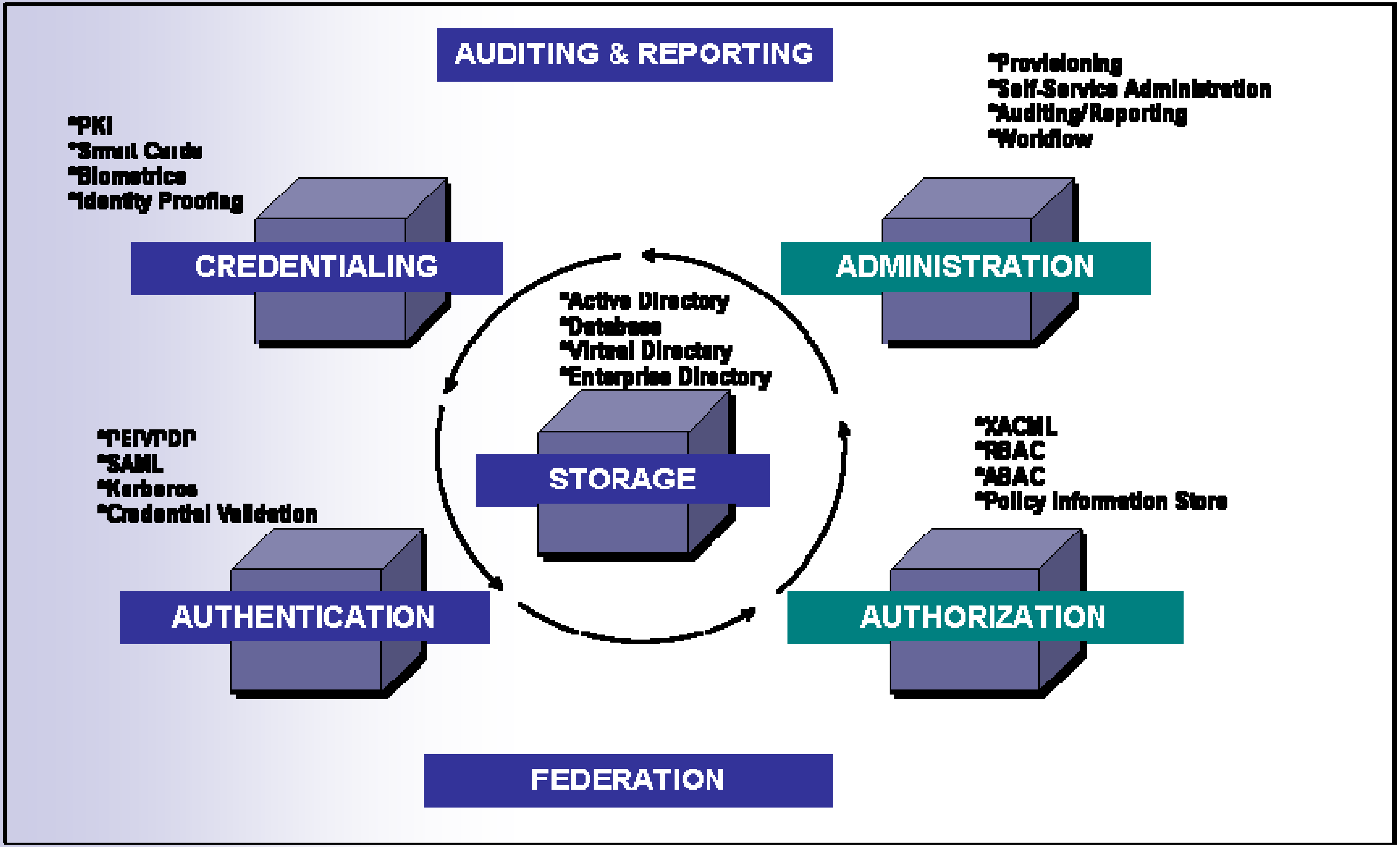
Compliance Services

Audit and Reporting Services

Infrastructure Services

Application Interaction Services

I&AM Core Components



AUDITING & REPORTING

*Provisioning
*Self-Service Administration
*Auditing/Reporting
*Workflow

ADMINISTRATION

*PKI
*Smart Cards
*Biometrics
*Identity Proofing

CREDENTIALING

*Active Directory
*Database
*Virtual Directory
*Enterprise Directory

STORAGE

*PEP/PDP
*SAML
*Kerberos
*Credential Validation

AUTHENTICATION

*XACML
*RBAC
*ABAC
*Policy Information Store

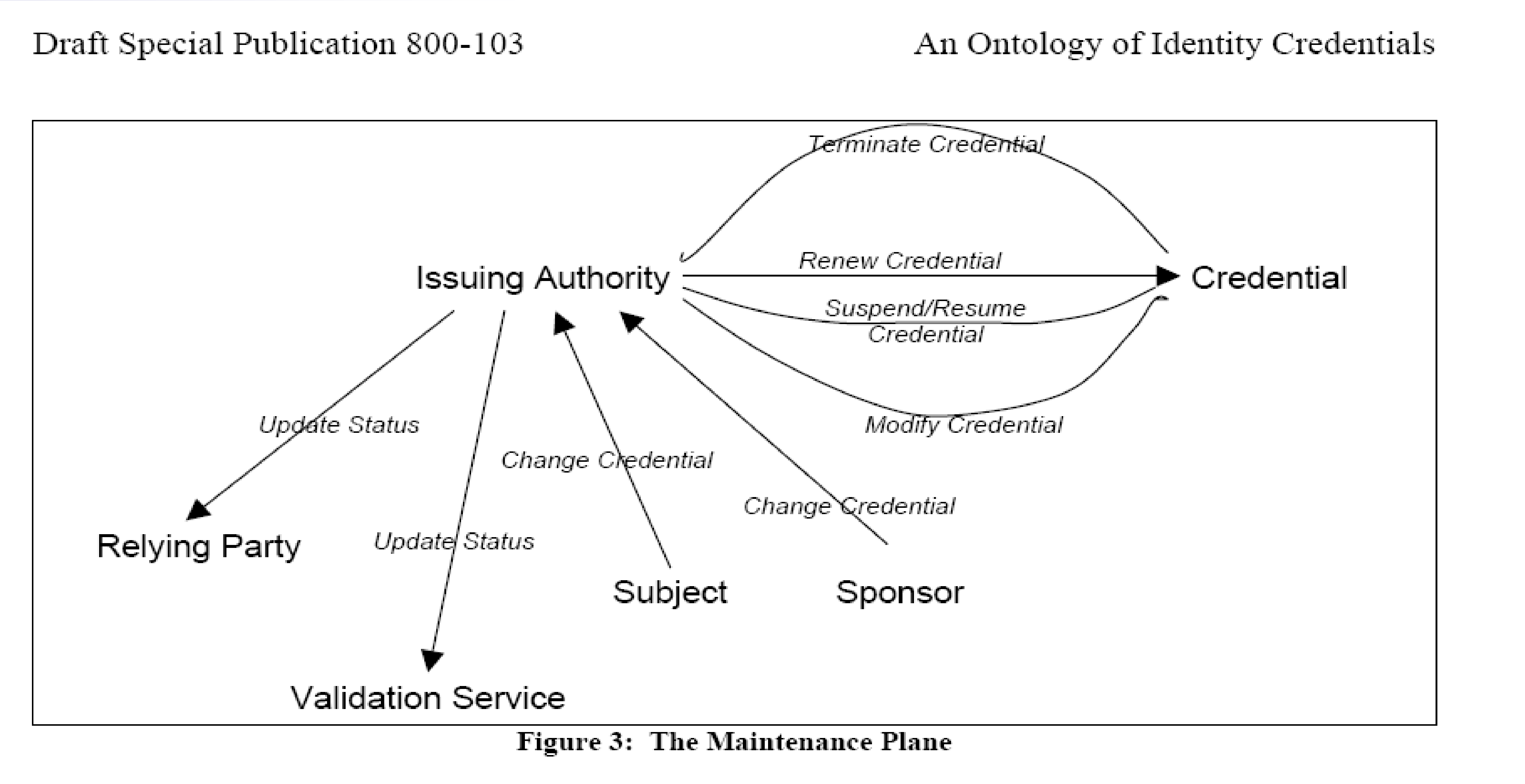
AUTHORIZATION

FEDERATION

Managing Credentials

Changing of user attributes, Revocation

- Maintenance Plane



Draft Special Publication 800-103 An Ontology of Identity Credentials

Figure 3: The Maintenance Plane

Boundaries

Identity Management

Does

- Establish unique identity and manage changes to identity
- Cross reference or correlate diverse systems

Does Not

- Establish what an identity can access
- Assign a specific token to an identity

Authentication

Does

- Provision credentials to authenticated individuals
- Validate an entity’s provided credentials
- Enable digital signature

Does Not

- Assign a unique identifier to every person
- Correlate identities between systems
- Establish what an identity can access

Authentication

Does

- Establish roles/policies for access to resources
- Provide/prevent access to resources consistent with authenticated person’s roles

Does Not

- Assign a unique enterprise identifier to every person
- Correlate identities between systems
- Establish what an identity can access

Access Management: Definition

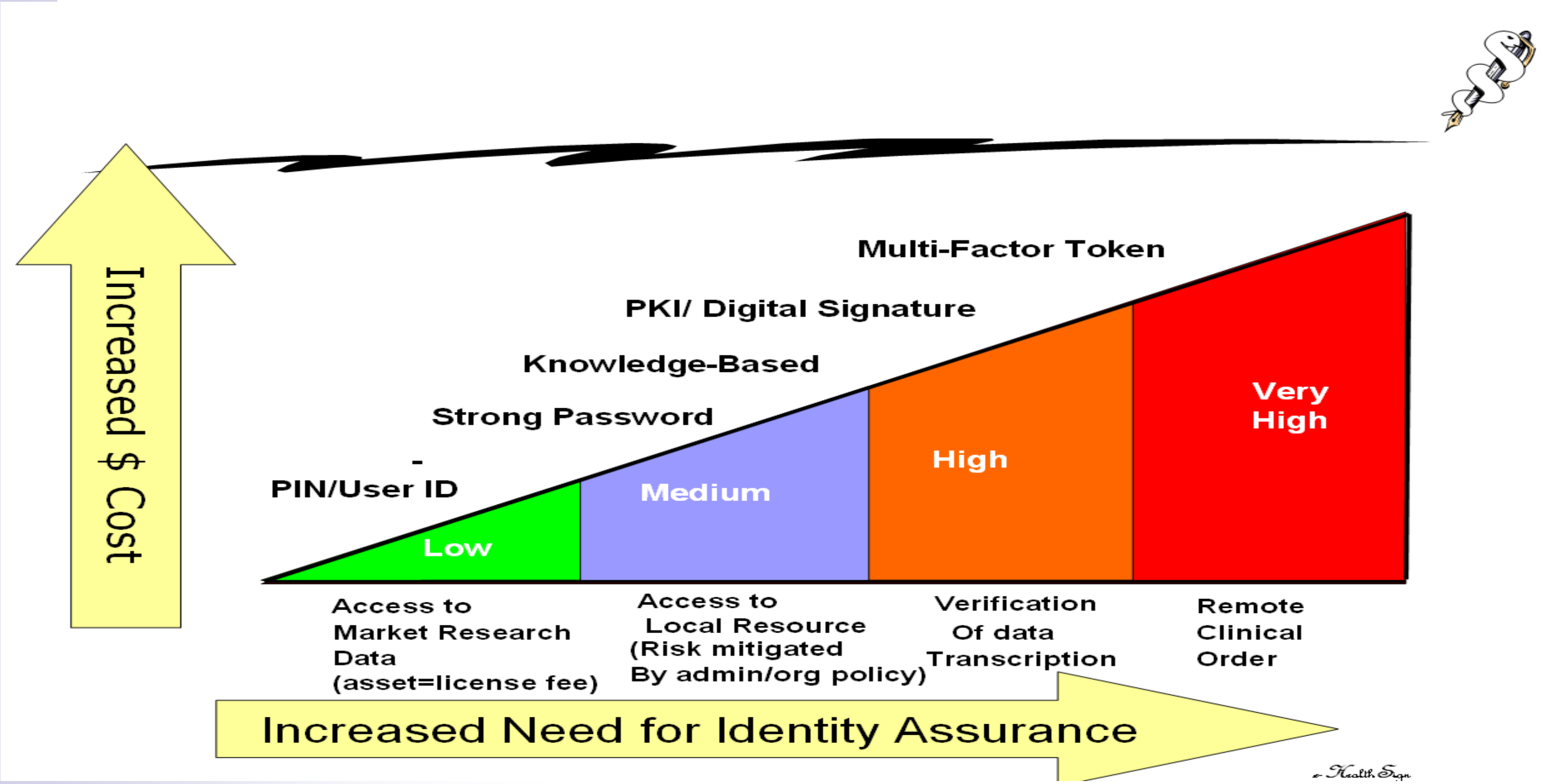
- Mechanism that provides control of entry to and use of protected resources (information systems, buildings, etc.)

Access Management: Definition

- An Access Management system is responsible for determining, based on person’s unique identity, person’s assigned role and their having been authenticated, what assets the person should be allowed to access/use.
    - Role Based Access Control
    - Application Integration
    - Delegation
    - Authentication
    - Authorization
- Localized enforcement of centrally managed security policies using roles or business rules

Federation

- E-Authentication Initiative
- SAML – Security Assertion Markup Language
- Assurance Levels


Increased $ Cost
Multi-Factor Token
PKI/ Digital Signature
Knowledge-Based
Strong Password
PIN/User ID
Low
Medium
High
Very High
Access to Market Research Data (asset=license fee)
Access to Local Resource (Risk mitigated By admin/org policy)
Verification Of data Transcription
Remote Clinical Order
Increased Need for Identity Assurance
e-Health Sign

Technical Assistance for Health Information Technology and Health Information Exchange in Medicaid and SCHIP

The Importance of Interoperability

Selecting and Adopting an Identity Management Approach

What is "Interoperability"

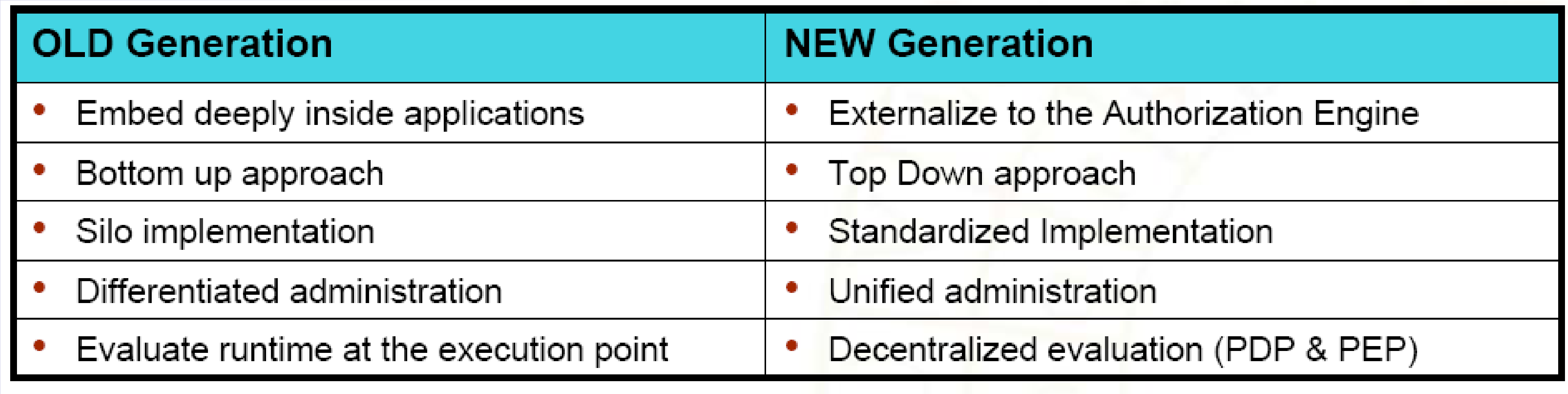
"The ability of different information technology systems and software applications to communicate, to exchange data accurately, effectively and consistently, and to use the information that has been exchanged."

Source: National Alliance for Health Information Technology, July 2005; "Consensus Conventions for the Use of Key HIT Terms" Project – ONC/HHS, 2008

Service-oriented Security Architecture

Fine-Grain Entitlement Management Implementation Approaches Enable Interoperability

Source: RSA Conference 2007 IAM-303 JPMorgan Chase



OLD Generation	NEW Generation
• Embed deeply inside applications	• Externalize to the Authorization Engine
• Bottom up approach	• Top Down approach
• Silo implementation	• Standardized Implementation
• Differentiated administration	• Unified administration
• Evaluate runtime at the execution point	• Decentralized evaluation (PDP & PEP)

- HL7 world-wide standard for interoperable permissions (RBAC) that can be used with healthcare applications, business partner exchanges and worldwide.
- HL7 Standard for Confidentiality Codes for patient consent directives

Technical Assistance for Health Information Technology and Health Information Exchange in Medicaid and SCHIP

Review of Standards

Standards

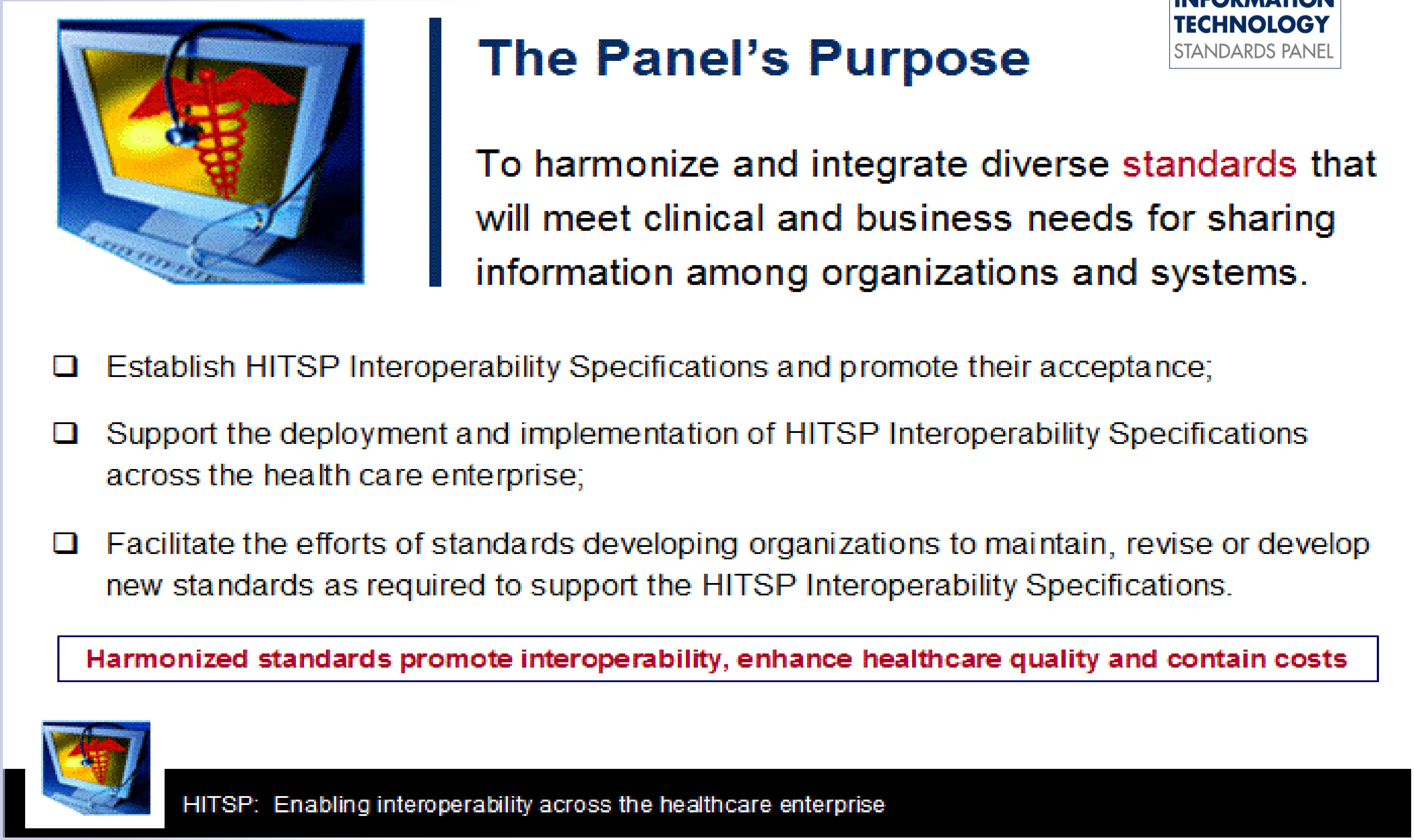
- **Enterprise Person Identifier**
  - **ASTM e1714-00**
- **Enterprise Person Identity Services**
  - **HL-7**
  - **OMG PIDS**
- **Security Services**
  - **NIST – FIPS 201-1**
  - **OASIS XACML**
  - **HL-7 CCOW**
  - **…and more…**
- **Other factors**
  - **HSPD-12**

Technical Assistance for Health Information Technology and Health Information Exchange in Medicaid and SCHIP

HITSP and Identity Management

Identifying Interoperability Specifications and Constructs

Health Information Technology Standards Panel (HITSP)



HEALTHCARE INFORMATION TECHNOLOGY STANDARDS PANEL

The Panel's Purpose

To harmonize and integrate diverse standards that will meet clinical and business needs for sharing information among organizations and systems.

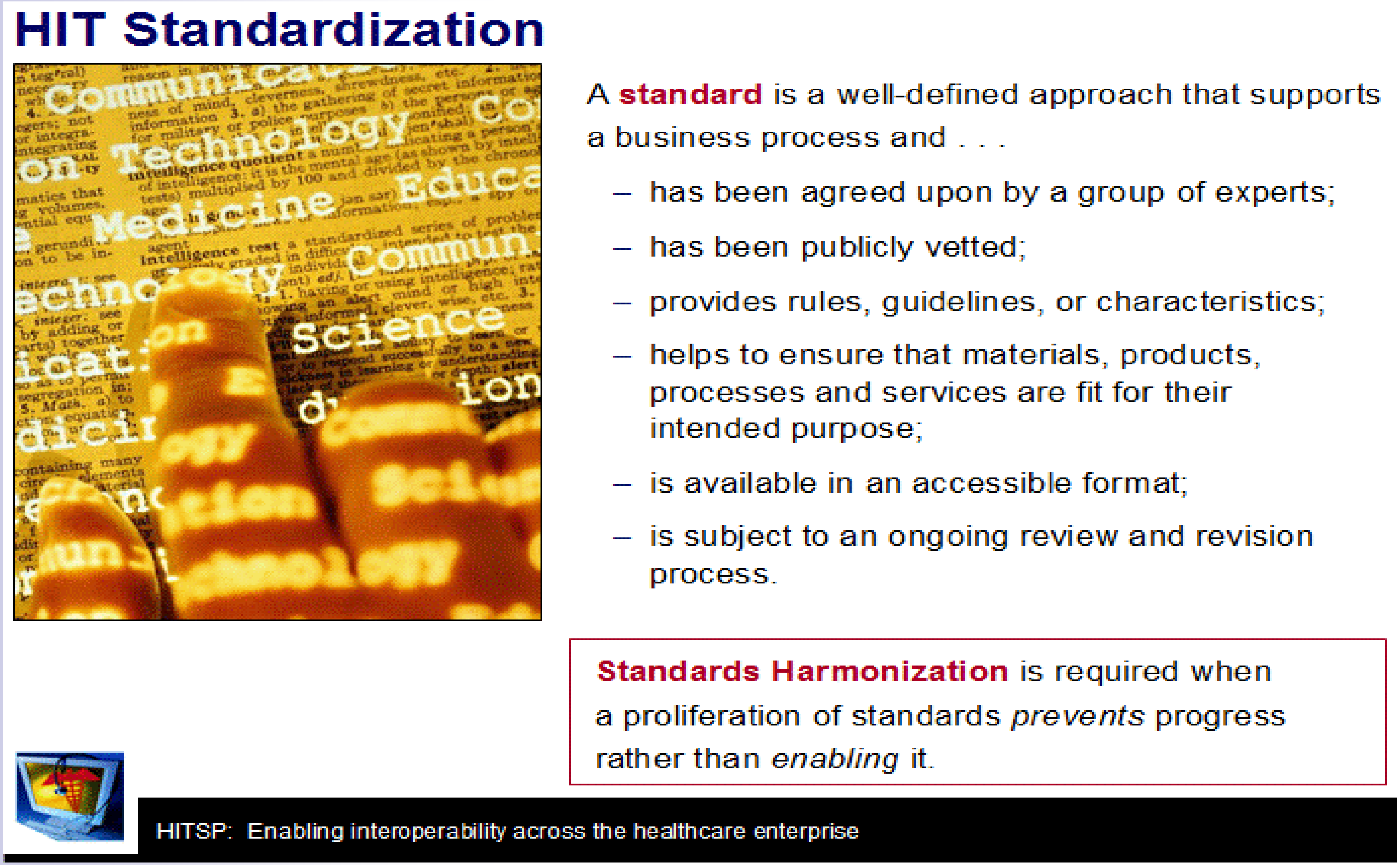
- ❑ Establish HITSP Interoperability Specifications and promote their acceptance;
- ❑ Support the deployment and implementation of HITSP Interoperability Specifications across the health care enterprise;
- ❑ Facilitate the efforts of standards developing organizations to maintain, revise or develop new standards as required to support the HITSP Interoperability Specifications.

Harmonized standards promote interoperability, enhance healthcare quality and contain costs

HITSP: Enabling interoperability across the healthcare enterprise

HITSP and Interoperability

HEALTHCARE INFORMATION TECHNOLOGY STANDARDS PANEL



HIT Standardization

A **standard** is a well-defined approach that supports a business process and . . .

- has been agreed upon by a group of experts;
- has been publicly vetted;
- provides rules, guidelines, or characteristics;
- helps to ensure that materials, products, processes and services are fit for their intended purpose;
- is available in an accessible format;
- is subject to an ongoing review and revision process.

Standards Harmonization is required when a proliferation of standards *prevents* progress rather than *enabling* it.

HITSP: Enabling interoperability across the healthcare enterprise

HITSP Standards Harmonization

HEALTHCARE INFORMATION TECHNOLOGY
STANDARDS PANEL

Open

Inclusive

Collaborative

Use Case Driven

www.hitsp.org

1. Identify a pool of standards for a general breakthrough area
2. Identify gaps and overlaps for specific context
3. Make recommendations for resolution of gaps and overlaps
4. Develop **Interoperability Specifications** for using the selected standard(s) for a specific context
5. Test the instruction for using the standard

HITSP Security, Privacy and Infrastructure (SP&I) Technical Committee

- Goal: Identity, evaluate and recommend security, privacy and infrastructure constructs to address interoperability needs and requirements defined by the AHIC-ONC Uses Cases
- Process:
  - Identify Security, Privacy and Infrastructure needs (requirements) from AHIC use-cases
  - Identify and document a set of common constructs that can be applied to the initial three AHIC use cases AND to future use cases.
- Recommend the adoption of constructs by the Secretary
  - Incorporate the recommended constructs throughout all HITSP Interoperability Specifications
  - Maintain/update constructs periodically (and develop new ones, as needed) based on new use cases issued by AHIC

HITSP Security and Privacy Constructs

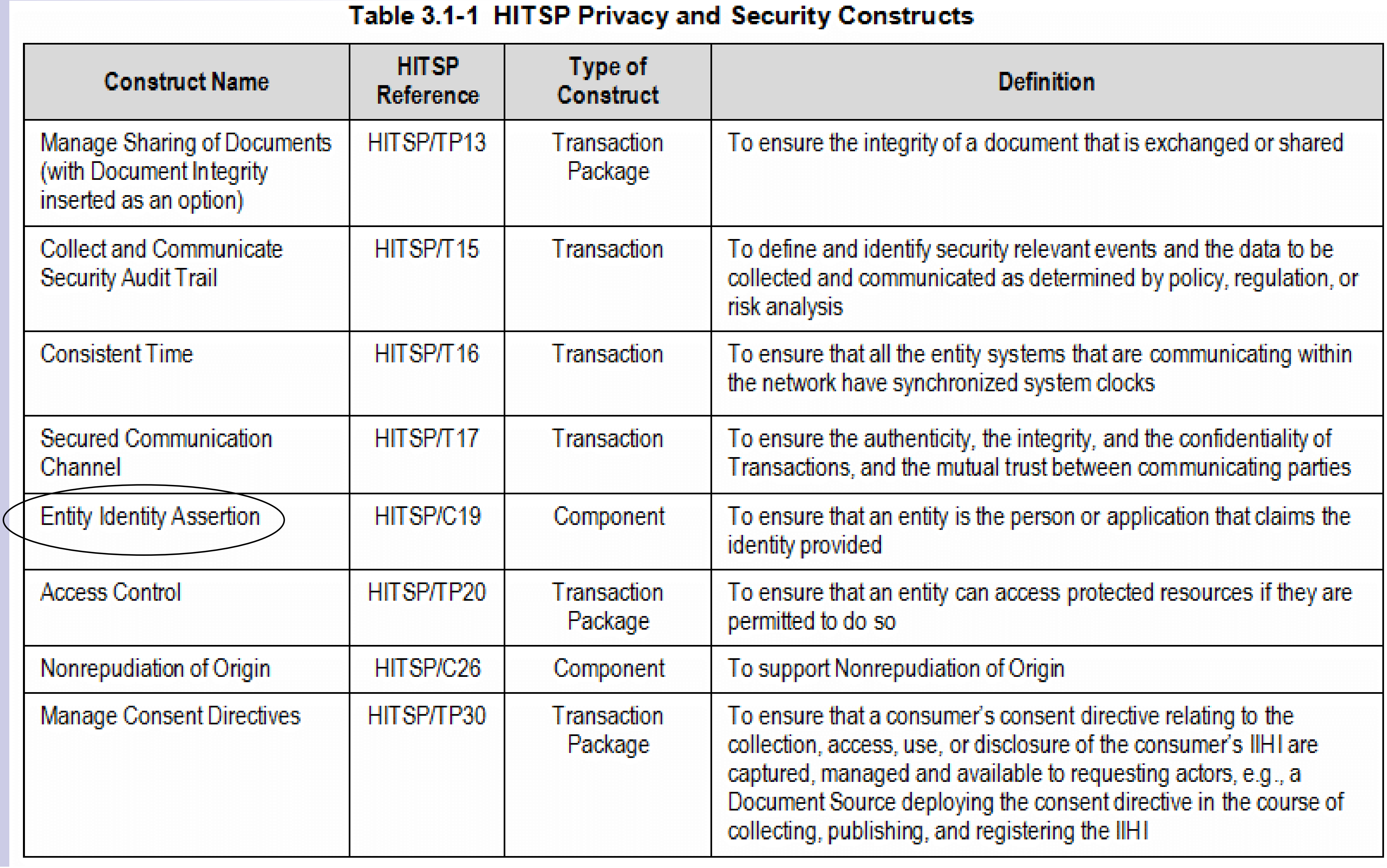


Table 3.1-1 HITSP Privacy and Security Constructs

Construct Name	HITSP Reference	Type of Construct	Definition
Manage Sharing of Documents (with Document Integrity inserted as an option)	HITSP/TP13	Transaction Package	To ensure the integrity of a document that is exchanged or shared
Collect and Communicate Security Audit Trail	HITSP/T15	Transaction	To define and identify security relevant events and the data to be collected and communicated as determined by policy, regulation, or risk analysis
Consistent Time	HITSP/T16	Transaction	To ensure that all the entity systems that are communicating within the network have synchronized system clocks
Secured Communication Channel	HITSP/T17	Transaction	To ensure the authenticity, the integrity, and the confidentiality of Transactions, and the mutual trust between communicating parties
Entity Identity Assertion	HITSP/C19	Component	To ensure that an entity is the person or application that claims the identity provided
Access Control	HITSP/TP20	Transaction Package	To ensure that an entity can access protected resources if they are permitted to do so
Nonrepudiation of Origin	HITSP/C26	Component	To support Nonrepudiation of Origin
Manage Consent Directives	HITSP/TP30	Transaction Package	To ensure that a consumer's consent directive relating to the collection, access, use, or disclosure of the consumer's IIHI are captured, managed and available to requesting actors, e.g., a Document Source deploying the consent directive in the course of collecting, publishing, and registering the IIHI

HITSP SP&I’s Entity Identity Assertion

- **Scope:**
  - This Component covers all scenarios in which HITSP Transactions cross enterprise boundaries, as well as transactions that may occur within an enterprise.
- **Construct Requirements**:
  - Entities are authenticated to assure that the entity is the person or application that claims the identity

HITSP SP&I’s Entity Identity Assertion

- **Functionality:** The key functionality supported by this construct is the identification and authentication of entities accessing the protected resources. At the end of the Component, the following conditions or outputs are provided:
  - Entity has authenticated
  - An error condition occurs. This can include errors in the verification step – malformed assertion; assertion from a distrusted identity provider; assertion from individual without enough information to perform verification; or identity provider is unknown
  - Entity identity assertion is verified
  - The results of the authentication are made available to the Authentication Provider
  - A security audit event is generated
  - Authentication information that was verified is available

HITSP SP&I’s Entity Identity Assertion

- **Example of Expected Use:**
  - User using a Document Registry or Document Repository is the patient. They are using an authorized PHR service which is handling the Document Consumer responsibilities. The Service Provider wants to restrict the information returned to those that have been released for patient consumption (for example a lab result that regulations require the provider to discuss in person before releasing the information)

Questions & Answers Session