



Pathfinding Session: IT Infrastructure for Intra-Enterprise

IHE North America Webinar Series 2008

Charles Parisot

**IT Infrastructure Planning Co-chair
GE Healthcare**



Learning Objectives

Your Product:

- What Profiles may be relevant?
- What do the Profiles do?
- If the relevance isn't clear, Ask now.

Goal:

Help you decide which detailed webinars to attend

What is IT Infrastructure Strategy for Intra-Enterprise versus Cross-Enterprise ?

- As much as possible, IHE ITI looks for solutions that serve both.
- A number of Cross-Enterprise Profiles may be used over time within the Enterprise (e.g. XDS, PIX/PDQ V3, etc).
- New use cases are always analyzed from both perspectives before deciding to embark into an Intra-Enterprise specific profile.

Product Classes Targeted

- **In-Patient/Acute Care including Departmental Information Systems.**
- **Larger Ambulatory Electronic Health Record Systems (EHRs / EMRs) and Specialized Centers (Imaging, Laboratories, etc.)**
- **Infrastructure Systems**

IHE IT Infrastructure

- Patient Identity & Administration Management
- Security and Infrastructure Services
- Special Profiles

Patient Identity & Administration Management

- **PAM – Patient Administration Management**
 - Management of patient identity, encounter information, as well as movements within an acute care facility
- **PIX – Patient Identifier Cross Referencing**
 - Management of patient identifiers amongst hospitals, sites, HIE networks. Supports HL7v2 & HL&v3
- **PDQ – Patient Demographics Query**
 - Facilitates the retrieval of patient information from a central server. Supports HL7v2 & HL&v3

Patient Administration Mgt (PAM)

CCHIT plan for 2009

- Coordinates exchange of patient registrations, updates, and movements for all clinical areas
- Information may be received and processed by consuming applications in any clinical domain
- Optionally allows unambiguous updating of historic patient movement events
- Demographic and encounter tracking works in both inpatient and ambulatory care settings
- Standardizes on HL7 V2.5 and its conformance structures
- Identified by CCHIT for 2009 certification

Patient Administration Management

Actor & Transaction: flexibility and compatibility

Patient Demographics
Source

→ Patient Identity Feed [ITI-030]

Patient Demographics
Consumer

Patient Encounter
Source

→ Patient Encounter Management [ITI-031]

Patient Encounter
Consumer

Patient Demographics
Consumer

Patient Encounter
Source

→ Patient Encounter
Management [ITI-031]

← Patient Identity Feed
[ITI-030]

Patient Demographics
Source

Patient Encounter
Consumer

OR

→ Patient Identity
Feed [ITI-030]

Patient
Demographics
Source

Patient Encounter
Source

→ Patient Encounter
Management [ITI-031]

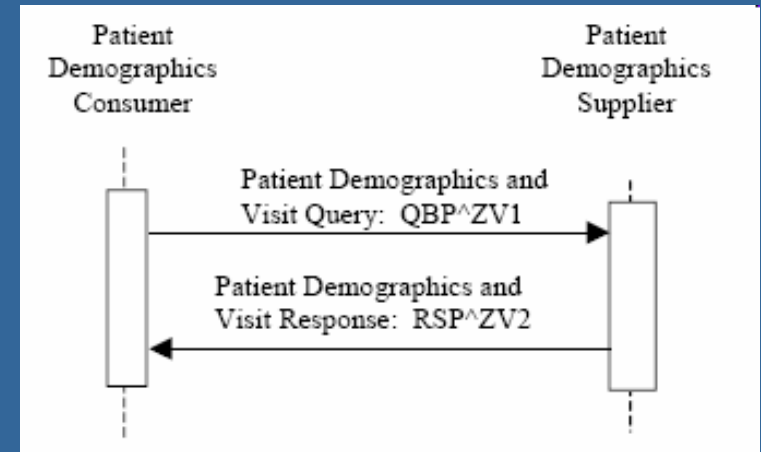
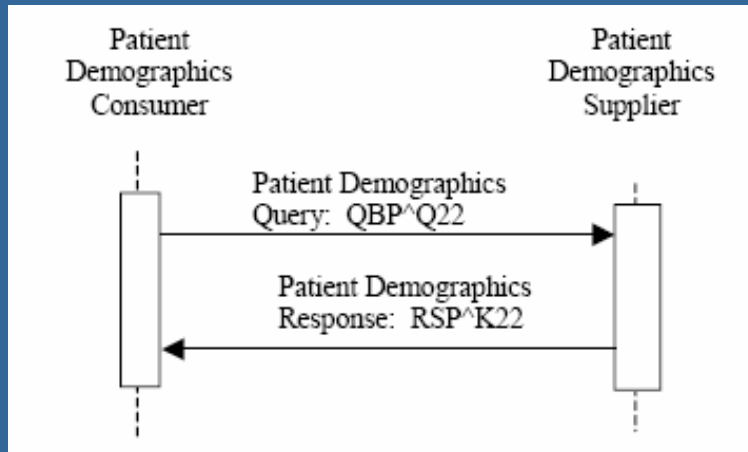
Patient
Demographics
Consumer

Patient Encounter
Consumer

*Flexible
Actor grouping*

PDQ Summary

- **Patient Demographic Query (PDQ) profile**
 - Given a partial set of patient demographics...
 - Return set of matching patients, their demographics and corresponding patient identifiers
 - If supplier supports visit data, search criteria may include combination of demographic and visit data
 - Patient Demographics and Visit Query is an optional transaction for both Patient Demographics Consumer and Supplier



PDQ Implementation Considerations

- Patient Information Source identification
 - A patient demographics supplier may contain patient information from multiple sources
 - PDQ query is evaluated within the context of a given patient information source
 - PDQ Consumer uses MSH-5/6 Receiving Application/Facility to identify patient information source context for PDQ query

PDQ Implementation Considerations...

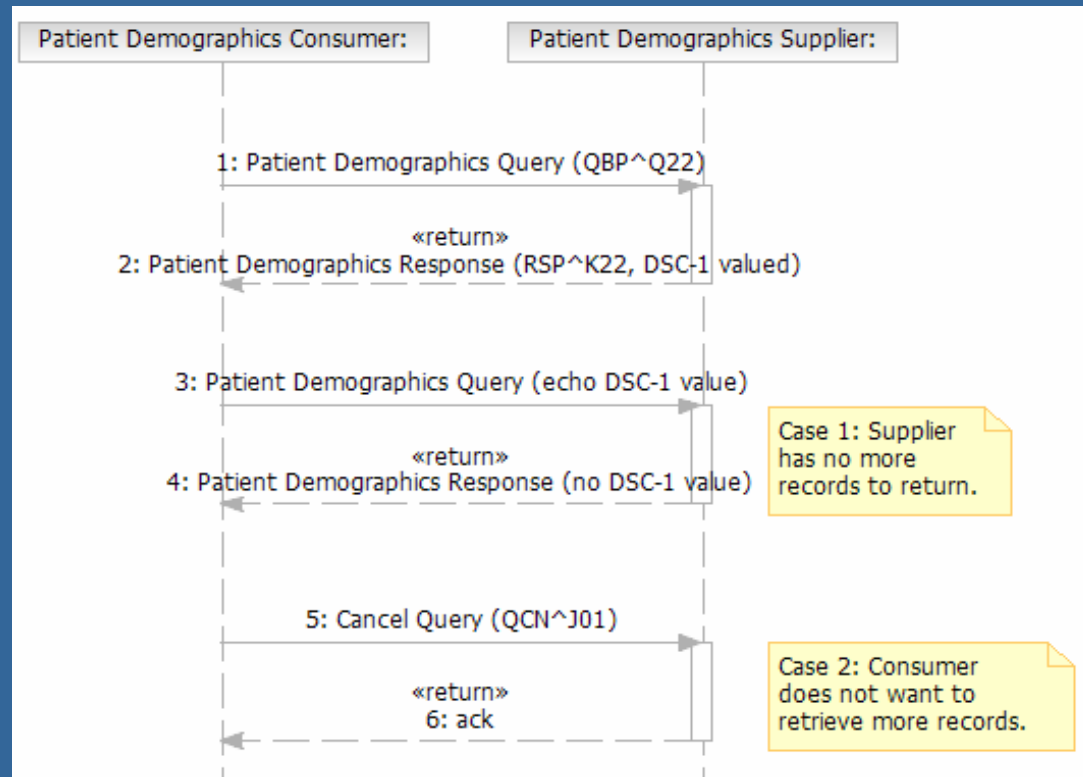
- Identifying domains for requested patient identifiers
 - QPD-8 used to identify list of domains for returned patient identifiers
 - If no value specified for QPD-8, you get all domains associated with patient information source
 - Patient information source identified in MSH-5/6
 - If using PDQ within XDS, will typically want to specify affinity domain in QPD-8

PDQ Implementation Considerations...

- Continuation protocol
 - Used to return query results “n” records at a time
 - PDQ Consumer uses RCP-2 to indicate how many records to return
 - All records returned if no RCP-2 value
 - PDQ supplier will return continuation pointer in DSC segment if there are more records to return
 - PDQ consumer echoes DSC value to get next set of records (CP for 2006)
 - Cancel query should be used when consumer finished retrieving records
 - Query Tag (QAK-1) assigned by consumer and can be used to correlate all request/response messages associated with the same query

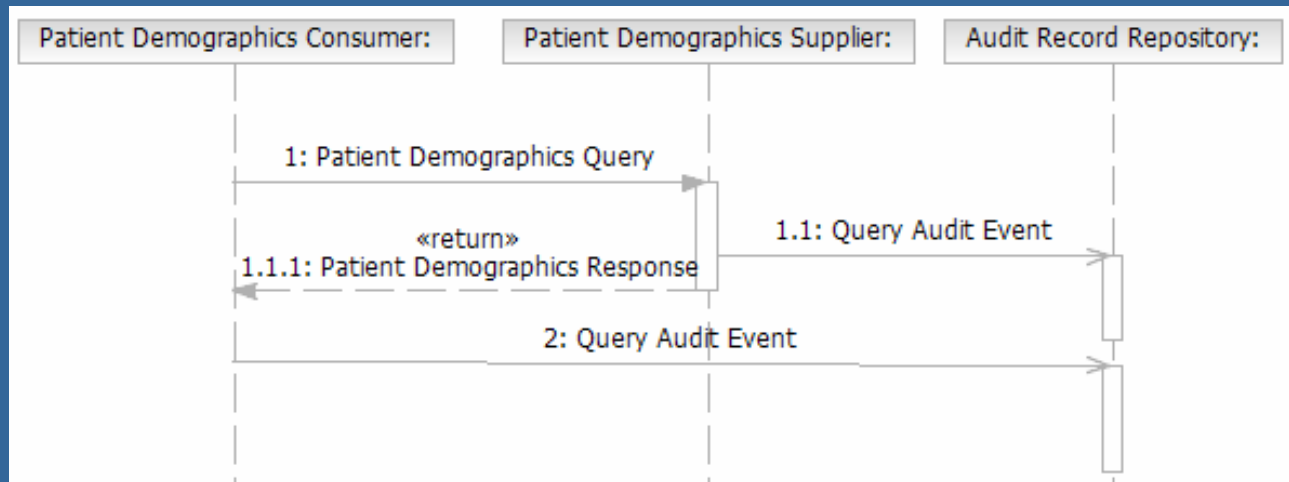
PDQ Implementation Considerations...

- Patient Demographics Query Consumer/Supplier interaction example:



PDQ Implementation Considerations...

- **ATNA audit requirements (CP for 2006)**
 - PDQ Query is defined as a Query Information event per ATNA Record Audit Event transaction
 - PDQ Consumer and PDQ Supplier responsible for generating Query audit messages per DICOM (Supp 95)



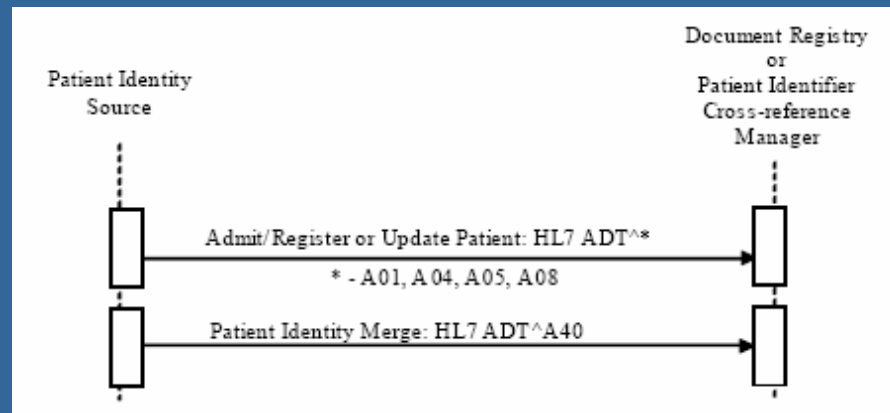
PIX Summary

- Patient Identity Cross Reference (PIX) profile defines 3 transactions:
 - Patient Identity Feed
 - PIX Update Notification
 - PIX Query

PIX Summary...

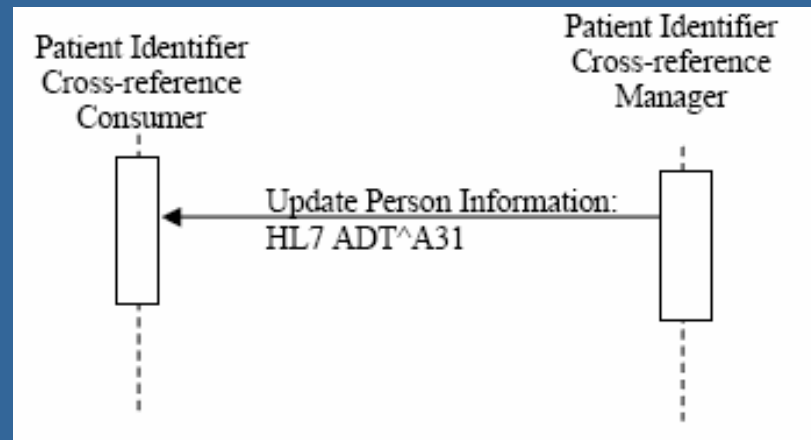
- **Patient Identity Feed**

- Patient Identity Source conveys patient demographic data and patient identifiers to PIX Cross Reference Manager and XDS Document Registry
 - XDS Document Registry uses information in the feed to identify patients that are members of the affinity domain
 - PIX Cross Reference Manager uses information in the feed to cross reference corresponding patient ids from multiple domains
 - Including linkage between hospital/clinic ids and affinity domain ids



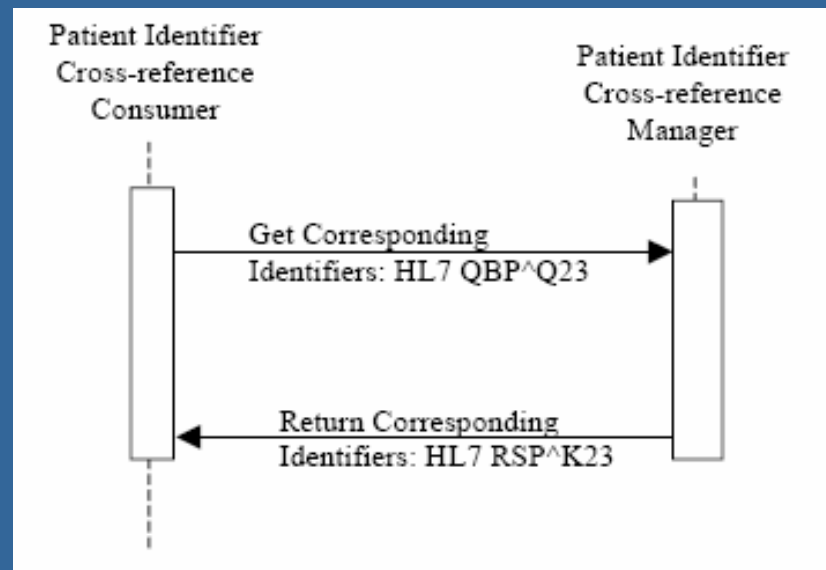
PIX Summary...

- **PIX Update Notification**
 - PIX Cross Reference Manager notifies PIX Cross Reference Consumer of changes in cross referenced identifiers for a given patient
 - PIX Cross Reference Manager actor must implement this transaction
 - Transaction is optional for PIX Cross Reference Consumer actors



PIX Summary...

- **PIX Query**
 - PIX Cross Reference Consumer presents a patient id to PIX Cross Reference Manager
 - PIX Cross Reference Manager returns corresponding ids for same patient within other domains



PIX Implementation Considerations

- Use of assigning authority for patient identifier domain
 - Patient identifier domains specified by Assigning Authority component of HL7 CX data type
 - Valid assigning authority value combinations
 - Namespace only
 - Universal Id, Universal Id Type Only
 - Name, Universal Id and Universal Id Type
 - If Patient Id Source supports multiple patient identifier domains; patient ids within PIX feed must be qualified by domain
 - Otherwise, PIX Cross Reference Manager and XDS Document Registry can default to single domain associated with the Patient Id Source
 - When using PIX within an XDS profile context...
 - Assigning authority shall be specified as Universal Id and Universal Id Type
 - Universal Id shall be an OID (which implies Universal Id Type == ISO)

PIX Implementation Considerations...

- **Specifying what domains to return on PIX Query**
 - Use QPD-4 to specify explicit list of domains for which cross-referenced patient ids are requested
 - If no domains specified in QPD-4...
 - Will receive cross-referenced patient identifiers for all domains known to the PIX Cross Reference Manager
- **More than 1 patient id can be returned for a given domain**
 - Consumer needs to handle all of the ids returned or must ignore all of the ids returned
 - To avoid situations where consumer presents incomplete set of information based on use of partial set of patient identifiers

PIX Implementation Considerations...

- **Use of PIX Update Notification**
 - Useful in situations where actor wants to keep a local cache of cross-referenced identifiers
 - Example:
 - XDS Document Source within a hospital maintains a list of local hospital patient ids and corresponding affinity domain ids
 - Typically used in lieu of PIX Query
 - **Mechanics of PIX Update Notification**
 - PIX Consumer indicates which domains they are interested in receiving cross reference event notifications
 - PIX Cross Reference Manager notifies PIX Consumer of changes to the set of cross-referenced patient ids spanning the domains of interest to a given PIX Consumer
 - This will typically result as a side effect of a Patient Identity Feed transaction

PIX Implementation Considerations...

- **ATNA audit requirements (CP for 2006)**
 - Patient Identity Feed is defined as a Patient Record event per ATNA Record Audit Event transaction
 - Patient Id Source responsible for generating Patient Record audit message per DICOM (Supp 95)
 - PIX Query is defined as a Query event per ATNA Record Audit Event transaction
 - PIX Consumer and PIX Cross Reference Manager responsible for generating Query audit messages per DICOM (Supp 95)
 - PIX Update Notification is defined as a Patient Record event per ATNA Record Audit Event transaction
 - PIX Cross Reference Manager responsible for generating Patient Record audit message per DICOM (Supp 95)

PIX, PDQ and HL7 V3

- Approach used to incorporate HL7 V3 messaging and Web Services transport into PIX/PDQ profiles
- HL7 V2.x and V3: what is optional vs. required
- Using HL7 V3 for PIX
 - PDQ changes should be similar in nature
- Web Service transport option

Profile Changes for HL7 V3

- What hasn't changed
 - Same set of actors for both PIX and PDQ
 - Same set of transactions
- What has changed
 - HL7 V3 version of each transaction
 - HL7 V3 message used in place of HL7 V2.x counterpart
 - HL7 V3 messages are XML-based
 - Web Service transport used instead of MLLP

Optionality

- Optionality within PIX/PDQ transactions for HL7 2.x version has not changed

Actors	Transactions	Optionality	Section in Volume 2 for HL7v2
Patient Identity Source	Patient Identity Feed[ITI-8]	R	ITI TF-2: 3A.8
Patient Identifier Cross-reference Consumer	PIX Query[ITI-9]	R	ITI TF-2: 3A.9
	PIX Update Notification[ITI-10]	O	ITI TF-2: 3A.10
Patient Identifier Cross-reference Manager	Patient Identity Feed[ITI-8]	R	ITI TF-2: 3A.8
	PIX Query[ITI-9]	R	ITI TF-2: 3A.9
	PIX Update Notification[ITI-10]	R	ITI TF-2: 3A.10
Patient Demographics Consumer	Patient Demographics Query[ITI-21]	R	ITI TF-2: 3A.21
	Patient Demographics and Visit Query[ITI-22]	O	ITI TF-2: 3A.22
Patient Demographics Supplier	Patient Demographics Query[ITI-21]	R	ITI TF-2: 3A.21
	Patient Demographics and Visit Query[ITI-22]	O	ITI TF-2: 3A.22

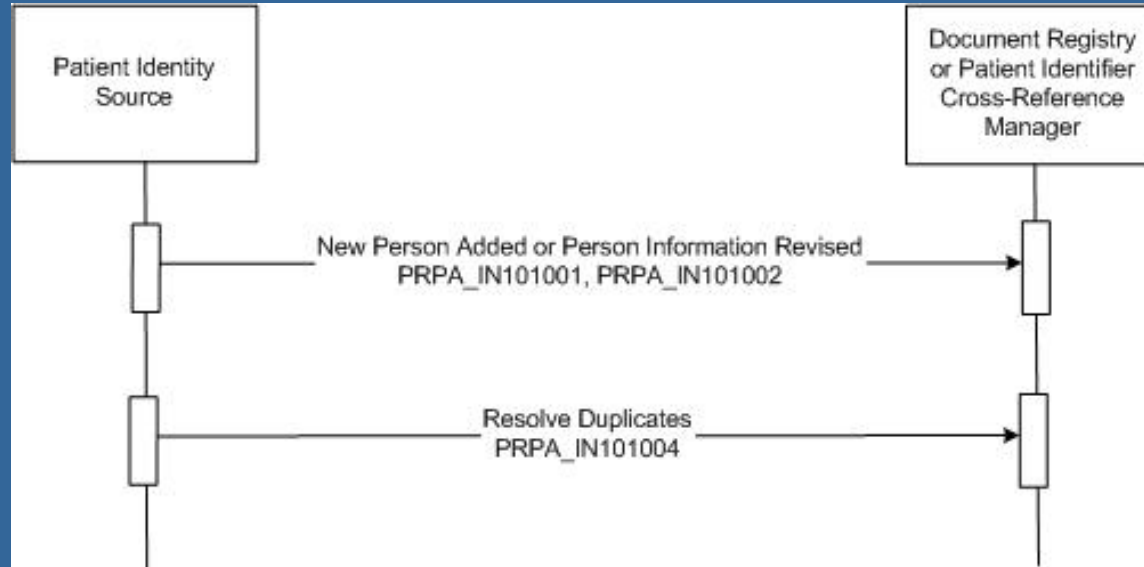
Optionality...

- **HL7 V3 version of transactions considered options for PIX and PDQ**
 - Described in separate sections of ITI TF-2

Actors	Options	Section in Volume 2 for HL7v3
Patient Identity Source	Patient Identity Feed[ITI-8]	ITI TF-2: 3B.8
Patient Identifier Cross-reference Consumer	PIX Query[ITI-9]	ITI TF-2: 3B.9
	PIX Update Notification[ITI-10]	ITI TF-2: 3B.10
Patient Identifier Cross-reference Manager	Patient Identity Feed[ITI-8]	ITI TF-2: 3B.8
	PIX Query[ITI-9]	ITI TF-2: 3B.9
	PIX Update Notification[ITI-10]	ITI TF-2: 3B.10

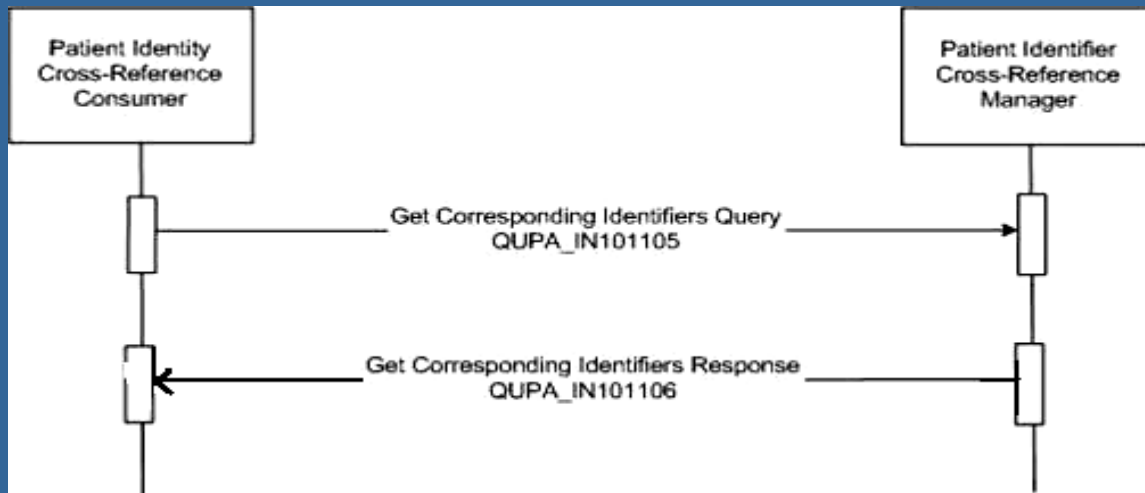
Using HL7 V3 for PIX

- **PIX Feed:**
 - **HL7 V2.x messages**
 - Admin/register/update patient (ADT^ A01, A04, A05, A08)
 - Patient Identity Merge (ADT^A40)
 - **HL7 V3 messages**
 - New Patient Added or Patient Information Revised
 - Resolve Duplicates



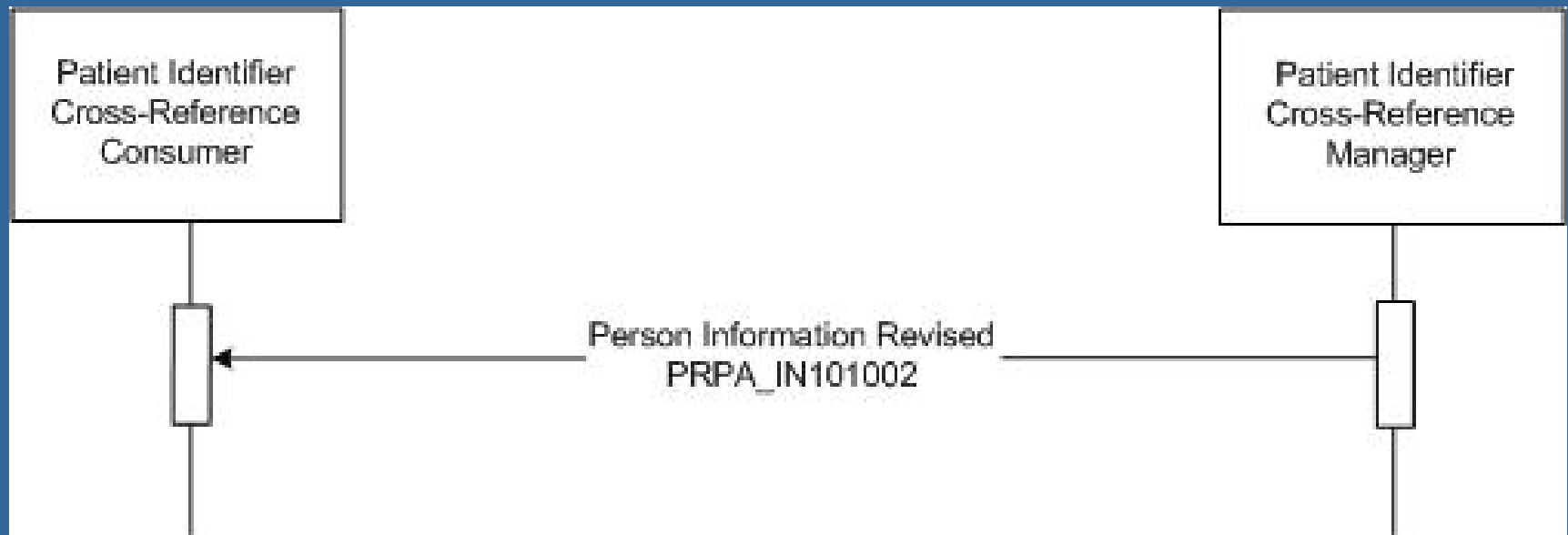
Using HL7 V3 for PIX...

- PIX Query:
 - HL7 V2.x message
 - Get Corresponding Identifiers (QBP^Q23)
 - HL7 V3 messages
 - Get Corresponding Identifiers Query



Using HL7 V3 for PIX...

- **PIX Update Notification:**
 - HL7 V2.x message
 - Update Person Information (ADT^A31)
 - HL7 V3 messages
 - Patient Information Revised



Web Service Transport Option

- Sender and receiver shall conform to the HL7 WS Basic and Addressing profiles with following constraint:
 - SOAP 1.2
- Sender and receiver should not implement the following HL7 WS profiles at this time:
 - HL7 WS Security
 - HL7 WS Reliable Messaging

IHE Security and Privacy Services

- **CT – Consistent Time**
 - auto-synchronize system clocks
- **ATNA – Audit Trail & Node Authentication**
 - record HIPAA events; use security certificates
- **EUA – Enterprise User Authentication**
 - Facilitates centralized user authentication with the convenience and speed of a single sign-on.
- **PWP – Personal White Pages**
 - provides access to basic directory information on human workforce members within the enterprise

Audit Trail and Node Authentication (ATNA)

- Defines basic security features for an individual system for use as part of the security and privacy environment for a healthcare enterprise.
- Provides host level authentication, which is used in conjunction with the user authentication from EUA.

- **Reasons: Clinical Use and Privacy**
 - authorized persons must have access to medical data of patients, and the information must not be disclosed otherwise.
 - Unauthorized persons should not be able to interfere with operations or modify data
- **By means of procedures and security mechanisms, guarantee:**
 - Confidentiality
 - Integrity
 - Availability
 - Authenticity

ATNA *Security Measures*

- Authentication: *Establish the user and/or system identity, answers question: “Who are you?”*
 - ATNA defines: How to authenticate network connections.
 - ATNA Supports: Authentication mechanisms, e.g. Enterprise User Authentication (EUA) or Cross Enterprise User Authentication (XUA)..
- Authorization and Access control: *Establish user’s ability to perform an action, e.g. access to data, answers question: “Now that I know who you are, what can you do?”*
 - ATNA defines: How to authorize network connections.
 - ATNA requires: System internal mechanisms for both local and network access.

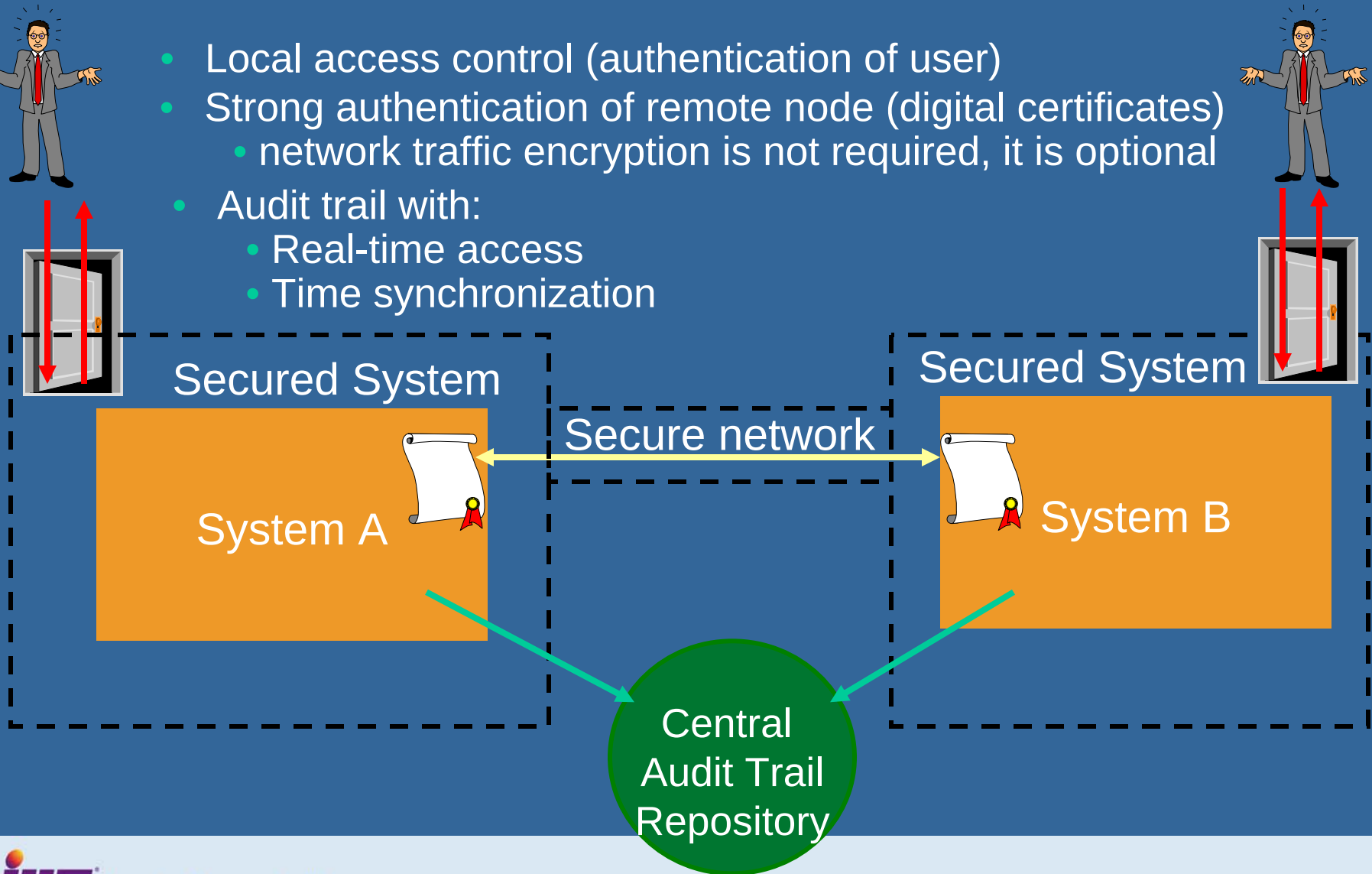
ATNA *Security Measures*

- Accountability and Audit trail:
Establish historical record of user's or system actions over period of time, answers question:
“What have you done?”
 - ATNA Defines: Audit message format and transport protocol

- IHE makes cross-node security management easy:
 - Only a simple manual certificate installation is needed, although more sophisticated systems can be used
 - Separate the authentication, authorization, and accountability functions to accommodate the needs of different approaches.
 - Enforcement driven by ‘a posteriori audits’ and real-time visibility.

ATNA *Integrating Trusted Nodes*

- Local access control (authentication of user)
- Strong authentication of remote node (digital certificates)
 - network traffic encryption is not required, it is optional
- Audit trail with:
 - Real-time access
 - Time synchronization



ATNA *Node Authentication*

- X.509 certificates for node identity and keys
- TCP/IP Transport Layer Security Protocol (TLS) for node authentication, and optional encryption
- Secure handshake protocol of both parties during Association establishment:
 - Identify encryption protocol
 - Exchange session keys
- Actor must be able to configure certificate list of authorized nodes.
- ATNA presently specifies mechanisms for HTTP, DICOM, and HL7

Why Node Authentication

- Many systems are shared access, e.g. CT systems, where the machine identity is more important than the operator's identity for security purposes.
 - A CT operator is only permitted to update CT records from a CT system.
- Some systems operate autonomously, e.g. PACS archive.
 - Knowing identity of the PACS administrator on duty is not useful when monitoring PACS activity. There might be nobody logged in.
- Machine access is usually controlled by the site administration.
 - Even authorized users are not permitted to use personal machines.

- Designed for surveillance rather than forensic use.
- Two audit message formats
 - IHE Radiology interim format, for backward compatibility with radiology
 - IETF/DICOM/HL7/ASTM format, for future growth
 - DICOM Supplement 95
 - IETF Draft for Common Audit Message
 - ASTM E.214
 - HL7 Audit Informative documents
- Both formats are XML encoded messages, permitting extensions using XML standard extension mechanisms.

ATNA *Auditable Events*

Actor-start-stop	<i>The starting or stopping of any application or actor.</i>
Audit-log-used	<i>Reading or modification of any stored audit log</i>
Begin-storing-instances	<i>The storage of any persistent object, e.g. DICOM instances, is begun</i>
Health-service-event	<i>Other health service related auditable event.</i>
Images-availability-query	<i>The query for instances of persistent objects.</i>
Instances-deleted	<i>The deletion of persistent objects.</i>
Instances-stored	<i>The storage of persistent objects is completed.</i>

ATNA *Auditable Events*

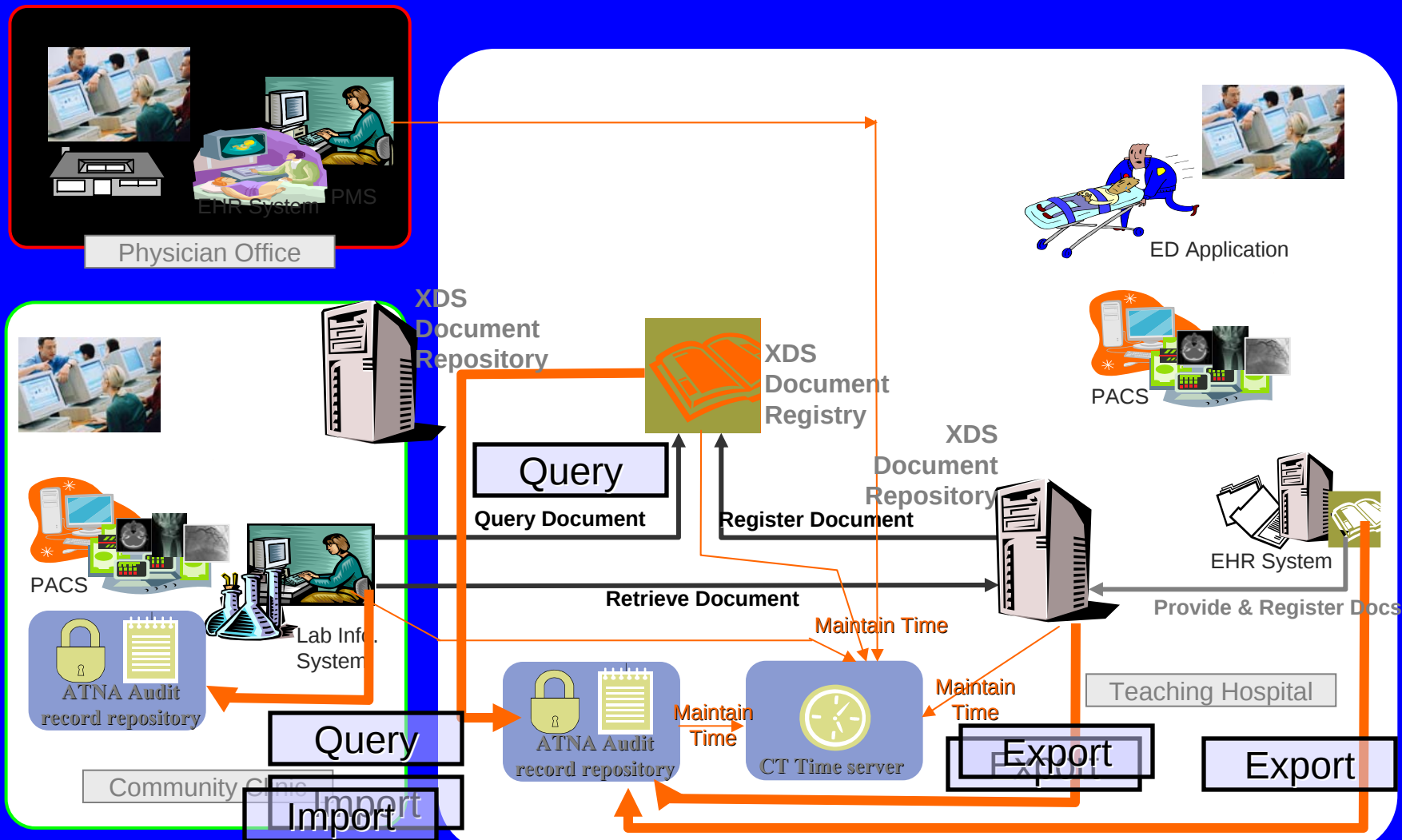
Medication	<i>Medication is prescribed, delivered, etc.</i>
Mobile-machine-event	<i>Mobile equipment is relocated, leaves the network, rejoins the network</i>
Node-authentication-failure	<i>An unauthorized or improperly authenticated node attempts communication</i>
Order-record-event	<i>An order is created, modified, completed.</i>
Patient-care-assignment	<i>Patient care assignments are created, modified, deleted.</i>
Patient-care-episode	<i>Auditable patient care episode event that is not specified elsewhere.</i>
Patient-record-event	<i>Patient care records are created, modified, deleted.</i>

ATNA Auditable Events

PHI-export	<i>Patient information is exported outside the enterprise, either on media or electronically</i>
PHI-import	<i>Patient information is imported into the enterprise, either on media or electronically</i>
Procedure-record-event	<i>The patient record is created, modified, or deleted.</i>
Query-information	<i>Any auditable query not otherwise specified.</i>
Security-administration	<i>Security alerts, configuration changes, etc.</i>
Study-object-event	<i>A study is created, modified, or deleted.</i>
Study-used	<i>A study is viewed, read, or similarly used.</i>

- BSD Syslog protocol (RFC 3164) is the interim approach while the IETF continues to resolve issues surrounding Reliable Syslog (RFC 3195).
- Audit trail events and content based on IETF, DICOM, HL7, and ASTM standards. Also, Radiology Basic Security audit event format is allowed for backward compatibility.

Accountability



XDS Affinity Domain (NHIN sub-network)

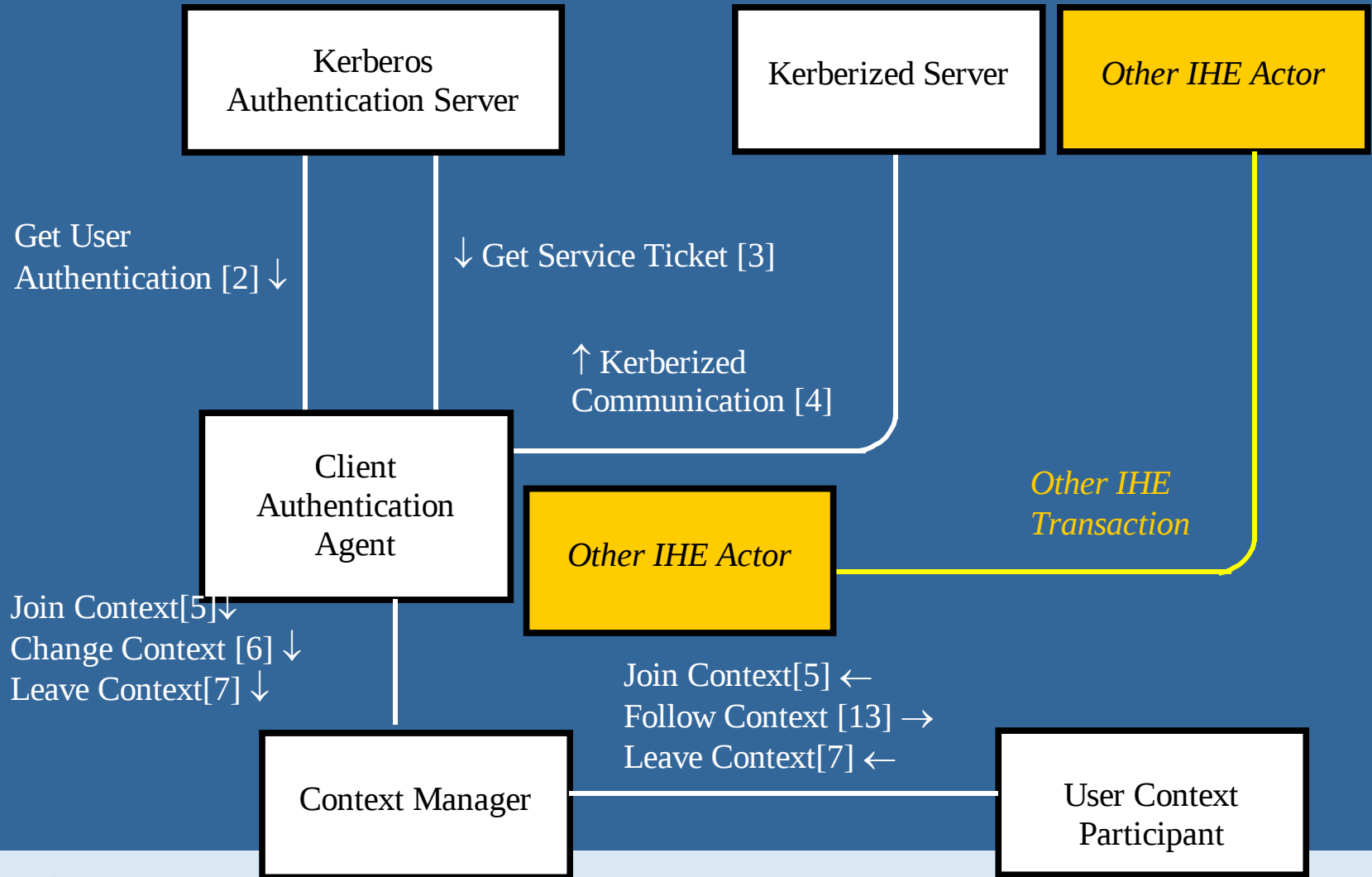
Consistent Time (CT)

- Network Time Protocol (NTP) version 3 (RFC 1305) for time synchronization
- Actor must support manual configuration
- Required accuracy: 1 second
- Optionally Secure NTP may be used
- Required for use of ATNA, EUA, XUA

Enterprise User Authentication - EUA

- Support a *single enterprise* governed by a *single set of security policies* and having a *common network domain*.
- Establish *one name per user* to be used *for all IT applications and devices*.
- Facilitate *centralized user authentication management*.
- Provide users with *single sign-on*.

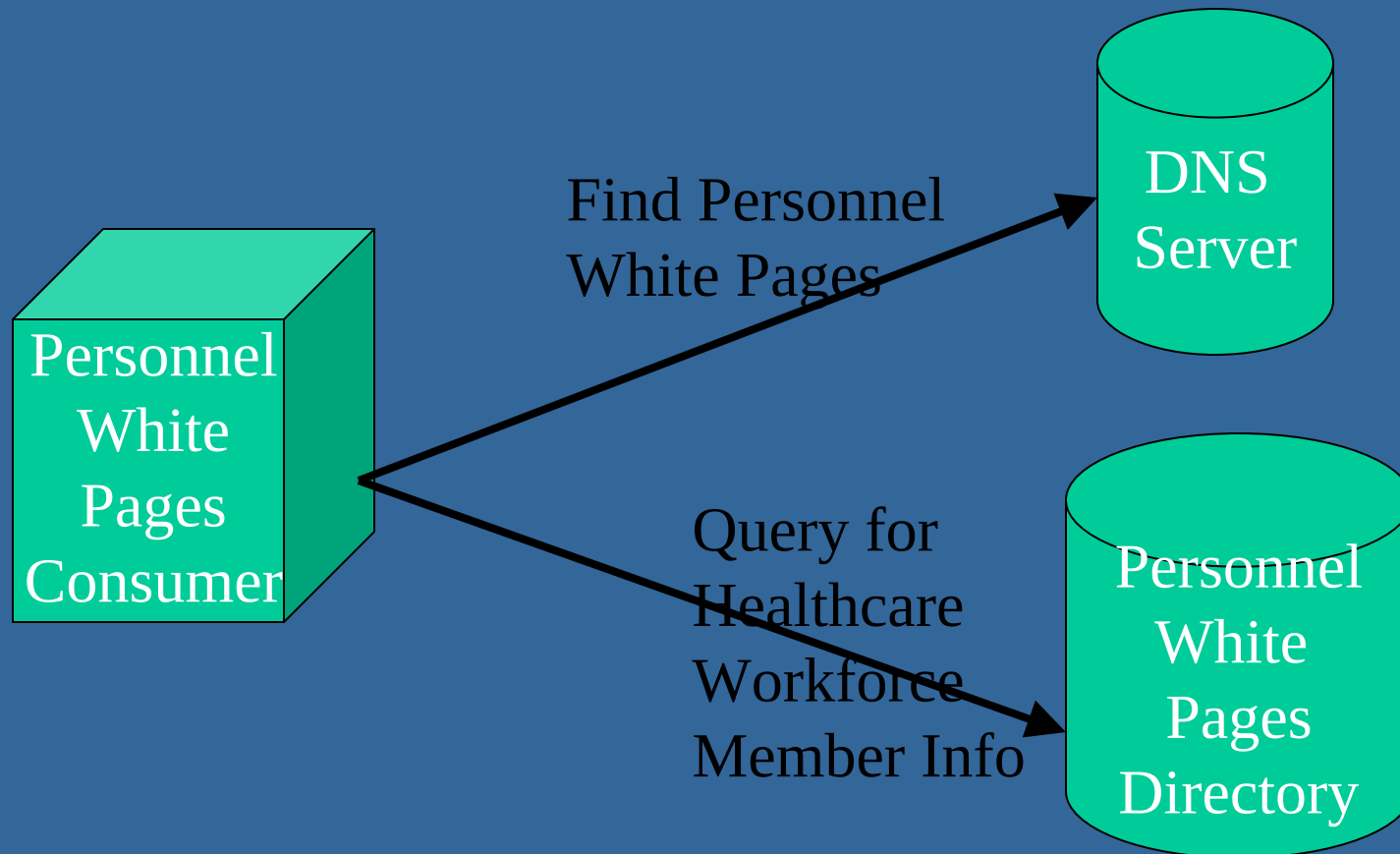
EUA – Transaction Diagram



Personnel White Pages (PWP)

- Provide access to basic information about the human workforce members
 - Does not include Patients
- Defines method for finding the PWP
- Defines query/access method
- Defines attributes of interest

PWP - Transactions



Special Profiles

- **RID – Retrieve Information for Display**
 - support simple web access to summary lists of documents and generic HTML content display.
- **PSA – Patient Synchronized Application**
 - facilitating the synchronization on the same patient of multiple applications on a desktop

Which Profile on which system ?

	In-patient HIS/EHR & Dept Systems	Ambulatory EHRs / EMRs and Specialized Centers	Enterprise Infrastructure Systems
PAM	X	X	
PIX	X		X
PDQ	X	X	X
RID	X	X	
ATNA/CT	X	X	X
EUA	X	X	X
PWP	X	X	X
PSA	X		X

Resources: www.ihe.net

Web Resources:

- http://www.ihe.net/north_america/connectathon2009.cfm
Info on Connectathon 2009 including timeline, Webinar schedule and recorded sessions
- http://www.ihe.net/Technical_Framework/index.cfm
IHE Technical Frameworks and Supplements
- <http://www.ihe.net/profiles/index.cfm>
Overview of IHE profiles and brief descriptions
- <http://wiki.ihe.net/index.php?title=Profiles>
More detailed descriptions of many profiles
- ihe@himss.org, ihe@rsna.org
Inquire about Connectathon, committee participation, IHE membership, etc.