



Security and Privacy Overview

Part 1 of 2 – Basic Security

IHE IT Infrastructure Planning Committee

John Moehrke – GE Healthcare



What IHE Delivers

Agenda

Part 1

- Overall Security and Privacy controls
- Consistent Time (CT)
- Audit Trails and Node Authentication (ATNA)
- Enterprise User Authentication (EUA)
- Cross-Enterprise User Assertion (XUA)

Part 2

- Document Digital Signature (DSG)
- Basic Patient Privacy Consents (BPPC)
- Access Control
- Gaps
- Conclusion

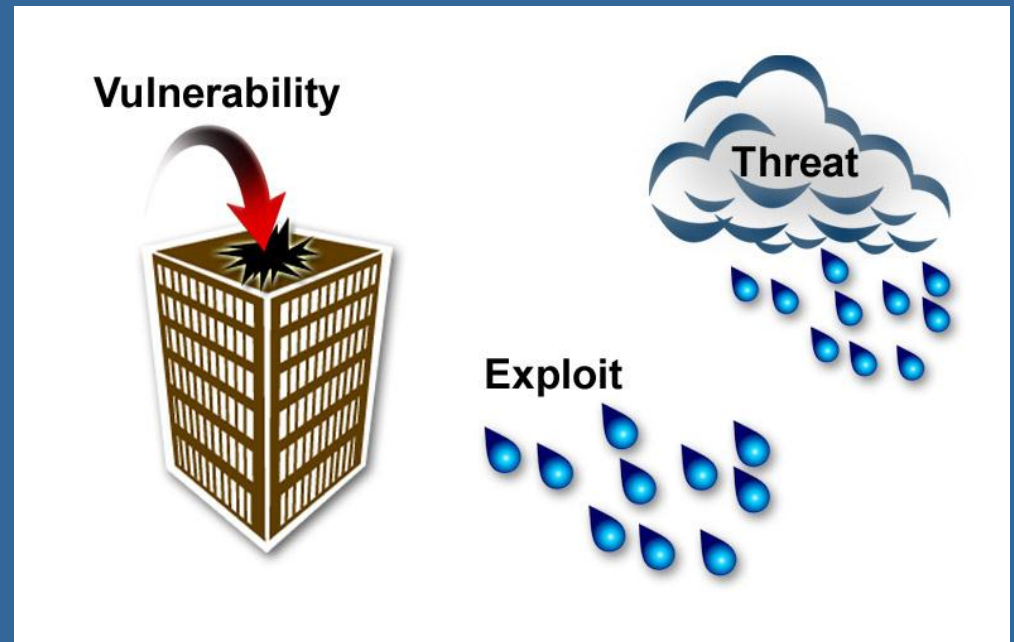
Layers of Policies



Risk Scenario

In this scenario:

- The vulnerability is the hole in the roof
- The threat is the rain cloud
- Rain could exploit the vulnerability



The risk is that the building and equipment in the building could be damaged as long as the vulnerability exists and there is a likely chance that rain will fall.

Security Mis-Use-Cases

- Prevent Indiscriminate attacks (worms, DOS)
- Normal Patient that accepts XDS participation
- Patient asks for Accounting of Disclosures
- Protect against malicious neighbor doctor
- Patient that retracts consent to publish
- Provider Privacy
- Malicious Data Mining
- Access to Emergency data set
- VIP (movie star, sports figure)
- Domestic violence victim
- Daughter with sensitive tests hidden from Parent
- Sensitive topics: mental health, sexual health
- Legal Guardian (cooperative)
- Care-Giver (assists w/ care)

Accountability Models

Access Control model – Prevention

- **Strong controls on User Identification and Authentication**
- **Strict Role-Based-Access-Control**
 - No one is given any more access rights than they minimally need
- **Typical in a Bank**

Audit Control model – Reaction

- **Strong control on User Identification and Authentication**
- **Relaxed Role-Based-Access-Control**
 - Emphasis on Training and Awareness of oversight
 - Told what you are normally allowed to do
 - Empowered to do what is right when necessary
- **Audit Logs are inspected regularly**
- **Abuse is detected and acted upon**

Healthcare: Typically mixture w/ emphasis on Patient Safety

Profiles mapped to Security & Privacy Controls

Security & Privacy Controls		Audit Log	Identification and Authentication	Data Access Control	Secrecy	Data Integrity	Non-Repudiation	Patient Privacy
IHE Profile	Profile Issued							
Audit Trails and Node Authentication	2004	√	√	√	√	√	√	√
Consistent Time	2003	√	.				√	
Enterprise User Authentication	2003		√	.			.	.
Cross-Enterprise User Assertion	2006		√	.			.	.
Basic Patient Privacy Consents	2006			.				√
Personnel White Pages	2004		√	√			.	
Healthcare Provider Directory	2010		√	.			.	
Document Digital Signature	2005		√			√	√	
Document Encryption (in development)	2011			√	√	.		



CT

Consistent Time

Introduction and Standards

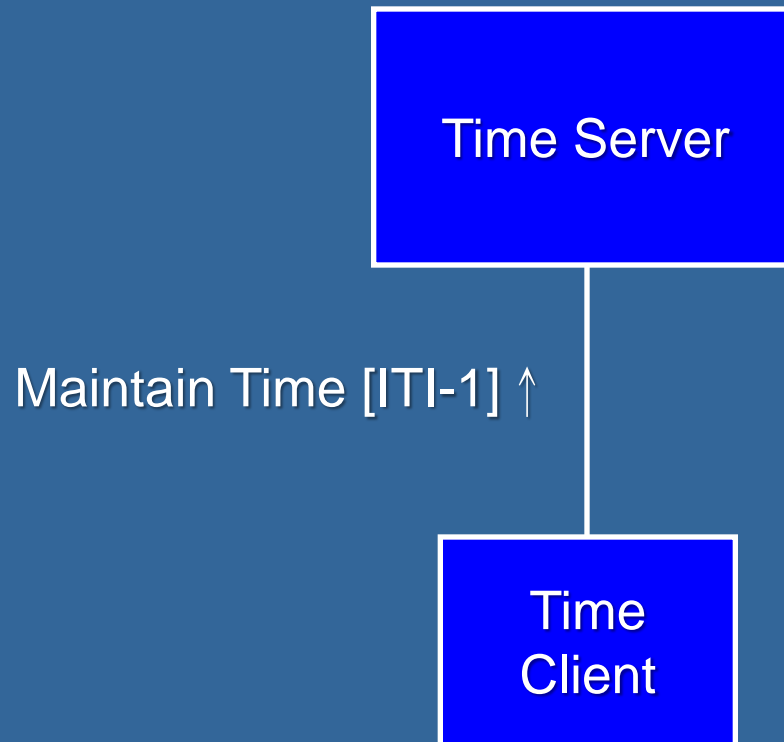
● Meet a basic security requirement

- System clocks and time stamps of the many computers in a network must be synchronized.
- Lack of consistent time creates a “security hole” for attackers.
- Synchronization ± 1 second is generally sufficient.

● Achieve cost savings/containment

- Use the Network Time Protocol (NTP) standard defined in RFC 1305.
- Leverage existing Internet NTP services, a set-up option for mainstream operating systems.

Transaction Diagram





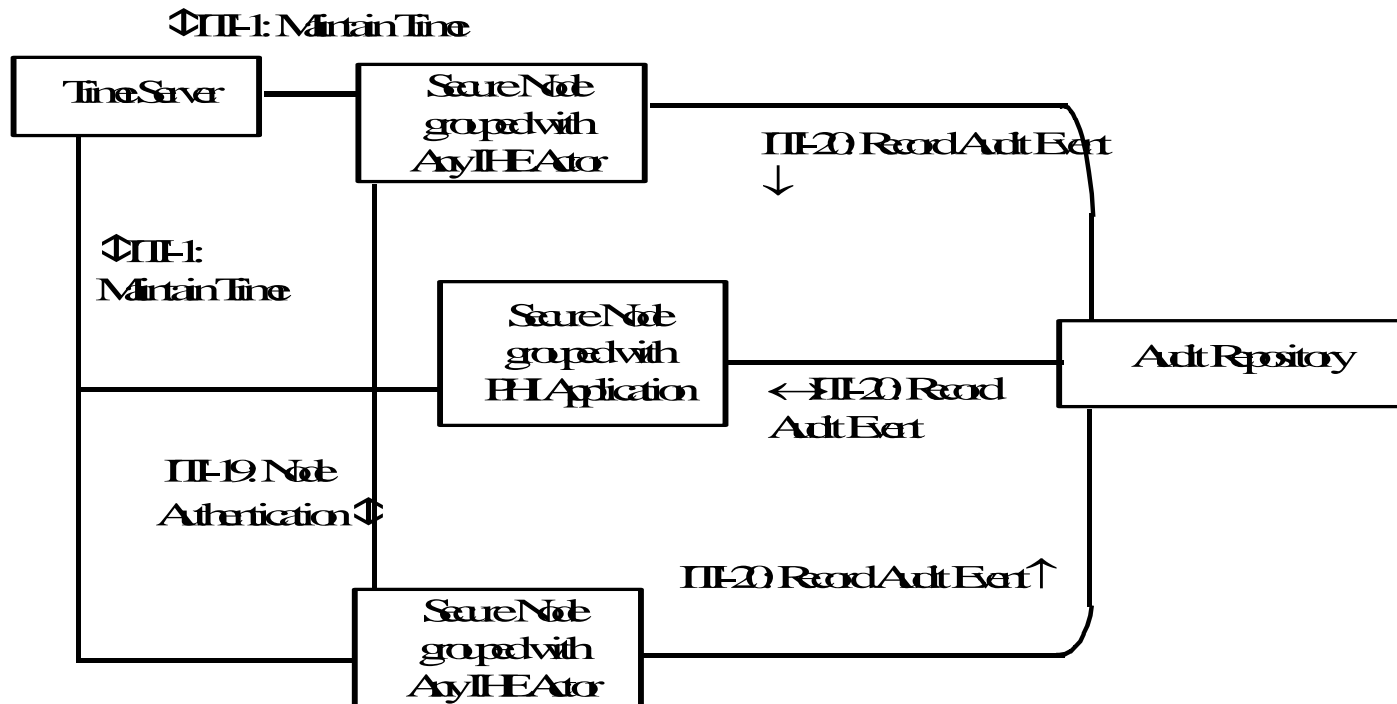
ATNA

Audit Trail and Node Authentication

ATNA Profile

- **Secure Node or Secure Application**
- **Access Controls**
 - Functional – can be shown to enforce policies
- **Audit Controls**
 - SYSLOG + IHE/DICOM/RFC3881 Audit Message
 - Auditable Events
- **Network Controls**
 - Mutually Authenticated TLS
 - Or S/MIME or WS-Security or physical isolation

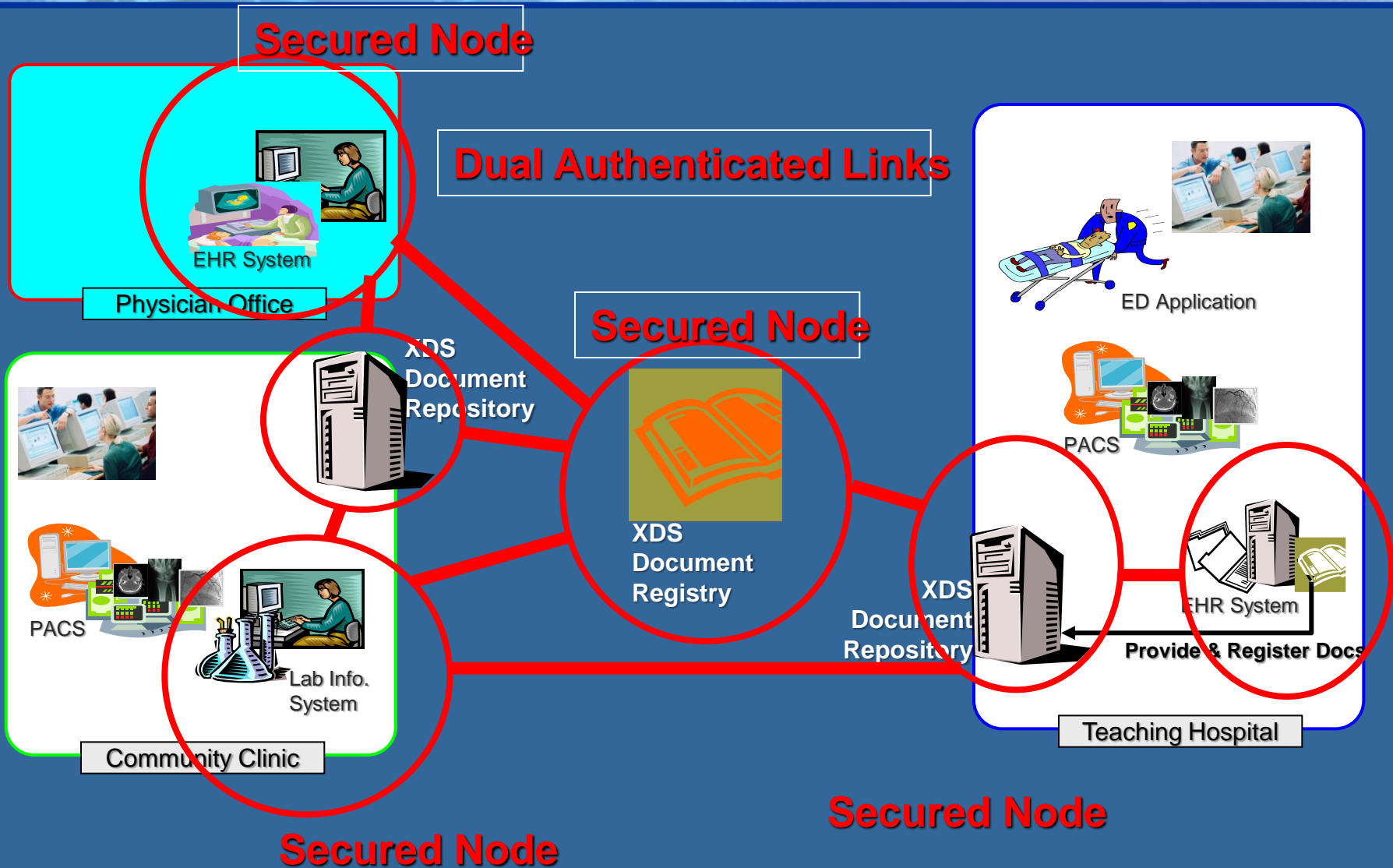
ATNA: Actors / Transactions



ATNA: Authenticate Node Transaction

- **Mutually Authenticate all network communications of Sensitive Information**
- **Encrypt and Integrity Protect**
- **Standards**
 - X.509 Digital Certificate
 - RSA Authentication
 - AES Encryption
 - SHA Integrity
 - Transport Layer Security (TLS) RFC 2246
 - Web-Services Security
 - S/MIME

ATNA Authenticate Node



Audit Log - Accountability

● Mitigation against unauthorized use

- Investigate Audit log for patterns and behavior outside policy. Enforce policy
- Secure Node requires appropriate Access Controls to enforce at the enterprise by XDS Source and Consumers

● Investigation of patient complaints

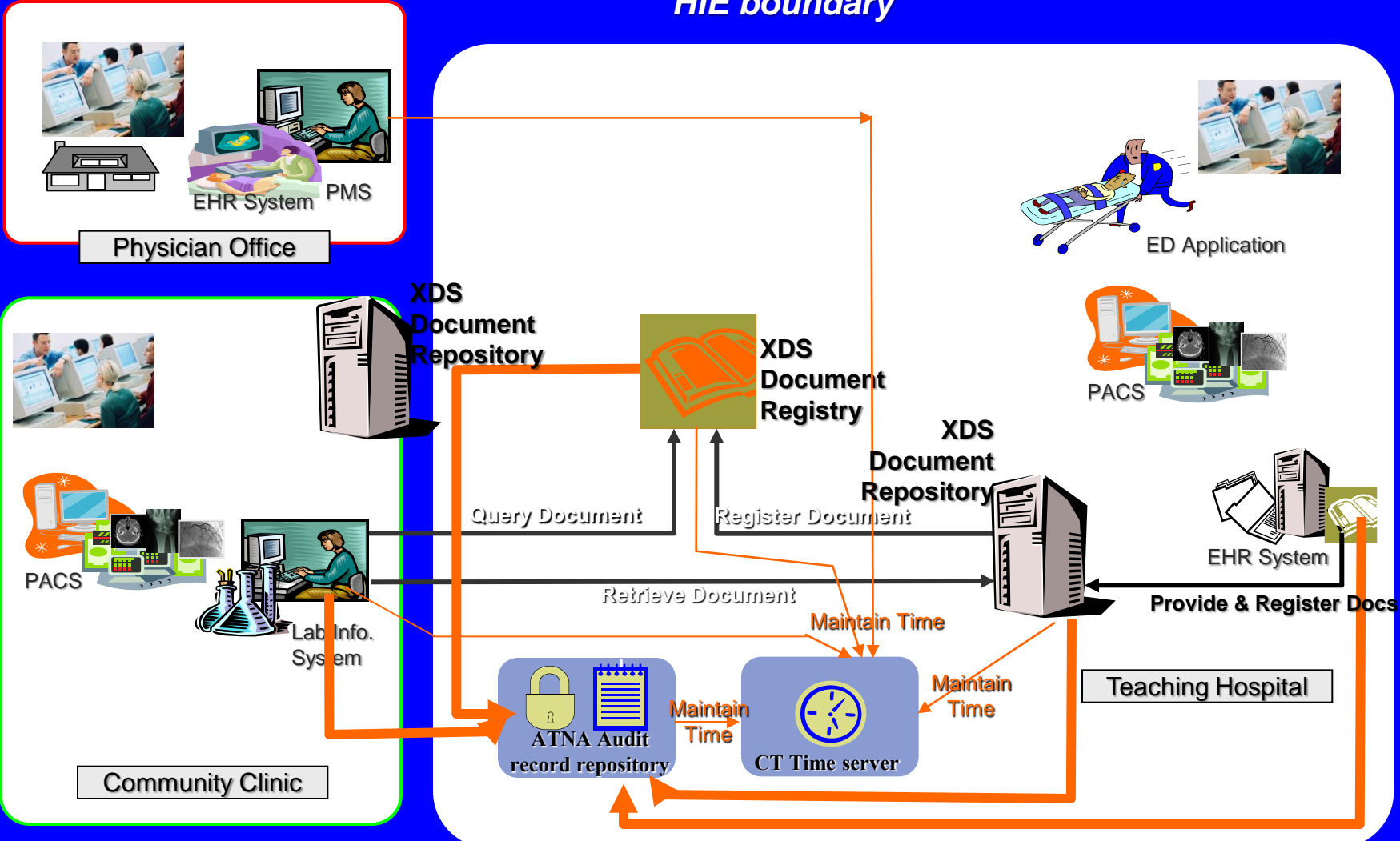
- Investigate Audit log for specific evidence
- ATNA Audit Repositories can filter and auto-forward

● Support an Accounting of Disclosures

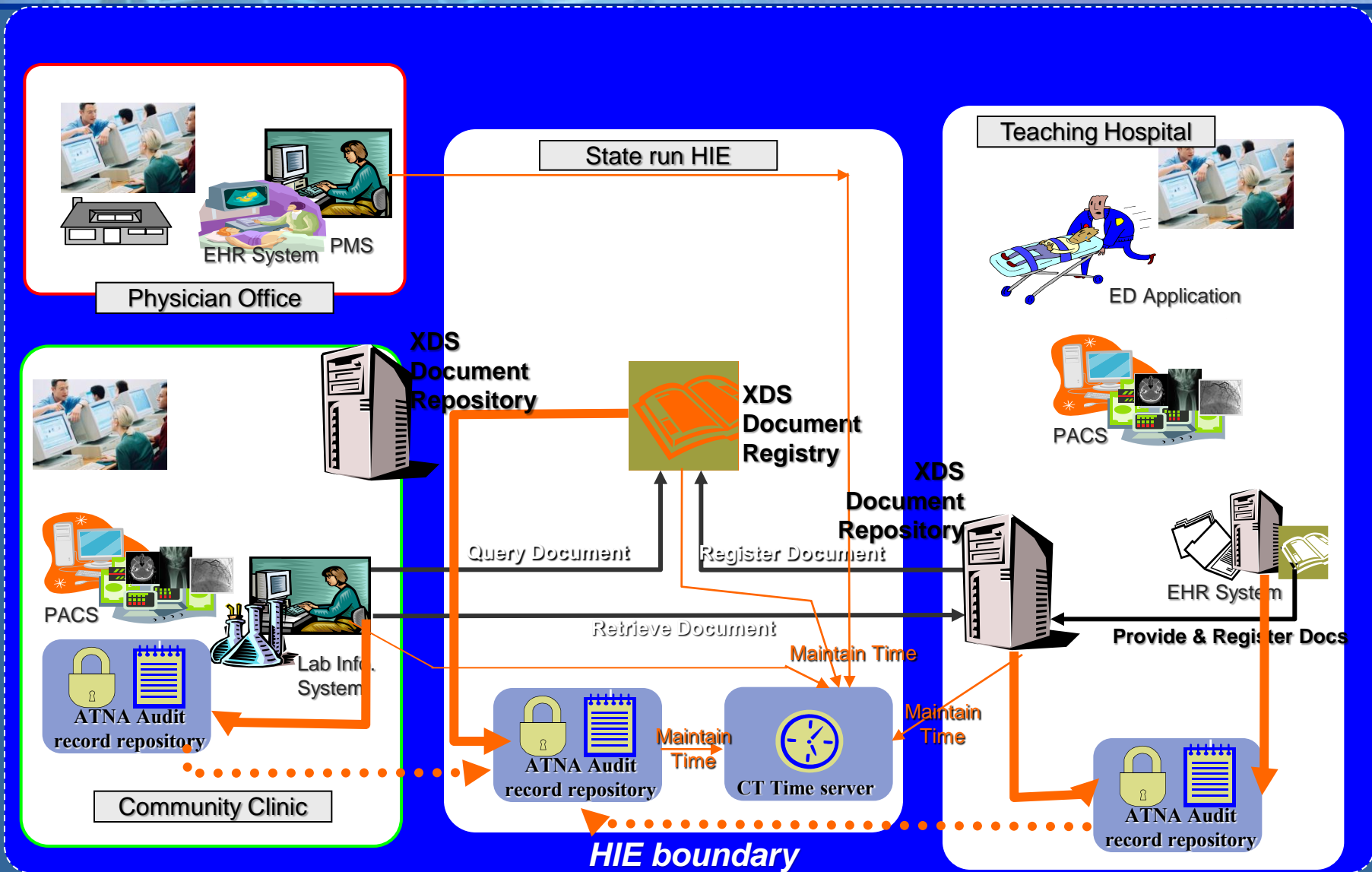
- ATNA Report is informed by XDS-Export + XDS-Import

Centralized Accountability

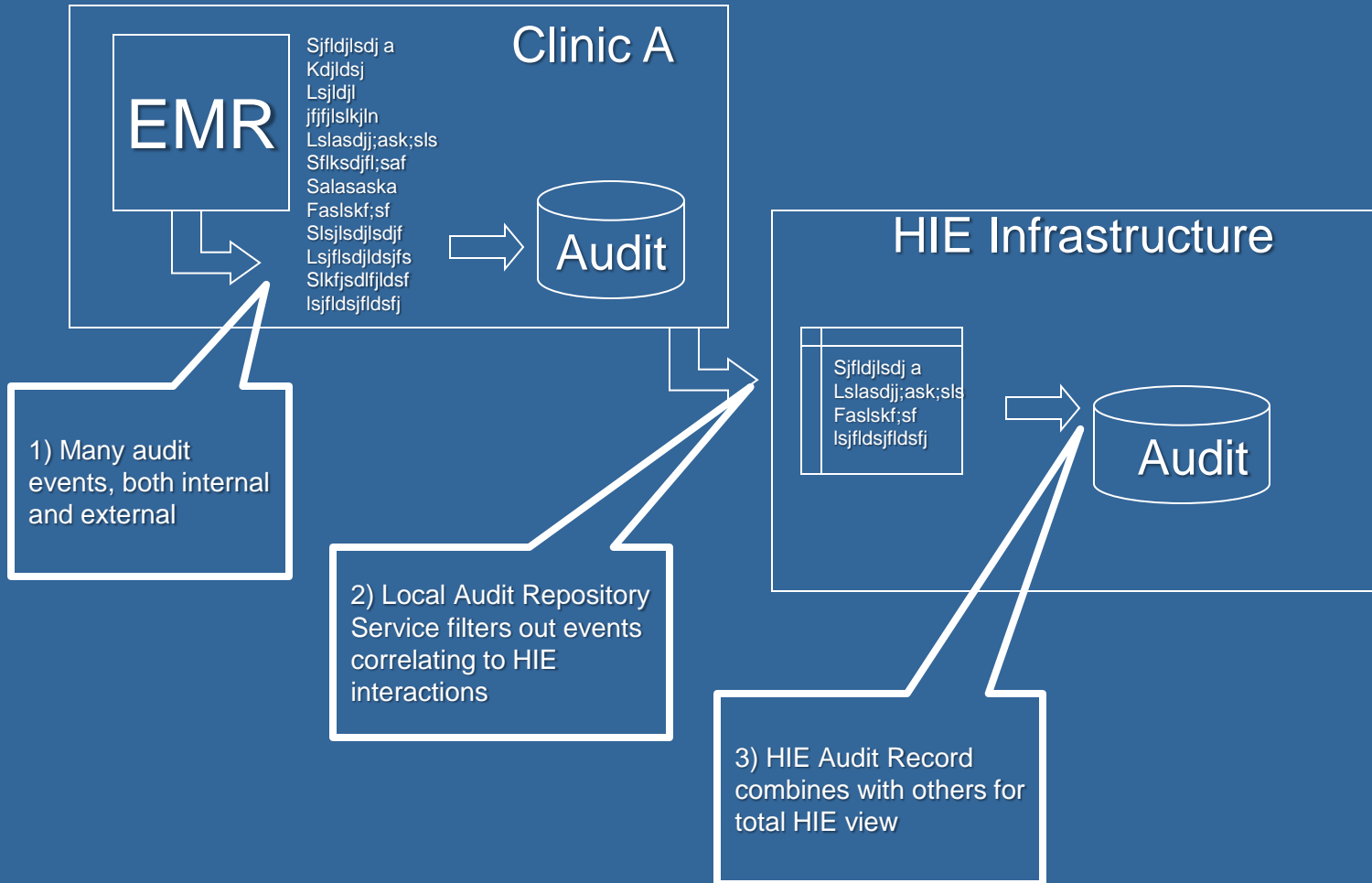
HIE boundary



Distributed Accountability



Example: Audit Log Cascade



ATNA: References

- **Status: Final Text**
- **IHE ITI Technical Framework**
 - Vol. 1 - Section 9
 - Vol. 2a - Sections 3.19, 3.20
- “Security Considerations” section found in other Profiles may specialize how ATNA is applied
- The Audit Event Message typically specialized in Vol 2 at the Transaction level
 - PIX QueryTransaction : See section Vol 2a:3.9.5.1
 - XDS Register Document Set-b: See section Vol 2b:3.42.7.1



EUA

Enterprise User Authentication

EUA Introduction

- 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.

Value Proposition

- **Meet a basic security requirement**
 - User authentication is necessary for most applications and data access operations.
- **Achieve cost savings/containment**
 - Centralize user authentication management
 - Simplify multi-vendor implementations
- **Provide workflow improvement for users**
 - Increase user acceptance through simplicity
 - Decrease user task-switching time.
- **More effective security protection**
 - Consistency and simplicity yields greater assurance.

Key Attributes

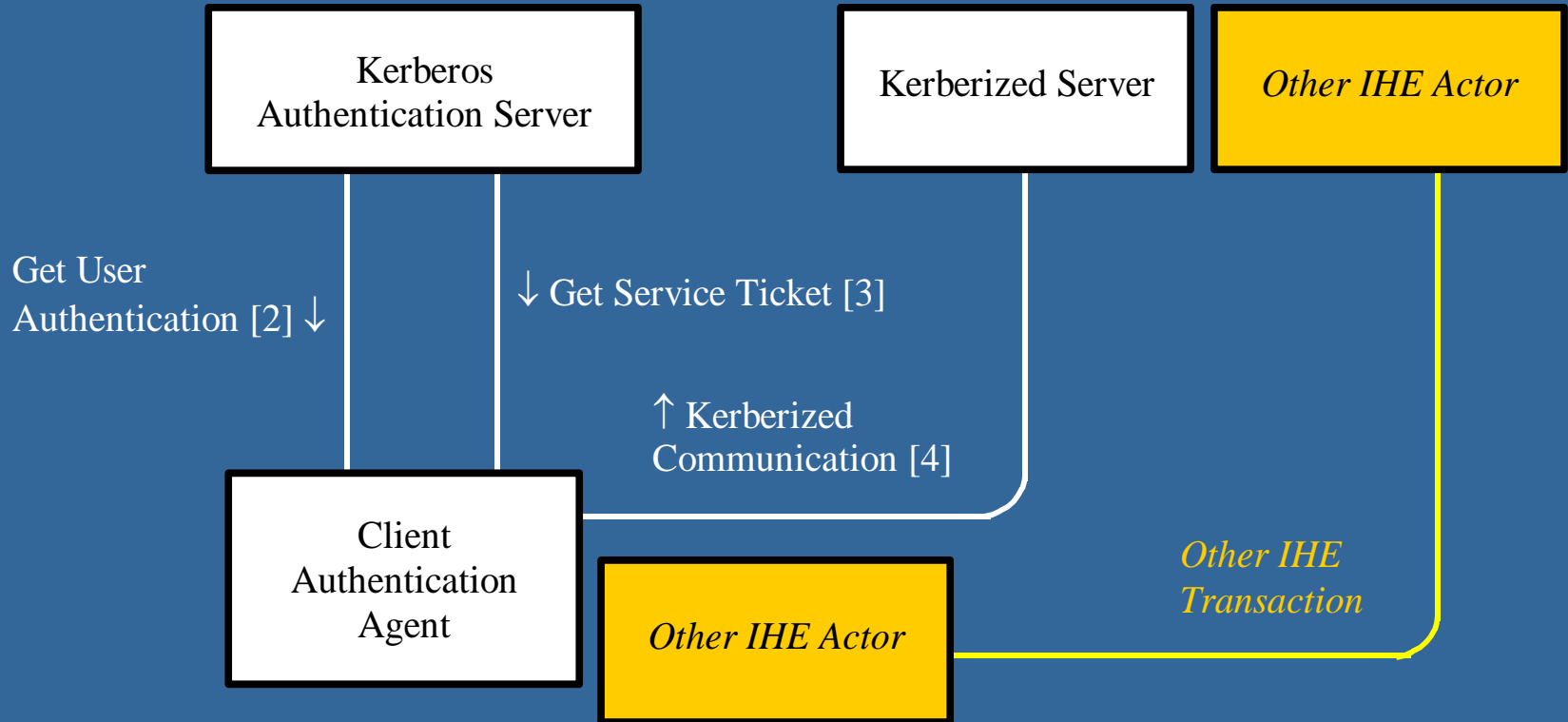
- **Limited network overhead**

- Kerberos is *network-efficient*, developed at a time when high-speed networks were rare.

- **Kerberos work with any user authentication technology**

- Tokens, biometric technologies, smart cards, ...
- Specific implementations require some proprietary components, e.g., biometric devices.
- Once user authentication is complete, network transactions are the same for all technologies.

EUA Transaction Diagram



EUA: References

- **Status: Final Text**
- **IHE ITI Technical Framework**
 - Vol 1: Section 4
 - Vol 2a: Section 3.2, 3.3, 3.4
- **Standards Used**
 - Kerberos v5 (RFC 1510)
 - Stable since 1993,
 - Widely implemented on current operating system platforms
 - Successfully withstood attacks in its 10-year history
 - Fully interoperable among all platforms
- **Minimal Application Changes**
 - Eliminate application-specific, non-interoperable authentication
 - Replace less secure proprietary security techniques



XUA

Cross-Enterprise User Assertion

What Problem is Being Solved?

- **XUA Problem Statement:** The industry needs a standards-based method to provide the initiating user's identity in cross-enterprise transactions in a way that the responder can make access decisions and proper audit entries.

Value Proposition

- **Extend User Identity across organizations**
 - Users include Providers, Patients, Clerical, etc
 - Must supports cross-enterprise transactions (e.g XDS, XCA), can be used inside enterprise
 - Distributed or Centralized Identity management (Directories)
- **Provide information necessary so that receiving actors can make Access Control decisions**
 - Authentication mechanism used
 - Attributes about the user (roles)
 - Does not include Access Control mechanism
- **Provide information necessary so that receiving actors can produce detailed and accurate Security Audit Trail**

Technical Solution

- **Initial scope to XDS.b Stored Query and Retrieve**
 - Relies on Web-Services
 - Easily extended to any Web-Services transactions
 - Leverage WS-I Basic Security Profile 1.1
- **Use SAML 2.0 Identity Assertions**
 - Does not constrain 'how' the Assertion was obtained
 - Supporting Kantara Initiative (formerly Liberty Alliance)
 - May be obtained using WS-Trust or SAML
- **Define grouping behavior with EUA and ATNA**

XUA: Attribute Extension supplement

● User Role

- To support Role Based Access Control

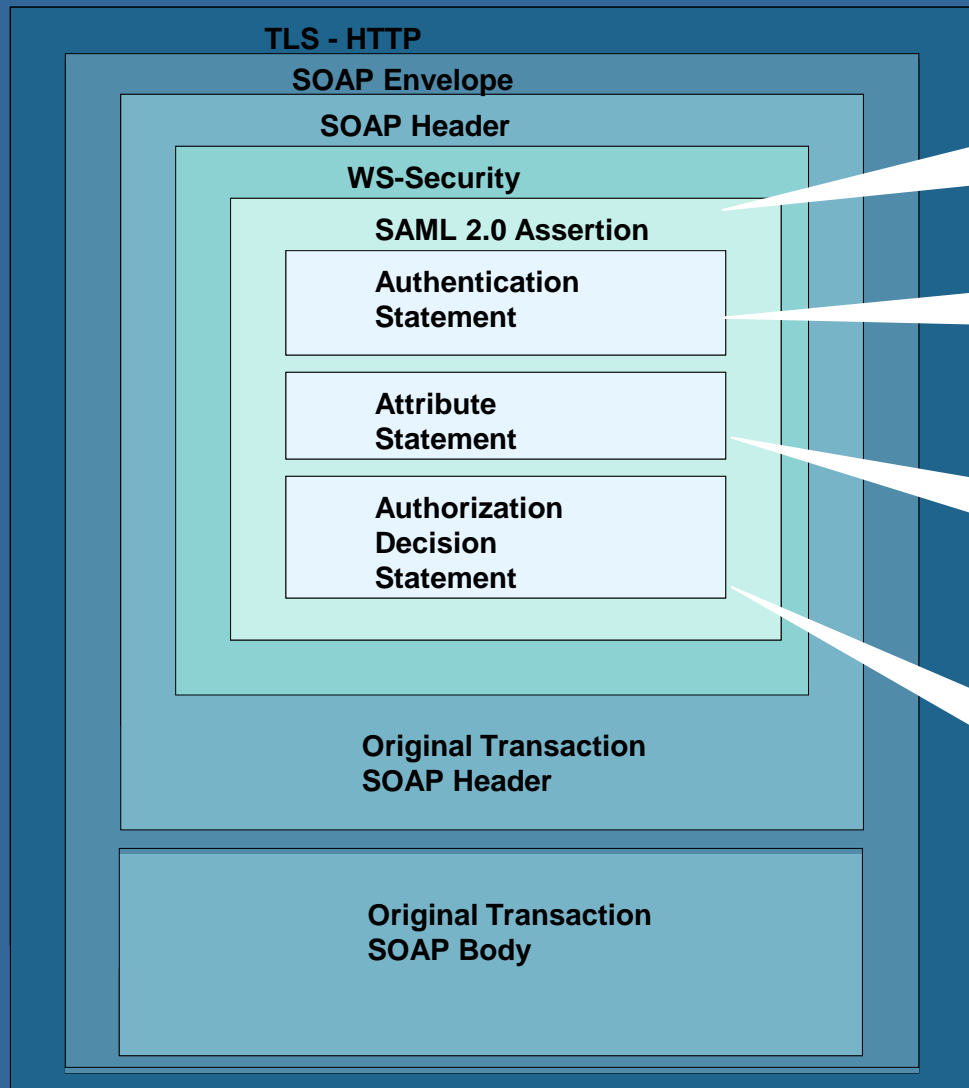
● Consent / Authorization

- To support use-cases where the requesting party has explicit consent

● Purpose Of Use

- Carry an indicator of what the reason for the transaction is and what will be done with the result

XUA encoded in Web-Services



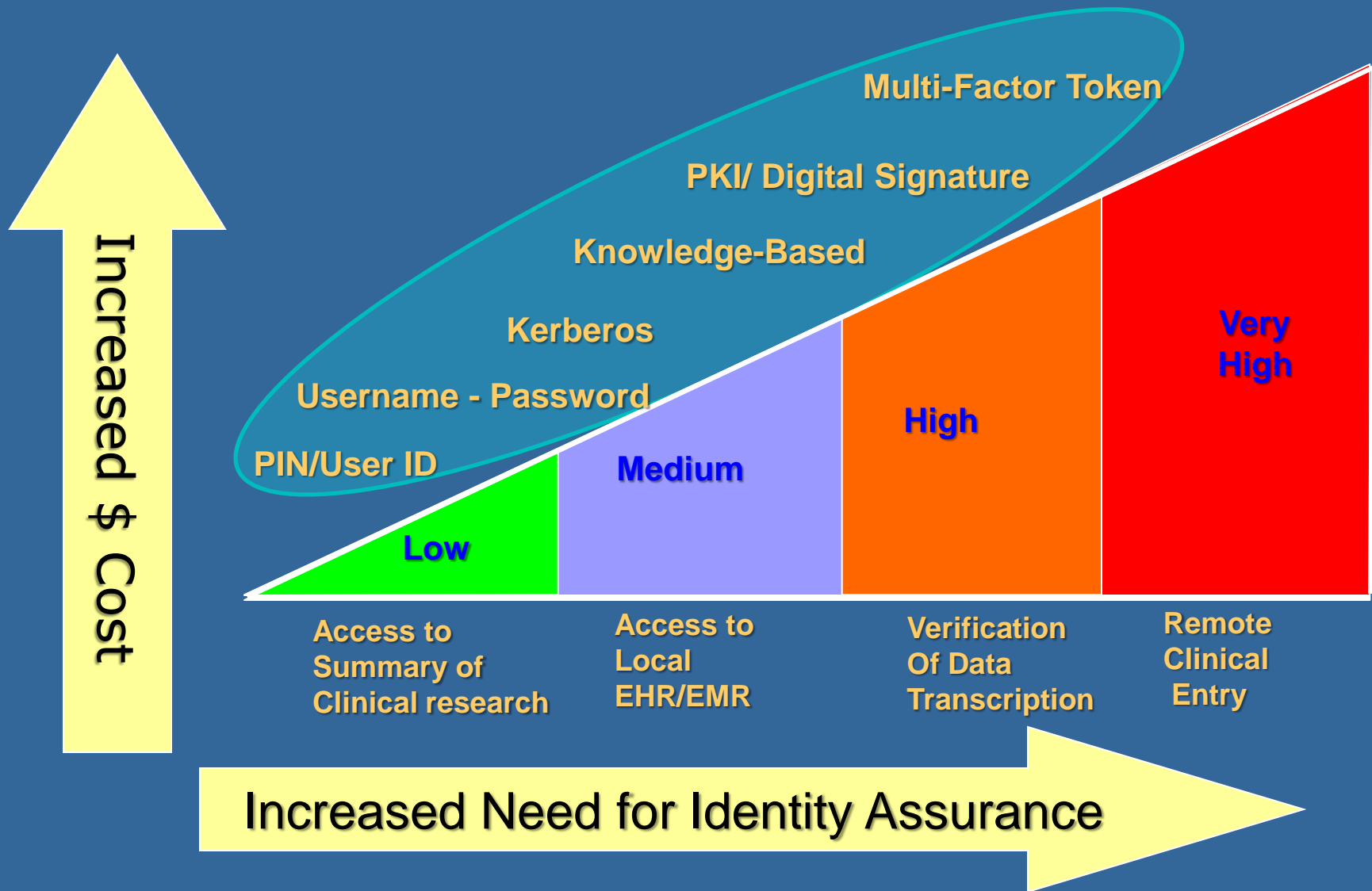
Who is Authority?
How/Why to Trust?
Constraints (time)?

Who is User?
How they were authenticated?

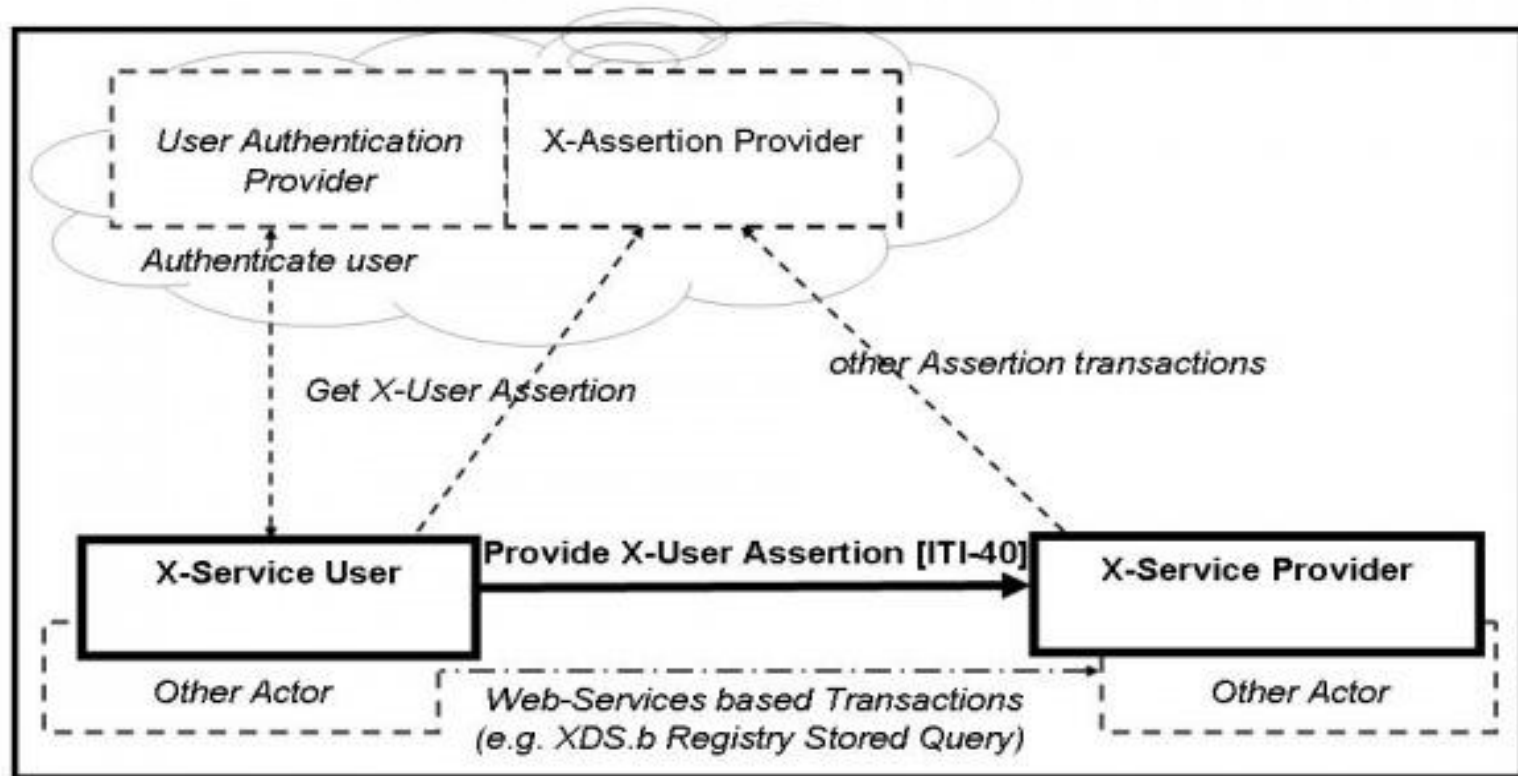
What Roles apply?
What is the Purpose?

What Consent applies?

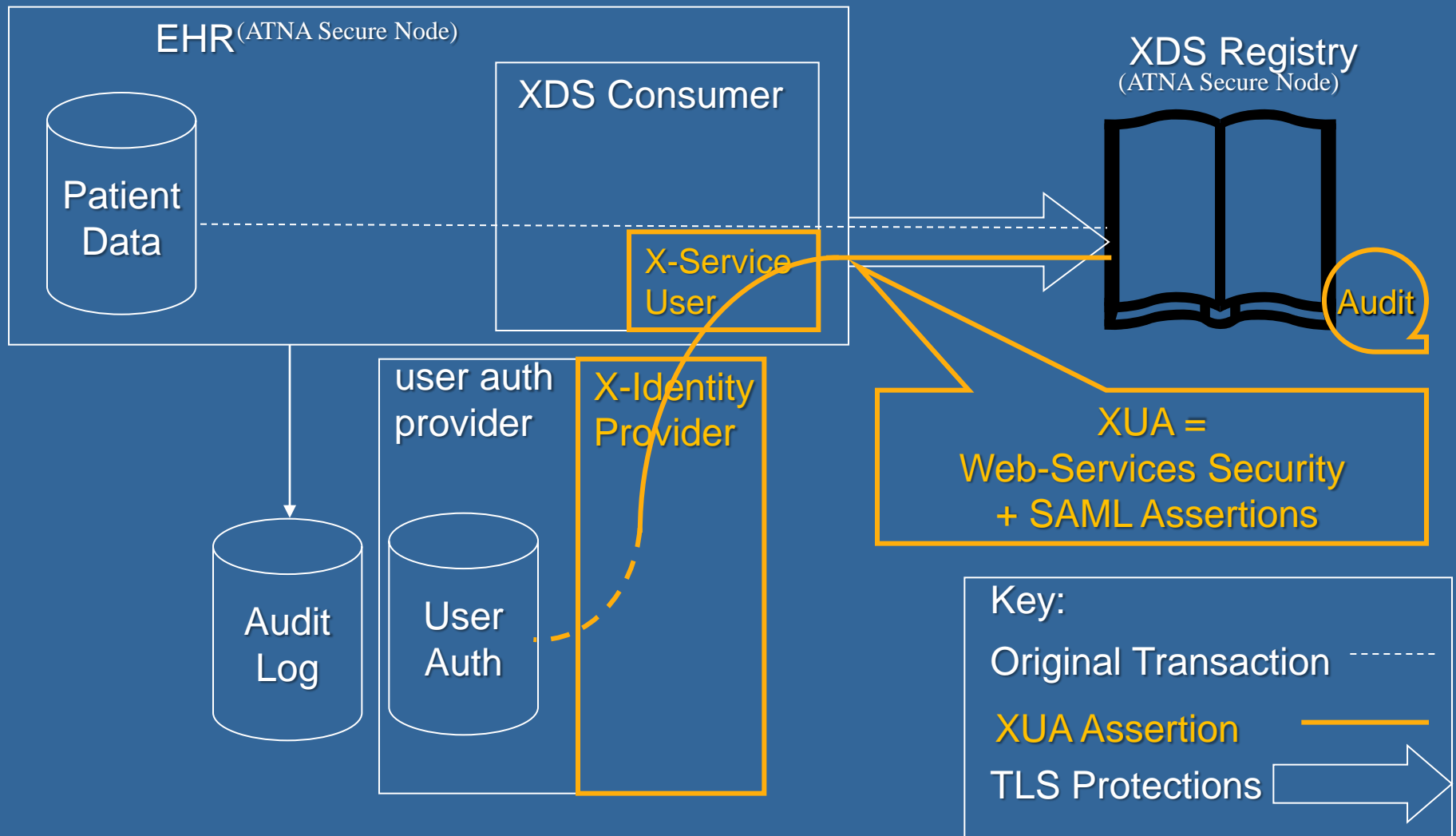
Level of Identity Assurance



XUA Actors



Implementation Example



XUA: References

- **Status: Final Text**
- **IHE ITI Technical Framework**
 - Vol 1: Section 13
 - Vol 2b: Section 3.40
- **Standards Used**
 - SAML 2.0 Identity Assertions
 - Web-Services Security header
 - WS-I Basic Security Profile

Profiles mapped to Security & Privacy Controls

Security & Privacy Controls		Audit Log	Authentication and Identification	Data Access Control	Secrecy	Data Integrity	Non-Repudiation	Patient Privacy
IHE Profile	Profile Issued							
Audit Trails and Node Authentication	2004	√	√	√	√	√	√	√
Consistent Time	2003	√	.				√	
Enterprise User Authentication	2003		√	.			.	.
Cross-Enterprise User Assertion	2006		√	.			.	.
Basic Patient Privacy Consents	2006			.				√
Personnel White Pages	2004		√	√			.	
Healthcare Provider Directory	2010		√	.			.	
Document Digital Signature	2005		√			√	√	
Document Encryption (in development)	2011			√	√	.		

More Information

- IHE Web site: www.ihe.net

- *IHE official material*
- *Technical Framework documents*

- IHE Wiki site: wiki.ihe.net

- *IHE committee pages*
- *Implementation Notes*
- *Ongoing committee work*

- *IHE ITI technical committee mailing list*

- *Instructions on the bottom of :*
- http://www.ihe.net/IT_Infra/committees



IHE Changing the Way Healthcare **CONNECTS**

WWW.IHE.NET

August 19, 2011