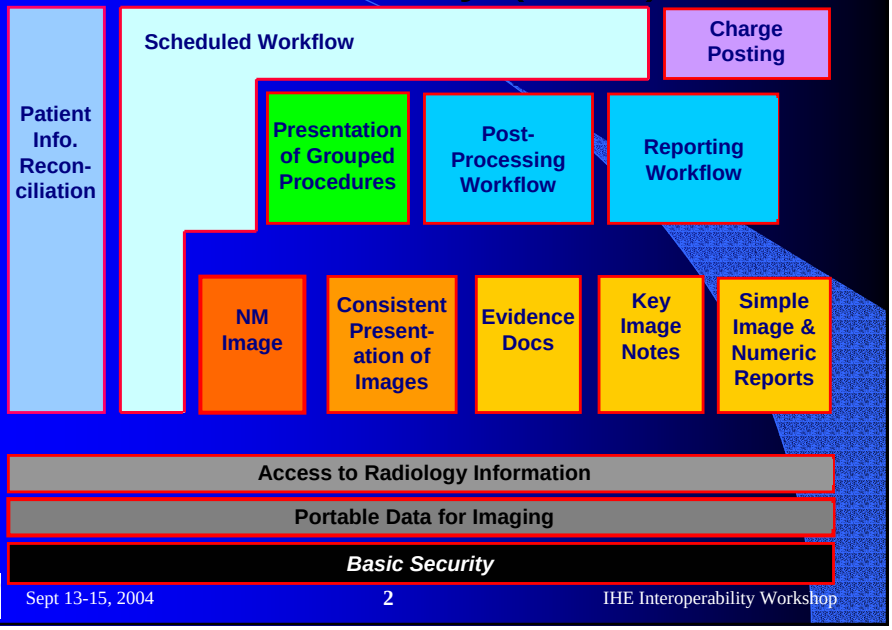
Integrating the Healthcare Enterprise

Basic Security

Robert Horn

Agfa Healthcare

Basic Security (SEC)



Overview

- Security Requirements
- Actors and Transactions

Security requirements

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

Security measures

- **Authentication:**
  Establish the user and/or system identity, answers question:
  "Who are you?"

- **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?"

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?"

IHE Goal

IHE is establishing the first level of enterprise-wide security infrastructure for meeting privacy requirements (HIPAA, and like regulations world-wide).

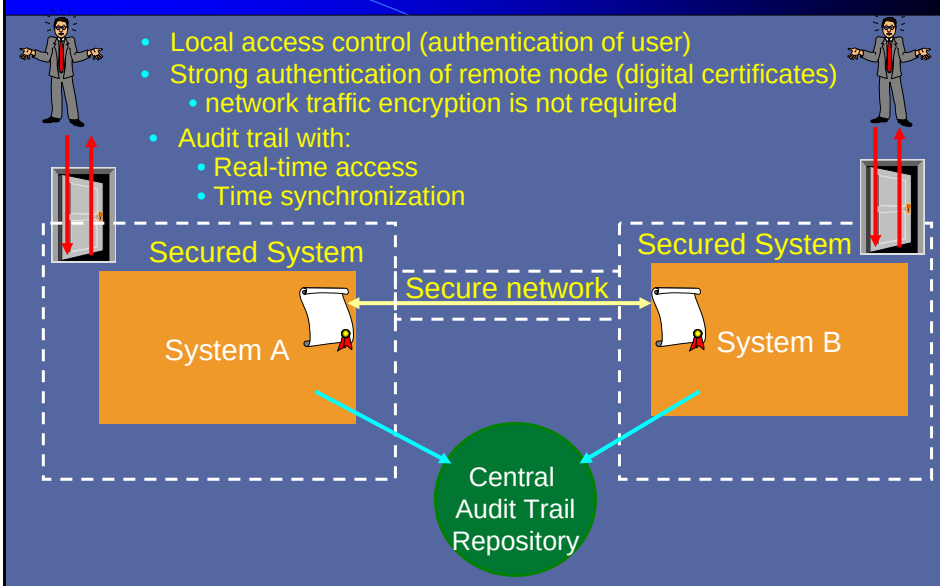
IHE Goal

IHE makes cross-node security management easy:

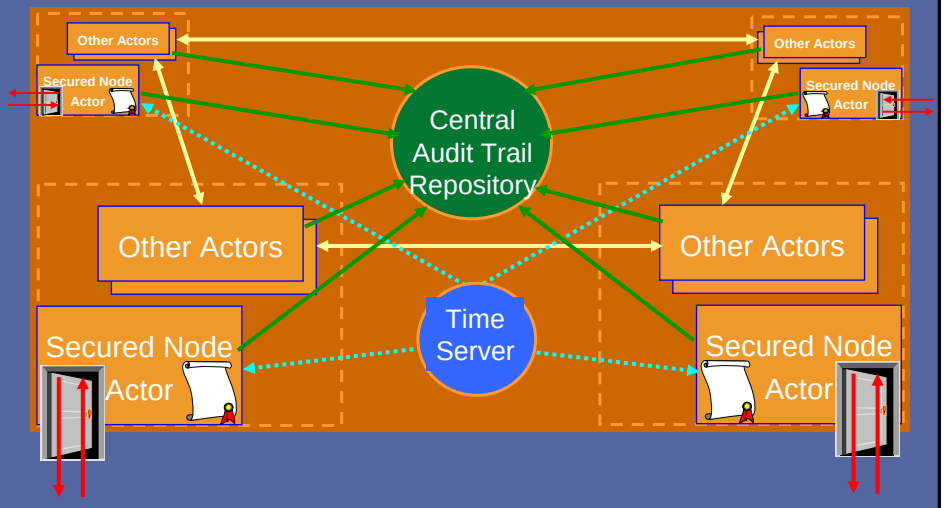
- Only a simple manual certificate installation is needed.
- Healthcare professionals are not hindered by ”complex” role based access control. However, policies may restrict them to ‘need to know information’.
- Enforcement driven by ‘a posteriori audits’ and real-time visibility.

Integrating trusted nodes

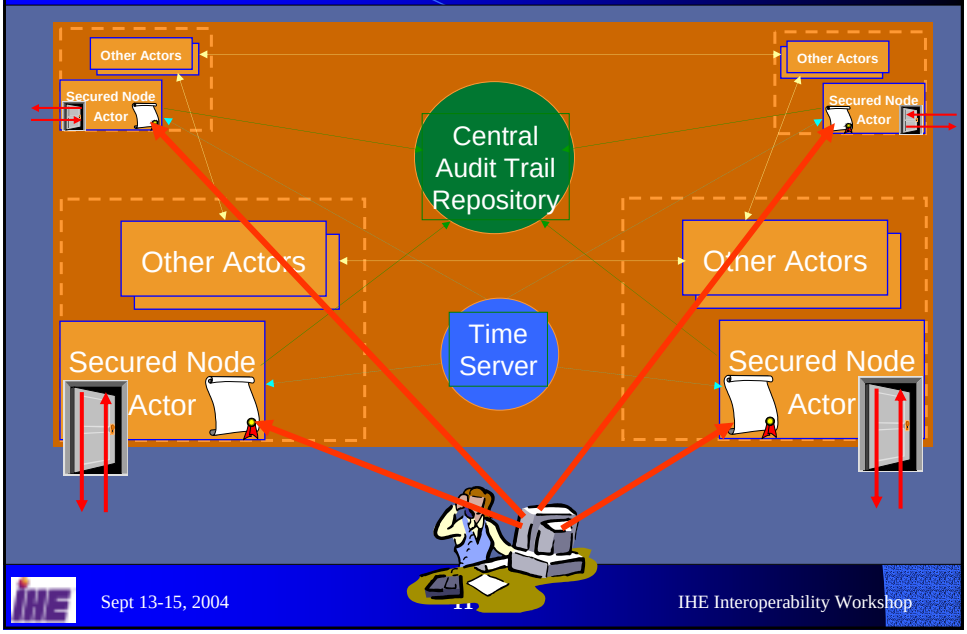
- Local access control (authentication of user)
- Strong authentication of remote node (digital certificates)
  - network traffic encryption is not required
- Audit trail with:
  - Real-time access
  - Time synchronization



Secured Domain: integrating trusted nodes



Secured Domain: Limited Administration
Audit Trail/Time Server + CA for certificates to each node



IHE Audit Trail Events
20 Non-Transaction Related

Trigger Event	Description
Actor-Start-Stop	Startup and shutdown of any actor.
Actor- config	Generated for any configuration change related to the actor.
PHI-export	Any export of PHI on media, either removable or files.
PHI-Print	Any printing activity that print PHI.
PHI-import	Any import of PHI on media, either removable or files.

IHE Audit Trail Events
20 Non-Transaction Related

Trigger Event	Description
Patient-record-event	Patient record created, modified or accessed.
Order-record-event	Order record created, accessed, modified, or deleted.
Procedure-record-event	Procedure record created, accessed, modified, or deleted
Begin-storing-instances	Begin storing SOP instances for a study.
Instances-stored	Instances for a particular study have been stored on this system.

IHE Audit Trail Events
20 Non-Transaction Related

Trigger Event	Description
Instances-used	SOP instances from a specific study are created, modified or accessed.
Instances-deleted	SOP instances are deleted from a specific study.
Begin-storing-reports	Reports have been sent for storage.
Report-Object-event	Reports have been created, modified or accessed.
Study-object-event	Study is created, modified or accessed.

IHE Audit Trail Events
20 Non-Transaction Related

Trigger Event	Description
Study-deleted-event	Study, or instances within a study, are deleted.
Node-authentication-failure	A secure node authentication failure has occurred during TLS negotiation.
User-authenticated	The local user authentication procedure has detected a failure.
Audit-log-used	The audit trail repository has been accessed or modified.
Mobile-machine-event	Mobile machine joins or leaves secure domain.

IHE Audit Trail Events, 18 Transaction Related

Trigger Event	Description
Modality-worklist-provided	Modality worklist query received.
Image-availability-query	Image availability query received.
Query-images	Image query received.
Retrieve-images	Images are transferred from one node to the other. Report by source node
Retrieve-images	Images are transferred from one node to the other. Report by receiving node

IHE Audit Trail Events, 18 Transaction Related

Trigger Event	Description
Query-presentation-states	Presentation states are queried.
Retrieve-presentation-states	Presentation states are transferred from one node to the other. Report by source node
Retrieve-presentation-states	Presentation states are transferred from one node to the other. Report by receiving node
Query-key-image-notes	Key image notes are queried.
Retrieve-key-image-notes	Key image notes are transferred from one node to the other. Report by source node

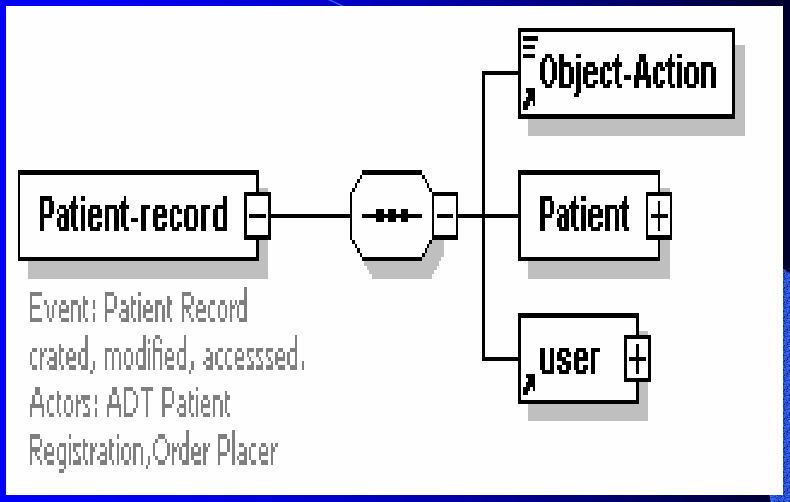
IHE Audit Trail Events, 18 Transaction Related

Trigger Event	Description
Retrieve-key-image-notes	Key image notes are transferred from one node to the other. Report by receiving node
Query-reports	A report repository has been queried for reports.
Retrieve-reports	Reports are transferred from one node to the other. Report by source node
Retrieve-reports	Reports are transferred from one node to the other. Report by receiving node
Structured-report-export	Reports have been sent to an external report repository.

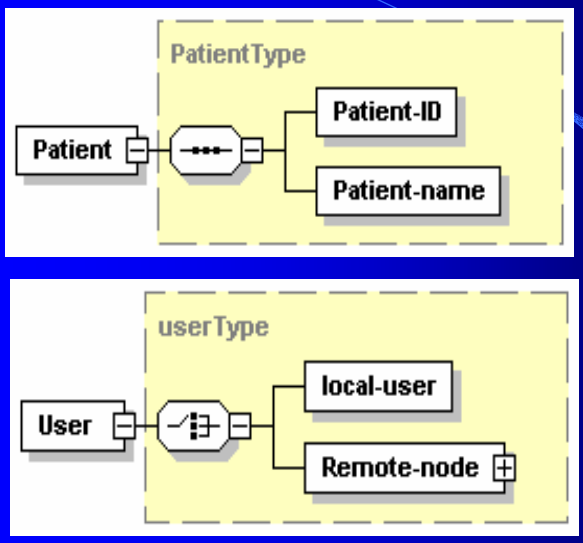
IHE Audit Trail Events, 18 Transaction Related

Trigger Event	Description
Report-submission	Reports have been sent to a report manager.
Report-issuing	Reports have been sent to a report repository.
Print-request-with-presentation-LUT	A print session specifying a presentation LUT has been sent.

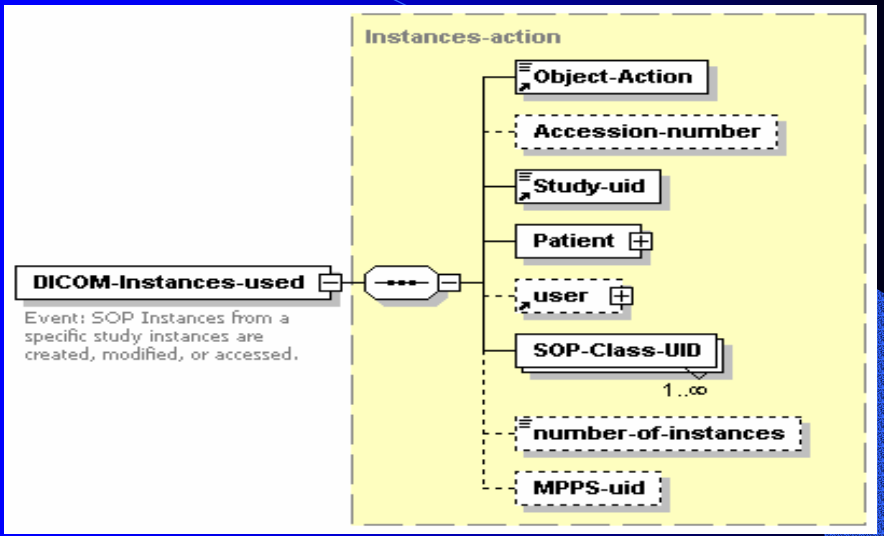
Example Audit Record for Patient-record-event



Example Audit Record for Patient-record-event

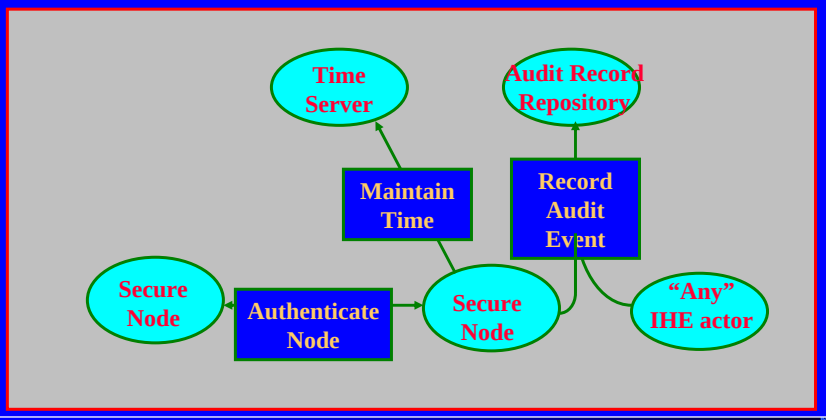


Example Audit Record for Instances-used



Basic Security Integration Profile
Actor and Transaction diagram

All existing IHE actors need to be grouped with a Secure Node actor.



Basic Security Integration Profile
Actor grouping rules

- If an actor wants to support the Basic Security Profile, this actor shall be grouped with a secure Node actor.
- All actors grouped with a Secure Node actor in an implementation must support the Basic Security Profile.

Authenticate Node transaction

- 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.

Authenticate Node transaction

- TLS_RSA_WITH_NULL_SHA cyphersuite shall be supported for authentication
- If the optional encryption is selected, the TLS_RSA_WITH_3DES_SHA cyphersuite shall be supported.
- The well-known port 2762" as specified by DICOM shall be supported.

Record Audit Event transaction

- **The BSD Syslog protocol (RFC 3164) for Audit Records**
- **Audit trail events and content, no standard available at the time of writing.**
- **IHE in Technical Framework :**
  Use IHE defined XML Schema for defined content in payload of Syslog message

IT Infrastructure – Secure Node

- **The Radiology Basic Secure Node is also an IT Infrastructure Secure Node, but**
- **IT Infrastructure adds:**
  - Use of reliable syslog as an option
  - Audit messages defined by IETF, HL7, and DICOM. These accommodate more than just radiology uses. The secure node may use either format.

Maintain Time transaction

- 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

More information….

- IHE Web sites:
  - http://www.himss.org/IHE
  - http://www.rsna.org/IHE
  - http://www.acc.org/quality/ihe.htm
- Technical Frameworks:
  - ITI V1.0, RAD V5.5, LAB V1.0
- Technical Framework Supplements - Trial Implementation
  - May 2004: Radiology
  - August 2004: Cardiology, IT Infrastructure
- Non-Technical Brochures :
  - Calls for Participation
  - IHE Fact Sheet and FAQ
  - IHE Integration Profiles: Guidelines for Buyers
  - IHE Connect-a-thon Results
  - Vendor Products Integration Statements