THE EDWARD MALLINCKRODT INSTITUTE OF RADIOLOGY

DICOM Security

Lawrence Tarbox, Ph.D.
Chair, WG 14

Mallinckrodt Institute of Radiology
Washington University in St. Louis School of Medicine

Security Mechanisms Available in DICOM

- Secure Exchange
  - Communications Channel
  - Media
- Secure Objects
  - Object Confidentiality
  - Digital Signatures
- Secure Infrastructure
  - Audit Trails
  - User Identity Exchange

Secure Exchange

- Goals
  - Entity authentication
  - Data integrity during transit
  - Confidentiality during transit via encryption
- Mechanisms
  - Secure Transport Connection Profiles
    - TLS 1.0 (derived from SSL) with 3DES
    - TLS 1.0 with AES
    - ISCL
  - Secure Use Profiles
    - Online Electronic Storage
  - Secure Media Profiles

Security Communication Profiles

- ISCL Secure Transport
  - Based on ISCL standard (from Japan)
  - Symmetric encryption for authentication
  - Specified for Online Electronic Storage standard

- TLS Secure Transport
  - TLS 1.0 framework
  - RSA based certificates for peer authentication
  - RSA for exchange of master secrets
  - SHA-1 hash as an integrity check
  - Triple DES EDE, CBC encryption
  - Optional AES encryption (preferred)

AES Secure Transport

- Backwards compatible with the existing profile
  - Request AES encryption, with fallback to Triple DES
- Why AES?
  - Not proprietary
  - Expected to be widely available
  - More efficient that 3DES
    - 10% to 30% of the computation load
    - Possible to encrypt and transmit at 100 Mbit/second without special hardware

What about VPN

- No DICOM profile at this time
- But not excluded for *private* networks (local policy issue)

Media Security

- Protects entire DICOM files
  - Includes DICOM directory
  - Files are held inside an encrypted envelope
- Utilizes Cryptographic Message Syntax
  - An internet standard
  - Only selected recipients can open the envelope
  - Data integrity check
  - Identifies a single file creator
- Several Secure Media Storage Profiles

Object Confidentiality

- De-identification
- Attribute-level Encryption

De-Identification

Why?

- Teaching files, clinical trials, controlled access

How?

- Simply remove Data Elements that contain patient identifying information?
  - e.g., per HIPAA's safe harbor rules

But

- Many such Data Elements are required

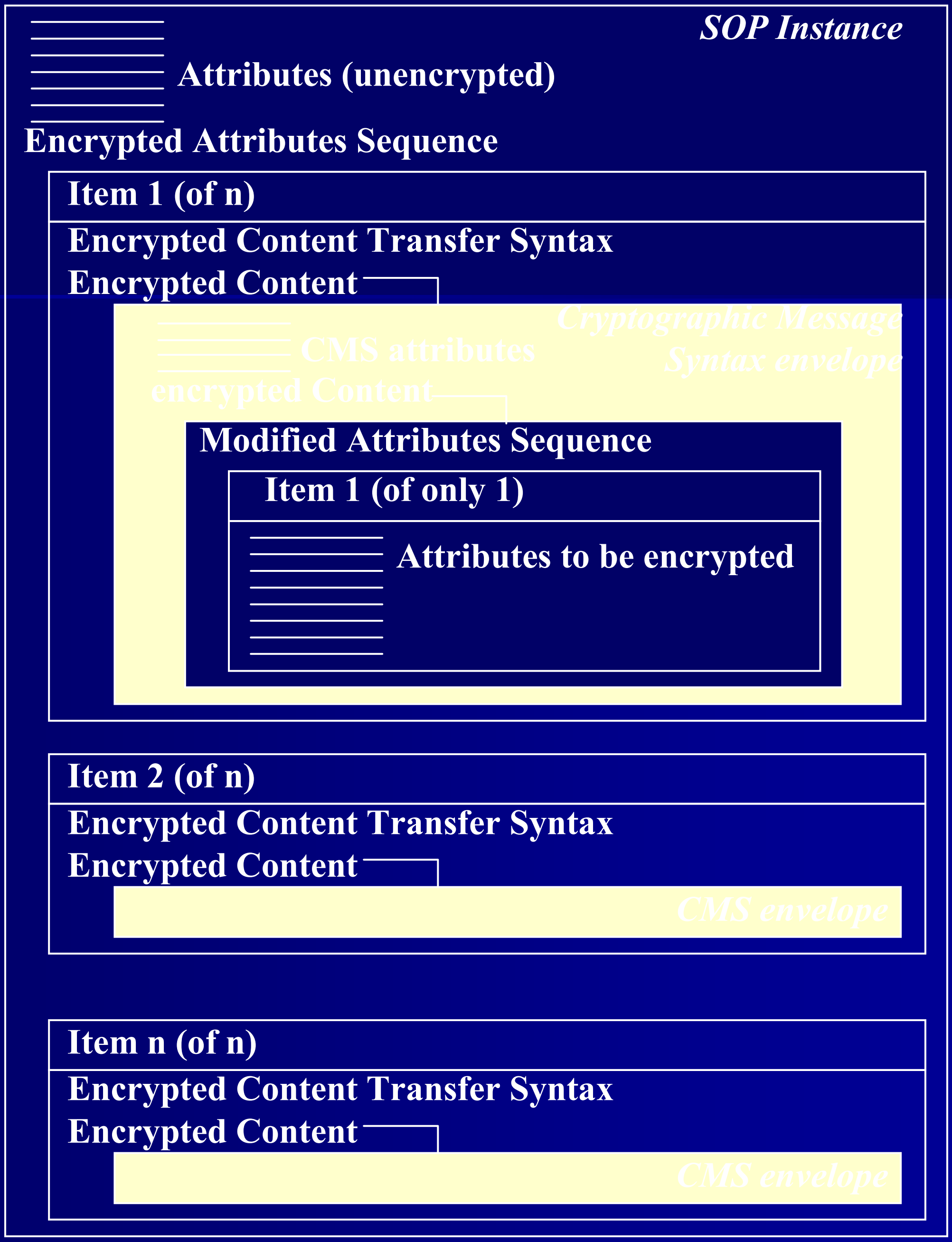
So

- Instead of remove, replace with a bogus value

Attribute Level Encryption

- Since some use cases require controlled access to the original Attribute values:
  - Original values can be stored in a CMS (Cryptographic Message Syntax) envelope
    - Embedded in the Data Set
    - Only selected recipients can open the envelope
    - Different subsets can be held for different recipients
  - Full restoration of data not a goal

- Attribute Confidentiality Profiles



SOP Instance

Attributes (unencrypted)

Encrypted Attributes Sequence

Item 1 (of n)

Encrypted Content Transfer Syntax

Encrypted Content

Cryptographic Message Syntax envelope

CMS attributes

encrypted Content

Modified Attributes Sequence

Item 1 (of only 1)

Attributes to be encrypted

Item 2 (of n)

Encrypted Content Transfer Syntax

Encrypted Content

CMS envelope

Item n (of n)

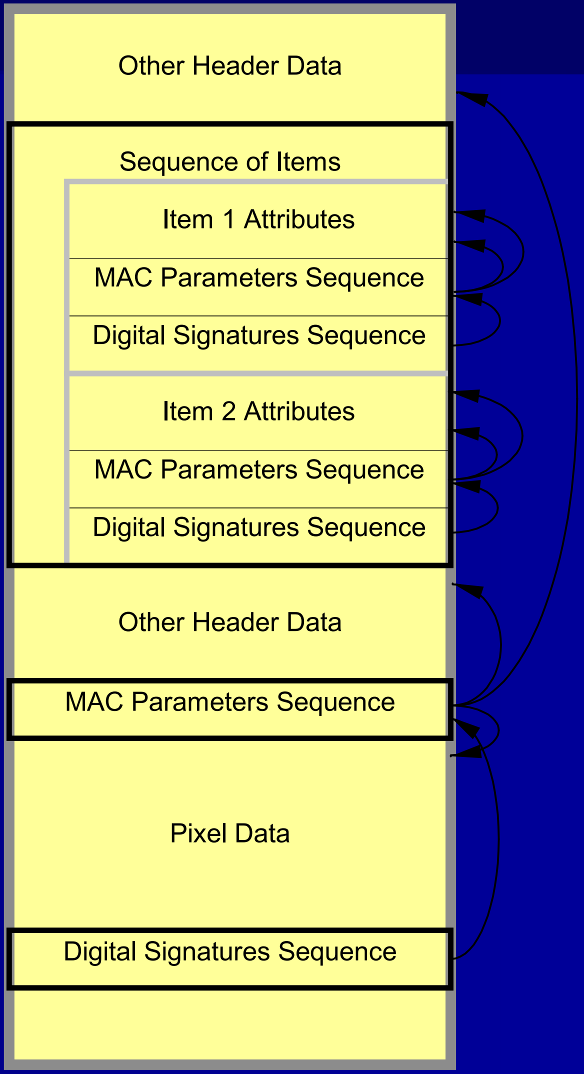
Encrypted Content Transfer Syntax

Encrypted Content

CMS envelope

Digital Signatures

- Embedded in SOP Instance
- Lifetime integrity check.
- Identifies signer
- Optional secure timestamp
- Multiple signatures
  - Overlapping subsets
  - Multiple signers
  - Signatures on individual items
- Signatures Have Purposes!

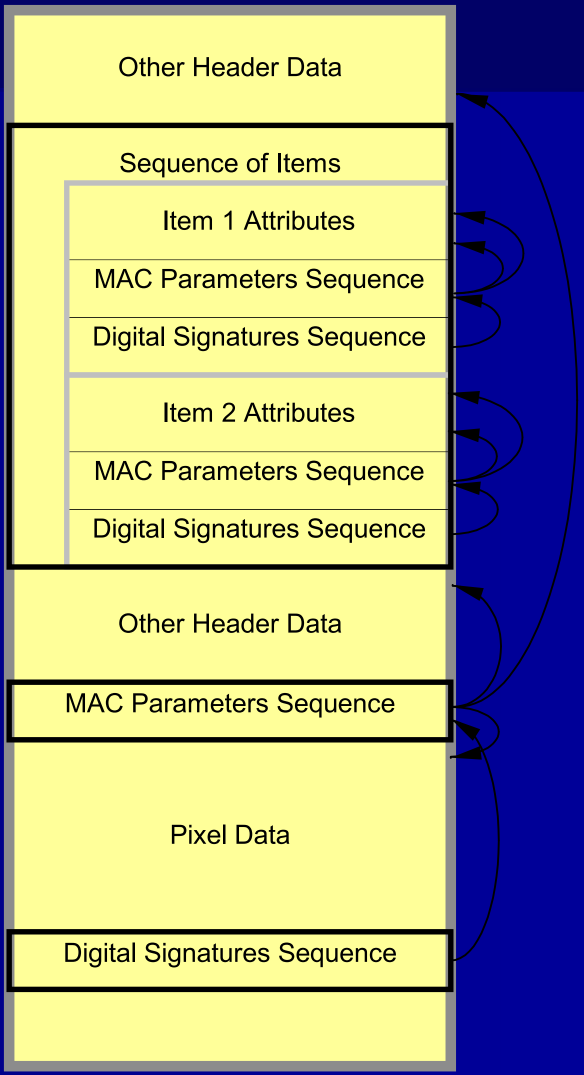


Purpose of Digital Signature

- "Purpose" field differentiates between signers (from ASTM 1762 standard), e.g.
  - Author
  - Verifier
  - Reviewer
  - Witness
    - Event
    - Identity
    - Consent
  - Administrative

Signatures Embedded in DICOM

- Selected Attributes within data set
- Sequence encoded as a single entity.
- Items in a sequence can be signed individually



Current Profiles

- Secure Use Profiles
  - Base Digital Signatures
    - For legacy systems
      - Verify on input
      - Create new on output
  - Bit-preserving Digital Signature
    - Possible future implementations?
- Digital Signature Profiles
  - Base RSA (referenced by other profiles)
  - Creator RSA (typically the equipment)
  - Authorization RSA (typically the operator)
  - Structured Report RSA

SR Digital Signatures

- What is signed?
  - SOP Class UID
  - Study and Series Instance UID
  - All of the SR Document Content Module
  - Current and Pertinent Evidence Sequence
  - Once “VERIFIED”
    - SOP Instance UID
    - Verification Flag
- Amendments are new SOP Instances

Secure References

- Objects that are already signed
  - Include Digital Signature UID and value
- Objects that are not signed
  - Include a secure hash of selected Attributes in the referenced object

  or

  - Reference other signed SRs that include secure hashes of the referenced object

Key Use Case for SR Digital Signatures

How can an application know what objects constitute a complete set?

Key Object Selection Extensions

- New Document Titles:
  - Complete Study/Acquisition Content
  - Manifest
  - Related Contend
- Allow Key Object Selection Documents to refer to other Key Object Selection Documents (not allowed previously)

Options Considered

- Why not MPPS?
  - MPPS is not a persistent (composite) object
  - MPPS could trigger generation of a signed Key Object Selection document
- Why not Storage Commitment?
  - Did not wish to change semantics some applications currently associate with Storage Commitment

Audit Trail Exchange

- Transmit audit trail data to a collection site
  - Simplifies long term storage
  - Simplifies monitoring and analysis
- Need goes beyond DICOM
  - Joint work HL7, DICOM, ASTM, IHE, NEMA, COCIR, JIRA, others?
  - Common base format
  - Specializations as needed

Lets Clear the Confusion!

- Base XML message format specified (IETF RFC 3881)
  - To be shared by multiple domains
  - Needs vocabulary definition to be useful
  - Transport mechanism blind
- Supplement 95 profiles, augments, and defines DICOM-specific vocabulary
  - Use the schema in Supplement to create messages and read DICOM extensions
  - Audit repositories can interpret key using the schema in the RFC
- Profile mandates Reliable Syslog (IETF RFC-3195)

Background on RFC-3195

- Reliable replacement for BSD Syslog
- Provides BEEP message structure, store and forward transport, common mandatory fields, and an XML payload.
- Options for encryption and signatures.

Level of detail

- Surveillance
  - Detail on the study level, not individual Attributes
  - Designed to detect intrusions

- ~~Forensic~~
  - ~~Could be very detailed~~
  - Determine how it happened

Extended Negotiation of User Identity

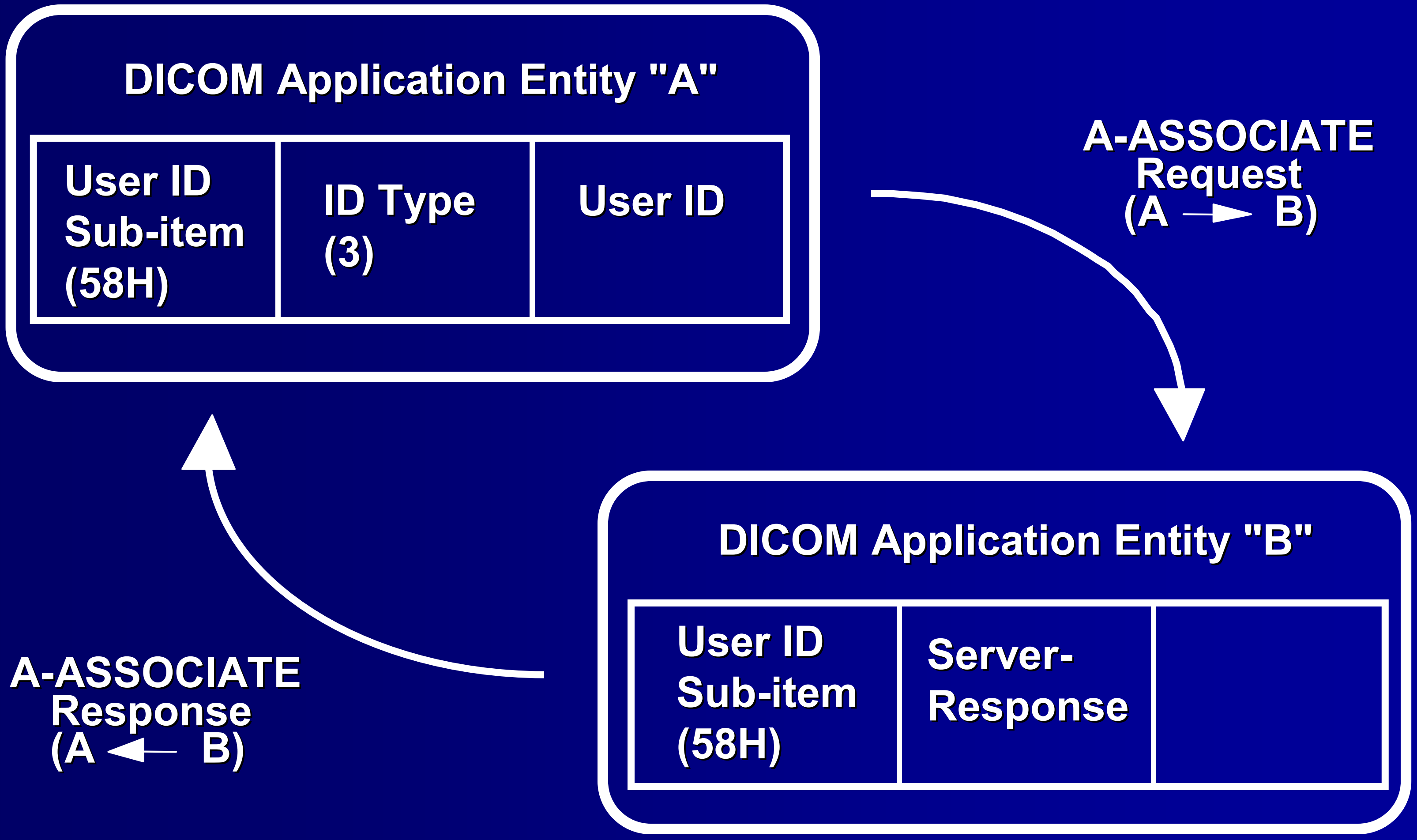
- Facilitates audit logging
- Step toward cross-system authorization and access controls
  - DICOM still leaves access control in the hands of the application
- Query Filtering
  - For productivity as well as security

Several Options

- User identity alone, with no other security mechanisms
- User identity plus the current DICOM TLS mechanism
- User identity plus future lower level transport mechanisms (e.g. IPv6 with security option)
- User identity plus VPN

Extended Negotiation

Response Expected



DICOM Application Entity "A"

User ID Sub-item (58H)	ID Type (3)	User ID

A-ASSOCIATE
Request
(A → B)

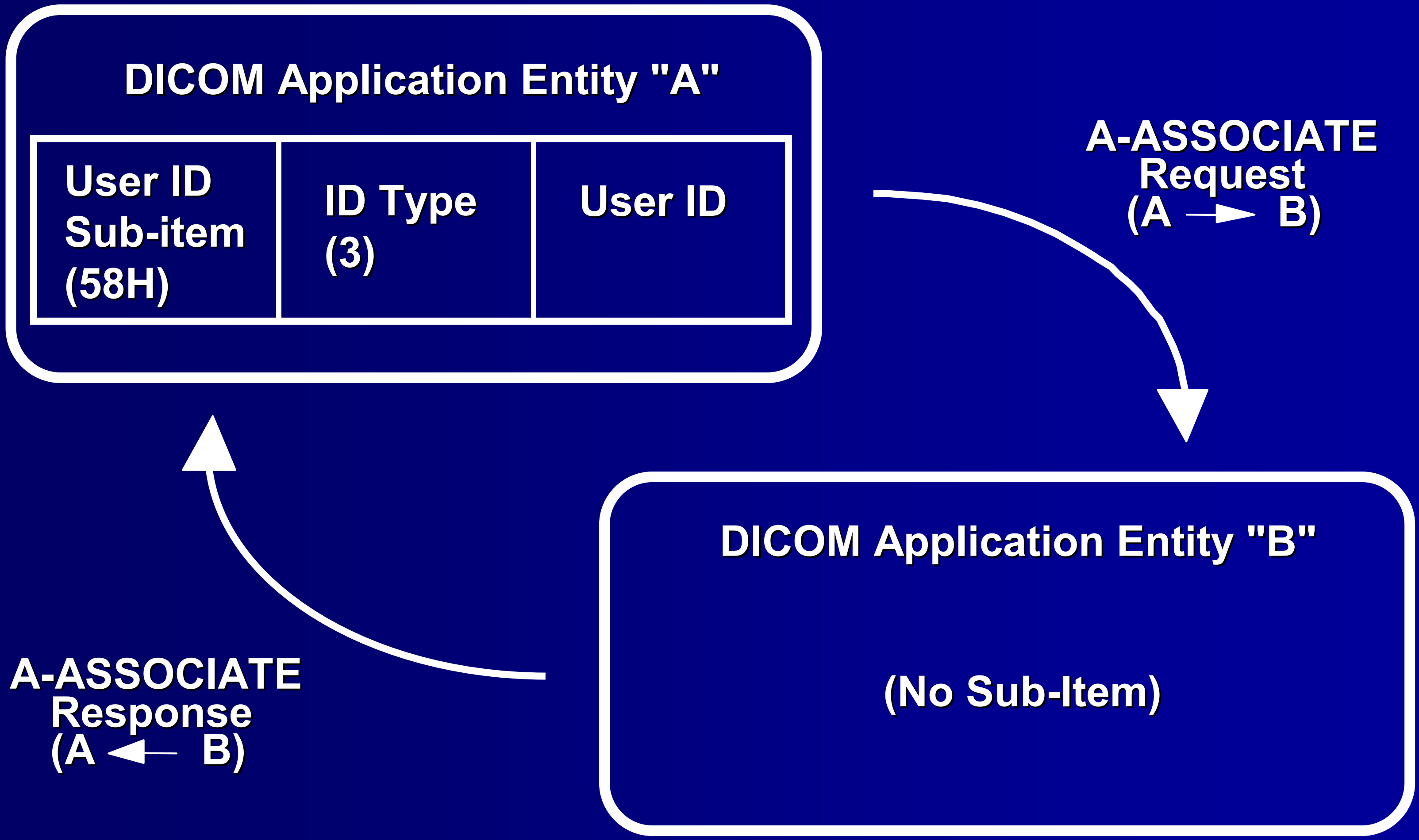
DICOM Application Entity "B"

User ID Sub-item (58H)	Server-Response	

A-ASSOCIATE
Response
(A ← B)

Extended Negotiation

No Response Expected



DICOM Application Entity "A"

User ID Sub-item (58H)	ID Type (3)	User ID

A-ASSOCIATE
Request
(A → B)

DICOM Application Entity "B"

(No Sub-Item)

A-ASSOCIATE
Response
(A ← B)

ID Type Profiles

- Un-authenticated identity assertion
  - Systems in a trusted environment
- Username plus passcode
  - Systems in a secure network
- Kerberos-based authentication
  - Strongest security

Kerberos

- Kerberos employs a Key Distribution Center (KDC) that
  - Authenticates the user
  - May be incorporated into local login process
  - Provides a Ticket Granting Ticket (TGT) to the local system
- Local application uses TGT to ask KDC to generate the Service Ticket, which then is passed in the Association Negotiation Request
- Remote application uses the Service Ticket to securely identify the user, and optionally generate a Server Ticket that is returned in the Association Negotiation Response

Prepared for the Future

- Could support any mechanism that supports uni-directional assertion mechanism (e.g. using PKI and Digital Signatures)
- Does not support identity mechanisms that require bi-directional negotiation (e.g. Liberty Alliance proposals)

Potential Future Security Topics

- Full user authentication between nodes, key management
- More sophisticated access control support
  - Role-based access
  - Institutional versus personal access
  - Patient authorization
  - List of intended recipients
- Support for new technology and algorithms
- Suggestions for future additions accepted!

We welcome your input!

Thank you.