Digital Imaging and Communications in Medicine (DICOM)

Supplement 99: Extended Negotiation of User Identity

Prepared by:

DICOM Standards Committee, Working Group 14

1300 N. 17th Street, Suite 1847

Rosslyn, Virginia 22209 USA

VERSION: Final Text

Table of Contents

Foreword

Security and privacy mechanisms require a method for establishing the identity of the person or entity that is responsible for DICOM transactions. This supplement defines three identity methods by means of a common mechanism. These are

a. the un-authenticated identity assertion. A string containing the user's identity in plain text, e.g. user's name.
b. a username plus passcode to permit authentication.
c. the authenticated Kerberos system. Kerberos authentication is widely used and well established. It provides strong authentication for network users, and strong authentication for network servers. It establishes a network wide user identity that spans many operating systems and devices.

User identification is independent of encryption, non-repudiation, and integrity checking mechanisms. Other DICOM mechanisms exist for those purposes. Their use does not conflict with this mechanism and this mechanism does not interfere with their use.

User identity can be used as part of an audit control mechanism for various privacy and security purposes. It can also be used as part of an access control mechanism to determine access to various features, capabilities, and data. This supplement does not define such audit or access control mechanisms.

The IHE presently uses Kerberos as the recommended network user identification system. Many commercial and academic systems have chosen Kerberos for their network user identification system. The un-authenticated identity assertion is not itself robust or secure, but may be sufficient in some environments. For example, in a physically secured environment the SCP and SCU may have sufficient authentication that the simple exchange of an identity string is sufficient.

The design goals for this approach are:

a. Permit user identity to be specified and used independently of choices for other security mechanisms.
b. Avoid incompatibility with the existing installed base.
c. Require no changes to current DICOM security mechanisms.
d. Minimum of changes to existing implementation libraries.
e. Extensible for future mechanisms, e.g. Security Assertion Markup Language (SAML).
f. User Identity should be established during association negotiation so that the association acceptor can determine whether the identity is acceptable, and decide whether to proceed or fail before any regular DIMSE transactions take place.
g. Permit any combination of security options:
    1. User identity alone, with no other security mechanisms.
    2. User identity plus the current DICOM TLS mechanism
    3. User identity plus future lower level transport mechanisms (e.g. IPv6 with security option).

These goals can be met by using the Association Extended Negotiation feature to provide identity information.

Kerberos was designed so that services like DICOM can implement the use of service tickets and ignore all the remainder of Kerberos. The user login, authorization, and ticket generation process is separated from the service communications.

Kerberos employs a Key Distribution Center (KDC) to perform the actual user authentication and provide service tickets that act to securely identify the user to specific services. It uses a two stage process:

1. First, the user at a local system is authenticated by the KDC. This may be a simple username password system, a secure token, a biometric, or some other system. The KDC then provides a ticket granting ticket (TGT) to the local system. Often the user login process for the local system is integrated with the KDC authentication process.
2. Second, whenever the user wants to use a Kerberized service, the local client sends the TGT and requested service information to the KDC. The KDC returns a service ticket. The local client then sends the service ticket to the remote service to identify the user to that service. The TGT is used to avoid repeating the user authentication system process for every request.

This two step process is a performance optimization to provide a secure single signon environment for many networked computers and services. It is similar to the airline travel process, where there is a complex process to get the reservation and e-ticket, followed by much more rapid simpler procedures to get each of the boarding passes needed for each leg of the trip.

The individual Kerberized services, like DICOM, can avoid implementing the complex user authentication procedures. The Kerberized server only needs to implement service ticket processing. The Kerberized client needs to implement the local access to the TGT and the KDC access to request the service ticket. The operating system usually provides a support library for these functions and often combines the login process with obtaining the TGT.

The proposed DICOM User Identity Negotiation defines support for simple username strings and Kerberos tickets. It should be extensible to support any identity mechanism that is based on uni-directional identity assertions. The digital signature technology and PKI technologies may introduce further uni-directional assertion mechanisms in the future. At present, there are many being defined or proposed for standardization.

This mechanism does not support identity mechanisms that require bi-directional negotiation, such as some of the Liberty Alliance proposals. Those require a series of back and forth messages to exchange and authenticate user identity. This back and forth mechanism does not fit easily into the DICOM

association negotiation process. They may later define a uni-directional assertion mechanism similar to Kerberos, but they have not done so.

Kerberos also includes support for an optional mutual user identification capability (where the service provider replies to the association request with a service provider ticket that the network user can use to confirm the identity of the service).

USE CASES

Audit Trails

One use case is the provision of user identity for purposes of audit trails. Security audit trails usually record the identity of the person performing activities such as query of archives and retrieval of data. When this is done by means of DICOM, the remote system would be informed of the identity of the local user so that the remote system's audit messages can include the identity information. Without this, the remote system can only include the identity of the requesting machine but not the requesting person.

Authorization and access control

The user identity may also be used as part of an authorization system. Different users may have different permissions to access data, modify data, etc. The DICOM identity could be used as input into such an authorization system. When this is being used, the DICOM association request would provide user identity, then the request acceptor would use its authentication and authorization systems to decide whether this association should be accepted, and if it is accepted, what restrictions should be placed on the data provided. The association acceptor then either accepts or rejects the association.

The specific details of authorization and access control mechanisms are separate from the mechanism used to convey identity and are outside the scope of DICOM.

Query Filtering

The response to a DICOM query could be augmented to incorporate knowledge of the requesting user. For example, a DICOM query response could be filtered to only return those patients that should be visible to the identified user. This might be done for security or privacy reasons. It can also be done to improve productivity.

Add to section 2 in Part 7

RFC-1510	The Kerberos Network Authentication Service (V5)
RFC-2289	A One-Time Password System

Add section D.3.3.7 in Part 7

D.3.3.7 User Identity Negotiation

The User Identity Negotiation is used to notify the association acceptor of the user identity of the association requestor. It may also request that the association acceptor respond with the server identity. This negotiation is optional. If this sub-item is not present in the A-ASSOCIATE request the A-ASSOCIATE response shall not contain a user identity response subitem.

The Association-requester conveys in the A-ASSOCIATE request:

- the form of user identity being provided, either a username, username and passcode, or a Kerberos service ticket.
- an indication whether a positive server response is requested.

The Association-acceptor does not provide an A-ASSOCIATE response unless a positive response is requested and user authentication succeeded. If a positive response was requested, the A-ASSOCIATE response shall contain a User Identity sub-item. If a Kerberos ticket is used the response shall include a Kerberos server ticket.

Since a system may ignore request subitems, the positive response must be requested if the association requestor requires confirmation. If the association acceptor does not support user identification it will accept the association without making a positive response. The association requestor can then decide whether to proceed.

The association acceptor may utilize the User Identity information provided during the association negotiation to populate the user information fields in DICOM audit trail messages. The association acceptor may utilize the User Identity information provided during the association negotiation to perform authorization controls during the performance of other DIMSE transactions on the same association. The user identity information may also be used to modify the performance of DIMSE transactions for other purposes, such as workflow optimizations.

Notes:

1. User identity authorization controls may be simple “allow/disallow” rules, or they can be more complex scoping rules. For example, a query could be constrained to apply only to return information about patients that are associated with the identified user. The issues surrounding authorization controls can become very complex. The User Identity SOP conveys user identity to support uses such as authorization controls and audit controls. It does not specify their behavior.
2. The option to include a passcode along with the user identity enables a variety of non-Kerberos secure interfaces. Sending passwords in the clear is insecure, but there are single use password systems such as RFC-2289 and the various smart tokens that do not require protection. The password might also be protected by TLS or other mechanisms.

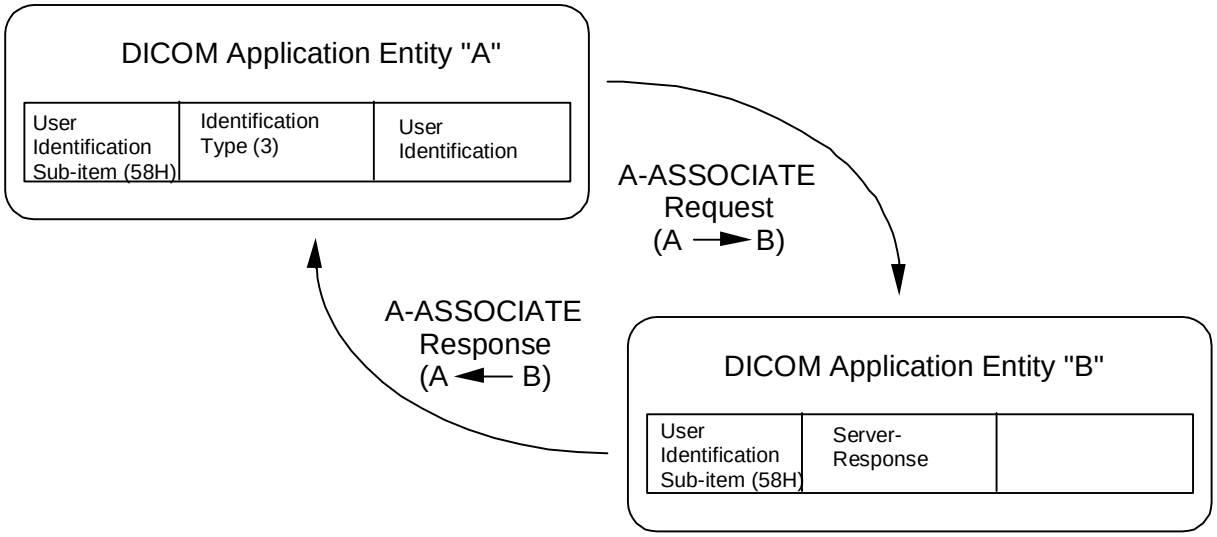

Figure D.3-5
User Identity Negotiation
(With server positive response requested)

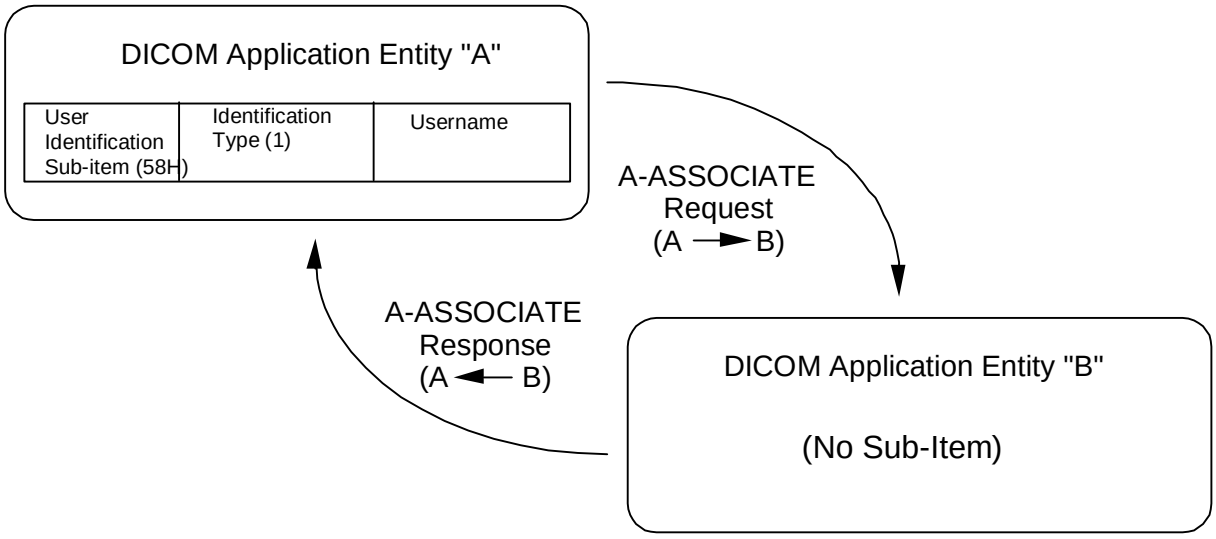

Figure D.3-6
User Identity Negotiation
(Application Entity “A” provides username identity)

D.3.3.7.1 User Identity sub-item structure(A-ASSOCIATE-RQ)

The User Identity Negotiation Sub-Item shall be made of a sequence of mandatory fixed and variable length fields. This Sub-Item is optional and if supported, only one User Identity Negotiation Sub-Item shall be present in the User Data Item of the A-ASSOCIATE-RQ. Table D.3-14 shows the sequence of the mandatory fields.

Table D.3-14
User Identity Negotiation SUB-ITEM FIELDS
(A-ASSOCIATE-RQ)

Item Bytes	Field Name	Description of Field
1	Item-type	58H
2	Reserved	This reserved field shall be sent with a value 00H but not tested to this value when received.
3 - 4	Item-length	This Item-length shall be the number of bytes from the first byte of the following field to the last byte of the last field sent. It shall be encoded as an unsigned binary number.
5	User-Identity-Type	Field value shall be in the range 1 to 3 with the following meanings: 1 – Username as a string in UTF-8 2 – Username as a string in UTF-8 and passcode 3 – Kerberos Service ticket Other values are reserved for future standardization.
6	Positive-response-requested	Field value: 0 - no response requested 1 - positive response requested
7-8	Primary-field-length	The User-Identity-Length shall contain the length of the User-Identity value.
9-n	Primary-field	This field shall convey the user identity, either the username as a series of characters, or the Kerberos Service ticket encoded in accordance with RFC-1510.
n+1-n+2	Secondary-field-length	This field shall be non-zero only if User-Identity-Type has the value 2. It shall contain the length of the secondary-field.
n+3-m	Secondary-field	This field shall be present only if User-Identity-Type has the value 2. It shall contain the Passcode value.

D.3.3.7.2 User Identity sub-item structure(A-ASSOCIATE-AC)

The User Identity Sub-Item shall be made of a sequence of mandatory fixed and variable length fields. This Sub-Item is optional and if supported, only one User Identity Sub-Item shall be present in the User Data Item of the A-ASSOCIATE-AC. Table D.3-15 shows the sequence of the mandatory fields.

Table D.3-15
User Identity Negotiation SUB-ITEM FIELDS
(A-ASSOCIATE-AC)

Item Bytes	Field Name	Description of Field
1	Item-type	58H
2	Reserved	This reserved field shall be sent with a value 00H but not tested to this value when received.
3 - 4	Item-length	This Item-length shall be the number of bytes from the first byte of the following field to the last byte of the final field. It shall be encoded as an unsigned binary number.
5-6	Server-response-length	This field shall contain the number of bytes in the Server-response. May be zero.
7-n	Server-response	This field shall contain the Kerberos Server ticket, encoded in accordance with RFC-1510, if the User-Identity-Type value in the A-ASSOCIATE-RQ was 3. This field shall be zero length if the value of the User-Identity-Type in the A-ASSOCIATE-RQ was 1 or 2.

If the Association-Requestor has requested a positive acknowledgement, the Server-response shall be returned with the Kerberos Server ticket when User-Identity-Type is Kerberos Service ticket (3).

D.3.3.7.3 User Identity rejection

The association acceptor may utilize the username or username and passcode information to determine whether the user is permitted to establish an association. If the Kerberos mechanism is chosen, the association acceptor shall utilize the Kerberos service ticket to determine whether the user is permitted to establish an association.

If the association acceptor rejects the association because of an authorization failure, the rejection shall be indicated to be rejected-permanent (see PS 3.8). The source shall be value (2) “DICOM UL service provided (ACSE related function)”. The rejection is indicated to be rejected-permanent because retries with the same user identity fields will continue to be rejected. A different and valid username, username and passcode, or Kerberos ticket must be provided.

This standard does not define how the association acceptor performs authentication or what rules apply to this authentication.

Add to Annex B in Part 15

B.4 BASIC USER IDENTITY ASSOCIATION PROFILE

An implementation that supports the Basic User Identity Association profile shall accept the User Identity association negotiation sub-item, for User-Identity-Type of 1 or 2. It need not verify the passcode. If a positive response is requested, the implementation shall respond with the association response sub-item.

The user identity from the Primary-field shall be used within the implementation as the user identification. Such uses include recording user identification in audit messages.

Table B.4-1
Minimum Mechanisms for DICOM Association Negotiation Features

Supported Association Negotiation Feature	Minimum Mechanism
User Identity	Username

B.5 USER IDENTITY PLUS PASSCODE ASSOCIATION PROFILE

An implementation that supports the User Identity plus Passcode Association Profile shall send/accept the User Identity association negotiation sub-item, for User-Identity-Type of 2. If a positive response is requested, the association acceptor implementation shall respond with the association response sub-item. The passcode information shall be made available to internal or external authentication systems. The user identity shall be authenticated by means of the passcode and the authentication system. If the authentication fails, the association shall be rejected.

The user identity from the Primary-field shall be used within the implementation as the user identification. Such uses include recording user identification in audit messages.

Table B.5-1
Minimum Mechanisms for DICOM Association Negotiation Features

Supported Association Negotiation Feature	Minimum Mechanism
User Identity	Username and Passcode

B.6 KERBEROS IDENTITY NEGOTIATION ASSOCIATION PROFILE

An implementation that supports the Kerberos Identity Negotiation Association Profile shall send/accept the User Identity association negotiation sub-item, for User-Identity-Type of 3. If a positive response is requested, the association acceptor implementation shall respond with the association response sub-item containing a Kerberos server ticket. The Kerberos server ticket information shall be made available to internal or external Kerberos authentication systems. The user identity shall be authenticated by means of the Kerberos authentication system. If the authentication fails, the association shall be rejected.

The user identity from the Primary-field shall be used within the implementation as the user identification. Such uses include recording user identification in audit messages.

Table B.6-1
Minimum Mechanisms for DICOM Association Negotiation Features

Supported Association Negotiation Feature	Minimum Mechanism
User Identity	Kerberos