HIMSS and RSNA

Integrating the Healthcare Enterprise

IHE/MESA Kerberos Authentication Server Tests

Electronic Radiology Laboratory
Mallinckrodt Institute of Radiology
510 South Kingshighway Blvd.
St. Louis, MO 63110
314.362.6965 (Voice)
314.362.6971 (Fax)

Revision 9.0.0
20-September-2005

1 Introduction

The MESA tests include a number of cases each of which rely on a sequence of messages between actors. These tests range across different integration profiles:

- Retrieve Information for Display
- Enterprise User Authentication
- Patient Identity Cross Reference for MPI
- Patient Synchronized Application
- Consistent Time

This document lists the transactions and messages for a number of cases. It may not describe the clinical scenario behind each case, but listing the transactions should clearly define what is expected of each actor. These are all of the transactions involving all of the actors. When you test with your particular actor, you may see only a subset of these messages.

1.1 Patient Identification

1.2 Submission of Results

Test descriptions below inform the reader to “submit results to the Project Manager”. This is does not mean “email”. The current submission process should be documented by the Project Manager, but will not include emailing files directly to the Project Manager.

2 Test Cases: EUA

This section describes test cases that are generally associated with the EUA Integration Profile. There may be some overlap with other profiles.

Each test case involves a series of transactions involving one test patient. Some patients may require that a single actor participate in multiple transactions. The tables in this section give the order of messages for an integrated system with all actors. This is provided as a centralized reference. To test an individual IHE actor, refer to the appropriate test document.

2.1 Test Case 10301: EUA Kerberos Authentication

Test case 10301 covers the EUA Kerberos Authentication. A user “logs-in” to a client computer using Kerberos authentication with a Kerberos Authentication Server.

2.1.1 References

ITI TF-2: 3.2

2.1.2 Instructions

This test does not involve any MESA software. The intent of this test is for your system to properly authenticate users on another system.

1. Configure your Kerberos Authentication Server. We have a separate document (*Kerberos Notes*) with notes about how to do this.
2. Create an account entry on the authentication server with the name “khimss”. Set the password to something of your choosing.
3. Obtain a Unix (Unix or Linux) system to act as the client computer. We use Red Hat Linux 9.0 for this task with appropriate notes in Kerberos Notes. Configure the Unix system to use Kerberos authentication with your Kerberos Authentication Server.
4. Logout from the client Unix system. Unplug the network adapter of that system so it cannot reach the Kerberos Authentication Server. Try to login to the Unix computer using the khimss account and password. If this is successful, it indicates you are not authenticating with the Kerberos Authentication Server; check your configuration and try again.
5. Reconnect the Unix system to your local network. Login to this computer using the khimss account and password you selected.
6. From a terminal emulator, run the command klist. This should print ticket information for your account. Redirect the output to the text file *grade_10301.txt*:

   ```
   klist > grade_10301.txt
   ```

   Email the grade file to the Project Manager.

2.1.3 Evaluation

The goal of this test is to make sure you know how to configure your computer system to use Kerberos authentication and that you have tested that in your lab. No further testing of Kerberized communication is required.