SETECS® Medical Technologies

SETECS® MIX™ System

Secure Medical Information Exchange (MIX™) System

~~~ Version 1.2 ~~~

1. Introduction: Current Situation with Medical IT Systems

Most medical institutions today use various hardware and software products for collecting, organizing, storing, processing and dissemination of data created by their regular activities. Such products are collectively known as Electronic Medical Records (EMR) systems. Characteristics of most of EMR systems today are:

- Functionally *incomplete*, i.e. they do not provide the full scope of functions and services needed for all activities in various medical institutions;
- Designed and implemented as *proprietary*, stand-alone systems, thus mutually not compatible and not interoperable with other similar systems;
- Do not encompass a secure and protection level required for sensitive medical data and documents.

The consequence of functional limitations is that medical institutions usually use multiple EMRs and other IT products or additional, small, add–on software modules, which complicates integration of data and functions even within a single institution. Very often creation and deployment of large–scale integrated medical information systems takes multiple vendors, millions of dollars, and several years.

The consequence of proprietary concepts is that with current EMR systems exchange or sharing of data is practically impossible, unless EMR products from the same vendor is used at all locations. And, the consequence of poor security is that sensitive medical data are exposed to various threats, unauthorized use and breach of patients' privacy. Very often, EMR vendors claim strong security, when they provide only simple passwords and SSL communication protocol.

The current situation needs an integrated, standards-based, and secure system for collection, storage, processing, distribution, and protection of medical data within individual institutions, within groups of these institutions, at regional, national and international levels.
~~~

2. Requirements and Needs

Current requirements and needs in the area of IT healthcare systems can be globally structured in three categories: integration, compliance to regulations, and security. Additional desirable properties are flexibility, elimination of administrative and professional errors, improvement of medical services, and reduction of operational costs.

Some of the most important functional and security requirements for healthcare information exchange systems are:

- Registration of patients based on HL7 and HIPAA standards with comprehensive set of demographic attributes
- Distribution and availability of patients' registration data in an integrated and distributed information exchange system
- Accurate identification of patients using biometric technologies
- Collection, storage and distribution of patients' medical data and control of their usage by patients
- Accurate tracking of patients in each institution and throughout multiple medical institutions
- Registration of all medical professionals based on HL7 and HIPAA standards with comprehensive set of demographic attributes
- Accurate registration of professionals and their relationships with locations / institutions of their professional activities
- Secure access to medical and other patients' data by professionals based on their roles and authorizations
- Registration of all institutions directly or indirectly related to healthcare activities: hospitals, primary care units, specialized medical institutions, insurance and pharmaceutical companies, pharmacies, etc.
- Secure exchange and sharing of medical data and information electronically between medical institutions
- Securely exchange of medical documents between medical institutions
- Secure and scalable role-based distributed security system to control access to patient's records

SETECS® Secure Medical Information Exchange (MIX™) System solves all the problems with integration and security of the current EMR systems. It is based on a flexible architecture that supports the integration, development and operation of a full spectrum of healthcare applications; it is structured as a large–scale integration and security infrastructure; and it may be easily installed, customized, and activated in individual medical institutions. In addition to local operations, each instance of the SETECS® MIX™ System may be connected into SETECS® MIX™ Infrastructure for easier sharing and exchange of demographic and medical data for all patients.

3. Global MIX™ and PKI Infrastructure

To meet all the stated requirements and needs for secure and integrated medical exchange systems, SETECS® has designed and implemented MIX™ system in the form of a large–scale architecture, called *MIX™ Infrastructure*. The architecture provides scaling

and federation of individual instances of the MIX™ system deployed in individual medical institutions.

MIX™ Infrastructure comprises three layers. The first is an instance of the system in each hospital. The second level is the system deployed in the Regional Center or for a group of hospitals. Its function is to interlink and federate individual systems in hospitals through the hierarchical approach. The third level is an unique, single MIX™ Global Server which links Regional/Group server and also serves as the central point for distribution of coding and other tables, common to the entire MIX™ system.

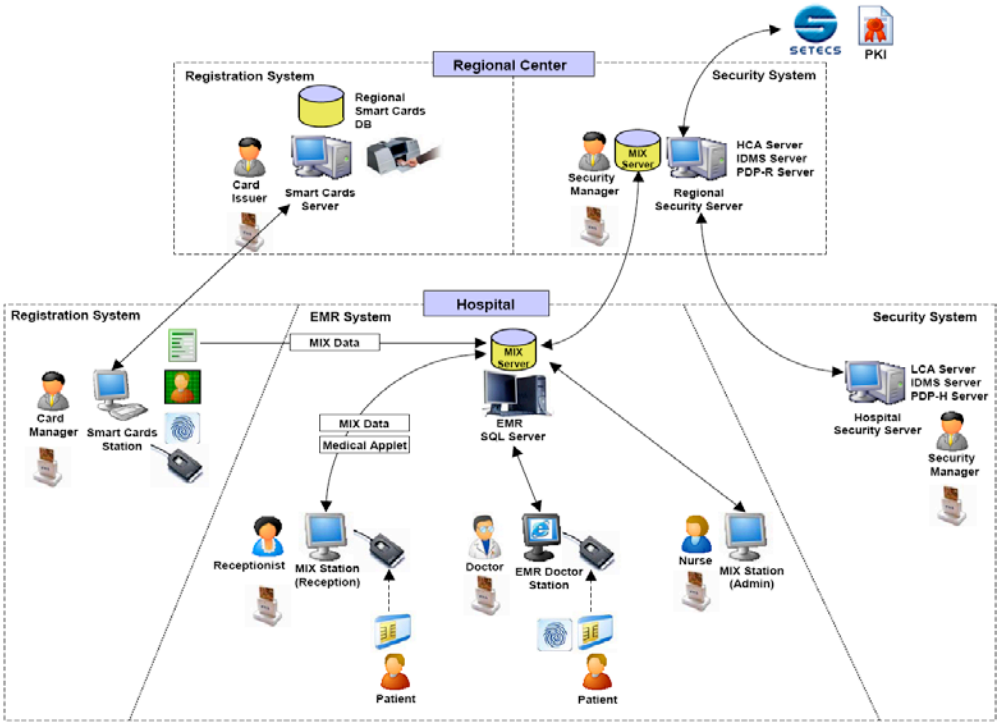

Figure 1. MIX™ Architecture and Components

Parallel to the MIX™ Infrastructure, SETECS® also runs public–key infrastructure (PKI) with the Top (Root) PKI Certificate Authority (CA) Server at the top of the PKI hierarchy. Under that CA Server is Policy CA Server that regulates SETECS® Certification Policy and distributes it to other, lower level CA Servers. The third PKI level is Geo–political CA Servers, associated with Regional or Group MIX™ servers. Finally, at the bottom are Issuing CA Servers, located in hospitals and other medical institutions. Those CAs are issuing certificates to all MIX™ Servers and Stations, and to smart cards of all medical professionals (SETECS Security Smart Cards) and patients (SETECS Medical Smart Cards).

4. Components and Structure of the MIX™ System

MIX™ Infrastructure comprises three layers with components at each layer: at the top is MIX™ Global System, below it is MIX™ Regional (or Group) System, and at the bottom of the hierarchy is MIX™ System in medical institutions.

4.1 MIX™ System in Hospitals and Medical Institutions

The structure, components and inter-relationships of the MIX™ system in each hospital are shown in Figure 2.

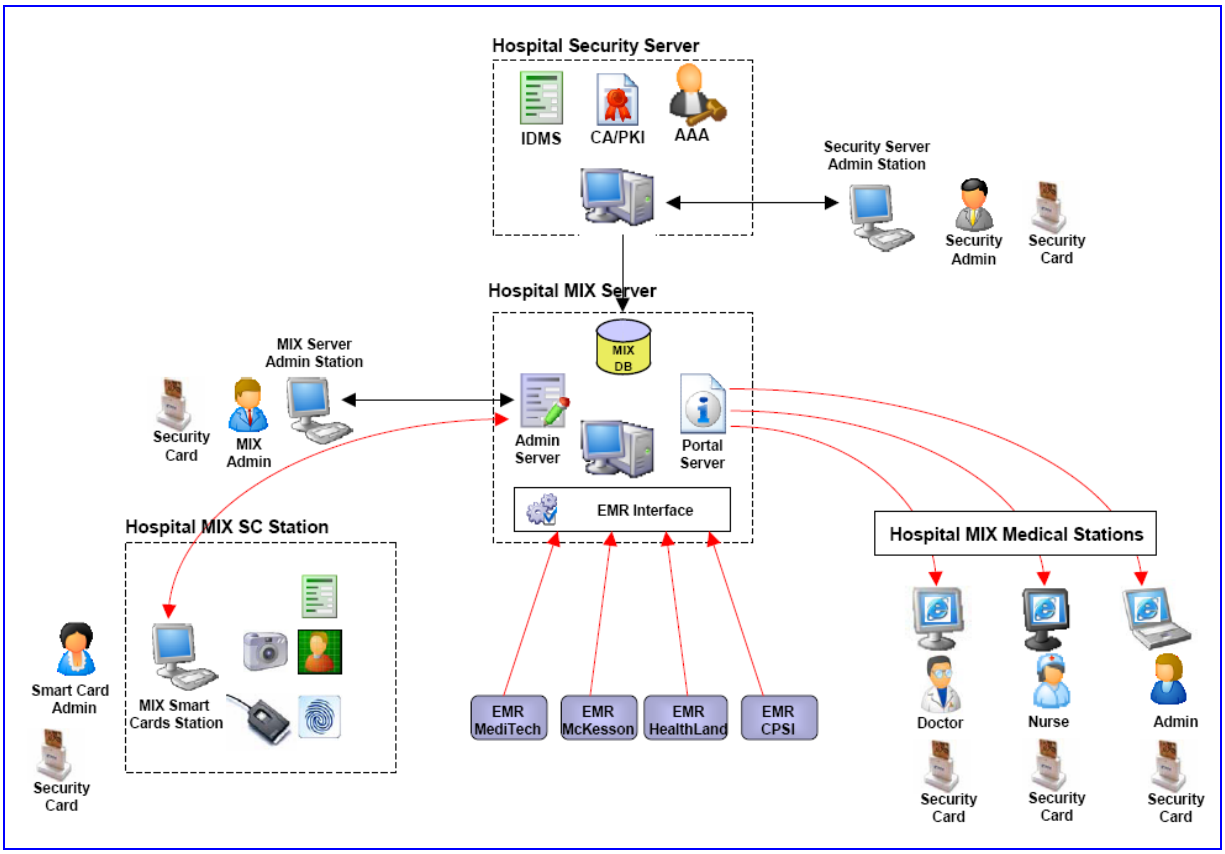

Figure 2. Components of the MIX™ System in A Hospital

In each hospital, an instance of the MIX™ system comprises three subsystems:

- *Registration System:* used to register institution and its organizational components, all patients, and all professional employed in the institution.
- *Extended EMR System*: used to manage patients' medical records both internally and externally. Internally by using the local EMR system to reference patients. Externally, by synchronizing databases with other EMR systems in other hospitals and the Regional Center.
- *Hospital Security System*: manages security credentials for employees. This includes certificates, authentication and authorization tokens and also security policies.
-

- ***Registration System*** in each hospital uses the following:
  - *Smart Cards Station*: shown in Figure 2, is used to enroll employees and patients and capture fingerprint biometric data and photo.

- *Local IDMS Server:* shown in Figure 2 integrated within the Hospital Security Server, is used to store registration data for employees in order to enforce their access and authorization privileges.
- *Local IDMS Station:* not shown in figure due to being integrated either the Hospital Security Server or used remotely from separate PC. This station is used to manage personal registration data in the IDMS server and their security credentials for local employees.

• ***Extended EMR System*** in each hospital contains the following:
- *Medical Information Exchange (MIX) Server:* displayed in Figure 2 adjacent to the standards EMR server, used for patient authentication based on fingerprint biometric and/or smartcard authentication. System has also been designed to cross-reference new Registration and Security systems and existing EMR system. This server also serves as Policy Enforcement Point (PEP) for all local Web Portals in each hospital.
- *EMR Registration Station*: this station is equipped to run new Web-based application, which uses patients' fingerprint biometric data for patient authentication.
- *EMR Physician Station*: has been developed to run another Web-based application which uses physician/nurses or other staff fingerprint biometric data to authorize access to patients' EMRs.
- *EMR Transfer Station*: runs a third Web-based application, which manages transfer of patients'' medical data and documents between hospitals within the secured federated architecture.

• ***Hospital Security System*** comprises of the following within each hospital:
- *Local Certificate Authority (CA) Server*: indicated in Figure 1 as the LCA server, it is used to generate and distribute X.509 certificates to all other components of the system.
- *Policy Decision Point (PDP) Server*: shown in Figure 2 as PDP-H Server, is used to create local hospital authorization policy and to make authorization decisions.

4.2 MIX™ System in Regional Centers and in Group of Hospitals

In the Regional Center, an instance of the MIX™ System comprises two subsystems:
- *Registration System:* used to issue smart cards to all employees and patients of hospitals associated within federated architecture.
- *Regional Security System*: is used to complement Security System servers in each hospital.

• ***Registration System*** within the Regional Center incorporates the following:
- Smart Cards Production Server: used to issue smart cards to all employees in hospitals and also to all patients.
- Smart Card Central Server: is utilized to hold data for all smart cards within issues within the region.

• ***Security System*** within the Regional Center comprises of the following:
- *Regional CA Server*: indicated in Figure 2 as the HCA Server, it is used to certify Local CA Servers in each hospital.
- *Regional IDMS Server*: shown in Figure 2 as IDMS Server, is used for registration of individuals and defined components in the Regional Center.
- *Regional PDP Server:* shown in Figure 2 as PDP-R Server, maintains common elements and policies for all hospitals.

- *Regional MIX™ Server*: shown in Figure 2 as MIX™ Server, is used as bridge for synchronization, inter-hospitals data and documents transfers, and for conversions of EMR data and formats.

4.3 Cooperation between Components in Hospitals and the Regional Center

The main purpose of the MIX™ System in the Regional Center (or in a group of hospitals) is to represent a "bridge" between MIX™ servers in individual hospitals. As such, it provides the following functions to MIX™ servers in hospitals:

- Distribution of standard HL7 coding tables after their updates at the Global MIX™ Server or at some of the hospital MIX™ servers;
- Distribution of registration information about hospital MIX™ servers that joined the infrastructure.
- Receiving and dispatching medical data and documents during their transfer between two hospital MIX™ servers;
- Cross–referencing of personal identifiers between individual EMR identifiers and unique, global MIX™ patients' and personnel's' identifiers.

Relationship between Regional MIX™ Server and MIX™ servers in individual hospitals is shown in Figure 3.

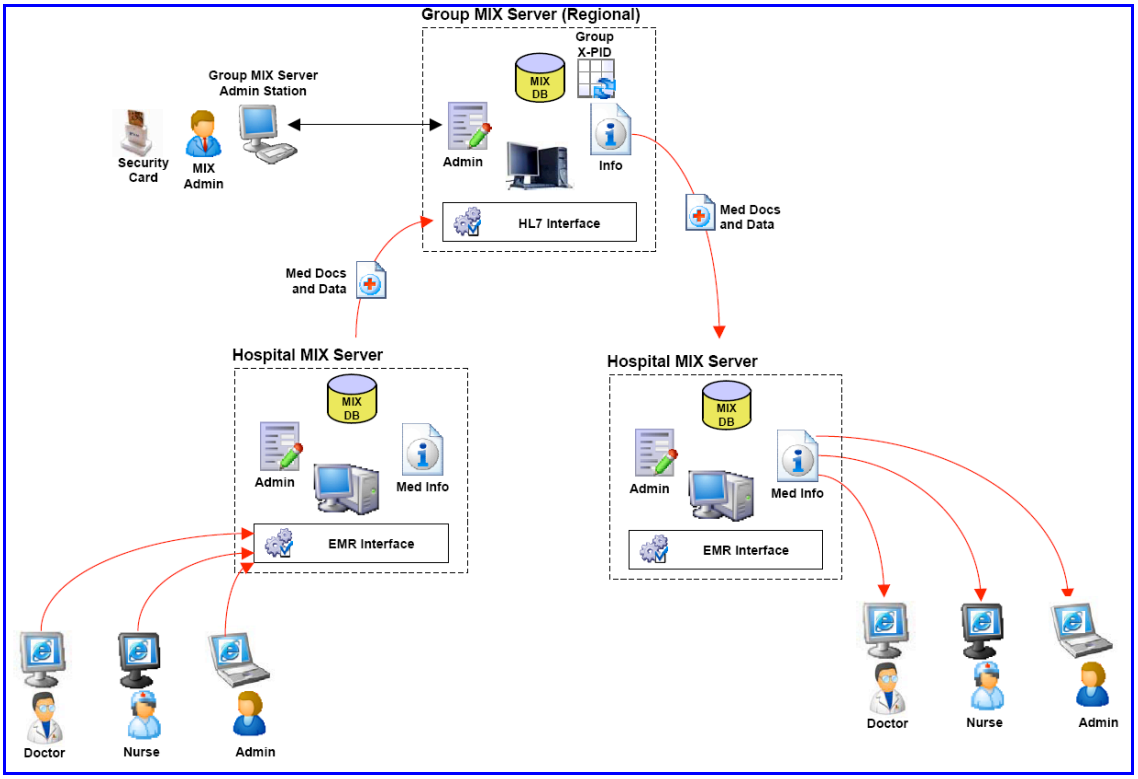

Figure 3. Relationship between Regional and Hospital MIX™ Servers

Smart Card Stations in hospitals are linked to the Smart Card Central Server located either in the Regional Center or in the hospital. The individual stations submit registration data for patients and professionals to issue their smart cards. The MIX™ Server in each

hospital is linked to the MIX™ Server in the Regional Center. Hospitals exchange referenced to medical data and medical documents using the MIX™ Server in the Regional Center. Policy Decision Point (PDP) Servers in each hospital access the Regional PDP server to fetch regional security policy, which is extended with additional policies in each hospital to create policy sets specific to each individual institution and globally compliant to the regional authorization policy. Two certificates of the Local CA servers in hospitals are certified by the Regional Certification Authority server in the Regional Center. Two certificates of that CA Server are in turn certified by SETECS®' US National Policy CA Server, thus linking Regional Public–Key Infrastructure (PKI) into global SETECS® international PKI.

5. Features and Compliance to Standards

MIX™ System has been designed to manage identities and security credentials of institutions where they are deployed and of two types of individuals: patients and professionals who are currently employed by the institution. The system is maintained by security administrators in each hospital and in the Regional Center.

In order to implement security services within a federated environment, the system is established in the form of multiple autonomous domains. MIX™ architecture utilizes standards to ensure compliancy and scalability options.

- ***HIPAA***: All identifiers for institutional and individual medical providers are official NPI (National Provider Index) identifiers issued by the CMI/HHS;
- ***HIPAA***: All coding tables are compliant to ISO, HL7, and other standards;
- ***HL7***: All messages exchanged between MIX™ servers are compliant to the HL7 standard;
- ***CCR/CCD***: All records and documents exchanged between MIX™ servers are compliant to the CCR and CCD standards;
- ***FIPS 201***: IDMS is compliant to the Federal Information Processing Standard 201 (FIPS 201), a Personal Identification Verification (PIV) standard
- ***X.509***: PKI components, protocols, services, and all certificates are compliant to the IETF X.509 standards;
- ***SAML/XACML***: Web Security Services (WSS), components and protocols are compliant to all SAML/XACML standards: World Wide Web Consortium (W3C), Organization for the Advanced of Structured Information Standards (OASIS), Internet Engineering Task Force (IETF), and Liberty Alliance standards, secure Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), Security Assertion Markup Language (SAML)
- ***IETF***: Secure transactions services for wired and wireless devices based on Secure Sockets Layer (SSL), Secure Multipurpose Internet Mail Extensions (S/MIME), and SAML standards
- ***FIPS 201***: Patient Registration Server capable of registering each patient into a unique Master Patient Index (MPI) number is using FIPS 201 (PIV) standard for patients' identifiers used to accurately cross–reference patients throughout the federated architecture.
- ***ISO 7816/Global Platform***: Smart Cards Management Services (CMS) and internal structure of smart cards are compliant to the smart card standards established by Global Platform, NIST FIPS 201 standard, and GSA/Federal

Government requirements for card management architectures suitable for large–scale card deployment services.

6. Operations and Use of the MIX™ System

This chapter and its subsections describe the procedures for each of the three current groups of users enrolled in the system: patients, professionals, and security administrators.

6.1 Procedures for Patients

1. *Registration of Patients:* A patient visits a hospital and approaches the reception desk. If the patient has not registered within any of the federated sites, he/she will be directed to the Smart Card Station. The station operator will register the patient, capture his/her photo and also two fingerprints, using a fingerprint biometric reader. All data will be deposited in the Smart Card Central Server in the Regional Center or in the Hospital, where smart card will be issued for the patient.

2. *Activation of the Medical Smart Cards*: When a patient, who has recently received his/her medical smart card, visits one of the hospitals within the federation he/she will be again directed to the Smart Card Station. There, the patient's photo printed on the card will be matched with the photo located on the hospital Web Portal, and his/her fingerprints inside the smart card chip will be verified. If verification is successful, the patient will set up his/her own smart card PIN. At the same time MIX™ Cross-Reference Data and MIX™ Medical Data will be loaded into the card. At this stage the card is ready to be used for patient's authentication in all hospitals within the designated federation.

3. *Subsequent Hospital Registration:* With the medical smart card activated, a patient approaches the reception desk in the hospital. There he/she will insert the card into a smart card reader available at the MIX™ station. After presenting his/her PIN and/or fingerprint, the patient's registration information will be retrieved by the receptionist.

4. *At the Physician's office*: If privacy and protection of patient's medical data is needed, this information will be retrieved only after a patient inserts and activates his/her medical smart card. Physicians, nurses and other medical personnel will have MIX™ security card, which will be used to authorize their access to the medical Web Portal and patient's medical data. These individuals will be able to access medical data stored at the local EMR server directly, using local EMR application and data stored at other hospitals using the MIX™ Cross-Reference data accumulated at the hospital's MIX™ Server.

5. *Patient Transfer to Another Federated Hospital*: When a patient is transferred to another hospital, medical administrators will use a Web Portal to create MIX™ Cross-Reference Data at the hospital's MIX™ server and transfer that data to the Regional MIX™ server. MIX™ Cross-Reference Data will be accumulated at the hospital's MIX™ Server, so that the complete medical history of a patient is available at each of the federated site's MIX™ Server.

6. *Patient Transfer from Another Federated Hospital*: When a patient visits a new hospital, the authorized hospital personnel will use a Web Portal at the MIX™ Station to retrieve all of the patient's Cross-Reference Data, add recent data from

the local MIX™ Cross-Reference Data, and include other data at the MIX™ Server. This data will be stored into the patient's medical smart card. As a result, the hospital MIX™ Server will contain cross-references to all patients' medical data in all other hospitals, while the patient's medical smart card will now contain MIX™ Cross-Reference Data from the hospital.

6.2 Procedures for Professionals

1. *Registration of Professionals:* All professionals employed within each of the federated hospitals that require access to patient's demographic and medical data, primarily physicians and nurses, will also be registered within the MIX™ System. The Smart Card Station within a hospital is also used for the registration of these individuals. In addition to data sent to the Regional Smart Card Central Server for issuance of security smart cards, the data for professionals will also be stored within the MIX™ Server at each hospital. This segment of data will be used for authorization policy of the hospital's security system.

2. *Activation of the Security Smart Cards*: When the security smart cards are received back from the Regional Center, they will be activated, equivalent as with the patient's medical smart cards. However, instead of MIX™ data being loaded onto the card, security data will be placed into the chip card and used for authentication and authorization of professionals.

3. *Access to Web Medical Applications*: To obtain access to the medical Web Portal, all professionals will insert the card in the smart card reader. After activating the card by providing PIN and/or fingerprint, security data will be retrieved from the card and used by the security system for single sign-on (SSO) user authentication and role-based authorization. Both of these security services will be enforced by the local security policies that have been put in place by the security administrators of each system.

6.3 Procedures for Security Administrators in the Regional Center

1. *Issuance of Smart Cards:* Based on registration data submitted by hospitals' Smart Card Stations, security administrator in the Regional Center will issue MIX™ Medical Smart Cards for patients and Security Smart Cards for professional staff. The respective cards will be mailed to both patients and professionals, as their mailing address must be completed prior to submitting card requests.

2. *Creation of Regional Security Policy*: The security administrator in the Regional Center will create regional security policy, which will be applicable to all federated hospitals across the region. The policy will contain common attributes, such as dictionary of roles and shared policy rules. The policy will be distributed to all hospitals' Security Servers. This common policy agreement, coordinated with the Regional Center, is appended to individual policies established by each hospital. This process ensures that common policy is enforced throughout the federation. However, each hospital is permitted the flexibility to implement additional policies that may be only specific to their institution.

6.4 Procedures for Security Administrators in Hospitals

1. *Import Regional Security Policy:* Security administrator in each hospital will import regional security policy from Regional Center. This policy can then be included within the hospital's local security policy.

2. *Registration of Local Groups and Applications*: In order to create local policies in each hospital, security administrators will specify local groups, register users into those groups, register local applications, and local authorization rules.

3. *Creation of Local Security Policy*: Security administrator will create local security policies in their respective hospitals by combining local policies and regional policy into their policy sets. Those policy sets will be used to support and enforce authentication and authorization of professionals when accessing medical applications and using medical data.

7. Conclusions

The concept, components and operations of the MIX™ system described in this paper will be evaluated, improved and tested in practice in close cooperation with medical and other institutions deploying the system. The system will be deployed with functions and features as described, but it will be continuously evaluated, upgraded, improved and extended to better meet security and interoperability needs and requirements of patients, medical professionals and medical authorities in all institutions using the system.