Departments' of the Army, Navy, & Air Force
Exceptional Family Member Program
Goals and Objectives

(EFMP - Forms Based Automation (EFMP)

- **Improve** EFMP infrastructure, services and program execution by developing and implementing Army-wide process improvements
- **Automate** EFMP manual business processes to enhance the quality of its services to Soldiers and their exceptional Family members
- **Create** an EFMP portal that will allow, EFMP personnel, Soldiers and authorized Family members the autonomy to track and manage documentation required for EFMP related services

- **Build** a web-accessible application that will control and support the following:

    - Documents Management
    - Electronic workflow process
    - Application eligibility assessment
    - Evaluating and applications/forms

- Complete Development in T*welve Months*.

- **Keeping** in prospective both the *Objective* and *Key Features* required by the Military Services

Section 1
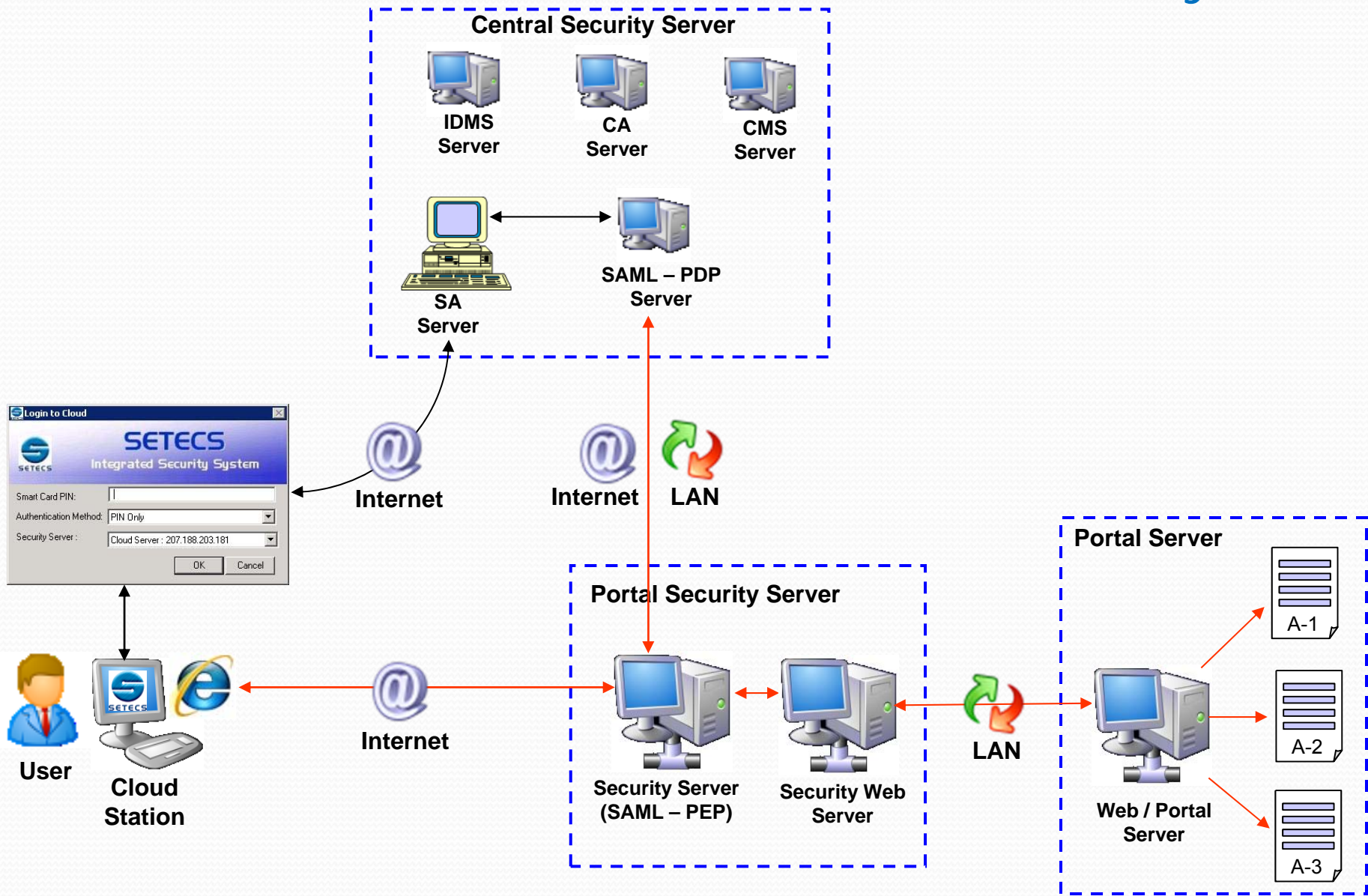
SETECS Portal Security : Products and Technologies

SETECS® Security Products

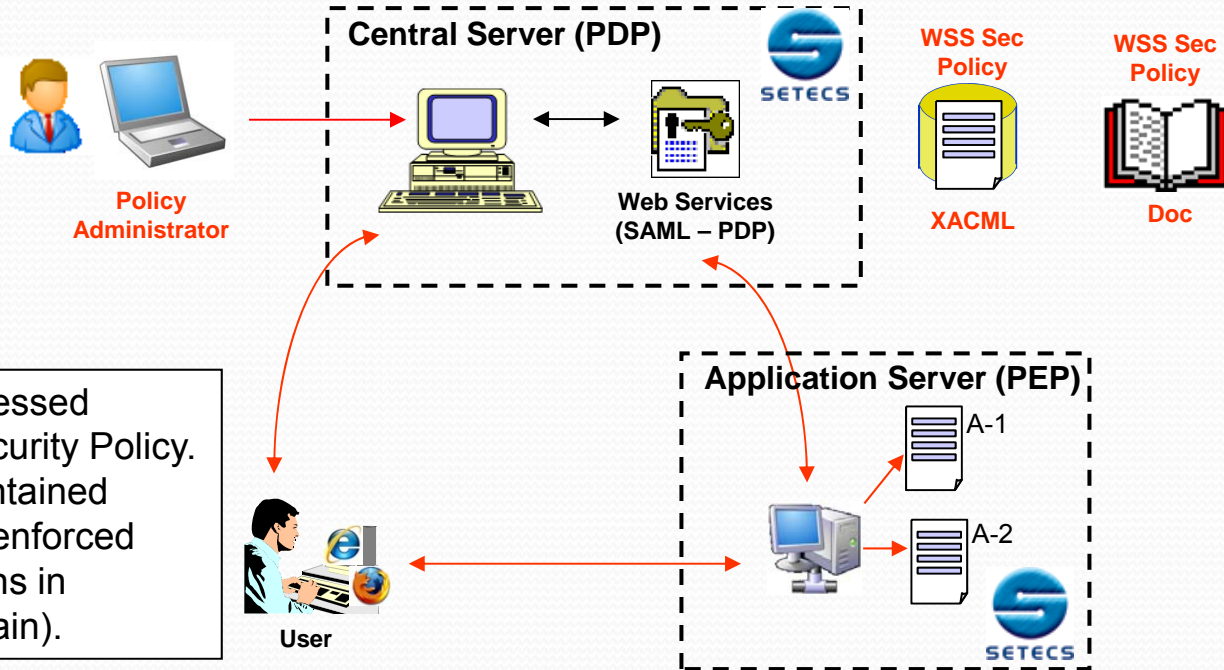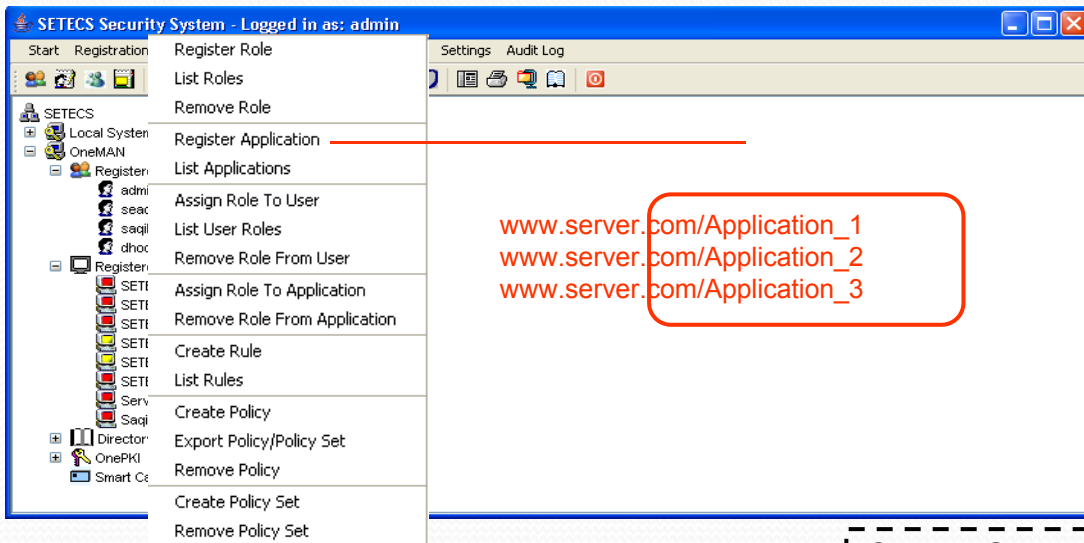## Integrated Security System for Portals and Network Environments

- **OneNET™ – Security System for Web Services**

- **OnePKI™ – Scalable Public Key Infrastructure**

- **OneMAN™ – ID Management System**

- **OneCARD™ – Smart Cards Management System**

- **OneSDK™ – Security Framework for Fixed and Dynamic/Mobile Network Environments**

- **OnePhone™ – Secure Mobile Applications**

SETECS® OneNET™ Portal Security

Central Security Server

IDMS Server

CA Server

CMS Server

SA Server

SAML – PDP Server

Internet

Internet

LAN

Login to Cloud

SETECS
Integrated Security System

Smart Card PIN:
Authentication Method: PIN Only
Security Server: Cloud Server : 207.188.203.181

OK   Cancel

User

Cloud Station

Internet

Portal Security Server

Security Server (SAML – PEP)

Security Web Server

LAN

Portal Server

Web / Portal Server

A-1

A-2

A-3

SETECS® OneNET™ RBAC and Authorization

www.server.com/Application_1
www.server.com/Application_2
www.server.com/Application_3

Central Server (PDP)

SETECS

Policy Administrator

Web Services (SAML – PDP)

WSS Sec Policy

XACML

WSS Sec Policy

Doc

Application Server (PEP)

A-1

A-2

SETECS

User

Applications at the Server are accessed selectively, based on the WSS Security Policy. The Policy is established and maintained by the Security Administrator and enforced for all Servers and their Applications in a local environment (security domain).

SETECS® OnePKI™ Certificate Management

Each component in the system has a certificate.

Users have three certificates: Authentication, Digital Signature and Key Exchange. **Servers** have two certificates: Authentication and Key Exchange. Certificates are issued to users and servers by a local Certification Authority (Issuing CA). Certificate Protocols are based on PKCS#7 and PKCS#10 standards.

Certificates are used for all security services: user local and remote authentication, signing and enveloping of messages, and non–repudiation.

Issuing CA Server

PKI Admin

PKI Policy — Specs

PKI Policy — Doc

Central Server (PDP)

Policy Administrator

Web Services (SAML – PDP)

WSS Sec Policy — XACML

WSS Sec Policy — Doc

Application Server (PEP)
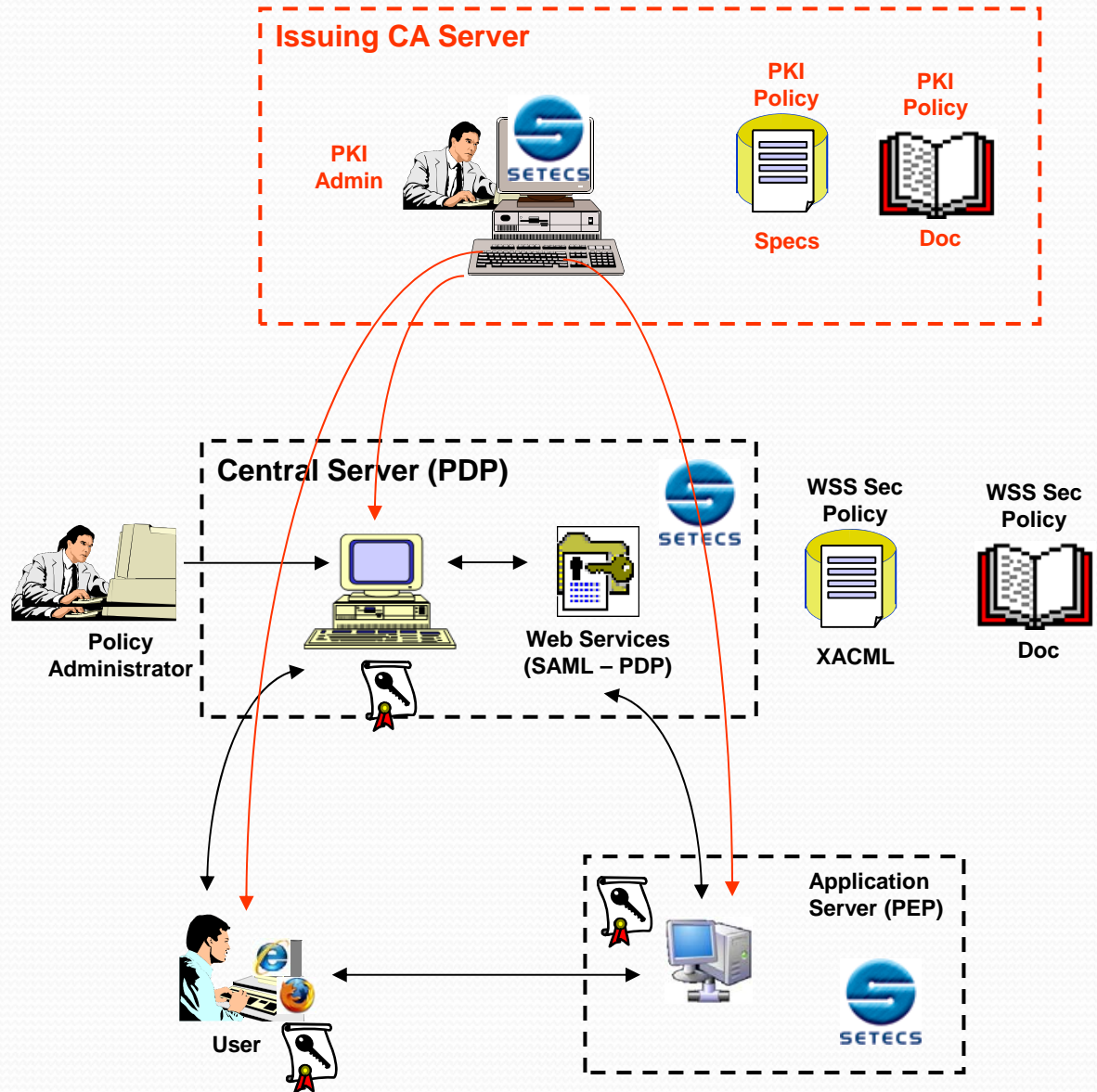
User

SETECS® OneCARD™ PIV Management System

Card Management System

- SETECS
- CMS Central Server
- PIV Policy / Roles
- PIV Policy / Doc
- CMS Enrollment Server
- CMS Card Production Server
- SETECS PIV Card
- CMS Enrollment Station
- Issuing CA Server
- Central Server (PDP)
- User
- Application Server
- SSL
- SSL
- SSL
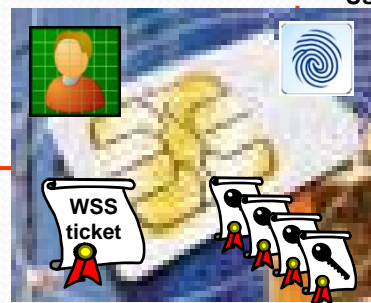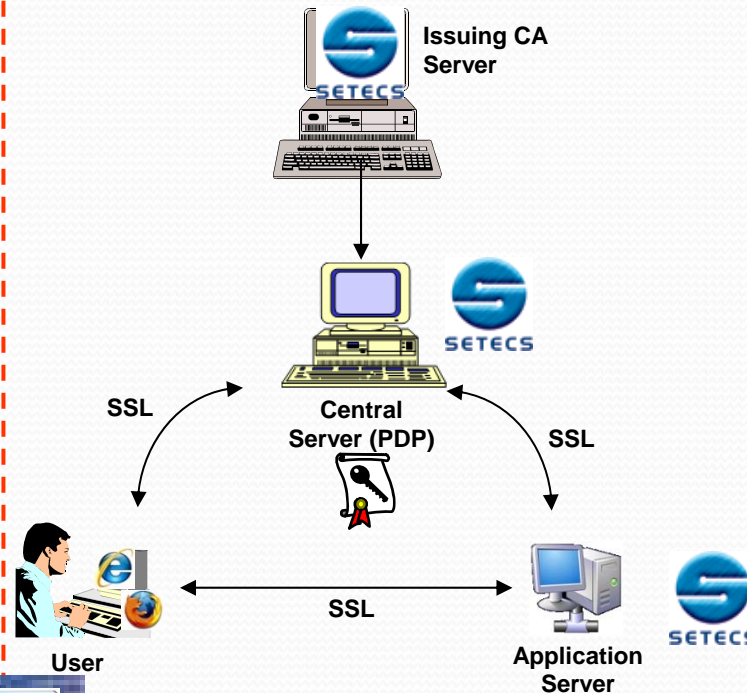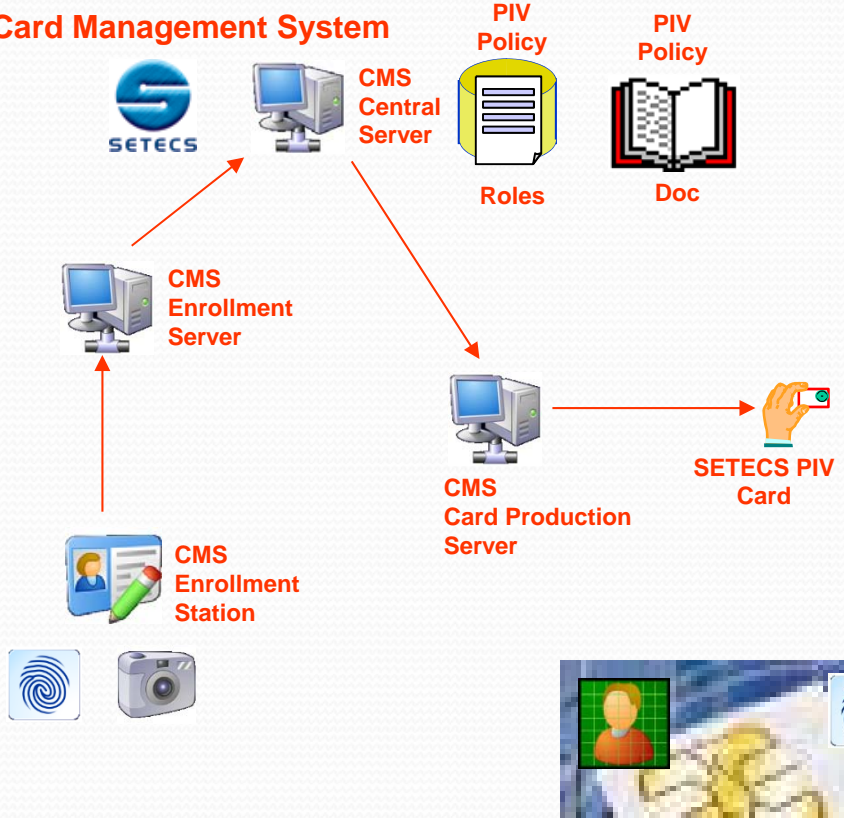
SETECS OneCARD™ PIV Card

WSS ticket

Certificates are complemented by smart cards for users and network security administrators. Smart cards are compliant to the FIPS 201 -2 (PIV) standard. SETECS provides Card Management System to issue and manage smart cards and several smart card security applications: local login, signing of messages, etc.

Section 2

SETECS Medical Security: Products and Technologies

SETECS® MIX™ System

Security System and Infrastructure
for Medical Information Exchange and Protection

- ➢ **Hospital MIX™ Server – Integration of data and procedures**

- ➢ **Hospital MIX™ Cards System – Station and Server to issue and manage MIX™ smart cards**

- ➢ **Hospital MIX™ Portal – Web Portal for sharing and distribution of medical data, documents and information**

- ➢ **Regional MIX™ Server – Regional connection between Hospital MIX™ Servers for data exchange**

- ➢ **Global MIX™ Server – National, top level server for synchronization of Regional MIX™ Servers**

SETECS® MIX™ System
Hospital MIX™ Server

Hospital MIX Server

MIX Server Admin Station

Security Card

MIX Admin

MIX DB

Admin Server

Portal Server

EMR Interface

Hospital MIX SC Station

Smart Card Admin

Security Card

MIX Smart Cards Station

EMR MediTech

EMR McKesson

EMR HealthLand

EMR CPSI

Lab IT System

Radiology IT System

Other IT System

Hospital MIX Medical Stations

Doctor

Security Card

Nurse

Security Card

Admin

Security Card

SETECS® MIX™ System
Hospital Security Server
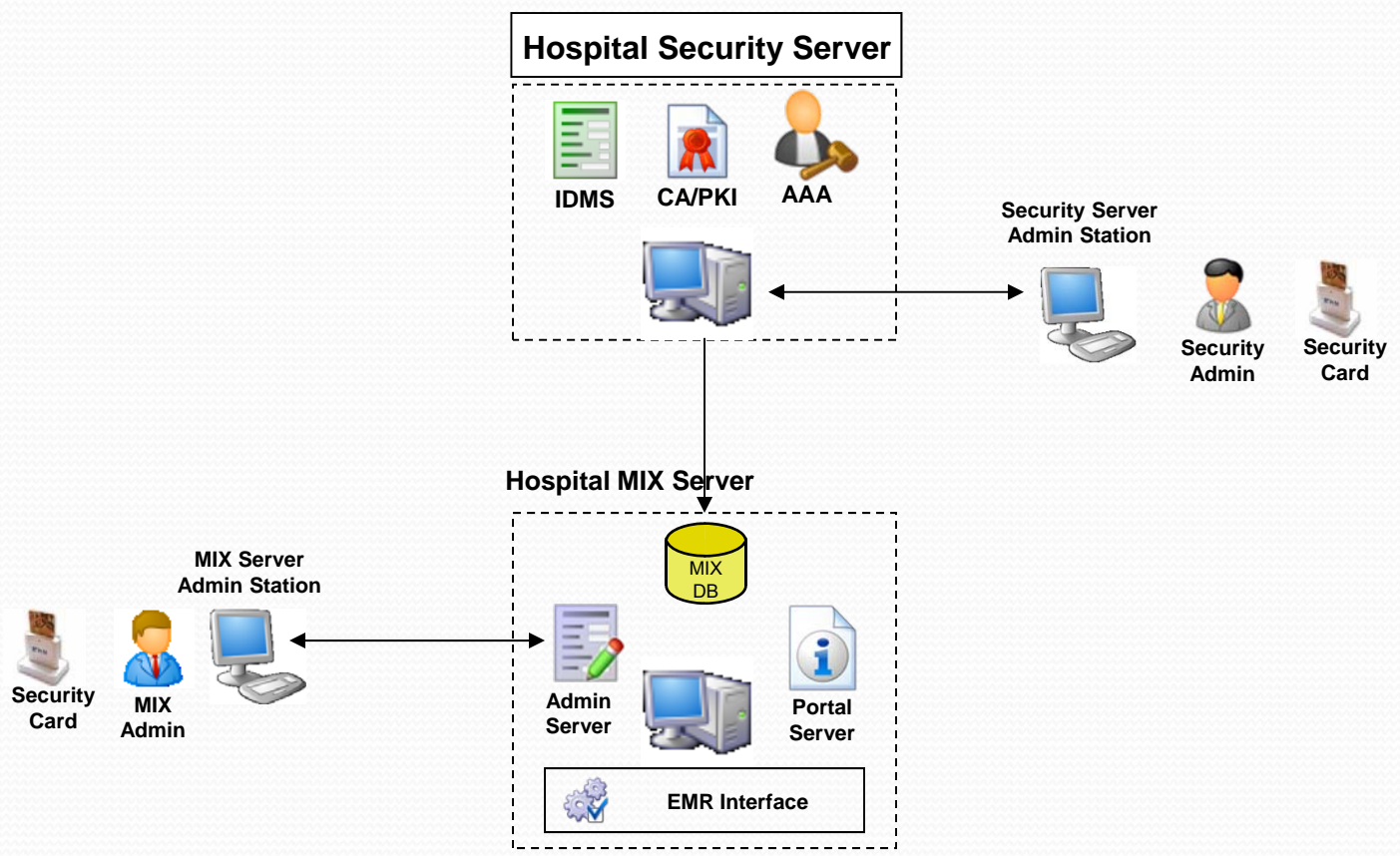
SETECS® MIX™ System
Regional MIX™ Server

Group MIX Server (Regional)

Group X-PID

MIX DB

Group MIX Admin Station

Security Card

MIX Admin

Admin

Info

HL7 Interface

Med Docs and Data

Med Docs and Data

Hospital MIX Server

MIX DB

Admin

Med Info

EMR Interface

Hospital MIX Server

MIX DB

Admin

Med Info

EMR Interface
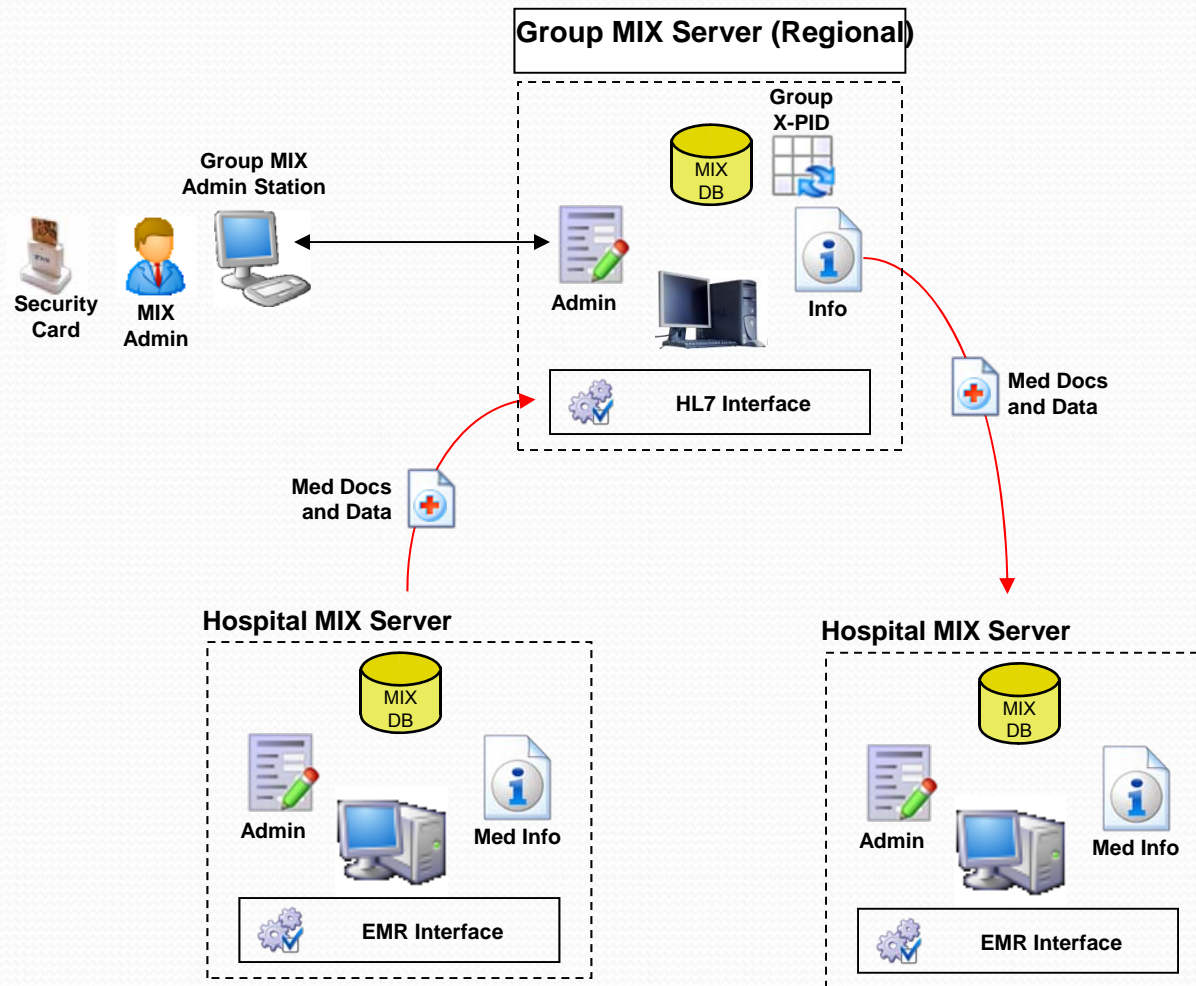
SETECS® MIX™
System Smart Cards

SETECS® MIX™ Provider Card

SETECS® MIX™ Patient Card

Section 3

eEFMP System Description based on SETECS Products

EFMP System
AUTHENTICATION USING CAC / MIX SMART CARDS
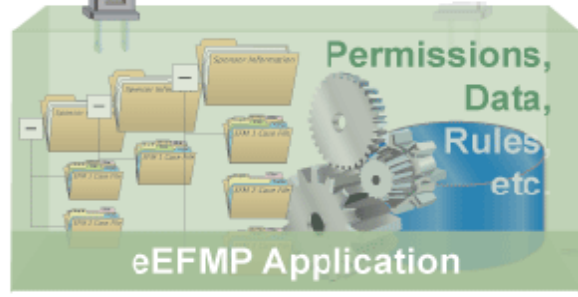
SAML Ticket
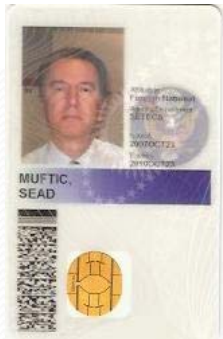
User name / password method will be replaced with CAC or MIX card login, using PIV Authentication and Single Sign-on (SSO) protocol.

EFMP System
MANAGEMENT PORTAL VIEW

Hospital Security Server

IDMS   CA/PKI   AAA

System Manager

Hospital MIX Server

MIX DB

Admin Server   Portal Server

After login the role of the person will be determined using RBAC policy. If he/she is a manager or specialist, Portal will display Management View. Database of the Hospital MIX™ Server will provide data for the Web interface.
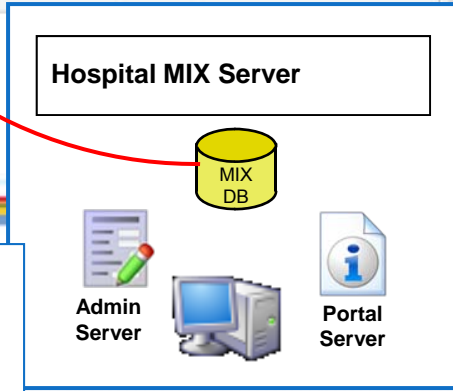
EFMP System
ROLE BASED ACCESS CONTROL
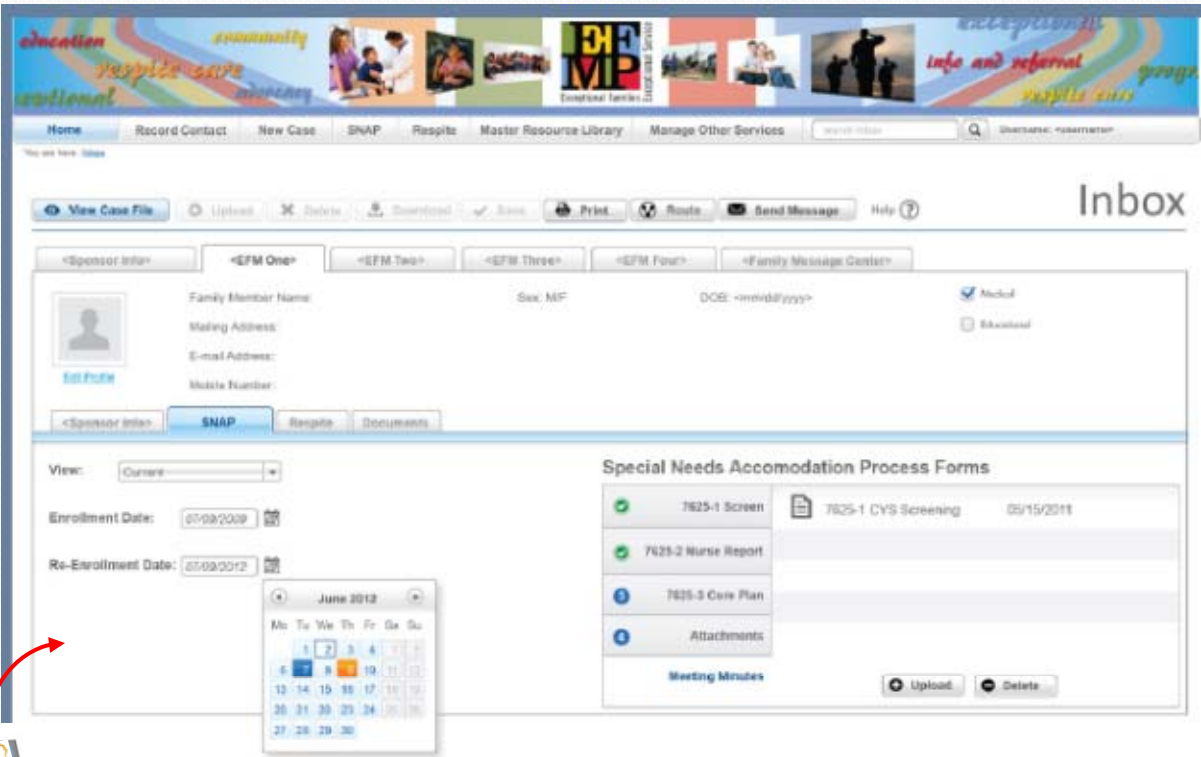
System Manager

Specialists

Users

System Manager

Role−based access will be simple: Each tab on the Portal's panel will be declared as system resource (target). There will be three roles in the system: **managers** (system administrators), **specialists** (medical providers), and **users**

EFMP System
MANAGING FORMS

Group MIX Server (Regional)

Group X-PID

MIX DB

Admin

Info

HL7 Interface

CCD Forms

System Manager

The system will also manage forms and documents. They will he be handled in the standard CCD format. Central repository of all forms will be either Regional or National MIX server. Forms will be encrypted and signed.

EFMP System
AUTHENTICATION USING CAC / MIX SMART CARDS

Soldiers will use CAC and MIX™ cards to log into the system.

EFMP System
DASHBOARD / HOME PAGE FOR SOLDIERS

Hospital MIX Server

MIX DB

Admin Server

Portal Server

After login the role of the person will be determined using RBAC policy. If he/she is a soldier, Dashboard / Home Page for soldiers will be displayed. Database of the Hospital MIX™ Server will provide data for the Web interface.
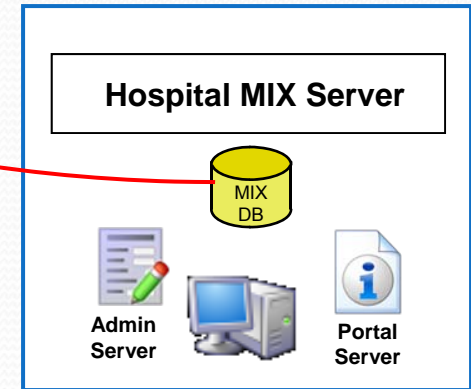
HANDLING AND PROTECTION OF FORMS
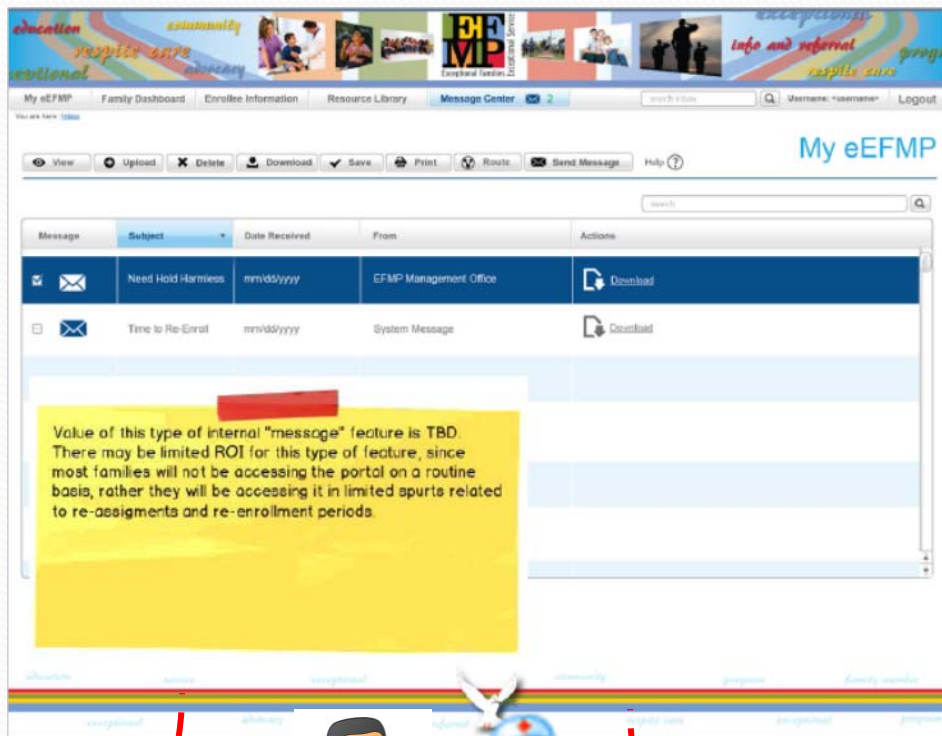

PIV Middleware

CAC or MIX Smart Card

The system will provide use / handling of forms. Forms will be digitally signed, using CAC or MIX™ smart cards and SETECS PIV Middleware.

EFMP System
MESSAGE CENTER (MOBILE TECHNOLOGIES)

Specialists

The system will distribute information, alert and any other messages to mobile phones.