

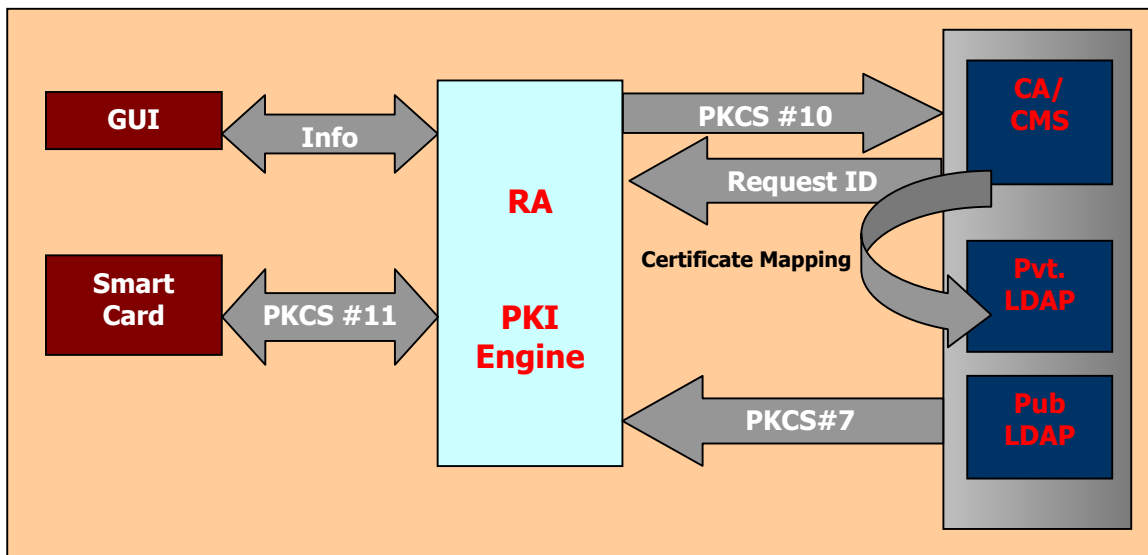
## Business Objective

Managing security in hospital network has been one of the core focus areas of our customer, a key player in medical equipment and healthcare information management system in Japan market. Ushustech's expertise in network security and cryptography made the customer to offload their requirement of developing proprietary software for registering and generating digital certificates for the hospital staff.

Regaut acts as a registration authority for digital certificates and issues smart cards for the staff. These smart cards contain a digital certificate generated using PKI which also contains details like the card holders access right to various locations both physical and in the hospital LAN. The hospital management can decide access rights and permissions. Since card is signed by a digital certificate generated by the most infallible or unbreakable cryptographic techniques no one can duplicate it.

## System Overview

Regaut is a GUI based client application that could be used as a Registration Authority (RA) adopting PKI architecture to run in Windows2000 environment. This package implements RA application for providing certificates to be used on Smart Cards using PKI. Features like managing new users, existing users, retired/lost persons, interacting with Certifying Authority (CA) and inventory/update operations on the Lightweight Directory Access Protocol (LDAP) Server are also included in the system.



Netscape directory server is used as the repository of Certificates and Certificate Revocation Lists (CRLs). Crypto APIs provided by Microsoft is used for the Key pair generation.

**Registration Authority (RA):** The functions which RA carry out includes personal authentication, token distribution, revocation reporting, name assignment, key generation, archival of key pairs etc. An RA is itself an end-entity.

## Regaut

In some cases end-entities will communicate directly with a Certifying Authority (CA) even where an RA is present (e.g., for initial registration and/or certification the subject may use its RA, but communicates directly with the CA in order to obtain certificate). Registration is the process by which subjects make themselves known to CA. Once registered with the CA, a certificate is issued to the subject, provided that the certificate is in compliance with the criteria established by the CA policy.

Following basic functionality exists in the system:

- Supports new users and old users.
- Automated registration authority including:
  - RA approval of requests meeting customer criteria
  - Key pair and CSR generation.
  - Transfer of requests between RA and CA.
  - Transfer of certificates between CA and RA
  - Update public key/private key.
  - Request CRL generation to CA
- Netscape Directory Server 4.12 based data repository
- PKCS#11 module, implemented in software provides appropriate drivers with OS enables the certificates to be written to smartcards.
- Support for X.509 certificates