The Use of X.509 in E-Healthcare

Professor David W Chadwick
University of Salford
X.509 Public-key and attribute certificate frameworks

- X.509 Public Key Infrastructure (PKI) provides a standard for strong authentication, based on public key certificates and certification authorities.

- X.509 Privilege Management Infrastructure (PMI) provides a standard for strong authorization, based on attribute certificates and attribute authorities.
E-Healthcare Projects

- X.509 PKI - Secure access to a hospital Diabetes Information System for high street opticians and general practitioners via the Internet

- X.509 PKI and PMI - Secure authorisations of prescribers, dispensers and patients in the Electronic Transfer of Prescriptions
  - D.W. Chadwick, D. Mundy, "Policy Based Electronic Transmission of Prescriptions", to be presented at IEEE POLICY 2003, 4-6 June, Lake Como, Italy
Components of a PKI

Certification Authority

Registration Authority

X.500/LDAP Repository

Subscriber

Public key

Private key

Public key certificate

Components: Public key, Private key, Subscriber, Registration Authority, Certification Authority, X.500/LDAP Repository.
PKI

- Authentication is External to the Application

- One password or pin to access private key

- Public Key Infrastructure

- Multiple Administrators
- High cost of administration
- No overall Security Policy

Digital Signature

Application Gateway

Access Control Lists
Components of a PMI

- **Target Gateway**
- **Attribute Authority**
- **X.500/LDAP Repository**
- **Subscriber**
- **Authorization Policy**
- **Attribute certificate**
- **Privilege**
PMI

- Authentication and Authorisation are External to the Application

One password or pin to access private key

Fewer Administrators
Lower cost of admin
Overall Authorization Policy
The Salford ETP System
A Prescription with Bar Codes