International Telecommunication Union

The Use of X.509 in E-Healthcare

Professor David W Chadwick

University of Salford

Workshop on Standardization in E-health
Geneva, 23-25 May 2003

ITU-T

X.509 Public-key and attribute certificate frameworks

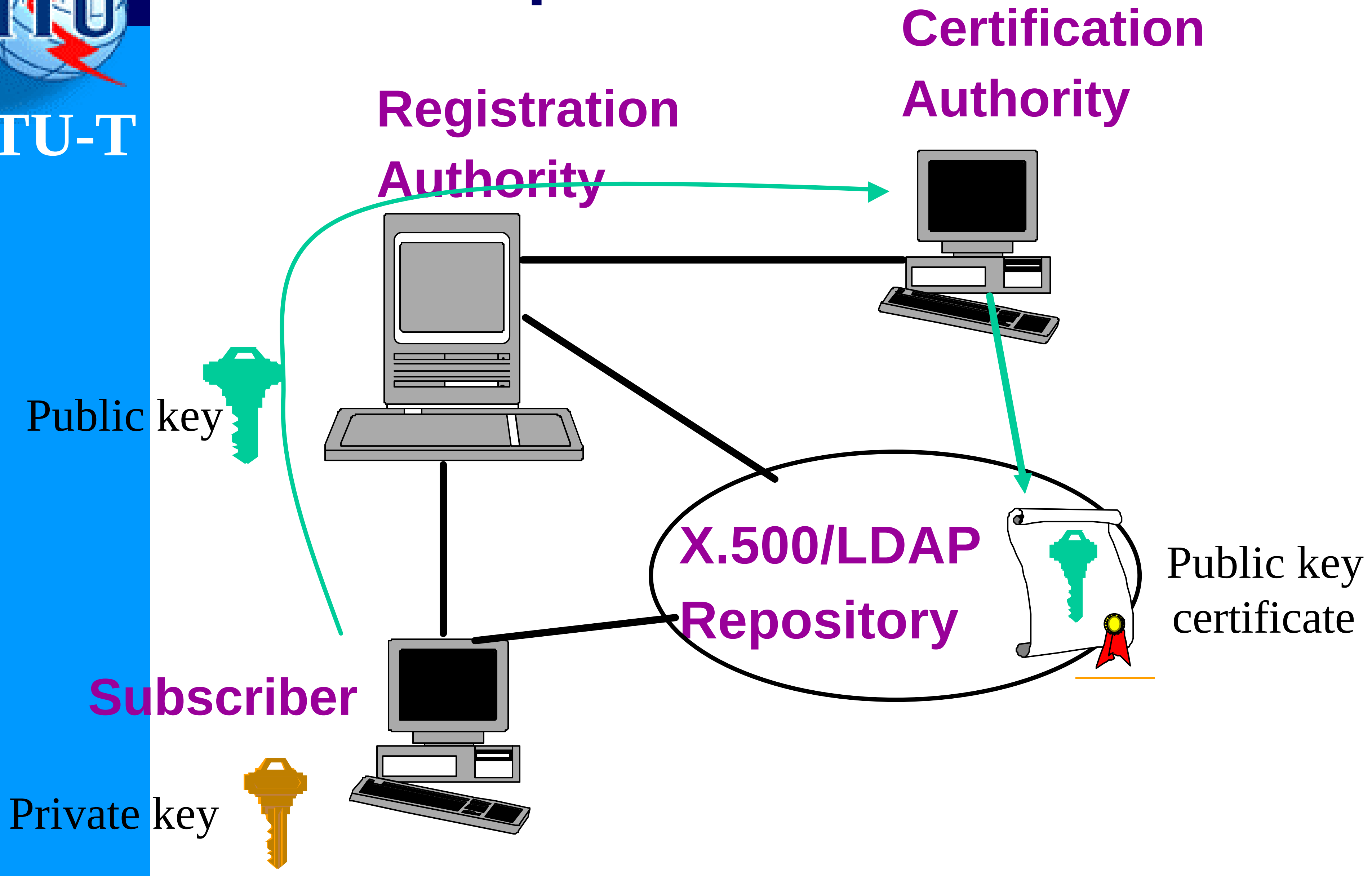
- X.509 Public Key Infrastructure (PKI) provides a standard for strong authentication, based on public key certificates and certification authorities
- X.509 Privilege Management Infrastructure (PMI) provides a standard for strong authorization, based on attribute certificates and attribute authorities

ITU-T

E-Healthcare Projects

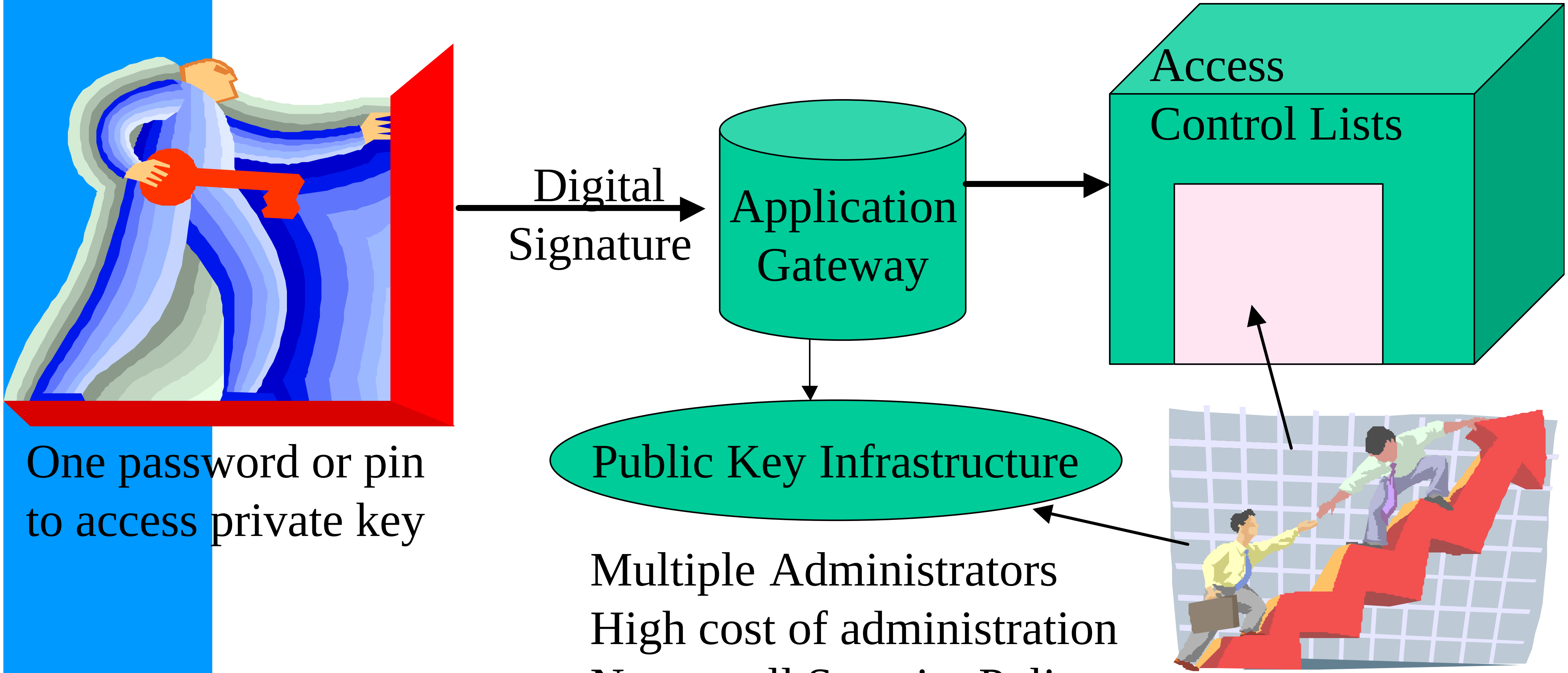
- X.509 PKI - Secure access to a hospital Diabetes Information System for high street opticians and general practitioners via the Internet
  - Chadwick, D.W.,Cook, P., Young, A.J., McDowell, D.M., and New, J.P., “Can the Internet be used to securely and confidentially access hospital diabetes information systems?” British Medical Journal, Vol 321, 9 Sept 2000, pp 612-614.
- 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



PKI

- Authentication is External to the Application



Digital Signature

Application Gateway

Access Control Lists

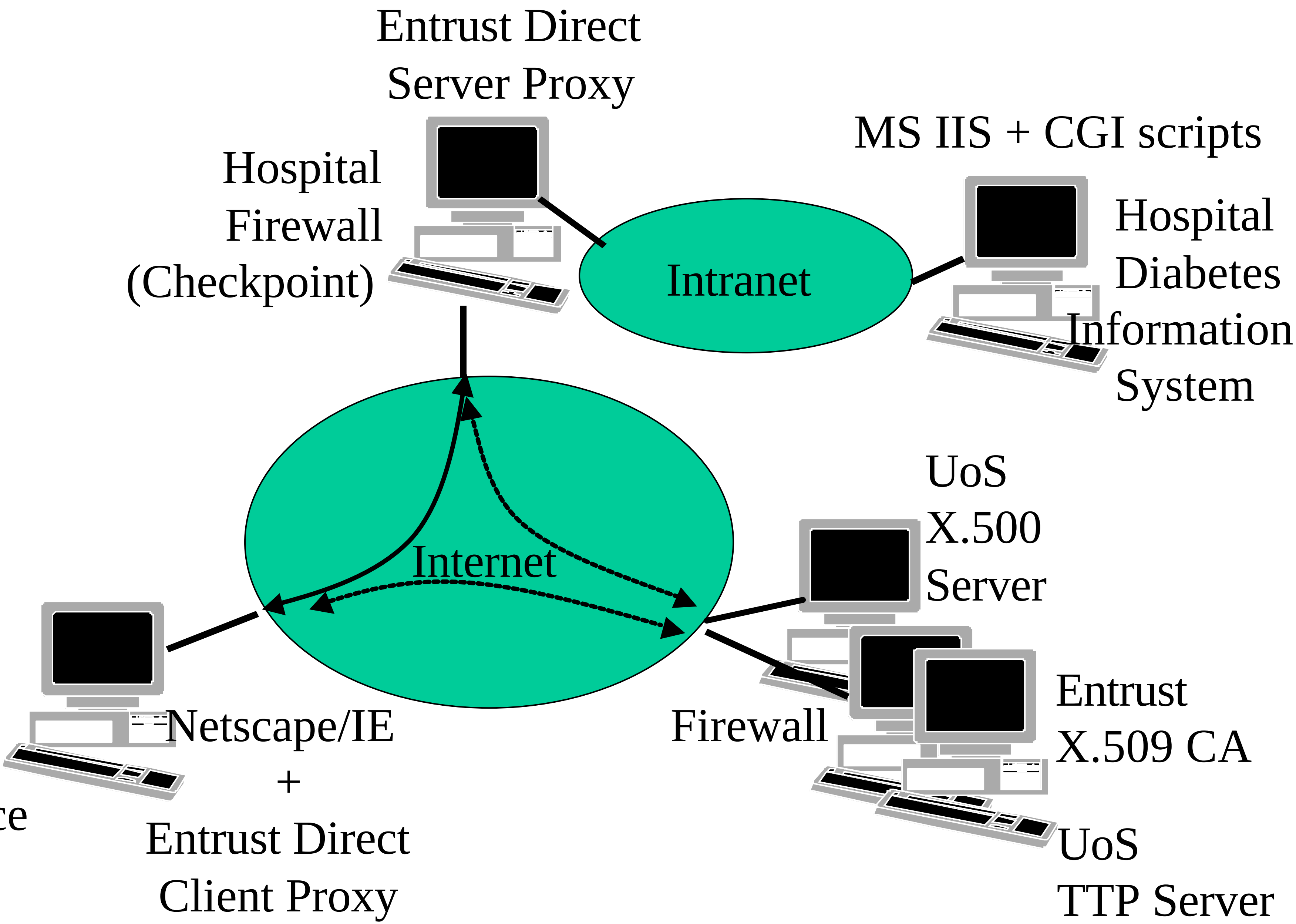
Public Key Infrastructure

One password or pin to access private key

Multiple Administrators
High cost of administration
No overall Security Policy

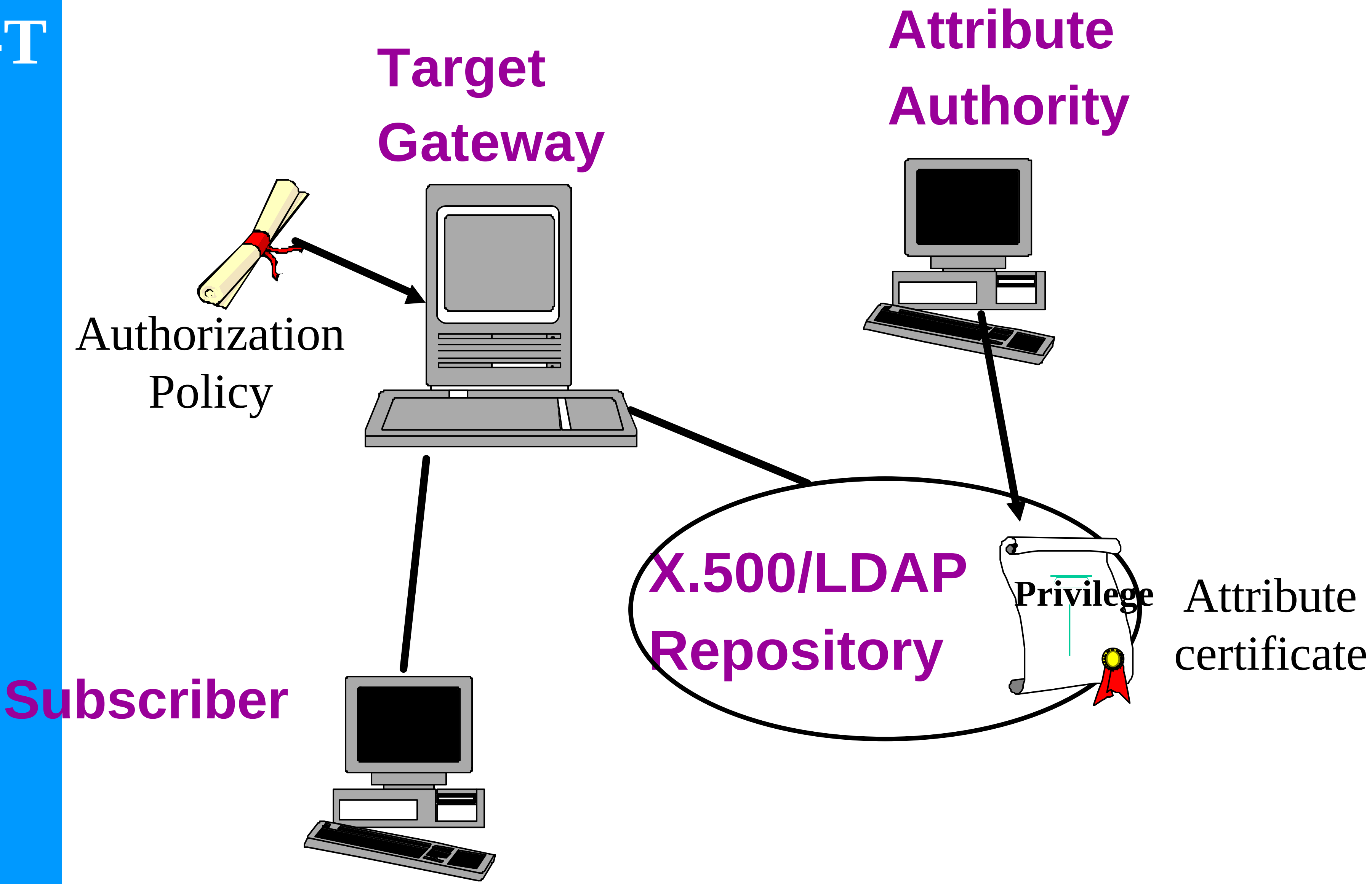
ITU-T

DIS Components



ITU-T

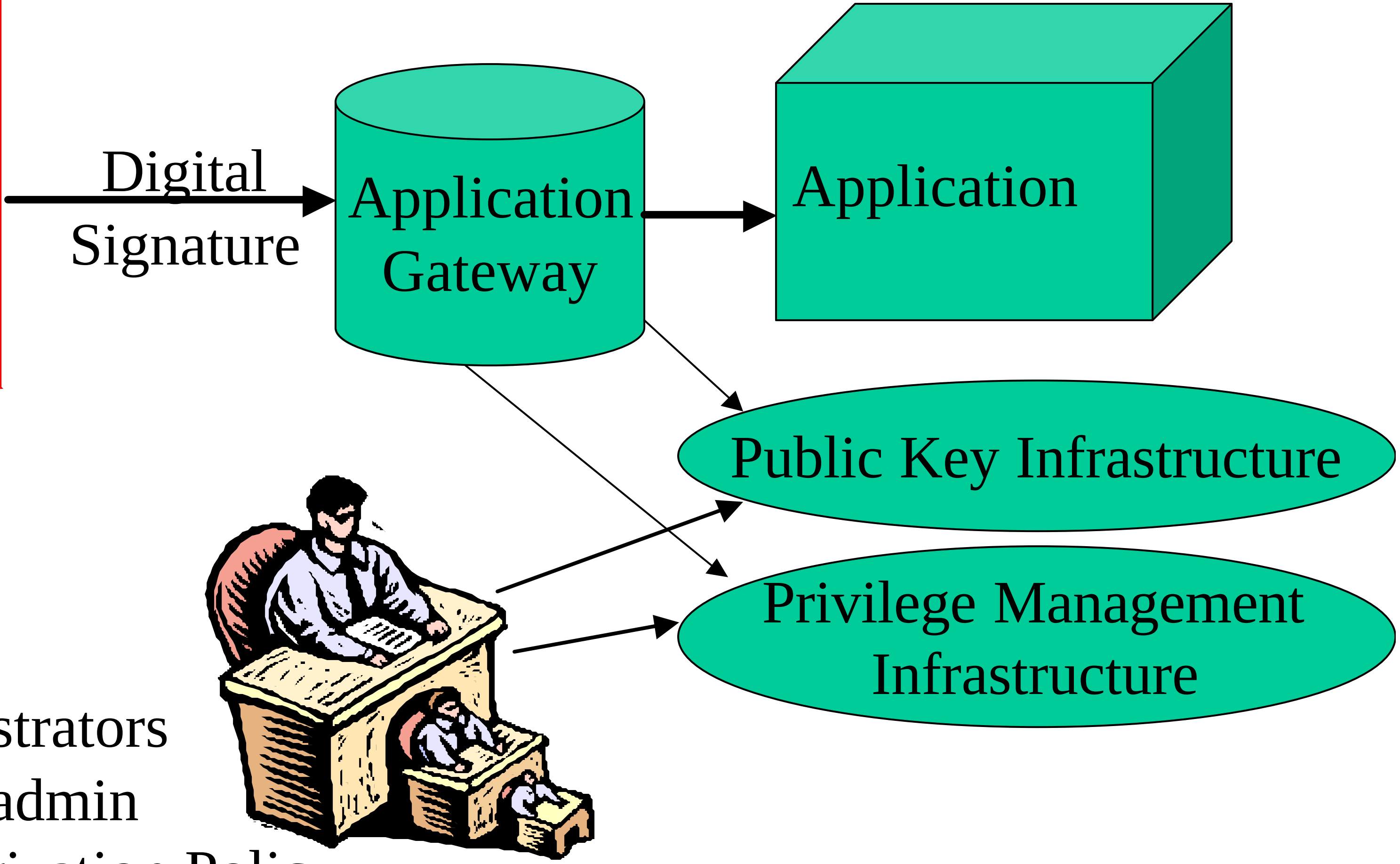
Components of a PMI



PMI

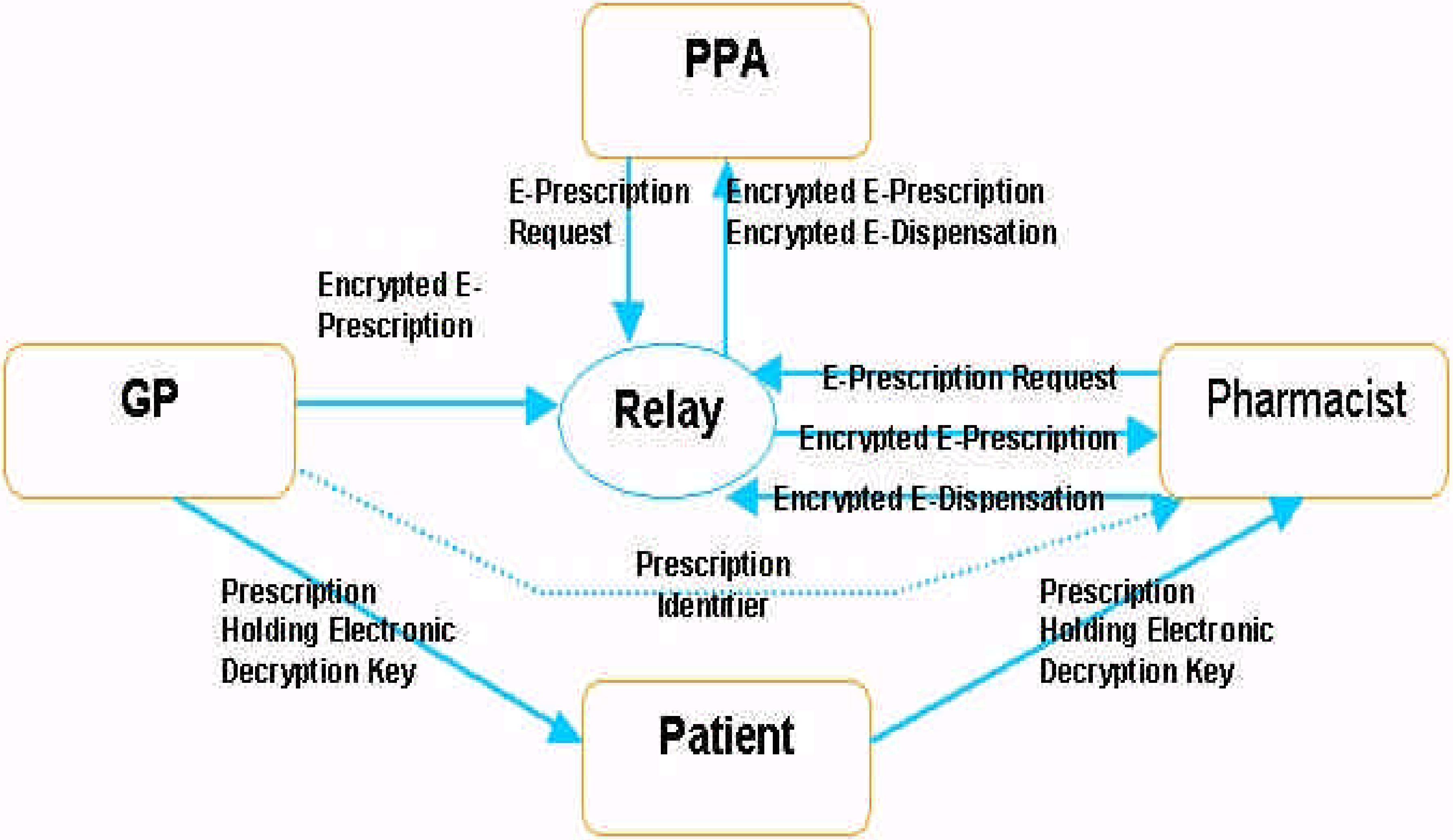
- Authentication and Authorisation are External to the Application

One password or pin
to access private key

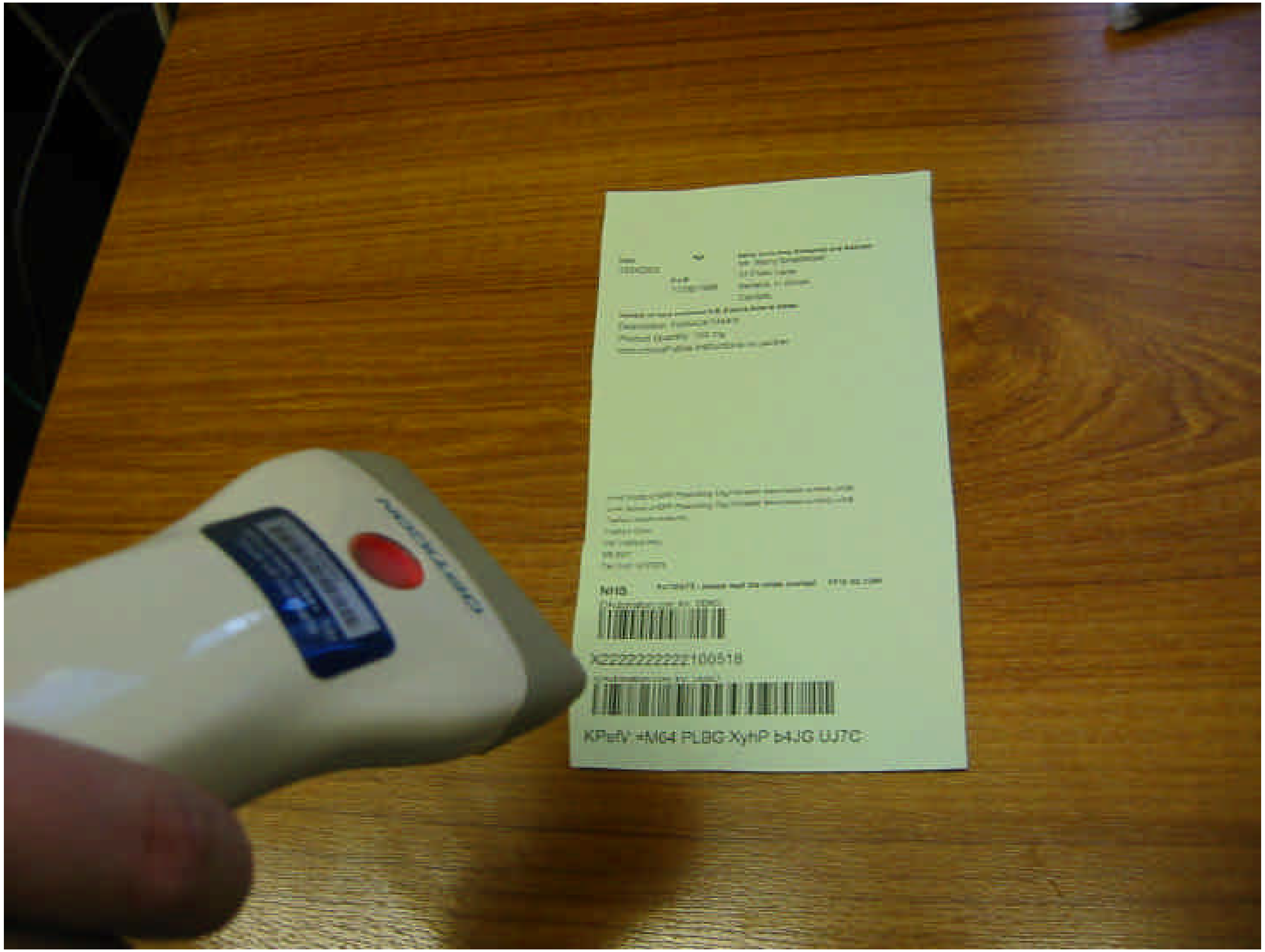


Fewer Administrators
Lower cost of admin
Overall Authorization Policy

The Salford ETP System



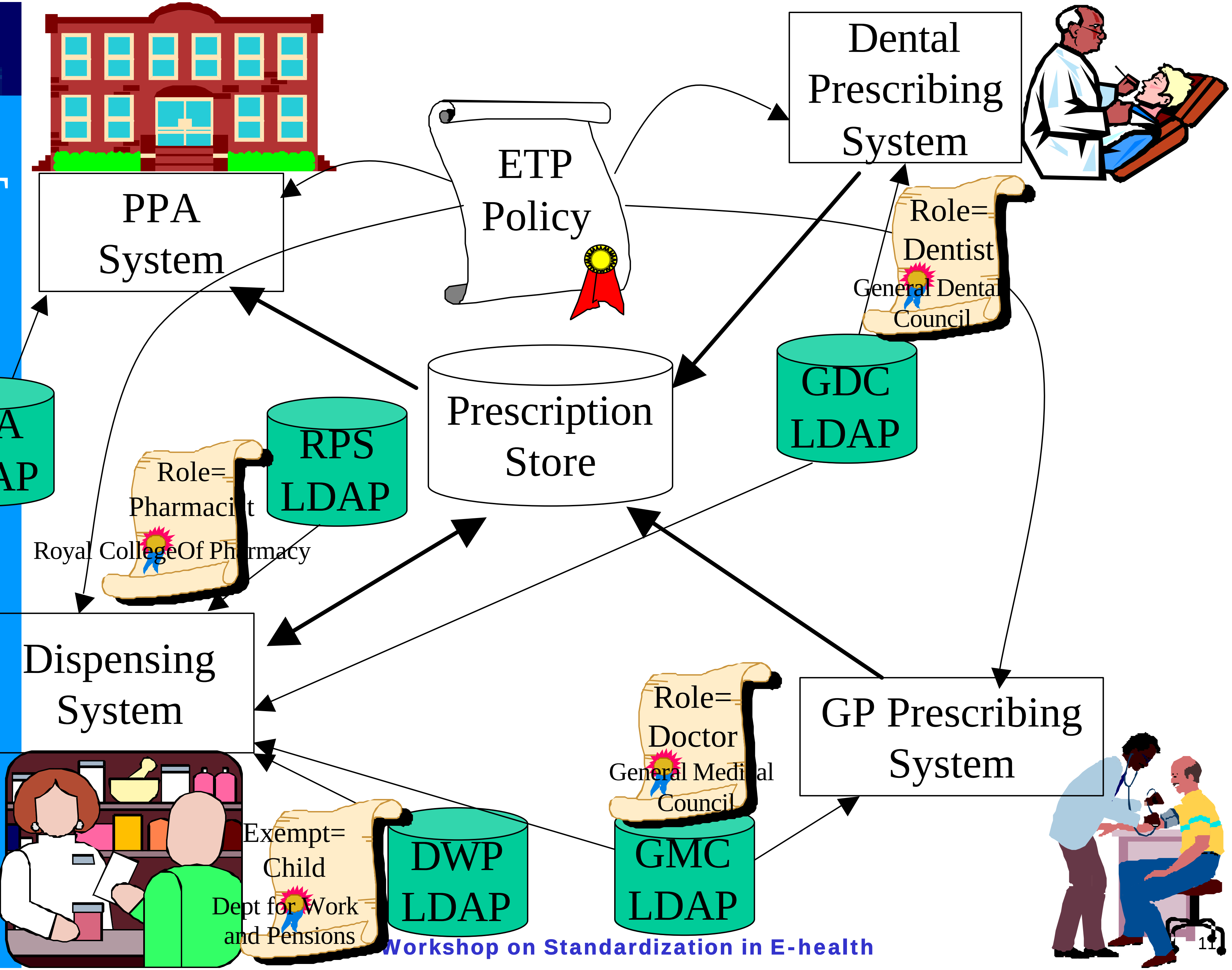
A Prescription with Bar Codes



X2222222222100518

KPeIV +M64 PLBG XyHP 54JG UJ7C

ITU-T



ETP Policy

Dental Prescribing System

Role= Dentist
General Dental Council

GDC LDAP

PPA System

PPA LDAP

Prescription Store

RPS LDAP

Role= Pharmacist
Royal CollegeOf Pharmacy

Dispensing System

GP Prescribing System

Role= Doctor
General Medical Council

GMC LDAP

Exempt= Child
Dept for Work and Pensions

DWP LDAP