

**1.1 Dr D W Chadwick**

**University of Salford**

<b>Higher Education Institute :</b>		<b>University of Salford</b>					
<b>Faculty/School/Group :</b>		<b>Information Systems Institute</b>					
<b>Address: The Crescent, Salford, M5 4WT</b>							
<b>Contact: Dr D W Chadwick</b>				<b>Tel: 0161 295 5351</b>			
<b>Email: d.w.chadwick@salford.ac.uk</b>							
<b>Keywords</b> <i>select as appropriate</i>	<b>Security</b>	x	<b>Fraud Control</b>	x	<b>Privacy</b>	x	
<i>(Add keywords from list)</i>	Trust			Authentication schemes			
Public Key cryptography	Authorisation schemes			Human Machine Interaction			
Distributed Systems							
<b>Research Overview:</b>							
<p>Our research is focused at the application level, rather than in the development of new cryptographic hardware or algorithms. We are primarily concerned with the usability of Public Key Cryptography, for both authentication and authorisation, and how the technology can be used to develop new and novel applications. Much of our focus is currently on Medical Infomatics, since medical data has a strong requirement for confidentiality and distribution. Consequently we are studying how strong cryptography can be used to design new distributed medical applications. Usability of the technology is an important consideration, because without this, the new applications that are developed will either not be used at all, or will be used incorrectly, thereby possibly circumventing their security. Scalability and performance are other interesting issues, particularly if the applications are to be widely distributed and frequently accessed. Finally, trust in PKIs is a further user consideration. How can users easily determine is a digital signature from a remote PKI is to be trusted or not? We are researching into tools and techniques that can be used to semi-automate the trust decision making process.</p>							
<b>Contact: Dr D W Chadwick</b>				<b>Tel: 0161 295 5351</b>			
<b>Email: d.w.chadwick@salford.ac.uk</b>							
<b>Research Project overviews:</b>							
<p><b>Researcher(s):</b> Dr D W Chadwick, Dr A Basden  <b>email:</b> d.w.chadwick@salford.ac.uk, A.Basden@salford.ac.uk  <b>details: Intelligent Computation of Trust.</b> We are building an expert system that evaluates the trust that one can place in a remote public key Certification Authority (CA), by analysing its Certification Practice Statement (CPS), through a human/computer dialogue, and by independently verifying that the CA does in fact do what it says it does in its CPS. This will help to semi-automate the trust decision making process of an individual.</p>							
<p><b>Researcher(s):</b> Dr D W Chadwick, Dr A J Young  <b>email:</b> d.w.chadwick@salford.ac.uk, A.J.Young@salford.ac.uk</p>							

**details: Distributed Diabetic Dietician.** We are documenting a generic method for taking a stand alone medical database application and converting it into a distributed application, accessible over the Internet using fully secured links. The communications are secured using public key cryptography and symmetric encryption. By way of an exemplar, we have made the Salford Diabetic Register, held at Hope Hospital, available to GPs in the Salford district. GPs can both read and update the database in real time from their surgeries. This underlying capability can then be used as the infrastructure for further clinical decision support systems, and we have built one such application as an example.

**Researcher(s):** Dr D W Chadwick, Dr A J Young  
**email:** d.w.chadwick@salford.ac.uk, A.J.Young@salford.ac.uk  
**details: Electronic Prescription Processing.** We are building an electronic prescribing system, based on X.509 attribute certificates, that will allow clinicians to write digitally signed electronic prescriptions, and store them in an X.500 database. This will allow the patient to visit any pharmacist and the prescription to be retrieved. The prescriptions and their dispensations may also be added to the patients Electronic Patient Record. This should help to minimise the large amount of fraud that is possible with the current paper based system.

**Researcher(s):** Dr D W Chadwick, Dr A J Young  
**email:** d.w.chadwick@salford.ac.uk, A.J.Young@salford.ac.uk  
**details: TrustHealth 2.** We are adding smart card support to our Distributed Diabetic Register application, and are measuring the user's acceptance of this technology, and comparing it to their acceptance of file based key storage.

**Researcher(s):** Dr D W Chadwick, Mr Simon Harvey  
**email:** d.w.chadwick@salford.ac.uk, Harvster@harvster.net  
**details:** We are studying the use of PKIs by organisations and are particularly interested in the usability aspects of the technology, as well as the business benefits that it might bring e.g. competitive advantage and fraud reduction.

**Source HEI**