

# Identity and Authentication

**Prof. Simon Rogerson**

**Sara Wilford**

**Originally published as ETHicol in the IMIS Journal Volume 10  
No 3 (June 2000)**

At the recent Computers, Freedom and Privacy Conference 2000 in Toronto, Canada there was an interesting session on identification and authentication in the on-line world. The panel consisted of Deirdre Mulligan - Panel co-ordinator, Karl Ellison from Intel, Phil Hestor of IBM, Margot Saunders a lawyer at the National Consumer Law Centre USA and David Flaherty the ex-privacy commissioner for British Columbia. This edition of ETHicol considers some of the main issues raised during that session.

How do you prove you are who you say you are? How do you know that someone is legitimate in his or her dealings with you, and how do you get redress if things go wrong? If your identity is stolen and used fraudulently, or personal records are altered without your knowledge or permission how do you prove that it was not you? It is difficult enough to verify someone's identity in the tangible world where forgery, impersonation and credit card fraud are everyday problems related to authentication. Such problems take on a new dimension with the movement from face-to-face interaction, to the faceless interaction of cyberspace.

The world of cyberspace has many difficulties of identification and verification due to its remote and electronic nature. You can never be sure with whom you are dealing or if the goods and services you are attempting to buy even exist. This is why the 'digital signature' and other authentication systems are being developed. Identity is however, important not only between individuals and organisations and from person to person, but also to promote trust in on-line companies and to verify their legitimacy.

In the UK, for example, these issues are being addressed by two initiatives which are in line with the E-communications Bill. The tScheme will help to deliver an industry-agreed code of practice governing the way digital certificates are issued and managed for the purposes of legally binding communications. Whilst TrustUK will accredit e-commerce codes and provide a 'hallmark' that accredited companies may use on their websites.

There are however, problems associated with digital signatures, even with the use of biometrics. For example, the use of a thumb print reader may only provide the equivalent of a three or four digit password, which is easily hackable by anyone with sufficient determination and know-how. The temptation is to presume that the certified key holder is the one actually holding the key. The authorising mechanisms may actually see the

access as legitimate even though the authorised person may not be the one using the system.

With the sheer size and scope of the on-line environment, it is becoming clear that the use of only names is increasingly unfeasible for authentication purposes. This is because it is impossible to be sure that the people you are dealing with are who you think they are. However, key-signing sessions and other methods attempting to vouch for a key holder still only identify the legitimacy of the key, and not the user.

Whilst the need for verification to promote e-commerce is relatively clear, the needs of business and governments in verifying identity must be carefully considered in the light of individual privacy and the increasing requirement that individuals reveal more and more details about their personal lives. Are we in danger of becoming so transparent to the data banks that the privacy of the individual is only to be found inside one's own mind? The unique data that will be required to verify identity will need to be carefully protected to ensure that potentially sensitive personal information does not enter into the public domain.

The use of very strong cryptography has been cited as one way that verification and authentication may be achieved. However, the need to enter several codes and to perhaps also provide a biometric identifier is unlikely to be workable in order to purchase an item from the Internet due to the sign-on burden placed on the consumer, and indeed may undermine the principle of easy on-line shopping.

As consumers, we need to be assured that our credit and debit card details do not go astray, and that only those documents with our authorisation and verification will be acted upon. The idea that someone may use our identity for their own means, or that third parties may access sensitive information is of great concern to many. The use of authentication and security techniques is vital in addressing these concerns. The use of a credit or debit card in an on-line environment is relatively safe due to the legal obligation of banks to reimburse customers. However, commercial organisations do not have as much to lose as the customer, particularly with regard to sensitive personal data, so they may not have the incentive to provide strong security. This lack of bargaining power by the consumer can be considered problematic and may only be overcome by strong legal pressure and monetary penalties on the holders of data.

The problems associated with authentication are not just related to the verification of identity but also involve greater public policy issues, which include the amount and kind of data required to confirm the identity of someone. The use and access to such data is an issue of major importance due to its potential for abuse by organisations seeking to maximise profits by using the data for marketing purposes. The confirmation of individual identity or the authentication of those accessing or amending data is an emotive issue. There has to be a fair balance between upholding personal rights whilst enabling authenticated and secure access to on-line services and products.

Please send your views on ethical and social responsibility issues and cases of ethical dilemmas to:

Professor Simon Rogerson  
Director  
Centre for Computing and Social Responsibility  
Faculty of Computing Sciences and Engineering  
De Montfort University  
The Gateway  
Leicester  
LE1 9BH  
Tel:(+44) 116 257 7475  
Fax:(+44) 116 207 8159  
Email:<srog@dmu.ac.uk>  
Home Page: ( <http://www.ccsr.cse.dmu.ac.uk> )