

The act of recognition is not the main hurdle for biometric systems – it is the rather less sexy issues of enrolment and identity management.

Identity crisis

By Charles Orton-Jones

Mission Impossible got it all wrong. There is nothing high-tech about iris recognition technology – in fact it is positively old-fashioned. Biometric recognition systems, using the iris, fingerprints, voice or even vein patterns, have been around since the 1950s.

Back then the security concern was verifying the identity of the US president in the event of a nuclear strike. These days the application can be far more mundane, such as logging on to a company network, or authorising a transaction, but the key problem remains the same. It is not the act of recognition that is holding up the progress of biometric systems, but the rather less sexy issues of enrolment and identity management.

Before a company can install biometric security systems it must decide how it will enter the details of its participants, and provide reassurance as to where this data will be stored, who will see it, how it can be manipulated, and how the information will be shared. Unlike a smartcard or password, biometric information cannot be transferred or altered in the life of the 'holder'.

One organisation currently facing these perplexing issues is the United States Immigration and Naturalization Service (INS), which is planning to base American national security on biometric technology. As part of the Enhanced Border Security and Visa Entry Reform Act, signed in March 2002, the INS is researching the possibility of making biometric recognition the core of national entry and exit security.

Responding to the INS's preliminary request for information is Irish biometric company Daon, whose chief executive Oliver Tatton believes the INS's biometric security network will become a reality as soon as the question of identity management can be dealt with by the Americans.

"Think about the issues they have to consider, such as how are people trying to enter the US going to be enrolled on the system? Will it be done by the national passport offices or the American embassies in those countries? What about the privacy arrangements? Who is going to get to see the information, and who will it be passed onto? Where is the information going to be stored?"

Tatton entered the field of biometric security to focus not on the recognition systems,



Daon chief executive Oliver Tatton says management of identities, not recognition, is the hard part of using biometric security.

which are now manufactured by dozens of firms across Europe and the US, but to provide software to help organisations solve these problems of identity management. His system is already in use at London City Airport, where the security staff themselves use a Daon enabled recognition system to gain access to restricted areas. There, as in a corporation, the same questions apply, such as enrolment.

"Self-enrolment, as device manufacturers suggest, is useless. You could be anybody," says Tatton. "We ensure you are enrolled through a controlled procedure – in the presence of recognised figures, such as the chief executive and system administrator." This means entering your details into the system, and then placing your finger, or iris, before the capture device before being authorised by users familiar to the system. This means only friends, and no foes, can slip in. Identities cannot be tampered with, and barriers exist to prevent unauthorised sharing. Users at the airport have reported no doubts over Daon's system.

Once up and running biometric systems offer quite staggering levels of accountability, by offering the possibility of tying actions to a person, and not just an interchangeable device, such as a password. "This means at an airport the baggage handlers can put their name to each piece of luggage as it passes through. A fingerprint is all that is required."

Daon's software utilises Private Key Initia-

tive (PKI) encryption, so documents can be 'signed' using a biometric signature. This means sending a document with a biometric authorisation, which stamps who sent what at what time onto a document. The procedure is so secure that the United States Federal Drug Agency recognises the procedure when receiving electronic documents – a massive endorsement.

Within a corporation almost any software and platform can be integrated with Daon's biometric systems. CRM systems can be hooked up, so a fingerprint can bring up all information related to the user. Privacy is ensured – there can be no tampering with the specifics of a user's identity. And as for the gruesome spectacle of intruders using severed fingers of enrollees to gatecrash, it is a myth according to Tatton. "A finger has to be attached to work," he says. Daon's extraordinary research into biometric use reveals that even children can be successfully enrolled onto the system.

"What the industry in Europe really needs to get going is legislation creating standards," says Tatton. "Guidelines are appearing, but we need common standards along the lines of GSM in the mobile world."

With the US government backing biometric recognition, mainstream take-up will surely follow. Tatton's dream of a world in which all 'tokens' of identity are redundant will be upon us. But who controls the keys to that world remains an open question.