

Information technology: Refining personal identification techniques using biometric data

Exciting times for ISO/IEC JTC1/SC17

By Freda Bennett, Secretary ISO/IEC JTC 1, *Information technology*, SC 17, *Identification cards and related devices*

The ground-breaking standardization work of ISO/IEC JTC 1/SC 17, Identification cards and related devices, has been mostly in the field of "smart" cards. Although the finance industry led the work on cards during the 1970s, other industry sectors are now making the running in the use of these cards for personal identification. Indeed cards are now commonly used for secure access control to buildings, computer systems, goods and services of a non-financial nature but nevertheless with the aim of unambiguously identifying the rightful cardholder.

Freda Bennett, Secretary ISO/IEC JTC 1/SC 17 surveys the work done, and reviews the exciting exploratory work on the newer areas around personal identification of the cardholder and the use of biometric data in identifying users.

For many years ISO/IEC JTC 1/SC 17, *Identification cards and related devices*, has been known as the "cards" committee. Its series of standards dealing with all aspects of card standardization is widely used throughout the world, and in many

and various industry sectors.

The set of SC 17 published standards and its current work programme are continually being revised to take account of new technology developments and enhancements and can be summarized as follows:

- physical characteristics of the ID-1 card (ISO/IEC 7810) and for thin flexible cards (ISO/IEC 15457);
- recording technologies (embossing, magnetic stripe, optical memory, integrated circuits with contacts and contactless integrated circuits); (ISO/IEC 7811, ISO/IEC 7816, (ISO/IEC 10536, ISO/IEC 14443, ISO/IEC 15693);
- numbering system for cards; (ISO/IEC 7812);
- terminal architecture ;(ISO/IEC 20060);
- application areas (machine readable travel documents (ISO/IEC 7501), driver licences (ISO/IEC 18013), financial transaction cards (ISO/IEC 7813);
- test methods associated with the above (ISO/IEC 10373).

Some of the standards relating to newer technologies, such as integrated circuits and contactless integrated circuits, are being revised to address interoperability issues and this is expected to continue as the market matures. The development of these newer technologies sees the emergence of more sophisticated cards offering expanded and improved services, particularly regarding security issues.

Although the finance industry led the work on cards during the 1970s, other industry sectors are now making the running in the use of these cards for personal identification. Indeed cards are now commonly used for secure access control to buildings, computer systems, goods and

services of a non-financial nature but nevertheless with the aim of unambiguously identifying the rightful cardholder.

Problems of PINs (Personal Identification Numbers), and identification of the cardholder

In the past, identification of the cardholder has been achieved by using a magnetic stripe card with either a Personal Identification Number (PIN) or a signature. In order to obtain access to buildings, goods, services or to a bank account, the card is read by a card reader and either the PIN keyed into a PIN Entry Device (PED) or a signature obtained which is checked against the signature on the back



of the card. However, there are real weaknesses with PINs and signatures, particularly when used in conjunction with magnetic stripe cards since both security techniques and storage capacity on the magnetic stripes are low. Cardholders have been known to divulge their PINs to partners or friends. They may write them down where they can easily be found, or PINs can be stolen, for example, by "shoulder surfing" at ATMs (Automatic telling machines), POS terminals or points of access. The cards themselves can then be stolen so that the card can be used fraudulently. The use of a card with a PIN



or signature is no guarantee that the card has been presented by the rightful holder.

Looking for more secure methods of authentication

This two-factor authentication using something the holders "has" (i.e. the card), and something the holder "knows" (i.e. the PIN) is not as strong as card issuers would like because of the inherent weakness of the PIN. The addition of a biometric as the third factor of identification, tying the card to the holder by something that the cardholder actually "is" is a more secure method of identification.

Biometric mechanisms measure physiological and/or behavioural characteristics to verify the identity of an individual. Well known commercial mechanisms include fingerprints, retinal and iris scanning, hand geometry, voice pattern and facial recognition. Academic laboratories have also investigated other techniques such as "keystroke dynamics", however the accuracy levels in terms of false acceptance rates (those cardholders accepted that should not be) and false reject rates (those cardholders rejected but that are valid cardholders) to date are generally not yet of an acceptable level. An important aspect of biometrics is that the result is not an absolute 100% match. A comparison is made of a profile against other previously recorded profiles to find an acceptable match. With PINs, however, the result is either right or wrong.

While the use of biometrics for personal identification has been talked about for many years, the early biometric devices were rather large and unwieldy, and were too expensive for most applications. Today, however, the devices on the market are

more accurate, and the cost per unit has fallen to a viable level. The technology has now matured so that false acceptance rates and the false reject rates are much closer to presently accepted limits. In addition, the processing time for the transactions is also becoming acceptable.

Prior to its plenary meeting in 1999, the SC 17 Chairman had received several requests to consider whether it had a role to play in the area of biometrics. In September 2000, SC 17 held a one-day workshop in London to assess the level of interest and to gauge whether there was anything SC 17 could usefully do on biometrics. The workshop identified four main areas of work that SC 17 might consider:

- Use of the technology for personal identification;
- Transposing existing non-ISO standards to ISO (SC 17 standards);
- Building on the WG 4, *Integrated circuit cards with contacts*, activity storing biometric data on integrated circuit cards but giving it a wider application;
- Addressing the specific requirements for cards and card-accepting device interfaces.

The discussions at the 2000 plenary meeting were both lively and positive, and a temporary working group was formed (OWG 2) to refine the four areas identified above and, if appropriate, to develop New Work Item proposals for SC 17.

The first meeting of OWG 2 was held in London in April 2001 and developed seven recommendations which will be considered by SC 17 at its plenary meeting in October 2001. Although these recommendations have not yet been ratified by the subcom-

mittee, much work is already being done within several SC 17 working groups to ensure that the standards currently under development will take account of the need to support biometric data on cards and other data carriers.

Confirming identity by use of biometric technology at border crossings

SC17/WG 3, *Machine readable travel documents*, has urgent and specific needs, requiring globally interoperable standards that enable identification cards/documents to be used when confirming identity with biometric technology for use at border crossings. WG 3 sees two main card-/document-related implementations:

- Personal identification of the card/document holder where the card/document must actually make the final determination of identity (e.g. evaluating the biometric data using on-board logic); and
- Personal identification of the card/document holder where the card/document provides details to an external processor that makes the final determination on identify (e.g. comparing biometric data against identity details carried on the card/document in a workstation or card reader).

Driver licences

The requirements for WG 10, *Motor vehicle driver licences and related documents*, are similar, with the national authorities requiring positive identification before issuing documents and then binding that identification by recording a biometric on the document. The present International Driving Permit (IDP) of the UN Conventions (1949 and 1968) on Driver Licenses is a paper document available throughout the world to anyone requesting it from an authorized issuing agency. In the USA, for example, any AAA office can issue an IDP without verifying the validity of the presented state driver license.

Additionally, the UN Conventions have

not been elevated to embrace the SC 17 machine readable technologies of today for either an IDP or a Domestic Driver Permit (DDP). It is internationally recognized that the present IDP document is easily counterfeited, and contains no security features. In essence, it is a meaningless document. The Massachusetts DMV on its web site advises "...do not accept International Driver Permits..."

These inadequacies have been recognized not only by ISO/SC 17/WG 10, but also by the United Nations/ECE-Transport Division responsible for the UN Conventions on Driver Licenses worldwide.

Using finger imaging, facial recognition and iris scanning

The scope of work of the standard under development will provide a secure IDP card that contains a minimum common "model" data element set in a prescriptive layout design on the front face of the card. The back of the card will provide, at the discretion of the issuing countries, supplementary (optional) data as well as SC 17 machine readable technologies (IC Contact/Contactless, Magnetic, Optical Memory) and Bar Codes. It also allows for co-existing machine readable technologies on the same card. The standard will contain interoperability standards for biometrics, including finger imaging, facial recognition and iris scanning.

The work will provide guidance for harmonization/interoperability in document authentication, data verification and identification of the document owner by both visual and/or SC17 machine readable technologies.

The end goal is to elevate the current UN Conventions into the information technology era of the 21st century.

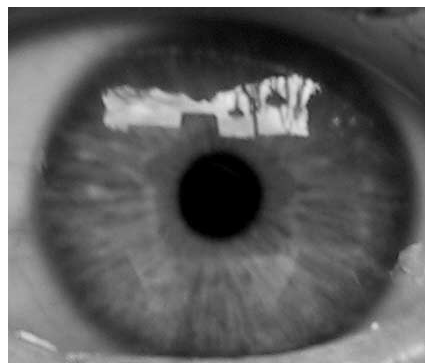
Data storage

In considering the work on machine readable travel documents and driver licences, taking account of the space restrictions on cards and other similar data carriers, OWG 2 recommended that SC 17 should adopt the Tag Length Value (TLV) format over ASN.1. WG 3 and WG 10 had already developed Logical Data Structures for bio-

metric data, but following the OWG 2 meeting they have both agreed the need to adopt a common syntax across SC 17 standards, and are reviewing the possibility of mapping their Logical Data Structures into TLV format.

ISO/IEC 7816-11, *Identification cards, Integrated circuit cards with contacts - Personal verification through biometric methods*, is being developed by WG 4 with these requirements very much in mind. It is an application-independent standard defining interindustry commands and interindustry data objects suitable for various kinds of applications using biometric user verification. It will reflect the usage of IC cards for on-card matching as well as the usage of IC cards (or any other cards) as carriers of biometric data.

Much of the work on biometrics has already been done or is being done outside of the ISO arena, and SC 17 intends to ensure that its work encompasses this and meets the requirements of the general biometrics industry. Indeed, ISO/IEC 7816-11 described above will take into account work done by NIST in the Common Biometric Electronic File Format (CBEFF) and ANSI standard X9.84, *Biometric Information Management and Security*.



Preferred biometric technologies

OWG 2 recognized three biometric technologies as those most suitable for use on cards and other biometric data carriers:

- facial recognition
- finger imaging
- iris scanning

The standards for these have already been developed or are being developed within ANSI, and SC 17 is determined not

to replicate work already done by others. However, it is recognized that these are still emerging technologies, and any standards produced based on today's technology will likely be revised regularly to take account of innovations in this technology. This is not unusual for SC 17 standards. Approaches are therefore being made to the developers of these standards to see if they will be willing to transpose them into ISO/IEC JTC1 standards. Feedback so far seems positive. Recognizing that they will need to be changed to meet the generic needs of the industry, it is being recommended to both SC 17 and to the owners of these standards that they undergo the five-stage ISO process rather than the Fast Track process. Plans are already underway to form a new working group to undertake the work and a P-member (participating member) has indicated that it would be willing to convene the group provided all goes to plan.

Although biometric techniques are heavily patented, SC 17 does not anticipate any problems in this regard. The ANSI standards were created to facilitate interoperability/functionality between different systems in such a way as to allow the original patent holders to retain their Intellectual Property Rights.

Exciting times

SC 17 intends to be proactive, and to establish itself as the focus of standardization for biometrics in support of personal identification. New liaisons will need to be formed and possibly closer ties with other ISO committees working in related areas.

This is an exciting time for SC17 which will be exploring ways in which it can publicize its work in order to attract new expertise at a time when attracting participants to work in the public domain standardization process is not without its problems.