Smart cards smart solutions

by Kevin Cowie

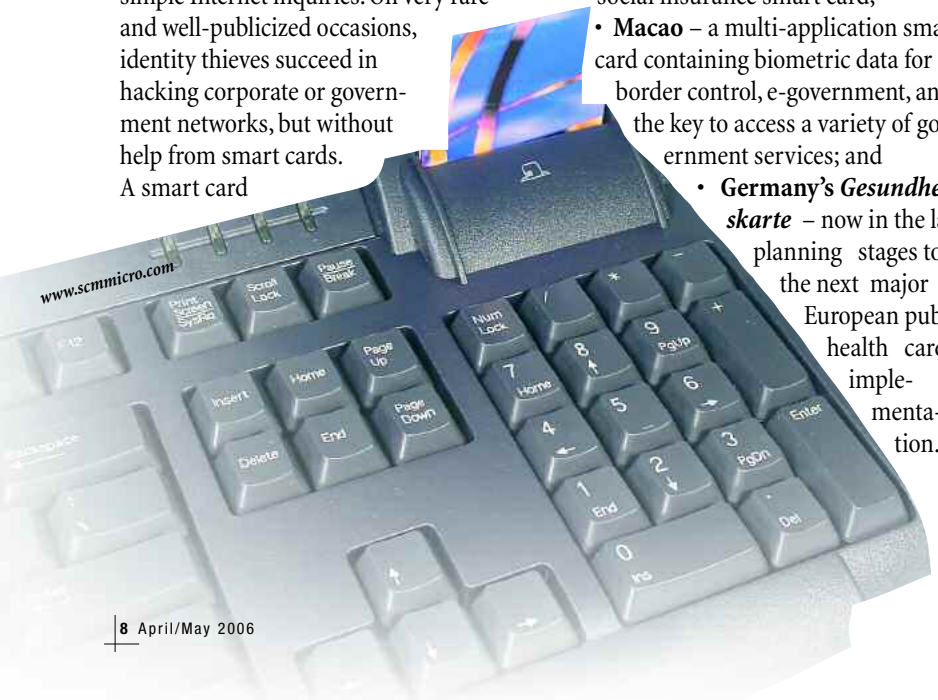
Addressing the myths and fears of implementation

GLOBALLY SPEAKING, WE are in the "sweet spot" of smart card adoption. No longer bleeding edge, the technology offers established standards, stable competition, and well developed solutions. Smart cards perfectly complement many governments' desire to deliver improved services, conveniently, at a lower cost and with greater security. Given the demand and the available solutions, why haven't smart cards been adopted in Canada?

Persistent myths and associated fears of the technology are part of the answer.

Myth #1: Smart cards will allow "big government" to track and gather more information on citizens. Government agencies collectively already know your complete medical history, family income, driving record. Smart cards have not been necessary for governments to collect information, nor will they add to this store.

Myth #2: Smart cards make it easier for identity thieves and fraudsters to access databases of information. Personal information can be gained through low-tech methods such as handwritten letters, telephone calls, office visits, fax messages, or simple Internet inquiries. On very rare and well-publicized occasions, identity thieves succeed in hacking corporate or government networks, but without help from smart cards. A smart card or two in the system could even help prevent such breaches.



These myths relate directly to two key information concepts: trust and security. Citizens must trust their government to make appropriate use of the information at its disposal. To ensure that our trust is not betrayed, and prevent misuse of personal information by *authorized* people, we create policies, laws, penalties and enforcement agencies. Misuse by *unauthorized* individuals is another matter. Security is needed; this is where smart cards fit.

Smart cards can carry information, authorization codes to access information, or the means to verify our own identity to establish such authorization. The following examples, implemented (or planned) by governments around the world, illustrate these capabilities:

- **Taiwan's health card** – the world's largest Java card implementation with 24 million cards distributed to citizens for health-cost tracking, electronic prescriptions, treatment history, pregnancy records, organ donation status and allergy data;
- **Austria's *ecard*** – a multi-application social insurance smart card;
- **Macao** – a multi-application smart card containing biometric data for border control, e-government, and the key to access a variety of government services; and
- **Germany's *Gesundheitskarte*** – now in the late planning stages to be the next major European public health card implementation.

Let's explore what's involved in implementing a national "smart" health card that would contain your personal health records. Regardless of where you need medical treatment, medical staff can access those records to help diagnose and treat life-threatening conditions avoiding therapies that could cause negative reactions. The health record is encrypted in a protected area of the card's memory; only legitimate medical professionals are permitted access, controlled by issuing them special smart cards of their own. These restricted cards enable medical professionals to access only the health information that you have pre-cleared for their authority level. How would we ensure that only the authorized medical professional acesses their own smart card? Smart cards can also contain specific information to verify the identity of the user. Everything from simple encrypted passwords to biometric scans offer built-in protection against unauthorized use.

In essence, smart cards can be used to provide convenient (some might fear *too* convenient) and secure access to sensitive information, such as a health record. But accessing this information requires a restricted piece of hardware with specially-issued secure identification cards built-in to them, plus a health professional card with the right level of authorized access, plus the right password or fingerprint or iris scan to activate the authorization, plus access to a patient's card. For thieves, the work involved to acquire all these components attempt to access the limited amount of information contained on an individual's health record wouldn't be attractive, compared to the volume of information accessible by hacking into a database, or breaking into a doctor's office, or blackmailing someone to copy sensitive files.

Smart cards can even help prevent these more "traditional" forms of theft. Network

and database security can be greatly enhanced using the same smart card technology used to authorize access to an individual's health card. Instead of a simple user name and password, card tokens, digital certificates and biometric authentication can provide more layers of security. Physical access to records storage can be secured the same way. Access to physical or electronic files can be automatically recorded and tracked, which also ensures they are returned properly.

Given these demonstrable benefits, government buyers and decision makers should think holistically about information security when addressing business or policy needs and consider the entire information flow, analyze the need for access to that information, identify areas at risk of unauthorized access, and build an overall information security architecture. Smart cards are just one highly economical element in an effective security architecture. A qualified vendor of smart card security solutions with a proven track record of successful large scale implementations could be consulted and undertake this analysis.

So, to revisit our initial question about smart card adoption in Canada, it turns out they have and continue to be – just not in the above-mentioned government service applications. Hundreds of corporations already use smart cards to control building and network access. Transit agencies are migrating to smart cards for fare payment. Canada's banking community has discovered the economic, convenience and security benefits of smart cards, and is now migrating all credit and debit cards to ones containing smart chips. As we learn to trust the integrity and security of smart chip technology in day-to-day financial transactions, everyone will become more comfortable with it. The benefits of smart cards in government may soon be realized.

Kevin Cowie is the director of product management, Government Solutions, Giesecke & Devrient. He can be reached at kevin.cowie@gi-de.com. For more information check the Smart Card Alliance, at www.smartcardalliance.org or Giesecke & Devrient at www.gi-de.com.