Committed to Australia's ICT, electronics
and electrical manufacturing industries

AEEMA

Access Card - Inquiry Into Human Services (Enhanced Service Delivery) Bill 2007

Senate Finance and Public Administration Standing Committee

COMMENTS BY AUSTRALIAN ELECTRICAL AND ELECTRONIC MANUFACTURERS' ASSOCIATION (AEEMA)

Introduction

Members of the Australian Electrical and Electronic Manufacturers' Association Ltd (AEEMA) support the introduction of the Health and Social Services Access Card to improve service delivery (notably in disaster and emergency situations), introduce efficiencies into the system, make service access easier for those in need, allow optional customisation by users and reduce fraud vulnerabilities. AEEMA welcomes the Government's efforts to articulate issues early and provide all draft legislation for comment. The Senate has now referred the Human Services (Enhanced Service Delivery) Bill 2007 to the Finance and Public Administration Standing Committee for inquiry and report by 15 March 2007. This bill seeks to establish the legal framework for the proposed access card. AEEMA notes that the Committee will be examining the bill's provisions relating to the intended scope and purposes of the card; the information to be included in the card register and card's chip and on the card's surface; and the range of offences aimed at prohibiting persons requiring an access card for identification purposes and prohibiting other improper uses of the card.

About AEEMA

The Australian Electrical and Electronic Manufacturers' Association Ltd (AEEMA) is the peak national, industry body in Australia representing some 400 infrastructure providers for Australia's ICT, electronics, and electrical manufacturing industries. AEEMA is organised in three principal divisions; member companies belong to some 17 industry forums. Two of these, the Asia Pacific Smart Card Forum and the Australian IT Security

Forum, have recently amalgamated into Smartcard and Information Security Australia (SISA), whose members are actively involved in research and development into the more efficient and secure treatment of corporate and personal data, particularly in relation to the finance, health and transport industries.

AEEMA's policy platform is based on adherence to competitive market principles, removal of trade barriers including non-tariff barriers, equivalent open access to markets, reduced red tape, regulation only where required, consumer safety and national benefit, appropriate environmental management regimes, equitable tax treatment for business and the removal of impediments to Australian manufacturing that harm its international competitiveness.

The security offered by smart card technology

Smart cards contain no more or less capacity to establish such an identity regime, if one were wanted. On the contrary, they *guarantee authentication and so are instrumental in ensuring privacy* – the protection they provide is dependent on making data available **ONLY** to eligible persons. Their current use in the passport system indicates a community belief that smart cards will make passports LESS liable to fraud. This belief is well founded, because a significant number of privacy concerns are allayed by confidence in the inherent security of the smart card, the security of the smart card application, and the security in the card-accepting terminal. Each of these systems requires accreditation to the appropriate international standards such as ISO, APCA, ITSEC and ICAO. The proliferation of national ID programs using secure chips and operating systems on smart cards is evidence of the value in raising security levels, particularly to overcome the risks associated with fraud and identity theft. The UK, Taiwan, Hong Kong & Macao are recent examples.

Most of these do not store significant amounts of data on the chip, but rather use the advanced technology to deliver a secure "key" to access the data. That data could be financial, health, tax, traffic infringements or other confidential data, held on secure databases, and accessed by encrypted transmission sessions.

The secret to success in implementing any government-initiated smart card program will be the ability to grow consumer confidence in accepting that smart card security allays privacy concerns over access rights to personal information. The essential principle is that a smart card is an authentication token. It authenticates a right to a service or it authenticates a User's identification. Whatever information is carried in the chip on the card (and this information will be determined at the outset during the policy and business rules architecture phase), the information can be protected and kept secret. The chip hardware is tailored and optimised for this purpose, along with suitable cryptographic methods for protecting the confidential data (even if this is only a PIN, a terminal authenticating password, or a biometric identifier of the user).

AEEMA is confident that as users increasingly realise the other applications and benefits to which the card may be put (emergency contact details, allergies, health alerts, organ donor status etc etc), most will be demanding extensions to its capability and capacity. The access card may become a useful identity tool for consumers, if they so choose. AEEMA commends the Exposure Draft's clear acceptance that users may opt for such customisation, or not, as their circumstances dictate. That said, data optionally stored by users on their cards is only beneficial to that user if it can be read and accessed easily. This will depend (for example) on whether emergency services organisations are equipped with appropriate readers to enable organ donor status to be accessed at the scene of an accident.

The draft Exposure Bill spells out the 15 pieces of information (p30-31) that may be included in the secure government area of the chip on the Access card:
Legal name
DoB
Gender
Residential Address
Photograph
Signature
Access Card #
Card Expiry date
PIN and or password (optional)
Benefits Card #
Medicare #
Reciprocal Health care card #
Emergency payment #
DVA information
Other info deemed necessary at time of registration.

AEEMA believes that this catalogue of client information is appropriate to provide the efficiencies and cost-savings inherent in the new regime.

AEEMA strongly believes that the choice of technology to support the new access card (including safeguards against function creep) is not as critical as ensuring the business rules behind the system are robust, widely debated and decided early. The Draft currently does not provide specific details supporting the registration process, and it is critical that this stage of the program roll-out be clarified early; it is integral to the success of card uptake and identity validation. The Draft recognises that registration and POI requirements for many residents may prove difficult – for example the homeless, remote, people at risk - and has included administrative heads of power for the establishment of appropriate alternative processes. This is welcomed, although the current vagueness of these proposals may cast doubt on the robustness of the registration process, thus further alienating opponents, particularly if there is a risk of possible compromise of POI levels through these alternative methods. In this regard the exposure draft mentions POI documents such as birth certificates, passports and drivers' licences. Many of these documents are currently susceptible to fraudulent use and identity theft; while the draft states that a new verification process will ensure duplicate documents are not used to fraudulently register, there is no detail as to what this new verification process will be. If verification relies on human checking as now, similar identity compromise issues may arise as are faced now.

The majority of potential registrants under the new program are already catered for within existing processes. Systems in place that support the provision of current cards in use will assist. There are 16 million people over the age of 15 in Australia and 8 million (12 million including children) in receipt of government payments including pensions as their main income source. They are also likely to be accessing Medicare benefits. This indicates that at least 8 million potential recipients of the new access card are already 'in the system', communicable, socially accustomed to the use of cards and the processes surrounding their issuance. Registration systems and processes for this population sub-set can thus build on current systems that are in place, apart from the added complexity of capturing photographs.

It will be necessary for Government to allocate funds for making the community aware of the most convenient process for them to be photographed. We note that recent tender documents contain some detail about registration processes for remote and rural areas not served by permanent government agencies. Facilities to register through 600 agency outlets across Australia complemented by Australia Post outlets will need to be further supported by mobile facilities to ensure coverage.

More importantly, the registration process will need to be reasonably rigorous, as there about 0.5 million Medicare cards in existence today that have no rightful owner. Fraudulent POI representations will need to be ascertained and dealt with at the time of registration. Needless to say these fraudulent card holders will not rush to register from April 2008 for a legitimate credential.

The draft notes that the new register to be established under clause 70 will not contain sensitive medical or health data nor will it be amalgamated with other current databases in the human services area. While recognising the public policy imperative compelling this decision, greater efficiencies across the entire health spectrum could have been guaranteed through a central database allowing (eventually) fully electronic health records systems linked with medical service delivery by hospitals and practitioners, prescriptions and admission/discharge procedures in public health facilities.

Privacy

AEEMA acknowledges that user concern about the new card program will centre on privacy. Any new regime of this complexity will struggle to respond quickly to the host of emerging technological and social policy issues inherent in such an ambitious plan as the access card presents. Regimes that endeavour to introduce technologies for better efficiencies and service delivery while promising to completely secure personal privacy or rights, may be better placed to respond to challenges if they educated consumers about the privacy-enhancing aspects of card technology. In addition, it behoves government and industry to remind users of the broader community context in which privacy regimes operate, and *the changing nature of a society which demands ever increasing benefits*, in particular:

- community demand for increased levels of consumer convenience, especially ‘linked up’ services in retail, finance and health;
- increased community demand for consumer-level control of, *and access to*, personal information.

Consumers are increasingly demanding more sophisticated access services allowing efficient and effective information manipulation in retail and finance; the corresponding requirement to confirm their identity, and seek ways to protect against that identity being compromised, can place pressure on public policy makers that sometimes appears insurmountable. Consumers need to be aware that *their demands are often parallel and sometimes competing*, thus making it difficult, but not impossible, to ensure a balance between competing demands. There is mounting evidence suggesting consumers are able to make sophisticated ‘trade-offs’ between the social goods they are seeking such as retail and banking convenience, and the balancing need for security and privacy.

This is not to suggest a weakening of privacy protections, but an acknowledgement that privacy *exists within a complex social environment* and that guidance may be needed to reconcile these competing demands. It does suggest, however, a refinement of the definition of privacy; in the past, anonymity was seen by some as the cornerstone of any privacy regime. But anonymity (literally, ‘without a name’ or identity) can no longer be consistent with consumer demands for increased convenience in dealing with their own data, because a *secure and verified identity is essential* if industry and policy makers are to meet consumer demands. That said, AEEMA recognises that user demand is not initially driving the introduction of the access card. But the successful marketing of the benefits of the access card, combined with the greater security of consumer privacy through privacy-enhancing technologies, may be a more appropriate strategy than attempting to counter emotive opposition to the access card by privacy advocates.

It should be said that industry is accustomed to the complex issues surrounding information protection. Protecting sensitive data and segregating it on a "need to know" basis is integral to the operation of agencies handling classified national security information, and the technologies and protocols used in this environment are equally applicable to the protection of personal information. Dealing with the conflicting requirements of access and dissemination are also well understood and are being addressed by defence and intelligence communities on a global basis.

Conclusion

AEEMA believes that the successful implementation of the access card is both achievable and necessary for the better efficiency of health services delivery. The smart card industry, within AEEMA’s corporate umbrella, has a long heritage of solving privacy issues through both technology and user education. There is no reason why current community concerns about the access card cannot be similarly solved; service delivery, cost savings and fraud mitigation depend on it.