DOCUMENT SECURITY ISSUES

Part of a Series of Datacard Group White Papers for the Secure Document Issuer

CONVERGENCE OF GOVERNMENT PROGRAMS WITH OTHER CARD SECTORS

Overview

Unprecedented growth in the demand for optimum national security throughout the globe has resulted in an expanding electronic identity document industry with smart technology leading the field. The rapid development of e-passports and identity card schemes is, perhaps, mirrored only by the 1990s smart card boom in the financial sector, which spawned the plastic card. National and international security is driving change with processes and technologies to enhance the security of documents. Many technologies are converging in the use and application of identification cards.

MARCH 2007

DatacardGroup

SECURE ID AND CARD PERSONALIZATION SOLUTIONS

CONVERGENCE OF GOVERNMENT PROGRAMS WITH OTHER CARD SECTORS

Developments in Passport Security

Machine-readable passports (MRPs) have been in circulation since the 1980s as hand-written passports became less secure in terms of data matching and being open to counterfeiting. Most are standardized by the International Civil Aviation Organisation (ICAO) document 9303, with a special machine readable zone providing the passport holder's personal information including name, passport number, check digits, nationality, date of birth and sex. The passport expiration date and personal ID number, where applicable, can also be read.

Between 2003 and 2006 the United States progressively introduced regulations making MRPs mandatory for anyone entering the US under the Visa Waiver Scheme. This means faster processing at immigration and secure matching of data. Since their introduction, MRPs are evolving to accommodate chip technology and biometric information – particularly since the ICAO recommendations are for biometrics using facial recognition technology and high capacity contactless integrated circuit chips.

The biometric passport combines paper and electronic identity (smart card technology) into a document using biometrics to authenticate the passport holder. Embedded chips hold all the critical information pertaining to the holder including all personal details and other digitized data such as signatures and photographs. Other biometrics such as fingerprint and retinal scanning, are being considered. The former is planned for adoption by many European countries, although the new UK version currently only employs digital imaging. The latter – retinal scanning, although a much feted technology is not being taken up by ICAO regulations.

The US version is not as complex as the European biometric passport, using only digital imaging on the contactless chip. However at 64 Kbytes, the chip is large enough to incorporate additional identifiers if and when the need arises. Production started in 2004 and it is expected all new or renewed passports will be issued to US citizens throughout 2006/2007. Similarly, the UK has already started its issuance for all new and renewed passports.

Biometric passports are becoming widespread in many EU countries – including Finland, Holland, Germany, France, Spain, Poland, Greece and Macedonia.

Elsewhere, in Australia, the biometric passport was introduced in 2005, again with only a digital photograph of the bearer's face on the chip. As in a number of European airports, control gates at Australian airports are being upgraded for fast clearance of e-passport holders using chip reader technology, and in some cases face recognition systems. A number of Eastern European countries have e-passport schemes underway or are planning rollouts. Russia has plans to introduce a biometric passport in 2007, while countries in the Middle East, Asia and Africa are extending national ID programs into the passport arena. Other established schemes include Canada with photographs on the chip and Singapore, which met the US Visa Waiver deadline of October 2006, by introducing biometric passports in August 2006.

Growth in National ID

Similarly there is global growth in national identity card programs.

In the EU counties, 10 countries have compulsory ID cards in circulation and a further 10 operate voluntary schemes based on delivering proven benefits to citizens. Of the remainder, Denmark, Latvia, Ireland and the UK currently have no ID cards and debate continues around the cultural and cost implications surrounding their introduction. While privacy activists in a number of countries

question the level and vulnerability of information contained in the chips on both ID cards and e-passports, technologists in the smart card industry are constantly improving data shields and reader protection devices. In some instances new electronic ID schemes are being introduced in parallel with e-passport programs in countries without these programs, and are looking for secure 'state-of-the-art' systems.

Requirements for ID cards and e-passports vary. What are being termed as international obligations to introduce programs, do not necessarily apply everywhere. ICAO and US requirements (apart from standard personal data), demand a digital photograph only, while the EU passport also needs to include two fingerprints by 2008. The French ID card will carry a face template in addition to a digital image while in Spain, the ID card carries no biometric data other than two fingerprints for foreign nationals.

In addition, the ICAO contracting states have recently publicized a 2010 deadline for which all nations shall be issuing machine-readable passports (MRP). Similar objectives focused on the deployment of electronic documents are currently limited to European member states and those countries within the United States Visa Waiver Program. While these countries may constitute the majority of passport volumes worldwide, it must be noted that it has taken some 22 years for the machine-readable technologies to reach today's acceptance level. Smart card industry government scheme integrators hope that the new electronic generation of documents is adopted more readily.

The holding of data in a central register is also an issue for many and policies vary. Currently, there is no central registration requirement under ICAO, EU or US passports guidelines. Indeed in Germany it is illegal to do so, but the French ID card is governed by a centralized system of limited data. In the UK, the jury is still out on this issue for both e-passports and the country's proposed and politically controversial ID card scheme.

All this rapid development is mirrored in other sectors such as finance. In the past, the financial card industry's credit and debit cards had relatively light security needs with magnetic stripes and signatures sufficing. Today, financial cards are highly secure with the introduction of chip and PIN technology, following rapid growth in fraud and criminal activity.

Public and Private Access Control ID is Maturing and Converging

Access control and ID management is maturing in a similar way, albeit with different levels of security need and sophistication. For example, entry to a theme park is relatively low risk compared to allowing access to a secure government institution or bank.

As a result, personalization solutions providers need to assess the needs of customers in terms of risk levels. The key question is whether there is 'value to defraud'. In other words, is it worth breaching a commercial enterprise's security? This can range from ensuring the safety of assets and staff to that of intellectual property and trade secrets.

The need for modularity, holds truer today than it did when the concept was first introduced in the early 1990s. A key consideration is the ability of companies and governments to upgrade security levels and technologies without throwing away their investment. This has led to the development of solutions allowing an enterprise to start low, with the purchase of modules wholly relevant to its business. If its levels of security change, the system can be upgraded to meet the need. This applies to both centralized issuance of large quantities of cards to desktop printers for remote and batch issuance.

The trends affect all industry sectors, from government applications to commercial, education, finance and healthcare, and the need for protection within these sectors is growing. Of these sectors, growth in the government, identity card and secure access market has been the most rapid following the events of 9/11 and other acts of global terrorism. Today, highly sophisticated personalization techniques are a standard requirement for passport personalization.

Modern laser technology can engrave high resolution text and images inside the polycarbonate holder page, making the document extremely difficult to alter or forge. This results in a highly durable passport with secure information. In addition, photographs, text, bar codes, micro-printing, signatures and other graphic elements can be added to the passport's high resolution.

Major Trends Affect Security Management Needs

Similarly, the commercial and business markets have identified needs for higher access security. Solutions providers see three major trends affecting customer assessment of badging and security management needs.

Generic offerings need to become more segment specific, allowing resellers to move away from price competition by adding value through integrated solutions. Segmentation can apply to a customer's specific need for access control, visitor badging, enterprise-wide ID or multi-applications in sectors such as higher education. Convergence of physical and logical security, or ensuring a badging solution is compatible with an organization's IT infrastructure, is critical for maintaining security at the highest level. As a result of this convergence, there is a definite interest from card issuers and end users to implement one ID management structure that bridges both physical and logical security. This means there is a need to agree to a common practice and achieve uniformity across systems in order to install a secure system that works in terms of quality, reliability and integration from the enrolment stage to data management.

The second trend is one of integration of enterprise-wide ID management for organisations that have a number of premises with employees in different locations, both nationally and globally. This often leads to incompatibility of systems in each location, requiring employees and regular visitors to be re-identified whenever they visit different premises.

In addition, with multiple systems from multiple vendors, it becomes difficult and expensive for an organisation to incorporate any new security technology, such as biometrics or digital video, within the enterprise. Even minor integration to other internal systems can be a major development project when customizing each system. This can result in an organisation following a rip and replace strategy, rather than integrating an ID management solution that bridges legacy systems across the business.

Innovative security management solutions for enterprise-wide ID now provide a flexible open platform, making it possible to integrate all existing security systems and incorporate new technologies. This means implementing a single interface for sharing and managing data for access control, identity management, CCTV, biometrics, logical security as well as an open interface to external systems such as human resources.

The third major trend affecting secure card issuance is the development of the badge or ID document from a common commodity into a secure entry pass crucial to the protection of an organization's property, business and staff or in government terms, its borders, public assets and citizens. As a result, cards require a higher level of sophistication in terms of the integration and encoding of smart chips, tamper evident technologies and, in some cases, biometrics. This also affects the card production systems. The issue is no longer merely about how fast a printer works or costs, it is about what technology exists in order to chart risk.

CONVERGENCE OF GOVERNMENT PROGRAMS WITH OTHER CARD SECTORS

Today, secure identity has become a crucial factor in maintaining an organization's security (whether it be government or private sector) not only in terms of physical access, but in ensuring intellectual capital, information, networks and other assets are protected without hindering an enterprise's productivity.

Wi-Fi networks, malicious codes, GPS tracking, industrial enterprise and terrorist threats are factors re-shaping the way business is conducted. And the most pressing question is: How does a business confirm the identity of every individual who interacts with an enterprise?

The same forces influence all area of public and working life including government agencies, colleges, universities, hospitals, leisure establishments, casinos and sports stadiums. Although there are now a host of systems allowing authorized personnel to gain electronic access to premises, unwanted visitors can often beat the system by using any number of public or private channels to enter buildings and systems. This means there is a need to keep one step ahead of fraudsters, criminals and terrorists. The exact nature of secure identity and how to maintain it in a complex organisation needs to be understood.

Identifying the Critical Issues to Secure Safety

In order to achieve business security, several critical issues should be explored so as to identify the most suitable and safe technology and system for any individual business. It is important to realize secure technology as an industry has grown rapidly. There are numerous solutions available and although this rapid innovation increases security, the time and costs involved in choosing the most effective solution, can make planning decisions much tougher and result in an implementation time-lag. This means organizations and governments remain insecure while decisions are being made.

Today's environment requires more than a visual ID which means that an effective point-of-verification requires a failsafe digital solution, driven by a central image database. In this regard, an integrated solution is crucial for security staff to operate effectively.

As card applications addressing a number of security issues, are converging, there are now measurable gains in efficiency, time and cost for consolidating personalization techniques, whatever the application. There is also the concept of 'smart card stovepipes' such as EMV payments, GSM mobile and ICAO travel documents all with relevant standards and centrally-held databases, but there is still a lack of standards for staff ID smart cards, particularly in government departments outside the US.

US homeland security directive for standards in ID cards, following the 9/11 attacks, demonstrated the speed at which governments could move when provoked. Elsewhere there are potential benefits for personal identity verification (PIV) standards for areas requiring high security where a standard would help. Public servants can hold cards for access to a variety of government services such as social and family affairs, benefit collections, travel and staff access that would not compromise privacy issues.

Exploring the Citizen-Centric Option

Cards could be introduced for citizen-centric reasons rather than for security in combating terrorism and crime. Similarly developments in drivers' license security mean license cards are likely to be replaced with more robust features including a smart chip. This is widely anticipated for the EU once agreements have been reached on standards for smart drivers' licenses, planned for issuance by 2009.

CONVERGENCE OF GOVERNMENT PROGRAMS WITH OTHER CARD SECTORS

There are also public/private initiatives underway around the world, bringing together private and public sectors, including police forces, in order to establish quality control for identity management. Discussions, particularly in the UK, are surrounding public and private sector convergence, consumer protection, identity theft, international best practice and legislative barriers. Main themes include consumer benefits and public-private partnerships. Meanwhile in local government there is a drive to collaborate on citizen card connections, including the role of smart cards and joining up applications for schools, public transport, healthcare libraries, leisure and local authority payment schemes.

Conclusion

Developing an integrated, secure solution is an absolute necessity. Photo ID cards with smart chips, biometrics, radio frequency and other technologies, combined with a centralized database, provide a range of benefits in security and productivity that no card or secure document issuer can afford to ignore.

The card industry expects to see an increase in the number of technologies that work together on a single card or document to produce a highly secure product. These would include features such as secure digital photographs and ghost images, microprint and UV as well as overt and covert technologies, including biometrics. As the technology becomes more complex to ensure issuers' authenticity, making it more difficult to falsify documents and cards, issuers will take multiple technologies and implement them to ensure holder authenticity. This is already being played out in government circles and will extend to the corporate sector as well as other markets such as transport and healthcare.

As cards become more sophisticated, people will need a higher level of training to guarantee legitimacy. This will ensure that credentials are sound and breeder documents such as birth certificates are verified to underpin the legitimacy of secure documents, passports and benefit cards. The strategic approach is to stay close to customers and governments around the world in order to align their security interests. As this is also driven by international standards, major players in this complex industry need to direct and establish their thought leadership to uphold these specifications and ensure full security is maintained.