Challenges and opportunities in identity assurance

March 2008

Sir James Crosby

Challenges and opportunities in identity assurance

March 2008

Sir James Crosby

HM Treasury contacts

This document can be found in full on our website at:
www.hm-treasury.gov.uk

If you require this information in another language, format or have general enquiries about HM Treasury and its work, contact:

Correspondence and Enquiry Unit
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Tel: 020 7270 4558
Fax: 020 7270 4861
E-mail: public.enquiries@hm-treasury.gov.uk

Printed on at least 75% recycled paper.
When you have finished with it please recycle it again.

ISBN 978-1-84532-391-2

PU186

Contents

Summary

In July 2006, our Public-Private forum was asked by the Chancellor to consider how the public and private sectors might work together in identity (ID) management for their mutual benefit and that of citizens and consumers.

Identity is "the new money"

There is nothing new in the importance of being able to prove our identity. The first passports were issued almost 600 years ago. But today, as our lives become more peripatetic and our dealings more rarely face to face, it is ever more important for each and every one of us to be able to assert our identity with ease and confidence.

Many hundreds of years ago, coins and notes facilitated trade between parties who didn't necessarily know each other. People put their trust in money, and trade multiplied many times. Now the rapid growth in remote "transactions" (by post, on the telephone, and over the internet), and the advent of many more processes that specifically call for identity to be verified in the public or private sectors, are significantly increasing the need for individuals to be able to assert their identity. As is still the case with money transmission today (for example the replacement of cheques with "Chip and PIN" cards), as ID systems improve and consumers' confidence grows, so we will continue to see rapid growth in demand for such systems.

It's the consumer's identity

At an early stage, we recognised that consumers constitute the common ground between the public and private sectors. And our focus switched from "ID management" to "ID assurance". The expression "ID management" suggests data sharing and database consolidation, concepts which principally serve the interests of the owner of the database, for example the Government or the banks. Whereas we think of "ID assurance" as a consumer-led concept, a process that meets an important consumer need without necessarily providing any spin-off benefits to the owner of any database. This distinction is fundamental. An ID system built primarily to deliver high levels of assurance for consumers and to command their trust has little in common with one inspired mainly by the ambitions of its owner. In the case of the former, consumers will extend use both across the population and in terms of applications such as travel and banking. While almost inevitably the opposite is true for systems principally designed to save costs and to transfer or share data.

The importance of ID systems extends well beyond commercial transactions. In practice, the quality of such systems determines the extent to which many desirable social goals, including border controls and restricting employment to those entitled to work, can be achieved. Indeed, an ID system will only help fulfil national security goals if it achieves mass take up and usage. If citizens don't use a system regularly, it will be capable of providing very limited data for national security agencies. Thus, even the achievement of security objectives relies on consumers' active participation.

Significant economic and social advantage ...

It follows that those countries with the most effective ID assurance systems and infrastructure will enjoy economic and social advantage, and those without will miss an opportunity. There is a clear virtuous circle. The ease and confidence with which individuals can assert their identity improves economic efficiency and social cohesion, which in turn leads to a greater number of transactions being reliant on such ID systems, further enhancing delivery of economic and social goals. As with money, the prospect is therefore one of lower costs per transaction coupled with a multiplier effect in terms of increased volumes of transactions.

... is available through "universal" ID assurance schemes

Equally, ID assurance systems which are in almost constant use by a very large proportion of the population across a wide range of applications offer the greatest potential for economic and social advantage. Frequency of use underpins assurance levels, it being no coincidence that fraudsters routinely target the identities of the deceased. At the same time, ubiquity builds familiarity among consumers. Almost by definition, their appeal to consumers lies in the superior levels of assurance they deliver. The criticality of such systems to everyday life also means that they must have hassle-free services for repairing compromised identity and replacing tokens. Almost inevitably, such "universal" ID assurance systems will be created by consumers for consumers. And like SMS messaging and Google usage, they will evolve over comparatively short time periods.

... which also deliver the strongest security outcomes

Provided the universal ID assurance system infrastructure embraces public services, banking, transportation and e-commerce, it will produce an unrivalled amount of data for national security agencies. Ironically therefore, the system that is genuinely consumer led because it meets consumers' needs and inspires their trust would deliver a better national security outcome than one with its origins explicitly in security and data sharing across government.

"Universal" schemes demand high quality assurance which calls for ...

Identity can be an overly technical topic. Ultimately, however, the quality of assurance achieved by any system is down to the quality of enrolment onto the system and the resilience of any subsequent verification process.

... a combination of biographic and biometric data ...

Even in 2008, it is the biographical data (name, address, date of birth, credit reference entry, etc) that largely defines the identity that consumers need to assert with ease and confidence. Almost regardless of the technology deployed, the highest levels of assurance are achieved on enrolment by cross checking a number of biographic databases. Biometric data (photograph, fingerprints, etc) will add value in ensuring that individuals appear only once on any ID database. It is also indispensable in ensuring good performance when re-issuing tokens or repairing identity. But precisely because it can't be a complete substitute for biographical data, it isn't the silver bullet.

... and a number of "independent" verification factors ...

Regardless of the technologies deployed, the resilience of verification processes is driven by the number of independent factors presented by an individual seeking to have their identity verified (e.g. something you have (a token), something you know (a PIN number), and something you are (a photograph)), and it is the combination of such independent factors, rather than their technological complexity and individual strength, which largely determines the resilience of the verification process. For example, subject to the quality of enrolment, an ID card which substantially consists of a "Chip and PIN" card with a photograph will deliver superior assurance through its use of three factors to the two factor "Chip and PIN" card.

... with scale being the critical success factor

ID assurance systems that cover a large number of people who use them across a range of applications (universal systems) can justify the cost of extensive cross checking of biographic data and the heavy investment required to establish and maintain biometric databases and related infrastructure. But scale, as measured by frequency of use, really is the defining advantage of the universal identity assurance system. Whatever the complexity of the system, high frequency of use encourages familiarity and hence ease of use. It also ensures that any token is closely guarded by its owner and that customers themselves (in very large numbers) effectively police assurance levels and fraud.

The UK is witnessing a proliferation of ID schemes ...

In the UK, and emanating from both the public and private sectors, consumers are experiencing a proliferation of ID systems and techniques of uncertain quality. Utility bills, passports, bank cards, driving licences, and endless supposedly different "usernames" and "passwords" all play their part. Such a haphazard array of assurance techniques has resulted in a degree of complexity for consumers that is becoming another source of social exclusion, typically affecting the elderly and socially disadvantaged. In general, businesses and government departments and agencies have designed business-centred systems, largely, but not exclusively, in isolation from one another.

... with common standards the preserve of the banks

With the most to lose financially, and therefore the greatest incentive to invest, banks have adopted common standards and established the most effective mass ID infrastructure in the UK through "Chip and PIN" cards for "face-to-face" transactions and most recently, hand-held card readers for internet transactions. Within the "banked" sector of the population, this infrastructure and system enjoys frequent usage and high levels of trust.

... inconsistent results in the public sector (particularly in relation to employee verification) ...

So far, the wider public sector, including agencies and local authorities, has been uncoordinated in its approach to the provision of ID systems. Indeed, it is on the verge of launching many different new ID tokens. Passports and driving licences are well established tokens of trust, but within five years, some citizens could have a wallet full of rarely used public-sector ID tokens. But despite all these initiatives, the public sector's limited capability in ID assurance systems means that it still struggles to achieve many core policy objectives, such as policing benefit claims. Perhaps the worst example is employment. Here it is the Government that is largely responsible for the panoply of ID assurance-related requirements that employers must satisfy for each new employee. And yet it is the

quality of the broader public sector's data systems (e.g. National Insurance numbers) and services (e.g. Criminal Research Bureau checks) which make it so expensive and difficult for employers to comply, particularly small businesses. This is bad for industry's costs, labour market flexibility, and the policy objectives linked to employee identity verification. There is a strong case for the Government to take the necessary steps to ensure that all employers, large or small, can verify employee's identity quickly and accurately.

... and a rapid growth in identity fraud

As individuals have become more and more reliant on ID assurance systems, so we have seen a rapid increase in identity fraud. A Home Office review concluded that the losses arising from ID fraud in 2005 were £1.7 billion. As identity fraud has risen, both government and the banks have established all sorts of initiatives to record and combat such fraud, most obviously the National Fraud Strategic Authority envisaged by the then Attorney General in 2006. However, consumers and citizens have a much narrower interest in such fraud, a need which until recently has been ill served. The new initiative by the National Consumer Council and the three Credit Reference Agencies to offer identity repair services for free, in relation to credit reference data, should be seen as only the first step in tackling identity theft from the perspective of consumers and citizens. It should be actively promoted to customers and ultimately developed to provide a broader service embracing other forms of identity across the public and private sectors.

The marketplace is not delivering the best outcome for consumers

In the UK, market forces are presenting citizens and consumers with an ever increasing array of ID systems of unknown quality, often with limited frequency of use and invariably the subject of increasing amounts of fraud. Set against the ideal of the universal ID assurance system created by consumers for consumers, this suggests that the market place is not about to deliver the best outcome for consumers.

Experience outside the UK highlights ...

Our research outside the UK identified no single large-scale ID assurance schemes which, if emulated in the UK, could reasonably be expected to be the catalyst for the creation of a truly consumer-led universal scheme.

... the limitations of ID cards issued as "security" tokens ...

Almost all ID cards or related schemes elsewhere have been inspired by a state's own requirements, invariably connected to security. However, more recently, for example in Australia and Ireland, there is evidence of such schemes being designed or redesigned to inspire much higher levels of consumer trust. While some ID cards schemes deliver a high level of assurance (variously the result of history and culture or a particular technology), relatively few have any links into core banking systems and taken together they embrace a wide variety of processes and technologies with no near term likelihood of any common standards being established.

... and the importance of banking systems and standards

In contrast, banks have generally adopted common standards and invariably use ID assurance techniques that operate internationally. By definition, their cards have very broad application (all purchases through all channels), benefit from frequent use, and enjoy the care and protection of

their owners. It is also clear that banks will always have the need to invest heavily in new and more effective ID assurance systems. Their ability to invest in and introduce such improvements at speed is likely to continue to exceed that of the public sector, at least in most countries. Even so, it is important to remember that banks' systems don't extend to an important minority, the "unbanked", and that they set their own levels of assurance to accord with their own exposure to loss. A successful universal scheme must achieve broader coverage of the population and achieve superior levels of assurance to that which underpins routine banking transactions.

To realise the greatest economic and social benefits every aspect of an ID card scheme should be designed from the consumer's perspective …

The Government has clearly stated its intention to introduce ID cards in the UK. It has passed enabling legislation and the Home Office has set out its plans to launch the cards in its Strategic Action Plan (2006). I have no remit to comment on the desirability or otherwise of this plan. However, in my opinion, the Strategic Action Plan (2006) will not be the catalyst for the emergence of the consumer-driven universal ID assurance system envisaged by this report. For that to be the case, I believe the design of any ID card scheme would need to be based on the following ten broad principles:

1. **The purpose of any scheme should be restricted to that of enabling citizens to assert their identity with ease and confidence.** The scheme should set targets for the quality of assurance achieved at enrolment and verification, which should generally exceed those achieved elsewhere, and it should regularly report its performance against those targets.

2. **The scheme's governance should be designed to inspire the highest level of trust among citizens.** It should be operated independently of Government (say, accountable directly to Parliament) and in principle its processes and security arrangements should be subject to the approval of the Information Commissioner, who should have the power periodically to review delivery.

3. **As a matter of principle, the amount of data stored should be minimised.** Full biometric images (other than photographs) should not be kept. Only non-unique digital representations of biometric images should be stored. Additional data accessed during enrolment and records of verification enquiries should not be retained. All data and systems should be protected by "state of the art" encryption technology.

4. **Citizens should "own" their entry on any register** in the sense that it should not be possible, other than for the purposes of national security, for any such data (to include digital representations of biometrics) to leave the register without their informed consent. Verification of identity should be performed without the release of data.

5. **Enrolment processes should be different for individuals with different circumstances, and change over time** so as to minimise costs and give citizens the simplest and most hassle-free experience consistent with the achievement of the published assurance targets.

6. In order to respond to consumer demand and achieve early realisation of economic and social benefits, **the scheme should be capable of being rolled out at pace**.

7. **Citizens who lose cards or whose identity is compromised should be able to rely on their cards being replaced or their identity being repaired quickly and efficiently** and in accordance with published service standards.

8. Technically **the scheme's systems should be closely aligned to those of the banks** (both initially and in the future) so as to utilise their investment, de-risk the scheme's development, and assist convergence to common standards across the ID assurance systems and processes deployed internationally by banks and other national ID card schemes.

9. To engage consumers' hearts and minds on the scale required, **enrolment and any tokens should be provided free of charge**.

10. **The market should play a role in delivering a universal ID assurance scheme**. This will improve the ease with which consumers can use the scheme and minimise costs.

I regard each aspect of these principles to be critical to the goal of creating the conditions for a consumer-driven universal ID assurance scheme to emerge and flourish.

Action on verifying employee's identity and identity repair services is essential ...

Quite legitimately, the Government may not regard its ID cards scheme as the best way to stimulate the creation of the universal ID assurance system as envisaged in this report. Even if this is the case, I strongly recommend:

1. Working with the private sector, Government should take all necessary action to ensure that, as soon as possible, consumers have access to a "one stop" agency for the swift repair of compromised identities across the public and private sectors; and

2. Government should commit to the development work across public sector databases necessary to ensure that all employers can quickly and confidently satisfy "right to work" and related regulations for all their employees.

In conclusion ...

In the absence of a universal ID assurance system, I believe consumers will have to grapple with an increasingly complex array of identity assurance processes of uncertain quality. As a result, the UK will fail to secure the economic and social advantage achievable at the forefront of ID assurance systems and processes. In a competitive world, any failure to secure advantage quickly becomes tantamount to locking in disadvantage. In other words, the opportunities inherent in ID assurance will not have been grasped but the challenges will remain.

I am particularly grateful to those public and private sector colleagues (listed in Annex A) who so willingly gave their time to serve on the Forum. We were also fortunate that so many individuals from outside the Forum were able to input to our work. Specialist consultants and innovators in ID matters, technology providers, special interest groups, and many users of ID assurance systems all made important contributions. Most of all I want to record my thanks to the officials in the Treasury and the Home Office who have been so tireless and patient in their support. In conclusion, I should however stress that the views expressed in this report are mine.

James Crosby
March 2008

1 Identity assurance in theory

Summary

- ID assurance meets a clear and growing consumer need whereas "ID management" addresses the interests of the owners of any identity database.
- Cross checking biographic databases, where possible underpinned by biometrics, gives the strongest assurance at enrolment.
- Biometrics help ensure a register contains no multiple records and facilitate token re-issue and identity repair.
- The quality of verification is the result of the number of independent factors presented in verification.
- Both the hardware and software (particularly encryption) will change over time as any ID assurance system invests to sustain its chosen level of assurance.

INTRODUCTION

1.1 In July 2006, a Public-Private forum was asked by the Chancellor to consider how the public and private sectors might work together in identity management for their mutual benefit and that of their citizens and consumers.

1.2 The key element in common between the public and private sectors is the consumer, and in order to answer the question set, the forum moved its focus to "ID assurance" rather than "ID management". The difference between these two concepts is explained below, but essentially, it is ID assurance that is best placed to meet a consumer's needs and to deliver mutual benefit to public and private sectors as well as to citizens.

WHAT IS IDENTITY ASSURANCE AND WHY IS IT IMPORTANT?

1.3 In order to conduct commercial and government business over any distance, it is necessary to demonstrate who one is beyond one's immediate circle. ID assurance is a consumer-led concept in which people prove who they are to others, be they retailers, financial institutions, domestic or foreign governments, etc.

1.4 The "identity" an individual seeks to assert is not their physical being as such, but rather an informational representation of the chain of life events that is defined by who they are. The particular events of relevance depend on with whom the individual is dealing and will lead to different entitlements. To a bank, a customer needs to assert that they are the person who opened an account and are therefore entitled to access the funds within it. To the Department for Work and Pensions, the individual needs to prove that they are the person who is out of work and therefore entitled to receive a benefit.

1.5 All customers will be concerned to protect the integrity of their personal data, but they will vary in the extent of privacy protection they demand. Some may wish to seek the potential benefits of 'joined-up government' and share their personal data across departments, if they are assured of the security of their data. Others will favour privacy over convenience and will prefer not to share any personal data. Ideally, ID assurance schemes should provide options and enable customers to make informed choices.

1.6 ID assurance is not ID management, in which an organisation keeps a close track of people and their movement. The distinction between the two is fundamental. ID management is designed to benefit the holder of the information. ID assurance is focused on bringing benefits to the consumer.

1.7 As a result, although the technology employed to achieve ID assurance and management may be similar, the end design of the system is likely to be very different. An ID assurance scheme built primarily to deliver high levels of assurance for consumers will address issues, such as the amount and type of data stored and the degree to which this information is shared, differently to one inspired mainly by the needs of its owners.

1.8 In any ID assurance system, the more regularly it is used, the more secure it becomes. As people use the system they check whether it is corrupted, and the more they do this the more it can be trusted. If a consumer uses a card frequently, he/she has an incentive to maintain its integrity and to keep the card and its PIN safe. Patterns of regular transaction activity make it easier for fraudulent activity to be identified and proven. This is demonstrated by the fact that some of the most common targets for identity theft are the deceased.

1.9 Importantly, there is no magical solution for ID assurance, and the quicker new solutions are developed, the quicker fraudsters will find ways to abuse them. All ID assurance systems will have to invest in new techniques and processes to maintain target levels of assurance. Any automated system needs to have a level of tolerance built in and the levels of assurance sought must be carefully balanced against the risk.

HOW DOES IDENTITY ASSURANCE WORK?

1.10 At its core, an ID assurance scheme involves enrolling consumers and verifying their identity to other organisations. Typically, an ID assurance scheme will store personal information in an ID register. All ID assurance schemes rely on someone or something that is independent of and trusted by both sides, such as a bank (debit cards) or the government (passports).

Enrolment

1.11 At the enrolment stage, a customer proves who they are by providing details of their identity. The steps of this process are:

1. individual asserts the existence of an identity;
2. provider determines the uniqueness of the identity;
3. individual confirms ownership of the identity;
4. the identity is created in the scheme; and
5. a means of binding the individual to the scheme identity is established for verification purposes (e.g. token is issued).

1.12 Two types of data are important at this stage: biographical and biometric.

1.13 **Biographical data** defines our identity and includes: personal details, such as name, date of birth, address (past and current); credit reference information; and other behavioural data. It tells the story of the person's past and current life and is the anchor of any ID assurance system.

1.14 Cross-referencing biographic databases at enrolment gives the highest levels of assurance. "Identity authenticator" companies check biographical data against trusted third-party sources. However, some of the most important and trustworthy sources of data are in the public sector and are not available to identity authenticators. These include: the Identity and Passport Service (passport data); Driver and Vehicle Licensing Agency (driving licence data); and Department for Work and Pensions (benefits and pensions data).

1.15 The 2006 Identity Cards Act allows these public sector sources to be used to authenticate a person's identity when an individual applies to be recorded on the National Identity Register (NIR).

1.16 Identity authentication through biographics does not, however, provide proof of uniqueness of an identity. For this, biometric data is required.

1.17 **Biometric data** can be used to physically and uniquely identify a person, and includes: a photograph; fingerprints; iris/retinal patterns; and voice patterns.

1.18 A biometric tells us little about the individual, but it can reduce duplication. When a new individual enrols into an ID assurance scheme, the system can confirm that no other records for that individual already exist, deterring fraudsters from using multiple identities to defraud others or avoid state controls.

1.19 Biometric data links an individual to their biographic information and enables efficient re-issuing of tokens or repairing of identity. But biometric data is not a substitute for a rich source of biographical information and provides no "silver bullet" in identity assurance. Neither is biometric data impregnable; fingerprints can be replicated from prints left on certain surfaces. Even aside from fraudsters' attempts to abuse the integrity of the system, biometric technologies do not work precisely 100 per cent of the time and biometric characteristics will adjust due to age and environmental changes.

1.20 Pure biometric images are irreplaceable as, once compromised, citizens can't acquire new fingerprints. However, in the case of fingerprints the database need only store one of a number of non-unique digital representations (a collection of points on the print) which can, if needs be, be replaced by another non-unique representation. The uniqueness of each entry on the database arises from the combination of the biographic data and the inability of anyone to reproduce any of the non-unique representations of a particular fingerprint without first owning that print.

Verification

1.21 At this stage, the individual needs to prove that they are the person who enrolled in the scheme in the first place.

1.22 Traditionally, a single token (e.g. paper driving licence) was used to verify identity. Possession alone was enough to prove entitlement. This "single factor" security has the advantage of being simple to implement and easy for users to understand.

1.23 Plain tokens can be adequate for low risk situations such as library cards, but where the presentation of a token can unlock benefits of value to a fraudster (e.g. a debit card), then additional confirmation is required.

1.24 In higher security situations such as bank transactions, strong "two factor" security – where the user has to produce the token and PIN number or password – is now common. It helps to reduce the incidence of crime by providing two independent and robust forms of security that a fraudster must crack. The most common example is "Chip and PIN", described in more detail in the next chapter. Chip and PIN has replaced the signature on a card, which was relatively easy to forge and therefore a weak second factor layer of security.

1.25 The most robust identity assurance techniques involve three or more factors. Typically, a three factor identity assurance technique checks:

- something you have (e.g. a card or other token);
- something you know (e.g. a PIN or password); and
- something you are (e.g. a picture or other biometric such as fingerprints).

1.26 Three factors produce a significantly stronger identity assurance technique. Fraudsters find it considerably more difficult to simultaneously replicate something you have, something you know and something you are. So much so that three relatively weak factors almost always produce a far higher level of identity assurance than a single strong factor. Three "independent" factors that individually provide 90 per cent assurance will provide 99.9 per cent assurance if used in conjunction[1].

1.27 It is important that each factor can be renewed if compromised. Lost tokens can be replaced. PIN numbers can be changed. Even biometrics such as fingerprints can be replaced provided they are not stored in their entirety (see 1.20 above).

1.28 Levels of assurance can be raised by strengthening an individual factor as well as by adding a second or third factor. For example, adding a fingerprint biometric to a photo card enhances the "something you are" factor.

[1] In mathematical terms, 90 per cent assurance means that there is a 10 per cent failure rate, but provided the risks of failure under each factor are uncorrelated (i.e. the factors are independent), three factors of 90 per cent assurance equates to a 0.1 per cent failure rate overall (0.1 x 0.1 x 0.1 = 0.001).

1.29 In practice, identity assurance techniques, whether single or multi-factor, will be reinforced in circumstances where the costs of failure are most significant. Providers and consumers will be encouraged to invest in and maintain, respectively, a system that protects against a commercial or personal material loss.

WHAT PART DOES TECHNOLOGY PLAY?

1.30 Numerous technologies are already in common use in identity assurance, for example Chip and PIN cards or iris recognition at airport immigration. Over time, the tokens typically used will change, perhaps from Chip and PIN cards to SIM cards in mobile telephones; the nature and level of encryption used in communication will certainly be enhanced.

1.31 Changes in technology will facilitate the strengthening of one or more of the independent factors used in verification. The managers of any ID assurance system should be investing in such changes so as to ensure they continue to achieve the chosen levels of assurance at the most affordable cost.

1.32 Quite separately, the choice of technology and related tokens should take account of which processes will be familiar or readily accessible to the largest number of individual users of that system. This is particularly the case for any ID assurance system which aspires to be consumer driven.

The principles are more enduring than any one technology

1.33 The principles underlying ID assurance will endure; namely the role of biographic and biometric data in enrolment and verification and the use of independent factors in the case of the latter. However, the technology deployed, be it hardware or software, will evolve over time.

2 Identity assurance in practice

Summary

- Many public and private sector organisations are engaged in ID assurance schemes.
- The proliferation of such schemes, most noticeably in the public sector, is resulting in duplicate effort and expense for providers, and complexity for consumers.
- The banks have made the most progress to date in implementing common standards and an effective mass infrastructure.
- Building on the banks' investment, there is an opportunity for Government to establish a single, universal ID assurance scheme.

2.1 Almost every organisation consulted during this review, be it private corporation or public sector body, is engaged in an ID assurance scheme of some kind. In the absence of any standard, universal solution, organisations are creating their own solutions. These vary from simple tokens that enable people to prove entitlement, to more complicated tokens (e.g. security passes) that facilitate more sophisticated identity assurance.

2.2 The financial services sector has made the most progress in ID and has established common standards and the most effective mass ID infrastructure in the UK. Other industries, such as travel, are following suit.

2.3 But the proliferation of schemes emanating from private and public sectors results in duplication of effort, and increasing complexity for consumers. The public sector already has at least seven major programmes issuing two-factor identity tokens, and examples of these public sector schemes are described below. The nature of the service to be delivered (from driving licences to benefits) may vary, but the challenge and potential solutions for proving identity are similar.

IDENTITY ASSURANCE IN THE FINANCIAL SECTOR

2.4 The financial services sector has a large incentive to invest in ID assurance. Banks, for example, need to be certain of whom they are dealing with, particularly in transactions of significant value. As banks have a duty to underwrite any fraud losses that their customers suffer through the banking system, they have a strong interest in ensuring the integrity of their verification systems. All financial organisations regulated in the UK also need to comply with government regulation, for example on money laundering.

2.5 As a result, the financial services sector has made the most advances in ID assurance, incorporating new technologies and tailoring their systems to the risks they face (fraud on the one hand and customer inconvenience on the other), and to the costs of implementation. Banks draw on multiple sources of an individual's biographic data when they sign up a new customer. They then carry out sophisticated techniques before each transaction to verify that a customer is genuine. The UK banks have made considerable progress in achieving common standards and an effective mass infrastructure in ID assurance through the use of Chip and PIN cards for face-to-face transactions and hand-held card readers for remote transactions.

Signing up a new customer – biographic checks

2.6 Banks perform *enrolment* checks to establish that a new customer will repay any loans. A customer's credit information is cross-checked against the electoral roll, or similar source, to confirm that this history is tied to a genuine person. This combination of biographic database checks gives the banks a sufficient level of assurance for them to lend against. The level of assurance sought will increase for high value or high risk transactions.

Protecting against fraud – Chip and PIN

2.7 To mitigate the risk of fraud losses, the banks have had to find increasingly robust ways to identify their customers, who now access their accounts by machine, over the telephone, or via the internet.

2.8 At the forefront of large-scale secure identity assurance, banks have to consider the following when developing new secure methods of authentication:

- the increasing risk of fraud, including through new business channels (e.g. internet banking);
- the cost of changing their systems to mitigate against that risk; and
- the impact on their existing customers.

2.9 The most widespread recent innovation has been the move from a signature to Chip and PIN security[1] (see box below). This has two key benefits: the card can be authenticated securely; and the PIN code can be checked automatically, minimising operator error.

Chip and PIN

Credit and debit card transactions in shops and restaurants used to be verified by signature. The system had a number of security flaws that were increasingly being exploited by criminals. A thief had a window of opportunity to use a stolen card and forge the card owner's signature before the card was reported stolen. The shop assistant had to judge whether the foil signature matched the card signature – and an embarrassing challenge to the customer resulted if it didn't.

The introduction in 2006 of Chip and PIN to the UK removes such ambiguity: the PIN must be entered correctly for the transaction to be authorised. The thief must steal or replicate both the physical card itself and the PIN associated with it. It therefore strengthens one of the layers of security – a PIN cannot be forged.

Credit and debit card transactions are still a target for thieves and fraudsters, but the introduction of Chip and PIN has resulted in a significant decrease in fraud conducted in face-to-face transactions in the UK from a peak of £218.8 million in 2005 to £72.1 million in 2006.

Source: APACS – Fraud the Facts 2007.

[1] See Chapter 1 for a description of single and multi factor security.

Further innovations to protect against fraud – hand-held card readers

2.10 While fraud in standard face-to-face card transactions has diminished rapidly since the introduction of Chip and PIN, 'card-not-present' fraud[2] has accelerated as consumers move to remote shopping and carry out more card-not-present transactions. This is now the largest plastic card fraud category according to the UK Payments Association (APACS) and cost more than £212 million in 2006.

2.11 Visa and MasterCard introduced password-based systems into their card-not-present transactions[3] to try to address this new type of fraud. However, passwords communicated via the internet or the telephone are vulnerable to theft by eavesdroppers or intermediaries to the transaction.

2.12 In 2007, certain UK banks[4] introduced a card reader that enables remote card authentication for online and telephone-based transactions. The reader verifies the card using the PIN and then generates a unique key, strengthening the "something I have" and "something I know" element of security. It allows the consumer to assert, even from a distance, that they are in possession of the genuine card and not, for example, just the details of that card.

2.13 Anecdotal evidence suggests that customers were initially reluctant to use this form of technology but are gradually adopting it. Remote card authentication is proving to be successful in reducing fraud and is likely to become the next banking 'standard' in identity assurance. The box below provides further details.

Remote card authentication for online and telephone-based transactions

The challenge with online banking or telephone transactions is being sure that the person in possession of the card is the genuine owner and not a fraudster. To combat this, the banks have issued a hand-held card reader (resembling a pocket calculator) that can validate the card's chip against a PIN.

The reader generates a unique, up to 12 digit, password that changes every time. The customer says the password to the telephone operator or keys it into the web page. Using encryption technology the bank can be certain that the card is genuine. Both the PIN and the encryption key operate on a standalone piece of technology that can't be accessed by online hackers.

This is currently being trialled in online banking. To carry out a secured banking transaction, the user therefore needs to:

- know details of customer account or 'private' facts, e.g. first school;
- be in possession of the genuine bank card and the card reader; and
- know the card's PIN number.

The reader is cheap to produce (around £2.50) and secure because it does not need to connect to the computer.

[2] The abuse of remote transactions over the telephone or internet in which a physical card cannot be validated.
[3] "Verified by Visa" and "SecureCode".
[4] Barclays, Royal Bank of Scotland (including NatWest) and Nationwide have all rolled out the hand-held device in significant numbers.

IDENTITY ASSURANCE IN TRAVEL

2.14 There is a strong business imperative to be clear on identity in the travel industry. This is true for a number of reasons. On commercial grounds, a transport company wants to be certain, particularly in high-value travel, that the passenger is entitled to their ticket. There is a risk, too, that if the passenger is not who they say they are, they may not be accepted at a border and the transport company will be legally obliged to take them back.

2.15 Importantly, if passengers can assert their identity with ease and confidence, their overall travel time will be reduced. As well as enhancing the customer experience, this can reduce costs (e.g. airport staff costs) for the transport company and boost revenues – a favourable journey is likely to encourage a customer to choose that travel company again.

2.16 On security grounds, verifying identity can be useful in limiting access to restricted areas (such as airside) and in providing reassurance that the ticket holder is unlikely to pose a threat to the safe passage of other customers and staff. But perhaps the most important security benefit of a robust ID assurance scheme is the automation it supports. The smooth and quick movement of passengers through a port can free up staff time as well as consumer tolerance for enhanced security checking procedures.

2.17 Some examples of successful ID assurance schemes in the travel industry are outlined below. In each case, the scheme improves efficiency, enhances the customer experience, and has knock-on benefits for security.

Machine readable travel documents

2.18 The travel industry has developed minimum standards for international travel documentation (the International Civil Aviation Organization or ICAO standards). The most recent ICAO standard requires that travel documents have a machine-readable strip and a biometric. Facial recognition is the primary biometric with iris and fingerprint as backup (but optional) biometrics. Machine-readable documents are harder to forge and enable faster border control, improving security as well as efficiency of travel.

Electronic ticketing systems

2.19 Electronic ticketing systems can prove that a ticket is validly issued to an individual and, as such, are a form of identity assurance. They are widely used in the airline industry and, increasingly, in public transport and at sports and other events.

2.20 The savings generated for the company from this trusted automated ticketing system are significant. The International Air Transport Association (IATA) estimates that an e-ticket costs US$1 to process versus US$10 for a paper ticket[5]. This equates to an overall efficiency saving to the airline industry in the order of $3 billion a year.

2.21 The use of electronic tickets can also reduce costs in time and money for consumers. The IATA has mandated that all airlines introduce electronic ticketing by 31 May 2008.

[5] *IATA Factsheet: Electronic Ticketing* – http://www.iata.org/pressroom/facts_figures/fact_sheets/e-ticketing.htm.

Iris Recognition Identity Scheme (IRIS)

2.22 IRIS enables registered passengers to avoid the queues at UK passport control. Instead of waiting to see an immigration officer, individuals enrolled on the scheme walk up to an automated barrier, look into a camera, and if the system recognises them, enter the UK.

2.23 The biometric technology works by photographing and storing a passenger's iris patterns in a database, and linking them securely to their passport details and immigration status in the UK. Enrolment takes around ten minutes. Once enrolled, each verification check takes around 25 seconds.

2.24 The IRIS system has around 170,000 registered users and has facilitated around 850,000 crossings, so it is still in its early stages. Anecdotal evidence varies, but so far, it appears to be a quick, fast and secure way to verify passenger identity.

IDENTITY ASSURANCE IN THE PUBLIC SECTOR

2.25 The identity management issues faced by the public sector are significant. The collection of revenues and delivery of services at a local and national level by the public sector accounts for around 42 per cent of the UK's Gross Domestic Product[6]. Each public sector function must have a sure means of identifying customers so that revenues are correctly attributed and services are only provided to those entitled to them.

2.26 Government departments are increasingly investing in identity assurance solutions to enable the delivery of personalised services through new channels (e.g. over the telephone and online). Many are seeking solutions to provide "strong" identity assurance. A number of examples are provided below: the Driver and Vehicle Licensing Authority (DVLA) and a number of local authorities are introducing sophisticated cards to address their ID assurance problems; the Department for Work and Pensions (DWP) is using rich biographic questioning to confirm the identity of their customers.

Driver and Vehicle Licensing Authority (DVLA)

2.27 The driving licence is a good example of a widely used and trusted identity token in the public sector. The photocard driving licence was introduced in 1998 and is now the most common means of identification within the UK, covering 28 million individuals.

2.28 The DVLA are constantly looking to upgrade their card. In June 2007, the licence format was changed to include a range of new security features. Building on the banks' success, the DVLA are introducing three-factor security provisional driving licences that include Chip and PIN as well as a photograph.

2.29 The DVLA scheme is the closest the UK public sector has got to an ID card which has some of the characteristics of a universal ID assurance scheme.

Local authorities

2.30 Responsible for the delivery of a wide range of services to local residents (from library facilities to housing), local authorities need a trusted means of identifying those people in their area who are entitled to specific services and benefits.

[6] But note that this covers all services, not just personalised ones.

2.31 Traditionally, local authorities have used many different ID assurance mechanisms, rendering it necessary for the customer to present different documents on each occasion.

2.32 Some authorities, as a means of streamlining their identity assurance schemes, are looking to "smart cards" (cards with an embedded microchip) as the answer[6]. The card enables local residents to prove their identity in multiple circumstances with the same token. Local authorities may need tailored solutions but a single universal ID assurance system could provide a realistic alternative to multiple standalone schemes.

Department for Work and Pensions (DWP)

2.33 DWP is responsible for delivery of the benefits available through the UK's welfare system. Benefits account for 21 per cent of government spending, and are increasingly being delivered through the internet. The Department's Customer Information System (CIS) holds a record for the vast majority of UK citizens, and many of the foreign nationals that have resided in the UK for a long period of time.

2.34 The Department needs a strong ID assurance solution to protect the Department from fraudulent benefit applications. But it also needs a system that is customer friendly to those who are often the most disenfranchised in society. DWP is currently exploring ways to improve its systems and expand the services it can offer remotely.

The ID assurance challenge for the public sector

2.35 There is no reason why solutions shouldn't be tailored to meet the needs of different departments. But there is considerable overlap in the challenges faced, and inevitable duplication in investment in standalone solutions. There are signs that departments are starting to work together, but there is too little sharing of best practice and not enough progress in building common infrastructure and adopting common standards.

2.36 This lack of public sector coordination in identity assurance is likely to lead to a sub-optimal service for consumers and duplication of effort and expense for Government. According to a recent survey[7], annual spending within the public sector on identity management solutions will total around £825 million for 2007 and reach around £1.4 billion by 2011.

2.37 The Identity Cards Act was passed in 2006 and a Strategic Action Plan published in that year, setting out the Government's plans for a National Identity Scheme. The aim was to provide a simple and secure means for citizens to prove their identity, and the capacity for organisations to check identity for stated purposes: preventing identity fraud and other crimes, including illegal immigration and employment; national security; and efficient delivery of public services.

2.38 But the persistent lack of a single high assurance universal scheme covering the public sector makes a number of core objectives, such as enforcing "right to work" legislation, difficult to achieve.

[6] For example, see: www.nationalsmartcardproject.org.uk.

[7] *Identity Management in the UK Public Sector to 2011*, Kable, July 2007.

IDENTITY ASSURANCE IN EMPLOYMENT

2.39 Proving entitlement to employment is critical for employees and employers and the UK as a whole: improving our flexible labour market is key to maintaining the strength of the economy and its ability to deal with changing circumstances.

2.40 Employment law states that employers must keep adequate records to ensure that all employees receive their entitlements. There are restrictions on those who are able to work (British nationals of working age) and different categories of worker are due different entitlements (e.g. age is a factor in the National Minimum Wage). Employers can be fined if they are found to be breaking this law. The box below describes the existing employment checks.

Existing employment checks

A number of checks must be carried out before hiring a new employee. These include:

- evidence that the new employee has the correct qualifications for the role;
- attainment of references from previous employers/institutions to verify appropriate experience and character for role;
- checking criminal records to ensure suitability for post;
- checking National Insurance number (NINO) (where held) to enable employer administer PAYE properly; and
- checking the "right to work" status of an individual is necessary to ensure that not only are they suitable for the post they are applying for, but are actually entitled to undertake employment in the UK.

In some cases, employers must comply with even more detailed procedures, for example:

- robust security checks for sensitive positions (e.g. staff with airside access at UK major airports); and
- Criminal Records Bureau Disclosures for employees working with children and vulnerable adults. This is becoming a prerequisite for a growing number of roles – over three million checks are now performed annually.

2.41 Discussions with stakeholders as part of this review suggest that there is considerable frustration in the private sector with the current employment system. Employers must carry out the extensive checks outlined above and yet, in order to do so, rely on data from the public sector. Due to the poor quality of certain government data systems (e.g. multiple National Insurance numbers) and services (e.g. delays in Criminal Records Bureau checks), it is expensive and time consuming for employers, particularly smaller organisations, to comply. This will impact disproportionately on small employers and may result in poor compliance. The resulting delays to hiring are significant and may restrict labour market flexibility.

2.42 A single universal ID assurance scheme could offer the opportunity to reform these systems so that employers can quickly and confidently satisfy "right to work" legislation.

3 Some lessons from mass identity systems outside the UK

Summary

- Many countries are engaged in ID assurance schemes.
- There is no obvious model that the UK should follow, but some important lessons can be learned from the schemes outside the UK:
  - recognise the importance of widespread and fast consumer adoption;
  - involve the private sector;
  - build on existing infrastructure;
  - design a scheme that accommodates technological advances;
  - public trust is critical; and
  - the banking sector is leading on common standards.

3.1 Many countries, including those with similar cultural and legal characteristics to the UK, are engaged in ID assurance but almost all are driven by the state's own requirements, predominantly security. Some countries have recognised the importance of customer take up to achieving these goals and are adjusting their schemes accordingly, but there is little evidence of the establishment of any common international standards.

3.2 Our research identified no single large-scale ID assurance schemes which, if emulated in the UK, could reasonably be expected to be the catalyst for the creation of a truly consumer-led "universal" scheme. Nonetheless, there are important lessons to be learnt from the mass schemes that are being set up around the world, and some of these lessons are outlined below. Set out in Annex C are some of the more interesting case studies.

Recognise the importance of widespread and fast consumer adoption

3.3 Governments can impose universal take-up but only consumers will bring about the breadth of usage that is so critical to the effectiveness of any national ID infrastructure. Countries such as Austria are clear that although universality may not be the starting point, it is certainly the targeted end state.

3.4 Convenience and speed of enrolment have been a major driver behind the take up of schemes in a number of countries. In Hong Kong, it takes just 15-30 minutes to register and around ten days to be issued an ID card, causing minimal disruption for customers.

3.5 Low-cost schemes have found it easier to persuade citizens of the scheme's benefits and have demonstrated higher take up. True low-cost schemes involve cheap or free tokens and a low-cost enrolment process.

3.6 While not the primary purpose of the scheme, a broad offering to the consumer can help drive demand. Estonia successfully rolled out an ID card to over 70 per cent of the population within four years of its launch, by introducing a smart card of wide-ranging use. The card can be used on public transport and to access online government services. 10 per cent of the population use it daily to use public transport in the capital. Since March 2007, the largest mobile telephone operator has been putting the identity verification application into their SIM cards, enabling mobile telephones to operate as an identity card.

3.7 Broad consultation has enabled some schemes to allay consumers' privacy concerns and reach scale fast. Consultations have typically included key government agencies, private sector organisations, and civil libertarian groups. In countries where there has been a lack of consultation (e.g. Finland), good technical solutions have remained under-used due to a lack of public utility. In spite of the many services on offer, the Finnish card has failed to attract customers and many organisations are taking a "wait and see" attitude about adopting the ID card authentication standard.

Involve the private sector

3.8 All the countries examined have recognised that the public sector is not well equipped to deliver a specialised IT system of this nature and have involved specialist private sector companies to a greater or lesser degree. Some countries have successfully standardised elements of the process, e.g. card production or enrolment, creating a market to deliver these elements, allowing the public to benefit from new or cheaper ways of delivery.

3.9 Austria defined the functionality of its scheme through standards and let the market deliver it to consumers. As a result, Austrians can use a range of ID tokens (including mobile telephones and USB tokens). Currently, cards with chips are the most common.

3.10 Allowing the private sector to add functions with a user's agreement has proved popular in some countries. Sweden offers an identity token that enables confidential and secure electronic payment methods in cooperation with major financial institutions to provide users with a choice of convenient payment methods (credit and debit card payments).

Build on existing infrastructure

3.11 Relatively few schemes have links into core banking systems, but several of the Scandinavian countries, such as Sweden, have used infrastructure already developed by banks rather than inventing their own systems to good effect.

3.12 Legacy environments clearly differ: countries such as Estonia were able to design their scheme without the restraints of integrating it into existing infrastructure. However, those countries with a history of ID cards and electronic service delivery, such as Belgium, have met integration challenges and built on existing infrastructure.

3.13 In spite of being one of the world's first smart ID cards, some applications of the Malaysian card (MyKad) have had little take up. Of ten million drivers, only 1.3 million have added their driving licence information to their MyKad. To an extent, infrastructure plays it part. The police don't carry MyKad readers and so still insist on drivers producing conventional driving licences.

Design a system that can accommodate technological change

3.14 Hong Kong has used a modular roll out to take advantage of new technologies. The current cards store laser-engraved data as well as thumbprint templates in the chip. The latter enables permanent residents to use automated border controls.

3.15 Austria set out technology-neutral standards for their scheme and, as a result, a range of technology solutions have been developed and adopted by consumers, for example some citizens use their mobile telephone to prove identity.

Public trust is critical

3.16 Sweden's ID assurance strategy has clear aims to engender public trust in the integrity and privacy of customer data. As such, they introduced a system that they were confident was both technically and financially feasible. Once the system gained the public's trust, refinements of the technical solutions were introduced.

3.17 Hong Kong uses techniques such as data encryption, simple system design, and 24-hour hotline support to achieve public trust in its identity enabled electronic service delivery.

3.18 The Austrian system requires sector specific identifiers to be issued for different applications. All of them link to a central identity store but sector-specific data are kept strictly separate. This particular architecture avoids data-sharing issues and protects data privacy but results in the use of multiple tokens and PINs.

The banking sector is leading on common standards

3.19 Bank cards operate around the world, due to the introduction of progressively more advanced interoperable standards. Most countries will accept payments from credit and debit cards, and a customer can take money out of their own account on the other side of the globe. Some standards do not yet operate globally, for example Chip and PIN is not prevalent in the United States.

3.20 An international identity assurance company named IdenTrust was set up in 1999 by a number of banks, including Citigroup, ABN AMRO and Bankers Trust. IdenTrust has developed standards for digital identities for the financial services sector, and provides an interoperable environment for authenticating and using these identities worldwide. Its customers include a number of large global financial institutions, such as HSBC who signed in January 2008 to enable HSBC customers to digitally and securely provide instructions to the bank.

3.21 IdenTrust has now begun to work with the US Government, such as the Department of Health and Human Services and the Department of Labor, to help improve identity authentication in the electronic delivery of public services.

4 Identity fraud and repair

Summary

- All types of identity related fraud are growing rapidly and now cost the UK around £1.7 billion a year.
- Hitherto the focus has been on identifying and preventing fraud.
- Consumers' interest is focused on the easy repair of their identity as and when it is compromised by identity theft.
- Identity repair services are an essential part of consumers' trust in any identity assurance scheme.
- The recent National Consumer Council initiative is a good first step, but there is a pressing need to upgrade identity repair services for existing identity assurance systems and any new schemes.

4.1 Identity crime is a generic term for identity theft, creating a false identity or committing identity fraud. A false identity is:

- a fictitious (i.e. invented) identity; or
- an existing (i.e. genuine) identity that has been altered to create a fictitious identity.

4.2 Identity theft occurs when sufficient information about an identity is obtained to facilitate identity fraud, irrespective of whether, in the case of an individual, the victim is alive or dead.

4.3 Identity fraud occurs when a false identity or someone else's identity details are used illegally: for commercial or monetary gain; to obtain goods or information; or to get access to facilities or services (such as opening a bank account). See box below for examples of the types of identity fraud.

Examples of identity fraud (as defined by CIFAS, a fraud prevention service)

- **Card-not-present fraud**: a fraudster uses stolen payment card details to obtain goods/services remotely via mail, telephone or the internet.
- **Change of address Fraud**: a fraudster uses stolen details of a genuine customer's account to contact a business and advise that he/she has moved. This is followed by a request for items of value such as a chequebook, debit card or account statement that are sent to the bogus 'new' address.
- **Current address fraud**: a fraudster applies for products in the name of the victim, and accesses/intercept the victim's post (for example individuals resident at a property that has a communal mailbox with shared access).
- **Total identity hi-jack**: the fraudster obtains extensive personal details for an individual enabling the fraudster to target more than 20-30 financial institutions.

4.4 It is difficult to obtain accurate statistics on the volume of identity fraud in the UK, due to differing definitions and incomplete reporting. It is likely that banking and financial institutions do not report all instances of identity fraud, preferring instead to absorb the losses. In February 2006, the Home Office quoted the estimated annual cost of identity fraud to the UK economy as £1.7 billion (up from £1.3 billion in 2002). The figure was drawn from dealings with public and private sector organisations. The detail of this review may be open to challenge, but such fraud losses are undoubtedly growing rapidly and run into £billions.

4.5 CIFAS (a UK fraud prevention service) recorded more than 65,000 victims of identity fraud in 2007[1]. Anecdotal evidence suggests that this may be a significant understatement of the scale of the problem.

4.6 Identity theft can cause major problems for individuals. A CIFAS-commissioned survey in 2006 shows that rectifying identity theft can take as long as six months. The average amount of time required was 200 hours, although this figure is skewed by the few for whom it took many months. A victim of identity fraud can typically expect to spend between three and 48 hours rectifying the problem. About half of fraud victims surveyed by CIFAS said that the experience had a big impact on their stress and health levels and for the majority it caused great inconvenience.

4.7 It is technically impossible for any identity scheme to provide 100 per cent assurance. The quick and efficient repair of identity is therefore a key element in any system of identity assurance, and an important way to secure public trust in the scheme.

[1] http://www.cifas.org.uk/default.asp?edit_id=790-57

CURRENT DEVELOPMENTS: THE FRAUD REVIEW

4.8 The Attorney General's Office published their final report of the Fraud Review in July 2006[2], which made recommendations on the measurement, investigation and handling of fraud. The Government response in March 2007[3] included agreement to:

- set up a National Fraud Strategic Authority (NFSA) as a public/private partnership to devise and implement a national fraud strategy;
- form a national lead police force, based on the City of London Police Fraud Squad, to act as a centre of excellence, disseminate best practice, give advice on complex inquiries in other regions, and assist with or direct the most complex of such investigations; and
- within the lead force, establish a National Fraud Reporting Centre (NFRC) – see box below.

Proposals for structure and function of the National Fraud Reporting Centre

- Collect and manage fraud data. Receive reports of fraud offences and incidents and translate these into useful analysis that can inform: criminal investigations conducted by police; confiscation investigations; or other actions taken by government departments, agencies, or industry.
- Provide an outward facing service to the public, the business community and police forces.
- Support publicity campaigns, risk assessment, remedial or preventive action by regional anti-fraud groups, local authorities or government bodies.
- Give fraud victims confidence that action is being taken as a result of their fraud experience, even if it is does not justify a criminal investigation.

THE FUTURE OF FRAUD RESPONSE

4.9 As identity fraud has risen, government and the banks have established a number of initiatives to record and combat fraud, most obviously the creation of the NFSA described above. This heightened focus on tackling fraud is welcome.

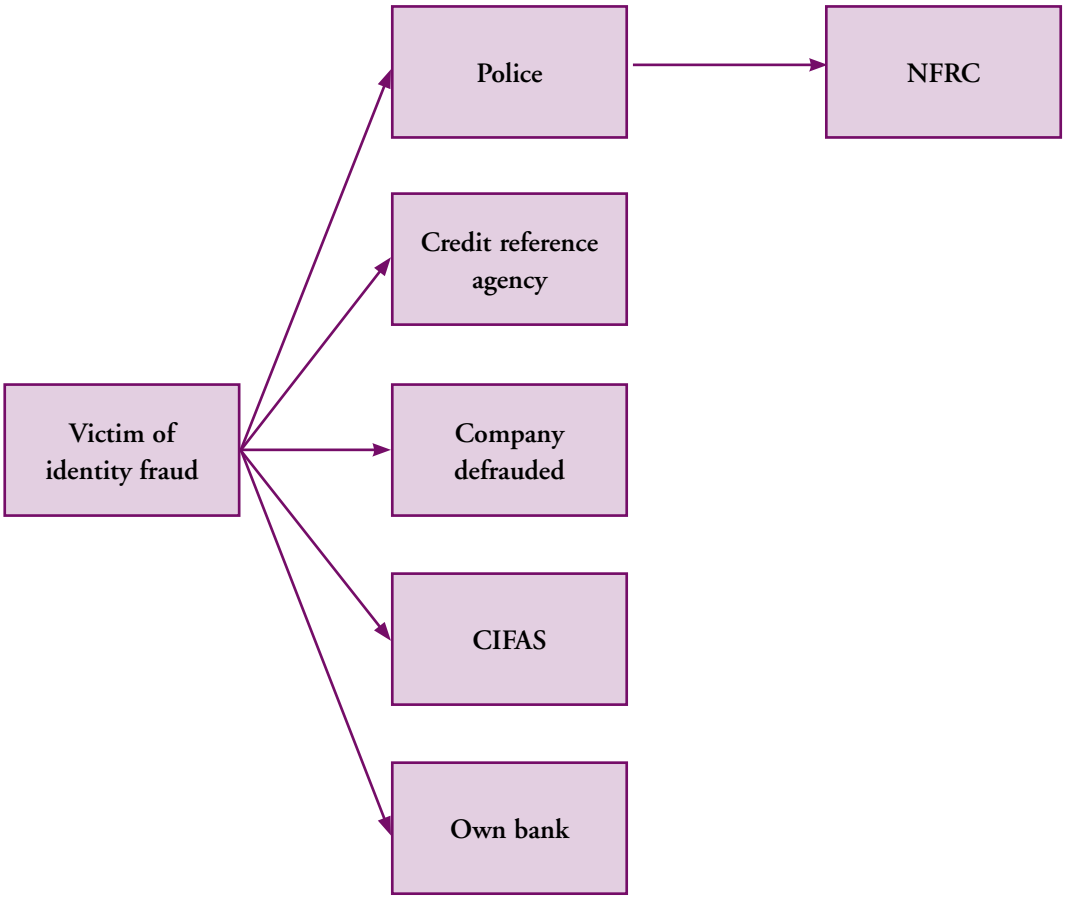
4.10 However, more needs to be done. The new national fraud initiatives will help authorities record and combat fraud. But they do not sufficiently address consumer needs. Identity theft matters most to consumers if it compromises their identity. If it does so, they need a quick and efficient way to repair their identity.

[2] http://www.attorneygeneral.gov.uk/Fraud%20Review/Fraud%20Review%20Final%20Report%20July%202006.pdf

[3] http://www.attorneygeneral.gov.uk/Fraud%20Review/Government%20Response%2015%20March%202007.pdf

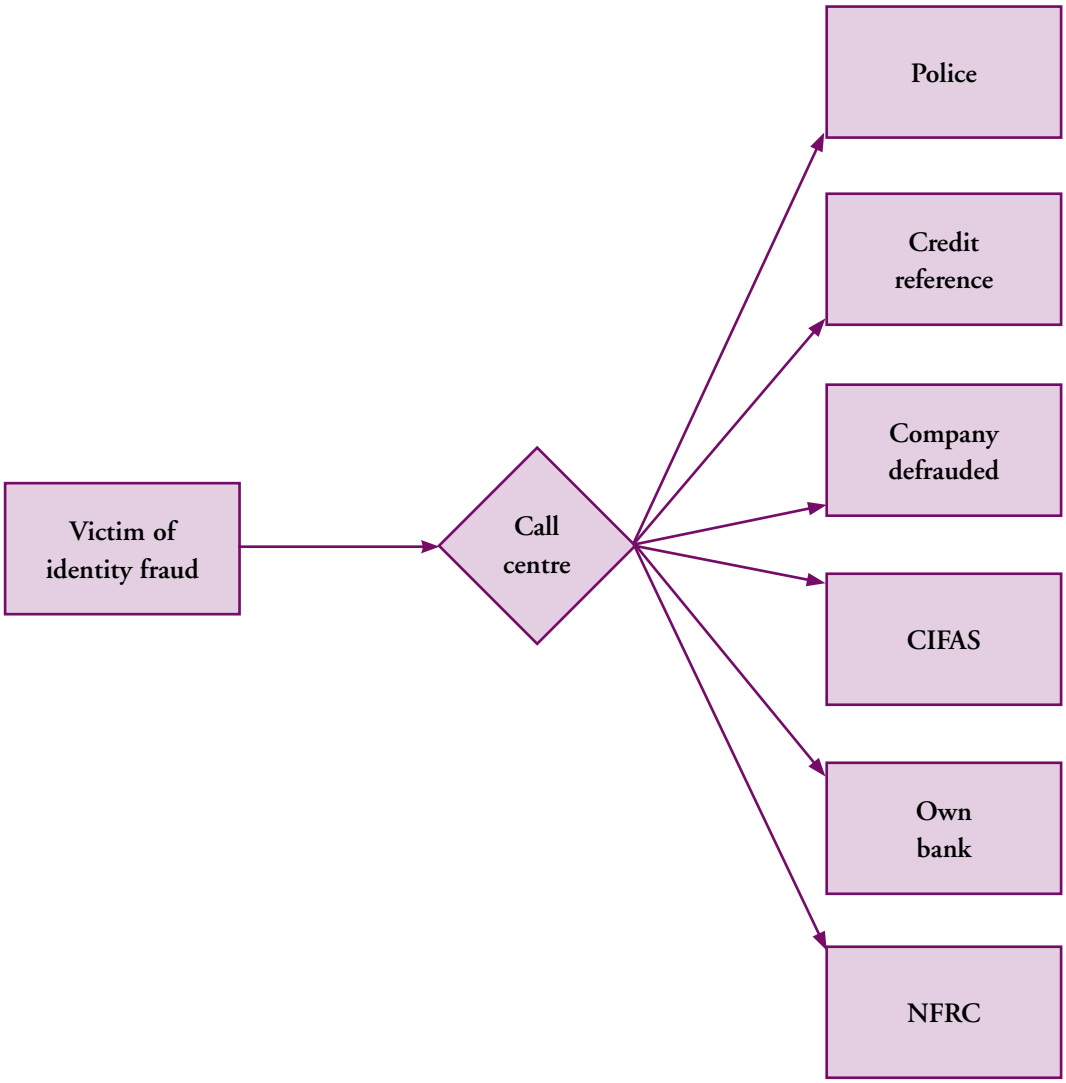
4.11 Today, victims of identity fraud have to contact a long list of agencies and institutions to report the incident, and may have to wait weeks or months for their credit history to be repaired and access to their money restored.

Figure 4.1: The multiple steps a fraud victim must take to repair their identity



4.12 The recent initiative by the National Consumer Council and the three credit reference agencies to offer free-of-charge identity repair services (in relation to credit reference data) is a significant step forward in addressing citizens' needs. CallCredit, Equifax and Experian now offer a single point of contact for identity fraud victims. Any of the individual agencies, when contacted by an identity fraud victim, will alert each of the other agencies and, together, they will restore the individual's credit history.

Figure 4.2: A single point of contact for fraud victims



4.13 However, this should be seen as only the first step in tackling ID theft from the perspective of consumers and citizens. Consumers' trust in any identity assurance system is dependent on repair services and there is a clear case for a consumer-centric identity repair service covering the public and private sector. Identity repair services will be a critical part of any universal ID assurance system.

5 The case for a universal identity assurance scheme

Summary

- An ID assurance scheme that enables a high proportion of the population to assert their identity with ease and confidence in a wide range of circumstances will be of great value to consumers.
- Such a "universal" scheme would deliver economic efficiency and would enable both the public and private sectors to deliver key policy objectives (e.g. border controls, money laundering rules).
- A consumer-led universal scheme would better deliver on national security goals than any scheme with its origins in security and data sharing.

THE BENEFITS OF A UNIVERSAL IDENTITY ASSURANCE SCHEME

5.1 A universal ID assurance scheme is a consumer-led system that empowers all citizens to assert their identity.

5.2 The confidence and ease with which individuals can prove who they are will influence their take up and use of existing and emerging technologies. An effective system of ID assurance supports the increase in remote transactions and can improve economic efficiency. In turn, the greater number and frequency of transactions that rely on such a system, the more effective and reliable that system becomes. A successful ID assurance system can create a virtuous circle in which regular use breeds improved effectiveness that encourages more regular use.

5.3 As for the introduction of money and the subsequent modernisation into coins, notes, cheques, internet transfers, etc, a universal ID assurance system offers the prospect of lower costs per transaction and an immediate gain in economic efficiency, coupled with a "multiplier" effect in terms of increased activity in number of transactions.

5.4 Consumers, able to assert their identity with less hassle and greater confidence, would be the principal beneficiaries of any universal ID assurance scheme. The public and private sectors would benefit from efficiency gains and would be more successful in enforcing their own and each other's policy objectives (e.g. border control or money laundering rules).

5.5 A universal identity assurance scheme will deliver significant economic and social advantage once it reaches scale. Scale is best measured by take up and frequency of use which then supports greater ease of use and trust in the scheme. And a token that people use regularly and attribute value to will be kept secure by the customer themselves, and the scheme becomes self-policing.

Benefits for the consumer

5.6 By definition, a universal ID assurance scheme meets consumers' needs in that it:

- allows them to assert their identity with confidence and ease;
- is open to all consumers;
- means that one system can be used in lots of different places, saving time and hassle; and
- provides superior levels of assurance.

Benefits for the public sector

5.7 As Chapter 2 explained, many government departments are involved in ID assurance initiatives, causing a number of issues:

- **Cost**: Departments are often individually, but in parallel, designing and developing new ID assurance schemes. Some are independently commissioning and paying Credit Reference Agencies (CRAs) to provide identity authentication services, incurring duplicate expense.
- **Effectiveness**: There appears to be too little sharing of resources and best practice between departments in the design of schemes. Meanwhile, the CRAs do not have access to many of the valuable public sector data sources that provide the best authentication services. By relying on the limited sources available to CRAs, departments are failing to make the most of their own public sector databases.
- **Customer focus**: A lack of agreed standards and procedures across all government schemes means that organisations do not necessarily trust data provided by each other. As a result, customers who have moved address find that each service provider must be informed separately.

5.8 Development of a universal assurance scheme would enable public sector organisations to address these issues, without necessarily sharing customer data, and certainly not without the informed consent of citizens:

a) Tokens, such as driving licences, are widely accepted, but many others are not. Agreed standards and procedures for customer enrolment across government will improve departments' trust of each other's tokens and documents and will eventually enable "joined-up government" where this is permitted or desired by the customer.

b) A commonly used infrastructure in which identity credentials can be authenticated and the customer verified against the credentials will reduce costs for individual departments and enable "best of breed" solutions to be built centrally and deployed as appropriate by departments.

c) A widely trusted scheme could enable the State to collect and store less data overall. Instead of each public sector database holding citizens' personal data, departments could store only the data relevant to the service they provide (benefits data by DWP, medical data by the NHS, etc). Without the release of any data, the universal scheme could provide the necessary assurance of an individual's identity to each department.

Benefits for the private sector

5.9 Companies need to be confident of the identity of their employees, their customers and their suppliers. A universal ID assurance scheme could significantly improve the position under all these headings.

5.10 More specifically, Chapter 2 explained the importance of ID assurance in employment. Government requires companies to confirm that any new employee is entitled to work. Companies will also want to be certain that applicants have the experience and qualifications they claim. A system that provides a quick and easy way to prove identity can therefore improve efficiency for business. It can mitigate the risks of recruitment errors. The gain to employees themselves of a faster and more effective route into a job is clear.

5.11 Companies are aware of the need and the opportunity that identity assurance present. A recent Economist Intelligence Unit[1] (EIU) survey of global business executives showed that most companies now see identity authentication strategy as critical, and many see it as a driver of business growth. Of the almost 250 respondents, 67 per cent said that identity authentication is a priority for their organisation, and can deliver business benefits (such as expediting receipts) as well as strategic gains (such as facilitating entry into new markets). An additional 18 per cent said identity authentication was a priority primarily for legal reasons.

Benefits for national security

5.12 Provided that a universal ID assurance system infrastructure embraces public services, banking, transportation and e-commerce, it will enhance security by making it more difficult for anyone to operate outside the system. It will ensure that suspect individuals leave trails of transactions that are ultimately traceable back to unique identity records, albeit only for the purposes of national security.

5.13 A universal ID assurance system would have the broadest coverage and widest application and produce rich data for national security agencies. A system that is genuinely consumer led because it meets consumer needs and inspires their trust would therefore deliver a better national security outcome than one with its origins in security and data sharing.

KEY PRINCIPLES OF A UNIVERSAL IDENTITY ASSURANCE SCHEME

5.14 A consumer-led ID assurance scheme which achieves "universal" status will do so because:

- it meets consumer's need to assert their identity easily and confidently;
- it inspires their trust; and
- it is seen to offer superior levels of assurance.

[1] *Digital identity authentication in e-commerce*, EIU, 2007.

The purpose of any scheme should be restricted to that of enabling citizens to assert their identity with ease and confidence

5.15 Governments can impose universal take-up but only consumers will bring about the breadth of usage that is so critical to the effectiveness of any national ID infrastructure. All elements of the scheme should be designed with the customers' interests at the core.

5.16 Once enrolled in the scheme, a customer may wish to enable "joined-up" government services and government should, using robust solutions to protect this data, give customers the option to do so.

5.17 The Government should identify the correct target level of assurance for verifying groups of individuals and then set the performance levels to meet these needs. It should avoid picking a technology and building a strategy to match.

The scheme's governance should be designed to inspire the highest level of trust among citizens

5.18 Countries with similar political systems and cultures to the UK (such as Ireland) are investing heavily in building consumer trust in their national identity system.

5.19 The scheme should be operated independently of government (for example, accountable directly to Parliament) and its processes and security arrangements should be subject to the approval of the Information Commissioner, who should have the power periodically to review delivery.

The amount of data stored should be minimised

5.20 To protect consumer privacy and engender trust, the amount of data stored should be minimised. Only non-unique digital representations of biometric images should be stored.

5.21 Any additional data accessed during enrolment should not be retained.

Citizens should "own" their entry on any register

5.22 Citizens should own their entry on any register in the sense that it should not be possible (other than for the purposes of national security) for any such data (including digital representations of biometrics) to be shared without their informed consent.

5.23 Verification of identity should be performed without the release of data.

Enrolment processes should vary between individuals and change over time

5.24 The system, from enrolment to point of use, needs to be simple, convenient, and cost effective for the consumer.

5.25 Enrolment processes should vary between individuals and over time so as to minimise costs, strengthen the focus on high-risk customers, and give citizens the simplest and most hassle-free experience consistent with the achievement of the published assurance targets.

5.26 For those with strong biographics, such as pensioners, it should be able to ascertain their identity to a high degree of certainty. They have typically lived in the same place for years, are in receipt of help from the state, and have a strong private sector history. For groups such as these, a simple 'opt-in' process could be employed. Tokens could be sent out that only require a telephone call to activate, in much the same way as credit cards are distributed.

5.27 Other people's identity will be harder to establish and will require closer scrutiny. Resources would be more effectively focused at this group rather than trying to assess everyone to the same degree.

5.28 Where physical enrolment is necessary it should, at least, be convenient. From discussions with the private sector, a minimum of 1,000 sites are required to provide coverage to the UK population. To avoid duplication of resources and a costly expansion in government real estate, other alternatives to a public sector solution (e.g. creation of a market) should be considered.

The scheme should be capable of being rolled out at pace

5.29 Fast roll out is important in order to be able to respond to consumer demand and achieve early realisation of economic and social benefits.

5.30 Private and public sector organisations are unlikely to depend on the system until a critical mass of customers have registered, and so the benefits of a universal ID scheme largely come once it is widely adopted. The challenge, then, is to roll out the scheme in significant volume over a short space of time, while providing a superior level of identity assurance to the public.

5.31 No technology provides total assurance nor is any one technology totally future proof, but a modular roll out will capture the benefits of technology change (approximately three to four-year rolling window) and allow the system to be kept up to date. A low cost token could be introduced and replaced on a rolling four-year cycle.

The scheme's systems should be closely aligned to those of the banks

5.32 Banks have adopted common standards and are leading the field in effective mass ID assurance in the UK, for example with Chip and PIN. Within the "banked" sector of the population, it enjoys frequent and almost universal usage.

5.33 Technically the scheme's systems should be closely aligned to those of the banks (both initially and in the future) so as to utilise their investment, de-risk the scheme's development, and assist convergence to common standards across the ID assurance systems and processes deployed internationally by banks and national ID card schemes.

5.34 A higher level of identity assurance than currently exists can be achieved by building on existing infrastructure, such as the Chip and PIN terminals, and adding another layer of security to a card, such as a photograph biometric. For instance, a Chip and PIN card with a photograph biometric would provide three-factor security: (i) card and chip; (ii) PIN; and (iii) photograph biometric. This would provide a stronger level of authentication than in any existing card in wide circulation today in the UK.

5.35 Beyond strengthening assurance levels, the role for the State is to reach those people that the banks won't reach, the "unbanked".

5.36 Existing identity tokens should also be used where possible. By leveraging existing tokens the infrastructure should remain current, as the original investors will continue to have incentives to invest. The familiarity of the tokens to the public should endear trust.

Citizens should be able to rely on their cards being replaced and their identity being repaired quickly and efficiently

5.37 No ID assurance system will ever eradicate fraud, so an effective ID repair service is important. Citizens who lose cards or whose identity is compromised in some way should be able to rely on their cards being replaced or their identity being repaired quickly and efficiently and in accordance with published service standards.

Enrolment and any tokens will have to be provided free of charge

5.38 The cost of signing up and using the system should not discourage customers. It should be cheap and ideally free. Indirect costs for the consumer, such as time taken and distance travelled to enrol, also need to be factored into the design. Options, such as remote enrolment should be considered. Remote enrolment for passports has shown that this method can make the transaction cheaper and more convenient for the public.

The market should provide a key role in delivering a universal ID assurance scheme

5.39 Government may wish to perform specific roles in the scheme, such as setting standards and maintaining the database. However, elements of the scheme are likely to be performed most efficiently and cost effectively by the private sector.

5.40 Competition should be encouraged to determine:

- **how best to enrol** (e.g. if biometrics are to be captured could these be in a booth, face to face, etc. A market could be created to capture fingerprints, much like the photograph booths of today);
- **which tokens** (e.g. card, mobile telephone) are used to deliver the scheme;
- **the degree of verification achieved** (inevitably some interfaces will be more expensive and/or more secure); and
- **the circumstances under which organisations choose to use the "infrastructure"** (e.g. banks will probably adopt common standards and share a common interface but elect to use it in different circumstances).

6 Recommendations

6.1 The Government's commitment to launch a national ID card scheme presents the best opportunity to establish the foundations of a consumer-driven "universal" identity assurance system that would bring economic and social advantage to the UK. In order to realise this opportunity the scheme should be launched on the basis of the ten key principles laid out in this report.

6.2 The costs and delays involved in verifying the credentials of new employees disadvantage employees and employers, particularly in smaller organisations. This undermines the flexibility and efficiency of the labour market, all the more important in an era of high immigration and more frequent job moves. As a matter of urgency, the Government should take all necessary steps to ensure that employers (large and small) can quickly and confidently satisfy "right to work" and related regulations for all their employees.

6.3 The National Consumer Council and the three Credit Reference Agencies are in the course of establishing a free service for the swift repair of compromised identity records. This is the most important example of an identity fraud initiative inspired solely by consumers' needs. The Government should work with the private sector to ensure that such a service is extended to other forms of identity and available to all consumers and citizens. Ideally, this should be achieved through a "one-stop" agency for the swift repair of compromised identity.

A Terms of reference

The Forum's original terms of reference as published on 12 July 2006 were to:

- review the current and emerging use of identity management in the private and public sectors and identify best practice;
- consider how public and private sectors can work together, harnessing the best identity technology to maximise efficiency and effectiveness; and
- produce a preliminary report for the Chancellor of the Exchequer and the Ministerial Committee on identity Management by Easter 2007.

In March 2007 the Chancellor of the Exchequer requested that detailed consideration be given to how the National Identity Scheme could be best developed to exploit the opportuunities identified in the first phase of the forum's work.

B Organisations and individuals consulted

This is not an exhaustive list of everybody consulted in the review, with apologies to any mistakenly omitted. Many organisations gave their time to be interviewed and to attend consultation workshops. The trade associations also held meetings for the Forum. With thanks to all those who contributed, the list below gives an illustration of the breadth of coverage of the Forum's discussions.

Forum member organisations

- BA
- Barclays Bank
- Boots
- City of London Police
- Compass Group
- Department for Work and Pensions
- Driver and Vehicle Licensing Agency
- HM Revenue & Customs
- Identity & Passports Service
- Linklaters
- O_2
- Serious Organised Crime Agency

Other organisations and individuals

- 192.com
- Accenture
- Amadeus
- APACS
- Argos
- Association of British Chambers of commerce
- Association of British Travel Agents
- Association of Train Operating Companies
- Atos Origin

- BAA
- Background checking Ltd (Experian group)
- Borders and Immigration Agency (formerly Immigration and Nationality Department, Home Office)
- Brainjuicer
- British Institute of Innkeepers
- BSI
- BT
- Business Services Association
- Cabinet Office Intelligence and Security Directorate
- Call Credit
- Campbell Gentry
- Lord Carter of Cole
- Confederation of British Industry
- CIFAS
- Communications Electronic Security Group
- Construction Industry Council
- Consult Hyperion
- Council of Mortgage Lenders
- CPP Ltd
- Department for Communities and Local Government
- Department for Transport
- e-dentity
- Enterprise Privacy Group
- Equifax
- Experian
- Lord Errol
- Eurostar
- Federation of Licensed Victualler Associations
- Federation of Small Businesses
- Financial Services Authority
- First On Demand

- Fujitsu UK
- Garlik.com
- GB Group
- GCHQ
- Gem Alto
- Home Office Scientific Development Branch
- Home Retail Group
- Iden Trust
- IBM UK
- Identity Fraud Victim Support Steering Group (see below)
- Identity theft Assistance Centre, ITAC (USA)
- Information Assurance Advisory Council
- The Information Commissioner
- Institute of Directors
- Intellect
- Interactive Media Retail Group
- Paul Johnson, Chief Micro-economist, HM Treasury
- Sir David King, Chief Scientific Advisor, HM Government
- Geoff Llewellyn (RPM Business Consultancy Ltd)
- Logica CMG
- London School of Economics
- Mastercard
- Microsoft
- Motorola
- Multos
- National Association of Funeral Directors
- National Consumer Council
- No 2 ID
- Nokia
- Office of Science and Innovation Horizon Scanning Centre
- Oracle

- Partnerships UK
- Police National Improvement Agency
- Post Office
- Prime Minister's Delivery Unit
- Remote Gambling Association
- Lord Renwick
- Royal Bank of Scotland
- SAMI Consulting
- SAP
- Prof .Angela Sass, University of London
- Scottish Executive
- Security Service
- Siemens
- Smartex
- Socitm Consulting
- John Suffolk, Chief Information Officer, HM Government
- Sun Microsystems
- Symantec
- t Scheme Ltd
- Tesco
- Thomas Cook
- Trusted Terminal Ltd
- Unisys
- URU
- Sir David Varney
- Visa International
- Voca

C The introduction of identity cards abroad

AUSTRIA

The Austrian government has stated that citizen cards shall become the "official identity documents" in the electronic administrative procedures, such as filing applications via the internet. Despite being called a "Citizen Card", devices such as mobile phones, PCs, and laptop attachments (such as USB tokens) can, if they conform to the scheme's standards, be used to assert identity.

This open, technology-neutral approach allows for a variety of providers of Citizen Cards. They either can be public sector (ID card, social security card, etc.) or private sector (certification service providers, bank/ATM cards, etc.), or can be based on other technologies (e.g. mobile phone signatures). The Citizen Card establishes a security infrastructure available to all, including commercial customers. Companies can develop secure online services for their customers by building on the infrastructure provided by the Citizen Card.

The Austrian system requires different Citizen Cards to be issued for different applications. All of them link to a central identity store but sector-specific data are kept strictly separate. This architecture helps to manage data sharing issues and enables the use of multiple tokens and PINs.

ESTONIA

Estonia has successfully rolled out an identity card that is internationally regarded as a success. Within four years of launch it had enrolled over 70 per cent of the total population.

As a relatively young state, Estonia started with little legacy IT infrastructure, allowing it flexibility in its choice of systems.

In 2002 Estonia implemented a smart ID card as the primary identity token. The Estonian card contains the technology to enable access to online government services such as immigration systems. 120,000 people (out of a population of 1.3m) use it every day to access public transport in the Capital. In December 2007 there were 100,000 public sector transactions and a million private sector transactions.

Since March 2007 the largest mobile telephone operator has been putting the identity verification application into their SIM cards, enabling mobile phones to operate as an identity card.

FINLAND

Finland has a system of identity that is based on a unique record number that does not divulge any personal details about the citizen such as age or gender. It can be associated with a card, a mobile phone (from 2005), and a digital "Citizen Certificate" which can be used online or for signing legal documents.

Despite the approximately 50 services that use the card there has been criticism of the process of developing the citizen ID card and the disappointing number of users. Many of the agencies interviewed are still taking a "wait and see" attitude about adopting the citizen ID card authentication standard. Poor uptake may be due to the fact that banks have historically provided access to public services leaving little room for a national ID card in the market.

HONG KONG

Hong Kong has a long history of ID cards. The first paper card was issued in 1949. With several generations of card in between, on 23 June 2003, the government began to roll out smart cards with a phased replacement program for existing cards.

These cards were introduced both to increase the security of the Identity Cards and to enable a greater degree of accessibility for public services. With each generation of card the government has taken security steps appropriate to the level of risk of fraud that the government carries.

The current cards issued in Hong Kong contain data laser engraved on different layer of the card and have the templates of thumbprints stored in the chip. The thumbprints allow the use of automated border control booths by permanent residents – speeding up border crossing.

MALAYSIA

Malaysia had a legacy of 15 million paper ID cards. The Malaysian national ID card, known as MyKad, and the Government Multi-Purpose Card (GMPC) have been issued on a smart card platform since 2001. In total over 20 million MyKads have been issued. This has been driven by free card replacement and a MyKad being a prerequisite for many important life events (e.g. opening a bank account).

Despite being one of the world's first smart ID cards there has been very little exploitation of its capacity to support multiple applications. For example, of the ten million drivers in Malaysia, only 1.3 million have added their driving licence information to their MyKads. The banks have still developed contactless payment functionality on their own ATM cards.

To an extent this is not helped by the lack of infrastructure. The police still don't have MyKad readers, meaning that they still insist on drivers producing conventional driving licences.

ISBN 978-1-84532-391-2