

T H E L O N D O N S C H O O L O F E C O N O M I C S

THE ECONOMIC BENEFIT OF IDENTITY MANAGEMENT &
ASSURANCE

Work Conducted for HM Treasury

FEBRUARY 2007

SUBMITTED BY

Policy Engagement Network
Information Systems Group
Enterprise LSE



THE LONDON SCHOOL
OF ECONOMICS AND
POLITICAL SCIENCE ■

Summary

This report has been prepared by the London School of Economics and Political Science at the request of H.M. Treasury and has been written with the intention of identifying the potential economic gains to business and customers arising from efficient identity management and identity assurance. Nothing in this report is intended, intentionally or otherwise, to assess the government's National Identity Scheme (NIS).

The economic significance of identity management cannot easily be overstated. Identity credentialing pervades organisations and underpins consumer and organisational relationships. Identity is central to relations between business, government and consumers and is a key element in the global marketplace. Rapid transformation of the public and private sectors suggests that the deployment of harmonised identity solutions will within five years be as economically significant as the development of Customer Relationship Management and Enterprise Resource Management strategies.

An effective identity management infrastructure at a national scale will be a crucial component of the future UK economy. Failure to broadly and deeply embed such a mechanism will result in escalating direct cost to government and industry, loss of competitive advantage at an international level, substantially increased opportunity costs, and will hamper future development of markets and services. Seizing global leadership in the field however will without doubt enhance the UK's future international competitiveness and permit a more integrated global engagement for industry and government.

UK leadership in this field has largely failed to materialise, and barriers to leadership and to competitiveness in some areas of the global marketplace will increase at an exponential rate if immediate action is not taken. Identity has proved to be a far more multifarious and sensitive issue than many people had predicted. Despite these challenges, other countries are moving at a much more aggressive pace to develop national identity management infrastructures.

Estimating costs and benefits is extremely difficult and highly conditional. However given the escalating cost savings and benefits associated with effective identity management (as illustrated by existing deployment within large and small organisations alike) we believe it is entirely reasonable to suggest that unless immediate action is taken the overall fig-

ure could be in the order of £5 billion to £10 billion per year within five years. Further research on economic implications is urgently required.

The current piecemeal approach to identity creates considerable obstacles for business. Existing identity practices can create substantial engagement costs with new and existing employees, customers, and between businesses.

- Transactional burdens and onerous security procedures can result in a cumbersome commercial environment that is not conducive to creating a responsive and rewarding commercial relationship with some customers. Commercial opportunity costs are likely to be high. Delayed take-up of new services, such as those offered on the mobile and Internet spectrum, and failure to fully realise the trust of customers in e-commerce are two key components in any economic assessment. U.S. estimates, if directly applied to the UK environment, would suggest that these facets alone might result in opportunity costs in the region of £2 billion to £3 billion annually within five years.
- The direct savings to private sector employers alone accruing from "best practice" identity management could be substantial. On the basis of submissions to this report by a number of large organisations it may cautiously be possible to extrapolate across the employment market gross savings to organisations of approximately £1 billion to £5 billion per year across the UK economy.
- A harmonised identity management approach is likely to deliver substantial economic gains that go beyond customer and employer interaction at the domestic level. Identity assurance requirements permeate business-to-business and business-to-government relationships, affecting the supply chain, cross-border transactions and even export licensing. A holistic approach to identity management should take into account these facets and ensure that organisations can engage identity management at all levels of their operation. The costs and benefits in this realm are even more difficult to quantify, even with detailed outreach and research, however economic gain in establishing the UK in a leadership role in such arenas is likely to be considerable.

Unfortunately, a highly disorganised approach to identity has spread across the UK public and private sectors. This must transmogrify into harmonised, trusted, systemic and cost effective identity strategies that

permeate all key sectors. A collaborative approach to the challenge, together with the creation of a genuine public-private partnership, will be required.

To support and enhance a dynamic economy the NIS and identity management must be seen as promoters of identity assurance, rather than establishing a monopoly over identity. The current policy emphases on law enforcement and legal compliance should be refocused on creating new economics opportunities. An appropriate and economically valuable identity infrastructure needs to support the development of solutions that are based on "buy-in" both by consumers and business. These solutions must be cost effective, flexible, secure, trusted and convenient to use, while being appropriate to their many operating environments. If an infrastructure achieves broad and deep usage it will bring in its wake correspondingly impressive rewards to the economy in general.

The essential work remains to be done. Increased consultation and cooperation will help secure the identity foundations of the UK. Such a dialogue should have regard to the practices of the leading countries and companies, focus on communities of trust, identify how we can assure trust across boundaries, and determine how the UK sectors and institutions can work together to find solutions. This work must be undertaken without delay. If immediate action is not taken the UK will miss out on substantial opportunities. The resulting implementation gap may cause great harm to the competitiveness and efficiency of the national economy.

About the LSE research team

Enterprise LSE Limited was established by the LSE in 1993 to enable and facilitate commercial application of its expertise and intellectual resources. A wholly-owned subsidiary of the LSE, the company offers a professional interface with the academic community. For more than a decade, Enterprise LSE has been serving government, corporate and individual clients from across the world. Enterprise LSE specialise in creating programmes to match precisely the requirements of clients, and have LSE graduates in several key disciplines including economics.

The Information Systems Group at LSE is one of the largest groups of its kind in the world. It is well known for its research and teaching in the social, political and economic dimensions of information and communications technology. It covers most areas of information systems and represents a range of academic approaches and specialisms, from systems design and management to theory and philosophy.

The Policy Engagement Network is an LSE initiative to bring research to policy-makers on a variety of topics. The two co-directors of this initiative were the lead researchers on this specific project, building on their previous policy work across the policy domains of governance, identity, privacy, regulation, and international policy-making. Simon Davies and Gus Hosein previously acted as mentors to the LSE's Identity Project, which resulted in the most exhaustive analysis of identity architecture and identity management so far produced in the UK. Both have been funded by the Canadian Federal Privacy Commission to assess options for a Canadian identity management infrastructure. They have worked with organisations and governments around the world in the domain of identity schemes and policies, with over thirty years of collective experience.

Table of Contents

INTRODUCTION	7
THE NEED FOR IDENTITY POLICY	8
WHY IDENTITY ASSURANCE IS IMPORTANT	9
FUTURE PROSPECTS	12
THE ECONOMICS OF IDENTITY ASSURANCE	14
USES FOR IDENTITY ASSURANCE IN VARIOUS SECTORS	18
COMPLIANCE	19
OPPORTUNITY	26
CHALLENGES IN QUANTIFYING BENEFITS	30
REPORTS ON BENEFITS	31
LESSONS FROM ABROAD	40
SWEDEN	40
HONG KONG	41
MALAYSIA	41
CANADA	42
BUSINESS POLICY LEADERSHIP	43
OTHER CASES	44
CONCLUSIONS AND NEXT STEPS	45
STEP 1. GUIDING POLICY	ERROR! BOOKMARK NOT DEFINED.
STEP 2. GUIDING PRACTICE	ERROR! BOOKMARK NOT DEFINED.

Introduction

Background

This report is the result of research conducted for HM Treasury by London School of Economics and Political Science researchers in technology policy. According to the Treasury's stated expectations:

"The report should review existing literature about the economic benefits of efficient ID management to businesses and their customers, consider the benefits to the public sector already described, and suggest the scope of complementary benefits to the private sector and its customers. The report should describe the different types of private sector benefits to be had and the general conditions for realising them, rank their importance to the economy, indicate the scale and so far as possible quantify them. Benefits may be in the form of direct gains or by reference to developments in ID management overseas, in the form of potential losses to competitiveness that may be avoided.

The report should indicate the priority areas for any further research and analysis, which it is not possible to complete in the time available for this project. "

We undertook this research through consultation meetings with various experts and stakeholders across industry and government to determine the extent to which identity management serves as a benefit to their operations. Our work was facilitated by the extensive information made available from the participants in our consultation meetings, with particularly helpful assistance and guidance provided by the Home Office Identity and Passport Service, based on the considerable research they have recently undertaken on strategic and financial benefits of the National Identity Scheme (NIS). Our research also draws on workshops conducted by the Public-Private Forum on Identity and also from similar workshops on identity management that we have facilitated in Canada, funded by the Canadian Federal Privacy Commissioner.

Our project builds on this work to move forward the focus of attention to envision the economic benefits of identity management, if applied across the UK. In the course of our work we found that some of these benefits were well known and quantified, while others emerged only through detailed discussions with key experts, officials and practitioners. These indirect

potential benefits tend to defy simple qualification and quantification and so a degree of 'blue sky thinking' is required to consider the nature of an identity-enabled marketplace of the future. We are optimistic that despite the lack of adequate discussion regarding identity management (by comparison with other leading jurisdictions) the level of expertise and interest in the UK is exceptionally high.

The Need for Identity Policy

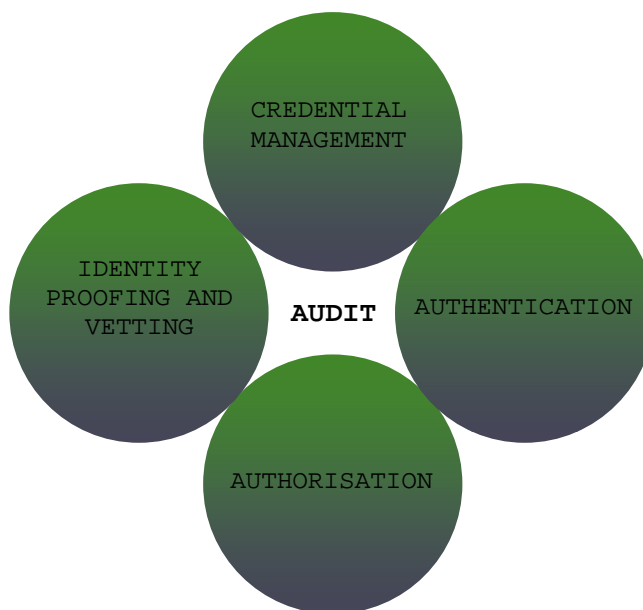
The UK is in the midst, as one observer described it, of a 'perfect storm' of activity that is leading to an increased emphasis on an identity focus within information management activities. Though this is an emergent area of interest, there have been a number of earlier activities that now act as the building blocks for current thinking about how to approach identity.

Countless generations of **credentials** have been issued by governments, companies and groups, usually in the form of identity cards, security passes, memberships cards and passports, often reliant upon some form of **identity verification and vetting** processes that use biographical, biometric and/or personal information. The growth of computing gave rise to renewed concerns regarding **authorisation** rights and profiles, linking roles with privileges. Combined with the spread of computer networking issues, renewed interest in authentication emerged as more people focused on how individuals could assert their rights within these privileges.

With concerns about financial, national and commercial security, all stakeholders needed to find a solution to the problem of confidence. How can confidence in our transactions be ensured in the age of global communications, travel and trade? Since the 1990s there has been a flurry of activity at the consumer, business and government levels to deal with the issue of **identity assurance** to ascertain the level of confidence one needs in a claimed identity for a specific context and transaction. In a number of countries this led to coalitions of government departments, business and consumer groups working together to look into how credentialing, identification, authorisation and authentication could work across multiple systems and business contexts. Working together towards a **national identity infrastructure** could prove beneficial to all these parties, and has led to confidence-enabling policy regimes and standards abroad.

Alarming, the UK has only recently embarked on such an initiative.

Figure 1. ASPECTS OF IDENTITY ASSURANCE



Why identity assurance is important

The establishment of a national identity assurance infrastructure in the United Kingdom, even at this late stage, may prove highly beneficial to the needs of business. For example U.S. studies have shown that as many as 30% of U.S. adults have changed their online behaviour due to fears of identity fraud, while some have even stopped shopping on-line, resulting in billions of dollars in lost business. Similar data from Europe has

shown that data protection, privacy and security concerns are among the top barriers to shopping online. Solutions are required to increase consumer confidence, and global co-operation is required in the search for technology and regulatory aids. These findings also show that consumers need support to repair their identity after a crime, a reform that unfortunately has yet to transpire in Britain. If the necessary support and protections arise then increased confidence may yet emerge.

Meanwhile, business concerns have transformed over recent years. According to one recent study, whereas a few years ago business drivers for identity assurance centred on efficiency/cost-cutting and improvements in user productivity and experiences, the current hierarchy of priorities for identity assurance is as follows:

1. protecting information assets
2. meeting regulatory/privacy obligations
3. enabling secure business partner communications
4. reducing cost and increasing efficiency of operations
5. increasing employee productivity
6. adapting more efficiently to mergers and acquisitions
7. enabling new revenue streams

These results are both interesting and alarming:

- This renewed emphasis on the management of a business's assets shows that there is an increased emphasis on security and privacy protection and fraud prevention, eclipsing efficiency as an overriding concern. This is not a surprising finding considering the renewed attention to information security around the world (e.g. data breaches and identity fraud), and the growth of legislative initiatives that require the reliability and security of identifying information (e.g. criminal records checks for employees, security clearance, identity fraud prevention techniques), but it is interesting that this trend has taken priority over business efficiency.
- Concerns about employee productivity have been downgraded, even though companies are now more aware of the extensive benefits to

employee management that can be achieved by effective identity management.

- The growing interest regarding enabling secure business partner communications shows that the marketplace is interested in effective identity management that moves beyond the single 'community of trust' within the organisation to bridging with other organisations' networks, giving rise to key concerns about interoperability and policy integration.

Business generally has a pragmatic approach to identity. Seeking absolute knowledge in the identity proofing and vetting in all these domains is beyond the realm of reality for many organisations. More pragmatic approaches generally involve the balancing of trust, convenience and risk, accepting that there is a threshold of tolerance for error, while there is also a threshold for the tolerance of inconvenience. Companies generally have to balance the efficiencies gained from sophisticated identity schemes, against the level of fraud that is being prevented. Thus a sophisticated approach to understanding organisational needs is often required before the introduction of advanced policies and technologies. As one commentator put to us, "identity assurance needs to be 'good enough' to solve today's problems without getting caught gazing at 'blue sky' solutions." Often the example of credit cards emerges, where credit card companies understand that consumers and merchants are not interested in sophisticated forms of identity assurance if they are inconvenient. As a result, credit card companies have incorporated the risk of fraud into their business models. It is no surprise, therefore, that credit card companies have never proposed a comprehensive identity scheme with onerous registration processes.

The growth in concern and interest in the identity space highlights an increasingly complex field for policy, regulation and technology. The growth of legal compliance for employment management (e.g. immigration verification, criminal records verification) has driven a significant level of activity by employers, likely also due to concerns regarding the mobility of labour. As employees work across boundaries, whether geographic or organisational, solutions are being sought to maintain efficiency gains from working in an 'e-trust' environment that must comply with numerous policies. Meanwhile, many companies, particularly in the finance sector, have encountered more extensive regulations on customer

authentication through 'Know Your Customer' requirements imposed to deter fraudulent and such illegal activities as money laundering.

This environment introduces a delicate balancing act for companies. Apart from the *efficiencies vs. fraud* balance, companies must also consider compliance risks through the pursuit of due diligence. They must take on additional verification procedures and processes that may go well beyond their original organisational risk assessments.

The increased attention to identity management introduced by regulatory activity should not be interpreted solely as an economic loss. Public trust and confidence may be raised through the deployment of effective identity assurance mechanisms, and this activity may actually lead to more advanced business models. If again we look at the example of the credit card industry, new techniques of authentication have been introduced (e.g. chip and pin), and new business models have also emerged (e.g. identity theft insurance and credit checking services) even within this highly regulated environment.

Competitive advantage may yet emerge through the advanced deployment of identity assurance policies and management practices. As businesses learn to find new ways to manage risk and make use of information they hold on consumers, and as businesses find new ways to interoperate with other organisations, the balancing act of *efficiency vs. risk* becomes even more sophisticated. New models of doing business may yet emerge.

Future Prospects

All these opportunities are for the taking. A comprehensive level of co-ordination will be required, as evidenced in other countries that have embarked on national consultations and policy-making exercises. It was frequently repeated to us that immediate action is required for the UK to remain globally competitive. This is not only to prevent the UK from being the ideal location for fraudulent transactions and illegal employment practices, but also for consideration of other current pressing policy and business initiatives.

Opportunity costs may have already emerged. The paucity of advanced payment mechanisms until recently may have left the UK - and UK consumers - vulnerable to card fraud. Similarly, the lack of policy on security breaches and registry verification may also have left UK citizens at risk of identity fraud. Competitive advantages may have been missed as other

countries' business sectors have collaborated to establish identity assurance schemes to achieve cross-business co-operation.

As for future opportunities, there is increasing discussion of the 'Green Agenda' and carbon-trading. Such a scheme can only be truly enabled through the deployment of a vast and expansive privacy-sensitive identity regime with credential and authorisation management, though the UK is perhaps too poorly positioned to consider such plans at this time.

The opportunities are great and the benefits are increasingly clear. In this report we will outline these benefits and highlight some of the opportunities. Where possible we will quantify the knowable benefits, to provide illustrations of the scale of influence some of these policy changes may introduce to Britain. But as with any such study it is impossible to clearly predict benefits because so much remains unknown and, in many cases, unquantifiable. We will endeavour to show the complexity of these dynamics while highlighting the economic benefits to Britain of effective approaches to identity assurance.

The Economics of Identity Assurance

The role that technological infrastructure can play in a national economy is the subject of much academic study and analysis. Information technology in particular has been identified as playing an essential role in increasing efficiency and productivity across a variety of sectors. Innovation may act as a key mechanism for competitive advantage amongst business, industry sectors and even national economies. Technologies can reduce transaction costs, and effective policy regimes can provide possibilities for effective institutions required for efficient markets. In an advanced developed economy technology can generate an economy that sustains innovation-driven global competitiveness, though this requires high rates of social learning and the ability to rapidly shift to new technologies. This likely requires the development of effective local mechanisms to support change through policy adaptation and training.

The challenge within the academic literature is the ability to discern which technologies have these effects, the extent to which technology may in fact be the driver and how local institutions manage in the wake of these changes. For instance, one of the classical views of technology and economic change is linked to the Schumpeterian view that waves of technological change drive business change in a form of 'creative destruction', but these 'waves' of change only occur over a period of decades (cases point to steam engines driving the industrial age). The problem with this approach is that it ignores all the other enabling technologies and the social adaptations that takes place through policy shifts and re-design. The ways that different contexts, countries and regions treat a variety of technologies within a specific era shows that local policy decisions still play predominant roles as some technologies are adopted while others are not.

A modern view of technology and economics looks more carefully at the 'technology' itself. This approach looks at the technology in detail by 'opening the black box' to see the markets, policies and the emerging institutions. This is done to monitor the interaction between institutions that govern innovative activities and market-based patterns of change to see the diffusion and use of technology, and how the technology becomes embedded in infrastructure. Much of the research shows the powerful role of policy and government in particular in choosing winners and losers while creating incentives for development and innovation. In many in-

stances, government and policies are seen as playing large roles in fostering innovation, and may in fact be necessary to innovation. Technology is devised within a 'techno-economic paradigm' that is defined by the needs that are meant to be fulfilled, the scientific principles utilised for the task and the material technology to be used.

The literature then looks at how infrastructures may emerge through the pervasive use of a generic technology such as electricity and information technology. While there are global drivers to adopting these technologies, we cannot ignore the varying local effects and deployment patterns. Pervasive economic effects arise when

- the infrastructure generates a wide range of new products and services,
- applies across many sectors of the economy, reduces the costs and improves the performance of existing processes,
- gains widespread social acceptance with minimal opposition (which leads to a favourable regulatory framework), and
- generates strong industrial interest based on perceived profitability and competitive advantage.

This may also be achieved through the creation of externalities which induce, and which are induced by, economic change.

These academic ideas may be applied to the case of the national identity assurance infrastructure. We are almost certainly reaching a consensus that the 'perfect storm' of activity around identity is evolving to the point where a wide variety of organisations, officials and consumer representatives agree that identity assurance is a pressing public policy. There is also a wide variety of policies and technologies being deployed in local environments. Our primary challenge is to assess how we harness and cultivate this new paradigm into activities that ensure the pervasive use of these technologies. The National Identity Scheme presents an ideal opportunity to undertake this task.

The NIS is emerging as the prime candidate for the monopoly provider of high quality identity authentication. This is in part because of the significant investment required for a national-scale identity verification scheme, but also because government is the source for the creation of the need for such a scheme (through policy and legislation). This could in

turn lead the NIS down the path of being the national utility for identity information and verification that can provide benefits to those who interface with it.

Such an infrastructure has the potential to change existing rules, routines, norms and power relationships regarding identity across the UK economy.

Two challenges remain for the NIS to become core to a National Identity Infrastructure, and in turn for it to benefit the UK economy:

1. We believe the benefits should be spread beyond government, so that the architecture truly benefits the economy. This requires particular attention to the private sector. The opportunities here are plentiful, as we will describe in later sections.

2. We must ensure that any future identity initiative does not become a mere monopoly institution that assumes market and technological stability, but instead acts as a change agent to nurture further policy and economic change. Through this dynamism there is the potential to create new opportunities through the establishment of further markets and economies. The prospects for an identity-based economy and the other services, applications and products that can be built on top of this (e.g. carbon-trading) are areas that are in great need of further research.

While the ideal situation may be the pervasive use of trusted and privacy-sensitive identity assurance mechanisms, considerable work is required to attain such an environment. Further externalities could be generated in line with previous practice through the expansion of Criminal Records Bureau checks and 'know your customer' regimes, but this top-heavy regulatory strategy may promote adoption for mere legislative compliance, and will not necessarily drive further opportunities. Even still, clear liability regimes need to be more clearly articulated to support decisions to sign up to schemes in order to meet legislative requirements.

Policy leadership is required from which regulation can steer activities through consultation and the creation of compelling argument for change, in turn guiding behaviour. Following on from examples we have seen in other countries where identity cards are nurtured not only for use in the private sector, but also where consultative processes are established to develop and promote authentication principles and assurance best practices.

Indeed, the NIS could play a key role in this national identity management infrastructure, but this presumes that the 'infrastructure' is based on technology alone. The infrastructure is much more than mere technology, and is instead also a forum where decisions and policy may be made regarding security, liability, shared experiences, practices and lessons; but must also nurture a myriad of other emerging techniques, practices and technologies. For instance, we found substantial support amongst those with whom we consulted for the NIS authentication to be built on top of the chip and pin infrastructure. It has also been argued that the mobile spectrum, along with utilisation of handset technology, would provide an ideal and convenient platform within an identity architecture. More such opportunities may emerge that will shape both government and business practices and institutions. A truly effective national identity infrastructure will shy away from monopolies that focus on governments' needs and will instead look to how a policy regime can be established to cultivate and nurture identity assurance across the UK economy.

Uses for Identity Assurance in Various Sectors

Business sectors are increasingly aware of the need for identity assurance. Companies are collecting increased amounts of personal information relating to their employees, their clients and collaborating organisations. As businesses become more aware of the need to manage their information assets in light of new business practices and new regulatory requirements, they are likely to seek new solutions for identity assurance.

Although there is increasing awareness of the role of identity within the business community, much of the recent attention on identity management has focused on legal **compliance**. While this approach has been helpful at raising the issue of identity management, it has not taken the dialogue as far as it should, to the extent of including identity into business practices as an **opportunity**. In this sense the UK entered this discussion space through the wrong door, looking at the benefits to government rather than to the country as a whole.

We have identified through our discussions and deliberations a number of business sectors - both online and off-line - within the UK that are potential beneficiaries of increased identity assurance.

Utilities - Gas, Electricity, Water, etc.

Transport - Trains and buses, automobile and road, aviation, etc.

Health and Social Care - Day care, hospices, retirement communities, etc.

Service and Leisure - Entertainment, restaurants and bars, fitness, etc.

Aerospace and Defence - Firms, Researchers, Contractors, etc.

Retail - Vendors of age prohibited items

Finance and Insurance - Banking institutions, investments and insurance, etc.

Compliance

Over the past decade there has been an increasing amount of research and development in the information technology sector to respond to the IT enabled regulatory compliance. There has been a noted rise in regulation governing information management practices emerging from a variety of policies including:

- accounting and transparency regulations such as Sarbanes Oxley Act,
- money laundering regulations requiring reporting of transactions
- privacy and data protection principles that compel organisations to manage the flows of personal information

to name a few. Some successful - though many unsuccessful technologies - have emerged from this process as developers come to terms with the difficulties of enshrining policy into technology while managing information assets across an organisation. In the area of identity assurance, the pressing compliance issues surround the area of fraudulent activity, problematic accounts and hiring practices.

Fraud

Fraud and fraudulent activity has emerged as one of the pressing challenges for legal compliance. With increased public concerns about identity fraud, businesses and policy-makers are calling on increased support for compliance with the law. Identity assurance has a key role to play in this respect.

Much of the attention regarding identity fraud has focused on the banking and payments sector. In this sector there are a number of forms of identified fraud, including:

- card fraud – although affecting only 0.141% of transactions, this involves the use of counterfeit cards that were stolen in the process of skimming at retail outlets. This form of fraud is also used in 'card-not-present' transactions amount to £183.2m in 2005. This form of fraud is also perpetrated when cards are sent by post and are not received by the intended recipients, amounting to 439.4m per year.
- cheque fraud – although 90% of cheque fraud is intercepted by banks, attempted cheque fraud reached £575m in 2005. This could be

reduced through requirements to verify additional credentials at the time of cheque exchange.

- online fraud – in 2004 the extent of UK online banking fraud reached £12m and online credit card fraud continues to grow because of the lack of secure readers available in 'card-not-present' transactions.

The larger scale crime occurring in this sector is identity fraud, where a person applies for an account in someone else's name, or conducts a take-over of an account through stealing and redirecting post and conducting transactions in someone else's name. According to CIFAS, there were 55,548 victims of impersonation on the CIFAS database at July 2005. 50% of this form of fraud involved attaining credit cards in the victims' names. Meanwhile, fraud conducted through impersonating the deceased is mounting, where there were nearly 30,000 cases predicted for 2004.

There are also problems with the opening of financial accounts for the purpose of money laundering. For this purpose, a 'Know Your Customer' regime has emerged, requiring new customers to provide an adequate level of identity and address information.

The mounting identity requirements to open new accounts and to reduced fraud has caused some concern. As a result, there is little doubt that a national identity assurance infrastructure, built to interact with the NIS, would go some way in preventing this form of fraud. When facing regulatory requirements, however, financial institutions must be aware of the liability and regulatory implementation issues. With regard to liability, financial institutions will expect to know where the risk and liability falls in the event that fraudulent transactions take place, even after some form of identity assurance has taken place.

Regarding regulatory compliance and identity assurance in the financial sector, it is important to note that identity assurance is merely one part of the solution. As the Chairman of the Financial Services Authority announced in 2005:

"We have given – repeatedly and I hope clearly – the message that we expect firms to manage their money laundering risks effectively by placing less emphasis on ID and using the full range of [Anti-Money Laundering] tools."

This statement follows a criticism made by the Better Regulation Task Force, referring to the increased identification requirements as 'creeping regulation'.

"Last year many of us found our banks writing to us to ask for proof of our identity, even when we had held accounts with them for many years. It's unclear where this requirement came from, and this is one of the examples that we will be investigating in our study on regulatory creep."

In fact the Better Regulation Task Force has repeatedly drawn attention to the poorly formed presentation of the case for identity checks that would introduce an additional layer of red tape. The NIS would go some way to reducing the inconvenience of having to provide onerous proof of identity. Financial institutions would be well served to use other mechanisms as well.

Alternative solutions have emerged to solve some of the problems, including:

- behavioural profiling on accounts to reduce fraudulent activity, particularly in card transactions.
- chip and pin to ensure that there is some 'secret data' involved in transactions that are not necessarily visible on the card (replacing the previous signature-based transaction)
- additional credential verification for credit card purchases online including (1) Address Verification System/Card Security Code (AVS/CSC) that allows for verification of credit cards for the accurate billing address, and (2) SecureCode from Mastercard and Verified by Visa are more global schemes that require additional authorisation
- increased online verifications where a card is verified in real-time to be active, with the additional safeguard of the Industry Hot Card File (IHCF). More than 80,000 retailers subscribe to this electronic file that distributes data on lost or stolen cards.

There have also been calls for the release of a list of 'deceased' records to prevent accounts being opened fraudulently.

Criminality and Employment

One key aspect of the compliance factor centres on the issue of employment. This form of identity assurance involves two aspects, and each will depend on the nature of the firm and the type of employment.

Firms today have an obligation in accordance with immigration law to verify the legal status of their employees to ensure that they are legally entitled to work. Failure to follow this legal requirement can result in the imposition of fines. As a result each firm is expending resources to verify the immigration status of their employees and this usually involves keeping copies of documentation provided (e.g. photocopies of passports, visas, etc.). Firms will also be expected to recognise the variety of passports available across EU member states (at least those with citizens who have the right to work in the United Kingdom), the variety of credentials from these member states, and the relevant visa regime in use.

In our consultations we found that this process has become one of industry's primary concerns. The National Identity Scheme may remove this paperwork requirement and may also remove a significant amount of the processing requirement. It would permit UK businesses to more quickly and flexibly adapt their workforce to seasonal and market shifts and speed the process of employment. This would result in a significant gain in efficiency.

The second aspect to identity assurance in employment practices is the verification of the employee's work status through the Criminal Records Bureau. The CRB is an Executive Agency of the Home Office that runs a service that enables organisations in the public, private and voluntary sectors to make safer recruitment decisions by identifying candidates who may be unsuitable for certain work, especially that which involves children or vulnerable adults. In order to prevent abuse, each request for a record check must be counter-signed by a Registered Body (RB). The RB, of which there are nearly 14,000, ensures that the check is consistent with the legislative framework that requires the verifications.

It is important to note that large portions of the users are small businesses or charities. The CRB generally charges a fee for this disclosure: £36 for enhanced check (verifying any local information held by police force), £31 for standard check (check of watch-lists). The applicant traditionally pays this fee, but if the employee is given the job, the employer tends to pay. Volunteer applications are free, but because there are such a high number of these, the CRB is repeatedly in deficit. For instance, according to the CRB, in a 12 month period 520,000 applications

were received purporting to be for voluntary posts, while it is estimated that only 20,000 were genuinely so. This suggests that while applicants are willing to abide by the requirement for the checks, they are unwilling to incur costs.

According to figures from the CRB, 2.8 million disclosures were expected to be issued in 2005/2006. In 2004 there were 20,000 job offers that were withdrawn because of information emerging from CRB.

Another form of disclosure is the POVAFirst scheme. This is a service for situations where employers need to employ new staff prior to receiving the disclosure. This form of early notification costs £6 and has become increasingly popular. In the period July 2005 to November 2005 the CRB processed 200,834 POVAFirst checks. This was calculated as 19,000 per month from the months of June to September 2005, costing CRB 100,000 GBP per month, with a total cost of £1,011,651.

The challenge for CRBs is that the process is sometimes lengthy, particularly due to problems of inaccuracy in the applications. For instance, 11% of application forms are identified as erroneous or incomplete upon receipt, where the most common error is the failure to supply 5 years of continuous addresses. Further, 12% of the errors are identified with such inaccuracies as missing middle name on the application form while the middle name has been provided on the identification documents.

The National Identity Scheme would again serve to remedy many of these errors particularly if the CRB could access the address and naming information held on the National Identity Register, in real time. It could speed up the service of disclosure, and thus reduce the cost for the CRB (thus reducing the POVAFirst costs, for instance), and in turn allowing employers to take on new staff more quickly.

The CRB is also working on additional schemes to increase the efficiency of their services. These include:

- I-PLX database helps to track down people as they move and to contact relevant police forces. This permits the CRB to now check if any force has intelligence or non-conviction information on an applicant. Previously this was a labour-intensive task that could result in gaps in information.
- the CRB is planning on delivering electronic-based services to customers, involving an online enquiry service to track progress of

disclosure application, as well as the potential for a web-based application, which would reduce the likelihood of data-entry errors or at least decrease the amount of time taken to make a correction.

It is important to note that CRB checks, by legislative design, only apply to a small sector of the UK economy, so the benefits gained from more effective checks will only have confined economic benefits. Reducing the obstacles posed by these barriers to flexible employment, however, through easing the verification process for the right to work will probably lead to substantial benefits for UK employers, ranging from large multinational firms, to small and medium-sized enterprises, and simplifying procedures for flexible engagement of contractors and seasonal workers.

Compliance of another sort: Business-to-Business

In the world of identity assurance much of the emphasis is placed on the citizen, consumer and employee, while the entity of business and its interactions with other businesses and even governments is often neglected. As businesses increasingly work within global business supply chains, they must share sensitive information across traditional and emerging organisational boundaries. The management of employees and authorisations across traditional boundaries requires an unprecedented level of coordination, interoperability and trust.

For instance, the U.S. Government is implementing Homeland Security Presidential Directive 12 (HSPD12) to ensure that all Federal employees and contractors using Federal facilities have compliant Personnel Identity Verification credentials. The U.S. Government is expanding this to First Responders (emergency services, medical, fire, police). The U.S. Department of Defense is considering a requirement to contract its suppliers to implement equivalent identity management mechanisms for anyone accessing Department of Defense information held on industry systems. The effect of this is that the aerospace and defence industry is forced to develop collaborative capabilities for identity and access management that individual companies can use. The UK Ministry of Defence has indicated that its policies will require similar or equivalent digital credentials for access to shared information. Together these requirements are likely to affect some 400,000 companies.

Each employee in this circumstance will need to be assigned with an identity, authenticated, and then authorised, to perform tasks across these boundaries. Each organisation participating in the scheme will have to

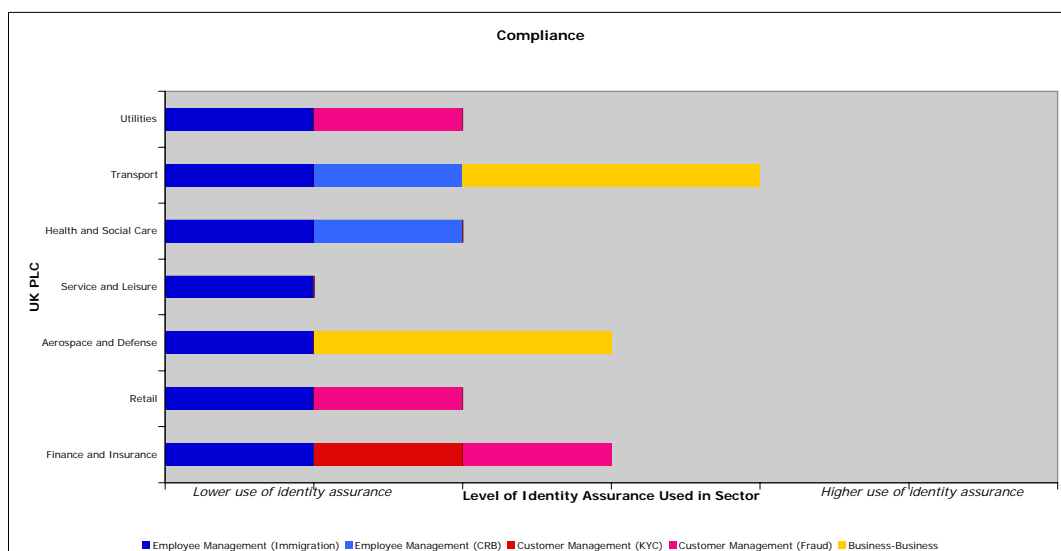
participate in an industry-wide standardisation process for identity assurance, to ensure that the entire supply chain can interoperate.

The initial identity vetting will most likely rely heavily on the National Identity Scheme, and will provide a significant benefit to UK companies involved in these communities of trust. But this is merely a part of the larger challenge of identity management, and much work must be done on policy alignment between the various schemes set up around the world. Working groups have already been established to perform this task.

Summary of Compliance Purpose

The NIS can play a pivotal role in solving many of the problems that business routinely encounters in complying with national law while also competing in the global marketplace.

As figure 2 shows, identity assurance can be applied across industry sectors.



This presumes that:

- All employees need to be vetted for immigration status.
- Utilities: Because of a recognised problem with telecommunications fraud, customer management issues can be resolved through identity assurance.
- Transportation: The aviation security industry requires background checks and various forms of authentication credentials for areas of

airports. Because of data-sharing across boundaries, airlines also must develop advance identity assurance schemes.

- Health and Social Care: Those working with vulnerable adults and with children require CRB checks.
- Aerospace and Defence: Firms and contractors must devise identity assurance mechanisms that reach across global supply chains. It is possible that this involves some form of employee vetting separate to CRB checks.
- Retail: Monitoring customer transactions for a variety of fraud, particularly identity fraud where card verifications may be required to reduce payment fraud. Credentials may also be verified to ensure that customers are permitted to receive goods, e.g. alcohol.
- Finance and insurance: Countering fraud and criminality in this domain requires the verification of identity credentials at registration stage and possibly subsequent verifications for specific transactions. Know Your Customer rules and other fraud mechanisms require advanced identity assurance regimes for customers, with carefully documented lines of risk and liability management.

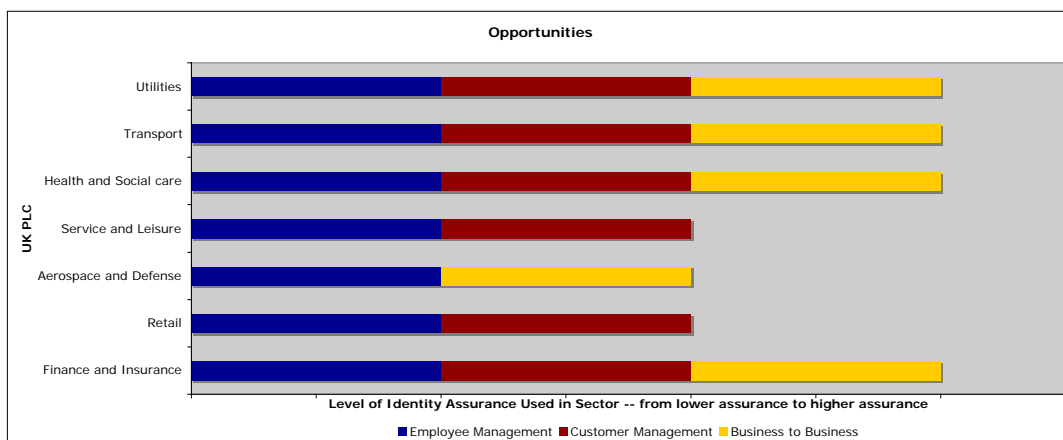
Opportunity

The incentives for a truly national identity assurance infrastructure requires more than mere compliance with laws that mandate assurance through use of the NIS. Users need to be convinced that there are many benefits to paying attention to identity assurance. In the case of the private sector, legal compliance alone is often an inadequate reason to change processes, procedures and technologies.

We often forget that legislation is one response to a condition within an environment. For instance, concern is expressed about fraud, and so legislation is set in place. But the concern about fraud is also symptomatic of a larger problem with the need to manage information within organisations. Consider for example the law requiring the vetting of some employees to ensure that they do not have criminal histories. This does not mean that there are not incentives to vet all employees for some form of qualification verification. A final example applies across business: just because the U.S. Government requires some form of identity assurance in the supply chains for aerospace contracts does not mean that such a

practice should only apply to defence contractors. Many companies are being compelled to work with global supply chains for a variety of purposes, and identity assurance across these jurisdictions is increasingly important.

Identity assurance can very well improve the state of the UK economy, and in some cases there can be substantial improvements achieved. As figure 3 shows, if we move away from the strict-compliance approach to identity assurance, opportunities exist across the UK to increase the use of identity assurance. These changes are not necessarily reliant upon the NIS.



Areas for improvement in identity management include:

- The introduction of risk management and liability management regimes within the private sector. We have already seen a number of solutions emerge from the private sector to reduce identity fraud, such as through online verifications, the use of chip and pin, and well-circulated lists of stolen cards. In our consultation we were repeatedly reminded how credit card companies have long managed the problems of fraud and criminality in the use of credit cards by including the risk of loss and abuse within their business models. We have also noted the entry into the marketplace by information aggregators who promise to deliver information to consumers so that they can themselves monitor fraudulent activity perpetrated in their names.
- In a world with global movement of the workforce and an increasing use of contractors who are self-employed and who work outside of the office environment (e.g. at home) more sophisticated regimes for identity assurance may be required. An entire industry could

emerge from the vetting of job applicants' qualifications to ensure that the applicant indeed has the requisite skills. Companies will also need to develop more sophisticated identity assurance techniques for mobile employees who may work from many places around the globe, and may never actually enter the formal office environment. This must occur even as enterprises learn to find ways to join up their databases and manage their employees' authorisations more effectively.

- More sophisticated customer management regimes will continue to emerge. With the advent of on-line marketplaces such as eBay we have seen how individuals may create multiple pseudonymous credentials but have verifiable chains of authorisations to conduct business without having to divulge too much personal information. Meanwhile, more sophisticated use of identity assurance may permit businesses to personalise product and service delivery while enhancing the autonomy and flexibility of their customers. Pay-as-you-go regimes have proven that this flexibility is required, and identity assurance mechanisms should proceed in step, e.g. to permit 24/7 or on-line upgrades and account top-ups.
- Global business chains are likely to continue developing more sophisticated form of identity assurance. For instance, in order to protect intellectual property, the pharmaceutical industry is investigating federated trust models to develop digital credentials. It has built the 'SAFE PKI' bridge and is in the process of cross-certifying with U.S. Government. This is already reaching into Europe.

As a result, figure 3 above postulates that all business sectors can benefit from advanced forms of employee management, beyond just verifying immigration status and criminal records. Similarly, customer management regimes will become much more sophisticated than relying only on 'Know Your Customer' to combat fraud and illegal activities, as more sophisticated behavioural profiles and, alternatively, 'chains of trust' emerge. And in most sectors we can see clear benefits to identity and trust assurance across global supply chains.

Summary of Opportunities

- Utilities: More effective management of employees and contractors could improve efficiency. Customer management could be improved to

enable more sophisticated services that meet the detailed needs of each customer. Identity information could be shared across businesses to improve portability and account transfers. Marketplaces could become more efficient, with fewer employees and use of more contractors who service multiple utility companies.

- **Transport:** Management of the global airline workforce could be improved, as well as B-B interaction with various staff in outsourced organisations around the world. Airlines already excel at customer management (e.g. loyalty schemes) but other transportation regimes could develop similar identity-based services, as we have seen emerge with Oyster, even given its anonymous pre-pay capabilities. Carbon-trading schemes could emerge provided a flexible identity infrastructure is established.
- **Health and Social care:** Employee vetting services will increase the flexibility of the workforce, particularly for applicants with foreign credentials. More sophisticated authentication processes are clearly needed for new health and social care databases. Similarly, more sophisticated regimes for managing patients and clients will better serve the needs of both the clients and the providers, permitting the transfer of information across to other providers. The healthcare 'supply chain' is already quite complex with research bodies, pharmacies, pharmaceutical companies, local governments, protection agencies, insurance companies etc. all trying to gain access to sensitive information.
- **Service and Leisure:** On a case-by-case basis, though increased knowledge and assurance of customers, organisations can improve service delivery.
- **Aerospace and Defence:** As above, A&D will continue lead in identity assurance. The business-to-business component is already part of its 'customer management' regime.
- **Retail:** New business models could emerge that might lead to new services, e.g. new payment services enabled by biometrics and enhanced by loyalty cards, in turn oriented around the user. This approach could permit more advanced customer and contact management.

- **Financial and Insurance:** Global employees and more secure employment practices to prevent data breaches will require better identity assurance mechanisms. New business or authentication models may evolve from customer management (e.g. biometrics at ATMs), while global investment markets may now be accessed through collaboration with companies around the world, e.g. sharing identity profiles from banking to insurance companies in emerging markets.

Challenges in Quantifying Benefits

There are numerous challenges in assessing the benefits of an identity infrastructure across an economy. While it is possible to estimate the cost of the creation of a large complex system, it is nearly impossible to assess or predict the environment that will exist when the system is complete. Similarly, it is difficult to identify the extent to which the NIS will permeate the UK's economic and social life. For instance, if the NIS is used to simplify the CRB, there will certainly be benefits, but we can not foresee if CRB checking will then be expanded for additional purposes, thus introducing further cost complexities. For the NIS in particular, there is a long time horizon, and the effects of globalisation, terrorism, communications and other dynamics may yet influence the course of that specific scheme. Any prediction we may make regarding accuracy this far in advance is likely to be unstable based on changing circumstances.

It is even more challenging to identify all the likely strands of the national identity assurance infrastructure when it emerges, because it will necessarily evolve in pieces and parts, through leadership in some sectors, dalliances in some and co-ordinated action in others. And despite the LSE's motto 'to know the causes of things', measuring the effects this far in advance is fraught with problems.

It is sometimes difficult to identify whether benefits are potential savings or efficiency gains. And gains are often difficult to quantify, particularly when they involve benefits created through the prevention of crime or terrorism. If something is prevented, we could never know how much it was going to cost, other than the basis of historical trends, but even still, to claim that future potential actions will resemble past ones is a significant assumption.

We may look beyond the purposes of the NIS, however, and estimate contributions to the UK economy through new opportunities. If new business models emerge and business opportunities come to reality we can offer specu-

lative ranges regarding their likely benefits based on the existing, though limited, information and experiences available to date.

Reports on Benefits

There have been a number of other attempts to estimate the benefits arising from identity assurance schemes. Through our consultations with key experts and organisations in this domain we were able to gain access to some of their findings and estimates. We outline the results of these reports below, but in some circumstances we have had to anonymise the sources due to the nature of our consultation.

Employee Management

The enhanced ability for employers to discern appropriate applicants and authorise their employees for the appropriate tasks could provide substantial benefits to the UK economy, as discussed in the last section.

At point of applicant adjudication, a strong identity assurance scheme could substantially improve the time taken to conclude CRB checks and immigration status. Since the latter applies to all employers this could have significant effects on the ability to nurture and maintain a flexible workforce. The benefit would be improved immigration enforcement through reduced illegal working. If this were to involve the use of the NIS, then the organisations involved would be required to integrate some components of the NIS into their practices and procedures. For instance, every medium to large-scale employer could invest in card readers and training for staff members within their human resources department. With estimates of 6m new recruits per year across the UK, where it has been estimated that 60% are employed by large firms, a speedier and cost effective means of immigration verification could result in substantial benefits in time and effort saved by personnel departments. However the investments may prove to be expensive for even large firms as this could centralise hiring processes across large organisations where one office would be responsible for card verification. For instance, if a large firm hires someone in their smaller Bristol office, either the Bristol office would require trained staff to scan the card and verify the validity to work, or the verification process would have to be sent on to another office where such access to the NIS has been implemented. Additionally, the benefits for this scheme would be delayed until a substantial portion of the population is registered on the NIR and have been issued with cards, although the Passport Validation Service and an equivalent for visas may provide an appropriate interim solution.

If employers were able to read the details on the card or the NIR into their own systems, this would also speed up the CRB process. Disputes over applicants' personal details costs the CRB a substantial amount, with some estimates reaching £400,000 per year. As staffs at both the CRB and the employers' office have to deal with these conflicts, the resulting reduction in staff costs could have substantial benefits.

In an attempt to understand some of the financial effects of these developments, we approached a large UK employer. Their response was particularly enlightening. Presuming that the NIS would provide 100% proof of ID, and presuming that their employees would need both right-to-work and CRB verifications:

- for Right to Work in the UK: Estimated checking time for potential new employees, to check, photo copy, file and check any concerns. Approximately 40,000 potential new recruits x 15 minutes = 10,000 hours per annum, at an average cost of £15 per hour = £150,000. A cost-effective means for conducting the verifications through the NIS could provide a substantial per year saving in the order to £150,000.
- for CRB Checking: There were in the order of 3600 checks done in 2006. With estimated administration time per check at 1 hour, cost per check excluding CRB cost = £15 x 3600 = £54,000. Additional cost from CRB check is approximately £130,000. If scanning the ID document will give sufficient information to make a judgement as to whether or not a person can work with vulnerable adults or children, then total saving to this organisation would be £184,000 per annum.

The CRB costs are not likely to disappear but they could be significantly reduced, and as a result the benefits to employers would still be substantial. But apart from these quantifiable costs, we were informed that employers would find it much easier to meet their legal obligations, would incur fewer administrative charges, less double checking would be required as documents would be easier to understand, employers would not have to keep copies of documentation, and waiting times would be substantially reduced.

Before we could estimate cost savings across the UK, however, we would need to be more certain of a few issues:

- what is the nature of the current burden upon small, medium, and large organisations over a period of five years?
- what are the integration costs over a five year period for each type of organisation?
- what are the costs of providing other interim solutions and whether these are sufficiently adequate? e.g. the Passport Validation Service
- will employers be able to waive their liability if they use the NIS at the time of employment, and will card expiry dates have ramifications on employee management?
- what will the costs of CRB checks be under the future regime?

Apart from the problem of mere compliance, the benefits of which are reliant upon the NIS, identity assurance can provide much more to the UK economy. There are additional opportunities for employers, who are not entirely reliant upon the NIS, because they can develop their ability to manage information and identity assurance across their organisations. Through appropriate identity management, administrative costs can be reduced with a once-only identity created and descriptive facts tied to it maintained such that descriptive data can be used to auto-populate and validate registration data (such as a loan request) and/or business decisions about a user request). That is, the facts linked to the identity have value, not the identity itself.

Previously identities were created by many departments (Human Resources, Finance, IT support, etc.), and sometimes in many regional locations and for different purposes. In fact these identities were often stored physically in a number of different places on different platforms. As users moved from place to place and job to job during their careers, and as processes affecting them (the facts linked to them) grow in volume and importance so to does the cost of maintaining them. This cost has been hidden somewhat thanks to being distributed across an organisation.

If organisations were able to improve the effectiveness of identity management, through a single enterprise directory, this could lead to substantial cost savings and efficiency gains. Critical transactions tied to a simplified and streamlined process will occur faster, generating additional market opportunities and therefore additional revenue and taxes. There exists a by-product that arises from bringing more structural empha-

sis on having one user across functions and boundaries, whether organisational or geographical, which is that businesses are forced to better understand the way in which users cross service silos and therefore eliminate redundancies in process. Processes that were previously impossible, or had latency built-in as they crossed business domain boundaries, are rendered faster and more convenient for users. As well as the direct administration advantage this represents an indirect (but directly associated) cost and service (or revenue) gain.

In turn, businesses would no longer have to build authentication processes into every application because the identity issuer will do that for them. Furthermore, as long as end-point security and access control is properly managed the possibility is opened up for transacting across public networks and in open communities because greater certainty as to the exact parties in a given transaction, and the encryption of data between them allows for the use of non-proprietary systems.

This also opens the possibility of sharing services between organisations whose primary emphasis becomes one of knowing the user and the context in their specific transaction relationship, rather than "defending the boundary" and tightly containing transactions within an application or domain. By introducing descriptive facts such as a change in status or social condition (such as the loss of a job) into business decisions may reduce risk and loss. The scale of web-enabled business and the volume of information transactions across networks is now allowing us to develop a more statistically relevant view of on average how many incidents are likely to occur as a result of failure to apply responsible approaches to identity assurance, and what the impact of an average "event" will be.

Likewise, pattern matching through combining statistically relevant data points together to draw conclusions at the network layer, which allows organisations to generalise intelligence around user-centric transactions, can calculate the risk that any given user is who they say they are. For low risk and or low value information exchanges this can even avoid the intrusive and expensive need for active authentication.

If identity and authentication processes were universal, corporations would not have to invest in a suite of products in a layered environment to protect against fraud. Annual spending in this domain is already in the billions.

As a result of these changes in organisational practices, hundreds of pounds per user per annum of direct cost can be saved, depending on the degree of improvement towards complete identity assurance compared with existing structures and approaches. According to studies undertaken by one of the largest firms in the UK, the implementation of such a scheme within their own organisation saved the firm £88m per year. The firm identified a variety of benefits including:

- Administration: Labour expenses to provide electronic access (identity, credential, privilege, and account configuration), supply resources and manage passwords.
- Lost Productivity: Paid for but not effective end-user hours waiting for access and resources, or waiting for password reactivation.
- Assets: Capital write-off and cash exposure (such as monthly cell phone or pager accounts not closed) assigned to terminating users.

The firm concluded that:

- Looking at 'hard benefits', through Improved IT efficiency, reduced help desk cost, and quicker access, the firm calculated savings of over £300 per user.
- If 'soft benefits' including IT Cost Reduction, User Admin Cost Reduction, Increased User Productivity, and Asset Management benefits were included, the annual benefit per employee can reach as high as £1900.

Based on studies conducted at five client sites, the firm found that, on average, avoidable expenses were as high as £60 per internal user. The firm calculated that on average, across the organisation each employee has six electronic identities and accounts that must be maintained, leading to costs of over £150 per user per year. The implementation costs, it is argued, would be recouped in the first year alone for all enterprises with 2000 or more users. The benefits round in one client site, involving a large European employer, were almost entirely process benefits. But without a trusted identity, they could not be achieved. Therefore, identity management has a huge opportunity cost, or more correctly, benefit that without it other capabilities can not be delivered. Not all of this necessarily requires a single national identity scheme, but instead presumes that the practices are rooted in good identity assurance.

In that firm's experience, the total process benefits are extraordinarily large - indeed so large that for a single corporation, let alone the national economy, they can appear to be non-credible. Large numbers associated with potential cost saving claims generally become credible on further analysis reflecting the comprehensive nature of some of the changes described above. Calculating the effects of these measures across the UK economy requires further research but it is highly likely that the long-term benefits will result in billions of pounds of benefits per year.

It is important to note that there are necessary costs in implementing these types of solutions that may erode some of the benefits. A number of oversight and support organisations will be required, including a Security Office, Regulatory Audit and Compliance Office, Privacy Office and help/support desk.

Fraud Reduction

If private institutions could properly review identity details then it would be possible to increase efficiency across the UK economy. We have already seen that there is a business case here, and this can be evidenced by the strong take-up of the 'Passport Validation Service' being run by the Home Office Identity and Passport Services. The PVS service is already being used across a variety of government departments and some in the private sector.

Experts and industry bodies have estimated that the NIS could reduce some types of fraud by up to 50%, but we must be careful when drawing on such assumptions. For instance, telecommunications fraud, where individuals order a telephone service without the intention of paying for it, could be reduced by 50% if stronger identity checks were required, and the estimate cost of this fraud is £372m per year. Yet how exactly the NIS will perform this task of identity assurance in this business process requires further investigation.

Complexity emerges in the integration stages. For instance, for banks to integrate the NIS into their practices, through purchasing scanners, training staff and developing communications systems. With 16 banks operating within the UK offering 11,025 branches, each branch would require a scanner and trained staff. While these costs are likely to be quite high at the start-up, particularly depending on the technology deployed, the benefits in reduced fraud could be quite substantial once the NIS is fully deployed. According to data that we have reviewed, insurers lose over

£22m per annum to fraud, and £3m by Building Societies. Some estimates show that the time spent by financial institutions in dealing with identity theft costs more than £22m per year. Account take-over fraud and credit card application fraud amount to more than £93m per year; and loss to pensions is more than £15m. Fraud at ATM withdrawals and bank withdrawals, according to APACS figures from 2003, is £96m. Again, if the costs of integration are kept low, the benefits to the financial sector will be substantial. For this to take place, a genuine public/private partnership is required at all stages.

Before we could estimate cost savings across the UK, however, we would need to be more certain about a few aspects:

- what is the nature of the current fraud burden upon small, medium, and large organisations over a period of five years?
- what are the integration costs over a five year period for each type of organisation?
- what are the costs of providing other interim solutions and whether these are sufficiently adequate? e.g. the Passport Validation Service, deceased' online checks, etc.
- will private entities be able to waive their liability if they use the NIS? Will expiration dates have effects on account management? e.g. will a bank have to discontinue an account if the card expires?
- what are the envisioned deployment schedules and when will benefits start accruing?

Separate from satisfying the current legal requirements upon organisations, there are other benefits to implementing identity assurance schemes. Sufficient thought about identity management and how it can be integrated into business and commercial transactions could lead to even larger gains by reducing fraud and increasing both consumer convenience and confidence. If properly implemented, this could result in reduced threats of impersonation and identity fraud, which has substantial financial impact if processes are integrated to leverage maintained descriptive facts.

Depending on circumstances, if applications are tiered for their sensitivity, many of the things a user does frequently may not require any real

time access control whatsoever avoiding associated administrative processes, and making the navigation of the session very easy even as the user engages multiple businesses. On top of this, the business process between companies that do not even have a relationship could be integrated. For instance, the user could order a retail vendor to debit a checking account at the bank named as a descriptive fact tied to the identity to trigger funds transfer before the session terminates, or the vendor could confirm payment prior to launching a shipment process. Avoiding redo and process confusion would reduce some internal costs. According to one estimate, citizens and consumers already have around 1,000 different identity registrations stored in a wide variety of places for a wide variety of purposes. If the user senses that the processes are embedded with greater security this would go some way to reversing current trends that have scared consumers away from online transactions, which according to reports has resulted in billions of lost commercial opportunities.

Other sectors

With widespread use of the NIS, there will most likely be a number of benefits across various sectors of the UK. The travel industry will gain from reduced processing time at check-in and registration, for both airlines and local public transportation. Payment for road tolling will likely be streamlined, and online access could be enabled. Similarly, retail transactions could be secured through the use of identity assurance on large transactions. These and other benefits can be achieved through appropriate measures on identity assurance and the concerted development of a national identity assurance infrastructure. The exact benefits are unknown but the increased consumer confidence, security in organisations and across organisations, and new business models that can be developed through confident and proportionate exchange of credentials and identity information could result in substantial savings, efficiencies and opportunities for the UK economy.

But quantifying these measures requires far too much speculation and we are alarmed that there has been so little discussion on this matter in the UK, even as other countries have spent nearly a decade conducting public-private dialogues, consultations and developing solutions. And while discussion in the UK has focused on the NIS, as we have discussed above, we are unsure whether the NIS needs to play an integral role in many of the benefits that may accrue.

It thus remains debatable as to whether the NIS or some form of national identity scheme is essential to this process. The lack of a national scheme inhibits process cycle speed and process responsiveness because individuals/consumers need to register for an identity for every new relationship, a process that takes anywhere from minutes to days depending on the transactions the account permits and the risk the processor faces. The unclear liability regimes will inhibit the entry of identity and credential providers into the marketplace. This type of infrastructure problem can only truly be solved by government through the establishment of at least a legal framework, with appropriate administrative breadth and investment capital, if necessary. This does not necessarily mean that the national identity scheme must to be a national identity provider per se, let alone the national monopoly, but it will need to be central in creating the conditions to make it happen.

Even still, there are a number of data life cycles (create, confirm and approve, update, suspend, reactivate, remove, archive) that have to be managed including the user and organisational affiliations that recognise the identity, rules that simplify privilege management, and the according entitlements. This is a much more complex problem operationally than the mere creation of an identity. A national infrastructure will need to consider the policy regime and the resources required so that these billions can be gained, provided that they are not offset by substantial costs.

Lessons from Abroad

Other countries and environments have long been conducting the necessary dialogue and research into identity assurance practices, procedures and techniques. We can learn from their experiences.

Sweden

The Swedish approach shows how much of the technological and development risk can be carried by the private sector with negotiated solutions with the public sector. Swedish citizens are active on-line users. For instance, in 2005 the number of income tax declarations performed electronically doubled to a third of all declarations.

Instead of issuing a unique identifier for all e-government services, Sweden opted for a market driven approach integrating standards from the private sector. With this model, private vendors rather than government agencies have carried the heavy investments. The market-led electronic identification procurement policy has no upper limit for suppliers thus, in principle, forcing government agencies to accept multiple software clients and electronic identification certificates. In practice however, the multitude of standards has not materialised as most suppliers use the same formats. When designing the software, particular attention has been paid to compatibility and hence the electronic identification solutions used in private banking services are accepted for government services and vice versa. As a result, more than 5 million Swedish electronic banking customers can now use their electronic identification to access the various services offered by both central and local government agencies as well as private businesses.

The electronic identification solution is based on a certificate that is stored on the citizen's computer or a smart-card solution where the information is stored to a credit card sized piece of hardware. The Swedish Agency for Public Management (Statskontoret) has signed an agreement for implementing a standard electronic signature with the six largest banks. Citizens who have online access to their bank account can freely download the software. The hardware solution is offered by the telecom operator Telia Sonera and the largest Nordic retail bank Nordea Bank. Nordea bank also offers their credit card account-holders a chip-based credit card that can also carry the electronic identity used for government services. The suppliers of the certificate are paid every time an identity assurance service is used.

Challenges remain in this market-led solution. As government agencies pay vendors per transaction, the cost of new services is difficult to discern, and thus agencies lose the incentive to introduce new services because of the higher financial risk involved. To mitigate this, the Swedish Agency for Public Management has struck an arrangement with a number of private vendors to supply verification services at a fixed cost. The deal only covers the largest agencies and regions, and hundreds of agencies and municipalities still have to pay per transaction, but it is not however expected to create major disruption in the innovation of new electronic services.

Hong Kong

The Hong Kong case shows how a limited-purpose strategy for identity assurance can be expanded into a national infrastructure. The Hong Kong ID card was initially introduced as a measure to deal with immigration and border control, in particular to manage the large temporary population and mass tourist flow from Taiwan. Policy-makers envisioned an expansive scheme, however, and as a result they implemented an advanced smartcard-based scheme as it cost only 10% more than the less flexible model and could be used eventually across multiple government services. The card itself only holds minimal data while the remaining data is held in a number of government databases.

This ability to include additional services on the card has enabled a number of other programs to make use of the identity infrastructure. The Hong Kong Post is now using the card, as it added an "e-Cert" option by which the card could be used to create digital signatures. Card-holders can visit kiosks located around the city to update the extra e-Cert information accessed by the card. In turn, online banking, stock trading, and on-line payments are thus enabled and made more secure and convenient.

Malaysia

Malaysia has an advanced identity card that has branched out in an attempt to become the core component of a national identity assurance infrastructure, but there were some obstacles on that path. Malaysia has long had a national ID card, but in 2001 moved towards a smartcard scheme to replace both the older ID card and the driving licence. The card is called 'MyKad', or Malaysian Card, and is also referred to as the Government Multi-Purpose Card.

The chip on the card originally had a 32k memory storage, but the next generation card consists of a 64k chip. The card is voluntary, and as a result the government has found it difficult to convince citizens to upgrade to the new chip-card, and went so far as to introduce a lottery-prize system for those who applied for the new cards (though this was recently abandoned). The new card's capacity would permit the storage of multiple certificates, issued for specific government services. The chip contains a thumbprint and other personal information, including basic health information. The plans were that the card would be used to pay road tolls, to access automated teller machines and also act as an electronic-purse. As a result, the card would be more of a 'wallet', acting as a national ID, passport, driving licence, health card, an e-Purse and ATM card, to enable contactless road tolling by placing the card into a transponder in the vehicle, and finally to enable remote authentication using a digital certificate. It also has the option for a payments scheme called 'Touch n' Go' where money can be loaded onto the card at a bank and then used for small payments.

The private sector has been reluctant to integrate their cards into the 'wallet' because of security concerns. Banks have dissuaded customers from using the card for banking purposes due to the same issue. Cardholders were also concerned that if they lost their identity card they would also lose access to their bank accounts. Instead, banks have added functionality to banking cards to make them more appealing. Similarly, according to reports, Malaysian police have insisted on asking for driving licences instead of the identity card because they lack the readers necessary to scan the driving licence credential off the smartcard. Less than 15% of the population have added the licencing functionality to their card. Also, reports indicate that few hospitals have the capacity to read the data.

Despite this, however, there are plans to implement digital signature technologies on the card to enable on-line transactions. There are also plans to introduce loyalty schemes for retailers to link to the card.

Canada

The Canadian government has for the past six years been leading discussions with industry, academia and civil society both in Canada and abroad regarding identity assurance, leading to its consensus-based 'authentication principles' that will guide future action by government and industry. The principles were devised through a number of meetings held around the

country since 2000, and were also informed through Canada's leadership at the Organisation for Economic Co-operation and Development (OECD).

The goal of the work, led by Industry Canada, was to devise a set of principles at the 'broad, technology-neutral policy level' to foster competition and ensure a well-functioning market place. The vision was to lay the groundwork for an industry-led approach to authentication, and develop a set of principles to guide development and use of authentication services in Canada. Yet the guiding principle for digital identities is firmly founded in end-user control over identity information. This work resulted in six principles that outline the responsibilities of participants in the authentication process, consideration of risk management, security, privacy, disclosure requirements and complaints handling.

The technology-neutral approach permits the re-assessment of the principles in light of new technological developments, where the participants in the working group discussions can consider the need for additional policy instruments as the need arises. The primary purpose of this approach was a sense amongst the Canadian officials that technology independent policies are needed for establishing assurances for identities in a 'fit for purpose' way.

Business Policy Leadership

The Transatlantic Secure Collaboration Program is a prime example of an industry-led enabling infrastructure that permits cross-boundary identity management. New European and U.S. regulatory and contractual requirements demand greater control of information in collaborative activities between companies and with governments. The requirement for being trustworthy by evidencing greater security, providing quality data and having auditable risk management is the underlying imperative for any leading organisation involved in collaboration, which wishes to retain or increase its market share. This perceived need led to the TSCP. Its aims are to reduce risks involved in a cross-industry, international collaboration. This will be enabled by providing a cost-effective secure model to support a collaborative environment, and creating a re-usable, standard means of secure collaboration to reduce overall integration complexity, coordination time and collaboration cost.

TSCP is working to support the development of an International Identity Proofing and Vetting Framework. It is working actively on finding ways to satisfy Identity Management regulations - primarily the U.S. Government's HSPD12/FIPS 201 - and is working with the UK government to develop plans

for its identity management in line with U.S. regulations. Current UK MOD policy for its information sharing with industry is to be Transatlantic Secure Collaboration Program compliant, based on PKI. Current and emerging U.S. regulations and policies require conformance of data standards, unique identification of items, compliance with the Department of Defense portal for all payments and mandatory use of DOD-approved PKI digital certificates. Some other European governments are considering similar policies.

As companies and governments are already implementing identity management regimes, bridges are required to cross these organisational boundaries. Several national bridges are being devised. Education, pharmaceuticals and aerospace and defence sectors are also developing compliant bridges in response to governments' policies. The Aerospace and Defence sector has developed one such bridge to ensure organisations' trust regimes have common policies and also act as a means for one organisation to check that a certificate from another organisation is still valid. Even still, the bridge does not receive, transmit or store company data.

Other cases

In our discussions with experts from across Britain and around the world, we were informed of other world-leading processes that we were unable to properly research and report here and we recommend further research on these: Norway, New Zealand, Asian APEC countries and the U.S. and its work through the Federal Trade Commission.

Conclusions and Next Steps

While many of the leading countries and companies have long been considering identity management and national infrastructures, we are alarmed by how little discussion has taken place in the UK. Perhaps perversely, in the UK the national dialogue to date first focused on the needs of law enforcement. Then the needs of government departments were considered. Now the dialogue between government and business is focusing on compliance around the National Identity Scheme. This discussion will have to transform radically to enable the emergence of a truly national identity assurance infrastructure that citizens, consumers, and businesses will want to buy-in to, engage with, and adapt to their own needs so that it will pervade the UK economy. If this occurs the economic benefits will be enormous. Far more research and discussion is urgently needed, yet we have little doubt that the yearly benefits, coming in terms of both cost savings and efficiency gains will be in the order of billions of pounds.

Much work is required before such an infrastructure emerges, and the UK can throughout this process learn much from international experience and leadership. A home-grown approach is required, however, and this must be done soon before it is too late, rendering the UK not only the leading environment for fraudulent activity, but impeding UK business in the global competitive marketplace.

How exactly is such a process to be established? The political debate must be moved away somewhat from the NIS. Although it has a large role to play in a national identity assurance infrastructure, it is merely one piece of a much larger and more sophisticated problem. As we have shown, there are by far many more benefits to be achieved through dialogue with UK businesses, and much of this discussion need not centre on the NIS. As a result, for the emergence of a dynamic economy the NIS must be seen as a promoter of identity assurance, rather than the monopoly over identity. The UK must establish the narrative and the discussion around how and why a national identity infrastructure is needed, can be enabled, and how it can be delivered. There is no predetermined outcome for this discussion. In our own consultations there was much uncertainty about what this infrastructure would look like, what role the various existing institutions would play, and how auditing, consumer protection, and enforcement would be managed within a distributed environment such as the UK.

Regardless, such a discussion must take place now, and solutions must be implemented soon. As we are all certain of the risks of fraud and the need for legal compliance, we cannot wait for solutions to organically appear sometime in the next decade when in reality benefits can only follow from near-full deployment of the NIS. Immediate and interim solutions must be promoted, stop-gap measures considered, market innovations tested, and consumer protections implemented. In this report we have identified a number of these measures that are already being considered and implemented.

In this dynamic process of promotion, testing and implementation a number of principles may yet emerge that, as evidenced in Canada, could guide further and future action. This level of innovation and activity would create a national movement to identity management that would educate consumers about their rights and their capacity to control their identity information. It would demonstrate how consumers could seek repudiation if abuse takes place, thus enabling business to move into identity assurance with confidence of their legal liabilities and with vigour regarding new market opportunities. All of this while enhancing interfaces between government and citizens, between government departments, and amongst business communities.

It has been suggested to us that the UK should create a long term working group on identity policy. The emphasis of this group's work might be to promote identity assurance policies across the UK economy for the purpose of increasing confidence in information management, while opening new opportunities for business. Based on our consultations, we conclude that particular emphases in such an initiative should be placed on consumer protection, business-to-business transactions, and flexible movement of people and identity data.