

**Information
Assurance
Advisory Council**



**IAAC's Identity Assurance
Programme 2006-2008:
Concluding Report**

September 2008

www.iaac.org.uk

The Information Assurance Advisory Council (IAAC) is a private sector led, cross-industry forum dedicated to promoting a safe and secure Information Society. IAAC brings together corporate leaders, public policy makers, law enforcement and the research community to address the security challenges of the Information Age.

IAAC is engaged with Government and corporate leaders at the highest levels; it produces innovative policy advice based on professional analysis and global best practice.

Corporate Sponsors



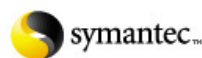
Anite



Microsoft

NORTEL

RSA
SECURITY



UNISYS
imagine it. done.

Strategic interaction with Government is through a Government Liaison Panel comprising representatives from CSIA, CPNI, CESG, DBERR, SOCA and MOD.

Disclaimer

IAAC's findings or recommendations should not be taken to represent the views of any individual member or sponsor, whether government or private sector.

Contents

EXECUTIVE SUMMARY	4
FOREWORD	7
INTRODUCTION	8
THE INITIAL CONTEXT IN THE UK.....	8
IAAC'S IDENTITY ASSURANCE PROGRAMME	10
SUBSEQUENT DEVELOPMENTS WITHIN THE UK	11
RETHINKING WHAT THE UK MIGHT WANT TO ACHIEVE	12
PROVIDING THE REQUIRED LEADERSHIP	13
THE WAY AHEAD	16
PHASE I – REQUIREMENT.....	16
PHASE II – DESIGN	17
PHASE III – OPERATION.....	20
GLOSSARY	26
APPENDIX - LINKS TO RELEVANT IAAC AND OTHER WORK.....	27

Copyright © 2008; all rights reserved.

Executive Summary

This report provides IAAC's view of the strategic risks relating to the use of electronic personal identities within the UK in the early 21st century. These risks create a number of challenges for the UK in establishing safe and secure identity systems for its citizens. Within this report, IAAC provides its view of the situation facing the UK in 2008 and its recommendations for the key actions that need to be taken, under UK Government leadership, in the immediate future.

The transformation of UK society into an increasingly digital society has been taking place over a number of years. The growth of the Internet and domestic broadband connectivity has introduced great new opportunities for economic development and for enhancing the lives of the citizen. The UK Government, for its part, responded in 2005 with "Transformational Government", a call for government services increasingly to be delivered electronically.

The authentication of the individual consumer is common to many on-line commercial activities. General practice is for the user to be identified by a convenient label such as their e-mail address or an assigned customer number. The UK's transformation to a digital society will necessitate this simple identification and authentication of the consumer evolving into a much stronger and more trustworthy authentication that the individual person to whom an electronic activity relates truly is the citizen he or she claims to be.

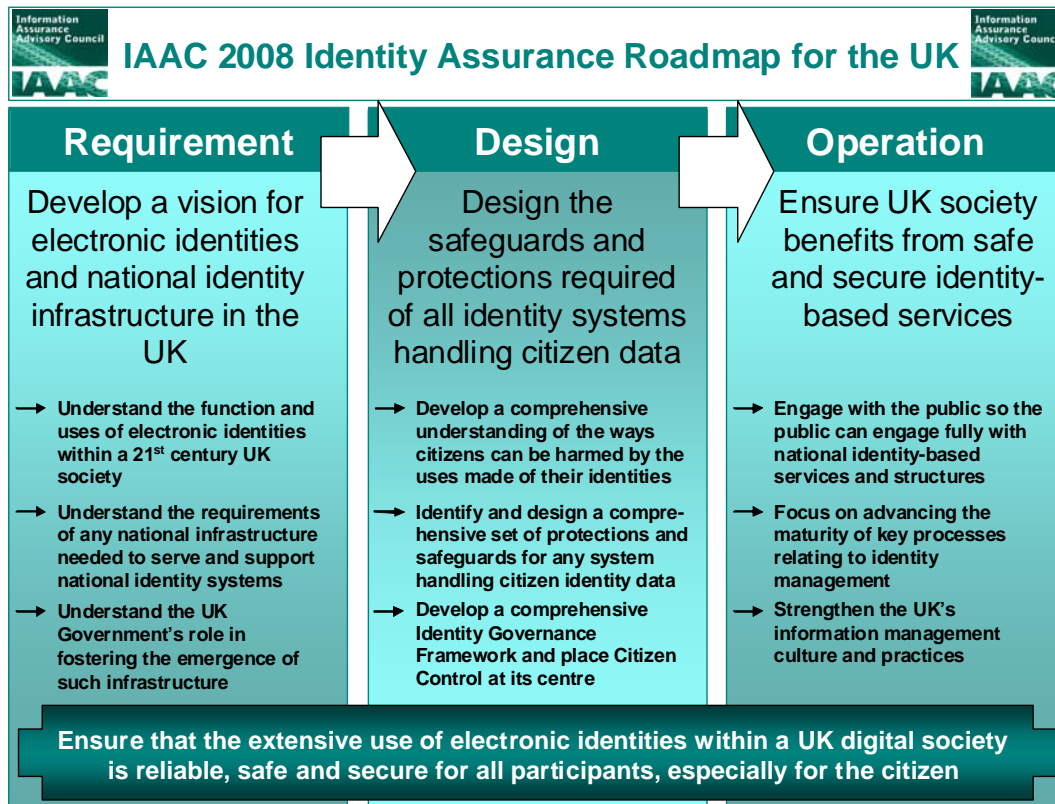
This requirement for trustworthy authentication of the citizen is likely to lead to each citizen having a legally-recognised electronic identity, probably as one of a number of electronic identities they manage. Trustworthy identities will be essential for the core systems and structures that will underpin the societal rather than purely commercial aspects of the UK digital society. It is expected that this will then lead to the emergence of some form of National Identity Infrastructure (NIID). This infrastructure will take the form of a variously integrated mesh of public and private sector large-scale identity management systems (IMS) bound together by a number of central bodies, structures and processes, collectively serving and supporting a wide variety of personal, commercial and governmental identity-based needs.

This move towards the wide and deep use of citizen electronic identities will be accompanied by significant assurance risks. These will include risks to the reliability and security of the identities themselves. They will also include a wide range of assurance risks to the information and systems used throughout society, as those systems become increasingly reliant on the trustworthiness of managed citizen identities. It is imperative, therefore, that Identity Assurance, the term used to describe the subject matter of ensuring the security and trustworthiness of electronic identities, should be understood in full by all who are involved in the development of identity-based systems for citizens.

This was the context within which IAAC launched its Identity Assurance programme in 2006. IAAC's goal has been to ensure that the extensive use of citizen electronic identities and the emergence of national identity infrastructure in the UK is reliable, safe and secure for all participants, especially for the citizen. Through research, workshops and policy debates, IAAC has brought together insightful contributions from a large number of experts across the field. IAAC has developed a deep understanding of a number of issues central to the assurance of identities, and has proposed a wide range of solutions to strengthen the reliability, safety and security of national identity systems and infrastructures within the UK.

Having followed its Identity Assurance programme for two years, IAAC now provides in this report its conclusions regarding the strategic situation for electronic identities within the UK. IAAC takes stock of the progress that has been made in the past few years and identifies what it considers to be the most important barrier that currently stands in the way of the UK making further progress. IAAC then develops its recommendations for the key actions that it believes need

to be taken forward within the UK. These actions are organised into three phases of activity and are presented here in the form of an IAAC 2008 Identity Assurance Roadmap for the UK.



IAAC's 2008 Identity Assurance Roadmap for the UK is as follows.

Firstly, UK public and private sectors need to work together under Government leadership to articulate a vision that describes the function and uses which will be made of electronic citizen identities in a 21st century UK society. Such a vision would:

- Enable focus and direction to be brought to the confusion of ideas and activities that currently exists in the field;
- Lead to an understanding of the structures, bodies and processes needed to support the extensive use of electronic identities within the UK. This would then lead to the requirements that national IMS (i.e. identity management systems which hold or use citizens' legally-recognised electronic identities) would need to satisfy if they are to form part of a successful NIdI.

This lack of a vision is, in IAAC's view, the most important barrier that currently stands in the way of the UK making further progress. Within the body of this report, and through the use of analogy, IAAC describes the form it believes such a vision should take and the key aspects such a vision should take.

Secondly, the UK Government needs to drive forward work on a number of topics essential to the design of successful national infrastructure. These include:

- The development of an Identity Governance Framework (IGF) to apply to all national IMS. Such a framework would ensure that the interests of all participants in the NIdI, namely the citizen, vendors and service providers, and the UK Government, are protected in proper balance.

- The definition of the protections, safeguards and support needed to make Citizen Control effective. Citizen Control is an essential component within the IGF. It serves to allow the citizen to take additional precautions, in situations where they feel this is needed, to ensure their safety and security when engaging with national IMS. Citizen Control has a very important role to play and it is imperative it is properly understood and supported by the designers of national IMS.
- The development of effective safety nets for national IMS. Safety nets to protect the citizen from suffering significant damage or harm when things go wrong are essential if the public is to have confidence in national IMS. In particular, there must be effective recovery and restitution arrangements covering a wide range of contingencies.

Within its Identity Assurance programme, IAAC has made many specific and detailed suggestions relating to the development of an Identity Governance Framework, Citizen Control and safety nets. IAAC recommends that the UK Government should develop an Identity Governance Programme to coordinate this work, and that it should, as part of that, take on board IAAC's many specific and detailed suggestions relating to the above topics, carrying them forward to completion and timely implementation.

Thirdly, IAAC believes there are a number of important areas of activity on which the UK should focus attention as the operation of national IMS expands. These include:

- Engaging with the public in an informative and educational dialogue. The public needs to understand what national IMS have to offer them and how they can benefit from them. They also need to understand the risks to them personally and what they can do to keep their electronic identities safe and protected;
- Improving the maturity of the key processes on which the effectiveness of national IMS will rely. The success of national IMS will depend as much on key processes (such as enrolment and identity repair) as it will on the suitability of key technologies. The current focus of R&D on technologies has allowed key processes, especially those affected by Social Science considerations, to remain relatively under-developed.
- Developing a strong information management culture with robust information management practices across the whole of the UK. This is an imperative for all government departments and public and private sector organisations which will use national IMS, to ensure that the operation and use of such systems is reliable, safe and secure and is deserving of the citizen's trust. It is also very much needed across the population of the UK to ensure citizens play their part, an essential part, in keeping their electronic identities safe and secure.
- Updating the UK's legal, law enforcement and judicial frameworks and structures to meet the needs of a digital society. This includes adapting them so that they can respond to change occurring at much greater speeds than policy and legislative process are normally equipped to accommodate.

The recommendations made within this report are either for the UK Government to address or for the UK Government to facilitate and co-ordinate. The necessary leadership has to come from the UK Government. IAAC, in support, has contributed many ideas that it believes are crucial to the UK developing safe and secure national identity-based infrastructures. These recommendations will also be of great interest to other parties active in the field, including technology providers, digital identity service providers, and subject matter experts. They are of most significance, however, to the citizen who is, in all of this, not just the principal subject at the centre of the digital society and the main recipient of its benefits, but also the main bearer of its risks.

Foreword

As Chairman of the Information Assurance Advisory Council (IAAC), I am delighted to be associated with this Report on the conclusion of the Council's Identity Assurance Programme, carried out over the past two years.

The nature of information usage and handling is changing, but our approach to managing it is not. Government Departments are still assimilating the full implications of the wide range of major issues raised in the reports that followed the recent, serious, data losses. These contained many common themes that are equally applicable to the private sector. Each loss has undermined the confidence of individuals in the ability and commitment of Government Departments, agencies and their private sector service providers, to protect their personal data. The importance of this was acknowledged by Sir Gus O'Donnell in his foreword to the Cabinet Office Report on Data Handling Procedures in Government:



“No organization handling information can guarantee it will never experience losses. But people have a right to expect that their public services achieve and maintain high standards in this important area. Those involved in delivering those public services must work harder and be more effective to meet and exceed those expectations. Every loss or near miss must make us more determined. The action now underway will raise our game, but the task of improving information security will always be a continuing process.”

No area can be more sensitive to individuals than that of assurance that data relating to their identity is safe in the hands of government. This report is therefore most timely, making a significant contribution to understanding the fundamentals of Identity Assurance. For each of us this represents a challenge. What are we, individually and collectively, to do to develop and disseminate this knowledge? How can we do this effectively, in order to increase the level of professionalism and self-confidence amongst individuals at home and at work?

In commending this thought provoking report to its readers, I make a direct link between the importance of developing this knowledge, and that of imparting it, effectively, to the widest possible community of users and managers across the UK. This will be a major theme for IAAC over the coming months.

Sir Edmund Burton
Chairman, Information Assurance Advisory Council

Introduction

The UK has made significant progress towards becoming a digital society, a society in which many of the activities of the citizen's daily life are conducted on-line. Growing numbers of people go to work on-line, shop on-line, socialise on-line and take their entertainment and news on-line. The range and variety of activities, exchanges and transactions that are possible on-line is ever increasing.

Electronic personal identity plays a central role within the systems and practices used for these on-line activities. Most on-line exchanges involve some form of providing or proving a personal identity, even if that is little more than proving the ability to access a given e-mail address. Electronic identities often provide the link, direct or indirect, connecting on-line exchanges with the physical persons to whom they belong.

This widespread use of electronic identities has been readily accepted by the on-line population as a regular part of their daily lives, much as many people today accept the use of a car as a regular part of their lives. However, our understanding of what is needed to support this extensive and growing use of electronic identities and, in particular, to address the risks and enable such use in the future to be reliable, safe and secure, is still embryonic.

There is no equivalent to the Highway Code to help people recognise the warning signs they might encounter as they travel about the Internet, or to set standards for what is and isn't safe use of an electronic identity. There are no 'traffic lights' to control the flow of personal information at junctions where different parties want to head in different directions. There are no standard safety features required of the identity systems people use, the 'seat belts and brakes' that would allow people to go about their business on the information highways without their electronic identities getting bruised or worse whenever they come across a bump in the road.

Much good work has been undertaken relating to these types of issues over the past few years. However, there is still much that remains to be done. There are some very important issues that need to be understood and addressed before the UK will have an adequate grasp on the risks and will be able to build the structures and systems needed to enable the extensive use of electronic identities to be safe and secure. This report provides IAAC's view of the strategic risks relating to the use of electronic personal identities within the UK in the early 21st century. It also provides IAAC's recommendations for the key actions that need to be taken by UK Government in the immediate future if it is to answer the challenges of establishing safe and secure identity systems for its citizens.

The Initial Context in the UK

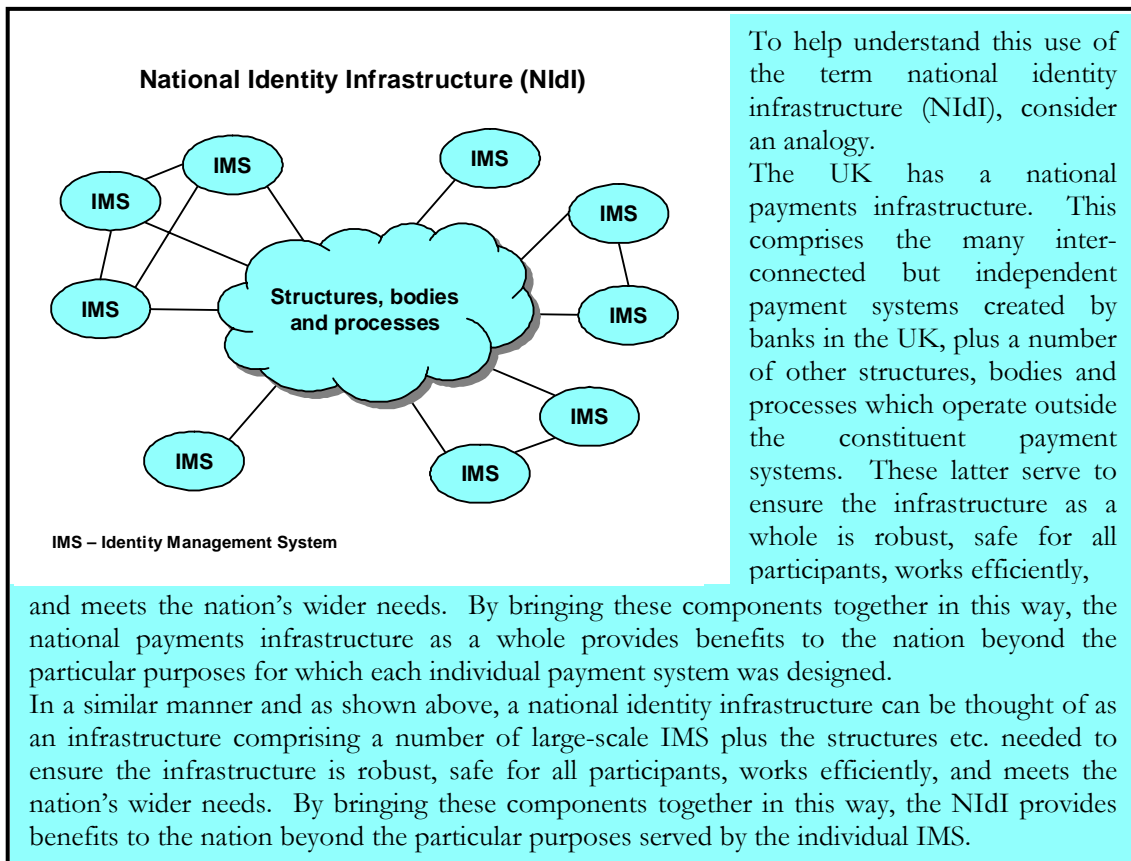
The transformation of the UK into an increasingly digital society has been taking place over a number of years, driven largely by the advent of the Internet and the growth of broadband connectivity, especially domestic broadband connectivity.

The UK Government, for its part, responded in 2005 with "Transformational Government", a call for government services increasingly to be delivered electronically¹. This was partly in response to, but was also to encourage, this transformation towards a digital society.

Proving one's electronic identity has emerged as a ubiquitous task within the digital society. Electronic identities, in one form or another, are a common feature of most on-line activities. If we are to be able to trust implicitly in the authenticity and reliability of the activities people conduct on-line, we will need to be able to trust in the authenticity and reliability of the identities people use.

¹ Please see the appendix at the end of this paper for directions to this Transformational Government work, plus to other related Government work.

This use of trustworthy identities will serve as a unifying principle across many of the core systems and structures that will underpin the UK digital society. Combining this need for trustworthy identities with the thrust of Transformational Government and with the political initiatives of the National Identity Scheme, it can be anticipated that the UK will witness the emergence of some form of National Identity Infrastructure (NIdI). This NIdI will take the form of a variously integrated mesh of public and private sector large-scale identity management systems (IMS) bound together by a number of central structures, bodies and processes, collectively serving and supporting a wide variety of personal, commercial and government identity-based needs. The UK Government's National Identity Scheme may or may not be one of the first components of that NIdI to be developed.



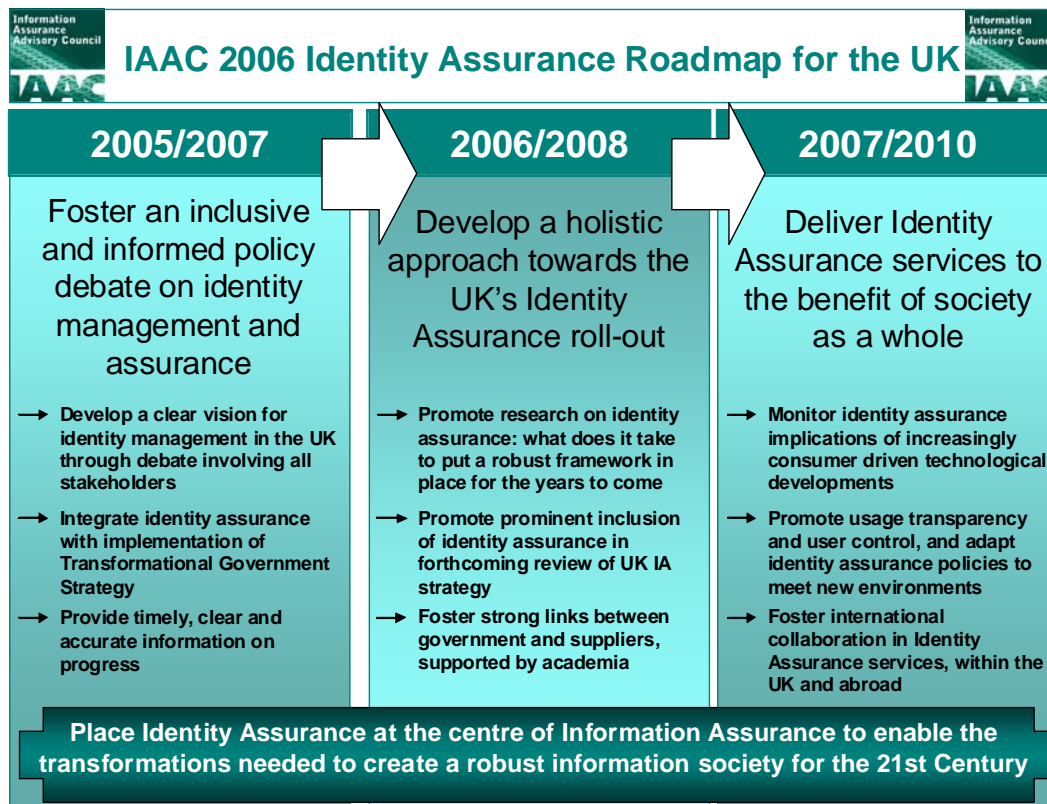
However, it is clear that this extensive use of electronic identities will be accompanied by new risks. Identity theft, on-line fraud, organised crime's exploitation of vulnerabilities, were recognised early as being significant threats to the public and to the nation. In addition, the concept of an emerging national identity infrastructure introduces further concerns of its own, for example regarding the non-intrusive gathering of identity data, maintaining the reliability and control of personal identity data, protecting identity subject privacy whilst not blocking progress, and the question of how to build and maintain the public's confidence in new electronic structures and services.

It became clear to IAAC in 2006 there was a need for a much greater level of understanding of a range of key policy issues. It was also clear to IAAC that established identity management techniques and practices would need to change significantly in the years ahead. Identity management had, up until that time, been concerned primarily with controlling users' accesses to private resources, usually on modest size scales within corporate IT infrastructures. It was clear that huge advances in thinking, approaches, methods and practices would need to take place if identity management was to be able to address the needs and risks of managing nation-wide public access to personal data-enabled services over disparately controlled public infrastructures.

IAAC's Identity Assurance Programme

IAAC's goal with its Identity Assurance programme has been to help ensure that the development of national identity-based services and infrastructure, whatever form those might take, does not endanger the UK. IAAC's primary objective has been to understand what would be required to ensure any emerging national identity infrastructure remains reliable, safe and secure for all participants and most importantly for UK citizens.

IAAC recognised that achieving this goal would require bringing together and co-ordinating a wide range of inter-related social, policy, technical and management aspects. In the middle of 2006, IAAC developed a "Roadmap for Identity Assurance in the UK"² in order to provide structure to the journey ahead.



The purpose of IAAC's 2006 Identity Assurance roadmap was to:

- Stimulate further dialogue, in the form of an inclusive debate encompassing all sectors in the UK, regarding the subjects of Identity Management and Identity Assurance;
- Clarify issues relating to the development of reliable, safe and secure electronic identity systems and structures, and to unveil areas of conflict that would need to be addressed;
- Suggest relevant areas for research and development;
- Highlight specific policy issues relating to the risks of identity management systems and structures coming together to form national infrastructure.

IAAC's view has been that fostering users' trust in the uses made of their electronic identities within on-line environments is central to making a national identity infrastructure successful.

² The paper describing IAAC's 2006 Roadmap is available from www.iaac.org.uk/Default.aspx?tabid=62

Having set out a roadmap, IAAC then embarked upon a two-year research programme that, building on from this view, focused on a number of key areas in which IAAC felt it could make a positive contribution. These were, primarily:

- Understanding the concerns and needs of the citizen relating to the use of their electronic identities within national IMS;
- Identifying how the UK Government should respond to those concerns and needs and how it should, as a result, set its approach.
- Developing specific solutions regarding the purpose, nature and requirements for Citizen Control and an Identity Governance Framework.

Subsequent Developments Within the UK

A number of paths have been followed by various parties within the UK since IAAC's release of its 2006 Roadmap. Two developments in particular are, in IAAC's view, key to understanding the difficulties the UK finds itself facing today.

- Much R&D work has been undertaken on various aspects of identity assurance, with many bodies contributing to the field. A large part of this activity has focussed on the solution space, and within that on the technological solution space, e.g. privacy-enhancing technologies; biometrics; authentication cards; permissions hubs, protocols for exchanging claims and attributes; federated architectures; and so forth. This technological bias is not surprising, but neither is it balanced. It is important for the UK to develop the social, policy, management and operational aspects of Identity Assurance, in order to achieve a comprehensive and sound foundation for further progress.
- The UK Government has continued to move forward with the construction of its NIS (National Identity Scheme). However, it is by no means clear that this initiative will result in a nucleus around which other large-scale IMS will want to coalesce.

There are a number of features of the NIS which give rise to this concern:

- The primary purpose of the NIS is to support national interests (national security, law enforcement, the protection of public order);
- The architecture of the NIS has been set from the start to be centralised;
- The design has been constrained by the need to leverage existing legacy databases (e.g. DWP's CIS³).

As such, key aspects of the NIS have been fixed in the absence of any substantive holistic assessment of the nation's wider NID requirements. There is a substantial risk that the NIS will not be suitable for participating in anything other than government purposes, and that it will not have the architecture to fit in with other constituent systems of the NID. These other systems will emerge in response to other purposes (e.g. individual consumer purposes), other objectives (e.g. the provision of commercially successful services), and other requirements (e.g. for successful business models, plus a multiplicity of service providers and access channels).

These two developments suggest that the road the UK is currently following might well not lead to the development of national infrastructure that will serve and support a wide variety of the UK's identity-based needs.

³ The Department for Work and Pensions' Customer Information System, holding in the order of 85 million records covering almost everyone in the UK, including the deceased and their beneficiaries.

It is also not clear that leaving it for the existing forces in play to work their way through (e.g. market forces and specific public policy initiatives) will bring the UK any nearer to this goal either. There are important differences between the skills and capabilities of the public and private sectors, for example regarding their understanding of customer needs, the risk management approaches they employ, and their ability to assign and transfer liability. As a result, one can expect that there might be significant differences, possibly serious incompatibilities, between the types of architecture and IMS functionality the public and private sectors will each develop.

The risk in this situation is that public initiatives such as the NIS and the many private sector initiatives that will be delivered over the coming years will lead only to a large number of isolated islands of localised identity infrastructure, created at great effort and expense and providing only limited economic and social benefit. It cannot be in the UK's long term interests for the infrastructures built to remain isolated and incompatible. To arrive at such a situation would mean that an opportunity had been lost to address the longer term needs of the UK digital society in a coherent, effective and efficient way.

Rethinking What the UK Might Want to Achieve

Much of the debate generated during IAAC's Identity Assurance programme indicated that the UK Government should think again about its strategic aims and objectives for the use of electronic identities in the UK. The Government should not only reconsider some of the particular details of its current identity programme but, more importantly, it should articulate clearly what it sees as its longer term aim for the UK. Where does the Government see current activity taking the UK, and what support does it believe would be needed to facilitate the transformation of the UK into a safe and secure digital society?

To this end, one idea which can be re-examined is the expectation that, in time, a number of large-scale IMS will naturally come together to create national infrastructure that provides benefits beyond the sum of its parts. Is this expectation misguided? Perhaps such coalescence is not the best way to maximise the benefits and reduce the risks for the digital society, and large-scale IMS will and should remain isolated and apart. Maybe the forms people's electronic identities will take, and the ways in which they will be used, will be too diverse.

There are arguments on both sides.

- Binding a person's physical identity to an electronic identity is not essential to enable electronic services to work. Chip-n-PIN is the most frequently used form of substantive personal authentication in operation within the UK. It enables people to perform non-trivial activities [issue financial instructions], and it is account-based not electronic identity-based.
- Making services identity-based is not essential for making them attractive to the public at large. There has been good take up of non-identity-based government services such as renewing a vehicle's car tax on line. The person renewing a car's tax does not have to be the owner of the car and does not need to identify themselves in order to have payment be accepted. There is no evidence to suggest that non-identity-based approaches are unnatural in the public mind or at a disadvantage with regard to the take up of the service by the public.
- It can be argued that an individual's identity would be better protected if IMS were not largely joined together. From this perspective, separation at the infrastructure level is an important safeguard for the citizen, given that no IMS can be 100% secure, whether run by the public or the private sector.

These are valid and substantive arguments. However, there are equally strong counter arguments.

- Looking across the range of digital services that will be used within the digital society, it is clear that there will be some which will need a person to have at least one of their electronic identities bound strongly to their legal physical identity. There are some essential services, primarily entitlement-based services provided by the public sector, which would be made extremely complex and clumsy unless each citizen were to have a unique electronic identity strongly bound to their legal physical identity.
- A fragmentary approach where each person can have several digital pseudonyms none of which serves as more than an index into a stand-alone database is not very different from the legacy approach we have today. This fragmented approach does not address the desire for portable electronic identities. In addition, it does not provide the convenience and efficiency it is believed the public wants of having the minimum number of different enrolment processes and different identity management regimes with which to comply.

The Crosby Forum⁴ approached the challenge of identifying the nation's requirement from a different perspective. In its report, the Forum confirmed that to maximise the potential benefits for an increasingly digital society the UK should construct a "universal system". By "universal system", the Crosby Forum meant a national-scale infrastructure encompassing all users, all types of transaction, frequent use of their electronic identities by each individual, common standards throughout, and enrolment free for the citizen.

Obtaining high volumes of transactions is, in the Forum's view, essential. It is the best, and possibly the only, way to achieve:

- The cost efficiency needed to support high grade assurance;
- Wide public acceptance of the use of electronic identities;
- The desired levels of convenience and ease of use for the consumer.

Importantly, it is also possibly the only way to address some significant risk issues. These are, in particular, to get consumers to look after their identity tokens or other means of access sufficiently and to contribute, as they must, to the fight against fraud and other forms of misuse and abuse.

The Crosby Report also confirmed that, in the Forum's view, market forces alone will not be sufficient to lead to the development of such a universal system. The UK Government will need to provide leadership, and will need to work closely with the private sector, especially the banks, if it is to achieve the level of penetration for electronic identities that it desires.

Providing The Required Leadership

The UK appears to be facing a dilemma. On the one hand, there is a case to be made, though not unequivocal, that the UK Government should facilitate the development of national identity infrastructure in order to maximise the benefits and minimise the risks. On the other, signs are at present that the UK is not following a path that will take it there. In this case, it is appropriate to ask the following question. What, in particular, needs to be done, whether by the UK Government or by others, to help the UK to make progress along the road towards one or more successful national identity infrastructures that will serve the national need?

IAAC's answer to this question is as follows.

All of the development work characterised above has been undertaken in the absence of a consensus regarding the function and uses of electronic personal identities within a UK digital society. **A consensus regarding the function and uses of electronic personal identities is**

⁴ Please see the appendix at the end of this paper for directions to the work of the Crosby Public Private Forum on Identity Management

absolutely essential before progress can be made. Further, to serve its purpose, that consensus must embrace both public sector and private sector uses of personal identity.

Because we lack that consensus, there is little understanding of what is needed to support the future uses of electronic identities, and in particular what is needed to ensure that those uses can be conducted safely and securely. Therefore, we cannot determine the characteristics required of any national infrastructure that might be needed to support those uses, nor can we derive the essential common principles which each IMS would need to satisfy if it is to participate within this national infrastructure. Clearly a comprehensive understanding of all the core requirements needs to be in place before the UK can make substantive progress towards bringing such national infrastructure into being and before developers of large-scale IMS can select the approaches and architectures their systems should adopt.

This lack of consensus has resulted in a confusion of many competing approaches, architectures and designs being proposed for the development of large-scale IMS. There is the user-centric camp vs. the organisation-centric camp, the centralised infrastructure camp vs. the federated infrastructure camp, those who want every citizen to have a single national ID card vs. those who believe the citizen should decide whether to have one, none or many ID cards, those who would hold identity information on a server vs. those who believe it should be held only on a token under the user's control, and so forth.

It is beyond question that there is a wide variety of different identity management approaches and architectures in use within the world today. Each of these is possibly a good solution to a specific set of requirements. However, without a shared understanding of the characteristics required of a UK NIdI and an agreed set of principles that the component systems would need to satisfy, there is no firm basis upon which the designers of national IMS can select between different approaches, architecture or designs for their systems. There are a number of weak selection criteria, for example Kim Cameron's so-called "Laws of Identity"⁵ (which are not laws at all but rather empirical statements of what was believed at the time to be good practice), but there are no agreed fundamental principles or requirements against which approaches and architectures suitable for national IMS can be chosen.

As well as hampering forward progress, this lack of a proper understanding of the nation's requirements has, at the same time, contributed to some of the confusion in present thinking. Take, for example, the topic of user-centricity. There is no clarity regarding what user-centricity properly means in the context of national infrastructure.

- Transformational Government called for the provision of public services to be more citizen-centric, meaning they should focus more on delivering the benefits citizens want to see and less on simply providing efficiency and convenience for the service provider.

User-centricity has since become a rallying cry for other aspects of the electronic provision of services, including for identity management. Debate regarding the role of user-centricity in identity management systems has, though, become somewhat polarised. IMS designs are commonly judged as being either user-centric or organisation-centric with there being no apparent middle ground.

However, while this debate has been intense, it has shed little light on what user-centric might properly mean in the context of national infrastructure supporting both individual citizen and common-good (e.g. law enforcement, national security) purposes.

Both the citizen (as private individual) and the government (acting on behalf of the public, i.e. all citizens collectively) have legitimate purposes that will need to be served and supported by a UK NIdI. For some of those legitimate purposes and in some situations, the

⁵ Kim Cameron's Identity Weblog and his Introduction to the Laws of Identity can be found at <http://www.identityblog.com/?p=354>

broader public interest will properly override the narrower private interests of the individual citizen. For example, the public interest in being able to investigate crime might, in certain circumstances, override the individual citizen's interest in maintaining their personal privacy.

If such overriding of citizens' interests is right and proper, what exactly does the term 'user-centric' mean in this context? It is clear it will need to mean something more complex and subtle than simply giving the user full visibility and control over the uses made of their identity data.

IAAC believes that it is the lack of a consensus regarding the function and uses of electronic identities which has frustrated progress and hampered the development of a clear understanding of what the UK needs from an NIDi or 'universal system'. If a vision could be formed based on a consensus regarding the function of electronic identities and how they will be used within a UK digital society, the UK could develop an understanding of the characteristics required of any national infrastructure. These characteristics would be those required to enable the NIDi to be successful at serving and supporting the agreed uses, plus those that would enable the UK to manage the risks which such an NIDi would introduce.

Armed with a comprehensive view of the core requirements, and of the rationale behind each requirement, the UK would then be in a position to move forward. It would be possible to identify what structures and bodies were needed to support the component IMS that various public and private sector parties would develop. It would then be possible to agree what was needed to bring such structures and bodies into being and, from that, to agree what role the UK Government should play in fostering their creation. In parallel, those parties looking to develop large-scale IMS would have a national context within which to position their plans, and a foundation from which to assess the capabilities and consequences of the different identity management approaches, architectures and designs they might employ.

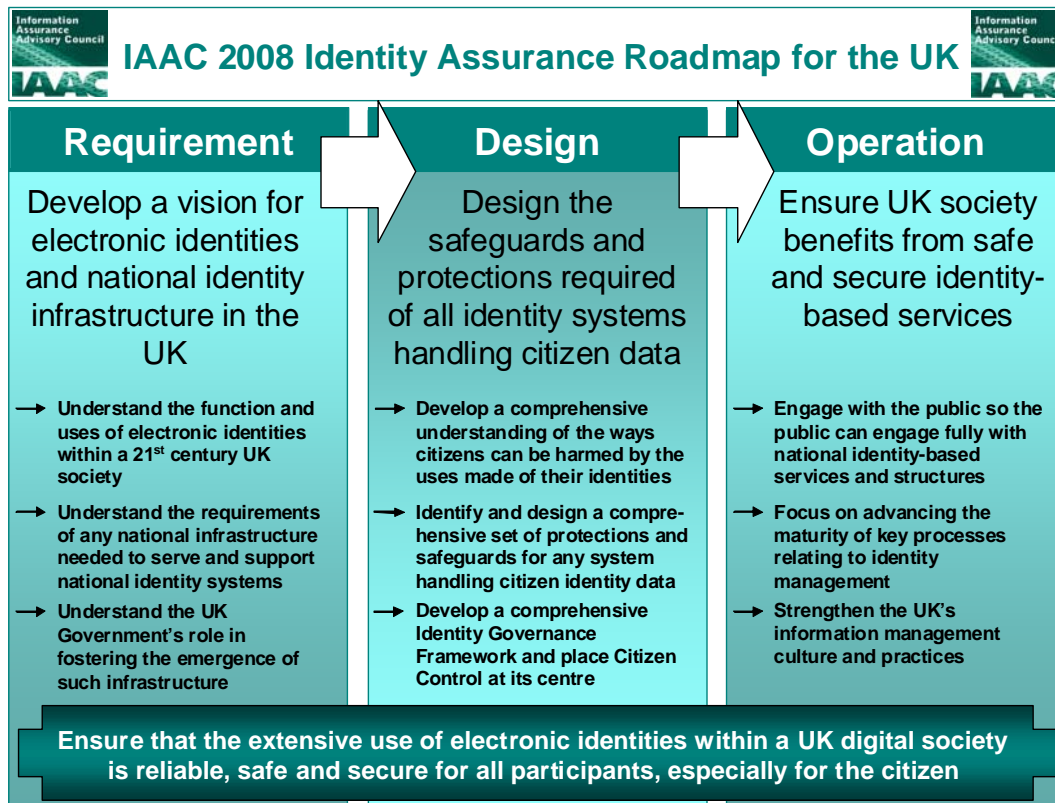
Developing this consensus and comprehensive understanding of requirements would enable the UK to answer a number of important NIDi design questions. For example:

- Should the citizen be required to have an electronic identity and to participate with national IMS (to serve national security and public interest purposes) or should participation be discretionary (to address the citizen's lack of confidence in their government's ability to protect them and their data)?
- Should each citizen be required to have a 'root' electronic identity (i.e., a primary electronic identity conferred and legally recognised by the state and based directly on their physical identity). If so, should the other electronic identities or digital personae by which the on-line citizen is known be linked to this root?
- What bounds should be placed on Citizen Control, given that the NIDi will be serving a mix of legitimate national and individual citizen purposes, and how would those bounds be applied?
- What responsibilities can be laid at the feet of the identity subject? For example, should the identity subject be made legally responsible for ensuring that their identity data is kept up to date and correct? If so, what penalties in law should be imposed on people who fail to do that?
- What is the appropriate architecture, or mix of architectures, for a UK NIDi? What are the key aspects of commonality between these different architectures that would allow the UK to maximise the benefits for the UK digital society without unnecessarily restricting future developments?
- Where there are trade-offs to be made, for example between anonymity and the desire of the state to be able to identify individuals, or between privacy and auditability, at which

level do relevant decisions need to be made (at the policy, design, operational, or management level)? Which trade-offs need to be fixed nationally for all component IMS and which can be selected on a per-transaction basis by the user?

The Way Ahead

IAAC has been following its Identity Assurance programme for two years, facilitating policy debate and research in support of the development of identity-based services and infrastructures within the UK which are reliable, safe and secure. In IAAC's view, the UK is facing a dilemma, as described above, and the presence of this dilemma is hampering further progress. IAAC believes that the way to resolve this situation is for the UK Government to provide the leadership and vision which has been missing so far. Resolving that dilemma would remove the barrier and open the path for further progress. Many actions would be needed as part of making that progress. The key, critical actions can be sorted into three phases of activity. These phases address, in turn, fundamental issues of requirement, major issues of design, and important issues of operation. IAAC's view of the way ahead is presented in the form of a 2008 Identity Assurance Roadmap for the UK.



Phase I – Requirement

The UK Government should, without further delay, lead the development of the vision for electronic identities and the requirements for national identity infrastructure as discussed and described above. This would provide the much needed common foundation from which other discussions could start and a centre around which other activities, such as R&D work, could revolve.

The UK's current situation is one of transition from a purely physical to an increasingly digital society. What is needed to facilitate this transition is for the UK Government to formulate sound strategic policy, to identify and support key initiatives to fill gaps in understanding, and to set the

direction of travel for the UK. Confusion is currently hampering progress. **A clear vision and understanding of the issues and requirements is essential if renewed progress is to be made. That vision and understanding cannot be formed without understanding the function and uses that will be made of electronic personal identities.**

- Consider an analogy to illuminate the vision this recommendation aims to create - a nation's transition from a barter economy to a cash-based economy.

Imagine that various bodies within that barter-based nation have developed first generation coinage and that there exist small communities within which some form of coin-based transaction and exchange are being conducted. The desire is to create a vision of what a cash-based economy might look like so moves can be made towards building the financial infrastructure, services and arrangements the nation would need to enable it to make that transition from barter to cash.

To create that vision of what a cash-based economy might look like, the nation's government would start by describing the function of money within the daily life of the nation and the ways in which money would be used by the various different parties. From that they would identify the requirements a national currency would need to satisfy and the way the national currency should be managed and controlled. They would start to sketch out some of the financial services that might be needed to support the various uses of money, and work up descriptions of the types of body or institution that might be needed to provide those services. This would enable them to answer some of the many design questions that would abound, such as whether there was a need for a national central bank and the role it should play, and whether there was a need for all parties to use just a single currency or whether many equivalent currencies could co-exist alongside each other.

This is the type of vision IAAC believes should be created for electronic identities in the 21st century UK. IAAC believes this type of vision is essential if progress is to be made.

Once this vision has been created, the UK Government should then develop an understanding of the characteristics and requirements for national infrastructure and the common principles that any large-scale IMS would need to satisfy if it were to connect with that infrastructure. The UK Government would then be in a position to identify the structures and bodies needed at the centre of that national infrastructure, to agree what was needed to bring such structures and bodies into being and, from that, to agree what role the UK Government should play in fostering their creation.

Phase II – Design

The core characteristics required of any national identity infrastructure would be derived from considering two principal objectives. These are:

- To enable the infrastructure to be successful at serving and supporting the purposes and functions for which electronic identities will be used;
- To enable the UK to manage the risks that such an infrastructure would introduce.

Each of the derived characteristics would then serve as the basis for developing more specific and more detailed design principles to be satisfied by individual IMS.

With respect to the first of these two objectives, the UK can rely upon the normal workings of the marketplace to lead to the development of IMS with suitable functionality. Requisite systems and services will be developed without the need for UK Government leadership wherever there are sufficient benefits to be had from the use of electronic identities. It is not necessary to try to identify in advance what those benefits might be or what system functionality might be required to realise them. We can be confident these will emerge naturally as the market develops.

With respect to managing the risks that an identity infrastructure would introduce, the situation is somewhat different. Though there are a number of organisations within the UK that are addressing aspects of this need⁶, IAAC believes UK Government leadership will be required to ensure that the component systems within the NIdI adequately protect individual citizens and the public at large from potential harms. This need to manage the risks leads to a number of recommendations, and forms the basis for Phase II of IAAC's 2008 Roadmap.

Understanding How Harms Can Arise

The UK Government should lead the development of a comprehensive understanding of the ways in which individual citizens could be harmed by things going wrong (i.e. accidents and incidents) relating to the use of their electronic identities within a national identity infrastructure.

Whilst the creation of an NIdI will undoubtedly help to address some existing risks associated with the way people gain access to personal electronic services today, it will also undoubtedly create other, new ways in which people can be harmed. It is incontestable that identity subjects could be harmed, in some situations seriously, by the types of accident, failure, mistake and security breach that could take place within a national IMS. It is also incontestable that no system can be 100% secure, and no system can be either 100% reliable or 100% failsafe. Hence, the UK Government has to accept that its citizens will be put at risk of harm from accidents and incidents arising within the operation of any national IMS.

It is essential that the UK understands fully the nature and magnitude of all these risks and that the designs of national IMS are channelled so that any new possible harms of significance are recognised and addressed.

Defining Standard Protections and Safeguards

The UK Government should lead the identification and design of a comprehensive set of standard protections and safeguards that would be mandated for any IMS which will hold or use citizens' electronic identities.

The most important part of this task is to develop a comprehensive set of safety nets to catch people when things do go wrong and minimise, if not prevent, any harm being caused to people. A wide range of support services and arrangements will be required catering for a very wide range of large and small incidents and accidents. Developing the required safety nets will be a major undertaking.

- National IMS do not need to be risk free for the individual, any more than the roads people drive on every day need to be risk free. However, they should be sufficiently safe on the whole that the risks that remain are acceptable to the vast majority of citizens, as is the case with the UK's roads. For most people, it should be extremely unlikely they would be involved in a serious identity incident or accident at any stage in their lifetime.

People recognise that things can sometimes go wrong with any system with which they engage. The TrustGuide work⁷ has shown that the provision of safety nets is essential if people are to have the confidence to engage with electronic systems that are still new to them.

It is not at all clear how some of the required NIdI safety nets will be provided. For example, if each person has a root electronic identity and that identity then becomes com-

⁶ For example, the Information Commissioner's Office. The ICO, armed with the Data Protection Act, has proven increasingly capable of holding UK Government accountable for breaches of security in protecting citizens' personal data.

⁷ The TrustGuide work is described at <http://www.trustguide.org.uk/>

promised in some way, for example by some form of identity theft, what are the possible recovery options? People will not be able to discard their root identity and register another one with the ease with which they could discard an old e-mail address and take on a new one.

To make safety nets effective will require a wide range of support services and arrangements. Consider an analogy. If there is a pile-up on the motorway, the ambulance service rushes out to tend to the injured, the fire service rushes out to put out any fires, the police rush out to close off that section of motorway and work out what happened, damaged vehicles get towed to a repair shop to be fixed, and write-offs get covered by the driver's insurance. What form will the emergency services take for the equivalent to a pile-up within a national IMS? Which body should have the authority to lead the investigation of incidents and breaches? Who should take responsibility for getting a damaged identity repaired, the identity owner or the owner of the system that caused the crash? How will identity repair be achieved, given the need for repair processes to be sufficiently rapid that people's lives are not hugely disrupted in the meantime? How will liabilities be assigned? What damages will be insurable and how would recompense be provided for those that are uninsurable?

At the other end of the spectrum are the small but frequent 'minor incidents' that people will need to be able to deal with themselves without incurring major inconvenience. Consider again the motoring analogy. By design, every car carries a spare tyre. If a car develops a puncture, the driver is expected to pull over, put on the spare, carry on with their journey (hopefully not too much inconvenienced by the delay) and get a new spare tyre at their next earliest convenience. What is the equivalent to a spare tyre for dealing with an 'identity puncture', e.g. if one day, for some reason, a person cannot authenticate successfully to their electronic identity? Most company Help Desks spend a considerable amount of their time resetting users' passwords. Would a Help Desk or Call Centre approach be practical for repairing identity punctures on a nation-wide scale? If identity subjects are expected to be able to deal with their identity punctures themselves, then the equivalent to spare tyres will need to be designed into every one of the identity system components people will be relying upon every day.

A large amount of very significant work will need to be undertaken to formulate the necessary policies, arrangements and standards needed to ensure that people can achieve swift and effective response, recovery and, where appropriate, restitution in the event of an accident, failure, mistake or security breach. A wide range of issues will need to be addressed and structures brought up to date with the NIdI. This work will need to be led by the UK Government but undertaken in collaboration with many other organisations⁸.

Developing a Governance Framework and Citizen Control

The preceding discussion and recommendation concerned protecting the citizen from the risk of their being harmed by things unexpectedly going wrong within a national IMS. In addition to that risk, citizens will find that sometimes their interests can also be harmed by legitimate uses made of their identity within the normal workings of a national IMS.

- Individual citizens have legitimate interests relating to the uses made of their identity data. For example, individuals have an interest in the maintenance of their privacy, in not being discriminated against unfairly, and in not having their freedom and autonomy be circumscribed. Each of these interests can be affected or harmed by the uses made of a citizen's identity data.

⁸ Within its Identity Assurance programme, IAAC has looked at identifying, understanding and addressing many of these issues. Please refer to the appendix at the end of this paper for links to the reports from IAAC's 4 September 2007 and 16 October 2007 workshops in which this work is described.

In addition to the individual citizen having interests, the government of the day, acting on behalf of the public at large, also has relevant interests. These include the maintenance of law and order, the maintenance of national security, and the prevention, detection and investigation of crime.

In some situations, the interests of one party can be in conflict with the interests of another party. This arises primarily in situations where legitimate public or national interest (e.g. law enforcement, national security) might conflict with the legitimate private interest of the individual (e.g. the protection of their privacy).

It is important to ensure that, within the operational arrangements established for national IMS, the interests of all parties are protected in proper balance, and that when, say, the legitimate interests of the identity subject are overridden in the national interest, the identity subject remains adequately protected so their interests are not harmed unnecessarily or inappropriately in the process.

It is through the creation of an Identity Governance Framework for the NIdI that the balance of conflicting interests should be defined and the relevant safeguards and protections specified. IAAC strongly recommends that the UK Government should develop an Identity Governance Action Plan and, within that, should work swiftly to develop, agree and deploy an Identity Governance Framework for the UK.

IAAC acknowledges that the National ID Cards Bill (2006) requires the appointment of an NIS Commissioner to oversee the operation of the NIS. However, this is but a first step. The Bill falls well short of defining a full governance framework laying out the complete array of powers, accountabilities or responsibilities needed to protect the citizen.

IAAC has devoted a significant amount of effort within its Identity Assurance programme to the clarification of this issue⁹. It has developed a structure for an Identity Governance Framework and, within that, for Citizen Control. Citizen Control is an essential component central to any properly constructed governance framework. IAAC believes that, through its work, it has made a valuable contribution to the creation of a successful governance framework for a UK NIdI. IAAC recommends that the UK Government should now take up this contribution and carry it forward to effect the design of a full NIdI Identity Governance Framework for the UK.

The UK Government should ensure its proposed governance arrangements are widely debated and agreed, and should move quickly to put the governance arrangements in place as soon as possible, not just “in due course” as was indicated in “Transformational Government”. A comprehensive governance framework should form the bedrock upon which each component of a UK NIdI is designed. Trying to retrofit previously developed infrastructure into a subsequently developed governance framework would undoubtedly cause significant difficulties and force otherwise unwarranted compromises in the safeguards and protections provided.

Phase III – Operation

Phase I of IAAC’s 2008 Identity Assurance Roadmap discussed formulating the requirements for national infrastructure, and Phase II the safety design for national IMS. National IMS will be developed by various parties and, as they come together to form national infrastructure, will play a steadily expanding role within the activities of a UK digital society. As this role expands, people will become increasingly aware of the extent of their engagement with national IMS and with the national structures and processes that support them. The UK Government needs to ensure that the citizen’s engagement with national IMS is positive and strengthens rather than undermines

⁹ Please refer to the appendix at the end of this paper for links to the reports from IAAC’s 5 March 2008 and 4 April 2008 workshops in which this work is described.

citizens' confidence in the digital society of which they will be a part. IAAC believes that the following aspects are critical to the success of this.

Engaging With the Public

The UK Government should formulate an action plan for developing a dialogue with the UK public so the public can learn to engage fully as well as safely and securely with national IMS.

The main part of this activity is concerned with two aspects. The first is about educating the citizen so they can understand how the use of electronic identities can benefit them in their lives, plus helping them to understand at a common sense level what they need to do to keep their electronic identities safe. The second is about establishing the ground rules regarding when and how other parties such as Identity Service Providers (IdSPs) will report to individual citizens if there are things relating to their personal electronic identity data they might need to know.

General Citizen Education

General citizen education is about providing the citizen with the knowledge and understanding they require so they can decide sensibly how they would like to engage with national IMS. It requires providing that information at a level citizens are able to take on, and making further information readily accessible to those who want or need to know more.

Consider an analogy to illustrate what is needed. We are all provided, through public channels, with the knowledge and understanding we require to enable us to drive on the roads sensibly and safely. Without being presented with levels of technical detail we do not need on a daily basis, we know the main ways in which driving can be dangerous, and we know how we are expected to behave so our use of the roads is kept safe for ourselves and for others. We know, for example, that safety is improved if we drive at moderate speeds, and that we mustn't allow ourselves to be distracted by talking on a hand-held mobile phone. We know what to do if we are involved in an accident, and we know how to find further details, such as specific telephone numbers to call, if ever we need them.

Similarly, the citizen will need to be given, through a multiplicity of channels, perhaps including the publication of a 'Highway Code for Electronic Identities', the knowledge and understanding they will need to enable them to engage sensibly and safely with national IMS. This includes giving them sufficient awareness of the dangers involved, of the warning signs they should look out for, of their role and responsibilities, and of the safeguards put in place for their safety and security. For most people, this doesn't mean they will need to understand any of these things in any great detail.

What the public will need to be given in detail, though, is specific guidance on the steps they need to take to keep their electronic identities safe from accidents and secure from attack. This will need to include specific steps for protecting their identity data and specific steps for securing the systems and technologies they use in the home. For example, any 'Highway Code' should give people specific guidance on how to set up a domestic wireless network so it is not open to casual connection by passing strangers.

The UK Government should formulate a comprehensive plan under which it determines what the citizen needs to know, decides how to present that information in a form that is comprehensible to citizens, and decides how that information can best be disseminated. The objective is to ensure relevant information is provided in an accessible manner. The dissemination channels will include the public media and Identity Service Providers.

With regard to how best to communicate this type of information to the public, the UK Government should collaborate with the private sector. The private sector has learned valuable lessons from needing to educate consumers regarding phishing and Internet security. **It is likely that most if not all of the security attacks seen today that target domestic PC users and their Internet banking accounts, for example phishing attacks and Trojans, will be equally**

applicable to the theft or abuse of electronic identity data. If the security attacks are much the same, then it can be expected that many of the security messages will be much the same. The private sector has valuable experience in how to communicate such messages effectively to the general public.

Individual-Specific Information and Advice

As well as needing to be furnished with the above body of general information provided at a common sense level, there will be a need for individual identity subjects to be given information from time to time that is specific to them and relates to their personal electronic identity data.

Some of this will be routine information and some non-routine.

- Routine information might come in the form of a quarterly statement, somewhat like a credit reference statement, provided by an Identity Service Provider, of what electronic identity data is held relating to that person and how many times it has been called upon for different purposes during the reporting period.
- Non-routine information might come in the form of alerts, perhaps helping to protect the citizen against attacks such as identity theft. For example, Identity Service Providers might, as part of their service, advise identity subjects if they appear to be making unusual uses of their electronic identity data. This would be similar to the way credit card issuers monitor cardholder spending patterns and advise the cardholder if they detect an unusual transaction.

The UK Government should consider what reporting standards it would like to impose as part of the regulation of Identity Service Providers, mindful of the need to ensure a suitable balance between auditability, privacy, timeliness and usefulness.

Advancing the Maturity of Key Processes

The UK Government should increase the focus of attention and R&D support given to improving the robustness and maturity of the key processes on which IMS depend.

The success of any NIDi will depend not only on the suitability of the technologies used within IMS but also on the suitability of the processes employed. For example, irrespective of whichever technologies are used within an IMS, no IMS can deliver a greater level of identity trustworthiness to a relying party than that which is inherent in its enrolment process. A weak enrolment process undermines identity trustworthiness in a way that no amount of high-grade technology can counter.

Whilst the UK Government can generally be confident that identity management technologies will develop and mature in a timely manner to meet the evolving needs of most IMS, it cannot have a similar level of confidence regarding the processes on which IMS depend. The current focus of R&D on technologies has allowed key processes, especially those affected by Social Science considerations, to remain relatively under-developed. The strength and maturity of these key processes are unlikely catch up without Government attention and support.

The UK Government should foster a number of activities to improve the understanding and robustness of the key processes underpinning electronic identity services. Building on the experience and learning already obtained by the private sector, it should strive to develop these processes to a level that will enable them to work effectively and efficiently on a nation-wide scale with a hugely diverse user community measured in the millions.

The key processes that would benefit from being fostered in this way include:

- Enrolment
- Dispute resolution
- Incident handling

- Recovery after failure
- Repair and restitution after identity or data theft

Improving Information Management Culture and Practice

The level of understanding and practice of good information management by government personnel, government agents, commercial organisations and the general public is currently far below that which is needed for an information-intensive society. **It is imperative that the UK Government should formulate a programme of action to strengthen the nation's information management culture and raise the nation's data security performance if the public is to have confidence in the safety and security of national IMS.**

There is widespread and deep general scepticism regarding the UK Government's ability to operate information-intensive systems safely and securely. The Freedom of Information (FoI) Act has brought to light that many areas of government still have poor information management cultures and practices. Government statistics¹⁰ show that a significant proportion of FoI requests are not satisfied within the required 20 day period, and that the proportion has, if anything, been falling over the past year. In addition, government data security breaches seem to arise continually and from a wide variety of sources. Whilst many data losses entail only the loss of data and do not lead to confidential data being disclosed, some data loss incidents are very significant. They have been described as being the equivalent to a "train wreck" and as exposing "institutional blindness" to the impact of handling personal data badly¹¹.

Information management practice in the commercial sector does not fare much better. Despite the fact that the UK has had data protection legislation on the statute books since 1984, the Information Commissioner's Office is still having to urge CEOs to "raise their game" following a number of "unacceptable privacy breaches"¹². Enforcement action was taken by the ICO against a major high street retailer after a laptop containing the unencrypted details of 26,000 employees was stolen. And the number of enforcement notices issued to private sector professional firms such as accountants and solicitors shows that careless information management is not limited to large organisations or the untrained.

However, it is also clear that the information management practices of the general public are typically no better. People still fall for phishing attacks and display very low levels of security common sense. As has been aired by the House of Lords Inquiry into Personal Internet Security¹³, the UK Government cannot rely on the average member of the public to be security aware, to be security informed, or to act with much security sense.

There is an overwhelming need for a much stronger level of information management to be practised by the population of the UK, ranging from government personnel, through company staff, to private individuals. Achieving this will be a significant challenge and will require Government leadership and a multifaceted action programme. The UK Government must demonstrate to the public that it is rectifying its current data security shortcomings immediately and taking a very firm line against those who commit security breaches with the public's personal data. It must make greater efforts to broadcast fundamental information safety and security messages to

¹⁰ Please see <http://www.justice.gov.uk/publications/freedomofinformationquarterly.htm>

¹¹ The UK's Information Commissioner described the loss by HMRC in October 2007 of 25 million confidential personal data records as a "train wreck". This loss was blamed on "institutional blindness" to the impact of handling personal data badly. The then Cabinet Secretary's response was to call for a "culture change" within the Civil Service. Please see the appendix at the end of this paper for directions to a number of reports on this and other data loss incidents.

¹² Please see the ICO's Annual Report Summary for 2008 available from <http://www.ico.gov.uk>

¹³ The House of Lords sub-committee's report plus subsequent responses and updates are available from http://www.parliament.uk/parliamentary_committees/lords_s_t_select/internet.cfm

the public, to match, for example, those it broadcasts each year with respect to drinking and driving. It will need to develop techniques to ensure that identity services and systems are designed in ways that minimise the opportunity for citizens themselves to be the cause of operational failings or breaches. And it should significantly strengthen enforcement provisions as the ultimate means to drive home the needed cultural sea-change.

Adapting Protective Structures for the 21st Century Digital Society

The UK Government should put in place a far-reaching programme to adapt policy, legislative, security, law enforcement and judicial structures and powers to meet the demands of the 21st century UK digital society.

There are three perspectives to be considered. In the more immediate, narrow perspective, this activity entails updating current protective structures to cater for the digital equivalents of unlawful physical activities. In an intermediate perspective, this activity entails updating protective structures to allow for changes that will arise due to the different characteristics of digital information. In the longer-term, broadest perspective, this activity entails understanding how the nature of providing protection to the public will differ in the digital society, and ensuring that the consent of the citizen is maintained as the means by which protection is provided change.

Catering for the Digital Equivalents of Unlawful Physical Activities

The new information systems and technologies underpinning the digital society will enable new functional capabilities to be exercised. Some of these new capabilities will be used beneficially, but many will also be used in ways that are unwelcome. Fresh opportunities will arise continually for the further exploitation of people, information or systems by those who are unscrupulous or criminal.

There is a clear need for policies, capabilities and practices relating to law enforcement and national security to be updated in a timely manner to accommodate the criminal use of information systems and technologies. If a significant lag develops between the rise in electronic identity crime and the capabilities of the police and security services to deal with that, public confidence in the security and safety of identity management systems will suffer.

As well as much redrafting of legislation and regulations, steps will be needed such as raising the level of law enforcement services' understanding of information technologies and related crimes, and ensuring that those services have sufficient access to relevant specialist expertise, skills, training and forensics facilities to enable them to be effective in combating these new types of crime.

Adapting to the Different Characteristics of Digital Information

Looking one step further forward, protective structures will need to be updated to reflect new societal perspectives on the misuse and abuse of digital information.

What might be called 'the laws of digital information' are different in some respects from the more familiar 'laws' of physical information. Compared to information held on paper, digital information is more easily retained, does not decay over time, and remains fully retrievable. IT enables the long-term retention and perfect recall of every iota of digital information. Organisational memories about each consumer or citizen remain crisp, comprehensive and instantly recallable. People are no longer able simply to slough off prior mistakes, misjudgements or misdemeanours and move on in their life. They remain vulnerable to tomorrow's misuse or misinterpretation of something they did or said or were on any previous day.

In many situations, these organisational memories can provide valuable intelligence that would otherwise be missed. For example, they can indicate when someone might be a threat to society. They can bring to light undesirable behavioural tendencies in an employee, a person's improper prior performance as a director of a company, a borrower's disregard for credit obligations taken on, and so forth. It is proper in many situations that past actions should be used as the basis on

which to constrain future opportunities within the same or a similar context. However, in many other situations, these organisational memories will be chaff of no meaningful value. To treat them as anything else could lead to the unfair denial of opportunity or liberty to the person to whom they relate.

There is a need for a consensus within the UK on what constitutes appropriate, and what inappropriate, use of digital information outside its original timeframe, circumstances or context, and on the severity with which different forms of digital information misuse or abuse should be treated. The UK Government should lead in the development of this consensus, and then in the development of suitable legislation, regulation, codes of practice and enforcement, bearing on both the public and private sectors.

Maintaining the Consent of the Citizen

Looking substantially further ahead, information technologies can bring about structural changes in the provision of protection and affect the consent of those being protected.

The UK has developed security, law enforcement and justice systems to enforce the rule of law and to protect citizens from unlawful harm. These systems have typically evolved slowly, usually over many decades, in response to social changes usually taking place over similarly long timeframes. In contrast with the past, in the 21st century digital society the nation's protective arms of state will need the versatility to respond to changes taking place within single decades, to the use of infrastructures that are pan-jurisdictional, and to threats for which the familiar geographical, physical and temporal constraints on the undesirable actions of intelligent threat agents no longer apply. Structural changes to the way in which protection is provided will need to be brought in to maintain protective effectiveness.

Many of the same new information technologies that are ushering in the digital society will be used to enhance the capabilities and reach of security, law enforcement and justice systems, for example by enabling greater powers of information collection, sharing, and analysis. However, at the same time, these IT-enhanced capabilities could enable the protective arms of state to extend their reach in ways that take them beyond the monitoring and restraining powers of traditional supervisory methods developed for the pre-digital world. By making traditional controls obsolete, the rush to develop security and law enforcement mechanisms effective against a new generation of cyber criminals and terrorists can lead to conflict with long established principles of a free society.

Security, policing and justice within the UK must be performed with the consent of all citizens. The UK Government should lead in the creation of an understanding of how the UK can adapt its protective powers to provide protection to the 21st century digital society. It will need to develop solutions that can enable it to provide safety, security, order and the rule of law whilst retaining consent, respecting the principles of a free society, and not stifling personal liberties and freedoms.

Glossary

Citizen Control	The collective set of policies and procedures under which the citizen has a measure of visibility and control over how their personal data is used and by whom, sufficient to maintain their confidence in electronic systems that might be new to them.
Federated Architecture	An architecture in which a number of component parts are able to interoperate to gain mutual benefits whilst maintaining diversity and autonomy.
Governance Framework	A framework under which various roles, accountabilities, responsibilities and powers are assigned, and structures are developed, to ensure that a complex entity (such as a large corporation or a national scheme) respects the legitimate interests of all stakeholders and is properly managed and controlled.
Identity Assurance	Within the subject of Identity Management, ensuring electronic identities are adequately secure, trusted, accessible only by authorised people, and available when needed.
Identity Management	Managing the lifecycle of electronic identities (i.e. their creation, storage, exchange, use and protection) in a manner that maintains their reliability and usefulness.
Identity Service Provider (IdSP)	An organisation or business set up to provide personal identity services to its customers, much as banks provide personal financial services to their customers. An IdSP might provide safe storage of personal identity data on behalf of a customer, and accept instructions from the customer regarding which data to release to which relying party for which purposes.
Identity Subject	The person to whom an identity and associated identifying data relates.
IMS	Identity management system(s): electronic systems that have Identity Management as their primary purpose.
National IMS	IMS which hold or use citizens' legally-recognised electronic identities. A national IMS is national in the sense it operates at the level of the nation state rather than that it is nationwide in scope.
NIdI	National Identity Infrastructure: the infrastructure formed when national IMS come together to various degrees, with common central bodies, structures and processes binding them together into a whole.
NIS	National Identity Scheme: the systems and arrangements planned by the UK Government to provide each person in the UK with a legally-recognised electronic identity, plus to provide the means by which identities can be found or authenticated.
Organisation-centric	An approach in which the needs or interests of the providing organisation are put first.
Relying Party	An organisation that uses a person's identity data as part of its provision of a service.
Root Identity	A primary electronic identity conferred and legally recognised by the state and based directly on the individual's physical identity.
User-centric	An approach in which the needs or interests of the user are put first.

Appendix - Links to Relevant IAAC and Other Work

IAAC is not responsible for the content on any of the non-IAAC links below.

Transformational Government

Please see http://www.cio.gov.uk/transformational_government/ for an introduction to the development of the UK's Transformational Government strategy.

See also

http://www.hm-treasury.gov.uk/pre_budget_report/prebud_pbr06/other_docs/prebud_pbr06_varney.cfm for the Varney Report 'Service transformation: A better service for citizens and businesses, a better deal for the taxpayer'.

The Crosby Public-Private Forum on Identity Management

Please see

http://www.hm-treasury.gov.uk/independent_reviews/identity_management/identity_management_index.cfm

IAAC Workshop Reports and Briefing Papers

Reports and Briefing papers from the four workshops mentioned are available from <http://www.iaac.org.uk/Default.aspx?tabid=55>

Data Breach Reports

Two of the more significant data loss incidents have attracted specific attention. Please see:

http://www.hm-treasury.gov.uk/independent_reviews/poynter_review/poynter_review_index.cfm for details of the Poynter Review into HMRC's loss of data discs containing the confidential personal details of 25 million UK families receiving child benefit;

http://www.mod.uk/nr/rdonlyres/3e756d20-e762-4fc1-bab0-08c68fdc2383/0/burton_review_rpt20080430.pdf

for Sir Edmund Burton's report following the loss of a MOD laptop containing the personal details of approximately 600,000 individuals who had expressed an interest in joining the Armed Forces.

See also

<http://www.cabinetoffice.gov.uk/~media/assets/www.cabinetoffice.gov.uk/csia/dhr/dhr080625%20pdf.ashx>

for "Data Handling Procedures in Government", the report resulting from the data handling review undertaken on behalf of the Cabinet Office, the objective of which was to improve Government data handling procedures following the HMRC and MOD data loss incidents.