



Identity Assurance

“Who do you think you are?”

A white paper from ISSA-UK



ISSA Chapter of the Year 2005 and 2006



INTRODUCTION

This ISSA research report is based on the findings and conclusions from a UK members' workshop, held on HQS Wellington on July 8th 2009. The subject was *identity assurance*, an increasingly important problem which aims to ensure the security and trustworthiness of managed citizen identities. Identity assurance is a relatively new term, which introduces a citizen-centric perspective to the more established field of *identity and access management*, reflecting growing societal concern about the need for greater attention to security, privacy and integrity in the use of personal identity information.

The theme of the workshop was "*Who do you think you are?*" an appropriate and ironic choice, as, like many statements on the subject of identity, it is an expression that can be interpreted in more than one way: on the one hand, reflecting the uncertainty of a person's identity in a dynamic, networked society; or on the other, the need to challenge individuals' claims about their privileges. When it comes to the provision of services, judgements about a person's identity and rights become the prerogative of the service provider rather than the customer. From that perspective, a more telling theme might be "*Who do other people think you are?*"

The event was attended by a broad range of information security professionals from both industry and government, and featured presentations from leading experts on the subject of identity, as well as round table discussions amongst members. The presentations included an opening keynote address by the Rt Honourable David Blunkett MP, followed by talks by Dr John Leach, of the Information Assurance Advisory Council; Dominic Hartley, Director of Strategy and Architecture for the Home Office Identity and Passport Service; Dr John Meakin, BP's Chief Information Security Officer; and Peter Bradwell, of Demos, an independent think tank. The event also included a set of "Dragon's Den style" pitches from selected vendors active in the identity assurance field including KPMG, NuBridges, NetWitness and Microsoft.

The content of this paper has been drawn from the workshop presentations and round table discussions. It has also built on earlier, ISSA facilitated discussions on the subject held at Infosecurity Europe 2009 at Earls Court London. As such, it represents a collective opinion of many different information security professionals on the state-of-the-art in information assurance, rather than the views of any particular individual or organisation.

IN SEARCH OF IDENTITY

A person's *identity* is more than a means of authentication; it is an emotional, personal claim. Some people are proud of their identity and the circles to which they belong. Many are happy to publicise their lifestyles on social networking sites. Others prefer anonymity, especially in online transactions. Celebrities set out to create a positive public image of their identity, but many end up the victim of negative media coverage. The entertainer Michael Jackson, for example, is an interesting, topical case study of the power of the media in creating both a good and bad persona for an individual.

Regardless of the individual's perspective, nobody likes to be impersonated or mistaken for another, especially when it can result in loss of privileges, or financial or reputational damage. Unfortunately there will always be a criminal element that seeks to exploit opportunities to assume or steal identities for personal gain. In 2007 alone, for example, more than 65,000 victims of identity fraud were identified and protected by the fraud prevention service CIFAS.

In today's online world, the concept of identity is a complex one, operating at many levels and in varying contexts. Identity management is essential to control access and authorisation to business or personal services. Personal identity data can also be exploited for marketing, intelligence or fraudulent purposes. Nobody has a monopoly on determining the content of an electronic identity. They can reflect an image that we have created for ourselves, perhaps on a social networking site, or something asserted about us by employers, colleagues or mischief-makers.

Identities can be based on different attributes, which might be *biological*, *attributed* or *biographical*. Credentials can be checked using mechanisms of varying strengths, using data gleaned from observations, through references, or from a person's physical characteristics. They can be based on inherited attributes, such as name or lineage, or derived from contact details, job title, qualifications, social class, club memberships, payment cards, credit ratings or geographic locations.

An identity can be based on a something as simple as a single credential to grant access to a single service, or it can be formed from the sum total of the knowledge available about a person's past or likely future behaviour. Ninety percent of the adult population possess some form of identity credential, the most common being passports, driving licences, birth certificates and household or phone bills. Such credentials can be held and managed by the customer, by a service provider or provided through an independent, third party authority.

Citizens can choose, or be required to assume, multiple identities and roles. An individual might, for example, have a separate identity or role as an employee, a computer user, a system administrator, a bank customer, a frequent flyer, a British subject, a taxpayer, a member of a library, or a card-carrying member of a political party. The only limit is the capacity of a person's wallet to accommodate each physical identity card.

In practice, identity is not so much an absolute fact, but a variable means to one or more particular ends. An identity makes little sense without a context and a purpose. The wide range of business and government applications requiring an identity means that not everyone perceives identity management or assurance in the same way. This is why we continue to encounter so many variants and practices in our everyday life.

But encouraging variations in systems and processes is inefficient, and it limits the potential for improvements in services as well as in the underpinning management systems. For this reason, the Government is proposing to centralise the management of personal identity data. Minimising the number of times that citizens are required to register their identity or present their credentials will obviously deliver benefits, such as greater convenience. But it also demands more stringent and effective oversight of how personal identity information is used, managed and safeguarded.

HOW PERSONAL IDENTITY DATA IS USED

The exploitation of personal identity information takes place at two distinct levels. Firstly, a small set of attributes can be used for the purposes of identification and authentication for access to facilities, whether physical or electronic, or to carry out a business transaction. Secondly, personal data can be accumulated and mined to analyse past events or predict future behaviour, either for marketing, sales, intelligence or investigative purposes.

The use of personal information in marketing is getting richer and more intrusive, as techniques move away from a traditional focus on designing products that might appeal to a static set of demographic classes, towards an online world of 'long tails' where business revenue can be

generated from personalised sales to individuals with specialised interests. All retailers today can benefit from better knowledge of what customers like, where they are, what they're currently doing and what they've just bought. But there are citizen concerns as well as benefits associated with this process.

Identity is a dynamic phenomenon. Many attributes are subjective, chosen by the individual or decided by others. They might also vary over time. Personal identity information carries both a cost and a value, but they are not the same for all stakeholders. The value of a piece of information is in the eye of the beholder, and its potential for exploitation can change over time. An item of data that helps generate a profit or meet a business objective today might not be as effective tomorrow. This varying perception of the cost and value of data can create a situation, in which service providers might not value personal data sufficiently highly to justify implementing an appropriate degree of security protection.

THE NEED TO PROTECT IDENTITY DATA

Public opinion on privacy is rarely consistent. Some people care deeply about their privacy rights. Others are carefree, and in some cases clearly enjoy exhibiting their personal details and behaviour. But a large number are uninformed about the implications of the risks associated with the exposure of personal identity information. In particular there is ignorance, as well as apathy, amongst young people about the longer-term implications of posting personal information on public networking sites. Better education and guidance is needed to protect the longer term interests of citizens from the exuberance of their youth.

Protecting personal information in a networked society is becoming increasingly harder. Management trends such as *globalisation* of business management and *centralisation* of business services raise the stakes by creating larger and larger collections of data. At the same time advances in technology are making it considerably easier to lose or steal large quantities of information. This trend has been clear for many years, though many service providers in government and the retail sector have only just woken up to the potential damage from large-scale breaches. This late recognition of the importance of safeguarding identity data presents a major legacy problem: the need to upgrade the security of established processes, as well as to raise standards and practices for risk assessments involving personal identity data.

The primary reason for this legacy situation is the rapid increase in the threat of identity theft, which has caught many organisations by surprise. But in some cases a further reason is the fact that a creator of a security risk or data breach is often insulated from its immediate impact. Responding to such a *moral hazard* is not easy: it requires carefully considered intervention through education, standards and regulation.

FAILINGS IN IDENTITY MANAGEMENT

Experience has shown that in practice there are numerous failings in the capability of organisations to manage identities and safeguard identity information. Many of these shortcomings are in management practices and process design, rather than technology. But better technology would also help to remedy the situation. Most contemporary authentication measures, such as passwords, have long been recognised as inadequate, especially in a networked environment in which an increasing amount of background information about citizens is available to enhance password guessing.

The complexity and scale of modern information systems also increases the size of the administration task for identity and access management. Many identity systems do not scale well, resulting in shortcuts in processes and a progressive dilution in the granularity of the management of access rights. Life-cycle control of users is also a major shortcoming, especially regarding third party users who now outnumber staff users in many organisations. De-registration of users who have left, or who no longer require access, is a particular weak point. Constant restructuring and centralisation of services exacerbates this problem. From a system design perspective, better facilities for life-cycle management are needed, as well as easy-to-use facilities for users or customers to view their information and make corrections.

Greater incentives are needed to encourage vendors and designers to spend more time designing security features that are easier for people to use. More focus is also required on the need to design systems that take account of the growing inside threat. Clearer privacy policies for websites are also desirable, as few people take the trouble to read and understand the contents of a dialogue box before clicking to signal their acceptance of the consequences.

Clearer, agreed terminology is also needed to prevent systems designers and information security managers from talking at cross purposes. There is a wide range of terms that are commonly used, sometimes interchangeably, with varying interpretations, such as: *identity, persona, identifier, credential, claim, assertion, identity asset, relying party, trust, token, subject, attribute, ID, enrolment, registration and verification*. The Jericho Forum, an independent, thought leadership group, is aiming to collect and publish a set of agreed (and disagreed) definitions. Simple initiatives such as this can help to improve the quality of debate, as well as the specification of standards and controls.

If there are serious failings in identity management today, then it is likely that they will, if not addressed, be worse in the future. Both the size of the problem space and the complexity of the processes associated with extended enterprise identity management are increasing. A step change in identity management standards and practices, as well as in the sophistication of the supporting systems and technology, will be needed to overturn this trend.

WHO IS RESPONSIBLE?

Some observers take the view that *information assurance* in the public sector suffers from a degree of unnecessary confusion regarding leadership, the result of a legacy of separate central agencies with overlapping responsibilities. Certainly to an outsider, there appears to be a confusing alphabet soup of specialist agencies with similar sounding roles and acronyms, including CESG, CSIA, CPNI and others. Responsibility for *identity assurance* also introduces the Home Office IPS in a major leadership role. Clearer responsibilities for overall direction would help promote stronger leadership across the public sector.

The solution space is further complicated by the increasing amount of outsourcing and collaboration between public and private sector organisations. Leadership in identity assurance advice and standards needs to be clear not only within government but also to a growing set of stakeholders in the private sector, or representing the citizen perspective. Although the public sector is the focus of most government identity assurance initiatives, the private sector is equally in need of stronger coordination to manage identity assurance across virtual supply chains and partnerships. Direction across private sector organisations requires much more than vision and policy guidance: it demands compelling thought leadership, regulation and economic incentives.

A major question put to workshop participants representing both public and private sector interests was “Should public and private sector strategies be aligned?” The answer was a clear ‘yes’ though there was little confidence that this could be achieved through the current structures and levels of representation and empowerment.

A 21ST CENTURY ROAD MAP FOR IDENTITY ASSURANCE

The Information Assurance Advisory Council (IAAC), a public policy research organisation, has recently published a long-range strategy and road map for identity assurance¹. This is the result of a two year programme of research, workshops and policy debates to develop a deeper understanding of the issues central to the assurance of identities. The IAAC programme recognised that the transformation of UK society into an increasingly digital society brings with it a number of changes to the practices by which users are identified for access to their online activities. In particular the evolution of identification of consumers from convenient labels, such as e-mail addresses, to legally-recognised electronic identities will be accompanied by significant risks, including risks both to the identities themselves as well as to the information and systems that rely on the trustworthiness of these identities.

The IAAC report on the conclusion of its two-year Identity Assurance Programme provides an informed view of the strategic risks relating to the use of electronic personal identities. It makes several recommendations for key actions that it believes need to be taken forward within the UK. The first recommendation is that the public and private sectors should work together to articulate a vision for the function and uses of electronic citizen identities in the 21st century. The IAAC notes that the current lack of a shared vision is potentially the most important barrier that impedes further progress.

A second major recommendation of the IAAC report is that government should drive work on a number of topics essential to the design of successful national infrastructure, including the development of an identity governance framework, the definition of the safeguards for effective ‘citizen control’ and the development of ‘safety nets’ to protect citizens from damage when things go wrong. A third recommendation of the IAAC report is that there should be greater engagement with the public to enable citizens to understand not only the benefits of identity based systems but also the personal risks, as well as what they need to do to keep their electronic identities safe and protected. In particular there needs to be improvements in the maturity of key management processes, such enrolment and identity repair, which remain relatively under-developed.

SAFEGUARDING IDENTITY IN THE PUBLIC SECTOR

Government information systems and processes for handling personal identity information have evolved in a way that has created many variations in how identity information is collected and used. The result is an inconvenience to citizens, as well as a potential source of security risk. The Home Office is leading a major government initiative to implement a government-wide strategy, ‘*Safeguarding Identity*’², to improve the way it uses and manages identity information. It aims to improve the accessibility of government information and to deliver enhanced citizen confidence in accessing services.

¹ See: <http://www.iaac.org.uk/Portals/0/IdAConcludingReportSept08.pdf>

² See: http://www.ips.gov.uk/cps/files/ips/live/assets/documents/13439_Safeguarding_Identity_w_opt.pdf

The Home Office strategy appears to follow on well from the IAAC road map. It has three several major strands, including common building blocks for identity (definitions, standards and credentials), improvements in the way public services are delivered, such as a common approach to assuring identity for online services, and a more consistent approach to the safeguards needed to protect personal identity information, in line with data protection principles, as well as the recommendations of recent Cabinet Office reviews.

The Home Office strategy aims to enable citizens to register their identity once and use it many times to access public services safely, easily and conveniently, whilst knowing that public services will only demand the minimum necessary information and keep their identity information safe. Citizens will also be able to see personal identity information held about them and correct it if it is wrong. The Home Office aims to meet these expectations by agreeing common definitions, standards and credentials to deliver improvements to public services and establishing a common approach to safeguarding personal citizen identity information.

The successful execution of this strategy will of course depend on the willingness of other government departments to adopt and meet these standards. In particular, departments need to the common definition of identity, make better use of biometric information and ensure that application-specific data is retained only where it should be and to minimum security standards.

Underpinning the Home Office strategy is a set of principles which are different from but not dissimilar to the Kim Cameron 'laws of identity'.³ In fact they represent one of the first examples of a practical set of design principles for a real-world identity management system, rather than a theoretical set of laws designed to promote thought leadership for longer term developments.

The Home Office strategy has merit in providing a common framework for identity management standards, risk management and the security of services. It is already encouraging collaboration between major government departments for joining up the delivery of citizen services. However, progress has historically been very slow in this area, considering that initiatives for joined-up government services commenced more than a decade ago.

DOES THE PUBLIC SECTOR IDENTITY STRATEGY MAKE SENSE?

New concepts are always difficult for people to grasp if they cannot relate it to something familiar. Passports make sense to people. But the purpose and benefits of identity cards and identity management schemes are far from clear to many citizens. Developments based on new technology also raise inevitable questions of feasibility and risk of failure. Greater clarity on the objectives, costs, benefits and risks is needed to reassure the public, as well the more informed IT and security communities.

A centralised identity scheme offers the potential for efficient delivery of services and better protection of personal information, but it also introduces further costs to taxpayers, significant management challenges and new risks to personal identity data. The public need to be reassured that the business case is sound, that the risks are adequately mitigated, and that steps are taken to avoid 'mission creep', i.e. to ensure that the scope and applications of the scheme are not extended beyond the objectives, budget or the capabilities of the management controls. If data is available, there will inevitably be temptations to exploit it for new purposes not necessarily for sinister purposes, but more likely in the interests of greater efficiency.

³ See: <http://www.identityblog.com/?p=354> for the Kim Cameron "laws of identity"

The use of a standardised access mechanism requires careful design to minimise the set of personal information that is needed to authenticate individuals and authorise their access to services, as well as to avoid unnecessary use of strong authentication mechanisms when they are not appropriate, e.g. for low-risk services such as applications for TV licences or road tax. A further challenge will be to ensure that all participants maintain minimum standards of security and are granted no more than the minimal access needed to personal information. Arrangements for information sharing across departments and agencies must discourage, rather than enable, unnecessary copying of database information.

Scale and technology are major potential sources of risk. The volume of citizen enquiries at peak periods will create a substantial pressure on security and incident response processes. In particular, plans and processes will need to be established to enable an efficient response to, and recovery from, a massive data breach affecting large numbers of citizen records. All security technologies have a limited effective life span. There are already weaknesses in contemporary security technologies, such as chip-and-pin-based smart cards. There is also a danger in placing too much dependence on a single identity token, which might be effective against today's risks, but not proof against future security threats. The increasing use of public networks to deliver citizen services is substantially increasing the attack surface, enabling attacks to be automated and launched from a distance, and with a greater degree of anonymity.

A further key concern is the effectiveness of the tests that will be conducted on the system to prevent attempts at identity fraud. Verification of information is especially important at the enrolment stage. The ongoing integrity and use of the data are also major concerns. Many government and industry databases are known to have very high degrees of error. Yet even a small error rate is significant for a national database, where a single percentage of records can represent a population the size of a medium-sized city.

Deliberate security threats to data quality, whether from hostile intelligence services, terrorists or organised crime, are also a major concern. Safeguards to ensure data integrity safeguards are rarely implemented in today's systems, as attempts to modify data have historically been few and far between. The threat landscape is changing, however, with increasing awareness of the potential opportunities and damage that can result from unauthorised modification of key reference data. Attacks on data integrity might be motivated by fraud, terrorism or mischief. But whatever the objective, the potential damage to business services and citizen interests can be substantial.

Pro-active risk management will be a pivotal factor in maintaining an adequate level of security protection. Not every current or emerging source of security risk is immediately obvious to system development managers. The risk landscape can be compared to a floating iceberg, with many risks hidden from the casual observer. Risk assessments for long-range, strategic schemes demand a much deeper and more forward-looking insight than is generally applied to traditional projects. But not all of the risks are completely new: many traditional paper filing systems also carried similar risks.

The scheme also raises the controversial question of who owns, or should own, personal identity data. In fact, the degree of perceived citizen control over the use of personal data varies across the world. In the USA, for example, information collected is more openly bought and sold than in Europe. But a large part of the responsibility for safeguarding personal data rests with the individuals themselves. Better education and incentives (perhaps even financial incentives) would be a sensible starting point for initiatives to improve the protection of personal identity data.

The level of ambition of the scheme is judged to be about right, but it was noted that such a programme would be unlikely to succeed in a more commercial environment, which would demand a more cohesive plan and business case, as well as a clear demonstration of buy-in from stakeholders. A broader vision might extend beyond the UK borders. But this was considered to be a step too far, as there are already many questions about the motivation, business case and the supporting technologies.

The proposed scheme demands exceptionally high levels of validation, trust and assurance, beyond those generally applied to traditional projects. Key enablers for the scheme are strong political will, sound risk management and a compelling presentation of the citizen benefits of the scheme. Public trust in the security of government services needs to be rebuilt following major data breaches at HMRC and other government departments. From this perspective, the proposed scheme offers both a threat and an opportunity.

A major public relations campaign will be required to ensure public acceptance of the scheme. A cohesive, cross-party, government plan would be a helpful vehicle for presenting the facts and the underpinning business case for identity management assurance. A visible, tougher audit process would help to build confidence in the checks and balances associated with the scheme. Support and oversight by trusted bodies, such as the Information Commissioner's Office, would also help to reassure citizens.

COLLABORATIVE WORKING IN THE PRIVATE SECTOR

The problem space in the private sector is dominated by the growing need to collaborate with business partners, suppliers and customers across corporate boundaries. Some large organisations now have more third party users than employees connected to their internal networks. Scale, complexity and cost are the major barriers to extended-enterprise identity management. Experience indicates that we can at best only solve two of these issues at any one time.

Many management processes do not scale easily or economically, even if the technology is able to support it. Scale also increases the size of the business impact and the time to recover when things go wrong. Complexity is generated by the wide variety of technologies that need to interact. Greater standardisation of identity management systems and protocols is needed. Measures are also needed to future-proof systems against advances in technology and changes in user requirements. Lifecycle management is a major issue for extended enterprise identity management. Companies not only need to trust the third party users and their identity credentials but also to understand the changes in their access needs over time.

Making the business case for infrastructure schemes such as identity management programmes is always difficult, especially in the current economic climate, as financial benefits cannot easily be realised within the payback period demanded by investment appraisal systems.

The legal environment presents additional challenges for identity management systems that have to operate across globalised business processes spanning different jurisdictions. Liability, monitoring and compliance are also major issues for extended enterprise environments. Compliance needs to be devolved to participating parties; in some cases down to the level of individuals. Efficient regulation and certification processes are needed to build trust across federated partners. Experience has shown that achieving a consensus within or across sectors demands pro-active participation by representatives who understand the risks and consequences, and who are empowered to take decisions on behalf of their organisations.

The increasing demand for extended enterprise identity management systems across markets, sectors and supply chains suggests that there might be an argument for the development of a private sector identity management strategy, perhaps mirroring the public sector approach. In fact there are arguments both for and against this concept. On the one hand, there are clear benefits in a unified strategy. But on the other, most industry sectors prefer to be left to progress their own agenda. The varying risk appetites of individual companies will also have a major influence on the levels of trust, quality and pricing associated with such services. The business drivers are less legal considerations, but more reputational and customer considerations.

De facto standards for extended enterprise identity management systems could emerge from several sources, perhaps even from government agencies supplying identity services to customers who are unable or unwilling to organise their own. If we can develop common, aligned goals, it should indeed be possible to align public and private sector identity management strategies. Certainly, from a technology or process maturity perspective, it would make sense to develop and exploit a single solution space. There are clear similarities in the problem space across public and private sectors. But there are also differences in strategic direction, detailed requirements and in the pace of development. All sectors, however, share a common need for interoperability across management processes and technology, as well as a common language for expressing confidence levels in identity checks and levels of identity assurance. Some observers took the view that, ideally, public and private sector strategies should be aligned, but that, in practice, it would not be achieved because of the many barriers that would need to be overcome.

PRODUCTS TO SUPPORT IDENTITY ASSURANCE

A range of technologies and services are now available to support identity assurance. A full overview of all product categories is outside the scope of this paper. But examples of the following products were presented at a Dragon's Den style vendor session.

Consultancy services, such as those provided by KMPG, have now developed very comprehensive methodologies for identity assurance. Risk management begins with the identification and management of risks across business processes, including insider threats such as downloading of customer data or the threats posed by moves of knowledgeable staff from back office to front office roles. It extends across the identity and access management life-cycle, encompassing dedicated processes for the management of key processes, including authentication, user management, authorisation, access management, data management, provisioning, systems management and business process management. The key to success is to build mature processes in small steps based on solid foundations. Attention to 'softer' issues such as cultural change, change management and compliance are especially important.

Federated access management enables devolved management of identities across organisational boundaries. It is a logical goal to support extended-enterprise collaboration and virtual supply management. But some critics have described it as no more than '*single sign-on on steroids*' because it relies on a single layer of security, presenting a potential single point failure, rather than the layered *defence-in-depth* approach presented by systems based on dedicated identification and access control systems. It is important not to trade off supporting layers of security in the interests of greater convenience, especially as perimeters are becoming more porous and personal data is increasing in value and sensitivity. Internal threats are also becoming more of a risk to sensitive data, demanding controls that operate within corporate network boundaries. One solution, offered by vendors such as NuBridges, is the concept of '*tokenisation*', which substitutes

anonymous tokens for personal identifiable data in application systems, thereby reducing the exposure of identification data across information systems.

Network traffic within organisations can be easily intercepted to reveal what's happening across networks. This can be used for good or bad purposes, either to spy on staff or to help detect illegal activity or security threats, such as attempts to plant Trojan horses that can trigger unauthorised exports of confidential data. Products such as NetWitness Investigator provide powerful, interactive visibility of security events and threats to security operations staff, auditors and security investigators. The benefit to organisations is reduced opportunity for unauthorised export of sensitive information, though such powerful tools require stringent management and oversight to mitigate the risk of illegal or unwarranted intrusions into personal data and transactions.

Microsoft have recently acquired U-Prove, an interesting privacy-enhancing technology that enables '*authenticated anonymity*' across information systems, using a central authentication server that only transmits the minimum identification data to each information system that the user wishes to access. This *minimal disclosure* approach sets a new standard by eliminating many of the risks to personal identity information across the corporate infrastructure.

The technology required to support better identity assurance is advancing rapidly, though the business case for justifying radical changes to the enterprise infrastructure that supports identity management systems is far from easy to make. Organisations, whether public or private sector, would clearly benefit from cross-sector initiatives that promote best practices and encourage higher standards for identity assurance. The future of information security and privacy protection will be increasingly determined by demands for secure business operations across organisational boundaries. Architectures and processes to facilitate identity assurance across extended enterprise environments need to be higher on the agenda of information security managers and systems developers.

David Lacey
Information Systems Security Association - UK Director of Research

July 2009

LIST OF CONTRIBUTORS TO THIS REPORT

Tolu	Aladejebi	Vladimir	Jirasek
Dr Alex	Baxendale	Tim	Kipps
Adrian	Beasley	David	Lacey
Rt Hon David	Blunkett	Anthony	Langdell
Frans	Bradshaw	Dr John	Leach
Peter	Bradwell	Ross	Leaning
Daniel	Brown	Bertrand	Lelaquet
Chris	Brown	Paul	Levy
Alan	Buglass	Dave	Marsh
Philippe	Chaput	Ian	McKinnon
Gabe	Chomic	Dr John	Meakin
Andrew	Churchill	Sharon	Michaels
John	Colley	Andy	Milborrow
Jonathan	Crabtree	David	Munge
Andrew	Cunnington	Simon	Murray
Peter	Curran	Chris	Neely
Dai	Davis	Brian	Niemi
Etienne	de Burgh	Toibudeen	Oduniyi
Federico	de la Mora	Aireni	Omerri
Rens	de Wolf	Mark	Pearce
Michael	Doherty	Matt	Ponting
Mike	East	Nick	Prescot
Claire	Elliott	Ben	Rexworthy
John	Elliott	Paul	Schwarzenberger
Roger	Ellis	Yvonne	Sears
Lord Merlin	Erroll	Keith	Shaw
Paul	Fisher	Michael	Sofowora
Matthew	Ford	Robin	Stafford
Les	Fraser	John	Strange
Louis	Gammon	Andrew	Sturman
James	Gosnald	Nick	Thomas
Matthew	Grist	Michael	Timms
Geoff	Harris	Bharat	Vagadia
Dominic	Hartley	Neal	Watkins
Mel	Holloway	Neil	Wheelwright
Tim	Holman	Marlene	Whyte
Danny	Ip	Michael	Wittenburg
Ken	Jacobie	Andrew	Yeomans