# IAAC Identity Assurance Programme 2007
# Report of IAAC's 4 September 2007 Workshop
# "Examining the Needs and Concerns of the Citizen"

## Summary

IAAC held a highly successful workshop on the 4th September 2007 to examine and understand the needs and concerns of the citizen with regard to the development of a national digital identity infrastructure (NDII).

Their concerns are that there are ways, including ways that they do not yet understand, by which they could be harmed, maybe even seriously harmed, by the development of an NDII. People do not have confidence that UK Government has grasped the full extent of the possible harms which its NDII could cause, that it has citizen protection as a central priority, or that it has the competence to design, develop and operate an NDII safely, securely and reliably.

Against this backdrop, citizens need to be given good reason if they are to acquire confidence in the government's NDII plans. They need to understand why the NDII is being developed and the benefits they might expect any engagement with the infrastructure to bring them. They need to understand, and be willing to live with, the harms that could befall them, believe that their protection is a central concern for the government and a priority within its development plans, and know that that safeguards are in place, including the design of reliable safety nets (workable repair and restitution arrangements), to protect them when thing go wrong.

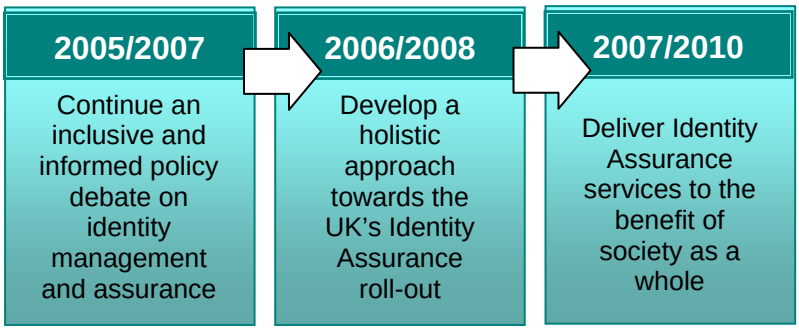
This paper is a report of the main ideas which emerged from the IAAC workshop held on the 4th September 2007 looking into the needs and concerns of the citizen. The results of this workshop served as input to the subsequent workshop, held on the 16th October 2007, which looked into the steps UK Government could take to address the needs and concerns articulated here.

A summarised version of this report is available as IAAC Briefing Paper 65.

## Background

In July 2006, IAAC published its Roadmap for Identity Assurance in the UK (the Roadmap). IAAC recognised from the start that there was no agreement regarding the desired goals any future assured identity developments should achieve, nor any programme for how to achieve those goals. IAAC's purpose is to promote the development of Identity Assurance within the context of Information Assurance. The aim of the Roadmap was to stimulate a greater understanding of Assured Identity within that context and to set out directions for future research and development.

The Roadmap envisaged three phases of activity:



In the period since the Roadmap was published, UK Government has shown a clear intention to develop a national digital identity infrastructure (NDII) and to use strong identity techniques and technologies to underpin, amongst other things, the cost-efficient delivery of a wide range of on-line services. IAAC, and others, have reasoned that the development of a UK NDII could have the potential to put each citizen's personal identity at considerable risk. Given how central a person's identity is to many of their daily activities, as well as the centrality of the role trusted identity is expected to play in the delivery of public and private sector on-line services, IAAC considers it essential that UK Government policy and plans should be formulated under a comprehensive appreciation of the associated risks and possible ramifications. If the emerging NDII is to be successful and to strengthen the UK Digital Society, any developments must not lead to the introduction of inappropriate or unacceptable risks or consequences. The IAAC IdA workplan since the Roadmap has been focussed on helping to avert this danger.

IAAC's work in the first half of 2007 focused on the UK Government's role in creating assured digital identities. The findings of that work were, in summary, that:

- There are some very substantial risks involved in UK Government's NDII plans, both assurance risks and project risks.
- A comprehensive and sound understanding of all the issues, and a cautious holistic approach, are both essential if any emerging NDII is to be successful.
- There are several critical goals which UK Government needs to achieve. Without success in all of these, Government's development plans would be at high risk of failure.

The most immediate of these critical goals was for UK Government to ensure that any developments it undertakes are acceptable to the citizenry of the UK and win the citizen's trust and confidence. This goal was carried forward and served as the central theme for IAAC's work in the second half of 2007. That work took the form of two workshops which IAAC ran in the Autumn of 2007, the first on the 4th September and the second on the 16th October. The 4th September workshop, entitled "Examining the Needs and Concerns of the Citizen", had as its objective to understand the key concerns of the citizen, and the reassurances and support the citizen needs, if people are to have the confidence to engage with the NDII. The workshop produced a clear understanding of the needs and concerns of the citizen, and its findings are the subject of this report. These findings are also summarised in IAAC Briefing Paper 65. The 16th October workshop, entitled "How UK Government can Gain Citizen Support", had as its objective to identify what Government could do to provide the reassurances and support the citizen needs. The findings of that workshop are contained within a separate report and summarised in IAAC Briefing Paper 66.

## *Workshop Results*

### Key Messages

The key messages which emerged from the 4th September 2007 workshop are:

- UK Government has to work on building the confidence of the citizen. It cannot presume that that confidence already exists or ignore the need for it.
- People need to understand the benefits that will arise as a result of any engagement they have with the NDII plus the Government's reasons for wanting to develop an NDII.
- People will need to know what types of accidents can happen and the ways in which they could be harmed by identity or infrastructure failures. People feel highly vulnerable if they are kept in the dark, even if their fears are, in actuality, unfounded. Turning on the light is the first step to dispelling fears and building confidence.

- People have expectations regarding the level of protection which should be built in to the infrastructures they use. They need to see that UK Government appreciates the importance of providing sufficient safeguards, and that UK Government will strive to protect their rights and wellbeing, even when that means protecting citizens against government itself.
- There is widespread distrust and scepticism regarding UK Government's ability to deliver a complex information-intensive infrastructure such as an NDII. People perceive the Government to have significant data security shortcomings and do not believe it has the ability to keep their data safely under control.
- To warrant citizen confidence, the NDII will need to have robust safety nets in place which limit the harm caused to the individual whenever anything goes wrong. People will need to understand how their digital identity would be repaired if it were compromised, and how Government would make good any problems or harm caused as a result of a basic service refused.

If the UK Government fails to create confidence in its national digital identity plans, then in all likelihood the private sector will end up creating multiple fragmented solutions. If the Government wants its NDII plans to succeed, it needs to heed the findings of this workshop.

## Findings

The following are the ideas which emerged from the 4th September 2007 workshop.

### Building Confidence

Trustguide (www.trustguide.org.uk) established that the key to understanding people's willingness to engage electronically within a digital society was not trust *per se* but was confidence, the confidence to take a risk with a service or counterparty new to them. Trust would grow thereafter when that confidence proved to be well founded.

Confidence is a balance between the individual's view of the benefits of engagement and their view of the possible harms they could face. People have shown they are willing to give up private information and keen to engage with e-services if they can see a direct benefit to themselves, even when they might already have articulated a number of concerns and acknowledge the existence of risks. Each person will form their own judgement regarding the balance of benefits and harms, and will develop their own personal level of confidence. For engagement to take place, the individual's judgement of the risks must not dominate their judgement of the benefits. The individual must understand and value the potential benefits they might expect to see, and must have confidence the potential risks are limited and acceptable.

Given the huge uncertainty in the likelihood of any of the various possible harms arising, plus the huge subjectivity in an individual's perception of what constitutes something happening "hardly ever" rather than "constantly", people's view of the risks they might face is determined primarily by their understanding of the possible failures that could occur and the degree to which any significant failure could cause them personal harm. To engage with the NDII, a person needs to be prepared to take on the risk that they might be harmed. Given that the magnitude of the possible harms, if unmitigated, could be very substantial, this means that they must have confidence that strong safeguards are in place, including the design of reliable safety nets (workable repair and restitution arrangements) which will protect them if thing should go wrong.

### Understanding the Purpose and Benefits

People need to understand and want the benefits that will arise as a result of any engagement they might have with the NDII, otherwise they will not engage with it no matter how risk free they might believe it to be.

As part of that, people need to understand how the NDII will be used and how much it will feature in their daily lives. For example, will people be using their digital identity every day in every way or will they be using it just once a quarter? Will the NDII be incidental to their daily life, playing a background role in support of other activities, or will it take on a foreground role of its own and itself become one of the activities around which they

have to build their life? Systems which are just a part of the furniture of daily existence are generally accepted unchallenged. Systems which take on a central role and have a direct impact on life are more likely to lead to irritation and be challenged.

People also need to know the Government's reasons for wanting to develop the NDII. Is the NDII to be a low-level tool to facilitate joined-up delivery of government services, as is the reasoning behind similar initiatives in other parts of Europe, or is it to be an infrastructure essential for our national security and for fighting terrorism, illegal immigration and crime? The benefits which it is clear people want are speedy and convenient access to services, cost savings, fraud reduction and personal security. Government can win the citizen over to its NDII plans on the basis of these benefits relatively straightforwardly. It can allow engagement to be optional and trust that people will see the connection between their engagement and their receiving these benefits.

If, on the other hand, the benefits are societal rather than individual, people's views are much less simple. If the Government's purposes behind developing the NDII are national security and fighting terrorism, these purposes are more removed from the individual, have less traction with the individual, people are more likely to want to have a say in the Government's direction, and the Government will find it much harder to win the citizen over on the basis of these types of benefits. Government will need to take care not to overstate its purposes and the associated benefits, as overselling undermines confidence. It is also clear that the Government would not be able to allow engagement to be optional. As soon as engagement becomes mandatory, the benefits become much harder to sell. They then need to be widely agreed benefits every citizen will recognise, otherwise people will not accept the price of compulsion is a price worth paying.

UK Government has yet to achieve clarity and agreement around its purposes and the associated benefits.

## Understanding What can go Wrong

People need to develop a realistic and proportionate understanding of the sorts of failures that could occur under an NDII, and the degree of harm they might suffer if they were to be affected. People will be reluctant to engage with the NDII if they feel they do not have sufficient information regarding the threats they might face or the harm they might be caused. They will feel vulnerable if they don't know what information is held about them within NDII systems, or if they don't know what government bodies or service providers might be doing with their information. Their perception of risk can be reduced greatly, and their confidence strengthened, if they feel themselves to be informed and the Government to be open about the dangers which might arise.

**The failures that can occur.**

- Again, people need to understand how a national digital identity infrastructure will be used. Will people be using their digital identity every day in every way, or will they be using it just once a quarter?
- People need to understand what can go wrong, i.e. the possible adverse outcomes which could be enabled by their use of their digital identity within an NDII, outcomes arising either as unintended consequences of the way the NDII is operated or as the results of failures of some form or other.
    - Are there any "disasters" which could befall an individual identity holder or is the worst that could happen that the citizen gets an identity "headache" which can be dealt with straightforwardly and the effects of which go away soon enough, something no more damaging than, say, a small domestic accident?
    - Are there any large scale disasters which could happen, equivalent to a motorway pile-up?
    - Is there, perhaps, a volume aspect to be considered? Instead of the citizen getting a modest headache from hitting the occasional bump in the identity road, might people find they get a whole cascade, hundreds of headaches, all arriving over a short period of time and all caused by just a single bump in the road? No one of these individual outcomes might be as serious as a broken bone but collectively they would be debilitating.

**The harm those failures can cause.**

- As well as understanding the failures, people need to understand how they could be affected by those failures. Can their physical safety be put under threat due to a privacy failure? Can the near impossibility of gathering in and repairing incorrect personal information once it has been released and widely shared mean that the burdensome effects of a data error could rumble on for years? Can a person be made stateless by a system that refused to acknowledge them? Can a person be deemed to be dead by "the system" despite being very much alive in real life?

- There is a sense that the nature of the individual person's relationship with their government is significantly different from that of their relationship with a private sector service provider. People usually feel that their relationship with a private sector service provider is well bounded and any harm which might arise from that is limited. For example, bank failures might be frustrating and take time to clear up but they almost never lead to incarceration and it is hard to imagine them being life threatening. The finite nature of these relationships acts as a safeguard. By contrast, people feel their relationship with government (local and central) is less bounded, more open-ended, and as a result the potential for harm almost unlimited. Physically vulnerable people will worry that their personal safety could be put at threat by privacy failures. Financially vulnerable people will worry that they could lose all financial support due to an identity mistake. A dissenter might worry they could be made stateless by a system that refused to acknowledge them.

- Privacy is, on the whole, relatively well understood and people are attuned to it as a right worth protecting. But it is not only one's privacy which could be affected by an NDII but also one's anonymity. It is not at all clear what standing anonymity has in people's minds, what value they place on it and what the impact might be of its loss. Anonymity is rarely voiced as an area of discussion or concern. However, it might start to become an important issue for people as identity infrastructures are developed. When it does, it could come to be seen as a rather complex issue.

There is a further complication to developing a clear understanding of the balance between benefits and risks. Sometimes, what is seen as a threat by one person is seen as a benefit by another. Consider data aggregation and data sharing. For some, the growing ability of government to aggregate and share data as technology advances is a threat to their privacy. For others it is a boon which enables joined-up service delivery. The perception of whether something is a threat or a benefit appears to be conditional upon one's underlying level of trust in government not to use one's personal information against one's proper interests.

## Citizen Protection as a Government Priority

People are increasingly aware of risk as an issue. They are concerned not only with the amount of harm they could be caused but also with whether or not they are going to be protected. People today have expectations that those promoting a new initiative or service will, as part of that, provide them with adequate protection. People need to believe that, despite their personal concerns, they will be kept safe. They need to see that their Government appreciates the importance of providing sufficient safeguards within any NDII it develops, and that UK Government will strive to protect their rights and wellbeing, even when that means protecting citizens against government itself.

Again, people see a difference between their dealings with the public and private sectors. Not only is the degree to which they could be harmed different, the presence of safeguards is different. People usually feel there are safeguards protecting them in their dealings with private sector service providers. If they don't like the service they receive, they have the power to take their business elsewhere, and Government protects them from the worst excesses and abuses the private sector might deliver. In contrast, people do not feel similarly safeguarded with respect to their dealings with their government. They do not have the power to take their business elsewhere and it is not clear there is any body in a position to protect them from the worst excesses and abuses of Government. In the UK currently, central government is not afforded a high level of trust by the citizen. People are not convinced that the Government has grasped the full extent of the possible effects and harms which an NDII could cause, and they do not see UK Government as a force for their protection. This

heightened sense of vulnerability in the face of their government increases people's need to see positive evidence that Government intends to make their protection a central priority.

In the face of this requirement, what people see instead are policy developments which appear to be driving in the opposite direction. Initiatives such as the ID Cards Bill can be taken to imply a change is taking place in the relationship between the citizen and their government and especially that UK Government does not trust its citizens. There is a sound argument, which remains to be answered, that the creation of a central national digital identity infrastructure actually increases the opportunity for citizens to be harmed by government errors and by fraud and other criminal activity. To this degree the creation of an NDII can be taken as evidence that UK Government does not have the interests and protection of the citizen close to its heart.

### UK Government's Competence

There is widespread scepticism regarding the Government's ability to design and deliver complex systems or to operate information-intensive infrastructures safely, securely and reliably. People are sceptical about the ability of technology designs to cater for every situation, and are concerned about function creep leading to technical infrastructure being used in ways which could have but were not foreseen by Government.

People are also sceptical of the Government's ability to keep data secure. Operational security breaches seem to occur continually, arising from a wide variety of sources: ignorance or carelessness by hapless "junior officials"; poor or unclear policies; poor design; technology failures; compromised procedures; corrupt officers. People perceive the Government to have significant data security shortcomings and do not believe it has the ability to keep their data safe whilst under its control.

### The Need for Safety Nets

Trustguide established, and the workshop confirmed, that a necessary component, essential if people are to develop the confidence to engage with an untried NDII, is for safety nets to be in place to protect people when something goes wrong. Not just safeguards in general but safety nets in particular, where safety nets are the types of safeguard which arrest a problem when it happens and then provide restitution and redress. When something goes wrong, the citizen expects Government to limit the extent of any damage and make good any harm caused. Safety nets are essential to creating citizen confidence.

There are a number of areas where the citizen will be particularly concerned to see safety nets in place.

- **Identity Repair**. Identity repair is a very challenging issue and it is not immediately obvious to people how a broken digital identity would be repaired. People will need a lot of reassurance that Government fully appreciates and understands the problem and knows how to solve it. The options and processes for the recovery of a compromised identity must be developed very thoroughly, not just on a "best efforts" basis.
- **Citizen Control**. While people have doubts about the fullness of the government's intention and ability to protect their interests, they need to feel that they individually have the ability to take whatever steps they deem necessary to keep themselves safe. The design of the NDII has to provide people with a sufficient level of personal control. This should include the option for an individual to scale down the level of their engagement should they feel that necessary, plus the ability to control what data is held about them and restrict how it may be used.
- **Biometric Data**. Biometric data is seen as deeply personal and people are very sensitive to the idea that if not strictly controlled it can be used against them in ways they don't understand. People cannot change their biometric data. Hence, they feel strongly that there must be very tight limits on who can access their biometric data and how it may be used. Publicity about how innocent people can find their DNA has been put onto the national DNA database (NDNAD) and how they do not have the ability to get it removed makes people feel very unsafe.
- **Redundancy and Contingency Arrangements**. When there is a major accident on the motorway, the emergency services close the road until they are confident it can be reopened safely. People will want to see

that when something goes wrong within the NDII, the Government immediately closes that part of the infrastructure involved and ensures it stays closed until any root causes have been resolved. Government will need to retain redundancy and contingency arrangements so people can continue to access services and go about the activities of life without being significantly inconvenienced as a result.

- **Independent Reporting**. People need to have confidence there will be reliable and prompt independent reporting of the problems which do arise. This will allow them to feel they have a true measure of just how well the NDII is working, how often things are going wrong, and what problems and dangers other people are having to deal with. They do not want UK Government to be able to hide "dirty linen" out of sight.
- **Legal structures**. People want their protections and their ability to seek substantial redress to be backed up by the force of law. There is a pressing need for legislation, policing and the justice system to catch up with the realities of the information age.
- **Accountability, Responsibility and Liability**. People need to see UK Government prepared to be held accountable for the NDII which emerges as a result of its plans and initiatives, to take full responsibility for the design and operation of the NDII, and to accept liability for when things under its control go wrong. Liability is a very important issue and it is not clear how UK Government will go about addressing it.

If the Government fails to create confidence in its NDII plans, then in all likelihood the private sector will move ahead and overtake it. The result will be multiple fragmented solutions, each limited in its scope but perhaps more readily acceptable to the public. If the government wants its NDII plans to succeed, it should heed the findings of this workshop.