IAAC Identity Assurance Programme 2008
Report of IAAC's 4 April 2008 Workshop
"Digital Identity Governance Framework"

Summary

IAAC held a workshop on the 4th April 2008 to identify and understand the components which make up a digital identity governance framework for a national digital identity infrastructure (NDII).

The purpose of a digital identity governance framework is to protect the interests of all NDII participants in proper balance. Within that purpose it has three main objectives.

The first is to lay out the protections in place for those situations where there is no conflict between the legitimate interests of the identity subject and those of other NDII participants (principally the public interest).

The second is to describe the way in which Citizen Control is provided, plus any constraints or conditions which might affect the way in which Citizen Control is exercised.

The third is in recognition that there will occasionally be situations where the interests of other NDII participants cannot be served without infringing and potentially putting at risk the legitimate interests of one or more identity subjects. The objective of the governance framework is then to lay out the safeguards provided so the interests of identity subjects are not harmed unnecessarily or inappropriately in those situations.

NDII primary records will need to be protected from abuse by authorised users or relying parties. Some of these requirements can be addressed by confirming that the NDII and relying parties will be fully subject to the Data Protection Act 1998 (DPA). There are, however, a number of areas where the provisions within the NDII governance framework might need to be strengthened beyond those contained within the DPA.

As has been mentioned in several IAAC reports, effective recoverability and restitution in the event of NDII failures and breaches is essential. The governance framework will spell out the particular requirements for achieving effective recoverability and restitution within the NDII.

The governance framework will also spell out the arrangements for protecting the citizen when their interests have been infringed in the public interest. These arrangements include notifying the citizen when this has happened, and providing the citizen with the ability to challenge such access if they feel it has been conducted improperly.

Having laid out a governance framework for the NDII, the UK Government should follow a governance-friendly approach tailored to support the governance framework. This might include performing Privacy Impact Assessments on the applications which use NDII data, ensuring the architecture of the NDII is well suited to the governance requirements, and following a staged development programme which limits the amount of harm the NDII can cause citizens until sufficient experience in its operation has been gained.

A summarised version of this report is available as IAAC Briefing Paper 69.

Background

For the background to IAAC's Spring 2008 workshops, please refer to the report on the findings from IAAC's 5th March workshop.

The subject of this April 2008 IAAC workshop was digital identity governance, i.e. what are the components of a digital identity governance framework for a UK NDII. IAAC also ran a related workshop in March 2008 (reported upon separately) to look at Citizen Control, i.e. what are the components which make up Citizen Control for a UK NDII. Citizen Control is a central component of an NDII governance framework.

Note that the findings from each of these two workshops are intended to relate to a UK NDII and are not intended to be specific to the present government's current plans for an NIS. The April workshop was run with the co-operation and active participation of the IPS and the findings are not intended to be, and should not be taken to be, implied or direct criticism of IPS' current NIS plans. Many of the recommendations stated here as being applicable to a UK NDII are already planned for implementation within the NIS.

It is recognised that digital identity information governance is just one aspect of the totality of the governance needs which should be addressed for the NDII. However, it is only those aspects of the NDII's governance arrangements which relate to digital identity which are of concern to IAAC here and are considered to fall within IAAC's use of the term digital identity governance framework.

Workshop Results

Key Messages

The key messages which emerged from the 4th April 2008 workshop are:

- Proportionality is a key principle within the NDII governance framework. The principle of proportionality will need to be defined carefully and comprehensively within the governance framework, as will other terms which form part of the description of permitted purposes.
- The UK Government should strive to define its data usage governance provisions as fully as it can within the NDII governance framework. Reliance on case law to resolve incompleteness and imprecision within the governance framework would enable questionable practices to be performed, or performed without due safeguards, whilst awaiting cases to be decided. This could put citizens at undue risk and undermine the confidence the Government wishes citizens to have in the NDII.
- It is essential for the UK Government to ensure that the design and operation of the NDII does not preclude identity recoverability. The citizen starts with the ability to authenticate themselves from outside the NDII and this is used when the citizen first enrols into the NDII. The operation of the NDII must not cause this external authentication capability to wither.
- As the NDII gets used, unexpected faults in the design or operation of one or other part of the infrastructure will emerge. The UK Government must ensure it retains the ability to force the repair of NDII faults within a prescribed timeframe, and, for significant faults, to suspend operation of the affected part of the NDII until those faults are rectified or a suitable work-around has been developed.
- The UK Government should limit the scope of the first generation of NDII specifically to avoid any ways in which the NDII could give rise to significant harms to individual citizens or to the public more generally. Only once the UK has gained experience using an NDII and has learned how the system fails should the Government allow the development of a more comprehensive NDII which is capable of giving rise to greater harms.

Findings

The following are the findings which emerged from the 4th April 2008 workshop[1].

The Purpose of a Digital Identity Governance Framework

The purpose of an NDII Digital Identity Governance Framework is to protect the interests of all participants in the NDII in proper balance. The governance framework has three primary objectives.

[1] IAAC ran two workshops in the Spring of 2008, this April workshop looking at the governance framework and a March workshop looking at Citizen Control. Inevitably, some of the ideas which were raised in the discussion on Citizen Control related to the wider governance framework. Where that is the case, the ideas have been covered in this report rather than in the Citizen Control report.

- The first objective is to lay out the protections in place for those situations where there is no conflict between the legitimate interests of the identity subject and those of another NDII participant (principally the public interest). The NDII should provide adequate safeguards to maintain an acceptable standard of safety and security for participating citizens without their needing recourse to additional protections.

- Given that different citizens will have differing views of the sufficiency of that standard of safety and security, additional protection capabilities (known collectively as Citizen Control) are provided by the NDII to allow the citizen as identity subject to take particular additional precautions, should they feel that necessary, to protect themselves from harm in situations where they feel themselves exposed to unnecessary or unwarranted heightened risks. Citizen Control is the fine tuning that allows a citizen to reduce their risk in those particular situations, and is exercisable when its exercise does not conflict with an overriding interest of another participant. The second objective of the NDII governance framework is to describe the supporting features and protections which enable Citizen Control, plus any further constraints or conditions which might be necessary on the way in which Citizen Control is exercised.

- There will, on occasions, be situations in which it is proper that the legitimate interests of the identity subject are overridden by those of another NDII participant. The interests of the identity subject should still be protected in those situations, in proper balance with the interests of the other participant. The third objective of the NDII governance framework is to lay out the safeguards provided so that the interests of the identity subject are not harmed unnecessarily or inappropriately in those situations.

  There will be many situations where the public interest can be served without harming the legitimate interests of identity subjects. This third area of concern for the NDII governance framework is specifically for those situations where the interests of other participants cannot be served without infringing and potentially putting at risk the legitimate interests of one or more identity subjects.

The Scope of an NDII governance framework

The NDII will be required to satisfy several sets of security requirements (not just those of the DPA but also those of the e-Borders programme, Human Rights Act, FoIA, Official Secrets Act). The UK Government also has a number of commissioners who might well have an interest in the operation of an NDII (not only the NDII's own commissioner but also those of the ICO and the ISC, and possibly the Pan-Government Accreditor for technical issues). The NDII governance framework should set out to address all these needs within one rational structure.

It is anticipated that the majority of accesses to NDII data will be identity subject initiated, rather than public interest initiated. Further, it is possible that the balance of accesses could be very highly skewed, with the overwhelming majority of accesses being identity subject initiated leaving public interest initiated accesses to form only a very small minority of the access traffic. Even if this emerges to be the case, the protection of the identity subject during this tiny proportion of accesses will remain an important objective and test for the NDII governance framework.

The NDII Standard Level of Safety and Security

The first objective of the NDII governance framework is to lay out the protections in place for those situations where there is no conflict between the interests of the citizen as identity subject and the interests of other NDII participants. The NDII should provide adequate safeguards to maintain as standard an acceptable level of safety and security for participating citizens in all such situations.

NDII primary records will need to be protected from unauthorised access.

- Threat actors of concern include hostile states and terrorists.

- To reduce the exposure of NDII primary records, the only direct links to the NDII's primary records should be very highly secure links to a limited number of highly secure end-points. NDII primary records should not be reachable from the Internet or any other public or private network with less than the highest level of security.

- To enhance the protection of NDII primary records, the primary record for an identity subject should be split physically and logically rather than all held within a single database.

NDII primary records will need to be protected from abuse by authorised users. Authorised users are those who have direct access either to the primary records or to the infrastructure in which primary records are stored or used, as part of the management and operation of the NDII. It does not include relying parties.

- To reduce the exposure of NDII primary records to abuse by authorised users, the number of authorised users should be kept to an absolute minimum.
- Experience shows that individuals with privileged access to sensitive information do sometimes abuse their access privileges. The NDII will need:
  - Controls to prevent such abuse (e.g., strong authentication, strong individual accountability, separation of duties, dual control on sensitive accesses);
  - The capability to achieve immediate detection of any type of abuse;
  - Strictly applied and severe penalties for those who do abuse their access privileges.

NDII primary records will need to be protected from abuse by relying parties. Relying parties includes those who make use of the NDII for an approved statutory purpose, e.g. service providers permitted to verify the identity or credentials of an individual before providing their services, those permitted to access the NDII in support of permitted public interest purposes.

As a general principle, the NDII should strive to reduce the threat surface:

- Only justifiable parties should be allowed access. Relying parties must have a justifiable purpose or need before they should be allowed to be NDII participants.
- The purposes for which the NDII is permitted to be used by relying parties should be defined unambiguously and carefully within the governance framework. The governance framework should expressly ban any purpose which is not expressly permitted.
- As a general principle, the mode of access relying parties make to the NDII for their permitted purposes should aim to minimise the exposure of primary data.

  For example, many of the services which the NDII is expected to support will require relying party access to no more than a single primary record at a time. Whenever possible, this access should be a simple enquiry mode of access, where the relying party asks the NDII a validation question and gets a Y/N answer back.
- It is recognised that enquiry mode minimises but does not eliminate the exposure of data to relying parties. It does not on its own prevent the external organisation from recording for its later use the personal data which the NDII has validated, or from recording any further details which are held on any token (passport; id card) that passes through its hands.

  Under all modes, not only under enquiry mode, relying parties should be barred from gathering or storing data which is not required for their permitted purposes, and should be required to delete any retained data as soon as it is no longer required for the permitted purposes for which it was gathered, unless expressly permitted by the citizen. Relying parties should not be permitted to retain personal details for future convenience.
- In situations where enquiry mode does not suffice, i.e. where the relying party needs primary data to be provided to it by the NDII, only that primary data properly necessary for the permitted purpose should be provided.
- For relying parties which need access to more than one primary record at a time, for example, those acting on behalf of the public interest, that access should be mediated. Only that subset of the primary records

which are needed for the stated permitted purpose should be provided and then only the subset of data from each primary record which is needed should be provided.

- No relying party should be able to modify or delete NDII records, either primary records or any extracts provided under mediated access.

- Restrictions are needed not only on the range of data which may be gathered by a relying party but also on the range of uses to which that data may then be put. Just because some of an identity subject's data might be in the public domain already does not mean the identity subject can be presumed to be willing for that data to be used in just any way regardless. For all modes of access, there should be limits imposed on the actions permitted on that data. Only those actions necessary for the permitted purposes should be permitted.

Some of the above requirements can be addressed by confirming that the NDII and relying parties will be fully subject to the Data Protection Act 1998 (DPA). The DPA has, over the past three decades, played an important role keeping UK citizens safe. To the degree that it remains appropriate and adequate to the needs arising from the NDII, the DPA should be given a central position within the NDII governance framework and should be used as an important part of keeping the citizen safe within the NDII.

There are a number of areas where the provisions within the NDII governance framework might need to be strengthened beyond those within the DPA.

- The provisions within the NDII governance framework covering the gathering of data by relying parties should be strengthened beyond those within the DPA by adding a requirement that relying parties should not use their commercial power to gain unneeded access to private data.

- The provisions within the NDII governance framework covering the use of data by relying parties should be strengthened beyond those within the DPA. Data aggregation is one capability which has expanded enormously due to technological advances since the DPA was constructed, and the control of data aggregation and dataveillance are major concerns under an NDII.

- Proportionality, i.e. that relying party access should be limited to only that data and those actions properly necessary for a permitted purpose, is a key principle within the NDII governance framework. Experience with the application and enforcement of the DPA has shown that the principle of proportionality will need to be defined very carefully within the governance framework. Similarly, other terms such as "serious crime" should be defined carefully where such terms form part of the description of permitted purposes (e.g., where the prevention and investigation of serious crime is to be one of the permitted purpose under which the public interest can override the citizen's interest). Specific consideration should be given to the means and methods by which proportionality will be enforced, taking on any lessons which can be learned from experience with the enforcement of the DPA.

  If proportionality provisions covering the use of data do not specify precisely or comprehensively enough what is and is not permitted, it might become the practice to allow the courts and case law to determine what is and is not permitted use of data. Given the highly technical nature of the NDII and of the provisions which need to be specified within its governance framework, the UK Government should strive to define its data usage governance provisions as fully as it can within the NDII governance framework. This would reduce the burden on case law to resolve incompleteness and imprecision within the governance framework. It would also minimise the extent to which questionable practices (for example, fishing exercises) could be performed, or performed without due safeguards, whilst waiting for cases to be decided, and would minimise the potential for harm to citizens. Lax definition could undermine the confidence the Government wishes citizens to have in the NDII, and could reinforce the general scepticism which has led to Citizen Control being so strongly required (in particular many citizens' doubts that the UK Government can be a force for their protection).

- The reporting provisions within the NDII governance framework should be strengthened beyond those contained within the DPA by adding a requirement on the NDII operator and relying parties to report to

the appropriate commissioner, and to place notice in the public domain of, any failure or security breach which might have exposed identity subjects or their data to heightened risk.

- The reporting provisions within the NDII governance framework should require the NDII operator and relying parties to notify privately each identity subject who may have been affected by a security breach, providing sufficient details of the breach, of how they might be affected by the breach, and guidelines for action, so the identity subject can take any appropriate actions, either within or outwith the NDII, to protect themselves from possible damage or harm (e.g. to protect themselves against the consequences of identity theft).

- There are circumstances under which exemptions from the DPA's normal force of application apply. Some of the DPA's requirements do not apply where a relying party is under a conflicting legal duty, e.g. to furnish information to the Secretary of State for a specified purpose. The UK Government should consider whether there might be circumstances in the context of the NDII where the DPA's exemptions should not apply.

- Penalties for infringements by authorised users or relying parties need to be strictly applied and severe, e.g. for relying parties that do not honour Citizen Control, for authorised users who misuse their access privileges. Given that the NDII would be a part of the UK's critical national infrastructure, penalties plus enforcement capabilities and enforcement resources should be considerably stronger than those currently in place for the DPA.

UK Government needs to give thought to how Citizen Consent is to be enforced on a relying party's use of NDII data. If a citizen allows one use of their data but not another, that permission needs to be carried forward in a manner which enables the citizen to have confidence that their wishes will be honoured and the relying party plus any other parties involved in the transaction will apply the citizen's wishes rigorously. In addition, sufficient auditability is required to support independent checking that a citizen's consent has been honoured and to ensure that actions are traceable in the event something does go wrong and a citizen is put at greater risk or is harmed.

Not only are the interests of the identity subject aided by ensuring the subject's NDII primary data is correct and current, the interests of other parties are aided by the same. Responsibility for ensuring the accuracy and currency of a subject's data needs to be assigned, and it seems natural that this responsibility should be given to the identity subject themselves. The UK Government should consider to what degree the identity subject should be given responsibility for maintaining the accuracy and currency of their NDII data, what means should be provided to the subject to enable them to access their data and fulfil that responsibility, and the nature and severity of any penalty which might be imposed should the identity subject fail to fulfil that responsibility.

Recoverability

Throughout its research into NDII identity assurance issues, IAAC has reported that recovery and restitution in the event of failures or breaches have a large part to play in the degree of confidence the citizen has in the safety and security of the NDII. IAAC has maintained throughout that the NDII must provide adequate safety nets so that, when things do go wrong, the NDII has the ability to provide adequate recovery and restitution for the affected citizen.

The NDII governance framework should ensure that adequate and effective recoverability and restitution is provided. The governance framework should require the NDII to provide:

- Rapid detection of security breaches. Data is usually not stolen, it is most likely copied. An identity subject might not know their data has been copied inappropriately until they see the evidence in the field, in which case damage might already have been done. The NDII needs to have detection capabilities which can detect promptly all failures or breaches affecting the safety or security of the citizen.

- Damage limitation. As much as possible, there need to be limits on the amount of damage or harm the identity subject is permitted to suffer as a result of NDII failures or breaches, analogous to the indemnities which protect the card holder in instances of credit card fraud.

- Rapid recovery and restitution. The NDII needs to provide rapid recovery to make good any damage caused, and swift restitution to undo any harm caused, especially in light of the fact that damage and harm might already have been caused before the failure or breach is detected. People on, for example, a low income, can find even a short disruption or small impact has a major affect on their life.

The NDII needs to provide safeguards against citizens being disadvantaged or worse by the incompleteness, incorrectness or inaccuracy of their information held within the NDII when that data disability is no fault of the identity subject themselves. Enrolment is the process by which a subject's identifying data is built up within the NDII. It is conceivable that, in some cases, for one reason or another, the data gathered through enrolment will be incomplete, incorrect or inaccurate, through no fault of the identity subject. It is also conceivable that, over the course of time, an identity subject's data can become incomplete, incorrect or inaccurate due to processes which are not of the identity subject's doing. In such situations, it is important for the identity subject to be protected against any disadvantage, damage or harm which might arise from a relying party having trusted in the subject's data.

Further to this, it is conceivable that in some cases an identity subject's data will be sufficiently corrupted or compromised, perhaps through an NDII failure or security breach, that no trust can be placed in any part of that identity subject's primary data. Given this, it is essential for the UK Government to ensure that the design and operation of the NDII does not preclude identity recoverability.

> Even if the NDII is built around the idea of each identity subject having a primary or root identifier, a single secure legal root identity which is intended to underpin all trusted identity-based activities within the UK, the UK Government cannot sensibly ignore the fact that some citizens' root identifiers will get compromised or corrupted.
>
> Even if the design of the NDII results in all of an identity subject's primary identifying data being brought together into one infrastructure, the UK Government has to ensure that a citizen retains the ability to authenticate themselves from outside that infrastructure. The citizen will need this ability should they be unfortunate enough to have their primary identity data be compromised or corrupted.
>
> The citizen starts with the ability to authenticate themselves from outside the NDII and this is used when the citizen first enrols into the NDII. The operation of the NDII must not cause this external authentication capability to wither. The UK Government is urged strongly to consider how this protection can be achieved and to ensure that the NDII governance framework contains any necessary provisions to prevent the identity subject's ability to authenticate from outside the NDII being weakened.

It is inevitable that, as the NDII gets used by an increasingly large and diverse community, both of identity subjects and relying parties, unexpected faults in the design or operation of one or other part of the infrastructure will emerge. Some of these faults might enable situations to arise in which the identity subject is placed at heightened risk. In these cases, faults will need to be fixed as promptly as is reasonably possible. The UK Government must ensure it retains the ability to force the repair of such NDII faults within a prescribed timeframe, and, for significant faults, to suspend operation of the affected part of the NDII until those faults are rectified or a suitable work-around has been developed.

Citizen Control

The second objective of the NDII governance framework is to describe the supporting features and protections which enable Citizen Control. IAAC addressed the topic of Citizen Control in the workshop it held on the 5th March 2008. For a full discussion of the Citizen Control aspects of the NDII governance framework, please refer to IAAC Briefing Paper 68 and the associated full workshop report.

Protecting the Citizen When their Interests are Overridden by the Interests of Another Participant

There will be many situations where the interests of other participants can be served without harming the legitimate interests of identity subjects. For example, if the NDII is used to discover a person's identity in the public interest, and to do so the identity records of a large number of identity subjects are accessed during the

search, there is no reason to believe that a properly conducted search should harm the privacy of those subjects shown by the search not to be the person being identified. However, there will also be some situations where the interests of other participants cannot be served without infringing and potentially putting at risk the legitimate interests of one or more identity subjects. For example, the investigation of a serious crime could result in the privacy of a number of identity subjects being infringed. The interests of the identity subject should still be protected in those situations, in proper balance with the interests of the other participant being served. The third objective of the NDII governance framework is to lay out the safeguards provided so that the interests of the identity subject are not harmed unnecessarily or inappropriately in those situations.

The NDII governance framework should cover:

- Informing the citizen. In the physical world, if, for example, a person is questioned by the police investigating a crime, that person is aware they are being questioned and is aware of the degree to which their liberty or their privacy or another of their legitimate interests might have been infringed by the fact of their being questioned or the nature of the questions. If parallel questioning can be conducted by interrogation of NDII data, that could be conducted without the citizen's knowledge. Hence, the citizen's legitimate interests could be infringed without their knowledge. In such situations, then, without undue delay, the citizen should be informed that their data has been accessed in such a manner and should be told when, by whom and for what purposes.
- Giving the citizen the right to challenge: In the physical world, if, for example, a person believes they have been stopped for questioning without reasonable suspicion, or if they believe they have been wrongfully arrested, that person may have the right to have the conduct of the police be reviewed. In parallel, if the citizen feels their information has been accessed improperly or disproportionately or outwith a proper purpose, they should be able to have this access be reviewed and scrutinised by an independent tribunal and, ultimately, the courts.
- Transparency: If there are limitations on the degree to which the citizen can be informed about matters which might have a bearing on their interests, then these limitations should be stated explicitly within the governance framework. For example, citizens should be able to find out if there are:
    - Any restrictions on what information can be obtained through the FoIA relating to, for example, access statistics or specific access purposes;
    - Any secret provisions regarding, say, the data held within the NDII or the actions which, say, the Secret Intelligence Service, are permitted to perform on citizen data;
    - Any restrictions on making public in full the assurance reports of the NDII commissioner;
    - Any temporary reporting restrictions which might be placed on major accidents and their outcomes.

Governance-Friendly Approach

As soon as the NDII Digital Identity Governance Framework has been defined, the UK Government's should review its approach to the development of its NDII and adjust that approach as indicated to support the governance framework. It would be difficult for the UK Government, having laid out a governance framework, then to explain why it was not following a governance-friendly approach.

- Privacy Impact Assessments. The ICO has developed the idea of Privacy Impact Assessments, PIAs, to help ensure that appropriate safeguards protecting personal privacy get built in to major developments. Just as risk management practitioners undertake a Business Impact Assessment as part of understanding the security risks of a system and to help ensure that all needed security controls get built into the system, the ICO is strongly recommending that a PIA should be undertaken as part of understanding the privacy risks associated with a new development and to help ensure appropriate safeguards and controls can be built in to the resultant systems.

It is understood that the ICO has said it will not undertake a PIA on the national identity register (NIR) as the NIR is already too far into development. However, there would still be significant benefit for the UK digital society from the ICO or other competent body undertaking PIAs on the applications which will use NDII data, and having a PIA be performed should be made part of the accreditation process for external applications. Mindful that a person's privacy is not the only personal interest which could be harmed by the NDII, PIAs may need to become CIIAs (Citizen Interest Impact Assessments).

- NDII architecture selection. There are a small number of different identity management architectures in use today within the private sector and different architectures (e.g. user-centric vs. organisation-centric, federated vs. centralised) support privacy protection to different degrees. The way in which different architectural options enable or constrain the NDII's ability to support particular aspects of a governance framework, and the ways in which relevant technologies can be used, misused or abused, needs to be clearly understood both by the UK Government and by the NDII's designers.

- Resolving Conflicts Between Safeguards. There may be a number of situations where safeguards, each valuable in themselves, can be in conflict with each other. For example, the conflict between Auditability and Privacy discussed in the report on Citizen Control. The ways in which conflicts of this type can arise, and the options for minimising the conflict and for adjusting the balance between safeguards, need to be explored and understood.

- Programme Planning. Despite all the effort it has expended so far, the UK Government cannot be confident it has identified and understood adequately all the risks associated with the NDII. Given this, plus that much NDII design work has commenced without an NDII governance framework having been developed beforehand, it is clear there is every chance that the NDII which results in the coming years might not provide as much safety and security for the citizen as the citizen should be able to expect. For the protection of the future UK digital society, the UK Government should be cautious and stage its development of an NDII. It should limit the scope of the first generation of NDII specifically to avoid any ways in which the NDII could give rise to significant harms to individual citizens or to the public more generally, even if that then limits the benefits achievable from the NDII. Once the UK has gained experience using an NDII, has learned how the system fails, how it gets misused or abused, and how recovery and restitution arrangements need to operate, only then should the UK Government feel it can safely allow the development of a more comprehensive NDII which is capable of delivering greater benefits but also of giving rise to greater harms.