πωχ

Australian Taxation Office

SBR Authentication DRAFT Privacy Impact Assessment

Phase 1: High Level Design
November 2008

Liability limited by a scheme approved under Professional Standards Legislation.

i. Document Control

Version	Issue Date	Author	Approved by	Comments or Change listing
0.1	28/11/08	PwC	PwC	Initial draft
1.1	1/12/2008	PwC	PwC	Updated following TPM feedback
1.2	9/12/2008	PwC	PwC	Added EOI/POI definitions, amended wording around EOI risks and use case documentation still to be developed

ii. Definitions/acronyms

ABN	Australian Business Number
ABR	Australian Business Register
ATO	Australian Taxation Office
CA	Certification Authority
CMP	Certificate Management Protocol
EAI	Enterprise Application Integration
ECI	Electronic Commerce Interface
EOI	Evidence of identity (EOI) is evidence provided to either the Commissioner of Taxation or the Registrar of the Australian Business Register (ABR) of the applicant's existence and identity. Evidence of identity is only required once, that is, at initial registration.
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
ICP	Integrated Core Processing
PIA	Privacy Impact Assessment
PKI	Public Key Encryption
POI	Proof of identity (POI) is a client proving they are who they say they are by quoting or writing, for example, their TFN. POI is provided each and every time a client contacts the Tax Office throughout the entity's life. The SBR authentication credential will act as POI for clients using the SBR authentication solution and SBR core services.
PwC	PricewaterhouseCoopers
RA	Registration Authority
SBR	Standard Business Reporting
SDK	Software Development Kit
TFN	Tax File Number

iii. Related documents

SBR-A TRA	SBR Authentication Solution – Threat and Risk Assessment (Phase 1: High Level Design), November 2008

Contents

This report has been prepared for the Australian Taxation Office. It should not be circulated to any other parties without written permission from PricewaterhouseCoopers, and no one other than the Australian Taxation Office should rely on this report for any purpose.

1 Executive Summary

Scope

This draft report presents the Australian Taxation Office's (Tax Office) findings of the preliminary Privacy Impact Assessment (PIA) conducted over the high level design of the Standard Business Reporting (SBR) Authentication solution.

The PIA process was conducted in accordance with the agreed scope as defined by IT 06-125 Official Order 14 and with reference to government and best practice security guidelines including:

- Australian Government Information and Communications Technology Security Manual (ACSI 33);
- Protective Security Manual (2005);
- ISO standards including 27001;
- Office of the Privacy Commissioner's Privacy Assessment Guide (2006) and related guidelines as applicable;
- *Privacy Act* (Cth) 1988 and associated Information Privacy Principles; and
- Tax Office and Commonwealth Government security policies and guidelines.

Background

Whilst a PIA is not a requirement under the *Privacy Act (1988)*, it is generally accepted as better practice that a PIA be conducted for projects that collect, use or disclose personal information. The results of a PIA may assist in the identification of a project's impacts and risks to privacy, and ensure that such implications are appropriately mitigated and/or managed.

PIA Process

At a high level, the process undertaken for this PIA included the following key activities:

- determining the nature of the project;
- conducting a Threshold Assessment in order to confirm that a PIA is required;
- mapping the flow of personal information apparent in the high level design of the authentication solution; and
- identifying treatments and controls to mitigate privacy risks.

As the SBR Authentication project is at a stage of high level design, not all personal information requirements of key processes have been defined. We have highlighted in Appendix A the areas of the high level design that require finalisation to enable a more thorough PIA to be performed.

Providing this information is determined within appropriate timeframes, a more comprehensive privacy impact analysis will be undertaken upon completion of the detailed design in February 2009. This will include the Information Privacy Principles Compliance Checklist components of the PIA Guide.

Threshold Assessment

Although some details of the authentication project have not been finalised, the threshold assessment has found that the extent of collection and use of personal information apparent in the high level design is sufficient to confirm that a PIA is indeed appropriate.

Summary of Significant Privacy Risks

The high level design of the SBR Authentication project was reviewed and the following privacy-related risks have been identified:

Significant Privacy-Related Risks	Assessment of Current Risk Exposure to the SBR Project
EOI process is insufficient to reliably establish that the person obtaining a credential is the individual to whom the EOI data relates.	Severe
Solution design is not expected to comply with legislative and government requirements and social norms.	Severe
The large-scale storage of personal information increases the likelihood and impact of unauthorised disclosure or usage for other purposes.	High
Privacy incidents may occur due to the use of third parties such as those who manage IT infrastructure components.	Significant
The amount of private information collected may be excessive given its collection is to enable business transactions. [1]	Moderate
Personal information is disclosed during transmission, storage and/or disposal.	Design insufficient to enable assessment
Personal information is used for purposes not initially permitted by the individuals.	Design insufficient to enable assessment
Public confidence is reduced by poor handling of privacy incidents.	Design insufficient to enable assessment
Information is collected without adequate disclosure of its collection or intended purpose.	Design insufficient to enable assessment
The EOI process for individuals not wishing to provide their TFN may require the collection and usage of extensive personal information in order to provide an alternative means of identity validation	Design insufficient to enable assessment
Excessive retention of private information.	Design insufficient to enable assessment

Table 1. Summary of significant privacy-related risks.

It should be noted that Privacy related risks cannot be fully assessed or mitigated because processes and information flows are yet to be defined at a detailed level. These areas of design could potentially have a severe impact on the SBR project.

Summary of Proposed Treatments

Proposed Treatments	Rating of Related Risk
Define processes and information flows to an appropriate level, enabling a more comprehensive privacy impact assessment to be conducted. (Details of the areas of the detailed design requiring finalisation are provided in Appendix A.)	Severe
Consider increasing the proposed individual's EOI requirements in order to confirm the identity of the individual applying for credentials. Consideration should be given to requiring specific details from a Tax Office generated notice in order to reduce risks of identity theft.	Severe
Actively involve ATO Legal in the design of the SBR Authentication project including reviewing the extent to which the proposed project design complies with legislative and government requirements.	Severe
If required, revise the project design or seek changes to legislation to enable TFN, ABN and Tax Office records to be used for the purposes proposed in the SBR Authentication high level design.	Severe
Restrict access to SBR Authentication subsystems, including databases and interfaces, through the use of access controls.	At least High

[1] In practice, organisations may require that individuals are to use the SBR solution as part of their duties. This would in turn require individuals provide personal information to the Tax Office which may be against their wishes and potentially in breach of their privacy rights. ATO Legal have indicated this has been an issue in a small number of cases in the past.

Proposed Treatments	Rating of Related Risk
Ensure that contracts with third parties contain clauses about protecting the confidentiality of personal information, in line with legal, government and Tax Office requirements.	Significant
Consider the appropriateness and extent of collecting personal information for business taxation purposes.	Moderate
Secure communications (both externally and between SBR Authentication subsystems in disparate environments) through the use of encryption.	Undetermined
Define information handling practices in relation to personal information.	Undetermined
Ensure that policies and procedures define appropriate and acceptable uses of information collected.	Undetermined
Ensure that users are encouraged to view a privacy statement prior to initiating the POI process. ATO Legal should be consulted to ensure that the privacy statement meets legal and government requirements.	Undetermined
Define incident management and response protocols that outline the procedures involved in managing a privacy-related incident such as a breach of confidentiality in relation to personal information	Undetermined
Define policies and procedures for the retention and disposal of personal information to enable achievement of archival, privacy and forensic requirements.	Undetermined

Table 2. Summary of proposed treatments.

Recommendations

It is recommended that:

1. The Tax Office use the results of this draft PIA to incorporate proposed treatment options in its detailed design of the SBR Authentication subsystem, in order to reduce the overall privacy risk of the SBR Authentication solution to an acceptable level.

2. The PIA be finalised once design considerations have determined to enable a comprehensive privacy assessment of the final design. This is currently planned and scheduled for February 2009.

2 SBR Authentication Project

2.1 Project Purpose

The SBR Authentication Project aims to provide a multi-agency authentication solution to support Business-to-Government online interaction. The project is being coordinated by the Tax Office. Other federal agencies are expected to develop future projects to leverage the authentication solution for the purpose of streamlining Business-to-Government reporting by reducing reporting requirements of business.

2.2 Stage of Project Development

The SBR Authentication project is currently at a conceptual stage of development. The high level design and architecture, and use cases in relation to the registration of a credential have been proposed.

2.3 Project Significance

The SBR Authentication Project is a significant element of the SBR Program, which in turn has a significant impact to the Australian business community. As a key enabling technology for the SBR Program, the SBR Authentication project provides a secure, reliable mechanism by which business can identify themselves to government, and vice versa.

2.4 Quantity of Personal Information Handled

The SBR Program will have a significant impact to the Australian business community, with an estimated peak take-up of 60% of the target business population (1.5 million businesses) within four years of implementation. With multiple credentials per business, this represents a large user base (i.e. a large number of SBR credential-holders), and thus, a large volume of personal information that will be collected and used in the process of registering for credentials.

Whilst the amount of a participant's personal information that is collected and maintained by SBR Authentication is limited (refer to Section 2.5), the volume of information collected significantly increases the privacy risks of the project.

Personal user data is collected during the registration process. Details including TFN, name and date of birth are recorded in a data store within the RA subsystem until the registration request has been validated by an administrator. Once credentials have been issued the user's name and email address and the ABN are passed to a data store within the Trust Broker subsystem in the VANguard environment. While it appears that the RA subsystem is intended to hold these details on a temporary basis only, their deletion may impact on fulfilment of legal/forensic traceability requirements.

2.5 Sensitivity of Personal Information

The SBR Authentication solution includes the collection of individuals' information for the purposes of validating their identity, such that they can be issued a credential. Participation in SBR is on a voluntary basis; information is only collected for individuals representing businesses that have selected to participate in SBR. The personal information of SBR participants that will be collected as a part of the online SBR Authentication registration process includes their:

- name;
- date of birth;
- ABN;
- personal Tax File Number;
- email address; and
- phone number.

From the personal information above, elements of higher sensitivity include an individual's name, date of birth and personal Tax File Number. This combination of personal information enables a single individual to be uniquely identified. Further privacy implications are introduced in the instances of suppressed ABNs.

Note: A manual Evidence of Identity (EOI) checking process will be in place when online registration is unable to complete. As the SBR Authentication project is in a stage of high level design, processes relating to the manual EOI check, and the nature and privacy impact of any personal information that will be collected in these processes, are yet to be defined.

2.6 Interaction with Other Agencies

The SBR program must be extensible to support existing Business to Government channels outside of SBR. This includes thin-client applications such as the existing ATO Tax Agent and Business Portals, ECI thick client applications and any other online business services offered by the Tax Office and other government agencies.

Personal information provided by SBR participants is validated against information already retained by the Tax Office. SBR Authentication interfaces with the VANguard system which is maintained and operated by the Department of Innovation, Industry, Science and Research.

2.7 Use of Third Parties (Outsourcers)

The collection and handling of SBR participants' personal information will be performed by Tax Office systems. However, the use of outsourced service providers to manage and support the SBR IT infrastructure would provide indirect access to the personal information that is processed and/or stored on such infrastructure.

2.8 New Technology

The SBR Authentication solution is a new system encompassing people, process and technology, that enables the issuing, management and use of credentials for business clients and intermediaries. The following components, or subsystems, of the SBR Authentication system will handle and/or store personal information:

- *Credential Management subsystem:* Provides self-service functions to the client, including the credential management website. These services are used by the client to request new credentials and to manage credentials for themselves or their business.
- *Registration Authority subsystem*: Provides Registration Authority (RA) functions for credential lifecycle management. This subsystem performs POI checks by calling ATO

Records and ABR Records subsystems, provides functions for manual credential management, and provides information to the VANguard Trust Broker subsystem about credential holders. Clients' personal information is stored on a database in this subsystem.

- *ICP subsystem*: The ICP subsystem is used for SBR Authentication workflow management. *Note: At the time of this assessment, the extent of involvement of the ICP subsystem in the SBR Authentication project was yet to be determined.*
- *ATO Records subsystem*: The ATO Records subsystem is used to check a client's name / date of birth and Tax File Number against Tax Office records, in order to verify the client's individual identity.
- *ABR Records subsystem*: The ABR Records system is used to check a client's authority to represent the business, through checking if the client is listed as a Business Associate on ABR records.
- *Trust Broker subsystem*: The Trust Broker subsystem (within the VANguard solution) receives the name and email address of each SBR client from the Registration Authority subsystem.

2.9 New Collection of Personal Information

Personal information about individuals registering for a credential will be stored in a new database ("SBR") in the Registration Authority subsystem of the SBR Authentication system. The personal information that will persist in this database is as follows:

- name;
- email address; and
- phone number.

In the time that an individual applies for an SBR credential until the request is approved (either through an EOI check, or by a person in the business with Administrator privileges), the following information is stored in this same database:

- name;
- email address;
- date of birth;
- ABN;
- personal Tax File Number; and
- phone number.

2.10 New Use of Personal Information

The proposed method of validating personal information provided by SBR Authentication applicants against existing Tax Office records is new. Such a method of validating an individual's identity does not currently comply with secrecy provisions in the various taxation laws, which states that Tax Office records may only be used for taxation-related purposes. Refer to Section 2.8 for further details. We understand that amendments are currently being considered to ABR legislation to enable the use of TFNs and Tax Office records in the manner proposed by SBR Authentication.

3 Threshold Assessment

3.1 Context

This Threshold Assessment relates to the Standard Business Reporting (SBR) Program. PricewaterhouseCoopers is assisting the Australian Taxation Office with preparation of a Threshold Assessment and Privacy Impact Analysis. The Threshold Assessment serves to provide an understanding of the project and to confirm that a PIA should be performed.

3.2 Project Overview

Standard Business Reporting (SBR)

Current reporting requirements impose a significant burden on business - a burden that the Australian Government is committed to reducing.

SBR is a multi-agency initiative that will simplify business-to-government reporting by:

- making forms easier to understand;
- using accounting/record keeping software to automatically pre-fill government forms; and
- introducing a single secure way to interact on-line with participating agencies.

As a result, businesses and their intermediaries will have a faster, more efficient reporting mechanism. Key benefits to business will include:

- reduced time and effort spent preparing reports for government by businesses, accountants and bookkeepers;
- reduced time and effort spent filing reports for government; and
- reduced time and effort spent dealing with errors.

SBR is expected to save Australian businesses $795 million per year on an ongoing basis, freeing up resources for more profitable activities. In addition, accountants, bookkeepers, tax professionals and software developers will have access to a powerful system for improving service delivery and productivity.

SBR Authentication

The SBR Authentication project aims to provide a multi-agency authentication solution to support the SBR program. This means that it must be extensible to support existing Business to Government channels outside of SBR. This includes thin-client applications such as the existing ATO Tax Agent and Business Portals, ECI thick client applications and any other online business services offered by government agencies.

The SBR Authentication scope covers all of the interactions and components that are involved in issuing, managing and using credentials for Business clients and intermediaries to deal electronically with the Australian Government. This includes client self-management services, Registration Authority (RA), Certification Authority (CA) and client-side software components and services.

The SBR Authentication scope does not include components that are related to authorisation, including delegated authorisation (where an intermediary such as a Tax Agent is authorised to act on behalf of another business).

The SBR Authentication solution interfaces to a number of external components that use the credential. These external components include Trust Broker components. These interactions are considered external to the SBR Authentication solution.

3.3 Use of Personal Information

The proposed project involves the collection, use and disclosure of personal information

The proposed SBR Authentication project involves the collection and use of personal information from a large number of individuals representing businesses Australia-wide. A summary of the personal information that is collected, used and disclosed in the SBR Authentication project is outlined in the table below:

Process	Elements of personal information collected, used or disclosed	Purpose for collection, use or disclosure	Authority to collect Personal information privacy risks*
Registration			
Applicant registration (via online registration page) – administrator credentials	• Name; • email address; • date of birth; • personal Tax File Number (TFN); and • phone number.	Information is collected in order to perform an Evidence of Identity (EOI) check on the applicant, for the issuing of a credential. The EOI check involves validation of the applicant's name, date of birth and TFN against existing records retained by the Tax Office. The applicant's email address and phone number is collected for the purposes of enabling correspondence with the applicant.	As per the *Taxation Administration Act 1953* and the *Tax File Number Guidelines* (as issued under s.17 of the *Privacy Act 1988*), the use of an individual's Tax File Number is restricted to purposes authorised by taxation, assistance agency or superannuation law. Under current taxation law, there are no provisions for the use of the Tax File Number as a means of identifying individuals for non-taxation purposes.
Applicant registration (via online registration page) – non-administrator credentials	• Name; • email address; and • phone number.	Information is collected for the purposes of enabling correspondence with the applicant.	Individuals choose to provide this information as part of the registration process. It is not mandatory to use the SBR solution so registration is voluntary.
Applicant registration (via manual process) – administrator credentials	Subject to further project design.	Information is collected in order to perform an Evidence of Identity (EOI) check on applicants that: • do not provide their TFN; • fail the automated EOI check on the SBR online registration page through: o not being listed as a Business Associate on the ABR; o a name, date of birth and TFN mismatch; or o the applicant not having a TFN. The information that will be used in order to perform the EOI check is yet to be determined.	This is still subject to ATO consideration at the time of this draft report. Dependent on the information to be collected – subject to further project design. It is not mandatory to use the SBR solution so registration is voluntary.

Process	Elements of personal information collected, used or disclosed	Purpose for collection, use or disclosure	Authority to collect Personal information privacy risks*
Maintain			
User contacts the system operator via telephone	Subject to further project design	Information is collected in order for the system operator to establish the identity of the user, and their authority.	Dependent on the information to be collected – subject to further project design. Expected to be consistent with existing Tax Office call centre POI processes.
Use			
User information is transmitted to the Trust Broker subsystem (VANguard) for storage	• Name; • ABN; • email address • Administrator status flag	Personal information is stored in the SBR User Data Store (in the Trust Broker subsystem) due to the SBR credential not containing all of the information about a user that may be required by an agency.	This is still subject to consideration at the time of this draft report.

** A formal Threat and Risk Assessment (TRA) over the SBR Authentication project is being conducted separately. This privacy risk column represents a selection of key risks identified during the Threshold Assessment process that led to the recommendation that a Privacy Impact Assessment (PIA) be conducted. These risks are set out in Section 3.4, below.*

Table 3. Summary of information collected, and the risks associated thereof

3.4 Privacy Risks

The selection of key risks identified through the Threshold Assessment process that led to the recommendation that a Privacy Impact Assessment (PIA) be conducted are presented in the table below:

Ref	Specific privacy-related risks	Assessment of Current Risk Exposure to the SBR Project	Key Assessment Considerations
R1	Personal information is disclosed during transmission, storage and/or disposal.	Design insufficient to enable assessment	• Proposed use of encryption in transmissions between the end user and the credential management subsystem • Other key components of the SBR Authentication design are yet to be defined. Refer to Appendix A for a list of areas requiring finalisation.
R2	Personal information is used for purposes not initially permitted by the individuals.	Design insufficient to enable assessment	• Key components of the SBR Authentication design are yet to be defined, including the exact purpose of collection. Refer to Appendix A for a list of areas requiring finalisation.
R3	Public confidence is reduced by poor handling of privacy incidents.	Design insufficient to enable assessment	• Key components of the SBR Authentication design are yet to be defined. Refer to Appendix A for a list of areas requiring finalisation.
R4	Information is collected without adequate disclosure of its collection or intended purpose.	Design insufficient to enable assessment	• Key components of the SBR Authentication design are yet to be defined. Refer to Appendix A for a list of areas requiring finalisation.

Ref	Specific privacy-related risks	Assessment of Current Risk Exposure to the SBR Project	Key Assessment Considerations
R5	The large-scale storage of personal information increases the likelihood and impact of unauthorised disclosure or usage for other purposes.	High	• Information submitted by users to perform an EOI check is stored on the RA until such time that the request is approved by an Administrator
R6	The EOI process for individuals not wishing to provide their TFN may require the collection and usage of extensive personal information in order to provide an alternative means of identity validation.	Design insufficient to enable assessment	• Key components of the SBR Authentication design are yet to be defined. Refer to Appendix A for a list of areas requiring finalisation.
R7	EOI process is insufficient to reliably establish that the person obtaining a credential is the individual to whom the EOI data relates	Severe	• Proposed information set required to provide identity is known to a broad range of individuals and does not bind an identity to a physical person with a reasonable confidence level • EOI for SBR Authentication is less stringent than current POI requirements for other Tax Office channels
R8	Unauthorised persons may access or modify an individual's data due to insufficient criteria used to validate an individual's identity.	Low	• Access requires two-factor authentication (certificate and password) • Without the password, a new POI must be performed • No user-modifiable personal information other than email address
R9	The amount of private information collected may be excessive given its collection is for business purposes.	Moderate	• Personal information collected as part of EOI is minimal (name, date of birth, TFN, ABN) • TFN and DOB are considered sensitive • The use of individual information as a means of validating one's identity for business-related transactions may be considered an unreasonable intrusion, however this is a voluntary opt-in system
R10	Excessive retention of private information.	Moderate (Design insufficient to enable assessment)	• The process for retaining and disposing of information has not been defined
R11	Project may not comply with all legislative and government requirements and social norms.	Severe	• The proposed SBR Authentication design appears to contravene current taxation laws which stipulate that TFNs and Tax Office records may only be used for taxation-related matters. We understand legislation revisions are being considered to address this. • ABNs may be linked to personal data and may only be used in accordance with legislative requirements • ATO Legal have not been extensively involved in the design of the SBR Authentication project
R12	Privacy incidents may occur due to the use of third parties such as those who manage IT infrastructure components.	Significant	• Proposed use of third parties in the development and support of the SBR Authentication IT infrastructure • Current third parties support existing Tax Office IT infrastructure, which contains sensitive personal information • IT support is subject to contract arrangements.

Table 4. Specific privacy-related risks in relation to the high-level design of the SBR Authentication project.

Privacy related risks cannot be fully assessed or mitigated because processes and information flows are yet to be defined at a detailed level. These areas of design could potentially have a severe impact on the SBR project.

3.5 Further discussion regarding proposed EOI standards

In order for the SBR Authentication Solution to be relied upon by agencies, the solution must provide comfort that firstly the physical person is appropriately bound to the credential holder's name, and secondly that the credential holder's name is appropriately bound to the organisation that they purport to represent.

The proposed standard to make this first binding differs from existing identity strategies and guidelines applicable to Federal Government organisations. The 2004 Standing Committee of Attorneys-General endorsed agencies' use of an Evidence of Identity (EOI) framework that requires validation of identity documents to confirm the identity has: commenced within Australia; is active in the community; and is linked to the applicant. This framework forms a part of the National Identity Security Strategy, which the Tax Office has endorsed as part of its 2008-09 compliance program. The Gatekeeper framework provides for differing types of EOI checks, but all must provide reasonable confidence that the physical person and the credential holder's name relate to the same identity.

The set of persons holding data sufficient to provide EOI under the proposed standard include current and past employers, financial institutions, superannuation funds, share registries, other government organisations delivering services to individuals, the individual, their family members and the individual's tax agent. The number of potential threat sources that could provide sufficient evidence of identity increases the likelihood of users being inappropriately registered for an Administrator level credential by other persons, without the knowledge of the legitimate individual.

To increase the likelihood that the applicant is who they claim to be, consideration should be given to reducing the number of threat sources by using additional EOI information. However, any requirement for additional information should be kept to a minimum so as to maintain usability. For example, information contained within a Tax Office-issued Notice is likely to only be known to a subset of the parties named in the preceding paragraph. Providing such additional information is currently required in order to access a range of other Tax Office services, such as those in Table 4 below.

Whilst stringent penalties currently exist in relation to the misuse of an individual's TFN, it is also germane to consider the impact on usability if a TFN had been subject to identity theft or fraud. In the case that the Tax Office detected that a TFN had been illegally used, then the TFN must be cancelled/revoked, and all related accounts and registration details are frozen to ensure no updates can be made. Where the TFN is related to an ABN, the ABN itself must also be cancelled as is any credential that is connected with it. This would not only have serious impact on the business concerned but also damage the reputation of the credential issuing authority and SBR agencies. For this reason the integrity of the identity verification process at registration must be sound.

Given that SBR functionality is likely to evolve, it would be prudent to adopt a sufficiently robust registration to ensure that future services are supported. As with any risk, management may determine that the residual exposure is sufficiently low to warrant acceptance.
However, requiring one additional item of EOI present on a Tax Office-issued Notice is believed to have a minor impact on the individuals concerned, but would bring a significant benefit in reducing the likelihood of Administrator identity theft in the SBR environment.

Situation	POI Required
Individuals calling to inquire about their tax affairs	• TFN OR (Name, date of birth, full address, postcode, other personal details until operator is satisfied) AND • Details from a Tax Office generated notice.
Organisations wanting to change details about themselves	• Address details • Financial institution account number • Details from a Tax Office generated notice OR details of amounts recorded on BAS statements or details of payments made to the Tax Office
Tax Agents wanting to access client details	• Tax Agent Number (TAN) AND • One of (client TFN, client ABN, client name, client's excise account number) AND • Provide POI for the client account with personal details of the client (name, DOB, bank details, reference data from a Tax Office generated notice).
Transferring superannuation balances between funds	One of (Passport, Drivers licence) OR One of (birth certificate, citizenship certificate, pension card) AND one of (Notice issued by Centrelink, Notice issued by federal govt or local council evidencing address within Australia)

Table 5. POI required in order to access selected Tax Office services

3.6 Conclusion

Although the project is still being designed, given the sensitivity and volume of the personal information being collected and stored, it was confirmed that a Privacy Impact Assessment should be conducted in order to assist with appropriately identifying, mitigating and managing privacy risks.

Note that some privacy risks identified during the Threshold Assessment process, such as risks relating to compliance with current legislation and the appropriateness of EOI processes, are significant and could have major impacts on the viability of the SBR project.

4 Information Flows

The table below outlines the information flows apparent in the high level design of the SBR Authentication project.

Ref	From	To	Information transmitted	Data security arrangements
Registration				
1(a)	Client subsystem (SDK, Browser Enabler or Mobile Access component)	Credential Management (Credential Management Security Proxy component)	Applicants requesting administrator credentials (including Business Associates, nominated first credential holders and nominated credential holder with administrator privileges) provide the following personal information for the purposes of completing an EOI check: • name; • email address; • date of birth; • ABN; • personal Tax File Number; and • phone number.	Encrypted Web session (HTTPS)
1(b)	Client subsystem (SDK, Browser Enabler or Mobile Access component)	Credential Management (Credential Management Security Proxy component)	Applicants requesting non-administrator credentials (including nominated credential holders without administrator privileges and custodians) provide the following personal information for the purposes of registering for a credential: • name; • email address.	Encrypted Web session (HTTPS)
2	Credential Management (Credential Management Reliable Messaging component)	Registration Authority (RA Request Validator component)	The following personal information pertaining to a request: • name; • email address; • date of birth (where applicable); • ABN (where applicable); • personal Tax File Number (where applicable); and • phone number (where applicable).	Reliable messaging (TBD)
3	Registration Authority (RA Registrations Support component)	ATO Records (EAI Integration component)	The following personal information pertaining to a request: • name; • date of birth; and • personal Tax File Number. Personal information is sent one way only, with confirmation of accuracy excluding personal details.	Subject to further project design.
4	Registration Authority (RA Registrations Support component)	ABR Records	The following personal information pertaining to a request: • name; and • ABN. Personal information is sent one way only, with confirmation of accuracy excluding personal details.	Subject to further project design.
5	Registration Authority (RA Registrations Support	ICP	Subject to further project design	Subject to further project design

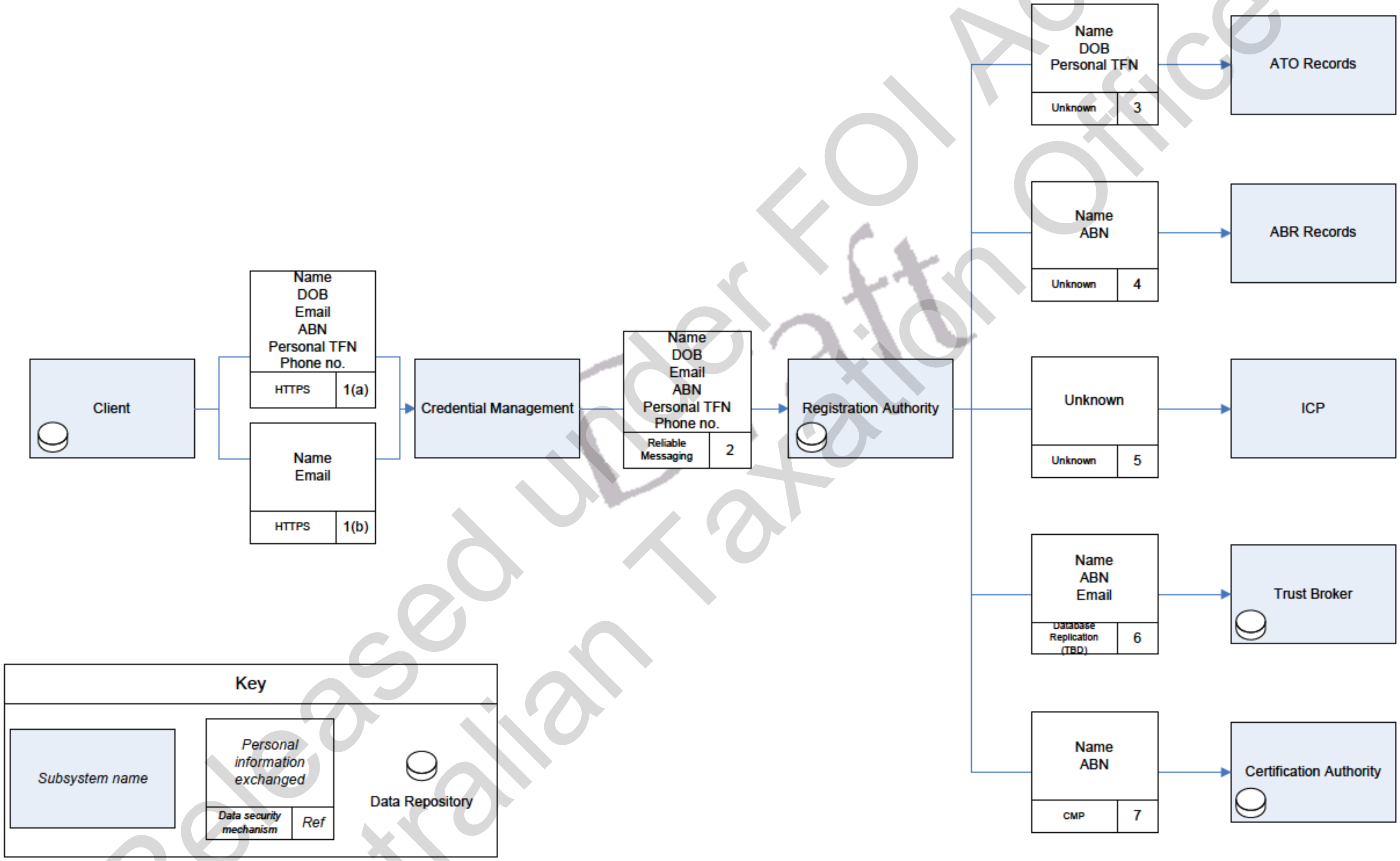
Ref	From	To	Information transmitted	Data security arrangements
	component)			
6	Registration Authority (RA Data Store component)	Trust Broker (VANguard SBR User Data Store component)	The following personal information pertaining to each SBR user: • name; • ABN; and • email address.	Database replication (TBD)
7	Registration Authority (RA reliable messaging component)	Certification Authority	The following personal information pertaining to an approved request for a credential: • name; and • ABN.	Non-repudiation is achieved through signing of the CMP message by the RA Request Handler.
Maintain				
8	SBR credential-holder (verbally, via telephone)	SBR system operator	Subject to further project design	Subject to further project design

Table 6. SBR Authentication – information flows

Note that Use Cases relating to maintaining and actual use of the credential are currently undefined (refer Appendix A for details) and will be examined as part of the PIA scheduled for February 2009.

The information flows in the table above are represented in the diagram below:

Personal Information Flow – Registration



Client

Name
DOB
Email
ABN
Personal TFN
Phone no.
HTTPS 1(a)

Name
Email
HTTPS 1(b)

Credential Management

Name
DOB
Email
ABN
Personal TFN
Phone no.
Reliable Messaging 2

Registration Authority

Name
DOB
Personal TFN
Unknown 3

ATO Records

Name
ABN
Unknown 4

ABR Records

Unknown
Unknown 5

ICP

Name
ABN
Email
Database Replication (TBD) 6

Trust Broker

Name
ABN
CMP 7

Certification Authority

Key

Subsystem name

Personal information exchanged
Data security mechanism *Ref*

Data Repository

5 Treatment and Controls

The following risk treatment options are focused on reducing the risks identified in Table 4. Note that in some instances a proposed treatment may be an effective mitigation strategy for more than one risk, and while some mitigation strategies may assist in reducing the risk exposure they may be insufficient on their own to reduce residual risk to an acceptable level.

Consideration should be given to the implementation of the risk treatment options during the detailed design phase of the SBR Authentication project.

Ref	Proposed Treatments	Mitigates Threats	Rating of Related Risk
PT1	Secure communications (both externally and between SBR Authentication subsystems in disparate environments) through the use of encryption.	R1	Undetermined
PT2	Define information handling practices in relation to personal information.	R1	Undetermined
PT3	Restrict access to SBR Authentication subsystems, including databases and interfaces, through the use of access controls.	R1, R5	At least High
PT4	Ensure that policies and procedures define appropriate and acceptable uses of information collected.	R2	Undetermined
PT5	Ensure that users are encouraged to view a privacy statement prior to initiating the POI process. ATO Legal should be consulted to ensure that the privacy statement meets legal and government requirements.	R2, R4, R6	Undetermined
PT6	Define incident management and response protocols that outline the procedures involved in managing a privacy-related incident such as a breach of confidentiality in relation to personal information	R3	Undetermined
PT7	Ensure that contracts with third parties contain clauses about protecting the confidentiality of personal information, in line with legal, government and Tax Office requirements.	R12	Significant
PT8	Define processes and information flows to an appropriate level, enabling a more comprehensive privacy impact assessment to be conducted. (Details of the areas of the detailed design requiring finalisation are provided in Appendix A)	R1, R2, R3, R4, R6, R10	Undetermined
PT9	Increase the proposed requirements in order to establish the identity of an individual. Consideration should be given to requiring specific details from a Tax Office generated notice in order to reduce risks of identity theft.	R7	Severe
PT10	Define policies and procedures for the retention and disposal of personal information to enable achievement of archival, privacy and forensic requirements.	R10	Undetermined
PT11	Actively involve ATO Legal in the design of the SBR Authentication project including reviewing the extent to which the proposed project design complies with legislative and government requirements.	R11	Severe
PT12	If required, revise the project design or seek changes to legislation to enable TFN, ABN and Tax Office records to be used for the purposes proposed in the SBR Authentication high level design.	R11	Severe
PT13	Consider the appropriateness and extent of collecting personal information for business taxation purposes.	R9	Moderate

Table 7. Proposed Treatments

6 Appendix A Areas Requiring Finalisation

As the SBR Authentication project is at a stage of high level design, not all processes have been defined. In particular, the areas below require finalisation in order for a more comprehensive PIA to be conducted.

Use cases

- UC802 – TFN EOI check fails [Manual EOI processing]
- UC803 – ABR check fails [Manual EOI processing]

The business processes relating to the following use case scenarios have not yet been formally documented:

- Download credential to portable device
- User authenticates with credential through browser
- User authenticates with credential through business software
- Administrator requests cancellation of device credential
- Administrator accesses Credential Manager to change details
- User accesses Credential Manager to change details
- Organisation no longer has registered administrator
- Failed activation codes.

Interfaces

Further detail (such as the information being transferred across the interface, the security requirements of the interface, the protocols used, and the mechanisms used to secure the interface) is required in the description of the following interfaces in the SBR Authentication subsystem:

- Interface between the Credential Management and RA subsystems
- Interface between the RA and ICP subsystems
- Interface between the RA and ATO Records subsystems
- Interface between the RA and ABR Records subsystems
- Interface between the RA and Trust Broker subsystems

Other

- An end-to-end process for managing suppressed ABNs should be defined. This process should outline the registration, maintenance and use of an SBR credential for individuals representing an organisation with a suppressed ABN.
- The interaction between the ICP system and the SBR Authentication system should be determined.
- The user consent disclaimer statement should be defined, including to explain the purpose for personal data collection and to address other privacy and legal considerations.
- The manual processes for EOI should be defined (if any), including the processes to be used when a user declines to provide a TFN or when automated EOI verification fails.
- Incident response procedures should be defined to mitigate the impact of a privacy breach.
- The process for retaining and disposing of personal information should be defined.

7 Appendix B Documents Reviewed

In preparation of this PIA, the following documents were reviewed:

- SBR HLD-02 v0.8 Working Draft – SBR Authentication Design Blueprint
- SBR HLD004 Use Cases v0.2 Draft – SBR Authentication Project Use Cases and Use Case Diagrams High Level Design
- SBR HLD006 System Architecture v0.2 Draft – SBR Authentication Project High Level Design
- AUTH UC001 v0.3 Draft – Business Associate Applies for own credential as part of ABN application
- AUTH UC002 v0.3 Draft – Business Associate from existing Business applies for their own credential
- AUTH UC003 v0.3 Draft – Business Associate Nominates another user as the first credential holder
- AUTH UC004 v0.3 Draft – User initiates registration for own credential
- AUTH UC005 v0.3 Draft – Administrator initiates registration of User credential without administration privileges
- AUTH UC006 v0.4 Draft – Administrator initiates registration of user credential with administration privileges
- AUTH UC007 v0.3 Draft – Administrator initiates registration for Device credential
- AUTH UC008 v0.3 Draft – Administrator initiates bulk registration of User credentials without administration privileges
- AUTH UC009 Draft – Administrator assigns Administrator privileges to a User
- AUTH UC010 v0.3 Draft – Administrator removes Administrator privileges from a User
- AUTH UC201 v0.3 Draft – Renew credential
- AUTH UC401 v0.3 Draft – Request Credential cancellation through the Credential Manager
- AUTH UC402 v0.3 Draft – Request Credential cancellation outside Credential Manager
- AUTH UC403 v0.3 Draft – Custodial requests revocation of device credential