PRIVACY IMPACT ASSESSMENTS

FOR

IGOVT PROGRAMME

For: The Department of Internal Affairs (NZ)

COMMERCIAL IN CONFIDENCE

8 DECEMBER 2010

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

1.1 BACKGROUND

The Department of Internal Affairs (DIA) asked Information Integrity Solutions to conduct a Privacy Impact Assessment (PIA) on some upgrades and functional improvements to the igovt Logon Service solution which is part of the igovt Build Programme.

The igovt Build Programme is a critical part of the New Zealand Government's move towards e-government and enabling citizens to more widely interact with government online.

This PIA focuses on igovt Logon Service release 9. This release is to implement non-functional technology upgrades and functional improvements to the igovt Logon Service solution. These are:

- Security Token Service;
- Help Desk Web Service; and
- Self Service Forgotten Username.

The purpose of the PIA is to identify any potential privacy impacts arising from the proposed functionalities. The PIA is to be a comprehensive report that includes the evaluation of the privacy risks and the associated implications of those risks along with mitigation strategies.

1.2 PROCESS

In conducting the PIA IIS:

- Consulted with DIA and finalised the work plan;
- Gathered information including reading High Level Requirement Specification documents and conducting phone conferences with relevant DIA staff;
- Analysed the information including developing a map of information flows where useful and identified any privacy risks;
- Prepared a draft report which DIA reviewed;
- Revised and finalised the report.

1.3 FINDINGS

IIS considers that on the information it has to hand so far DIA has taken significant steps to address the possible privacy risks associated with the updates proposed through igovt Release 9. IIS has not identified any major concerns in relation to the information supplied so far in the design or process. It has identified some ways in which the implementation could be improved and has made recommendations about this.

IIS has identified some longer terms risks which will need further consideration in the context of further phases of implementation of the STS exchange of information enhancement and to the igovt programme as a whole.

1.4 RECOMMENDATIONS

Recommendation 1: Governance and accountability – Audit of Service Agency Help Desk Web Service applications

IIS recommends that DIA audits the help desk applications of agencies using the igovt Help Desk Web Service to ensure that the applications comply with DIA policies about what information should not be recorded from a Service User support session. In particular the audit should check to ensure that Service Agency help desk applications do not record an individual's igovt account username or registered email address. IIS suggests an audit cycle of no longer than every two years.

Recommendation 2: Governance and transparency – Informing Service Users

DIA should engage experts in plain language and online useability to ensure that Service Users are easily able to access and understand important information about how the upgrades to the STS will work including how source and target agencies will collect, use and disclose information about Service Users. The information that Service Users need to know most should be prioritised and made most accessible.

DIA should develop a strategy for publicising changes to the privacy policies and corresponding changes to privacy notices as they occur over time.

Recommendation 3: Governance and accountability – Conditions imposed on agencies using Help Desk Web Service

IIS recommends that DIA makes it a condition of service agencies gaining access to the Help Desk Web Service that they have appropriate procedures for vetting staff that will have access to igovt details. The condition should include that the Service Agency regularly audits staff access to ensure that it appears appropriate and related to a particular caller request.

Recommendation 4: Business as Usual – Education about shared registered email addresses

IIS recommends that igovt Service Users are warned about the consequences of using a registered email address that is shared with other people. This could be done at the time that Service Users register for an igovt account, when they change their registered email address and when they use Self Service Forgotten Username.

Recommendation 5: Business as usual and accountability for deletion of help desk information when no longer needed

IIS recommends that it be a condition of using the Help Desk Web Service that the Agency conducts an assessment of the kinds of information it stores as a result of a help desk session with a Service User. The Agency should identify whether there are good reasons, such as statistical or accountability reasons, for keeping that information and, if so, document for how long it will be needed. The Service Agency should ensure it has regular processes by which it deletes such information from its records when it is not needed or no longer needed. The process should be governed by a memorandum of understanding between igovt and the Agency which could include a requirement to report to igovt about the information it keeps relating to help desk sessions and the Agency's destruction schedule for such information.

DIA should explore the use by agencies of developing technology that enables efficient and cost effective deletion of data by building retention and deletion policy into data at the time it is generated.

Recommendation 6: Business as usual – Expanding the range of exchange of information
IIS Recommends that DIA conducts a PIA at the point at which it proposes to extend the ability to exchange information about a Service User electronically beyond one source Agency and one target Agency or to enable an Agency to seek an FLT source outside the context of a current logon event through which an individual has given the source Agency direct consent.

Recommendation 7: Governance of igovt and the electronic exchange of information
IIS recommends that DIA should put in train steps to review what might be an appropriate governance mechanism to ensure that as the STS develops and the choice to interact offline diminishes, other governance and accountability mechanisms are introduced to compensate for the diminishing power of consent. At the latest, the first review should commence 3 years from now.

Recommendation 8: Governance – Managing failure and mistakes when information is exchanged between agencies
IIS recommends that DIA ensure that it has in place a coordinated and responsive customer support system to handle mistakes or failures in the electronic exchange of information between agencies, even where the STS is not directly involved.

Recommendation 9: Safety mechanisms – Fair allocation of risk
DIA should review the terms and conditions for Service Users in relation to the STS, Help Desk Web Service and Self Service Forgotten Username to ensure that the burden born by Service Users when they fail or problems arise is not unfair. Questions that could be asked to help determine fairness include:

- Is DIA excluding itself or agencies from liability in areas it has main responsibility for and over which the Service User has little or no control?
- Do the provisions mean that Service Users could be substantially out of pocket, or their lives substantially disrupted through no fault of their own?
- Will Service Users be required to exercise a level of care that is unrealistic or beyond the average person's knowledge or competence?
- Do the provisions accurately reflect the allocation of responsibility that DIA would be likely to have if a Service User took legal action, or complained to the Privacy Commissioner?
- Are the terms and conditions buried in fine type and framed in language that a Service User is unlikely to find, read or understand?
- Have we identified the problems that individuals most frequently face and assessed and addressed any unfair allocations of risk?

2 INTRODUCTION

2.1 BACKGROUND TO PIA

The Department of Internal Affairs (DIA) has asked Information Integrity Solutions to conduct a Privacy Impact Assessment (PIA) on some upgrades and functional improvements to the igovt Logon Service solution which is part of the igovt Build Programme.

The igovt Build Programme is a critical part of the New Zealand Government's move towards e-government and enabling citizens to more widely interact with government online.

These initiatives can lead to much greater efficiency, effectiveness and convenience. However, leading edge, but practical, thinking must accompany them to ensure that citizens do not see them as inappropriate 'digital God' monitoring and sharing of citizen information by government.

The New Zealand government has taken this issue seriously including through adopting a strongly citizen centred approach and through conducting PIAs at important stages of its igovt Programme.

2.2 PRINCIPLES UNDERPINNING ONLINE AUTHENTICATION

The igovt programme is underpinned by Cabinet approved policy and implementation principles for government to person (G2P) online authentication.[1] The Policy Principles are:

- Security - Suitable protection must be provided for information owned by both people and the Crown;
- Acceptability - Ensuring that the proposed authentication approach is generally acceptable to potential Service Users, taking into account the different needs of people and emerging industry standards, and avoids creating barriers;
- Protection of privacy - Ensuring that the proposed authentication approach protects privacy appropriately;
- All-of-government approach - Balancing public and agencies' concerns about their independence with the benefits of standardisation while delivering a cost-effective solution;
- Fit for purpose - Avoiding over-engineering, recognising that the levels of authentication required for many G2P transactions will be relatively low;
- Opt-in - Ensuring that members of the public retain the option of authenticating their identity and carrying out transactions offline and are not disadvantaged by doing so. However, it will not be possible for an individual to conduct secure online G2P transactions without the use of the appropriate authentication process.

[1] http://www.e.govt.nz/services/authentication/policywork/authprin

Implementation principles include:

- Service User focus - Ensuring the recommended solutions are as convenient, easy to use and non-intrusive as possible;
- Enduring solution - Providing a solution that is enduring yet sufficiently flexible to accommodate change and a wide range of current and future transactions;
- Affordability and reliability - Ensuring the recommended solutions are affordable and reliable for the public and government agencies;
- Technology neutrality - Ensuring a range of technology options is considered, and as far as possible avoiding "vendor capture";
- Risk-based approach - Providing an approach based on agreed trust levels that protects identity and personal information;
- Legal compliance - The solution must comply with relevant law, including privacy and human rights law;
- Legal certainty - Relationships between the parties should be governed in a way that provides legal certainty;
- Non-repudiation - The issue of non-repudiation must be considered for those transactions that require it, so that the risk of transacting parties later denying having participated in a transaction is minimised;
- Functional equivalence - Authentication requirements should be similar to those that apply to existing transactions except where the online nature of the transaction significantly changes the level of risk.

These principles demonstrate a strong government commitment to a Service User-centric and privacy focussed approach. This is reflected in the way that DIA has gone about designing the Release 9 updates to the igovt Logon Service.

2.3 PURPOSE AND SCOPE PIA

This PIA focuses on igovt Logon Service release 9. This release is to implement non-functional technology upgrades and functional improvements to the igovt Logon Service solution. These are:

- Security Token Service;
- Help Desk Web Service; and
- Self Service Forgotten username.

The purpose of the PIA is to identify any potential privacy impacts arising from the proposed functionalities. The PIA is to be a comprehensive report that includes the evaluation of the privacy risks and the associated implications of those risks along with mitigation strategies.

2.4 IIS APPROACH TO THE PIA

IIS took a consultative and practical approach to conducting the PIA. It consulted with the relevant staff of DIA. It bases its approach on the New Zealand Privacy Commissioner's Privacy Impact Assessment Handbook, and also draws on best practice identified elsewhere in current Australian and International approaches.

The IIS approach goes beyond mere compliance with privacy law; it looks to wider privacy challenges including allocation of risks and individual trust and looks for solutions so that information flows are appropriate and to everyone's benefit.

In conducting the PIA IIS drew on its "layered defence" approach. This applies a number of possible "tools" to arrive at practical solutions that fit the particular circumstances. The layers and examples of possible tools include:

- "Business as usual" good practice, including education, process and culture change regarding the expectations about the way things are done by staff, and the actions that Service Users need to take to protect themselves;
- Additional law where risks are particularly high, for example, specific use and disclosure limitations, criminal penalties and special measures to ensure review before critical changes are made in addition to compliance with law currently in statutes;
- Technology, including design limits on information collected, what can be connected and who can see what;
- Governance, including transparency and accountability;
- Safety mechanisms, including easily accessible and responsive complaints mechanisms for Service Users when failure or mistakes occur.

IIS uses combinations of these strategies to achieve the desired level of trust and privacy protection while also achieving project goals. For example, where individuals have a reduced level of personal control, the appropriate level of trust and protection may be achieved thought such measures as increased emphasis on accountability, risk allocation and safety net mechanisms.

IIS considers that in outlining its analysis in the PIA is it not necessary or efficient to focus in detail on every possible privacy risk: rather, it is better to focus on the most critical issues, particularly those that have not been resolved.

2.5 ASSUMPTIONS APPLIED TO THE PIA

IIS applied the following assumptions to the PIA.

- That the reader is familiar with the igovt Logon Service and the igovt programme;
- That there will be further PIAs conducted on the igovt Logon Service, for example, when DIA proposes to extend the ability to exchange information about a Service User electronically beyond one source Agency and one target Agency or where DIA proposes to allow FLT token translation without Service User authentication;

- That IIS has most of the required information that is most critical to its analysis.

2.6 METHODOLOGY

IIS took the following steps for its PIA on the igovt Logon Service Release 9.

2.6.1 CONSULTED WITH DIA AND FINALISED WORK PLAN

IIS discussed with the relevant people in DIA the project approach and then finalised a project plan to deliver the work.

2.6.2 GATHERED INFORMATION

In this phase, IIS gathered information about igovt Logon Service release 9 including the following High Level Requirements Specification documents.

1. Security token service web service: 7 September 2010 – Version 1.0;
2. Help desk web service: 18 October 2010 – Version 0.9;
3. Self-service forgotten username: 11 October 2010 – Version 0.2;

IIS also had phone conferences with relevant DIA staff.

2.6.3 CONDUCTED ANALYSIS

IIS developed a description and map of information flows and identified privacy risks taking into account the Information Privacy Principles (IPPs) and other privacy risks that could arise that go beyond mere compliance with the law.

2.6.4 PREPARED DRAFT REPORT AND DIA REVIEW

Once analysis was completed, IIS prepared a draft report which included draft recommendations. IIS provided the draft to DIA for comment.

2.6.5 WROTE FINAL REPORT

IIS then wrote the final report taking into account feedback from the DIA.

3 GLOSSARY

Term	Description
Authentication token	This is the result of a User logon. It contains the User's FLT for the domain for which they have authenticated, the strength of the authentication performed, constraints of the scope of the authentication and security features. The authentication token is formatted as a SAML v2 assertion.
FLT	Federated Logon Tag A persistent pseudonym for a logon (noun) that is valid only within a specific Agency context.
FLTsource	The FLT for a logon (noun) within the context of the Agency initiating an authenticated web service transaction.

FLTtarget	The FLT for a logon (noun) within the context of the Agency that is the destination of an authenticated web service transaction.
igovt Logon Service	An all of government shared service to manage the logon process for online services of participating agencies.
STS	Security Token Service The Security Token Service is a web service that is a component of the igovt Logon Service. It issues security tokens. It exchanges authenticated tokens for one Agency context for tokens for a different context.
igovt Help Desk	This Centre, run by DIA contractor Datacom provides support for logon queries/requests using a help desk web application.
igovt Help Desk Operator	This igovt role provides an Agency user with rights to access the igovt help desk functions at the igovt Help Desk (Datacom).
igovt Help Desk web application	The igovt Help Desk web application provides help desk operators with browser based access to the system functionality required to provide Level 1 support to igovt Logon Service Users. Centralised support is offered by the igovt Help Desk Centre run by DIA contractor Datacom. A number of Service Agencies have opted to use the igovt Help Desk web application to access the subset of support functions required to provide assistance to the Logon Service Users of their Agency applications.
Initiating Agency	The Service Agency where the online Service User has asked for a service that initiates the business process that will involve one or more agencies.
Logon	(noun) The combination of a username (logon identifier component) with one or more authentication keys (the authentication component) that is authenticated by the Logon Service when presented by the Service User. (verb) The action a Service User performs to supply their authentication credentials.
Opaque token	An opaque token is an authentication token that has been encrypted by the igovt STS to obscure the User's FLT and to make the token safe to share. The token is encrypted in such a way as to prevent any party other than the igovt STS from decrypting the token.
SAML	Security Assertion Markup Language - is an XML-based standard that defines messages for communicating a range of security related statements about individual parties, including their authentication.
Service Agency	A participating Agency providing an online service that uses the Logon Service to authenticate Service Users.

Source Agency	The Agency (SAML Service Provider) which provides the Service User's FLT or authentication response in order to identify the individual involved in the cross Agency service delivery activity at another Service Agency.
SSL	Secure Socket Layer: A protocol for transmitting sensitive information across the Internet in a secure way. The later TLS standard may also be used instead of SSL.
Target Agency	The Service Agency's web service which receives an opaque token from another Service Agency in order to identify the individual involved in the provision of the cross- Agency service delivery activity.
Service User	This entity represents any individual entity that needs to make a service request at a service provider.

4 DESCRIPTION OF THE RELEASE 9 IGOVT UPGRADES

4.1 SECURITY TOKEN SERVICE

The Security Token Service (STS) is a Web service that is a component of the igovt Logon service. The igovt Logon Service allows a person to use the same logon to access various government online services. Individuals using the service do not have to remember multiple logon details for different services. However, to prevent government agencies from being able to gain a picture of an individual's interactions across government the igovt Logon Service uses pseudonymous identifiers. The service delivers a persistent identifier called a federated logon tag (FLT) to a Service Agency when a Service User logs on seeking to access that service. The FLT is unique to that Service User and Service Agency and contains no identity information. The Service Agency then links the FLT to User's account and any information they have for the Service User.

In Release 9 of the igovt Logon Service the STS component is being created to enable agencies to exchange information about a Service User (with their permission) without agencies having to share an identifier. The knowledge of the individual's Agency FLT remains within the Service Agency for which it was issued.

An example of where an Agency may seek to share information in the online environment could be where an individual is seeking information from the Department of Inland Revenue (IRD) about his or her student loan repayments. To do this, IRD will need information from the Ministry of Social Development that administers student loans (MSD). The STS will enable this to happen online in real time. The process it uses, based on this hypothetical example, will be the following:

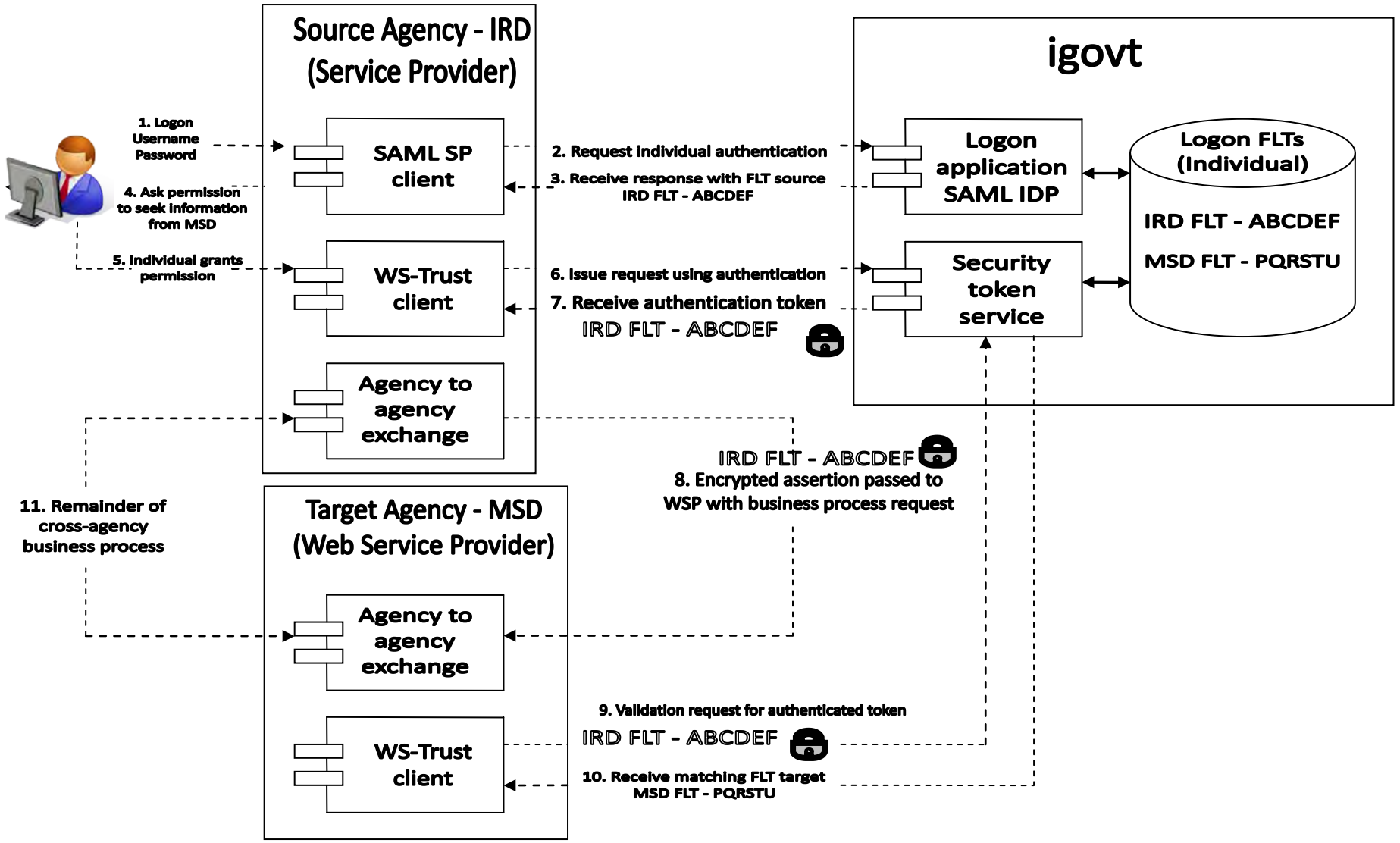
- The individual will have logged on to the IRD website using the igovt Logon Service.
- During the logon process the igovt Logon Service will have returned to IRD the individual's FLT for IRD. This is part of a SAML authentication token which includes such information as the strength of authentication performed and who issued it, but no identity information.

- When the individual asks IRD online for information about their loan repayments, the web page would ask the individual for permission to seek information from MSD.
- If the individual agrees, IRD will then ask for an opaque token for the individual. This opaque token will include the FLT returned when the individual logged on but is encrypted in such a way that it can only be decrypted by the STS.
- IRD then sends a web service request including the opaque token to MSD's web service provider (the Target Agency) asking for information about loan repayments. At this stage MSD does not know who the request is about. This step does not involve igovt.
- MSD's web service provider forwards the encrypted individual's opaque token onto the STS asking it to validate the individual's opaque token.
- The STS decrypts the individual's opaque token and validates it by accessing the federated logon tag directory and looking up the FLTsource using the Service Agency ID of the source Agency.
- The STS then looks for the individual's FLT for MSD and out of that creates a new authentication token using the Service Agency ID of MSD.
- The STS sends to MSD the individual's authentication token for MSD.
- MSD, having authenticated the individual, sends the relevant information about the individual's loan repayments to IRD. This step does not involve igovt.

The design is to ultimately enable a chain of agencies to pass information about an individual to each other. This could mean that a 'source' Agency in a particular part of the chain may not be the initiating Service Agency. However, all instances of passing information between agencies will be with the consent of the individual.

This could mean, for example, that once MSD has sent its information back to IRD, it could forward the initial request with the encrypted source FLT on to the person's University to check enrolment status. Another option is that it might seek a new FLTsource and forward that on the University.

However, IIS understands that at this stage the scope of the proposed implementation will only allow two-party transactions. This is because there is not yet developed an appropriate user managed consent mechanism to follow the requests. The following is a diagram of the information flows for the STS.


Source Agency - IRD
(Service Provider)
igovt
1. Logon
Username
Password
SAML SP
client
2. Request individual authentication
3. Receive response with FLT source
IRD FLT - ABCDEF
Logon
application
SAML IDP
Logon FLTs
(Individual)
IRD FLT - ABCDEF
MSD FLT - PQRSTU
4. Ask permission
to seek information
from MSD
5. Individual grants
permission
WS-Trust
client
6. Issue request using authentication
7. Receive authentication token
IRD FLT - ABCDEF
Security
token
service
Agency to
agency
exchange
IRD FLT - ABCDEF
8. Encrypted assertion passed to
WSP with business process request
11. Remainder of
cross-agency
business process
Target Agency - MSD
(Web Service Provider)
Agency to
agency
exchange
9. Validation request for authenticated token
IRD FLT - ABCDEF
WS-Trust
client
10. Receive matching FLT target
MSD FLT - PQRSTU

4.2 HELP DESK WEB SERVICE

igovt currently mainly provides help desk support to Service Users through its contractor Datacom. It provides help desk support using a help desk web application. igovt also provides for the capacity for an Agency to sign an agreement with DIA and get access to the same web application that Datacom uses. Once the Service Agency has signed up, they can perform a subset of the same help desk activities as Datacom. Two agencies have so far signed up to provide help desk support in this way.

Support functions include such activities as password resets and changing email address.

However, a number of large agencies including IRD have indicated an interest in performing igovt support functions in order to be able to provide 24/7 customer support including igovt support.

The current process for an Agency providing its own igovt logon support is slow and cumbersome. The service desk operator must activate the igovt application in their browser and must also log on before being able to handle a call from a Service User seeking support.

The user interface and navigation in the igovt help desk application is not very efficient and has a different user interface and navigation methods to those that the Agency service desk operator is using for handling the majority of calls.

DIA considers it unlikely to be acceptable to large agencies that need to handle large volumes of calls quickly and efficiently.

igovt Logon Service Release 9 is seeking to streamline the process by developing a web service mechanism that can be integrated with the Service Agency's own support desk application. The web service does not provide any new functionality and does not increase the scope of what support can be provided.

The main change is that the web service will create a new class of help desk person. In addition to the igovt Help Desk Operator, who has rights to access the igovt help desk functions at the igovt Help Desk (Datacom), there will be a Service Desk Operator and a Service Desk Administrator. The igovt Operator/Administrator will delegate to the Agency Service Desk Administrator the role of setting up Agency Service Desk Operators to have access the igovt Help Desk Web Service. The igovt Logon Service will need to support functions to set up and maintain an Agency service desk, including:

- Enabling an Agency Service Desk Administrator to set up a Service Desk Operator; and
- Enabling the igovt operator (Administrator) to assign the role of the Service Agency Administrator.

In order to operate a Service Agency version of the igovt support functions via the Help Desk Web Service mechanism, the Agency's support desk application will need to include a number of use cases. These include the ability to:

- Search the Logon Service for a particular Service User that has called in needing support;

- View the Service User's logon attributes or review recent igovt activity including prior service desk actions;
- Perform an unauthenticated request such as a forgotten username request;
- Perform secondary (non-logon) authentication, such as via the Service User's secret questions or, if this fails, using an alternative method;
- Perform an authenticated request such as update contact details, or reset password, change mobile phone number.
- Authenticate an operator – to enable igovt to audit all igovt-related actions performed by a Service Desk Operator, all operators will need to be authenticated including through recording the operator's uniquely identifying FLT and associating every action with the operator.

4.3 Self Service Forgotten Username

The igovt Logon Service currently provides an online self service option for password recovery. It does not yet have an online self service option for recovering a forgotten username.

Currently a Service User must call the help desk to recover their username. This process involves sending the username to the email address supplied by the caller without revealing during the call itself the username or the usernames registered with that registered email address.

igovt Logon Service release 9 will provide a self service function for recovery of username.

In addition to providing a more convenient process for the Service User and a less labour intensive process for igovt, it will ensure that the correct procedure is always followed.

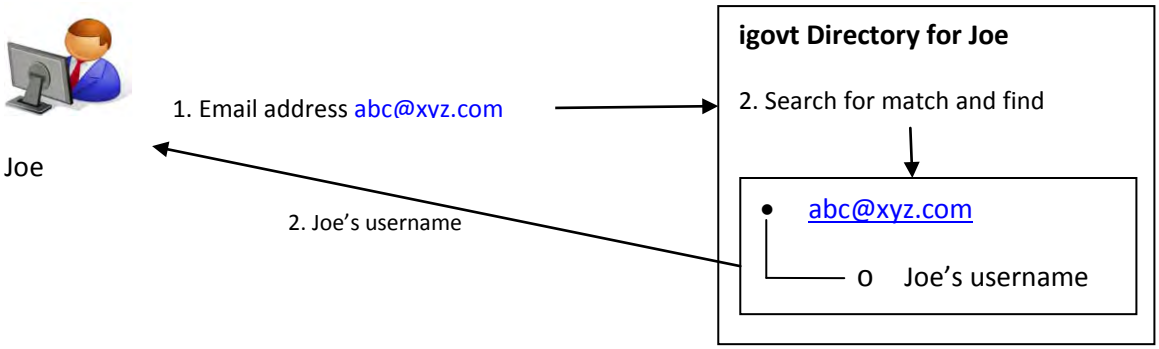
The self help business process will be similar to the current process. It will involve the following steps:

- The Service User (who has already created an igovt logon) seeks to subsequently logon to igovt, but cannot because they cannot remember their username and the username they enter is not correct;
- The Service User clicks on a link and is asked to enter the email address they entered at the time they registered for igovt (or has subsequently updated);
- The system searches the igovt directory to check that the email address provided is valid and matches a registered email address.
- If the system finds a valid matching email address it sends the username or usernames associated with the email address to the registered email address;
- If the system does not find a matching registered email address the Service User will see that the system has completed the email recovery process, but it will not send an email.

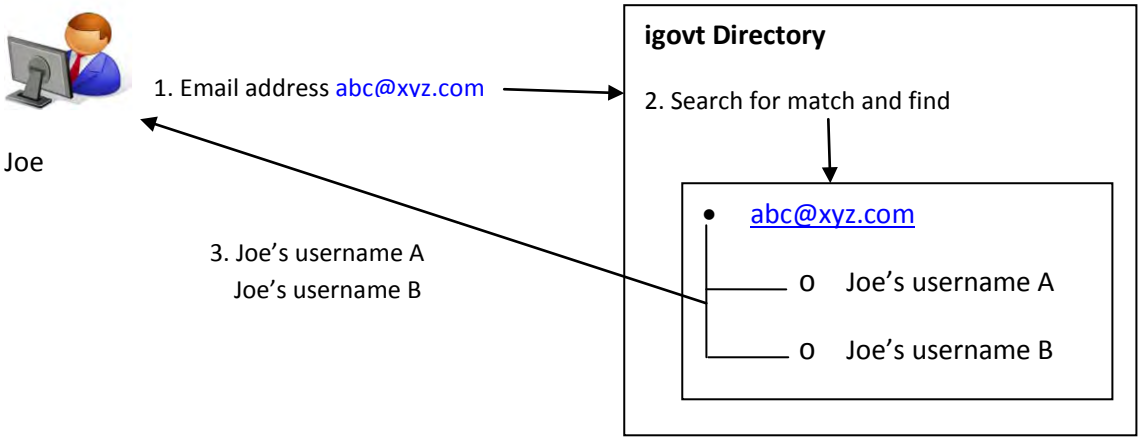
The main challenge for the self service process arises where the person enters an email address which is shared and the system finds more than one logon associated with it. This could arise, for example where family members share the same email address, but have different logons (usernames) or where a Service User has a number of different logons. Whereas a call based service can sort this out, an automated self service process is not able to do this, particularly if there are quite a few usernames.

The solution will address this problem by referring a Service User who enters an email address shared by more than 5 usernames to the applicable help desk. The following are information flows for Self Service Forgotten Username.

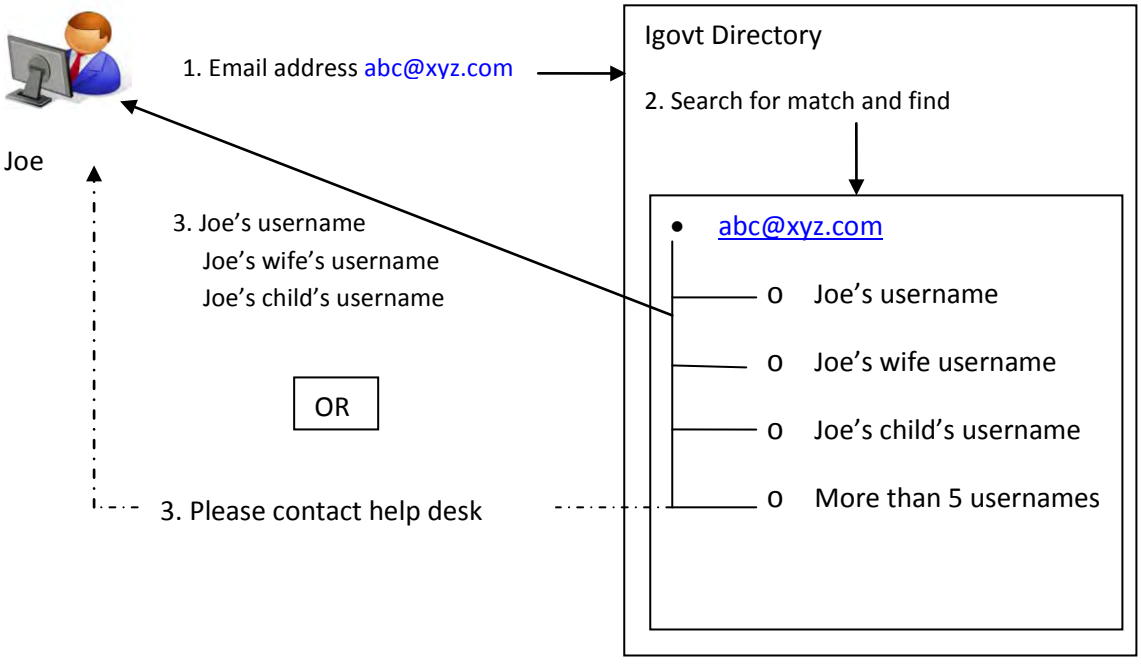
Service User forgets username – one email address only



Service User forgets username – same email address – a number of accounts



Service User forgets username – shared email address



5 POSSIBLE RISKS IDENTIFIED

The following section identifies the possible risks that could arise in relation to the implementation of the STS, Help Desk Web Service and Self Service Forgotten Username.

Privacy Principle	**Possible risk**
Lawful purpose, collection necessary (1)	**STS** That a source Agency collects information for a purpose that is not lawful or connected with a function or activity of the Service Agency. That the STS collects more information about an individual's interactions with government agencies than it needs to for the purpose of enabling single sign-on (as per PLS005b). That the source or target agencies collect more information about an individual than they need for the purpose of transferring information between them.
	Help Desk Web Service That an Agency using the Help Desk Web Service collects information for a purpose that is not lawful or connected with a function or activity involved in providing support to a Logon Service User. That an Agency using the Help Desk Web Service collects more information from the Logon Service about an individual than it needs to handle a help desk call including through logs it collects and stores (as per PLS004).
	Self Service Forgotten Username There do not appear to be any issues here in relation to the Self Service Forgotten Username.
Direct collection (2)	**STS** Risk that an Agency may collect information about an individual indirectly and without their knowledge or consent for example: • An Agency uses an individual's FLT source to gain access to information about them from another Service Agency without the individual's knowledge or consent.
	Help Desk Web Service Risk that an Agency using the Help Desk Web Service collects information about an individual from the igovt Logon Service without

	the individual's knowledge or consent
	Self Service Forgotten Username There do not appear to be any issues here in relation to the Self Service Forgotten Username.
Notice/Transparency (3)	**STS** That information about individuals could move between agencies without individuals being aware of what happens to the information.
	Help Desk Web Service Risk that individuals do not understand how the Help Desk Web Service works and that an Agency using the Help Desk Web Service may collect information about them from the igovt Logon Service.
	Self Service Forgotten Username Risk that individuals do not understand how the Self Service Forgotten Username works
Unfair, intrusive collection (4)	This is unlikely to become an issue in relation to these services.
Storage and security (5)	**STS** Release 9 does not appear to create any additional risk here.
	Help Desk Web Service Risk that information such as username will be available to Service Agency help desk staff which could make the information vulnerable to unauthorised or fraudulent access, use or disclosure.
	Self Service Forgotten Username Risk that an individual's username or usernames could be revealed to someone other than the person who has sought to recover it. Risk that the service could be used to harvest email addresses.
Access (6) Correction (7)	**STS** Risk that individuals will not know what information is held about them by source or target agencies as a result of the information exchange capability and hence be unable to take action to correct it if it is wrong.

	Help Desk Web Service Risk that individuals will not be aware of information stored about them by an Agency as a result of its use of the Help Desk Web Service and so be unable to take action to correct it if it is wrong.
	Self Service Forgotten Username There do not appear to be any issues here in relation to the Self Service Forgotten Username.
Accuracy (8)	**STS** Risk that a target Agency may pass inaccurate information about an individual back to a source Agency.
	Help Desk Web Service There do not appear to be any issues here in relation to the Help Desk Web Service.
	Self Service Forgotten Username There do not appear to be any issues here in relation to the Self Service Forgotten Username.
Retention (9)	**STS** There do not appear to be any issues here in relation to the STS beyond the already existing risks.
	Help Desk Web Service Risk that agencies using the Help Desk Web Service will retain information about an individual they collect through the web service for longer than they need to for the purpose of helping a caller to the help desk.
	Self Service Forgotten Username There do not appear to be any issues here in relation to the Self Service Forgotten Username.
Limits on use (10)and disclosure (11)	**STS** Risk that a source Agency may use an individual's Service Agency FLT to gain information about the individual from other agencies without the individual's knowledge or consent. Risk that a target Agency may disclose information to the source Agency for purposes unrelated to the purpose for which the

	individual gave the target Agency information, and without the individual's knowledge or consent.
	Help Desk Web Service Risk that an Agency using the Help Desk Web Service uses or discloses information collected for providing help desk support to a caller for a purpose for purposes unrelated to this, for example: • Use of contact information to check whether the Service Agency's address information about the individual is accurate; • Use or disclosure for malicious or fraudulent purposes.
	Self Service Forgotten Username There do not appear to be any issues here in relation to the Self Service Forgotten Username.
Unique identifiers (12)	**STS** There do not appear to be any issues here in relation to the STS beyond the risks that already exist in relation to the STS.
	Help Desk Web Service There do not appear to be any issues here in relation to the Help Desk Web Service.
	Self Service Forgotten Username There do not appear to be any issues here in relation to the Self Service Forgotten Username.
Allocation of risk	That when mistakes or problems occur in the new Release 9 processes individuals' lives are severely disrupted and individuals must bear the burden of ensuring that errors are rectified because: • Individuals may not know who to contact if things go wrong; • No one Service Agency is prepared to take ultimate responsibility for fixing the problems and the individual is passed from Service Agency to Service Agency; • There is no easy way to access a 24/7 support service; • The burden of security and other risk is placed on the individual through the 'Terms and Conditions'. • The assumption is that the individual is at fault if something

	goes wrong.
Function creep	That the functions of the STS Release 9 information exchange process will evolve in ways that come to be regarded as unwelcome and unacceptable function creep. For example, the protection provided by consent might reduce as the choice to use offline sources diminishes.

6 FINDINGS ON PRIVACY RISKS AND RECOMMENDATIONS

6.1 PURPOSE OF COLLECTION AND IPP 1

6.1.1 COLLECTION FOR LAWFUL PURPOSE

IIS notes that the STS, Help Desk Web Service, and Self Service Forgotten Username are extensions of existing services. IIS does not have any reason to believe that the collections proposed by Release 9 are for anything but lawful purposes.

6.1.2 COLLECTION NECESSARY FOR PURPOSE

6.1.2.1 STS

IIS considers that the STS process is designed to minimise the information about an individual a target Agency receives in a request for information sent from the source Agency. For example to avoid sharing identifiers and other personal information relating to the individual:

- The individual's FLT from the source Agency is encrypted when it is sent to the target Agency;
- The target Agency only receives the individual's target Agency FLT, and so only receives information that it would have already.

The only information that travels to the target Agency in the clear with the encrypted FLT is:

- The Agency ID of the originating organisation (which the target Agency would have anyway in the message which includes the encrypted FLT);
- Information about the validity period of the FLT (the assertion only has a short validity period);
- The strength of the Service User authentication.

No personal information travels in the clear.

The FLTsource is encrypted so that only the STS can decrypt the the FLT source and only for the purpose of changing the FLTsource to the individual's FLT for the target Agency.

The STS will have logs that indicate that the individual has interacted with one Service Agency (the source Agency) for which the STS has issued an FLTsource and that following this the target Agency has asked to have the encrypted FLTsource converted into the individual's FLTtarget.

The STS will not have any information about the reasons for these transactions.

IIS considers that these design features appropriately prevent agencies sharing unnecessary information, such as identifiers, about an individual igovt Service User.

6.1.2.2 HELP DESK WEB SERVICE

The design of the Help Desk Web Service limits the information that an Agency Help Desk Operator using Help Desk Web Service has access to. The Help Desk Operator will have access to sufficient information to enable them to help out with password or username resets, or change of email address. So they will have access to such information as:

- The fact that the individual has reset their password or changed their email address, but not the Service Agency context in which this occurred;
- The individual's logon attributes such as username, email address, phone number, token and logon type.

Some of this the Help Desk Operator will gain because the individual Service User gives the information to them for the purpose of fixing a problem. As with the current function the Operator may also gain access to this through the Help Desk Web Service search function.

On the other hand the Operator's access to other information is filtered so they only see information relevant to the particular Service Agency. For example, the Operator only has access to:

- The FLT the individual has for the particular Service Agency providing the help desk support. The Operator cannot see any of the individual's FLTs for other agencies.
- The transactions the individual has had with Service Agency providing the help desk support, for example, that the individual has logged on to the Service Agency, but not to the fact that the individual has logged onto other agencies.

The igovt policies and terms and conditions associated with Service Agency access to the Help Desk Web Service will require that Service Agency applications do not record information such as the username, phone number or registered email address that they have access to in order to handle a support request, but do not need after the support request has been dealt with.

IIS considers that these measures significantly mitigate the risks of unnecessary collection by agencies using the Help Desk Web Service. However, they would be strengthened if there was a mechanism to ensure that agencies using the Help Desk Web Service have complied with this requirement.

Recommendation 1: Governance and accountability – Audit of Service Agency Help Desk Web Service applications

IIS recommends that DIA audits the help desk applications of agencies using the igovt Help Desk Web Service to ensure that the applications comply with DIA policies about what information should not

be recorded from a Service User support session. In particular the audit should check to ensure that Service Agency help desk applications do not record an individual's igovt account username or registered email address. IIS suggests an audit cycle of no longer than every two years.

6.2 DIRECT COLLECTION AND IPP 2

6.2.1 STS

Indirect collection can create privacy risks particularly if the individual does not know about the collection and would be unlikely to agree to it. It can result in the individual losing control over information about them. If individuals do not know who holds information about them, they cannot correct it if it is wrong or seek redress if wrong decisions affecting their lives are made on the basis of that information.

The STS Release 9 enables an Agency, with an individual's permission, to collect information electronically about him or her indirectly from another Service Agency.

IPP 2 allows indirect collection as long as the Service Agency has the individual's permission, or some other exceptions apply.

Release 9 will require an Agency to ask for the individual's consent to collect information about them indirectly from another Agency. It will provide a mechanism for the Agency to tell the STS that it has obtained the individual's consent. If the Agency does not explicitly tell the STS that it has received such consent, the STS will not honour the request for the opaque authentication token necessary to make the indirect collection.

However, the system has not yet been sufficiently developed to enable the consent status to travel to the target Agency with the opaque token and the message asking for the information. The target Agency must assume that the individual has consented. Because the consent arrangements are not very sophisticated at this stage of the design, DIA will not be implementing the ability to pass a request for information to a second target Agency along the chain in this Release.

This keeps the events closely linked and reduces the risk that an Agency may be collecting information from another Service Agency without the individual knowing about it or agreeing to it.

There could be a risk that an Agency may, independently of a Service User's logon session, try to use an individual's local Agency FLT to request an FLTsource and send it to a target Agency with a request for information. To reduce the risk of this happening, the STS is designed so that it will only provide an FLTsource if the request is made in the context of a current logon event.

In addition, all requests for FLTs would be logged by STS and a Service User would be able to see all the requests on their account and take action if it appeared that requests had been made without their consent.

IIS considers that these arrangements provide adequate protection against unauthorised indirect collection at this stage of the implementation.

6.2.2 Help Desk Web Service

The Help Desk Web Service allows a help desk Operator to access an individual's igovt details only with their consent. The individual would have to give the help desk relevant details to enable such access.

There is a possible risk that a staff member of an Agency using the Help Desk Web Service could then use those details to access such information indirectly outside the help desk context. These use and disclosure and security issues and are discussed in Section 6.9 Limits on use and disclosure and Section 6.5 Storage and security.

6.3 Notice and transparency

DIA appears to have every intention of being as transparent as possible about the matters outlined in IPP3, including in cases where an Agency will collect information indirectly such as in the case of the proposed changes to the STS. The real privacy risk arises out of the manner in which transparency is achieved. It is all too common for key matters to be buried in fine print in terms and conditions, or in unintelligible language in lengthy privacy notices many clicks away from where Service Users access a service.

The key strategies for ensuring Service Users receive the information they need include:

- Using clear and non legalistic language;
- Designing web pages so that the particularly important information is placed where it is most meaningful and likely to be read by the Service User (for example, at the point where information is entered);
- Adopting a layered notice approach consistent with the approach adopted by Privacy Commissioners globally (www.privacyconference2003.org/resolution.asp and www.hunton.com/files/tbl_s47Details/FileUpload265/1405/Ten_Steps_whitepaper.pdf).

A key mechanism for transparency will be the information available to a Service User in their igovt account which will show all Service Agency interactions with their igovt account.

Recommendation 2: Governance and transparency – Informing Service Users

DIA should engage experts in plain language and online useability to ensure that Service Users are easily able to access and understand important information about how the upgrades to the STS will work including how source and target agencies will collect, use and disclose information about Service Users. The information that Service Users need to know most should be prioritised and made most accessible.

DIA should develop a strategy for publicising changes to the privacy policies and corresponding changes to privacy notices as they occur over time.

6.4 Unfair and intrusive collection and IPP 4

IIS has no information to indicate that this is likely to be a risk arising in relation to the igovt Logon Service updates.

6.5 STORAGE AND SECURITY AND IPP 5

6.5.1 HELP DESK WEB SERVICE

As identified above there is a risk that sensitive information such as username will be accessed and stored by an Agency using the Help Desk Web Service without the knowledge or consent of the Service User. This is already a risk with the current help desk arrangements and IIS has not identified anything in the design of the Help Desk Web Service that would increase this risk. The likelihood of such a risk eventuating increases, however, as more agencies use the Help Desk Web Service and there are more staff accessing igovt information.

There are already a number of measures in place to mitigate the existing risk including:

- Limiting the information available to help desk staff to that which is necessary for providing help desk support;
- igovt logging in detail every access help desk staff make to a Service User's igovt details;
- igovt making information about help desk staff access available to the Service User through their igovt account

The fact that the function of setting up Service Agency help desk operators will be delegated to the Service Agency help desk administrator might be regarded as a loosening of control by igovt over who has access to help desk functionality and a potential increase in risk. However igovt has maintained control over who can become a Service Agency help desk administrator. Release 9 also provides for more fine grained access controls than is case for the current web application.

The key here will be for DIA to ensure that Service Agencies using the Help Desk Web Service have appropriate measures in place to vet staff that will have access to the Web Service.

Recommendation 3: Governance and accountability – Conditions imposed on agencies using Help Desk Web Service

IIS recommends that DIA makes it a condition of service agencies gaining access to the Help Desk Web Service that they have appropriate procedures for vetting staff that will have access to igovt details. The condition should include that the Service Agency regularly audits staff access to ensure that it appears appropriate and related to a particular caller request.

6.5.2 SELF SERVICE FORGOTTEN USERNAME

6.5.2.1 SHARED EMAIL ADDRESSES

There is risk with design of the Self Service Forgotten Username that a person seeking to recover their username because they have forgotten it could end up receiving the username or usernames of someone else. This is because the service sends the email containing the forgotten username to the registered email address of the person seeking help. However, because of the way that Service Users are able to establish their igovt account, an email address registered with igovt could be one that is shared with other people, such as other family members. As a result, using the email address to search for a person's username may return more than one username. The family member could then potentially use the username to find out the password for the username and thereby gain access to the family member's account and Service Agency services. This is unlikely to be a major

risk if family members have consciously and with full understanding agreed to share this kind of information.

This risk will also be partially addressed by ensuring that the email returning the username will not include any other information (which is also the case for recovery of a password).

In addition, the solution will limit the number of usernames that will be returned to the Service User if there is more than one. The proposed number is 5 usernames. If there are more than 5, the Service User will be referred to the help desk.

Allowing people to have more than one logon and to provide a shared email address is a privacy protecting aspect of igovt which provides choice and reduces the number of unique identifiers that could be used to link information about an individual. IIS would not propose to change these features in order to address the risk of a username being exposed to someone other than the individual seeking help with their username.

IIS considers that the key here is to ensure that Service Users are made aware of the consequences of using a registered email address that is shared. Warnings could be issued at the time Service Users register an email address, change an email address and when they use Self Service Forgotten Username.

Recommendation 4: Business as Usual – Education about shared registered email addresses
IIS recommends that igovt Service Users are warned about the consequences of using a registered email address that is shared with other people. This could be done at the time that Service Users register for an igovt account, when they change their registered email address and when they use Self Service Forgotten Username.

6.5.2.2 Email address harvesting

There is a risk that the Self Service Forgotten Username provides a web interface that could be used to harvest registered email addresses. Or a person could pretend they have forgotten a username and type in an email address to find out if it is a valid email address or not.

The solution will address this issue by not confirming or revealing whether the entered email address has been registered with the igovt Logon Service. It is proposing to present the same request completed message regardless of whether the email is matched with a username.

IIS considers that these measures adequately address these risks.

6.6 Access by Service User to information (IPP 6) and Correction (IPP 7)

A key tool to give individuals control over personal information held about them by others is to enable the individual to gain access to that information and to correct it if it is wrong.

A key mechanism that igovt uses to provide individuals with access to information collected, used and disclosed through igovt services is to include information about every interaction in the Service User's igovt account. This gives the Service User a picture of what information about them is stored in the igovt Logon Service and will also alert a Service User to any issues or concerns and enable them to take action to address any issues of concern with the Service Agency concerned, including

by seeking access to information held by the Service Agency through the access and correction processes required by IPP 6 and IPP 7.

IIS considers that these measures are an excellent way to provide individuals with access rights in a complex system such as igovt.

6.7 ACCURACY OF INFORMATION IPP 8

6.7.1 STS

There is a risk that a target Agency may send inaccurate information about an individual back to the source Agency.

IIS considers that the STS does not increase the risks associated with inaccurate information being held or exchanged between agencies as long as the Service User is aware that the exchange has taken place and is therefore able to identify the source of any inaccuracy. IIS considers that the measures outlined in Section 10.6 and elsewhere relating to consent and transparency address the issue of awareness.

6.8 RETENTION OF INFORMATION AND IPP 9

6.8.1 HELP DESK WEB SERVICE

There could be a risk that an Agency using the Help Desk Web Service may keep information about a help desk session longer than it needs to for the purpose of helping a caller to the help desk. As discussed above, some of the risk associated with this will be addressed if Service Agency applications comply with igovt policies that prohibit the recording of important identity attributes such as username, email address or security questions.

The remaining information an Agency might store would include information that they had helped a Service User and the actions a Help Desk Operator had taken to address an issue. This might include that the Operator had, at the same time, updated a User's Agency mailing address. This information could be important for statistical or accountability reasons. It would not contain any personal information, but could potentially be linked to a person. For this reason the information should be deleted if not needed or when no longer needed for statistical or accountability reasons.

Recommendation 5: Business as usual and accountability for deletion of help desk information when no longer needed

IIS recommends that it be a condition of using the Help Desk Web Service that the Agency conducts an assessment of the kinds of information it stores as a result of a help desk session with a Service User. The Agency should identify whether there are good reasons, such as statistical or accountability reasons, for keeping that information and, if so, document for how long it will be needed. The Service Agency should ensure it has regular processes by which it deletes such information from its records when it is not needed or no longer needed. The process should be governed by a memorandum of understanding between igovt and the Agency which could include a requirement to report to igovt about the information it keeps relating to help desk sessions and the Agency's destruction schedule for such information.

DIA should explore the use by agencies of developing technology that enables efficient and cost effective deletion of data by building retention and deletion policy into data at the time it is generated.

6.9 LIMITS ON USE AND DISCLOSURE IPP 10 AND 11

6.9.1 STS

As identified above, there is a risk that a source Agency may use an individual's local Agency FLT to gain information about the individual from other agencies without the individual's knowledge or consent.

The associated risk is that the target Agency may then use this process to disclose information to the source Agency for purposes unrelated to the purpose for which the target Agency originally collected the information without the individual's knowledge or consent.

In line with the principles underpinning igovt, there is every intention to develop a solution that ensures that information is only shared with the Service User's consent.

The solution proposed for the current implementation relies heavily on the up front consent gained by the source Agency. The consent information does not travel with the FLTsource and the target Agency has to assume that the source Agency has the relevant consent based on its understanding of requirement placed on the source Agency and the way the STS works.

The solution includes a number of measures designed to ensure this including the business rule that the STS will not issue an FLTsource or FLTtarget unless there is a current logon event. This is backed up by the ability for a Service User to see in their account every Service Agency interaction with the STS.

The approach to consent in Release 9 is not ideal, but IIS considers these measures are adequate in the context where the ability to share is limited to one source Agency and one target Agency. Should the capacity to share beyond this be implemented or the capacity to issue a FLTsource or FLTtarget outside a current logon session be implemented there will need to be more sophisticated and effective means of ensuring that such exchanges only occur the with individual's full knowledge and consent. IIS understands that this is an issue that DIA will work on as the capability is further implemented. IIS considers that without such mechanisms there is a real risk that Service Users could lose control over information about them held by agencies.

IIS considers there should be another PIA conducted when the ability to exchange information electronically is extended beyond more than one source and target Agency and/or an Agency is able to seek a FLT source outside the context of current logon event and which the individual has given direct consent.

Recommendation 6: Business as usual – Expanding the range of exchange of information
IIS Recommends that DIA conducts a PIA at the point at which it proposes to extend the ability to exchange information about a Service User electronically beyond one source Agency and one target Agency or to enable an Agency to seek an FLT source outside the context of a current logon event through which an individual has given the source Agency direct consent.

6.9.2 Help Desk Web Service

There could be a risk that an Agency using the Help Desk Web Service might use information accessed or collected for providing help desk support for intentional purposes unrelated to the purpose of providing help desk support, for example to check the currency of an Agency's email address. This would only be possible on an ad hoc basis when a caller requires help desk support and is unlikely to be useful as a general strategy for keeping addresses up to date. As discussed above, there are a number of measures in place to reduce this risk including:

- Auditing the activities of Service Agency help desk operators;
- Making the activities of Service Agency help desk operators apparent to Service Users;
- igovt policies about what can and cannot be recorded by Service Agency help desk applications.

Privacy Act provisions would also prevent this.

IIS considers that these measures are adequate to address this kind of risk.

IIS has considered the risks related to internal malicious use in Section 6.5 Storage and Security.

6.10 Unique identifiers and IPP 12

None of the Release 9 updates appear to raise any issues relating to the use of unique identifiers. The main unique identifier used by the STS is the username. This is not exposed during the exchange of information between a source and target Agency. An individual's Agency FLT is not exchanged with another Agency as each FLT is encrypted and only able to be decrypted by the STS.

A username may be exposed to an Agency Help Desk Service Operator but this is in their capacity as an igovt help desk operator in a similar way to Datacom and only for purposes related to igovt support. igovt has policies in place to prevent an Agency from recording key identifiers such as username, or other identifiers such as email address.

6.11 Function creep

There is always a risk that there will be an expansion of the use of the STS to exchange information between agencies beyond those provided for in Release 9.

Whether or not expansions will be welcome or accepted by the community or seen as unwelcome "function creep" will depend on their nature and how they are made. The difference may simply be the speed of introduction, the degree to which the community is taken into confidence and other subtle matters. At other times, the difference is more real and will never be considered as anything but function creep because it is seen as an inappropriate invasion of privacy, for example if the changes were introduced with insufficient surrounding governance mechanisms such as transparency and accountability mechanisms to ensure abuse or unintended consequences do not happen.

A key privacy protection in the current situation is that individuals have choice about the ways in which to interact with agencies including about the way they go about sharing information. Offline options are still readily available. However, IIS considers that there is a significant risk that as the

STS makes it easier for agencies to collect information about individuals indirectly from other agencies electronically, collection of information about individuals indirectly in this way could become the norm and this could bring with it additional privacy risks.

In relation to STS, the risks appear to be that that the system could be used to exchange information about individuals electronically without their consent or that the protection consent provides is increasingly undermined as agencies increasingly conduct business online and the choice to interact offline or in other ways is slowly eliminated.

6.11.1 Exchange without consent

IIS considers that a move to exchange information about individuals electronically using the STS without their consent is unlikely in the current environment where there is strong adherence to the igovt principles. This could change down the track, but if wholesale exchange became a strong government interest, the whole purpose for having FLTs and the STS in the first place would be undermined. There would be a high risk of losing Users' trust and confidence. IIS considers that the move away from a consent based approach is unlikely to occur without there being a significant public debate about it.

6.11.2 Effectiveness of consent

IIS considers that DIA is to be congratulated for the extent to which Service User consent continues to be a significant part of the design of STS in Release 9. But as has been pointed out in previous PIAs the power of choice as a privacy risk mitigation mechanism will inevitably erode overtime particularly if the STS is successful and widely taken up, and online government services consequently expand. In the ongoing search for greater efficiencies it is likely that other channels for interacting with agencies and exchanging information will slowly fade away. For convenience and these other reasons individuals will be increasingly locked into using igovt to interact with agencies.

The significance of this is that, in the long term, DIA will need to rely on the other privacy "tools" to address privacy risk. In particular there must be strong governance and accountability measures backed up by strong safety net mechanisms for when failure occurs.

Recommendation 7: Governance of igovt and the electronic exchange of information
IIS recommends that DIA should put in train steps to review what might be an appropriate governance mechanism to ensure that as the STS develops and the choice to interact offline diminishes, other governance and accountability mechanisms are introduced to compensate for the diminishing power of consent. At the latest, the first review should commence 3 years from now.

6.12 Unfair or inappropriate allocation of risk

It is a common feature of many new IT systems that those implementing it pay significant attention to managing their own risks, but often forget to consider and manage the risks that the system might pose for Service Users. Some of the most common ways this occurs is:

- Terms and conditions that disclaim any liability on the part of the service provider for any failure in the system and for any loss, or damage that might be suffered by the Service User as a result;

- Placing significant responsibilities on the Service User in relation to the information they provide and its protection;
- Uncoordinated customer support mechanisms which means that the Service User is passed between various Service Agencies, none of whom will take responsibility for the problem, or for ensuring, particularly where more than one Service Agency is involved, that addressing the problem is coordinated and then finally resolved;
- Hard to access, unresponsive and often hostile complaints mechanisms.

All of these mean that Service Users will find themselves having to bear all the inconvenience, disruption to life and cost of resolving their problem and restoring order to their lives.

6.12.1 CUSTOMER SUPPORT

6.12.1.1 STS

There is significant potential for a Service User's life to be disrupted through failure of the STS or through failures occurring at the source or target Agency level, particularly as online interactions with government and other organisations for key services become increasingly the norm. For example, if an individual's attempt to seek a service is unsuccessful because a problem in the exchange of information between agencies it may be hard for the individual to know where the problem has occurred or to know who to approach to have the problem dealt with.

It is critical to ensure that igovt takes appropriate responsibility for preventing and addressing mistakes and failure in the information exchange process and has top class coordinated customer support available 24/7. This should be available even if the STS is not the immediate cause of the problem.

Recommendation 8: Governance – Managing failure and mistakes when information is exchanged between agencies

IIS recommends that DIA ensure that it has in place a coordinated and responsive customer support system to handle mistakes or failures in the electronic exchange of information between agencies, even where the STS is not directly involved.

6.12.2 TERMS AND CONDITIONS

IIS has not seen any of the proposed terms and conditions to be used for the igovt Logon Service Release 9 updates and is not in a position to comment on these. IIS considers it would be valuable for DIA to review any proposed terms and conditions for Service Users before they go into effect to consider the question of whether they unfairly allocates too much risk to the Service User. The risk if this balance is not got right is that Service Users will be unwilling to use the STS, the help desk or the Self Service Forgotten Username for fear that if something goes wrong they will be left having to bear financial or other loss or damage.

Recommendation 9: Safety mechanisms – Fair allocation of risk

DIA should review the terms and conditions for Service Users in relation to the STS, Help Desk Web Service and Self Service Forgotten Username to ensure that the burden born by Service Users when they fail or problems arise is not unfair. Questions that could be asked to help determine fairness include:

- Is DIA excluding itself or agencies from liability in areas it has main responsibility for and over which the Service User has little or no control?
- Do the provisions mean that Service Users could be substantially out of pocket, or their lives substantially disrupted through no fault of their own?
- Will Service Users be required to exercise a level of care that is unrealistic or beyond the average person's knowledge or competence?
- Do the provisions accurately reflect the allocation of responsibility that DIA would be likely to have if a Service User took legal action, or complained to the Privacy Commissioner?
- Are the terms and conditions buried in fine type and framed in language that a Service User is unlikely to find, read or understand?
- Have we identified the problems that individuals most frequently face and assessed and addressed any unfair allocations of risk?

7 CONCLUSIONS

IIS considers that on the information it has to hand so far DIA has taken significant steps to address the possible privacy risks associated with the updates proposed through igovt Release 9. IIS has not identified any major concerns in relation to the information supplied so far in the design or process. It has identified some ways in which the implementation could be improved and has made recommendations about this.

IIS has identified some longer terms risks which will need further consideration in the context of further phases of implementation of the STS exchange of information enhancement and to the igovt programme as a whole.