Privacy Impact Assessment: Full report

One Time Identity

15 August 2020

INTERNAL AFFAIRS
Te Tari Taiwhenua

New Zealand Government

Contents

1. Glossary of Terms

Term	Definition
CLR	Colour Light Reflection Liveness method
Client	An MSD customer
Customer	A member of the public
Daon	Biometric provider for OTI solution
DIA	Department of Internal Affairs
IICA	Identity Information Confirmation Act 2012
MSD	Ministry of Social Development
OTI	One Time Identity Service
PAD	Presentation Attack Detection- that the captured biometric is that of a live and present human being
PHRaE	Privacy, Human Rights and Ethics Framework
Selfie	A photograph of an individual taken by themselves

2. Executive Summary

2.1. Introduction

The Ministry of Social Development, Te Manatū Whakahiato Ora (MSD), supports many vulnerable communities with social services. This role includes providing employment, income support and superannuation support. Given the people seeking services are applying for support, it is critical that barriers to access services are reduced. One such barrier for applicants is establishing evidence of identity.

MSD is proposing to use a new tool, One Time Identity Service (OTI) provided by DIA, which leverages technology to provide remote identity verification, without applicants being required to visit an MSD office or to have a RealMe Account. The tool uses facial recognition technology, passport biometric templates, and an evidence of liveness check (to prove that the captured selfie photo is a person and is not, for instance, a photo).

A client who is required to confirm their identity to MSD is offered a number of choices on how they wish to complete this step. If they select to use the OTI they are redirected via a URL to the DIA OTI service. They are then required to complete two initial steps:

- Provision of their passport information and a selfie
- Completeness of a liveness check.

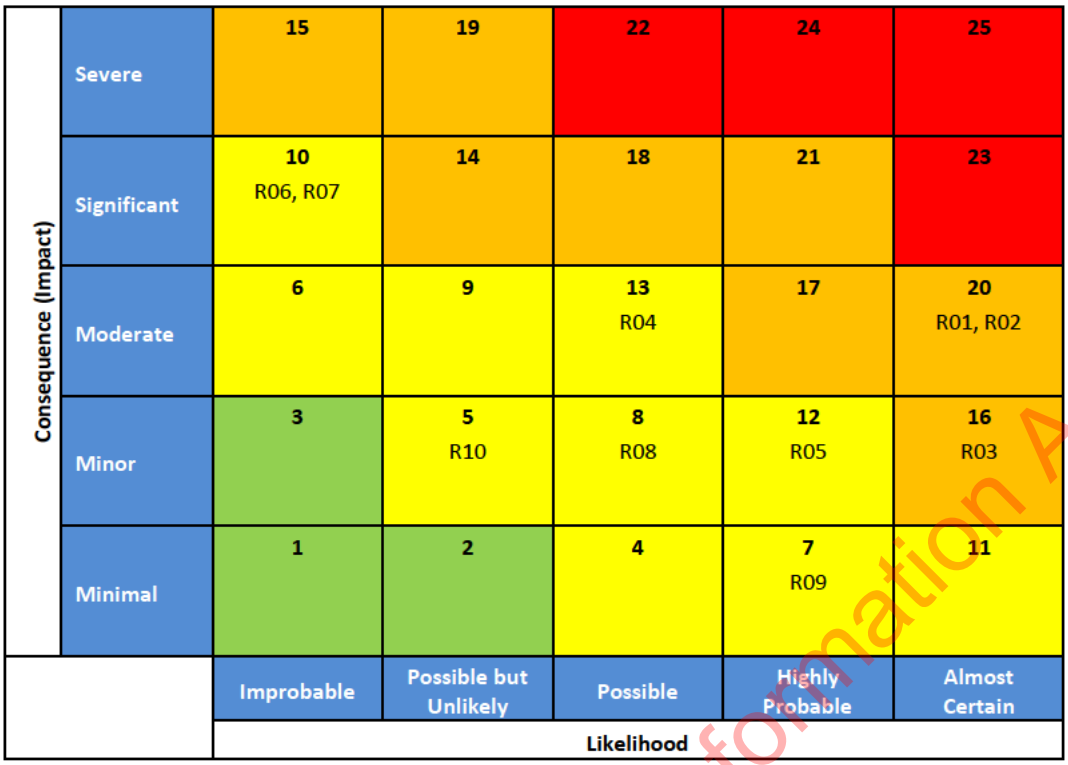
If the selfie and the liveness check are completed successfully and relate to the same individual, then the details are compared to the passport details provided. The confirmation is authorised under the Identity Information Confirmation Act. If the passport details including the passport photo match the information provided, then the client is asked to authorise the disclosure of their full name, date of birth, liveness confirmation and passport photo match confirmation to MSD.

In a subsequent release it is proposed clients will also be able to separately authorise the disclosure of their selfie photo to MSD.

2.2. Inherent risk level

This PIA has identified ten privacy risks as shown below.

Assuming all planned controls are implemented and functioning effectively, there are no zone one risks and three zone two risks.



The three zone two risks relate to the following:

- R01 - Selfie photos, liveness videos and metadata are kept for longer than required.
- R02 - Reporting of use of the manual confirmation is unavailable as required under the Customer Nominated Services AISA due to a lack of developed procedures.
- R03 - Due to an incorrect failed match by the OTI certain people can't use the service to verify their identity.

2.3. Residual risk level

If the recommended additional controls are implemented and working effectively the risk profile will reduce as shown below. This would result in no zone one or zone two risks remaining.

Consequence (Impact)						
	Severe	15	19	22	24	25
	Significant	10 R06	14	18	21	23
	Moderate	6 R01, R02	9 R04	13	17	20
	Minor	3 R05	5 R08, R10	8	12	16
	Minimal	1 R07	2	4 R09	7	11 R03
		Improbable	Possible but Unlikely	Possible	Highly Probable	Almost Certain
		Likelihood				

3. Related Documents

The following documents relate or are related to this PIA:

Document	Link
Confirmation Agreement	Cohesion Link
Customer Nominated Services AISA	Cohesion Link
Customer Nominated Services AISA Operating Procedures - MSD	Cohesion Link
Daon Master Services Agreement	Cohesion Link
DIA-MSD Memorandum of Understanding - Ongoing support schedule	Cohesion Link
Identity Binding and Liveness Summary	Cohesion Link
Client Journeus	
One Time Identity – Non-Functional Requirements	
One Time Identity Simple Architecture	Cohesion Link
OTI Privacy Statement	Cohesion Link
OTI Terms of Service	

4. Project Summary

4.1. Problem Statement

The Ministry of Social Development, Te Manatū Whakahiato Ora (MSD), supports many vulnerable communities with social services. This role includes providing employment, income support and superannuation support. Given the people seeking services are applying for support, it is critical that barriers to access services are reduced. One such barrier for applicants is establishing evidence of identity.

If a client wishes to obtain services from MSD for the first time, the client is required to ring the call centre to request a client number prior to logging into MyMSD to apply for services.

After being provided a client number and applying for services either online or in person they are currently required to provide physical documents that:

- support their identity – two different documents are required
- show use of the identity within the community.

MSD are looking to increase the ability for clients to complete all interactions online. This requirement was further amplified as a result of Covid-19 and related lockdown arrangements.

A key component of MSD being able to take services fully online is the requirement to be able to confirm an online client's identity.

MSD have approached DIA regarding a new service they are offering called One Time Identity Service (OTI) for individuals over the age of 18. This will be one of multiple methods that clients can choose from to confirm their identity.

4.2. One Time Identity Service (OTI)

The OTI is provided by DIA Service Delivery and Operations. Users are directed to the service from other organisations, in this case MSD.

The service will be developed in a number of stages:

- Release One - confirmation that the selfie provided matches the individual using the device and also matches with the passport relating to the individual concerned. Provision of the user's full name, date of birth, liveness confirmation and passport photo match confirmation to MSD with consent.
- Release Two - addition of the provision of the selfie photo to MSD with consent.

To use the service the user's passport:

- can be a child or adult passport
- must have been issued since 1st January 2004
- may be current or expired.

The service is underpinned by a facial recognition solution provided by Daon and hosted onsite by DIA.

5. PIA Scope

This PIA covers:

- Release One - confirmation that the selfie provided matches the individual using the device and also matches with the passport relating to the individual concerned. Provision of the user's full name, date of birth, liveness confirmation and passport photo match confirmation to MSD with consent.
- Release Two - addition of the provision of the selfie photo to MSD with consent.
- Consideration of risks associated with changes in the upcoming Privacy Act 2020.

This PIA does not cover:

- The use of OTI by clients of MSD who are under 18 years old.
- Consideration of how MSD will utilise the client's selfie and other details once confirmed by DIA.
- The processes used by MSD for confirming the identity of clients who do not utilise or are unsuccessful in using the OTI.

6. Applicable Legislation

6.1. Privacy Legislation

The OTI will primarily be utilised by individuals within New Zealand and therefore the New Zealand Privacy Act 1993 will apply and the subsequent Privacy Act 2020 when it comes into force.

However, MSD will utilise the OTI functionality for clients based overseas in future releases. These will primarily be New Zealand Super Beneficiaries. The majority of MSD clients who are not located in New Zealand are located in:

- Australia
- Europe
- The United Kingdom.

The Australian Privacy Act 1988 only applies to organisations outside of Australia where they have an Australian link. This link is established if the organisation or operator is:

- an Australian citizen
- a person whose continued presence in Australia is not subject to a limitation as to time imposed by law
- a partnership formed in Australia or an external territory
- a trust created in Australia or an external territory
- a body corporate incorporated in Australia or an external territory
- an unincorporated association that has its central management and control in Australia or an external territory
- the organisation or operator carries on business in Australia or an external territory.

DIA and the OTI do not meet any of the above criteria therefore the Australian Privacy Act 1988 will not apply.

The Regulation (EU) 2016/679 (GDPR) and the UK Data Protection Act 2018 both have extra territorial scope provisions. MSD will be promoting the use of the DIA OTI to these clients to confirm their identity including those in the UK and Europe. The scope of the GDPR and UK Data Protection Act means that DIA would be viewed as offering goods or services in the Union under Article 3 and therefore also in scope of the GDPR.

6.2. Identity Information Confirmation Act 2012

The Identity Information Confirmation Act 2012 (IICA) governs the use of confirmation services. The IICA defines a confirmation service as one which confirms identity information of an individual so as to:

- contribute to the prevention of a crime (particularly identity-related crimes) and
- ensure that agencies can use and, if necessary, record confirmed identity related information.

Identity information is defined in the IICA as including passport related information but doesn't include a selfie. The IICA is not a complete code and information that is not covered by it can still be shared, but that sharing needs to be lawful in its own right. Where there is an inconsistency between the IICA and other relevant legislation, including the Privacy Act and the Passports Act 1992, the IICA prevails (s21 of the IICA). This means where the IICA applies, it needs to be complied with instead of that other legislation. This also includes AISAs as they are enacted in accordance with the Privacy Act.

Because the purpose of the OTI Service is to confirm the identity of the individual for MSD purposes, it falls within the definition of a confirmation service. Therefore, where the IICA applies (the sharing of passport details, other personal information and the result of the identity verification) the IICA needs to be complied with. Where other personal information is shared that sits outside the IICA (the selfie) sharing needs to be lawful in some other way, for example, by being authorised in accordance with the Privacy Act and/or applicable AISA.

6.3. Customer Nominated Services Approved Information Sharing Agreement

The Customer Nominated Services Approved Information Sharing Agreement (Customer Nominated Services AISA) is a multi-party information sharing agreement supported by an Order in Council that came into effect in July 2020.

The Customer Nominated Services AISA involves six agencies including MSD and DIA. The AISA allows DIA to share personal information with the other agencies, and allows the other parties to share information with DIA.

The first two objectives of the AISA are to:

- gain customer service efficiencies and reduce the compliance load for individuals associated with provision of personal information through facilitating increased collaboration between parties
- verify aspects of an individual's identity or entitlement of an individual applying for or receiving public services.

The public services the Customer Nominated Services AISA intends to facilitate include:

- accurate and efficient assessment of eligibility for and entitlement to receive public services that an individual applies for or decides to utilise
- accurate and efficient delivery of public services that an individual applies for or decides to utilise.

These objectives, together with the purpose of the AISA cited above (verifying an individual's identity) are a very good fit with the nature and intention of the OTI.

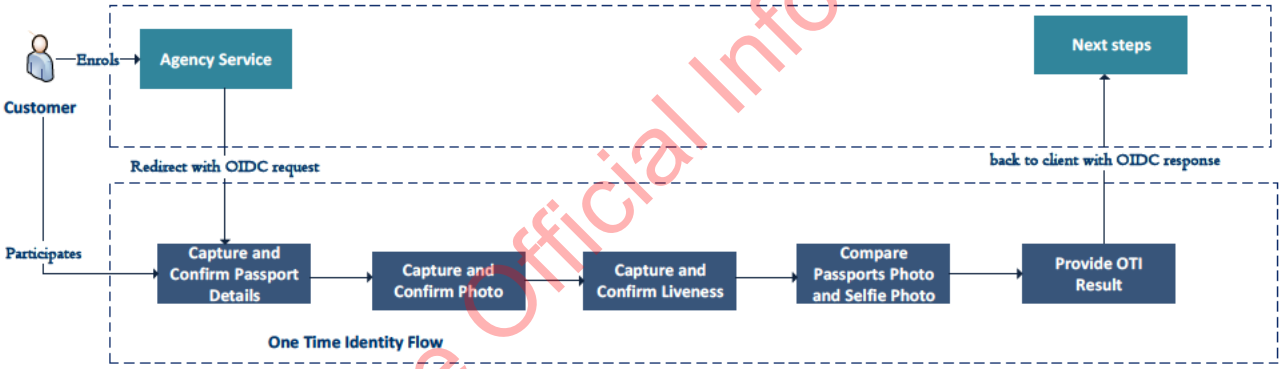
7. Architecture

7.1. High Level Process

The OTI involves an identity verification workflow which includes four key stages:

- the participant enters their passport details
- a selfie photo is then captured
- a liveness challenge is then undertaken to create assurance that the selfie photo captured is of a live and present individual
- the selfie photo is matched to the claimed identity relating to the passport provided.

A backend record stores the attempted OTI verifications and the outcomes of each stage. The record includes the user provided selfie photo, liveness video and passport FID if a passport match is completed.



7.2. Presentation Attack Detection

While facial recognition technology is mature, liveness testing has undergone significant developments over recent years in the "arms race" against bad actors attempting to impersonate others. Current spoofing techniques include digital masks, deep fake videos, and screen replay video attacks, as well as two-dimensional printed mask attacks.

To mitigate the risks around spoofing Daon's technology includes Presentation Attack Detection (PAD). This is intended to ensure that the face presented is a genuine live and present user. For example, it measures light received to detect reflections, the lack of micromovements, screen bezel edges which all suggest that the presented biometric is a photo.

Active detection also involves presenting variable coloured lights, to code the liveness test, and to ensure a video made as part of a previous attempt cannot be re-used.

7.3. Liveness matching

It is also important that the selfie photo matches the liveness video. For this reason, an algorithm scans the video/frames and extracts the best still image of the user's face. Still frames extracted from each liveness video/frames are evaluated against the still selfie photo taken by the user, to confirm they are the same person, thereby reducing the risk of video spoofing.

If the identity evaluation of the still frame fails, then the user is prompted to re-perform the liveness challenge. They are able to reattempt this three times before no longer being able to use the OTI as a method for identity validation. The liveness facial recognition evaluation result is stored within the Daon solution as either pass or fail result.

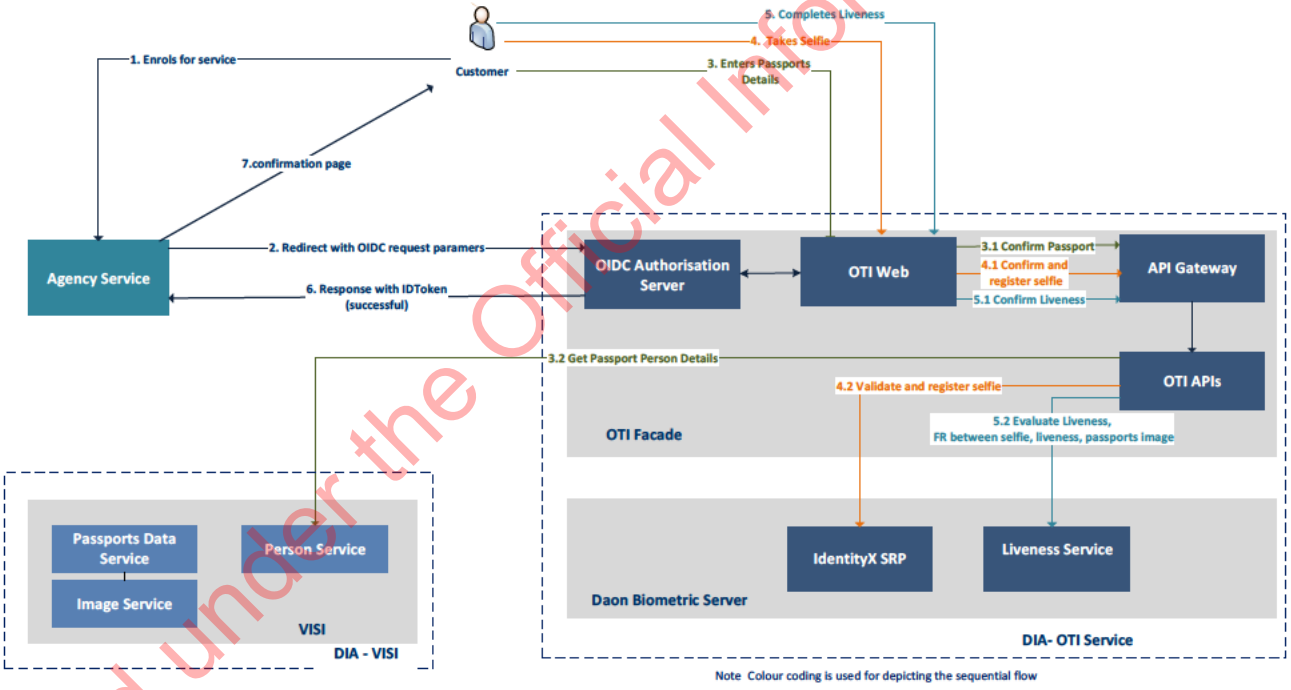
7.4. Key stage limitation

In order to reduce the risk of a brute force attempt, stage limitations are set for the entry and exit steps. A user in a session may only make five attempts to enter correct identity details matching those contained within their passport and can only make three attempts at the liveness challenge.

The limited number of attempts reduces malicious attempts to spoof liveness and to learn from previous failed attempts. Any user who fails to confirm their identity within these session limitations will have to try again later, or use another method such as presenting their physical passport in person at a MSD Service Centre.

7.5. System view

The system architecture supporting the OTI is as below.



8. Collection

8.1. Notice

Prior to the collection of any information within the OTI the user is provided the following privacy information.

> *"Your information is collected by the Department of Internal Affairs to confirm your identity. Find out how your information is managed and how you can access it in the Identity Check Privacy Statement".*

The privacy statement details:

- how information provided will be used
- that metadata will be shared with MSD in all circumstances
- that the selfie photo (when applicable), liveness confirmation and passport details will be shared with MSD with the user's consent.
- how to request a copy of information held by DIA.
- how MSD will use information provided by DIA.

The user is also provided a link to the Terms of Use for the OTI which include an agreement to the privacy statement. The user is not able to proceed until they have agreed to the OTI Terms of Use.

At any time whilst using the OTI the user can access the privacy statement through a link at the bottom of the screen.

8.2. User of the service

The first step is for the user to provide details of their passport. The following information is required to be provided as shown in the user's passport:

- passport number
- given names
- surname
- date of birth

Once the passport information has been confirmed to be valid the user is asked to provide a selfie of themselves. The user is advised that they need to provide access to their device's camera to take a photo when prompted. If they do not provide access, then they will not be able to proceed to use the service.

The user is also provided guidelines to aid in the capturing of a selfie photo that can be utilised. When they are ready for the photo to be taken the user selects continue. A countdown is provided and then the photo is taken. During the countdown the user can switch which camera on their device is to be used to ensure the photo is of themselves. The selfie photo is checked to determine it meets the criteria of the service, if the criteria are not met the user can retake the photo. Once there is a successful photo taken it is then displayed to the user who can either accept the photo or retake it as many times as they wish until they are happy with the photo.

The next stage is for a liveness check to be completed. The user is advised that this stage will involve the flashing of lights onto their face and caution should be exercised if they have epilepsy or light sensitivity conditions. When they are ready for the liveness check to be completed the user clicks continue. A video or series of frames lasting three to five seconds is produced as the Colour Light Reflection Liveness (CLR) is completed. If upon evaluation the user has failed the liveness check, they are able to reattempt the liveness check a further two times.

8.3. Metadata

For each use of the OTI metadata about the timing of events of each stage of the process are captured by the OTI. A transaction ID is also collected from MSD when the user is transferred to the OTI. This ID is used to allow MSD and DIA to know they're communicating about the same client for the purposes of that OTI transaction. An OTI ID is also created by DIA which is also shared with MSD. This can be used for requesting a manual check and billing purposes.

8.4. Google Analytics

Google Analytics 360 is used within OTI to track the access and use of the various webpages. This information is collected for the purpose of identifying pain points in the client journey so that improvements can be made. Although this information is collected at an identifiable level it is always used at an aggregate level.

9. Use

9.1. Use of the selfie photo and liveness video

The selfie photo and liveness video will be compared to each other to determine if the individual in the liveness video is:

- alive and
- the same individual as that in the selfie photo.

If the match is confirmed, then this enables DIA to confirm that the individual in the selfie photo is the user of the OTI at that time and request authorisation from the user to share the confirmation with MSD.

The selfie photo and liveness video will not be used by DIA for any purpose other than offering users the ability to confirm their identity to MSD.

9.2. Use of passports information

The passport information provided at the beginning of the process is used to confirm that a unique passport can be identified for the user. At this stage the issuance date of the passport is used to confirm that the passport was issued post 1st January 2004 which is required for the OTI to be utilised.

At the point where the user has completed and passed the liveness check the selfie photo is then compared to the passport photo. This enables the confirmation of the individual's identity to allow the release of confirmation of their passport information under the Identity Information Confirmation Act 2012 (IICA). If the selfie photo does not match the passport photo, then the user is unable to proceed to authorise the sharing of the identified passport with MSD.

9.3. Use for manual checks

In the event of MSD wishing to confirm the identity match of an individual they will contact DIA and provide the transaction ID in question. A member of the OTI Team will then extract from the system the selfie photo and liveness video along with the confirmation of the consent to share the result with MSD. If the user did not consent to share their details with MSD, then no manual check will be completed.

If the user consented to the share, the DIA staff member will then complete a manual assessment of the level of match between the two items based on existing identity proofing procedures used for RealMe verified identities.

If as part of the use of the OTI a passport match was also completed the DIA staff member will then access the passport system and complete a manual assessment of the level of the match between the selfie photo and the user's passport photo in the passport used.

Based on the manual assessments made by the DIA staff member a determination will then be made if the identity is valid. The only information to be provided to MSD will be a confirmation of a successful or unsuccessful match.

9.4. Use of metadata and Google Analytics information

The metadata and Google Analytics information will be used to generate reports in aggregate form about how the OTI service is performing. These will be used by DIA to analyse the performance of the service and identify areas of improvement.

The metadata will also be used in an identifiable form to create the invoices for use of the OTI by MSD. A report will be created by DIA to support reconciliation of the invoice by MSD.

The metadata will also be utilised on an annual basis to allow reporting on the use of the IICA where the selfie has been compared to an individual's passport. This reporting will be at an aggregate level.

9.5. Use by other DIA Identity products

The information collected as part of the MSD instance of OTI is segmented from both other instances of the OTI used for other organisations and from other DIA solutions.

There is no authorised use of the OTI information within the MSD instance in relation to other DIA Identity products. Furthermore, the OTI information is not information that can be shared under the DIA Identity Services AISA.

9.6. Use by third parties

The Daon and Google's contracts with DIA have a requirement that they will not use any DIA data for their own purposes.

10. Accuracy

10.1. Ability to match accurately

The identity binding technology used for OTI is currently implemented in RealMe—there it is demonstrating accuracy rates of approximately 99% over the past three months. The system is weighted towards false negatives rather than false positives to ensure robust evidence of identity.

10.2. Known errors factors

To date no statistical research has been completed on the factors influencing the accuracy rates.

However key known accuracy factors relate to significant changes in face shape. This is impacted by the age of the passport used for reference and the age of the individual (children's faces change significantly). For example, successful identity matching for young adults with expired child passports is lower, given their face shape may have changed significantly since their passport photo was taken.

It is known that skin tone impacts facial contrast across all facial recognition technology, resulting in variable rates of successful biometric templating. However, the rates of successful biometric templating remain consistently high across ethnicities using this technology. Testing in 2019 did find that CLR has variable error rates relating to skin tone, with medium skin tone users having a higher false negative rate than dark skin tone or light skin toned individuals. In all instances, incorrect

results remain under 5%. The algorithm has been improved since then, but new figures are not currently available.

10.3. Impact of errors on users

The OTI project is to create a positive identity gateway for users. There is no adverse impact of a failed biometric. A user can attempt a new session or can use another method to prove their identity to MSD.

11. Disclosure

11.1. Overview of disclosure arrangements

The disclosure arrangements are varied as part of this project. The following table provides an overview of the arrangements which are then further discussed in the following sections:

Item	Legislation	Agreement
Passport confirmation (automated)	Identity Information Confirmation Act	Confirmation Agreement
Metadata	Privacy Act – Advised disclosure within the privacy statement	OTI MOU
Selfie photo	Privacy Act - Consent	OTI MOU
Selfie photo and liveness confirmation (manual investigation)	Privacy Act - Consent	OTI MOU
Passport confirmation (manual investigation)	Privacy Act – Customer Nominated Services AISA	Customer Nominated Services AISA Operating Procedures - MSD
Selfie photo, liveness video or passport details (offence)	Privacy Act	Request under IPP11 (e)
Billing Information	Privacy Act - Consent	OTI MOU

11.2. Disclosure of passport information to a user

When using the service the user has to provide details of an individual's passport. This information must identically match with the information contained on a passport within the passports database. The user is not able to proceed to the next step until a match to a passport has been confirmed. The user has five attempts to provide the passport details before they are unable to use the service.

In normal circumstances the expectation is the user will provide their own passport information. However, if the user provides another individual's information the act of being able to proceed or not to the next stage in the process will confirm the existence of a passport issued after 1st January 2004 matching the passport information provided.

This disclosure alone will not enable the user to masquerade as the other individual to MSD as it is also required that the selfie matches the passport photo prior to any information being disclosed to MSD. However, the confirmation of the passport information to the user may enable them to commit identity related crimes in other circumstances.

11.3. Disclosure of information to MSD with consent

Upon successful completion of the liveness check and the passport match, the user is asked to authorise the sharing of their identity check information with MSD for the purposes of verifying their identity. The user must make an active step to check the consent box before they are able to proceed.

If the user selects to share their results with MSD then DIA provide to MSD the following:

- the transaction number
- confirmation the user passed the liveness check
- the full name
- the date of birth.

The IICA provides authorisation for disclosing the passport information in the form of confirmation of the match. The following passport information will be confirmed to MSD:

- full name
- date of birth
- selfie photo match to the passport photo.

A Confirmation Agreement is currently being consulted on with the Privacy Commissioner as changes to the previously agreed agreement are required due to the slightly different model utilised by the OTI.

The privacy statement details that the disclosure of the details to MSD is at the sole discretion of the user. If the user selects not to share their results with MSD, then no information is provided over and above the metadata relating to the transaction.

MSD will utilise the provided details as part of their process for identity verification. More information is provided within the MSD PHRaE.

11.4. Disclosure of the selfie photo

In the second release the user will be able to additionally authorise the provision of their selfie photo to MSD along with confirmation of their passport details. The user must make an active step to check the additional consent box before they are able to proceed.

The privacy statement details that the disclosure of the selfie photo is at the sole discretion of the user. The user can choose to share their details but not their selfie photo if they wish.

MSD will utilise the selfie photo to identify the user if they visit a Service Centre. If MSD doesn't have the individual's selfie then they will need to show a government issued ID and/or answer some security questions to prove their identity when visiting a Service Centre. More information is provided within the MSD PHRaE.

11.5. Disclosure of metadata

When a user uses the OTI, details of their actions are captured in the metadata. The full details of the metadata will not be released to MSD by DIA. However, they will provide details on a per transaction basis about the time and date and whether during the transaction the user:

- completed the transaction successfully
- had an unsupported browser or device

- exceed the timeout period
- exceeded the number of possible attempted to complete the liveness check
- chose to exit the OTI
- sharing Not authorised
- had an unsuccessful OTI transaction due to failing the liveness check, passport photo match or passport data match.

The disclosure of this information is not optional or controllable by the user if they choose to proceed to use the OTI.

The information is disclosed to MSD to enable MSD to identify how the service is functioning and where any particular pain points are that need to be addressed.

The information is shared at a per transaction level rather than at a summary level to enable MSD to augment the OTI information with other information regarding the client to identify trends and issues relating to specific groups of clients e.g. clients who are applying for a certain benefit are more likely to have an unsupported browser or device.

11.6. Disclosure in the event of investigation by MSD

In the event that MSD wishes to investigate whether the selfie photo, liveness video and passport photo have been correctly matched then MSD will request a manual check by DIA. The user is not required to authorise this additional manual check. A manual check can only be completed where the individual has previously authorised the sharing of their verified identity with MSD.

The outcome of the manual review of the match between the selfie photo, liveness video and passport photo where appropriate will result in DIA advising a confirmation of the existence of a match. If a match does not exist no further information will be provided as to the differences and the passport photo will not be provided.

The privacy statement along with the user's original authorisation will provide the authorisation for the disclosure of the confirmation of the selfie photo and liveness video match. The Customer Nominated Services AISA provides authorisation for disclosing the passport information in the form of confirmation of the match to MSD. This is for the purpose (AISA para 4.2.c) of ensuring that an individual applying for or utilising MSD Services is not required to provide identity and life event records that DIA holds, in this case their passport.

11.7. Disclosure in the event of a suspected offence

MSD can confirm the individual's identity is required:

- to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences
- for the enforcement of a law imposing a pecuniary penalty
- for the protection of the public revenue
- for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation).

MSD will make a request in writing to DIA for release of the selfie photo, liveness video and passport information as required under the exceptions to the Privacy Act under IPP 11 (e). DIA's standard process for handling requests for disclosure under the Privacy Act will be utilised.

11.8. Disclosure of Google Analytics information

The information contained within Google Analytics 360 will not be disclosed in a form that allows identification of an individual user. However aggregate level reporting regarding use of the service by MSD clients will be provided to MSD. This is provided for the purpose of understanding how the OTI service is performing.

11.9. Disclosure for billing purposes

A report containing the transaction ID and the date verified will be provided to MSD by DIA on a regular basis. This report contains a subset of the information provided as part of confirming an identity. Only users who authorised sharing of their information with MSD will be detailed within the report.

The report is utilised by MSD to enable the billing amounts to be reconciled against successful verifications.

11.10. Disclosure by Daon

The Daon Master Services Agreement requires Daon to only disclose confidential information to DIA employees, agents and contractors as required and for reasonably necessary purposes. Daon by default do not have access to any information within OTI as the solution is hosted onsite at DIA. The only scenario where they may gain access is when a defect occurs and DIA request support. Daon must keep the information confidential in all other circumstances. The exception to this is where the disclosure is:

- required by law
- to the courts of any competent jurisdiction
- to any government regulatory or financial authority.

Prior to making a disclosure Daon must consult with DIA.

11.11. Disclosures to law enforcement agencies

DIA may voluntarily disclose, or be compelled to disclose, personal information in OTI to law enforcement agencies such as NZ Police or the Serious Fraud Office. This would occur via the 'maintenance of the law' exception in the Privacy Act for voluntary disclosures. Compulsory disclosures occur via Production Orders under the Search and Surveillance Act 2012 and court orders.

DIA's current process for disclosing to law enforcement agencies will continue to be utilised.

11.12. Disclosures relating to Privacy Act requests

DIA's already established process for handling Privacy Act requests will continue to be utilised. If requested both the selfie photo and liveness video will be released under a Privacy Act request.

12. Security

A security risk assessment, penetration test and Certification and Accreditation (C&A) is currently underway for the OTI.

13. Retention and Disposal

13.1. Selfie photos, videos and liveness confirmation

The retention of the selfie photos and liveness confirmation depends on the outcome of the check and if the individual authorised for the information to be shared with MSD.

If the information has been shared with MSD then the selfie photo, video and liveness confirmation will be retained for a period of six months within the Daon solution. The information is retained for this period to enable MSD to query DIA in the event of an investigation or suspected offence. After six months the selfie photo, video and liveness confirmation will be securely disposed.

If the user does not share their information with MSD or is unable to successfully complete the liveness confirmation or passport match then the selfie photo, video and liveness confirmation as appropriate will not be retained as standard. However, DIA may choose to retain these items for up to one month if investigating issues around the performance of the OTI.

There is currently no Disposal Authority under the Public Records Act that explicitly details the handling of the OTI information by DIA.

13.2. Metadata

The metadata relating to both successful and unsuccessful confirmations will be held for 13 months before being securely disposed of. The information is retained for this period to allow year on year analysis of the OTI and also to enable legislative reporting requirements to be met.

There is currently no Disposal Authority under the Public Records Act that explicitly details the handling of the OTI information.

13.3. Google Analytics

The Google Analytics information is retained for 13 months before being securely disposed of. The information is retained for this period to allow year on year analysis of the OTI usage.

There is currently no Disposal Authority under the Public Records Act that explicitly details the handling of the Google Analytics information at DIA.

13.4. Information held by Daon

Upon termination of the Daon Master Services Agreement they are required to return or destroy all confidential information if requested in writing by DIA. Upon completion of such a request Daon will issue a certificate to DIA stating the actions taken.

14. Ongoing Management

14.1. Privacy and security breaches

In the event of a privacy or security breach the standard DIA processes for handling a breach and notifying the Office of the Privacy Commissioner and impacted users, if required, will be followed.

In the event of Daon becoming aware of a potential or actual privacy or security breach they are required in accordance with the Master Services Agreement to notify DIA as soon as possible. Daon are also required to cooperate in the prevention or limitation of the breach.

14.2. Correction of personal information

DIA's existing Privacy Act request process will continue to be utilised for the correction of information. However, due to the nature of the OTI it is unlikely that any requested corrections will be made to the information held within the OTI as it is accurate at the time of collection.

14.3. Change management

MSD and DIA will collaboratively work together to develop the roadmap for the OTI. This collaboration will be formalised through a Memorandum of Understanding between MSD and DIA prior to the launch of the OTI.

In the event of changes being made this PIA will be updated to reflect any changes prior to the release of the changes into production.

15. Risk Assessment

The following table details the risks identified as a result of the use of the OTI from a DIA perspective:

Ref	Description	IPP	Existing planned controls	Inherent risk rating			Recommended mitigations	Residual risk rating		
				Likelihood	Consequence	Rating		Likelihood	Consequence	Rating
R01	Selfie photos, liveness videos and metadata are kept for longer than required.	9	• Selfie photos and liveness videos to be kept for 6 months. • Metadata and Google Analytics to be kept for 13 months.	Almost Certain	Moderate	20	• A01 - Review with MSD the requirement to complete manual confirmations for 6 months to see if it can be reduced.	Improbable	Moderate	6
R02	Reporting of use of the manual confirmation is unavailable as required under the Customer Nominated Services AISA due to a lack of developed procedures.	11	• Operating procedures under the Customer Nominated Services AISA defining the process for manual confirmations.	Almost Certain	Moderate	20	• A02 - Develop work instructions for DIA staff processing the manual queries.	Improbable	Moderate	6
R03	Due to an incorrect failed match by the OTI certain people can't use the service to verify their identity.	8	• Known understanding of areas of challenge. • Restriction to passports issued after 1st January 2004. • Requirement for users to be over 18. • Advisement to users about light conditions.	Almost Certain	Minor	16	• A03 - Consider reducing the maximum age of a passport for young adults. • A04 - Manually review a series of failed matches to determine the rate of false negatives and influencing factors. • A05 - Work with Daon to refine the algorithms based on the findings of the review of failed matches.	Almost Certain	Minimal	11
R04	The OTI is non-compliant with GDPR and other overseas legislation.	Other	• Review of key applicable legislation. • Staggered launch to outside of New Zealand.	Possible	Moderate	13	• A06 - Review solution and Daon for GDPR compliance. • A07 - Inclusion of a Data Processing Agreement with Daon.	Possible but Unlikely	Moderate	9
R05	More information is provided to MSD in response to a manual query request than authorised due to a lack of developed procedures.	11	• Agreement to only provide confirmation or denial of match. • Operating procedures under the Customer Nominated Services AISA defining the process for manual confirmations.	Highly Probable	Minor	12	• A02 - Develop work instructions for DIA staff processing the manual queries.	Improbable	Minor	3
R06	Information gathered and held by the OTI is insecure resulting in a privacy breach.	5	• Secure coding methods used to design the solution. • Industry leading vendor used. • Security considered as part of the design. • Completion of a penetration test. • Completion of a Certification and Accreditation.	Improbable	Significant	10		Improbable	Significant	10
R07	The legal basis is challenged around the disclosure of passport confirmation to MSD for OTI validations.	11	• Legal advice received about applicability of the IICA. • Development of a Confirmation	Improbable	Significant	10	• A08 - Introduce legislative change to the IICA to confirm applicability where the individual provides their identity information direct to DIA.	Improbable	Minimal	1

Ref	Description	IPP	Existing planned controls	Inherent risk rating			Recommended mitigations	Residual risk rating		
				Likelihood	Consequence	Rating		Likelihood	Consequence	Rating
			Agreement. • Consultation with the Office of the Privacy Commissioner.							
R08	Confirmation of an individual's passport is provided to a user who is not the passport holder.	11	• Limit to five attempts to provide passport information. • 100% match required. • No evidence of what information does not match. • Limited passport information confirmed.	Possible	Minor	8	• A09 - Reduce the number of possible attempts to provide passport details. • A10 - Move the screen to input passport details after the selfie liveness check so the identity of the user is captured. • A11 - Include in the terms of service a requirement to only provide your own information.	Possible but unlikely	Minor	5
R09	Privacy Act requests relating to the selfie photo or video are sent to MSD rather than DIA.	6, 7	• Privacy statement details DIA as the collector of information and provides DIA contact details. • Process to transfer requests under the Privacy Act.	Highly Probable	Minimal	7	• A12 - Remove co-branding of the OTI service.	Possible	Minimal	4
R10	An incorrect match is made between the individual's selfie photo, liveness check and passport photo resulting in an incorrect identity confirmation being provided to MSD.	8	• System leans towards false negative rather than false positive by design.	Possibly but Unlikely	Minimal	5	• A13 - Manually review a series of matches to determine the rate of false positives and influencing factors. • A14 - Work with Daon to refine the algorithms based on the findings of the review of false positives.	Possible but Unlikely	Minimal	5

16. Recommendations to Minimise Privacy Impact

Ref	Recommendation	Agreed Y/N
A01	Review with MSD the requirement to complete manual confirmations for 6 months to see if it can be reduced.	
A02	Develop work instructions for DIA staff processing the manual queries.	
A03	Consider reducing the maximum age of a passport for young adults.	
A04	Manually review a series of failed matches to determine the rate of false negatives and influencing factors.	
A05	Work with Daon to refine the algorithms based on the findings of the review of failed matches.	
A06	Review solution and Daon for GDPR compliance.	
A07	Inclusion of a Data Processing Agreement with Daon.	
A08	Introduce legislative change to the IICA to confirm applicability where the individual provides their identity information direct to DIA.	
A09	Reduce the number of possible attempts to provide passport details.	
A10	Move the screen to input passport details after the selfie liveness check so the identity of the user is captured.	
A11	Include in the terms of service a requirement to only provide your own information.	
A12	Remove co-branding of the OTI service.	
A13	Manually review a series of matches to determine the rate of false positives and influencing factors.	
A14	Work with Daon to refine the algorithms based on the findings of the review of false positives.	

17. Authorisation

Authorised by	Signature	Date
Russell Burnard		

Forward a copy of the signed document to privacy@dia.govt.nz.