Australian Government

Attorney-General's Department

Evaluation of the Prototype Document Verification Service

November 2006

Table of Contents

Executive Summary 1
1. PURPOSE 2
2. THE pDVS 3
2.1. Overview of the pDVS 3
2.2. The prototype approach 3
2.3. Prototype design and process 3
3. THE EVALUATION PROCESS 7
3.1. Evaluation Goals 7
3.2. The data collection process 7
4. FINDINGS 9
4.1. DFAT results 9
4.2. DIMA results 10
4.3. Combined agency results 10
4.4. Reasons for non-verification 11
4.5. Adjusted verification rates 13
4.6. Findings related to the information technology employed 14
4.7. Reviewing privacy impacts 14
5. CONCLUSIONS 16
5.1. Assessment of the pDVS 16
Attachment A 17
Attachment B 19
Attachment C 20

Executive Summary

On 14 April 2005, the Australian Government announced that it would develop a national strategy to improve identity security, combat identity crime and protect the identity of Australians from being used for illegal purposes. In the 2005-06 Budget the Government allocated funding to the strategy, which included a pilot project involving a prototype Document Verification Service (pDVS) to check the accuracy and validity of key proof-of-identity documents.

In September 2005, the Council of Australian Governments (COAG) agreed to the development and implementation of the National Identity Security Strategy. COAG also specified that the development and implementation of a national document verification service to combat the misuse of false and stolen identities would be a key component of the Strategy.

The pDVS was designed to operate online and in real time and to explore the technical and operational issues associated with a document verification service. The pDVS would help inform the development and implementation of a national verification service.

The pDVS operated from early February until 30 June 2006 allowing the Department of Foreign Affairs and Trade (DFAT) and the Department of Immigration and Multicultural Affairs (DIMA) to check proof of identity details offered by individuals seeking Australian passports and citizenship. During that period the pDVS was used for 51,551[1] separate verifications to check the details appearing on birth certificates, citizenship certificates, driver's licences and passports. The pDVS did not detect any false documents.

The overall verification rate associated with these queries was approximately 90%. Such verification failures are mostly attributable either to inconsistencies between the details recorded on the document and the electronic record, or to the document details being inaccurately recorded by applicants on application forms. Excluding these instances alone would raise the verification rate to approximately 96% and the experience of the pDVS has identified corrective action that can be undertaken.

The pDVS was only able to proceed because of the efforts and assistance of the agencies involved in the pilot. In particular, acknowledgement needs to be made to Centrelink, DIMA, DFAT, Austroads and the NSW Registry of Births, Deaths & Marriages.

Additional acknowledgement also needs to be made to the Office of the Privacy Commissioner for the invaluable advice and assistance the Office provided in relation to the pDVS and the National Identity Security Strategy.

[1] The figure 51,551 was calculated by combining the number of documents input by DFAT (51,118) with the documents input by DIMA (433)

1. PURPOSE

The pDVS was developed to test the practicality and effectiveness of online, real-time document verification processes.

In September 2005, the Council of Australian Governments (COAG) agreed to the development and implementation of a national document verification service to combat the misuse of false and stolen identities as part of the National Identity Security Strategy.

This paper evaluates the operation of the prototype, reporting on the results of the verifications conducted through the pDVS, why some documents did not verify, the reliability of the technology used for the prototype, and any operational constraints identified. Its findings will assist the design, cost and build of the full-scale national DVS whilst also complementing other work being undertaken on the development of the National Identity Security Strategy.

2. THE pDVS

2.1. Overview of the pDVS

The pDVS is a computerised system which allows the online verification of documents presented as proof of identity (POI).

When verifying a document, the pDVS is able to confirm that:

- the document was issued by the issuing agency specified on its face
- the details recorded on the document correspond to those held in the issuing agency's register, and
- certain types of documents have not been superseded or cancelled.

The pDVS was tested by DFAT and DIMA in verifying POI documents presented to them by applicants enrolling for an Australian passport or requesting a certificate of evidence of Australian citizenship respectively. DFAT and DIMA participated as querying agencies and as document issuing agencies in their own right. The IT infrastructure for the pDVS was constructed and maintained by Centrelink.

In the pDVS, the POI documents verified and their issuing agencies were:

- birth certificates – NSW and ACT Registries of Births, Deaths and Marriages (BDMs)
- citizenship certificates – DIMA
- driver's licences – NSW and ACT Road Transport Authorities, and
- Australian passports – DFAT.

2.2. The prototype approach

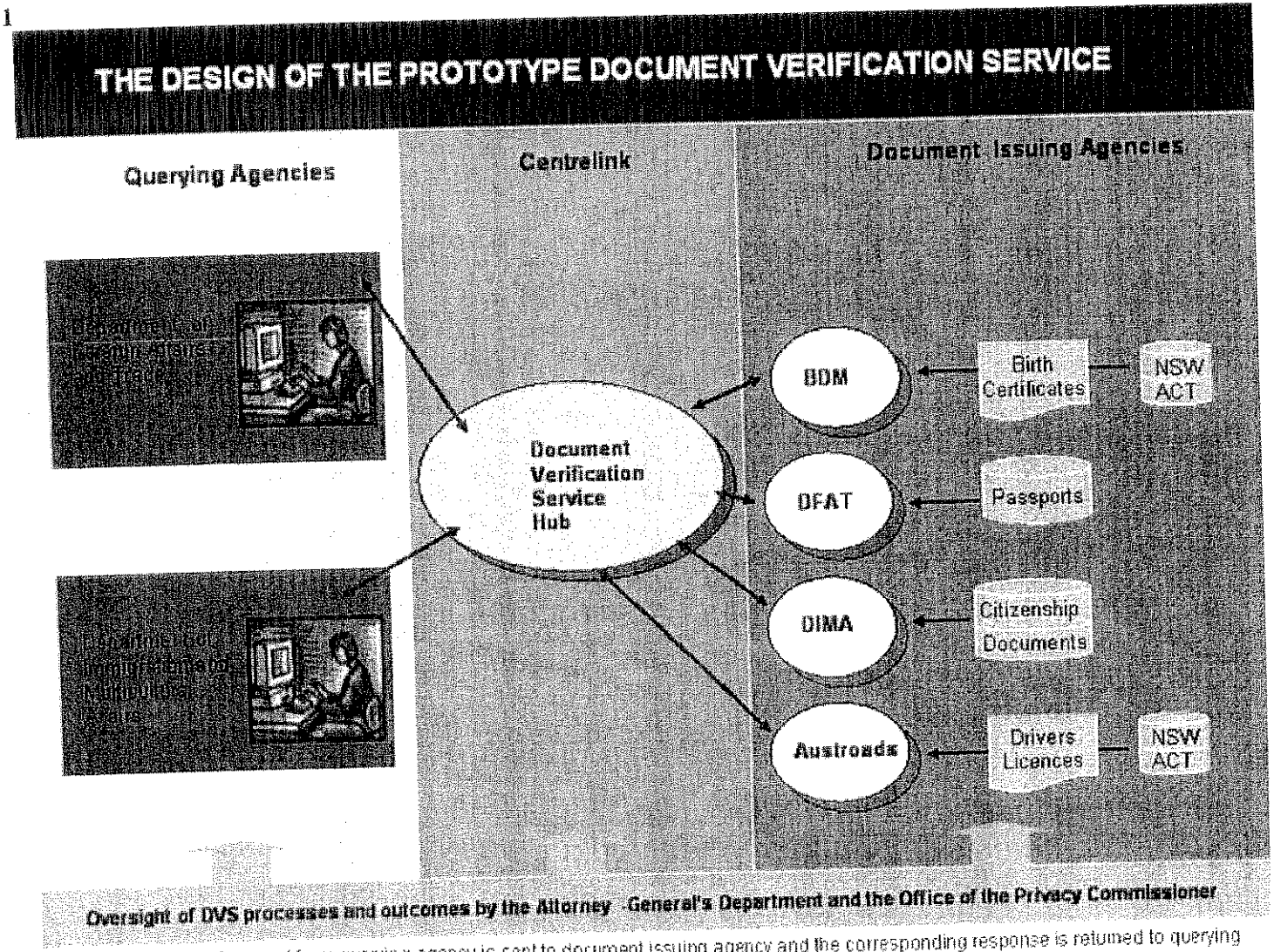
The goal in pursuing a prototype was to test conceptual presumptions about the effectiveness of online, real-time document verification in a real world setting. That effectiveness was assessed in terms of the extent to which relevant POI documents in use in the community could be verified in an automated and cost effective manner against the registration databases held by the document issuing agencies.

Additionally, the prototype approach allowed the exploration of technical and operational issues associated with implementing and operating a secure, online and real-time system. It also gave participating agencies an opportunity to assess the value of a document verification service to them.

2.3. Prototype design and process

The various components of the pDVS and their interaction are depicted in Diagram 1.

Diagram 1



Arrows indicate that request from querying agency is sent to document issuing agency and the corresponding response is returned to querying agency

From a human perspective, the steps involved in the verification process were:

- an individual presented their POI documents to DFAT or DIMA in support of their application for enrolment
- the applicant authorised the agency to undertake checks to verify the documents they presented
- the agency used the pDVS to check the document details and generated a verification request (details to be verified including full name, date of birth, official registration number or other identifying details of the document), and
- in normal circumstances a response to the verification request was returned in a couple of seconds.

As an IT process, the steps were:

- the verification check, or query, took the form of an electronic message which was sent as a package of data from the agency's computer system, via secure electronic communications pathways, to an electronic intermediary/processor called the pDVS Hub
- the pDVS Hub registered the incoming query by assigning a virtual reference number (VRN) and associated certain other transactional data (metadata) with that VRN (eg time of the query, electronic notification of the querying party)
- the pDVS Hub gave the data package a second VRN, for the use of the document issuing agency, and referred the query to the computer system of the relevant document issuing agency
- the computer system of the document issuing agency consulted the relevant database, established if the query matched the particular data fields, and returned a "YES", "NO" or "ERROR" response to the pDVS Hub, that communication was identified with the second VRN
- the pDVS Hub made a connection between the two VRNs, and
- the pDVS Hub communicated the "YES", "NO" or "ERROR" response to the querying agency's computer system, identified by the first VRN.

ACT and NSW BDM Registries verified the birth certificate details received in queries through the pDVS Hub by directing them to their Certificate Validation Service (CVS). The verification results were then returned through the pDVS Hub to the agency initiating the query. Centrelink built, implemented and managed the IT service hub for the pDVS.

It should be noted that Austroads and the National Exchange of Vehicle and Driver Information System (NEVDIS) acted as the clearing house for queries involving NSW and ACT driver's licenses. NEVDIS allows for real time access to, and exchange of driver's licence information between States and Territories. The NSW and ACT Road Transport Authorities did not engage directly with the pDVS Hub.

Similarly, verification of ACT and NSW birth certificate details was directed through the CVS operated collectively by BDM Registries.

Although it was intended that VicRoads and the Victorian BDM Registry participate in the pDVS, an appropriate Memoranda of Understanding (MOU) with those agencies was unable to be finalised within the necessary timeframe.

DFAT participated through selecting passport applications approved in the two weeks preceding the test period and conducting a subsequent verification through the pDVS. DIMA was able to implement the pDVS in its workplaces and replicate the real-world situation in which documents were verified online and in real-time.

MOU were agreed with Centrelink, DFAT, DIMA, the NSW BDM Registry, ACT BDM Registry and Austroads for building and operating the pDVS.

A diagram showing the organisational arrangements for pDVS is provided at Attachment B.

3. THE EVALUATION PROCESS

3.1. Evaluation Goals

The evaluation of the pDVS has focussed on two particular areas with the greatest relevance for the participating agencies in the pDVS and for the design and implementation of the national DVS.

Testing the effectiveness of online processes

The primary goal of the prototype was to test the effectiveness of online document verification processes by demonstrating that verifications could be:

- conducted in an automated fashion
- performed in a real-time and online manner, and
- fast and reliable.

Testing the reliability of technology used

It was of key importance that the computer system infrastructure underpinning the deployment of the pDVS created not only a secure environment for processing the verifications but also assured a high level of availability. Accordingly, the pDVS was built upon dedicated communication lines and ICON links which ensured security as well as the ability to handle large numbers of requests.

An estimate of the maximum capacity of the pDVS to handle transactions was also of interest. A series of tests was devised to simulate heavy transactional loads. These tests indicated that the pDVS Hub was capable of supporting a load of up to 3 million transactions per day. It was not possible however to conduct load testing of the systems employed by the document issuing authorities. A detailed description of technical features associated with the pDVS Hub is provided at Attachment C.

An additional exercise was undertaken to ascertain if the flow of information associated with any particular verification query could be readily reconstructed end-to-end sometime after the actual event. This involved selecting a small sample of completed verifications to simulate, for example, a Freedom of Information (FOI) request lodged with the document issuing agency. The aim was to identify the actual logon or officer who initiated the pDVS request relating to a particular document. This exercise was successfully undertaken through the joint involvement of the three agencies who participated in each of the selected verifications. That is, the agency seeking to verify the document, the agency which issued the document and Centrelink as the manager of the pDVS Hub.

3.2. The data collection process

Centrelink collected data on all verification queries undertaken through the pDVS Hub in daily transaction logs for the period 6 February 2006 to 30 June 2006. At the conclusion of this pilot, the daily logs generated over the period were first combined to create a dataset of all queries and then divided on the basis of whether they were for DFAT or DIMA verifications. The two resulting datasets were subsequently

sorted by the document type (i.e. Australian passport, Citizenship Certificate, birth certificate or driver's licence) and the verification result (i.e. "Yes", "No" or "Error") to provide the data for the statistical analysis conducted in this evaluation.

For verification queries which failed to verify (non-verifications), additional data was collected from DFAT and DIMA to explain the reason the non-verifications occurred. As a further quality control measure, a small sample of positive verifications were also selected and checked in order to confirm the accuracy of the result.

It should be noted that each participating agency maintained records of all transactions received from and returned to the pDVS by their agency.

4. FINDINGS

4.1. DFAT results

DFAT selected cases for the pDVS by extracting POI document data from passport applications which had been approved during the two week period immediately preceding the selection date. DFAT employ a general practice of scanning passport application forms and identifying and extracting the relevant POI document data from each application. This data was then stored electronically to provide the input for the pDVS.

The scanning process was on occasion imperfect, introducing inaccuracies for some records. Since it is not intended that the national DVS would involve scanning, these errors were removed from the overall sample prior to the analysis of the verification results. An estimate was made of the extent to which corrupted records could be attributed to the scanning process by comparing a sub-sample of the scanned POI document data against the associated application forms. This approach enabled the statistical extrapolation of the number of documents of each type likely to be affected by scanning problems, enabling their overall impact to be eliminated from the verification results (these estimates are shown in Table 1).

Table 1: DFAT: POI document data scanned from applications

Document Type	Number Scanned	Scanning Problems (estimate)	Number for Verification
Birth Certificate	16,860	771	16,089
Citizenship Certificates	18,113	2,037	16,076
Driver's Licence	16,145	1,848	14,297
Total	51,118	4,656	46,462

The outcomes of the document verifications conducted through the pDVS by DFAT are summarised in Table 2 which shows that 89% of all documents checked by DFAT through the pDVS were verified. Of the 11% of queries overall that were not verified, 16% were of driver's licenses, 14% birth certificates and 2% citizenship certificates.

Table 2: DFAT: Results of the verification queries

Document Type	Verified		Not Verified		Total
	Number	(%)	Number	(%)	
Birth Certificate	13,778	(86)	2,311	(14)	16,089
Citizenship Certificates	15,744	(98)	332	(2)	16,076
Driver's Licence	12,038	(84)	2,259	(16)	14,297
Total	**41,560**	**(89)**	**4,902**	**(11)**	**46,462**

The non-verifications were then subject to examination by DFAT to identify the underlying reasons why the document data did not verify. This work was supported by extracting a sample of records for detailed follow-up. The result of this analysis is reported later in this report.

4.2. DIMA results

DIMA were able to incorporate the pDVS into their usual operational face-to-face enrolment process. DIMA reported that this integration of the pDVS was very successful, enabling staff to successfully verify the POI documents presented without recourse to more expensive and slower manual verification processes.

Appropriate liaison arrangements were instigated between DIMA and the relevant document issuing authority to facilitate the manual checking of documents which failed to verify. These arrangements were necessary to ensure DIMA could be assured of the authenticity of a suspect document and to ascertain the specific reason why the document did not verify through the pDVS. The need for an effective and efficient manual follow-up process proved valuable to the operation of the pDVS.

At the outset it should be noted that the only document type verified by DIMA in significant numbers was the driver's licence. This occurred because no individuals in the sample of applicants requiring evidence of citizenship were born in Australia and additionally, only two presented an Australian passport. Reference to Table 3 shows that, of the total of 433 POI documents checked by DIMA, all but two of these were for Australian driver's licences.

Table 3: DIMA: Results of the verification queries

Document Type	Verified		Not-Verified		Total
	Number	(%)	Number	(%)	
Birth Certificate	0	(0)	0	(0)	0
Driver's Licence	384	(89)	47	(11)	431
Aust Passport	2	(100)	0	(0)	2
Total	**386**	**(89)**	47	**(11)**	**433**

DIMA readily verified 89% of the 433 POI documents presented through the pDVS. However, it is worth noting that 52 of these were not verified through the initial query due to the DIMA pDVS operator incorrectly inputting the POI document details. In such cases the operator would as a matter of course re-submit the query in order to guard against the occurrence of data entry errors. When the operator re-submitted the query to the pDVS with the correct details the document was verified.

4.3. Combined agency results

The total number of POI documents checked through the pDVS was 46,895[2], composed of Australian birth certificates, citizenship certificates, driver's licences and passports. The combined agency verification rate for all documents was 89.5% (see Table 4).

[2] The figure 46,895 was calculated by combining the revised number of DFAT verifications (46,462) with the DIMA verifications (433)

Table 4: Combined agency results of the verification queries

Document Type	Verified		Not-Verified		Total
	Number	(%)	Number	(%)	
Birth Certificate	13,778	(85.6)	2,311	(14.4)	16,089
Citizenship Certificate	15,744	(98.0)	332	(2.0)	16,076
Driver's Licence	12,422	(84.3)	2,306	(15.7)	14,728
Aust Passport	2	(100)	0	(0)	2
Total	**41,946**	**(89.5)**	**4,949**	**(10.5)**	**46,895**

4.4. Reasons for non-verification

DFAT and DIMA undertook detailed examination of those pDVS queries of POI documents that did not verify in order to satisfy themselves that:

- the details recorded on the document aligned with the document issuer's electronic record, and
- the details had been recorded correctly to the pDVS.

Where the above factors were confirmed, the reasons why documents had failed to verify were documented.

The reasons identified for non-verification for each particular document type along with its relative incidence are listed in Table 5.

Table 5: Reasons for non-verification by Document Type

Document Type	Reason for non-verification	Incidence (%)
Birth Certificate	Change of format for displaying registration number led to incorrect details recorded on passport application	95
	Courthouse issued a certificate having different registration number to that recorded in the register	5
Driver's Licence	First name and/or middle name did not match	46
	Licence number with incorrect prefix	40
	Incorrect licence details recorded on passport application	14
Australian Citizenship Certificate	Incorrect certificate number recorded on passport application	100

In all cases the non-verifications were a result of some details on a legitimate document not according with the electronic record held by the document issuing agency. On occasion more than one data item on the document (eg multiple components of first name, middle name and surname) may have failed to correlate.

No instances of false POI documents were detected in the samples verified through the pDVS, although in a small number of cases the document was no longer current.

By far the most common reason for the non-verification of birth and citizenship certificates was due to confusion as to what represented the official document registration number, with the passport applicant quoting the wrong number on to the DFAT passport application form. Since the actual POI documents were not electronically verified at the enrolment interview stage (but at a later date after the data had been scanned and input to the passport processing system), these errors were not initially detected.

Of particular importance in this regard are the errors which arose in relation to the verification of the birth certificate registration number. Specific issues relating to each document type are addressed below.

Birth Certificates

Reference to Table 5 shows that 95% of the birth certificates which failed to verify were directly attributable to a change occurring in the format in which the number was displayed on the certificate. The year of birth is now often presented as part of the registration number. For example, NSW's electronic birth register records a certificate with the number of 123456, but the certificate itself presents the number as 123456/1992 (note the additional '1992" digits). A pDVS query on the extended certificate number would not be verified. It appears that this problem is isolated to certificates issued to persons born after 1991. Rectification of this inconsistency would reduce the non-verification rate associated with birth certificates from 14% to 1% in those jurisdictions which participated in the pilot. Consequently an overall verification rate of 99% could be expected for birth certificates once this problem was corrected.

Driver's Licences

The reasons for non-verification of driver's licences were due to some additional factors which are listed in Table 5. The single largest cause (46% of non-verified documents) was due to mismatches between the first names/middle names displayed on the licence and those recorded electronically. Although the licences are genuine the detail and format of names printed on the licence are not consistent with the details stored on NEVDIS. The differences appear to have been caused by the use of preferred names, use of middle initials rather than middle names, and the amount of room available on the licence to print the driver's name.

As with birth certificates, problems arose because some licences did not match. Reasons for this included:

- the driver's licence card number being confused with the licence number
- the jurisdiction being incorrectly recorded, or
- the parent's licence number being recorded on a child's passport application.

One further difficulty with licence numbers is that some driver's licences include superfluous digits, in the form of leading zeros, prefixing the registration number displayed on the face of the licence. These digits were not recorded on the electronic record and the resultant inconsistency between the numbers led to them not matching. This particular inconsistency in the recording of licence numbers contributed to 40% of the non-verified driver's licences encountered.

DIMA became aware of this inconsistency early in the project and addressed it by adjusting their data entry practices to omit leading zeros from driver's licence numbers when inputting to the pDVS. This work practice enabled the verification of driver's licences that would have otherwise returned a non-verification response and resulted in DIMA eliminating this aspect as a reason for the non-verification of licences. Accordingly the driver's licence non-verification rate for DIMA is significantly lower at 11% than the 16% found by DFAT who contended with the problem caused by the extraneous zero digits. Adjusting to exclude this problem, the overall non-verification rate for driver's licences is estimated at 7.5%. Correcting for the 'leading zero' issue would be a straight-forward matter for a national DVS.

Citizenship Certificate

The reason that citizenship certificates failed to verify was due to the incorrect certificate number being recorded by the passport applicant on the DFAT passport application form.

Although all Australian Citizenship certificates have a 'stock number', which is the document serial number displayed on the certificate, its format has changed over time. This sometimes has led to confusion and consequent quotation of the wrong number by individuals. It is reasonable to suggest that errors of this type could be avoided in the national DVS where trained staff would be checking the citizenship certificate details through the DVS at the enrolment interview.

4.5. Adjusted verification rates

As the previous point suggests, the non-verification figure in Table 4 for each document type overstates the extent to which legitimate documents were not verified. This was predominantly due to variations between the details displayed on the face of the document and the underlying electronic record mismatching and therefore causing non-verification, and the enrolling applicant transcribing incorrect document details to an application form which were subsequently input to the pDVS.

Elimination of these two factors as potential contributors to legitimate documents failing to verify will result in substantially higher verification rates than those shown in Table 4. Assuming these factors can be addressed and their effect eliminated from a fully functioning national DVS, we estimate the overall verification rates would be those shown in Table 6 below.

Table 6: Adjusted verification / non-verification rates

Document Type	Verified (%)	Not-Verified (%)
Birth Certificate	99	1
Citizenship Certificate	100	0
Driver's Licence	92.5	7.5
Aust Passport	100	0

4.6. Findings related to the information technology employed

Centrelink's approach when building the pDVS Hub was to implement a hybrid system incorporating a combination of the latest technology where required and also utilising existing facilities available in the participating agencies.

The findings from the pilot showed that:

- it is important that the DVS Hub can accommodate the diverse range of technological infrastructure in use in relevant government agencies, and
- the use of dedicated links and communication protocols between the participating agencies must be reliable technologies (the pDVS had a connection down time only once).

The matching rules specified for the prototype were designed to enable an exact comparison of the information printed on the document with the electronic details of the document held by the document issuing agency. Of course, this provided no flexibility in comparing the data items – they either matched exactly with each other or they did not. It may be necessary to consider less rigorous rules where appropriate. This would assist those issuing agencies which are concerned about the frequency of false negatives and the detrimental affect on their workload if a substantial increase in the manual follow up of non-verifications was to occur.

4.7. Reviewing privacy impacts

A draft Privacy Impact Assessment (PIA) was compiled in the early stages of the development of the pDVS and continually updated and enhanced during the progress of the pilot. This Evaluation Report can therefore be read in conjunction with the final version of the PIA on the pDVS.

In summary, the pDVS complied with the Information Privacy Principles under the *Privacy Act 1988* (Cth) (Privacy Act) and relevant state and territory regimes and a number of impacts were noted:

- *Personal information*: The personal information collected by participating agencies and sent through the DVS hub for verification by document issuing agencies took place in accordance with current agency practices.
- *Purpose*: The pDVS demonstrated that the system is capable of reducing current handling and exposure of personal information by agencies and will ensure a consistent set of processes and standards are used.
- *Consent*: The prototype DVS verified sample identifying documents from participating agencies. In accordance with standard agency practices, general consent to the use of an individual's personal information for proof of identity purposes occurred at the point of application.
- *Security*: As a general rule, security standards should be appropriate to the potential harm that might occur from a privacy breach. Protection of data through the DVS Hub is ensured through a secure pathway and by the assignment of a VRN to the incoming/outgoing enquiries followed by an automated verification response. Agencies participating in the DVS project currently verify proof of identity documents using both manual and automated

communications with document issuing agencies. The pDVS was accessed and administered only by authorised staff within participating agencies.

- *Data quality*: The DVS Hub processes only personal information that is relevant to the purpose for which it is collected by participating agencies. Data may only be retained by the hub for a short period in the event of a system error. During the prototype phase of the DVS project, data on verification transactions were logged for statistical purposes without access to, or inclusion of, personal information.

5. CONCLUSIONS

5.1. Assessment of the pDVS

The 2005-06 Budget provided funding to develop and operate the prototype. The pDVS was a cost effective means of demonstrating that the document verification concept was viable as well as identifying details which require resolution when building the national DVS.

The pDVS demonstrated that document verification can be achieved in both an automated online manner and in real-time. Additionally, the pDVS worked well with existing operational processes. In most cases, the verification results were provided by the pDVS within a few seconds.

The prototype has identified the major reasons why, for a small percentage of legitimate documents, the verification query returned a 'not verified' response. This will allow techniques to be developed to lessen the incidence of non-verifications in the proposed national DVS. The integrity of privacy and security protections were maintained throughout the pDVS.

The pDVS system was built within the specified timeframe, established the 'proof of concept' and performed IT testings. The joint working group operated successfully despite differences in IT systems, formats and approaches.

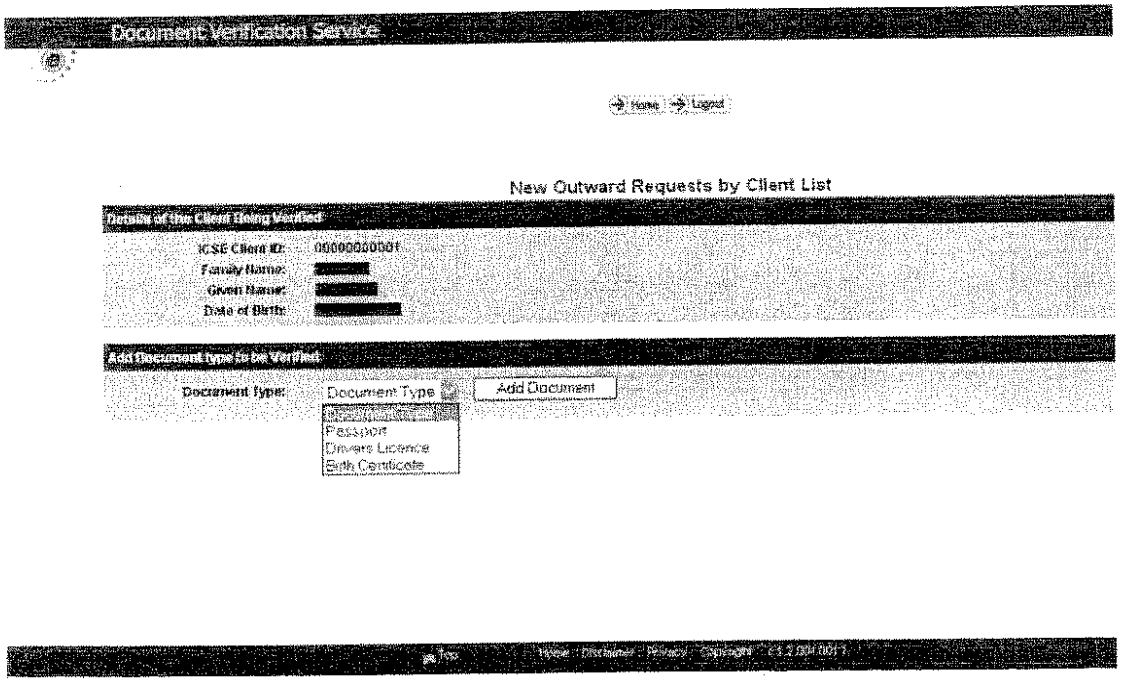
The pDVS has demonstrated how agencies enrolment processes can be strengthened by the introduction and integration of document verification.

Attachment A

pDVS SCREEN SHOTS

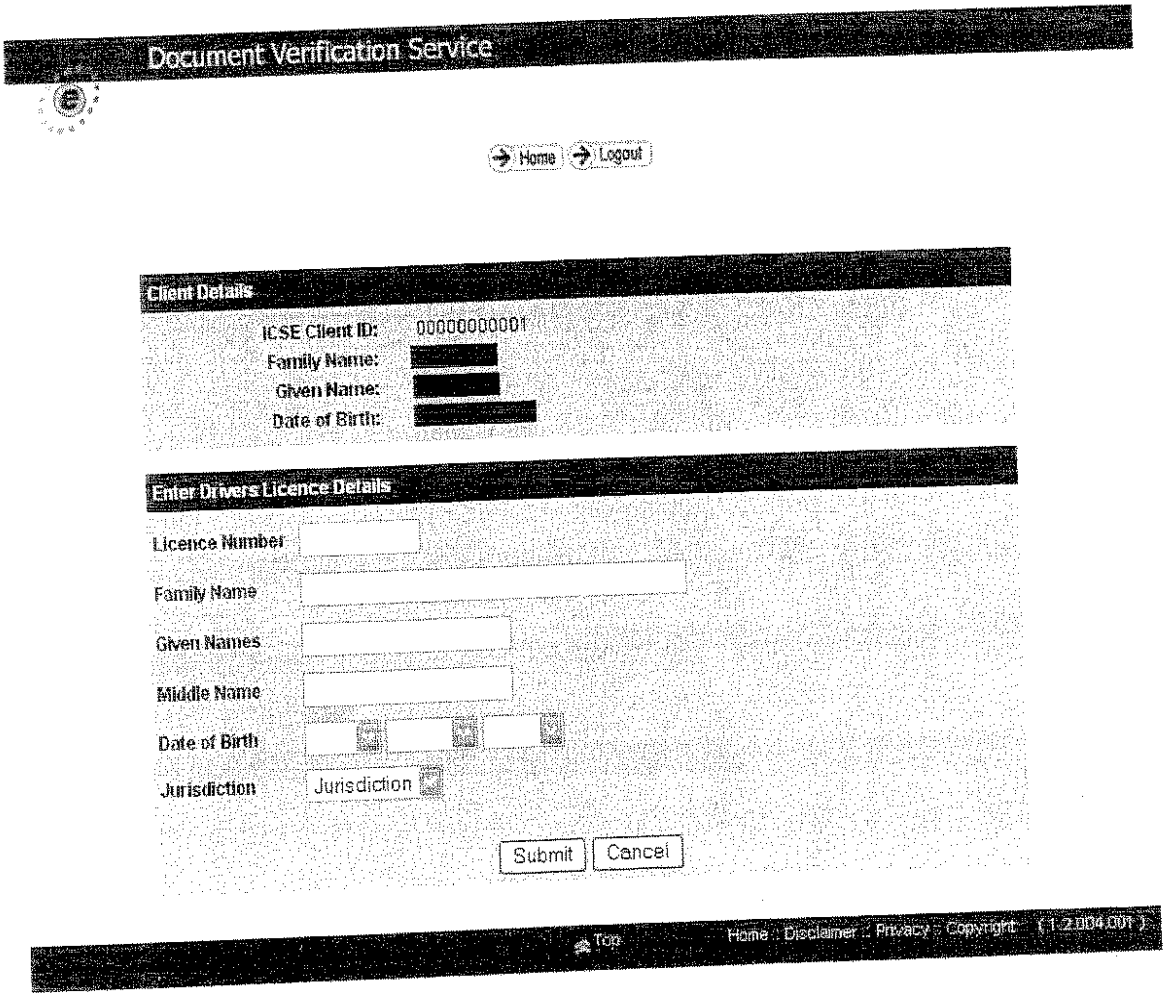
Example 1: Input data screen for selecting a document type

The following is an example of an input data screen for selecting a document to be verified through the pDVS. The document types to select from are Passport, Driver's Licence and Birth Certificate.



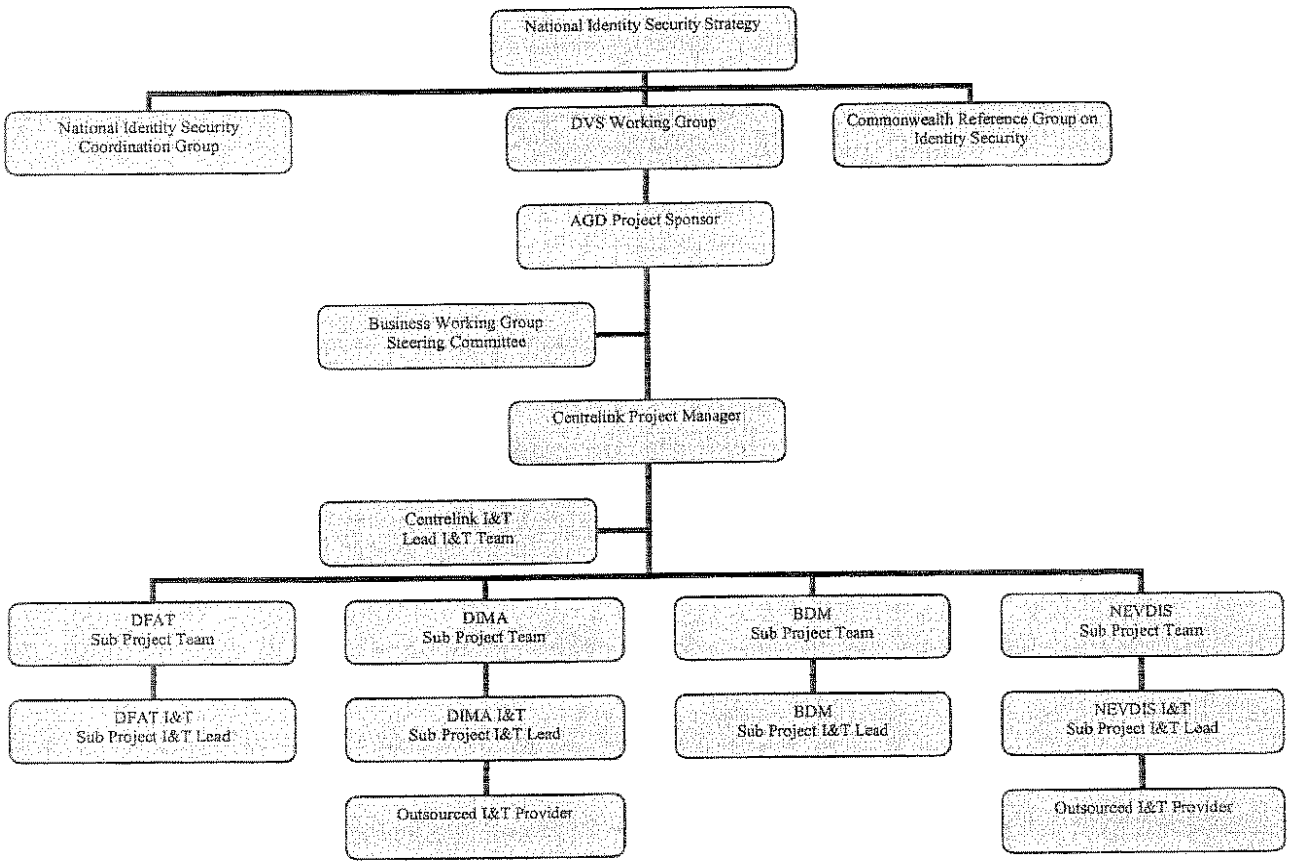
Example 2: Input data screen to verify Driver's Licence

The following screen would be displayed if a participating agency wished to query a driver's licence. Details such as licence number, family name, given names, middle name, date of birth and jurisdiction would be entered in the relevant fields. When submitted the details would be sent to the relevant RTA.



Attachment B

ORGANISATIONAL ARRANGEMENTS FOR pDVS



TECHNICAL DESCRIPTION OF THE pDVS HUB

Specifications

The main role of the Centrelink Hub for the pDVS is to provide a common message interface, intelligent message transformation, routing, verification responses, security, error handling, retries and basic Meta data collection as defined by Attorney-General's Department. Each of these capabilities is briefly detailed further below.

The existing hub was built to accommodate and support the requirements of each of the individual DVS prototype participants whilst still meeting the prototype requirements as stipulated by Attorney-General's Department.

Each participant had specific technical constraints and standards, which did not necessarily reflect or even complement the other participants. The design and capability of the pDVS Hub demonstrates the functionality required to enable each participant to maintain their existing technical designs and standards and still ensure they were able to communicate for the purpose of document verification.

Dedicated links

Each participant agency is linked to the pDVS Hub via dedicated links. DFAT and DIMA have a dedicated ICON IPSEC link whilst BDM NSW and NEVDIS each have an IPMAN Frame Relay connection.

The choice of different connections was based largely on the physical location of data centres for each participant. A Federal ICON network is available currently, but only within the ACT.

Both ICON and the dedicated IPMAN Frame Relay ensure a high level of security and privacy whilst still ensuring costs are kept to a minimum.

DFAT, NEVDIS and DIMA all communicate over the dedicated links using MQSeries point to point message transports. This is their preferred communication method. BDM NSW prefers a HTTP(s) or 'web based' method for communication.

DVS Hub functionality

Common Messaging Interface: Each agency participating in the pDVS had its own unique messaging standard and in some cases transport standards. The Hub implemented and integrated the four DVS client/providers onto a common messaging hub (framework). This integration was achieved in the pDVS through the use of IBM's WebSphere Business Integration Message Broker (Broker), MQSeries and WebSphere Applications Server V6 (WAS6). The Broker and WAS6 form the main hub or integration capabilities for the pDVS messages.

As the majority of the messages and the transport layer are MQSeries, the Broker initially provides the main functionality of the hub. The Broker has a tried and proven track record for over ten years in large enterprise systems for integrating disparate messaging systems and standards.

Intelligent Transformation and Routing: The Hub provides a common message interface to all clients and providers using the pDVS systems. It sends and receives messages of varying data formats to the clients/providers on both the MQSeries and HTTPs transports. As messages arrive on the Hub, these are translated and converted into the expected message formats (vice versa on return) and routed to the intended destinations for a verification response. Each agency only needs to know about one interface and schema (besides their own), which is the prototype Hub. The Hub in turn provides the capability for at least 4 interfaces to many service consumer relationships.

Error Handling

Transport Layer: Where MQSeries was implemented at the transport layer the Hub can handle communication and transport faults with standard MQSeries return codes and processes. These error codes are used for message retry and error handling.

Persistent messaging has been selected which ensures MQSeries will log and provide assured, once only delivery of messages. For example if a channel connection is down (broken) MQSeries will store and automatically retry/resend these messages when the problem is resolved.

With the exception of the original request to the Hub, all other retries and errors will be handled within the Hub itself. Error codes or information will not be sent back to the requesting agency. If these errors are in the form of a verification type "Error" then this will be captured in the Meta data information for reporting purposes.

A simple Yes (Y), No (N), or Error (E), answer is the only acceptable response to the requesting agency (Consumer). Replies with a status of pending were logged into the MI data store until resolved.

Australian Government

Attorney-General's Department

Evaluation of the Prototype Document Verification Service

November 2006

Executive Summary

On 14 April 2005, the Australian Government announced that it would develop a national strategy to improve identity security, combat identity crime and protect the identity of Australians from being used for illegal purposes. In the 2005-06 Budget the Government allocated funding to the strategy, which included a pilot project involving a prototype Document Verification Service (pDVS) to check the accuracy and validity of key proof-of-identity documents.

In September 2005, the Council of Australian Governments (COAG) agreed to the development and implementation of the National Identity Security Strategy. COAG also specified that the development and implementation of a national document verification service to combat the misuse of false and stolen identities would be a key component of the Strategy.

The pDVS was designed to operate online and in real time and to explore the technical and operational issues associated with a document verification service. The pDVS would help inform the development and implementation of a national verification service.

The pDVS operated from early February until 30 June 2006 allowing the Department of Foreign Affairs and Trade (DFAT) and the Department of Immigration and Multicultural Affairs (DIMA) to check proof of identity details offered by individuals seeking Australian passports and citizenship. During that period the pDVS was used for 51,551[1] separate verifications to check the details appearing on birth certificates, citizenship certificates, driver's licences and passports. The pDVS did not detect any false documents.

The overall verification rate associated with these queries was approximately 90%. Such verification failures are mostly attributable either to inconsistencies between the details recorded on the document and the electronic record, or to the document details being inaccurately recorded by applicants on application forms. Excluding these instances alone would raise the verification rate to approximately 96% and the experience of the pDVS has identified corrective action that can be undertaken.

The pDVS was only able to proceed because of the efforts and assistance of the agencies involved in the pilot. In particular, acknowledgement needs to be made to Centrelink, DIMA, DFAT, Austroads and the NSW Registry of Births, Deaths & Marriages.

Additional acknowledgement also needs to be made to the Office of the Privacy Commissioner for the invaluable advice and assistance the Office provided in relation to the pDVS and the National Identity Security Strategy.

[1] The figure 51,551 was calculated by combining the number of documents input by DFAT (51,118) with the documents input by DIMA (433)

2. THE pDVS

2.1. Overview of the pDVS

The pDVS is a computerised system which allows the online verification of documents presented as proof of identity (POI).

When verifying a document, the pDVS is able to confirm that:

- the document was issued by the issuing agency specified on its face
- the details recorded on the document correspond to those held in the issuing agency's register, and
- certain types of documents have not been superseded or cancelled.

The pDVS was tested by DFAT and DIMA in verifying POI documents presented to them by applicants enrolling for an Australian passport or requesting a certificate of evidence of Australian citizenship respectively. DFAT and DIMA participated as querying agencies and as document issuing agencies in their own right. The IT infrastructure for the pDVS was constructed and maintained by Centrelink.

In the pDVS, the POI documents verified and their issuing agencies were:

- birth certificates – NSW and ACT Registries of Births, Deaths and Marriages (BDMs)
- citizenship certificates – DIMA
- driver's licences – NSW and ACT Road Transport Authorities, and
- Australian passports – DFAT.

2.2. The prototype approach

The goal in pursuing a prototype was to test conceptual presumptions about the effectiveness of online, real-time document verification in a real world setting. That effectiveness was assessed in terms of the extent to which relevant POI documents in use in the community could be verified in an automated and cost effective manner against the registration databases held by the document issuing agencies.

Additionally, the prototype approach allowed the exploration of technical and operational issues associated with implementing and operating a secure, online and real-time system. It also gave participating agencies an opportunity to assess the value of a document verification service to them.

2.3. Prototype design and process

The various components of the pDVS and their interaction are depicted in Diagram 1.

From a human perspective, the steps involved in the verification process were:

- an individual presented their POI documents to DFAT or DIMA in support of their application for enrolment
- the applicant authorised the agency to undertake checks to verify the documents they presented
- the agency used the pDVS to check the document details and generated a verification request (details to be verified including full name, date of birth, official registration number or other identifying details of the document), and
- in normal circumstances a response to the verification request was returned in a couple of seconds.

As an IT process, the steps were:

- the verification check, or query, took the form of an electronic message which was sent as a package of data from the agency's computer system, via secure electronic communications pathways, to an electronic intermediary/processor called the pDVS Hub
- the pDVS Hub registered the incoming query by assigning a virtual reference number (VRN) and associated certain other transactional data (metadata) with that VRN (eg time of the query, electronic notification of the querying party)
- the pDVS Hub gave the data package a second VRN, for the use of the document issuing agency, and referred the query to the computer system of the relevant document issuing agency
- the computer system of the document issuing agency consulted the relevant database, established if the query matched the particular data fields, and returned a "YES", "NO" or "ERROR" response to the pDVS Hub, that communication was identified with the second VRN
- the pDVS Hub made a connection between the two VRNs, and
- the pDVS Hub communicated the "YES", "NO" or "ERROR" response to the querying agency's computer system, identified by the first VRN.

ACT and NSW BDM Registries verified the birth certificate details received in queries through the pDVS Hub by directing them to their Certificate Validation Service (CVS). The verification results were then returned through the pDVS Hub to the agency initiating the query. Centrelink built, implemented and managed the IT service hub for the pDVS.

It should be noted that Austroads and the National Exchange of Vehicle and Driver Information System (NEVDIS) acted as the clearing house for queries involving NSW and ACT driver's licenses. NEVDIS allows for real time access to, and exchange of driver's licence information between States and Territories. The NSW and ACT Road Transport Authorities did not engage directly with the pDVS Hub.

Similarly, verification of ACT and NSW birth certificate details was directed through the CVS operated collectively by BDM Registries.

3. THE EVALUATION PROCESS

3.1. Evaluation Goals

The evaluation of the pDVS has focussed on two particular areas with the greatest relevance for the participating agencies in the pDVS and for the design and implementation of the national DVS.

Testing the effectiveness of online processes

The primary goal of the prototype was to test the effectiveness of online document verification processes by demonstrating that verifications could be:

- conducted in an automated fashion
- performed in a real-time and online manner, and
- fast and reliable.

Testing the reliability of technology used

It was of key importance that the computer system infrastructure underpinning the deployment of the pDVS created not only a secure environment for processing the verifications but also assured a high level of availability. Accordingly, the pDVS was built upon dedicated communication lines and ICON links which ensured security as well as the ability to handle large numbers of requests.

An estimate of the maximum capacity of the pDVS to handle transactions was also of interest. A series of tests was devised to simulate heavy transactional loads. These tests indicated that the pDVS Hub was capable of supporting a load of up to 3 million transactions per day. It was not possible however to conduct load testing of the systems employed by the document issuing authorities. A detailed description of technical features associated with the pDVS Hub is provided at Attachment C.

An additional exercise was undertaken to ascertain if the flow of information associated with any particular verification query could be readily reconstructed end-to-end sometime after the actual event. This involved selecting a small sample of completed verifications to simulate, for example, a Freedom of Information (FOI) request lodged with the document issuing agency. The aim was to identify the actual logon or officer who initiated the pDVS request relating to a particular document. This exercise was successfully undertaken through the joint involvement of the three agencies who participated in each of the selected verifications. That is, the agency seeking to verify the document, the agency which issued the document and Centrelink as the manager of the pDVS Hub.

3.2. The data collection process

Centrelink collected data on all verification queries undertaken through the pDVS Hub in daily transaction logs for the period 6 February 2006 to 30 June 2006. At the conclusion of this pilot, the daily logs generated over the period were first combined to create a dataset of all queries and then divided on the basis of whether they were for DFAT or DIMA verifications. The two resulting datasets were subsequently

4. FINDINGS

4.1. DFAT results

DFAT selected cases for the pDVS by extracting POI document data from passport applications which had been approved during the two week period immediately preceding the selection date. DFAT employ a general practice of scanning passport application forms and identifying and extracting the relevant POI document data from each application. This data was then stored electronically to provide the input for the pDVS.

The scanning process was on occasion imperfect, introducing inaccuracies for some records. Since it is not intended that the national DVS would involve scanning, these errors were removed from the overall sample prior to the analysis of the verification results. An estimate was made of the extent to which corrupted records could be attributed to the scanning process by comparing a sub-sample of the scanned POI document data against the associated application forms. This approach enabled the statistical extrapolation of the number of documents of each type likely to be affected by scanning problems, enabling their overall impact to be eliminated from the verification results (these estimates are shown in Table 1).

Table 1: DFAT: POI document data scanned from applications

Document Type	Number Scanned	Scanning Problems (estimate)	Number for Verification
Birth Certificate	16,860	771	16,089
Citizenship Certificates	18,113	2,037	16,076
Driver's Licence	16,145	1,848	14,297
Total	51,118	4,656	46,462

The outcomes of the document verifications conducted through the pDVS by DFAT are summarised in Table 2 which shows that 89% of all documents checked by DFAT through the pDVS were verified. Of the 11% of queries overall that were not verified, 16% were of driver's licenses, 14% birth certificates and 2% citizenship certificates.

Table 2: DFAT: Results of the verification queries

Document Type	Verified		Not Verified		Total
	Number	(%)	Number	(%)	
Birth Certificate	13,778	(86)	2,311	(14)	16,089
Citizenship Certificates	15,744	(98)	332	(2)	16,076
Driver's Licence	12,038	(84)	2,259	(16)	14,297
Total	**41,560**	**(89)**	**4,902**	**(11)**	**46,462**

The non-verifications were then subject to examination by DFAT to identify the underlying reasons why the document data did not verify. This work was supported by extracting a sample of records for detailed follow-up. The result of this analysis is reported later in this report.

Table 4: Combined agency results of the verification queries

Document Type	Verified		Not-Verified		Total
	Number	(%)	Number	(%)	
Birth Certificate	13,778	(85.6)	2,311	(14.4)	16,089
Citizenship Certificate	15,744	(98.0)	332	(2.0)	16,076
Driver's Licence	12,422	(84.3)	2,306	(15.7)	14,728
Aust Passport	2	(100)	0	(0)	2
Total	**41,946**	**(89.5)**	**4,949**	**(10.5)**	**46,895**

4.4. Reasons for non-verification

DFAT and DIMA undertook detailed examination of those pDVS queries of POI documents that did not verify in order to satisfy themselves that:

- the details recorded on the document aligned with the document issuer's electronic record, and
- the details had been recorded correctly to the pDVS.

Where the above factors were confirmed, the reasons why documents had failed to verify were documented.

The reasons identified for non-verification for each particular document type along with its relative incidence are listed in Table 5.

Table 5: Reasons for non-verification by Document Type

Document Type	Reason for non-verification	Incidence (%)
Birth Certificate	Change of format for displaying registration number led to incorrect details recorded on passport application	95
	Courthouse issued a certificate having different registration number to that recorded in the register	5
Driver's Licence	First name and/or middle name did not match	46
	Licence number with incorrect prefix	40
	Incorrect licence details recorded on passport application	14
Australian Citizenship Certificate	Incorrect certificate number recorded on passport application	100

In all cases the non-verifications were a result of some details on a legitimate document not according with the electronic record held by the document issuing agency. On occasion more than one data item on the document (eg multiple components of first name, middle name and surname) may have failed to correlate.

No instances of false POI documents were detected in the samples verified through the pDVS, although in a small number of cases the document was no longer current.

DIMA became aware of this inconsistency early in the project and addressed it by adjusting their data entry practices to omit leading zeros from driver's licence numbers when inputting to the pDVS. This work practice enabled the verification of driver's licences that would have otherwise returned a non-verification response and resulted in DIMA eliminating this aspect as a reason for the non-verification of licences. Accordingly the driver's licence non-verification rate for DIMA is significantly lower at 11% than the 16% found by DFAT who contended with the problem caused by the extraneous zero digits. Adjusting to exclude this problem, the overall non-verification rate for driver's licences is estimated at 7.5%. Correcting for the 'leading zero' issue would be a straight-forward matter for a national DVS.

Citizenship Certificate

The reason that citizenship certificates failed to verify was due to the incorrect certificate number being recorded by the passport applicant on the DFAT passport application form.

Although all Australian Citizenship certificates have a 'stock number', which is the document serial number displayed on the certificate, its format has changed over time. This sometimes has led to confusion and consequent quotation of the wrong number by individuals. It is reasonable to suggest that errors of this type could be avoided in the national DVS where trained staff would be checking the citizenship certificate details through the DVS at the enrolment interview.

4.5. Adjusted verification rates

As the previous point suggests, the non-verification figure in Table 4 for each document type overstates the extent to which legitimate documents were not verified. This was predominantly due to variations between the details displayed on the face of the document and the underlying electronic record mismatching and therefore causing non-verification, and the enrolling applicant transcribing incorrect document details to an application form which were subsequently input to the pDVS.

Elimination of these two factors as potential contributors to legitimate documents failing to verify will result in substantially higher verification rates than those shown in Table 4. Assuming these factors can be addressed and their effect eliminated from a fully functioning national DVS, we estimate the overall verification rates would be those shown in Table 6 below.

Table 6: Adjusted verification / non-verification rates

Document Type	Verified (%)	Not-Verified (%)
Birth Certificate	99	1
Citizenship Certificate	100	0
Driver's Licence	92.5	7.5
Aust Passport	100	0

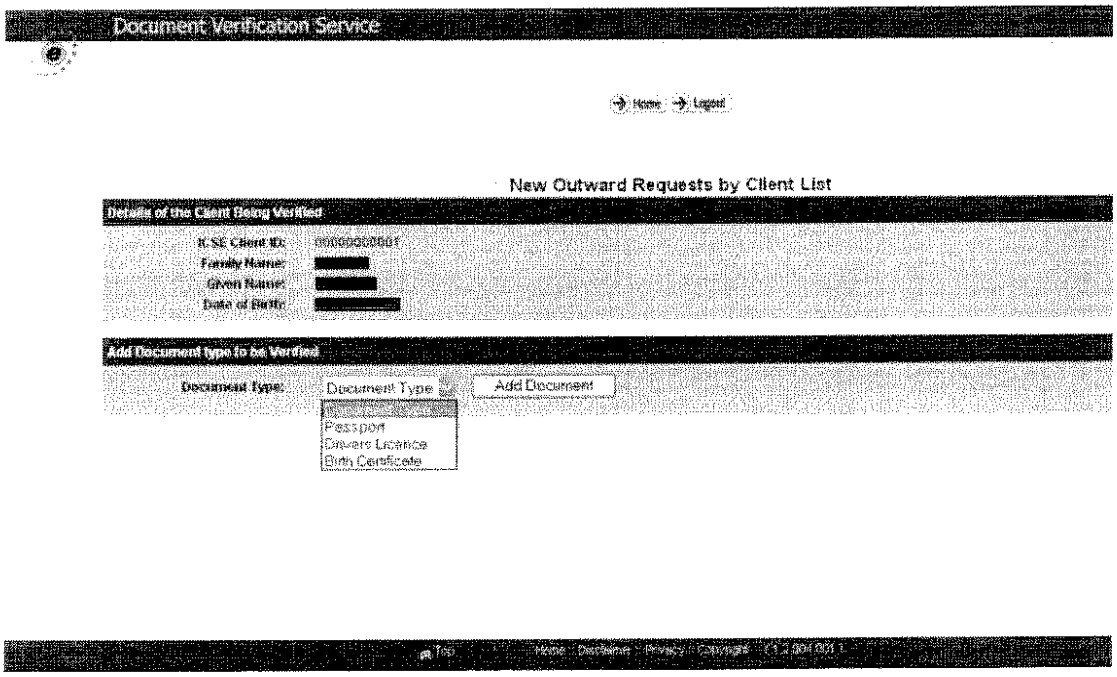
communications with document issuing agencies. The pDVS was accessed and administered only by authorised staff within participating agencies.

- *Data quality*: The DVS Hub processes only personal information that is relevant to the purpose for which it is collected by participating agencies. Data may only be retained by the hub for a short period in the event of a system error. During the prototype phase of the DVS project, data on verification transactions were logged for statistical purposes without access to, or inclusion of, personal information.

pDVS SCREEN SHOTS

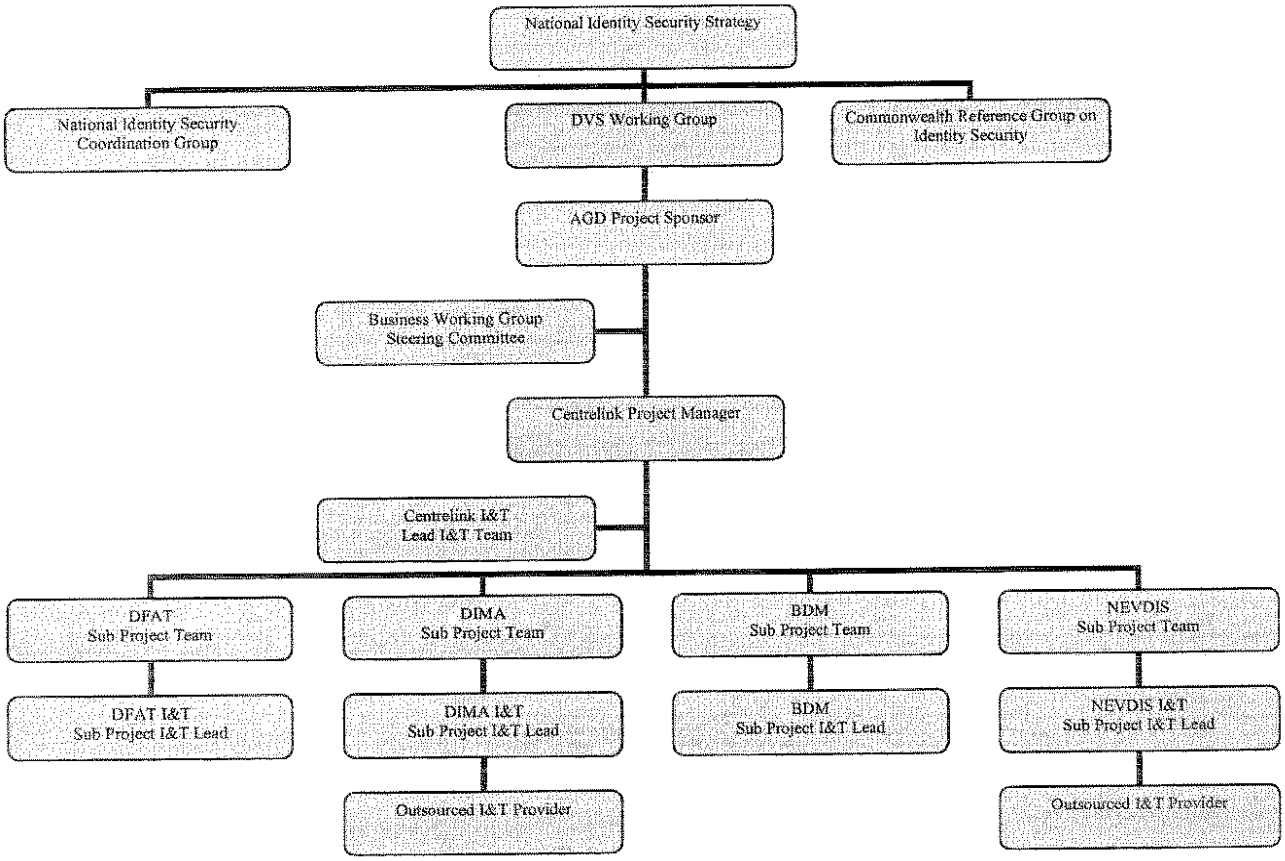
Example 1: Input data screen for selecting a document type

The following is an example of an input data screen for selecting a document to be verified through the pDVS. The document types to select from are Passport, Driver's Licence and Birth Certificate.



Attachment B

ORGANISATIONAL ARRANGEMENTS FOR pDVS



As the majority of the messages and the transport layer are MQSeries, the Broker initially provides the main functionality of the hub. The Broker has a tried and proven track record for over ten years in large enterprise systems for integrating disparate messaging systems and standards.

Intelligent Transformation and Routing: The Hub provides a common message interface to all clients and providers using the pDVS systems. It sends and receives messages of varying data formats to the clients/providers on both the MQSeries and HTTPs transports. As messages arrive on the Hub, these are translated and converted into the expected message formats (vice versa on return) and routed to the intended destinations for a verification response. Each agency only needs to know about one interface and schema (besides their own), which is the prototype Hub. The Hub in turn provides the capability for at least 4 interfaces to many service consumer relationships.

Error Handling

Transport Layer: Where MQSeries was implemented at the transport layer the Hub can handle communication and transport faults with standard MQSeries return codes and processes. These error codes are used for message retry and error handling.

Persistent messaging has been selected which ensures MQSeries will log and provide assured, once only delivery of messages. For example if a channel connection is down (broken) MQSeries will store and automatically retry/resend these messages when the problem is resolved.

With the exception of the original request to the Hub, all other retries and errors will be handled within the Hub itself. Error codes or information will not be sent back to the requesting agency. If these errors are in the form of a verification type "Error" then this will be captured in the Meta data information for reporting purposes.

A simple Yes (Y), No (N), or Error (E), answer is the only acceptable response to the requesting agency (Consumer). Replies with a status of pending were logged into the MI data store until resolved.