FASTER-PrivBio Project Summary Report

Kim Scott-Burrett
WorldReach Software

Michael Andre
Jean-Guy St. Amour
Immigration, Refugees and Citizenship Canada

David Bissessar
Canada Border Services Agency

Prepared by:
WorldReach Software
2650 Queensview Drive, Suite 250
Ottawa, ON K2B 8H6

Defence Research and Development Canada

Contract Report
DRDC-RDDC-2018-C197
October 2018

**IMPORTANT INFORMATIVE STATEMENTS**

This document was reviewed for Controlled Goods by Defence Research and Development Canada using the Schedule to the *Defence Production Act*.

Disclaimer: This document is not published by the Editorial Office of Defence Research and Development Canada, an agency of the Department of National Defence of Canada but is to be catalogued in the Canadian Defence Information System (CANDIS), the national repository for Defence S&T documents. Her Majesty the Queen in Right of Canada (Department of National Defence) makes no representations or warranties, expressed or implied, of any kind whatsoever, and assumes no liability for the accuracy, reliability, completeness, currency or usefulness of any information, product, process or material included in this document. Nothing in this document should be interpreted as an endorsement for the specific use of any tool, technique or process examined in it. Any reliance on, or use of, any information, product, process or material included in this document is at the sole risk of the person so using it or relying on it. Canada does not assume any liability in respect of any damages or losses arising out of or in connection with the use of, or reliance on, any information, product, process or material included in this document.

FASTER-PrivBio
CSSP-2015-CP-2114
Project Summary Report
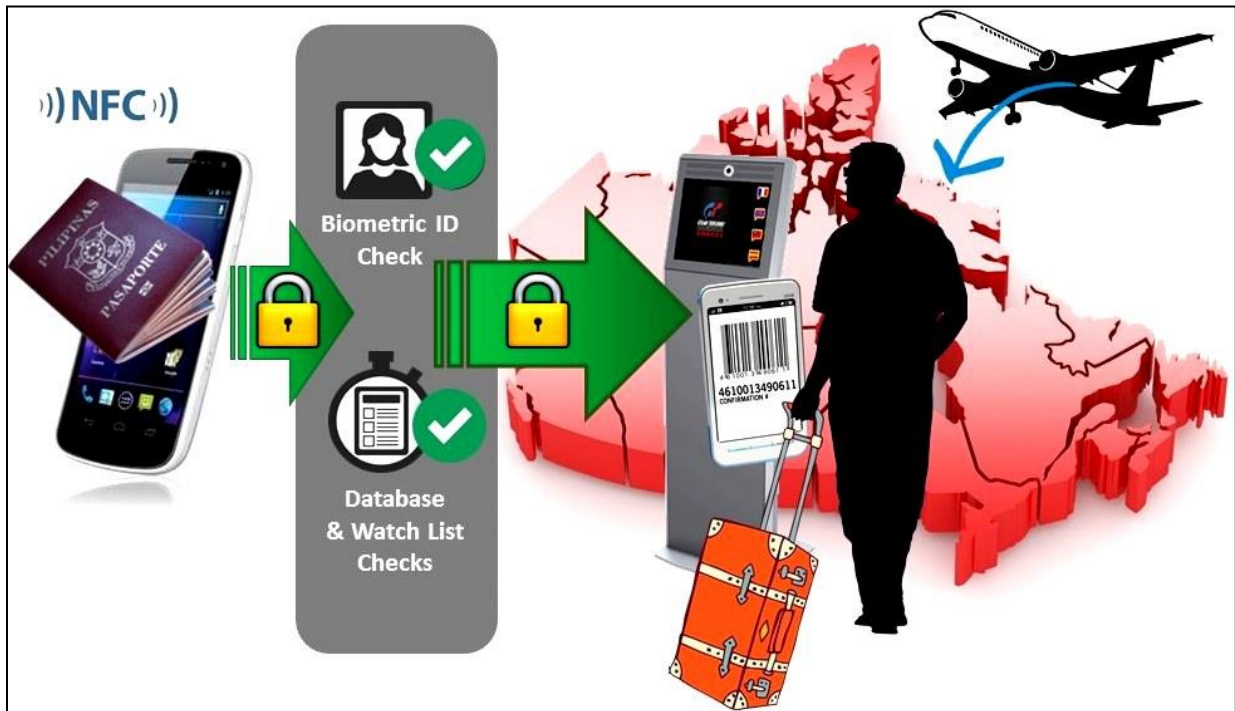
May 2017

Record of Amendments

Version No.	Amendment / Section Amended	Entered By	Amendment Date
0.1	First Draft	Michael Andre	2017-02-09
0.2	Input from WorldReach	Kim Burrett-Scott Jean-Guy St-Amour	2017-02-17
0.3	Input from IRCC	Michael Andre	2017-03-17
0.4	Input from Jean-Guy	Michael Andre	2017-03-22
0.5	Input from WorldReach	Michael Andre	2017-03-28
0.6	All partners final input	Kim Burrett-Scott Jean-Guy St-Amour	2017-05-24

Table of Contents

Acronyms

CBSA	Canada Border Services Agency
CoT	Chain of Trust
CSSP	Centre for Security Science Program
DRDC	Defence Research and Development Canada
eTA	Electronic Travel Authority
GCMS	Global Case Management System
ICAO	International Civil Aviation Organization
IRCC	Immigration, Refugees and Citizenship Canada
NFC	Near-Field-Communication
PbD	Privacy by Design
PIA	Privacy Impact Assessment
PIN	Personal Identification Number
PKD	Public Key Directory
QR	Quick Response (code)
RBR	Renewable Biometric Reference
TRL	Technology Readiness Level

1.   Project Background and Context

This project is a Defence Research and Development Canada (DRDC) managed initiative under the CSSP.

It represents a unique collaboration between Immigration, Refugees and Citizenship Canada (IRCC), the Canada Border Services Agency (CBSA), WorldReach Software Corporation, Regula Forensics Inc., the University of Ottawa, and Ryerson University.

FASTER-PrivBio, originally an 18 month project (extended to 24), aimed to develop the proof-of-concept that:
- facilitates the remote identification and authentication of individuals applying for an IRCC Program, Electronic Travel Authorization (eTA), leveraging the chip capabilities of the ePassport and smartphone Near-Field-Communication (NFC) and camera functionalities;
- allows for early validation of identity and ePassport, alignment with Program criteria, background check using facial biometric of the applicant; and
- creates an encrypted Renewable Biometric Reference (RBR) reusable credential, that is stored on the smartphone, all while respecting Privacy by Design (PbD) principles.

The smartphone solution would allow the application of low-risk travellers to be automatically adjudicated (an enriched online solution) and clear Canadian borders efficiently, seamlessly and rapidly using self-service kiosks.

The project was originally planned for the period of 1 September 2015 to 30 November 2016. Milestones were delivered on time and on budget. The project was extended to 31 March 2017 to conduct additional research to produce a more robust prototype by doing the following:

- Conduct further robustness tests of a range of ePassports from numerous countries;
- Identify improvements to the security of data acquisition, transmission and storage between smartphone and server;
- Investigate identity assurance processes to include liveness detection of the self-photo in mobile applications;
- Introduce the use of a two dimensional QR code to use in communication at the kiosk to open the credential on the phone; ;
- Explore variability in biometric encryption to deal with inconsistency that can occur when capturing a facial image; and
- Assess security of architecture information flow to ensure ePassport integrity is maintained in the data acquisition through to credential verification process.

The funding for this project was as follows: $1,073,653 financial support from CSSP; as well as $1,072,702 in-kind co-investment and $176,352 cash co-investment from project partners.

2.   Project Outcomes

The project was divided into three main deliverables, all accompanied by a wide array of supporting research analysis.

2.1.   Exercise 1 – Issuance Process

2.1.1. Purpose

The purpose of this exercise was to demonstrate the use case in which a smartphone running a prototype of the FASTER mobile App was used to complete the application process for an electronic travel authorization (eTA) and illustrate the additional data integrity and authentication features this process provided. The first exercise focussed on the interface points between the smartphone, the ePassport, IRCC simulated databases and the PrivBio application and server determined to be in scope by the project team. All the interfaces were documented prior to the exercise in the concept of operations. Simulations were done of some of the screening processes including links to Interpol's Stolen and Lost Travel Documents database and IRCC Watch-lists. Creation of a Renewable Biometric Reference (RBR) based on the traveller's ePassport photo and the generation of a token as a travel credential without storing the biometric or template on the smartphone were also part of the prototype for demonstration.

2.1.2. Results

The project team effectively developed and demonstrated a prototype of the eTA mobile issuance process. The prototype application process included remote application and assessment of travellers' eligibility for the eTA program for travel to Canada and automatic approval of low risk travellers. This exercise demonstrated the ability to remotely verify the authenticity of an applicant's ePassport using the smartphone NFC capability to read the chip of the ePassport, conduct data group checks and then compare the ePassport photo to a self-photo taken at time of application, providing a higher level of assurance that the applicant is the owner of this ePassport.

This process also results in provision of better data integrity for applicant information which is read from the ePassport rather than being keyed by the applicant, a process which is known to be prone to error. Exception handling via manual processes using an interface available to processing agents was also covered. Approved applicants were notified of their approval by e-mail and were able to generate their RBR that is stored on the smartphone.

For any travellers who do not get automatic approval the file is flagged for a live agent to review the application, take appropriate action and notify the applicant by e-mail to return to the mobile App for the assessment results. The application does not automatically reject applicants.

A pictorial of the proof-of-concept for the application and issuance process is found in Figure 1.

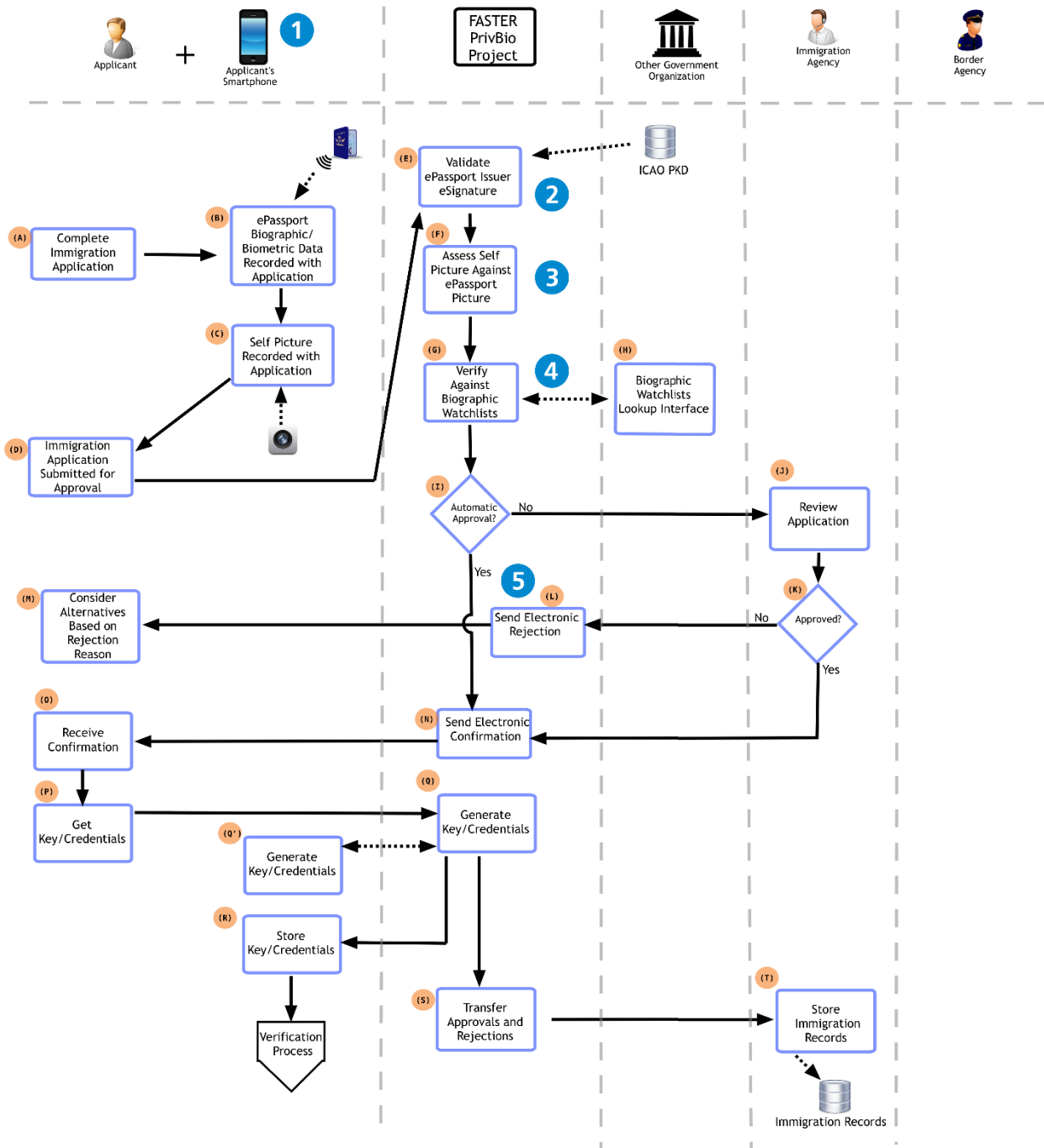## Application and Issuance Process

Figure 1

2.2. Exercise 2 – Verification Process

2.2.1. Purpose

The purpose of this exercise was to demonstrate the Proof of Concept using a smartphone, ePassport and point of entry self-service kiosk by foreign travellers who have been granted an eTA to quickly and securely pass through the port of entry, while flagging travellers requiring inspection by customs agents. The verification process includes the authentication of the traveller against their ePassport photo by taking a photo at the kiosk, the retrieval of their token from the smartphone and recreation of the RBR followed by a final call to the IRCC database to ensure that the traveller's eTA has not been revoked.

2.2.2. Results

The project team effectively developed and demonstrated the verification process using a kiosk and interfaces to the prototype database to represent communication to IRCC. In addition, the exercise covered updates to the FASTER mobile App resultant from the feedback from exercise 1. A pictorial of the proof-of-concept for the verification process is found in Figure 2.

For both the issuance and verification processes, videos were prepared that describe the full process. These videos have been used as supplementary materials for meetings with various project stakeholders and interested parties in situations where there was very little time to provide the full demonstration or facilities were not available to accommodate it (e.g. no WIFI to access FASTER adjudication system or no access to the kiosk).
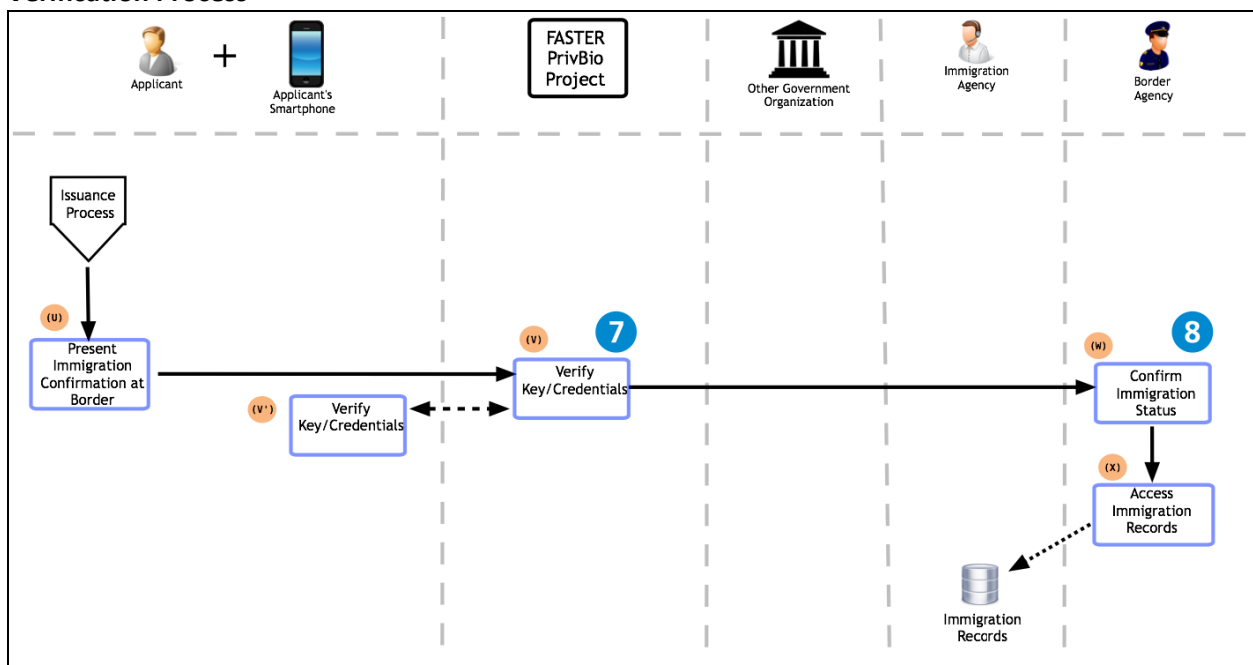
Verification Process

Figure 2

2.3. Exercise 3 – Issuance and Verification Process Remote Live-capture Testing and Biometric Variability

2.3.1. Purpose

The purpose of this exercise was to demonstrate further refinements in the robustness of the proof-of-concept including liveness detection of the applicant at time of remote enrolment, more testing with a variety of ePassports, as well as investigating the use of a biometric identity algorithm to account for variability. The later addition is among the first steps to reducing the need for use of an ePassport book at a border kiosk.

This involved the use of the ePassport as verification of identity during the eTA application process. The photo taken by the smartphone was used to generate an encrypted RBR which was then stored on the smartphone. At a border entry point the QR code is read by the kiosk to retrieve the information required to decrypt the RBR and matched the photo taken by the kiosk to verify the identity of the traveller.

2.3.2. Results

The refinements to the original proof-of-concept are significant in making the system component more robust and thereby getting this project closer to being ready for pilot. Liveness detection during the applicant's taking of self-photos will improve security by reducing the likelihood of spoofing. Privacy improvements included, the addition of a time out function during the application process to help ensure no data is left on the smartphone's memory. As well, testing of as many country's ePassports as could be accessed confirmed that the FASTER mobile application could successfully read the chip on 80% of those ePassports which represent 93% of the applicants coming to Canada from eTA countries.

The variability testing was done to illustrate that an RBR could be used to match two photos for the same person. This could be a self-photo verses a kiosk photo or ePassport photo verses a kiosk photo or a three-way match. In the demonstration, a photo taken on the smartphone was used as a reference against another photo taken by the smartphone.

This could eventually reduce the need to use the ePassport at check points after an eTA application, thereby improving convenience to the traveller. Using improved encryption technology enhances security of the facial biometric and privacy of the traveller. What is stored is a random series of characters that cannot trace back to a biometric.

3.   From Proof-of-Concept to Prototype for Pilot Project

As can be seen from the results, the Project has successfully developed a functional prototype, based on a concept of operations for the foreign traveller to use when applying on their smartphones for an eTA, then using the RBR stored on the phone at a border control kiosk. The application was developed using PbD principles which respects the privacy of the traveller. The data collected is securely transmitted, is verified to determine the eligibility of the traveller to enter Canada and the ePassport holder is authenticated.

There are a number of supporting activities undertaken during the course of the project which are essential in order to proceed beyond this initial stage. These are briefly described below.

3.1. Development of a Privacy Impact Assessment

Any new or substantially modified programs or activities involving the creation, collection and handling of personal information undertaken by the Canadian Government must be assessed to determine their privacy impacts. During this project, this work was initiated and findings to date documented in the following paper "Preparation for a Privacy Impact Assessment Impact on IRCC IT Infrastructure" (see Bibliography Annex N). This provides a strong foundation for the completion of a PIA, should the concept move to pilot preparation.

3.2. Policy Development

The proof-of-concept has used the current process developed by IRCC for applying for an eTA using an online application as a use case. However, there is additional functionality built into the Project's proof-of-concept mobile application (e.g. acquisition of an App, use of a self-photo) and consideration will have to be made to modify or develop policies with respect to them should some or all of them be made part of the standard process. In addition, the acceptance/rejection thresholds for self-photos against ePassport photos using facial matching software algorithms of travellers will have to be considered from a policy perspective. This can be accomplished through additional testing with large sample sets of images, as well as through calibration of the thresholds following initial launch of this capability. Setting the acceptance thresholds too high will can result in significant false rejection rates which needs to be balanced against the intended objective of auto approvals of those applicants considered to be low risk.

A follow on CSSP project (Chain of Trust: Continuous Risk Assessment for Air Travel - CSSP Reference ID: 0407) has already been approved which will provide more opportunities for more testing with exposure to a wider range of ePassports and user feedback as well as adding predictive analytics for both IRCC and CBSA and a risk assessment engine to manage the assessment and approval policies and processes.

Both IRCC and CBSA assessment of policy and process implications and adjustments will continue as we move towards a target of a pilot implementation.

3.3. Technological Advances

Technology is advancing rapidly in biometrics collection and verification, such as tools for liveness detection as part of facial authentication. Extensive research was conducted on available tools for liveness detection, reviewing usability, compatibility with other toolkits used in this project, cost, etc. In total over 20 solutions were reviewed and two were obtained as trial versions for testing and analysis. These two were demonstrated to the project partners in exercise 3 and further work to integrate a selected tool will be pursued in the Chain of Trust project. Details on the tools are documented in Annex R "Liveness Detection Investigation".

The Project's mobile application, as currently built, can only be used on Android devices as they are the only devices that allow NFC reading of the ePassport chip. If Apple unlocks their NFC capability to permit use of their phones, it would expand the use of the Project's application. In the interim, the mobile application can be configured to skip the reading of the ePassport chip, but still does an Optical Character Read (OCR) of the ePassport MRZ lines which provides significant added value to the eTA process by recording accurate information to the eTA application form, thereby avoiding user data entry errors. The mobile application configured this way can be used by a wide range of devices, including iPhones.

Other technology advancements in the area of biometrics such as finger print and iris scans are coming into greater use all the time and when uptake is such that they are significant enough for consideration as part of the processes covered by future projects like this one, will also be investigated.

There are also new technologies related to border management will be explored during the Chain of Trust project with the intention of moving beyond the use of kiosks.

3.4. Global Case Management System and the Issuance Process

The Global Case Management System (GCMS) is IRCC's single, integrated and worldwide system used internally to process applications for citizenship and immigration services including ePassport and the eTA program. The CBSA information system manages border control information. As the developed prototype parallels that of the established eTA on-line application process no major changes to existing infrastructure are anticipated. More details are documented in "Technical Report for PrivBio Project" in Annex V.

GCMS is key to the use of the Project's application for the issuance process. For the testing, development and exercises carried out during the Project, a representative environment was specifically established to simulate the required system components containing only test data. Figure 3 displays the interactions.
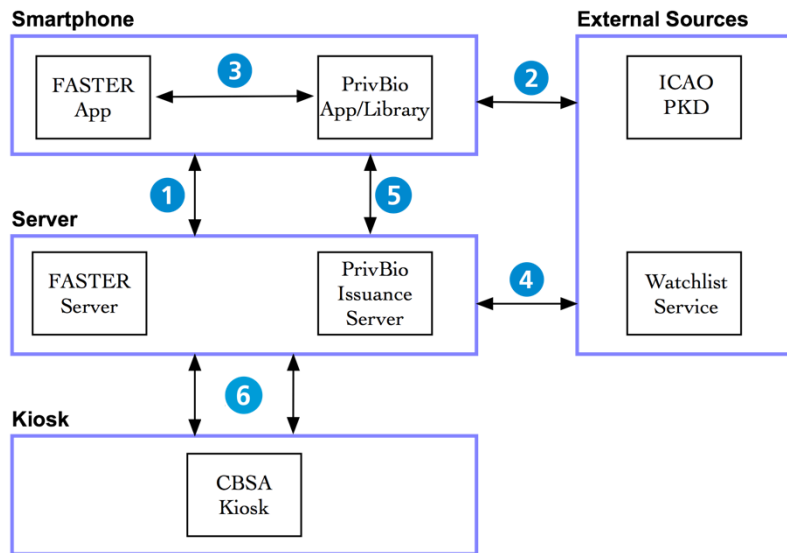
FASTER—PrivBio Interface Diagram

Figure 3

For a pilot project, these interfaces will have to be incorporated into existing infrastructure. Preliminary discussions with GCMS representatives during the project indicated that the technical requirements of FASTER were compatible with the current infrastructure and the elements that could involve changes were documented to the extent possible prior to authorization to proceed to a pilot. For initial pilot IRCC could gain significant benefit from the implementation of the FASTER mobile application component (as noted in the results of Exercise 1) and then as a next step look at the addition of the PrivBio component.

Incorporation of PrivBio would involve establishing connectivity between the FASTER GCMS server and the PrivBio CBSA server, as well as to other suggested databases or systems for Watch List and STLD lookups to get the full benefit.

To assure success of a pilot project, a study will have to be conducted on the cost, feasibility and specific architectural impacts of establishing these connections for this environment.

3.5. Program Support

To bring the Project's proof-of-concept to a functional prototype ready for use in practical application, strong Program support will be key. The next step in the process will be to seek approval for a cost/benefit analysis and business model, which could include various staged options or subsets of functionality if it is determined that full functionality is considered impractical or too costly.

4. Conclusions

The FASTER-PrivBio project has developed a prototype user-friendly tested mobile app and process for an eTA application that incorporates privacy by design principles in its design to assure that traveller's privacy and security of information is maintained. The following conclusions were drawn as a result of the project:

1) NFC reading of ePassport biometric and biographical data ensures data integrity in application processing.
2) Selfie-photo to ePassport photo comparison provides an early mechanism for self-serve document authentication by travelers.
3) ePassport validation of data on the chip confirms its integrity.
4) Mobile travel credentials can be used to represent travel authorizations and are securely verifiable between Immigration and Border Security.
5) Privacy-respecting biometrics secure the mobile travel credential to the traveller. Without storing a biometric, strong verification of the credential to the traveller prevents unauthorized sharing between users.
6) Mobile travel credentials are deemed to be at least as private & secure as the current ePassport book.

The developed system has the potential to provide faster approvals for low risk travellers who make up a large proportion of population of travellers. The use of the mobile App should also provide more convenience for many foreign travellers, as a majority are in possession of a smartphone. By automating the border control processes, travellers should be able to pass through the border more quickly, efficiently and conveniently. IRCC and CBSA should also gain cost savings as only the higher-risk travellers pass through the manual process.

IRCC could use a modified FASTER App for other programs such as passport renewals. IRCC could also pursue the use of the mobile app to facilitate the current eTA program.

5. Follow-on Actions

In light of FASTER-PrivBio Project's success, phase II of the project, Chain of Trust (CoT) will commence on April 1, 2017 for a period of one year, with IRCC, CBSA and WorldReach Software Corporation as partners. The objective is to identify the necessary requirements and target the overall proposed technology up to TRL 7. The demonstration of a prototype will be performed in a representative rather than an operational environment.

The CoT project will enhance targeting solutions and make use of all available data, and biometrics to identify through the use of predictive analytics, low-risk travellers from the eTA application to the moment when a traveller reaches a Canadian point of entry.

6. Bibliography

The following documents resulting from the Project are attached to this report:

	Project Charter		WorldReach Contract			
ANNEX	**Task**	**Title**	**WBS**	**Mstn**	**Title**	**Document Title**
A	1	CSSP Project Charter FASTER-PrivBio				CSSP Proj Charter FASTER-PrivBio 2015-CP-2114
B	2.1	Concept of operation	1.1.3	1	Concept of operations	Concept of Operations – Use Case Model
C		Preliminary scenarios	1.1.3	1	Preliminary test scenarios	Issuance Exercise Test Scenarios
D		Baseline demonstration report	1.1.6	1	Demonstration report	Baseline Demonstration Report
E	2.2	Integration analysis report	1.2.2	1	Integration Analysis Report	Integration Analysis Report – Issuance Process
F			1.2.4	1	Scenario Execution Plan	Exercise Plan
G	2.3	Issuance Exercise Report	1.3.4	4	Issuance Exercise report	Issuance Exercises Report
H	2.4	Integration Analysis Report	1.4.1	5	Integration Analysis Report	Integration Analysis Report
I		Verification Exercise Report	1.4.4	8	Verification Exercise report	Verification Exercise Report
J	3.1	Identity Assurance policy report	2.1.4	6	Identity Assurance Tech review	ID Assurance Level of Confidence Report
K		Alignment with Imm programs	2.1.5	6	Input to policy review report	Preliminary Privacy Review (FASTER)
L	3.2	Hosting Platform Security report	2.2.2	6	Hosting Platform Security rpt	Statement of Sensitivity Report
M	3.3	User Experience Results Report	2.3.3	6	User experience result report	User Experience Test Results
	4	Capability Reviews	3.2	8	Contractor review documents	No Report Required
N	5	Policy Analysis prep for PIA	4.1	9	Policy Analysis prep for PIA	Prep for PIA Impact on IRCC IT Infrastructure
O	6	E-ppt specimen testing report	5.1	10	E-ppt specimen testing report	Robustness Testing Results
P	7	Design of Data Security enhancements	6	11	Design documentation	Issuance Data Security Enhancements Design
	8	Integrate Biometric Encryption	8.1	13		No report required
Q	9	End to end exercise report	8.2	13	End to end exercise report	End to End Exercise Report
R						Liveness Detection Investigation
S	10	Evaluation report	9.2	14	Evaluation report	Project Summary Report
T	11	Impact Summary quad chart	10.2	15	Impact Summary quad chart	Impact Summary report
U		Close out report	10.3	15	Close out report	Completion Report
		Videos				FASTER-PrivBio Video
						Priv-Bio Video
			University of Ottawa Contract			
V	3.2	Mobile Platform security report				Technical Report for PrivBio Project
W	7	Issuance data Security Enhancements				ePassport Priv-Bio Security Comparison
	8	Integrate Biometric Encryption				No report required
			Ryerson University Contract			
X	4	Case study of privacy by design				Privacy Analysis: Case Study in Privacy by Design
Y		Bio Encryption Policy Impact				The Policy Analysis
Z						Android Platform Analysis

Note: Unless otherwise stated the deliverable encompasses FASTER-Priv-Bio activities

DOCUMENT CONTROL DATA

*Security markings for the title, authors, abstract and keywords must be entered when the document is sensitive

1. ORIGINATOR (Name and address of the organization preparing the document. A DRDC Centre sponsoring a contractor's report, or tasking agency, is entered in Section 8.) WorldReach Software 2650 Queensview Drive, Suite 250 Ottawa, ON K2B 8H6	2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.) CAN UNCLASSIFIED
	2b. CONTROLLED GOODS NON-CONTROLLED GOODS DMC A

3. TITLE (The document title and sub-title as indicated on the title page.) FASTER-PrivBio Project Summary Report		
4. AUTHORS (Last name, followed by initials – ranks, titles, etc., not to be used) Scott-Burrett, K.; Andre, M.; St. Amour, J.-G.; Bissessar, D.		
5. DATE OF PUBLICATION (Month and year of publication of document.) May 2017	6a. NO. OF PAGES (Total pages, including Annexes, excluding DCD, covering and verso pages.) 14	6b. NO. OF REFS (Total references cited.) 0
7. DOCUMENT CATEGORY (e.g., Scientific Report, Contract Report, Scientific Letter.) Contract Report		
8. SPONSORING CENTRE (The name and address of the department project office or laboratory sponsoring the research and development.) DRDC – Centre for Security Science NDHQ (Carling), 60 Moodie Drive, Building 7 Ottawa, Ontario K1A 0K2 Canada		

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.) B8625-160470-001-SV
10a. DRDC PUBLICATION NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.) DRDC-RDDC-2018-C197	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11a. FUTURE DISTRIBUTION WITHIN CANADA (Approval for further dissemination of the document. Security classification must also be considered.) Public release
11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

12. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Use semi-colon as a delimiter.)

Biometrics; Border Security; Immigration

13. ABSTRACT/RÉSUMÉ (When available in the document, the French version of the abstract must be included here.)

Contract was prior to July 2017 (abstracts not provided).