Digital Identification and Authentication Council of Canada (DIACC)

Proof of Concept – Online Proof of Residency

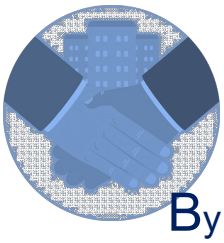
June 2016

Table of Contents

Executive Summary

Residency is used by governments, the private sector and the social-profit sectors to ensure products and services are delivered to eligible individuals who live in a specific province, area or community, and to help reduce risk. Today, to conduct a proof of residency, an organization must request that their clients physically bring in a utility bill, financial statement or similar document that would demonstrate a tie to a physical address. This experience is neither privacy enhancing nor convenient for the client, and organizations are forced to maintain antiquated processes that are increasingly susceptible to fraud. In short, it is currently a lose-lose situation.

Recognizing this challenge, and an ongoing desire to move to digital services, the DIACC has undertaken a review of the opportunity to modernise a proof of residency experience. The DIACC has further explored whether information available within participating DIACC organizations could provide sufficient evidence to enable an online residency proof.



In our review, a number of opportunities were identified that would improve the client experience and reduce business risk.

Client Experience

By putting the client at the centre of the proof of residency, the DIACC was able to focus on developing an online proof of residency framework that is privacy enhancing, secure, transparent, robust and efficient. This would open up many online opportunities where technological capabilities were once a limiting factor.

By putting the client, and more specifically the client's privacy, at the centre of the framework, control is in the hands of the client. The client initiates any requests. No information is requested or shared without the express and clearly informed consent of the client.

The focus on Privacy by Design is key to the framework. By putting the client, and more specifically the client's privacy, at the centre of the framework, control is in the hands of the client. The client initiates any requests. No information is requested or shared without the express and clearly informed consent of the client.

Utilizing this proof of residency framework, in the future, an individual could confirm domestic tuition rates, qualify for a regional cell service discount or apply for provincial health insurance online.

Traditionally, the addition of online services has come with an increase in sharing of personal information. One of the unique advantages of the proposed framework is that it limits the information exchanged to an initial request, followed by a simple Yes or No. Additionally, a transparent, consent based framework to proof ensures that the client is in control every step of the way.

Business Risk Reduction

When an organization requests a proof of residency[i] they could be looking for a number of corresponding residency elements, including:

- Is this address valid?
- Does the individual have a strong tie to that address?
- Is the individual active within a geographic area?

The proposed online proof of residency has some substantial improvements over existing paper based in person solutions. Paper proofs could be forged, and disclose a substantial amount of personal information. Further, not all household residents have bills in their name. A brokered connection from an Authoritative Party to a Relying Party can reduce fraud, strengthen the proof, and enable a quick evaluation of history or duration of stay.

Finally, the Relying Party can request proof that goes beyond a tie to a residential address, extending to evidence of actual presence in the area. For example, financial institutions' ATM, branch and payment terminal presence and telecommunication's companies' insight into cellular phone activity can, when aggregated, provide strong evidence for activity within geographic areas. All of this can be done without the client having to share the actual details of the transactions with a client service agent– as they would be required to do today.

The recommendations in this paper describe where Canada may lead the world and create an ecosystem that is privacy enhancing and enables new business opportunities, enables online application to more services, and protects clients, one proof at a time

This granularity opens up new service opportunities to qualify, or to manage risk based on a requested geographic area.

The Opportunity

The recommendations in this paper describe where Canada may lead the world and create an ecosystem that is privacy enhancing and enables new business opportunities, enables online application to more services, and protects clients, one proof at a time.

Background

As part of DIACC's ongoing investigation into new applications for Digital Identity and Authentication a proposal to solve physical residency emerged.

The proposal was to develop a Proof of Concept that would:

- Identify and demonstrate effective ways to verify, with a reasonable level of confidence, that an individual was resident within a geographic area for a specified period of time.
- Solve the problem in a manner that is privacy enhancing and uses available technologies
- Inform the opportunity and interest for residency checks by identifying regulatory, policy, client service and other considerations for developing a digital proof of residency framework in Canada.

Members of the team followed a collaborative process to deliver this whitepaper and a working mock-up. The team consisted of representatives from the public, private and social-profit sectors.

In Scope:

- Start with the client centric and privacy enhancing principles.
- Supporting activities include:

    - A review of general considerations and key principles for residency
    - A review of the types of proof of residency framework
    - Identification of sources and characteristics that provide strong proof of residency
    - Enumeration of public and private sector residency use cases
    - Identification of potential relying parties and the business model for residency proofing
    - The selection of a model that could deliver an effective framework
    - Evaluation of how proof of residency fits within the DIACC Trust Framework activities
    - A proof of concept mock-up
    - A whitepaper discussion on the feasibility, opportunities, barriers and results

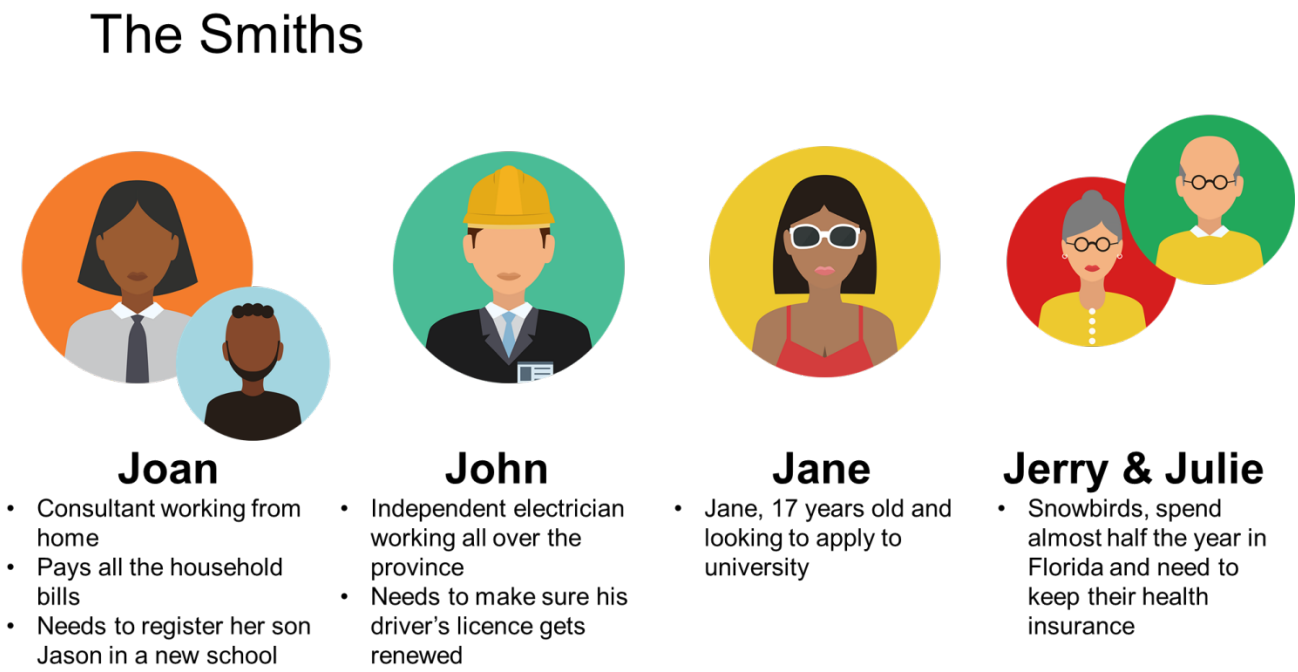
Out of Scope:

- Proof of identity
- Entry and departure information at border crossings as a source of information
- Detailed technical solutions
- Current market analysis and summary

Supporting Story

To demonstrate why online proof of residency is important, consider the Smiths.

The Smiths are a pretty typical family in Canada; they are busy with multiple household jobs, have growing families and are concerned about aging parents.



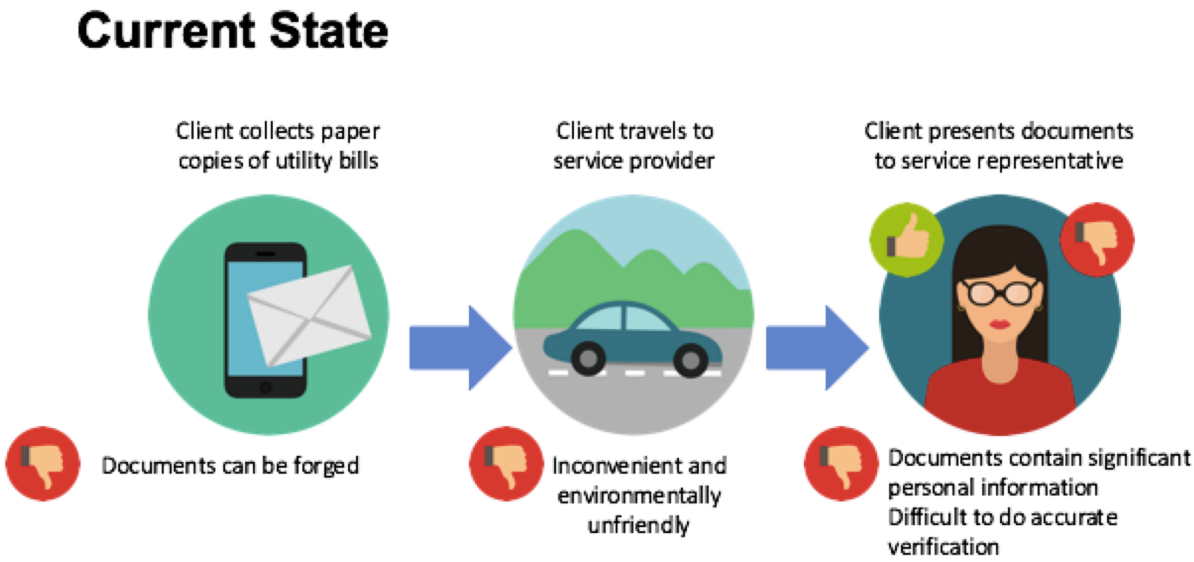
For each of the services above and dozens more, proof of residency is essential.

Current State

However, residency proofing has been done for decades, but has not improved substantially: it is inconvenient for clients, labor intensive (costs have gone up) and it keeps getting more complex as fraud and tools to make forged documents become more accessible and sophisticated.

Today, there is no online method to reliably "prove" an applicant's residency in a given jurisdiction and for a given period of time. Residency is currently determined offline, using a variety of documents as evidence (e.g. a utility bill under the person's name, for a qualifying address) which may or may not provide a strong indication of their presence, and which can be easily forged.

.



This process is complex to administer, to validate and, for the resident, to understand. For example, a provincial health plan may require three original documents: a proof of citizenship a proof of residency and a support for identity. Typically, over 15 types of documents may be accepted for any one of these proofs, although programs may also reserve the right to request additional documents. This process can be confusing for clients. And because they do not fully understand the types of documents needed, some clients may bring more information than necessary, undermining their own privacy.

Additionally, many of the documents that are accepted as proof could be easily forged in today's digital age. As a result, the person validating the residency needs to be trained with all types of documents, to be able to detect forgeries and to spend time analyzing the original documents. Parties that keep copies of the proofs also need to securely administer the document's lifecycle to manage the risk of privacy disclosure at all times.

Overall, this burdensome process translates into costs, delays, errors, fraud, privacy issues and frustration for all stakeholders.

But it doesn't have to be this way.

An effective Proof of Residency and Activity framework can be a game changer that will enable greater efficiency – both in person and online. Consider, for example the, many government programs that require proof of residency – from health insurance plans to grants programs, or the school fees that are dependent on whether you live in a specified neighbourhood or not. These are just a few of the ways that hundreds of thousands of residents across Canada need to prove their residency each year.

The Framework

The Framework sets out a proposed set of principles, practices and relationships that would enable citizens to provide proof of residency online to both private and public sector parties. By creating a common Pan-Canadian framework for all online residency proofing activities private and public sector parties will realize efficiencies in operations while clients will enjoy greater convenience and privacy than exists within the current in-person experience.

This Pan-Canadian residency proof framework is based on datasets, generally correlated, that provide a confidence level of a client's residency. The residency validation provides a simple and efficient answer: either the input data (evidence) meets or does not meet the level required by the requestor. The benefits for all parties are compelling:

- Data correlation can be constantly adjusted and improved to lower fraud, errors and costs.
- The client is at the centre of the data exchange. Source datasets are never exposed and remain confidential to all parties, ensuring privacy.
- Original proofs don't need to be copied and are safely archived over time by the program.
- Privacy by Design – authentication is only done with the explicit and clearly informed request of the client; only the minimum personal information is accessed to validate the client's assertion

As with any framework of this type, this one errs on the side of caution. The objective is to address the most common cases at first. Exceptions would be handled using the existing framework: in-person proofing.

Foundational Elements

The following six pre-requisites are required prior to implementing electronic Proof of Residency validation:

a) The level of validation required for a given program.
b) The validation processes and data sources that are acceptable to use.
c) The legislation and policy changes to use various data sets both in public and private sector organizations.
d) The legislative changes to be able to collect and disclose information electronically, across the public and private sector organizations, as selected by the client.
e) A framework for trust between organizations offering and accepting a proof of residency
f) Review of the in-person alternative to ensure it does not become the easier validation process.

This paper focuses on establishing a consistent foundation for pre-requisites a) and b). Additional work will be required to more fully address the other pre-requisites.

Different Confidence Levels for Different Programs

(see Sources of Residency Proof – Authoritative Parties)

Each stakeholder has their own requirements for proof of residency; balancing risk and burden, decision makers, administrators and clients understand that requirements for purchasing a cell phone are not as stringent as those to get provincial health insurance coverage.

The same logic applies to online residency validation. As such, four simple levels have been defined for the proof of residency:

Level Of Proof (LOP)	Description	Characteristics	Acceptable Proofs
1	The **address exists**.	Have a Verified Address	• A claim or statement of address Verification that address is valid
2	The address exists and the **individual is associated to that address**	• Have an address associated with a name, and; • Have proof that the address is in use by the individual OR • Have proof that the individual has been physically active within the geographic area	• An identity document AND • A utility bill, with usage, addressed to the individual • Address activity verification OR • Received services from the organization recently Physical activity at a trusted 3rd party within a geographic constraint
3	The address exists and the individual is active within the jurisdiction **for a given period of time**.	• Have an address associated with a name, • Have proof that the address is in use by the individual, and; Have proof that the individual has been physically active within the geographic area	• An identity document AND • A utility bill, with usage, addressed to the individual • Address activity verification • Received services from the organization recently Physical activity at a trusted 3rd party within a geographic constraint
4	The address exists, the individual is active within the jurisdiction and **there are multiple corroborating proofs of that activity**.	• Have an address associated with a name, • Have proof that the address is in use by the individual, • Have proof that the individual has been physically active within the geographic area, and; • Have multiple, corroborating, parties confirm proof of physical activity • Physical presentation of claim OR Authoritative proof of entry and exit to geographic area	• An identity document AND • A utility bill, with usage, addressed to the individual • Address activity verification • Received services from the organization recently • Physical activity at trusted 3rd parties within a geographic constraint • In-person presentation of residency claim within geographic area OR (hypothetical and wouldn't solve provincial residency) Border exit/entry control

A higher level is not always necessary, or even wanted, as it raises costs, privacy issues and can be a burden for the client. The framework envisioned is flexible so different risk tolerance can be managed through different proof types.

Residency Eligibility Characteristics

Location: Primary home address and its geographic location is the most obvious element of residency and is the key element of proof. The type of proof, for residency, attempts to increase trust that an individual was within the specific geographic location(s) to be eligible for a program.

Time: Each program has a separate requirement for time associated with residency. The requirement for a new application may be different than at time of renewal. Note that the levels of proof 3 and 4 require some longer term residency within the geographic area to be resolved.

Legal: Legal is another independent measure of residency. Each program may have its own legal residency (e.g. citizenship and/or immigration status) requirement and the burden of proof for that is based on the program qualifiers. A person may achieve a level 4 of residency proof even though they are not a legal resident (or do not have to prove legal residency). Likewise, an individual who asserts legal residency does not prove that they are physically associated with a qualified geography.

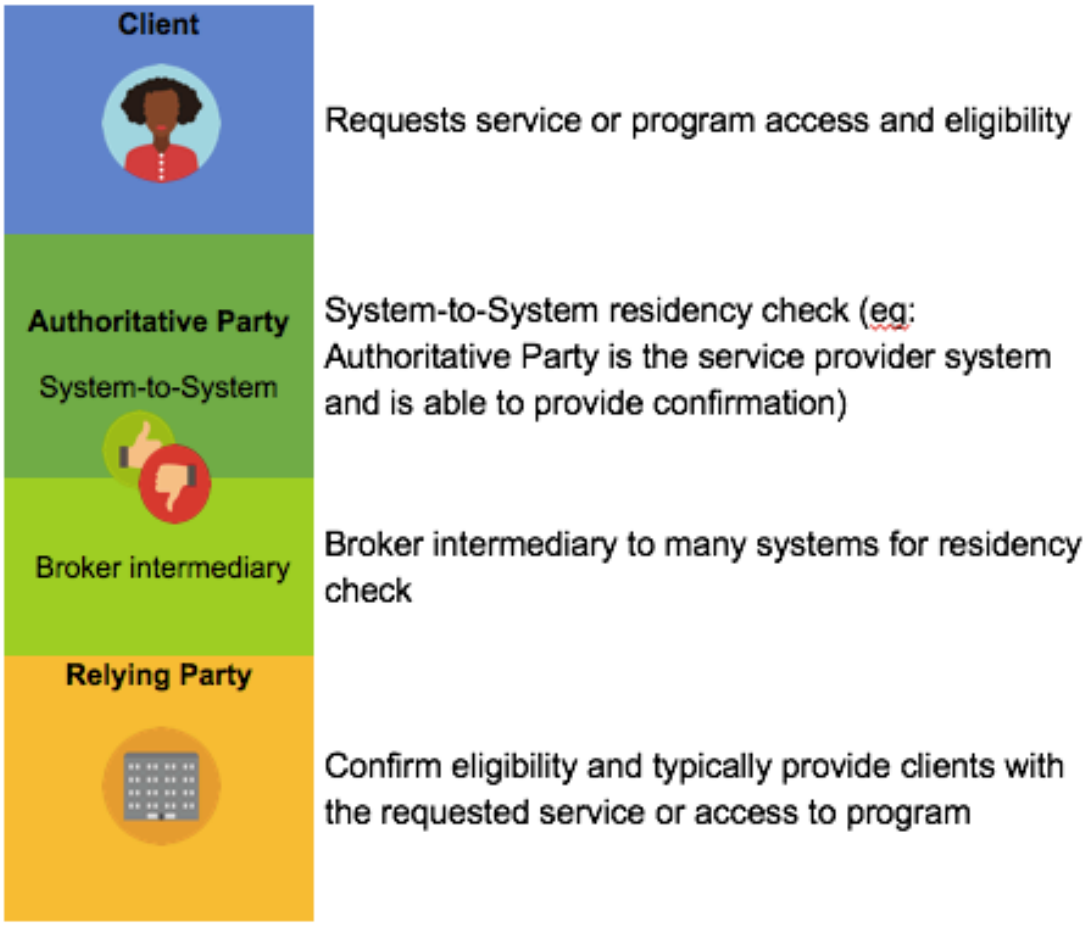
Stronger Ties: There are situations where an individual may maintain enough of a presence to pass residency qualifications in more than one jurisdiction. Under this scenario, programs will need to adjudicate whether the strong claim to residency is within one jurisdiction or another.

Impacts/Relations to Identity Levels of Assurance (LOA)

The Identity framework issued by Federal Treasury Board Secretariat (TBS) provides a strong foundation for assessing levels of identity assurance. Replicating these practices and principles for residency should provide us with an equally reliable method to determine the strength of proof of an applicant’s residency.

Business Model

To support the generic business use case, there are up to four identified parties that may play a role:



This section aims to provide a framework by which the various parties will engage to provide a confirmation of residency to meet the requirements of the Relying Party, for program eligibility or continuity of eligibility, as required.

The default process is to confirm identity, and confirm that the individual's claim of residency is supported and validated. The identity requirement is used for two things:

a) Informed and knowledgeable consent to disclose information related to claims of residency
b) Confirming the individual's residency claim based on the level required by the Relying Party

An underlying assumption is that the Relying Party's business objective is to validate the residency claim to support eligibility for a program, service or grant.

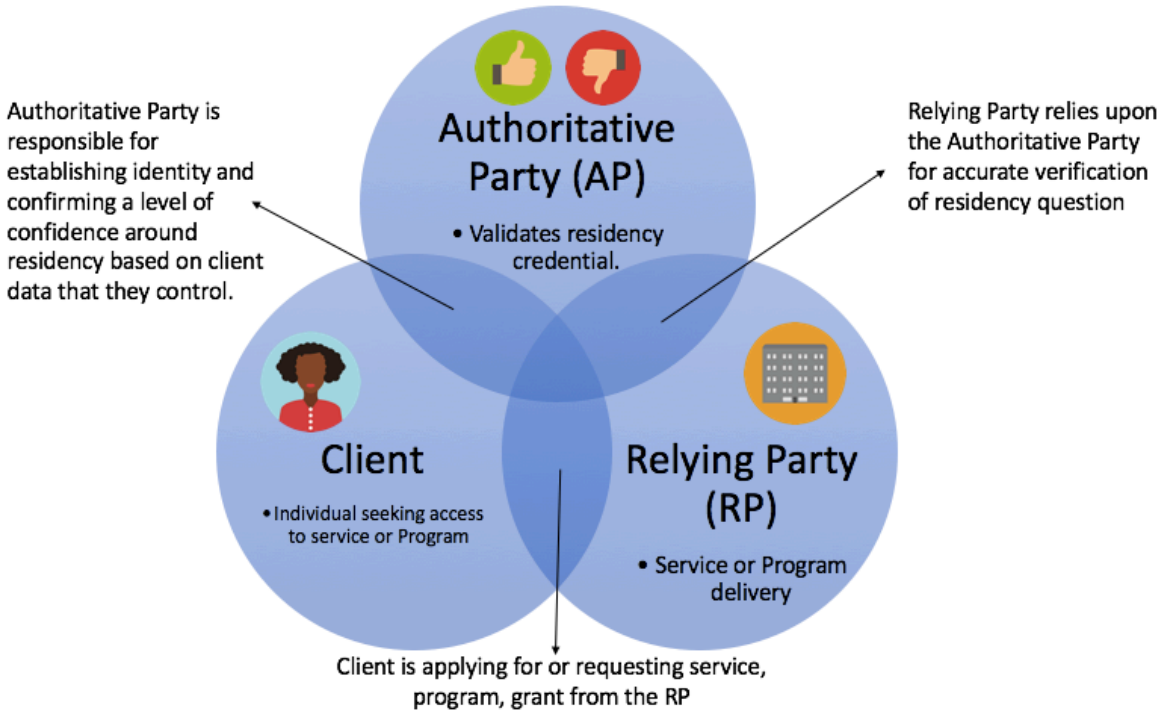
Business Model for Authoritative Party and Relying Party

To satisfy program eligibility, as confirmed by the Relying Party, typically the client must demonstrate their residency. The Relying Party is responsible for the policies by which the level of confidence required on residency and activity at such residency is satisfied.

As with identity validation and verification, the Authoritative Party will receive the request from the client, if required to confirm identity, and will use a set of standardized requests to validate the residency to the level required by the Relying Party. Depending on the level of confidence required, options may be presented to the client to select the method by which they wish to validate their address and activity at the specified address.

To this end, the client will have a single and simple transaction to complete. The act of selecting the option(s) to use for validation will also enable the consent process to share personal information with the Authoritative Party, a potential intermediary broker, and to the service providers selected by the client.

As noted in the section above, there are several sources of residency information and validation. Each of these service providers may have a different approach or algorithm to confirm the confidence level associated to the residency requirement, but should provide a standardized 'yes/no' answer to the Relying Party.



More investigation needs to be done to compare and contrast the data available and possible implementation alternatives between the various service providers to ensure they are each providing the equivalent semantic answer.

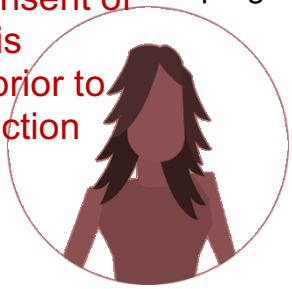
For example, how does a mobile phone carrier's data (e.g. call origination and text message geo-scoping) compare with a financial institution's data (e.g., ATM withdrawals and payroll data) in answering 'has this client demonstrated a living footprint in a geographic area for the past 200 days?'.

Framework

Getting the privacy model right is key for meeting both policy objectives and for client acceptance. Best practices promote the use of user-centric models for this purpose. So a transaction to validate the client's claim of residency would be orchestrated between the Authoritative Party and Relying Party through a service, and completed with guidance to the client about the scope of data to be shared, for what duration, and the named parties that will have access to the information. If a number of options are available to confirm the claim of residency, the client should have the ability to select which he or she wishes to use. By providing a complete disclosure of the proposed transaction details, based on the selection of service providers, the explicit consent of the client is obtained prior to the transaction commencing and being completed.

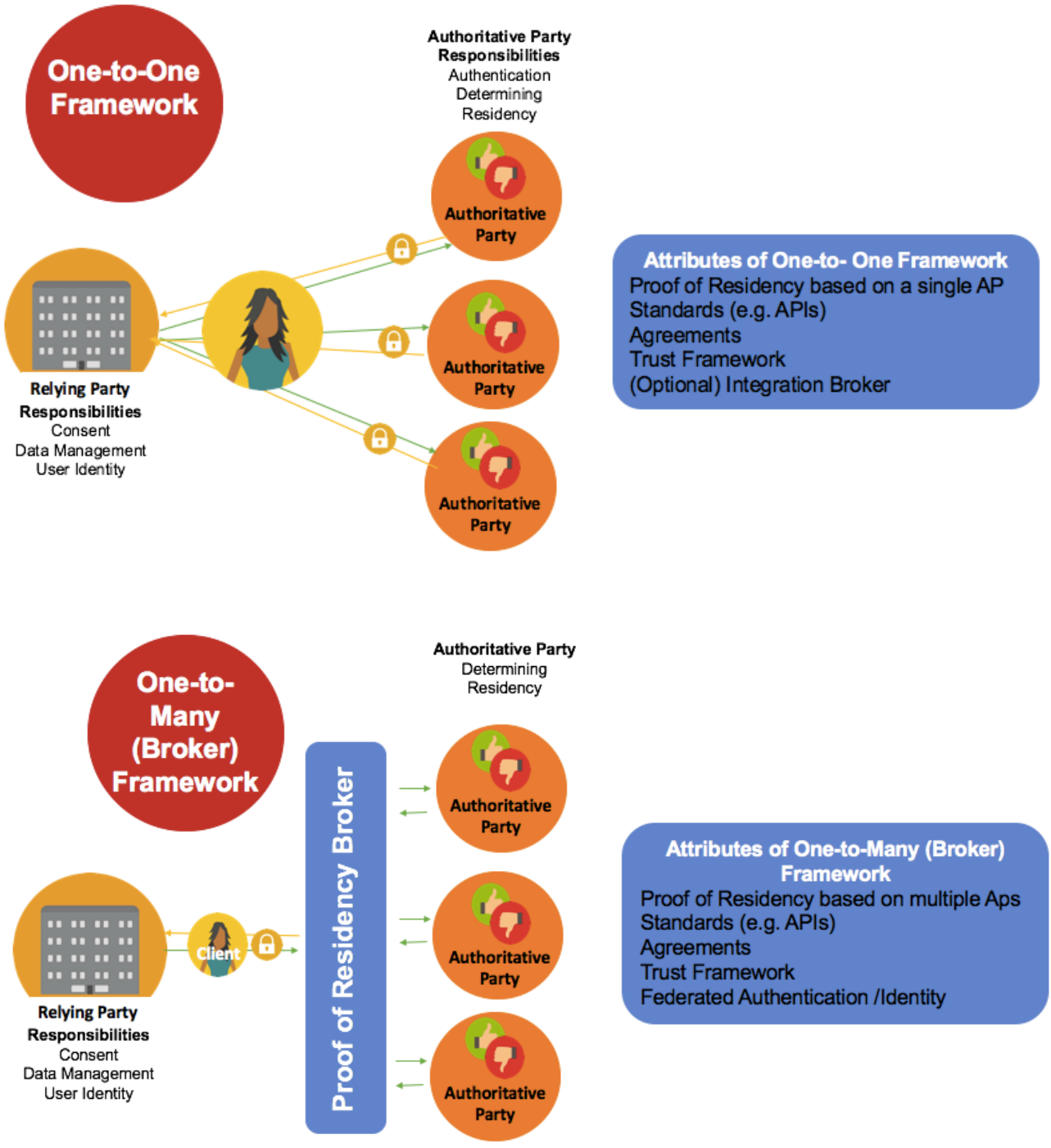
By providing a complete disclosure of the proposed transaction details, based on the selection of service providers, the explicit consent of the client is obtained prior to the transaction

There will be different needs dependent on programs. Some will require a proof of residency to be completed on each enrolment, where others may require it depending on the type of transaction or risk (e.g. an existing client is lower risk and wouldn't require additional proof). For some programs, there may also be a requirement to verify continued eligibility over a period of time, and the eligibility would be provided with an expiry for revalidation prior to continuation. This would translate into one transaction per client per program, per eligibility period. For example, one residency check per client every five years is typically required to reconfirm eligibility for health coverage. Whereas only one residency check is typically required for students enrolling at a new university.



As there are multiple Authoritative Parties, depending upon the proof level required, Relying Parties may determine which Authoritative Parties are appropriate or that a number of Authoritative Parties will be required.

There are two different operating frameworks that could provide proof of residency one-to-one and one-to–many. The one-to-one model enables a client to have complete control over the entire transaction, however it also requires the client to establish a direct relationship with each relying party and authoritative party every time that the client wishes to prove their identity online. By contrast, the one-to –many model works through a trusted broker who is able to connect the client with multiple authoritative parties delivering a more efficient client experience.



Recommendation: Proof of residency should not be done on a Relying Party by Relying Party basis. It must be developed as a framework that can be deployed across both public and private sectors to enable one-to-one or one-to-many verifications.

Sources of Residency Proof – Authoritative Parties

(see Different Confidence Levels for Different Programs)

There are many sources that can become Authoritative Parties from which we can poll and gather Residency proof on individuals.

Principally, there are information sources available at the Municipal, Provincial and Federal levels, as well as through Crown Corporations and private sector sources. Examples include the following:

	LOP 1	LOP 2	LOP 3	LOP 4
Canada Post	**X**	**X**		
Utility Companies	**X**	**X (weak)**		
Financial Institutions	**X**	**X**	**X**	
Telecommunications Companies	**X**	**X**	**X**	
Loyalty Companies (e.g. Aeroplan)	**X**	**X**	**X**	
Government (e.g. Border Services)	**X**	**X**	**X**	**X**
Multiple Level 3 Providers	**X**	**X**	**X**	**X**

X – May have data to provide this Level of Proof

Recognizing that individual clients have different profiles and relationships, there is no single authoritative party which has the ability to provide 100% coverage or definitive accuracy of the data. Below is an initial list of potential Authoritative Parties which have some coverage of the population. Value from an Authoritative Party comes from having broad population coverage, accuracy and currency of data, preferably with continuous interactions to populate the database over a period of time.

Government Sources

Some areas that could potentially provide information on an individual's residency include:

- **Provincial Health Insurance Organizations** – information on frequency of use
- **Provincial Driver Licencing** – by law, address must be current
- **Canada Revenue Agency** – information from tax forms could be used to help determine a client's address
- **Land and/or Municipal Tax Office** –can provide proof as to an individual's association with a given address
- **Canada Border Services Agency** - may have information to provide definitive entry / exit information for a geographic area that spans Canada (Out of Scope)

Although much data rich information exists within governments, collaboration and ease of access are areas that require further exploration.

Crown Corporations

- **Canada Post** - An authoritative source on valid addresses (level 1). Canada Post also has the ability to provide evidence of a correlation between a specific address and an individual to satisfy level 2. Since Canada Post is unable to ascertain information about activity away from a registered address it is unable to provide any confidence in level 3 or 4 proofs on its own.

- **Utility Companies** - Utilities can provide a weak correlation between the individual named on the agreement and the physical location. Without a reasonable measure for occupancy, the strongest assertion a utility could make is that the address exists (level 1) and that the named individual pays the bills (weak level 2).

Private Sector

Possibly the best two types of organizations that could provide sources of residency assurance are financial institutions and telecommunications organizations. They maintain key information on each client (name, DOB, etc.) and frequency of service or issuance of services are both elements that could be used to aid in residency assurance.

- **Financial Institutions -** Financial institutions have a unique view into their clients' activities for the sake of client service and protecting the integrity of the institution. While a mortgage institution may be able to provide strong evidence of ownership to a specific property, it doesn't imply a link to the individual's activity. Daily activity on a chequing account or credit card that is physically based within the jurisdiction is reasonable evidence that the individual making the claim is resident.
- **Telecommunications Companies -** Recognizing the diversity of business within Canada's telecommunications companies (internet, wireless, home phone, television), telcos may be active at multiple levels of proof within this framework. While the level of data available would depend upon the service provided (Pre-paid/ monthly billing/ business) wireless (cell phone) providers, as an example, can develop strong evidence that the individual tied to a phone was active within the jurisdiction. The expectation is that telecommunications companies would determine whether the device was used in a manner consistent with an individual resident within the geographic area. Once this determination is made, the company could attest that evidence of residency exists.
- **Loyalty Companies -** Similar to financial institutions, loyalty companies (like Aeroplan, Optimum or Air Miles) can provide evidence to support use of their products within the given geographic area. The nature of the transaction (swipe) provides a weaker level of authentication; however, the "big data" approach to loyalty products may provide stronger correlation to average activity of its users.

The exercise identified a few key sources for residency information and the expected levels of proof they would provide.

Multiple Level 3 Providers: For corroborated evidence, a relying party may select to query more than a single level 3 provider. If all providers provide evidence of residency this could be considered a level 4 proof.

Recommendation: Authoritative and Relying Parties establish common rules of engagement to ensure data accuracy, consistency, transparency and that the client's privacy and security concerns are addressed and respected. A Canadian Trust Framework would go a long way to ensuring a common approach.

Anticipated Volumes

It is very difficult to project volumes for a service like this without more data and time to explore the Relying Party requirements, programs, and current volumes. Some Relying Parties are only going to use the service once per user (like a university, for example) and others will be conducting transactions every five years (eg: healthcare).

Composition of a Proof

Four key factors of a proof were identified:

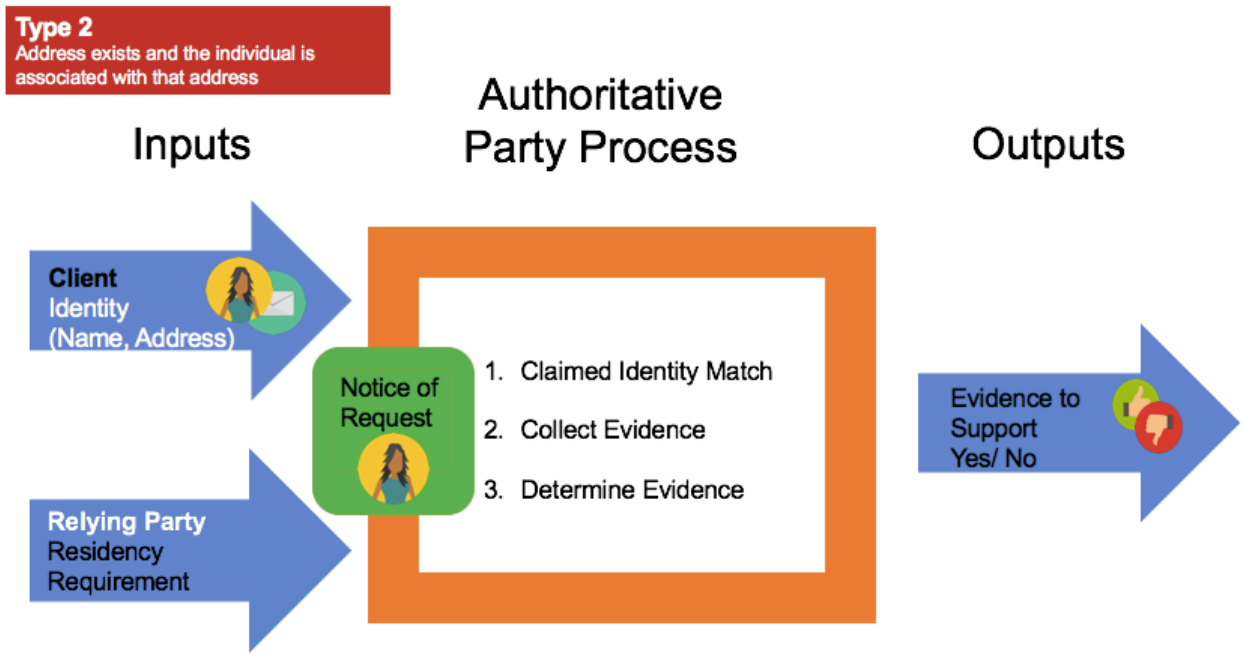
- Consistent questions independent of Authoritative Party
- Transparent information being passed between parties
- Identity and authorization captured in appropriate places
- Minimization of data transfer or data sharing

The process for a Level of Proof 1 and 2 are slightly different than a level of Proof 3 and 4. The critical difference between the levels is the amount of information required from the individual to collect and provide the residency proof.

Level of Proof 1 & 2

The information for a level 1 and 2 is nearly public and, with a weak level of confidence, could be determined from a phone book. Given the nature of the proofs, the burden of user proof and consent is lowered.

As with all transactions, the client must be informed of options on a negative result including the use of legacy processes. In all events, the relying party will not receive any of the client's personal data beyond a yes/no response to the initial question.



Input:

- The client must provide a validated address and name (level 2 only).
- The Relying Party must provide a Level of Proof request

Notice of Request:

- Provide the individual a notice of request against the authoritative party

Authoritative Party Process:

- The Authoritative Party processes the request
- On a match of name and address AND evidence of residency the Authoritative Party provides a positive response
- If a name and address do not match, or information is wrong the Authoritative Party's response is negative. Specific error code responses are not permitted.

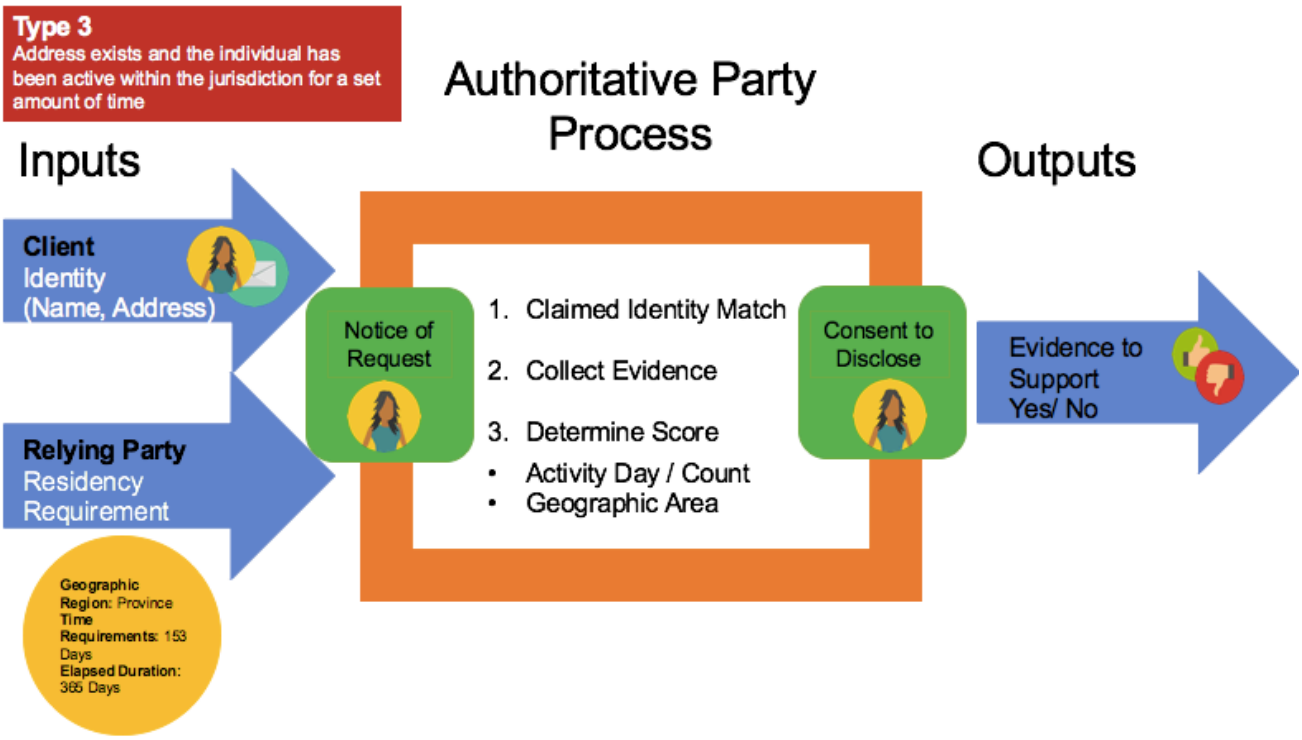
Output:

- A positive or negative response based on the information available to the Authoritative Party

Level of Proof 3 & 4

The information for a level 3 and 4 is generally more private and identifying. Given the nature of the proofs, the burden of user proof and consent is raised. A Relying Party may leverage multiple providers to achieve sufficient proof of residency to meet their individual risk requirements. For example, they may query Canada Post for an authoritative address and a Financial Institution for activity within that geographic area over a given period of time. The Relying Party may also allow the client to query alternate providers on a failure.

As with all transactions, the client must be informed of options on a negative result including the use of legacy processes. In all events, the relying party will not receive any of the client's personal data beyond a yes/no response to the initial question.



Input:

- The client must provide a validated address and name
- The Relying Party must provide:
    - Geographic Region (based on Postal Codes)
    - Time Requirement
    - Elapsed duration
    - Level of Proof request

Notice of Request:

- Provide the client a clear and transparent notice of request against the Authoritative Party – make it clear what information is being sought, how it will be shared, used and stored

Authoritative Party Authentication:

- Where available and supported, a federated authentication from the Relying Party may be used, otherwise the Authoritative Party must authenticate the individual against their records

Authoritative Party Process:

- The Authoritative Party processes the request
- On a match of name and address AND evidence of residency provides a positive response
- If a name and address do not match, or information is wrong the Authoritative Party's response is negative. Specific error code responses (such as name mismatch) should not be permitted

Consent to Disclose:

- Prompt the client to confirm that the residency proof can be provided back to the relying party
- This is a confirmation, for purposes of transparency, of the client's informed, knowledgeable consent to provide information to the Relying Party

Output:

- A positive or negative response based on the information available to the Authoritative Party

Calculating Confidence

After selecting a level of Proof, there are multiple ways to calculate confidence in that level.

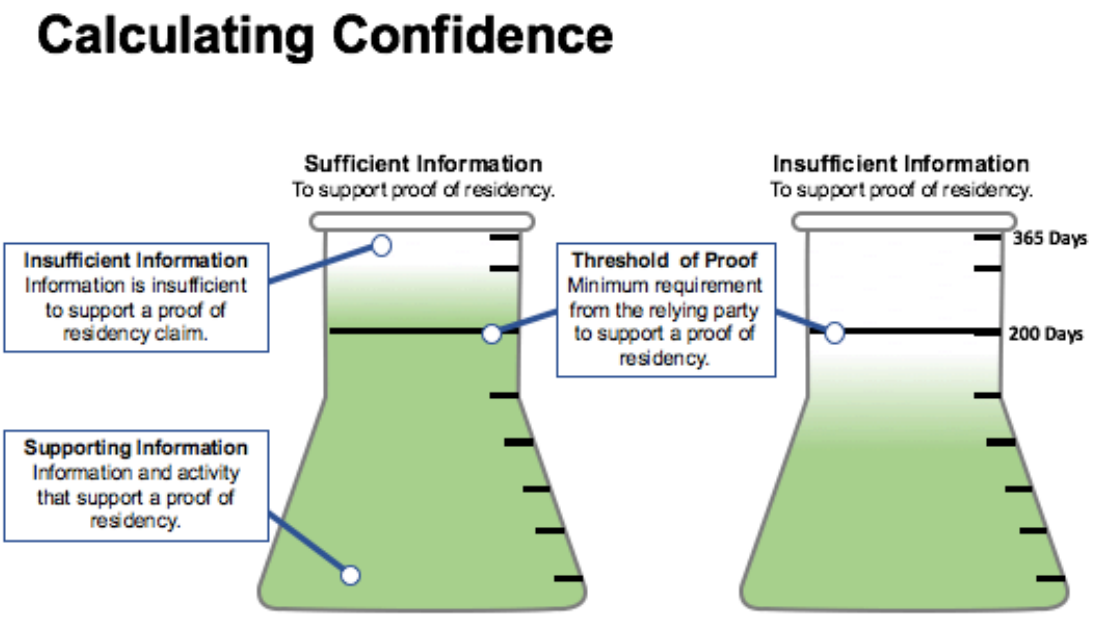
Level 1 and 2 do not provide evidence of activity within the geographic area and have a slightly different approach to confidence. The validity of an address (Level 1) is a binary decision and the correlation of the individual to an address is dependent on the provider organization. A utility may provide a connection to the name on the bill, whereas Canada Post may provide proof of the address being used by any occupant.

Level 3 and 4 proofs require evidence of activity. For initial implementations, it's recommended to use a straight-forward method – specifically counting the number of activity days.

Each provider may have different patterns of use, below are hypothetical examples of the types of patterns seen in the Financial and Telecommunications industries.

The question posed to the providers was the same: *"Was this individual resident within the province for 156 days in a 365 period?"*

While both providers have enough evidence to support a possible assertion, they each had different patterns of activities.



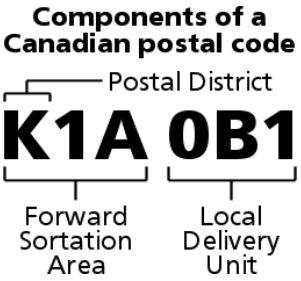
Long Term Evolution

Over the longer term there are opportunities to enhance the framework to calculate confidence and provide a more specific measure.

Geographic Assertions

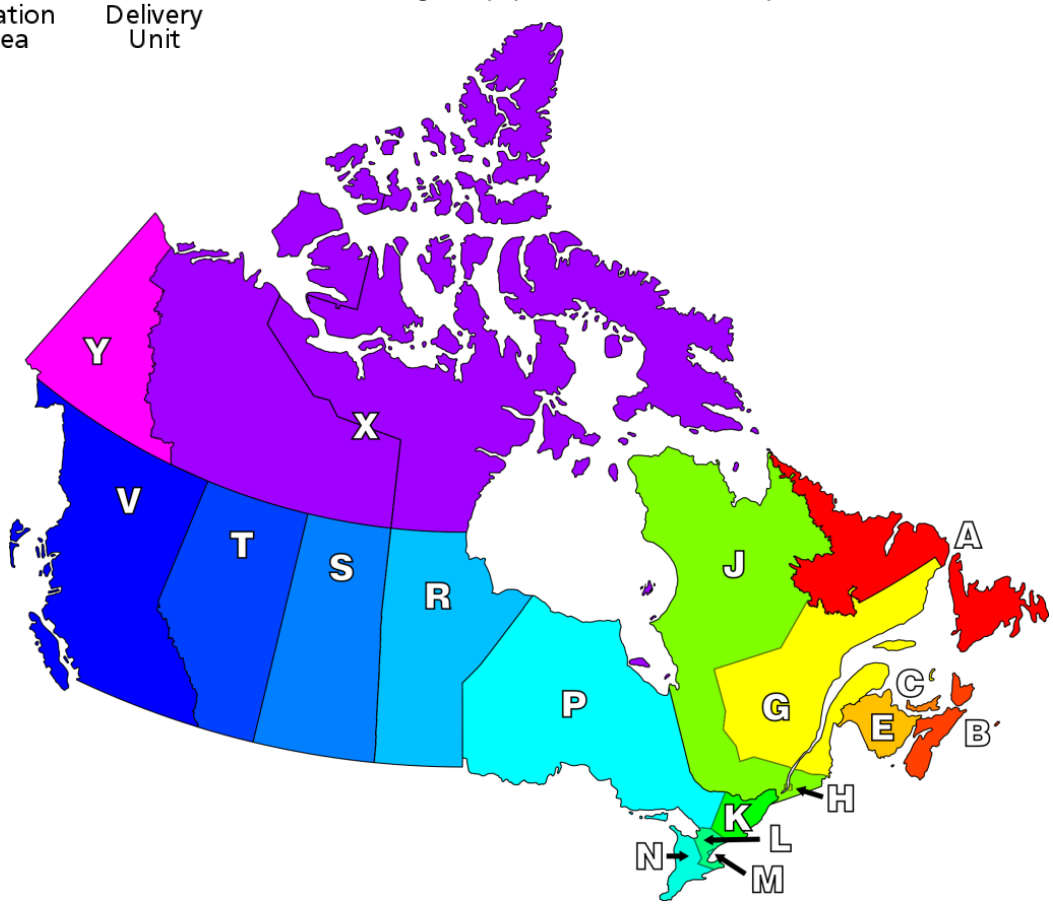
Proof of residency should not be limited to traditional federal or provincial borders. A pan Canadian framework must allow for requests based on specific geographic regions. The recommended approach is to leverage the existing Postal Code system within Canada to constrain the geography of the requests.

This should allow municipalities, school districts, and other regional boundaries to make residency requests. This approach will also permit requests that span multiple provincial boundaries, such as rural and northern programs.



The request should consist of one or more Canadian Postal Districts and/or Forward Station areas. There should be very few scenarios requiring a local delivery unit, unless the request is to verify a specific address which is already part of a residency proof.

The following map provides an example of how the Postal Districts are distributed across Canada (source: Wikipedia).



Recommendation: Leverage the existing Canadian Postal Code system to codify requests for specific geographic areas.

Key Considerations

This section outlines the barriers and challenges that could be faced in developing an electronic residency check service.

We would also point out that, as set out in the problem statement above, there are a number of barriers and challenges within the current system, many of which are addressed with the online model that we are proposing including: increasing privacy, decreasing ease of fraud, and increasing client convenience.

There are five key areas to consider:

- Will this framework create new legal liability risks or modify existing ones?
- How can this framework comply with the tenets of privacy law at the provincial, territorial and federal levels?
- What existing legislative or policy barriers may need to be overcome to launch an electronic residency check service? And how should an electronic residency check framework policy be devised to maintain or strengthen current framework integrity?
- What incentives are required to create a healthy ecosystem of Authoritative Parties?
- Are the current procurement methods and vehicles of government suitable? What issues or risks should be taken into consideration?

Legal / Liability

It is important to consider whether an electronic residency check service would create new legal liability risks or modify existing ones as decisions made as a result of erroneous information can have serious financial implications for clients and/or relying parties. Further, the degree to which an Authoritative Party may be held liable for erroneous information will affect an organization's decision on whether or not to become an Authoritative Party.

Setting aside privacy considerations which are dealt with in the next sub-section, the following legal issues should be considered:

1. **Would an Authoritative Party incur liability with regards to erroneous information provided to a Relying Party?**[1]

   This issue would arise in a situation where an Authoritative Party tells a Relying Party that an individual satisfied a level of proof whereas, in reality, the individual failed to meet that level of proof. Further, based on that error, the Relying Party incurs costs.

   This issue could also arise in the event that a client is denied access to a service or other benefits by a Relying Party because they fail to meet a level of proof according to erroneous information provided by an Authoritative Party

[1] Note: requires different analysis and results depending on the applicable level of proof

Recommendations:

a. Relying Parties and Authoritative Parties should have a shared understanding that Authoritative Parties have an obligation of means not of results. In other words, the normative framework (legislation, regulations and policies) and/or contract should impose on Authoritative Parties an obligation to put in place and maintain sufficient processes and IT safeguards to provide correct information according to the levels of proof but no obligation to provide correct information for every request;
b. Authoritative Parties should remain liable for intentional or gross negligence errors leading to erroneous information being provided to Relying Parties;
c. However, a negative response from an Authoritative Party must only conclude that there is insufficient information and must not be interpreted as a definitive statement that the individual was not resident. Given the nature of a proof of residency, the Authoritative Party could only, at most, claim that it doesn't have information to conclude the individual is resident.
d. The normative framework and/or contract should allow Relying Parties to submit Authoritative Parties to discretionary process audits at the expense of Relying Parties. This would ensure that processes put in place by Authoritative Parties meet the applicable level of proof;
e. Alternatively, insurance coverage could be sought to address such cases (either by the Authoritative Party or the Relying Party).
f. Additionally, Relying Parties should provide clients with the opportunity to select an additional Authoritative Party and provide an alternate form for proving residency.
g. Relying Parties should provide clients with recourse to appeal decisions that involve an Authoritative Party. Such recourse should afford clients an opportunity to present evidence of fulfillment of residency conditions and such evidence, together with the evidence provided by the Authoritative Party, should be weighed on a balance of probabilities - whichever side is most convincing wins the appeal.
h. Relying parties should plan for and work out an appropriate compensation strategy and/or let the framework outlined above, take its course (see a, b, e and f)

2. **Would an Authoritative Party incur liability if unable to provide the information requested by the Relying Party?**
   This issue would arise in a situation where an Authoritative Party, operating under a Level of Service Agreement with a Relying Party, fails to meet the stated level of service in that agreement. This could occur, for example, in the event of excessive Authoritative Party downtime. Technology always fails and it sometimes fails beyond what was contemplated in a Level of Service Agreement. In this case, an Authoritative Party would logically attempt to limit or even avoid liability altogether whereas a Relying Party would likely insist on liquidated damages to put pressure on the Authoritative Party. This traditional approach may foster adversarial relationships and might be best accommodated differently.

Recommendations:

a. Plan for such failures and have backup services in place. Relying parties should plan for alternative sources of information or client service delays;
b. Relying parties should execute planned and unplanned Authoritative Party downtime simulations in order to gain confidence that Authoritative Party downtime can be efficiently accommodated.

Privacy

The focus on Privacy by Design is key to the framework. By putting the client, and more specifically the client's privacy, at the centre of the framework, control is in the hands of the client. The client initiates any requests. No information is requested or shared without the express and clearly informed consent of the client.

Clients have a right to privacy and many are concerned about how their information is collected, used and disclosed by governments, businesses and other organizations. Around one-in-ten Canadians cite privacy and confidentiality concerns as their reason for not accessing government services online.[2] Further, about eight-in-ten Canadians express concern about privacy, identity theft and how their information might be used.[3]

Given these considerations, it is clear that to implement a framework that has the public's trust and confidence, the privacy protections afforded by existing residency verification processes must either be matched or enhanced. That in mind, a future electronic residency check framework should be governed by fundamental tenets of privacy law which outline the rights of an individual with respect to their own personal information and how organizations may collect, use, and retain personal information. These tenets include the following:

1. An individual has the right to control his or her own personal information;
2. An individual must be notified when his or her personal information is being collected and when it has been disclosed to third parties.
3. Organizations may collect, use and retain personal information about individuals only when all the following conditions are met:
    a. The information requested is reasonably necessary for the provision of benefits, services or products and no supplementary information is requested;
    b. This information is kept for only the period of time necessary for the provision of benefits, services or products, and to ensure that the individual to whom the information relates has a reasonable opportunity to obtain access to their personal information, but no longer;
        i. Retention will be dependent on program or service and specific legal requirements for that industry or government program
        ii. Both APs and RPs are expected to keep audit records of the query
    c. The individual must have consented to how their personal information will be used;

[2] Citizens First 7, National Report, 2014
[3] Ibid

Recommendations:

a) Any future framework should build in privacy by design.
b) A future framework should be based on a client-consent model. Where clients do not consent to an electronic residency verification process, alternative means to prove residency should be provided.
c) Only the minimum information necessary to process a request should be exchanged between the Authoritative Party and the Relying Party.

Policy

A future residency check service must either comply with existing legislation, regulation, program and operational policies or those policies must be changed to reflect modern needs and requirements. For example, existing legislation related to privacy, accessibility, and the provision of French language services must be taken into consideration by all organizations (whether public, private or social-profit sector) involved in the provision of an online proof of residency.

While policy requirements may vary from organization to organization and across jurisdictions, generally, policy considerations could include:

- Establishing a legislative framework to enable an electronic residency verification to take place
- Establishing a contractual framework dictating the methods and standards by which an electronic residency verification could take place
- Defining service-specific policies for acceptable levels of proof and/or streamlining and standardizing policies across similar programs/services to ensure consistency in the verification of different types of residency claims
- Changing legislation or regulation to enable full online delivery of services that would rely on an electronic residency check service as one component of verifying program/service eligibility

More generally a policy statement outlining the governance for an online residency check should be developed. This statement could include the following terms:

- Relying Parties (Governments, Private Sector Users and Social-Profit Organizations) will ensure that reliable evidence is used to evaluate an individual's residency claim in determining eligibility for programs, services or benefits.
- Considering reliable residence evidence helps ensure fair access to benefits and services.
- In processing a residency check, Relying Parties will request only the minimum information required related to the individual requesting the service/benefit. The individual may at any time refuse to provide the information by not pursuing the service/benefit.
- Should the individual accept to provide the information, they may select who will provide the information to meet the type of residency proof specified by the Relying Party.

- Relying Parties will only keep the information related to a residency check for the duration needed, as authorized by the individual.

Business

The previous legal liability, privacy and policy considerations are factors that must be addressed to remove obstacles. However, even if all obstacles are removed, there is no guarantee that anyone will move forward.

To move forward, private sector participants need incentives - a business interest. At issue therefore is how can an Online Proof of Residency successfully attract the right balance and quality of Authoritative Parties (who are providing the information) and Relying Parties (who are relying on the information)? In other words, how can a win-win-win scenario be crafted for Authoritative Parties, Relying Parties, and Clients?

Recommendations:

a) Identify how much each Online Proof of Residency confirmation is worth to Relying Parties at levels 1, 2, 3 and 4. Worth is ideally determined by Relying Parties transparently answering the question “How much am I willing to pay for this?”;
b) Alternatively to (a), estimate the approximate savings per program a more reliable Online Proof of Residency would generate, divide those savings per the number of Online Proof of Residency requests to come up with a “per request” unit price;
c) Lead consultation sessions with representatives of Authoritative Parties to ascertain what Online Proof of Residency requests (at each level) can be accommodated at what price;
d) Build a business model taking into account high and low velocity Authoritative Parties, volume of transactions, Levels of Proof and capacity of Relying Parties to pay vs. value obtained;
e) Build consensus around the business model.

Recommendation: Develop a robust and consensual business model to help the Online Proof of Residency POC evolve into a full-fledged program.

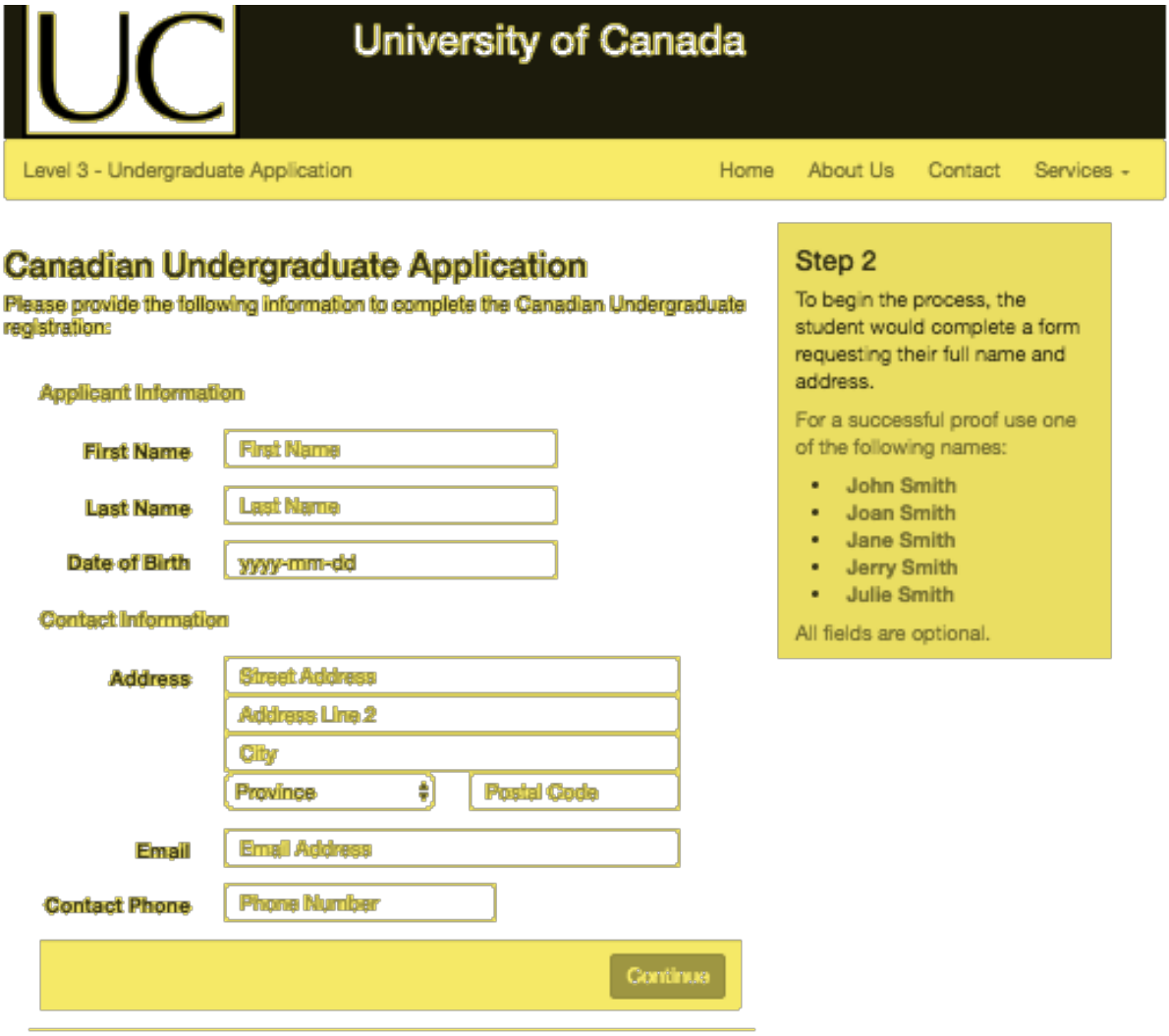
Procurement

As a non-profit association made up of public and private sector members, the DIACC does not advocate for any individual provider, platform or technology solution. Any procurement decisions will be made by the individual Relying Parties in accordance with their respective policies and practices.

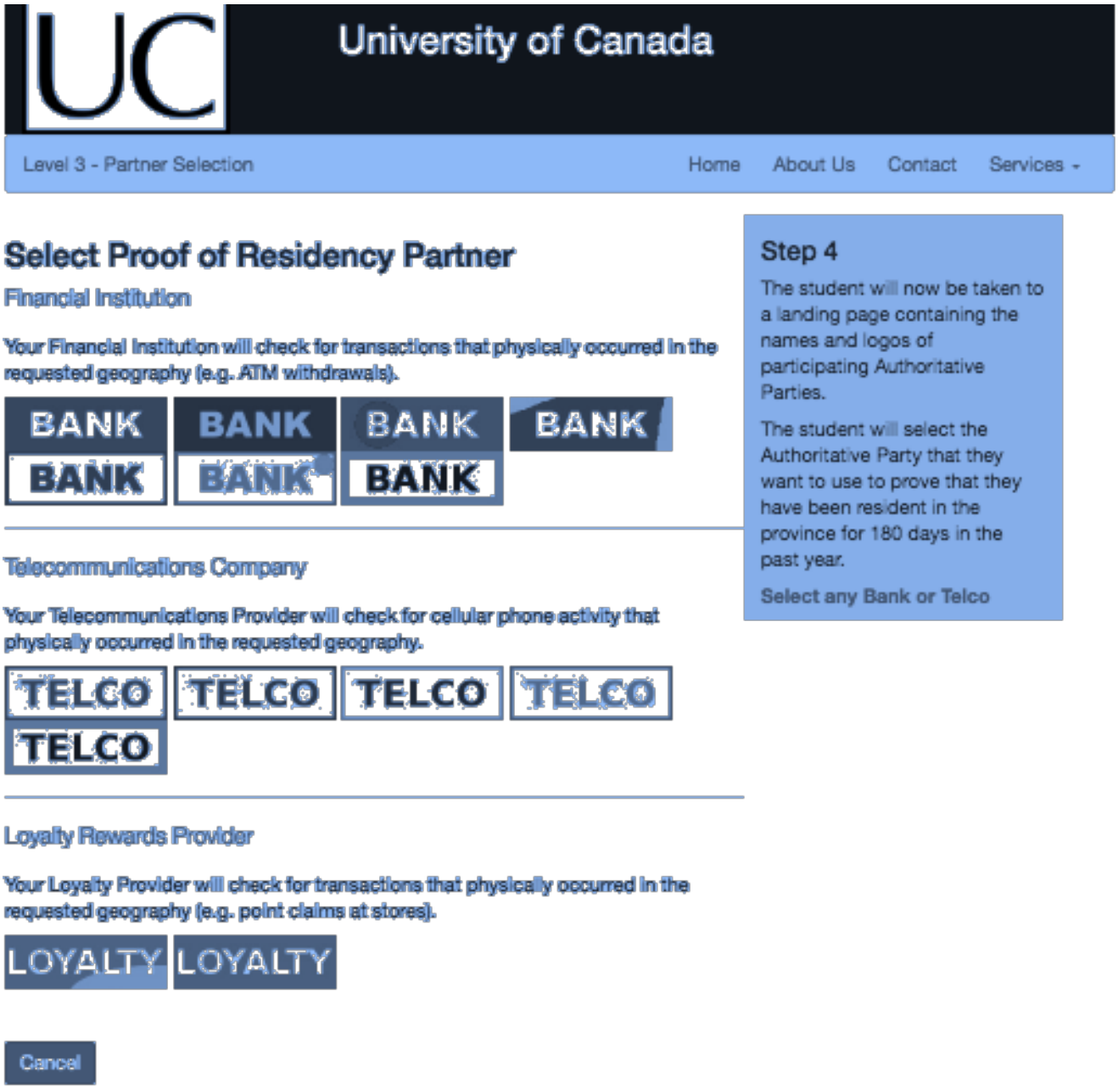
Proof of Technology

Detailed Explanation and Screenshots

Note that the following shots are of the level 3 residency proof. The model is similar for levels 1,2,4 and can be accessed here


University of Canada
Level 3 - Undergraduate Application
Home
About Us
Contact
Services
Canadian Undergraduate Application
Please provide the following information to complete the Canadian Undergraduate registration:
Applicant Information
First Name
First Name
Last Name
Last Name
Date of Birth
yyyy-mm-dd
Contact Information
Address
Street Address
Address Line 2
City
Province
Postal Code
Email
Email Address
Contact Phone
Phone Number
Continue
Step 2
To begin the process, the student would complete a form requesting their full name and address.
For a successful proof use one of the following names:
John Smith
Joan Smith
Jane Smith
Jerry Smith
Julie Smith
All fields are optional.


University of Canada
Level 3 - Proof of Residency
Home
About Us
Contact
Services
Proof of Residency Required
In order to qualify for Canadian Undergraduate student rates, we need to confirm eligibility.
University of Canada will allow you to select a partner organization to provide a proof of residency statement.
The provider will verify your account for activity to support your claim of residency. This does not provide UC access to any account information.
If your selected provider is unable to provide a confirmation, you will be asked to select another or use an alternate method. A negative result will not disqualify you.
The information sent to your provider inlcudes:
Your First Name
Your Last Name
Your Full Address
A request for a Level 3 proof of residency, within Canada, for at least 180 days in the past year.
Cancel
I Consent
Step 3
Reflecting the focus on enhancing privacy, transparency and client-centricity the student will now see a separate screen that will advise them that they will now be asked to select an Authoritative Party to confirm to their claim of residency.
The student will also be advised of what information is being transferred to the Authoritative Party, as well as the question that is being asked.
For the transaction to continue the student must explicitly consent to this activity.
CLICK I CONSENT to continue with the demonstration.


University of Canada
Level 3 - Partner Selection
Home
About Us
Contact
Services
Select Proof of Residency Partner
Financial Institution
Your Financial Institution will check for transactions that physically occurred in the requested geography (e.g. ATM withdrawals).
BANK
BANK
BANK
BANK
BANK
BANK
BANK
Telecommunications Company
Your Telecommunications Provider will check for cellular phone activity that physically occurred in the requested geography.
TELCO
TELCO
TELCO
TELCO
TELCO
Loyalty Rewards Provider
Your Loyalty Provider will check for transactions that physically occurred in the requested geography (e.g. point claims at stores).
LOYALTY
LOYALTY
Cancel
Step 4
The student will now be taken to a landing page containing the names and logos of participating Authoritative Parties.
The student will select the Authoritative Party that they want to use to prove that they have been resident in the province for 180 days in the past year.
Select any Bank or Telco

Sign in to Online Banking

Note: This site is for demo purposes only, please do not enter valid banking credentials

Card Number 1234********4321

Password Password

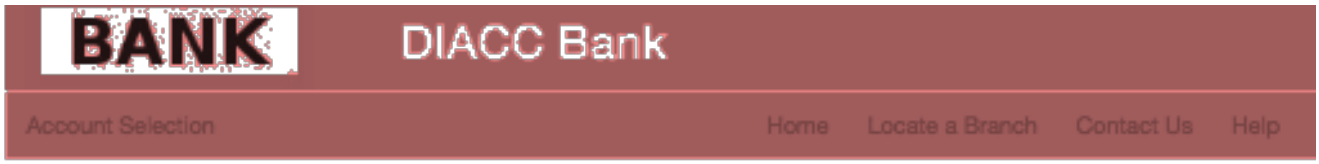
Cancel Continue

Step 5

The student will be asked to enter their banking credentials to log into their selected Authoritative Party.

It is important to note that while the banking credentials are being used to prove the student's residency, **no banking information is ever shared with the Relying Party.**

Click Continue



Select Account

Select the account to be used to verify residency

- **Chequing - 123 *** 321**
- **Savings - 321 *** 123**
- **Joint - 111 *** 333**

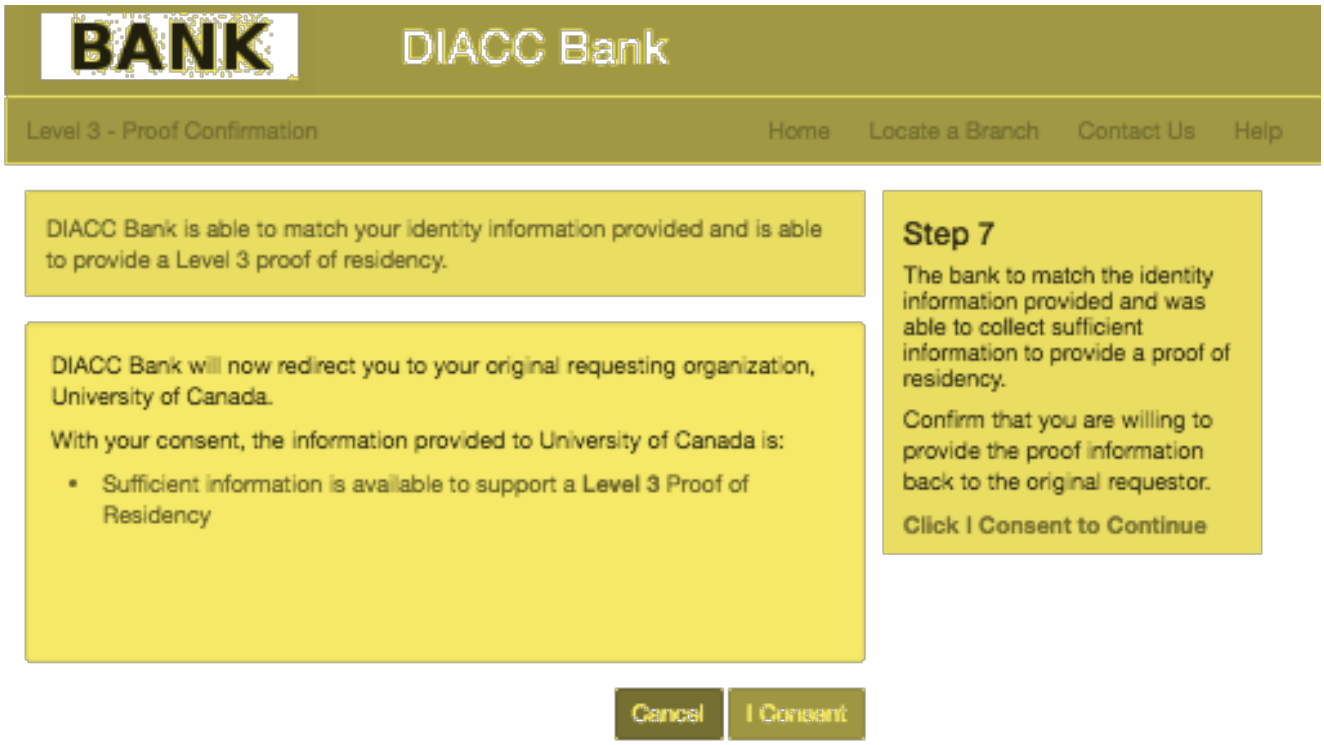
Cancel Continue

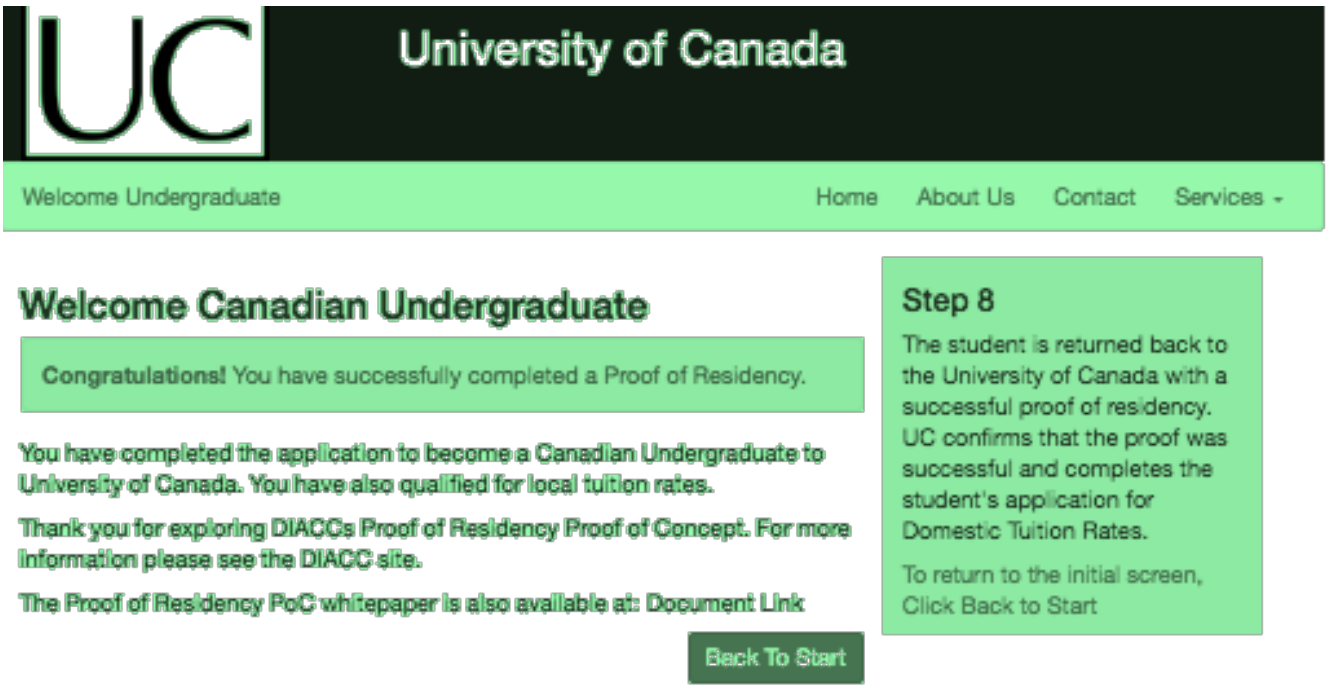
Step 6

The student will be asked to select the account that they want to use as proof of their residency.

It is important to note that while the banking credentials are being used to prove the student's residency, **no banking information is ever shared with the Relying Party.**

Click Continue


BANK
DIACC Bank
Level 3 - Proof Confirmation
Home
Locate a Branch
Contact Us
Help
DIACC Bank is able to match your identity information provided and is able to provide a Level 3 proof of residency.
DIACC Bank will now redirect you to your original requesting organization, University of Canada.
With your consent, the information provided to University of Canada is:
Sufficient information is available to support a Level 3 Proof of Residency
Cancel
I Consent
Step 7
The bank to match the identity information provided and was able to collect sufficient information to provide a proof of residency.
Confirm that you are willing to provide the proof information back to the original requestor.
Click I Consent to Continue


UC
University of Canada
Welcome Undergraduate
Home
About Us
Contact
Services
Welcome Canadian Undergraduate
Congratulations! You have successfully completed a Proof of Residency.
You have completed the application to become a Canadian Undergraduate to University of Canada. You have also qualified for local tuition rates.
Thank you for exploring DIACCs Proof of Residency Proof of Concept. For more information please see the DIACC site.
The Proof of Residency PoC whitepaper is also available at: Document Link
Back To Start
Step 8
The student is returned back to the University of Canada with a successful proof of residency. UC confirms that the proof was successful and completes the student's application for Domestic Tuition Rates.
To return to the initial screen, Click Back to Start

Conclusion and Recommendations

Traditional, in person, validation of residency has been the standard process for checking where people live for a variety of applications. However, the increase in demand, from clients and organizations, to move more transactions online to satisfy convenience and cost reduction objectives is pushing program and service providers to adapt and change the method of validating residency.

The challenge of validating residency online has been to develop a framework that stands up to the perception that physical documents and in-person transactions are the only reliable way to ensure clients are making truthful statements. With the increase of transactional data available on almost every client, it is now possible to confirm residency online with as much or more confidence than the in-person experience.

The challenge of validating residency online has been to develop a framework that stands up to the perception that physical documents and in-person transactions are the only reliable way to ensure clients are making truthful statements. With the increase of transactional data available on almost every client, it is now possible to confirm residency online with as much or more confidence than the in-person experience.

What can be a client experience nightmare, a sometimes frustrating process of proving residency can be made easier and enable previously marginalized clients access. Using a consent-based framework, individual privacy can be enhanced and transparency increased.

The focus on Privacy by Design is key to the development of any on-line identity and authentication framework. The client, and more specifically the client's privacy, must be at the centre of the framework, and control must rest in the hands of the client. The client initiates any requests. No information is requested or shared without the express and clearly informed consent of the client.

There is an opportunity to enhance how residency is evaluated within Canada. Private sector players (e.g. Financial Institutions, Telecommunications Companies, Postal Providers) and Government Organizations all have information that can provide benefits to other organizations.

The development of a trusted, transparent and privacy enhancing online proof of residency framework, built upon shared principles and rules, would:

- Increase privacy and convenience for clients
- Present cost savings for service and program providers
- Generate revenue opportunities for organizations providing proof.

The opportunity exists for a proof of residency framework in Canada that aligns well to Canadian progress in identity management. This framework requires trust and transparency between all parties to enable a quick and accurate digital proof of residency process. Failing a robust and consensual business model, the Online Proof of Residency POC may never evolve into a full-fledged program

Recommendations:

1. Any future framework should build-in privacy by design.
2. Any future framework should be based on a client-consent model. Where clients do not consent to an electronic residency verification process, alternative means to prove residency should be provided.
3. Enable an electronic proof of residency only if a privacy enhancing method of doing so is available
4. Proof of residency should not be done on a Relying Party by Relying Party basis. It must be developed as a framework that can be deployed across both public and private sectors and enable one-to-one or one-to-many verifications.
5. Authoritative and Relying Parties establish common rules of engagement to ensure data accuracy, consistency, transparency and that the client's privacy and security concerns are addressed and respected. A Canadian Trust Framework would go a long way to ensuring a common approach.
6. Leverage the existing Canadian Postal Code system to codify requests for specific geographic areas.
7. Only the minimum information necessary to process a request should be exchanged between the Authoritative Party and the Relying Party.
8. A negative response from an Authoritative Party must not be interpreted as a definitive statement that the individual was not resident.
9. More generally a policy statement outlining the governance for an online residency check should be developed. This statement could include the following terms:
    a. Relying Parties (Governments, Private Sector Users and Social-Profit Organizations) will ensure that reliable evidence is used to evaluate an individual's residency claim in determining eligibility for programs, services or benefits.
    b. Considering reliable residence evidence helps ensure fair access to benefits and services.
    c. In processing a residency check, Relying Parties will request only the minimum information required related to the individual requesting the service/benefit. The individual may at any time refuse to provide the information by not pursuing the service/benefit.
    d. Should the individual accept to provide the information, they may select who will provide the information to meet the type of residency proof specified by the Relying Party.
    e. Relying Parties will only keep the information related to a residency check for the duration needed, as authorized by the individual.
10. That a memorandum between DIACC members be created to confirm interest in developing a framework to prove residency online that would be open to competitive forces as one or more DIACC members may wish to pursue building this framework as a competitive business.
11. Develop a robust and consensual business model to help the Online Proof of Residency POC to evolve into a full-fledged program.

Annex 1

Use case 1: Public sector

Organization	Simplified problem statement and solution
Provincial Health Insurance	To qualify for provincial health care coverage, a client must be in the province for 160 days in any 12-month period. This is often difficult to prove: at least 10% of applicants are turned away at the counter, mostly due to a lack of residency documentation. A proof of residency with validated activity for a specific minimal duration (e.g.: level 3 proof) would simplify the process for everyone.
School Zones	Many school boards require that students live within a specific geographic area in order to gain access to specific schools. A more robust online proof of residency (e.g.: level 2 proof) would not only make the application process easier for parents, it would also help to decrease the use of fraudulent addresses and proxies by helping to ensure that an individual is actually resident at a given address.
Census Mailing	Statistics Canada needs to be able to confirm that an address exists and that it is a residence, though it does not need to be associated to a specific individual.

Use case 2: Social-profit Community Organizations

Organization	Simplified problem statement and solution
Post-Secondary Tuition	Many colleges and universities provide preferential pricing for in province/ country students. These discounted rates generally require a student to prove that they have been resident in a given jurisdiction for a set period of time. An online level 3 proof would enable students to register more efficiently and would cut down on the work that the institutions need to do to verify residency.

Use case 3: Private Sector

Organization	Simplified problem statement and solution
Mobile phone retailers	Mobile phones and mobile phone service are high value targets by criminals. They fraudulently obtain a mobile phone service with a subsidized phone using forged documents, ship the phone to another country where it is used to make expensive long-distance calls. The retailer is generally responsible to assume the cost of the fraud. Validating that the client has been living at a given address for a given amount of time (e.g.: Level 3) doesn't provide a fraud proof solution, but would help retailers lower fraud when used with other means at their disposal.

Annex 2

Considerations and structures for the next stage to encourage activation of digital proof of residency.

Given the commercial and sensitive nature of the discussions that would be required to move the POC to the next phase of activation, the working group felt that next steps fall to the Relying Parties and Authoritative Parties to undertake discussions.

By way of recommendations, the POC working group does suggest that any business case discussion should include representatives from Authoritative Parties (AP), Relying Parties (RP), Legal, Privacy as well as a consultation with client/citizen representatives.

Further, the group suggests that the question of what fees would be paid by RPs to APs is critical and should be addressed early in the discussions. It was also made clear that for the business case to be successful, the online framework would need to be at or below the current cost.

As the current counter cost and third party completion fees are commercially sensitive the group was not able to provide guidance on benchmarks for fees.

Glossary

Term	Primary Definition
Assurance Level	A level of confidence that may be relied on by others.
Authentication	The process of establishing truth or genuineness to generate an assurance of credential or identity.
Authoritative Party	An authoritative party is an entity member who provides assurances (of credential or identity) to other parties.
Client	The intended recipient of the service output. The entity can be an individual or an organisation.
Credential	A credential is a unique physical or electronic identifier associated with a person or organisation.
Identification	The process of associating identity-related attributes with a particular person.
Identifier	The set of identity attributes that is used to uniquely distinguish a unique and particular person, organisation or device.
Identity	A reference or designation used to distinguish a unique and particular individual, organization or device.
Relying Party	A relying party is an entity who accepts assurances about a user or subject (of credential or identity) from another member (the authoritative party).

About the Digital ID and Authentication Council of Canada (DIACC)

Created as a result of the federal government's Task Force for the Payments System Review, the DIACC is a non-profit coalition of public and private sector leaders committed to developing a Canadian digital identification and authentication framework to enable Canada's full and secure participation the global digital economy**.** DIACC members include representatives from both the federal and provincial levels of government as well as private sector leaders.

The DIACC's objective is to unlock economic opportunities for Canadian consumers, and businesses by providing the framework to develop a robust, secure, scalable and privacy enhancing digital identification and authentication ecosystem that will decrease costs for governments, consumers, and business while improving service delivery and driving GDP growth.

Board Members

BMO
CANADA POST / POSTES CANADA
CIBC
Desjardins
Government of Canada
Innovation, Science and Economic Development &
Treasury Board of Canada Secretariat
BRITISH COLUMBIA
Ontario
pwc
SECURE KEY
TD
TELUS

General Members

- Capco
- CIRA
- Credit Union Central of Canada
- Deeth Williams Wall
- Equifax

- Equitable Bank
- ForgeRock
- Interac
- miiCard
- Notarius
- Online Business Systems
- PacificEast
- PlaceSpeak
- Province of New Brunswick
- Rogers
- Royal Bank of Canada
- Scotiabank
- Securefact
- Sierra Systems
- Simeio Solutions
- Symantec
- Thirdstream
- Thoughtwire
- Ticoon
- TransUnion
- 2Keys