Digital ID & Authentication for Citizen Engagement

Towards an open, transparent, and authenticated democratic process

This innovation paper explores how the advance of the internet and information communications technology (ICTs) can have a significant impact on the application of the democratic process and explains how digital identity authentication and proof of residency are employed to ensure authenticated engagement. This paper shares the experience and learnings of DIACC Member PlaceSpeak.
Table of Contents

GENERAL 3

ABSTRACT 3

ABOUT DIACC 4

ABOUT PLACESPEAK 4

BACKGROUND 5

PROBLEMS: TRADITIONAL ENGAGEMENT 5

LEGITIMACY AND DEFENSIBILITY OF DATA FOR DECISION-MAKING 6
ANONYMITY FOR DISCOURSE 7

SOLUTION: DIGITAL ID & AUTHENTICATION 8

WHAT IS DIGITAL IDENTITY AUTHENTICATION? 8
PROOF OF CONCEPT ON ONLINE PROOF OF RESIDENCY 9
THE TWO-SIDED MODEL 9
IAP2 SPECTRUM OF PUBLIC PARTICIPATION 10
CREATING A CITIZEN-CENTRIC MODEL 11
CASE STUDY: SURREY SCHOOL DISTRICT 13

CONCLUSION 14

CONTACT US 15

WORKS CITED 15
General

Digital ID & Authentication Council of Canada (DIACC) innovation white papers explore use cases and experiences that focus on current issues and opportunities in emerging identity markets. DIACC innovation white papers are guided by the DIACC’s ten Digital ID & Authentication ecosystem principles and by the priorities of DIACC members.

DIACC innovation papers are intended to provide insights to business, legal, and technical general audiences on issues related to digital ID and authentication in Canada and around the world.

DIACC innovation papers are not endorsements and do not represent a qualified organization opinion of the DIACC.

DIACC innovation papers:
- are pragmatic and addresses real-world issues;
- are open and transparent;
- vision future opportunities;
- communicate learning from past projects;
- are authored by DIACC member domain experts with real-world business, legal, and technical expertise.

Abstract

Citizen engagement is an essential element of a well-functioning democracy. Also known as ‘popular control’, the central idea is that citizens influence their representatives in between elections regarding policy and decision-making within their jurisdictional boundaries. This white paper explores how the advance of the internet and information communications technology (ICTs) can have a significant impact on the application of popular control, provided digital identity authentication and proof of residency are employed to ensure legitimate engagement.

Traditional citizen engagement does not meet the demands of the digital transformation. Negative user behaviour, data legitimacy, and data defensibility for decision-making are particularly challenging. Digital identity and authentication solutions help to address challenges.

DIACC is comprised of a coalition of public and private sector organizations committed to developing a robust, secure, scalable and privacy enhancing digital identification and authentication ecosystem. PlaceSpeak became a member of the DIACC to connect with digital ID innovators with a shared vision to unlock societal and economic opportunities by supporting the establishment of an ecosystem of world-class solutions that Canadians can use with confidence.
About 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 in 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 is comprised of a coalition of public and private sector organizations committed to developing 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. A made-in-Canada digital identification ecosystem will reflect Canadian values and priorities, and empower Canadians to conduct a wide range of secure online transactions and interactions both domestically and internationally.

DIACC members work together by sharing resources and perspectives to address the needs of the digital transformation through the development of components of the Pan-Canadian Trust Framework (PCTF). The PCTF enables Canada’s full and secure participation in the global digital economy through economic sector innovation and the enablement of modernized digital service delivery. The PCTF supports open government principles. DIACC members collaborate to accelerate innovations by developing market educating innovation white papers, proof of concepts, and applied research to showcase world-class Canadian innovations.

About PlaceSpeak

PlaceSpeak is a location-based citizen engagement platform developed with the support of the National Research Council of Canada (NRC-IRAP). Designed to enable online consultation with individuals residing within specific geographical boundaries, its unique approach to geo-authenticating participants is closely aligned with DIACC’s Proof of Concept on Online Proof of Residency.

PlaceSpeak became a member of the DIACC to connect with digital ID innovators with a shared vision to unlock societal and economic opportunities by supporting the establishment of an ecosystem of world-class solutions that Canadians can use with confidence.

PlaceSpeak’s technology is unique, and yet part of a developing ecosystem of services which includes banking, e-commerce, and online service provision. By developing a unique use case around digital engagement, PlaceSpeak leverages advances in technology for improving online democratic legitimacy and making online feedback defensible.
Background

Citizen engagement is an essential component of a well-functioning democracy. In between elections, it is necessary for representatives to seek out and understand the opinions of their constituents. Governments at all levels (e.g., cities/municipalities, regions, provinces, federal) have an obligation to consult with residents within specific jurisdictional boundaries. For example, in Canada, governments have a legal duty to consult with First Nations peoples on issues that may affect their Aboriginal or Treaty rights, while municipalities need to engage with residents around issues related to ward boundaries.

A key tenet of democracy is the ability for citizens to influence the decisions that impact them and their communities in a meaningful manner. Graham Smith developed an analytical framework that allowed for the evaluation of institutions for citizen participation based on six criteria: inclusiveness, popular control, considered judgement, transparency, efficiency, and transferability.

- **Inclusiveness:** Citizen engagement processes must be inclusive and accessible to all. With the increasing ubiquity of digital/mobile technologies, online engagement has the potential to give people who are underrepresented in traditional forms of public input a voice.
- **Popular control:** Citizens must be empowered to participate meaningfully, in a legitimate process, and have an impact on decisions that affect them.
- **Considered judgement:** Not only should citizens have the ability to participate, they should do so in a reasonable, informed, and respectful manner.
- **Transparency:** The public input and decision-making processes should be open to citizens in order to build trust and confidence in the system.
- **Efficiency:** Digital forms of citizen engagement have the potential to save time and money while reaching a greater number of people.
- **Transferability:** Online participation is not limited by scale: from local decisions to large-scale matters involving the national or even global, best practices from the local level can scale quickly.

Problems: Traditional Engagement

Traditional forms of citizen engagement, such as town hall meetings and public meetings, are time-consuming and inconvenient for many. Public meetings on emotionally-charged topics tend to draw the “vocal minority” and lobby/interest groups comprised of individuals who may not live in the area. The adversarial tone of many in-person forms of engagement excludes more moderate members of the community, who may not feel comfortable participating amongst those with extreme views.

In an interview with *Wired*, former US President Barack Obama said that filing taxes should be “at least as easy as ordering a pizza or an airline ticket.” In today’s world, banking, shopping, learning, even dating — these can all now be done at the click of a mouse or a swipe of an app. Ben Berkowitz, founder of SeeClickFix, an app that allows citizens to report infrastructure issues in their community, said that interacting with government “should not feel like a lesser form of
digital interaction designed by a time traveller from the late 90’s.”

Citizens increasingly expect to be able to engage with decision-makers online, in their own time, while maintaining at least the same level of rigour and security as an in-person experience.

Digital platforms can diversify and increase engagement by connecting with demographic groups who are less likely to attend a public meeting, such as young people, families with children, people with physical disabilities, and more. Online techniques also allow proponents of consultations to modify and tailor their approach with greater flexibility, based on their target demographics. However, there are serious drawbacks to the current methods of engaging and consulting with citizens online.

**Legitimacy and defensibility of data for decision-making**

Some of the most ubiquitous online methods such as polls and surveys are convenient and user-friendly, even for people with minimal technological skills. However, their results are extremely prone to manipulation.

**Ballot-stuffing** refers to the process of having people creating multiple accounts to participate multiple times, creating the illusion of a false majority, or in cases where anyone can take the poll or survey, simply having people participating numerous times. This can also take place via bots, that can provide hundreds, even thousands, of false or duplicate responses. For example, Boston’s Massachusetts Bay Transportation Authority (MTBA) put forth several designs for its trains on three transit lines. Over 175,000 ballots were received; they found that “hundreds of the votes came from the same IP address, which submitted as many as three survey responses per second”.

**Astroturfing** refers to the practice of falsifying the identity of participants, usually part of the decision-making organization, to make it appear that there is extensive grassroots or community support. Online, there is no way to tell who is hiding behind an alias.

From the tobacco industry to government agencies, astroturfing undermines the public engagement process and seeks to drown out dissenting opinions. For example, the United States Air Force has put out a tender calling for software which will create “10 personas per user, replete with background, history, supporting details, and cyber presences that are technically, culturally and geographically consistent”.

These practices contribute to a lack of trust and undermine the internet’s potential to foster constructive debate and discussion. There is simply no way to defend the data that emerges from a flawed methodology and process. It would be unjustifiable to make large-scale decisions using data that is illegitimate and unrepresentative of the general population at large.

Governments are also increasingly turning to social media, such as Facebook and Twitter, to dialogue with residents and crowdsource information in real-time. For example, former US President Barack Obama held Facebook town halls to target the young and tech-savvy, and used Facebook Live Q&As to interact with that audience. However, in 2014, Facebook reported that up to 11.2% of its users could be fake accounts. The company revealed that it struggled with figuring out which accounts were real, and which weren’t.

Likewise, Twitter town halls have become a popular campaign strategy for real-time dialogue. However, a report by analytics firm Twopchart suggests that 44% of Twitter users have never
sent a single tweet, and only 23% have tweeted in the last 30 days.\textsuperscript{13} Internal metrics also indicate that 14% of Twitter users were bots.\textsuperscript{14} In short, the majority of tweets and active participants are coming from a small minority of users. Combined with the self-selecting nature of political participation on social media, sentiment analysis and data collection renders the feedback impossible to use for any kind of serious evidence-based decision-making.

\textbf{Anonymity for discourse}

Anonymity is a hallmark of many forms of online interactions. People are increasingly conscious of the fact that their online activity is being monitored – from surveillance to micro-targeting. In jurisdictions where the arrest of activists and crackdowns on political dissent are commonplace, the anonymity tools are crucial for facilitating a safe space for political discourse and organizing. Even in Western liberal democracies, whistleblowers face consequences for revealing uncomfortable truths when their identities are revealed. Despite these benefits, the negative consequences of anonymity cannot be ignored.

A study from the Pew Research Center indicates that, “73% of adult internet users have seen someone be harassed in some way online and 40% have personally experienced it.” While men experience more online harassment such as name-calling, women are more likely to encounter severe forms of harassment, such as stalking and sexual harassment.\textsuperscript{15}

Unfortunately, many current forms of digital engagement facilitate and support negative online behaviour. Some governments have turned to Facebook and Twitter to engage in dialogue with residents and crowdsource ideas. However, the anonymous or pseudonymous nature of social media only serves to encourage trolls and cyberbullies to act with impunity. Trolling – deliberately posting offensive, malicious or provocative content online to incite anger – is extremely common on platforms that allow for user-generated content, such as forums and social media (e.g., Facebook, Twitter, etc.). By hiding behind the veil of anonymity, internet trolls deliberately provoke anger through inflammatory attacks on others. As social media platforms are plagued with fake accounts, there is no way to hold people responsible for what they have said.

While governments and law enforcement are beginning to take online harassment and other forms of threats more seriously, it is still commonplace for them to suggest that people who are facing these problems simply stay off these platforms.\textsuperscript{16} Other activities, such as doxxing (the publication of individuals’ personal information, such as address, telephone number, etc.) or swatting (calling in a fake police emergency using the target’s address), have serious offline consequences that make people hesitant to participate in controversial or heated discussion online.\textsuperscript{17} Suggesting that citizens simply refrain from engaging on social media is ineffective and prevents them from being able to participate in their communities.
Solution: Digital ID & Authentication

When attending an open-house event, one of the first things participants are asked to do is to put on a name tag and introduce themselves. Most focus groups sessions start with a roundtable introduction where participants state their name and affiliations to avoid conflicts of interest. Municipalities and governments often require people to provide their name and residential address to sign into a public hearing or be added to the speakers’ list. These measures ensure that participants establish a baseline of mutual respect.

Governments need to be confident that they’re interacting with their constituents in a way that is secure and verifiable while meeting the modern-day client demands of convenience and 24/7 access. As online access to services and citizen participation become increasingly normalized, digital identity authentication presents a substantial opportunity for public sector service delivery.

What is Digital Identity Authentication?

Digital identity authentication plays a crucial role in ensuring that people are who they say they are online. Processes of validating and authenticating one’s identity – that is, proving that you are the person who you say that you are – are taken for granted in the physical world. For example, in the physical world, people are required to show identification in order to open a bank account, vote, or board an airplane. This is usually a straightforward process that occurs without much fanfare. Online authentication is also becoming normalized. For example, people understand why it is important to verify their identity or address to use sharing economy services like AirBnB.

How can governments be confident that people are who they say they are online, while protecting their privacy? Currently, online access to government services is limited and pragmatic concerns with regard to security and personal information protection – a global challenge – have slowed the modernization of public sector digital services.

In 2015, a cyberattack crashed Canadian federal government websites and email for nearly two hours. Far from being an isolated challenge, the number of cyber-attacks and security breaches in the United States government increased by 35% between 2010 and 2013. These challenges demonstrate the critical need for the development of a robust strategy for digital identity in Canada.

In Canada, these challenges have driven innovations and pushed public and private service providers to develop compelling, world-class services that are secure and privacy-respecting. For example, Canada has developed “privacy-enhancing technologies” including the Privacy by Design framework, which approaches privacy in a proactive, not reactive manner, anticipating and preventing breaches of privacy before the fact.
**Proof of Concept on Online Proof of Residency**

As governments and organizations at all levels have a responsibility to consult with people within their jurisdiction, the ability to authenticate people online to physical location is crucial to developing robust online public consultation processes which result in verifiable and defensible feedback data. DIACC has undertaken a review to develop a Proof of Concept on Online Proof of Residency, to provide a residency check, on demand, with a reasonable level of assurance.21 Residency is used by governments, the private sector and the social-profit sector to ensure that eligible individuals receive the products and services they need.

Under DIACC’s proof of concept framework, there are four levels of proof (LOP) of residency:

- **Level 1:** The address exists.
- **Level 2:** The address exists and the individual is associated to the address.
- **Level 3:** The address exists and the individual is active within the jurisdiction for a given period of time.
- **Level 4:** The address exists, the individual is active within the jurisdiction and there are multiple corroborating proofs of that activity.

**The Two-Sided Model**

The citizen-centric two-sided model consists of: (1) Participants, who contribute feedback to public consultation topics, and; (2) Organizations such as local government, regulated authorities, private sector land developers, and community associations, who have a responsibility to consult with residents within specific areas or jurisdictions.

![Fig. 1: PlaceSpeak’s two-sided model](image)

The model verifies the location of potential respondents before they participate in a public consultation. This represents a significant advantage over traditional online tools which, at best, can only verify that only one response is provided from a specific internet (IP) address. The model leverages authentication mechanisms to provide more assurance that participants are real and relevant based on assertions of where they live. By doing so, participant contributions provide decision makers with more actionable and defensible data towards effective decision-making and outcomes.
The model currently employs a distributed and iterative approach to digital identity authentication to place. The initial enrolment process is simple:

- Users provide their mailing address while a visual map zooms into their address for verification.
- Google Maps API locates their address.
- Users must verify their account through an email confirmation.
- A third party service, Maxmind, verifies the IP address through geolocation to identify possible address fraud.
- Users are encouraged to add additional authentication mechanisms to their account, including two-factor authentication through home phone (audio PIN) or mobile phone (SMS PIN).

In the future the model may leverage additional authentication mechanisms and identity proofing and validation services from third party organizations including: banks, telecommunications service providers, and government services (e.g., validation of driver’s license, health card numbers, etc.)

By leveraging additional authentication and identity proofing mechanisms, the information provided by users becomes more influential. Organizations may choose from multiple types and levels of authentication providing flexibility to modify the levels of verification needed to appropriately mitigate identified risks associated with a specific consultation.

Digital identity authentication cannot exist without trust and privacy. Measures have been designed into the architecture of the site. The personal information that individuals use to create their profiles and verify their location is specifically disaggregated from the feedback data that they provide during public consultations. Organizations running consultations never have access, by design, to the private information of participants. In this manner, individual privacy is protected while reliable geospatial feedback data is provided to inform evidence-based decision-making.

**IAP2 Spectrum of Public Participation**

The International Association of Public Participation (IAP2) Spectrum identifies five increasing factors of engagement: inform, consult, involve, collaborate, empower. The IAP2 and digital identity authentication industry standardizations, such as those being developed in the DIACC, accelerate the delivery of the innovative tools that governments require to address the needs of the digital transformation.

Enabling participants to stay informed is a first step towards ensuring meaningful participation that elicits pragmatic judgement. Governments require the necessary tools to consult and collect feedback using polls, surveys, interactive map-based commenting, and more. These tools enable governments to involve citizens in the decision-making process in discussions forums using text, images or video.

Participants can upvote/downvote comments, and respond to each other’s comments creating two-way dialogue. Participants can also collaborate with decision-makers and each other to co-create solutions, which can then be carried forward to decision-making and policy development. By leveraging the multiple layers of authentication that users add to their profile, it is possible to enable direct decision-making, including online voting. Direct decision-making empowers citizens.
By leveraging the IAP2 Spectrum of Public Participation, a citizen-centric digital engagement model demonstrates an emerging real-world ecosystem in which informed constituents have the option to provide consent to be notified about consultation topics in their area – enabling meaningful localized digital engagement.

**Creating A Citizen-Centric Model**

A citizen-centric model supports the breakdown of silos between governments (federal, state/provincial, local/municipal). A citizen-centric model places the user at the centre of service design, connecting people with one another and with the places where they live, work, and play. This makes it convenient for citizens to stay informed, engage with their neighbours, and consult with decision-makers within jurisdictional boundaries.

![Diagram showing traditional vs. citizen-centric models](image)

Fig. 3: Traditional models of citizen engagement are unidirectional. The citizen-centric model puts the citizen at the centre of the process.

By providing a digital engagement service that leverages a citizen-centric model, civically-engaged and informed participants can make a meaningful impact on their communities.

Organizations that utilize digital engagement for public consultations contribute to a lively “one-stop shop” for dynamic feedback on a wide range of issues. Residents that participate in digital engagement can view relevant issues occurring in their local area and choose to engage. For example, a user who is interested in providing feedback on local transportation issues can view and participate in other consultations in their area, such as a school boundary redistricting, or a newly proposed construction development in their neighbourhood. By leveraging the network effect, consultations cross-pollinate one another and support greater overall digital engagement.
A citizen-centric model also ensures that participants are able to speak their mind in a safe and secure environment. Digital identity authentication has proven to be an effective deterrent against trolling, spamming, and other negative online behaviour. By authenticating digital identity as part of the user sign-up process, individuals take responsibility for their online contributions, and that online abuse or harassment will not be tolerated.

Additionally, users need to be confident that the information which has been used to authenticate their identity cannot be abused or compromised. The PlaceSpeak citizen-centric model has been architected to reflect Privacy by Design principles. The feedback data collected during citizen engagement processes is disaggregated from the participants’ private information (e.g., physical address, email address, etc.)

Organizations conducting consultations never have access to the personal information of participants, by design. To protect privacy, the personal information of users is also never shared, sold, or otherwise distributed with any other organization or company. The citizen-centric model also allows users to determine their own privacy settings. Additionally, registered and authenticated users may choose to be publicly shown as anonymous in discussion boards. That being said, less than 5% of PlaceSpeak users choose to be publicly anonymous: the authentication process establishes the norm where people tend to stand behind their feedback and contributions.

As a result of these measures which simultaneously allow for authentication and privacy, PlaceSpeak is now home to a growing community of civically-engaged and informed users who continue to have a meaningful impact on their communities.

A digital engagement service must continue to innovate to improve the user experience and enhance opportunities for participation. Open data civic notifications and neighbour social networking encourages ongoing engagement between constituents and decision-makers and also amongst authenticated neighbours. By providing a more trustworthy digital engagement experience, the act of democratic participation becomes more frequent and habit-forming.

An innovative digital engagement service will deploy a system for the automation place-based civic notifications using open data. By leveraging standardized machine readable open data, a digital engagement service can deliver information directly to an authenticated participating neighbour who wishes to be notified about specific consultations in their local community.

By providing further assurance that a neighbour is who they claim to be, an accountable community of trust is enabled to grow. Authenticated participants may also choose to engage by connecting with their neighbours. This type of engagement encourages neighbours to interact on an ongoing basis, in between consultation topics. Users may communicate privately with their neighbours about community issues including public safety, local events, and more. The information shared within an online neighbourhood is not accessible to people outside of online neighbourhood, a principle that reinforces the privacy of neighbours.
Case Study: **Surrey School District**

**Level of Proof required:** Level 2 (The address exists and the individual is associated to the address.)

<table>
<thead>
<tr>
<th>Level Of Proof (LOP)</th>
<th>Description</th>
<th>Characteristics</th>
<th>Acceptable Proofs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The address exists.</td>
<td>Have a Verified Address</td>
<td>A claim or statement of address Verification that address is valid</td>
</tr>
<tr>
<td>2</td>
<td>The address exists and the individual is associated to that address</td>
<td>• Have an address associated with a name, and; * OR • Have proof that the address is in use by the individual</td>
<td>• An identity document AND * • A utility bill, with usage, addressed to the individual</td>
</tr>
<tr>
<td>3</td>
<td>The address exists and the individual is active within the jurisdiction for a given period of time.</td>
<td>• Have an address associated with a name, and; * OR • 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.</td>
<td>• An identity document AND * • A utility bill, with usage, addressed to the individual</td>
</tr>
<tr>
<td>4</td>
<td>The address exists, the individual is active within the jurisdiction and there are multiple corroborating proofs of that activity.</td>
<td>• Have an address associated with a name, and; * OR • 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, and; * • Have multiple, corroborating, parties confirm proof of physical activity * • Physical presentation of claim OR * Authoritative proof of entry and exit to geographic area</td>
<td>• An identity document AND * • A utility bill, with usage, addressed to the individual</td>
</tr>
</tbody>
</table>

Fig. 4: Level of Proofing Chart, DIACC Proof of Concept – Online Proof of Residency

A new secondary school is under construction in the Clayton area of the City of Surrey, British Columbia, Canada. The new school is intended to address the overcrowding at three secondary schools in the area. The Surrey School District was seeking parent and student feedback to establish catchment boundaries for the new school.
To ensure that the feedback received would be relevant to the new secondary school, the District specifically sought feedback from parents and families who live in the area. By leveraging a citizen-centred digital engagement model, the City of Surrey had assurance that consultation participants were appropriately geolocated as they signed up and participation was limited to include only those participants whose geolocation was within the desired boundaries.

**Conclusion**

Digital engagement tools, can provide powerful capabilities to support and enhance the democratic process in the age of the digital transformation. In order to provide effective digital engagement services must also leverage appropriate use of digital identity, authentication, consent, and notice practices. These practices provide further assurances that make data provided through consultation more relevant and influential.

Engagement principles, such as the IAP2 Spectrum of Public Participation (inform, consult, involve, collaborate, and empower), provide strategic guidance for the delivery of effective digital engagement services. Digital identity authentication principles, such as the DIACC’s ten Digital ID & Authentication ecosystem principles, provide strategic guidance for the binding of digital identity authentication to industry specific services.

Governments and organizations are becoming increasingly aware of the importance of digital identity authentication and verification as imperative tools to safely, securely, and accurately modernize the delivery goods and services. As we look to the future where citizens become increasingly authenticated, combined with checks and balances to ensure security and privacy, the opportunities for online democratic legitimacy can truly be realized.
Contact Us

For further information about the topics discussed in this paper, or to join the DIACC community, visit https://diacc.ca or contact: info@diacc.ca

Works Cited


