Digital Identity in Employment

Improving security, efficiency, and convenience, while reducing risk and fraud.

Insights from Interac Corp.

"A Digital ID becomes the unique identifier linking an individual to their credentials and accreditations."

Introduction

The efficient allocation of human resources is reliant on an employer accurately assessing a set of skills-based claims by a potential employee. A growing challenge, however, is being able to understand and verify these skills in a more comprehensive and efficient manner. Moreover, standard methods of pursuing candidates, determining their organizational fit, as well as conducting the pre-hire verification process, can be painfully slow and inefficient. The ability to submit verifiable credentials would enable employers to instantly confirm a candidate's accreditation.

Verifiable credentials, linked to unique digital IDs, can modernize human resources, particularly the relationship between employees, employers, accredited institutions, and governments. A digital ID becomes the unique identifier linking an individual to their credentials and accreditations.

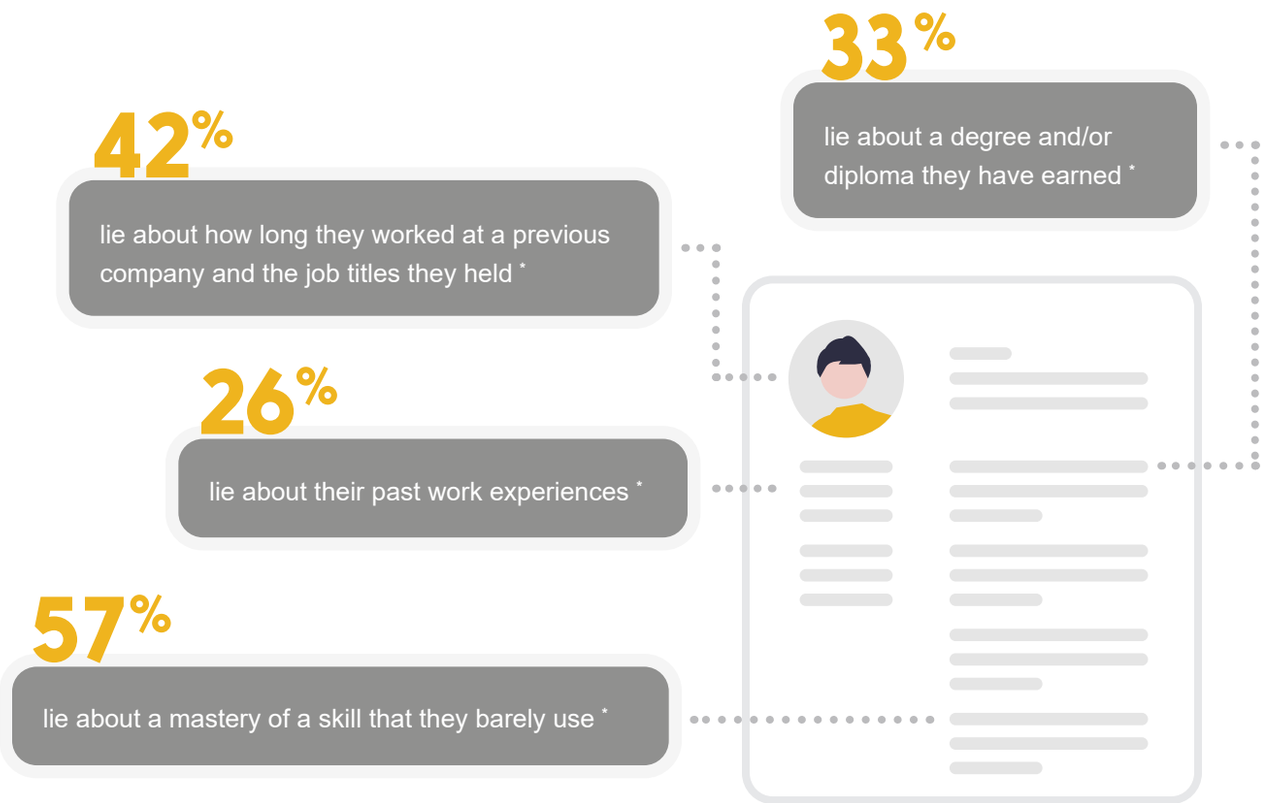
Employers can easily validate a candidate's credentials, issued by accredited institutions, while governments can request employment records for accessing public services and other needs such as taxation. Most importantly, individuals will be able to grant or revoke access to their validated resumes, sensitive banking information, and other immutable personal data, while keeping it private and secure.

In addition to the efficiency afforded by automating recruitment, digital IDs will improve security oversight, reduce the risk of fraud, validate credentials, and reduce the resources required to find and hire talent in the modern economy.

How will HR evolve in Canada?

Surveys have shown that many job candidates misrepresent past work experience or education. Digitally verifying the applicant's credentials, linked to their government issued digital identification credentials, not only mitigates the risk of fraud, but it significantly increases efficiency when confirming an applicant's past work experience, skills certifications, or academic degrees.

Remaining competitive in a modern, digital, service-based industry will involve seeking and processing vast amounts of applicants in order to find and hire the best talent. Beyond background checks, digital identification credentials also offer an opportunity for employers to secure employee records, issue smart contracts, adhere to compliance and regulation, and process payments and benefits.



* Source for data shown in graphic:
Career Builder (2014) *Fifty-eight Percent of Employers Have Caught a Lie on a Resume, According to a New CareerBuilder Survey*

How does digital ID help?

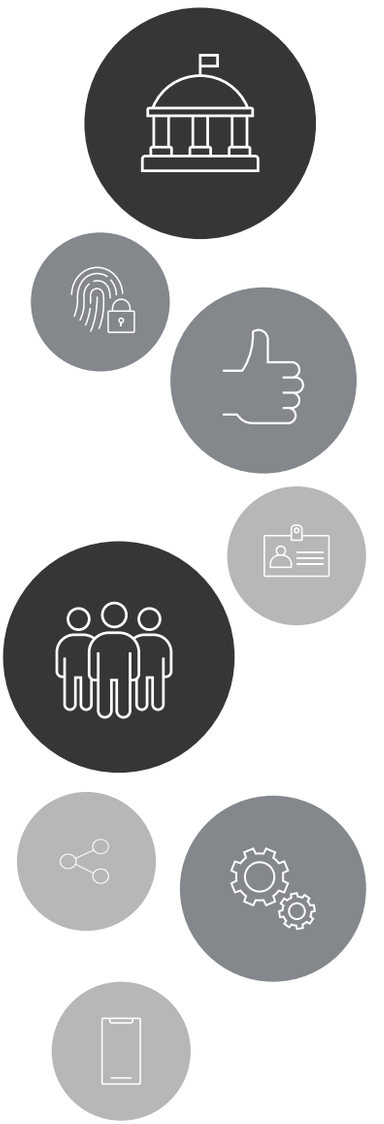
Beyond improving security, efficiency, and convenience, a digital identification exchange network will also allow all parties involved to exchange data in a compliant manner, for the overall improvement of allocating and managing human capital.

Employers

Strengthens security, by not storing sensitive employee records, but being granted permission to relevant information by applicants, when necessary, in tokenized form.

Enables increased capacity and efficiency, while mitigating the risk of resume fraud, when verifying candidate credentials such as work experience, skills certifications, or academic degrees.

Decreases costs by increasing likelihood of hiring qualified talent and reducing turnover.



Applicants

Offers greater convenience, by reducing the amount of paperwork exchanged and elapsed time throughout the interview process.

Provides a detailed view of what information an employer requests and for what purpose. This is known as informed consent, and it is a critical component of any Digital ID solution.

Enables data compliance, where employees can retract personal information made available to an employer upon termination of employment.

User Journey

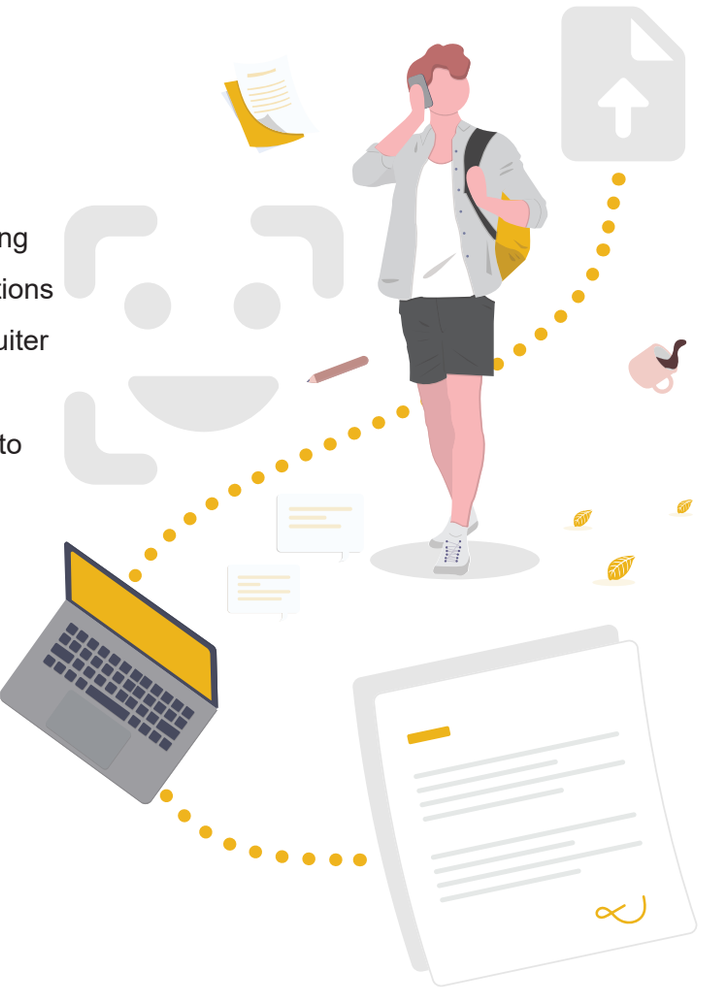
Digital identity will enable automated verification of qualifications, all while removing the need to store sensitive information, by radically improving authenticity and security through tokenization. Improvements become evident at every stage of the labour cycle.

Step 1:
Submitting a Resume

Ivan is applying for a product designer position at a growing tech company. He is about to submit his candidacy for the role, but the company is requesting proof of an undergraduate degree prior to proceeding. Through the company's website, he is prompted to digitally verify his undergraduate diploma issued by his university.

Step 2:
Attending an Interview

Meeting the requirements for the role, he has been invited to attend a virtual interview. During the interview, he is asked more specific questions regarding his past work experience. The recruiter sends Ivan a request to share the contact information for his references. Ivan consents to sharing that additional information.



Step 3:
Accepting Offer

By the end of the week, Ivan is extended an offer, outlining his new job description, salary, bonus structure, and benefits. Ivan digitally signs and is ready to start work immediately.

User Journey...continued

Step 4:

Receiving Payment

Upon signing on, Ivan is prompted to share his social insurance number and banking information with HR. He accepts and the company is now able to register him as an employee and perform direct deposit by-weekly.

Step 5:

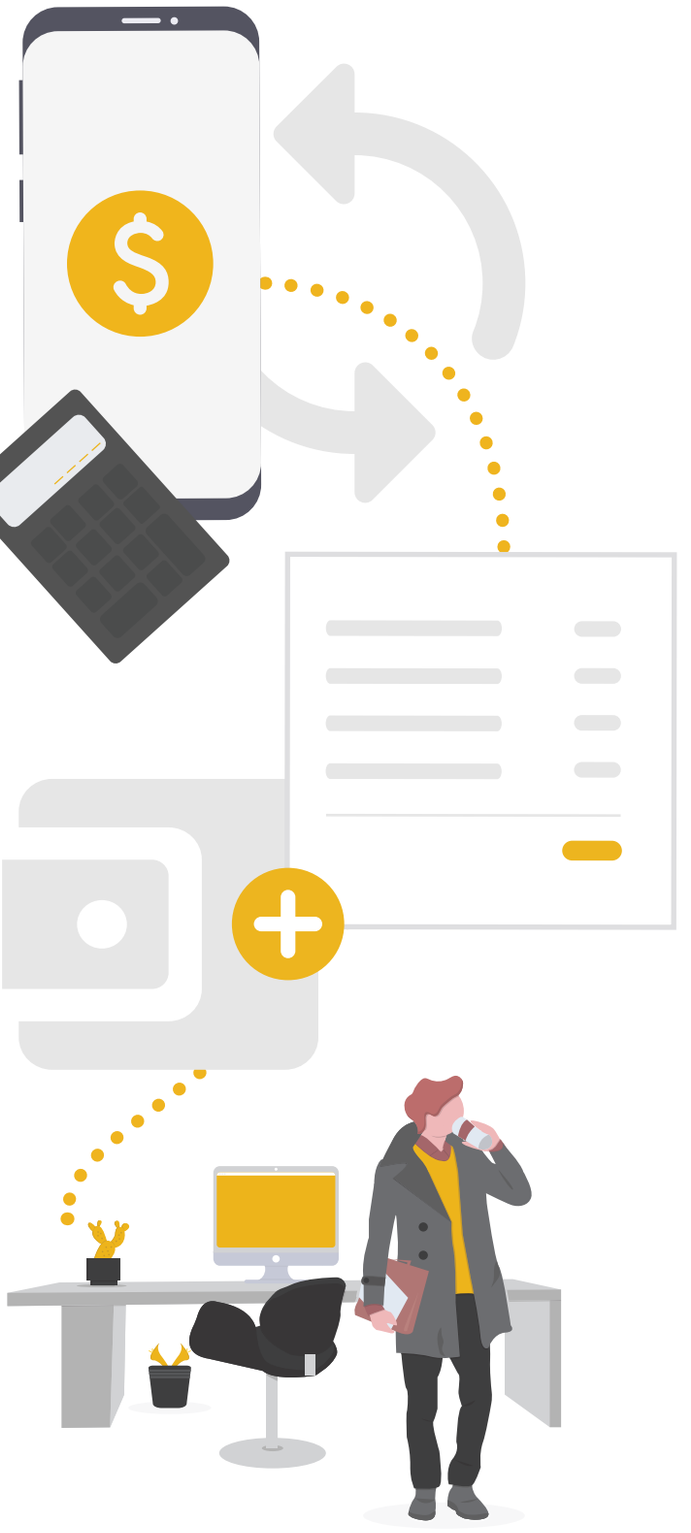
Submitting Taxes

Ivan has been in the role for 6 months, and tax season is fast approaching. He is issued a T4 by his employer, which he adds to his digital wallet, to eventually share with the provincial and federal government, along with any other tax forms.

Step 6:

Leaving Employment

Ivan has found a new opportunity offering a higher salary and has submitted his two weeks' notice. His current employer issues him a verifiable credential that he can use as a reference in the future. Ivan can revoke access to his personal information following his last day at work.



What is a Verifiable Credential?

A Verifiable Credential is a digitally verifiable proof of attributes such as a qualification (university degree) or piece of information (social insurance number). It validates qualities or properties of a claim put forward by a user, establishing its existence and uniqueness. [1]

1. **W3C Working Group** (2019)

Our Principles

Digital identity is easy to theorize, but architecting and implementing a comprehensive, secure, and sustainable system is another matter entirely – and an important part of getting it right is having a clearly articulated set of principles to guide the effort. We believe that there are five:

User Control & Convenience

No one wants to entrust a system with their personal details if those details are going to be transferred to and stored by numerous parties – especially if this happens without the user's knowledge and express consent. While ensuring user control, an identity system must also be convenient and easy; if it isn't, it won't be adopted by users, many of whom are already used to intuitive apps on mobile devices.

Standards & Openness

In any dynamic system, it's difficult to predict what the future will look like – so it's important to build today's solutions on universally-agreed standards. Not only does this reduce costs by eliminating the expense of building and then later having to adapt custom, one-off solutions, but it enables solutions built by others in the future to "plug into" the initial solution. Openness encourages adoption, innovation, and flexibility.

Ubiquity

Security risks abound when people create different identities and passwords for each public and private service they access. They'll often default to a single, easy-to-remember (and easy to crack) password, for example. At the same time, a digital identity that only applies to a handful of services will probably not be well- adopted. A ubiquitous system is a more convenient and a more secure system.

Trusted Brand

No user is likely to adopt an identity solution built or maintained by an organization they don't trust. The question of identity is simply too important, and the impact of identity theft too great, to leave this to chance. Further, building a large-scale (and ubiquitous) solution will require the cooperation and coordination of many players, and these players need to trust each other and the organization leading the effort.

Security via Abstraction

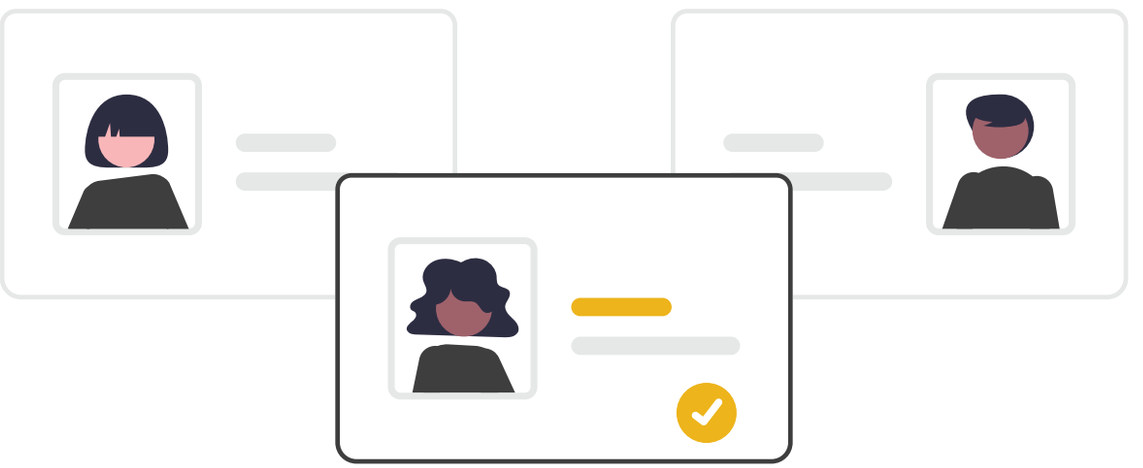
Even with the best user controls, a certain amount of identity data must be part of transactions in any given ecosystem. A highly effective way of securing that data is to "abstract" it, by replacing a private identifier with a publicly available one (like a person's email address) or by replacing it with a randomized number that serves as an authorized "token" for the purposes of the transaction – and is not useful for any other purpose.

Conclusion

Finding the right talent to fulfill a role is a laborious process of sifting through a plethora of resumes and cover letters, followed by valuable time spent validating an applicant's claims and accreditations. A standardized digital ID framework will integrate into this emerging human resource ecosystem where a user's identity and skills are securely authenticated without copying and storing sensitive data.

Employers will not be liable for storing any employee information, because the information is uniquely owned, shared, and revoked by the employee. Therefore, in addition to personal or sensitive information, a user's digital ID is at the core of storing and sharing their skills and qualifications.

As more accredited institutions and recognized education platforms begin issuing verifiable credentials, businesses will undoubtedly leverage this secure resource-saving approach to parsing applicants and finding the right fit for the role.



If you're interested in collaborating with Interac on the future of Digital ID, drop us a line at

digitalid@interac.ca

"A standardized digital ID framework will integrate into this emerging human resource ecosystem where a user's identity and skills are securely authenticated without copying and storing sensitive data."

For more information on this topic, visit innovation.interac.ca

Published October 2021