Jobs for the Future

Verifiable Credentials Wallets in a Skills-First Talent Marketplace

MARCH 2025

AT A GLANCE

With predictions that digital skill wallets will shape careers by 2030, JFF believes widespread adoption will encourage institutions to radically rethink credentials, transform hiring practices, and empower individuals' professional destinies.

AUTHORS

Sharon Leu, Executive in Residence
Joan Lee, Consultant

Contents

About This Project

Project to Catalyze Skills-First Practices

JFF supports transformational efforts to champion skillsfirst practices, reshaping how workers, employers, and educational institutions communicate and assess skills, experience, and knowledge. The Project to Catalyze Skills-First Practices, funded by Walmart, seeks to redefine andenhance the way an array of actors – including employers, policymakers, learning and education providers, philanthropy, and workforce development leaders – interpret and utilize information about a worker's skills and experiences.

The Verifiable Credentials Project

The Verifiable Credentials Project, incubated at JFF Labs, supports development of an open standards-based infrastructure for digital credentials.

Introduction

In April 2022, Jobs for the Future (JFF) shared the findings of in-depth research into the state of the market for digital wallets used to store and share World Wide Web Consortium's Verifiable Credentials (W3C VC) in a report titled *Building a Skills-Based Talent Marketplace*. Our research for that report revealed that for the developers of these wallets, the primary focus was on supporting the development of an interoperable technology infrastructure that would truly enable LERs to live up to their full potential and that development of features beyond core wallet functionality—to store and enable sharing of credentials—was in nascent stages.

Three years later, from banking to customer loyalty programs, individuals and organizations are increasingly using digital wallets to conduct everyday transactions. For jobseekers and employers, digital wallets that store verifiable information about jobseekers' skills, experiences, and credentials have tremendous potential to transform the job market. This information, now more commonly known as a learning and employment records (LER), also provides jobseekers with new tools to engage their job searches.

In a 2024 JFFLabs survey of more than 2,000 jobseekers, 75% of the respondents said they would find a digital wallet to be helpful in their job searches, and 58% said they would likely include digital credentials as part of their job applications, regardless of whether or not they were required to do so.

Our research for this updated report shows that wallet developers have matured their products and shifted focus to real applications and demonstrations of how to use the W3C's Verifiable Credentials Data Model (VCDM 2.0) as the foundation of a decentralized ecosystem that can expand opportunities for economic advancement, enabling people to find good jobs and be active members of their communities.

Our research for the April 2022 report uncovered many examples where digital wallet solutions that contain W3C VCs could have a significant impact on efforts to expand access to career and educational opportunities throughout the work and learning ecosystem if innovators focused on developing systems that support and advance the following four priorities: lifelong learning, individual agency and control, privacy, and universal accessibility. We've seen advances in those four areas that have led to the maturing of an ecosystem that uses digital wallets to develop relationships between wallet vendors, credential issuers, employers, and jobseekers.

As with any technology adoption, there are growing pains and lessons learned that strengthen each new iteration of the solution. But as the examples in this update will show, there have been meaningful advances that have given individuals the ability to control, access, and retain the privacy of their skills data, especially for people who may be overlooked by traditional approaches to recruiting and hiring that don't recognize learning or experiences that aren't credentialed.

As the implementation of this technology progresses, our research has revealed many ways that progress toward our proposed opportunities for impact—largely focused on individual jobseekers and technology providers—can have even greater impact on system-level transformations in education and workforce development and the technologies that drive economic advancement. This change in focus is guided in part by an emphasis on advances that will drive progress toward the ambitious goal that we at JFF have embraced as our North Star: By 2033, 75 million people facing systematic barriers to advancement will work in quality jobs. However, it also reflects the speed at which we see the understanding of these products grow, as well as how quickly they are being adopted and used to change the world around us.

In reading this, we hope you find similarities between these projects and your own initiatives to inspire your work. We will also highlight resources specifically developed to ensure that a solution you may be considering is truly interoperable from a technical perspective. By fostering collaboration and sharing insights, we aim to drive innovation and unlock the full potential of interoperable solutions in the talent marketplace to create a more connected and efficient ecosystem that benefits everyone.

Digital Wallets Powering a Skills-First Talent Marketplace

Adopting digital wallets with W3C verifiable credentials can help the U.S. workforce adapt to predicted labor market changes, including shifts driven by automation and artificial intelligence (AI), increased demand for construction workers due to investments in alternative energy projects and infrastructure initiatives, and a growing need for health care workers as the population ages.

A 2024 McKinsey report titled *Generative AI and the Future of Work in America* showed that workers making less than $38,000 a year are up to 14 times more likely than the highest earners to need to change occupations in the years ahead, and most will need additional skills to do so successfully. Those workers would benefit from using digital wallets that hold W3C VCs, which will enable them to store, send, and own information about the skills they've acquired over a lifetime of learning and employment in ways that are secure and tamper-proof. Not only that, the open standards-based ecosystem underlying these wallets will be a crucial part of the infrastructure for the workforce system of the future, accelerating skills-first hiring and ensuring that everyone will have opportunities to participate in the labor market. In addition to giving jobseekers the ability to share a full picture of their skills and capabilities, it also helps employers that have adopted skills-first policies, who will increasingly be seeking information about what job candidates can actually do, not the degrees and credentials they've earned.

Using W3C Verifiable Credentials

The World Wide Web Consortium, the international standards body that develops protocols and guidelines to ensure interoperability on the web, has created the Verifiable Credentials Data Model (VCDM) standard for digital credentials. The VCDM is the global standard for ensuring that digital credentials are cryptographically secure, tamper-evident, and privacy-protecting, even as they are exchanged and shared. Throughout this report, we use the term verifiable credentials to mean digital credentials in the W3C verifiable credential data format.

A digital credential that conforms to the VCDM provides structured terms to describe assertions, including details on personal identity, employment history, or skills. Digital credentials built on the VCDM can also describe learning- and work-related records, such as diplomas, certifications, and training, providing critical information about who issued the records, who earned them, and how the records can be verified.

VCDM-based records can be verified instantaneously by employers, admissions officers, government entities, and other parties requesting verifiable credentials. These "relying parties" may still need to additionally validate the accuracy and relevance of the information that the credential contains. For example, when a jobseeker submits a certification in the VCDM format, the hiring manager can instantly see the training hours required to obtain it. However, if these hours fall short of the position's minimum experience requirements, the employer will know that the certification, while accurate, does not meet the job qualifications.

Employers need more than just static resumes and lists of past roles; they need insight into the true competencies of candidates and employees. A 2024 Upskill America report titled *Employer Insights on Digital Credentials and Skills Profiles: Lessons Learned* shows that employers want to see skills of potential candidates. If a skill is presented as a digital credential, the data should indicate what the credential is for and what competencies the holder possesses in a simple way they can trust.

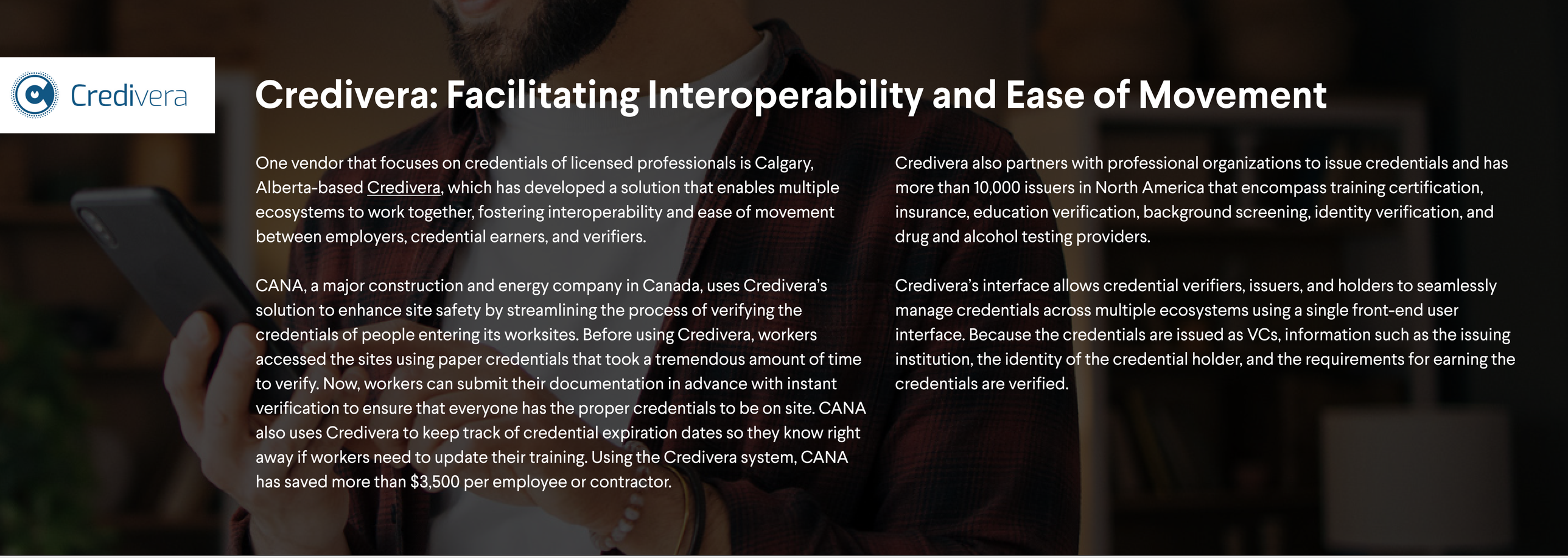
To meet employers' needs, metadata in the credential can show the requirements needed to earn the credential and provide other artifacts that support a person's claim that they know a skill. For example, Territorium has partnered with Conalep Nuevo León, a technical high school in San Nicolás de los Garza, Nuevo León, Mexico, to provide digital credentials to the school's students. These digital credentials also contained video evidence of a student's mastery of a skill. Students sent these digital credentials to local employer partners, including Kia, Hyundai, and Chrysler. Since the program's start, Conalep has seen a 4% increase in its graduation rate and a 19% increase in graduates getting auto industry jobs that previously were only available to candidates with college degrees.

Wallets with W3C VCs are critical to enabling skills-first hiring and advancement practices. With the transitions that are expected to happen in the labor market, employers need to embrace more expansive approaches to hiring, including skills-first hiring and advancement practices, to expand recruitment pools and include people with some college education but no degree, rural workers, veterans, or immigrants whose professional credentials or identity documents were issued by other countries. All this can be facilitated by wallets with VCs.

In 2018, Alabama Governor Kay Ivey announced a plan to add 500,000 individuals with postsecondary credentials to the state's workforce by 2025. As part of that effort, the state created a skills-based talent marketplace called the Alabama Talent Triad that offers a digital wallet solution for jobseekers, a skills-based job description generator for employers, and a statewide credential registry for education and training providers. Currently over 1,600 employers use the platform.

Wallets with W3C VCs also remain critical for enabling people to collect skills from multiple sources, allowing them to demonstrate skills they acquired through education, employment, and other activities across their lifetimes. Another initiative that's advancing the use of digital wallets is the Manufacturing Readiness Project. A joint undertaking of Solutions for Information Design Inc. (SOLID) and the Manufacturing Institute, the project's goal is to reshape how employers recognize job applicants' military experiences. SOLID has developed a model that translates military-acquired skills into competencies that are recognized by manufacturing industry employers. More than 600 veterans have earned some 2,400 credentials recognizing skills they learned in the military through the project, and those credentials are stored in digital wallets as badges that the holders can easily share.

When credentials are interoperable, it expands the pool of qualified candidates across state and international borders. In collaboration with JFF, the National Governors Association Center for Best Practices launched a community of practice to assist state leaders in exploring the use of digital wallet technologies to enhance data flow within and between states. This initiative evolved into the Skills in the States Community of Practice, which now supports 27 states and one territory in implementing skills-based hiring and talent management strategies. Shifting talent acquisition and management approaches to prioritize skills can accelerate the adoption of digital credentials and wallet technologies, because they offer a practical and reliable way for jobseekers to showcase their skills to employers. Another way to drive the adoption of digital wallet technologies is by focusing on real-world business cases, such as accelerating the review process for licensed professionals across state lines or improving access to job opportunities for members of immigrant populations or people who are returning to their communities following incarceration who may be eligible for occupational licensure.



Credivera: Facilitating Interoperability and Ease of Movement

One vendor that focuses on credentials of licensed professionals is Calgary, Alberta-based Credivera, which has developed a solution that enables multiple ecosystems to work together, fostering interoperability and ease of movement between employers, credential earners, and verifiers.

CANA, a major construction and energy company in Canada, uses Credivera's solution to enhance site safety by streamlining the process of verifying the credentials of people entering its worksites. Before using Credivera, workers accessed the sites using paper credentials that took a tremendous amount of time to verify. Now, workers can submit their documentation in advance with instant verification to ensure that everyone has the proper credentials to be on site. CANA also uses Credivera to keep track of credential expiration dates so they know right away if workers need to update their training. Using the Credivera system, CANA has saved more than $3,500 per employee or contractor.

Credivera also partners with professional organizations to issue credentials and has more than 10,000 issuers in North America that encompass training certification, insurance, education verification, background screening, identity verification, and drug and alcohol testing providers.

Credivera's interface allows credential verifiers, issuers, and holders to seamlessly manage credentials across multiple ecosystems using a single front-end user interface. Because the credentials are issued as VCs, information such as the issuing institution, the identity of the credential holder, and the requirements for earning the credentials are verified.

Beyond the Labor Market

Digital wallets that hold W3C VCs are becoming a crucial part of the labor market infrastructure because they enable people to share and store information on skills they've acquired across a lifetime of learning and employment, along with documents that can prove their identity and offer evidence that they meet skills-based competencies for given positions.

But the immense benefits extend well beyond the job market. For example, because VCs can securely store information about individuals' identities, digital wallets have been used to distribute aid to members of hard-to-reach populations, including farmworkers in California.

Entidad: Building Human Trust to Enable Digital Trust

Many people who work in California's agriculture industry receive benefits from a variety of nonprofits, each serving a different geographical region. And the nonprofits need a way to track the benefits they distribute to these individuals, many of whom lack official identification or other documentation regarding their status as workers in and residents of the United States.

A technology services provider called Entidad has taken steps to address that issue, partnering with the United Farm Workers Foundation (UFWF) on a series of projects related to how to collect verifiable identification data from farmworkers and store it digitally in wallets. At the height of the COVID-19 pandemic, the systems developed in these projects played a critical role in the delivery of emergency relief aid to farmworkers.

Entidad's first challenge was to find an effective way to collect and verify identity information from people with frequently changing phone numbers. Aid organizations had typically gathered this information at large in-person events. With Entidad's solution, the Farmworker Wallet, nonprofit staffers are able to digitize farmworkers' data as soon as they collect it.

A key to the success of the deployment of the digital solution was the fact that Entidad partnered with nonprofits that had spent decades building trust in the community. Having staff from UFWF and other groups serve as the first touchpoint and collectors of the information allowed Entidad to refine the digital information collection process and understand what information was really needed to verify identity before launching a full-scale solution with farmworkers themselves. This process eventually shifted to a phone-based process where a farmworker could call a nonprofit and the organization's staff could input and verify the information during the call. When the app was ready, the link to download came from a trusted member of a nonprofit during these phone calls.

This digital identity solution streamlined the identity verification processes, increasing operational efficiency and reducing fraud. Oftentimes farmworkers would have to provide the same information to multiple nonprofits to qualify for aid. With Entidad's solution, organizations can securely access and reuse verified farmworker information, removing the need for repeated data collection.

Eight organizations use the verified identity information that's available through Entidad's app to distribute roughly $80 million in one-time disaster relief payments to more than 125,000 farmworkers through the U.S. Department of Agriculture's Farm and Food Workers Relief Program.

The Farmworker Wallet provides identity verification using decentralized identifiers (DID), verifiable credential technologies and layers DIDComm-based communication capabilities such as text and video (coming soon) chat to make engaging with organizations easier. These technologies give farmworkers safety, privacy, and control over the information that verifies their identity digitally.

Entidad packaged these solutions into an open source utility called the Farmworker Wallet OS, which is now available through the Open Wallet Foundation. The lessons learned from this process led to a new a product called Unmio, a digital solution for nonprofits that serve other hard-to-reach populations.

Digital Wallets Accelerate System-Level Transformation

The technological advances that have enabled the evolution of digital wallets containing W3C VC-based LERs have the potential to drive system-level transformations. In particular, we believe there will be opportunities for sweeping change within education and workforce ecosystems and a reimagining of many of the technological systems that underpin daily life.

Transforming Education and Workforce Systems

With W3C VC-based systems, education and workforce systems will have an opportunity to redesign their existing service models. Rather than adapting systems originally designed for paper-based credentials and time-intensive verification processes, they can reimagine their operations and design new systems that leverage the efficiencies that W3C VCs enable. They could begin the redesign process by examining the purpose behind current service models, understanding how they evolved, and exploring how new technologies can transform these approaches. It will be especially important for organizations adopting W3C VCs to engage current users and other stakeholders to identify pain points, brainstorm how new technologies could address these challenges, and develop innovative service models that capitalize on the advantages these technologies provide.

ASU: Helping to Build a Large-Scale VC Ecosystem

Arizona State University (ASU) is on a mission to enable digital credentialing of learning using verifiable credentials. In 2022, ASU introduced a digital wallet called the ASU Pocket to empower students to take control of their learning, whether through employment or further education, as they pursued postsecondary opportunities. The vision for the digital wallet app was to store and share credentials that showcase users' academic, extracurricular, and professional achievements.

ASU also supports other institutions and organizations that issue credentials through its Trusted Learner Network (TLN), a community of digital credential experts and enthusiasts who are building an ecosystem to empower learners as they share their educational experiences. Upon joining the TLN, institutions can receive assistance in implementing VC technology or utilize shared standards-based technology to host their credentials. For example, Center for Future of Arizona partnered with the TLN to issue skills as VCs into ASU Pocket for employees at Karsten's ACE Hardware in Phoenix.

The TLN is now ready to begin issuing certain students verifiable digital credentials—including records of courses taken, and microcredentials earned, and other achievements—that can then be exported to ASU Pocket.

The goal of TLN is to create a consortium of organizations working together, sharing resources and providing support to develop applications and a networked infrastructure. The cornerstone of the effort is the technology stack that the TLN team—in collaboration with architecture advisors from multiple institutions, a graph database development firm, and ASU software engineers—has built to enable institutions of all kinds to deploy verifiable credentials utilizing their existing data. It also includes a governance body to develop policies to ensure digital trust for the credentials it issues, with the goal of having a network where VCs are trusted and accepted between organizations.

Through these efforts, ASU is fostering a transformation in both education and the workforce, reshaping how credentials are issued, accepted, and utilized to unlock new opportunities.

Photo credit: ASU Enterprise Technology

Transforming Technology Systems

The transition to wallets that use W3C VCs includes efforts that could transform the technology systems that underpin daily life, support the pursuit of opportunities, and enable the expression of authentic identities. This evolution will go beyond simply applying new technologies to existing service models; it requires a reimagining and redesigning existing models and systems to fully leverage technological advances.

For instance, state governments that are transitioning to skills-based hiring of state employees can use this opportunity to improve how data is stored and exchanged across agencies, enhancing data quality and facilitating seamless service delivery. Skills-first talent management practices should extend beyond the hiring process to address the management of data currently siloed within individual agencies. In the pursuit of data interoperability, it's essential to evaluate the quality, type, and exchange of data within existing systems and apply the potential of W3C VCs across multiple ecosystems, focusing on redesigning, rather than retrofitting data exchange processes.

Digital Bazaar: Building Systems to Expedite Disaster Responses

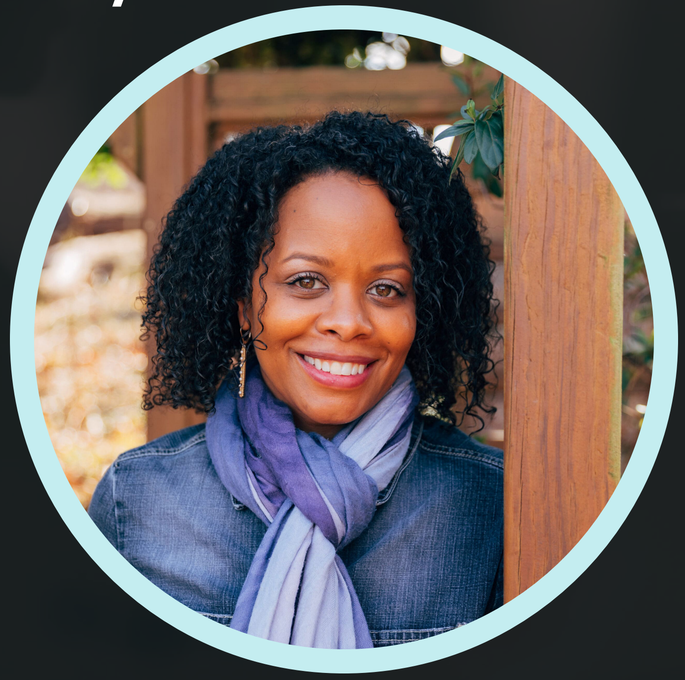
When a large-scale natural disaster, such as a hurricane or wildfire, occurs, incident commanders need ways to quickly confirm the identity and skills of every first responder brought on site to assist.

Digital Bazaar, in partnership with the U.S. Department of Homeland Security, has created a solution for first responders from different departments, states, and agencies that incident commanders can use to quickly validate individuals' credentials and assign them responsibilities based on their previous experiences and skills. A replacement for paper-based credentials, the additional metadata in the VC makes the expedited deployment process possible. It not only upgrades current methods of verification, but also enables the design of new systems of assignment that are based on skills data.

Digital Bazaar is using the same technology infrastructure to design new ways to support disaster victims. Through the use of VCs, a first responder would be able to issue credentials to people who have lost or are unable to access their identity documents. And because access to mobile networks or power sources and device chargers can be limited during a disaster, the VC can be issued with a barcode and printed on paper. People displaced by disasters could use these temporary credentials to access benefits until they regain access to their documents or are issued new ones.

By 2026, Gartner predicts that over 500 million smartphone users worldwide will rely on digital identity wallets for identity verification—marking a significant shift in our global digital infrastructure. As this technology becomes more deeply integrated, we see it at the forefront of transforming talent practices. Now is the time to embrace an abundance mindset and lean into the possibilities ahead.

Kristina Francis, Executive Director, JFFLabs



Foundational Components of a Digital Wallet Ecosystem

The widespread adoption of a digital wallet ecosystem can transform the labor market. While significant progress has been made in developing capabilities for issuing W3C VCs and digital wallets, foundational components remain to be built—particularly those critical to ensuring the functionality and ease of verification tools and the mainstream use of wallets.

These critical developments have occurred to support components that allow the entire digital identity and trust ecosystem to function as a whole. For example, governments around the world have started to use digital wallets to issue official identity documents to citizens; there have been advances in systems that promote digital trust—including the emergence of issuer registries and digital wallets with built-in verification tools; and networks of stakeholders committed to developing systems that support an interoperable cross-border digital wallet ecosystem have emerged.

State-Issued Digital Identity

Governments around the world have started to issue national identity documents to citizens in digital wallets. Most notably, in May of 2024, the EU finalized the European Digital Identity Framework with the goal of having each member state offering at least one version of the European Digital Identity Wallet by 2026. This will allow citizens to travel to other EU member states, find employment, conduct financial transactions, and access health care and benefits in any EU member state.

In Latin America, Colombia launched a digital ID program in 2020 and updated it in 2023 to include new services. Among other things, Colombians can use the country's cédula digital as a passport for cross-border travel to other South American countries. In Africa, South Africa, Kenya, Nigeria, Benin, and Namibia are working together to launch an interoperable digital ID by 2030. In Asia, Bhutan, Japan, and South Korea offer digital identification cards.

Bhutan: Leading the Way for Other Countries

In 2021, the government of Bhutan began researching ways to digitize official identity documents and services and two years later launched the Bhutan National Digital Identity (NDI) system, a fully digitized ID solution that uses decentralized identifiers and verifiable credentials. Services provided in the wallet include identity documents and the ability to bank and sign contracts digitally, and the country is continually expanding its functionality. Civil servants apply for leave through the NDI app, and citizens can use it to register for the country's mandatory national service requirement when they turn 18.

Privacy of citizens was a key priority in building the Bhutan NDI, which is why it is based on a completely decentralized system and with verifiable credentials. Initially, a nationally issued identity document, such as a passport or driver's license is biometrically verified against the census database. Once the identity is established in the wallet, it breaks the connection so that the government can't track how a citizen uses the wallet. A decentralized approach was also cost-effective because it saved the government the cost of building the infrastructure required to protect the digital information of every citizen.

Because mobile connectivity can sometimes be spotty in rural areas of Bhutan, the wallet was designed to function without internet access. There's a photo identification component that can be used to visually verify the wallet holder, and the trust registries that list all of the verifiers and issuers can function without internet access. The Bhutan NDI wallet is available on the iOS and Android platforms, and there's a version with a more limited feature set for inexpensive KaiOS phones, which are widely used in Africa and India. For the future, NDI is developing custodial and web versions so that larger portions of the population can use Bhutan NDI, even if they don't have access to their own mobile device.

Bhutan NDI is an example of a nationwide rollout of W3C VC-based digital ID system that's cost-effective and future-forward. In building this low-cost national infrastructure, the country developed a good deal of internal expertise around digital wallets that it's able to share with other countries. Currently, the solution is being adapted for Papua New Guinea.

These advances are significant because they have accelerated the development of tools that support W3C VCs as an LER use case and help foster widespread adoption because, when people are accustomed to using digital wallets in day-to-day life, it will be easier for them to transition to using these technologies in the hiring process. Identity verification is a required component for employment offers, and having identity documents in a W3C VC format makes it easier for employers to review them.

Although no effort to develop national digital identity documents or digital wallets is currently underway In the United States, the U.S. Department of Homeland Security (DHS) Silicon Valley Innovation Program has been investing in the development of open-standards-based digital credentialing infrastructure, including wallets, credential issuer tools, and verifier software based on VCDM. The technical requirements for these projects adhere to the most rigorous federal security standards, comply with privacy regulations, and are globally interoperable and accessible to all.

In addition, an increasing number of states are offering a version of a mobile driver's license. Adoption rates vary from state to state, and they often depend on the policies that dictate how driver's licenses based on the ISO's Mobile Driving Licence (mDL) standard can be used. For example, in Louisiana, state law requires that any location that accepts a physical identification card must also accept a mobile version. California is currently engaged in a pilot of a mobile driver's license that supports data formats used by the U.S. Transportation Security Administration, as well as the state's department of motor vehicles. The California license was based on interoperable standards, which enables users to move their credentials from the state-supported digital wallet to a wallet of their choice, such as Apple Wallet or Google Wallet.

As digital identity cards become more widely used, it's imperative to build systems that are interoperable within both national data systems and global data systems. Mobile identity cards that use the VCDM standard allow for that interoperability and enable data to flow between individuals and employers and even across countries. As people become more accustomed to using digital wallets for government-provided services and functions, it increases the likelihood for widespread adoption for other use cases, like LERs for skills-first hiring.

Decentralized Digital Trust

There has been progress in the development of the infrastructure that enables trusted transactions using verifiable credentials. Digital trust is when the identities of the credential holder, the issuer, and the verifier, and the integrity, authenticity, and legitimacy of the data can be established without relying on a centralized services.

VERIFIES THAT CREDENTIAL IS:	DESCRIPTION WHAT DOES IT MEAN?	EXAMPLE	TECHNICAL DESCRIPTION HOW DO I KNOW?
Authentic	Credential issuer exists, and the identity has been substantiated; learner identity is the same as the credential subject's identity, and a proof of signature is required to establish authenticity.	State University is an accredited institution, authorized to confer degrees on the issue date of the credential.	Public key of the issuer exists on a trusted registry. Private key was used to sign and issue the credential. The valid digital signature was resolved cryptographically.
Unaltered	Credential has not been altered.	This individual has earned the degree and achieved the GPA claimed.	Proof hash value is identical to the value generated by the verifier replication.
Valid	Credential is not expired or revoked.	This driver's license is valid.	Expiration date of the credential does not exist or is later than the current date; revocation status lists

When a verifier receives a W3C VC, digital trust ensures that the identity of the credential holder is accurate and the information within the credential applies to that credential holder. Digital trust is created in VCs because the digital signature ensures that the credential hasn't been tampered with. Public key infrastructure and other related infrastructure, like trust registries, enable the verifier to know that the credential issuer is the expected entity and the credential holder is the legitimate recipient.

Self-Sovereign Identity

Unlike centralized repositories managed by governments or technology companies, self-sovereign identity (SSI) ensures that individuals retain ownership of and autonomy over their information. Core principles of SSI include user control, privacy by design, decentralization, and interoperability, which ensures that individuals can securely manage and share their credentials across platforms with minimal data exposure. It prioritizes portability, inclusivity, and transparency, ensuring identities are accessible, open, and flexible for all.

Decentralized Identifiers

Decentralized identifiers (DID) are unique identifiers that serve as the foundational building block of decentralized credentialing ecosystems. They enable portability and interoperability, and they support the principles of self-sovereign identity (SSI), empowering individuals with complete control over their digital identity and personal data. Individuals can choose which DID is included in each of their credentials and control ownership of each DID. This makes it possible for privacy-enhancing capabilities such as preventing cross-correlation of online identity. Issuing organizations use DIDs to identify the identity that digitally signs credentials. These DIDs are included in trust registries so that verifiers have a decentralized way of substantiating that the issuer identity has been reviewed by a trusted party.

Since the adoption of the W3C DID specification, more than 100 types of DIDs have been developed, facilitating compatibility across various decentralized credentialing methods. To streamline this diversity, the Decentralized Identity Foundation (DIF) offers the Universal Resolver, a unified interface for resolving any DID type. Learn more on the DIF's Universal Resolver web page.

Personhood Credentials

As AI tools make deceptive activities more convincing and easier to execute, verifying human identity for online and digital transactions has become increasingly critical. Decentralized solutions are emerging as powerful tools to address this challenge, emphasizing privacy by minimizing data exposure and ensuring that user information is only shared when necessary. These solutions build progressive trust by ensuring that users on both sides of an online transaction are human and not AI bots, while prioritizing the protection of civil liberties by reducing centralization of data and preventing issuer and credentialing services from misusing user data without authorization. For example, online job application systems could apply these personhood credentials to deter spam during the initial onboarding phase and provide job applicants with opportunities to provide more relevant identifying information as they progress through the process. The limited data could also protect applicants from potential profiling and discrimination during the application review process and limit opportunities for tracking and other data misuse throughout the process.

Trust Registries

In addition to cryptographically verifying the data in the credentials, digital wallets can choose to take an additional step in confirming the identity of the issuers that sign the credentials. This can be done by searching for issuer DIDs on a list of issuer information hosted by organizations that digital wallets and verifiers trust, known as a trust registry. When a DID is found on a trusted issuer registry, it's possible to substantiate that the identity of the issuer has been confirmed by the hosting organization. Trust of issuer registries can be determined by their published governance policies, which can include information about how they establish proof of identity. Issuer registries streamline the process for verifiers by centralizing issuer identity information, eliminating the need to consult multiple sources. This step is a useful utility in W3C VC ecosystems because, unlike digital credentials that are hosted on platforms, portable credentials are intended to be shared privately. Trust registries provide a way for issuer identity to be confirmed without the knowledge of the issuer.

To advance this functionality, the MIT Digital Credentials Consortium (MIT-DCC) is collaborating with Credential Engine to research and establish guidelines and recommendations for issuer registries in learning and employment contexts. These guidelines will be established by developing prototype registries that reflect governance policies, including technology decisions that will make it possible for digital wallets and verifiers to have standardized methods for looking up issuers.

Embedded Verification Tools

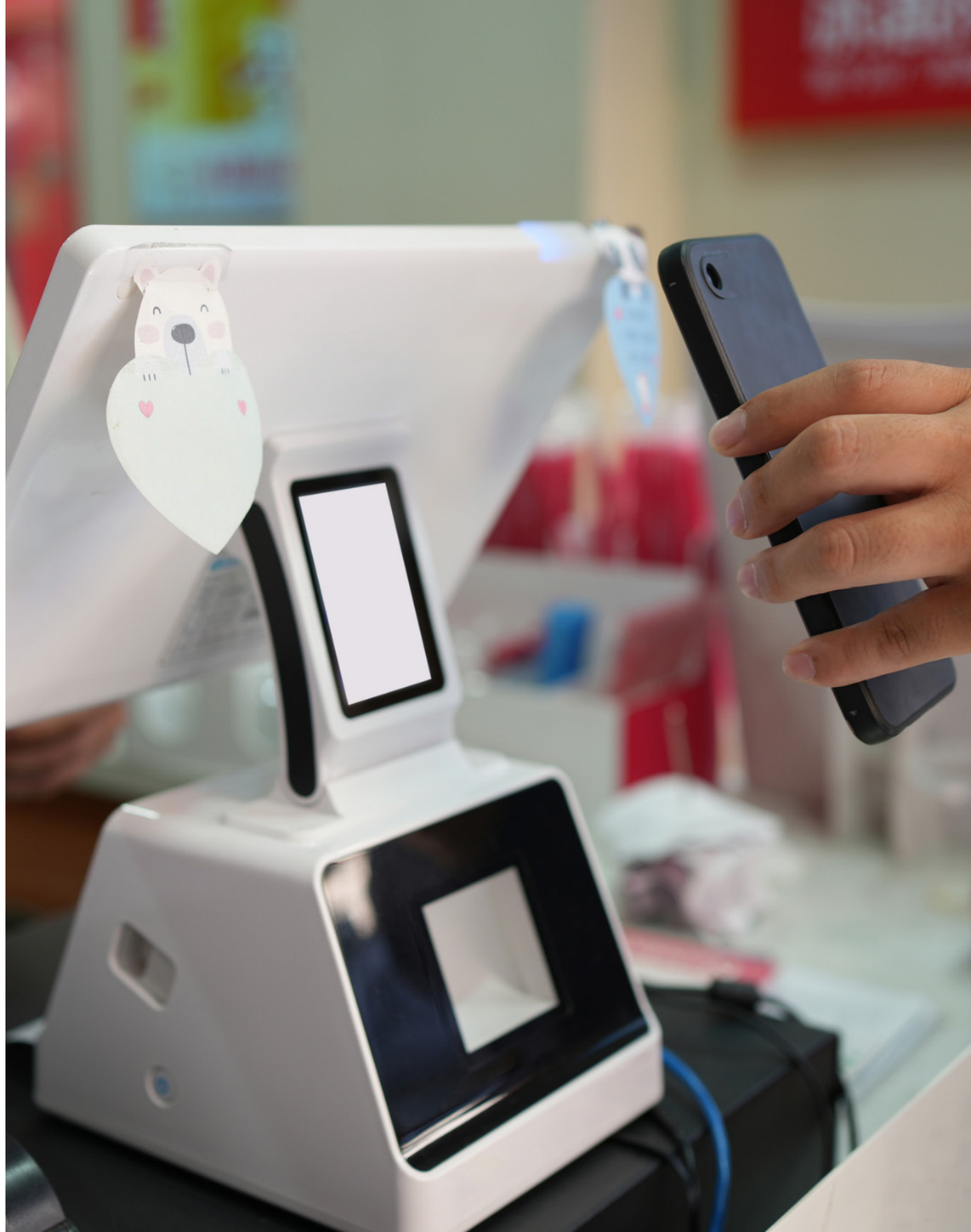
Manually verifying credentials outside of regular business processes can be inconvenient, especially for organizations without enterprise solutions supporting verifiable credentials. This challenge is particularly acute for small businesses, nonprofits, community-based organizations, and resource-constrained learning providers. Solutions that integrate embedded verification tools into web and mobile wallets—and seamlessly within existing business processes—can significantly enhance adoption. These integrated tools make verification more accessible and practical, enabling a broader range of organizations to participate in the ecosystem.

Innovative solutions are emerging that demonstrate how embedding verification capabilities into existing tools and workflows can drive adoption and usability across diverse contexts. For instance, during the Decentralized Identity Foundation's 2024 DIF Hackathon, participants developed Chrome extensions to enable web wallets to receive and verify credentials directly within any application, simplifying workflows for users. Other solutions were developed during California DMV mDL hackathons, including a solution utilizing NFC and Bluetooth, point-of-sale verification, and verification in the California driver's license app itself.

Digital Public Infrastructure

As the use of digital wallets increases, public infrastructure is essential to the efficient delivery of effective digital services that are widely accessible even to people and organizations with limited resources. The Ayra Association (formerly Global Acceptance Network) creates public frameworks that address identity or trust issues that arise when domain-specific ecosystems are siloed. Ayra will provide a sustainable layer of decentralized digital trust infrastructure that enables parties to form authentic, private, and secure digital relationships and exchange permissioned verifiable data within and across the digital trust ecosystem.

The OpenWallet Foundation (OWF), established by the Linux Foundation Europe, is a collaborative initiative dedicated to developing open-source software that supports interoperability across a wide range of digital wallet use cases. Its mission is to create a secure, multipurpose open-source engine that organizations and companies can use to build their own interoperable digital wallets. The OWF maintains a collection of open source code for W3C VC wallets and works with governments to advocate for the acceptance of W3C VCs as the standard for digital identity applications.



The Digital Credentials Consortium (DCC) has built an open-source infrastructure to empower learners to securely share academic credentials across institutions and employers, fostering learner agency and expanding access to career pathways. The DCC's open-source tools include the following: 1) code libraries for issuing verifiable academic digital credentials; 2) an iOS and Android mobile app called the Learner Credential Wallet (LCW), which can be used to store and share verified academic achievements; 3) a web platform called VerifierPlus for verifying digital academic records; and 4) Registries that support credential issuance and verification. These tools collectively advance secure, interoperable, and learner-focused credential ecosystems. DCC members and initiatives such as ASU's Pocket and Case Western Reserve's Skills Genome Project have used DCC's open-source software as scaffolding for their implementation.

As previously mentioned, the ASU Trusted Learner Network offers a decentralized system for securely storing, managing, and sharing educational and professional records. Focused on learner-centric governance and interoperability, the TLN fosters an inclusive ecosystem that supports mobility, reduces barriers, and enables lifelong learning.

SpruceID: Advancing Decentralized Identity

SpruceID provides versatile decentralized identity tools that empower individuals and organizations to securely manage and verify credentials while maintaining privacy and user control.

SpruceID has demonstrated the flexibility of a decentralized identity ecosystem through successful collaborations with a diverse array of partners across the country. Here are three examples:

- The Verify Utah digital wallet, which SpruceID developed with the Utah Division of Outdoor Recreation, offers tools for displaying and sharing off-road vehicle registrations and permits, along with intuitive features that allow state personnel to verify the validity of the registrations and permits offline.
- In partnership with the California Department of Motor Vehicles, SpruceID implemented the California mobile driver's license program and wallet.
- Working with the Colorado Workforce Development Council, SpruceID introduced the ColoradoFWD Skills Wallet, which enables Colorado residents to store and share their learning and employment records and skills credentials. This wallet will also integrate with the myColorado digital wallet, unifying identity document management for users.

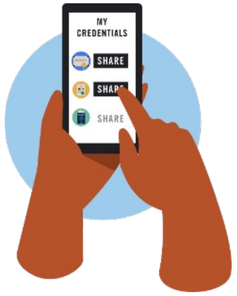
All of these solutions were built using SpruceKit, a comprehensive open-source developer toolkit designed to simplify the integration of decentralized identity and verifiable credentials into applications. SpruceKit empowers developers to issue verifiable digital credentials, create identity wallets, enhance existing solutions with verifiable credentials, and build tools to verify digital credentials. It plays a pivotal role in advancing the decentralized identity ecosystem.

Opportunities for Impact

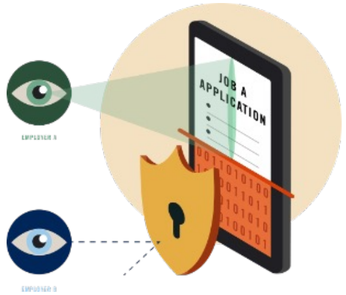
Efforts to promote the interoperability of the technical infrastructure across wallet vendors have made significant progress, and wallet applications have evolved to include features designed to enhance the usability of W3C VCs for LERs.

Below, we discuss key developments aligned with the four opportunities for impact highlighted in the April 2022 report—lifelong learning, individual agency and control, privacy, and universal accessibility—with a look at technical features that made these developments possible.

Lifelong Learning



Individual Agency and Control



Privacy

Universal Accessibility

Lifelong Learning: Competition in a Global Economy

People need to be able to keep track of the skills and work experiences they gain over their lifetimes. Since many credential issuers could give a single credential in a wallet, it's important to be able to move credentials from wallet to wallet in order to consolidate information in a location of the holder's choosing.

Interoperability Plugfests

In 2022 and 2023, JFFLabs hosted three interoperability plugfests in partnership with the National Governors Association, the W3C VC-EDU Task Force, the MIT Digital Credentials Consortium, and the U.S. Department of Homeland Security. These events brought together 39 organizations, including universities, education technology companies, wallet developers, and credential issuers, to demonstrate the use of W3C VC standards. Credentials showcased included Open Badges v3, U.S. Permanent Resident Cards, the TruAge age-verification app, ASU course credentials, European Learning Model v3, and ServSafe certifications for food service workers. The plugfests highlighted how these credentials could support jobseekers and produced open-source resources for future interoperability testing.

Analysis Capabilities

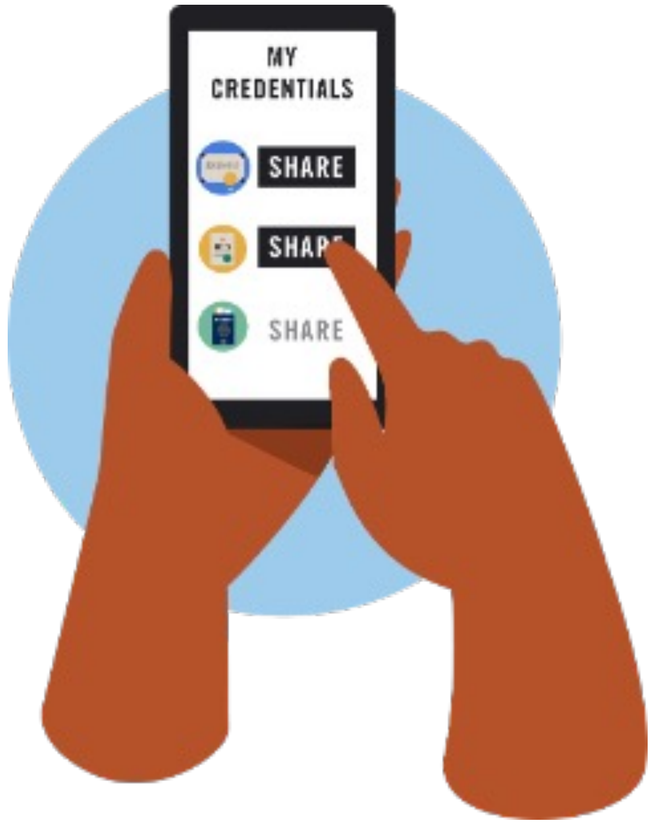
Digital credentials contain a wealth of information about people's skills and experiences. To help jobseekers make the most of their many talents, some wallet providers have chosen to add analysis capabilities that can let people know what careers they might be able to pursue based on the skills they've acquired or suggest additional credentials that they might need in order to qualify for new positions that interest them or prepare for new career trajectories.

Individual Agency and Control: Trust in a Digital World

Wallets should allow individuals to access the credentials they've earned at any time and control who can see them. Organizations should also be required to request permission from users before issuing credentials to their wallets. Individual agency and control should also include the ability to create verifiable presentations combining multiple credentials to enable people to share a full picture of their abilities.

Standards Development: renderMethod

Credential issuers need to provide an array of choices of where and how a credential could be displayed, or rendered. Therefore renderMethod, a programming function that takes information and translates it into the visual elements users see on the screen—with credentials potentially displayed as PDFs, for example, is an important consideration in the development of W3C VC wallets. Each credential could contain hundreds of properties, and wallets need to be able to decide which pieces of information should be displayed. Important factors to consider in this process are the choices an individual could make about how information inside a credential could be displayed and the visual appearance of the credential when it's transmitted to a recipient.

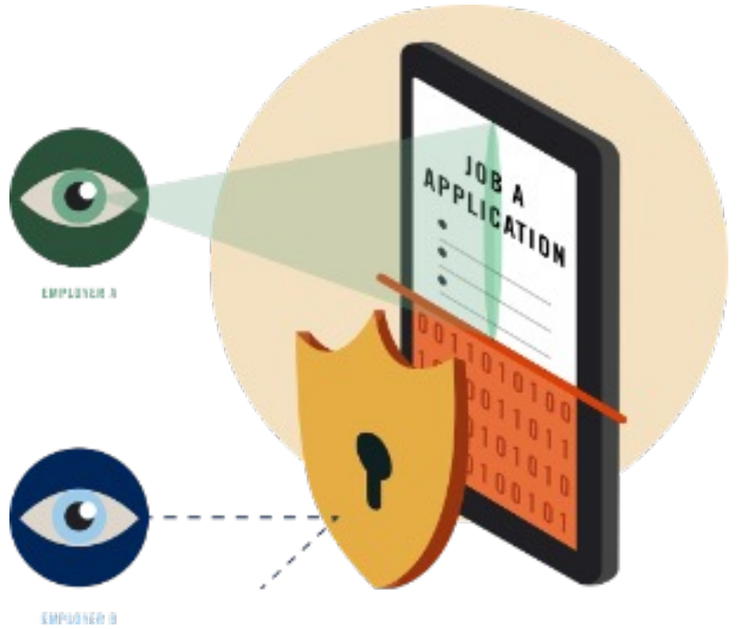


Privacy: Protecting Individual Rights in the Digital Future

Digital wallets should hold and share credentials at the will of the credential holder. It should not be possible for other individuals or organizations to see the data inside a W3C VC without user consent. Credential holders must be able to decide which information inside a credential the people they are sending it to will see.

Standards Development: BBS Signature Suites

VCDM credentials allow for selective disclosure, meaning the credential holder can choose which parts of a credential to share with other parties. A classic example of this is sharing only the information that someone has a valid driver's license without also revealing personal details like their address, birthdate or height and weight. Another example includes sharing proof of completion of a course or a degree without sharing dates or grades if not required by the verifier. BBS signature suites, including BBS+, Blind BBS, and BBS pseudonyms, are signature methods that make it possible for users to share only the elements of credentials that they want to share, provide security features that prevent credential cloning, and ensure that personally identifiable information and other data can't be correlated or linked across different verifiers.



Universal Accessibility: Strengthening Inclusion in Digital Democracies

It's essential for digital wallets to be universally accessible. Everyone should be able to earn, store, and issue W3C VCs, including people with varying physical and learning abilities, people who lack access to tech devices and broadband services, and those with limited experience using digital tools. This should be true regardless of the languages people speak or the countries in which they earned their credentials.

Wallet-Enabled Storage

A key to ensuring that wallets are accessible to everyone is to make it possible for individuals to choose where to store their credentials. For example, wallet-attached storage allows users to put VCDM credentials in applications other than digital wallets, including Google Drive, Dropbox, or other cloud-based storage systems. This gives users more control over their credentials by making it possible to access and share their credentials and control permissions without a digital wallet.

Multilingual Credentials

Since the adoption of the Open Badges credentials format, the vast majority of digital credentials have been exchanged in English. Though many language translation tools exist, the metadata of LERs, including details about skills, qualifications, and experiences, require additional understanding of idiosyncrasies across industries, regions, and cultures. Multilingual credential data formats, especially those developed to understand non-Latin-based languages, provide capabilities that respect the agency of learners and credential issuers in communicating this information. This enables credentials to be recognized internationally, increasing their usability in countries with multiple official languages, enabling jobseekers to pursue cross-border opportunities, and allowing U.S. employers to hire workers with credentials earned abroad.

Standards Development: W3C VCs on Paper

For people who don't have a mobile phone or don't want to install a digital wallet app, technology exists to print a VCDM credential as a PDF 417 barcode (the type of barcode that's on the back of physical driver's licenses) on a piece of paper. The information in a VCDM credential that's digitally signed can then be accessed by scanning the barcode, and users can even carry printouts of these barcodes in their physical wallets. This gives people who lose their digital devices or don't own one at all an easy and inexpensive way to distribute and share their credentials.

Standards Development: Web Content Accessibility Guidelines 2.1

In April 2024, the U.S. Department of Justice issued a final rule under Title II of the Americans With Disabilities Act requiring improvements in access to government services through web content and mobile applications. This rule adopts the Web Content Accessibility Guidelines 2.1 as the standards for ensuring that everyone has access to digital services. The regulation applies to vendors providing services to state and local government entities, including developers of technology products for public schools, libraries, parks and recreation programs, and public health facilities.

The Work Ahead: Making the Digital Wallets Vision a Reality for Everyone

Digital wallets for learning and employment hold remarkable potential to reshape the talent marketplace, advance skills-first hiring policies, and foster practices that empower people of all backgrounds with access to lifelong learning and economic advancement opportunities. Built on interoperable, decentralized, and open standards, the foundational infrastructure driving the LER ecosystem could transform systems across a wide range of sectors.

By leveraging verifiable credentials, this global framework ensures that individuals maintain control over their data, unlocking opportunities across a multitude of domains and paving the way for a more connected future. However, there's a lot of important work to do in order to make that vision a reality.

Supporting the Transition to Open Standards. Digital credentials and badges have been around for years, beginning with the Mozilla Open Badges project in 2011 and gaining momentum with the 2018 launch of the Open Badges v2 (OBv2) standard by IMS Global (now 1EdTech), both of which predated the VCDM. Various learning and employment records, including transcripts, licenses, and skills credentials, exist in multiple digital formats, and while some can be converted to VCDM, issuers need additional support for a full transition. To bridge this gap, the VC ecosystem should focus on developing tools that make both VC-based and non-VC-based credentials accessible to all learners and jobseekers. Initiatives like the LER Accelerator, undertaken by the American Association of Collegiate Registrars and Admissions Officers, are fostering innovation that drives these efforts forward. In addition, we should continue to focus on high-impact use cases that demonstrate portability and interoperability of credentials, rather than standards conformance testing.

Balancing Incentives of Open Ecosystems. Despite the increasing use of digital credentials and LERs, employer adoption of these solutions for use in job applications remains limited. To address this "cold start" problem, some organizations have opted to develop closed, membership-based credential ecosystems or implement incentive structures that impose payment-based restrictions on verification or otherwise limit access to verified records. As stakeholders evaluate participation in credential networks, it's essential to prioritize the needs of jobseekers. Portability and interoperability of credentials across diverse networks and ecosystems will empower jobseekers with the greatest flexibility and opportunity, ensuring broader accessibility and value.

Safeguarding Privacy. As the ecosystem evolves and adoption of these technologies gains traction, it will be even more important to safeguard people's privacy and restrict access to individual data. While the W3C VC format itself is designed to protect privacy, once a credential is shared, the data becomes subject to the policies of the institution or organization that receives it. To fully protect personal data, robust frameworks must be established and best practices must be agreed upon to ensure accountability and transparency in data usage.

Combatting Domain-Specific Isolationism. The rapidly growing interest in LERs has spurred the development of a diverse array of credential management technologies designed to serve education stakeholders. However, as digital credentials and wallet technologies become more widespread and VCs grow increasingly common, it will be crucial for LER stakeholders to guard against self-imposed technological isolationism. This includes avoiding the creation of noncompatible variations of existing open standards, which can limit portability and wallet selection for credential holders, or creating novel interpretations of widely understood technological terminology, which limits interoperability and usability of credentials for users.

Addressing Big Tech's Dominance. Google and Apple wallets dominate the digital wallet market, leveraging their extensive reach to scale quickly and support a wide range of credentials, from public transportation passes and driver's licenses to movie tickets and credit cards. However, there are concerns about whether these technologies adequately prioritize privacy or comply with stringent regulatory standards for privacy and accessibility. Meanwhile, newer wallet developers are advancing solutions based on W3C VCs, focusing on privacy-by-design principles and rigorous accessibility standards. Despite their smaller market share, these innovators are often better equipped to serve users and use cases that mainstream providers tend to overlook. It will be fascinating to see how smaller players coexist with Google and Apple wallets, especially as they both evolve in their adoption of open-standards-based ecosystems and ethical web principles.

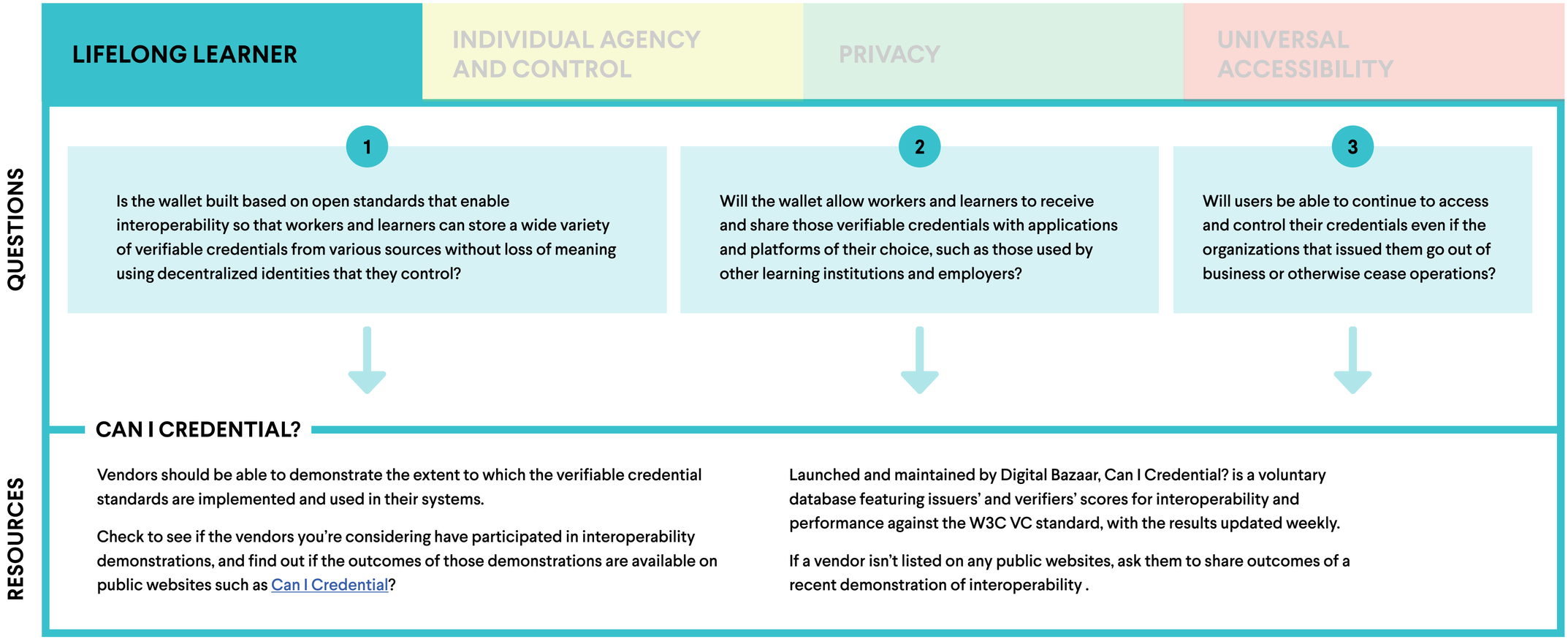
Building a globally competitive and locally prosperous workforce requires cross-border interoperability to drive innovation and ensure mobility in critical industries such as the green economy, advanced manufacturing, IT, and health care. For the U.S. workforce to continue its leadership in these sectors, it's essential to enable people to build new skills, establish clear classifications for these skills, and ensure that these classifications are recognized and understood across borders. This approach not only supports workers as they navigate a global economy but also strengthens the U.S. workforce domestically by embracing the contributions of immigrants, who play a vital role in driving growth and enriching the workforce with varied perspectives and experiences.

By developing truly interoperable technologies and scaling the use of verifiable credential digital wallets that help create systems that promote credential portability and removing barriers that prevent access to opportunity, the United States can establish itself as a leader in fostering both global competitiveness and local prosperity.

Appendix

A Vendor Selection Toolkit

Here's a list of questions to ask and a list of resources that can help you choose a digital wallet vendor. The questions are grouped into categories based on the four opportunities for impact identified in the 2022 JFF market scan report *Building a Skills-Based Talent Marketplace*.



A Vendor Selection Toolkit

Here's a list of questions to ask and a list of resources that can help you choose a digital wallet vendor. The questions are grouped into categories based on the four opportunities for impact identified in the 2022 JFF market scan report *Building a Skills-Based Talent Marketplace*.

LIFELONG LEARNER | **INDIVIDUAL AGENCY AND CONTROL** | PRIVACY | UNIVERSAL ACCESSIBILITY

QUESTIONS

1. If users decide to use different wallets, will they be able to take their credentials to those wallets or request deletion of their credentials and data from any platforms?

2. Is the wallet based on open standards that enable users to create custom profiles of their credentials, including those stored in other wallets, to share with applications, platforms, or people?

3. Does the wallet allow users to choose where they store their data?

RESOURCES

VERIFIABLE CREDENTIALS PLAYGROUND

During demos of wallet solutions, ask vendors to receive a credential from the Verifiable Credentials Playground. When you're meeting with credential issuers, ask them to issue their credential to a wallet from the VC Playground website.

Make sure that wallets are able to receive a credential from VC Playground. For credential issuers, VC Playground tests can ensure that a vendor's credential can be received by a digital wallet that supports the VCDM.

In addition to asking vendors to test their solutions with VC Playground, you can download wallets from an app store and run the tests yourself. If the tests are unsuccessful, follow up with the vendor to ask for clarification on their interoperability status.

If a solution is listed on Can I Credential? and/or is capable of accepting or issuing credentials from VC Playground, it conforms to the VCDM.

A Vendor Selection Toolkit

Here's a list of questions to ask and a list of resources that can help you choose a digital wallet vendor. The questions are grouped into categories based on the four opportunities for impact identified in the 2022 JFF market scan report *Building a Skills-Based Talent Marketplace*.

LIFELONG LEARNER | INDIVIDUAL AGENCY AND CONTROL | **PRIVACY** | UNIVERSAL ACCESSIBILITY

QUESTIONS

1. Will users be provided with clear information about how their data will be collected, stored, and used?
2. Will users be able to select the amount and type of information they share with others or understand their rights to opt out of nonessential data sharing?
3. Can users easily change tracking preferences and privacy settings and find out whether—and if so, how—wallet developers are sharing their data?

RESOURCES

THE ACLU

The American Civil Liberties Union (ACLU) has published a report that lays out the potential security risks of mobile driver's licenses and other digital ID systems and offers 12 recommendations of laws state legislatures can pass to protect user privacy and foster accessibility as they transition to digital ID cards.

While you may not be involved in crafting regulations governing implementations of digital ID cards, the ACLU's recommendations highlight important factors that all users of digital wallets should consider, including the level of access law enforcement and technology vendors (including application developers) should have to digital credentials, and accountability and reporting mechanisms.

Addressing questions like these during the procurement process can mitigate the risk of exploitation of digital records and preserve the privacy of wallet users.

A Vendor Selection Toolkit

Here's a list of questions to ask and a list of resources that can help you choose a digital wallet vendor. The questions are grouped into categories based on the four opportunities for impact identified in the 2022 JFF market scan report *Building a Skills-Based Talent Marketplace*.

LIFELONG LEARNER | INDIVIDUAL AGENCY AND CONTROL | PRIVACY | **UNIVERSAL ACCESSIBILITY**

QUESTIONS

1

Did the wallet's developers employ a Universal Design for Learning (UDL) approach when designing the architecture?

2

How can users with limited access to tech devices or broadband internet service gain access to their credentials?

3

What is the onboarding process for users who have limited experience using digital tools? Are the instructions available in plain language or in relevant language translations?

RESOURCES

THE GENERAL SERVICES ADMINISTRATION

The U.S. General Service Administration's Section508.gov website offers tools and resources that you can use to assess whether digital wallet applications are universally accessible.

You can ask vendors to share accessibility conformance reports they have filed with the federal government to ensure that their products and services comply with the accessibility standards outlined in Section 508 of the Rehabilitation Act. If a vendor hasn't filed an accessibility conformance report, you can ask them to submit a voluntary product accessibility template (VPAT®).

About JFF

Jobs for the Future (JFF) drives transformation of the U.S. education and workforce systems to achieve equitable economic advancement for all. www.jff.org

About JFF's Language Choices

JFF is committed to using language that promotes equity and human dignity, rooted in the strengths of the people and communities we serve. We develop our content with the awareness that language can perpetuate privilege but also can educate, empower, and drive positive change to create a more equitable society. We will continually reevaluate our efforts as language usage continues to evolve. info.jff.org/language-matters

About JFF Market Scans

At JFFLabs, we believe that innovation and technology, in concert with the continued transformation of traditional systems and policy change, can revolutionize the learn and work ecosystem and, in turn, the ways in which we all live, learn, and work.

Our market scans are based on deep dives into innovation and technology landscapes filled with solutions that are transforming learning and working. Our goal is to identify opportunities, trends, market dynamics, and impact investment insights. Those efforts yield market scans that feature mission-aligned companies and nonprofit organizations of all sizes, from seed-stage startups founded by inspiring innovators and entrepreneurs to growth-stage organizations that are already creating significant social impact and business value.

We review hundreds of organizations to assess their approach to and concern for social impact, and the traction their efforts have gained. We identify the most innovative and advanced technologies and programs connecting people to rewarding jobs and careers, valuable education and training opportunities, effective workforce and education systems, and equitable, resilient opportunities for economic security and mobility—at scale.

For more information about JFFLabs Insights, visit jff.org/insights.

Acknowledgments

The Verifiable Credentials Project would like to thank the following people for taking the time to be interviewed for this report.

Kate Giovacchini, Arizona State University
Hayley Glover, Upskill America Aspen Institute
Renise Walker, Colorado Workforce Development Council
Amber Garrison Duncan, Competency-Based Education Network
Dan Giurescu and Niall O'Driscoll, Credivera
Kim Hamilton Duffy, Decentralized Identity Foundation
Jilian Metz, Wesley Smith, Manu Sporny, and Benjamin Young, Digital Bazaar
Kerri Lemoie, Digital Credentials Consortium
Jesus Torres, Entidad
Amanda Winters, National Governors Association
Amanda Welsh, Northeastern University
Ildiko Mazar, NTT DATA/European Learning Model, vc-ed Co-Chair
Daniel Goldscheider, Open Wallet Foundation
Wayne Chang, Libby Brown, and Ishaan Das, Spruce
Guillermo Elizondo and Keith Look, Territorium
Kymberly Lavigne-Hinkley, Western Governors University

Jobs for the Future