Open Source Student Wallet Final Report

U.S. Department of Education Contract Number: 91990020C0105

Executive Summary

Academic credentials are becoming transformed by digital technology with institutions, government agencies, industries, and others working together to develop digitally enhanced mechanisms to express academic learning outcomes and achievements enabling equitable academic and career prospects for all. These digital credentials can be described in terms of a document (the description of the credential) and an envelope (a container that protects its contents and their authenticity, and specifies an "issuer" and "recipient") into which the document is placed. A learner can store their digital credentials in a wallet that allows them to manage and share them with others. Many organizations in the U.S. and worldwide are experimenting with digital credentials; and emerging standards and specifications are being developed to describe them, define how they may work together and how they might be used by individuals and organizations.

The Massachusetts Institute of Technology, and other U.S. and international members of the Digital Credentials Consortium[1] (DCC)—including Harvard University (USA), McMaster University (Canada), Tec de Monterrey (México) and the Technical University of Munich (Germany)—are working together to develop new digital systems for academic credentials. The DCC approach focuses on open standards, as well as developing tools, systems and approaches to ensure learner control of their digital credentials.

In 2020, MIT entered into an agreement with the U.S. Department of Education to design and implement a wallet to store digital credentials, a critical but under-developed element in the digital credentials technology ecosystem. In fulfillment of this work, the project team at MIT:

- **Developed a Learner Credential Wallet specification**. This specification is informed by the team's leadership and participation in the international digital credentials open standards working groups through the World Wide Web Consortium (W3C), with plans to introduce it through the open standards community.
- **Developed an open source Learner Credential Wallet** mobile application to store open standards-compliant digital credentials (Verifiable Credentials) with learner control (through Self Sovereign Identifiers). The wallet is open source software; it is built upon existing open source libraries developed through international working groups to enable other institutions, governments and vendors to adopt or build upon the wallet. The wallet is published in the Apple App Store for iOS devices and the Google Play Store for Android devices.
- **Deployed the wallet with three institutions of higher education**, College Unbound, Georgia Institute of Technology and San Jose City College, representing a diversity of institution types.
- **Provided technical assistance** to each institution to issue digital credentials.
- **Disseminated the work** via digital credentials ecosystems and communities.
- **Reflected on the Open Source Student Wallet project:** (1) developing the Learner Credential Wallet specification and wallet were straightforward and (2) there is a lack of production-ready tools for issuing Verifiable Credential-compliant credentials and technical assistance will likely be needed to facilitate adoption with Institutions of Higher Education.

[1] For more information on the Digital Credentials Consortium see https://digitalcredentials.mit.edu/.

The project team's work is guided by a consideration for the potential impact of digital credentials in efforts towards more equitable academic and career landscapes in a variety of contexts. The project team expects that the use of this technology will increase the ease with which institutions securely confer credentials. The team also hopes institutions find that a learner-centered approach will offer solutions to some of the issues faced by learners from vulnerable communities in the United States. These could include the financial cost of requesting credentials, an inability to demonstrate competencies obtained from a partially completed or non-traditional degree program or lack of access to credentials from institutions that have closed.

Project Management and Administration

The period of performance began with a kick-off meeting with the project team and the Department on September 30, 2020. Following introductions and acknowledgement of personnel and roles, the project team submitted a work plan and timeline describing the anticipated steps towards achieving milestones and deliverables. As per the agreement, the project team submitted progress reports on a monthly basis, making the Department aware of tasks completed, in progress, and in need of additional time, advice or support. The project team and the Department met virtually on a monthly basis to discuss project progress in more detail.

Develop Open Source Standard & Code Base for Student Credential Wallet

Develop Open Source Standard for Student Credential Wallet

In May 2021, the team published a Learner Credential Wallet Specification, https://digitalcredentials.mit.edu/docs/Learner-Credential-Wallet-Specification-May-2021.pdf. The specification describes the necessary wallet features and technical requirements enabling individuals to curate and present their learning and employment records to others—for example, as applicants to educational programs or employers—in an interoperable manner. The specification is written for a technical audience seeking information about interoperable credential wallets. Credentials related to educational, training and professional development are the primary focus.

The specification builds on ongoing standards work in the World Wide Web Consortium, IEEE, and the Decentralized Identity Foundation focused on interoperable verifiable credentials, decentralized ecosystems enabling their secure exchange, and digital wallet standards enabling interoperability for credential holders. These design choices promote broad interoperability and relevance (even beyond learning and employment credentials).

Specification Name	Description
W3C Verifiable Credentials (VCs) Data Model	A lightweight, interoperable standard for expressing a wide variety of tamper-evident claims whose authenticity can be verified. The VC data model is associated with a range of emerging standards around the request and transfer of credentials, as well as identifier verification. The VC data model functions as an interoperable, secure wrapper around a variety of content (diplomas, transcripts, badges, competencies, etc.). See: https://www.w3.org/TR/vc-data-model/

LER Wrapper and Wallet Specification	Informs wallet functional requirements and provides methods for wrapping payload data models in the envelope, compatible with the VC data model. See: https://cdn.filestackcontent.com/preview/FeqEJI3S5KelmLv8XJss
Universal Wallet 2020	Provides an interoperable digital wallet standard and implementation. This specification is based on the universal wallet interoperability specification and describes how the wallet relates to it. See: https://w3c-ccg.github.io/universal-wallet-interop-spec/

The Learner Credential Wallet specification includes:

1. Wallet functional requirements
2. Conceptual wallet flows supporting flexible use of relevant standards and data models
3. Foundational, extensible wallet design based on, and in support of, (2)
4. Design and implementation choices for wallet standards and credential data models for an initial wallet application
5. Interoperability requirements in sufficient detail to be implemented in software code
6. Overview of extensibility mechanisms

Develop Open Source Student Credential Wallet Code Base

In October 2021, the team released open source code for the Learner Credential Wallet. The source code is:

- Available from the project's Github repository, https://github.com/digitalcredentials/learner-credential-wallet.
- Released under the MIT License, https://github.com/digitalcredentials/learner-credential-wallet/blob/main/LICENSE.
- Documented in the Github repository readme.md (https://github.com/digitalcredentials/learner-credential-wallet/blob/main/readme.md) and in the source files themselves.

In March 2022, the team released versions of the wallet to the Apple App Store and Google Play Store. The mobile apps are available from the wallet website at: https://lcw.app. The project team published an Accessibility Conformance Report after completing a Voluntary Product Accessibility Test at: https://github.com/digitalcredentials/learner-credential-wallet/blob/main/docs/Learner%20Credential%20Wallet%20VPAT2.4Rev508-December%202021.pdf.

Initial Learner Credential Wallet Features

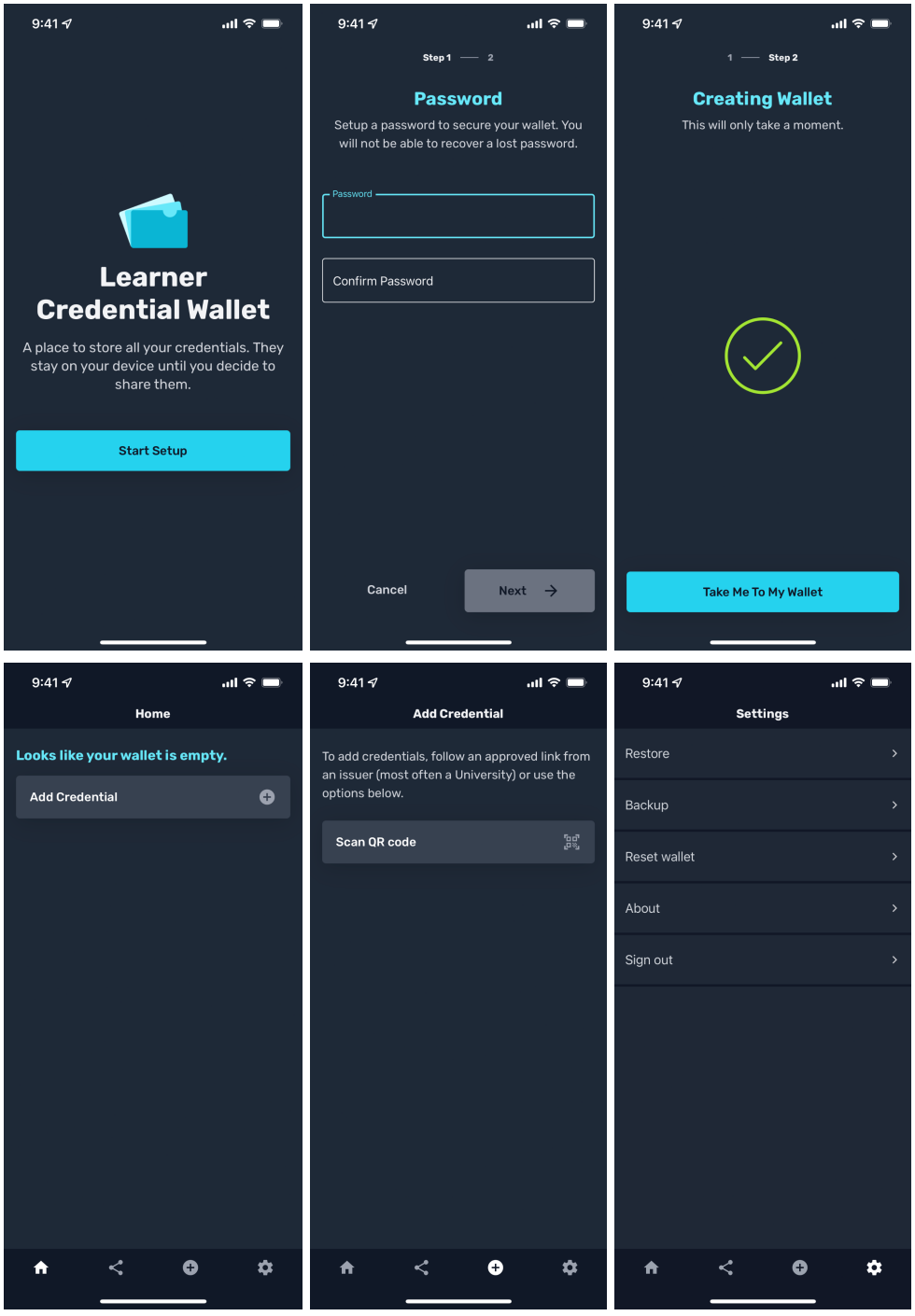
The initial release of the open source Learner Credential Wallet implements the required features of the Learner Credential Wallet Specification.

The key features of the Learner Credential Wallet include:

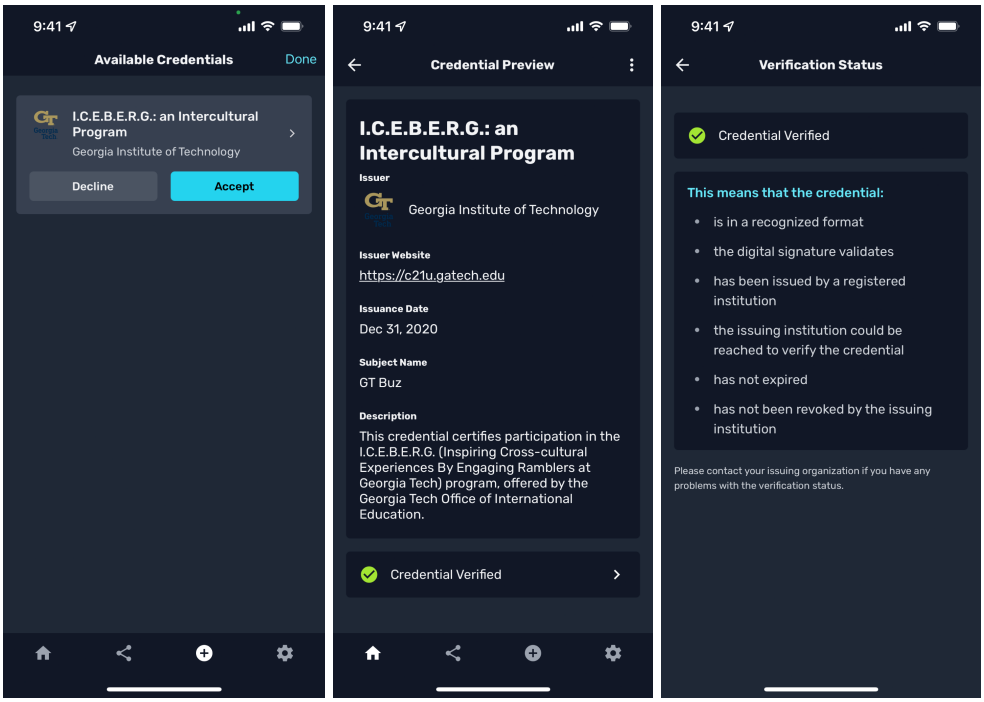
- Login to secure the wallet
- Add a credential (VC) via deep link (URI or QR Code) or via a fully encapsulated QR code
- Display credential(s) locally—Issuer, issuer logo, credential name, credential description, issuance date
- Select and share credential(s) via mobile operating system sharing mechanisms (e.g., save as a

file, send a file, etc.)
- Delete credential(s)
- Backup and restore the wallet from a file

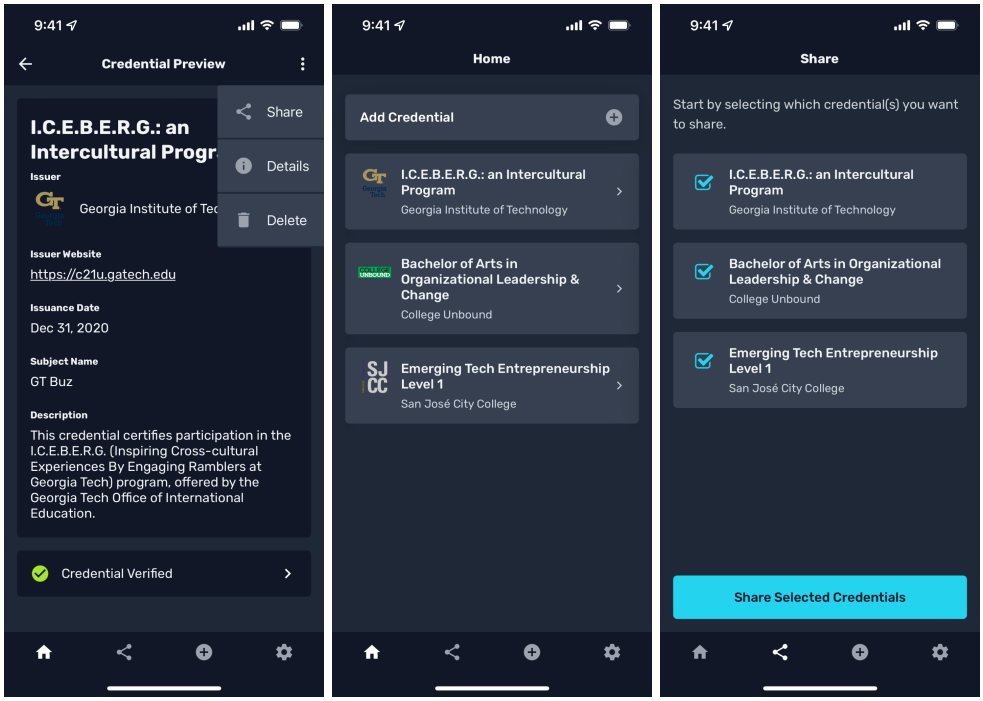
Screenshots of Setting up Learner Credential Wallet in iOS and Settings



Screenshots of Credentials in Learner Credential Wallet:
Add Credential, Credential Preview and Verification Status



Screenshots of Credentials in Learner Credential Wallet:
Actions (Share, Details, Delete), Home and Share Selected Credentials



Comparing the Learner Credential Wallet with the Specification

Below, items marked with a ✓ indicate where the initial release of the Learner Credential Wallet meets the Learner Credential Wallet specification.

1. Request Credential
    a. ✓ The wallet must be able to (on behalf of the holder) request a credential from an issuer.
        i. ✓ The credential request must allow the request to enable holder and subject binding.
        ii. ✓ The wallet must be able to request a credential in response to a holder action.
    b. The wallet may be able to request a credential using a subscribe model in which VCs representing earned credentials from one or more issuers are requested / received / persisted so that the wallet stays up-to-date with available credentials from those issuers.
    c. The wallet may be able to request other records that serve as a proxy for credential-like employment experience.
2. Receive Credential
    a. ✓ The wallet must be able to receive credentials.
    b. ✓ The wallet must be able to decline credentials.
    c. ✓ The wallet must be able to persist credentials and store the appropriate metadata (see Persist Credential).
    d. ✓ The wallet may be able to unpack the credential payload, but it is not required to do so.
    e. The wallet may be able to request, listen for, or subscribe to credential updates, if offered, and if the holder chooses to enable.
        i. The holder must be able to decline a credential received via subscription.
    f. The wallet may be able to persist other records that serve as a proxy for credential-like employment experience.
3. Persist Credential
    a. ✓ Wallet must be able to persist credentials with native format encoding from multiple standards.
    b. ✓ Stored credentials must be persisted with sufficient metadata to allow the wallet to execute the minimal functions described in these requirements.
    c. ✓ Credentials may be stored in both the native format and/or a processed format preferred by the wallet so long as the wallet can fully produce the original record intact (see Send Credentials).
    d. ✓ Wallet must be able to respond to a holder's request to remove a credential and stop persisting that credential.
4. Select Credentials by querying the wallet data store
    a. ✓ The wallet must be able to discover Learner and Employment Records (LER) [i.e., Verifiable Credentials] at least by the name property and description property in the LER.
    b. The wallet may discover content by other parameters.
    c. The wallet may expose an external API.
5. Send Presentation
    a. ✓ The wallet must have a mechanism to create and submit a Verifiable Presentation to a relying party in response to
        i. ✓ A wallet owner action
        ii. A request for a Verifiable Presentation obtained from an Relying Party through a push or pull action, if approved by the wallet holder

   b. The wallet may have a mechanism for receiving and processing presentation requests.
   c. ✓ The wallet must allow the presentation to include holder and subject binding.
   d. The wallet may support pre-packaged presentation bundling options for convenience to the user, depending on parameters such as the type of relying party, credentials requested, etc.
6. Log Activity
   a. The wallet may be able to log activity (e.g., credentials and presentations sent and received for privacy auditing).
7. Holder and Subject Binding
   a. ✓ The wallet may be able to generate identifiers enabling proof of identifier control.
      i. Examples include pairwise decentralized identifiers, other decentralized identifiers, and other methods resulting in a URI identifier that can serve as subject in a Verifiable Credential or a holder in a Verifiable Presentation
   b. ✓ The wallet may be able to generate proofs of identifier control.
8. Management functions
   a. The wallet may be able to manage identity and identifier data. This includes the ability to:
      i. perform Create, Read, Update, Delete operations on decentralized identifier methods (not just create, from previous). I.e., update key material, read, delete.
      ii. group identifiers, attributes, and credentials into “persona” or profiles for use in different contexts.
   b. The wallet may be able to manage connections (e.g. to issuers, Relying Parties, and other parties).
   c. The wallet may be able to manage privacy and sharing settings.

Below, items marked with a ✓ indicate where the initial release of the Learner Credential Wallet meets the additional design decisions and goals described in the Learner Credential Wallet Specification.

- ✓ Minimize technical and infrastructure requirements for learners and issuers
- Ensure requirements are applicable/adaptable to ✓ mobile and web wallets
- ✓ Enable integration into existing systems (including authentication solutions)
- Ensure design is applicable/extensible to emerging protocols (such as authentications built with awareness of decentralized identifiers)
- ✓ Use JSON-LD data formats where possible due to advantages of Linked Data in the educational data standards ecosystem, but support integration of other data formats, including JSON-formatted VCs, non-VCs (including unstructured data)
- Support range of proof mechanisms (✓ JSON-LD, JWT, data minimization proofs), with ✓ initial prioritization of JSON-LD proof mechanisms (based on initial use cases)

Deploy Reference Implementation of Open Standards

In March 2022, the project deployed reference implementations of the Open Standards at three Institutions of Higher Education—College Unbound, Georgia Institute of Technology, and San José City College.

The project team developed and used the criteria listed below to assess the suitability of deployment sites in an effort to examine the implications of digital credentialing in a diverse set of educational contexts.

- Institutions should identify a type of credential and a cohort of learners to participate in the

project.
- Institutions should have the appropriate administrative support to participate in the project and be able to provide project coordination and technical support.
- Ideally, institutions should have initiated basic credential mapping activities, including potentially describing summative credentials in terms of outcomes and/or linkages to industry competencies.
- Ideally, institutions should be able to provide the necessary technical support to participate in the deployment.
- Institutions should be prepared to collaborate with the project team on developing and providing learner-focused documentation, communication and support.
- If an institution is engaged with a vendor who provides credential issuing services, the vendor must be willing and able to collaborate on necessary modifications to vendor services to support the Learner Credential Wallet specification.
- Preference will be given to institutions that serve student populations who are underrepresented in higher education or have otherwise faced barriers to obtaining a degree through traditional means.

After considering a number of institutions, and in consultation with the Department, the project team selected three institutions. Two of these sites, San José City College (SJCC) and College Unbound (CU), primarily serve adult learners—many of whom are first generation, underrepresented in higher education, or have faced significant barriers towards fulfilling their academic goals. The third is the Georgia Institute of Technology (Georgia Tech), a major public research university. Together the sites represent a diverse set of technical capabilities to reflect the wide range of potential adopters of digital credentials. Their technical capabilities run the full gamut, with CU outsourcing most of their administrative and academic computing with limited access for customization and limited in-house technical capabilities to the Georgia Institute of Technology having a project team with deep technical expertise in digital credentials and capable of significant in-kind support.

The site selection also has an eye to the future for the types of digital credentials offered by institutions. The project work focuses on a comprehensive credential at each institution—a final certificate from a program or a whole undergraduate degree. In addition, two of the three sites have already identified granular learning outcomes and competencies for the credential participating in the pilot which provides an interesting avenue for further exploration.

Described below in further detail are the institutions, the credentials selected for the deployment, and the major steps in the deployment. The Technical Assistance section describes the details of the technical assistance required and provided in order to conduct the deployments.

Georgia Institute of Technology

The Georgia Institute of Technology (Georgia Tech) is a public research university located in Atlanta, Georgia. The undergraduate and postgraduate student body is made up of more than 36,000 students with satellite campuses in Europe and Asia. Georgia Tech awards undergraduate and graduate degrees and offers numerous certificate programs through Professional Education and other departments.

The project team worked with Georgia Tech's Center for 21st Century Universities (C21U), a living laboratory focused on the future of higher education, which works to identify, develop, and test innovative educational platforms and methodologies. Both founding members of the Digital Credentials Consortium, MIT has collaborated with Georgia Tech for several years to promote academic digital credentials that empower learner control.

Georgia Tech is exploring the issuance of digital badges, certificates, and microdegrees. These include digital badges for learners that complete non-credential certificate programs (e.g., via Professional Education) and mechanisms for digital credential issuance through their Instructure Canvas-based learning management system for enrolled students. Georgia Tech has prior experience in both issuing digital credentials and developing the technology to support them. The project provided them an opportunity to explore Verifiable Credential-based digital credentials, as their prior efforts have used an alternate form of digital credentials (Blockcerts).

C21U worked with the Georgia Tech Office of International Education (OIE) to select the Inspiring Cross-cultural Experiences By Engaging Ramblers at Georgia Tech (I.C.E.B.E.R.G.) Intercultural Learning Series program for the deployment. “This program addresses various topics, including improving communication abilities, developing intercultural skills, and navigating cultural differences. Students build community by engaging with other students at Georgia Tech, developing skills to recognize cultural differences and the tools to advance their own understanding, gaining self-awareness, empathy, and adaptability, so they may navigate new challenges at Georgia Tech, abroad, and in their future careers.”[2]

College Unbound

College Unbound[3] (CU) is an emerging educational institution in Providence, Rhode Island that aims to provide alternative pathways for adults who have faced significant barriers to completing a traditional Bachelor’s degree program. Founded in 2015, CU is a fully accredited institution with a mission of serving “returning adult learners,” those who began a degree program but had their educational trajectories disrupted due to socio-economic reasons or unexpected life events. CU creates a particularly compelling opportunity for the project team to observe the value and impact of the credential wallet for learners with partially completed degrees.

CU selected their Bachelor of Arts degree for use in the deployment. As a young institution, CU confers a single Bachelor of Arts degree and has a small, yet growing student body of 165 learners which is expected to reach 500 enrolled students by 2025.

At the time of this report CU had not issued digital credentials to graduates of their degree program.

San José City College

San José City College (SJCC)[4], founded in 1921 and a member of the San José-Evergreen Community College District, is a fully accredited community college located in San José, California. The SJCC student body of over 9,000 is 86% minority enrollment, with the majority being Hispanic learners. SJCC has 68 degree and certificate programs, awarding 1,320 degrees in 2019-2020. In addition, they maintain a high transfer rate to public and private four year colleges. SJCC’s mission is to serve students and the community by offering high quality, relevant, and innovative instruction for basic skills, career pathways, university transfer, and life-long learning. They award certificates and associate degrees to eligible students taught in a multicultural environment where student achievement, successful learning, and social justice are highly valued, supported, and continually assessed.

SJCC selected their Technest credential, a program built in 2016 through a collaboration with businesses

[2] I.C.E.B.E.R.G., https://iceberg.oie.gatech.edu
[3] College Unbound, https://www.collegeunbound.org/.
[4] San José City College, https://sjcc.edu/.

and collaborating institutions including MIT, for use in the deployment. The Technest program is comprised of a four course sequence including CIS 106: Introduction to Computer Coding Using Python[5], CIS 107: Data Science[6], CIS 108: Internet of Things[7], and BUS 068: Entrepreneurship. This award winning blended learning program is designed to bridge Silicon Valley's wage and skills gap and offers career counseling and hands-on training as students progress through the courses.

Currently SJCC does not issue digital credentials (i.e., Open Badge-based or Verifiable Credentials-based digital credentials) to graduates of their degree programs nor to participants in non-credential certificate programs. They do make electronic transcripts available for their students.

Technical Assistance

Once selected, the project team worked with the institutions selected as deployment sites to provide technical assistance. The technical assistance provided each site included:

- Coordination with deployment site on any policy / process issues (e.g., student data access concerns)
- Implementation of the Issuing Approach
- Provision of Access to the Institution's Authentication System
- Identification of Key Personnel
- Setting up the Issuer and Testing with the Learner Credential Wallet
- Preparation of the Pilot Credential
- Running the Pilot

Issuing Approach

The project team identified two issuance approaches to be used by the deployment sites. These approaches balanced the technical capabilities of the deployment sites, the support capacity of the deployment sites during the deployment, and the overall timeline. The approaches included:

- Deployment Site Issues Credentials: The deployment site hosts a web application that the wallet can access thereby allowing the institution to "issue" the digital credentials to the wallet. (This may be accomplished by deploying the MIT- / DCC-developed sign-and-verify service or integrating issuance libraries into another application.) This approach includes creating a signing key and adding it to the (DCC) issuer registry and providing issuer authentication metadata for wallet configuration. This approach requires the deployment site technical staff to provide the application (which may require development and implementation effort).
- MIT "Issues" Credentials on Behalf of the Deployment Site: If the deployment site chooses, they could authorize MIT to "issue" digital credentials as part of this deployment on their behalf. The deployment site may choose to do this for technical capability or capacity reasons. This approach requires limited technical involvement on the part of the deployment site and instead requires MIT to provide the issuing technical infrastructure.

Access to the Institution's Authentication System

In order to assure the issuing institution that the provided credential is issued to the intended individual, the Learner Credential Wallet authenticates with the institution's Identity Provider (IdP) / Single Sign On

[5] An 18-week coding course built upon the MITx Introduction to Computer Science and Programming Using Python course.
[6] An 18-week course built on the BerkeleyX Data 8 Foundations of Data Science course.
[7] Built on a Renesas and Microfacturing Institutes course.

(SSO) mechanism. The Learner Credential Wallet requires an authentication step between requesting and issuing the credential to ensure the individual requesting the credential from the mobile device is indeed the individual for whom the credential is issued.

The project team was fortunate that all three deployment sites supported OpenID Connect (OIDC), the default supported protocol in the MIT-/DCC-developed libraries, in their Identity Providers / Single Sign On. The project team was prepared to, but did not need to, extend the underlying libraries to support additional authentication schemes such as Security Assurance Markup Language 2.0 (SAML 2.0).

Identifying Key Personnel

The issuance of credentials at institutions of higher education typically involves cooperation and coordination with and between a number of units at each institution. The issuance of digital credentials adds additional technical requirements and support from technical staff to the typical credential issuance process (which is usually the purview of the registrar and academic departments). In addition, for a successful pilot or long term service for the issuance of digital credentials, institutions will be served well by developing internal processes and developing strong communications and collaborations between units. This project anticipated these needs and worked with the deployment sites to help them form a local project team to support the deployment. In general, the team should include the following roles:

- Project Sponsor: The project sponsor should be an administrator at the institution who can marshall local resources to support the deployment.
- Project Coordinator: The day-to-day contact for the deployment, typically a staff member.
- Program Representative: A representative of the program issuing the digital credentials for the deployment, this might be a registrar, program coordinator or faculty member.
- Technical Representative: A staff member charged with coordinating the technical aspects of the deployment or one or more directly responsible individuals.

Individuals might fill multiple roles depending on the institution. In addition, the project sponsor and project coordinator may need to draw upon the expertise of legal counsel, institutional research, and student-facing support resources.

Setup Issuer and Test with Learner Credential Wallet

The project team worked with deployment sites to set up and configure their issuer, to configure access to the institution's authentication system, and to ensure credentials could be added to the Learner Credential Wallet.

Preparing the Pilot Credential

The pilot institution determined what information to include in their credential for this pilot. The minimum set of credential data are the following fields from the W3C Verifiable Credentials Data Model:

- `name`: Name of the credential
- `description`: Textual description of the program / course / credential
- `issuer.name`: The institution's name or program's name issuing the credential
- `issuer.url`: The institution's website
- `issuer.image`: URL to logo of the institution's choosing
- `issuanceDate`: Date on which the credential was issued, or the current date (for example a program might issue certificates on a specific date such as December 31, 2021)
- `credentialSubject.name`: Name of the individual receiving the credential

The project team provided CU and SJCC a draft csv file to use with the Issuer. Georgia Tech's application used the course information to provide the `credentialSubject.name` and was configured to provide the other data whereas this information was included in the csv by CU and SJCC.

Implementing the Deployments

The project team worked with the deployment sites to implement a multi-step process to run the pilot at their institution.

Step 0: Institution emails participants about the Learner Credential Wallet pilot.

- The email includes a description of the pilot.
- The email may include a consent form to participate in the pilot (if desired by the institution).
- The email may include a consent form to participate in a survey and/or focus group (if desired by the institution).

Step 1: Institution emails participants to start the Learner Credential Wallet pilot.

- The email contains instructions on how to access their credential. Depending on how the issuance is setup:
    - They might receive a (deep) link directly to their verifiable credential (after authentication). [College Unbound and San José City College]
    - They might receive instructions to login to a student portal or learning management system and then how to access their verifiable credential (both steps requiring authentication). [Georgia Tech]
- The email contains instructions on how to install Learner Credential Wallet and includes a link to https://lcw.app.

Step 2: Participants install and setup the Learner Credential Wallet for iOS or Android.

Step 3: Participants add their credential to the Learner Credential Wallet on their mobile phone.

- Students follow instructions from the email from their institution to add their digital credential.
- Students login (authenticate) with their institution before receiving their digital credential.

Step 4: Participants view and share their credentials on their mobile phone.

Step 5 (optional): Participants share their verifiable credential with a school administrator.

- To close the loop on the pilot, the project team discussed whether the institution wanted to add a "confirmation" step to let them know if the participants received their verifiable credential.
- Note: Step 5 was discussed with each deployment site but not implemented.

Step 6: Participants provide feedback on the Learner Credential Wallet experience via survey.

- The institution sends a survey to participants in the pilot cohort. Participants complete the survey.
- Note: At Georgia Tech only, selected participants are also invited to take part in a brief qualitative interview.

Dissemination

The project team successfully developed an open source, proof of concept for a student wallet. The project team engaged with a number of stakeholders over the course of the project for whom the findings

of this report will be valuable and is committed to the open and timely sharing of insights.

The outcomes from this project will be useful for and disseminated to a number of constituencies including:

- The U.S. Department of Education
- Technical and Standards Community: Including the W3C Verifiable Credentials for Education Task Group, IMS Global and especially the Open Badges v3 and Comprehensive Learner Record v2 working groups, IEEE P1484.2 Integrated Learner Records (ILR) Working Group and others
- Broader Ecosystem in the U.S.: Organizations and universities working in the digital learner credentials ecosystem including Jobs for the Future, the U.S. Chamber of Commerce's T3 Innovation Network, Walmart and others.
- University members of the Digital Credentials Consortium

For the technical and standards communities, the active participation of the project team, as well as the open source contributions from the project, are key contributions of this work. This work also represents the dissemination efforts of the project team with these communities. Active participation, code submissions, maintenance of core libraries, contributions to specification and standards development are the lingua franca of these communities. A core value of the project team has been to do this communication and participation from the start, and the team will continue to do so after the close of the project. By hosting the Learner Credential Wallet source code and documentation openly on its Github repository, the project team invites those with a similar interest in promoting equitable learner pathways to build upon this work. The project team presented the Learner Credential Wallet to the W3C VC-EDU Task Group on March 28, 2022.

For the broader ecosystem, the project has participated in initial dissemination efforts and plans to continue beyond the project end. To date, the project activities and outcomes have been disseminated with or have been scheduled to be disseminated with:

- Groningen Declaration Network[8] Annual Meeting: Muramatsu, B. & W.F. van Valkenburg. (2021, November 10). Digital Credentials Enabling Mobility and Verification of Educational Achievements. 2021 Groningen Declaration Network Annual Meeting. Ottawa, Canada.
- NERCOMP Annual Conference: Walsh, G. (2022, March 16). Digital Credentials Consortium: The Learner Credential Wallet. NERCOMP Annual Conference. Providence, Rhode Island, United States.
- ASU+GSV Summit: Schmidt, P. (2022, April 4). The Future of Higher Education A.D. (Stage X panel). ASU+GSV Summit, 13.0 Ed on the Edge.
- Jobs for the Future's forthcoming "Verifiable Credentials Wallets for Learning and Employment Records Market Scan".

The project team has been invited to participate in a number of digital credentials ecosystem activities in which the team is contributing to the overall discussion of digital credentials, identifying interoperability requirements and testing deployment of the project work in additional contexts. The project team is:

- an invited participant in Jobs for the Future's "VC EDU" Wallets Interoperability Working Group
- participating in the U.S. Chamber of Commerce's T3 Innovation Network Pilot Projects

[8] The Groningen Declaration Network is an international, nonprofit and voluntary network that supports academic and professional digital credential mobility so that citizens worldwide are able to consult and share their authentic educational data autonomously, with the expectation of fair recognition. It does this by bringing together stakeholders from across the global Digital Student Data Ecosystem. See https://www.groningendeclaration.org/.

Over the next year, the project team will explore dissemination opportunities with the annual IMS Global Global Digital Credentials Summit, with annual and regional events of EDUCAUSE, and others where the use and adoption of digital credentials are discussed. The project team welcomes the recommendations of the Department.

The project team will also share this report with the Digital Credentials Consortium members, several of whom are in various stages of development with digital credentialing pilots at their respective institutions. The DCC hosts quarterly community calls, highlighting work being done by DCC members and beyond. A project update will be shared with this broader network of institutions during a call in Spring 2022.

Further updates on the work described here, as well as future activities, will be available from the Digital Credentials Consortium Website, https://digitalcredentials.mit.edu/.

Reflections on the Open Source Student Wallet Project

1. Developing the Learner Credential Wallet specification and wallet were straightforward.
2. There is a lack of production-ready tools for issuing Verifiable Credential-compliant credentials and technical assistance will likely be needed to facilitate adoption with Institutions of Higher Education.

1. Developing the Learner Credential Wallet specification and wallet were straightforward.
Developing the specification for an open source student wallet and the wallet mobile application were straightforward. The project team's participation and leadership in the digital credentials standards communities greatly facilitated the speed and ease in developing the specification. The project team was well aware of prior work and the necessary elements for a student wallet from its national and international standards work. In addition, the project team shared drafts of the specification with the standards community and incorporated their review and comments to improve the final specification.

Implementing the specification as iOS and Android applications was also straightforward. The open source community, as well as Apple (iOS) and Google (Android), have provided tools and libraries to enable the development of mobile applications in general. In addition, the project team shepherds and is a significant contributor to the development of underlying libraries that support the features required for the use of W3C Verifiable Credentials in education. These libraries support the open source student wallet directly, as well as enable institutions to issue digital credentials. The specification defined the requirements that any student wallet must support at a minimum thereby defining the features for the minimum viable product. The project team implemented these must-have features, as well as a number of additions to improve the user experience, in the initial release of the Learner Credential Wallet to the Apple App and Google Play Stores.

The open source Learner Credential Wallet for iOS and Android provides a viable open-source alternative to closed wallets to allow individuals to carry their verifiable credentials from any issuer whether that be an institution of higher education or a vendor providing a service to an issuing organization.

2. There is a lack of production-ready tools for issuing Verifiable Credential-compliant credentials and technical assistance will likely be needed to facilitate adoption with Institutions of Higher Education.

The development of the wallet was the primary focus of this project. However, to demonstrate the wallet's capabilities, the project team worked with institutions of higher education to issue digital credentials that could be added to the wallet.

The work with institutions of higher education can be described as: identifying potential deployment sites, identifying and building trust with a team at the deployment site, and working with the deployment site team to issue credentials. Each of the elements of this approach are straightforward, but nonetheless took time to accomplish. As described elsewhere, the deployment site teams were enthusiastic and supportive of the efforts and pleased to have been selected as a deployment site which greatly facilitated the work. Nevertheless, it took about a month of elapsed time with each deployment site to work with the institution's technical representatives to prepare for and initiate the deployment.

Similar to the wallet, the project team took a minimum viable product approach to issuing the digital credentials. The approach consisted of issuing digital credentials from a comma separated value file, or essentially a static list of learners and credentials. This list would then be used by a project provided, self-contained application to issue the credentials. This application was provided as a Docker container that could be hosted anywhere after the modification of a single configuration file with a handful of parameters. This application would use an authentication method (to match individuals and credentials) already supported by each institution. For each site those authentication services needed to be configured in coordination with the local technical representative. In the end, this approach proved challenging with institutions that did not have prior need to integrate outside services with their authentication services. Providing general documentation alone was not sufficient—each institution had a bespoke infrastructure and required a technical expert from the project team to work directly with the institution's technical representative to install, configure and ultimately issue digital credentials.

In addition, there are a number of considerations beyond "issuing" that institutions will need to consider to provide digital credentials to their students and graduates. These include:

- A real time or batch integration of the "issuing" of digital credentials with their student information system. (The project deployments used a one time data transfer to issue credentials.)
- Development of processes and policies to regularly issue credentials.
- Managing the lifecycle of the digital credentials they issue. Institutions will need to address questions such as: In which situations does the institution revoke or update credentials? Do credentials expire?
- Determining if blockchain-based credentials are appropriate. (Or if registry-based issuing is sufficient.)

The project team's experience with these initial deployments made it clear that some form of technical assistance would likely be required with many institutions of higher education to issue digital credentials, and that many would also need or want fully developed "products" to manage and issue digital credentials.

Putting together a team composed of the key personnel described above is a good starting point for institutions interested in offering digital credentials to their students and graduates. Future work is needed to better understand what is needed for integration with student information systems. Case studies and the public sharing of process and policy documents will make it easier for the higher education community to begin issuing digital credentials. Also, national or state policy could facilitate the rate at which institutions offer a wide range of digital credentials beyond microcredentials to include high stakes certifications and degrees.