A National Learning and Employment Records Infrastructure

Progress Towards a Skills Economy

A white paper from Central New Mexico Community College, IBM, Western Governors University, Randa, Public Consulting Group, and Solutions for Information Design

August 2022

This work has been greatly aided by the efforts of these and other organizations that have already developed, piloted, or implemented architectures supporting Learning and Employment Records (LER) and by the cooperation of the specific grant participants to create the model infrastructure that supports the interoperability of these and other architectures. The report results from the participating organizations' individual and collaborative efforts to develop the blueprint, go-forward recommendations, and plans for a national LER infrastructure for the United States.

Central New Mexico Community College, and its collaborative partners, wish to acknowledge the generous financial support for this work by Walmart.

CONTRIBUTORS

The principal contributors to this white paper are:

CENTRAL NEW MEXICO COMMUNITY COLLEGE

Erica Barreiro, Future of Work Strategist
Bill Halverson, Senior Technology Advisor
Kyle Lee, CEO, CNM Ingenuity
Juan Munoz, Student Intern
Angelica Ruiz-Olivas, Digital Platform Architect

RANDA SOLUTIONS

Marty Reed, CEO
Kimberly Linson, Director of Credential Ecosystems

IBM

Rick Goldgar, Associate Partner, Digital Credentials
Alex Kaplan, Partner and Global Leader, Digital Credentials
John Kirby, Managing Consultant, Blockchain

WESTERN GOVERNORS UNIVERSITY

Darin Hobbs, Vice President of Academic Records, Credentials & Careers

PUBLIC CONSULTING GROUP

Joshua Marks, Senior Solutions Architect/Advisor
Greg Nadeau, Manager

SOLUTIONS FOR INFORMATION DESIGN, LLC

Taylor Davis, Analyst
Lauren Runco, Director of Strategy
Rita Dietrick, Project Manager

WORDSLINGERS, LLC

A special thanks for your editing and formatting wizardry

INDIVIDUALS PROVIDING REVIEWS AND COMMENTS INCLUDE:

Naomi Boyer, Education Design Lab
Holly Custard, Strada Education
Deb Everhart, Credential Engine
Gordon Freedman, GoEducate
Taylor Kendal, Learning Economy Foundation
Sharon Leu, JFF Labs
Nick Moore, Office of the Governor of Alabama
Ricardo Torres, National Student Clearinghouse

TABLE OF CONTENTS

EXECUTIVE SUMMARY

A national Learning and Employment Record (LER) infrastructure revolutionizes outdated credentialing and hiring systems. Using an LER infrastructure, learners and employers will communicate through a shared skills language and interoperable technology infrastructure designed to easily connect workers with both jobs and skills-building opportunities. The LER infrastructure will become core to an individual's lifetime cradle to career skills-building journey. It will assist them in charting and managing their career as they move from one learning and employment environment to the next. The LER will also enable community and non-profit organizations, government agencies, learning providers, and employers to create actionable, linked, and interoperable systems that support each individual's education and employment journeys. With an LER, learners, earners, employers, and education providers will effortlessly and efficiently exchange trusted information about proven learning and employment achievements. These exchanges will reduce the complexity of navigating talent pathways by providing everyone with clear roadmaps to careers and skills-building activities. All of this will make it easier to connect workers with jobs that fit their skills, interests, and aspirations. Finally, the LER will ensure all this exchange of personal information is protected and under the control of each individual as they navigate their journey.

BACKGROUND INFORMATION ON (1) SKILLS-BASED HIRING PRACTICES, (2) THE LEARNING AND EMPLOYMENT RECORD (LER) ECOSYSTEM, AND (3) WHY EXPANDING EMERGING TECHNOLOGIES LIKE BLOCKCHAIN ARE THE FUTURE

The needs of our workforce have moved us towards an economy where "skills are the currency of the future" (Estrada, 2020). The national Learning and Employment Record (LER) ecosystem revolutionizes our outdated and confusing skills-credentialing and hiring systems. This revolution will come about through the broad-scale adoption of new standards and technologies, making it easier for individuals to navigate the talent marketplace and employers to connect with the right talent for their jobs. This national LER ecosystem, designed and deployed using open-standards-based blockchain architectures, makes it possible for the effortless and efficient exchange of verifiable lifelong skills and employment history.

> "By moving towards a system where individuals and employers can understand the skills an individual has by the credentials they hold, we enhance the power of the LER as an accelerator for skills-based hiring and education practices." (American Workforce Policy Advisory Board, 2020, p.8).

THE LER INFRASTRUCTURE AND INTEROPERABILITY: (1) WHAT IS AN LER, AND (2) WHY INTEROPERABILITY IS IMPORTANT IN DESIGNING AN LER INFRASTRUCTURE

The LER infrastructure (learning and employment records) provides a digital record of an individual's education, training, and work achievements. As interoperable records, they connect with other digital records providing broad insights concerning jobs, careers, and the skills required for success. The T3 Innovation Network noted that LERs are for skills and hiring what Electronic Health Records (EHRs) are for medical care. Both combine data about the individual that allows the person to understand better their "diagnoses" and available options based upon these "diagnoses." Individuals easily find matching educational and employment opportunities by exchanging, viewing, and verifying LER records. In addition, an LER empowers individuals with informed decisions about career and educational possibilities. This efficient and private means of sharing verified credential information lowers barriers to education and employment. The LER infrastructure provides shared and interoperable services connecting employers, education, and individuals through standards-based technology, secure data repositories, and well-defined governance practices.

Essential to the success of the LER Ecosystem, interoperability enables an individual to carry their LER information with them as they move through their cradle to career journey. Interoperability allows information to be transferred, linked, and aggregated from different education entities, employers, and other sources. To achieve interoperability, LERs must utilize a commonly agreed-upon set of public domain data and technology standards that are not proprietary to any one LER system provider.

EXECUTIVE SUMMARY

CURRENT STATE OF THE LER INFRASTRUCTURE: (1) ISSUES WITH TRADITIONAL CREDENTIALING, (2) ISSUES WITH CURRENT TALENT MARKETPLACES, AND (3) HOW ADVANCEMENTS IN THE LER ADDRESS THESE CHALLENGES

The recommended LER infrastructure overcomes the limitations of traditional credentialing and talent marketplace systems by taking advantage of advancements in current LER systems. The limitations of traditional systems include the inability to share trusted skills-based credentials between systems and a lack of standardization which impedes credential reviewers' understanding of the value and provenance of the provided credentials. Further, traditional systems make it difficult to trust the credential's authenticity and to assure that control of the credential belongs to the individual. These limitations hamper broad-scale adoption.

Advancements in LER systems address these limitations by using common standards and governance approaches that mitigate these issues. These advancements include governance approaches that use permission-based and decentralized blockchain-based technologies. Blockchain technologies provide a decentralized "ledger" with strong support for credentials verification, an individual's control over their data, and "permissioned" governance structures that assure all ecosystem users have the appropriate rights and permissions for their specific activities in the LER ecosystem. In addition, the LER systems support robust trust protocols that empower the user to decide who can access and share credential-based information while also supporting the confirmation of the owner's identity.

REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

An LER infrastructure consists of shared services that include a technology platform, technology and data standards, registries to assure identity and trust, and governance structures that support the management of the national LER infrastructure.

The LER infrastructure is part of a much larger talent and education ecosystem that uses LERs for various needs around identifying skills, hiring, jobs, educational needs, and staying current with a job's evolving skill requirements. Stakeholders will rely on the LER infrastructure technology platform functions and the services it provides:

- management of issuing, updating, maintaining, and revoking credentials, wallet provider's solutions enabling individuals to store and manage their credentials,
- career and learning pathways solutions that guide learners on their cradle to career journey,
- operator services to run the permission-based LER infrastructure.
- cryptographically based trust to ensure insights into the authenticity and provenance of the credential
- technological standards that enable interoperability of credentials between different LER systems,
- governance frameworks that ensure regulatory compliance and data privacy protection.

EXECUTIVE SUMMARY

THE ESSENTIAL ROLE OF SKILLS-BASED LEARNING IN A NATIONAL LER INFRASTRUCTURE AND LER ECOSYSTEM & THE ROLE OF DATA AND TECHNOLOGY STANDARDS

The increasing diversity of existing job classifications and the acceleration in creating novel job categories make a national interoperable LER infrastructure timely and important. It is not enough to have a degree: a person must also demonstrate employment-ready specialized skills. Employers need to both confirm and understand these skills by verifying an individual's credentials and having insight into the credential's provenance and content.

The national LER infrastructure addresses these requirements, identifying and confirming skills across interoperable LER systems. The national LER infrastructure also benefits individuals by giving them control over the records of their achievements, skills, and credentials, all using technology that will protect the individual's privacy.

The recommended national LER infrastructure requires adherence to standards. Standardized data assures LER records can be widely shared and understood. Furthermore, open standards, rather than proprietary ones, will help ensure no single vendor can control the LER and that it will belong to the individual. In the United States, collaboration between the government, business, and education stakeholders enables common, shared standards. Supported by policies and security functions, these standards help assure individual privacy.

LEGAL AND REGULATORY REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

As LER systems evolve, applicable legal and regulatory requirements will guide their use and adoption. The legal landscape will continue to be dynamic as the transition to digital credentials accelerates, adoption increases, and people and organizations interact with each other through these interoperable digital credentials. Long standing laws and regulations governing the world of physical skills-based credentials will evolve along with the creation of new emerging laws for the digital world. How the LER infrastructure evolves and is adopted will be intertwined with the changing legal and regulatory landscape.

Four primary regulatory frameworks guide the current environment:

- The European Union's General Data Protection Regulation (GDPR), one of the strictest privacy and security regulations, imposes obligations on worldwide organizations collecting data related to EU citizens.
- The California Consumer Privacy Act (CCPA), a consumer privacy law like the GDPR; with a broad view on what constitutes private information.
- The Family Educational Rights and Policy Act (FERPA) guides any LER implementation that uses data from educational agencies receiving federal education funding.
- The Fair Credit Reporting Act (FCRA) governs, in part, the permissible use of personal data, which requires explicit permission from individuals for their data to be used for education admissions, college transfers, and employment. FCRA also governs audit controls on the use of data and actions taken to contest erroneous data.

EXECUTIVE SUMMARY

NATIONAL LER INFRASTRUCTURE RECOMMENDATIONS

LER infrastructure development is at a critical juncture in the United States, requiring state and national leadership to help craft policy and create the necessary infrastructure. To achieve the adoption of the national LER infrastructure, we recommend that state and national leaders, in partnership with employers, educational providers, and learners, advance the following:

- Technical Standards:
  - ✓ Continue to mature LER-related standards to support our evolving job roles and hiring practices.
- Shared Services:
  - ✓ Create a technical infrastructure that provides shared identity/trust and skill/credential services for all LER ecosystem stakeholders.
- Talent Marketplace:
  - ✓ Integrate Talent Marketplace provider offerings with the LER infrastructure.
- Regional LER Projects:
  - ✓ Invest in regional/sectoral LER projects, connect-a-thons, reference implementations and develop a supporting LER Issuer Maturity Model.
- Legal and Regulatory Frameworks:
  - ✓ Develop and document standard legal and regulatory terms of use, user agreements, and requirements for data sharing and trust.
- LER Infrastructure Compliance:
  - ✓ Create an organization that certifies LER technologies and applications as “LER infrastructure compliant.”

EXECUTIVE SUMMARY SYNOPSIS

The complete report describes the current state of LERs, the requirements for that infrastructure, and the proposed efforts to scale to a national LER infrastructure. Appendices include case studies on the four most mature LER ecosystems, a summary of applicable core LER legal and regulatory frameworks, and a technical decision guide for the adoption of LER infrastructure systems and applications.

This report is a collaborative effort between six organizations engaged in projects representing some of the most mature LER efforts. These organizations are Central New Mexico Community College, IBM, Public Consulting Group, Solutions for Information Design, LLC, Randa Solutions, and Western Governors University. This effort was coordinated by Central New Mexico Community College, a Hispanic and Native American serving technical and transfer community college and the first community college in the nation to issue non-degree and degree credentials to students on a blockchain.

Over almost one year, this team met bi-weekly to define, debate, and synthesize their knowledge of and perspectives on a definition of a shared infrastructure that allows interoperability between current leading and future LER architectures. Our goals were to discuss and describe how the United States could create an infrastructure that would make it easier to connect workers with jobs and provide decision-makers and technologies guidance on the “nuts and bolts” of creating a national LER infrastructure. Before the publication of this report, the team engaged in a peer review process, inviting 20+ individuals from organizations who have been pioneers and thought-leaders in the work to create a national LER infrastructure. Their generous feedback on this report’s concepts, architecture, and recommendations are greatly appreciated and acknowledged.

BACKGROUND

There is a growing chorus of voices calling for a robust skills ecosystem (Ark, 2022; Deegan, 2021; Ed Design Lab, 2022; Watson, 2019, Forbes 2020) motivated by desires to achieve better and more equitable education and employment outcomes, and as a means to an economy in which "skills are the currency of the future" (Estrada, 2020). A global pandemic, which displaced millions of American workers and triggered the Great Resignation, happened in concert with a greater reckoning that all lives are not equal inside our organizations—built on the legacies of system inequities. The convergence of these, and other events, has catalyzed both the skills revolution and the "future of work" occurring now.

Millions of American workers will need reskilling and upskilling documented as part of their lifetime learning record. Employers will need to rely more heavily upon skills-based hiring to recruit the diverse talent they need, and educational providers will need to offer more skills-based learning aligned to various career pathways. In this context, we know we must build equitable and efficient systems that can better connect people to learning and work, leading to economic mobility.

> "BY MOVING TOWARDS A SYSTEM WHERE INDIVIDUALS AND EMPLOYERS CAN UNDERSTAND THE SKILLS AN INDIVIDUAL HAS BY THE CREDENTIALS THEY HOLD, WE ENHANCE THE POWER OF THE LER AS AN ACCELERATOR FOR SKILLS-BASED HIRING AND EDUCATION PRACTICES. LERS ILLUMINATE HOW SKILLS ALIGN WITH INDUSTRY-SPECIFIC CAREER PATHWAYS. THIS ENABLES WORKERS AND EDUCATION INSTITUTIONS TO UNDERSTAND HOW A SET OF SKILLS CAN TRANSLATE INTO VARIOUS CAREER PATHWAYS AND PROVIDE GUIDANCE ON SPECIFIC STEPS TO TAKE TO UPSKILL OR RESKILL"
>
> AMERICAN WORKFORCE POLICY ADVISORY BOARD, 2020, P.8

Current credentialing systems have many significant limitations, including the decision-making value of non-degree credentials. As a result, their weight in hiring and career advancement is still relatively undervalued compared to that of a college degree (Wellspring Initiative, 2021). This undervaluing exacerbates talent pipeline issues and perpetuates the gap in economic mobility opportunities afforded to historically underserved populations, as they are far more likely to have gained skills and competencies through alternative learning and credentialing pathways (Rockeman, 2022).

Over the last few years, adoption of and interest in skills-based hiring practices have grown, motivated by better and more equitable hiring outcomes (Wellspring Initiative, 2021). At the same time, there has been dramatic growth in the issuing of digital credentials. In the U.S. alone, nearly one million unique credentials are issued by various organizations (Credential Engine, 2021). Educational institutions, new professional education providers, and employers are issuing records of achievement in response to job market demands. However, current credentialing systems have many significant limitations, including a lack of clarity around the value of these many types of credentials (Credential Engine, 2021).

Current credentialing systems provide a limited means of determining the skills and competencies of an individual based on their credentials. And while credential holders have many means to communicate credentials (e.g., resumes, job boards, social media, and online applications), there is no clear trust anchor for these credentials. On the other hand, the transcript — the traditional means of assuring trusted college credentials — is problematic, as the learning records in a college transcript seldom detail specific skills and competencies. In addition, sharing such credentials is often a slow and costly process. Although they provide additional means of displaying and exchanging credentials, the recent increase in the issuance and management of non-traditional credentials (e.g., badging) has only increased the need for a means to assure trust in the accuracy of these claimed skills and competencies.

Several recent projects have created the building blocks of a nationally scalable infrastructure that can support a skills-based learning and LER ecosystem in the United States.

BACKGROUND

In 2018, the U.S. Chamber of Commerce Foundation and the Lumina Foundation launched the T3 Innovation Network to "explore the emerging technologies and standards in the talent marketplace to create more equitable and effective learning and career pathways." LER-related efforts are central to this work. Cheryl Oldham, senior vice president of the U.S. Chamber Foundation, stated: "Learning and employment records will operate like digital passports, giving people a lifelong record that consolidates their skills and work experiences throughout their career. This is the next step in creating the future of work where people are empowered with their information and employers can more efficiently recruit the talent they need to thrive in the modern economy" (LER Resource Hub, 2020).

In 2019, the American Workforce Policy Advisory Board (AWPAB) Data Transparency Group published a white paper identifying interoperable learning records as "a novel and technically feasible, achievable way to communicate skills between workers, employers, and education and training institutions" that would enable "the ability to more efficiently match people with jobs [and] will benefit both workers and employers by reducing time to hire and creating a more efficient labor market" (American Workforce Policy Advisory Board, 2019, p. 6). This paper laid out definitions, principles, and recommendations informed by an expanding landscape of pilot LER efforts.

In 2020, the AWPAB Digital Infrastructure Working Group published a white paper on LERs that advocated for an "LER imperative" to address the significant disruptions in the labor market due to the pandemic and rapid digital transformation. "LER technology enables us to dynamically respond to the labor market challenges of our current moment by providing a foundation upon which we can build infrastructures, systems, and services that support a future in which individuals are empowered to pursue lifelong learning and career advancement, to demonstrate their capabilities on a level playing field, and support employers in finding and investing in talent" (American Workforce Policy Advisory Board, 2020, p. 3). This paper described LER pilots that tested and effectively demonstrated the technical feasibility of LERs and helped lay the foundation for interoperable scaled LER technology.

The 2020 AWPAB paper also identified key qualities that a national system of LERs needs to enable robust labor market outcomes. The report summarized these qualities: "LER data must be interoperable so that that information can be easily exchanged and understood, and verifiable so that information can be trusted. Individuals must be assured that their personal information is secure and private until they wish to share it. LERs should be accessible and shareable from anywhere and on any device" (American Workforce Policy Advisory Board, 2020, p. 5).

In 2021, a report on the Education Blockchain Initiative, funded by the U.S. Department of Education and managed by the American Council on Education (ACE), documented the lessons learned from four LER pilots. Stakeholders in the pilots shared their perspectives on the potential for LER ecosystems that center on "the premise that learner employment records, blockchains, and interoperability standards must empower learners to generate social and economic equity" (Hansen et al., 2021). Critical guidance for developing and deploying these pilots outlined "solutions that leverage interoperability, open standards, and protocols." Among the lessons learned through these pilots was the necessity of designing solutions to fit many different schemas and platforms and the need to mature the technology for broader adoption.

Designing solutions to serve the most marginalized individuals in the workforce is critical to ensuring LERs are not reproducing existing talent pipeline inequities. Digital Promise's 2022 report outlines inclusive design principles and user profiles created for LER platform designers/issuers from their research collaboration with frontline workers. The design principles include allowing for self-issuing and third-party endorsements, providing individuals with the agency in how their information is presented and shared, addressing safety and privacy concerns, and ensuring ease of use and accessibility over a lifetime.

BACKGROUND

Numerous other projects are helping to advance the frameworks, technology, policy, and practices needed to create an accessible, equitable, and impactful LER ecosystem. With the LER work currently underway, it is challenging to stay current, even among the pioneers who are helping map this new terrain for broader participation in the LER ecosystem. However, it has also created a robust community of practitioners, researchers, and technologists committed to sharing their knowledge and expertise.

This report results from a collaborative effort between six organizations engaged in projects representing some of the most mature LER infrastructure efforts. For almost one year, this team met bi-weekly to identify, debate, and synthesize their knowledge and perspectives around what constitutes and defines a shared and interoperable LER infrastructure encompassing the current LER initiatives. The team also engaged in a peer review process of the draft paper with 20+ individuals and organizations who have been pioneers and leaders in the LER work. These peer reviewers provided feedback on this report's concepts, architecture, and recommendations.

THE LER & INTEROPERABILITY

While there are different interpretations of what constitutes an LER, a commonly accepted one is published on the T3 Innovation Network website:

> "A learning and employment record (LER) is a digital record of learning and work that can be linked to an individual and combined with other digital records for use in pursuing educational and employment opportunities" (J Goodell, 2020).

The T3 Innovation Network also noted that an LER could be compared to electronic health records (EHRs). However, while EHRs have resulted in improved healthcare delivery outcomes, they were not designed in a way that makes them transferable or exchangeable across technology systems. The results are that users—both patients and health providers—are frustrated by fragmented and siloed medical records. With improving education, economic mobility, talent pipeline, and economic growth outcomes, we can learn from the limitations of EHR systems as we develop and deploy interoperable LER systems that can form the basis of national LER infrastructure.

In a white paper written in support of the U.S. Department of Education, Office of Educational Technology's Education Blockchain Initiative, the authors articulate why interoperability is so important in designing LER infrastructure:

> "It is currently very challenging to prove what we know and what we can do in efficient, expedient, and equitable ways. Verifiable data about our learning and work histories are in the hands of institutions, employers, and third-party data aggregators. It's hard to understand the many different processes for the verification of different types of records. We can list our history in our CVs and on sites like LinkedIn, but for potential employers or educators to verify experience, they must contact the education, training, military, and/or employer organizations involved or third parties who manage verifications...siloed data cannot paint a clear picture of a person's knowledge level and capabilities. It is not only disconnected, but it isn't aligned to be communicated clearly or understood" ("Understanding Interoperability for Education Blockchains," U.S. Department of Education, Office of Educational Technology's Education Blockchain Initiative, 2020).

"A LEARNING AND EMPLOYMENT RECORD (LER) IS A DIGITAL RECORD OF LEARNING AND WORK THAT CAN BE LINKED TO AN INDIVIDUAL AND COMBINED WITH OTHER DIGITAL RECORDS FOR USE IN PURSUING EDUCATIONAL AND EMPLOYMENT OPPORTUNITIES"

J GOODELL, 2020

Interoperability is essential to the success of an LER infrastructure where information can be transferable, linked, and aggregated from different sources. The AWPAB Digital Infrastructure Working Group defined interoperable as:

> "using open standards and common ontologies/frameworks to enable data to be machine-readable, exchangeable, and actionable across technology systems and, when appropriate, on the Web." (American Workforce Policy Advisory Board, 2020, p. 12).

While new technology tools such as digital wallets, blockchain, and machine-readable protocols play a critical role in interoperability, there is no guarantee that interoperability will occur. To achieve interoperability, LERs must utilize a commonly agreed-upon set of public domain data and technology standards that are not proprietary to a particular LER system.

As LER system providers evolve, the LER infrastructures should provide data in formats easily consumed by interoperable LER systems. The new LER system deployments will need to be able to ingest learner data from multiple sources in open, non-proprietary data standard formats established throughout the LER ecosystems. The T3 Innovation Network is an organization that is helping LER pilots adopt and build systems that can cooperate throughout an LER ecosystem.

THE LER & INTEROPERABILITY

As T3 Innovation Network and many other stakeholder groups advance LER infrastructure, a definition of an LER should evolve to support the type of functionality required for interoperability. The definition below reflects this evolution with the underlined additions to the existing T3 Innovation Network definition.

> "A learning and employment record (LER) is an ***open***, ***standards-based***, ***non-proprietary*** digital learning and work record that can be linked to an individual and combined with other digital records to pursue educational and employment opportunities." (T3 Innovation Network)

The LER is one of the primary building blocks of an LER infrastructure(s) that will support a wide range of technology platforms and applications that enable learners, earners, employers, and organizations to document, share, view, and analyze learning and employment data.

THE CURRENT STATE OF LEARNING AND EMPLOYMENT RECORDS

To lay out an approach for creating LER infrastructure(s), it is helpful to understand both the limitations of traditional credentialing and talent marketplace systems and the advancements in recent LER systems that have addressed these limitations.

ISSUES WITH TRADITIONAL CREDENTIALING SYSTEMS

Initially, the process for software systems managing digital credentials was simply a replication of its paper-based predecessor. This replication led to the following challenges with traditional credentialing systems:

TRADITIONAL SYSTEMS HAVE LIMITED MEANS OF KEEPING CREDENTIALS CURRENT.

Traditionally, a limited subset of the holder's complete learning or employment data is held and controlled by an entity. In some instances, this entity is a department within the issuing organization. However, in many others, the entity managing the credential repository is not the issuer. Separate data is held in different systems by colleges, employers, state licensing boards, credential management organizations, etc. Though this approach provides a control point for a particular subset of records, it also means that every subset of an aggregate set of LERs for an individual may reside in a different repository and that the security and integrity of each repository are highly dependent on the owner of that repository, and that any attempt to collect credentials will require the requestor to solicit each repository manager and be subject to each manager's policies, methods, and fees for providing credentials. Since virtually all individuals have credentials from multiple credential issuers, collecting and validating them can be a cumbersome and costly process for all stakeholders.

TRADITIONAL SYSTEMS TYPICALLY USE SEGREGATED, CENTRALIZED DATABASES.

Traditional systems which depend on paper or image-based transmission of credentials are open to fraud through the falsification of those credentials. Mitigation is typically addressed by requiring the requestor to contact the credential's issuer directly. However, as mentioned above, the number of credential issuers for a single holder of a collection of credentials often works against the requestor, taking the time and cost to verify the credentials. It is also often difficult to detect fraud by credential holders, especially in cases where the issuer of the credential does not provide means of verification independent of their system.

TRADITIONAL SYSTEMS HAVE LIMITED CAPABILITY TO SUPPORT THE VERIFICATION OF CREDENTIALS.

Traditional systems vary widely in their mechanisms for verifying credentials. Such systems may rely on human interactions and review and may require duplicate data entry into an authoritative system to manage verification. In many cases, the data entry person or organization is legally liable for the data entered into the authoritative system. There exist entire groups in both government and private organizations who deal with legal claims from individuals against the organization seeking recognition for credentials (e.g., certifications) that were improperly awarded. This creates a high cost of time and money for these organizations, and the disputes can negatively impact the individual's livelihood.

TRADITIONAL SYSTEMS HAVE LIMITED FRAUD PREVENTION MECHANISMS.

Many traditional systems have limited, if any, interoperability with the issuers of credentials systems. This means that the traditional system may not have the most current status for a credential except for highly regulated licenses and certifications that formally require updates (e.g., health care professionals). In addition, even with mechanisms that allow issuers to update credential status, the system may enable credential holders to prevent those updates (e.g., to prevent showing a revoked license).

THE CURRENT STATE OF LEARNING AND EMPLOYMENT RECORDS

The Talent Marketplace represents the whole spectrum of solutions (e.g., human resources management information systems (HRMIS), applicant tracking, job posting boards, etc.) designed to assist employers and job seekers through the recruitment life cycle. Within this ecosystem, credentials act as a "currency" between the holder of the credential, the job seeker, and the credential consumer, the employer. While talent marketplace systems have evolved, especially with the adoption of automation and the use of artificial intelligence, they still have many limitations.

ISSUES WITH CURRENT TALENT MARKETPLACE SYSTEMS

TALENT MARKETPLACE SYSTEMS AND TOOLS VARY WIDELY AND HAVE LIMITED INTEROPERABILITY.

Currently, the talent marketplace is both very dynamic and very fragmented. Though larger employers typically use one of a few market-leading HRMIS and applicant tracking systems, employers' policies, compliance rules, and best practices can vary widely. Except for a few instances, most of these systems maintain the job and candidate data in either proprietary or simple text formats, which are only interoperable through rudimentary application-specific or custom developed interfaces.

JOB SKILLS, DESCRIPTIONS, AND TITLES MAY VARY SIGNIFICANTLY ACROSS EMPLOYERS IN THE SAME SECTOR.

Any two employers may have different titles, descriptions, and requirements for what is fundamentally the same position. The lack of standardization of required skills, job descriptions, and titles complicates the application and hiring process. It often confuses candidates and recruiters, who must tailor resumes and applications for each employer.

TALENT MARKETPLACE SYSTEMS DO NOT HAVE EFFICIENT MECHANISMS TO VERIFY LER CLAIMS.

The most common talent marketplace systems providing educational and work records have little or no means of assuring the claims' veracity or authenticity. Most professional and social networks allow job seekers to document their learning and employment history without providing any vehicle for independent verification.

THE CURRENT STATE OF LEARNING AND EMPLOYMENT RECORDS

More recent credentialing systems contain built-in mechanisms to prevent or mitigate the issues with traditional systems.

ADVANCEMENT IN LER SYSTEMS ADDRESS ISSUES IN TRADITIONAL SYSTEMS

SOME EMERGING BLOCKCHAIN-BASED SYSTEMS USE SECURE, DECENTRALIZED "LEDGER" REPOSITORIES.

In these systems, LER data or its reference is placed in a "ledger" type repository that is replicated across multiple sites, supports multiple issuers, holders, and requestors, contains entries that are unalterable (i.e., "immutable"), and is only available to those who have permission to use it. These decentralized repositories are peer systems that replicate data in shared repositories and do not rely on a centralized (or individually owned) source of truth. This means multiple issuers can publish to the same ledger, allowing holders to collect credentials from multiple issuers and share them with permissioned requestors with a single request. If an issuer goes out of business (e.g., a college closes), the information permanently remains in the distributed system and is not "lost."

ADVANCED SYSTEMS CAN SUPPORT STRONG TRUST IN LERS.

More recent systems are created as permission-based systems, allowing only qualified and permissioned issuers to issue and maintain their LERs. Of course, this approach must be implemented by the specific system. Systems that enable any issuer to issue any LER have no advantages in this capability. A few traditional systems support this, but typically only for a small group of credentialing systems.

NEW DIGITAL IDENTITY MECHANISMS SUPPORT THE DEFINITIVE CONFIRMATION OF THE OWNER'S IDENTITY.

Recent technologies create unique, secure identities for the users of these systems. This identity confirmation is essential in matching the person to their credentials and assuring a proper chain of ownership. Digital identity solutions are part of a broader set of technological developments adopted by governments and enterprises to confirm "you are who you claim you are."

EMERGING SYSTEMS CAN KEEP LERS CURRENT.

By automating the issuing and updating process and shifting the LER verification to a ledger shared across multiple issuers, blockchain-based systems provide an efficient mechanism to easily maintain LERs, allowing the issuer to update and revoke credentials in real-time. Of course, this requires that the issuer perform that action. However, the mechanism for updates and revokes can be the same as the mechanism for issuing LERs, so that any participating issuer has a standard mechanism for these actions.

EMERGING SYSTEMS HAVE ROBUST CRYPTOGRAPHIC CAPABILITIES THAT LIMIT FRAUD AND EXPOSE ANY TAMPERING WITH AN LER.

Since blockchain-based systems feature unalterable entries, attempts to change the entry or signature are immediately visible and will not be incorporated into the ledger. In addition, a permission-based system assures all stakeholders are known (not anonymous); hence, they are auditable and traceable.

EMERGING SYSTEMS HAVE A STRONG CAPABILITY TO SUPPORT THE VERIFICATION OF CREDENTIALS.

Blockchain-based systems are based on entries to an otherwise unalterable ledger. As a result, these systems give the requestor a high assurance of the verifiability of the LER.

REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

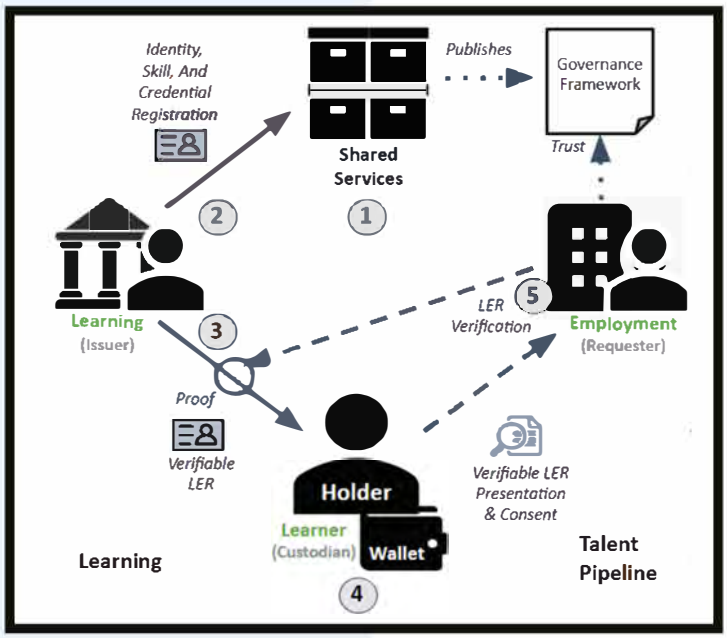
LER infrastructure consists of shared services, including technology (e.g., blockchain-based LER systems, assertion tools, credential publishers, digital wallets, digital identity), technology and data standards, registries, and governance that provide the functionality and management for an LER system. A national LER infrastructure must have a clear means to enable interoperability between different LER systems, require a standardization of shared data, preserve security for the various stakeholders, and support user agency over their data. LER infrastructure must be a means to satisfy the following needs simply and efficiently:

- Allow LER holders to manage and permit the viewing of their LERs
- Discover a candidate's LERs (when permissioned by the holder).
- Verify a candidate's LERs accuracy and currency.
- Understand the skills and competencies identified or implied in a candidate's LERs.
- Assure compliance with legal privacy and security requirements for all stakeholders.
- Manage digital identity to assure a proper chain of ownership.

Satisfying these needs will provide participating stakeholders with increased efficiency through the elimination of manual processes and by automating the interchange of data between systems. The increased efficiencies will, in turn, shorten cycle times for trusted LER activities (e.g., hiring, college admission, and verification of certifications).

The cost savings of these efforts will be measurable in actual manual labor, the cost of quality (dealing with errors and non-conforming data and data loss), the cost of fraud, and the opportunity cost of time spent/saved in fulfilling the stakeholder needs (e.g., the value gained in shortening hiring cycles).

The current draft IEEE LER ecosystem framework provides a high-level set of requirements:



IEEE Global LER Standard Recommended Practices

The five (5) recommended standards are:

1. Shared Services: Trust and credential meta registries that enable a network of networks:
   a. Trust Meta Registries
      i. Identity (legal, digital)
      ii. Trusted issuers
   b. Credential Meta Registries
      i. Skill / course crosswalks
      ii. Revocation services

2. Learning and Experience Ledger: Registered services that enable instructor / evaluators to assert that a learner has achieved a skill or credential as machine interpretable data by unknown future systems.

3. Credential Publisher: Services to enable achievement assertions to be wrapped in credentials that are cryptographically, or otherwise, signed onto distributed ledgers. Or other technologies used for verification from requesters in the talent marketplace.

4. Digital Wallet: An app that enables learners and their adult guardians to subscribe, curate, and control access to achievement assertions and other credentials and create a presentation shared with verifying parties.

5. Talent Marketplace: Services that enable credential requestor systems to automate actions, validate, and view credentials and other assertions.

REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

An LER infrastructure also needs to provide for the exchange of LERs with traditional systems while providing mechanisms to remedy the gaps in these systems. Likewise, this infrastructure needs to address the integration and interoperability of current systems such that newer systems can co-exist, exchange credentials, maintain their integrity, trust, and provenance, and support multiple applications.

This section defines LER infrastructure and the requirements necessary for scaling to a national level. It draws upon the experiences of those involved in leading four of the most advanced LER ecosystem projects in the United States. While these projects are still in nascent stages, they are demonstrating—not as a pilot but rather "in production"—LER infrastructure that meets the identified needs.

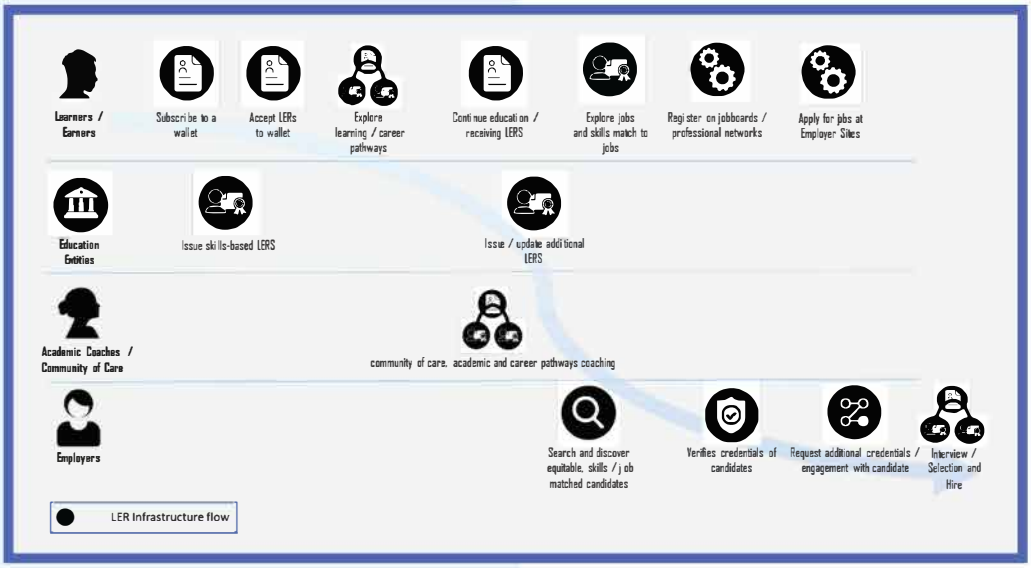
NATIONAL LER INFRASTRUCTURE AND THE LER ECOSYSTEM

LER infrastructure is part of a larger ecosystem that uses LERs for various needs. The LER ecosystem includes many stakeholders: learners/earners, educational and other credential providers, employers, military, government, certification and licensure agencies, and communities of care. These stakeholders are any who will rely on LER infrastructure and its supporting LER system providers for various job marketplace, education marketplace, employer HRMIS, and other needs. LER technology and services providers include credential management (issue, update, maintain, revoke) systems, wallet providers, holder subscription systems, learning and career pathways solutions, and LER systems operator services.

The LER ecosystem supports key LER stakeholders' use of LER shared services based on trust in the governance frameworks. The LER infrastructure flow best illustrates the ecosystems as it portrays the journey from learner to earner.

The following is an example learner-to-earner journey in the LER Ecosystem encompassing key stakeholders and their actions. The circles represent parts of the LER Ecosystem that would utilize LER Infrastructure.

Example Learner to Earner Journey in the LER Ecosystem



The complexity of these relationships is difficult to capture in a single, two-dimensional visual. Appendix B includes a conceptual technical and governance model that supports how digital trust must work in an LER ecosystem.

REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

A national LER infrastructure will allow LER technology and service providers to make available solutions that directly serve the LER ecosystem stakeholders with LER-specific applications and provide integration and automation among the LER ecosystem technology and service providers' offerings. Providing efficient solutions for LER ecosystem participants and providers requires a shared, standardized and interoperable LER infrastructure. (Appendix B provides the requirements for the infrastructure.) Establishing a national LER infrastructure is critical for "frictionless" integration and execution within this larger ecosystem.

An LER ecosystem will provide deep insight into an individual's actual cradle-to-career journey traversing both their education and jobs. These data sets are combinable with other information about the individual, e.g., tax and unemployment records, and will inform deep analysis and understanding of education and career outcomes. As these insights are gained, they can be used to create definitions of quality aligned with specific outcomes for employment, retention, mobility, wage gains, and more.

THE ROLE OF SKILLS IN A NATIONAL LER INFRASTRUCTURE AND LER ECOSYSTEM

A critical piece of a national interoperable LER infrastructure and its surrounding ecosystem is the support for skills-based LERs. The increasing diversity of existing job classifications and the acceleration in creating novel job categories conflict with traditional education programs and offerings. For example, in the mid-twentieth century, there were relatively few jobs for computer programmers and very few institutions offering training in the limited number of skills required to be a programmer. Today, most institutions provide programming and software engineering training and training for the hundreds of specializations in the programming field (e.g., machine learning, front-end development, gaming). However, it is not enough to have a degree: a person needs employment-ready specialized skills.

Employers are increasingly focusing on skills-based hiring for candidates based on competencies (knowledge, skills, and abilities) needed to perform for successful job execution. This demand is, in turn, pushing education institutions to provide skills-based mappings for their existing courses and degree credentials and offer many specialized, skills-focused training programs needed by business and industry.

To address this focus on skills, a national LER infrastructure supports the ability to represent trusted LERs in the form of skills achieved. This requires technology to support schemas, such as CTDL, (Credential Transparency Description Language), which map credentials to skills. It also requires the adoption and expansion of government, academic, or industry-endorsed skills frameworks, such as the US Cybersecurity Infrastructure and Security Agency's National Initiative for Cybersecurity Education (NICE) Workforce Framework, a government and industry-sanctioned skills framework used for training at over 200 education institutions.

SKILLS AND COMPETENCY FRAMEWORKS

Skills frameworks are critical to supporting skills-based LERs. However, 'skills' is often used ambiguously across the learning and

Where skills frameworks are defined and accepted as standard (e.g., NICE) and available in human and machine-readable linked open data schemas (e.g., CTDL in the Credential Registry), stakeholders can readily use them to create structured data alignments in curriculum, credentials, job definitions, and learning pathways. Unfortunately, many disciplines and job categories do not have well-defined skills frameworks. However, numerous efforts exist to expand the number of accepted skills frameworks. As an example, the Open Skills Network (OSN) is looking into how skills metadata can be further refined and put into context with the goal of publishing standardized Rich Skills Descriptors (RSD). Developed collaboratively by employers and academics, RSDs are expected to bring more alignment between talent providers and those who seek talent.

The current gaps around a common vernacular of skills, understanding competencies, and competency frameworks are challenging. However, they also present an opportunity to work collaboratively toward alignment. The work of organizations such as OSN and the Competency-Based Education Network (C-BEN) is promising. They have created a necessary conversation between talent developers and employers around the appropriate vernacular through their work. Learners, employers, and education providers will be the long-term beneficiaries of aligning skills to learning outcomes and competency frameworks and may even serve as the impetus to develop more competency frameworks around job roles or occupational sectors.

REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

Six key attributes of skills frameworks are needed for LER systems and the national LER infrastructure:

1. Published in machine and human-readable form as linked open data supporting connections to credentials, jobs, and pathways.
2. Containing unique IDs to enable alignment to skills.
3. Open reference document. Skill statements must be openly accessible without cost or access constraints.
4. Sufficient detail to align curriculum, assessment, and job requirements.
5. Supports defining skill levels and learning sequences. Where appropriate, express proficiency or experience levels or required mastery of prerequisite skills.
6. Contributed/endorsed by key stakeholders (educators, employers, learners). A process-based endorsement by key stakeholders to merit use.

CAREER AND EDUCATION PATHWAYS

A pathway is a sequence or progression of achievements consisting of structured sets of objectives, qualifying conditions, and milestones along a route to the fulfillment of a credential, job, occupation, or career. Pathway components may include competencies attained (knowledge, skills, abilities), relevant credentials, courses, assessments, jobs, experience, and other related achievements.

Pathway components may include competencies attained (knowledge, skills, abilities), relevant credentials, courses, assessments, jobs, experience, and other related achievements. Pathways require some number of component achievements, which themselves may have pathways that must be completed.

Higher education institutions, industry bodies, government agencies, and employers vary in their approaches to defining pathways, making it challenging to determine the skills required for any one path. This makes it difficult for all stakeholders who want to define and match a person's skills to the opportunities they choose to pursue along a given pathway.

But as with skills, when pathways are defined and contextualized with data available in human- and machine-readable linked open data schemas (e.g., CTDL for pathways in the Credential Registry), stakeholders can create structured data alignments to curriculum, credentials, job definitions, etc. from multiple sources.

Pathways enabled with structured LER data can provide numerous opportunities, for example:

- Education and career planning and transitions
  - Support learners searching and planning for career pathways, including pathway options through stackable and latticed credentials and career clusters.
- Credential and course discovery
  - Finding credentials and courses that best meet a person's career and/or education goals along career and education pathways that provide the following:
    - Best transfer value for credentials they have already earned
    - Potential to stack and build on other credentials
- Skill Analysis
  - Identifying learning and career pathways in terms of the skills that they require
  - Representing current achievement of desired skills based on the learner's LERs
  - Discovering relevant credentials for each skill on a pathway from multiple providers

SKILLS AND CREDENTIAL TRANPARENCY

For effective LERs, we need to ensure that credential and skill data speak a common language. There are too many ways to describe similar credentials, skills, and jobs—making it nearly impossible to compare and connect them. We can promote skill and credential transparency by utilizing a common language, or schema, to describe a person's achievements. The expression of learning in terms of skills, regardless of whether that learning occurs in an academic setting or on the job, promotes transparency and leads to increased access to pathways and opportunities throughout an individual's learning lifecycle. This transparency needs to be based on machine and human-readable data such as the CTDL.

REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

THE ROLE OF TECHNOLOGY AND DATA STANDARDS

Establishing clear and concise standards helps reduce the time spent translating data and aligning with technology requirements that enables interoperability within the LER ecosystem. Technology standards optimize the adoption of an LER infrastructure and make it less expensive to operate. Data standards make it easier to create, share, and integrate data by ensuring the data used in the LERs are represented, understood, and interpreted correctly within the LER ecosystem.

INFRASTRUCTURE TECHNOLOGY STANDARDS

A national LER infrastructure would give individuals personal agency over the verified and detailed record of their skills and achievements. Doing so will transparently communicate individuals' skills to current and prospective employers and educational institutions while preserving an individual's right to control how that data is shared and their right to privacy. Infrastructure technology standards support this through verifiable credentials tied to a decentralized digital identity with identity-proofing attributes embedded into its structure. These technology standards provide a privacy-enabling way to prove control over an identifier associated with authentication methods, signing keys, and other secure means of interacting with an individual's digital data.

INFRASTRUCTURE DATA STANDARDS

Infrastructure data standards provide the common structure that allows the LER to be machine-readable and actionable to other LER systems through a consistent mechanism for categorizing and describing individual data. To efficiently share, exchange, and understand data, both the format and the meaning of the data must be standardized. Data standards are a way to format data for interoperability and are the rules by which data are described and recorded. Data standards make it easier to publish, transfer, and understand data. Moreover, unlike proprietary standards, open standards ensure that no single vendor or organization controls the longevity of the application and that the data is easily used or converted.

Data standards exist across industries and are used to define a wide variety of data types. As related to talent management, credentialing, and workforce development, various data standards define numerous types of information that may be important. Generally, these are oriented to data related to education, credentialing, human resources, and learner records. Open-source standards developed by widely known and established organizations that use stakeholder input and a consensus approach are likely to be widely adopted.

It is important to note that any government use of data standards must be undertaken with the consideration of privacy and security risks, particularly as it relates to military data. Even non-classified data can pose security concerns when aggregated. Moreover, exposing military and other data improves accessibility and openness but can make it vulnerable to misuse or misinterpretation. Therefore, when considering infrastructure data standards, technology standards that bolster privacy and security must be simultaneously implemented.

THE NEED FOR LER SYSTEM STANDARDS

The technology that uses and maintains LER information must give learners agency over and access to their records, allow records to be verifiable and assure compliance with data and security regulations. "The LER infrastructure is interoperable by design and should accommodate a diverse set of platforms and applications that employers, institutions, and learners can use to record, view, share, and analyze data" (Learning and Employment Records Progress and the path forward, American Workforce Policy Advisory Board, 2020, page 9). Adopting or creating ecosystem standards, like a common language describing skills, ensures LER data can be communicated between decentralized entities. Utilizing an LER system standard to represent achievements also helps legitimize them, as it provides all the information needed to understand and verify achievements included in the LER ecosystem.

REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

LEGAL AND REGULATORY REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

As LER systems evolve, we must be aware of the applicable legal and regulatory requirements. The legal landscape is likely to be dynamic for years to come as the transition to digital credentials evolves, adoption increases, and people and organizations interact with each other through these digital credentials. In this report, we look at the long-standing laws and regulations governing the world of physical academic credentials and the newly emerging laws and regulations for the digital world.

In the "Digital Credentials Legal and Regulatory Requirements," Appendix C, the main issues reviewed are:

- The role of blockchain in the emerging LER environment.
- Core legal and regulatory pillars required for an LER-compliant infrastructure.
- The design of the LER ecosystem that comports with privacy law best practices for digital credentials anchored in digital self-sovereignty.

Before delving into the key legal and regulatory pillars, we begin by defining some key concepts in the field: (1) LER digital credentials assert that a person demonstrated a level of competency with the referenced skills; (2) digital self-sovereignty, a set of principles enabling individual autonomous control over personally-identifying information like verified skills-based achievements and employment; and (3) blockchain (in this document, also referred to as a distributed ledger), a secure distributed data repository shared among the computer network nodes, storing information electronically in digital format.

THE ROLE OF BLOCKCHAIN IN THE EMERGING LER ENVIRONMENT

Given the current maturity of the LER infrastructure in the United States and globally, there is a preference for blockchain technologies to serve as a core component of the LER infrastructure. However, the data structure of a blockchain includes an irreversible timeline of data stored in a decentralized environment. As skills-based credentials are referenced from the blockchain, those with the proper privileges can see information created about those skills and records over time, and impossible to erase those transactions. Because of blockchain's immutable nature, it is challenging to fulfill data protection rights and raises challenging privacy law questions.

On the other hand, the trend toward permissioned blockchains is powerful at enabling the blockchain to comply with the emerging LER legal and regulatory environment. A permissioned blockchain is only accessible to users who have permission to perform actions granted to them by the blockchain's administrators. A permissioned blockchain supports managed and auditable compliance with privacy rules.

CORE LEGAL AND REGULATORY PILLARS REQUIRED FOR AN LER-COMPLIANT INFRASTRUCTURE

LERs and the transition from physical to digital credentials are emerging and maturing areas of technology. As with all emerging and evolving technologies, new services and solutions are being invented and tested to provide new and innovative approaches to solving business and service challenges. These business and service challenges range from:

- improved efficiency through automation, e.g., replacing paper transcripts with digital ones,
- more effective ways of providing legacy services, e.g., transitioning career services from human interaction to highly personalized career pathways driven by artificial intelligence and anchored on trusted credential data,
- changing the description of required/desired skills for jobs from legacy assumptions about what is needed to succeed in a position to informed job descriptions based upon deep machine learning insights into what combination of skills are required for job success.

These innovations and transitions raise essential questions around data privacy, trade secrets, appropriate and ethical use of data, data ownership issues, intellectual property, and informed consents, amongst others. The legal and regulatory environments surrounding these changes and challenges are a continuously evolving landscape with no end in sight. This section reflects key developments in this evolving area to provide a general overview of the major trends and thinking in the legal and regulatory domain.

REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

The European Union's General Data Protection Regulation (GDPR) is one of the strictest privacy and security regulations, imposing obligations on worldwide organizations collecting data related to EU citizens. In this legal environment, an LER infrastructure faces challenges meeting expectations around data erasure, rectifying data errors, and compliance with regulations on international data transfer. Emerging best practices for implementing a GDPR-compliant infrastructure include identifying the different roles played by the various actors in the LER ecosystem. The roles require identifying the responsibilities of the data controller versus the data processor, documenting appropriate privacy roles and responsibilities, securing informed consent for uses of the data, storing personal data off the blockchain, and using encryption methods to secure the data.

The California Consumer Privacy Act (CCPA) is a consumer privacy law like the GDPR. However, there are some critical differences between the two laws and how they apply to digital credentials. Notably, California takes a broader view of what constitutes private information. This is important because of liability: if the data controller shares private information with the data processor, it is not considered a sale under CCPA, making the data processor not directly liable. However, the CCPA still holds the data processor liable if the processor shares private data outside a contract's terms. The CCPA allows individuals to sue companies for violating privacy guidelines, even if there is no breach.

The Family Educational Rights and Policy Act (FERPA) will guide any LER implementation that uses data from educational agencies receiving federal education funding. FERPA requires schools to obtain informed consent before disclosing students' records. Before records can be released from a federally funded academic institution, a person must provide informed consent before the LER can facilitate the data sharing of academic records. However, once the data is released to the student, it is no longer protected by FERPA, and the student can do with it what they wish.

The Fair Credit Reporting Act (FCRA) also broadly applies to LERs. Since the FCRA appears to govern a more permissible set of data use, LERs will need to focus on gaining permission from individuals to use the data for purposes of education admissions, college transfers, and employment. The transfer of this type of information falls under the FCRA's definition of consumer information–and thus, is protected and regulated under the FCRA.

THE DESIGN OF AN LER ECOSYSTEM THAT COMPORTS WITH DIGITAL CREDENTIAL AND SELF-SOVEREIGNTY PRIVACY LAW BEST PRACTICES

Assuring the LER infrastructure complies with applicable laws and regulations requires looking at which laws apply to the different members of the LER ecosystem. There are different requirements at each level of the ecosystem, and separate agreements must address the rights and obligations of each party contracting for the use of the LER to assure compliant solutions.

For the primary users of the ecosystem, there are unique requirements each must address through agreements and informed consent. The requestor's focus is on needing a representation stating the credentials will only be requested when there is a permissible purpose. For the issuer, they must ensure the credentials issued are accurate to the best of the issuer's knowledge and are obligated to resolve disputes relating to the accuracy of the credential. And for the wallet provider, they must state in the agreement a means to resolve disputes concerning credentials with the wallet holders.

Ensuring informed consent is a significant requirement for an LER infrastructure, and the LER wallet must enable specific actions for compliance with the FCRA. Users need to know what their participation will involve, what rights they have, and what permissions they grant to the data processor and data controller. This report explores how the legal and regulatory requirements apply to the construction of an LER wallet infrastructure and digital credentials.

All ecosystem members must also agree to avoid discriminatory hiring practices (including fully automated practices that adversely impact an individual's legal rights) under applicable laws.

The emerging LER ecosystem in the United States and globally operates in the context of existing data privacy laws and is informed by the historical legacy of physical credentials and personally identifiable information. All members of the LER ecosystem will need to be aware of the relevant legal and regulatory frameworks and will need to "engineer in" the tools to assure compliance.

NATIONAL LER INFRASTRUCTURE RECOMMENDATIONS

Drawing from the expertise of people engaged in multiple LER-related practices, initiatives, and projects, we put forth the following recommendations to grow a national LER infrastructure.

RECOMMENDATION 1 – TECHNICAL STANDARDS

Continue to mature LER-related standards to support our evolving job roles and hiring practices.

There are currently mature standards that support LERs and are integral to the LER infrastructure.

Data Standards that concern the structure of the data for electronically maintained LERs:

- CTDL – a common language standard for human- and machine-readable linked open data describing credentials, skills, jobs, pathways, and related information (for inclusion of meaningful data in all types of digital credential packages)
- MS CASE v1.0 – the Competencies and Academic Standards Exchange (CASE) is the standard that enables the exchange of information about learning outcomes, competencies, and skills in an open, machine-readable format.
- IMS CLR Standard v1.0 – a Comprehensive Learner Record (CLR) common standard for the content of collections of LERs
- IMS Open Badges v. 2.1 – a common standard for individual LERs
- PESC - a common standard for LER content

Security Related Technical Standards which concern the security of LERs in systems and in transit:

- W3C Verifiable Credentials – A globally established standard that provides "a standard way to express credentials on the Web in a cryptographically secure, privacy-respecting, and machine-verifiable manner." (Note that W3C VCs use a broad definition of "credentials," including, for example, identity credentials and employment records.)
- W3C DID – The global specification for working with "decentralized identifiers," which support a trusted means for securely identifying entities (e.g., individuals or documents) without requiring a central repository.

In addition, many emerging standards are already demonstrating value for an LER infrastructure. Some of these standards are either in process or draft form or are evolving from earlier versions of established standards. These standards include:

Emerging / Evolving Data Standards which concern the structure of the data for electronically maintained LERs

- IMS Open Badges v3.0
- IMS CLR Standard v2.0
- W3C VC-ED - focused on education and training use cases for W3C VCs

Emerging / Evolving Security Related Technical Standards

- Trust over IP (ToIP) interoperable decentralized digital trust infrastructure

RECOMMENDATION 2 – SHARED SERVICES

Create a technical infrastructure that provides shared identity/trust and skill/credential services for all LER ecosystem stakeholders.

The deployment and scale of a national LER infrastructure depend, in part, on the development of standards-based, open shared services that can be made available to any appropriate LER technology vendor. These services may include but are not limited to identity management, trusted LER transactions (issuing, updating, sharing, viewing, revoking), verification of LERs, presentation of LERs, and any registration processes and registries and repositories supporting such services. The creation and availability of these open shared services and any related registries will discourage the creation of proprietary services and interfaces that limit interoperability. These pre-existing shared services also provide for more rapid development of LER infrastructure compliant solutions.

The LER infrastructure and associated data sets will serve as rich sources of information for a range of private and public education and talent technology applications in providing personalized services for people navigating their cradle-to-career journey. Examples include career pathways explorations, guidance to aligned apprenticeships, social services that assist the workers/learners in being successful, etc. These data sets can be made available to related HR, job boards, social services, etc., applications through the LER's open and interoperable standards, which both enable and govern the use and exchange of these data sets. In all instances, informed consent by the user will be required for any data exchange to occur and a governance model that assures proper stewardship of the data provided by the LER ecosystem.

NATIONAL LER INFRASTRUCTURE RECOMMENDATIONS

RECOMMENDATION 3 – TALENT MARKETPLACE

Integrate Talent Marketplace provider offerings with the LER infrastructure.

To achieve this, the following actions are recommended:

- Early adopter employers will collaborate with their HRMIS – Applicant Tracking systems providers to create and demonstrate interoperable LER infrastructure integrations in production
- Early adopter job posting/candidate matching sites and professional and social networking sites will adopt LER technology as a means to provide LER trust and verification for holder LERs.
- Early adopter job posting/candidate matching sites, professional and social networking sites will collaborate with employers to create and demonstrate LER infrastructure interoperability in exchanging LERs between these systems and HRMIS – Applicant Tracking Systems in production.

Early adopter employers should include governments at the Federal and State levels, large private sector employers, and the military.

As a result of this integration, all stakeholders will benefit by participating in a trusted, efficient talent marketplace. Employers will use HRMIS and Applicant Tracking Systems that utilize automated, secure, and trusted exchange of LERs. Employer job descriptions, skills, and titles will either match or align to well-defined LER-related career frameworks, and they will be able to search for candidates based on skills (not just degrees or job titles). Candidates, recruiters, and job sites will have the ability to share verifiable LERs through the LER infrastructure.

RECOMMENDATION 4 – LER REGIONAL / SECTORAL INFRASTRUCTURE

Invest in regional/sectoral projects, reference implementations, and develop a supporting LER Issuer Maturity Model.

Current deployments of LER infrastructure have focused on developing “regional” or “sectoral” approaches—state-based or spanning multiple states but bound by a particular stakeholder group. As the report has noted, these approaches may vary widely in their use of technologies, including architecture and data formats. (Paragraph continued in next section.)

But to realize a skills-based ecosystem that allows us to thrive as a society, we must prioritize our future investments (of private, public, state, or federal resources) to advancing those projects which are engaging all the following:

- Organizations developing pathways to success for in-demand skills expressed using portable digital credentials aligned to open skill definitions driven by local/regional market demand.
- Organizations working on LER infrastructure investments provide equitable access to earners and learners.
- Employers using skills-based digital credentials for talent acquisition and talent management.

Designing a national LER infrastructure requires leveraging regional and national experts to work with community stakeholders to adopt preferred technology solutions that can interoperate within a well-defined national LER system.

The next steps toward building a national LER infrastructure are to invest in developing and advancing multiple LER regional projects. These projects should represent a cross-section of the country. They should be deployed in a diverse set of states where legislation or state support is either in place or underway, promoting skills-based education and workforce integration. This integration should include K-12 and the state’s higher education departments as well as the state’s labor and workforce development agencies.

The projects selected for funding should have a cohort of ecosystem partners already engaged in designing or deploying one or more of the “utilities” of LERs, including skills-driven hiring, skills-based learning, career pathways, digital wallets, and credential networks. These projects should represent different maturity levels so that an LER Issuer Maturity Model can be developed as a by-product of this work. The effort should prioritize scaling a few projects that can demonstrate the desired outcomes of what LERs can achieve within 24-36 months of funding.

Selected regional projects should be defined by the technical recommendations of this document; however, they should allow for different technical approaches. These technical differences will prevent the emergence of a one-size-fits-all or one-company-to-rule-them-all approach. Instead, the focus should be on an interoperability strategy around the point of communication and collaboration within and between regional projects. In fact, we recommend the projects selected for funding are composed of a diversity of “best of breed” approaches and strategies to the overall deployment of a credential ecosystem.

NATIONAL LER INFRASTRUCTURE RECOMMENDATIONS

RECOMMENDATION 5 – LEGAL & REGULATORY REQUIREMENTS

Develop and document standard legal and regulatory terms of use, user agreements, and requirements for data sharing and trust.

Primary amongst the compliance requirements will be the need to assure both informed consent on the part of the users, functional solutions that allow for remediation in the event of errors in the data, and strong data privacy protections. Any LER infrastructure-compliant solution will need to determine how it will engineer these requirements into the user experience and associated enabling technologies. (See Appendix C for additional detail on legal and regulatory issues.)

RECOMMENDATION 6 – LER INFRASTRUCTURE COMPLIANCE CERTIFICATION

Create an organization that can certify LER technologies and applications as "LER infrastructure compliant."

As this report has explained, the LER infrastructure requires certain technical, functional, and legal/regulatory capabilities amongst its participating members. Assuring compliance with these capabilities requires organizational capacity in the United States that provides guidance on whether proposed LER solutions conform. And if not, what changes are needed to come into compliance. In other comparable technical ecosystems, there are organizations that fulfill that role, such as standards bodies, labs, universities, government agencies, etc. We recommend an organization be identified to fulfill that role for the national LER infrastructure of the United States.

RECOMMENDATION 7– NATIONAL AND STATE LEADERSHIP

Promotion of a national LER infrastructure by national and state leadership

Our national and global employers, governing bodies, and other organizations must promote the architecture of a skills-based learning and work ecosystem. Federal and state governments' promotion of a national LER infrastructure will include encouraging or requiring education and training institutions to move toward the use of the LER infrastructure, allowing for LER data to be used for regulatory reporting requirements, adopting LERs for public sector hiring, and providing funding for LERs as a component of the workforce and economic development initiatives. Industry organizations can be effective in the same way by encouraging or requiring their industry stakeholders to support LER infrastructure. Companies can also lead by example, adopting the LER infrastructure and encouraging their partners to participate.

These recommendations will allow us to achieve the following goals:

- Enable and prove success with interoperable LER systems' application and technology providers.
- Expand the use of industry-endorsed, skills-based frameworks for LERs.
- Measure the efficacy and impact of LERs.

PROPOSED EFFORTS TO SCALE NATIONAL LER INFRASTRUCTURE

Next, we provide a more detailed outline of the criteria to guide the selection of a few regional or sectoral projects to fund (see Recommendation 6). These projects should be designed to demonstrate the ability to meet multiple goals in support of the recommendations, as well as demonstrate many of the functional and technical requirements identified in Appendix B. Additionally, a high-level timeline and budget are included.

CRITERIA FOR PROJECTS TO FUND

Guidance in this section focuses on supporting and scaling regional/sectoral projects that will demonstrate the interoperability required to advance regional LERs. These regional LERs will serve as the basis for the national LER infrastructure, where we can see the potential intersection, alignment, and/or phased adoption of these projects.

KEY ECOSYSTEM STAKEHOLDERS

When evaluating which regional/sectoral projects to fund, projects should have a plan for meaningful engagement of the core ecosystem partners representing learners, employers, and higher education.

The three core key ecosystem stakeholders are:

- Learner/Earner
- Employer
- Education and training providers

Other ecosystem stakeholders, some of whom fall into the above broader categories, that provide specific value are:

- K-12
- Other credential/educational providers
- LER systems application providers
- Workforce
- Military
- Industry organizations
- Workforce Development
- Government
- Certification and licensure bodies
- Communities of care/community service providers
- Technology and platform organizations
- Standards' bodies
- Policymakers

IMPLEMENTATION OF LER INFRASTRUCTURE COMPLIANT APPLICATIONS AND TECHNOLOGIES

Regional/sectoral projects should be designed to implement LER systems, applications, and technology providers, engage with employers of size and education entities, and implement interoperable systems at scale. The key system applications that the collection of funded projects should demonstrate interoperability among include the following:

- Assessment Systems
- Student information systems
- Learning management systems/ Professional Development systems
- HRMIS
- Applicant tracking system
- Licensure systems
- Job boards
- Identity Systems
- Accommodation Systems
- Social networks
- State unemployment
- Tax Records
- Content Management Systems/Education Catalog systems
- State longitudinal data system
- Related Government systems

IMPLEMENTATION OF LER INFRASTRUCTURE-COMPLIANT WALLETS

Key stakeholders endorse and adopt one or more LER infrastructure-compliant holder wallets, including no-cost holder wallets targeted at students and employees.

EDUCATIONAL CAMPAIGNS

Regional/sectoral projects will implement educational campaigns to engage the public, state agencies, government officials, employers, and learners in understanding the resources available to them with the LER deployment and the value propositions of those resources. The myColorado marketing efforts by the Office of the Governor are a great reference implementation of a public-facing education strategy. The resources these LER regional projects develop can become additional reference implementations for those who will follow in their footsteps.

PROPOSED EFFORTS TO SCALE NATIONAL LER INFRASTRUCTURE

LEARNER / EARNER ENGAGEMENT

The regional/sectoral projects selected should represent those who have taken novel approaches to digital credentials and have approached the work from the perspective of this report's recommendations. Projects that test novel approaches to engaging learners/earners in using digital wallets and sharing their digital credentials with educational institutions and employers will also positively add to the LER corpus. Convening the selected regional projects, the vendor community, and the underlying infrastructure providers will quickly encourage common approaches to this work with the intent of a scalable national architecture.

EVALUATION AND SUSTAINABILITY

Regional/sectoral projects selected should have an evaluation plan that considers the following:

- Key stakeholder engagement
- Interoperability of the various LER systems, applications, and technology providers
- Interoperability of regional/sectoral system with other sectoral/regional systems
- Adoption by individual record holders
- Consumption by employers
- The impact on hiring diverse learners for in-demand roles that lead to economic and career mobility.

PROGRAM MANAGEMENT METHODOLOGIES

The deployment of LER infrastructure projects will require expertise in complex program management and systems integration methodologies. These projects will be like any complex technology deployment that brings together data from multiple systems of record, involves numerous stakeholders, and reengineers existing business processes. There is ample experience demonstrating the value and investment required to manage these projects according to standard program and project management methodologies. The projects cited in this report all used these methodological approaches.

PROPOSED TIMELINE

Title of Effort	Initial (6-12 m)	Expansion (1-2 yr)	Goal (2-4 yr)
Planning	Assemble stakeholders Identify ecosystem bottlenecks Designate pilot scope Encode scope pathways	Bring in new stakeholders, broaden the accessibility, and integrate new technical components	Broadscale adoption across multiple industries and connections among regional LERs
Implementation of LER-compliant applications and technologies.	Regional projects are funded to demonstrate interoperability with key LER system applications and technologies.	Adoption, deployment, and user engagement with selected LER technology systems and applications. Development of standard requirements based on purchasing criteria	LER business models, state and federal policies and regulations, and LER infrastructure compliance certification rolled out for other regional/sectoral projects.
Digital Wallets	Adopted by a few key institutions and employers	Adopted by Federal and States, number of institutions and employers	In use by more than 15 % of US students and employees.
Skills Frameworks	Coalitions develop skills and competency frameworks. Frameworks integration with HRMIS by key employers. Use of skills and competency frameworks in LER infrastructure.	Federal occupation data aligned to frameworks. Mapping overlapping frameworks. Mapping curriculum to skills-based achievements. HRMIS providers application integration.	Framework standards for any industry. Federal and State legislated roadmap for state education institutions mapping curriculum to frameworks.
State Support	Convening, recommendations	Mandates, Gov. adoption	Legislated requirements

PROPOSED EFFORTS TO SCALE NATIONAL LER INFRASTRUCTURE

PROPOSED BUDGETS

LER pilot projects and deployments have been underway for more than two years. These deployments inform our recommendations about the required budgets for a successful production-grade deployment.

- Typically, projects will have a 3-year horizon. This time frame supports the creation and deployment of a baseline LER infrastructure and the development of the community of stakeholders that will be affected by and benefit from the LER infrastructure.
- Costs for this infrastructure dimension will vary by project, but the investment required is significant.
- Systems integration and program management expertise must be included as part of the deployment strategy. Costs for these types of services range from 15%-20% of the project costs.
- All projects should encourage the creation of an entrepreneurial ecosystem that can work with the LER ecosystem and create interesting and compelling new applications to support learners, earners, and employers.
- Early-stage deployments will typically require a public-private sector partnership. Since this is an emerging infrastructure area for our country, collaboration will be essential for LERs to gain traction at the local, regional, and national levels.

APPENDIX A
LER INFRASTRUCTURE CASE STUDIES

The four case studies described involved the five organizations responsible for this research grant project. These case studies were initially selected because each case study had participating members who were thought leaders and contributors to multiple LER ecosystem projects. In addition, these team members are actively engaged in projects representing the most mature-to-date LER infrastructure projects currently underway. Each case study describes the project, its goals, the ecosystem partners involved, key lessons learned, and the next steps required to support project maturity. These case studies also informed the requirements for; creating a national LER infrastructure, recommendations, and proposed efforts to scale the national LER infrastructure.

PROJECT: PROVIDE TEACHERS MORE CONTROL OVER THEIR LICENSES - RANDA

THE LIFELONG LEARNER

PROJECT (LLP)

OVERVIEW

Powered by Teachers is a group of stakeholders addressing the barriers to teacher license portability and implementing reciprocity strategies. The project's goal was to give teachers agency over their credentials and augment the teacher shortage problem nationwide in a meaningful way.

ABOUT THE PROJECT

The Lifelong Learner project recognizes the challenge teachers have accessing and leveraging their licenses and professional learning to maximize their impact on students. The first steps taken by the project were to identify stakeholders who agreed with the premise that empowering teachers through agency over their data was critical to the future of teaching. Throughout the pandemic, issues related to credentialing teachers were exacerbated and have led to a continuing exodus of teachers. The State of Utah, ETS, and Digital Promise recognized that we are at a critical juncture and have collaborated to develop a Teacher wallet bridging credential silos that can impact the speed with which a teacher can be licensed and ultimately placed in a classroom. The project has raised the visibility of the teaching profession as a critical consumer for LERs and, in doing so, has created multi-state momentum to solve for true license reciprocity between States and the empowerment of teachers with their licensure data.

PARTNERS

The State of Utah, Educational Testing Service (ETS), Digital Promise, RANDA Solutions, Evernym, IDRamp, University Instructors, Fluree, the University of Colorado at Colorado Springs, and Blockframe. These organizations invested time and effort in bringing this project forward as a winner of the American Council of Education's Blockchain innovation challenge. Since the project's inception, other stakeholder organizations and States have been added.

LESSONS LEARNED

LLP took an iterative approach to bring forward best-of-breed strategies and architectures to maximize ease of use, and infrastructure stability and bring stakeholders forward in this next generation of technology. Specifically, the project highlights the challenges experienced from a state perspective, both functionally and legislatively, how teachers perceive their credentials, and their value. The interoperable approach exposed many opportunities to improve systems and processes in the existing record systems while maximizing the value to all stakeholders. This project is critical for the future of teaching.

NEXT STEPS

The LLP continues to recruit partners amongst the community invested in teacher professional learning. The project needs regulatory support in the empowerment of teachers to maximize their abilities to teach across state lines. It has also introduced new concepts for the national architecture of the entire teacher licensure system of record to fully realize its opportunity to impact teachers and students in a meaningful way.

MILGEARS SUPPORTING SERVICE MEMBER TRANSITION TO CIVILIAN EDUCATION AND EMPLOYMENT

PROJECT: LEVERAGE TECHNOLOGY TO SUPPORT SERVICE MEMBER TRANSITION TO CIVILIAN EDUCATION AND EMPLOYMENT –SOLUTION FOR INFORMATION DESIGN

OVERVIEW:

The MilGears platform, developed by Solutions for Information Design, LLC (SOLID), documents learning wherever it occurs: in the workplace, through an education program/experience, and through military training and experience. MilGears then shows service members and veterans how their unique and comprehensive qualifications, obtained through military and civilian education, employment, and experience, match the skills needed for career pathways. The results displayed show the user both academic and non-academic education and training opportunities to address existing skills gaps that must be filled to attain their desired occupation.

Beyond career pathway exploration, service members and veterans can manually upload their military service records (e.g., JST, ETJ, etc.). MilGears will parse the relevant data from these records to build a personalized Military Learning and Employment Record (MLER). The MilGears MLER provides service members with a comprehensive digital record of their military-based training, education, and experience. Users can also add self-attested military training and experience since not all military-based learning is captured on a user's service record.

Navy MilGears is live and available to the public; an expansion of MilGears functionality for all Services is underway.

PARTNERS:

MilGears was developed in partnership with the Department of Defense, Force Education & Training (DOD, FE&T), and all five Military Departments. The team actively participates in a variety of forums that focus on LER efforts, including skills, data standards, verified credentials, and digital identity.

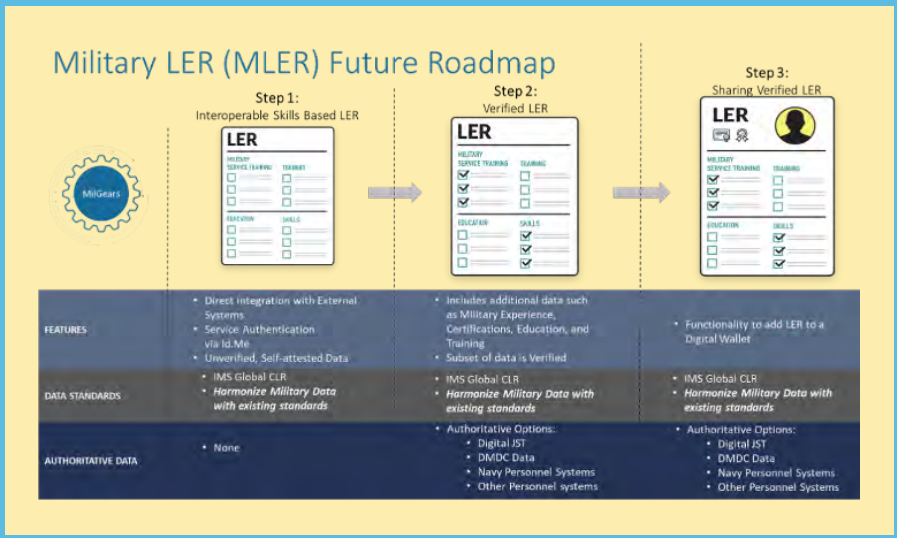
LESSONS LEARNED:

- DOD and other government agency issuing systems must be capable of exporting verified data to external systems.
- DOD and other government agency systems must implement data standards to facilitate machine readability. It may be necessary to further describe existing data standards for military-specific data elements.
- To access and connect to DOD and receive personnel information, the MLER must be in an "Authority to Operate" (ATO) environment, exist in a FedRAMP environment and have certain cybersecurity precautions to protect PII.
- Receiver systems must be capable of systematically consuming military-specific LER data.
- Each Military Department operates independently of the other. To create a singular MLER, the harmonization of varying personnel systems and data tracking methods is required.

ABOUT THE PROJECT:

The MilGears MLER produces a record that articulates an individual's complete service history, including duty stations, in-service training, job roles, and other military-related experiences. Current functionality allows service members and veterans to upload their military service records, including the Electronic Training Jacket (ETJ), Joint Service Transcript (JST), and/or Verification of Military Experience and Training (VMET), to the MLER and self-attest to any military-specific additional experience, education, credentials, or training not included on the record. MilGears then displays a digital MLER for review and provides a downloadable PDF version along with an encrypted session file allowing them to access and edit the document later. No personally identifiable information (PII) is stored within the MilGears application or on its servers. The information is recoverable only through the encrypted session file provided to the individual user. This allows the individual complete control over who has access to their information and how it is shared. At this time, the user can share a PDF version of their MLER with credential providers, employers, career counselors, and others interested in understanding and recognizing military-based learning.

While the MLER includes only self-attested data, upon receipt of the Authority to Operate (ATO), the ability to connect directly to personnel systems will soon exist, allowing the MLER to obtain a user's verified service records. As improvements to the current MLER and overall MilGears functionality are made, we will explore potential interoperability with various government systems. The MLER will be portable, interoperable, transferable, and recognizable across military and non-military student information systems, employer HR systems, and military systems, enabling service members to share any portion of the MLER as they apply for jobs or educational opportunities.



NEXT STEPS:

The next steps for the MLER include interoperability with external systems that may benefit from consuming the data within the MLER and government systems and allow for verifying the user's information.

NORTH DAKOTA OPEN CREDENTIAL PUBLISHER CO-LAB

PROJECT: NORTH DAKOTA OPEN CREDENTIAL PUBLISHER CO-LAB (OCP) – PUBLIC CONSULTING GROUP, RANDA SOLUTIONS, EVERNYM, ID RAMP

OVERVIEW:

The North Dakota Co-lab is a collaborative laboratory convened by the State of North Dakota IT Department with a community of vendors and state stakeholders. The co-lab was initiated to develop a proof-of-concept open-source platform that provides North Dakota students control over their eTranscripts. This new platform is independent of the State's infrastructure and leverages blockchain technologies to implement a Trust Over IP (ToIP) compliant system.

PARTNERS:

North Dakota published a competitive RFP to source expertise in blockchain technology. The partners selected through the competitive process include but are not limited to Public Consulting Group, RANDA Solutions, Evernym, and IDRamp. These four partners were the primary contributors to the open-source project and developed the system in the open through the IEEE SA Open platform under an Apache 2 license.

NEXT STEPS:

This project continues to push the boundaries of the data standards prevalent in the education community. It has integrated not only the existing eTranscript from North Dakota, CLR, and OpenBagdes but also Verifiable Credential, Verifiable Presentation, and SSI models across the spectrum. The system, developed as a visible technology platform, does not cater to a simple UX. Now that the technology is in place, user experience development is required to meet the next generation of learners in support of their digital native lifestyle.

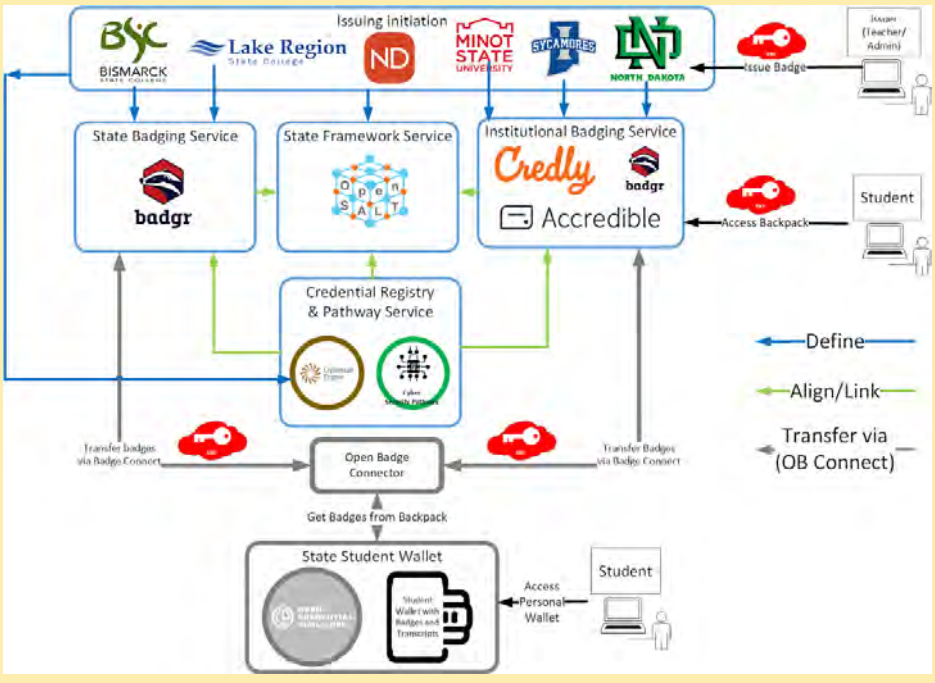
ABOUT THE PROJECT:

The project took an iterative approach to develop a scope of deliverables. These deliverables were explored in bi-weekly meetings with community members who desired to contribute to the open-source project. The Co-lab developed documentation representing an open-source approach with two primary services, an Achievement service aligning the achievements represented in the State's SLDS which already produced an eTranscript into a machine-readable IMS Global CLR 1.1 certified JSON object. The achievement service then signs the JSON object and each assertion within the CLR as a Verifiable Credential (VC). Further, the VCs produced can be published to a Trust Over IP compliant blockchain-based wallet. This project demonstrated the ability of multiple open-source standards and bodies to interoperate and bridge the technical gaps between what had, up to the point of this project, existed in their silos. The solution represents what many communities are striving to produce, an interoperable LER. This project also demonstrated and catalyzed forward motion in each of these standards bodies by using the iterative approach and pivoting with the continually developing standards and architectures throughout its lifespan.

LESSONS LEARNED:

The OCP developed new approaches to integrating multiple standards while honoring their core use cases. In doing so, the education and VC communities have overlapped in many ways. A multi-assertion VC had not been published in a production environment until this point. Further, many existing systems were challenged with production-level data and iterated alongside the development of this project. Primary learnings include the limitations of single-assertion architectures in multi-assertion environments and represent genuine user interactions with these standards. These standards must be bridged through interoperable use cases such that the workflows and user experiences can be flushed out in the K-12 environment. Systems of record are and will continue to be integral parts of the community of development and are empowered to move this market forward, unlike any POC not directly integrating the current system of record architecture.

CREATING INTEROPERABLE BADGES THAT ENABLE COLLEGE TRANSFER CREDIT



Indiana Achievement Wallet

PROJECT: HELP LEARNERS UNDERSTAND HOW THEIR SKILLS CONNECT WITH CAREERS

OVERVIEW

The Indiana Achievement Wallet (IAW) is a collaborative development effort of organizations based upon the Cyber-pilot concept demonstration provided to the American Workforce Advisory Board (AWPAB) by IBM, the National Student Clearinghouse (NSC), iQ4, and Western Governors University (WGU) in fall 2019. The project incorporates a wallet application, compassing application, and blockchain infrastructure that delivers a working LER and learner Achievement Wallet supporting self-sovereign control of personal data. By utilizing open data standards and skills or competency-aligned digital credentials, job roles can be surfaced that reveal to learner-earners how their skills compare to geo-located job roles, identify skills gaps, and identify other educational opportunities that can provide missing skills. Employers will be able to search for talent that matches their employment needs and can trust the verified credentials possessed by learner-workers. Learner-earners will be supported by a community of care that helps learners onboard into the Achievement Wallet, utilize the wallet to maximize the development of their unique talent brand, and facilitate smooth transitions across education providers.

PARTNERS

The Indiana Achievement Wallet collaborative consists of WGU Indiana, Ivy Tech Community Colleges, Goodwill Excel Centers of Indianapolis, the National Student Clearinghouse, IBM, iQ4, and Skillful Indiana. Phase I of the Indiana Achievement Wallet was made possible through a generous grant from the Lilly Foundation. Phase II of the project is made possible through a generous grant by Walmart. As the project continues and evolves, other talent developers will be engaged to participate, as will their learner-earner populations. Employers will be actively approached to evaluate the value proposition of the LER Achievement Wallet as a solution to help them address their talent needs. Early efforts to expand the partner base have included a co-branding/badging agreement between Goodwill Excel Centers and Vincennes University and two healthcare provider employers.

ABOUT THE PROJECT

The Indiana Achievement Wallet leveraged technology developed by IBM, NSC, and iQ4 for the AWPAB Cyber-pilot demonstration. The IAW initially focused on the healthcare sector with two high-demand job roles - medical assisting and pharmacy technician. These job roles were identified through the congruence of credentials offered by the Goodwill Excel Centers of Indianapolis and Ivy Tech. The credentials can lead to jobs in medical assisting and pharmacy tech. The project also leveraged the abilities of the Goodwill Excel Centers high school diploma to stack into certificates and associate degrees issued by Ivy Tech.

Learners struggle to identify how their learning relates to occupational goals and to represent how they are qualified for jobs at a given skill level. Credentials lack transparency for both learners and employers. In addition, learners do not own their “records” and must request transcripts, certificates, and diplomas (sometimes cost-prohibitive) from their institution(s) as they enter or re-enter the workforce and attempt to assert their qualifications via a resume. The IAW project provides ownership to learners of their achievements and credentials via the Wallet and gives them the control to decide how their records are searched and shared. Credentials and achievements are expressed digitally and provide clear descriptions and alignments. Learners will see their achievements in the context of how they align to jobs, any skills gaps they may have, and where they may seek additional education to address those skills gaps.

Through an iterative approach the partners seek to demonstrate how education and other talent providers can participate in a growing LER Achievement Wallet ecosystem through various points of engagement, utilizing existing technology and practices, or by endeavoring to define credentials in new ways. For example, WGU and Goodwill Excel Centers worked collaboratively to define and align their credentials represented in the open badges data standard at a ‘Rich Skills Descriptor’ (RSD) level, with higher-order alignments to O*NET job codes. In contrast, Ivy Tech credentials are already defined in CTDL within the Credential Engine repository and are aligned to competency frameworks. Work is underway to bridge degree verification data filed by Ivy Tech with the NSC and the CTDL definitions within the Credential Engine repository so Ivy Tech credentials can be surfaced within the IAW and surface job roles using competency framework alignments. IMS Global has been engaged to investigate how credentials defined within Competencies, and Academic Standards Exchange (CASE) may also be leveraged. Lastly, WGU is working with the NSC to explore how digital diplomas may be used by institutions not yet participating in data standards.

Recognizing that learner-earners may face real barriers to accessing education, jobs, and technology, the partners are working with Skillful Indiana to provide a community of care approach that supports learner-earners. Minimally, the community of care onboards wallet holders to the technology and supports transfers and transitions between education providers. The larger vision of the community of care is to develop standards of practice engagement by community-based organizations that can assist learner-earners facing food or housing insecurity, transportation needs, and day and elder care needs.

Employers are struggling to locate, recruit and retain the talent they need for their businesses. Employers are signaling that the degree is no longer a satisfactory proxy for what an individual can do and are seeking new ways to identify better talent fits. Through aligning credentials to skills and competencies, the partners aim to provide and deliver a more efficient way for employers to locate needed talent, minimize recruitment costs, and streamline the employment of talent requiring minimal job training. Presently, the partners are putting in place the needed technology requirements to deliver verified credentials (VC) to employer participants that can be trusted and verified.

Indiana Achievement Wallet

LESSONS LEARNED

The partners recognized that many credential providers are not yet positioned to represent learner outcomes, achievements, and credentials in open data standards and that institutions must be provided a low threshold point of entry to participate in the LER ecosystem. Therefore, the partners are investigating how institutions and other credential providers may begin issuing into the LER ecosystem by utilizing current practices (such as publications in Credential Engine or CASE repositories, digital transcripts, diplomas, etc.). This may also include using proxy issuers such as the National Student Clearinghouse.

In addition to FERPA and GDPR compliance, the partners identified that the use of the LER technology subjects the issuers, technology providers, and employers to consumer protection requirements under the Fair Credit Reporting Act (FCRA). The partners are now engineering solutions to ensure compliance with FCRA.

Through learner focus groups and feedback, the partners recognized the need for the inclusion of a community of care component in the LER ecosystem to socialize the concept of the LER Achievement Wallet, onboard and coach learners on the use of the technology (IAW) and support the smooth transfer and transitions between education providers. More ambitiously, the partners recognize the need to develop and address how a broader community of care should be utilized to address and ease barriers to access to education, jobs, and technology.

Lastly, the partners learned that such an ambitious, national project as the LER ecosystem is best solved through robust, expanding partnerships across many organizations and stakeholders.

NEXT STEPS:

As the Indiana Achievement Wallet progresses into Phase II and beyond, additional credentials and alignments to healthcare jobs will be added. The user base will increase as students from Goodwill Excel Centers, Ivy Tech, and WGU are added to the IAW. The partners plan to expand beyond healthcare careers into other industry sectors and add related program offerings from new institutions and talent providers. As the IAW grows, the LER ecosystem will continue developing, establishing, and implementing open infrastructure standards that ensure long-term sustainability, compliance (regulatory and best-practice), and portability of learner-earner achievements independent of any blockchain and/or wallet provider. The partners will continue to partner with the Open Skills Network (OSN) and work towards direct integration with open skills libraries and the Open Skills Management Tool (OSMT), thus providing more skills (RSD) alignments for credential providers. Employers will be invited to participate and use the IAW as a talent sourcing solution. Additional data standards will be incorporated into the architecture, such as CTDL/CTDL-ASN, PESC XML, EDI, and CLR. Future data standards such as HR open and JDX will be investigated. Through employer engagements, API integration with existing ATS and HRIMS will be explored.

APPENDIX B: REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

This section describes the essential functional and technical requirements to engage in an LER deployment project. The key stakeholders who should read this section are education, state, and corporate. Federal and certification board administrators, CIOs, education provider registrars, enrollment managers, employer HR managers, and HRMIS administrators. The requirements detailed in this section provide information to accomplish a successful determination, engagement, and deployment of an LER infrastructure implementation.

The section also provides information on technology, services, registries, and standards to support interoperability between various LER-related solutions and implementations.

LER ECOSYSTEM, INFRASTRUCTURE, AND APPLICATIONS

The LER Ecosystem brings together participants, technologies, and standards to enable trusted interactions and secure data exchange for LER-related activities, either directly using LER Infrastructure or through interoperable applications.

The LER Infrastructure supports common, shared open standards and provides shared services and registries (data repositories) available to applications that directly support LER-related activities.

Key applications that directly support LER activities include Issuing: Management applications, Credential Management Platforms, Wallets for Individual LER Holders, Requestor / Verifier Applications, and Learning Pathway Applications.

An **LER ISSUER APPLICATION** allows organizations that assert LERs for Holders (e.g., an education institution asserting a degree award to a student) to issue and update the LER that already exists in their native systems to a shared LER credential management system. Issuer Applications also typically provide the capability for marking an LER as “revoked” (e.g., when certification has lapsed).

An **LER CREDENTIAL MANAGEMENT PLATFORM** is typically a blockchain-based, Software as a Service (SaaS) set of functions that can receive, maintain, update, share, and transmit LERs that support and comply with the shared, open LER-related data and legal standards. The Credential Management Platform may not have any stakeholder user interfaces (though it will typically include a platform administrator interface). The platform will often be architected as a permission-only system where only permissioned participants will have specific rights for use based on their role and identity.

- Issuers will typically have the rights to issue, update, and revoke LERs in the system through an Issuer application that uses platform services
- Holders will have the right to accept and manage their own LERs in a wallet or equivalent application, using system services provided through the wallet that uses platform services.
- Requestors/Verifiers will have the ability to search and request permission to view or receive LER presentations based on Holder’s provisioned permissions using an application or integrations with existing applications (e.g., HRMIS) that integrate with and use platform services.

An LER Credential Management Platform may also include the ability to support mappings between LERS and related skills, either directly or through shared or developed skills frameworks. The ability of an LER Credential Management Platform to show support relationships between skills and LER achievements is considered important for today’s skills-based job economy. This may also occur in other related applications that use these features.

APPENDIX B: REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

An LER Reviewer / Verifier Application typically provides the LER Reviewer / Verifier with the ability to search for LER Holders based on a variety of Holder attributes (e.g., skills, degrees, certifications, geography, and other information) and uses the facilities of the LER Credential Management Platform or supporting LER Infrastructure capabilities to retrieve matching Holders who have given some form of permissions for their information to be shared. The Holder controls the permissions for their information.

Requestor / Verifier functions may be provided in a stand-alone Reviewer / Verifier application, or they may be incorporated in talent acquisition, HRMIS, or Applicant Tracking System application (or other applications), using the common, shared open standards and shared services and registries (data repositories) available to applications.

An **LER WALLET** is an application that allows the Holder to accept and maintain their LERs from Issuers through the LER Credential Management Platform (or its services). The Wallet will also allow the Holder to include Holder information (e.g., name, address, other non-LER related claims, and assertions) in the Wallet. The Wallet should provide the Holder a means to determine who will be allowed to see their information, at what level of detail, and for how long. A Holder will typically subscribe to a Wallet made available through a Wallet Provider, who maintains the application for all their subscribers and is responsible for Wallet compliance and security. The Wallet provides interoperable, secure, and trusted methods to share credentials and identity with other applications and entities.

An **LER PATHWAYS APPLICATION** is an application that provides a means for Holders (and as warranted or delegated, education providers, academic and other counselors and coaches, and perhaps others) a means to represent sequences of activities and achievements that lead to other LER achievements, jobs, career advancement, and other opportunities. A robust LER Pathways Application will not only provide learning sequences (which may be simple linear sequences or complex multi-option pathways) the LER Pathways Application will also:

- Provide a means to show skills and competencies achieved along the pathways
- Provide the learner (or, as warranted, others) with the ability to perform tradeoff analysis (e.g., regarding learning locations, costs, time to achievement, and other factors) between learning pathways offered within the same and among multiple institutions and programs.
- Provide the learner with a gap analysis concerning their current LERs and projected pathway goals.
- Potentially provide market and job information concerning the viability of pathways.
- Provide a means for others supporting the learner to coach and counsel the learner concerning pathways

To support these tasks, the LER Pathways tools must be capable of accepting and maintaining (including updating) applicable pathway components for course and program description/skills data from education institutions, industry skills framework information, job descriptions, and with the permission of the learner, holder information concerning current LER achievements/skills and future goals. This last capability will require explicit agreement with the Learner / Holder of LERs and legal compliance to support their rights and privacy.

Some or all of these functions may also be found in multiple other applications, such as Learning Management Systems (LMS), Student Management Systems, and other applications that may use the common shared open standards and shared services and registries and data repositories to support these functions.

Depending on the solution, the functionality described in these applications may be combined or fragmented across systems supporting LERs. For example, an HRMIS system may incorporate Reviewer / Verifier application functionality directly into its system. Similarly, a Student Information System (SIS) may incorporate credential Issuer application functionality directly into its system. Also, note that the applications described above will include administrative services to onboard and manage their users and privileges and monitor use and security.

APPENDIX B: REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

LER ECOSYSTEM, INFRASTRUCTURE, AND APPLICATIONS

The recommendations for the LER standards, shared services, and registries and data repositories underlying those application functions are outlined below. These services must comply with associated privacy and rights protections and standards applicable to stakeholders in the LER job economy (see Security and Privacy standards listed below).

For the purposes of this section:

- An achievement is an accomplishment by an individual that can be documented as an LER
- A Credential is a formalized achievement that provides a shared, accepted definition of an accomplishment. These are typically badges, courses, certifications, degrees, or other similar achievements. Credentials are distinguished from other achievements that have not (yet) been "credentialed," for example, four years of Java programming or self-assertion of skills that have not been independently verified and promoted to the status of a credential.

An Achievements Assertion Tool utilizes information concerning achievements from traditional systems of record as the basis to create digital credentials placed in a credential management platform. The Achievement Assertion Service supports standards that provide detailed information concerning the credential and the issuer. This information is defined in standards such as Open Badges and the more recent and in-depth IMS CLR standards. The credentials, as asserted achievements, must be capable of being used to inform a variety of search, skills-based description, and learning pathways functions.

Credential Publishing Services are the process of securely providing the issued credential from the platform to an individual or entity that has appropriate rights and privileges to receive the credential. The most typical example is the publication of a credential to an individual's wallet. In this case, the individual has the right to accept the credential to their self-sovereign wallet and manage the credential in their wallet. Depending on the request, privileges, and rights, the credential may be published to an HRMIS, or another system. For such systems to consume these credentials, they must support the standards for LERs (see below) and preserve the rights and privileges described in the applicable standards.

A Universal Requestor/Validator Service provides the capability to request credentials from the platform or platforms where those credentials reside. Though its purpose is straightforward, the service must be capable of performing requests and validations for all LER Infrastructure compliant platforms. A Validator / Requestor Service that only supports one platform is not considered interoperable and, therefore, not compliant.

A Shared Met Data / Registry Service aims to facilitate any required "crosswalks" to define credentials, identity, and skills. Credential Engine's Credential Registry provides CTDL-linked open data describing credentials, competencies and skills, pathways, jobs, and federal frameworks (such as NICE and O*Net). There are also skill/competency registries such as IMS CASE and the Open Skills Network (OSN). Registries need to support human- and machine-readable data that can be exchanged throughout the LER infrastructure. s.

APPENDIX B: REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

FUNCTIONAL REQUIREMENTS

Any interoperable LER system that fully supports the business needs encompassed in national interoperable LER infrastructure and its role in the larger business ecosystem would include the functionality described in the table below. This table includes both the "actors" using the functionality and the typical application using the functionality.

Providing these functions will assure that an LER system is interoperable, not only with other LER systems and LER infrastructure components but also with the larger ecosystem in which it resides.

HIGH-LEVEL FUNCTIONAL REQUIREMENTS FOR AN INTEROPERABLE LER SYSTEM

Req ID	Stakeholder Use / Application Functionality	Issuer Actor	Holder Actor	Requestor/ Verifier Actor	Issuer Application Functionality	Wallet Functionality	Credential Management Platform Functionality	Requestor / Verifier App. Functionality	Learning Pathways Functionality
	FUNCTIONALTY								
ALL 1	Maintain Compliance with privacy and confidentiality requirements				*	*	*	*	*
ALL 2	APIs and services to embed functionality into other applications					*	*	*	*
Issuer 1	Issue, update, expire, revoke LERs as credentials to a credential management platform	Primary			*		*		
Issuer 2	Use an Issuer User Interface	Primary			*				
Issuer 3	Use an Issuer Batch Interface	Primary			*				
Process 1	Support a process to promote achievement assertions to the status of credentials	Primary(1)	Primary(1)	Primary(1)		Optional			
Platform 1	Create equivalence between LER based credentials (usually called "articulations" in education)	Primary					*		
Platform 2	View equivalence between LER based credentials (usually called "articulations" in education)	Viewer	Viewer		*	*	*	Optional	
Platform 3	Provide a means for credentials to be available in multiple wallets		Primary				*		
Requestor 1	Verify a credential in the credential management platform	Viewer		Primary	*		*	*	*
Requestor 2	View the status of an LER based credential (preferably in real time)	Viewer	Viewer	Primary	*	*	*	*	*
Requestor 3	View the provenance of an LER based credential	Viewer	Viewer	Primary	*	*	*	*	*
Requestor 4	View the composition of an LER based credential	Viewer	Viewer	Primary	*	*	*	*	*
Requestor 5	View any skills associated with an LER based credential	Viewer	Viewer	Primary	*	*	*	*	
Requestor 6	View any skills-frameworks mapped to skills that are part of an LER based credential	Viewer	Viewer	Primary	*	*	*	*	
Requestor 7	Use a Requestor / Verifier User Interface			Primary	Optional			*	
Requestor 8	Support a variety of search parameters (.e.g. including skills, various credentials, frameworks, etc)			Primary	Optional		*	*	
Requestor 9	Perform search using a variety of parameters (.e.g. including skills, various credentials, frameworks, etc)							*	
Wallet 1	Provide Holders with self-sovereignty in managing their wallets		Primary			*			
Wallet 2	Provide Holders with self-sovereignty in accepting credentials in their wallets		Primary			*	*		
Wallet 3	Provide Holders with self-sovereignty in sharing their credentials		Primary			*	*		
Wallet 4	Provide Holders with discrete control over how they share credentials, how long, and to what detail.		Primary			*	*		
Wallet 5	Maintain Holder permissions		Primary			*	*		
Wallet 6	Manage engagement of requestors with holders		Primary	Viewer		*	*	*	
Wallet 7	Use a Holder User Interface (the Wallet)		Primary			*			

(1) This process is currently considered outside the LER technical infrastructure. Once self-assertion has been promoted to become a credential, it can be issued in the system by the appropriate issuer. As the market matures, a well-defined, shared process for promoting assertions to the status of credentials may be supported by additional technology and applications.

APPENDIX B: REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

LER INFRASTRUCTURE STANDARDS, SERVICES, REGISTRIES, AND INTERFACES

LER infrastructure will include a set of documented, shared standards, services, interfaces, and data registries and repositories that fundamentally define the technology services. The infrastructure depends crucially on a shared LER infrastructure that supports a set of documented, shared standards, services, interfaces, and data registries and repositories that fundamentally define the core infrastructure. Therefore, LER infrastructure core features must include but are not limited to:

- Compliance with applicable Standards
- Compliant use of a well-defined set of shared services, including services for:
  - o Credential Management
  - o Permissions Management
  - o Identity / Access Management
  - o Policy Enforcement
- Compliant use of a well-defined set of data repositories and registries supporting data about
  - o LERs
  - o Individuals

TECHNICAL REQUIREMENTS FOR INTEROPERABILITY OF AN LER INFRASTRUCTURE

The LER infrastructure is interoperable by design. To maintain the core functions of an interoperable LER infrastructure, the common data standards and general requirements provide a guide to utilize and continue to build shared services that support its evolution.

GENERAL REQUIREMENT - STANDARDS

Insofar as they are applicable to the subject area, the following standards are pre-requisite requirements necessary for any technology or services that will be compliant with national LER infrastructure. As described in Recommendation 1, insofar as it is applicable, any supporting technology or service should be in alignment with the following standards:

Common Data Standards
- PESC - a common standard for LER content (less preferable than the following two)
- IMS Open Badges v. 2.0 – a common standard for individual LERs
- IMS CLR v2.0 – a common standard for the content of collections of LERs

Security Related Technical Standards
- W3 Verifiable Credentials – An established standard that provides "a standard way to express credentials on the Web that is cryptographically secure, privacy-respecting, and machine-verifiable."
- W3 DID – The specification for working with "decentralized identifiers," which support a trusted means for securely identifying entities (e.g., individuals or documents) without requiring a central repository.

Privacy and Rights Standards

Concerning the governance of individual and organizations' rights and privacy protections concerning LERs:
- FERPA
- GDPR
- CPRA (California Privacy Rights Act)
- FCRA (Fair Credit Reporting Act)

Note that compliance with these standards is required to support the national LER infrastructure. Depending on the functionality and the actual implementation, one or more of the requirements of these standards may be pre-requisite for any given application or work process.

APPENDIX B: REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

GENERAL REQUIREMENTS - SERVICES

Any technology or services compliant with the national LER infrastructure should use the defined, shared set of national LER infrastructure services to support interoperability, transaction, and data services. This does not preclude the use of other services or technology, except when those other services or technology are used instead of equivalent defined, shared LER infrastructure services, as this will limit interoperability and integration and may compromise security or privacy.

GENERAL REQUIREMENTS - REGISTRIES / REPOSITIORIES

Any technology or services compliant with the national LER infrastructure should use the defined, shared set of National LER Registries / Repositories to support data management for LER infrastructure-related actions. This does not preclude the use of other data repositories, except when those other repositories are used instead of equivalent LER infrastructure services, as this will limit interoperability and integration and may compromise security or privacy.

SPECIFIC REQUIREMENTS FOR STANDARDS

The following table depicts key requirements for a fully functional regional/sectoral implementation. Such an implementation will include an LER infrastructure provider, one or more LER technology and service providers that support key LER functions and LER ecosystem systems that integrate with LER infrastructure technology and services.
The table below provides insight into the core pillars of a regional/sectoral LER implementation. These pillars include who the stakeholders are, what applications they should get, and how compliance can be attained.

Using the table below, a technical manager (e.g., a state CIO) can determine how to assess or create a regional / sectoral implementation, determining which proposed components are compliant with the National LER Infrastructure.

* - expected for compliance if supporting this type of functionality + - watch for future adoption as part of the LER Infrastructure, when published ^ - use to be encouraged to assure interoperability			
CATEGORY	**LER Infrastructure**	**LER Technology and Services**	**LER Ecosystem systems**
Standards			
IMS CLR v2.0	*	*	^
IMS Open Badges v3.0	*	*	^
IEEE ILR	+	+	+
Services			
Achievement Assertion	*	*	*
Credential Publishing	*	*	*
Wallet Subscription	*	*	*
Wallet Curation	*	*	*
Credential Presentation	*	*	*
Credential Validation	*	*	*
Registries / Repositories			
Skills Crosswalk	*	*	*
Trust	*	*	*
Accreditation	*	*	*
Resources	*	*	*
Distributed Ledger	*	*	*
Credential Management	*	*	*
Revocation	*	*	*

NOTE: Since the functionality required of an LER system may be fulfilled by various applications (e.g., either by providing requestor/verifier functionality in its application or by extending an HRMIS application to support this functionality), vendors may choose to extend their functionality and, at a minimum will need to either natively or through interfaces that must be developed, support data exchange standards and legal standards for LER systems.

APPENDIX B: REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

RECOMMENDATIONS CONCERNING ADOPTION AND ON-BOARDING

The adoption and use of an LER infrastructure will include the following management decisions, roughly in the order shown:

Note: These efforts need to include training (whether online or direct) and support for the stakeholders involved.

Inventory, assessment, and determination of potential providers (e.g., Issuer, Reviewer, Wallet, and Platform providers). This may include decisions to integrate some of this functionality with legacy systems (e.g., a decision to incorporate Reviewer/Verifier functionality directly into a legacy HRMIS system rather than purchasing a separate Reviewer/Verifier application).

Scheduling and staffing any required integration efforts.

Scheduling the adoption and rollout of the production system. For the broadest set of stakeholders, this may include:

1. Approval and agreement with permissioned Issuers (e.g., colleges and other trusted education providers, certification boards that issue credentials, and potentially including corporate training departments) to allow them to issue holder credentials to the system.
2. Determination of any skills-based frameworks supporting the credentials and agreement with issuers to support (either immediately or long term) the enriched skills-based information to be included in issued credentials.
   Approval and agreement with a wallet provider (unless the organization creates its own compliant wallet) who supports the privacy and sovereignty rights described in the standards.
3. Schedule for the deployment of wallets to holders (including learners in various institutions, employees at various companies, members of industry organizations, citizens of a state or geography, and others).
4. Approval and agreement for the use of the system by Reviewers / Verifiers (typically employer HR staff, college registrar staff, certification board reviewers, and others who will search for or verify candidate credentials.
   In addition, the following effort, is also likely, short or long term, approval and agreement with one or more compliant learning pathways tools providers who support the privacy and sovereignty rights described in the standards.

APPENDIX B: REQUIREMENTS FOR A NATIONAL LER INFRASTRUCTURE

SCHEDULING RECOMMENDATIONS

The successful deployment will be best achieved by the broad adoption of Holders and Requestor / Verifiers, but only for trusted issuers. Otherwise, the trust in the credentials is undermined.

Likewise, successful engagement will be best achieved by having many Wallet Holders with credentials in their wallets that interest the targeted employers. Therefore, it is recommended that once agreements are in place the priorities should be to:

1. Get Issuers on board and issuing (preferably skills-based) credentials to the platform (preferably in certified IMS CLR Standard or IMS Open Badges format) is a critical success factor and the first task.
2. Get Holders on board with Wallets is a critical success factor, but only after the Issuers have started issuing credentials to the platform. Providing Holders with Wallets and no credentials to populate the Wallets is likely to create Holder dissatisfaction and deter use.
3. Get Requestors/Verifiers to use the infrastructure assumes #1 and #2. Once credentials are in the system and Holders who have populated wallets, employers (and other requestor/verifiers) will quickly find the infrastructure that provides the most efficient and trusted means to do their job.

This approach may also be initially targeted to a specific industry, geographic area, or population segment with a strong interest in education, community, and industry. Starting with a well-defined target can shorten deployment cycles and better assess engagement.

As the targeted segment(s) begin to engage successfully, deployment can be expanded to additional segments until the deployment reaches the entire forecasted population of stakeholders.

FINAL NOTE ON NON-STANDARD ASSERTIONS OF SKILLS OR ACHIEVEMENTS

The National LER infrastructure supports the LER ecosystem of trusted, skills-based credentials. However, a vast amount of LER data is not “credentialized,” residing in the form of data such as tenure in a job, number of years of performing activities, individual learning, and other data. To best support the LER ecosystem, there needs to be a way to capture this data and process to facilitate the promotion of these LERs to the status of credentials when warranted.

It is expected that wallets will provide a means to capture this data as non-trusted information (similar to demographic information and individual comments about “interests” found in resumes), but there is still a need to be able to present this information to prospective Requestor / Verifiers with the proviso that the information is not of the status of a verified credential. This is expected to occur as collateral engagement between the Holder and Requestor / Verifiers, who initially engage through the Platform and applications.

As the national LER infrastructure evolves, it is expected that processes will be established for assessing non-standard assertions and, where viable, promoting them to the status of credentials vouched by permissioned Issuers. Efforts are underway by numerous organizations to help evolve this process.

THIS APPENDIX EXPLORES THE CORE LEGAL AND REGULATORY PILLARS REQUIRED FOR AN LER-COMPLIANT INFRASTRUCTURE. THIS INFRASTRUCTURE IS DESIGNED TO SUPPORT THE ISSUANCE, EXCHANGE, VERIFICATION, AND HOLDING OF SKILLS-BASED CREDENTIALS. BEFORE DELVING INTO THE LEGAL AND REGULATORY PILLARS, IT IS IMPORTANT TO DEFINE SOME KEY CONCEPTS.

APPENDIX C

LEGAL AND REGULATORY CONSIDERATIONS

KEY CONCEPTS

HOW IS AN LER DIGITAL CREDENTIAL DEFINED?

As skills-based digital credentials are used more frequently, the LER infrastructure moves us towards the digital badge serving as the certifying evidence that a person has taken the appropriate development courses to demonstrate mastery of the referenced set of skills. This “certification” is provided by a trusted source such as a higher education institution or private company. Conceptually, a digital credential consists of two primary components from the physical world: a document (like a degree issued to a student with their name and credential description) and a sealed envelope into which that document is placed (ensuring the “credential,” e.g., a transcript cannot be altered in a manner that assures its authenticity). The envelope also communicates information about the credentialing institution and allows its contents to be verified to detect fraud or tampering. The transition from the original physical form of the credentials to the digital world is cryptographically managed and provides a higher level of trust and transparency to all parts of the digital credentials ecosystem.

WHAT IS DIGITAL SELF-SOVEREIGNTY?

Self-sovereign digital identity is a set of principles enabling individual control over personally-identifying information like verified skills-based achievements and employment. Self-sovereign digital identity is important for holders in the LER ecosystem because it enables increased transparency and control of digital credentials. It also empowers credential holders to make their own “self-sovereign” decisions about what organizations can do with the credentials they have elected to share. This principle is important as it minimizes the risk of unwanted data sharing and unapproved use of the data by putting in the hands of the credential holder the ability to make critical decisions regarding the Holder’s credentials. An LER infrastructure, architected with the principles of self-sovereign digital identity, places the individual at the center of the credentialing process as the key manager of their credentials. As such, it better aligns with the primary data privacy legal and regulatory frameworks that will govern LER skills-based records.

WHAT IS BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGY?

Given the current maturity of the LER infrastructure in the United States and globally, there is currently a preference for distributed ledger technologies, like blockchain, to serve as a core component of that infrastructure.

A blockchain is a distributed database shared among the nodes of a computer network. Blockchain is also referred to as a distributed ledger. As a database, a blockchain stores information electronically in digital format. One key difference between a typical database and a blockchain is how the data is structured. A blockchain collects information together in groups, known as blocks, that hold sets of information. For LERs, digital credentials may be stored as these types of blocks. Blocks have certain storage capacities and, when filled, are closed and linked to the previously filled block, forming a chain of data known as the blockchain. All new information that follows the freshly added block is compiled into a newly formed block that will be added to the chain once filled. This data structure inherently makes an irreversible timeline of data when implemented in a decentralized nature. When a block is filled, it is set in stone and becomes a part of this timeline. Each block in the chain is given an exact timestamp when added to the chain. As skills-based credentials are placed onto the blockchain, it will be possible to see all information about those skills and the record of all changes made to those skills over time. It will also be impossible to erase those transactions.

Due to its immutable nature, the permanence of information recorded on the blockchain makes it difficult to fulfill all data protection rights. It also raises interesting yet unresolved questions on a range of data privacy laws. However, blockchain compatibility with data protection laws can only be assessed through case-by-case analysis, considering the governance and specific technical aspects of the relevant blockchain use case. In some instances, privacy challenges arising from blockchain-based technologies can be overcome.

THE PILLARS OF THE LEGAL AND REGULATORY REQUIREMENTS DERIVE FROM BOTH LONG-STANDING AGREEMENTS THAT HAVE GOVERNED PHYSICAL CREDENTIALS AND NEWLY EMERGING AREAS THAT ARE RELEVANT TO THE DIGITAL WORLD. IT IS IMPORTANT TO NOTE THAT THE TRANSITION FROM PHYSICAL TO DIGITAL CREDENTIALS IS A RELATIVELY NEW PHENOMENON. HENCE, LEGAL AND REGULATORY PILLARS ARE LIKELY TO BE DYNAMIC FOR YEARS TO COME.

APPENDIX C

LEGAL AND REGULATORY CONSIDERATIONS

LEGAL & REGULATORY ENVIRONMENT

HOW DOES GDPR AND SIMILAR DATA PROTECTION LAWS (DPL) LAW APPLY TO DIGITAL CREDENTIALS?

Put into effect on May 25, 2018, the European Union's (EU) General Data Protection Regulations (GDPR) are the strictest privacy and security regulations in the world, imposing obligations onto organizations anywhere that are targeting or collecting data related to people in the EU. Failure to comply with GDPR can mean harsh fines against anyone who violates its privacy and security standards, with penalties reaching into the tens of millions of euros.

Under the GDPR, data controllers (an organization that determines the purposes and means of processing personal data) must ensure they comply with GDPR before the fact, and they can demonstrate that accountability principles are in place to protect individual data. Primary amongst these accountability principles is the right to know who processes the data, how, and for what duration. And by extension, the right to demand the data be rectified, or the right to restrict data processing or to cease data processing altogether.

Some of the complex challenges a GDPR-type legal environment would create for an LER infrastructure using blockchain are:

- The use of a decentralized data structure like blockchain implies a distributed repository and management of stakeholder privileges that can complicate data and privilege management.
- Data erasure and rectification are granted as rights to data subjects by GDPR, and this contrasts with the impossibility of modifying or deleting data stored on a distributed ledger decentralized data structure, like a blockchain.
- International data transfer that requires mapping and additional safeguards versus distributed ledger technologies with nodes rapidly growing globally.

To address these challenges, best practices for a data controller include identifying who is acting as the data controller versus the data processor (an organization that processes personal data on behalf of the controller) based on factual assessment, clearly documenting privacy roles and responsibilities into applicable documents, storing personal data off the blockchain, and using encryption methods.

Another complexity is how the GDPR applies to a blockchain depends on whether it is a public or a permissioned blockchain. Public blockchains are characterized by the fact that anyone can access them on equal terms, making the information equally available to all parties. As the name implies, permissioned blockchains are only accessible to users with permission to perform certain actions granted to them by the blockchain's administrators. They allow for better control over data governance, including international transfer, and easier compliance with privacy rules.

In this early stage of maturity for an LER infrastructure, there are examples of both public and permissioned blockchains. The trend appears to be toward permissioned blockchains due to their superior abilities to manage the legal and regulatory environment for LERs.

THE PILLARS OF THE LEGAL AND REGULATORY REQUIREMENTS DERIVE FROM BOTH LONG-STANDING AGREEMENTS THAT HAVE GOVERNED PHYSICAL CREDENTIALS AND NEWLY EMERGING AREAS THAT ARE RELEVANT TO THE DIGITAL WORLD. IT IS IMPORTANT TO NOTE THAT THE TRANSITION FROM PHYSICAL TO DIGITAL CREDENTIALS IS A RELATIVELY NEW PHENOMENON. HENCE, LEGAL AND REGULATORY PILLARS ARE LIKELY TO BE DYNAMIC FOR YEARS TO COME.

APPENDIX C

LEGAL AND REGULATORY CONSIDERATIONS

LEGAL & REGULATORY ENVIRONMENT

HOW DOES THE CALIFORNIA CONSUMER PRIVACY ACT APPLY TO APPLY TO DIGITAL CREDENTIALS?

California passed AB 375 in 2018; the California Consumer Privacy Act (CCPA) is a consumer privacy law that could have similar repercussions on the United States as the GDPR has had in Europe. CCPA allows any California consumer to demand to see all the information a controller has stored on them, and a complete list of all the third parties data is shared. In addition, the CCPA allows consumers to sue companies if the privacy guidelines are violated, even if there is no breach.

A key difference between GDPR and CCPA is that CCPA takes a broader view of what constitutes private data. When a company acts as a data processor under the CCPA, it is subject to the CCPA indirectly, meaning it is subject to the CCPA through the data controller. Therefore, sharing personal information pursuant to the terms of an agreement with the data controller would not be considered a" “sale” under the CCPA. If a master agreement is entered into with the data controller that requires the company to share personal data with certain specific businesses (called “Providers” in this offering), such sharing would not be considered a “sale,” either.

However, a company cannot share personal data with others who are not specified in a master agreement nor use personal data for a purpose that is not specified in the master agreement.

When a company acts as a data controller and collects personal data directly from individuals who reside in California, disclosure of personal data (e.g., university degree, course information, etc.) to another business" ("data controller") would typically be considered a sale unless an exception applies. If there is a sale of personal data within the meaning of the CCPA, a company needs to give notice to these individuals before collecting their data and provide them with certain rights (e.g., the right to opt-out of the sale of personal data, right to delete information, and right to access information). Additionally, before a Provider would have the ability to retrieve information about a particular individual, the Issuing Organization would need to grant permission to the Provider to pull this information from their organization. If someone is sharing personal data for money or otherwise profiting using the LER infrastructure, and if the CCPA applies, this activity will be considered as selling personal data, based on the CCPA definition of selling.

APPENDIX C

LEGAL AND REGULATORY CONSIDERATIONS

HOW DOES THE FAMILY EDUCATIONAL RIGHTS AND POLICY ACT APPLY TO DIGITAL CREDENTIALS?

The Family Educational Rights and Privacy Act (FERPA) allows parents and eligible students to exercise control over their education records and consent to disclosures of their Personally Identifiable Information (PII). Student records are generally considered to be records that are “directly related” to an individual student and are “maintained by a school or post-secondary institution or a party acting on their behalf,” including data on students that may contain direct or indirect identifiers. FERPA requires schools to obtain consent before disclosing students’ records unless applicable exceptions apply. Any LER implementation that utilizes data from educational agencies that receive Federal education funding will bring FERPA into the mix. In these cases, student consent will be required to facilitate data sharing on the LER. However, once this data is released to the student, FERPA no longer protects the data because it is in the hands of the student, who is free to leverage and share the data as they see fit.

HOW DOES THE FAIR CREDIT REPORTING ACT (FCRA) APPLY TO DIGITAL CREDENTIALS?

The Fair Credit Reporting Act defines a “consumer reporting agency” as “any person who, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing a consumer report.”

Any company that meets the legal definition of “consumer reporting agency” is a CRA under the law. Issuing a disclaimer to the contrary is not an effective method of evading this status. As the use cases for LERs have matured, it appears FCRA will broadly apply to LERs since one of their intended purposes is to allow people to provide personally identifiable information about themselves with the purpose of finding a job. The concept of “other information on consumers for the purpose of furnishing consumer reports to third parties” appears to also apply to this type of transaction.

Although FCRA conceives more permissible purposes, LERs should focus on providing the following options for Verifiers to select based on the currently known use cases: (1) Education admissions and transfer and (2) Employment.

However, an LER could provide a means for a Verifier to submit a request for an additional permissible purpose to be added, reviewed, approved, or implemented by the data controller.

HOW DOES THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 (FISMA) APPLY TO DIGITAL CREDENTIALS?

The Federal Information Security Modernization Act 2014 (FISMA) is a United States federal law passed to update all of the federal government’s cybersecurity practices for its cloud providers. It defines a legal information security framework for government agencies and contractors. FISMA requires agencies to implement an information security program that effectively manages risk. A FISMA Authority to Operate (ATO) applies to a single executive branch such as the DOD. In contrast, FedRAMP is a standardized security framework created for cloud products and services. With FedRAMP, you only need authorization for one Cloud Service Offering (CSO), and it will be recognized by all executive branch federal agencies.

The National Institute of Standards and Technology (NIST) is a non-regulatory agency that issued specific guidance (NIST 800-53 aka RMF) to meet FISMA ATO or FedRAMP Authorization requirements. The NIST 800-53 compliance will not guarantee FedRAMP authorization or a FISMA ATO, but it is an over-arching set of security recommendations and practices that will secure an organization’s data no matter which agency or customer is served.

When crafting an LER solution for military-connected individuals, additional considerations need to be addressed for the federal government (or DOD specifically) to act in the capacity of a Verifier or issuer. This includes the technical solutions required to maintain a Service member or veteran's personally identifiable information within an environment that meets DOD standards if interoperability with any DOD systems is to occur. This interoperability is necessary if the LER solution wants to provide verifiable information regarding their military training and experience versus self-attested data. In order to signal its readiness to interoperate with DOD systems directly, the solution must obtain an Authority to Operate (ATO) for the DOD as an Impact Level 4 (ILE4) information system. The NIST Risk Management Framework (RMF) standards are used in an exhaustive, rigorous process that culminates in the security authorization and risk acceptance for an IT system to operate in the DOD environment.

HOW DOES THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 (FISMA) APPLY TO DIGITAL CREDENTIALS? (CON'T)

Documentation and evidence are collected from all phases (planning requirements, design, development, testing, implementation, and maintenance) of the Software Development Life Cycle and System Engineering Life Cycle. NIST's baseline set of security controls are implemented and then assessed to determine effectiveness prior to authorization. A monitoring program is implemented to determine if the set of planned and deployed controls are effective over time, given the inevitable changes that will occur.

After completing this process, a system hoping to issue a Military LER would be able to operate securely within the DoD to handle, process, and protect the confidentiality, integrity, and availability of Controlled Unclassified Information (CUI) such as PII data from service branch HR systems, a Joint Service Transcript, or a Military LER.

APPENDIX C

LEGAL AND REGULATORY CONSIDERATIONS

WHAT RIGHTS DO HOLDERS HAVE TO CONTROL THEIR SKILLS-BASED RECORDS?

Physical credentials have been in use for decades by education institutions and employers. As a result, well-developed legal and regulatory frameworks govern their use. This history provides a solid basis for managing the evolving digital credentials world. For those enrolled in learning institutions, regulations protect personal education records, and for those employed, regulations protect sharing of employment data. As an example, a student record often chronicles a person's academic life from kindergarten through graduation, and many schools keep student files for many years after the person has graduated or de-matriculated. According to the ACLU" "Student records can include quantitative information like test scores, intelligence quotients (IQs), and grades. They also can include more personal data like progress reports, psychological and psychiatric reports, and teacher evaluations."

For both types of data to be shared, the concept of informed consent is an essential legal and regulatory bedrock for the digital world. Informed consent means there must be an agreement between the issuer of the protected information, e.g., the academic institution or the business, and the Holder, e.g., the learner or employee. Once consent is granted, digital credentials can be moved between members of the LER ecosystem. This movement can include an academic institution sharing a transcript with a former student, who can then share that credential with an employer as proof of degree attainment. The LER infrastructure will use cryptographic means to; record that informed consent is obtained, provide business logic and an audit trail to manage consents and sharing and allow for dispute resolution to occur when there is an issue.

WHAT RIGHTS DO ISSUERS HAVE TO CONTROL SKILLS-BASED RECORDS?

The LER provider must take reasonable care in vetting the accuracy and reliability of permissioned credential issuers and provide transparency to users with respect to the identity of the credential issuers. If requested by the user, the LER operator likely needs to agree to provide (a) non-digital alternatives for credential verification and (b) clear notice and an option to opt-out of the recording or subsequent use of information related to a verification event.

In addition, informed consent on the part of the issuer, Holder, or receiver for purposes of using the credentials to apply for jobs requires the parties to agree to avoid any discriminatory hiring practices under Title VII of the Civil Rights Act of 1964, Title I and V of the Americans with Disabilities Act of 1990, Sections 501 and 505 of the Rehabilitation Act of 1973, Age Discrimination in Employment Act of 1967, Age Discrimination in Employment Act of 1967, and other applicable laws.

The issuer, holders, or receivers must also agree to avoid making fully automated decisions that adversely impact an individual's legal rights or otherwise creates or modifies a binding, enforceable obligation.

To meet FCRA requirements, the digital credential issuer must agree to only issue credentials for which they have authority, issue the credentials accurately, and maintain an accurate status of credentials issued. In addition, issuers must agree to resolve disputes about a credential under Section 611(a)(i)(A), which allows 30 days for investigation and response to a dispute.

WHAT RIGHTS DO VERIFIERS HAVE TO CONTROL SKILLS-BASED RECORDS?

Verifiers are organizations that request a digital credential from a Holder. With appropriate informed consent, a Holder of a credential can make that credential available to others as they seek employment, apply to school, etc. When a Verifier wishes to get more information from a holder, they need to provide a method for the Verifier to disclose that the request is for a permitted purpose. Permitted purposes would include proof of employment, that they had attained a degree, and a determination about them may be made, e.g., employment, school admission, etc., and that the Holder has agreed to the request. The Verifier will have an application that provides the method for a Verifier to view the Holder's positive or negative acknowledgment of the disclosure. The Verifier application will also provide a method for a Verifier to view the Holder's written authorization. In addition, the Verifier will maintain an audit trail of signatures, disclosures, and presentation activity. Finally, the Verifier asserts that the credentials will solely be utilized for the provided permissible purposes and will follow appropriate adverse actions regulations.

ASSURING THE LER INFRASTRUCTURE COMPLIES WITH THE LEGAL AND REGULATORY REQUIREMENTS

APPENDIX C

LEGAL AND REGULATORY CONSIDERATIONS

THE EMERGING LER INFRASTRUCTURE IS RESPONDING TO THE LEGAL AND REGULATORY REQUIREMENTS THROUGH VARIOUS TECHNOLOGICAL AND CONTRACTUAL MEANS. BOTH IMPACT THE DESIGN AND USE OF THE LER INFRASTRUCTURE BY THE ECOSYSTEM MEMBERS.

WHAT AGREEMENTS ARE REQUIRED BETWEEN MEMBERS OF THE LER ECOSYSTEM?

Separate agreements for requestors, issuers, and wallet providers that address the rights and obligations of the party agreeing to engage as stakeholders in the ecosystem will help assure a compliant solution. This is true even if some organizations will occupy multiple roles (e.g., a company may be both an issuer and a requestor or hold all three roles) and even if many of the provisions of the agreements that are not role-specific may be the same in all agreements. This approach is preferable to a single longer agreement with role-specific provisions, although this latter approach would also be acceptable if all relevant terms are included. The rights and obligations will be defined both by the legal and regulatory environment and the business model of the LER provider.

The requester agreement. This agreement will include a representation by requestors stating that credentials will only be requested when there is a permissible purpose. Next, the LER organization should determine that each requestor represents a legitimate organization entitled to do business for the permissible purpose before the digital credential distribution system organization signs the requester agreement. This further necessitates that a process is in place for the LER organization to vet requestors who sign up, as well as the individuals who will be granted access to the infrastructure (i.e., account holders) on behalf of each requestor organization.

In addition, the requester agreement must prohibit the requestor from using credentials (or other data) received through the LER for any purpose other than the permissible purpose for which the information was requested. Should the credentials be used for employment purposes, the agreement will require the requestor to comply with all laws associated with using credentials for employment purposes. This includes refraining from using credentials received in violation of applicable equal opportunity laws or regulations and complying with all legal requirements relating to adverse actions.

The issuer agreement. The issuer must declare that the credentials being issued are accurate to the best of their knowledge. A statement to this effect must be in the agreement signed by the issuer. The agreement must also establish that the issuer has authority to disclose all issued credentials, and it must obligate the issuer to resolve disputes asserted by a holder relating to the accuracy of the credentials in a timely manner.

The wallet provider agreement. The wallet provider must provide a means to resolve holder's disputes concerning their credentials. A statement to this effect must be in the provider's agreement. The wallet provider must also enable processes to authenticate and verify the Holder's identity before presenting credentials to the Holder in the wallet. In addition, the provider must maintain security for privacy of data in transit and at rest. The agreement and the technical requirements for the wallet application must address these needs.

HOW ARE THE LEGAL AND REGULATORY REQUIREMENTS APPLIED TO THE CONSTRUCTION OF AN LER INFRASTRUCTURE?

Since a blockchain LER infrastructure that includes digital wallets is a likely path forward, certain functional and legal agreement requirements are being technically engineered into the solution to assure all members using the LER ecosystem are legally and regulatorily compliant consistent with their differing roles.

SEARCH

The LER infrastructure will have search request capability, and these results will be transmitted as part of the system activity logs. The LER does not intend to keep the results of any digital credentials search or request, so the intent is if a permissioned organization wishes to retain search results, they will have to put the results on their local system and manage these records off the chain, with appropriate permissions provided. To determine how long the LER must retain that information, we need to understand what information is involved, specifically whether personal data is involved, and if so, which type of personal data.

PII STORAGE

If there are PII on the LER, this will require that personal data be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. There are some exceptions, as personal data may be stored for longer periods in instances in which the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

DIGITAL WALLETS

As Digital Wallets will be an integral part of an LER digital credential distribution system, Wallet providers and issuers will need to comply with certain FCRA-focused data privacy and compliance requirements before entering a contract with a digital credential issuer. A Wallet Provider must ensure that the wallet provides a method to confirm a credential holder's identity at onboarding or prior to credentials being issued to them so as not to violate privacy laws.

To meet FCRA data privacy requirements, a Wallet Provider must make the digital credential holder "clearly and conspicuously" aware in a stand-alone disclosure of two things: (1) their Verifiable Presentation of education credentials will be utilized for a potential employment determination, and a consumer report may be obtained and (2) their rights under the FCRA. The Wallet Provider must also provide a method for the learner to provide written authorization for any disclosures, and the Wallet Provider must make the signature available to the Verifier. Furthermore, the Wallet Provider must maintain an audit trail of signatures, disclosures, and presentation activity and provide a method for the Holder to raise a credential dispute with the credential issuer.

REFERENCES

American Workforce Policy Advisory Board. (2019). White paper on Interoperable learning records: Data transparency working group [White paper]. Data Transparency Working Group. https://www.commerce.gov/sites/default/files/2019-09/ILR_White_Paper_FINAL_EBOOK.pdf

American Workforce Policy Advisory Board. (2020, September). Learning and employment records: Progress and the path forward [White paper]. Digital Infrastructure Working Group. https://www.commerce.gov/sites/default/files/2020-09/LERwhitepaper09222020.pdf

Credential Engine. (2020). Making sense of credentials: A state roadmap and action guide for transparency. Washington, DC: Credential Engine. Retrieved April 18, 2022, from https://credentialengine.org/wp-content/uploads/2020/10/State-Roadmap-and-Action-Guide.pdf

Estrada, S. (2020, November 5). 'Skills are the currency of the future': The rise of a skills-based economy. HR Dive. Retrieved April 18, 2022, from https://www.hrdive.com/news/skills-currency-future-skills-based-economy/588475/

J Goodell. (2020, September 22). LER information & resources. U.S. Chamber of Commerce Foundation. Retrieved April 18, 2022, from https://www.uschamberfoundation.org/t3-innovation-network/ilr-pilot-program

Hansen, T., Soares L., Spires M., and Tran H. (2021). The education blockchain initiative final report. Washington, DC: American Council on Education.

Lemoie, K., Leu S., Everhart, D., and Nadeau, G. Understanding interoperability for education blockchains [White paper]. Washington, DC: U.S. Department of Education. https://docs.google.com/document/d/1emJ7YMmkbs1QIIRojVyJ4urA0VuUD_Z-3domGHXwmYE/edit

LER Resource Hub. (2020, July 20). Introducing the LER Hub – The Next Phase in the Development of Learning and Employment Records. U.S. Chamber of Commerce Foundation. Retrieved April 18, 2022, from https://www.uschamberfoundation.org /blog/post/introducing-ler-hub-next-phase-development-learning-and-employment-records

Rockeman, O. (2022, February 24). Dropping Degree Demands Would Help Boost U.S. Hiring, Study Says. Bloomberg. Retrieved July 26, 2022, from https://www.bloomberg.com/news/articles/2022-02-24/dropping-degree-demands-would-help-boost-u-s-hiring-study-says

Wellspring Initiative (2021). Digital credentials & competency frameworks: Exploring employer readiness and use in talent management. Boston, MA: IMS Global Learning Consortium. Retrieved April 18, 2022, from https://www.imsglobal.org/sites/default/files/wellspring/Wellspring_II_Employer_Research.pdf

Disclaimer: The research included in this report was made possible through funding by Walmart. The findings, conclusions, and recommendations presented in this report are those of the authors alone and do not necessarily reflect the opinions of Walmart.