Trybe.ID

Digital Credential Vendor Selection: An Organizational Fiduciary Responsibility

Digital Credential Vendor Selection: An Organizational Fiduciary Responsibility

This white paper serves as a governance guide for both educational institutions and their IT departments as part of fulfilling their fiduciary duty. This includes performing crucial due diligence on their shortlist of digital credential solutions on behalf of vulnerable learners.

Assuming that an educational institution has decided digital credentials are part of their strategy, this document is explicit about the calls to action for their IT department when seeking to deploy those credentials, and also for an institution looking to review said strategy with regard to this important area.

Lead Authors

- Guy Pearce, Chief Digital Officer & Chief Data Officer, Convergence.tech
- Chami Akmeemana, CEO, Convergence.tech and Trybe.ID

Contributors

- Borhene Chakroun, Director for Policies and Lifelong Learning Systems, UNESCO
- Kim Duffy, Co-Chair W3C Credentials Community Group
- Janette Hughes, Canada Research Chair, Technology & Pedagogy, Ontario Tech University
- Kelly O'Neill - Dean, Program Planning, Development & Renewal, Humber College Institute of Technology & Advanced Learning
- Prof. John Pollaers, OAM, Chair Swinburne University, Australia
- Stephan Vincent-Lancrin, Deputy Head of Division and Senior Analyst, OECD

Table of Contents

Introduction

A decade down the line, digital badges - recognizing the skills and competencies gained at a more granular level than those typical of higher education courses - are still regarded as a relatively innovative technology in formal educational institutions and even in informal learning contexts. Also referred to as microcredentials, digital badges, as a subset of digital credentials, are a critical form of digital transformation in the education sector.

As a form of digital transformation:

- **Digital credential vendors are responsible** for ensuring that their offerings are learner-centric as per digital transformation practice and according to global IT codes of conduct, including privacy and security.
- **Educational institutions have a fiduciary responsibility** to ensure that their selected digital credentials vendor serves the best interests of the learners, given that said learners will bear the outcomes of these decisions for their entire careers.
- **Educational institution Information Technology (IT) departments have a fiduciary responsibility** to ensure that their operating model is in a state of digital readiness and able to sustain the deployment of digital credentials technology, as per digital transformation practice

Originally, the intent of digital badges was to recognize the achievement of granular skills. However, today, digital badges may equally serve traditional educational credentials, themselves all a subset of the broader digital credentials ecosystem.

Learner-Centricity and the Best Interests of Learners

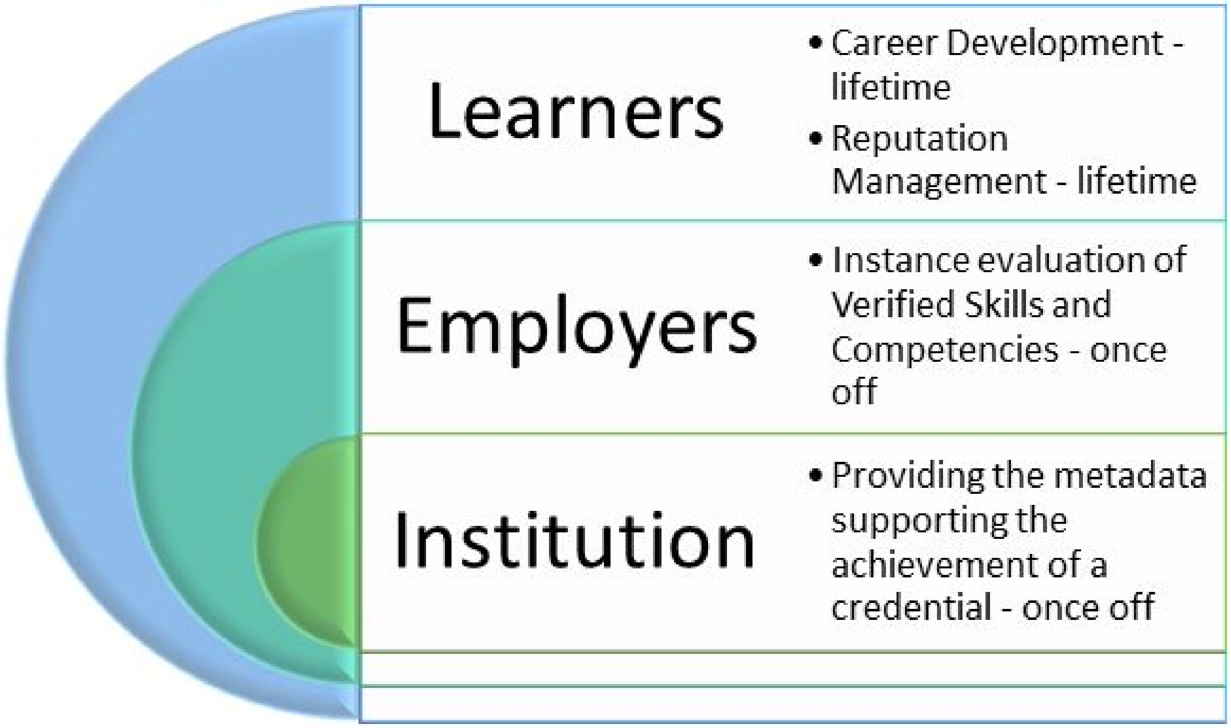
Learners are an educational institution's clients and lay their future in the hands of those who teach them. As such, it is fair that they expect these institutions to act in their best interests. This is true both in terms of curricula; relevant in a rapidly changing world in terms of teaching and learning quality, as well as for digital credentials - important in shaping their future careers.

Furthermore, the primary principle of digital transformation is that it is user-centric[1], lending further credence to the imperative for a learner-centric approach to digital credentials. In this respect, some research focuses on institutional and employer value creation, but with no apparent consideration of value created for learners: "...*case*

[1] Pearce, G.; "Digital transformation governance: What boards must know," Governance Institute of Australia, Vol 72(5), 2020, https://www.governanceinstitute.com.au/resources/governance-directions/volume-72-number-5/digital-transformation-governance-what-boards-must-know/

studies do exist that indicate one of the biggest obstacles to implementing badges as a form of recognition is the lack of perceived value by institutions and employers[2]." The value to learners seems under-estimated, given that learners will live with the consequences of digital credentials decisions and actions for their entire careers. Yet learners are also the subject of the greatest and most sustainable value creation of the paradigm.

Figure 1: Measured by duration of impact, learners are the subject of the greatest value of three stakeholder groups. Value creation strategies should therefore include them, in alignment with generally accepted digital transformation frameworks:



Learners

- Career Development - lifetime
- Reputation Management - lifetime

Employers

- Instance evaluation of Verified Skills and Competencies - once off

Institution

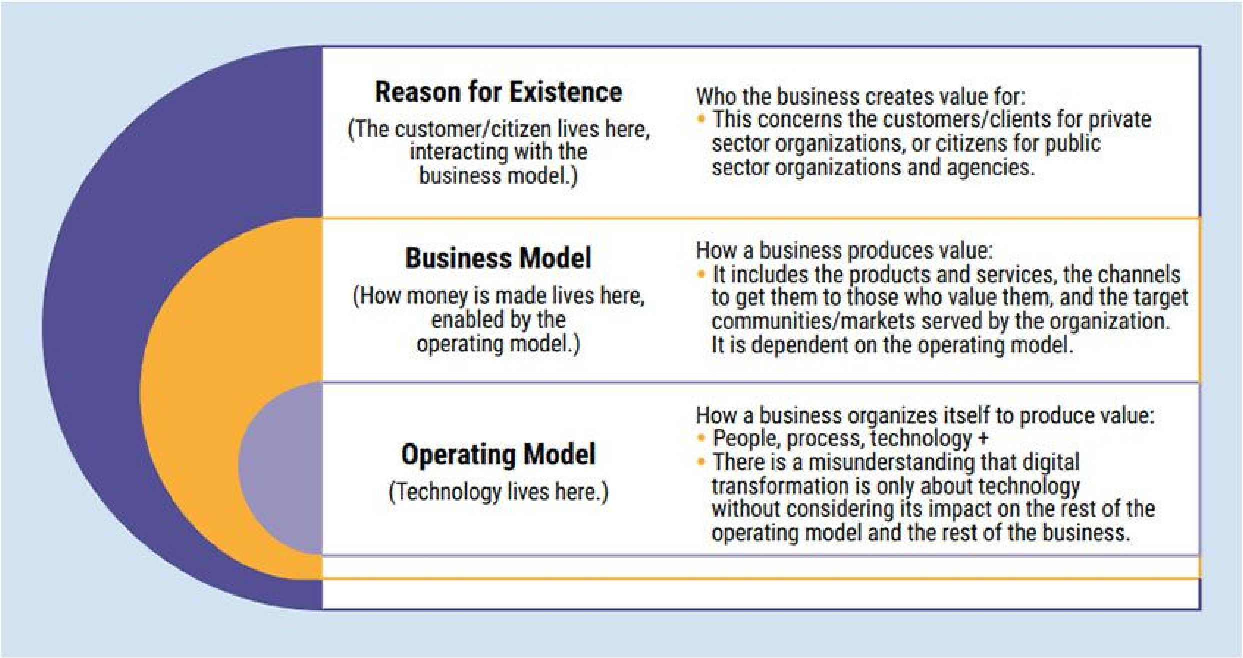
- Providing the metadata supporting the achievement of a credential - once off

Perhaps the root cause of some of the challenges being encountered in the adoption of digital credentials is that learners, the major beneficiaries, are not consulted enough as part of digital credentials value chain development.

[2] eCampusOntario; "Key Findings: Open Badges," Open Library Pressbooks, n.d., https://ecampusontario.pressbooks.pub/edtechsandbox/chapter/chapter-1/

Figure 2: An educational institution's reason for existence is its learners, and therefore learner benefits should be the primary goal of digital transformation[3]. The organization's strategy should be about how maximum value can be created for learners by "*tuning*" the organization's business model and its operating model.

Figure 1—The Relationship Between the Customer, the Business Model and the Operating Model



Reason for Existence
(The customer/citizen lives here, interacting with the business model.)

Who the business creates value for:
- This concerns the customers/clients for private sector organizations, or citizens for public sector organizations and agencies.

Business Model
(How money is made lives here, enabled by the operating model.)

How a business produces value:
- It includes the products and services, the channels to get them to those who value them, and the target communities/markets served by the organization. It is dependent on the operating model.

Operating Model
(Technology lives here.)

How a business organizes itself to produce value:
- People, process, technology +
- There is a misunderstanding that digital transformation is only about technology without considering its impact on the rest of the operating model and the rest of the business.

The Fiduciary Responsibility of Educational Institutions

Learners trust that their educational institutions act in good faith and in their best interests, while educational institutions trust that their IT departments make decisions and perform deployments that serve the best interests of the institution. This places a significant responsibility on the part of educational institutions as a whole to select the digital credentials technology - if this is aligned with their strategy - that best serves the interests of their learners.

Achieving Digital Readiness as a Critical Success Factor

Digital transformation is an imperative in most industries today. While some industries find the cloud, artificial intelligence (AI), robotics and the industrial internet of things (IIoT) to be the technology drivers of change, the education sector is undergoing its own changes, one of them being how they utilise verifiable digital credentials technology.

[3] Pearce, G.; "Attaining Digital Transformation Readiness," ISACA Journal, vol. 1, 2020, https://www.isaca.org/archives

As with any industry undergoing change, effecting it is not simply about deploying technology. Digital readiness and alignment are critical considerations in ensuring that digital transformations, like digital credentials, create the value that educational institutions and learners expect of them. From an organizational perspective, "… barely one in eight [digital transformation initiatives] are successful. Even worse, only 3 percent of … 1,733 executives … report any success at sustaining the change required for successful digital transformation….[4]"

Performing and responding to a digital credentials solution due-diligence process significantly increases the likelihood of success and sustainability of the digital transformation initiative, especially when performed in alignment with a recognized digital transformation framework. As with anything new, if one performs the due diligence on a product or project, one is far more likely to stick with it for the long haul.

IT Codes of Conduct and the State of the Digital Credentials Industry

Digital credentials technology should primarily serve the best interests of learners to fortify their futures. This includes protecting or enhancing privacy, and ensuring ownership and the sustainability of their academic achievement records.

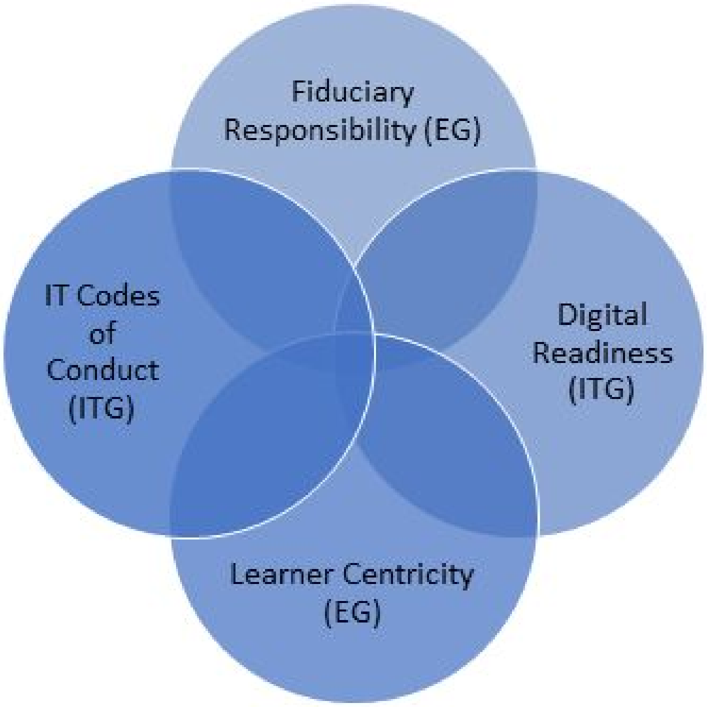
Like other industries, the IT sector has codes of conduct as part of its governance constructs to guide activities, including software development. For example, both the Institute of Electrical and Electronics Engineers (IEEE) and the Association of Information Technology Professionals (AITP) have long-standing codes of conduct detailing requirements for integrity, professional responsibilities, societal responsibilities and a commitment to "*avoid injury to others, their property, reputation, or employment*[5]."

While we could cite global IT players that have failed in these responsibilities (e.g. the failures to uphold privacy), it does not imply that these responsibilities are not relevant. Indeed, they continue to present the standards that many ethical IT organizations strive to uphold. As part of IT due diligence, it is useful to identify instances where IT codes of conduct are not adhered to by the institution's current or shortlisted digital credentials vendors.

[4] Pearce, G.; "Attaining Digital Transformation Readiness," ISACA Journal, vol. 1, 2020, https://www.isaca.org/archives

[5] Woo, M.; "Ethics and the IT Professional," Educause Review, 27 March 2017, https://er.educause.edu/articles/2017/3/ethics-and-the-it-professional

Figure 3: Selecting a digital credentials vendor is made at the intersection of two IT Governance (ITG) constructs and two Enterprise Governance (EG) constructs. Data Governance plays a role too and will be discussed later in this document.



Digital Badges: Birth and Early History

Badges - a subset of digital credentials that can include other forms of digital identification, digital certificates, user accounts and even website security certificates[6] - are digital certificates of achievement. In the learning community, these represent "*... evidence and competency based …*[7]" achievements. Besides being a record of a learner's achievements, they benefit from being easily shareable by means of Linkedin and other social media networks, email, elsewhere on the Internet, and even by QR-codes.

They started in 2010 from work performed at "... *the Mozilla and MacArthur Foundations, and out of the research of Erin Knight, founding director of the Open*

[6] Iafrate, M.; "Digital Badges: What Are They And How Are They Used?" eLearning Industry, 6 November 2017, https://elearningindustry.com/guide-to-digital-badges-how-used
[7] Open Badges; "Issue," IMS Global Learning Consortium, n.d., https://openbadges.org/Issue

*Badges project at Mozil*la.[8]" Version 1.0 of the open badges specification was released by Mozilla in 2013, and in 2017, IMS Global assumed responsibility for the digital badges charge[9]. Version 2.0 was released in 2018.

The entire purpose of the badge ecosystem was to support real world lifelong learning and other career development activity[10], because learning has never really been limited to the traditional education sector constructs of schools, colleges and universities and their paper-based credentials. Indeed, usable and reusable career education readily comes in the form of, for example, on-the-job-training, by means of Massive Online Open Courses (MOOCs) and other forms of informal adult learning.

Investments in badges recording these outcomes are therefore as much investments in learners' futures as traditional certifications alone once were. This is particularly true at a time when a large share of workers change jobs and sectors over their careers and have to constantly adjust to an evolving skills demand, or as evidenced in this time of global pandemic.

Global Digital Credentials Standards

Digital credential vendors adopting a recognized and comprehensive digital credentials standard for their developments are able to present confidence both directly to the educational institution and indirectly to their learners about the portability, privacy, ownership, verifiability and interoperability of the digital credentials platform deployed.

Fortunately for learners, digital credentials standards have become much more rigorous than those originally presented by the Open Badges standard (see Table 1), and as such, the original Open Badges specification is no longer the hallmark of a quality digital credentials vendor, as we shall see.

W3C Verifiable Credentials Data Model as the Next Generation Standard

Instead, today's leading standard is that provided by the World Wide Web Consortium (W3C), an international community of professionals working together to develop Web standards. W3C develops interoperable technologies (specifications, guidelines, software, and tools) aimed at leading the web to its full potential.[11]

[8] Open Badges; "History," IMS Global Learning Consortium, n.d., https://openbadges.org/about/history
[9] Open Badges; "History," IMS Global Learning Consortium, n.d., https://openbadges.org/about/history
[10] The Mozilla Foundation and Peer 2 Peer University, in collaboration with The MacArthur Foundation; "Open Badges for Lifelong Learning," Working Document, n.d. Updated 27 August 2012,
[11] Berners-Lee, T.; "Tim Berners-Lee," Biography, n.d. https://www.w3.org/People/Berners-Lee/https://www.w3.org/People/Berners-Lee/

In particular, the W3C specification for verifiable credentials defines standards for file format (JSON), data flexibility (Open), and the ability to facilitate all of the following: recipient control, evidence of tampering, time stamping, integrated data/display, shareability, revocability, expirability and legal enforceability in a decentralized manner (i.e. without the need to consult the issuer).

Furthermore, W3C provides specific, coherent guidelines for a diverse range of verifiable credential use cases that are accommodated by the specification. This is not only in education, but also in retail, finance, healthcare, the professions (legal, accounting, medicine), government, legal identity and also for devices[12]. This will be of particular interest to educational institutions, because highly detailed use case standards exist in the W3C standard for digital transcripts, taking a test, transferring schools and online classes, the latter being especially prevalent in a time of Covid 19.

Comparing Standards

Table 1 serves to compare some of the older standards (or current versions of those standards) relative to the new W3C standard as at 2019. Furthermore, with the blockchain-based Blockcerts standards also seeking to align with the W3C standard[13], the recommendation to our clients is to ask their digital credentials vendor to demonstrate alignment with the W3C data model in the interests of pursuing the highest possible digital credentials product standard.

At the very least, it is important to ensure that a digital credentials vendor complies with the latest version of the standard it aligns with, noting the potential ramifications of old versions of the standard with reference to key issues like digital credential portability, privacy, verifiability and interoperability.

In this context, W3C is about next generation (nextgen) certification of credentials. Note that due to blockchain still being in its infancy, there is a risk of vendor lock-in for any digital credentials systems that leverage this technology[14]. Therefore, this is something that an educational institution should also consider.

[12] Otto, N., S. Lee, B. Sletten, D. Burnett, M. Sporny and K.Ebert; “Verifiable Credentials Use Cases,” W3C Working Group Note, 24 September 2019, https://www.w3.org/TR/vc-use-cases/

[13] Blockcerts Community; “Verifiable credentials,” Blockcerts, December 2019, https://community.blockcerts.org/t/verifiable-credentials/2210

[14] Hamilton Duffy, K., H. Pongratz and J.P. Schmidt (eds); “Building the digital credential infrastructure for the future,” Digital Credentials Consortium, January 2020, https://digitalcredentials.mit.edu/wp-content/uploads/2020/02/white-paper-building-digital-credential-infrastructure-future.pdf

Table 1: A comparison of the major digital credentials standards and technologies (based on Dugan, Streun and Jagers 2019[15])

	Hosted Open Badges	**Digital Signatures**	**Blockcerts**	**W3C Verifiable Credentials**
File Format	Fixed Image	Fixed Layout	JSON machine and human readable	JSON machine and human readable
Data Flexibility	Strict but expandable	Open	Strict but expandable	Open
Recipient Proof of Control Method	Email	No	Bitcoin address	Decentralized Identifiers
Tamper Evidence	No	Tiered (electronic vs digital signature)	Yes	Yes
Timestamping	No	Yes	Yes	Yes
Integrated Data/Display	No	Yes	Yes	Yes
Sharing mechanisms	Share by file and link, BadgeConnect	Share by file and link	Share by file and link	Share by file and link, wallet protocols
Revocation Mechanism	Hosted revocation list (centralized and correlatable)	Only by vendor	Hosted revocation list (centralized and correlatable)	Flexible mechanisms, including privacy-preserving
Expireable	Yes	Only by certificate authority	Yes	Yes
Ability to align with a variety of legal digital signature requirements	No	Yes	No	Yes

[15] Dugan, M., C Streun and C Jagers; "Digital Credentials Comparison Report," IMS Global, February 2019, https://www.imsglobal.org/sites/default/files/DCsummit2019/2019-0206Summit-Comparison%20Report.pdf

Vendor Standards

From a legacy perspective, there are vendors that are aligned with the original Open Badges standard. However, the Open Badges standard is also seeking alignment with the W3C standard, described as "*a significant enough change to require a 2.1 version*[16]."

Furthemore, be aware that some vendors (that may not fully subscribe to modern standards for digital credentials) host badges on behalf of the issuing institution, which risks effectively disempowering the recipients of those badges - the learners - from any control over their credentials. This situation occurs in spite of recommendations that, "*badge recipients need the option of being able to print off badge details, share their badges on different social media and networking sites, and have control over displaying and hiding different badges they receive*," as well as in the interests of sustainability, ensuring "*... that digital badges are not tied to institutional email addresses or proprietary institutional software*[17]."

Call to Action #1

Determine the digital credentials standard that your envisaged or current vendor aligns with to arrive at conclusions consistent with the ethics and policy standards of your institution.

You may find the structure provided in the Appendix to be of assistance when evaluating a digital credentials vendor against the W3C standard, and also with reference to the requirements of digital credentials vendors as proposed by the Digital Credentials Consortium outlined below.

The Global Standard Expectations of Digital Credentials Products

The global, university-led Digital Credentials Consortium sets the following requirements for digital credentials service providers[18]:

[16] Otto, N.; "Open Badges as Verifiable Credentials (Claims)?" Github, 19 January 2018, https://github.com/w3c-ccg/edu_occ_verifiable_credentials/issues/2

[17] Dyjur, P. and G. Lindstrom; "Perceptions and Uses of Digital Badges for Professional Learning Development in Higher Education," Springer, 10 March 2017, https://link.springer.com/article/10.1007/s11528-017-0168-2

[18] Hamilton Duffy, K., H. Pongratz and J.P. Schmidt (eds); "Building the digital credential infrastructure for the future," Digital Credentials Consortium, January 2020,

Prioritizing Learner Agency (Sovereignty) and Privacy

Any digital credentials product having functionality that contradicts any of these requirements compromises learner sovereignty and privacy, thereby going against the spirit of the global digital credentials ecosystem.

- Interoperability - Offer multiple options for credential storage
- Privacy - Requires learner consent for credential issuance
- Privacy - Issue credentials optimizing learner flexibility and privacy
- Privacy - Minimum disclosure of personally identifiable information (PII)
- Privacy - Prevent tracking
- Resilience - Enable recovery of lost credentials
- Security - Prove trusted learner identity
- Security - Enable seamless verification without involving the issuer (the latter could be the subject of social engineering fraud)

Trust Enablement

Any digital credentials product having functionality that contradicts any of these requirements compromises trust and therefore fails any test of fiduciary responsibility within the global digital credentials ecosystem.

- Integrity - Prevent tampering and fraud
- Integrity - Provide display integrity across devices
- Privacy - Allow only necessary auditability

Supporting Diverse Use-Cases and Technology Best Practices

Any digital credentials product having functionality that contradicts any of these requirements compromises technology best practices, thereby going against the spirit of the global digital credentials ecosystem.

- Accessibility - Provide accessibility (assistive technologies)
- Interoperability - Build on open standards
- Interoperability - Prevent platform lock-in
- Interoperability - Support internationalism
- Interoperability - Enable integration with existing infrastructure
- Interoperability - Support different issuers and types of credentials such as PESC, EQF, CTDL, CASE, CLR, ELMO, Open Badges and others

https://digitalcredentials.mit.edu/wp-content/uploads/2020/02/white-paper-building-digital-credential-infrastructure-future.pdf

- Reliability - Remain efficient, scalable, fault-tolerant and highly available
- Survivability - Ensure credential longevity - lifetime use
- Survivability - Design for sustainability by having technical design and governance structures able to support new use cases

Call to Action #2

Determine the extent to which your digital credentials solution provider aligns with these universally expressed requirements. Even more importantly, you should establish whether any product feature contradicts these standard non-functional requirements.

This will enable conclusions consistent with the ethics and policy standards of your institution.

The Fiduciary Responsibility to Act in Learners' Best Interests

The global Digital Credentials Consortium noted the priority of "*... Learner Agency [(Sovereignty)] and Privacy*[19]" which is already aligned with the end goal of digital transformation, being the end stakeholder - customer, client, citizen[20], or in this case, the learner. However, what is the nature of the considerations an institution needs to ponder to ensure the sustainability of the initiative? What does a learner-centric approach to Digital Credentials mean from an institutional perspective?

As an example of what it does not mean, badge achievements earned on one MOOC provider's site were only ever visible on their site, and only if one was logged on[21]. This had zero value for learners who might want to share their learning achievements with their employers or even on social media. This may still be the case for some well known MOOC providers or companies today.

An example of what it does mean is badge issuers working with learners to design programs that will have the maximum effect based on how learners plan to use the

[19] Hamilton Duffy, K., H. Pongratz and J.P. Schmidt (eds); "Building the digital credential infrastructure for the future," Digital Credentials Consortium, January 2020, https://digitalcredentials.mit.edu/wp-content/uploads/2020/02/white-paper-building-digital-credential-infrastructure-future.pdf

[20] Pearce, G.; "Enhancing the Board's Readiness for Digital Transformation Governance," ISACA Journal, vol. 5, 2019, https://www.isaca.org/archives

[21] Grant, S.; "History and Context of Open Digital Badges," Digital Badges in Education, Routledge, January 2016, https://www.researchgate.net/publication/305488404_History_and_Context_of_Open_Digital_Badges

badges[22]. It has also been proposed that program design should incorporate the consumers of those badges, like employers, to further accelerate the acceptance of badges as alternative measures of learning[23].

Agency (Sovereignty) Violations are Not in a Learner's Best Interests

The rise of self-sovereign identity, where individuals have ownership of the various attributes describing themselves[24], has been described as "*inevitable.*[25]" Self-sovereign identity includes attributes about an individual, including data about their credentials. In this context, learning credentials constitute a specific persona (education) of a given identity (the person as a whole), which can be uniquely identified by, for example, a national identity number, or even as a pair of cryptographic keys.

Learner self-sovereignty means the learner has the exclusive authority to decide what happens to data about themselves - to have the freedom to transfer their credentials from one platform to another. It also means their ability to share credentials with whomever they wish, and to do with the data whatever they would like, without having to ask for permission to do so, or to be constrained by the management of their own data. It is also important that issuers provide credentials to learners in manners that allow them to share only the data that they want, depending on the context..

Unfortunately, some digital credentials products provide no such learner sovereignty, which means the learner is at the mercy of the vendor, having no control over data about themselves. This goes against the spirit of digital credentials, and is certainly not in the best interest of the learner.

Vendor Privacy Infringements are Not in the Learner's Best Interests

[22] Clements, K., R. West and E. Hunsaker; "Getting Started with Open Badges and Open Microcredentials," International Review of Research in Open and Distributed Learning Vol 21(1), January 2020, https://files.eric.ed.gov/fulltext/EJ1240709.pdf

[23] Clements, K., R. West and E. Hunsaker; "Getting Started with Open Badges and Open Microcredentials," International Review of Research in Open and Distributed Learning Vol 21(1), January 2020, https://files.eric.ed.gov/fulltext/EJ1240709.pdf

[24] Wang, F. and P. de Filippi, "Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion," Frontiers in Blockchain, 23 January 2020, https://www.frontiersin.org/articles/10.3389/fbloc.2019.00028/full

[25] Tobin, A. and D. Reed.; "The Inevitable Rise of Self-Sovereign Identity," Sovrin Foundation, 28 March 2017, https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

Digital credentials vendors that do not implement the principle of learner self-sovereignty have unfettered access to all the learner data within their client institutions. This raises privacy issues.

With the relatively low knowledge of the inner mechanisms of digital credentials products by most digital credentials clients, it is unlikely that the educational institutions will sufficiently recognize this learner privacy risk. This means that educational institutions will not be in a position to specify explicit conditions about access to learner data by the vendor in a legally binding document.

As we have seen earlier, some privacy considerations to consider include asking whether the vendor:

- Is capable of tracking learner activity beyond regional legislative requirements that may apply (a privacy violation). A high integrity system will not allow the vendor to collect data to facilitate tracking, and therefore will not be able to present a diversity of insights that may be the outcome of a privacy compromise, potentially with the learner having no knowledge that tracking is in place
- Is capable of changing any credentials or student data (an integrity violation). A high integrity system will be tamper (fraud) proof
- Uses Personally Identifiable Information (PII) as part of its unique identifier mechanism. The availability of PII in this way can result in privacy violations with credentials data that might otherwise not have been identifiable by the vendor. A high integrity system will use cryptographic keys to identify data in such a way that the cryptographic key has no relationship with any user attributes

Call to Action #3

Determine the extent to which your vendor ensures self-sovereign identity and ensures the privacy of learners. This determination enables conclusions consistent with the ethics and policy standards of your institution.

Additional Digital Credentials Risks

In the same way that paper-based credentials face challenges, especially fraud (e.g. “More than 50,000 PhDs are purchased from diploma mills every year,” exceeding the quantity legitimately awarded[26]) which most digital credentials incidentally resolve - the

[26] Duffy, K.; “Deploying Decentralised ID Authentication in DFS,” Financial Inclusion Global Initiative (FIGI) Security Clinic, 4-5 December 2019, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201912/Documents/Part%202%20-%20Kim%20Hamiliton.pdf

aspirations for digital credentials face some of their own challenges, especially those hosted on previous generation digital credentials platforms. These can best be expressed as risks to learners, and as risks to educational institutions. However, these are not the only risks to consider:

Hidden Costs for Validators

Why is it preferable to work with a W3C-compliant verifiable digital credentials vendor? One motivation may take the form of the hidden costs associated with the previous generation Open Badges Platform. For example, the so called "phone home" dependency requires verifiers to contact the badge provider every single time a credential needs to be verified. Each verification request must interact with the badge provider, or the badge's "host", in order to confirm the badge's existence and legitimacy. Therefore this requires that the host be online and accessible at all times and places complete trust and dependence on a single central service.

This is performed differently today. In conformance with the W3C Verifiable Credentials Data Model each digital credential is itself a cryptographically verifiable proof. This means that the credential can be shared and verified privately and independently by any verifier. There are no centralized dependencies or interaction required with the issuer or digital credential vendor. In fact, sharing and verification can be completely offline.

The Institutional Responsibility for Rigorous and Meaningful Digital Credentials

A risk for the digital credentials ecosystem is that the proliferation of badges have diluted the effectiveness of badges[27], especially where these credentials are conferred for activities other than for verifiable learning achievements. Furthermore, if the credentials are conferred for learning, without metadata for the credential (a description of the skills and competencies learned to achieve that level of learning) this dilutes the effectiveness of the credential for employers looking to understand the learning scope. It has therefore been proposed that it is the badging community's responsibility to ensure that deployed badges are both rigorous and meaningful[28].

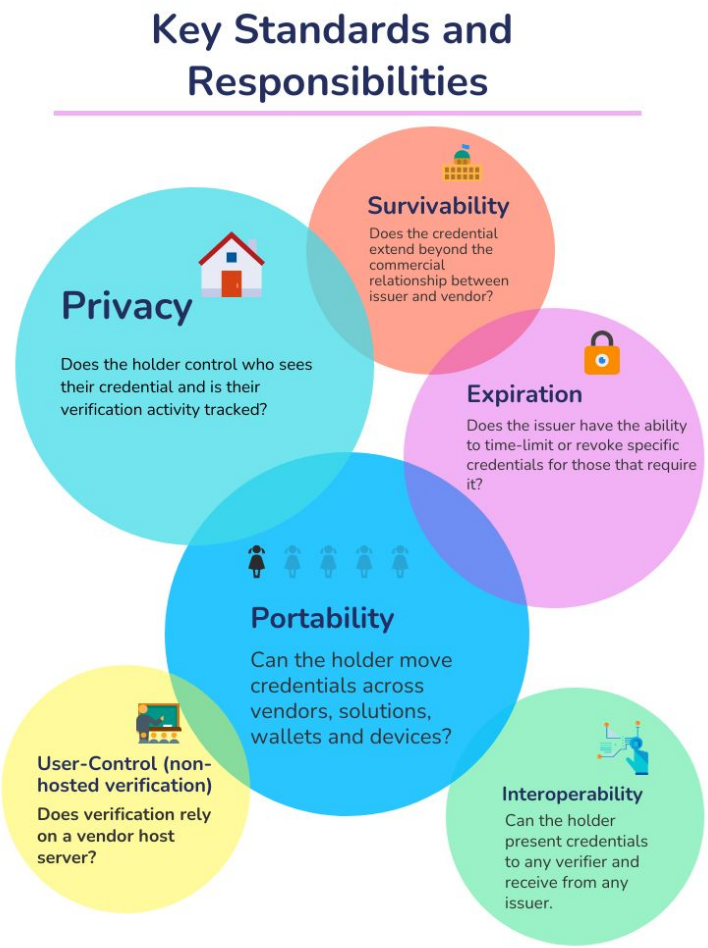
[27] Farmer, T. and R.E. West; "OPPORTUNITIES AND CHALLENGES WITH DIGITAL OPEN BADGES," Foundations of Learning and Instructional Design Technology, Pressbooks, 2016, https://lidtfoundations.pressbooks.com/chapter/open-badges/

[28] Farmer, T. and R.E. West; "OPPORTUNITIES AND CHALLENGES WITH DIGITAL OPEN BADGES," Foundations of Learning and Instructional Design Technology, Pressbooks, 2016, https://lidtfoundations.pressbooks.com/chapter/open-badges/

Call to Action #4

Determine whether the process of validating a digital credential with the envisaged digital credentials tool is frictionless and costless for the validator. Then come to conclusions consistent with the ethics and policy standards of your institution.

Figure 4: Key Standards and Responsibilities



Key Standards and Responsibilities

Survivability

Does the credential extend beyond the commercial relationship between issuer and vendor?

Privacy

Does the holder control who sees their credential and is their verification activity tracked?

Expiration

Does the issuer have the ability to time-limit or revoke specific credentials for those that require it?

Portability

Can the holder move credentials across vendors, solutions, wallets and devices?

User-Control (non-hosted verification)

Does verification rely on a vendor host server?

Interoperability

Can the holder present credentials to any verifier and receive from any issuer.

SOURCE 1, 2

Conclusion

This document serves as a basis for the due diligence required before selecting a digital credentials vendor, and advises on an approach educational institutions can follow when pursuing the design and deployment of digital credentials. It also serves to highlight various risks inherent in some digital credentials offerings, with the burden of risk borne by learners, who stand to suffer most due to privacy and sustainability vulnerabilities that braided through some legacy digital credentials products.

Some facts established through the pages of this article were that:

- The original intent in supporting digital credentials was the acknowledgement of the alternative learning pathways a person may follow as they support their career competency-building and career advancement aspirations
- W3C’s verifiable credentials data model serves as the leading standard for digital credentials, creating the foundation for the next generation of digital credentials
- Many of today’s major digital credentials providers are aligned with a previous generation’s compliance standard. This introduces risk for educational institutions, learners, and their data. Furthermore, it incurs costs for any institution wishing to validate, for example, an employee’s credentials with that service provider

Primary Lessons for Learners

Ensure that you have full control over your own credentials, including who is granted access to view them. Furthermore, in the interests of transferability, make sure there are no barriers to managing your credentials across platforms (interoperability and portability), in the spirit of the original Mozilla intent. Any compromise here means that your credentials are out of your control, and could entirely disappear if a particular vendor goes out of business. All of your lifelong educational achievements should be able to accompany you for your entire career, for you to do with exactly as you wish, and should not be the subject of any single vendor’s vagaries.

While learners do not have direct control over an educational institution’s digital credentials product, they can engage in advocacy work through existing student government channels, or create a special interest group to raise these concerns if the product fails against any number of criteria raised in this article. It also pays to remember that educational institutions have a responsibility to act in your best interests.

If the product does not create value for you, then the question to the university is, “Who is this system meant to serve?” The principles of digital transformation require that initiatives create value for the end-user, and in this case, it is you, the learner, with the longest point of contact with the product by means of digital credentials that serve you for your entire career.

Primary Lessons for Educational Institutions (Issuers)

Ensure that you, and not the digital credential product vendor, have full control over the issuing of credentials and the associated metadata. Also ensure that you have full control over the options available to the learner, that you control the ability to revoke credentials according to your institutional policies, and that your credentials comprise part of the larger credential ecosystem rather than being the subject of vendor lock-in. Also ensure that credentials can be verified without having to consult the vendor or even the original issuer. Any compromises here have the potential to bring your reputation into disrepute should disputes or other issues arise.

It is also important for the educational institution to create a structured deployment plan for the productionalization of your digital credentials vision, and to ensure that value is created from this intervention by means of the appropriate governance constructs.

Closing Comments

For both learners and issuers, it is crucial to ensure that the credential vendor aligns with the most stringent standards in the industry - the W3C Verifiable Credentials Data Model as the Next Generation Standard. The stakeholder that has the most to lose in any of this is the learner, who could be exposed to considerable risks if shortcuts are taken regarding compliance. For the issuer, there needs to be trust in the mechanism itself, and demonstrated vendor alignment with the W3C standard which provides assurance of this trust[29]. As Eleanor Roosevelt once said *"The future is literally in our hands to mold as we like. But we cannot wait until tomorrow. Tomorrow is now."*

[29] Lesavre, L., P. Varin, P. Mell, M. Davidson, and J. Shook; "A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems, " White Paper. National Institute of Standards and Technology, January 14, 2020. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01142020.pdf.

APPENDIX: How Well Does Your Vendor Fare Against the Requirements of the Digital Credential Ecosystem?

Summarizing the content of this document, use this table as a basis to evaluate your digital credentials vendor.

Table 4: Vendor checklist

#	Group	Category	Your vendor alignment notes
1	**W3C Standard Alignment**	File Format	
2		Data	
3		Flexibility	
4		Recipient Ownership	
5		Tamper Evidence	
6		Timestamping	
7		Integrated Data/Display	
8		Shareable	
9		Revocable	
10		Expireable	
11		Ability to align with a variety of legal digital signature requirements	
12	**Prioritizing Learner Sovereignty and Privacy**	Interoperability - Offer multiple options for credential storage	
		Privacy - Require learner consent for issuing credentials	
13		Privacy - Issue credentials optimizing learner flexibility and privacy	
14		Privacy - Minimum	

		disclosure of personally identifiable information (PII)	
15		Privacy - Prevent tracking	
16		Resilience - Enable recovery of lost credentials	
17		Security - Provide trusted learner identity	
18		Security - Enable seamless verification without involving the issuer	
20	**Trust Enablement**	Integrity - Prevent tampering and fraud	
21		Integrity - Provide display integrity across devices	
22		Privacy - Allow only necessary auditability	
23	**Supporting Diverse Use Cases and Technology Best Practices**	Accessibility - Provide accessibility (assistive technologies)	
24		Interoperability - Support internationalism	
25		Interoperability - Support different issuers and types of credentials	
26		Interoperability - Enable integration with existing institutional infrastructure	

27		Interoperability - Prevent lock-in	
28		Reliability - Remain efficient, scalable, fault-tolerant and highly available	
29		Standardization - Build on open standards	
30		Survivability - Ensure credential longevity - lifetime use surviving even issuer existence	
31		Survivability - Design for sustainability and flexibility	
32	**Privacy Standard**	GDPR compliance	

Trybe.ID

Trybe.ID is a digital credentials platform that makes issuing, accessing and verifying digital credentials easy and secure. It is the only solution that grants users true complete ownership over and access to their credentials in the education market today. Trybe.ID allows credentials to be shared directly with only the parties the holder wishes as well as verified entirely independent of any third party, respecting end user privacy and security.

Please contact Uri Carnat at uri@trybe.id for further information on our digital credentialing programs with schools and ongoing pilot opportunities.

✉ uri@trybe.id

in /trybeid

https://trybe.id

@trybeid

Trybe.ID is actively being utilized by over 30 issuing institutions globally, spanning 10 countries. Our Client Partners include:

Spectrum Health Care · STEAM-3D Maker Lab · Identity NORTH · HTS HOLY TRINITY SCHOOL · WBLC Work Based Learning Consortium · SLIIT Discover Your Future · DIACC · TextileExchange · COMMUNITECH · TFA 2020 · Health · DLT4EU · Elmbrook Schools become what's next