D2.1

Report on State of the Art of Digital Credentials

Deliverable created as part of the following task:

T2.1 State of the Art of Digital Credentials

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Title of the document	State of the Art of Digital Credentials	
Work package	WP2	
Date of beginning/date of completion	02/02/2024 / 20/08/2024	
Responsible partner	TU Graz	
Deliverable (title and number)	D2.1 Report on State of the Art of Digital Credentials	
Deadline	31/08/2024	
Autors	Chiara Ruß-Baumann, Carina Kern	
Contributors	Alexander Nussbaumer, Christian Gütl, Carlos Alario Hoyos, Carlos Delgado Kloos	
Involved partners	TU Graz, UC3M, UG, KINAL	
Version	1.0	
State	**Borrador** ☐	**Final** ☒

Table of Contents

1. Introduction

In a flexible and technology-enhanced working environment, education and training change and face new challenges when it comes to learning, learning outcomes and recognition of these outcomes. Various possibilities to recognize learning outcomes have gained popularity in the past few years, e.g., digital credentialing.

This report provides an overview of the current state of digital credentials. It serves as a foundational resource for understanding and engaging with the dynamic field of digital credentials. By covering different perspectives of digital credentials, it aims to provide a holistic view of the current landscape of digital credentials and to recognize the vast and rapidly evolving nature of the field. However, it is important to note that this report does not claim to be exhaustive and it is not created to provide a comprehensive representation.

The report is subdivided into four main parts. Section 2 clarifies different terms and meanings in the context of digital credentials. In section 3, the operation process of digital credentials as well as relevant technological foundations and non-functional requirements are explained. Section 4 highlights important developments in the field of digital credentials around the world, including providers and relevant infrastructures used for digital credentialing.

This report is a deliverable (D2.1) that is part of the Erasmus+ Project ECOCredGT (http://www.ecocredgt.org/?lang=en) and serves as a basis for a general understanding of relevant aspects in the scope of digital credentials. It is available in English and Spanish.

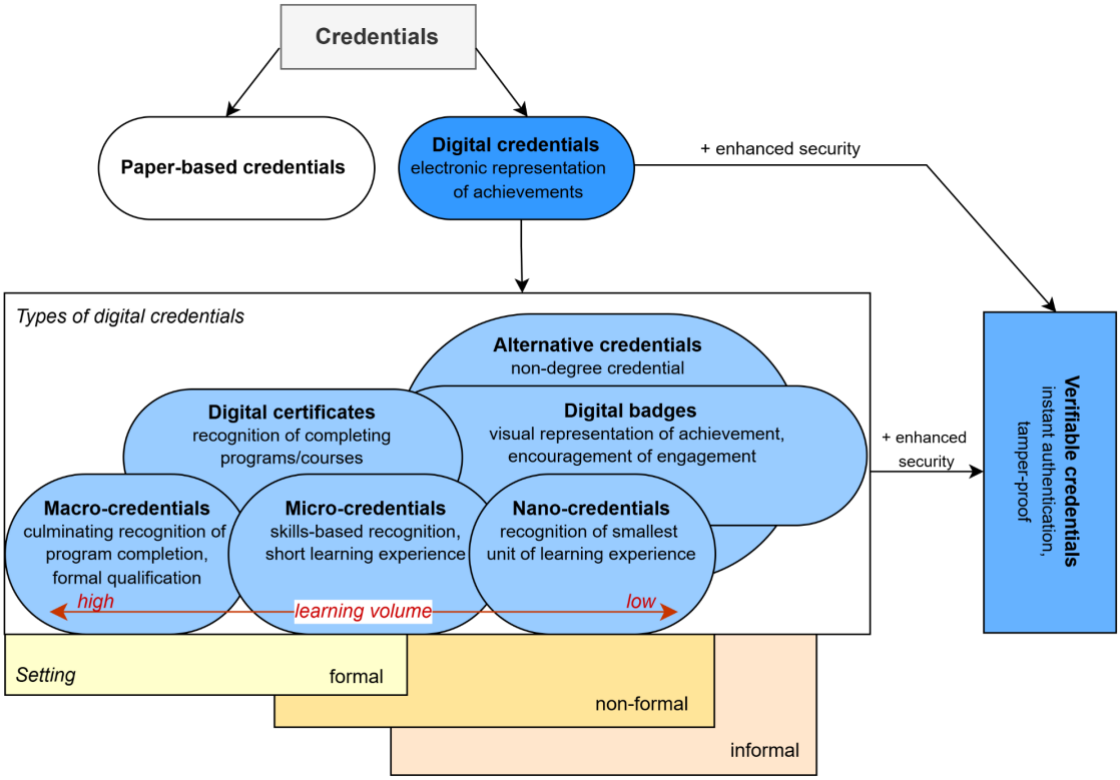
2. Definitions

Since there have been confusions with terms and meanings in the context of credentials, it is important to define “credentials” and related concepts. In the following, some common confusions are specified, beginning with the term “credential” itself, which can be used to describe a certification document, but is also used to describe methods of transport for credentials like wallets and platforms. In their report from 2022, the “American Association of Collegiate Registrars and Admissions Officers” (AACRAO) uses the term “micro-credential” interchangeably with “micro-credential program” to refer to a certain design or program in which learners should gain competences. Furthermore, it is also common to use the terms “badge” and “digital credential” or “micro-credential” interchangeably. A lack of specific definitions of used terms is observable in scientific literature, as well as in providers, which can result in a lack of a common understanding.

Therefore, this section is dedicated to definitions of relevant and often similar used terms in the context of digital credentials. Although we try to include commonly used definitions and understandings in research and professional practice in this section, the trending usage of digital credentials results in different

circulating understandings and meanings, which makes it impossible to clarify all of them in this report. Hence, we do not claim to be complete and all-encompassing in the included definitions. Rather, the main goal of this chapter is to point out differences, as well as similarities between various terms and to form an accepted terminology within the project. Therefore, this section of definitions is initiated with a figure (Figure 1) that highlights overlappings and peculiarities between terms in the context of digital credentials. In the following chapters, each of these mentioned terms is then described in detail.

Figure 1: *Spectrum of digital credentials*



2.1. Credentials

Before specifically engaging with digital credentials, where the focus of the project ECOCredGT lies (ECOCredGT, n.d.), the definition of a credential itself has to be clarified. The Oxford English Dictionary defines credentials as “the qualities, training, or experience that make you suitable to do something” or as “documents such as letters that prove that you are who you claim to be, and can therefore be trusted” (Oxford University Press, 2024). In higher education, the definition of credentials focuses on documents that certify the achievement of a certain level of knowledge and are documented by an authorized third party (AACRAO, 2023). Credentials represent different learning outcomes acquired by an individual and verify, validate, confirm, or corroborate learning achievements, knowledge, and readiness to perform tasks (Keevy & Chakroun, 2015).

In general, credentials are either electronic or paper-based, and are often referred to as transcripts (UNESCO, 2018). Since there are many different types of credentials, depending on the format, purpose, status, provider, extent of learning and training activities, and the context, the term “credential” is often used as an umbrella term. Different forms of credentials and connected terms, that are relevant in the context of educational and vocational training, are described in the following chapters.

○ 2.2. Digital Credentials

Digital credentials refer to electronic representations of achievements, skills and competences and are typically stored and transmitted in digital formats. Digital credentials are equivalent to paper documents, tangible tokens or other haptic objects issued by a trusted party (Brands, 2002). Therefore, the electronic format is an important characteristic of digital credentials, which enables the storage, transmission and usage of platforms. “Digital credential” is a broad term encompassing different types of credentials such as digital badges, digital certificates, and micro-credentials. They represent an evolution from traditional paper credentials like certificates, results, and awards. Digital credentials are utilized in various domains including education and training (Quigley, 2023). Especially in this context, security is an important factor when it comes to reliability and authenticity. Therefore, the employment of blockchain technology, cryptography or digital signatures is establishing fast in this context. To ensure authenticity, tamper-proofness, compatibility and interoperability among diverse credentialing ecosystems, the credentials also have to be verified. With uprising technologies, standardized formats and specifications, the verification of digital credentials is often assumed or presupposed for digital credentials. Nevertheless, in the original emergence of the term, the focus was on the format, which is not a paper-based, but an electronic representation of various achievements.

2.2.1. Classification of Digital Credentials

As mentioned above, the spectrum of digital credentials is extremely broad. Therefore, it might often be necessary to categorize them. In general, there are several characteristics that allow the description and categorization of digital credentials in education and training.

- **Formality:** Digital credentials can either be formal, non-formal, or informal. Each type serves different purposes and is recognized in distinct ways within educational, professional, and personal contexts. Formal credentials are officially recognized qualifications that are typically awarded by accredited institutions following a structured curriculum. They are often required for professional practice or for higher education entry. Non-formal credentials are typically awarded for learning that occurs outside of the traditional academic setting. They are more flexible and targeted toward specific skills or knowledge areas. Informal credentials are less structured and often involve learning experiences that occur

naturally in daily life. They are typically self-directed and do not follow a formal curriculum.

- **Provider:** Various organizations and platforms provide digital credentials, each serving different purposes and audiences. Providers are either public or private and offer proprietary or open access software that is used to issue, manage or verify digital credentials. Some of the key providers of digital credentials are educational institutions, professional organizations, online learning platforms (e.g., Udacity, edX, Coursera), certification bodies (e.g., Microsoft, CompTIA), or professional networks (e.g., LinkedIn, Credly).
- **Learning volume:** Some specific terms in the context of digital credentials focus on the learning volume of a credential (e.g., micro-credentials with a small volume of learning). For every credential, the learning volume can be described in quality and quantity, ranging from very small to very large. To assure comparability, the learning volume should be described within a quality or qualification framework (e.g., European Qualifications Framework for Lifelong Learning - EQF; CEDEFOP, 2024) or another standardized system, like a credit point system (e.g., European Credit Transfer and Accumulation System - ECTS; European Commission, n.d.-a).
- **Verifiability/authorization:** Digital credentials can be authorized and verified to ensure the authenticity, validity, and trustworthiness of the credentials issued and received. These processes involve several technologies, including digital signatures, blockchain, and secure verification platforms that can be described.
- **Purpose:** Within these different categories, there often is a specific purpose for receiving a digital credential, which can be the achievement of a qualification, a specific skill, or it could serve as a motivational factor.

2.3. Digital Certificates

As mentioned above, a digital certificate is a specific type of a digital credential that certifies an individual's competence in a specific skill or field and has the purpose of recognizing and acknowledging achievements in the context of structured learning, like the completion of formal courses, training programs, or professional certifications. Digital certificates are commonly used to validate professional skills and competencies, and often required for certain job roles or professional advancements. They are common in academic institutions, corporate training, and certification programs (Sertifier, 2023). A digital certificate includes some kind of proof that confirms an entity is what it says it is, like an electronic signature from one or more trusted parties that guarantee the authenticity and validity (European Union Agency for Cybersecurity, n.d.).

The primary purpose of digital certificates, in the context of recognizing achievements, is to acknowledge the completion of a formal course, training

program, or professional certification. On the contrary, other forms of digital credentials, like digital badges, are more versatile and can represent a broader range of achievements, since they are used to recognize accomplishments also from informal learning experiences, workshops, conferences, volunteering, and other skill demonstrations.

Digital certificates and digital credentials have a lot in common. Nevertheless, while a certificate is a specific type of a credential, focused on recognizing the completion of a formal program or achievement, a credential is a more encompassing term that includes various forms of validation (e.g. informal achievements) and all of the following described terms.

○ 2.4. Alternative Credentials

The term “alternative” within the context of digital credentials means alternative to traditionally used credentials in higher education (degrees from bachelor´s, master´s and doctoral study programmes) (AACRAO, 2022). In align with this, Kato and colleagues (2020) define “alternative credentials” as “credentials that are not recognised as standalone formal educational qualifications by relevant national education authorities”. Furthermore, there is no need for a specific level of education, where alternative credentials can be awarded. In their understanding, certificates, digital badges and micro-credentials are three forms of alternative credentials that are conceptually distinct.

Also AACRAO (2022) defines alternative credentials as “non-traditional (non-degree) credentials”. When they are offered by institutions of higher education, they may include various other credit alternatives, including Massive Open Online Courses (MOOCs), micro-credentials, badges, and certificate programs. Furthermore, they are stated to be issued typically in a digital format. While AACRAO focuses on credentials that are offered by institutions of higher education, alternative credentials also gained interest outside of traditional academic institutions, e.g., in vocational training to support employability. Therefore, alternative credentials highlight the diverse nature of learning activities with a focus on the achievement of skills and competences to support lifelong learning and upskilling.

○ 2.5. Verifiable Credentials

Verifiable Credentials are digital credentials that can be cryptographically verified for authenticity and integrity. The term “verifiable” within the context of verifiable credentials denotes the characteristic of credentials to be confirmed by a verifier and the possibility to independently check and authenticate them to confirm their legitimacy. Designed to be secure, tamper-proof, and easily shareable, verifiable credentials allow individuals to present credentials such as identity, qualifications, or other personal details to organizations needing to verify them (such as employers, educational institutions, or government agencies). Unlike physical documents, verifiable credentials streamline the verification process and enhance security by eliminating the need for physical handling, reducing the risk of forgery, and ensuring that the credentials can be trusted and authenticated

digitally. This process typically involves cryptographic techniques (Shoemaker, 2022; World Wide Web Consortium, 2022b). This is often facilitated by technologies like blockchain or decentralized ledgers, which provide a transparent and immutable record of the credential's issuance and validity (World Wide Web Consortium, 2022b). Verifiable credentials can represent identical information as a physical credential. However, the integration of technologies can enhance the tamper-evident nature and trustworthiness compared to their physical equivalents (World Wide Web Consortium, 2024b). Nevertheless, the fact that the credentials are verified does not automatically mean that the accuracy of the claims encoded can be assessed and evaluated.

Verifiable credentials can also be digital credentials. The primary distinction between digital credentials in their original meaning and verifiable credentials lies in the ability for instant authentication. Verifiable credentials, unlike their predecessors, are cryptographically protected versions of both physical and online credentials (Dock Labs AG, 2023). In summary, while also verifiable credentials can be electronic (digital credentials), verifiable credentials offer enhanced security, privacy, and ease of independent verification through cryptographic methods. When these characteristics are met, the usage of the term “verifiable credential” might be more specific and accurate.

○ 2.6. Macro-Credentials

Macro-credentials are formal qualifications that denote the completion of comprehensive educational programs, usually culminating in academic awards such as degrees, diplomas, certificates, and licenses. These credentials cover a broad range of knowledge and skills acquired over an extended period, often several years, and are typically awarded by accredited, recognized, or regulated educational and other institutions or organizations. Macro-credentials signify the attainment of a comprehensive body of knowledge, transferable skills, or technical proficiency, often requiring several years to complete. While some individuals pursue these credentials for personal or general educational growth, others seek them to qualify for a specific profession or career path (UNESCO, 2022).

The European Commission (2020a) explains that macro-credentials are awarded after the successful completion of extensive academic programs. These credentials encompass multiple subjects or areas of expertise, ensuring that the holder has achieved a significant level of mastery and competence. Macro-credentials are essential for higher education and are frequently prerequisites for entering professional fields or pursuing further advanced studies.

In contrast to micro-credentials, which focus on specific skills or short-term learning outcomes, macro-credentials provide a holistic representation of an individual's educational achievements. They involve rigorous assessment and validation by accredited institutions, thus offering substantial evidence of an individual’s qualifications. In summary, macro-credentials are vital qualifications that signify extensive learning and skill acquisition, validated through formal

awards like degrees and diplomas. They play a crucial role in academic advancement, as well as professional development.

○ 2.7. Digital Badges

According to AACRAO (2022) “badges” or “digital badges” refer to the issued artifact and visual demonstration of an accomplished skill. They are “online representations that recognize skills, achievements, membership affiliation, and participation”. Badges are typically awarded for completing a specific task or course, can be displayed on digital platforms, e.g. websites, social media profiles or online portfolios (1EdTech, 2024a), and also serve to showcase achieved skills and accomplishments to employers, peers and other stakeholders (Khalil & Ebner, 2015).

Kato and colleagues (2020) refer to a definition from SURFnet (2016) and state digital badges as “digital pictograms or logos that can be shared across the web to show accomplishment of certain skills and knowledge”. These skills can vary widely in quantitative and qualitative form and do not need to be related to an academic study programme, nor to other standards (e.g., industry or professional standards). Therefore, they are often used to recognize informal learning experiences, but also formal achievements.

UNESCO (2018) refers to a definition from Lemoine and Richardson (2015) and defines digital badges as clickable graphics that contain the record of an achievement, the work and the evidence of this work that is required for this achievement, and information about the issuing entity. They view badges as examples of micro-credentials.

In the past, digital badges have already been used to promote the online gaming community in the mid-2000s, e.g., by Microsoft´s Xbox 360 Gamerscore. In the context of education, digital badging had little interest before the 2010s (Gibson et al., 2015). McDaniel and Fanfarelli (2016) published a paper that describes that there can be quite a lot of comparable goals to receive a badge in computer games and in education. In both contexts, digital badging can be effective to encourage engagement and earning of further badges. Also in higher education and vocational training, digital badges often borrow aspects of gamification and can be awarded as a reward for effort, without being tied to a specific outcome of learning activities (Flintberg, 2022).

While sometimes the term “digital badges” is used interchangeably with micro-credentials (Brown et al., 2021), an important difference is the focus on the visual representation of the acquired competences and learning outcomes in digital badges. They are intended to be displayed and shared online and therefore also can contain metadata that provide more information about the actual credential behind the digital badge (Foshay & Hale, 2017; Gibson et al., 2015). Nevertheless, with their focus on the visual presentation, digital badges can also be used as a motivation factor to promote the engagement in smaller learning activities and to provide a technological solution to represent learning outcomes independently from qualifications (UNESCO, 2018). In a similar way, Mah (2016)

suggests that digital badges have five main roles in the educational setting: motivation, learning-recognition, signaling of achievements, capturing of learning paths and in the higher education sector the potential to contribute to student retention.

Digital badges can be collected through platforms, e.g., social media, but also in more formal platforms from established institutions, like 1EdTech with its Open Badge programme (UNESCO, 2018). The Open Badges specification, with its format for digital badges, exists since 2012 and has issued more than 40 million badges worldwide. An Open Badge consists of the image and data about the digital credential, which is machine-readable (1EdTech, 2024a).

○ 2.8. Micro-Credentials

AACRAO (2022) describes a micro-credential as a competency or skills-based recognition that enables a learner to demonstrate expertise and learning in a specific area. Typically, a micro-credential represents a smaller set of learning achievements or outcomes, not amounting to a full degree.

Micro-credentials are small-scale indicators, can either be performance-based or completion based and can be provided by a range of entities, including commercial businesses, private providers, professional bodies, traditional education and training institutions, community organizations, and various other organizations (World Wide Web Consortium, 2022b). Micro-credentials that are provided internally in a company can also be less formal and oriented more towards acquired skills, competences (i.e. performance-based) and business impact (Foshay & Hale, 2017). Although many micro-credentials reflect the results of conventional learning experiences, others validate achievements gained through different means, such as in the workplace, volunteering, or personal interest learning. They are often considered as an effective method for upskilling workers throughout their careers (World Wide Web Consortium, 2022b).

The “Microcredentials Higher Education Consultation Group” of the European Commission has defined a micro-credential as follows: “A micro-credential is a proof of the learning outcomes that a learner has acquired after a short learning experience. These learning outcomes have been assessed against transparent standards” (European Commission, 2020a). This definition clearly states that a micro-credential is a documented certification awarded by a trusted organization, indicating that a learner has met specific learning outcomes through assessment, according to established standards and quality assurance principles. Implicitly, this definition suggests that micro-credentials should ideally be referenced to, or integrated within qualification frameworks (European Commission, 2020a).

In a similar way, the Council of the European Union (2022) defines micro-credentials as a “record of the learning outcomes that a learner has acquired following a small volume of learning.” These formal, non-formal or informal learning experiences resulting in learning outcomes are assessed by the provider or other recognized assessment providers with clearly defined,

transparent criteria to assure quality following certain standards that are agreed on in a specific sector or activity area.

In the context of digital credentials, there is a lot of literature, initiatives and projects regarding micro-credentials. Nevertheless, there is a widely varying understanding of the spectrum of micro-credentials, like Brown and colleagues (2021) exemplified in their credential-ecology framework. Kato and colleagues (2020) mention this broad spectrum for the size of micro-credentials and the connected learning setting in different OECD-countries. In the United States a micro-credential is a learning activity that is less than a full degree, but more than one single course. Furthermore, the extent also depends on the provider of the definition (Pickard, 2018). The New Zealand Qualifications Authority (2019) defines that micro-credentials can range from 5 - 40 credits, and also European countries vary in their understanding of the range of a micro-credential. In Austria, a micro-credential ranges from 3-15 ECTS (Bundesministerium für Bildung, Wissenschaft und Forschung, n.d.) and in Spain a micro-credential is defined as less than 15 ECTS (Agencia Nacional de Evaluación de la Calidad y Acreditación, 2022). In Denmark, a micro-credential is a small unit of learning with 1-2 ECTS (Danmarks Akkrediteringsinstitution, 2021), while Ireland defines credentials with a maximum of 30 ECTS as micro-credentials (Quality and Qualifications Ireland, 2021). This highlights the high variety of understandings of micro-credentials.

The Council of the European Union (2022) promotes European standard elements to describe a micro-credential. These elements include a) the identification of the learner, b) the title of the micro-credential, c) the country or region of the issuer, d) the awarding body, e) the date of issuing, f) the learning outcomes, g) the workload that is needed to achieve the learning outcomes, h) the level of the learning experience, i) the type of assessment, j) the form of participation in the learning activity, and k) the type of quality assurance used to underpin the micro-credential. These elements are described as mandatory and are complemented with optional elements that should be included where relevant: a) prerequisites needed to enroll in the learning activity, b) supervision and identity verification during assessment, c) grade achieved, d) integration and stackability options, and e) further information.

In addition to these standard elements, the European principles for designing and issuing micro-credentials include quality, transparency, relevance, valid assessment, supporting learning pathways, recognition, portability, learner-centering, authenticity, and incorporation of lifelong learning guidance services (Council of the European Union, 2022).

Micro-credentials are owned by the learner, who can store them and share them with a party of choice (portability) and combine them into larger credentials (stackability), which does not necessarily entitle the learner to a certain qualification or a degree, but can motivate learners and support more flexible learning pathways (UNESCO, 2022). According to Wolz and colleagues (2021), although micro-credentials can be referred to as “mini-certifications”, the focus lies more on the content and less on the replacement of traditional certificates.

○ 2.9. Nano-Credentials

A nano-credential represents a very small, specific set of skills or knowledge acquired through a brief learning experience. These credentials are designed to be highly focused and can often be completed in a matter of hours or days, as opposed to the weeks or months typically required for other forms of credentials, e.g. micro-credentials. In general, badges and nano-credentials represent the smallest unit of recognition of a learning activity, which can be just a single learning experience or a specific skill (West, 2023). Nano-credentials are often used to quickly demonstrate proficiency in a particular area or competency, making them valuable for both learners and employers seeking to address immediate skill gaps. Therefore, a nano-credential is smaller than a micro-credential with the ability to be stacked into micro-credentials (Pahuja, 2023).

○ 2.10. Conclusion

As highlighted above, the terminology of (digital) credentials is complex, since it has become a trending topic in research and practice, which results in different usage and definitions, depending on the context and the purpose of each credential. It is also very important to mention that most of the terms have a lot of overlapping shares in their meanings, as depicted in Figure 1.

● 3. Technological Aspects

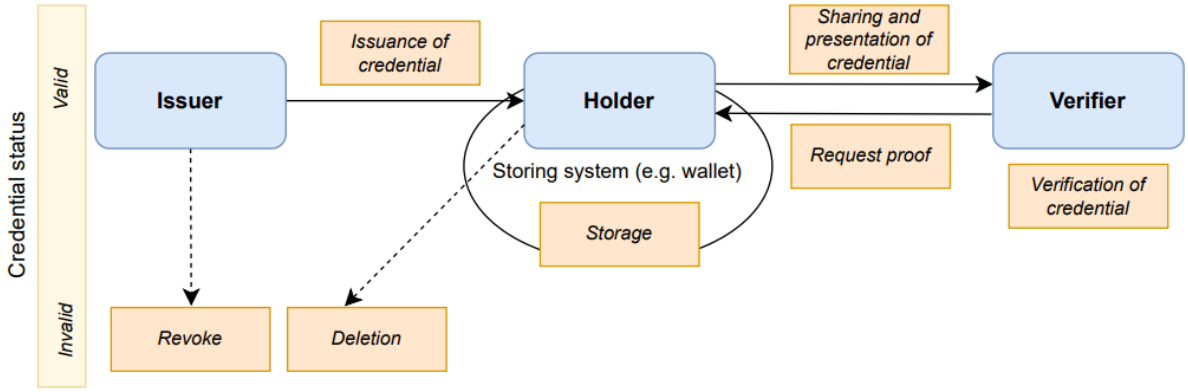
○ 3.1. Ecosystem of Digital Credentials

This section describes the roles of core actors (i.e., holder, issuer, verifier) and the general operation processes (i.e., issuance, storage, sharing, verification, revoking) within a digital credential ecosystem.

There are different actors that have specific roles within an ecosystem of digital credentials. The holder is the entity that possesses one or more verifiable credentials (e.g., a person) and generates presentations from them. The issuer is the entity that creates the verifiable credential (e.g., vocational training institution) by asserting claims about the subject and issuing the credentials to the holder. The verifier is the entity that requests information about a credential, and receives and verifies the verifiable presentation (e.g., employer) to make trust decisions based on the information it contains (World Wide Web Consortium, 2024b).

In the next sections, the general operation process within a digital credential system is explained, including the role of the actors described above and respective information flows within this process. In the following figure (Figure 2), the roles (blue), operation processes (orange) and information flows (illustrated with arrows) within a digital credentialing ecosystem are depicted.

Figure 2: *Roles, operation processes and information flows within a digital credential ecosystem*



3.1.1. Issuance

Issuing digital credentials is a process that involves the creation and distribution of electronic representations of qualifications, skills, or achievements. Digital credentials are typically issued by accredited institutions, such as universities, certification bodies, or governmental agencies. The issuance process begins with the assessment or verification of the individual's achievements or qualifications. This can involve a combination of document reviews, examinations, or practical assessments. Once confirmed, the issuing body creates a digital credential, which is signed and issued to the recipient (Chardrand et al. 2018).

3.1.2. Storing

After a digital credential is issued, the holder needs to store the credential, which includes the secure preservation and management of the credentials and is critical for ensuring the longevity, accessibility, and security. A commonly used possibility of storing digital credentials are digital wallets, which are applications that allow individuals to manage their credentials and share them as needed. These wallets use advanced cryptographic techniques to protect the credentials from unauthorized access and tampering. The storage solutions for digital credentials must address several key considerations, including security, privacy, interoperability, and user control (Sedlmeir et al. 2021).

Security is a paramount concern in the storage of digital credentials. Cryptographic methods, as described in chapter 3.2, are employed to ensure that the credentials remain secure and tamper-proof. Each credential is signed using the issuer's private key, and this signature can be verified using the issuer's public key, ensuring the credential's authenticity and integrity (Gräther et al., 2018). Additionally, digital wallets often implement multi-factor authentication (MFA) and encryption to further protect the stored credentials from unauthorized access (González et al., 2018).

Furthermore, protecting the privacy of individuals' credentials is crucial. Storage systems like digital wallets must ensure that the credentials are only accessible to authorized parties and that sensitive information is not exposed. Techniques such as zero-knowledge proofs allow individuals to share only the necessary

information without revealing all the details of their credentials. This approach enhances privacy by minimizing the exposure of personal data (World Wide Web Consortium, 2024b).

For digital credentials to be widely usable, they must be stored in a manner that ensures interoperability across different platforms and systems. Data models such as the Open Badges standard and the Verifiable Credentials standard facilitate this interoperability by providing a common framework for representing and exchanging credentials (Casilli & Hickey, 2016; World Wide Web Consortium, 2022b). These standards enable digital wallets to store credentials in a format that can be easily shared and verified by various entities, regardless of the underlying technology.

User control over digital credentials is another important aspect of their storage. Individuals must have the ability to manage their credentials, decide who can access them, and control what information is shared. Digital wallets empower users by providing a user-friendly interface for managing credentials and setting permissions for access and sharing. Self-sovereign identity (SSI) frameworks, described in chapter 3.2, further enhance user control by allowing individuals to own and manage their digital identities independently of any central authority (Allen, 2016).

3.1.3. Sharing

Before the respective credential can be verified by a verifier, the holder of a credential has to be able to choose if a credential should be sent and presented to a verifier. If the holder decides to share a credential or certain information, it must be possible to restrict the amount of information exposed and the duration for which the information is shared (World Wide Web Consortium, 2022b). To share their digital credentials, individuals can provide a direct link or a QR code that leads to their digital wallet or repository, where the credential can be viewed. The use of blockchain technology in digital credential systems ensures that these links are secure and that the credentials are tamper-proof (Grech & Camilleri, 2017). Aspects like standardizations and interoperability are essential in this operation step as well, since digital credentials need to be effectively shared across various platforms and institutions. Therefore, standardized formats for digital credentials, like the Open Badges specification (1EdTech, 2024a) evolved as standards in the context of digital credentialing systems. This standardization allows credentials to be shared and recognized across different systems and platforms, facilitating a seamless sharing process.

Similar to the process of storing, also the sharing of digital credentials raises important privacy and security concerns, since sensitive personal information is being handled. Therefore, also the respective legislation in the context of privacy needs to be respected. To name an example from Europe, the General Data Protection Regulation (GDPR) mandates that personal data must be processed with the individual's consent and protected against unauthorized access (EUR-Lex, 2016). Therefore, digital credential platforms must incorporate robust

security measures, such as encryption and secure authentication protocols, to protect user data during the sharing process.

3.1.4. Verification

The verification of a credential occurs when a third party, such as an employer or an educational institution, needs to validate the credential. The verifier can access the credential's metadata through a digital wallet or a secure online platform. Advanced technologies like blockchain (described in chapter 3.2.5) ensures that the credential's information is immutable and tamper-proof, providing a high level of trust in the verification process (Grech & Camilleri, 2017). The decentralized approach eliminates the need for intermediaries and reduces the risk of fraud (Chen et al., 2018). Furthermore, all credential transactions are publicly recorded and any attempt to alter a credential would be easily detectable. This transparency of blockchain also enhances trust among stakeholders and is essential for maintaining the integrity of the verification process (Grech & Camilleri, 2017).

For the verification process to be effective, digital credentials must adhere to standardized formats (e.g., Open Badges) that ensure interoperability across different platforms and institutions. This standardization facilitates the seamless sharing and verification of credentials across various systems, enhancing their utility and acceptance. The verification process must also address privacy and security concerns. Digital credentials often contain sensitive personal information, necessitating robust data protection measures. In Europe, according to the General Data Protection Regulation (GDPR), personal data must be processed securely and with the individual’s consent (EUR-Lex, 2016). Digital credential platforms must implement encryption, secure authentication protocols, and privacy-by-design principles to protect user data during the verification process (Digital Credentials Consortium, 2018).

3.1.5. Revoking

The revocation process typically starts when an issuing authority, such as an educational institution or a certification body, determines that a digital credential needs to be invalidated. This might be due to the expiration of the credential, the discovery of fraudulent activity, or if the credential holder no longer meets the required standards (Grech & Camilleri, 2017). The revocation process involves marking the credential as revoked in the credentialing system. In Blockchain technology, to revoke a credential, the issuing authority adds a new transaction to the blockchain that updates the credential’s status to "revoked" (Chen et al., 2018). This ensures that anyone attempting to verify the credential will see its revoked status, preventing its misuse.

○ 3.2. Technological Foundations

The evolution of digital credentials has necessitated the development and adoption of technology standards to ensure interoperability, security, trust, and widespread acceptance. These technologies are crucial for creating a reliable and cohesive ecosystem that supports the issuance, verification, storing and

sharing of digital credentials across various sectors and regions (Mühle et al., 2023).

In this section, relevant technological foundations that are based on cryptographic techniques are described. Cryptographic techniques are methods used to secure information and communications through the use of codes, ensuring that only those for whom the information is intended can read and process it. They are essential for securing data in digital communications, protecting privacy, ensuring the integrity and authenticity of messages, and securing transactions in various fields. Two relevant cryptographic techniques are symmetric and asymmetric encryption. Symmetric encryption involves the use of the same key for both encryption and decryption, while asymmetric encryption utilizes a pair of keys, one for encryption (public key) and one for decryption (private key) (Reynolds & Winks, 2021).

The techniques that are mentioned in the following chapters are not independent and standalone, but rather combined and relying on each other in a digital credential system in various ways. This interaction of technological foundations is highlighted at the end of this chapter in a figure (Figure 3), which shows an example of a blockchain-based system that can be used for operating and managing digital credentials.

3.2.1 Digital Signatures

Digital signatures are cryptographic techniques that are akin to handwritten signatures but far more secure. Digital signatures are a key application of a Public Key Infrastructure (PKI, described in chapter 3.2.3), allowing users to sign data with their private key (Menezes et al., 1996). To sign a digital credential, the issuer generates a hash of the credential's contents. This hash is a unique representation of the credential. The issuer then encrypts the hash with their private key to create the digital signature. This process binds the signature to the credential, ensuring that any alteration of the credential's content would be detectable. When a verifier receives a digital credential, they use the issuer's public key to decrypt the digital signature and retrieve the original hash. The verifier also independently generates a hash of the received credential's content. If the two hashes match, it confirms that the credential has not been altered and was indeed signed by the issuer, thereby validating its authenticity (Katz & Lindell, 2007).

3.2.2. Zero-Knowledge Proofs (ZKPs)

ZKPs are cryptographic techniques that enable one party to prove to another that a statement is true without revealing any additional information. In the context of verifiable credentials, ZKPs can be used to prove possession of certain attributes or qualifications without disclosing the actual data, thus enhancing privacy (Goldreich et al., 1986).

3.2.3. Public Key Infrastructure (PKI)

PKI is a framework for managing digital keys and it provides encryption by using asymmetric cryptography with the application of public key cryptography. Each

entity involved in the credentialing ecosystem is issued a pair of public and private keys by a trusted certificate authority (CA). The CA handles all aspects of credential management and confirms that the subject imprinted on the certificate is the owner of the public key. The public key is meant for public distribution and can be shared openly, while the private key is being kept secure by the owner. The public key is used to encrypt data in a way that only the owner can decrypt the data with the private key. Conversely, only the key pair owner can encrypt data using the private key. This ensures the authenticity of the sender to all recipients, for only the associated public key will decrypt the data (European Union Agency for Cybersecurity, n.d.).

Because of the binding of public keys to entities within a traditional PKI system, centralized identifiers play a crucial role, since PKI traditionally rely on them. Nevertheless, there is growing interest and development in integrating PKI principles with decentralized identifiers. This integration aims to combine the robust security and trust frameworks of PKI with the user-centric, decentralized nature of DIDs. The integration of DIDs into PKI frameworks represents a significant advancement, addressing some of the inherent limitations of traditional PKI systems (Bakhtina et al., 2023; Shi et al., 2022).

Centralized Identifiers

Centralized identifiers are unique identifiers, issued and managed by a centralized authority or organization and are widely used in many sectors, including education. Centralized identifiers are typically issued by a central authority, such as a government, educational institution, or corporation. The central authority's role is to ensure the uniqueness and validity of these identifiers. These identifiers are designed to be unique and persistent, meaning each identifier is assigned to a single entity and remains consistent over time. Examples include driver’s license numbers, student IDs, and employee numbers. This uniqueness and persistence are critical for maintaining accurate records and ensuring that the identifiers reliably link to the same entity over time. The verification process for centralized identifiers involves querying a central database maintained by the issuing authority. For instance, verifying a university degree might require checking the institution's records. While centralized identifiers offer structured and authoritative means of identification, they also present several challenges. The reliance on centralized databases can pose privacy risks, as these repositories may be vulnerable to breaches and misuse. Centralized systems can become single points of failure, where the compromise of the central authority can lead to widespread issues. Furthermore, users and relying parties must trust the issuing authority, which may not always be feasible in cross-border or inter-organizational contexts (Sedlmeir et al., 2021).

3.2.4. Self-Sovereign Identities (SSIs)

SSIs is a digital identity model that gives individuals control over their own identity data. Unlike traditional identity systems, where identity information is managed by central authorities such as governments or corporations (centralized), SSIs allow users to own, manage, and share their personal information independently. Personal data is stored in a decentralized manner, often using blockchain or

other distributed ledger technologies (described in chapter 3.2.5). SSIs are designed to be interoperable across different platforms and services, allowing users to use their digital identity across various systems without needing multiple logins or registrations (Preukschat & Reed, 2021).

Decentralized Identifiers (DIDs)

DIDs are fundamental to the concept of self-sovereign identity and represent a new type of identifier that is designed to enable verifiable, self-sovereign digital identities. Unlike traditional identifiers that are issued and controlled by centralized authorities, DIDs are created, managed, and owned by the individual or entity that they identify, without the need for an intermediary. DIDs are designed to be interoperable across different systems and platforms. They follow open standards to ensure that they can be used seamlessly in various digital ecosystems (World Wide Web Consortium, 2022a). DIDs enhance privacy by allowing users to control their identity information and share only the necessary details with others. The use of cryptographic techniques ensures the security of the identity data and protects it from unauthorized access and tampering. With the use of DIDs within the concept of self-sovereign identity, users have full control over their digital identities and can authenticate themselves without relying on third parties (Preukschat & Reed, 2021).

3.2.5. Blockchain and Distributed Ledger Technologies (DLTs)

DLTs are a broad category of technologies that encompass various systems (e.g., blockchain) that enable the decentralized issuance and verification of digital credentials. The core concept of DLT is the decentralized distribution of data among a network of participants, which reduces the need for a central authority. DLTs operate on a peer-to-peer network architecture where each participant (node) maintains a copy of the entire ledger. This decentralization is fundamental to the security and reliability of DLTs as it removes the risk of a single point of failure and enhances the resilience of a credentialing system (Narayanan et al., 2016; Zheng et al., 2017). Furthermore, decentralization enhances trust, as no single entity has control over the entire system (Yli-Huumo et al., 2016).

Blockchain is the most well-known type of DLTs and offers a decentralized and immutable record of transactions in blocks that are linked together in a chain. As the name implies, blockchain contains a chain of various data blocks. Each block contains a number of transactions. A transaction can involve physical goods as well as intangible assets (e.g., intellectual property) (El Ioini & Pahl, 2018). Blockchain's cryptographic hashing ensures that once a credential is recorded on the blockchain, it cannot be altered or deleted. Any attempt to change a credential would require altering all subsequent blocks, which is computationally impractical in a well-established blockchain network. This immutability is crucial for digital credentials, as it guarantees the integrity and authenticity of the credentials. (Yli-Huumo et al., 2016).

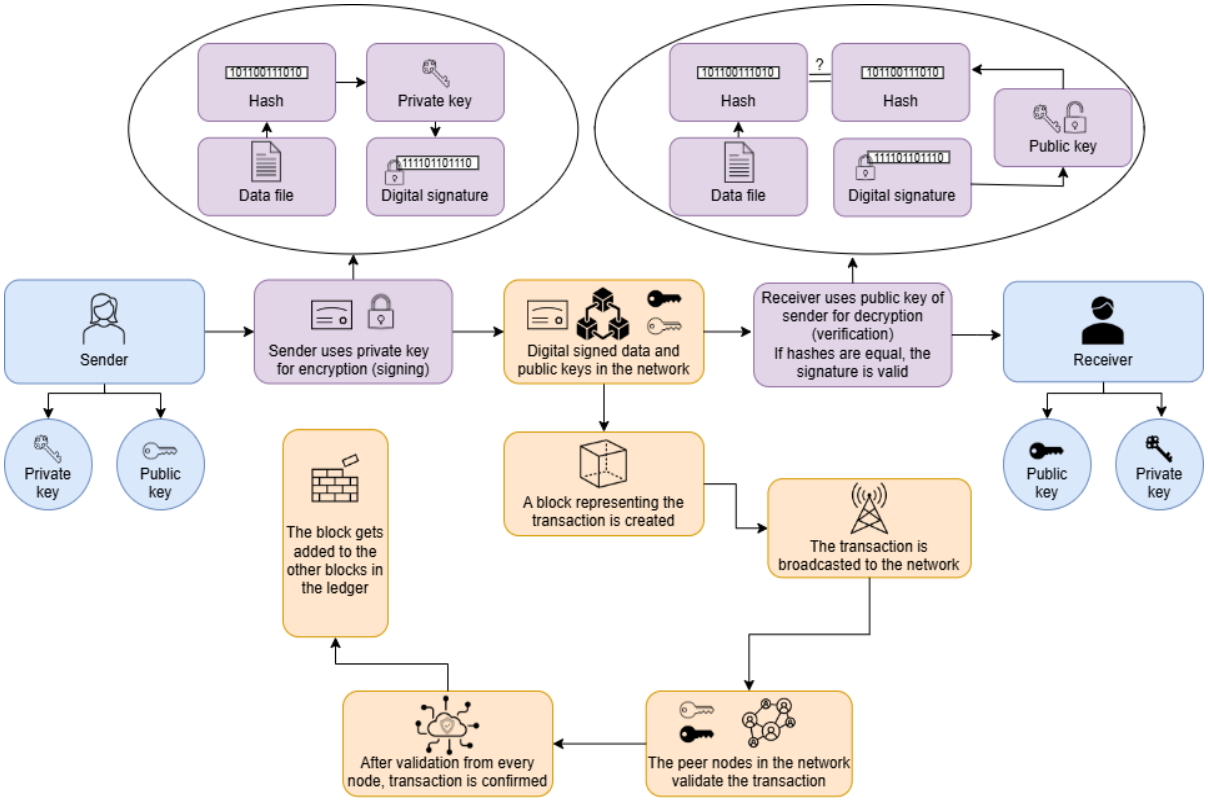
Blockchain technology has emerged as a robust and secure foundation for managing digital credentials, since its properties of decentralization,

immutability, and transparency make it particularly well-suited for this purpose (Grech & Camilleri, 2017). Furthermore, blockchain provides a transparent and publicly verifiable record of transactions. For digital credentials, this means that anyone can verify the authenticity of a credential by checking the blockchain. This public verifiability reduces the risk of fraud and enhances the credibility of the credentials (Narayanan et al., 2016).

“Blockcerts” was one of the first open standards that used blockchain technology to create, issue, and verify digital certificates (MIT Media Lab, 2016).

The following Figure 3 displays an example of a blockchain-based system and integrates the technological foundations described in the previous chapters.

Figure 3: *Operation process of a blockchain-based system*



○ 3.3. General Non-Functional Requirements

The technical implementation of a digital credential system has to consider technological as well as social requirements. Mühle and colleagues (2023) modeled the requirements of a digital credential system based on existing literature, a multitude of projects, and interviews with experts. In the following, this conceptual framework is described. It takes into account all-encompassing requirements consisting of seven categories.

- **Basic Functionality:** The basic functionalities of a digital credential technology consist of issuing, presenting, storing, verifying and revoking (Mühle et al., 2023).

- **Controllability:** Controllability describes the users need to control the basic functionalities. Beginning with the issuance process, it includes requesting credentials and issuance consent. After receiving the credential, the user also needs to control the subsequent use of it. This includes sharing consent, verifier restrictions as well as user notifications and deletion. This aspect also falls under the term of Self-Sovereign Identity (SSI), which centers on independence of third parties. It gives the user control over their own data (Mühle et al., 2023).
- **Privacy:** This aspect also overlaps with SSI-principles. One of the requirements is pseudonymization, which allows anonymity for the users, who are therefore not trackable through their information. In addition, data minimization and selective disclosure are relevant: Only directly relevant personal information should be stored and the users can decide for themselves which information should be revealed (Mühle et al., 2023).
- **Usability:** Another essential part for the educational sector is the consideration of convenience features for the user, as well as accessibility, which encompasses technical requirements and barrier-free options. Convenient features include the portability, which means being able to access the system from different devices as well as storage and backup solutions. Furthermore, the possibility of a visual representation (e.g., with digital badges) must be considered, in order to allow users to display the achievement (Mühle et al., 2023).
- **Security:** As already mentioned in previous chapters, security is a crucial aspect on many different levels. First of all credentials need to be tamper-evident to ensure integrity. Data protection further has to be considered on a system architecture level. Another important requirement is not only the validity of the credential, but the verification of the actors (learner and issuer) themselves to establish authenticity and trust in a digital credential ecosystem (Mühle et al., 2023).
- **Trust:** Besides security on a technical level, it is also important to consider trust on an organizational level, not only for the identifiers used for technical verification, but trust into the real identity of an organization. To maintain trust in the system it should be transparent and verifiable, following an open source mentality (Mühle et al., 2023).
- **Deployability:** To enable the stability and future-proofness of the system, the requirements of scalability, longevity, interoperability and integration have to be contemplated on a technical and procedural level (Mühle et al., 2023).

4. Global Development of Digital Credentials

One reason for the emergence of digital credentials in education and training is the general development of the education sector that aims for high quality vocational education, e.g., defined by the universal 2030 Agenda for Sustainable Development of the United Nations. In this agenda, 17 Sustainable Development Goals (SDGs) were decided, one of them being education with the overall goal to “ensure inclusive and equitable quality education and promote lifelong learning opportunities for all” (United Nations, 2022). This agenda leads the way towards a more flexible, inclusive and high quality education system all over the world.

New requirements and standards and the evolving needs of learners and employers in educational training resulted in technological advancements, new and more flexible learning paths and alternative learning settings. Parallel to this development, digital credentials emerged as a response to the limitations of traditional, paper-based certificates and began gaining traction in the early 21st century. The concept was popularized within informal learning settings, communities and among online platforms, where participants sought recognition for completing tasks or courses. In recent years, higher education institutions have increasingly embraced the usage of digital credentials as an addition to traditional degrees and certificates (UNESCO, 2022).

The possibility to also recognize smaller learning volumes allows learners to acquire specific skills that help to enhance employability and career advancement prospects. Therefore, digital credentials also gained interest in vocational training, since the development of targeted skills is an important factor in fast changing working environments and for dynamic needs of the labor market to ensure adaptability, flexibility and quality of work. The following chapters give an overview of regional and international developments, as well as public and private providers for digital credentials and credential management. The section concludes with advantages and challenges of digital credentials. The mentioned developments, initiatives, projects and infrastructures serve as examples. Since digital credentials are a rising topic in education and elsewhere, there is no claim to give a complete report on current developments, but rather to show various aspirations with different focuses to highlight the high variety and widespread scope of developments in the context of digital credentials.

4.1. Europe

Europe has been at the forefront of developing and implementing digital credentials to enhance educational and vocational mobility, transparency, and recognition. The development in Europe is enhanced by important frameworks and initiatives from the European Union, that aim to create a standardized, secure, and interoperable environment for the issuance, recognition, and verification of digital credentials across the continent. This section describes

general regulations and exemplary initiatives and frameworks that accelerate the development and simplify the use of digital credentials in Europe.

4.1.1. Legislation

The legislation around digital credentials in Europe is largely influenced by the European Union's initiatives to create a more integrated and digitalized educational and professional environment. However, there might be additional regulations on a national level. These regulations vary widely between different member states, also depending on the sector where digital credentials are being used (e.g., healthcare, education, finance etc.). In the following, two relevant regulations for Europe are described that serve as a basis for national developments in Europe.

General Data Protection Regulation (GDPR)

GDPR is a critical piece of legislation that impacts the handling of digital credentials. It sets stringent requirements for the protection of personal data, which includes information contained in digital credentials. Issuers of digital credentials must ensure that personal data is processed lawfully, transparently, and securely. GDPR is a regulation that directly applies to all EU member states. Compliance is mandatory, and all countries are required to implement and enforce its provisions. National data protection authorities in each country oversee compliance and can impose penalties for violations. However, the level of enforcement and public awareness can vary between member states (EUR-Lex, 2016).

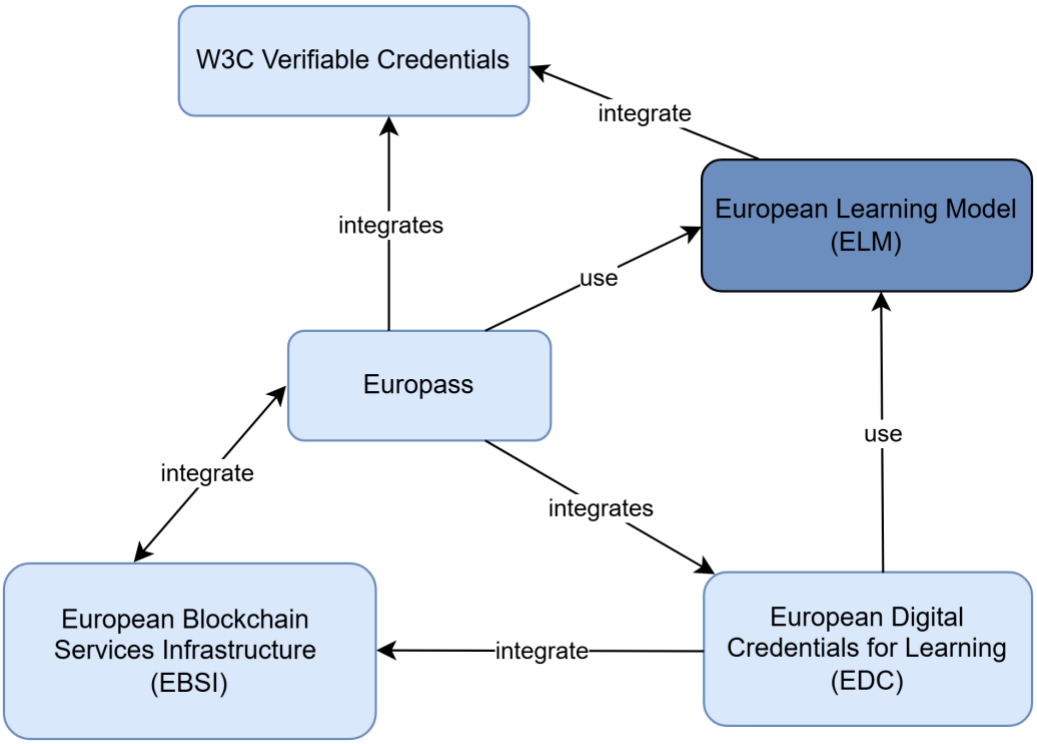
eIDAS Regulation

The eIDAS (electronic Identification, Authentication and trust Services) Regulation establishes a European framework for electronic identification and trust services. It provides the legal recognition for electronic signatures, seals, timestamps, and other trust services, which are essential for the validity and trustworthiness of digital credentials. The eIDAS Regulation is directly applicable in all EU member states and sets a framework for electronic identification and trust services. While all countries must comply with its requirements, the level of adoption and integration of eIDAS services can differ. Some countries have advanced digital identification systems and trust services, while others are still developing their infrastructure (European Commission, 2024).

4.1.2. Exemplary initiatives and infrastructures

In the following chapters, relevant European initiatives, models and infrastructures are described. They are connected and complementary, which shows the following figure (Figure 4).

Figure 4*: Synergies of European initiatives, frameworks and infrastructures*



Note: Adapted from Europass (2023).

European Learning Model (ELM)

The European Learning Model (ELM) is a comprehensive framework designed to support the recognition, validation, and accreditation of learning achievements across Europe. It aims to ensure that learning outcomes, qualifications, and skills are uniformly understood and accepted across different European countries, facilitating mobility and lifelong learning (European Commission, 2018).

The ELM emphasizes the importance of clearly defined learning outcomes, which are statements of what a learner is expected to know, understand, and be able to do after completing a learning process. These outcomes are standardized to ensure consistency and transparency across different educational and training systems (European Commission, 2018). The model promotes a competency-based approach, where the focus is on the actual skills and competencies acquired rather than the time spent on learning. This approach supports personalized learning pathways and recognizes both formal and informal learning experiences. This ensures that skills and competencies acquired outside of traditional educational institutions, such as through work experience or community activities, are acknowledged and valued (CEDEFOP, 2019). The ELM is closely linked to the European Qualifications Framework (EQF), which provides a common reference framework to compare the qualifications of different countries. The EQF uses eight reference levels, based on learning outcomes, to facilitate the recognition and transferability of qualifications across Europe (European Commission, 2018).

The ELM supports the use of digital tools and platforms to document and share learning achievements. This includes the use of digital credentials and badges that can be easily verified and recognized across borders, enhancing the transparency and portability of qualifications. The ELM is built on the specification of W3C Verifiable Credentials (European Commission, 2020b).

European Digital Credentials for Learning (EDC)

This initiative is part of the European Commission's broader effort to promote digital education and mobility across Europe. The European Digital Credentials for Learning framework allows educational institutions to issue digital diplomas and other learning credentials that are tamper-proof and can be easily verified across borders. This system is supported by the Europass framework, which aims to standardize and simplify the recognition of qualifications and skills across the EU. The adoption of European Digital Credentials for Learning is an ongoing process. While the framework provides guidelines and tools for standardization, the extent to which each country has integrated these credentials into their educational systems can differ. Some countries are early adopters and have made significant progress, while others are still in the initial stages of implementation (European Union, n.d.).

Europass

Europass is an initiative of the European Union designed to enhance the transparency and portability of skills and qualifications across Europe. It was established by the European Parliament and the Council in 2004 as part of the EU´s efforts to promote lifelong learning and mobility within the labor market. The initiative emerged from the Copenhagen Declaration of 2002, which emphasized the need for enhanced cooperation in vocational education and training across Europe. Europass provides a standardized framework for presenting qualifications, skills, and experiences, thereby facilitating mobility for learners and workers across member states (European Union, 2004). Updated in 2020, the Europass framework provides tools for documenting and sharing information on skills and qualifications. It includes the Europass Digital Credentials Infrastructure (EDCI), which enables the issuing, sharing, and verification of digital credentials in a secure and interoperable manner. This framework ensures that digital credentials are consistent and recognizable across member states (European Commission, 2023). The Europass framework is widely adopted across EU member states. It provides a standardized format for documenting and sharing qualifications and skills, making it easier for individuals to present their credentials across borders. Most countries have set up national Europass Centers to facilitate the use of Europass tools and resources (European Commission, 2023).

Europass consists of different tools that support individuals in their learning and career development: The “Europass CV” is a comprehensive curriculum vitae format that allows individuals to systematically present their skills, qualifications, and experiences. The “Europass Language Passport” is a tool for self-assessing language skills and qualifications. “Europass Mobility” is a record of the skills and knowledge acquired in another European country through work placements,

internships, or other learning experiences. The “Europass Certificate Supplement” provides additional information to that included in official certificates, making it easier to understand the nature and level of qualifications. Finally, the “Europass Diploma Supplement” supplements higher education diplomas by providing a standardized description of the nature, level, context, content, and status of the studies completed. These Europass tools and documents can be accessed and completed online through the Europass portal. The portal also integrates various services such as job searching tools and information on learning opportunities, making it a comprehensive platform for career management and educational planning (European Commission, 2023).

Europass offers several key benefits. First of all, it provides a unified and standardized format for presenting qualifications and skills, facilitating the comparison of credentials across different countries. It is available in multiple languages, ensuring that individuals from different linguistic backgrounds can utilize the tools effectively. Furthermore, the portability is an important benefit, since it supports mobility by allowing individuals to present their qualifications in a manner that is easily understood and recognized across member states. Europass enhances trust in the authenticity and validity of qualifications through standardized documentation and digital verification processes, and it assists individuals in planning and managing their careers by providing tools to document and present their skills and qualifications comprehensively (European Commission, 2023).

European Blockchain Services Infrastructure (EBSI)

The European Blockchain Services Infrastructure (EBSI) is an initiative launched by the European Commission and the European Blockchain Partnership (EBP) to leverage blockchain technology in providing cross-border public services across Europe. EBSI aims to create a secure and trusted digital infrastructure that can be used to enhance the efficiency and transparency of digital services within the European Union. To ensure transparency, security, and immutability of data, EBSI uses blockchain and operates through a network of nodes managed by various European countries. Each node in the network maintains a copy of the blockchain, ensuring reliability (European Commission, n.d.-b).

One of EBSI's core objectives is to facilitate interoperability between different blockchain platforms and traditional IT systems. This is crucial for integrating blockchain services with existing administrative processes and for ensuring smooth cross-border data exchanges. One of the primary use-cases of EBSI are academic credentials that are issued and verified on the blockchain. EBSI supports self-sovereign identity (SSI), which allows students to own and control their digital identity and credentials. Students receive their diplomas in a digital wallet, where they can manage and share their credentials as needed. Various pilot projects have been conducted to test and refine the Diploma Use Case. These pilots involve multiple universities and educational institutions across different EU member states, providing valuable insights and feedback to improve the system (European Commission, n.d.-b).

EBSI's governance is managed by the European Blockchain Partnership, which includes representatives from member states and the European Commission. This partnership sets the strategic direction, oversees implementation, and ensures that the infrastructure aligns with EU regulations and policies. It also collaborates with standardization bodies to ensure that its solutions are compatible with global blockchain standards (European Commission, n.d.-b).

○ 4.2. Latin America

This section provides an overview of key developments surrounding digital credentials within Latin America. By examining key initiatives, this section aims to provide a foundational understanding that will support the successful adoption and integration of digital credentials in professional contexts in this region, as intended by the project ECOCredGT (ECOCredGT, n.d.).

4.2.1. Legislation

The legislative environment for digital credentials in Latin America is varied, reflecting the diverse educational policies and technological infrastructures across different countries.

Specifically in Guatemala, to the authors´ knowledge there is no specific legal framework dedicated to digital credentials. However, there are existing laws that may apply to personal data processing. Notably, the Law on Access to Public Information, although primarily intended for State entities or those funded by the State, contains provisions that can be interpreted to apply to any form of personal data processing, including by private entities. Additionally, there have been proactive ambitions in this area, initiating significant legal actions against entities that process personal data. This has led the Constitutional Court to issue several rulings, consistently affirming the protection of data subjects. These rulings recognize the rights of data subjects in data processing contexts, including informed consent, access, rectification, cancellation, and opposition. Furthermore, any transfer of personal data, whether local or international, requires the data subject's consent, provided in writing or in a digitally retrievable format (OneTrust, 2024).

Guatemala is progressing towards digitization, but faces administrative and cultural challenges, according to a United Nations Development Program (UNDP) blog post. The blog highlights Guatemala's involvement with the UNDP’s Digital Readiness Assessment (DRA), which aims to foster inclusive digital transformation by engaging a wide range of stakeholders, including government, businesses, civil society, and academics. Guatemala performed well in areas such as connectivity, political leadership, and public engagement, but faces challenges common to global digitization efforts. Regulatory issues, particularly in data protection and e-commerce, were identified as critical areas needing improvement. Additionally, gaps in existing legislative frameworks could hinder successful digital transformation.

A significant challenge lies in Digital Public Infrastructure (DPI), including data exchange, digital payments, and the national digital ID. Despite progress, issues such as data management and the lack of digital skills and technical capacity are barriers to widespread DPI adoption.

The UNDP recommends Guatemala to adopt a sustainable DPI approach, emphasizing robust governance, gender-responsive measures, and rights-based inclusivity. Improving connectivity and adopting a people-centered design approach are also key to ensuring successful digital transformation in the country (Biometrics Research Group, 2023).

4.2.2. Exemplary Initiatives and Infrastructure

Regional developments in Latin America in the context of digital credentials in education are currently more focused on academic institutions. However, there are also some advanced examples of digital credential systems outside the academic world. In the following chapters, some exemplary initiatives and infrastructures are described. This is not all-encompassing, but rather a selection that should reflect the broad range of developments in the context of digital credentials in Latin America.

Academic Institutions

As already mentioned, there are several developments in the sector of higher education. To mention some national examples, the university “Tecnológico de Monterrey” (Tec de Monterrey), one of Mexico's leading universities, has implemented a digital credentialing system to enhance the recognition and portability of academic achievements. The university uses blockchain technology to issue secure, tamper-proof diplomas and certificates, making verification easier for employers and other educational institutions (Tecnológico de Monterrey, 2023).

The university “Universidad Nacional de Córdoba”, one of Argentina's oldest and most prestigious universities, has started issuing digital badges to recognize students' participation in workshops, seminars, and extracurricular activities. These badges are designed to complement traditional academic records and provide a more comprehensive view of students' skills and achievements (edX, 2024).

The university “Universidad de Chile” has developed a digital certification platform to issue and verify academic credentials. This platform uses secure digital signatures and a centralized database to ensure the authenticity and integrity of diplomas and certificates, facilitating their acceptance both nationally and internationally (Universidad de Chile, n.d.).

The university “Pontificia Universidad Católica del Perú (PUCP)” has expanded its online learning offerings and integrated digital credentials to recognize the completion of courses and programs. This approach supports lifelong learning and provides students with verifiable proof of their achievements that can be shared with employers and other educational institutions (PUCP, 2024a). Furthermore, they also offer various training programmes with digital

certifications in the field of vocational and educational training for companies (PUCP, 2024b).

Professional Institutions

In Brazil, the National Service for Industrial Training (SENAI), which is the largest private technical and vocational education center in Latin America, has launched an initiative to provide micro-credentials for various vocational and technical courses. This program aims to meet the evolving needs of the labor market by offering flexible, modular learning opportunities that can be easily verified and recognized by employers (Confederação Nacional da Indústria n.d.).

The National Training Service (SENA) in Colombia has embraced blockchain technology to issue digital certificates for its vocational training programs. SENA is a Colombian public institution offering free vocational and technical training to about 9 million Colombians each year. As the country's largest public institution, SENA has comprehensive national coverage through 117 industry-specific training centers and an extensive online platform. Its mission is to cultivate and expand a technically skilled workforce to meet the demands of Colombia's national development and a growing international economy (100.000 Strong in the Americas, 2024).

IDB Digital Credential Framework for Creating and Issuing Credentials

Since 2018 the Inter-American Development Bank (IDB), which describes itself as “the main source of development financing for Latin America and the Caribbean" (IDB, n.d.) rewards different learning opportunities with digital credentials. In 2023, they established a roadmap to recognize knowledge building and learning with digital credentials with clear principles and guidelines for the creation and issuance of such credentials, not only for the IDB Group, but also for organizations and citizens of the LAC-region. As of January 2023, IDB has issued more than 200.000 digital badges. This initiative aims to promote student and worker mobility within Latin America and the Caribbean by creating a unified framework for digital credentialing and therefore acts as a pioneering initiative in the context of digital credentials in the LAC-region (Porto & Presant, 2023).

○ 4.3. International Developments

The international landscape of digital credentials is characterized by a mix of governmental initiatives, projects, and private sector innovations. Furthermore, standard formats like the Open Badges specification and W3C Verifiable Credentials are used globally by educational institutions, professional organizations, and online learning platforms to recognize a wide range of skills and achievements and to provide a standardized format for creating, issuing, and verifying digital credentials (1EdTech, 2024a; World Wide Web Consortium, 2022b). In the following chapters, exemplary international initiatives, networks, and standards are described.

4.3.1. Digital Credential Consortium (DCC)

The Digital Credentials Consortium (DCC), which was founded in 2019 is an example for an initiative, which includes partners worldwide, from Europe, the United States, Canada and Mexico. They are building an infrastructure for digital academic credentials to support the future education systems. DCC is exploring the possibilities of recent developments in credential data standards and cryptographic methods for recognition in academic achievements and providing various resources in this context. Furthermore, they are designing a governance system, as well as a technology infrastructure for academic credentials. All of the developed software is open source, which supports the issuing of credentials for organizations (MIT Open Learning, 2024).

4.3.2. Groningen Declaration Network

The Groningen Declaration Network is an international, nonprofit network of individuals and organizations that focus on digital student data portability, building on the Groningen Declaration. Today the network consists of participants and signatories of over 29 countries worldwide. The purpose of the Groningen Declaration Network is to develop, offer, support, and advise on Digital Student Data Portability (DSDP), particularly focusing on mutual consultation and information exchange among interested parties worldwide, especially higher education institutions. They want to develop and promote best practices and globally accepted standards for safe, citizen-oriented consultations and information exchanges on DSDP. The Network seeks to achieve its objectives by creating and facilitating a network aligned with the foundation's goals, bringing together stakeholders in the field of DSDP, utilizing multimedia for the foundation's purposes, generating publicity by any means to support the foundation's objectives, acquiring and providing resources, and engaging in any activities directly or indirectly related to these objectives (Groningen Declaration, n.d.).

4.3.3. Credential Engine

Credential Engine is a non-profit organization that originated from the Credential Transparency Initiative (CTI) in 2013. CTI aimed to develop a centralized registry of credential information, create a common credentialing language, and build a credential search engine. In December 2016, Credential Engine was officially established to implement CTI's work. Credential Engine is dedicated to map the credential landscape by providing clear and consistent information. Its mission is to empower individuals to discover the best pathways for their needs. Credential Engine offers a range of web-based services, including the first centralized Credential Registry that houses current information about all types of credentials and provides standardized data on the attributes of credentials, such as their competencies, costs, and outcomes, making it easier for learners, educators, employers, and policymakers to understand and compare them. It also provides the Credential Transparency Description Language (CTDL), a common description language that facilitates credential comparability and enhances quality assurance, and a platform for developing customized applications to search and retrieve credential information. Credential Engine works with

learners, credential providers, employers, as well as policy-makers to help them understand the value of digital credentials (Credential Engine, 2024).

4.3.4. Digital Credentials Monitor

The Digital Credentials Monitor is a joint initiative from the German Academic Exchange Service (DAAD), the Groningen Declaration Network (GDN) and UNESCO and has the aim to create a collaborative knowledge source for digital credentials in education all over the world. The main goal of this initiative is to collect data regarding initiatives, pilots, projects, best practices, and implemented technological infrastructures from all over the world to conduct analyses and depict the results within a visual tool. Furthermore, these results should lead to new perspectives on digital credentials in different countries and open up a space for discussions and exchanges. The creation of the visual tool is community-based, where data can be added individually through an online survey (Deutscher Akademischer Austauschdienst e.V., 2023, 2024).

4.3.5. World Wide Web Consortium (W3C) and Verifiable Credentials

The World Wide Web Consortium (W3C) is an international non-profit organization that develops recommendations (web standards, technical specifications, and guidelines) within a community: over 350 member organizations from around the world, staff, and the public (World Wide Web Consortium, 2024a).

In the context of digital credentials, the open standard “Verifiable Credentials Data Model v2.0” might be considered as one of the most important international developments. The latest version was published in 2024 and the specification aims to provide a standardized method for expressing credentials on the web (such as driver's licenses, university degrees, and passports) in a manner that is cryptographically secure, privacy-respecting, and machine-verifiable. It builds upon previous versions by enhancing the security and privacy features, addressing issues like device theft and impersonation, and providing detailed guidelines for accessibility and internationalization. It includes comprehensive sections on the components of verifiable credentials and presentations, an ecosystem overview, and privacy considerations. There are different roles within this specification: the issuer, the holder, and the verifier, as described in chapter 3.1. A verifiable credential contains information about the credential subject (e.g., a person), the issuer (e.g., a government body), the claims being made (e.g., the subject's age), and proofs (e.g., digital signatures) to ensure the integrity and authenticity of the credential. It may include data such as pictures, names, identification numbers, type of credential, issuance date, and expiration date. The data model supports privacy-preserving techniques, such as zero-knowledge proofs, which allow the holder to prove a statement without revealing all the underlying data. Furthermore, the specification includes guidelines to ensure that credentials are accessible to a broad range of users and can be used internationally, e.g. with support for different languages. The model aims to make digital credentials more trustworthy and easier to manage, compared to their

physical counterparts. Furthermore, comments from the community and the implementation of feedback for this specification is actively seeked by W3C (World Wide Web Consortium, 2024).

4.3.6. 1EdTech, Open Badges and Comprehensive Learner Record (CLR)

1EdTech is an organization with over 900 member organizations in more than 32 countries around the world. This collaborative community is dedicated to creating an open, reliable, and innovative educational technology ecosystem that addresses the lifelong learning needs of every individual. 1EdTech wants to empower all stakeholders to actively contribute to enhancing educational opportunities and experiences for the benefit of society (1EdTech, 2024b).

In the context of digital credentials, one of the most important developments is the “Open Badges Specification”. It describes a norm on how information about acquired achievements is aggregated and embedded in a file as a digital badge. Furthermore, it defines procedures for verifying badge authenticity and an API for exchanging badge information. Using this standardized format ensures the interoperability, verifiability and portability of digital badges. The main stakeholders of the specification are the badge earners, whose achievements are represented by the badges. The badge issuers define, assess, and provide the achievement through the badges. A badge viewer is everyone that looks at the badges to understand the learner's achievement, for example educators or employers. Furthermore, there are badge endorsers who are beneficial to examine and acknowledge the value of the badges. The latest version of this standard is the “Open Badges 3.0 specification” with the extension of blockchain technology and decentralized identifiers compared to previous versions. It aligns with the conventions of the Verifiable Credentials Data Model v2.0 (1EdTech, 2024a).

Another important technical specification established by 1EdTech for global use is a standard for lifetime learning records, called the Comprehensive Learner Record (CLR). This standard supports the recognition of a wide array of academic and workplace accomplishments, including courses, competencies, skills, and employer-based achievements. It is designed to be user-friendly and intended for use, curation, and control by the learner. It provides an interoperable and web-friendly format that is easy to understand and flexible enough to support various use cases. This adaptability ensures that it meets the diverse needs of learners, workers, registrars, and employers. Digital credentials produced with the format of W3C Verifiable Credentials or Open Badges are easily bundled into CLRs (1EdTech, 2024c).

At the core of both, Open Badges and CLR is the concept of an assertion about one or more achievements. These assertions are specific to one learner and include claims about a particular achievement, along with metadata such as issuer, learner, date of achievement, expiration date, as well as potential evidence supporting the claim (1EdTech, 2024c).

The CLR allows for the bundling of multiple credentials and creating associations among them. This can be visualized as adding another layer around the credentials, which are also verifiable individually. CLRs can include achievements from various issuers, reflecting a learner's progression across different organizations or departments within a large educational institution. Furthermore, issuers can group multiple related credentials into transcripts and other comprehensive records within a CLR, known as a ClrCredential. This ClrCredential is signed in the same manner as individual credentials, ensuring authenticity. Furthermore, credentials can be enhanced with an EndorsementCredential from a third party, adding another layer of validation and support to the quality or relevance of the credential data (1EdTech, 2024c).

4.3.7. Blockcerts Standard

Since blockchain technology evolved as a well suited and commonly used technology for the management of digital credentials, standardization is also relevant in this context. The Blockcerts standard is an open standard for creating, issuing, viewing, and verifying blockchain-based certificates. It was developed by the MIT Media Lab in collaboration with Learning Machine, now Hyland Credentials (Hyland, 2024). Hyland is continuing the ongoing development as the primary steward of this project.

The Blockcerts standard leverages the blockchain's capabilities to provide a secure and tamper-proof method for handling digital credentials. Its code and documentation are open source, which encourages the widespread adoption and collaboration, allowing developers and institutions to build on and improve the standard. While initially designed to work with the Bitcoin blockchain, Blockcerts is blockchain agnostic, meaning it can be implemented on any blockchain platform. This flexibility allows institutions to choose the blockchain that best suits their needs and preferences. Other key components of the standards are interoperability, enhanced security by leveraging immutable ledgers, and decentralized verification. Blockcerts empowers recipients by giving them ownership of their digital credentials. Individuals can store their certificates in digital wallets and share them as needed, controlling who has access to their information.

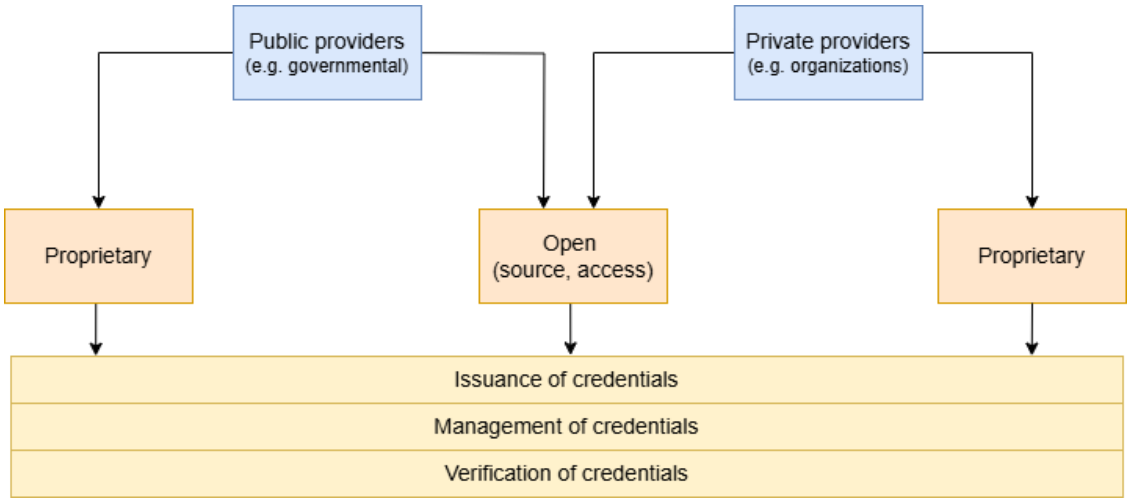
Blockcerts has been adopted by various educational institutions, professional organizations, and certification bodies worldwide. It has the potential to streamline credentialing processes, reduce fraud, and empower individuals with greater control over their achievements. The goal is to create technical resources that other developers can utilize in their own projects. By providing a reliable and verifiable method for issuing and sharing digital certificates, Blockcerts supports the broader adoption of blockchain technology in education and beyond (MIT Media Lab, 2016).

○ 4.4. Providers

Providers are essential in a digital credential ecosystem because they can facilitate the issuance, management, verification, and recognition of digital

credentials. They help to ensure that credentials are secure, trustworthy, and recognized across various sectors. There is a wide range of public and private providers for digital credentialing. The choosing of a provider depends on various factors including the nature of the credential, its intended use, the level of trust and recognition required, and organizational preferences (UNESCO, 2018).

Figure 5: *Provider of a digital credential (system)*



4.4.1. Public Providers

Public providers are typically government or state-backed and issue digital credentials for official purposes. They enforce standards, so that credentials meet specific legal, privacy, and security requirements. Therefore, they are widely recognized across different sectors and through international borders. Due to their legal weight, trust and legitimacy can be mentioned as main advantages. Furthermore, they help to create standardized frameworks for credentialing to ensure consistency and interoperability. On the other hand, due to bureaucratic structures, they might also be slower in adapting new technologies (UNESCO, 2018).

Public providers are connected to or operated by the government and often issue digital credentials nationwide or in a certain region. These include the ministries of education of the respective countries, other regulating authorities (e.g., Australian Skills Quality Authority), or public universities.

4.4.2. Private Providers

Private providers include non-governmental organizations and companies (e.g. professional organizations, technology companies). They are market-driven and compete with other providers. They often have a focus on specific sectors, for example tech certifications. One of the benefits of private provides is their flexibility and adaptability to the needs of the industry and they can offer customized solutions as well as innovative technologies. However, credentials from private providers may not always have the same level of recognition or trust

as those from public entities (UNESCO, 2018). In the following, an overview of established private providers is presented.

Educational Institutions and Online Learning Platforms

- **Coursera:** Coursera is an online learning platform that offers courses, specializations, degrees as well as digital certificates for universities and companies worldwide. It is partnered up with institutions like Stanford, Yale, and Google to provide a wide range of subjects in their courses (Coursera, 2024).

- **edX:** EdX is a well-known massive open online course (MOOC) provider founded by Harvard and MIT. It offers university-level courses in a wide range of disciplines, including free courses and programs for professional certifications, micro-credentials, and full online degrees (edX, 2024).

- **FutureLearn:** FutureLearn is a MOOC platform based in the United Kingdom, that offers online courses and degrees from universities and cultural institutions around the world. It provides a social learning experience and opportunities to earn certificates and micro-credentials (FutureLearn, 2012).

- **LinkedIn Learning:** LinkedIn Learning offers a vast library of video courses in software, creative, and business skills. It is integrated with LinkedIn profiles, allowing users to display completed course certifications (LinkedIn Learning, 2024).

- **Udacity:** Udacity focuses on technology, offering "Nanodegree" programs designed to train individuals in fields like programming, data science, artificial intelligence, and digital marketing. It collaborates with industry leaders like Google and IBM to design its courses (Udacity, 2011).

Professional Organizations and Companies

- **CompTIA**: The Computing Technology Industry Association (CompTIA) is an advocate for the global information technology ecosystem. They support industry growth through education, training, certifications, and market research, aiming to develop a highly-skilled workforce and promote an environment conducive to innovation. It has awarded over 2.5 million certifications in areas such as cybersecurity, networking, cloud computing, and technical support. CompTIA also maintains an international partner program with thousands of academic institutions, not-for-profits, job corps centers and other organizations (CompTIA n.d.).

- **Credly:** Credly is a digital credentialing platform that works with organizations to issue, manage, and verify digital credentials and badges. It supports various industries and integrates with learning management systems (Credly by Pearson, 2024).

- **IBM:** IBM provides digital credentials through its IBM Digital Badge Program, which recognizes skills and achievements in areas such as

cloud computing, AI, and cybersecurity. These badges are designed to showcase verified skills and are recognized within the industry (IBM, n.d.).

- **Microsoft:** Microsoft collaborates with industry and educational partners to provide digital credentialing solutions. Through its Azure cloud platform, Microsoft supports the development of verifiable credentials that can be securely shared and verified (Microsoft Security, 2024).

4.5. Advantages and Possibilities of Digital Credentials

As already highlighted in previous chapters, there are a lot of possibilities and advantages in using digital credentials. In addition to encouragement in engaging in learning activities, also building and engaging with the community is an important benefit of digital credentials. Different studies show that the online sharing of badges and earned micro-credentials motivates learners. In addition, instructors and educators engage with the community as well, so that badges can assist in the standardization of credentialing criteria and curricula and in the forming of a collaborative instructional community (Stefaniak & Carey, 2019; Carey & Stefaniak, 2018).

Another benefit of digital credentials is their enhanced security compared to traditional paper-based credentials. Digital credentials use cryptographic techniques to prevent tampering and ensure that the information remains unchanged and verifiable (Gräther et al., 2018). The use of blockchain technology further enhances security by providing a decentralized and immutable ledger that records the issuance and verification of credentials. Each credential is assigned a unique identifier, making it nearly impossible to alter or forge (Sharples & Domingue, 2016).

The interoperability of digital credentials is another significant advantage. Digital credentials can be designed to be compatible with various standards and systems, facilitating their use across different platforms and jurisdictions. This interoperability is crucial for individuals who need to present their credentials to employers, educational institutions, or government agencies in different regions or countries. Standards, such as the Open Badges specification, provide a framework for the creation, issuance, and verification of digital credentials, ensuring that they can be widely recognized and accepted (Casilli & Hickey, 2016).

The European Union describes benefits for different stakeholders: Individuals, employers and education and training providers. Individuals can build an online portfolio to track all of their learning achievements, while being in full control of their data. They can easily reuse their credentials to apply for a job or for further training, and they can present and have their credentials verified at any point in their career. Employers can significantly reduce the time and cost of verifying credentials and processing job applications. They can better understand the credentials of candidates, especially from other member states as they will be translated in their own language and they can trust tamper-proof credentials.

Education and training providers can reduce their administrative burden and the costs for issuing credentials, while also accelerating issuing procedures by going digital (European Union, n.d.).

○ 4.6. Implications and Challenges

By leveraging technologies such as blockchain and PKI, verifiable digital credentials offer enhanced convenience. However, addressing the challenges of security, privacy, interoperability, and adoption is crucial for realizing their full potential.

For digital credentials to be widely accepted, they must be interoperable across different systems and platforms. Standards for formats, technologies and quality assurance are essential for ensuring that credentials issued by different organizations can be easily understood and verified globally

Another challenge is the lack of awareness and understanding among stakeholders, resistance to change from traditional credentialing systems, and the need for robust legal frameworks to support digital credentials' validity and recognition (van der Hijden & Martin, 2023). Furthermore, due to the high relevance and focus on digital credentials in research and practice, even more initiatives, projects, infrastructures, guidelines and recommendations will emerge. This can result in a difficulty to maintain a clear view in this complex landscape. To avoid overburdening of learners, as well as possible future providers or other stakeholders, ongoing and future initiatives, projects, and networks need to work together to form collaborative and widely accepted solutions and outcomes for digital credentialing.

● 5. Conclusion

This state of the art report has provided a broad overview of digital credentials with a focus on education and vocational educational training. In defining digital credentials, we explored various understandings and meanings of digital credentials and related terms and concepts. This is crucial for understanding the landscape and potential impact of digital credentials.

By outlining the operation process of a digital credential ecosystem and the foundational technologies that enable secure and verifiable digital credentials, such as blockchain and public-key infrastructure, we highlighted the mechanisms that ensure the integrity and trustworthiness of digital credentials. Furthermore, we addressed critical non-functional requirements like security and privacy.

The section on global developments showcased significant initiatives and advancements in the context of digital credentials, with a focus on European initiatives and current developments in Latin America, as well as international efforts that support standardization and interoperability of digital credentials. These sections provided insights into how different regions are adopting and

integrating digital credentials to enhance educational and professional outcomes.

Although this report serves as a comprehensive overview, it is important to note that it does not claim to be exhaustive. The rapidly evolving field of digital credentials is marked by continuous innovation and development. This report aims to provide a foundational understanding and a snapshot of the current state of digital credentials, recognizing that future advancements will further shape this dynamic landscape.

References

100.000 Strong in the Americas (2024). *SENA (Servicio Nacional de Aprendizaje)*. Retrieved from https://www.100kstrongamericas.org/sena/

1EdTech (2024a). *Open Badges Specification Conformance and Certification Guide*. Retrieved from https://www.imsglobal.org/spec/ob/v3p0/cert/

1EdTech (2024b). *About 1EdTech*. Retrieved from https://www.1edtech.org/about/1edtech

1EdTech (2024c). *CLR Standard*. Retrieved from https://www.1edtech.org/standards/clr

American Association of Collegiate Registrars and Admissions Officers (AACRAO) (2022). *Alternative Credentials: Considerations, Guidance, and Best Practices. Alternative Credentials Workgroup Report*. Retrieved from https://www.edalex.com/wp-content/uploads/2023/07/Alternative-Credentials-Considerations-Guidance-Best-Practices-2022.pdf

American Association of Collegiate Registrars and Admissions Officers (AACRAO) (2023). *Credential Confusion: A Call for Uniformity in Practice and Terminology*. Retrieved from https://www.aacrao.org/research-publications/aacrao-research/credentials-confusion-a-call-for-uniformity-in-practice-and-terminology

Agencia Nacional de Evaluación de la Calidad y Acreditación (ANECA) (2022). *Microcredenciales. Formación inclusiva en todos los formatos y para todas las edades*. Retrieved from https://www.aneca.es/documents/20123/49576/MICROCREDENCIALES_Informe_V3.pdf/db424827-b464-d41d-ae09-717eb95e5742?t=1660907214565

Allen, C. (2016, April 16). *The Path to Self-Sovereign Identity*. Life With Alacrity. https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/

Bakhtina, M., Leung, K. L., Matulevičius, R., Awad, A., & Švenda, P. (2023, August 29-September 01). *A decentralised public key infrastructure for X-Road* [Conference paper]. Proceedings of the 18th International Conference on Availability, Reliability and Security, Benevento, Italy. https://doi.org/10.1145/3600160.3605092

Biometrics Research Group (2023, December 18). *UNDP lauds Guatemala's digital transformation efforts, offers recommendations*. Biometric Update. Retrieved from https://www.biometricupdate.com/202312/undp-lauds-guatemalas-digital-transformation-efforts-offers-recommendations

Brands, S. (2002): A Technical Overview of Digital Credentials. Retrieved from http://www.credentica.com/overview.pdf

Brown, M., Nic Giolla Mhichil, M., Beirne, E., & Mac Lochlainn, C. (2021). The Global Micro-credential Landscape: Charting a New Credential Ecology for Lifelong Learning. *Journal of Learning for Development*, *8*(2), 228-254. doi:10.56059/jl4d.v8i2.525

Bundesministerium für Bildung, Wissenschaft und Forschung (n.d.). *Micro-credentials. Positionspapier der österreichischen Hochschulbildung*. Retrieved from https://www.bmbwf.gv.at/Themen/HS-Uni/Europ%C3%A4ischer-Hochschulraum/Die-Themen-des-Europ%C3%A4ischen-Hochschulraums/Microcred.html

Carey, K. L., & Stefaniak, J. E. (2018). An exploration of the utility of digital badging in higher education settings. *Educational Technology Research and Development*, *66*(5), 1211-1229. https://doi.org/10.1007/s11423-018-9602-1

Casilli, C., & Hickey, D. (2016). Transcending Conventional Credentialing and Assessment Paradigms with Information-Rich Digital Badges. *The Information Society*, *32*(2), 117-129. https://doi.org/10.1080/01972243.2016.1130500

Chen, G., Xu, B., Lu, M., & Chen, N. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*, *5*(1), 1-10. https://doi.org/10.1186/s40561-017-0050-x

CompTIA (n.d.). *About us*. Retrieved from https://www.comptia.org/about-us

Confederação Nacional da Indústria (n.d.). *Exporte seu produto com segurança e competitividade*. Retrieved from https://www.portaldaindustria.com.br/cni/canais/assuntos-internacionais/o-que-fazemos/solucoes/certificado-de-origem-digital/

Council of the European Union (2022). *Proposal for a Council Recommendation on a European approach to micro-credentials for lifelong learning and employability*. Retrieved from https://data.consilium.europa.eu/doc/document/ST-9237-2022-INIT/en/pdf

Coursera (2024). *Coursera: Degrees, Certificates, & Free Online Courses*. Retrieved from https://www.coursera.org/

Credential Engine (2024). *Bringing Credential Transparency Through Technology*. Retrieved from https://credentialengine.org/about-us/

Credly by Pearson (2024). *Unlock the Power of Your People*. Retrieved from https://info.credly.com/

Danmarks Akkrediteringsinstitution (2021). *Nye fleksible uddannelsesveje gennem hele livet. Europæiske og danske perspektiver på micro-credentials på videregående uddannelsesniveau*. Retrieved from https://akkr.dk/wp-content/filer/akkr/micro-credentials-publikation-web.pdf

Deutscher Akademischer Austauschdienst e.V. (2023). *Digital Credentials Initiatives Monitor*. Retrieved from https://www.digital-credentials-monitor.com/

Deutscher Akademischer Austauschdienst e.V. (2024). *Digital Credentials Initiatives Monitor - Data Collection*. Retrieved from https://www.daad.de/surveys/261944?lang=en

Digital Credentials Consortium (2018). *Building the digital credential infrastructure for the future*. Retrieved from https://digitalcredentials.mit.edu/docs/white-paper-building-digital-credential-infrastructure-future.pdf

Dock Labs AG (2023). *What Are Digital Credentials? Dock*. Retrieved from https://www.dock.io/post/what-are-digital-credentials

ECOCredGT (n.d.). *About ECOCredGT.* Retrieved from http://www.ecocredgt.org/?page_id=366&lang=en

edX (2024). *Cursos en línea gratuitos de Universidad Nacional de Córdoba*. Retrieved from https://www.edx.org/es/school/uncordobax

El Ioini, N., Pahl, C. (2018, October 22-26). *A Review of Distributed Ledger Technologies* [Conference paper]. On the Move to Meaningful Internet Systems, Valletta, Malta. https://doi.org/10.1007/978-3-030-02671-4_16

European Centre for the Development of Vocational Training (CEDEFOP) (2019). *European guidelines for validating non-formal and informal learning*. Retrieved from https://www.cedefop.europa.eu/en/publications/3093

European Centre for the Development of Vocational Training (CEDEFOP) (2024). *European qualifications framework (EQF)*. Retrieved from https://www.cedefop.europa.eu/en/projects/european-qualifications-framework-eqf

Europass (2023). *Launch of the European Learning Model - Video*. Retrieved from https://europass.europa.eu/en/node/2149

European Commission (2018). *European Qualifications Framework: a common reference framework*. Retrieved from https://europass.europa.eu/en/europass-digital-tools/european-qualifications-framework

European Commission (2020a). *Final report: A European approach to micro-credentials. Output of the Microcredentials Higher Education Consultation Group*. Retrieved from https://ec.europa.eu/education/sites/default/files/document-library-docs/european-approach-microcredentials-higher-education-consultation-group-output-final-report.pdf

European Commission (2020b). *Digital Education Action Plan 2021-2027*. Retrieved from https://education.ec.europa.eu/focus-topics/digital-education/action-plan

European Commission (2023). *Europass: Improve your Career and Learning Opportunities*. Retrieved from https://europa.eu/europass/en/about-europass

European Commission (2024). *eIDAS Regulation*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

European Commission (n.d.-a). *European Credit Transfer and Accumulation System (ECTS)*. Retrieved from https://education.ec.europa.eu/education-levels/higher-education/inclusive-and-connected-higher-education/european-credit-transfer-and-accumulation-system

European Commission (n.d.-b). *Experience cross-border services with EBSI*. Retrieved from https://ec.europa.eu/digital-building-blocks/sites/display/EBSI

European Union (n.d.). *European Digital Credentials for learning*. Retrieved from https://europass.europa.eu/en/europass-tools/european-digital-credentials

European Union. (2004). Decision No 2241/2004/EC of the European Parliament and of the Council of 15 December 2004 on a single framework for the transparency of qualifications and competences (Europass). *Official Journal of the European Union*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D2241

European Union Agency for Cybersecurity (n.d.). *Public Key Infrastructure (PKI)*. Retrieved from https://www.enisa.europa.eu/topics/incident-response/glossary/public-key-infrastructure-pki

Eur-Lex (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council on the on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union.* Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Flintberg, B. (2022). *Digital micro-credentials for upskilling and reskilling in the vocational sector. A study on the potential use of a blockchain-based ICT system for micro-credentials in Sweden* [Degree Project, Linnaeus University]. Retrieved from https://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-115173

Foshay, W. R., & Hale, J. (2017). Application of principles of performance-based assessment to corporate certifications. *TechTrends*, *61*(1), 71-76. https://doi.org/10.1007/s11528-016-0125-5

FutureLearn (2012). *What could you achieve with FutureLearn?* Retrieved from https://www.futurelearn.com/business

Gibson, D., Ostashewski, N., Flintoff, K., Grant, S., & Knight, E. (2015). Digital badges in education. *Education and Information Technologies*, *20*(2), 403-410. https://doi.org/10.1007/s10639-013-9291-7

Goldreich, O., Micali, S., & Wigderson, A. (1986). Proofs that yield nothing but their validity and a methodology of cryptographic protocol design. *27th Annual Symposium on Foundations of Computer Science*, 174-187. doi: 10.1109/SFCS.1986.47

González, C., Rodríguez, M., & Chamoso, P. (2018). Multi-Factor Authentication for Enhanced Security in Digital Credential Storage. *Journal of Information Security and Applications*, *42*, 94-106. doi:10.3390/cryptography2010001

Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Torres, C., & Wendland, F. (2018). *Blockchain for Education: Lifelong Learning Passport* [Conference paper]. Proceedings of 1st ERCIM Blockchain Workshop 2018, Amsterdam, Netherlands. doi: 10.18420/blockchain2018_07

Grech, A., & Camilleri, A. F. (2017). Blockchain in education. *Joint Research Centre of the European Commission.* doi:10.2760/60649. Retrieved from https://publications.jrc.ec.europa.eu/repository/handle/JRC108255

Groningen Declaration (n.d.). *The Groningen Declaration Network*. Retrieved from https://groningendeclaration.org/the-groningen-declaration-network/

Hyland (2024). *Hyland: Empowering innovators every day*. Retrieved from https://www.hyland.com/en/company

IBM (n.d.). *IBM Innovation Center for Education (ICE)*. Retrieved from https://www.ibm.com/support/pages/ice-digitalbadges

Inter-American Development Bank (IDB) (n.d.). *We are the IDB*. Retrieved from https://www.iadb.org/en/who-we-are/about-idb

Kato, S., V. Galán-Muros & T. Weko (2020). The emergence of alternative credentials. *OECD Education Working Papers*, *No. 216*. https://doi.org/10.1787/b741f39e-en

Katz, J., & Lindell, Y. (2007). *Introduction to Modern Cryptography: Principles and Protocols*. Chapman and Hall/CRC Press. https://doi.org/10.1201/9781420010756

Keevy, J. and Chakroun, B. (2015). *Level-Setting and Recognition of Learning Outcomes: The Use of Level Descriptors in the Twenty-First Century*. Retrieved from https://doi.org/10.54675/GKWN6283

Khalil, M., & Ebner, M. (2015). *Learning Analytics: Principles and Constraints*. [Conference paper]. Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications, Chesapeake, Virginia. doi:10.13140/RG.2.1.1733.2083

Lemoine, P. A. and Richardson, M. D. (2015). Micro-credentials, nano degrees, and digital badges: new credentials for global higher education. *International Journal of Technology and Educational Marketing,* 5(1), 36–49. doi: 10.4018/ijtem.2015010104

LinkedIn Learning (2024). *A learning experience built for skill builders*. Retrieved from https://learning.linkedin.com/

Mah, D. (2016). Learning analytics and digital badges: potential impact on student retention in higher education. *Technology, Knowledge and Learning, 21*(3), 285–305. https://doi.org/10.1007/s10758-016-9286-8

McDaniel, R., & Fanfarelli, J. (2016). Building Better Digital Badges: Pairing Completion Logic With Psychological Factor. *Simulation and Gaming*, *47*(1), 73–102. doi: 10.1177/1046878115627138

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press. https://doi.org/10.1201/9780429466335

Microsoft Security (2024). *Microsoft Entra Verfied ID - Trustworthy interactions for a digital world*. Retrieved from https://www.microsoft.com/de-de/security/business/identity-access/microsoft-entra-verified-id

MIT Media Lab. (2016). *Blockcerts: Open Standard for Blockchain Certificates*. Retrieved from https://www.media.mit.edu/projects/blockcerts

MIT Open Learning (2024). *Digital Credentials Consortium*. Retrieved from https://digitalcredentials.mit.edu/our-work

Mühle, A., Assaf, K., Köhler, D., & Meinel, C. (2023). *Requirements of a Digital Education Credential System* [Conference paper]. IEEE Global Engineering Education Conference (EDUCON), Kuwait. doi: 10.1109/EDUCON54358.2023.10125183

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from http://dx.doi.org/10.2139/ssrn.3440802

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press. https://doi.org/10.1016/S1353-4858(16)30074-5

New Zealand Qualifications Authority (2019). *Guidelines for applying for approval of a training scheme or a micro-credential.* Retrieved from https://www2.nzqa.govt.nz/assets/Tertiary/Approval-accreditation-and-registration/Guidelines/Guidelines-for-programme-approval-and-accreditation-L1-7-2023.pdf

OneTrust (2024). *Guatemala - Data Protection Overview*. Retrieved from https://www.dataguidance.com/notes/guatemala-data-protection-overview

Oxford University Press (2024). *Credentials.* Oxford Learners Dictionaries. Retrieved from https://www.oxfordlearnersdictionaries.com/definition/american_english/credentials

Pahuja, N. (2023). *Micro-Credentials: Future of Modern Skilling*. Retrieved from https://www.ilo.org/resource/presentation-neena-pahuja-micro-credentials-future-modern-skilling

Pickard, L. (2018). *Analysis of 450 MOOC-Based Microcredentials Reveals Many Options But Little Consistency*. Retrieved from https://www.classcentral.com/report/moocs-microcredentials-analysis-2018/

Pontificia Universidad Católica del Perú (2024a). *Oferta académica*. Retrieved from https://educacioncontinua.pucp.edu.pe/oferta-academica/

Pontificia Universidad Católica del Perú (2024b). *Para organizaciones*. Retrieved from https://educacioncontinua.pucp.edu.pe/programas-a-medida/

Porto, S. & Presant, D. (2023). *The IDB Digital Credential Framework: Principles and Guidelines for Creating and Issuing Credentials*. Retrieved from https://publications.iadb.org/en/publications/english/viewer/The-IDB-Digital-Credential-Framework-Principles-and-Guidelines-for-Creating-and-Issuing-Credentials.pdf

Preukschat, A., & Reed, D. (2021). *Self-Sovereign Identity: Decentralized digital identity and verifiable credentials*. Manning Publications. ISBN: 9781617296598

Quality and Qualifications Ireland (2021). *QQI early exploration into Micro-credentials in Higher Education, 2014–2020*. Retrieved from https://www.qqi.ie/sites/default/files/2021-10/early-exploration-into-micro-credentials-in-higher-education-2014-20.pdf

Quigley, J. (2023). *What Are Digital Credentials and How Are They Used?* Accredible. Retrieved from https://www.accredible.com/blog/what-are-digital-credentials

Reynolds, L., & Winks, J. (2021). Data Protection Techniques: A Cryptography Approach. *Journal of Technology and Systems*, *3*(1), 14–21. doi: 10.47941/jts.533

Sedlmeir, J., Smethurst, R. & Rieger, A. (2021). Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering, 63*, 603–613. https://doi.org/10.1007/s12599-021-00722-y

Sertifier (July 24, 2023). *What is the difference between a digital certificate and digital badge?* LinkedIn. https://www.linkedin.com/pulse/what-difference-between-digital-certificate-badge-sertifierco-1f/

Sharples, M., & Domingue, J. (2016). *The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward* [Conference paper]. Proceedings of the 11th European Conference on Technology Enhanced Learning (EC-TEL), Lyon, France. https://doi.org/10.1007/978-3-319-45153-4_48

Shi, J., Zeng, X., & Han, R. (2022). A Blockchain-Based Decentralized Public Key Infrastructure for Information-Centric Networks. *Information*, *13*(5), 264. https://doi.org/10.3390/info13050264

Shoemaker, P. (2022). *Verifiable Credentials: The Future of Digital Identity*. Identity. Retrieved from https://www.identity.com/what-are-verifiable-credentials/#:~:text=Verifiable%20Credentials%20%28VCs%29%20are%20digital%20credentials%20that%20use,versions%20of%20passports%2C%20driver%E2%80%99s%20licenses%2C%20and%20other%20credentials

Stefaniak, J., & Carey, K. (2019). Instilling purpose and value in the implementation of digital badges in higher education. *International Journal of Educational Technology in Higher Education*, *16*(1), 1–21. https://doi.org/10.1186/s41239-019-0175-9

SURFnet (2016), *Whitepaper on Open Badges and Micro-credentials*. Retrieved from https://www.surf.nl/en/white-paper-on-open-badges-and-micro-credentials

Tecnológico de Monterrey (2023). *Tec de Monterrey launches digital credentials to certify skills*. Retrieved from https://conecta.tec.mx/en/news/national/education/tec-de-monterrey-launches-digital-credentials-certify-skills

Udacity (2011). *About us*. Retrieved from https://www.udacity.com/about-us

UNESCO (2018). *Digital Credentialing Implications for the recognition of learning across borders*. Retrieved from https://oer4nosp.col.org/id/eprint/16/1/264428eng.pdf

UNESCO (2022). *Towards a common definition of micro-credentials*. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000381668#:~:text=Micro-credentials%20are%20often%20promoted%20as%20an%20efficient%20way,standards%20and%20is%20awarded%20by%20a%20trusted%20provider.

United Nations (2022). *The Sustainable Development Goals Report 2022*. Retrieved from https://unstats.un.org/sdgs/report/2022/The-Sustainable-Development-Goals-Report-2022.pdf

Universidad de Chile (n.d.). *Information about the revalidation and recognition processes at the University of Chile*. Retrieved from https://uchile.cl/english-version/international-relations/information-about-the-revalidation-and-recognition-processes

van der Hijden, P., & Martin, M. (2023). *Short courses, micro-credentials, and flexible learning pathways: A blueprint for policy development and action*. Paris: UNESCO, International Institute for Educational Planning. Retrieved from https://www.iiep.unesco.org/en/publication/short-courses-micro-credentials-and-flexible-learning-pathways-blueprint-policy

West, R.E. (2023). *Flexible Open Credentials: How Micro and Nanocredentials Can Revolutionize Higher Education*. Working Paper. Center for Growth and Opportunity at Utah State University. Retrieved from https://www.thecgo.org/research/flexible-open-credentials-how-micro-and-nanocredentials-can-revolutionize-higher-education/

Wolz, E., Gottlieb, M. & Pongratz, H. (2021). Digital Credentials in Higher Education Institutions: A Literature Review. *Wirtschaftsinformatik 2021 Proceedings, 5*. Retrieved from https://aisel.aisnet.org/wi2021/KDigitalEducation15/Track15/5

World Wide Web Consortium (2022a). *Decentralized Identifiers (DIDs) v1.0*. Retrieved from https://www.w3.org/TR/did-core/

World Wide Web Consortium (2022b). *Verifiable Credentials Data Model 1.0*. Retrieved from https://www.w3.org/TR/vc-data-model

World Wide Web Consortium (2024a). *About us*. Retrieved from https://www.w3.org/about/

World Wide Web Consortium. (2024b). *Verifiable Credentials Data Model v2.0*. Retrieved from https://www.w3.org/TR/vc-data-model-2.0/

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. *PloS One*, *11*(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). *An overview of blockchain technology: Architecture, consensus, and future trends* [Conference paper]. IEEE International Congress on Big Data, Honolulu, USA. doi: 10.1109/BigDataCongress.2017.85