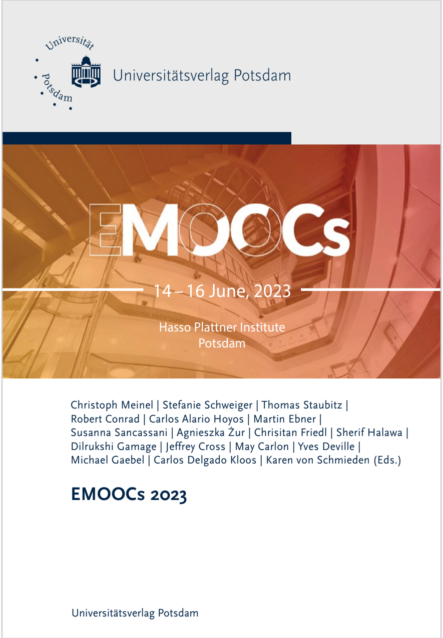

Universitätsverlag Potsdam

EMOOCs

14 – 16 June, 2023

Hasso Plattner Institute
Potsdam

Christoph Meinel | Stefanie Schweiger | Thomas Staubitz |
Robert Conrad | Carlos Alario Hoyos | Martin Ebner |
Susanna Sancassani | Agnieszka Żur | Chrisitan Friedl | Sherif Halawa |
Dilrukshi Gamage | Jeffrey Cross | May Carlon | Yves Deville |
Michael Gaebel | Carlos Delgado Kloos | Karen von Schmieden (Eds.)

EMOOCs 2023

Universitätsverlag Potsdam

Challenges and Proposals for Introducing Digital Certificates in Higher Education Infrastructures

Anja Lorenz, Stefanie Bock, and Juleka Schulte-Ostermann

Technische Hochschule Lübeck
Lübeck, Germany

Questions about the recognition of MOOCs within and outside higher education were already being raised in the early 2010s. Today, recognition decisions are still made more or less on a case-by-case basis. However, digital certification approaches are now emerging that could automate recognition processes. The technical development of the required machine-readable documents and infrastructures is already well advanced in some cases. The DigiCerts consortium has developed a solution based on a collective blockchain. There are ongoing and open discussions regarding the particular technology, but the institutional implementation of digital certificates raises further questions. A number of workshops have been held at the Institute for Interactive Systems at Technische Hochschule Lübeck, which have identified the need for new responsibilities for issuing certificates. It has also become clear that all members of higher education institutions need to develop skills in the use of digital certificates.

1 Introduction

Discussions about awarding credits points for MOOCs began shortly after they emerged in the early 2010s [6]. However, there was no rush to the exam offices so far. Rather, MOOCs are used for personal development. Recognizing them to study programs, on the other hand, remains complex and is often still handled on a case-by-case basis. The widely predicted opening up of universities has not yet happened. Instead, the introduction of micro-credentials opens up yet another "currency" in further education.

A crucial factor seems to be the time-consuming verification of certificates: the learning outcomes have to be compared with those of the study modules in order to decide whether the MOOC is relevant to the study program at all. If this is the case, it is also important to check that the MOOC meets the university's quality standards for content, exercises and, most important, assessments.

There are now some approaches to automate these processes. The basis for this is a standardized competence model, which can be implemented by digital certificates. In addition, the content of the certificates must be sufficiently verifiable to make it difficult to fake them. Finally, a digital infrastructure is needed on the university platforms to issue and manage the certificates. Additional services such as recognition databases or automated recommendation systems can then be established.

In section 2 of this article, current approaches and proposals from the projects of the Technische Hochschule Lübeck (TH Lübeck, https://www.th-luebeck.de/) are presented and described. The technical implementation is often well advanced and prototypical implementations are already in use. In the course of the step-by-step implementation of the infrastructure in productive learning programs, however, new questions have arisen that go beyond purely technical aspects. This paper will focus on these. These challenges and the first results of our workshops are presented in section 3 , and further steps and limitations of digital certificates are finally discussed in section 4.

2 Background: digital certificates

Initially, the development of digital certificate infrastructures focused on technical issues and solutions. The need to support also institutional implementation became apparent as the technical implementations were progressively rolled out into productive learning modules. At this point, decisions had to be made about organizational implementations that did not have established processes and solutions in place for paper certificates.

With the development of the first MOOCs in 2014 [9], we have already issued certificates of participation that can be described as *electronic certificates*. We have built our platform using the open source learning management system Moodle (https://moodle.org/), which supports rule-based certificate issuance. This creates PDFs that can be configured in terms of content and design. But these certificates are merely electronic reproductions of their paper counterparts. They lack one important feature: they are not machine-readable. As a result, they cannot be processed automatically. Students at higher education institutions in Germany have their academic achievements electronically stored and managed in a database. To this end, about 220 higher education institutions in Germany have set up a cooperative called HIS Hochschul-Informations-System eG (translated: HIS Higher Education Information System, registered cooperative), which organizes not only the academic achievements for individual modules, but also the administration of diplomas. These diplomas require further legal specifications (e.g. they have to be signed by the head of the university) and are therefore not considered further in this article.

There are three key aspects to the implementation of digital certificates:

1. An important precondition for machine-readability of certificates is a **standardized competence model**, which enables cross-platform documentation of certificate contents. For this purpose, Europass provides a practical basis [2]. Since 2004, the European Parliament and the Council have been working on this harmonized description of competences [5], which is intended to improve the interfaces between the worlds of education and work and to facilitate the international recognition of qualifications. It was updated in 2018 [4]. Within the Europass framework, XML schemas, web services and other components have been developed on which digital certificates can – and should – be based in order to achieve the intended compatibility.

2. When implementing digital certificates, the **ability to verify the data** is important. Digital documents (especially text and images) can be easily created, copied, manipulated and thus forged. In the case of paper certificates, efforts are made to prevent these possibilities, e.g. by using special types of paper, embossing, stamps, seals or signatures of authorized persons. In the case of digital documents, cryptographic techniques can also be used to significantly reduce the possibility of alteration. The DigiCerts, of which our institute is a member, has developed a solution based on a consortial blockchain (see https://www.digicerts.de/). This means that the hashes of the issued certificates are written to the blockchain and can also be subsequently verified via the blockchain. If the document has been manipulated, the hash will no longer be valid. As part of the DigiCerts consortium, we have already developed a Moodle plug-in that can be used to issue digital certificates. The blockchain technology approach is currently being debated [8, 7], particularly in favor of using less complex cryptographic techniques, e.g. public key infrastructure (PKI). However, the specific technical implementation of the verification features is not relevant for this article.

3. However, the benefits of digital certificates will only be realized if they are made available to as many stakeholders as possible. The PIM project (Platform for International Student Mobility, https://pim-plattform.de/en/), in which our institute is involved, aims to facilitate the mutual recognition of academic achievements through the use of a database. Time-consuming case-by-case checks will no longer be necessary and will be replaced by an **automated matching process**. This could significantly reduce the resources required by higher education institutions to carry out the checks, thus overcoming a major barrier to students requesting such checks at all. As a result, more competences acquired outside higher education could possibly be recognized. Digital certificates with a stan-

dardized description of the academic achievement provide the basis for this recognition.

In the future, digital certificates should enable further services, e.g. to improve the search for interesting job offers or to make suggestions for useful further qualifications [3].

3 Identification of Challenges beyond technology and further workshop results

Once the technical progress was mature, digital certificates have been tested in the first online courses. Both MOOCs on the FutureLearnLab platform (https://futurelearnlab.de/hub/) and online courses available only to students from the federal state of Schleswig-Holstein via the FutureSkills platform (https://futureskills-sh.de/) were selected. As the first trials raised a number of issues that could not be resolved at a technical level, a series of workshops were organized to address the main requirements for the implementation of digital certificates.

For the workshops, an open invitation was sent to three departments of TH Lübeck: Institute for Interactive Systems (ISy) is a research institute and competence center in the field of digital learning solutions and interactive systems. The Centre for Digital Teaching is a service unit of the university that supports educators on issues related to digital teaching and learning. The oncampus GmbH is a company and a wholly-owned subsidiary of the TH Lübeck, providing academic professional development programs and infrastructure services for university networks and schools.

The resulting team for the workshops was interdisciplinary: In addition to Moodle developers, blockchain, media and UX experts, the instructional designers provide the link to professional authors. Program managers and project developers have many years of experience with the structures and processes of universities as well as the policy objectives of the federal and state governments.

As a first step, issues related to the handling of digital certificates were collected, clustered and divided into topics for a series of workshops. The challenges identified can be divided into three main groups (with examples of questions):

1. Questions about instructional design: At what point in the course or platform will it be useful to issue digital certificates? What explanatory text is needed? What design elements should or can be used for better recognition?

2. Questions about the current level of competence and required competence development of all participants: What is the difference between digital certificates

and previous electronic documents (usually PDFs as well)? How can educators issue and sign digital certificates? How can learners archive their certificates? How can examination offices and boards verify digital certificates? What other stakeholders can use digital certificates and how? What do platform providers need to consider when implementing digital certificates?

3. Questions about institutionalization in universities and other (educational) institutions: Who is authorized to issue certificates? Who decides if they are valid? What are possible frauds and how can they be prevented or contained? What preparations need to be made for a sustainable infrastructure?

The complexity of these questions increases in this list: questions about the design of teaching are rather easy to answer and only help to reduce the workload by providing standardized guidelines and templates. Questions about institutionalization in universities sometimes require the extension or redesign of existing structures. For example, the DigiCerts concept recognizes certifying authorities (e.g. a university) and certifying persons (e.g. a staff member in the examination office or individual lecturers). How and by whom these roles can be assigned is a matter for the individual higher education institution, which needs to understand this concept. It is also necessary to consider whether the legal framework of the higher education institutions is sufficient or whether extensive change processes need to be initiated here as well.

A first key outcome was a **sharpened understanding and scope of different types of credentials**. In general, digital credentials can

- document learning achievements (portfolio function),
- serve as record for third parties (access function), and
- support gamification (motivational function).

Basic Moodle certificates are only used for platform-internal documentation and processing, or outside the certificate consortium. Digital certificates, on the other hand, are machine readable and verifiable, which makes them important as proof for third parties. Digital badges, in turn, are mainly used to increase motivation (gamification), also because their acceptance beyond particular platforms is rather low.

When introducing digital certificates, it is important to **support recognized standards** such as ESCO from the European Union's Europass framework [1]. Otherwise, the value of the certificates is unclear. Although these standards are seldom supported for paper certificates, the resulting added value only comes into play with digital certificates because they are processed afterwards. Conversely, without the support of standards, digital certificates add complexity and extra effort to the development of services based on them. However, with this conclusion comes the awareness that the visual representation of certificates is likely to contain only a subset of the machine-readable data. For example, a full representation of the ESCO competences on which Europass is based would require several pages of text for even the simplest certificates of participation.

Verification of authenticity also remains a key function of digital certificates. This poses a particular challenge when it comes to organizational and institutional processes: On the one hand, it should be possible to correct typing errors or altered data, e.g. vital records, but on the other hand, it should not be possible to manipulate data without authorization. The cryptographic method must be suitable for this, but it should also be possible to prevent as many variants of social hacking as possible. Again, paper certificates are far from secure against tampering, but digital certificates can provide additional protection through authorization mechanisms, rights and roles.

A major challenge in implementing digital certificates in everyday university life is the **sustainability** of the implemented solutions. Paper certificates can be read for decades, if not centuries. In contrast, it is already being discussed whether the implemented technical solution based on a consortial blockchain is too complex and could be achieved with less complex approaches like PKI. Future development is therefore open to a variety of alternative technologies.

Last but not least, the **development of skills** in handling digital certificates is considered to be of great importance for the success of digital certificates for all stakeholders. In contrast to simple electronic documents, digital certificates are not simply a one-to-one reproduction of the paper version; they bring new possibilities, but also new requirements. The use of digital certificates in universities is not yet well established and needs to be understood by all parties involved.

- Learners need to understand, for example, that although the digital certificate (in our implementation) is a PDF, the essential content is in the embedded metadata (in our implementation as JSON).
- Educators need to understand how digital certificates are signed and the importance of careful handling of the required private key.
- Examination authorities and other recipients of the certificates need to understand how to validate them and that it is not enough to look at the visually presented information on the PDF page.

Each educational institution will need different sets of information materials, which strongly encourages the publication of such materials as Open Educational Resources (OER).

4 Conclusion and outlook

Digital certificates have the potential to finally fulfill one of the first hopes of MOOCs: the transversal recognition of learning outcomes and thus improved educational and labor mobility. Although based on paper documents and (often one-page) PDF files, they cover much more by providing machine-readable and standardized components for describing competences. Their key advantage is that they can be issued, verified and further processed automatically. Services based on them, such as recognition databases, are envisaged by both the public and private sectors and are already under development.

The current implementation of DigiCerts provides a PDF file with integrated metadata in JSON format to support both machine and human readability. However, visualization in particular needs to be made much simpler if standards such as ESCO are to be supported and a compact, human-readable presentation is to be ensured. We anticipate that higher education institutions will need a high level of support in making the transition and, in particular, in understanding the benefits of digital certificates.

It remains to be seen whether the DigiCerts' technical solution, based on a consortial blockchain, will take hold. Other verification options like PKI may also emerge in the future. Another question that remains to be answered is whether the new roles required to issue digital certificates (e.g. certification authorities) can be filled by existing people (e.g. lecturers or examination office staff) or whether entirely new positions will have to be created.

Finally, digital certificates cannot overcome the limitations of credentials in general. These include, for example, the need to verify the identity of the learner and, where applicable, of the person issuing the certificate, so that ghost writing or other models of fraud cannot be applied. Similarly, digital certificates cannot tell us whether the constructive alignment was appropriate, nor the extent to which competences can be maintained over time without further practice. Finally, it is difficult to consider competences that were primarily developed in informal contexts. These include, for example, the 4C competences (communication, collaboration, creativity and critical thinking, [10]. In these cases, alternative approaches like placement tests remain useful.

References

[1] ESCO. *ESCO by European Union*. 2023. URL: https://esco.ec.europa.eu/en (last accessed 2023-07-17).

[2] Europass. *Europass by European Union*. 2023. URL: https://europa.eu/europass/en (last accessed 2023-07-17).

[3] Europass. *Europass for Education and Training*. 2023. URL: https://europa.eu/europass/en/stakeholders/education-and-training (last accessed 2023-03-22).

[4] European Union. *Decision No 2018/646 of the European Parliament and of the Council of 18 April 2018 on a common framework for the provision of better services for skills and qualifications (Europass) and repealing Decision No 2241/2004/EC (Text with EEA relevance.)* 2018. URL: http://data.europa.eu/eli/dec/2018/646/oj/eng (last accessed 2023-07-17).

[5] European Union. *Decision No 2241/2004/EC of the European Parliament and of the Council of 15 December 2004 on a single Community framework for the transparency of qualifications and competences (Europass)*. 2004. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32004D2241 (last accessed 2023-07-17).

[6] K. Jordan and F. Goshtasbpour. "JIME Virtual Special Collection – 2012 to 2022: The Decade of the MOOC". In: *Journal of Interactive Media in Education 2022* 1 (2022). DOI: 10.5334/jime.757.

[7] D. Knop. *Schlechtes Zeugnis für Zeugnisse in der Blockchain*. 2022. URL: https://www.heise.de/news/Schlechtes-Zeugnis-fuer-Zeugnisse-in-der-Blockchain-6370807.html (last accessed 2023-07-17).

[8] M. Laaff. *Digitale Zeugnisse: Braucht das digitale Zeugnis eine Blockchain?* 2022. URL: https://www.zeit.de/digital/2022-02/digitale-zeugnisse-schule-blockchain-digitalisierung (last accessed 2023-07-17).

[9] A. Lorenz, A. Wittke, T. Muschal, and F. Steinert. "From moodle to mooin: Development of a MOOC platform". In: *Proceedings Papers of the European MOOCs Stakeholder Summit 2015*. EMOOCs2015. EMOOCs2015, Université catholique de Louvain, Mons, 2015, pages 102–106.

[10] P21. *P21 Framework Definitions. The Partnership for 21st Century Skills*. The Partnership for 21st Century Skills. 2009. URL: https://files.eric.ed.gov/fulltext/ED519462.pdf (last accessed 2023-07-17).