EPiC Series in Computing

Volume 95, 2023, Pages 181–192

Proceedings of European University Information Systems Congress 2023

A Distributed Infrastructure for Secure Diplomas: Proof of Concept and First Experiences

Alexander Knoth[1], Erwin Soldo[2], Kathleen Clancy[3] and Ulrike Lucke[4]

[1]German Academic Exchange Service, Germany

[2] Contractor, German Academic Exchange Service, Germany

[3]German Academic Exchange Service, Germany

[4] University of Potsdam, Germany

knoth@daad.de,extern_soldo@daad.de,clancy.berlin@daad.de,
ulrike.lucke@uni-potsdam.de

Abstract

Higher Education Institutions (HEIs) are being confronted with a growing number of student applications. This is associated with the verification of documents, which in the case of university entrance qualifications is becoming increasingly complex and error-prone in view of the diversifying education system. Various solutions to this problem have already been proposed, but due to technical, organisational, legal, or financial problems, they have not yet found widespread use. Against this background, this article presents an approach that integrates existing methods and services for digital signatures into a national infrastructure for education and connects them to existing information systems in schools to issue digital diplomas and verify them in HEI application processes. The article describes a technical solution and experiences from a proof-of-concept. First recommendations are given, and an outlook illustrates how the upcoming broad field test will be conducted.

[1] https://orcid.org/0000-0003-4674-6003
[2] https://orcid.org/0000-0001-6675-5156
[3] https://orcid.org/0000-0003-0425-2689
[4] https://orcid.org/0000-0003-4049-8088

1 Digital Credentials as Building Blocks of a Learner's Journey

Digital credentials become most apparent at transition points during the learner's journey, when a diploma is obtained and used to apply for jobs, subsequent degrees, or scholarships. However, these credentials are an integral part of learner agency throughout a person's academic and professional life, as they are a basis for flexible learning paths, the documentation of individual achievements and provide the infrastructure for national and international mobility. The rise of international, collaborative, and digital learning scenarios, such as the European University Alliances alongside new teaching and learning formats (e.g., MOOCs, virtual exchange, and blended mobility) bring about the need for digital credentials. The number of undetected cases of credential fraud or alteration remain unknown, while the verification of application documents is a laboursome task for HEIs requiring individual expertise of registrars and manual processes (Knoth et al., 2023). In Germany, the non-profit organisation "Uni-assist" inspects more than 60% of international applications for enrolment at German universities thereby processing approximately 300,000 student applications from over 180 countries and regions worldwide per year[5]. Types of fraud encountered by the organisation include "text lifted from other documents, fictitious language capability or education history, forged qualifications, fictitious references, impersonation and stolen identity" (O'Malley, 2010). To verify application documents, the organisation makes use of a database of bogus documents, recruits and trains personnel with national expertise and establishes direct links with institutions in countries where documents are more commonly forged, in order to assist with verification. The digitisation of issuance and verification processes may benefit HEIs through efficiency gains while also benefiting students. "[Students] could easily share their digital transcripts with a potential employer or university, who could then quickly and easily verify the authenticity of the credential saving both time and effort [...]" (Meinel et al., 2023). In addition, digital credentials offer more security features than paper-based credentials such as digital signatures and encryption to protect against tampering.

The Federal Ministry of Education and Research (BMBF) in Germany is currently promoting the emergence of a *digital education space* with a *national education platform*. Among other things, the networking infrastructure is intended to bundle digital education offerings that already exist today for various target groups in the digital education space. If solutions across different educational institutions are linked in this digital education space, the benefits of digital learning can be fully utilised. The networking approach is now intended to provide a meta-platform based on open standards and open source technology that is also compatible across Europe and serves as the basis for an ecosystem for digitally supported education. In this context, the digitalisation of learning and complementary administrative processes is becoming increasingly important. Therefore, digital credentials and more specifically verifiable credentials are crucial building blocks within the ecosystem because they document individual learning achievements and support each step learners take on their educational journey at the same time. The overarching term digital credential is used as a generalisation for digitised versions of a certificate or document representing achieved learning (Wolz et. al, 2021), from a technical viewpoint a credential can be defined as a set of claims (attributes about a learner) made by an issuer, whilst a verifiable credential is a tamper-evident credential where the authorship can be cryptographically verified. (Chartrand et. al, 2020).

The research and development project "BIRD" (**BI**ldungs**R**aum **D**igital is the German for digital education environment), which serves as the BMBF-funded validation platform and testbed for the component-based development of the national education platform, has also made digital credentials a scenario-driven priority (Knoth et al., 2022). In the context of the prototypical federated service infrastructure, the exchange of digital artefacts (e.g., documents) is increasingly coming to the fore. These include those that contain educational achievements of learners. An important aspect in the

[5] https://www.uni-assist.de/en/about-us/profile/ , 20.02.23

networking and use of this data is its authenticity. In order to be able to reliably verify the authenticity of this data, it is technically converted into verifiable credentials or claims (VC). This issue is currently well-known through the use of digital COVID vaccination certificates in Germany - especially regarding their authenticity and validity. In this example, content such as vaccination status and other personal information is converted into a VC. Learning outcomes contain, for example, statements (claims) of an issuing entity (issuer) about a person, an organisation or thing (object). The issuer (and thus author) of the claim transfers the VC to the owner. For a third party (verifier) and the object itself (if technically feasible), it must be possible to verify whether these VC were generated by the issuer and are still valid at the time of verification. For such VC, the verification of the authenticity of the VC should be combined with the authenticity of the issuer and, if necessary, also with the authorization of the issuer for the output of the respective VC, without having to query the issuer directly. These conceptual preliminary considerations are the bases for the presentation of a specific proof of concept which was carried out in the context of the implementation of the Single Digital Gateway Act in Germany (Open Access Act - Onlinezugangsgesetz, OZG)[6].

This article presents work in progress and focuses on the engagement of the BIRD project with the "field test of the digital school diploma" in the German state North Rhine-Westphalia[7]. The pilot project "field test" is aiming at digitising paper-based school diplomas to make admission processes easier and more tamper-proof.

The remainder of the article is organised as follows. In section 2, we provide an overview on existing solutions for secure diploma infrastructures against the variety of national backgrounds. The components of the proposed solution and their interplay for the targeted use cases are presented in section 3. This is followed by a description of the results gained from the proof-of-concept in section 4. Finally, conclusions are drawn and an outlook to future work is given in section 5.

2 State of the Art: The Digital Credentials Landscape

The VC or the general digital credentials landscape worldwide is diverse and highly active. Both government-directed approaches to regulation and infrastructure development as well as projects and platforms driven by universities, private sector companies, or diverse consortiums contribute to this. While several projects worldwide focus on solutions on a national scale, international cooperation in this area is driven by the European Commission as well as networks such as the Groningen Declaration Network and standardisation bodies such as the W3C.

In recent years, various projects and ventures have investigated the usability of VC in the domain of education. For example, the BMBF-funded project "Digital Credentials for Higher Education Institutions" (DiBiHo) is pursuing an approach that involves using the technological approaches of "self-sovereign identity" and "distributed ledger technology" (DLT) to generate fraud-proof credentials and enable their handling, as current identity management governance practices are often siloed and rarely consider the "networked nature of digital ecosystems" (Anand et al., 2021). DiBiHo is based on the US-based approaches of the "Digital Credentials Consortium"' (DCC). In Europe this is mirrored by many EU initiatives aiming to provide a framework for the use of VC based on an EU-wide DLT infrastructure in combination with an SSI for different domains. In education the European Self-Sovereign Identity Framework (ESSIF) forms part of the European Blockchain Services Infrastructure (EBSI). EBSI was launched by the European Commission with governments of member states in order to offer cross-border government services (Grech et al., 2021).

Europass is broader in its approach offering a varied set of online tools for learning and career management for European citizens to promote career mobility within the EU. The Europass Digital

[6] BMI - Onlinezugangsgesetz (bund.de), 20.02.23

[7] Feldtest Digitales Zeugnis NRW | Digitales Zeugnis NRW (digiz.nrw), 20.02.23

Credentials Infrastructure (EDCI) consists of standards, services and software outlining a data model for the issuance, storage, view, export, and verification of credentials alongside an accreditation database for institutions. The Council of Europe's Platform on Ethics, Transparency, and Integrity in Education (ETINED) also calls governments to action in order to counter education fraud by legislating for digital credentials. Not only should "member States [...] take all necessary measures to ensure the accessibility and integrity of data relating to students, qualifications and awards through digital solutions [...], [but] [w]herever technically possible, they should also provide services for verifying the authenticity of diplomas and professional certificates that are simple, accessible and multilingual" (Council of Europe, 2022, p. 13). Secure digital credentials can provide tamper-proof verification of documents, improved transparency for both the learner and receiving institution as well as simplified credential portability and interoperability between institutions and countries.

The usage spectrum of VCs in the education domain is broad. This includes usage across different educational institutions and sectors as well as usage in the context of formal and non-formal education. The following challenges, among others, are the reason no overarching standard for making VCs usable has yet been established (as in Rentzsch, 2021):

- Harmonisation of administrative processes related to the issuance of credentials in the field of formal education. This applies in the national context regarding federal structures, but also to the EU and worldwide.
- Technologies currently favoured in science and administration (for example, DLT, SSI, eIDAS, eID) for the use of VC have little appeal in the domain of education. Issues such as data protection and data security, GDPR compliance of DLT, legal feasibility of SSI-Verifiable Presentation, governance, effort required to implement DLT, incompatibility of DLTs with one another, autonomy of certain education sectors and the use of trust service providers, as well as resource expenditure and a negative carbon footprint are obstacles.
- The solution approaches and business models associated with these technologies do not correspond to sustainable use (licensing models and associated investments and costs, vendor lock-in, intransparency with regard to the code base), which is necessary in the domain of education for broad acceptance.
- Usability and ease of use for all stakeholders is strongly neglected in existing approaches.
- Confidence in the authenticity of the publisher and their authorization to publish the respective VCs can only be provided by an independent quality-assured central authority that acts on the basis of a technical framework accepted by all stakeholders involved. This authority can only be provided by either the state or a state-approved institution.

The architectural framework and the proof-of-concept presented is a practically oriented approach to address the above challenges and to provide solutions.

3 A Distributed Infrastructure for Secure Diplomas

Currently, there are four use cases involved in the scenario discussed in this article:

- First, education institutions that shall issue diplomas have to be integrated in the system.
- Afterwards, secure certificates can be issued by this institution.
- If necessary, an issued certificate can be revoked.
- Later, these certificates can be verified by any third party.

Other use cases might follow, during the proposed "field test."

3.1 Integrating an Institution

The usability of digital credentials in the domain of education is diverse. School leaving certificates and university transcripts of records, for example, are used in a wide variety of everyday life scenarios. Both for the issuer, the owner, and for third parties who make decisions based on these documents, trust

in the integrity of these documents is of immense importance. The integrity is generated by establishing the authenticity of the issuer and the right to release the respective types of evidence at the respective time of release. This information must be available in a trusted data source for all stakeholders.

A multi-stage process is used to determine both the authenticity of the educational institution and its acting employees and their authorisation to issue the respective digital credentials. Trust intermediaries play a crucial role in this process. As gatekeepers in the process, they ensure that the institution that has authenticated itself in the conventional way is authorised to issue certain credentials for the relevant period. The conventional authentication of an organisation and/or the acting person must take place via known mechanisms of a registration authority as a component of a trust service provider.

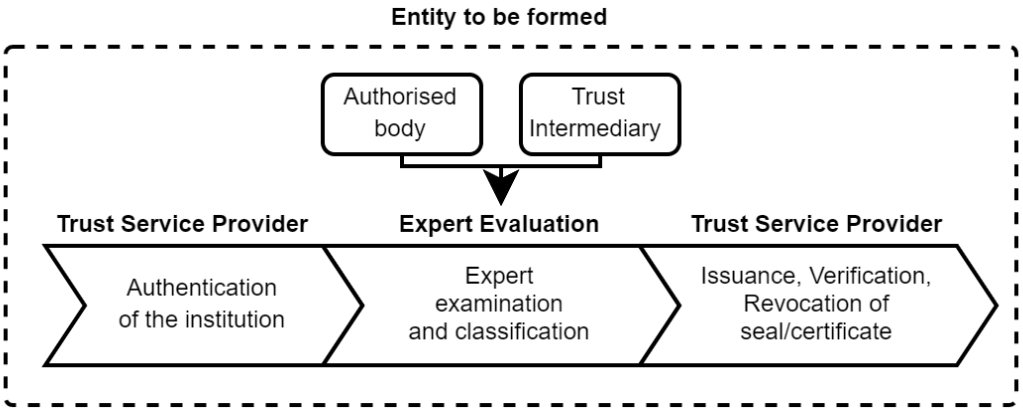

Figure 1: The educational institution verifies its legitimacy towards the infrastructure.

The technical basis for this is standardised procedures and technologies that are familiar from the use of public key infrastructures (PKI). Unlike other known PKIs from the domain of education, a so-called leaf certificate or end-entity certificate is issued to the issuer, with which no further certificates can be signed. The background to this decision is again trust. In the context of the process described above, it is assumed that only a central authority will be able to achieve cross-education-sector quality in the assessment of institutions in the domain of education.

3.2 Issuing a Digital Credential

The advantage of digital credentials over conventional paper-based credentials lies in the possibility of simultaneously displaying the contents or results pictorially, processing them automatically in a machine-readable manner, and verifying them securely. For this purpose, the issuer uses the already existing tools for the generation of education certificates, the storage of which is then mostly done in paper form. Instead of printing the education certificate, the image data of the results, the structured data of the results and other structured metadata are passed to a local component with the command to sign the digital education certificate. This component is addressable through a REST API. The distinctive feature of the process is that the results-related data is not passed on. Hash values are determined, which are then in turn signed by the central signature service as a remote signature and transmitted back to the local component. Using the PDF/A-3 format, signed (advanced seal with qualified time stamp) structured data (XML, JSON) can be integrated into a PDF here and then provided with a qualified seal (eIDAS compliant).

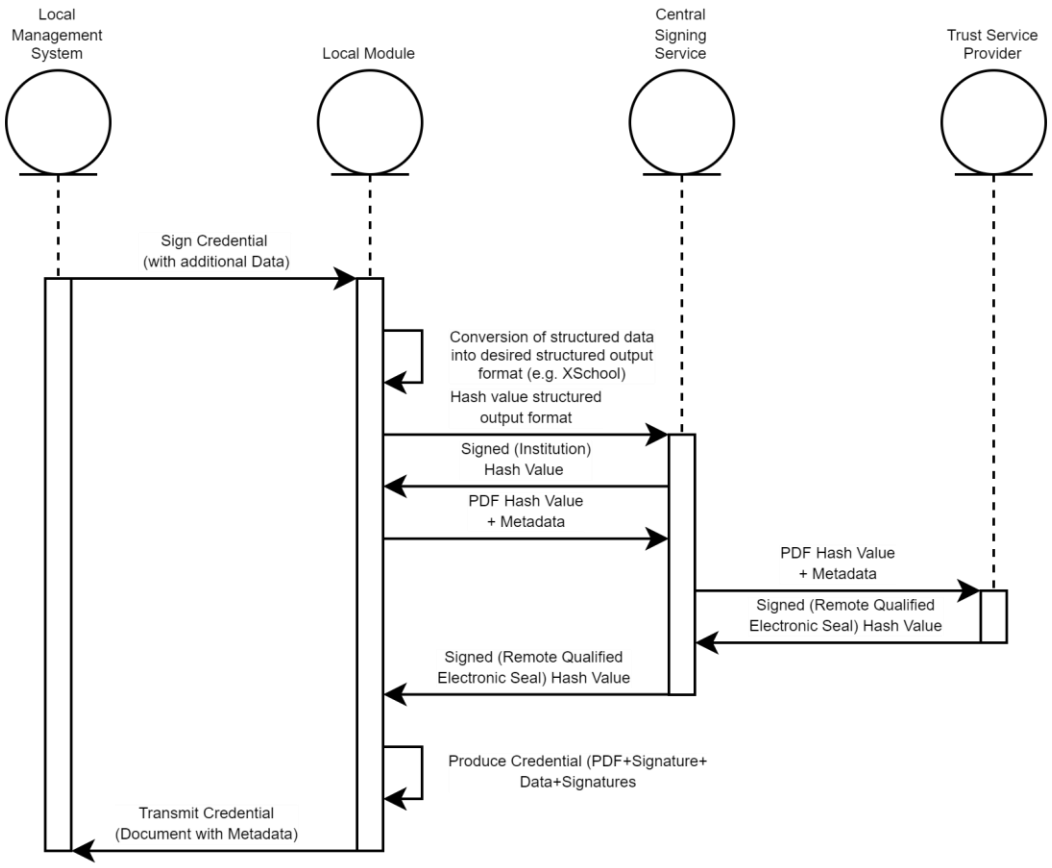

Figure 2: The hash values of the decorative document and the data set are digitally signed.

3.3 Revoking a Digital Credential

Withdrawing a digital credential may be necessary for a variety of reasons. For example, a security problem or an attempt to deceive that is discovered after the incident may make it necessary to withdraw the credential.

The administration system of the educational institution has the respective metadata of the already issued digital credentials. Based on an event, the withdrawal of a specific credential is initiated. This is done via a call to the REST API of the local component by passing the relevant parameters (including the digital education certificate, if applicable). An advantage in this procedure is that each digital education record created by the central issuing service is stored in a central database. Here, as shown above, for privacy reasons not the actual result data and further personal data of the education certificate are stored, but metadata and hashes. Thus, these credentials can be registered for withdrawal with the central withdrawal service via the specific local component based on the metadata. As a result, the completion of the withdrawal with corresponding metadata is reported to the respective administrative system via the specific local component.

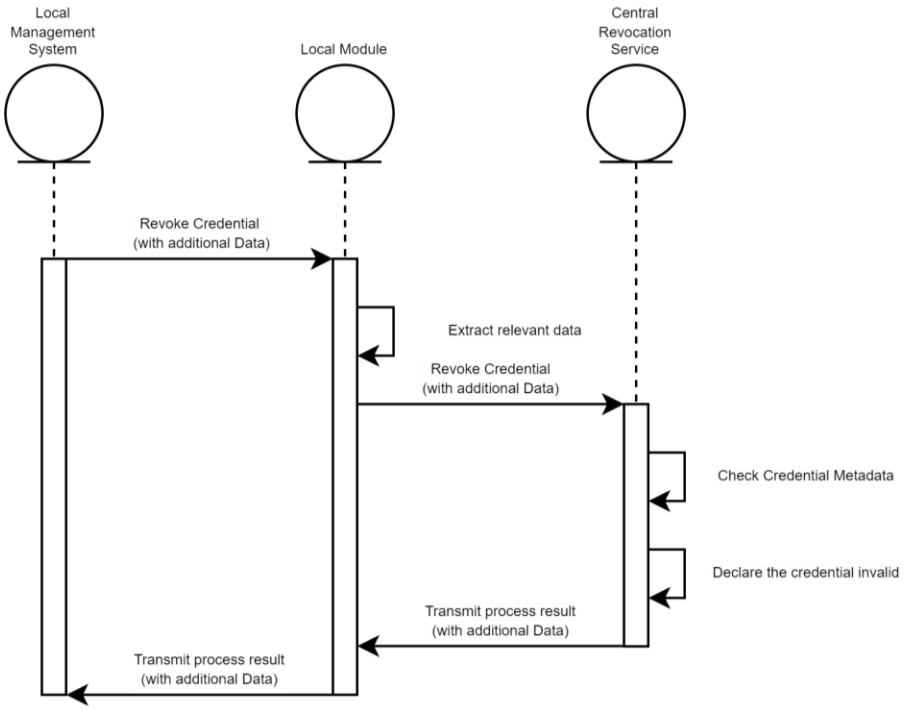

Figure 3: The credential submitted by the local management system can be automatically revoked.

3.4 Verifying a Digital Credential

Due to the particular importance of digital credentials in the individual educational journey, the verification of these credentials can be of great value to the respective stakeholder, depending on the application scenario. In the underlying procedure here, not only the authenticity of the digital proof is checked. The respective stakeholder can find out for himself whether a) the document is still valid, b) the issuer is authentic, and c) whether the issuer has possessed the rectification for issuing the respective types of evidence in the respective period. Depending on the use case, this in-depth check may be necessary.

Technically, three different procedures are envisaged, whereby only one procedure is presented here in more detail as an example. The other two procedures are based on the same methods: one procedure for checking a large number of digital certificates at once (of interest to stakeholders like universities, Uni-Assist and the Stiftung für Hochschulzulassung, for example), and another procedure for checking a single digital credential via a web user interface (for the owner and/or employer, for example). As already described above, no result or personal data is transferred to the central verification service during the verification of the digital proof. The respective administration system transfers the respective digital proof of education to the local component as part of a function call via a REST API. The local component then extracts all relevant information from the document and transfers the respective metadata and hashes of the digital credential to the central verification service.

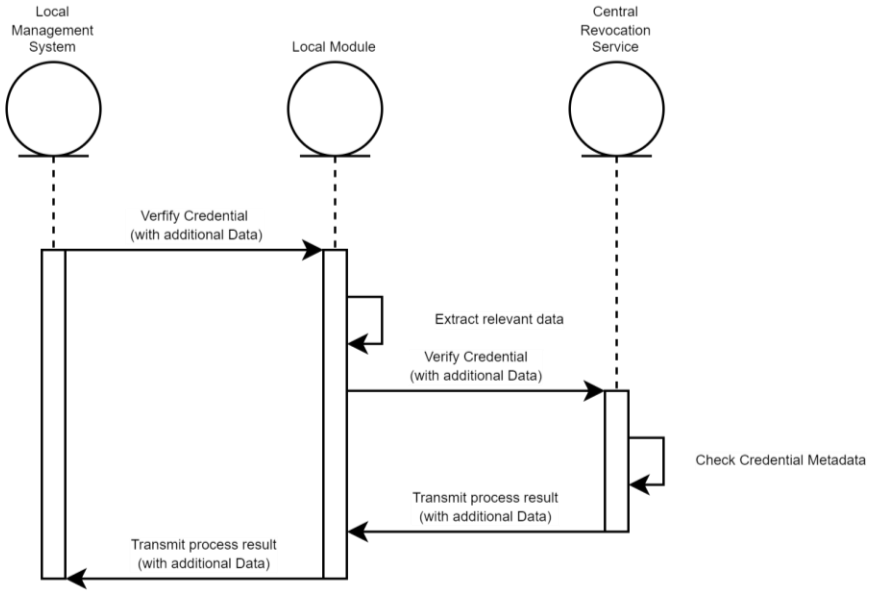

Figure 4: The certificate submitted by the applicant can be automatically checked for authenticity.

The central service checks in a central database whether the respective document a) has been created, b) has not been withdrawn, c) the respective signatures are correct and d) the status of the respective institution and e) its authorisation to issue the respective evidence in the respective period. The result of this check is returned to the local service, which in turn passes the result on to the facility's management system.

4 Experiences from the Proof of Concept

The “Digital School Diploma” implementation project is of particular importance in the education area of the SDG implementation in Germany. This is due to, among other things, the diverse challenges that arise in the implementation of this topic. Decentralised aspects, due to the federal structure of the formal education landscape, must be collated with central aspects such as standardisation according to the German XBildung [XEducation] approach, the OZG portal network and the goal of an EfA (One for All principle) compliant solution.

As the research and development driven prototype and the reference implementation of the networking infrastructure digital education funded by the BMBF, the BIRD project set itself the goal of developing, among other things, a solution for digital credentials and other digital certificates as part of the overall architecture design (Knoth et al., 2022). This solution was to offer an approach for the entire domain of education across all education sectors. In the first step, BIRD developed a generic architecture that was discussed in workshops with the federal state of Saxony-Anhalt, which is the lead state in the topic area of education, the lead federal department, the Federal Ministry of Education and Research (BMBF), and other stakeholders involved in the "Digital School Certificate" project. The objective of these discussions was to compare this overall architecture with the experiences of the lead department of the education topic area from the first "Digital School Diploma" field test and to develop a common target architecture in the process.

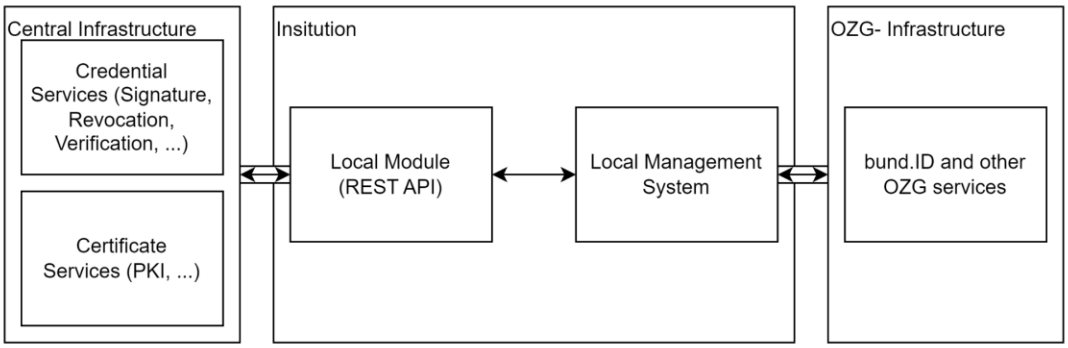

Figure 5: Common understanding of a target architecture.

After the completion of these discussions, it was decided to develop a prototype within the framework of a proof of concept with the state of North Rhine-Westphalia (NRW) based on this joint target architecture. BIRD's task was to develop the necessary components as prototypes and to adapt them so that they could be embedded in the NRW infrastructure. To this end, the state of North Rhine-Westphalia developed additional components to simplify integration. At the end of January, it was determined that the primary functions (issuing, withdrawing, and verifying a digital proof of education), of the components developed by BIRD were functional and could successfully interact with components of the NRW infrastructure. This concludes the project's task with respect to components for digital education credentials and certificates. The results will be incorporated into the implementation of the networking infrastructure digital education.

On the basis of these results, the steering committee of the Education topic area and the state of North Rhine-Westphalia have decided to conduct a field test for the 2023 high school graduation class in May/June 2023. A few dozen schools, students and universities will participate in this field test. The objective of the field test is to conduct a university application with a digital printout of a high school diploma and to assess both the technical and organisational processing. The findings will then be evaluated among the project participants and further measures agreed upon.

5 Conclusions and Preliminary Recommendations

The goal of the prototype for digital credentials as a part of the BIRD project was to evaluate various aspects of digital credentials in the domain of education. The goal to develop a generic and thus cross-education-sector solution remains. The proof-of-concept for the digital school diploma has offered fruitful insights into what needs to be taken into account and what will be considered during the planned field test: (1) Trust in digital credentials, (2) practical usability (and administration) of digital signatures and their technical implementation in a wide variety of environments, (3) costs (one-time and ongoing), and (4) governance and policies.

(1) Trust is one of the most critical issues for stakeholders in the administration of digital credentials. Only when a secure and automatable management of digital credentials becomes possible, the respective advantages arise for all stakeholders involved. BIRD has determined that purely technical solutions such as qualified electronic seals and signatures (QeS/S) alone do not provide a solution at all. Partial use per institution is not advantageous in terms of costs and management. With regard to security and trust, QeS/S cannot provide a qualitative classification of an institution. Theoretically, an elementary school could issue a high school diploma, and practically, a legal entity could claim to be an educational institution. In order to prevent this, BIRD follows the approach of a cross-sectoral education PKI. This would ensure

that, on the one hand, authentication and, on the other hand, also a qualitative evaluation of the acting parties is possible. As described above under 3.2, a PDF document is used as the presentation layer, into which the machine-readable data of the credential is then integrated. For the presentation layer, a QeSiegel is used that guarantees the integrity of the PDF document and provides a positive user experience for presentation in PDF viewers. The actual verification is performed by a separate central service, as shown in 3.4, which can be addressed by different services (local, web-based) and can verify all integrated components of the digital proof. Through the central approach, as described in 3.3, an individual digital credential can then be withdrawn and thus an up-to-date statement can also be made about the respective document regarding verification.

(2) In terms of usability, a solution that is as easy to operate or integrate as possible has been designed. The local component can be simply integrated into the respective IT infrastructure via a REST API. All functions (signing, retracting, and verifying) can be addressed via this REST API. An important function is the conversion of the respective structured data into a desired output format (see for instance XHochschule) and the merging into an overall artefact as a digital credential. Due to the use of a remote signature, there is no need to handle private keys on site.

(3) The costs of the proposed solution are low in terms of integration into on-site processes, the QeSiegel to be used, and the PKI in combination with the central services presented, based on the experience of the prototype. The use of a QeSiegel for the integrity of the PDF is advantageous. With a corresponding number of sealing processes, a price of a few Euro cents per QeSiegel can be achieved here. From the perspective of the BIRD project, the operation of the education PKI should be taken over permanently by the federal government as part of the provision of public services.

(4) From the perspective of the BIRD project, governance of the education PKI can only be executed by the state. Regardless of the costs, only a central service for digital credentials in the domain of education that is secured by the state can build trust among all stakeholders. But education PKI and the topic of digital credentials are to be understood as partial aspects of the development, implementation, and operation of a national education platform, for which smart governance solutions are needed overall. Initial study results are available (Gleiß et al., 2023), but further evidence-based research which goes along with the prototypical and component-based development of the networked education infrastructure is needed.

The prototype and the knowledge gained from the proof-of-concept will be transferred to the networked infrastructure for digital education at the BMBF. There, the prototype will be further developed into a minimum viable product aiming at providing a generic solution for the domain of education. The expected results from the field test in North Rhine-Westphalia can be seen as a complementary deep-dive which will help to implement generic solutions of the digital networking infrastructure education on the ground level at the institutions in different (German) states.

Acknowledgements

This work was partially funded by the German Federal Ministry for Education and Research under grant no. 16NB001 (project “Bildungsraum Digital”). The authors are deeply grateful to their teams and the partners of the project especially the Ministry for School Education for their great cooperation.

References

Anand, N. and Brass, I. (2021). Responsible innovation for digital identity systems. Data & Policy, Vol. 3, No. 35. https://doi.org/10.1017/dap.2021.35

Chartrand, J., Freeman, S., Gallersdörfer, U., Lisle, M., Mühle, A. and van Engelenburg, S. (2020). *Building the Digital Credential Infrastructure for the Future. A White Paper by the Digital Credentials Consortium.* https://digitalcredentials.mit.edu/wp-content/uploads/2020/02/white-paper-building-digital-credential-infrastructure-future.pdf

Council of Europe (2022). Countering Education Fraud – Recommendation CM/Rec(2022)18 and explanatory memorandum. Council of Europe. p. 13 https://rm.coe.int/ok-prems-137222-gbr-2512-cmrec-2022-18-et-expose-motifs-a5-web-1-/1680a96147

Gleiß, A.; Degen, K.; Knoth, A.; Pousttchi, K. and Lucke, U. (2023). Governance Principles and Regulatory Needs for a National Digital Education Platform. Submitted to: Public Policy and Administration, under review.

Grech, A., Sood, I., & Ariño, L. (2021). Blockchain, Self-sovereign Identity and Digital Credentials: Promise Versus Praxis in Education. Frontiers in Blockchain, 4, [616779]. https://doi.org/10.3389/fbloc.2021.616779

Knoth, A.; Blum, F.; Soldo, E.; Lucke, U. (2022). Structural Challenges in the Educational System meet a Federated IT-Infrastructure for Education – Insights into a Real Lab. In: *Proc. 14th International Conference on Computer Supported Education (CSEDU 2022)*, 369–375. https://doi.org/10.5220/0011085800003182

Knoth, A., Clancy, K., Peters, L., & De Leeuw, H. (2023). Chapter on Global Networking for Secure Academic Credentials in *Handbook of Academic Integrity* (S. E. Eaton Dr, Ed.) (1st ed.). Springer. To be published in June 2023.

Meinel, C., Mühle, A., Köhler, D., Assaf, K., Hoops, F., Knoth, A., Clancy, K., Peters, L., Soldo, E. (2023). *Considerations for Future Implementations from the DiBiHo Project.* To be published in March 2023 at https://www.it.tum.de/en/it/dibiho/publications/

O'Malley, B. (2010). GLOBAL: Detecting Application Fraud. University World News Africa Edition https://www.universityworldnews.com/post.php?story=20100326124132375

Rentzsch, R. 2021. *Digital Credentials in Education – The Situation in Germany and Europe in 2020*. Berlin, Institute for Innovation and Technology (iit) within the VDI/VDE Innovation + Technik GmbH. https://www.iit-berlin.de/wp-content/uploads/2021/05/03-Kurzstudie-DigitalCredentials.pdf

Wolz, E., Gottlieb, M., & Pongratz, H. (2021). *Digital credentials in higher education institutions: A literature review.* Innovation Through Information Systems: Volume III: A Collection of Latest Research on Management Issues, 125-140.

Author Biographies

Alexander Knoth is Chief Digital Officer (CDO) and Head of Section Digitalisation at the German Academic Exchange Service (DAAD) in Berlin. He is responsible for the strategic planning and management of DAAD's digitalisation activities. Before, he worked as an Advisor for the Digitalisation of Teaching and International Affairs at the President's Office of the University of Potsdam. He also worked at the chair of Complex Multimedia Application Architectures and at the chair of Gender Sociology both at the University of Potsdam. Alexander is an Educational Expert Fulbright Alumnus. He has been honoured by the Federal President of Germany and he has won the Teaching Award of the Federal State Brandenburg twice. His mobile application "Reflect.UP" has been nominated for the German E-Learning Innovation award (delina).

Erwin Soldo is an external consultant and works as an enterprise architect within the research and development projects "BIRD" and "Digital Campus" contracted by the German Academic Exchange Service (DAAD). In previous positions, Erwin gained experiences in the field of digitalising logistics, banking and telecommunications.

Kathleen Clancy is researching digital infrastructures and interoperable digital credentials for Higher Education and corresponding policy developments for the German Academic Exchange Service (DAAD) and hosts the Digital Credentials Regulars. An experienced project manager, she has previously developed a digital archive for the renowned Berliner Künstlerprogramm and worked with high-ranking international delegations from the education sector within Berlin's political landscape. After studies at King's College London and University College Dublin, she held roles at the Berlin Senatsverwaltung für Kultur & Europa and the dapd news agency before joining DAAD.

Ulrike Lucke is professor of computer science at the University of Potsdam, Germany. She obtained her PhD at the University of Rostock, Germany. Her research activities include institutional infrastructures for education, research, and administration. Currently, among other activities, she coordinates a large-scale national initiative to create a digital ecosystem for education across Germany and acts as an independent evaluator for two European projects on policy experimentation in the educational sector. Until 2018, she was responsible for e-learning and IT strategy as Chief Information Officer of the University of Potsdam. She is a founding member and was vice chair of the German University CIO Association until 2020. Since 2020, she is a Vice President of the German Informatics (GI) society.