WHITE PAPER

Digitalisation of certificates

with the support of blockchain technology

As of: March 2020

Version: 1.0

Content

Content

About gender

To improve readability, this white paper uses the singular they as described in the 7th edition of the Publication Manual of the American Psychological Association and thus avoids the simultaneous use of he/she. All references to persons apply to all genders.

Picture credits

Cover picture: Avel Chuklanov, licence-free via Unsplash
Graphics: Bundesdruckerei GmbH

1. Management summary

Together, the "Blockchain"[1] coordination project of the IT Planning Council [2], the actors responsible for the "Education" subject area of the Online Access Act (OZG), other players in the education system of the Federal Republic of Germany, and those active in international education work have set themselves the goal of digitising the certification system and making it forgery-proof and efficient to use.

This white paper summarises the results of the analysis and discussion phase to date. It is intended to validate the concept in a wider circle of schools, universities, ministries and companies, to promote consensus-building for a Germany-wide solution and, in view of global mobility and cross-border educational biographies, to contribute to the international dialogue on interoperability and harmonisation in education. The intention here is to support lifelong, individual educational pathways via all routes (including vocational training).

Today, certificates for school and university degrees are issued in written form, while application processes mainly take place online.

This white paper describes how certificates can be created digitally in addition to in written form, how they can be issued and how they can be created such that they are forgery-proof and their origin and integrity can be verified over a lifelong period. In addition, these certificates should be machine-readable so that the data can be automatically transferred into downstream specialist procedures.

The concept has been designed in such a way that, first, educational institutions will hardly have to expend any additional effort in creating the additional digital certificates and, second, a certificate, once received, can easily be checked for authenticity. The objective is not to provide a single solution but rather to ensure the interoperability of emerging solutions.

The concept is GDPR compliant because no personal data is processed and the certificates themselves are not stored centrally.

The concept provides for the use of one or more distributed ledger infrastructure(s) (blockchains) to register and secure the checksums of the certificates, thus guaranteeing protection against forgery. Here, the concept relies on open source technology to increase IT security and confidence in the system. The structure and operation of these infrastructures have not yet been conclusively defined in the concept. In principle, however, a permissioned

[1] https://dezentraleverwaltung.de

[2] https://it-planungsrat.de

blockchain with defined governance structures can be used to distinguish this from blockchains like bitcoin.

There are already several prototypical implementations underway to test the concept. Interested parties can request demonstrations from the developers (see contact persons under 7.1).

2. Initial situation and description of solution

Applications, both for university courses and for jobs, are now generally made digitally in many countries. The applicant enters their personal data in a digital application form and sends it to the university or company. Proof of qualification in the form of educational certificates is a difficult issue. These are only handed over to the applicants in printed, sealed and signed form (written form). The current method of scanning the paper document and subsequently confirming its authenticity by presenting a certified copy requires a great deal of effort from all those involved and enables fraud through the manipulation or complete forgery of documents.

This white paper describes a user-centred solution for Germany, which was developed together with users and adapted to their needs, especially with regard to usability. The proposed solution also takes into account the federal organisation of the German education system, the requirements for data protection and data security, and compatibility with existing solutions, including beyond the borders of Germany. In view of individuals' increasingly international education biographies, it underscores the importance of open standards and aims to achieve the greatest possible interoperability in the globally developing ecosystem surrounding digital educational certificates. The concept is vendor-neutral, open to participation by other institutions and designed to support different types of certificates such as school-leaving certificates, training certificates, bachelor's degree certificates, master's degree certificates, but also individual results from courses such as an Erasmus year abroad. It can also be used in the field of professional and internal further education.

The technological prerequisite for the implementation of the concept is a decentralised security system, e.g. a blockchain. This could be operated by a trustworthy consortium of public data centres.

The concept described here would act as a supplement to the current process in Germany and provide impetus for international cooperation. Certificates in written form would continue to be produced and issued as usual. In addition, a digital file that is both human- and machine-readable would be generated. Using a mathematical one-way function, the system automatically generates a checksum of the file, a so-called hash value[3], which is written in a tamper-proof blockchain together with the identity code of the issuing institution. It is not technically possible to draw any conclusions about the contents of the certificate file from the hash value. The digital certificate file is transmitted by the issuing institution via a secure channel to the student, who is responsible for storing and managing their digital certificate, as is the case in the written version. The owner of the educational certificate retains control over their data and is free to decide to whom they present their educational certificate.

[3] To the question of whether hash values e.g. of certificates allow conclusions to be drawn about personal data there is still no conclusive legal opinion or case law. A Spanish assessment can be found here https://edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf. From a technical perspective, this problem could e.g. be solvable by introducing a so-called SALT value.

During the application process, the applicant now submits the digital certificate file instead of a scan of the paper certificate. The recipient has the option to use simple technical means to check the authenticity of this file. This can be done in different ways:

- Via a secure website with an online verification service,
- Via a client program that runs on the recipient's computer,
- Via an interface (API), which can, for example, be integrated into HR systems and which performs an automatic check in the background,
- Via mobile apps, which enable the user to manage the certificates and also carry out a check.

For validation, the checksum of the certificate file is calculated in the recipient's local device. If this checksum can be found in the blockchain, the authenticity and genuineness of the file is proven beyond doubt. As additional information, the system provides the time of writing, the institution that issued the certificate and the resolution of the so-called trust chain. Using the trust chain, the user can identify which institution issued the certificate and which overarching institution issued the authorisation to issue certificates.

Another advantage for recipients of digital certificates is that processes are significantly streamlined. The automatic authentication of the digital version of the certificate means that all previous processes based on the original certificates (paper) and their officially certified versions (paper) are no longer necessary. These paper versions no longer need to be sent, presented, checked, archived or returned at any time. All associated costs for certificate holders, central university admissions offices, and later for all universities and companies are eliminated.

The electronic processing of the data contained in digital certificates is important for recipients of digital certificates. The present concept envisages embedding a machine-readable part in the digital certificate file (before the hash is generated) so that the data can be read automatically and transferred to IT systems. The concept attaches great importance to data protection, data security, and compatibility with existing standards such as OpenBadge[4] or the European certificate exchange format ELMO, which is based on the European standard CEN EN 15981 2011 EuroLMAI[5]. ELMO is being used and further developed for the digital transfer of student data in the EMREX project, for example[6].

Education can counteract global prejudice, social injustice, unemployment and hunger. Accordingly, educational qualifications, both from secondary schools and from universities, are of great importance to citizens. They prove that the holder has completed several years of (partly academic) education and training and serve as an important decision-making criterion when recruiting employees in professional contexts. Despite their great importance for the development of the holder's career, as of 2019, educational certificates are still not secured

[4] https://openbadges.org/
[5] European Learner Mobility – Achievement information (EuroLMAI)
[6] https://emrex.eu/

against forgery or manipulation or are only weakly so. In Germany and in many other countries, certificates are currently only issued in paper form.

The digitalisation of educational qualifications offers the greatest added value for all users if the emerging ecosystem is as inclusive, sustainable and open to innovation as possible. Ideally, all existing and future educational institutions should be able to interact with each other and exchange certificates. Learners, public administrations, employers and HR services would have access to secure, trustworthy, sustainably operated and user-centric validation services. Open, interoperable standards would ensure that, from the system-provider side, there is competition for the best services.

In this specific case, the concept aims to establish a system that will meet with broad acceptance by addressing the requirements of local issuers and users. Schools, for instance, should not incur any additional costs. Hence, the concept attaches great importance to compatibility with existing solutions such as the LUSD database used in Hesse and Berlin[7] and the Schild-NRW software used in North Rhine-Westphalia[8].

From an international perspective, research questions emerge that go beyond the present concept. They concern technology and educational governance. For example, it remains to be seen how the desired connectivity to the globally growing number of certificate systems can be established and maintained in a sustainable and trustworthy manner. It should also be possible to validate a certificate in 50 years' time, when the issuing educational institution may no longer exist due to crises, wars or climatic disasters, or when the infrastructure no longer operates as originally intended. To ensure that learners across world can rely on the verifiability of their digital certificates in the long term, it is important to ensure that validation services are available and the corresponding storage locations – here: blockchains – can be technically located and accessed based on the certificate alone. The questions associated with such scenarios relate to the emergent character of the technologies used as well as to the great potential of digital educational certificates for the digitally networked, global society.

3. Stakeholders and requirements

3.1. Stakeholders

The most important stakeholders, i.e. participants in the system, are:

Issuing institutions such as schools, universities and other tertiary institutions. If the system is accordingly widespread, other institutions that certify educational qualifications will also be involved, e.g. the chambers of industry and crafts, adult education centres, online educational

[7] https://www.egovschool-berlin.de/node/975
[8] https://www.svws.nrw.de/download/schild-nrw

institutions, institutions for continuing vocational training or companies that issue references to departing employees.

Certificate holders such as school students, university students or other persons issued with proof of an educational qualification. A certificate as envisaged by this concept can be a school certificate or university degree or another type of certificate.

Parties using the verification service are institutions where a certificate holder presents his or her certificate, such as universities, central application institutions or companies.

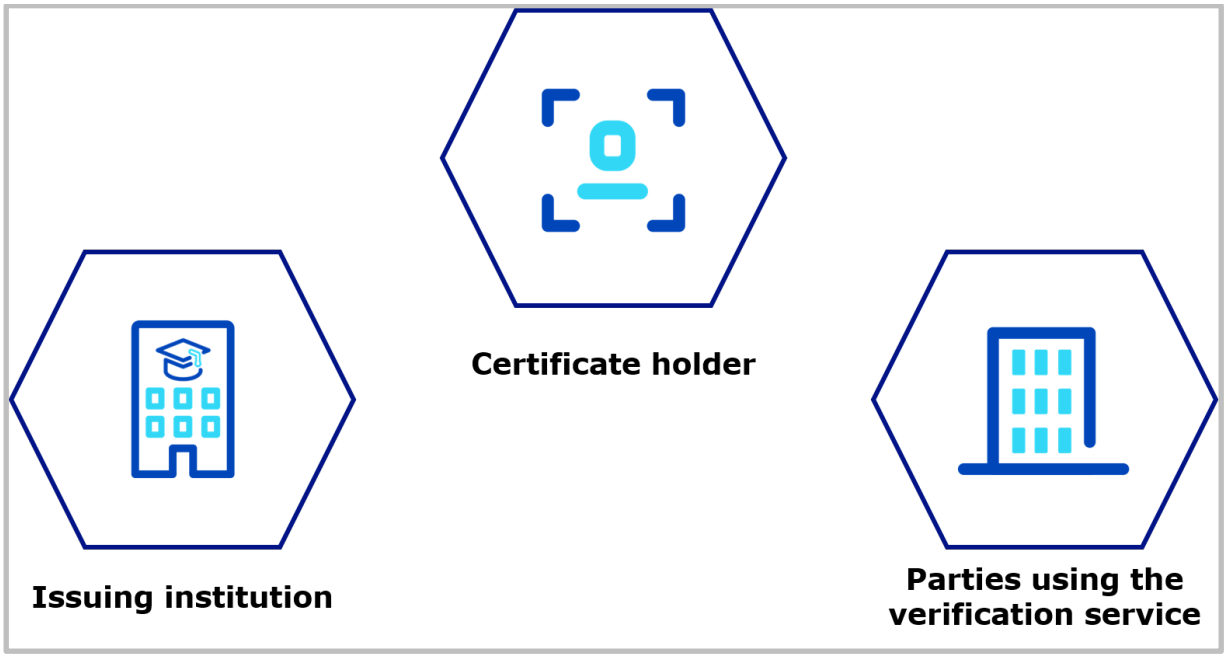

Figure 1: Stakeholders in the system

3.1.1. Issuing institutions

Role in the system	Creates certificates and distributes them to certificate holders such as school or university students
Main need	Simple creation of certificates Compatibility with existing legacy systems, if any Connection to institution's existing management system
Interactions	Uses service that creates and stores certificates

3.1.2. Certificate holder

Role in the system	Receives certificate from the issuer, stores it in a place which they control, and passes it on to participating institutions within application processes
Main need	Wishes to transmit trustworthy certificates (equivalent to the original or a certified copy) multiple times electronically without any administrative procedures
Interactions	Receives certificates, manages them independently and forwards them electronically in a self-determined way

3.1.3. Parties using the verification service

Role in the system	Receives electronic certificates from certificate holders and checks them
Main need	Digital receipt and efficient (automatic) verification and processing
Interactions	Uses a service that checks certificates, reads the data digitally and processes it

3.2. Requirements

As part of the development of the present concept, the requirements for a system to digitally exchange educational certificates were identified in discussions with users and experts in the education sector. The following list contains a selection of these requirements without claiming to be complete.

- A certificate should be able to take a number of forms (school-leaving certificate, master's degree, licence to practise medicine, official transcript of grades for a degree programme, welder's pass, certificate of further education); in federal states that do not centrally issue school-leaving certificates, certificates differ from school to school
- An applicant must have direct access to the officially verified version of the certificate in order to use it during an application
- The system must support student mobility and enable universities to exchange credit points digitally at module level
- Digital certificates should only be available to the certificate holder and to those whom they have sent the certificate to[9]
- It must be ensured that a certificate can only be used in an authorised manner by its owner; it should not be useable by other applicants
- The system should be available via the internet and work without paper; it should not be necessary to install special software
- Paper documents should be issued and used in parallel as before; they should not be necessary for the process
- The information contained in a certificate (school/university, holder, grades) should be electronically readable
- A certificate should be automatically verifiable (issuing institution, date of issue, integrity)
- Institutions that write in the system (i.e. that secure certificates by entering the checksum) must either be registered in the system and/or have a digital identity
- Reading access (checking a checksum) should be public and possible for everyone
- The system should be compatible with existing solutions and standards and can be integrated via interfaces

[9] Within the scope of legal archiving requirements, possibly also at the institution responsible for archiving. Options for electronic archiving are not considered in this concept.

3.3. Functionality of the system

3.3.1. Functionality for issuing institutions

The focus of the system is on safeguarding educational qualifications and preparing them for automatic processing in downstream processes. If not already covered by existing systems, the system can be used by authorised institutions to issue educational certificates.

The issuing institution uses a web interface (API) or a suitable exchange format (e.g. json, xml, openbadge) to import the certificate data from a school or campus administration system (e.g. LUSD or similar) or transfers it manually. If required, a human-readable file such as a PDF that contains the data file or vice versa can also be created. Via an approval workflow, this file is approved by the responsible authorities (e.g. examination board, school management). The checksum of the certificate file is then calculated and written permanently and unchangeably in a blockchain together with the unique identity of the issuing institution. The human-readable file can be printed out as usual and handed over to the certificate holder. In addition, the issuing institution transfers the digital file to the certificate holder in a secure way. The certificate data is processed on the issuing institution's client. The contents of the certificate file are not transferred at any time (security by design).

3.3.2. Functionality for certificate holders

The certificate holder (e.g. school or university student) receives a report in paper form from the educational institution as usual. In addition, they receive a digital file for their own safekeeping. This file can be opened using freely available standard software, copied digitally as often as required and saved and passed on at the holder's discretion. A change of the file name does not constitute a change of the file as understood by the security concept. The certificate holder can check the authenticity of their certificate at any time via a freely available web service. As part of application processes, the certificate holder may, at their own discretion, pass on the digital file to third parties (e.g. universities, companies) as proof of the educational qualifications they achieved.

3.3.3. Functionality for users of the verification service

Parties using the verification service (e.g. universities, central admissions services such as the Stiftung für Hochschulzulassung or companies) already receive certificates in PDF format from their applicants during the application process. The files transferred today are usually scans (images) of the paper certificates. These are susceptible to manipulation and are not suitable for automatic further processing. The files created according to the present concept represent an added value for the institutions using them, as they are of consistently high quality, can be checked for authenticity and integrity using simple technical means and can be automatically processed. Participating institutions that receive a digital certificate file can process it without installing additional software via a web service. The web service calculates the hash value belonging to the file in the user's browser without transferring the file via the internet. A query regarding the hash value in the blockchain provides direct information about the issuing

institution and the authenticity of the document. Using additional software, authorised institutions can read the certificate's machine-readable data and transfer it to downstream systems (e.g. campus management systems).

4. Architecture concept

4.1. Decentralised architecture concept

The proposed concept is based on decentralisation and an open source strategy. There is no single entity that controls the system or the blockchain.

The architecture consists of three essential parts:

Blockchain as a database

The database (blockchain) does not store any personal data; it only stores public keys, hashes[10] and references to public institutions such as schools and universities. Because it operates multiple nodes, it is fail-safe and can withstand attacks[11]. As envisaged by the authors of this white paper, the infrastructure would be operated by a consortium of municipal and public data centres. This would make it easier to secure and thus increase confidence in the system. The blockchain is private and access-protected. Certificate files are checked by certificate holders or users via the web service provided or interfaces that interact with one or more blockchain nodes. The system benefits from the known advantages of a blockchain (forgery protection, immutability, etc.) and at the same time avoids the disadvantages of completely public blockchain infrastructures (e.g. increased power consumption due to methods for building trust). The envisaged infrastructure does not offer crypto money[12] that can be used speculatively. The costs for operating the blockchain are comparable to those of other distributed IT systems.

Web client for creating certificates

Certificates are generated via a web service that can either run in the browser in the issuing institution or be integrated into an existing system via an interface. If required, the web service can be integrated into a client program. The web service can only be accessed by authorised institutions whose identity and authorisation to issue certificates has been confirmed by overarching authorities. The digital certificates created in this manner are transferred to the certificate holder securely. The current concept does not provide for the storage of the digital certificate file (either centrally or at the issuing institution). If, in the future, legislators impose requirements for the digital archiving of certificates, these can be easily implemented within the present concept.

Web service for checking certificates

A publicly accessible web service shall be provided to verify the authenticity and integrity of certificate files. This web service can be used by anyone who has a certificate file, that is, by the certificate holder themselves and all third persons and institutions to whom the certificate holder submits their digital certificate file. By presenting the file, the hash value is calculated in

[10] https://de.wikipedia.org/wiki/Kryptologische_Hashfunktion
[11] Ensuring security by implementing the recommendation of the BSI Blockchain
[12] https://de.wikipedia.org/wiki/Kryptow%C3%A4hrung

the browser and checked for its presence in the blockchain. The certificate itself does not leave the browser. While there may be various causes for the result of the checking process to be negative (hash not written in the blockchain, file manipulation, etc.), a positive result confirms without doubt the document's authenticity and integrity as well as the issuing institution.

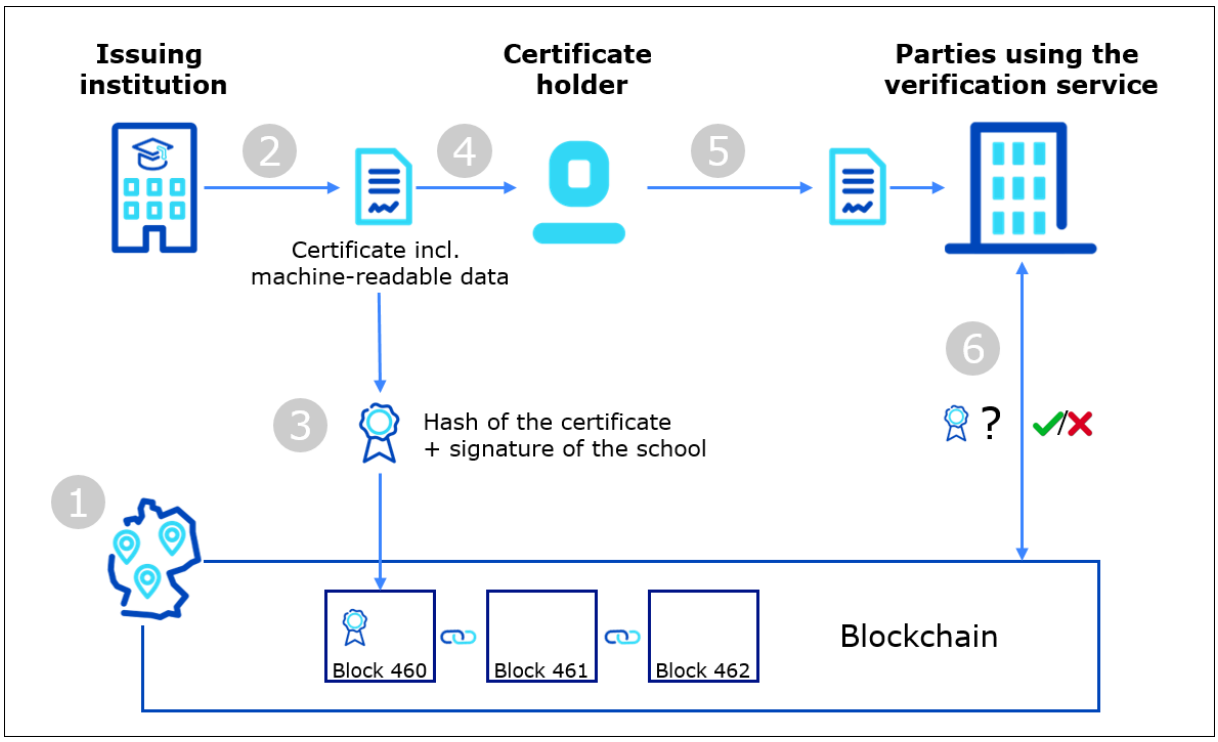

Figure 2: System architecture

Process flow

1. Trustworthy consortium based on and administered by municipal and public data centres operates a distributed infrastructure consisting of a blockchain and web services
2. Approved, authorised schools generate digital certificates. These contain the print layout of the certificate and machine-readable certificate data
3. Authorised schools write a hash value associated with the certificate together with the identity of the school in the blockchain
4. Digital certificates are securely distributed to certificate holders[13]
5. School student uses digital certificates to apply for a job on a web portal or by e-mail
6. Parties using the verification service can ensure the authenticity of the certificate via a web service for checking the certificates. This service calculates the hash of the

[13] The method for doing this remains to be specified. Different solutions are plausible, e.g. a secure download portal

certificate file and compares it with the data in the blockchain. The identity of the issuing institution is displayed.

4.2. Authorisation of issuing institutions

A central point for establishing trust in the system is the authorisation of the issuing institutions. It is important to ensure that only authorised institutions can write in the blockchain. In addition to technical security, the so-called trust chain is also important. This indicates which higher authority has authorised an issuing institution to write in the blockchain.[14]

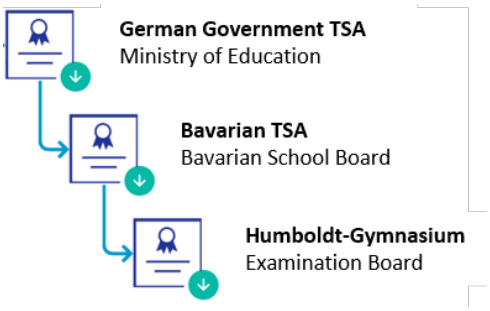

Figure 3: Example of a chain of trust

4.3. Compatibility with standards and existing systems

In order to ensure the greatest possible acceptance and dissemination of the system, great care has been taken in its design and development to ensure compatibility with existing systems and national and international standards. The following standards and initiatives have been taken into account, among others.

- EU eIDAS Regulation
- W3C Decentralised Identifiers (DIDs)
- W3C Verifiable Credentials Data Model 1.0
- OpenBadges
- Blockcerts
- PESC
- ELMO and EMREX[15];
- Erasmus without Paper
- Lehrkräfte-Unterrichts-Schul-Datenbank (LUSD)
- School Administration Programme of the State of North Rhine-Westphalia (SCHILD-NRW)

[14] A detailed conception of the authorisation procedure will be published in an updated version of this white paper.
[15] Comparison of PESC and ELMO

Initiatives

- European Blockchain Partnership
- Groningen Declaration
- StudIES+
- Digital Credentials Initiative

5. Implementation

At present, there are various prototypes that have demonstrated the technical feasibility of the system. In addition, so-called click dummies were developed as part of user-centred development and continuously tested with users in order to achieve a high degree of usability, positive user experience (UX) and system acceptance.

The existing prototypes and UX concepts can be requested from the relevant persons at Bundesdruckerei, Fraunhofer FIT, regio IT, Trustcerts and Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ).

The authors of this white paper suggest the timely implementation of a pilot project in close coordination with the politically responsible authorities and in cooperation with schools, a central university admissions office and universities.

5.1. Universal verification page

A certificate holder receives certificates issued by different verification systems. To make the verification of different certificates as easy as possible, the authors envisage a universal verification page that checks certificates from different systems. A certificate would be uploaded to this page, then the verification page would analyse the certificate and apply the corresponding method for verification and display for the system in question. In the process, specific check algorithms for the respective issues would be accessed.

Universal verification pages should be provided by trusted parent sites. Only generally accepted systems are to be offered. The user should be able to recognise which systems the verification page offers.

The verification page would be publicly accessible.

Procedure

The verification page recognises the format of the certificate, determines the appropriate test routine and uses this to perform the verification and display the results.

For these purposes, the various procedures each provide a JavaScript library that initiates a REST service offered by the respective provider and performs the verification there.

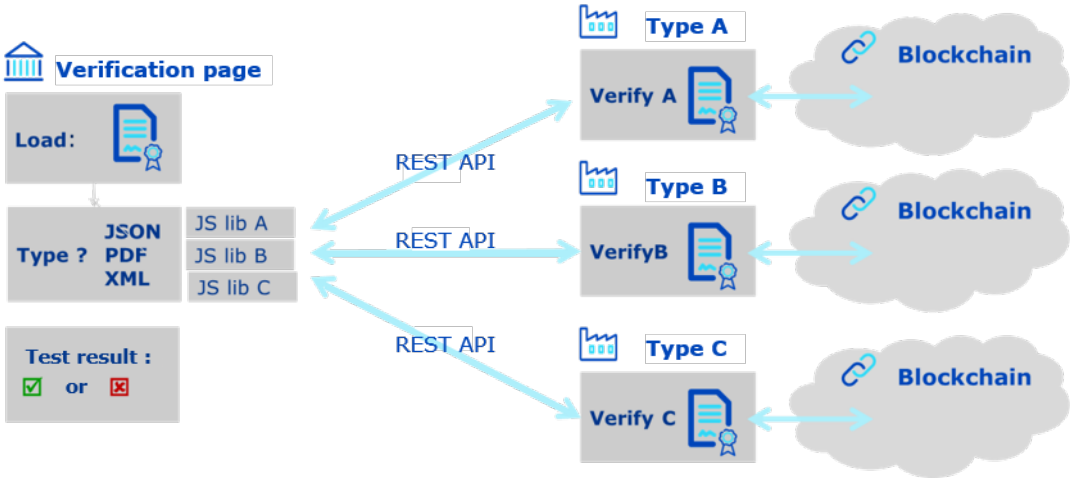

Figure 4: Structure of the verification page

Detailed description:

- **Analysis of the format, calculation and verification of the hash value**
  - **Recognition of the format**
    - Drawing on a property attribute entered in the certificate, the type of certificate is determined so that the appropriate verification routine is triggered.
    - Then, a Javascript library specific to the type is accessed via the checkCertificate() function.

  - **Calculation of the hash value**
    The Javascript library calculates the specific hash and initiates the specific verification via a Rest API.

  - **Verification of the hash value**
    The hash value is checked in the respective blockchain.

Display of the result and the certificate
The individual systems define a method that interprets the result of the verification process, generates the certificate based on the data and displays both with the displayCertificate() function.

6. Outlook

6.1. Regulatory tasks

In addition to the technical challenges, it is also important to keep an eye on the legal framework.

– Is it legally possible to issue only a digital certificate,
– Are the paper certificates and the “electronic certificate” (and copies thereof) both originals?

6.2. Technical tasks

In many areas, the concept of so-called "verifiable credentials" (VC) is currently being discussed. The webpage of the W3C Verifiable Credentials Data Model 1.0[16] provides good information about this generally applicable concept. In a future version of this white paper, we will look at how VC could be used in the education sector.

7. Participants in a cooperation project on certificate digitalisation

Coordinator of the cooperation project
CIO NRW; Ministry of Economic Affairs, Innovation, Digitalisation and Energy NRW
https://www.wirtschaft.nrw

Block Chain in Administration in Germany (BiVD)

An initiative of the federal government, the states and companies to develop essential basic infrastructure in Germany for a modern and legally compliant public administration. Together with partners from federal and state authorities, partners from industry, start-ups and institutions and initiatives throughout Europe, BiVD aims to develop a resilient, legally compliant and forward-looking infrastructure for digital public administration services.

http://bivd-initiative.de

Berlin Partner

As a unique public-private partnership, Berlin Partner für Wirtschaft und Technologie is backed by both the Senate of the State of Berlin and more than 280 companies and scientific institutions that are committed to their city. Berlin Partner is also responsible for global marketing for the German capital, for example, with the successful "be Berlin" campaign.

https://www.berlin-partner.de

Bundesdruckerei GmbH

The Bundesdruckerei GmbH offers innovative and complete IT security solutions for companies, states and authorities. With technologies and services “Made in Germany”, it protects sensitive

[16] http://www.w3.org/TR/vc-data-model/

data, communication and infrastructures. The solutions are based on the secure identification of citizens, customers, employees and systems in the analogue and digital worlds.

https://www.bundesdruckerei.de

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

As a service provider with worldwide operations in the fields of international cooperation for sustainable development and international education work, GIZ works with its partners to develop effective solutions that offer people better prospects and sustainably improve their living conditions. The GIZ Blockchain Lab provides ideas for innovative project approaches. It is currently implementing an open source pilot for forgery-proof education certificates.

http://giz.de/blockchain

German Academic Exchange Service (DAAD)

DAAD is the world's largest funding organisation for international exchanges by students and scientists. It is an association supported by German universities and student bodies. Its activities go far beyond awarding scholarships: DAAD promotes the internationalisation of German universities, strengthens scholarship in the field of German studies and the German language abroad, supports developing countries in establishing efficient universities and advises decision-makers in education, overseas science policy and development policy.

https://www.daad.de/de

Digital Business University of Applied Sciences

The DBU is a business school for the digital age, which consistently aligns its courses and research services with the digitalized business and working world. Their declared goal is to impart extensive digital skills to the students and thus prepare them for the changing professional requirements in an increasingly digital world of work.

https://dbuas.de

Fraunhofer FIT

Fraunhofer FIT has about 30 years of experience in the human-centred design of intelligent system solutions that integrate seamlessly into business processes. Our customers enjoy more efficient processes and increasing quality, better internal company networking and growing employee satisfaction. Fraunhofer FIT is your partner for digitalisation, industry 4.0 projects and solutions for the internet of things.

Fraunhofer FIT's Blockchain Lab has been working on blockchain technology and applications since 2015. It supports companies in identifying innovations and potential for efficiency improvement via blockchain and guides them in implementing them.

https://www.fit.fraunhofer.de

Institute for Applied Blockchain (IABC)

The Institute for Applied Blockchain at the Digital Business University in Berlin enables the systematic identification of blockchain-based fields of application and conveys a deep understanding in combination of science and economy. The IABC's activities focus on training and further education as well as projects to research the use of blockchain for industry and public administration.

http://www.iabc.dbuas.de

Institute for Internet Security – if(is)

The Institute for Internet Security – if(is) was founded in 2005 at the Ruhr Master School, Gelsenkirchen by Prof. Norbert Pohlmann to create innovations in the field of application-oriented internet security research. If(is) has its roots in the Department of Computer Science. Here, around 50 employees are working daily on research on solution-oriented methods for increasing internet security for all target groups – from large and medium-sized companies to the operators of critical infrastructures and end users in their everyday digital lives.

The Blockchain research group is concerned with blockchain technology as an enabler of new business models and more efficient business processes. Apart from implementing pilot projects with partners from public administration and industry, it conducts academic research with a special focus on cyber security, data autonomy and cryptography.

https://www.internet-sicherheit.de

regio IT

regio iT GmbH is the ideal IT partner for public sector clients – for municipalities and schools, energy suppliers and waste management companies as well as non-profit organisations. Based in Aachen and with a branch in Gütersloh, the company offers strategic and project-related IT consulting, integration, IT infrastructure and full service in four service areas: IT services and operation, administration and finance, energy and waste disposal, education and development.

https://www.regioit.de

Stiftung für Hochschulzulassung

Under the brand name “hochschulstart.de”, the Stiftung für Hochschulzulassung (Foundation for Higher Education Admissions) operates a service platform that provides access to degree programmes at state-recognised universities. On behalf of the federal states, the platform centrally allocates course places on nationally restricted programmes in medicine, veterinary medicine, dentistry and pharmacy via hochschulstart.de. In addition, on behalf of the universities, it coordinates the admission offers for both locally restricted and unrestricted degree programmes at well over 100 locations.

https://hochschulstart.de

Technical University of Munich (TUM)

The Technical University of Munich (TUM) is one of the best universities in Europe, regularly achieving excellent results in international and national rankings. More than 41,000 students, 30% of whom come from abroad, study at its 15 faculties. 566 professors teach and research at TUM.

TUM is ready for the challenges of the digitalisation of our society. It consistently applies the model of the “Digital University” – an efficient, secure and user-friendly information and communication infrastructure is the basis for research, teaching and administration at the highest level.

https://www.tum.de/

TrustCerts

This spin-off from the Institute for Internet Security in Gelsenkirchen seeks to develop tamper-proof decentralised systems. A specially developed blockchain system guarantees complete independence by avoiding a single point of failure or single point of control.

Several approaches have been evaluated in research and pilot projects, which considered the issue of the long-term security of sensitive data alongside usability and scaling. Using a very generalised procedure, two universities have already been able to secure their certificates digitally via the blockchain in a test phase.

https://www.trustcerts.de/

7.1. Contact person/contact

Institution	Contact person	Function	E-Mail	Telephone	Address
Ministry of Economic Affairs, Innovation, Digitalisation and Energy NRW	Helmut Nehrenheim	Consultant	helmut.nehrenheim@mwide.nrw.de	+49 211 61772 512	Berger Allee 25 40213 Düsseldorf

Block Chain in Administration in Germany (BiVD)					
Berlin Partner für Wirtschaft und Technologie GmbH	Shoshana Schnippenkoetter	Project manager for innovation in ICT	shoshana.schnippenkoetter@berlin-partner.de	+49 30 46302-106	Fasanenstr. 85 10623 Berlin
Bundesdruckerei	Eric Stange Jörg Rückriemen	Project manager Technical project manager	eric.stange@bdr.de joerg.rueckriemen@bdr.de	+49 160 979 186 25 +49 172 383 6284	Kommandantenstr. 18, 10969 Berlin
German Academic Exchange Service (DAAD)	Alexander Knoth	Senior expert digitalisation	knoth@daad.de		Büro Berlin, Markgrafenstraße 37, 10117 Berlin
Fraunhofer FIT	Prof. Wolfgang Prinz, PhD	Deputy director of the institute	wolfgang.prinz@fit.fraunhofer.de	+49 2241 142730	Schloss Birlinghoven, 53754 Sankt Augustin
Institute for Applied Blockchain	Dr. Christoph Haupenthal	Head of the institute	christoph.haupenthal@iabc.dbuas.de	+49 (0)30 40365992	Oranienstraße 185 10999 Berlin
Institute for Internet Security – if(is)	Kevin Wittek	Head of Blockchain research group	wittek@internet-sicherheit.de	+49 209 95 96 696	Neidenburger Straße 43, 45897 Gelsenkirchen
regio IT	Peter Niehues	Enterprise architect	Peter.Niehues@regioit.de	+49 241 41359-1595	Lombardenstraße 24, 52070 Aachen
Stiftung für Hochschulzulassung	Guido Bacharach	Head of Strategy and Digitalisation Unit	guido.bacharach@hochschulstart.de	+49 231 1081 – 1090	Sonnenstr. 171 44137 Dortmund
Technical University of Munich (TUM)	Dr. Hans Pongratz	Vice president / CIO	pongratz@tum.de	+49-89-289-28240	Arcisstr. 21 80333 Munich
TrustCerts	Mirko Mollik	Managing director	mollik@trustcerts.de	Office: +49 209 95 96 877 Mobile: +49 1577 600 9706	Neidenburger Straße 43, 45897 Gelsenkirchen
GIZ Lab	Franz von Weizsäcker	Head	franz.weizsaecker@giz.de	+49 151-27671669	GIZ @Impact Hub, Friedrichstr. 246, 10969 Berlin

7.2. Examples of formats

- JSON → OpenBadge fields found → B4E fields found -> Fraunhofer
- JSON → Claim data found → TrustCerts
- URL → Claim parameters found → Evaluate parameters and create claim -> TrustCerts
- PDF → QR Code found → URL
- PDF → JSON data found in attachment → JSON
- PDF → ELMO data in annex → Bundesdruckerei
- XML → ELMO data found → Bundesdruckerei

7.3. Sample process for issuing a certificate

Issuing a certificate

- The issuer (school, university, etc.) creates an account (e.g. in a system such as "Schild-NRW") and has this account authorised by a higher authority, e.g. school authorities.
  (Both the accounts and authorisation are in a blockchain)

- The issuer (school, university, etc.) records the certificate data (e.g. in a system like "Schild-NRW") and creates a certificate file in PDF format.

- The issuer transfers the PDF and certificate data (json list) to a signing component integrated in the school management system.
  The signing component checks the authorisation of the issuer and adds the Elmo xml file to the pdf and signs this file and the pdf. Then the hash is entered into the blockchain and the complete certificate is returned.

- The issuer stores the digital certificate on their electronic systems and according to data protection requirements for as long as they would have had to store an analogue certificate. The processes relating to the creation of duplicate certificates are the same as for paper certificates.
  (The BDR will develop a solution for this later)

Giving the certificate to learners (school students, university students etc.)

- The digital certificate is
  - either on a data storage device (USB stick, CD or similar) to be given to the learner personally
  - or can be downloaded by the learner from a portal within a certain period of time.

Transfer of a certificate (to a third party)

Direct transfer

- The learner sends the digital certificate as a file directly to the recipient by email or similar.

Delivery via the recipient's application portal

- The learner uses the recipient's application portal to apply there.
- In the process, the learner is asked to upload their digital certificate.
- A functionality of the application portal allows the learner to upload their digital certificate (from any data storage device).
- The application portal activates an ***external validation functionality***. This validates the digital certificate or prevents it from being uploaded.

Receipt of a certificate (by a third party)

After direct receipt

- The recipient uses an ***external validation portal*** to validate the digital certificate.
- The data is transferred manually.

After submission via the recipient's application portal

- The plain data received is read by the recipient's application portal and processed without media discontinuity.