Digitization of certificates -
with Blockchain technology

White Paper

BiVD
BUNDESDRUCKEREI
hochschulstart.de
Stiftung für Hochschulzulassung
Berlin Partner
für Wirtschaft und Technologie
DAAD
Fraunhofer FIT
regio iT
if(is)
internet-sicherheit.
TrustCerts
Technische Universität München

Contents

1. Management Summary

Several actors in the education system of the Federal Republic of Germany have set themselves the goal to digitize credentials to prevent forgery and improve efficiency of credential related processes like applications.

The present white paper summarizes the results of the previous analysis and discussion phase and is intended to validate the concept in an extended circle of schools, universities, ministries and companies and to lead to a consensus for a Germany-wide solution.

Today, certificates for school and academic degrees are issued in writing, while application processes are predominantly carried out online.

The present concept describes how, in addition to written form, certificates can be created digitally and be represented in a forgery-proof way so that its origin and integrity can be verified over a lifelong period of time. In addition, these certificates are machine-readable so that the data can be automatically transferred to downstream administrative procedures.

The concept is designed in a way that educational institutions have little extra effort in creating the additional digital certificates and that received certificates can simply be checked for authenticity by everyone.

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

The concept envisages the use of a Distributed Ledger Infrastructure (Blockchain) to register and secure the checksum of the certificates and thus guarantees the security against counterfeiting. The concept relies on open source technology to increase IT security and trust in the system. How this infrastructure is to be built is not yet finalized in the concept.

There are already several prototype implementations for testing the concept. Demonstrations can be requested from the developers (see table in chapter 6).

2. Situation and description of the concept

Application processes, both for university places and for workplaces, are generally done digital in Germany today. The applicant enters his personal data in a digital application form and transfers it to the university, the authority or the company. However, problems arise when it comes to proving the educational qualifications. Certificates from school or university will only be handed over to applicants in printed, sealed and signed form (written form). The current way of scanning the paper document and subsequently verifying the authenticity by presenting a certified copy causes a great deal of work for all those involved in the process and offers opportunities for fraud through manipulation or complete forgery of documents.

This paper describes a user-centric solution that has been developed with users and tailored to their needs, especially in terms of ease of use. The proposed solution also takes into account the federal organization of the German education system, the requirements of data protection and data security as well as the compatibility with existing solutions, even beyond the borders of Germany. The concept is manufacturer-neutral, open to participation of other institutions and designed to support different types of certificates such as Abitur (German university entrance qualification), certificate of training, Bachelor, Master as well as individual results from courses such as Erasmus stays abroad. It is also transferable to professional and in-house training applications.

The technological prerequisite for the implementation of the concept is a decentralized hedging system, eg a blockchain. This should be operated by a trusted consortium of public data centers, according to the authors.

Also in the present concept, institutions produce written testimonials for graduates. In addition, a digital file is generated, which is both human and machine-readable. The system automatically generates a checksum of the file via a mathematical one-way function, a so-called hash value, which is written tamper-proof into the blockchain together with the identity identifier of the issuing institution. Technically it is not possible to derive any conclusion on the contents of the certificate file from the hash value. The digital certificate file is forwarded by the issuing institution to the student who is responsible for the retention and management of his digital certificate, as he is for the paper version. The owner of the educational diploma keeps his sovereignty over his data and decides confidently, to whom he presents his certificate.

In the application process the applicant submits his digital certificate file. The receiver has the possibility to check the authenticity with simple technical means. This can be done in different ways:

- via a secure website offering an online testing service,
- via a client program running on the recipient's computer,
- via an interface (API), which is integrated into HR systems, for example, and performs automatic check in the background,
- via mobile apps, which on the one hand allow easy management of different certificates by the user and additionally perform an authenticity 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, authenticity and integrity of the file are proven beyond doubt. As additional information, the system provides the writing time and the institution that issued

the certificate as well as the so-called chain of trust. Through the chain of trust, the user can understand which institution has issued the certificate and which higher-level institution has granted the right to issue certificates.

Another advantage for recipients of digital certificates are greatly streamlined processes. Thanks to an automatic authentication of the digital certificate version, all previous processes are completely superfluous on the basis of the original certificates (paper) and their attestations (paper). These paper versions no longer need to be submitted, presented, reviewed, archived or returned. All associated costs will be eliminated for the certificate holders, the central contracting points for study places and later for all universities and companies.

For recipients of digital certificates, the electronic processing of the data contained is important. 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 automatically read out and transferred to IT systems. The concept attaches great importance to data protection, data security and compatibility with existing standards such as OpenBadge[1] or the European certificate exchange format ELMO, which is based on the European standard CEN EN 15981 2011 EuroLMAI[2] . For example, ELMO is used further developed for the digital transfer of student data in the EMREX project[3].

Educational qualifications, especially university degrees, are very important to citizens. They prove the completion of many years of academic education and serve in professional context as an important decision criterion for the hiring of employees. Despite their great importance for the development of their carrier's career, educational qualifications in 2019 are still not or only weakly secured against counterfeiting or manipulation. The obvious solution of digitally signing testimonials has not been widely accepted in the past. Distributing and administering signing certificates is only possible for larger IT-enabled entities and is difficult to implement, especially for small, resource-constrained schools.

The greatest value for all stakeholders is added by a system for the digital exchange of educational qualifications, if as many as possible, ideally all, educational institutions work with the system. The prerequisite for this is that the system reaches a broad consent by addressing requirements of schools, universities and companies equally and, in particular on the part of schools, does not cause any additional expenses. In this sense, the concept attaches great importance to compatibility with existing solutions.

[1] https://openbadges.org/
[2] European Learner Mobility - Achievement Information (EuroLMAI)
[3] https://emrex.eu/

3. Stakeholders and requirements

3.1. Stakeholders

Stakeholders, ie those involved in the system, are essentially:

Issuing institutions such as secondary schools, universities, or even the chambers of industry and craft. With greater dissemination of the system also adult education centers, online educational institutions, institutions for professional training or companies issuing employment certificates.

Certificate holders such as pupils, students or other persons who get a certificate for their academic achievements. A certificate in the sense of the concept can be a school or university certificate or another certificate.

Applicant institutions are institutions in which a certificate holder submits his / her certificate, such as universities, central application institutions or companies.

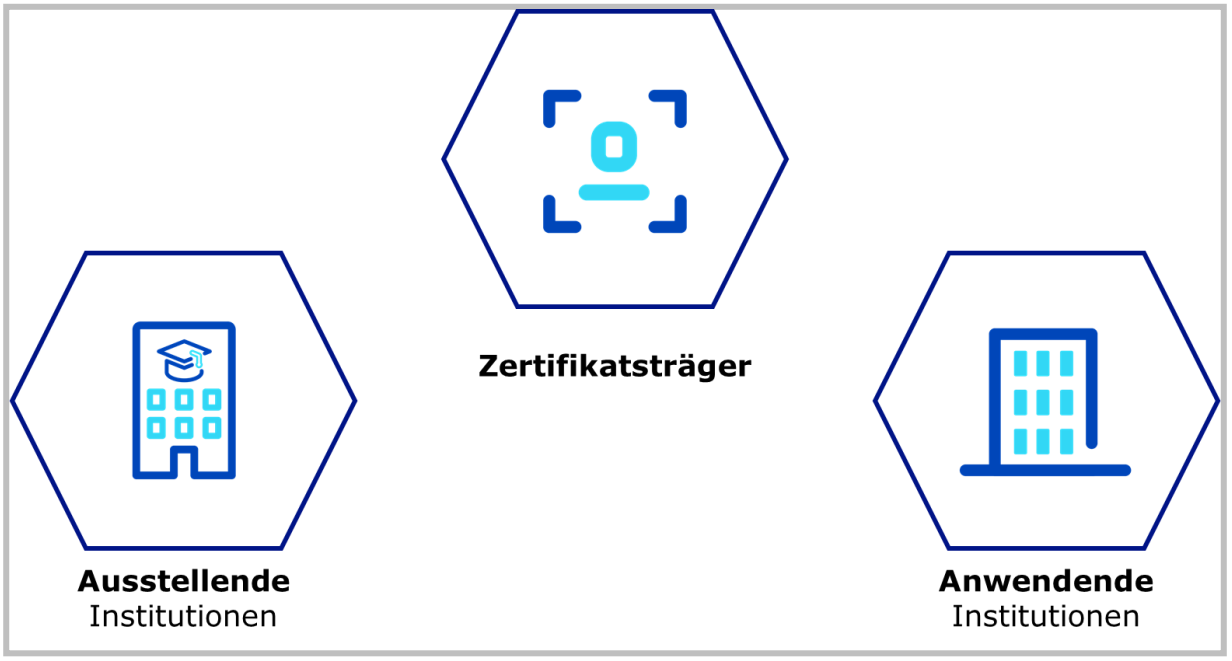

Figure 1: Stakeholders in the system

3.1.1. Issuing institutions

Task in the system	Generates certificates and distributes them to certificate holders such as pupils or students
Main need	Simple generation of certificates If legacy system exists, import via interface Connection to existing management system of the institution
Interactions	Usees service which generates and seals certificates

3.1.2. Certificate Holder

task in the system	receives certificates from issuing institution and forwards these to applying institution
main need	Wants to use trusted certificate (equivalent to the original or certified copy) without administrative procedures electronically several times
interactions	receives certificates, manages them independently and uses them sovereign

3.1.3. Applying Institutions

task System	Receives electronic certificates from certificate holders and checks them for authenticity
main needs	Digital reception and efficient (automatic) testing and processing
Interactions	Uses service the checks certificates for authenticity, reads out the data digitally and transfers it to another system

3.2.Requirements

- Certificates may vary in form (high school diploma, certification, performance records course in the study, operator pass, training certificate)
- The system supports student mobility and allows universities a digital exchange of credits at the module level
- certificates are stored only by the creator, the student and those to whom the student has sent the certificate
- The system should be available over the Internet and work without paper. The installation of special software is not necessary.
- Paper documents can be issued and used in parallel as before. However, they are not necessary for the process.
- The data of the certificate (school/ university, owner, grades) is electronically readable.
- A certificate can be checked automatically by a machine.
- Institutions writing to the system (securing credentials by entering the checksum) must either be registered in the system and / or have a digital identity.
- Read access (checking a checksum) is public and available to everyone
- The system is compatible with existing solutions and standards.

3.3.Functionality of the system

3.3.1. Functionality for issuing institutions

The issuer

- Selects a suitable certificate for which he is authorized to issue (eg Abitur)
- Fills in the form of certificate data (student name and results) via a web interface or a special client software.
- The web interface or client software can be connected via APIs or exchange formats (cvs, json) with school or campus management systems
- can create one or many certificates

A paper document and a certificate file are created during the process. Their checksum is stored with the identity of the issuing institution in the blockchain to ensure integrity of the certificate.

The certificate remains with the Issuer and is never uploaded to the internet. (Security by Design)

3.3.2. Certificate holder

The certificate holder

- Receives the certificate as a file from the Issuer
- Can digitally copy and save the certificate as often as desired
- Passes the certificate to other institutions if required (application)
- Can examine the certificate with the same mechanisms if interested, as well as the applying institutions.

3.3.3. Applying institutions

The applying institution

- receives certificate(s) from the certificate holder
- Can check the integrity of the certificate vie a webservice without the need to install additional software
- Can display the printed image of the certificate
- Can export the machine-readable data of the certificate into different systems (eg in a Campus Management System)

4. Architecture concept

4.1. Decentralized architecture

The proposed concept focuses on decentralization and open source. There is no single place that controls the system or blockchain.

The architecture consists of three main parts:

- **Block Chain as a database**
  - the database (block chain) does not store any personal data but only public key, hashes[4] and references to public institutions such as schools and universities.
  - The blockchain is fail-safe by operating multiple nodes and has been thoroughly hardened against attacks.
  - It is operated by a consortium of municipal and public data centers . It is private and access protected.
  - The system benefits from the well-known advantages of a blockchain (fake security, immutability, etc.).
  - This blockchain does not provide any crypto currency[5] that can be used speculatively.
  - The costs of running the blockchain are comparable to those of other distributed IT systems.
- **Webclient for generating certificates**
  - The generation of the certificates takes place in a Webclient, ie in the browser of the creator.
  - This webclient is only accessible by authorized schools.
  - The certificate is directly handed over to the certificate holder and is not stored centrally anywhere.
  - Alternatively, a client software can be used.
  - The system should also offer an API for integration into legacy systems.
- **Web Service for checking certificates**
  - This web service can be used by anyone who has a certificate file.
  - By showing the file, the hash value is calculated in the browser and compared with the blockchain. The certificate does not leave the browser. The identity of the school is displayed with metadata

[4] https://de.wikipedia.org/wiki/Kryptologische_Hashfunktion
[5] https://de.wikipedia.org/wiki/Kryptow%C3%A4hrung

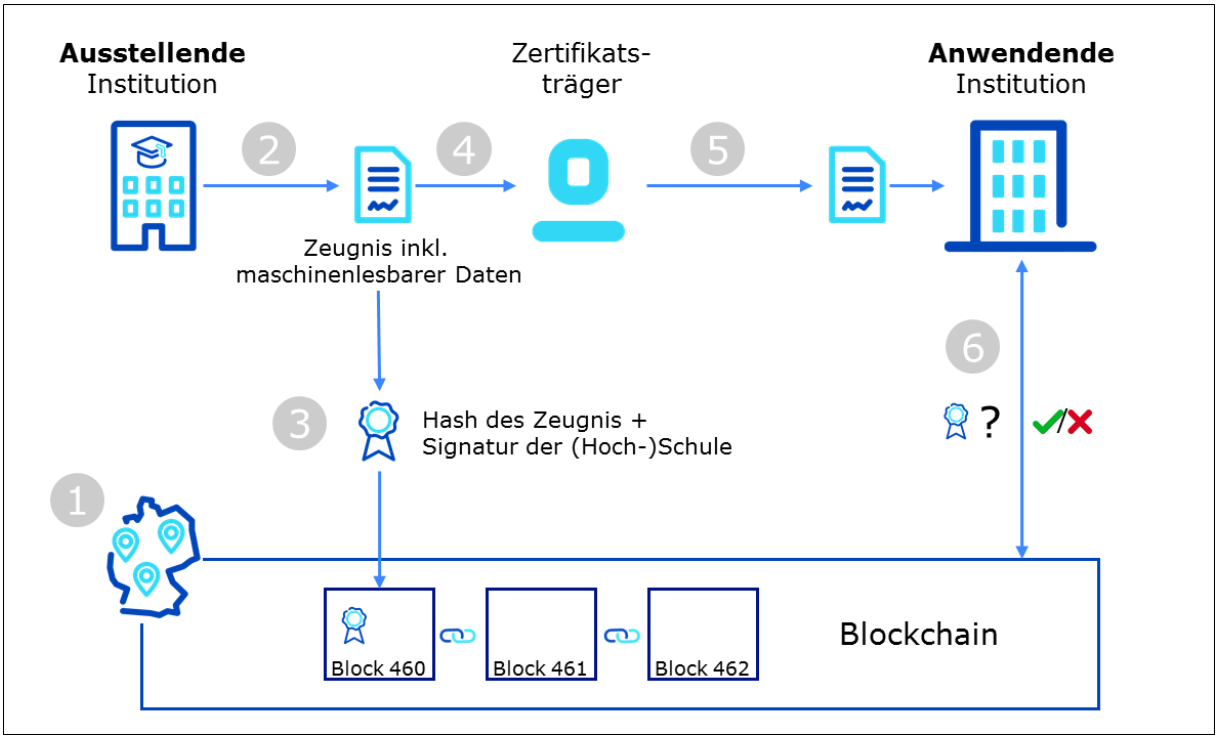

Figure 2: System Architecture

Process Flow

1. Trusted consortium based and sponsored by municipal and public data centers operates a distributed infrastructure consisting of a blockchain and higher level web services

2. Authorized schools issue digital credentials. These include the printed image of the certificate and machine-readable credentials

3. Authorized schools write a hash value associated with the certificate and sign with the school's identity in the blockchain.

4. Digital credentials are distributed to students (path to be specified).

5. Student uses digital certificate to apply in a portal or by mail.
   If a portal is used, the portal can read and process the machine-readable data of the certificate.

6. Companies can ensure the authenticity of the certificate by using a web service to verify the certificates. This service will calculate the hash of the certificate file and compare it to the data in the blockchain. The identity of the school is displayed.

7. German citizens can use foreign application services that support an EMREX client installation, to upload their certificates to the application process. For EMREX a server installation with the above-mentioned functions has to be created as a so-called "National Contact Point" (NCP).

4.2. Authorization of issuing institutions

A central point for establishing trust in the system is the authorization of the issuing institutions. It must be ensured that only authorized institutions can write to the blockchain. In addition to technical backups, the so-called chain of trust is important. This indicates from which higher-level instance an issuing institution was authorized to write to the blockchain.

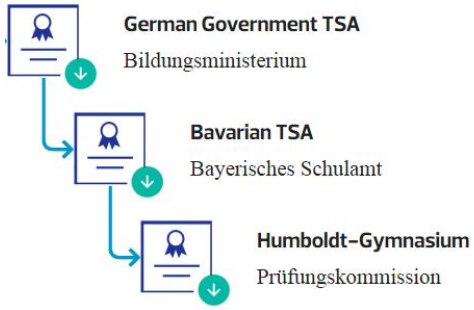

Figure 3: Example of a chain of trust

The technical implementation of authorization is done as follows:

[...]

4.3.Advantages and disadvantages of the concept

The following grafik shows a comparison of the herein described decentralized solution (right column) with a possible central solution

	Zentrale Lösung	Dezentrale Lösung
Vertrauen	… entsteht durch vertrauenswürdige Wurzelinstanz und Vergabe von Berechtigungen	… entsteht durch Technologie selbst
	- Einsatz bewährter EIDAS Mittel (Zertifikate, Siegeln) und Vertrauen über europäische Standards und Zertifizierungen	- Blockchain Technologie verbindet einfache Handhabung, niedrige Kosten und hohe Sicherheit[1] - Privacy by Design, Zeugnisinhalte verlassen den Browser der Schule nicht, lediglich Hashwerte werden in Blockchain gespeichert - Monetarisierung des Systems lässt sich nach Bedarf festlegen, z.B. Gebühr für Verifikation - Kein zentraler Anbieter kontrolliert das System - Selbstbestimmung der Weitergabe des dig. Zeugnisses durch Inhaber
	- Zentraler Angriffspunkt (mind. Accountdaten, ggf. Zeugnisse werden zentral verwaltet) - Schwieriges Verfahren zur Identifizierung der Lehrer, sichere Verteilung der Zertifikate an legitimierte Lehrer aufwendig - Kosten entstehen auf falscher Seite. Bei Ausstellung wird Signatur auf Zeugnis aufgebracht und Kosten verursacht, spätere Prüfung ist durch jeden kostenfrei möglich	- ggf. aufwändige Abstimmungen im Konsortium, Beschlüsse über Eigenschaften und Regeln des Systems müssen gemeinsam gefällt werden

1: Bearing Point

Figure 4: advantages and Disadvantages

A central solution with signed PDF files has been technically possible for many years. This has not been established until now, among other things, because the creation and distribution of certificates for a large number of schools such as high schools is difficult to carry out.

5. Implementation

There are currently several prototypes.

Prototype:

- Prototype Bundesdruckerei
- Prototype Fraunhofer FIT (website, test system)
- Prototype of the regio iT
- Prototype TrustCerts

These will be extended, tested and made available In

2019, the determination of the architecture and the interfaces is aimed at.

In 2020, pilot tests will be sought with several types of certificates and educational institutions.

6. Other solutions

International standards and initiatives will be taken into account in further implementations.

These include:

- W3C Verifiable Credentials Data Model 1.0 (https://www.w3.org/TR/vc-data-model/)
- OpenBadges (https://openbadges.org/), 2011 by Mozilla with financial support from the MacArthur Foundation and a network of partners, since 2017 coordination of further development by IMS Global Learning Consortium.
- Blockcerts (https://www.blockcerts.org/) relies on OpenBadges, initially only Bitcoin Blockchain, now also Etherum possible. Process graphics https://www.blockcerts.org/guide/. Open source software is used by some companies worldwide for their own solutions.
- Possibly. PESC
- ELMO and EMREX; 2017 PESC and ELMO comparison https://confluence.csc.fi/display/EMREX/Comparing+PESC+to+ELMO
- EWP (Erasmus without Paper)

Identity

- Management EU eIDAS Regulation
- W3C Decentralized Identifiers (DIDs) (https: // w3c -ccg.github.io/did-spec/)
- If necessary https://identity.foundation/
- In the university area eduGain of Géant (world-wide federated IdM)
- if necessary. Shibboleth

Initiatives

- Groningen Declaration https://www.groningendeclaration.org/
- Digital Credentials Initiative https://digitalcredentials.mit.edu/

A number of comparable solutions already exist, which are briefly presented here.

System	Blockchain	Certificate representation in Blockchain	Certificate repre-sentation	Learner must be registered Blockchain user	Community. Provider Model
Blockchain in Education Fraunhofer FIT	Ethereum public Quorum private	#OpenBadge and metadata eg validity [date]	Open Badge	No	Community
Blockcerts	Bitcoin, Ethereum public	#OpenBadge and metadata eg status [expired, revoked]	Open Badge	Yes	Provider
Diplo-Me	Quorum; or any open permission Blockchain	Data and metadata encrypted by CA and then encr. by learner	JSON format; ontology for qualifications	Yes	providers
bestr Digital Credentialing System	Ethereum public	need clear, probably similar to Blockcerts	Open Badge	No, probably	provider
CVtrust	Centralized certificate repository, block chain as add on		proprietary format		provider
BCDiploma	Ethereum public	AES 256 (Certificate)	Proprietary format	No	provider

7. concerned to the Cooperation in the Digitalization of Certificates

Blockchain in the Administration

An initiative of the federal government, federal states and companies to develop essential basic infrastructure in Germany, for a modern and legally compliant administration. Together with partners from federal and state authorities, industry partners, startups and institutions and initiatives throughout Europe, the BiVD wants to develop a robust, legally compliant and future-oriented infrastructure for digital administration services.

Berlin Partner

As a unique public-private partnership behind Berlin Partner for Business and Technology stand both the Senate of the State of Berlin and more than 280 companies and scientific institutions that are committed to their city. In addition, Berlin Partner is responsible for worldwide marketing for the German capital, for example with the successful "be Berlin" campaign.

Bundesdruckerei

Bundesdruckerei GmbH offers innovative and complete IT security solutions for companies, states and public authorities. With technologies and services "Made in Germany" it protects sensitive data, communication and infrastructures. The solutions are based on the secure identification of citizens, customers, employees and systems in the analog and digital world.

German Academic Exchange Service

The DAAD is the world's largest funding organization for the international exchange of students and scientists. It is supported by the German universities and student bodies as an association. Its activities go far beyond the awarding of scholarships: The DAAD promotes the internationalization of German universities, strengthens German studies and the German language abroad, supports developing countries in setting up high-performing universities and advises decision-makers in education, outdoor science and development policy.

Fraunhofer FIT

Fraunhofer FIT has around 30 years of experience in the humane design of intelligent system solutions that integrate seamlessly into business processes. Our customers benefit from more efficient processes while increasing quality, internal company networking and employee satisfaction. Fraunhofer FIT is your partner for digitization, Industry 4.0 projects and solutions in the Internet of Things.

The Blockchain Laboratory of Fraunhofer FIT has been working on blockchain technology and applications since 2015. It supports companies in identifying innovations and efficiency enhancement potentials through Blockchain and supports their realization.

Institute for Internet Security

The Institute for Internet Security - if (is) was founded in 2005 at the Westfälische Hochschule, Gelsenkirchen by Prof. Norbert Pohlmann to create innovations in the field of application-oriented Internet security research. The if (is) has its roots in the Department of Computer Science. Every day, about 50 employees work on research into solution-oriented methods for increasing Internet security for all target groups - from large corporations and SMEs to operators of critical infrastructures to end users in their daily digital lives.

The blockchain research group is engaged in blockchain technology as the enabler of new business models and more efficient business processes. Aside from implementing pilot projects with public administration and industry partners, she conducts academic research with a particular focus on cybersecurity, data autonomy and cryptography.

regio IT

The regio iT GmbH is the ideal IT partner for public clients - for municipalities and schools, energy suppliers and waste disposal companies as well as non-profit organizations. Based in Aachen and based in Gütersloh, the company offers strategic and project-related IT consulting, integration, IT infrastructure and full-service in four service areas: IT service and operations, administration and finance, energy and waste disposal, education and development.

Foundation forUniversities

Admission toThe Foundation for Admission to Universities (SfH) is a public law foundation under public law in Germany with the task of "supporting the universities that use the Foundation in the implementation of admission procedures" as well as for courses of study in the central allocation procedure "to award places for the first semester at public universities in competitions.

Technische Universität München

The Technical University of Munich (TUM) is one of the best universities in Europe, and regularly performs excellently in international and national rankings. More than 41,000 students study at their 15 faculties, 30% of them from abroad. 566 professors teach and research at the TUM.

The TUM faces the challenges of digitizing our society. It consistently implements the leitmotif 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.

TrustCerts

The spin-off company from the Institute for Internet Security in Gelsenkirchen deals with the development of manipulation-proof decentralized systems. A specially developed block chain system guarantees complete independence by avoiding a Single Point of Failures or Single Point of Controls.

In research and pilot projects several approaches could be evaluated, whereby beside the user friendliness and scaling the point long-term security of sensitive data was considered. By a very generalized procedure already two universities could secure their certificates digitally over the blockchain in a test phase.

Contact person / contact

Institution	Contact person	Function	E-Mail	Phone	Address
Blockchain in the administration	Helmut Nehrenheim		helmut.nehrenheim@mwide.nrw.de	+49 (0) 211 61772 512	Ministry of Economic Affairs, Innovation, Digitization and Energy NRW 40213 Düsseldorf
Berlin Partner for business und Technologie GmbH	Shoshana Schnippenkoetter	Project Manager Innovation in the field of ICT	shoshana.schnippenkoetter@berlin-partner.de	+49 30 46302-106	Fasanenstr. 85 | 10623 Berlin | Tel.
Bundesdruckerei	Eric Stange Jörg Rückriemen	Project Manager Technical Project Manager	eric.stange@bdr.de joerg.rueckriemen@bdr.de	Mobile: +49 (0) 160 979 186 25 Mobile: +49 (0) 172 383 6284	Kommandantenstr. 18, 10969 Berlin
German Academic Exchange Service	Alexander Knoth (Katrin Haufe-Wadle)		knoth@daad.de (haufe@daad.de)		
Fraunhofer FIT	Prof. Wolfgang Prinz, PhD	Deputy Director	wolfgang.prinz@fit.fraunhofer.de	Office: +49 2241 142730	Schloss Birlinghoven, 53754 Sankt Augustin
Institute for Internet Security	Kevin Wittek	Head of Research Unit Blockchain	wittek@internet-sicherheit.de	+49 (0) 209 95 96 696	Neidenburger Straße 43, 45897 Gelsenkirchen
regio IT	Peter Niehues	Enterprise Architect	Peter.Niehues@regioit.de	Office +49 241 41359-1595	Lombardenstraße 24, 52070 AachenAdmission
Foundation forto Universities	Guido Bacharach	Head of Department Strategy and Digitization	guido.bacharach@hochschulstart.de	Tel .: 0231 1081 - 2270	Sonnenstr. 171 44137 Dortmund
Technical University of Munich (TUM)	Dr. Hans Pongratz	Vice President / CIO	pongratz@tum.de	+ 49-89-289-28 240	Arcisstr. 21 80333 Munich
TrustCerts	Mirko Mollik	Managing Director	mollik@trustcerts.de	Office: +49 (0) 209 95 96 877 Mobile: +49 (0) 1577 600 9706	Neidenburger Straße 43, 45897 Gelsenkirchen